NEC

GVT-245343-001-00 1.9

QX-W2300AC シリーズ アクセスコントローラ

オペレーションマニュアル

改版履歴

版数	日付	改版内容
1.0	2024/08	初版発行
1.1	2024/08	・「18-謝辞」を更新しました。
1.2	2024/11	・「06-WLAN アクセス」の「1 章 WLAN アクセス」の「AP へのコンフィグレーションファイルの設定」の説明を更新しました。 ・「12-WLAN アドバンスド機能」の「3 章 IoT 機能の設定」に以下のコマンドに関する記載を追加しました。 **・rfid-tracking mode** **・rfid-tracking radio** **・display wlan rfid-tracking radio** ・誤記訂正
1.3	2025/03	・「09-無線管理」の「1 章 無線管理の設定」を更新しました。

版数	日付	改版内容
1.4	2025/09	・「01–ライセンス管理」の「3 章 AP ライセンス同期」にクラウドクラスタとデュアルリンクバックアップ併用不可の注記を追加しました。 ・「03-システム管理」の「1 章 装置管理」に「装置の特定」と「LED の点滅開始」の記述を追加しました。 ・「03-システム管理」の「5 章 Information Center」に「キープアライブログ送信の設定の有効化」を追加しました。 ・「06 WLAN アクセス」の「1 章 WLAN アクセス」 **display wlan client** コマンドの **frequency-band 6** のパラメータをサポートしました。 ・「07-AP 管理」に「2 章 コンフィグレーションプロファイルの設定」の章を追加しました。 ・「09-無線管理」の「1 章 無線管理の設定」の「802.11g 保護の設定」と「802.11n 保護の設定」に 802.11abe と 802.11gbe での利用に関するメモ書きを追記しました。 ・「09-無線管理」の「1 章 無線管理の設定」の「6GHz 帯の無線の設定」の「6GHz 帯無線サービス検出の設定」に 6GHz 無線を使用した 6GHz 無線サービス検出の記述を追加しました。 ・「09-無線管理」の「1 章 無線管理の設定」に「マルチ BSSID の設定」を追加しました。 ・「09-無線管理」の「1 章 無線管理の設定」の「6GHz 帯の無線の設定」の「サービステンプレートの設定」に 6GHz 帯の無線での WPA3 パーソナル(optional)と 192bit セキュリティなしの WPA3 エンタープライズの利用に関する記述を追加しました。 ・「12-WLAN アドバンスド機能」の「1 章 WLAN 最適化」に「AP のトラフィックスケジューリングモードの設定」を追加しました。 ・「12-WLAN アドバンスド機能」に「4 章 HotSpot2.0 の設定」の章を追加しました。 ・「14–高可用性」の「1 章 WLAN 高可用性」にクラウドクラスタとデュアルリンクバックアップ併用不可の注記を追加しました。 ・「14–高可用性」の「3 章 クラウドクラスタ」にクラウドクラスタとデュアルリンクバックアップ併用不可の注記を追加しました。 ・「18-謝辞」を更新しました。 ・誤記訂正
1.5	2025/10	・「07-AP 管理」の「1 章 AP 管理」に W2300AC シリーズアクセスコントローラで管理可能な AP モデル、動作モードの説明を追加しました。

版数	日付	改版内容
1.6	2026/02	・「05-ネットワーク接続」の「2 章 リンクアグリゲーション」の「リンクアグリゲーションモード」のメモ欄を削除しました。 ・「05-ネットワーク接続」の「10 章 Proxy ARP」の「ネットワーク要件」の説明を修正しました。 ・「08-WLAN セキュリティ」の「1 章 WLAN セキュリティ」の「管理フレーム保護の設定」の設定例を修正しました。 ・「13-ユーザアクセスと認証」の「3 章 AAA」の「RADIUS 属性」の一般的に使われる標準 RADIUS 属性の表を修正しました。 ・「14-高可用性」の「3 章 CloudCluster」の「3.1 クラウドクラスタについて」のメモ欄を修正しました。 ・「14-高可用性」の「3 章 CloudCluster」の「メンバデバイスの物理クラスタからの離脱」の説明を修正しました。
1.7	2026/04	・「03-システム管理」の「5 章 Information Center」に「キープアライブログ送信の設定の有効化」のデフォルト値の記載を更新しました。 ・「04-インタフェース」に「4 章 マネジメント Ethernet インタフェース」の章を追加しました。 ・「08-WLAN セキュリティ」の「1 章 WLAN セキュリティ」の「Enhanced Open システム認証の設定」をサポートしました。 ・「08-WLAN セキュリティ」の「1 章 WLAN セキュリティ」の「移行モードでの推奨サービステンプレートの指定」をサポートしました。 ・「09-無線管理」の「1 章 無線管理の設定」に Enhanced Open システム認証のサービステンプレート利用に関する記述を追加しました。 ・「09-無線管理」の「1 章 無線管理の設定」の「6GHz 帯の無線の設定」の「サービステンプレートの設定」に 6GHz 帯の無線で WPA3 パーソナル(optional)と 192bit セキュリティなしの WPA3 エンタープライズを利用した場合の内部動作の説明を追記しました。 ・「09-無線管理」の「1 章 無線管理の設定」の設定例に、「6GHz 帯の無線(Enhanced Open)の設定例」と「6GHz 帯の無線(WPA3 エンタープライズ 192bit セキュリティなし)の設定例」を追加しました。 ・「12-WLAN アドバンスド機能」の「3 章 IoT 機能の設定」に BLE 機能の利用に関する記述を追加しました。 ・「13-ユーザアクセスと認証」の「3 章 AAA の設定」に「EAP プロファイル追加」と「Radius サーバ追加」を追加しました。 ・「17-ネットワーク管理と監視」の「10 章 NetMeister の設定」「NetMeister を利用するための設定」に、イベントログ(syslog)の送信を無効化する手順を追加しました。 ・「18-謝辞」を更新しました。 ・誤記訂正

版数	日付	改版内容
1.8	2026/07	・「06-WLAN アクセス」の「1 章 WLAN アクセス」の SSID ステルスに、6GHz 無線に関する注記を追加しました。 ・「08-WLAN セキュリティ」の「2 章 WIPS の設定」に、無線通信と WIPS センサの併用に関してメモを追加しました。 ・「10-WLAN ローミング」の「2 章 WLAN ローミングの設定」に、「802.11k の設定」を追加ました。 ・誤記訂正
1.9	2026/11	・「02-基本機能」の「1 章 CLI の概要」に、コマンド履歴バッファの管理と使用について記載しました。 ・「03-システム管理」の「3 章 ハードウェアリソース管理」に、トランシーバの診断を追加しました。 ・「03-システム管理」の「5 章 Information center」で、ログファイルへのログの保存、およびログの最小記録期間の設定の説明を修正しました。 ・「05-ネットワーク接続」の「5 章 STP」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** ・「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** ・「08-WLAN セキュリティ」の「2 章 WIPS」の、分類ポリシーの設定にメモを追加しました。

Copyright © NEC Corporation 2024-2026

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-W2300AC シリーズアクセスコントローラ 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-W2300AC シリーズアクセスコントローラ 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 9.4.x 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-W2300AC シリーズアクセスコントローラに関する詳細な説明があります

マニュアル	内容
QX-W2300AC シリーズアクセスコントローラ 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-W2300AC シリーズアクセスコントローラ 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-W2300AC シリーズアクセスコントローラ 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-W2300AC シリーズアクセスコントローラ 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。
QX-W シリーズ Web 認証(ポータル認証) オペレーションマニュアル	QX-W シリーズ の Web 認証 (ポータル認証)に関する設定について説明しています。
QX-W シリーズ Web 認証(ポータル認証) コマンドマニュアル	QX-W シリーズ の Web 認証 (ポータル認証)に関するコマンドについて説明しています。

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。

- **ライセンス管理**

  ライセンス管理の設定について説明します。

- **基本機能**

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

- **システム管理**

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

- **インタフェース**

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

- **ネットワーク接続**

  ARP、IP アドレス（IPv4）、DHCP 関連機能、IP パフォーマンスといった、ネットワークプロトコル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。

- **無線管理**

  ロードバランス、RRM などの無線管理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 トラフィック最適化**

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

- **WLAN アドバンスド機能**

  WLAN メッシュ、IoT 機能の設定について説明します。

- **ユーザアクセスと認証**

  WLAN 認証などの設定について説明します。

- **高可用性**

  Track、クラウドクラスタの設定について説明します。

- **セキュリティ**

  ACL、AAA、RADIUS、SSH 等の設定について説明します。

- **QoS**

  QoS の設定について説明します。

- **ネットワーク管理と監視**

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

- **謝辞**

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。

表記規則	説明
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 18 個のセクションで構成されています。

01 - ライセンス管理

02 - 基本機能

03 - システム管理

04 - インタフェース

05 - ネットワーク接続

06 - WLAN アクセス

07 - AP 管理

08 - WLAN セキュリティ

09 - 無線管理

10 - WLAN ローミング

11 - WLAN トラフィック最適化

12 - WLAN アドバンスド機能

13 - ユーザアクセスと認証

14 - 高可用性

15 - セキュリティ

16 - QoS

17 -ネットワーク管理と監視

18 - 謝辞

QX-W2300AC シリーズ アクセスコントローラ

オペレーションマニュアル

1. ライセンス管理

本マニュアルは以下に示す章で構成されています。

01-ライセンス管理

02-ローカルライセンス

03-AP ライセンス同期

目次

このセクションのページは **1-x-x** です。

1 章 ライセンス管理 1-1
1.1 ライセンス 1-1
1.2 ライセンスタイプ 1-1
1.3 基本概念 1-1
1.4 制限とガイドライン 1-2
1.4.1 一般的な制限とガイドライン 1-2
1.4.2 異なるデバイスタイプのライセンス 1-3
1.4.3 ライセンスファイルの安全性 1-3
1.5 ライセンスの適用 1-3
1.5.1 ライセンスの新規適用 1-3
1.5.2 ライセンスの移植適用 1-4

1章 ライセンス管理

1.1 ライセンス

ライセンスベースの機能を使用するには、NEC からライセンスを購入し、ライセンスをインストールする必要があります。

ライセンスベースの機能、ライセンスステータス、およびライセンスの可用性に関する情報を取得するには、装置で **display license feature** コマンドを実行します。その後、必要に応じてライセンスを購入してインストールできます。

1.2 ライセンスタイプ

ライセンスは、永久ライセンスです。

ライセンスは、管理するアクセスポイントの台数により、以下のタイプが入手可能です。

- アクセスポイント 1 台用ライセンス
- アクセスポイント 8 台用ライセンス
- アクセスポイント 64 台用ライセンス
- アクセスポイント 256 台用ライセンス

ライセンスは複数適用することが可能です。例えば、アクセスポイント 8 台追加したい場合は、8 台用ライセンスを 1 つ購入します。72 台追加したい場合は、8 台用ライセンスを 1 つ、64 台用ライセンスを 1 つ購入します。

 装置限定－ラインセンスは、特定 DID 装置にのみインストールできます。誤った装置へのライセンス新規適用を行った場合、および装置の故障時は、該当装置と同じ型番の別装置にライセンスを移植適用することが可能です。

1.3 基本概念

以下の情報では、ライセンス登録、インストール、および管理を行う際に発生する可能性のある基本的な概念について説明します。

I. NEC ライセンス管理プラットフォーム

NEC ライセンス管理プラットフォームは、NEC のお客様に製品ライセンスサービスを提供します。このシステムにアクセスして、ライセンスのアクティベーション情報を取得したり、ライセンスを転送したり、アンインストールされたライセンスの装置とライセンスのバインドを削除したりできます。

NEC ライセンスサーバには、https://www.qx-info.com/License からアクセスできます。

II. ソフトウェアライセンス証明書

ソフトウェアライセンス証明書により、ユーザはライセンスベースの機能を使用できます。ライセンスキー、ライセンス容量、およびその他の情報が含まれています。

III. ライセンスキー

ライセンスキーはライセンスを一意に識別します。

IV. 装置シリアル番号

装置シリアル番号 (SN または S/N) は、装置を一意に識別するバーコードです。

V. デバイス ID (DID) と DID ファイル

DID は、ハードウェア装置を一意に識別する文字列です。DID ファイルには、DID とその他の情報が格納されます。装置には DID または DID ファイルが付属しています。

VI. アクティベーションファイル

アクティベーションファイルは、ライセンスをシステムに適用します。

システムでライセンスベースの機能を使用するには、以下のタスクを実行する必要があります。

1) ライセンスキーとシステムの SN および DID 情報を使用して、NEC ライセンス管理プラットフォームからアクティベーションファイルを取得します。
2) システムにアクティベーションファイルをインストールします。

VII. キーのアンインストールとファイルのアンインストール

ライセンスをアンインストールすると、アンインストールキーを含むアンインストールファイルが作成されます。ライセンスの移行にはアンインストールキーが必要です。

VIII. ライセンスストレージ

ライセンスストレージは、ライセンス情報を格納するための固定サイズの永続ストレージです。この情報にはライセンスの状態、有効期間、キーまたはアンインストールファイル、およびその他の関連情報が含まれます。

ライセンスストレージ内のデータは再起動後も保持されます。これによりライセンスの正確性と継続性が保証されます。

1.4 制限とガイドライン

1.4.1 一般的な制限とガイドライン

ライセンスを管理する場合の一般的な制限とガイドラインを示します。

- 対応装置のライセンスを購入していることを確認してください。
- ライセンス機能表示コマンドを使用して、ライセンスベース機能とそのライセンス情報を確認します。
- 使用装置で他の誰もライセンス管理タスクを実行していないことを確認してください。
- オペレーティングシステムやブラウザのエラーなどの問題によりアクティベーションファイルを取得または登録できない場合は、QX サポートにお問い合わせください。

1.4.2 異なるデバイスタイプのライセンス

- ライセンス登録には、ライセンスキー、シリアル番号、DID を使用します。これらは、装置固有情報です。登録ライセンスは、登録装置で有効です。

1.4.3 ライセンスファイルの安全性

- ライセンスを管理する場合のライセンスファイルの安全性に関する制限とガイドラインを示します。
- 紛失に備えて、取得したアクティベーションファイルを保存してバックアップします。
- FTP を使用してアクティベーションファイル（”.ak”ファイル）を転送する場合は、バイナリモードを使用します。
- ライセンスエラーを避けるために、装置にライセンスを適用した後はアクティベーションファイル（“.ak”ファイル）の名前を変更しないでください。
- 装置の flash:/license ディレクトリでファイルを削除したり移動したりしないでください。ライセンス管理機能は、ライセンス管理のために、このディレクトリを使います。誤ったファイル操作は問題を引き起こす可能性があります。たとえば、使用可能、または、使用中のアクティベーションファイルを削除すると、関連する機能が正しく動作しません。ファイルが存在しないか破損している場合は、アクティベーションファイルをディレクトリにコピーしてライセンスを回復します。 復元されたライセンスの状態が使用中にもかかわらず、ライセンスされたすべての機能が動作しない場合は、装置を再起動してください。ライセンスの状態を確認するには、**display license** コマンドを使用します。

1.5 ライセンスの適用

本装置はアクセスポイントを管理するために、管理台数分のライセンスを適用する必要があります。(ただし、本装置にはデフォルトで 8 ライセンスがバンドルされています。クラウドクラスタ運用時はマスタ装置とスタンバイ装置でライセンスが共有されますが、この 8 ライセンスはクラウドクラスタ運用時に共有されません。)

クラウドクラスタ構成装置を含むデュアルリンクバックアップ構成では AP ライセンス同期機能は使用できません。

1.5.1 ライセンスの新規適用

装置に新規にライセンス適用を行う場合、以下の手順でライセンスの適用を行います。

また、装置にライセンス追加適用する場合も、追加分について新規適用と同様の手順でライセンス適用を行います。

1) ライセンスキーを用意してください。ライセンスを購入することにより、ライセンスキーを入手可能です。
2) 装置のデバイス ID ファイルを用意してください。**display license device-id** コマンドにより装置のデバイス ID ファイルのパスを確認可能です。デバイス ID ファイルを FTP/TFTP で取得してください。転送モードは binary モードを使用してください。
3) 装置のシリアル番号を用意してください。装置背面のラベル、もしくは **display device manuinfo** コマンドによりシリアル番号を確認可能です。
4) ライセンスサーバ(URL: https://www.qx-info.com/License)にアクセスしてください。

5) ライセンスキー/装置のデバイス ID ファイル/装置のシリアル ID を用いて以下の手順でアクティベーションファイルを発行してください。指定したメールアドレスに、ライセンス発行 URL が送付されます。



6) 一定時間(10 分程度)待った後に、ライセンス発行 URL にアクセスしてアクティベーションファイルを取得してください。(同一装置のアクティベーションファイルは、デフォルトで同じ名前となっているため任意の名前に変更して取得してください。)

7) 取得したアクティベーションファイルを FTP/TFTP で装置に転送してください。（転送モードは binary モードを使用してください。）装置に転送後、**license activation-file install** *file-name* コマンドでライセンスのアクティベーションを行ってください。

🕮 **メモ：**

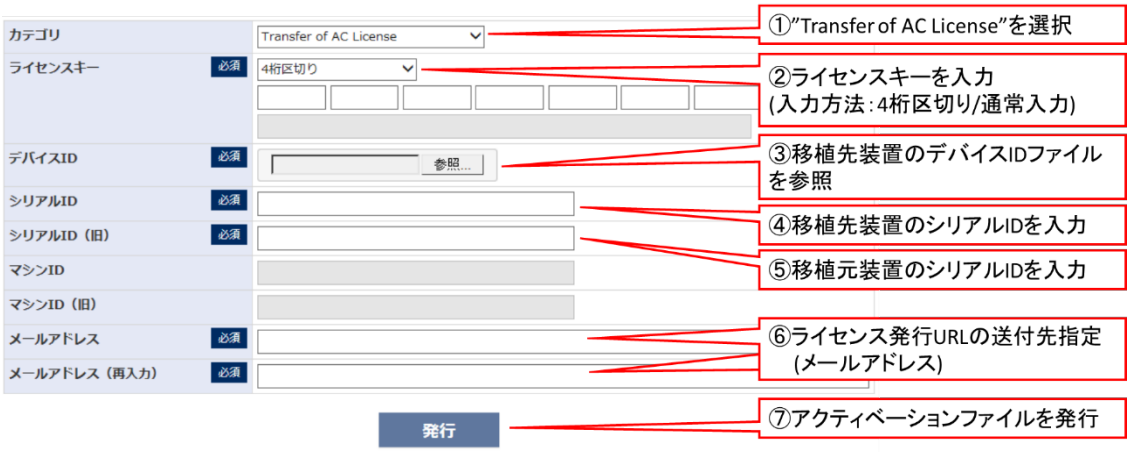
デバイス ID ファイルとは、License フォルダ内の拡張子が.did のファイルのことを指します。
表示例）
<AC>dir license/
Directory of flash:/license
  0 -rw-　　1026 Mar 01 2018 04:16:49　210235A3KYC17B000013.did

1.5.2 ライセンスの移植適用

誤った装置へのライセンス新規適用を行った場合、および装置の故障時は、該当装置と同じ型番の別装置にライセンスを移植適用することが可能です。以下の手順でライセンスの移植適用を行います。

1) ライセンスキーを用意してください。移植元の装置で使用したライセンスキーを使用可能です。
2) 移植先装置のデバイス ID ファイルを用意してください。**display license device-id** コマンドにより移植先装置のデバイス ID ファイルのパスを確認可能です。デバイス ID ファイルを FTP/TFTP で取得してください。転送モードは binary モードを使用してください。
3) 移植先装置のシリアル番号を用意してください。装置背面のラベル、もしくは **display device manuinfo** コマンドによりシリアル ID を確認可能です。
4) 移植元装置のシリアル番号を用意してください。装置背面のラベル、もしくは **display device manuinfo** コマンドによりシリアル ID を確認可能です。

5) ライセンスサーバ(URL: https://www.qx-info.com/License)にアクセスしてください。
6) ライセンスキー/移植先装置のデバイス ID ファイル/移植先装置のシリアル ID/移植元装置のシリアル ID を用いて以下の手順でアクティベーションファイルを発行してください。指定したメールアドレスに、ライセンス発行 URL が送付されます。



7) 一定時間(10 分程度)待った後に、ライセンス発行 URL にアクセスしてアクティベーションファイルを取得してください。(同一装置のアクティベーションファイルは、デフォルトで同じ名前となっているため任意の名前に変更して取得してください。)
8) 取得したアクティベーションファイルを FTP/TFTP で移植先装置に転送してください。(転送モードは binary モードを使用してください。) 移植先装置に転送後、**license activation-file install** *file-name* コマンドでライセンスのアクティベーションを行ってください。(*file-name* はライセンスの移植適用で取得したアクティベーションファイル名となります。)
9) [誤った装置へのライセンス適用をした場合(装置故障時は本操作不要)]移植元装置において **license activation-file uninstall** *file-name* コマンドでライセンスのインアクティベーションを行ってください。(file-name はライセンスの新規適用で取得したアクティベーションファイル名となります。)
10) [誤った装置へのライセンス適用をした場合(装置故障時は本操作不要)]移植元装置において **license compress** コマンドでライセンスストレージを圧縮してください。

⚠ **注意：**

- ライセンスの移植適用は、誤った装置へのライセンス新規適用を行った場合、および装置の故障時のみ実行可能です。これ以外のケースでライセンスの移植適用を行わないでください。不正なライセンスの移植適用を行った場合、該当ライセンスが適用されている装置はサポート対象外となります。
- **license activation-file uninstall** *file-name* コマンドでライセンスのインアクティベーションを行ったライセンスは、削除した装置に再度適用することはできません。

目次

このセクションのページは **1-x-x** です。

2 章 ローカルライセンス 2-1
2.1 ローカルライセンス 2-1
2.2 ライセンス登録とインストール 2-1
2.2.1 ライセンス登録とインストールのワークフロー 2-1
2.2.2 ライセンスストレージの識別 2-2
2.2.3 ライセンスストレージの圧縮 2-3
2.2.4 ライセンス登録に必要な情報の取得 2-3
2.2.5 アクティベーションファイルのインストール 2-4
2.3 ライセンスの移管 2-5
2.3.1 ライセンス転送ワークフロー 2-5
2.3.2 アンインストールファイルの取得 2-6
2.4 ライセンスのアンインストール 2-7
2.4.1 ライセンスのアンインストール 2-7
2.4.2 ライセンスのアンインストールワークフロー 2-7
2.5 アクティベーションファイルの回復 2-7
2.6 ライセンス管理の表示と維持 2-8

2章　ローカルライセンス

2.1　ローカルライセンス

ローカルライセンスでは、装置ごとにライセンスアクティベーション装置が必要です。小規模ネットワークに適用できます。

装置にライセンスをインストールするには、以下の手順を実行します。

1)　機器のライセンスキー、SN、DID 情報を取得します。
2)　NEC ライセンス管理プラットフォームにアクセスし、ライセンスキーと装置の SN および DID 情報に基づいてアクティベーションファイルを申請します。
3)　ライセンスをアクティベートするには、アクティベーションファイルを装置にインストールします。

ライセンスのアクティベーション情報は装置ロックされています。ある装置のアクティベーションファイルをインストールして、別の装置でライセンスをアクティベートすることはできません。

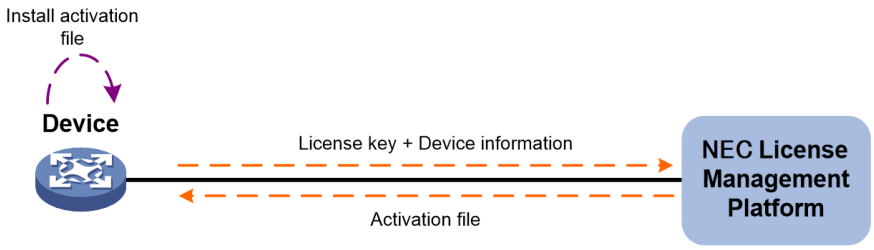


図 2-1 ローカルライセンス手順

2.2　ライセンス登録とインストール

2.2.1　ライセンス登録とインストールのワークフロー

正式ライセンスとトライアルライセンスの登録とインストールの手順は、図 2-2 のように同じです。

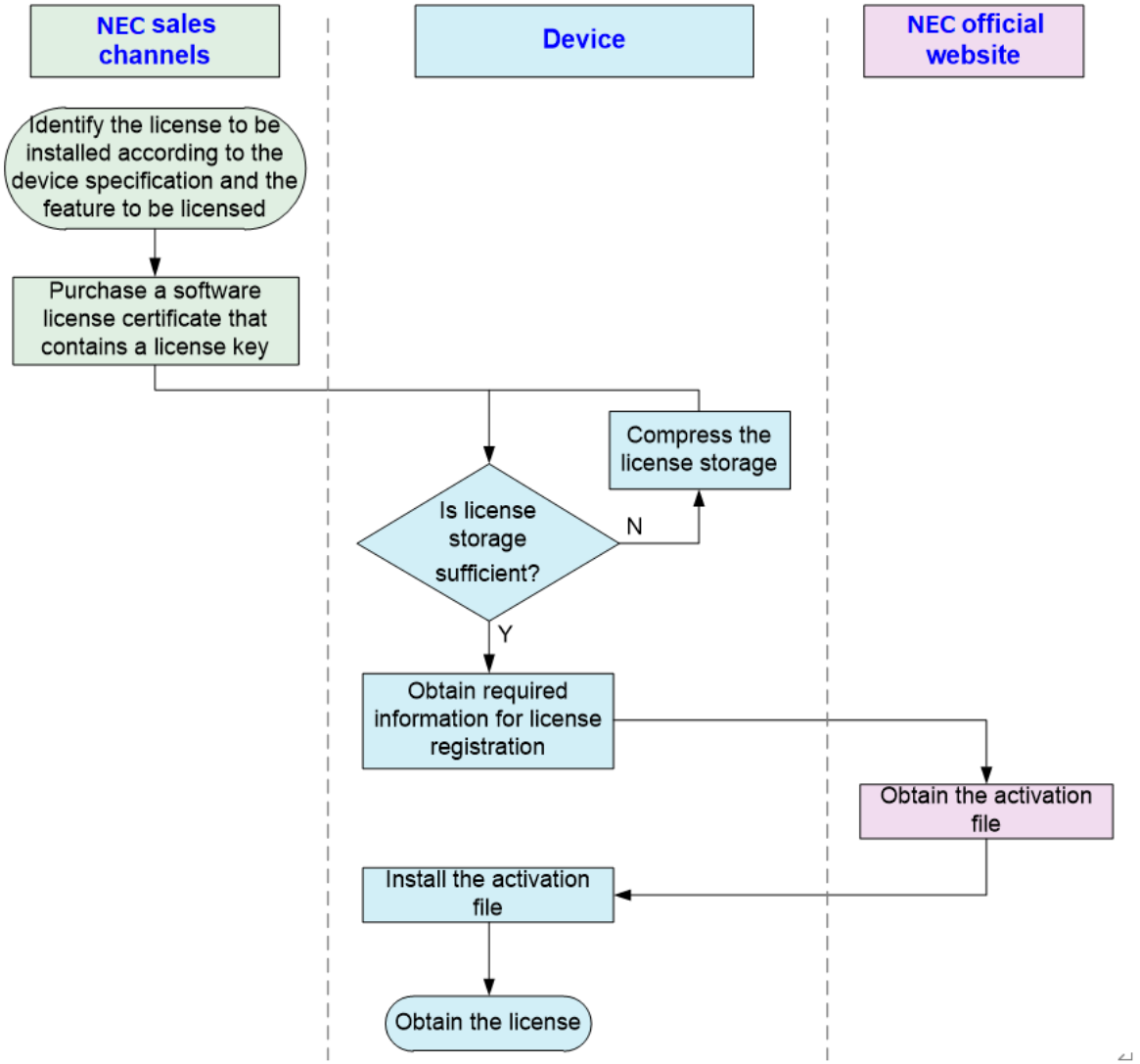


図 2-2 ライセンス登録とインストールのワークフロー

2.2.2 ライセンスストレージの識別

すべての view で以下のコマンドを実行します。

操作	コマンド
ライセンスストレージの空き領域を特定する	**display license feature**

コマンド出力から、**Total** フィールドと **Usage** フィールドを表示して、残りのライセンスストレージが新しいライセンスをインストールするのに十分かどうかを確認します。残りのライセンスストレージが十分でない場合は、ライセンスストレージを圧縮します。

2.2.3 ライセンスストレージの圧縮

ライセンスストレージにはライセンス情報が格納され、サイズは固定されています。ライセンスをインストールできるのは、装置にアイドルライセンスの保存スペースがある場合だけです。

ライセンスストレージ圧縮を使用すると、期限切れおよびアンインストールされたライセンスエントリを削除して、装置に新しいライセンス用の十分なストレージスペースを確保できます。新しいライセンスを正常にインストールするには、ライセンス登録に必要な情報を取得し、新しいライセンスのアクティベーションファイルを申請する前に、このタスクを実行します。

装置にライセンスがインストールされていない場合は、ライセンスストレージを圧縮する必要はありません。

I. 前提条件

その後のライセンス転送または NEC ライセンス管理プラットフォームでのライセンスのアンインストールのために、アンインストールされたライセンスのアンインストールキーまたはアンインストールファイルをバックアップします。

アンインストールされたライセンスまたは期限切れのライセンスが装置に存在する場合、圧縮操作によって DID または DID ファイルが変更されます。古い DID または DID ファイルを使用して取得したアクティベーションファイルを装置にインストールすることはできません。圧縮を実行する前に、古い DID または DID ファイルに登録されているすべてのアクティベーションファイルをインストールすることをお勧めします。

古い DID に登録されているアクティベーションファイルをインストールしていない場合は、以下の操作を実行します。

- ライセンスストレージが十分な場合は、アクティベーションファイルを装置にインストールします。詳細は QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*1 ライセンス管理*”の”*1 章 ライセンス管理*”を参照してください。
- ライセンスストレージが不十分で、圧縮後にアクティベーションファイルをインストールできない場合は、販売店もしくは担当営業にお問い合わせください。

II. 設定手順

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． ライセンスストレージを圧縮する	**license compress**	―

2.2.4 ライセンス登録に必要な情報の取得

すべての view で以下のコマンドを実行します。

操作	コマンド
SNおよびDID情報を取得する	**display license device-id**

2.2.5 アクティベーションファイルのインストール

⚠ **注意**：
インストールする前に、アクティベーションファイルをバックアップします。アクティベーションファイルが誤って削除された場合や、その他の理由で使用できなくなった場合は、バックアップアクティベーションファイルでライセンスを復元できます。

ライセンスベースの機能を使用するには、その機能のアクティベーションファイルを装置にインストールします。

アクティベーションファイルには、以下のいずれかの形式で提供されます。

- 単一の.ak ファイル

ak アクティベーションファイルを取得するには、ライセンスキーを購入し、NEC ライセンス管理プラットフォームにアクセスして、ライセンスキー、SN、および DID 情報を提供します。

- tar ファイルパッケージ

tar アクティベーションファイルパッケージを取得するには、複数のライセンスキーを購入し、NEC ライセンス管理プラットフォームにアクセスして、ライセンスキー、SN、および DID 情報を提供します。

アクティベーションファイルパッケージは、ライセンスキーに対応する.ak アクティベーションファイルのセットです。アクティベーションファイルパッケージは、単一のアクティベーションファイルがインストールされるのと同じ方法でインストールされます。アクティベーションファイルパッケージを使用すると、アクティベーションファイルの登録とインストールの回数が減り、アクティベーションファイルの管理が簡素化されます。ただし、ライセンスをアンインストールするには、.ak アクティベーションファイルを 1 つずつのみアンインストールできます。

I. 前提条件

FTP または TFTP で装置にインストールするアクティベーションファイルをアップロードします。FTP でアクティベーションファイルを転送する場合は、バイナリモードで設定します。

II. 設定手順

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． アクティベーションファイルをインストールする	**license activation-file install** *file-name*	1回の操作で1つの.akファイルまたは複数の.akファイルをインストールできます。複数の.akファイルをインストールするには、すべてのアクティベーションファイルを同じディレクトリに保存し、そのディレクトリを*file-name*の値として指定します。

2.3 ライセンスの移管

同じ製品シリーズ内の装置間で有効期限が切れていないライセンスを転送するには、以下の作業を実行します。

2.3.1 ライセンス転送ワークフロー

ある装置から別の装置にライセンスを転送するには、図 2-3 のワークフローを使用します。

この章では、送信元装置で実行される操作についてのみ説明します。対象機器での操作は、本資料の“*ライセンス登録とインストール*”を参照してください。ライセンス転送の詳細は、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*1 ライセンス管理*”の”*1 章 ライセンス管理*”を参照してください。

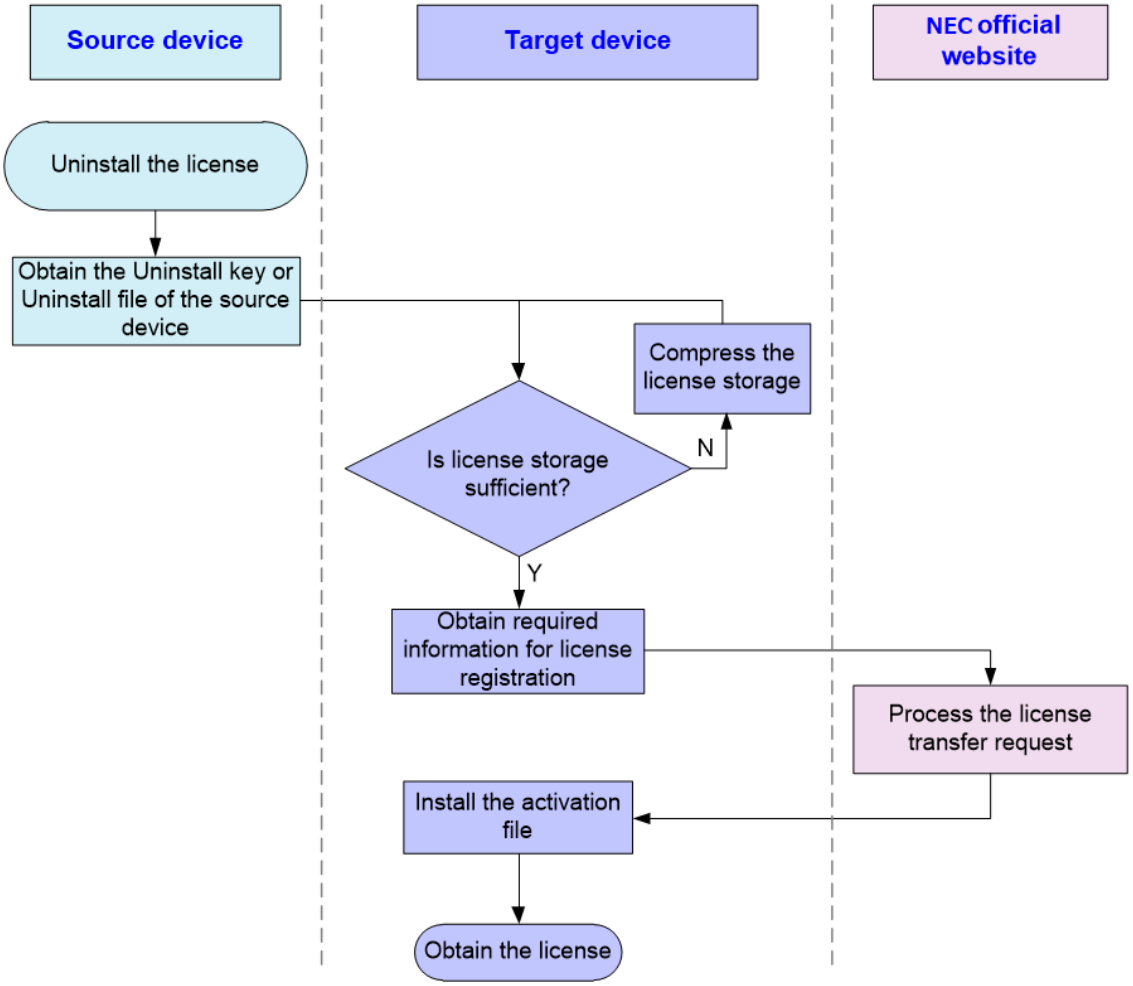


図 2-3 ライセンス転送ワークフロー

2.3.2 アンインストールファイルの取得

操作	コマンド	補足
1. アンインストールするアクティベーションファイルを表示する	**display license**	ー
2. system view に移行する	**system-view**	ー
3. アクティベーションファイルをアンインストールする	**license activation-file uninstall** *license-file*	1回の操作で1つの.akファイルまたは複数の.akファイルをアンインストールできます。複数の.akファイルをアンインストールするには、すべてのアクティベーションファイルを同じディレクトリに保存し、そのディレクトリを*license-file*の値として指定します。

2.4 ライセンスのアンインストール

2.4.1 ライセンスのアンインストール

NEC ライセンス管理プラットフォームでライセンスキーをアクティブ化すると、ライセンスキーが装置にバインドされます。このライセンスキーを別の装置にバインドすることはできません。装置から期限切れになっていないライセンスのライセンスキーをアンバインドするには、装置上のライセンスのアンインストール キーまたはアンインストールファイルを入手します。次に、NEC ライセンス管理プラットフォームでライセンスのアンインストールを要求します。

ライセンスのアンインストールが正常に要求されたら、このライセンスキーを使用して NEC ライセンス管理プラットフォームで新しいアクティベーションファイルを要求できます。

新しいアクティベーションファイルは、ライセンス転送のために別の装置にインストールすることも、ライセンス復元のためにローカル装置にインストールすることもできます。

2.4.2 ライセンスのアンインストールワークフロー

ライセンスのアンインストールの詳細は、QX-W2300AC シリーズアクセスコントローラ オペレーションマニュアルの“*1 ライセンス管理*”の”*1 章 ライセンス管理*”を参照してください。

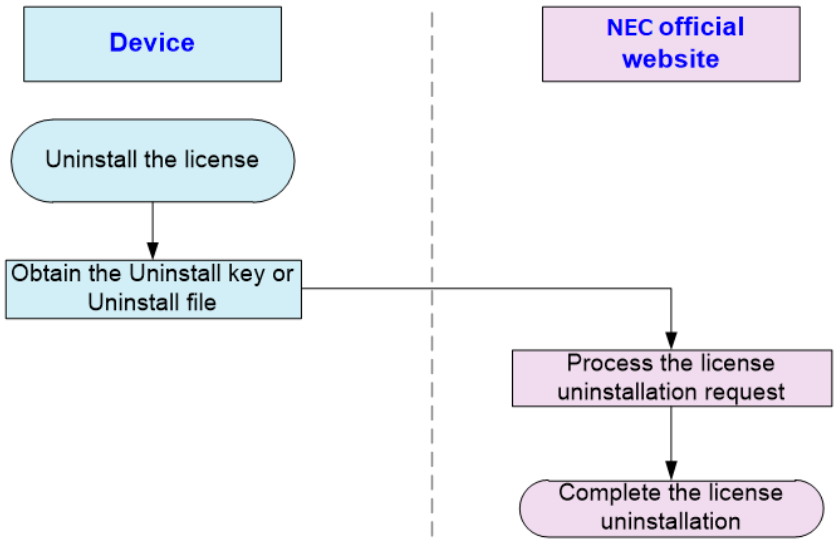


図 2-4 ライセンスのアンインストールワークフロー

2.5 アクティベーションファイルの回復

誤ってアクティベーションファイルを削除した場合は、以下の手順に従ってアクティベーションファイルを回復します。

1) **copy** コマンドでバックアップアクティベーションファイルをストレージメディアのルートディレクトリにある **license** フォルダにコピーします。
2) **display license** コマンドで回復したアクティベーションファイルの状態が **In use** であることを確認します。
3) ライセンスの状態が **In use** になっていてもライセンス機能が正常に機能しない場合は、装置を再起動します。

2.6 ライセンス管理の表示と維持

すべての view で **display** コマンドを実行します。

操作	コマンド
ライセンスの詳細情報を表示する	**display license** [**activation-file**]
機能ライセンスの概要情報を表示する	**display license feature**

目次

このセクションのページは **1-x-x** です。

3 章 AP ライセンス同期 3-1
3.1 AP ライセンス同期 3-1
3.1.1 AP ライセンス同期ネットワーキング 3-1
3.1.2 AP ライセンス同期接続の確立 3-2
3.2 制限とガイドライン 3-3
3.3 AP ライセンスの同期の表示と維持 3-3
3.4 AP ライセンス同期の設定例 3-4
3.4.1 AP ライセンス同期の設定例 3-4

3章 AP ライセンス同期

⚠ **注意**：
クラウドクラスタとデュアルリンクバックアップ機能は併用できません。

3.1 APライセンス同期

この機能により、マスタ AC は、AP ライセンス同期接続を介して、ローカルライセンスを AP ライセンス同期グループのバックアップ AC と同期できます。N+1 コールドバックアップまたはデュアルリンクバックアップネットワークでは、ライセンスは AC 単位でインストールされます。マスタ AC に障害が発生すると、バックアップ AC がサービスを引き継ぎ、AP がバックアップ AC に再関連付けされます。この機能により、AP ライセンスがないことによるバックアップ AC での AP アソシエーション障害を回避できます。

⚠ **注意**：
AP ライセンス同期を設定している状態で、故障などによってライセンスの同期が取れなくなった場合、以下の条件でライセンスが使用できなくなります。

- AC の再起動
- 30 日経過

3.1.1 AP ライセンス同期ネットワーキング

N+1 コールドバックアップネットワークでは、バックアップ AC は複数のマスタ AC のライセンスをバックアップできます。AP ライセンス同期グループでは、最小 1 つの AC をバックアップとして、最大 4 つの AC をマスタとして設定できます。

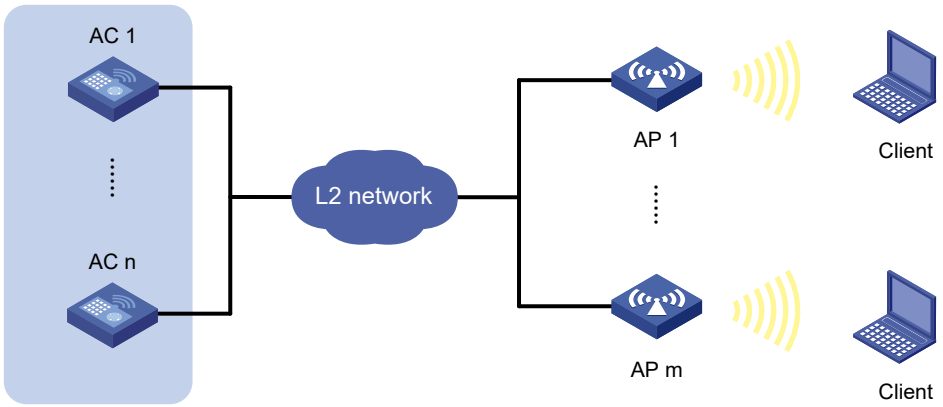


図 3-1 N+1 コールドバックアップのネットワーク図

デュアルリンクバックアップネットワークでは、2 つの AC が互いのライセンスをバックアップします。両方の AC をマスタ AC として設定する必要があります。

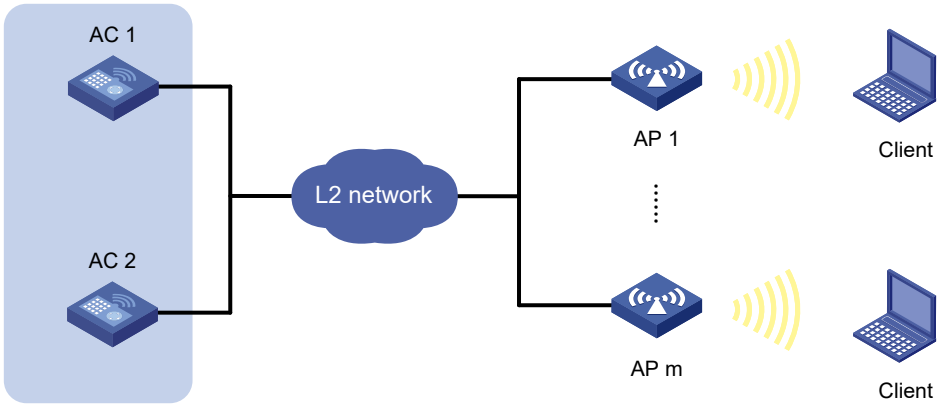


図 3-2 デュアルリンクバックアップのネットワーク図

3.1.2 AP ライセンス同期接続の確立

両方の AC に AP ライセンス同期機能が設定されている場合、次の手順を使用してそれらの間に AP ライセンス同期接続が確立されます。

1) N+1 コールドバックアップネットワークでは、バックアップ AC がマスタ AC への接続要求を開始します。デュアルリンクバックアップネットワークでは、IP アドレスの小さい AC から IP アドレスの大きい AC への接続要求が開始されます。
2) マスタ AC は、受信した要求パケット内のライセンス同期グループ設定とローカルライセンス同期グループ設定を比較します。一致が見つかった場合、マスタ AC は接続要求を受け入れます。
3) 接続が確立されると、バックアップ AC はライセンス同期要求を開始します。
4) マスタ AC は、ローカルライセンス情報をバックアップ AC と同期し、ローカルアクティベーションファイルをバックアップ AC にコピーします。

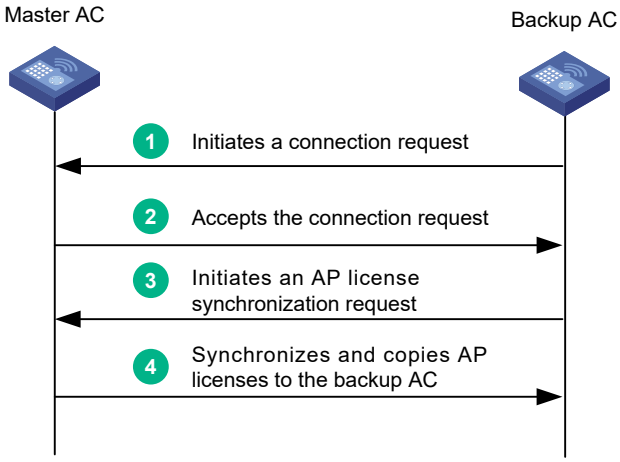


図 3-3 AP ライセンス同期接続の確立

バックアップ AC は、10 分ごとに同期要求を開始して、各マスタ AC にインストールされているライセンスと使用されているライセンスに関する情報を取得します。ネットワークでサポートされるオンライン AP の数はライセンス制限されています。既存の AP の数が連続 3 回の同期でサポートされている数を超えた場合、バックアップ AC は既存の AP の数がサポートされている数の範囲内になるまで AP をログオフします。

3.2 制限とガイドライン

AP ライセンス同期を有効にする前に、AP ライセンス同期グループで AC とそのメンバ AC の IP アドレスとロールを指定する必要があります。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP license synchronization group view に移行する	**wlan ap-license-group**	—
3. AP ライセンス同期グループのローカル AC の IP アドレスとロールを指定する	**local ip** *ipv4-address* [**backup**]	デフォルト：設定なし
4. AP ライセンス同期グループにメンバを追加する	**member ip** *ipv4-address* [**backup**]	—
5. AP ライセンスの同期を有効にする	**ap-license-synchronization enable**	デフォルト：無効

3.3 APライセンスの同期の表示と維持

すべての view で **display** コマンドを実行します。

操作	コマンド
APライセンス同期グループ情報を表示する	**display wlan ap-license-group**

3.4 APライセンス同期の設定例

3.4.1 AP ライセンス同期の設定例

I. ネットワーク要件

図 3-4 に示すように、AP はスイッチを介して AC 1 および AC 2 にデュアルホーム接続されています。AC の 1 つで障害が発生した後に、ある AC のライセンスを別の AC で使用できるようにするため、AC で AP ライセンス同期を設定します。

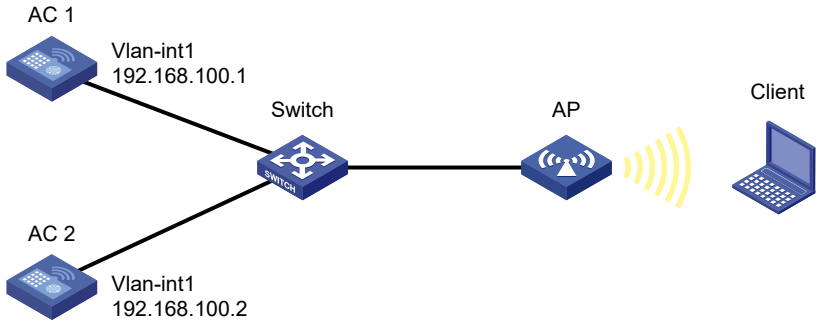


図 3-4 ネットワーク図

II. 設定手順

1)　AC 1 を設定します。

AC 1 にライセンスをインストールします。(詳細は省略します)

VLAN-interface 1 を作成し、VLAN インタフェースに IP アドレスを割り当てます。

```
<AC1> system-view
[AC1-wlan-ap-ap1] interface vlan-interface 1
[AC1-Vlan-interface1] ip address 192.168.100.1 24
[AC1-Vlan-interface1] quit
```

手動 AP **ap 1** を作成し、モデルとシリアル ID を指定します。

```
[AC1] wlan ap ap1 model WA6320
[AC1-wlan-ap-ap1] serial-id 219801A28N819CE0002T
[AC1-wlan-ap-ap1] quit
```

AP ライセンス同期グループ view に入り、AP ライセンス同期グループのローカル AC の IP アドレスを指定し、メンバをライセンス同期グループに追加します。

```
[AC1] wlan ap-license-group
[AC1-wlan-ap-license-group] local ip 192.168.100.1
[AC1-wlan-ap-license-group] member ip 192.168.100.2
```

AP ライセンス同期を有効にします。

```
[AC1-wlan-ap-license-group] ap-license-synchronization enable
```

2)　AC 2 を設定します。

AC 2 にライセンスをインストールします。(詳細は省略します)

VLAN-interface 1 を作成し、VLAN インタフェースに IP アドレスを割り当てます。

```
<AC2> system-view
[AC2] interface vlan-interface 1
[AC2-Vlan-interface1] ip address 192.168.100.2 24
[AC2-Vlan-interface1] quit
```

手動 AP **ap 1** を作成し、モデルとシリアル ID を指定します。

```
[AC2] wlan ap ap1 model WA6320
[AC2-wlan-ap-ap1] serial-id 219801A28N819CE0002T
```

AP ライセンス同期グループ view に入り、AP ライセンス同期グループのローカル AC の IP アドレスを指定し、メンバをライセンス同期グループに追加します。

```
[AC2] wlan ap-license-group
[AC2-wlan-ap-license-group] local ip 192.168.100.2
[AC2-wlan-ap-license-group] member ip 192.168.100.1
```

AP ライセンス同期を有効にします。

```
[AC2-wlan-ap-license-group] ap-license-synchronization enable
```

III. 設定の確認

AP ライセンス同期グループが作成されたことを確認します。

```
<AC1> display wlan ap-license-group
 Group total licenses: 256
 Group used licenses: 1
 AP license synchronization: Enabled
 Local IP: 192.168.100.1
 Local role: Master
 Member information: 1
 IP address         Total      Used      Member role      State      Online
duration
 192.168.100.2      64          1          Master            UP          00hr
16min 51sec
```

QX-W2300AC シリーズ アクセスコントローラ

オペレーションマニュアル

2. 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-RBAC
03-ログイン管理
04-コンソールポートによる最初のログイン
05-CLI によるログイン
06-Web コンソールによるログイン
07-ログインユーザの制御
08-FTP
09-TFTP
10-ファイルシステム管理
11-コンフィグレーションファイル管理
12-ソフトウェアアップグレード
13- Python
14- Comware 9 拡張 Python API
15-Tcl
16-Auto Config

目次

このセクションのページは**2-x-x** です。

1章 CLI 1-1
1.1 CLI viewの記述 1-1
1.1.1 user viewからsystem viewへの移行 1-2
1.1.2 各viewから上位viewへの戻り 1-2
1.1.3 user viewへの戻り 1-2
1.2 コマンドラインを使ったオンラインヘルプ 1-2
1.3 コマンドのundo 1-3
1.4 コマンドの実行 1-4
1.4.1 コマンドラインの編集 1-4
1.4.2 引数の文字列あるいはテキストタイプ値の入力 1-5
1.4.3 インタフェースタイプの入力 1-5
1.4.4 コマンドの補完 1-6
1.4.5 コマンドエイリアスの設定と使用方法 1-6
1.4.6 ホットキーを使用した設定と使用方法 1-8
1.4.7 情報の同期出力 1-9
1.5 コマンドラインのエラーメッセージ 1-9
1.6 履歴コマンドの保存 1-10
1.7 コマンド履歴バッファの管理と使用 1-11
1.7.1 コマンド履歴バッファ内のコマンドの表示 1-11
1.7.2 コマンド履歴バッファ内のコマンドの呼び出し 1-11
1.7.3 コマンド履歴バッファでコマンドの繰り返し 1-11
1.8 CLI表示の管理 1-11
1.8.1 出力のスクリーンの休止 1-12
1.8.2 表示コマンドの各出力ラインの番号表示 1-12
1.8.3 出力のフィルタリング 1-13
1.8.4 displayコマンドのファイルへの保存 1-16
1.8.5 displayコマンドからの出力の有効的な表示、管理 1-17
1.9 稼働中の設定の保存 1-17

1章 CLI

Command-Line Interface (CLI)は、装置とユーザ間の相互運用インタフェースです。装置の設定、管理、モニタリングを行うため、CLI からコマンドを入力します。

CLI にはコンソールポートを使用する以外にも、Telnet、SSH などを使用してログインすることができます。

1.1 CLI viewの記述

コマンドは機能によって異なる view にグループ分けされています。コマンドを使用する場合、その view に入る必要があります。

CLI view は図 1-2 に示すような階層構造となっています。各 view は、どこで何を行うのかを一意に示すプロンプトとなります。たとえば[AC-vlan100]という view は、VLAN100 view で、その VLAN の属性を設定することができます。

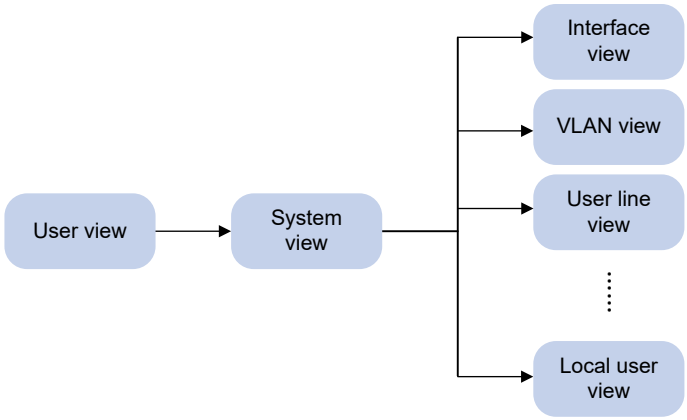


図 1-1 CLI views

CLI でログインした後、最初に user view に入ります。user view のプロンプトは<Device-name>で、Device-name は装置名を示します。デフォルトは装置名で、sysname コマンドを使用して変更することができます。

user view では以下の操作を行うことができます。

- 表示、デバッグ、ファイル管理、FTP、Telnet、日時の設定、再起動などの基本的な操作を行うことができます。
- user view から system view に移行することができます。system view のプロンプトは[Device-name]です。

system view では以下の操作を行うことができます。

- グローバルの設定（時間の設定、バナー、ショートカットキーなど）といくつかの機能を行うことができます。

- system view からさらに、異なる view に移行することができます。たとえば、以下の操作を行うことができます。
  - interface view に移行し、インタフェースパラメータの設定ができます。
  - VLAN view に移行し、VLAN にポートを追加することができます。
  - user line view に移行し、ログインユーザの属性を設定することができます。

view プロンプトでクエスチョン“?”を入力することで、その view で利用できるすべてのコマンドを表示します。

1.1.1 user view から system view への移行

操作	コマンド
system viewへ移行する	**system-view**

1.1.2 各 view から上位 view への戻り

操作	コマンド
各viewから上位viewに戻る	**quit**

user view で **quit** コマンドを実行することで、装置の接続を終了します。

public key view で **peer-public-key end** コマンドを実行することで、system view へ戻ります。

1.1.3 user view への戻り

return コマンドあるいはホットキー**Ctrl+Z** を実行することで直接 user view に戻ることができます。

操作	コマンド
user viewに戻る	**return**

Tcl configuration view から user view に戻るには、**tclquit** コマンドを使用します。

Python シェルから user view に戻るには、**exit ()** コマンドを使用します。

1.2 コマンドラインを使ったオンラインヘルプ

CLI オンラインヘルプは状況に応じてヘルプ情報が異なります。すべてのプロンプトで“?”を入力し、その view で利用できるコマンドを表示するか、コマンドのいずれかの位置で、すべての有効なオプションを表示することができます。

CLI オンラインヘルプにアクセスするには以下の方法を行います。

- 各 view で “?” を入力することで、その view で利用できるすべてのコマンドの最初のキーワードを表示します。

```
<AC> ?
User view commands:
  archive           Archive configuration
  arp               Address Resolution Protocol (ARP) module
  backup            Backup the startup configuration file to a TFTP server
  boot-loader       Software image file management
...
```

- コマンドキーワードの後ろにスペースを空けて”?”を入力することで、設定可能なキーワードかパラメータが表示されます。
  - □ キーワードの場所にスペースを空けて”?”を入力したとき、設定可能なキーワードの概要が表示されます。

```
<AC> terminal ?
  debugging  Enable to display debugging logs on the current terminal
  logging    Display logs on the current terminal
  monitor    Enable to display logs on the current terminal
```

  - □ パラメータの場所にスペースを空けて”?”を入力したとき、設定可能なパラメータの概要が表示されます。

```
<AC> system-view
[AC] interface vlan-interface ?
  <1-4094>  Vlan-interface interface number
[AC] interface vlan-interface 1 ?
  <cr>
[AC] interface vlan-interface 1
```

<1-4094> は引数の範囲で、<cr>はコマンドを示します。完了させるには、Enter キーを押してコマンドを実行することができます。

- コマンドの後ろに?をつけて入力すると、この文字列で始まるすべてのキーワードが表示されます。

```
<AC> b?
  backup       Backup operation
  boot-loader  Software image file management
  bootrom      Update/read/backup/restore bootrom
<AC> display ftp?
  ftp         FTP module
  ftp-server  FTP server information
  ftp-user    FTP user information
```

1.3 コマンドのundo

コマンドにキーワード undo をつけると、**undo** コマンドを形成できます。

ほとんどの設定コマンドに、**undo** を付加できます。以下のことができます。

- システムをデフォルトの状態に戻します。
- 機能を無効にします。
- 設定を取り消すときに使用します。
- たとえば Information Center を有効にするために、**info-center enable** コマンドを使用した場合、**undo info-center enable** コマンドで Information Center を無効にします。

1.4 コマンドの実行

コマンドを入力することで以下のことができます。

- キーあるいはショートカットキーを使用してコマンドラインを編集できます。
- 省略したキーワードあるいはエイリアスを使用することができます。

1.4.1 コマンドラインの編集

コマンドラインを編集するために、表 1-1に示すキーや表 1-4に示すショートカットキーを使用することができます。終了するには **Enter** を押してコマンドを実行します。

表 1-1 コマンドラインの編集キー

キー	機能
コマンドキー	編集バッファが一杯でなければ、カーソルの位置に文字を挿入し、カーソルを右に移動します。コマンドの最大の長さは、511文字です。コマンドの最大の長さに達した場合、システムは次の行に自動的に移ります。次の行に移るには、**Enter** を押します。
Backspace	カーソルの左側の文字を削除し、1文字分カーソルを戻します。
左矢印キー (←)	カーソルが左に1文字分移動します。
右矢印キー (→)	カーソルが右に1文字分移動します。
上矢印キー (↑)	前に入力した履歴コマンドを表示します。
下矢印キー (↓)	次に入力した履歴コマンドを表示します。
Tab	キーワードの一部でTABキーを押した場合、システムは自動的にキーワードを補完します。 • ただ1つマッチングしたら、システムは不完全なキーワードを完全なキーワードに置き換えて、それを次の行に表示します。 • マッチするものが複数ある場合、キーワードを選択するためTABキーを複数回押してください。 • マッチするものが全くない場合は、システムは不完全なキーワードを補完せず、再度それを次の行に表示します。

コマンドラインの最大長は 512 文字を超過することができません。512 文字にはスペース、特殊文字が含まれます。

装置は以下の特殊文字をサポートします。

- **#**－システムによって隣接セクションと区別するためにコンフィグレーションファイルの中で使用します。

- **version**－ソフトウェアバージョンを示すため、コンフィグレーションファイルの中で使用します。たとえば **Version 7.1.xxx** です。

これらのコマンドは以下の理由があるため特殊文字となります。

- CLI でユーザが使用することはできません。
- すべての view で特殊文字を入力する、あるいはすべての値を入力することができます。たとえば、**# abc** あるいは **version abc** を入力することができます。しかし設定は適用されません。
- 装置はこれらの特殊文字に関するオンラインヘルプはありません。

1.4.2 引数の文字列あるいはテキストタイプ値の入力

テキストタイプの引数はクエスチョンマーク（?）を除く印刷可能な文字列を使用することができます。

文字列タイプの引数は以下の文字列を除く印刷可能な文字列を使用することができます。

- クエスチョンマーク（?）
- クオーテーションマーク（”）
- バックスラッシュ（\）
- スペース

特定の引数が必要となる場合があります。特定の引数については、関連するコマンドマニュアルを参照してください。

印刷可能な文字列は、文字あるいは ASCII コード（範囲は 32～126 です）を入力することができます。

1.4.3 インタフェースタイプの入力

以下のフォーマットでインタフェースタイプを入力することができます。

- インタフェースタイプのフルスペル
- インタフェースを識別する固有な短縮形
- インタフェースの頭文字

コマンドラインではすべてのインタフェースのタイプは大文字、小文字を区別しません。表 1-2にインタフェースタイプのフルスペルと短縮形を示します。

たとえば、GigabitEthernet 1/0/1 の view に移行するため、**interface** コマンドを入力する場合、コマンドラインで以下のフォーマットを入力することができます。

- interface gigabitethernet 1/0/1
- interface g 1/0/1
- interface ge 1/0/1
- interface gigabitethernet1/0/1
- interface g1/0/1
- interface ge1/0/1

表 1-2 インタフェースのタイプのフルスペルと短縮形

フルスペル	短縮形
Bridge-Aggregation	BAGG
GigabitEthernet	GE

フルスペル	短縮形
LoopBack	Loop
M-GigabitEthernet	MGE
NULL	NULL
Ten-GigabitEthernet	XGE
Tunnel	Tun
Vlan-interface	Vlan-int

1.4.4 コマンドの補完

コマンドは、キーワードの一部を入力することでコマンドを実行できます。ただし、入力するコマンドを識別するのに十分な文字列を入力した場合のみ有効です。たとえば **system-view** で **s** から始まるコマンドは、**system-view** と **startup saved-configuration** があります。**system-view** を指定する場合、最低でも **sy** を入力する必要があります。**startup saved-configuration** を指定する場合、最低でも **st s** を入力する必要があります。

Tab キーを押すことで、完全なコマンドを表示,入力することができます。

1.4.5 コマンドエイリアスの設定と使用方法

キーワードで始まるコマンドや **undo**＋キーワードで始まるコマンドを実行するとき、以下のエイリアスを使用することができます。

- **undo** コマンドを除くコマンドの先頭キーワード
- **undo** コマンドの 2 番目のキーワードのエイリアス

たとえば、**display** のエイリアスとして **show** を設定する場合、**display clock** コマンドを実行するのに、**show clock** コマンドを入力することができます。

たとえば、**display ip routing-table** コマンドの **alias shiprt** を設定する場合、**display ip routing-table** コマンドを実行するため、**shiprt** を入力することができます。**display ip** コマンドの **alias ship** を設定する場合、**display ip** で始まるすべてのコマンドを実行するため、**ship** を入力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** を入力します。
- **display ip interface** コマンドを実行するため、**ship interface** を入力します。

I. ガイドライン

コマンドエイリアスで定義したコマンドを実行したのち、装置はエイリアスの代わりにキーワードを保存します。カレントコンフィグレーションはオリジナルコマンドが表示されます。

エイリアスによって説明できる文字列は 9 つのパラメータまで設定することができます。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 **alias shinc** コマンドを設定することができます。**display hotkey | include CTRL_C** コマンドを実行するため、**shinc hotkey CTRL_C** を入力することができます。

パラメータがあるコマンドのエイリアスを使用する場合、各パラメータの値を指定する必要があります。パラメータの指定を設定するのに失敗した場合、コマンドは不完全で、エイリアスで表示されるコマンドの文字列を表示します。

表 1-3にシステム定義のコマンドエイリアスを示します。システム定義のコマンドエイリアスは削除することができませんが、設定を変更することはできます。システム定義のコマンドエイリアスを元に戻すと、システム定義のコマンドエイリアスが復元されます。

表 1-3 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

II. 設定手順

以下にコマンドエイリアスの設定を以下に示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. コマンドエイリアスを有効にする	**command-alias enable**	デフォルト：無効
3. コマンドエイリアスを設定する	**alias** *alias command*	デフォルト：設定なし システム定義のコマンドエイリアスは表 1-3を参照してください。
4. （オプション設定項目）コマンドエイリアスで定義されたコマンドを表示する	**display alias** [**alias**]	すべてのviewで実行可能です。

1.4.6 ホットキーを使用した設定と使用方法

装置は一連のホットキーをサポートしています。ホットキーを押すと、そのホットキーに割り当てられたコマンドまたは機能が実行されます。表 1-4 に、ホットキーとそのデフォルト定義を示します。**Ctrl+]** を除くすべてのホットキーを設定できます。

装置との対話に使用している端末ソフトウェアでもホットキーが定義されている場合は、ホットキーを再設定するか、ホットキーを削除できます。

端末のソフトウェアから装置と相互に運用する場合、これらのキーは他の操作を実行するために定義されている可能性があります。その場合は、端末のソフトウェアの定義が優先されます。

以下の手順でホットキーを設定します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. コマンドをホットキーに割り当てる	**hotkey** *hotkey* { *command* | **function** *function* | **none** }	表 1-4 にホットキーのデフォルト定義を示します。

すべての view で以下のコマンドを実行できます。

操作	コマンド
ホットキーを表示する	**display hotkey**

表 1-4 ホットキーのデフォルト定義

ホットキー	昨日
Ctrl+A	カーソルを現在の行の先頭に動かします。
Ctrl+B	カーソルを 1 文字分左に動かします。
Ctrl+C	コマンドの実行を停止させます。
Ctrl+D	現在カーソルがある位置の文字を削除します。
Ctrl+E	カーソルを現在の行の末尾に動かします。
Ctrl+F	カーソルを1文字分右に動かします。
Ctrl+G	実行中の設定を表示します。
Ctrl+H	カーソルの左側の文字を削除します。
Ctrl+K	外部接続を終了します。
Ctrl+L	IPv4 ルーティング テーブル情報を表示します。
Ctrl+N	履歴バッファの次のコマンドを表示します。パスワード設定コマンドはスキップされます。
Ctrl+O	すべてのデバッグ機能を無効にします。
Ctrl+P	履歴バッファの前のコマンドを表示します。パスワード設定コマンドはスキップされます。
Ctrl+R	現在の行のコマンドを再表示します。
Ctrl+T	該当なし
Ctrl+U	該当なし
Ctrl+V	クリップボードの中身を貼り付けます。
Ctrl+W	カーソルの左側に続く文字列の文字をすべて削除します。
Ctrl+X	カーソルの左側の文字をすべて削除します。
Ctrl+Y	カーソルの右側の文字をすべて削除します。
Ctrl+Z	終了し、user viewに戻ります。
Ctrl+]	内部接続またはリダイレクト接続を終了します。

ホットキー	昨日
Esc+B	カーソルを左側に続く文字列の先頭の文字に移動します。
Esc+D	現在カーソルがある位置の文字列の文字および右側の文字をすべて削除します。
Esc+F	カーソルを右側に続く次の文字列の先頭に移動します。
Esc+N	カーソルを1行下に移動します。Enterキーを入力する前にホットキーを使用することができます。
Esc+P	カーソルを1行上に移動します。Enterキーを入力する前にホットキーを使用することができます。
Esc+<	クリップボードの先頭にカーソルを移動します。
Esc+<	クリップボードの最後にカーソルを移動します。

1.4.7 情報の同期出力

情報の同期出力とは、システム出力によりユーザの入力が中断された場合、システム出力が完了した後に、システムがコマンドラインプロンプトやそれまで入力していたものを表示する機能を指し、ユーザは操作を中断したところから継続させることができます。

以下の手順で情報の同期出力を設定します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. 情報の同期出力を有効にする	**info-center synchronous**	デフォルト：無効 QX-W2300ACシリーズアクセスコントローラコマンドマニュアルの“*3 システム管理*”の”*5章 Information Center*”を参照してください。

1.5 コマンドラインのエラーメッセージ

Enter キーを押した後、コマンドラインは、コマンドの最初から順番に構文をチェックします。

- 構文エラーがある場合、エラーメッセージが表示されます。
- 構文エラーがない場合、コマンドを実行します。

表 1-5 コマンドラインのエラーメッセージ

エラーメッセージ	原因
% Unrecognized command found at '^' position.	マークしたポジションにあるキーワードが無効です。
% Incomplete command found at '^' position.	1つ以上のキーワードあるいは引数が不完全です。
% Ambiguous command found at '^' position.	入力した文字列があいまいです。
% Too many parameters.	入力した文字列が多すぎます。
% Wrong parameter found at '^' position.	マークしたポジションにあるパラメータが正しくありません。

1.6 履歴コマンドの保存

システムは、使用したコマンドを自動的に保存できます。保存したコマンドを必要に応じて呼び出し、繰り返し使用できます。

システムは、ログインユーザによって実行されたコマンドを自動的に、以下の 2 つの履歴バッファに保存します。

- user line 用のコマンド履歴バッファ
- すべての user line 用のコマンド履歴バッファ

表 1-6に 2 つのコマンド履歴バッファの違いを示します。

表 1-6 コマンド履歴バッファの比較

アイテム	user line のコマンド履歴バッファ	すべての user line のコマンド履歴バッファ
バッファに保存されるコマンドの種類	user lineにログイン中のユーザによって実行されたコマンド	すべてのログインユーザによって実行されたコマンド
ユーザがログアウトしたときに履歴がクリアされるか？	Yes	No
履歴を表示するコマンド	**display history-command**コマンド	**display history-command all**コマンド
履歴を実行するために呼び出す方法	バッファのコマンドを誘導します。Enterキーを押します。バッファ内のコマンドに移動するには上下の矢印キー（↑または↓）を使用します。 パスワード設定コマンドは呼び出せません。	履歴を呼び出すことはできません。
バッファサイズの設定方法	user line view で **history-command max-size** *size-value* コマンドを使用します。 デフォルト：10コマンド	バッファサイズをデフォルトから変更することはできません。 デフォルト：1024コマンド
バッファを無効にする方法	バッファサイズの設定を0にします。	バッファを無効にすることはできません。

履歴コマンドを使用したときのルールを示します。

- 正しいフォーマットで入力されたコマンドを履歴します。たとえば、不完全なコマンドが入力された場合、バッファされたコマンドも不完全となります。
- コマンドを入力するのにエイリアスを使用した場合、コマンドをバッファする前に表示されているコマンドあるいは *command* パラメータにエイリアスを変換します。
- 同一フォーマットのコマンドを連続して複数入力した場合、履歴コマンドには 1 回のみ履歴します。異なるフォーマットのコマンドを連続して複数入力された場合、各コマンドが履歴されます。たとえば **display cu** コマンドと **display current-configuration** コマンドの 2 つのエントリが連続して入力された場合、**display cu** コマンドが繰り返されたと認識し、コマンドのみが履歴されます。
- バッファが一杯の状態では、新しいコマンドを保存するため、最も古いコマンドの履歴が削除されます。

1.7 コマンド履歴バッファの管理と使用

1.7.1 コマンド履歴バッファ内のコマンドの表示

コマンド履歴バッファにコマンドを表示するには、任意のビューで次のコマンドを実行します。

操作	コマンド
ユーザ行のコマンド履歴バッファにコマンドを表示します。	**display history-command**
すべてのユーザ行のコマンド履歴バッファにコマンドを表示します。	**display history-command all**

1.7.2 コマンド履歴バッファ内のコマンドの呼び出し

⚠ **重要**：
パスワード設定コマンドは呼び出せません。

上下矢印キーを使用してコマンドに移動し、Enter キーを押します。

1.7.3 コマンド履歴バッファでコマンドの繰り返し

現在のコマンド履歴バッファにあるコマンドを複数回呼び出して実行できます。

I. ガイドライン

repeat コマンドはどのビューでも使用できます。ただし、コマンドを繰り返すには、まずコマンドのビューを入力する必要があります。複数のコマンドを繰り返すには、最初のコマンドのビューを最初に入力する必要があります。

repeat コマンドは実行された順にコマンドを実行します。

システムは対話型コマンドを繰り返すとき、ユーザの操作を待機します。

システムはすべてのパスワード設定コマンドをスキップします。

操作	コマンド
現在のユーザ行のコマンド履歴バッファでコマンドを繰り返します。	**repeat** [*number*] [**count** *times*] [**delay** *seconds*]

1.8 CLI表示の管理

この項では、CLI 表示を早急に認識できることを補助する管理機能を説明します。

1.8.1 出力のスクリーンの休止

表示する情報が 1 つのスクリーンを上回る場合、以下の表で示される方法のうちの 1 つを用いて情報出力を休止することができます。休止した箇所で----more----と表示します。詳細な情報を表示させるために出力管理キーに記載されているキーを使用したり、表示を停止することができます。

通常、24 行が 1 つのスクリーンに表示されます。スクリーン画面に表示される行数を変更するため、**screen-length** *screen-length* コマンドを使用できます。詳細は、QX-W2300AC シリーズアクセスコントローラコマンドマニュアルの“*2 基本機能*”の”*3 章 ログイン管理*”を参照してください。

現在のセッションで出力のスクリーンの休止を無効にすることができます。すべての出力は一度に表示され、最後にスクリーンが表示されるまで連続してスクリーンが更新されます。

I. 出力管理キー

キー	機能
Space	次画面ページの情報を示し続けます。
Enter	次のラインの情報を示し続けます。
Ctrl+C	表示とコマンド実行を中止します。
<PageUp>	前のページを表示します。
<PageDown>	次のページを表示します。

II. 複数のスクリーン出力機能の無効化

複数のスクリーン出力機能を無効にするには、user view で以下のコマンドを実行してください。

操作	コマンド	備考
現在のセッションで複数のスクリーン出力機能を無効にする	**screen-length disable**	デフォルト：**screen-length** *screen-length* コマンドの設定に依存します。 このコマンドは現在のセッションのみ適用されます。

1.8.2 表示コマンドの各出力ラインの番号表示

display コマンドで**| by-linenum** オプションを使用して、各出力ラインに番号を表示させることができます。

各出力ライン番号は 5 文字とコロン（：）あるいはハイフン（－）で表示されます。

| by-linenum オプションと**| begin** *regular-expression* オプションが指定される場合、正規表現にマッチしないすべての行でハイフンが表示されます。

display コマンドから各出力ラインに番号を表示させる方法を以下に示します。

操作	コマンド
番号付けされた**display**コマンドを表示する	**display** *command* **| by-linenum**

例：

VLAN 999 の情報を各出力ラインに番号付けして出力します。

```
<AC> 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: None
```

1.8.3 出力のフィルタリング

display コマンドに、[**|** [b**y-linenum**] { **begin** | **exclude** | **include** } *regular-expression*]&<1-128>オプションを使用して出力をフィルタリングすることができます。

- このオプションを使用すると、最大 128 個のフィルタ条件を指定できます。すべての条件を満たす出力行のみが表示されます。
- **by-linenum** – 各出力行の前に数字が表示されます。1 つのフィルタ条件でのみ指定する必要があります。
- **begin**– 指定した正規表現から後の情報を表示します。
- **exclude**– 指定した正規表現を含まない情報を表示します。
- **include**– 指定した正規表現を含む情報だけを表示します。
- *regular-expression*– 1～256 文字の文字列で、大文字と小文字を区別します。正規表現は表 1-7に示す特殊文字をサポートします。

複雑な正規表現を使用すると表示に多くの時間が必要となります。コマンドを中止する場合、**Ctrl+C** を押します。

表 1-7 サポートする正規表現の特殊文字

文字	意味	例
^	キャレット。この後の文字列が行の先頭にのみ現れる場合にマッチします。	正規表現“^user”は、”user”で始まる文字列にマッチします。”Auser”はマッチします。
$	ドル記号。この前の文字列が行の最後にのみ現れる場合にマッチします。	正規表現"user$”は、”user”で終わる文字列にマッチします。“userA”はマッチします。
. (period)	ピリオド。空白を含む任意の一文字を示します。	“.s”は“as”と“bs”どちらにもマッチします。
*	アスタリスク。直前の文字の 0回以上の繰り返しにマッチします。	”zo*”は“z”や“zoo”にマッチします。(zo)*は”zo”と”zozo”にマッチします。
+	プラス。直前の文字の1回以上の繰り返しにマッチします。	”zo+”は"zo"や”zoo”にマッチするが、"z" にはマッチしません。

文字	意味	例
|	パイプ。左または右の文字列にマッチします。	”def|int”は、”def”または”int”を含んでいる文字列とマッチします。
( )	括弧。文字列を指定します。"+”や“*”と一緒に使われます。	”(123A)”は文字列“123A”を意味し、“408(12)+”は”40812”” 408121212”にマッチします。”408”にはマッチしません。
\N	Nで表した回数の文字列の繰り返しを示します。文字列とは\の前の( )内の文字列です。 \の前の文字列が一文字の場合は、Nは1のみが指定できます。\の前の文字列がn個の場合、Nは1からnの指定ができます。	“(string)\1”は、stringstringを含む文字列にマッチします。“(string1)(string2)\2”はstring1string2string2を含む文字列にマッチします。“(string1)(string2)\1\2”はstring1string2string1string2を含む文字列にマッチします。
[ ]	ブラケットです。ブラケット内の1文字にマッチします。	“[16A]”は1、6、A、のいずれか1文字にマッチします。“1-36A”は1、2、3、6、Aのうちの1文字にマッチします。(-はハイフン)。“]”にマッチするためには“[”のすぐ後に“]”を入力します。たとえば“[]abc]”です。
[^]	[ ]内の文字列以外を指定します。	“[^16A]“は1、6、A以外で少なくとも1文字を含む文字列にマッチします（例”abc“）。1、6、Aを含む文字列(例”m16“)はマッチするが、1、6、Aのみの文字列（例1、16、16A）はマッチしません。
{n}	正の整数のn回の文字列にマッチします。	“o{2}”は“food”にマッチするが、“Bob”にマッチしません。
{n,}	正の整数のn回以上の文字列にマッチします。	“o{2,}”は“foooood”にマッチするが、“Bob”にマッチしません。
{n,m}	正の整数のnからm回以上の文字列にマッチします。mはnm以上の整数です。	“o{1,3}”は“fod”、“food”、“foooood“にマッチするが、“fd”にマッチしません。
\<	文字列の最初からマッチします。 \<の次の文字列のパターンを含みますが、英数字、アンダーバーは含まれません。	”\<do”は”domain”、”doa”にマッチします。
\>	文字列の最後からがstringにマッチします。\>の次の文字列のパターンを含みますが、英数字、アンダーバーは含まれません。	”do\>”は”undo”や"cdo"にマッチします。
\b	[^A- Za-z0-9_]に等しい文字列にマッチします。 英数字、アンダーラインは含みます。	“\ba”は“-a”にマッチするが、“2a”、“ba”にマッチしません。
\B	[A- Za-z0-9_]に等しい文字列にマッチします。 英数字、アンダーラインは含みません。	“\Bt”は“install”にマッチするが、“big top”にマッチしません。
\w	\Bと同一です。	“v\w”は“"vlan”、“service”にマッチします。
\W	\bと同一です。	“\Wa”は“-a”にマッチするが、"2a"、"ba"にマッチしません。
\	エスケープ文字です。この表に記載された特殊文字が\に続くと、その文字を取り除くことを意味します。	”\\”は、”\”を含む文字列にマッチします。”\^”は、”^”を含んでいる文字列にマッチ、”\\b”は”\b”を含んでいる文字列とマッチします。

例：

 # display current-configuration コマンドで**| begin line** を使用し、**line** を含む最後の行の後の情報を表示します。

```
<AC> display current-configuration | begin line
line class aux
 user-role network-admin
#
line class vty
 user-role network-operator
#
line aux 0
 user-role network-admin
#
line vty 0 63
 authentication-mode none
 user-role network-admin
 user-role network-operator
#
...
```

 # display ip routing-table コマンドで**| exclude Direct** を使用し、ダイレクトルート以外のルートを表示します。

```
<AC> display ip routing-table | exclude Static

Destinations : 13       Routes : 13

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
```

 # display current-configuration コマンドで**| include wlan** を使用し、**wlan** だけを含むエントリを表示します。

```
<AC> display current-configuration | include wlan
wlan global-configuration
wlan ap-group default-group
...
```

 # ログバッファ内の SHELL と VTY の両方を含むログエントリを表示します。

```
<AC> display logbuffer | include SEHLL | include VTY
%Feb   6 10:38:12:320 2020 Sysname SHELL/5/SHELL_LOGIN: VTY logged in from
169.254.100.171.
%Feb   6 10:52:32:576 2020 Sysname SHELL/5/SHELL_LOGOUT: VTY logged out from
169.254.100.171.
%Feb   6 16:03:27:100 2020 Sysname SHELL/5/SHELL_LOGIN: VTY logged in from
169.254.100.171.
%Feb   6 16:44:18:113 2020 Sysname SHELL/5/SHELL_LOGOUT: VTY logged out from
169.254.100.171.
```

1.8.4 display コマンドのファイルへの保存

display コマンドは装置の設定と動作情報を示します。出力は時間、ユーザ設定、動作によって異なります。今後の復旧やトラブルシューティング用に設定をファイルに保存することができます。

display コマンドから出力を保存する方法を、以下の手順の 1 つを使用します。

- ファイルを分離して出力を保存します。1 つの **display** コマンド用に 1 つのファイルを使用する場合に使用します。
- ファイルの最後に出力を追記して保存します。複数の **display** コマンド用に 1 つのファイルを使用する場合に使用します。

display コマンドからファイルからに保存するため、以下のコマンドのどちらか 1 つを使用します。

操作	コマンド
コマンドからファイルを分離して出力を保存する	**display** *command* **>** *filename*
ファイルの最後に出力を追記する	**display** *command* **>>** *filename*

例：

VLAN 1 の設定をファイル名 vlan.txt のファイルに分離して保存します。

```
<AC> display vlan 1 > vlan.txt
```

VLAN 1 の設定がファイル名 vlan.txt のファイルに保存されているかどうか確認します。

```
<AC> more vlan.txt
VLAN ID: 1
 VLAN type: Static
 Route interface: Not configured
 Description: VLAN 0001
 Name: VLAN 0001
 Tagged ports:   None
 Untagged ports:
```

ファイル名 vlan.txt の最後に VLAN 999 の設定を追記します。

```
<AC> display vlan 999 >> vlan.txt
```

VLAN 999 の設定がファイル名 vlan.txt のファイルに追記保存されているかどうか確認します。

```
<AC> more vlan.txt
VLAN ID: 1
 VLAN type: Static
 Route interface: Not configured
 Description: VLAN 0001
 Name: VLAN 0001
 Tagged ports:   None
 Untagged ports:
    GigabitEthernet1/0/2

 VLAN ID: 999
 VLAN type: Static
 Route interface: Configured
 IP address: 192.168.2.1
 subnet mask: 255.255.255.0
```

```
Description: For LAN Access
Name: VLAN 0999
Tagged ports:   None
Untagged ports:
```

1.8.5 display コマンドからの出力の有効的な表示、管理

display コマンドからファイルへの出力とフィルタリングを組み合わせることができます。

- **display** コマンドから各出力ラインを番号付けします。
- **display** コマンドからの出力をフィルタします。
- **display** コマンドからの出力をファイルへ保存します。

以下に **display** コマンドからの出力の有効的な表示、管理を組み合わせる方法を示します。これはすべての view で実行可能です。

操作	コマンド
displayコマンドからの出力の有効的な表示、管理を組み合わせる	**display** *command* [| [**by-linenum**] { **begin** | **exclude** | **include** } *regular-expression*]&<1-128> [> *filename* | >> *filename*]

例：

各ラインに番号付けして、分離したファイル test.txt に、稼働中の設定を保存します。

```
<AC> display current-configuration | by-linenum > test.txt
```

ファイル test.txt に、稼働中の設定の中で snmp を含む行を追記します。

```
<AC> display current-configuration | include snmp >> test.txt
```

user-group で始まる最初の行から行番号をつけて稼働中の設定を表示します。

```
<AC> display current-configuration | by-linenum begin user-group
  114:  user-group system
  115-  #
  116-  return
```

//（：）は user-group が含まれる行を示します。（ー）は user-group が含まれない行を示します。

1.9 稼働中の設定の保存

すべての view で、**save** コマンドを使用して、実行されたコマンドを設定ファイルに保存することができます。設定ファイルに保存されたコマンドは、再起動して復活させることができます。**save** コマンドは、指定された情報を表示する **display** コマンドや指定された情報をクリアする **reset** コマンドのような 1 回限りのコマンドには適用されません。1 回限りのコマンドは保存されません。詳細は、QX-W2300AC シリーズアクセスコントローラコマンドマニュアルの“*2 基本機能*”の”*7 章 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。

目次

このセクションのページは**2-x-x** です。

2章 RBAC 2-1
2.1 概要 2-1
2.1.1 許可の割り当て 2-1
2.1.2 ユーザロールの割り当て 2-3
2.2 設定作業リスト 2-4
2.3 ユーザロールの作成 2-4
2.4 ユーザロールのルールの設定 2-4
2.4.1 設定の制限とガイドライン 2-5
2.4.2 設定手順 2-5
2.5 機能グループの設定 2-5
2.6 リソースアクセスポリシーの設定 2-6
2.6.1 ユーザロールのインタフェースポリシーの設定 2-6
2.6.2 ユーザロールのVLANポリシーの設定 2-7
2.7 ユーザロールの割り当て 2-7
2.7.1 デフォルトユーザロール機能の有効化 2-7
2.7.2 リモートAAA認証ユーザへのユーザロールの割り当て 2-8
2.7.3 ローカルAAA認証ユーザへのユーザロールの割り当て 2-8
2.7.4 ユーザラインで非AAA認証ユーザへのユーザロールの割り当て 2-9
2.8 一時的なユーザロールの許可設定 2-9
2.8.1 設定ガイドライン 2-9
2.8.2 ユーザロールの認証の設定 2-11
2.8.3 一時的なユーザロールの許可の取得 2-11
2.9 RBAC設定の表示と維持 2-11
2.10 RBACの設定例 2-12
2.10.1 ローカルAAA認証ユーザのRBACの設定例 2-12
2.10.2 RADIUS認証ユーザのRBACの設定例 2-14
2.10.3 RBACの一時的なユーザロールの許可の設定例 2-18
2.11 RBACのトラブルシューティング 2-21
2.11.1 ローカルユーザで許可していないコマンドにアクセスできる 2-21
2.11.2 RADIUSユーザによるログインが常に失敗する 2-21

2章 RBAC

2.1 概要

RBAC(Role based access control)は、ユーザロールの設定に従って、ユーザのアクセスとシステムリソースを制御します。システムリソースにはインタフェース、VLAN を含みます。

複数のユーザにアクセス許可を与える場合、同一のユーザロールを異なるユーザに適用してコマンドやリソースへのアクセス許可を与えることも可能です。ユーザと異なりユーザロールは持続するため、ユーザの許可を分割することで、許可管理が容易になります。また、ユーザの責任分担の変更、追加、削除を行う場合、運用中のユーザロール設定の変更や、新規ユーザロールの作成、割り当てをするだけで管理可能です。

2.1.1 許可の割り当て

以下の方法により、ユーザロールに許可を割り当てることができます。

- アクセスの可否を決定するためのルールを定義します。
- アクセスを許可するインタフェース、VLAN を指定するアクセスポリシーを定義します。

インタフェース、VLAN のリソースに関連したコマンドを使用するには、ユーザロールで、必要なコマンドとリソースにアクセスできるように設定します。

たとえば、ユーザロールは、**qos apply policy** コマンドと **Ten-GigabitEthernet** 1/0/1 インタフェースにアクセスできるように設定した場合、このユーザロールでは、interface view に移行し、**qos apply policy** コマンドを使用することができますが、ほかの interface view に入ることはできません。またほかのコマンドを使用することもできません。もしユーザロールでインタフェースへのアクセスを設定し、**qos apply policy** コマンドへのアクセス許可していない場合、**qos apply policy** コマンドを使用することはできません。

I. ユーザロールのルール

ユーザロールのルールは、コマンドを許可あるいは禁止します。以下に示すように、異なるアクセス制御のルールを詳細に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セットのアクセスを管理します。
- **Feature rule**– コマンドタイプにより、コマンドへのアクセスを管理します。
- **Feature group rule**– コマンドタイプにより、コマンドのグループへのアクセスを管理します。

コマンドは以下のタイプにもとづいて管理されます。

- **Read**– 設定の表示と保守コマンドです。たとえば、**display** コマンド、**dir** コマンドがあります。
- **Write**– システムの機能を設定するコマンドです。たとえば **info-center enable** コマンド、**debugging** コマンドがあります。

- **Execute**– 指定した機能を実行するコマンドです。たとえば **ping** コマンド、**ftp** コマンドがあります。

ユーザロールは、ユーザロールのルールで許可された指定コマンドセットにアクセスできます。ユーザロールは定義済みのユーザロール(*sys-n* で識別されます)とユーザ定義のユーザロールがあります。

II. リソースアクセスポリシー

リソースアクセスポリシーは、以下のタイプのように、システムリソースへのユーザロールのアクセスを管理します。

- **Interface policy**– インタフェースへのアクセスを管理します。
- **VLAN policy**– VLAN へのアクセスを管理します。

リソースアクセスポリシーでは **display** コマンドでのインタフェース、VLAN の情報表示についてのアクセス管理は行いません。ユーザロールルールに **display** コマンドのオプションを指定することで、アクセス制御をすることができます。

III. 定義済みユーザロール

システムには定義済みのユーザロールがあります。すべてのユーザロールはすべてのシステムリソース(インタフェース、VLAN)にアクセスできますが、これらのコマンドはアクセス許可とは異なります。表 2-1を参照してください。

すべての定義済みのユーザロールで、**network-admin** と **Level-15** は以下のことを行うことができます。

- RBAC 機能にアクセスすることができます。
- user line view の user-role コマンド、authentication-mode コマンド、protocol inbound コマンド、set authentication password コマンド等の設定変更ができます。
- ローカルユーザとローカルユーザグループの作成、変更、削除を行うことができます。ローカルユーザとローカルユーザグループを設定する権限を持つほかのユーザロールは、自身のパスワードを変更することのみ行うことができます。
- Level-0～Level-14 のユーザは、**display history-command all** コマンドを除いて自身の許可を変更することができます。

表 2-1 定義済みユーザロールと許可

ユーザロール名	許可
network-admin	システムのすべての機能とリソースにアクセス可能です。
network-operator	• すべての機能の**display**コマンドとリソースにアクセス可能です。ユーザロールでアクセス可能なコマンドを表示する場合、**display role**コマンドを使用します。 • 自身のパスワードを変更するため、ローカルユーザへのローカル認証が有効です。

ユーザロール名	許可

level-*n* (*n* = 0 ～ 15)	• **level-0**– **ping**、**quit**、**ssh2**、**super**、**system-view**、**telnet**、**tracert** コマンドを含む診断コマンドにアクセスできます。**level-0** のアクセス権は設定変更可能です。
	• **level-1**– **level-0**のコマンドに加えて**display history-command all**コマンドを除く**display**コマンドとリソースが使用可能です。**level-0**のアクセス権は設定可能です。
	• **level-2**～**level-8**、**level-10** ～**level-14**– デフォルトでアクセス権はありません。アクセス権は設定変更可能です。
	• **level-9**– 以下の機能を除いたすべての機能とリソースにアクセス可能です。もしユーザロールが**level-9**のローカルユーザアカウントのユーザにログインした場合、自身のアカウントのパスワードを変更することができます。**level-9**のアクセス権は設定変更可能です。
	  • RBAC-非デバッグコマンド
	  • ローカルユーザ
	  • ファイル管理
	  • 装置管理
	  • **display history-command all**コマンド
	• **level-15**– network-adminと同じアクセス権があります。

guest-manager	ゲスト関連のWebページのみへのアクセス権があります。コマンドへのアクセス権はありません。

2.1.2 ユーザロールの割り当て

ユーザに、少なくとも 1 つのユーザロールを割り当てることによって、アクセス権を割り当てます。ユーザは割り当てられたユーザロールで許可設定されたコマンドとリソースを使用することができます。たとえば、以下に示すユーザロールを設定することで、すべてのインタフェースで **qos apply policy** コマンドを使用することができます。

- ユーザロール A は **qos apply policy** コマンドの禁止と GigabitEthernet 1/0/1 インタフェースのみアクセス許可を行います。
- ユーザロール B は **qos apply policy** コマンドの許可とすべてのインタフェースのアクセス許可を設定します。

ユーザロールの割り当ては認証方法に依存して以下の方法があります。

- **AAA 許可**– scheme 認証が使用されている場合、AAA モジュールはユーザロールの割り当てを操作できます。
  - □ ユーザがローカル認証にパスした場合、装置はローカルユーザアカウントで指定されたユーザロールを割り当てます。
  - □ ユーザがリモート認証にパスした場合、ユーザにサーバで指定したユーザロールを割り当てます。AAA サーバは RADIUS サーバを使用できます。
- **非 AAA 許可**– ユーザが認証を使用していない、あるいはパスワード認証の場合、装置はユーザラインで指定されたユーザロールを割り当てます。この方法は公開鍵あるいはパスワード－公開鍵認証を使用する SSH クライアントにも適用されます。SSH クライアントに割り当てられたユーザロールは、ローカル管理に関係するユーザアカウントに指定されます。

AAA の詳細は、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*13 ユーザアクセスと認証*“の”*3 章 AAA*“を参照してください。SSH の詳細は、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*15 セキュリティ*”の”*5 章 SSH*”を参照してください。ユーザラインの詳細は、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*2 基本機能*”の”*1 章 CLI*”を参照してください。

2.2 設定作業リスト

作業リスト
(必須設定項目)ユーザロールの作成
(必須設定項目)ユーザロールのルールの設定
(オプション設定項目)機能グループの設定
(オプション設定項目)リソースアクセスポリシーの設定
(オプション設定項目)ユーザロールの割り当て
(オプション設定項目)一時的なユーザロールの許可設定

2.3 ユーザロールの作成

詳細なアクセス管理を行うために、あらかじめ定義されたユーザロールに加えて、64 個までカスタムユーザロールを作成することができます。

以下にユーザロールを作成する手順を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． ユーザロールを作成し、user role view に移行する	**role name** *role-name*	デフォルト：定義済みのユーザロール ● network-admin ● network-operator ● level-n (nは0～15です) level-0～14のユーザロールの許可と説明のみ設定することができます。
3． (オプション設定項目)ユーザロールの説明を設定する	**description** *text*	デフォルト：設定なし

2.4 ユーザロールのルールの設定

指定されたコマンドにユーザロールのアクセスを許可あるいは禁止するため、コマンド、機能、機能グループを設定します。

2.4.1 設定の制限とガイドライン

RBAC ユーザロールのルールを設定するとき、以下の制限とガイドラインに従ってください。

- 1 つのユーザロールには最大 256 個までのルールを設定することができます。ただし、システム全体で 1024 個を超えるルールを作成することはできません。
- ユーザロールの変更、追加、削除は、変更完了後にユーザロールでログインしたユーザのみ適用されます。
- 同じタイプの 2 つ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、以下のコマンドが設定されたルールがある場合、ユーザロールは、**tracert** コマンドを使用しますが、**ping** コマンドを使用しません。
  - **rule 1 permit command ping**
  - **rule 2 permit command tracert**
  - **rule 3 deny command ping**
- level-0～14 のユーザロールにおいて、定義済みのユーザロールとユーザ定義のユーザが混在する場合、ユーザ定義のユーザロールが適用されます。

2.4.2 設定手順

以下にユーザロールのルールの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. user role view に移行する	**role name** *role-name*	―
3. ルールを設定する	• コマンドルールの設定：**rule** *number* { **deny** | **permit** } **command** *command-string* • 機能ルールの設定：**rule** *number* { **deny** | **permit** } { **execute** | **read** | **write** } * **feature** [*feature-name*] • 機能グループの設定：**rule** *number* { **deny** | **permit** } { **execute** | **read** | **write** } * **feature-group** *feature-group-name*	デフォルト：なし ユーザロールを複数のルールを作成する場合、繰り返し設定します。最大256まで設定することができます。 ⚠ **重要：** 機能ルールを設定したとき、システムで有効な機能のみ指定することができます。省略した機能名ではなく、大文字小文字を区別して、表示された機能と同じ機能名を正確に設定してください。

2.5 機能グループの設定

機能グループは、機能のセットにコマンドのアクセス権をまとめて割り当てます。あらかじめ定義された機能グループに加えて最大 64 個の機能グループを作成することができ、複数の機能グループに機能を割り当てることができます。

以下に機能グループの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―

操作	コマンド	補足
2. 機能グループを作成し、feature group view に移行する	**role feature-group name** *feature-group-name*	デフォルト： • **L2**– すべてのレイヤ2コマンドを含みます。 • **L3**– すべてのレイヤ3コマンドを含みます。 この2つのグループはユーザで設定できません。
3. 機能グループに機能を追加する	**feature** *feature-name*	デフォルト：設定なし 複数の機能を作成する場合、繰り返し設定します。 ⚠ **重要：** システムで有効な機能のみ指定することができます。省略した機能名ではなく、大文字小文字を区別して、表示された機能と同じ機能名を正確に設定してください。

2.6 リソースアクセスポリシーの設定

各ユーザロールは 1 つのインタフェースポリシー、VLAN ポリシーを持ちます。デフォルトでポリシーはすべてのインタフェース、VLAN にアクセスするユーザロールを許可します。ユーザが定義したユーザロールのポリシー、インタフェース、VLAN へのアクセス制限を行う、あらかじめ定義された Level-*n* のユーザロールを変更することができます。変更されたポリシーは、変更後にユーザロールでログインしたユーザのみ適用されます。

2.6.1 ユーザロールのインタフェースポリシーの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. user role view に移行する	**role name** *role-name*	ー
3. interface policy view に移行する	**interface policy deny**	デフォルト：すべてのインタフェースへのユーザロールのアクセスは有効です。 **permit interface**コマンドが設定されていない場合、このコマンドにより、すべてのインタフェースへのアクセスが禁止されます。
4. (オプション設定項目) 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指定する	**permit interface** *interface-list*	デフォルト：設定なし アクセス可能なインタフェースを追加する場合、この操作を繰り返し行ってください。

2.6.2 ユーザロールの VLAN ポリシーの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． user role view に移行する	**role name** *role-name*	ー
3． VLAN policy view に移行する	**vlan policy deny**	デフォルト：すべてのVLANへのユーザロールのアクセスは有効です。 このコマンドは**permit vlan**コマンドが設定されていない場合、すべてのVLANへのアクセスを禁止します。
4． (オプション設定項目) ユーザロールにアクセス可能な VLAN を指定する	**permit vlan** *vlan-id-list*	デフォルト：設定なし アクセス可能なVLANを追加する場合、この操作を繰り返し行ってください。

2.7 ユーザロールの割り当て

システムにユーザロールを管理するため、少なくとも 1 つのユーザロールを割り当てる必要があります。装置または、サーバによって少なくとも 1 つのユーザロールが割り当てられていることを確認してください。ユーザロールはリモート AAA 認証ユーザ、ローカル AAA 認証ユーザ、AAA 認証を行わないユーザで割り当てる手順が異なります。AAA 認証の詳細は、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*13 ユーザアクセスと認証*“の”*3 章 AAA*“を参照してください。

2.7.1 デフォルトユーザロール機能の有効化

AAA サーバがユーザロールをユーザに許可していない場合、デフォルトユーザロール機能は AAA で認証されているユーザにデフォルトユーザロールを割り当てます。ユーザはデフォルトユーザロールでシステムにアクセスできます。

デフォルトユーザロールとしてシステムに存在するすべてのユーザロールを指定することができます。

以下に AAA 認証ユーザにデフォルトユーザロール機能を有効にする設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． デフォルトユーザロール機能を有効にする	**role default-role enable** [*role-name*]	デフォルト：無効 ローカルユーザ用に許可されていない場合、デフォルトユーザロール機能を有効にする必要があります。

2.7.2 リモート AAA 認証ユーザへのユーザロールの割り当て

リモート AAA 認証ユーザリモート認証サーバでユーザロールを設定します。RADIUS ユーザにユーザロールを設定する方法については、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*13 ユーザアクセスと認証*“の”*3 章 AAA*“を参照してください。

🕮 **メモ：**

- 特権レベルによるアクセス管理に互換性を持たせるために、装置は自動的に、AAA サーバによって割り当てられた特権レベルにもとづくユーザレベル(0～15)を、RBAC ユーザロール(Level-0～Level-15)に変換します。
- AAAサーバが割り当てたユーザレベルによりユーザロールをユーザに割り当てる場合、ユーザレベルとユーザロールの両方にアクセス可能なコマンドとリソースの組み合わせを使用することができます。

2.7.3 ローカル AAA 認証ユーザへのユーザロールの割り当て

ローカルユーザアカウントのローカル AAA 認証ユーザにユーザロールを設定します。各ローカルユーザはデフォルトユーザロールを持っています。もしデフォルトユーザロールが適当でない場合、削除する必要があります。

以下にローカルユーザにユーザロールを割り当てる設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． ローカルユーザを作成し、local user view に移行する	**local-user** *user-name* [**class** { **manage** | **network** }]	―
3． ユーザがユーザロールを保有することを許可する	**authorization-attribute user-role** *role-name*	デフォルト：ユーザロール network-adminあるいはlevel-15のユーザが作成したローカルユーザのユーザロールは network-operatorが割り当てられます。 ユーザに最大64のユーザロールを割り当てる場合、この操作を繰り返し行ってください。
4． (オプション設定項目) 不要なユーザロールを削除する	**undo authorization-attribute user-role** *role-name*	ユーザは割り当てられたユーザロールに対してアクセス可能なシステムのアイテムとリソースを使用することができます。 ユーザロールが不要である場合(たとえばデフォルトユーザロール)、ユーザロールを削除するため、このコマンドを使用します。

2.7.4 ユーザラインで非 AAA 認証ユーザへのユーザロールの割り当て

ユーザラインで以下の 2 タイプのログインユーザにユーザロールを指定します。

- パスワード認証あるいは認証をしていないユーザにユーザロールを指定します。
- 公開鍵あるいはパスワード公開鍵認証を使用する SSH クライアントユーザロールを指定します。SSH クライアントに割り当てられるユーザロールは関連するローカル装置管理ユーザアカウントで指定されます。

ユーザラインの詳細は、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*2 基本機能*”の”*2 章 CLI によるログイン*”を参照してください。SSH の詳細は、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*15 セキュリティ*”の”*5 章 SSH*”を参照してください。

以下にユーザラインで非 AAA ユーザにユーザロールを割り当てる設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. user line view あるいは user line class view に移行する.	● user line viewに移行する： **line** { *first-num1* [*last-num1*] | { **aux** | **vty** } *first-num2* [*last-num2*] } ● user line class viewに移行する： **line class** { **aux | vty** }	user line viewとuser line class viewの優先順位と設定方法については、QX-W2300ACシリーズアクセスコントローラオペレーションマニュアルの“*2 基本機能*”の”*2章 CLIによるログイン*”を参照してください。
3. user line 上でユーザロールを指定する	**user-role** *role-name*	デフォルト：AUXユーザラインでnetwork-adminが指定されます。ほかのユーザラインでnetwork-operatorが指定されます。 ユーザに最大64のユーザロールを割り当てることができます。複数のユーザロールを割り当てる場合、この操作を繰り返し行ってください。

2.8 一時的なユーザロールの許可設定

一時的なユーザロールを許可することで、ログインしていないユーザが装置に再接続することなく、ユーザロールを取得することができます。この機能は設定を行うために一時的にユーザロールを使用する場合に有効です。

一時的なユーザロールの許可の設定は現在のログインにのみ適用されます。この機能は、すでにログインしているユーザアカウントのユーザロールの設定を変更しません。次回、ユーザアカウントでログインする場合、元のユーザロールの設定が適用されます。

2.8.1 設定ガイドライン

一時的なユーザロールの許可を設定する場合、以下のガイドラインに従ってください。

- ユーザが装置に再接続をしないで別のユーザロールを取得するため、ユーザロール認証を設定する必要があります。表 2-2に有効な認証モードと設定要件を記載します。
- RADIUS 認証が使用されている場合、以下のルールを適用します。
  - 装置はユーザロールの認証を要求するためのユーザ名を使用しません。装置は**$enab*n*$**のフォーマットを使用します。*n* はユーザロールレベルです。ドメイン名はユーザ名に含まれません。パスワードが正しいとき、ユーザロールの認証にパスすることができます。
  - level-*n* のユーザロールを取得するため、RADIUS サーバで**$enab*n*$**のフォーマットで level-*n* のユーザのユーザアカウントを作成する必要があります。*n* はターゲットのユーザロールのレベルです。たとえば、level-3 のユーザロールの許可を取得する場合、ユーザ名を入力します。装置はサーバからユーザロール認証を要求するため、ユーザ名**$enab3$**を使用します。
  - 非 level-n のユーザロールを取得するため、以下の処理を行う必要があります。
    - サーバでユーザアカウント**$enab0$**を作成します。
    - **allowed-roles="***role***"**の形式のアカウントの cisco-av-pair 属性を設定します。変数のロールはターゲットのユーザロールを示します。
- 装置は以下の順番でユーザロール認証の認証ドメインを選択します。

a) 入力されたユーザ名が含まれるISPドメイン

b) デフォルトISPドメイン

- ユーザロールを許可した後、**quit** コマンドを実行した場合、現在のユーザラインをログアウトします。

表 2-2 ユーザロールの認証モード

キーワード	認証モード	記述
local	ローカルパスワード認証のみ(local-only)	装置は認証用にローカルに設定されたパスワードを使用します。 ローカルパスワード認証が設定されない場合、AUXユーザは文字列を入力するか、何も入力しないでEnterキーを押すことでユーザロール許可を取得することができます。
scheme	RADIUSによるリモートAAA認証(remote-only)	装置はリモート認証を行うためRADIUSサーバにユーザ名とパスワードを送信します。 このモードを使用するため、以下の設定を実行する必要があります。 ● 要求されたRADIUS scheme、ユーザのschemeを使用するISP domainを設定します。詳細はQX-W2300ACシリーズアクセスコントローラオペレーションマニュアルの“*13 ユーザアクセスと認証*“の”*3章AAA*“を参照してください。 ● RADIUSサーバにユーザアカウントとパスワードを追加します。
local scheme	最初にローカルパスワード認証を行い、次にリモートAAA認証を行う(local-then-remote)	最初にローカルパスワード認証が実行されます。もしローカルパスワードが設定されていない場合、以下となります。 ● 装置はAUX およびVTYユーザ用にリモートAAA認証を実行します。
scheme local	最初にリモートAAA認証を行い、次にローカルパスワード認証を行う(remote-then-local)	最初にAAA認証が実行されます。ローカルパスワード認証は以下のいずれかの状況で実行されます。 ● リモートRADIUSサーバからの応答がありません。 ● 装置でのAAAの設定が無効です。

2.8.2 ユーザロールの認証の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． 認証モードを設定する	**super authentication-mode** { **local** | **scheme** } *	デフォルト：ローカル認証のみ適用します。
3． (オプション設定項目) ー時的なユーザロール許可のデフォルトターゲットのユーザロールを指定する	**super default role** *rolename*	デフォルト：**network-admin**
4． ユーザロールのローカル認証パスワードを設定する	**super password** [**role** *rolename*] [{ **hash** | **simple** } *string*]	デフォルト：設定なし ローカルパスワード認証のために、この操作を使用します。 もし**role** *rolename*を指定しない場合、コマンドは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。

2.8.3 ー時的なユーザロールの許可の取得

ログインを行うユーザアカウントにユーザロールがない AUX や VTY ユーザは、ユーザロールを使用する前に認証をパスする必要があります。

user view で以下の設定を行います。

操作	コマンド	補足
ユーザロールを使用したー時的な許可を取得する	**super** [*rolename*]	[*rolename*]を指定しない場合、ー時的なユーザロールの許可のデフォルトターゲットユーザロールを取得します。 3回連続してパスワードの認証に失敗すると、ユーザロールの取得に失敗します。 現在のユーザロールが**super**コマンドを実行できることを確認してください。

2.9 RBAC設定の表示と維持

すべての view で **display** コマンドを実行することができます。

操作	コマンド
ユーザロール情報を表示する	**display role** [**name** *role-name*]

操作	コマンド
ユーザロール機能の情報を表示する	**display role feature** [**name** *feature-name* | **verbose**]
ユーザロール機能グループ情報を表示する	**display role feature-group** [**name** *feature-group-name*] [**verbose**]

2.10 RBACの設定例

2.10.1 ローカル AAA 認証ユーザの RBAC の設定例

I. ネットワーク要件

図 2-1に示すように、装置は 192.168.1.58 の Telnet ユーザ用にローカル AAA 認証を実行します。Telnet ユーザはユーザ名 **user1@bbb** を持ち、ユーザロール **role1** を割り当てます。

role1 に以下の許可を設定します。

- すべての機能の read コマンドを実行します。
- VLAN10～VLAN20 のみ設定できるようにします。他の VLAN へのアクセスは拒否されます。

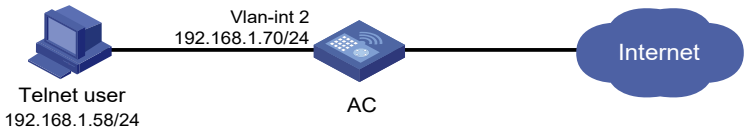


図 2-1 ネットワーク図

II. 設定手順

Telnetユーザが接続されているVLANインタフェース2にIPアドレスを割り当てます。

```
<AC> system-view
[AC] interface vlan-interface 2
[AC-Vlan-interface2] ip address 192.168.1.70 255.255.255.0
[AC-Vlan-interface2] quit
```

Telnet サーバを有効にします。

```
[AC] telnet server enable
```

Telnet ユーザのユーザラインで scheme 認証を有効にします。

```
[AC] line vty 0 4
[AC-line-vty0-4] authentication-mode scheme
[AC-line-vty0-4] quit
```

ISP ドメイン **bbb** 用にローカル認証、許可を有効にします。

```
[AC] domain bbb
[AC-isp-bbb] authentication login local
[AC-isp-bbb] authorization login local
[AC-isp-bbb] quit
```

ユーザロール **role1** を作成します。

```
[AC] role name role1
```

すべての機能の read コマンドにアクセスするようにユーザロールを許可するルール 1 を設定します。

```
[AC-role-role1] rule 1 permit read feature
```

VLAN を作成し、VLAN view でコマンドにアクセスするユーザロールを許可するルール 2 を設定します。

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

VLAN 10～VLAN 20 のみ設定するユーザロールを許可するために VLAN ポリシーを変更します。

```
[AC-role-role1] vlan policy deny
[AC-role-role1-vlanpolicy] permit vlan 10 to 20
[AC-role-role1-vlanpolicy] quit
[AC-role-role1] quit
```

装置管理ローカルユーザ **user1** を作成し、local user view に移行します。

```
[AC] local-user user1 class manage
```

ユーザ用にプレーンテキストのパスワード **123456TESTplat&!**を設定します。

```
[AC-luser-manage-user1] password simple 123456TESTplat&!
```

サービスタイプを Telnet に設定します。

```
[AC-luser-manage-user1] service-type telnet
```

ユーザにユーザロール **role1** を割り当てます。

```
[AC-luser-manage-user1] authorization-attribute user-role role1
```

ユーザからデフォルトユーザロール **network-operator** を削除します。この設定はユーザでユーザロール **role1** のみ許可するために行います。

```
[AC-luser-manage-user1] undo authorization-attribute user-role network-operator
[AC-luser-manage-user1] quit
```

III. 設定の確認

AC に Telnet を行い、AC にアクセスするため、ユーザ名とパスワードを入力します(詳細は省略します)。

VLAN 10～VLAN 20 を作成できることを確認します。この例では VLAN10 を使用します。

```
<AC> system-view
[AC] vlan 10
[AC-vlan10] quit
```

VLAN 10～VLAN 20 以外の VLAN を作成できないことを確認します。この例では VLAN30 を使用します。

```
[AC] vlan 30
Permission denied.
```

すべての機能の read コマンドが使用できることを確認します。この例では **display clock** コマンドを使用します。

```
[AC] display clock
09:31:56 UTC Fri 01/01/2016
[AC] quit
```

機能の書き込みあるいは実行コマンドが使用できないことを確認します。

```
<AC> debugging role all
Permission denied.
<AC> ping 192.168.1.58
Permission denied.
```

2.10.2 RADIUS 認証ユーザの RBAC の設定例

I. ネットワーク要件

図 2-2に示すように、装置は 10.1.1.1/24 の FreeRADIUS サーバを使用し、Telnet ユーザを含むログインユーザに AAA サービスを提供します。Telnet ユーザはユーザ名 **hello@bbb** を持ち、ユーザロール **role2** が割り当てられます。

ユーザロール **role2** に以下の許可を設定します。

- ISP domain view ですべてのコマンドを実行します。
- **arp**、**radius** 機能の read、write コマンドを実行します。
- **acl** 機能の read コマンドへのアクセスを禁止します。
- VLAN 1～VLAN 20 のみを設定変更可能にします。

AC と FreeRADIUS サーバは共有鍵 **expert**、認証ポート 1812 を使用します。装置はサーバにドメイン名のユーザ名を送信します。

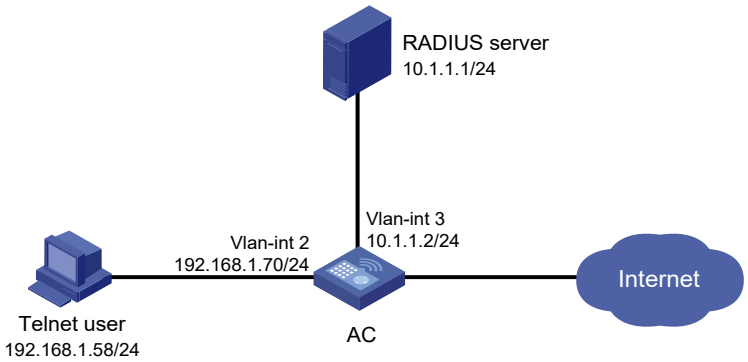


図 2-2 ネットワーク図

II. 設定手順

Switch と RADIUS サーバで設定が一致していることを確認します。

1)　AC を設定します。

Telnet ユーザと同じサブネットから IP アドレスを VLAN インタフェース 2 に割り当てます。

```
<AC> system-view
[AC] interface vlan-interface 2
[AC-Vlan-interface2] ip address 192.168.1.70 255.255.255.0
[AC-Vlan-interface2] quit
```

RADIUS サーバと同じサブネットから IP アドレスを VLAN インタフェース 3 に割り当てます。

```
[AC] interface vlan-interface 3
[AC-Vlan-interface3] ip address 10.1.1.2 255.255.255.0
[AC-Vlan-interface3] quit
```

Telnet サーバを有効にします。

```
[AC] telnet server enable
```

Telnet ユーザ用に、ユーザラインの scheme 認証を有効にします。

```
[AC] line vty 0 4
[AC-line-vty0-4] authentication-mode scheme
[AC-line-vty0-4] quit
```

RADIUS scheme **rad** を作成し、RADIUS scheme view に移行します。

```
[AC] radius scheme rad
```

scheme で、プライマリサーバアドレス 10.1.1.1、サービスポート 1812 を指定します。

```
[AC-radius-rad] primary authentication 10.1.1.1 1812
```

AC とサーバの認証 scheme における専用の共有鍵として expert を設定します。

```
[AC-radius-rad] key authentication simple expert
[AC-radius-rad] quit
```

ISP ドメイン **bbb** 用の認証、許可 scheme として scheme **rad** を指定します。

重要：

RADIUS ユーザ認証の情報は許可(authorization)属性を認証(authentication)の応答に含められて送信します。そのため、authorization の radius-scheme と authentication の radius-scheme には同じ scheme を使用してください。

```
[AC] domain bbb
[AC-isp-bbb] authentication login radius-scheme rad
[AC-isp-bbb] authorization login radius-scheme rad
[AC-isp-bbb] quit
```

機能グループ **fgroup1** を作成します。

```
[AC] role feature-group name fgroup1
```

機能グループに機能 **arp**、**radius** を追加します。

```
[AC-featuregrp-fgroup1] feature arp
[AC-featuregrp-fgroup1] feature radius
[AC-featuregrp-fgroup1] quit
```

ユーザロール **role2** を作成します。

```
[AC] role name role2
```

ISP view ですべてのコマンドを使用するユーザロールを許可するルール 1 を設定します。

```
[AC-role-role2] rule 1 permit command system-view ; domain *
```

fgroup1 ですべての機能の read、write コマンドを使用するユーザロールを許可するルール 2 を設定します。

```
[AC-role-role2] rule 2 permit read write feature-group fgroup1
```

acl 機能の read コマンドのアクセスを禁止するルール 3 を設定します。

```
[AC-role-role2] rule 3 deny read feature acl
```

VLAN を作成し、VLAN view ですべてのコマンドを使用するユーザロールを許可するルール 4 を設定します。

```
[AC-role-role2] rule 4 permit command system-view ; vlan *
```

interface view に移行し、interface view ですべてのコマンドを使用するユーザロールを許可するルール 5 を設定します。

```
[AC-role-role2] rule 5 permit command system-view ; interface *
```

VLAN 1～VLAN 20 を除く VLAN の設定を無効にするユーザロール VLAN ポリシーを設定します。

```
[AC-role-role2] vlan policy deny
[AC-role-role2-vlanpolicy] permit vlan 1 to 20
[AC-role-role2-vlanpolicy] quit
```

2) RADIUS サーバを設定します。

Free RADIUS サーバのディレクトリファイルにどちらかのユーザロールの属性を追加します。

```
Cisco-AVPair = "shell:roles=\"role2\""
Cisco-AVPair = "shell:roles*\"role2\""
```

装置と通信する Free RADIUS サーバの必要な設定を行います。(詳細は省略します)

AC と RADIUS サーバで設定が一致していることを確認します。

III. 設定の確認

AC に Telnet し、AC にアクセスするためのユーザ名、パスワードを入力します(詳細は省略します)。

ISP view で有効なすべてのコマンドが使用できることを確認します。

```
<AC> system-view
[AC] domain abc
[AC-isp-abc] authentication login radius-scheme abc
[AC-isp-abc] quit
```

radius、**arp** 機能についてのすべての read、write コマンドを使用できることを確認します。この例では **radius** を使用します。

```
[AC] radius scheme rad
[AC-radius-rad] primary authentication 2.2.2.2
[AC-radius-rad] display radius scheme rad
…
(display 表示結果は省略します。)
```

VLAN 1～VLAN 20 以外の VLAN を設定できないことを確認します。この例では VLAN 10 と VLAN 30 を使用します。

```
[AC] vlan 10
[AC-vlan10] quit
[AC] vlan 30
Permission denied.
```

2.10.3 RBAC の一時的なユーザロールの許可の設定例

I. ネットワーク要件

図 2-3に示すように、装置はログインユーザ用にローカル認証を実行します。Telnet ユーザはユーザ名 **test@bbb** を持ち、ユーザロール **level-0** が割り当てられます。

一時的なユーザロールの許可を行うため remote-then-local の認証モードを設定します。装置はユーザロール network-admin の認証を許可するため、RADIUS サーバを使用します。AAA の設定が無効あるいは RADIUS サーバが応答していない場合、装置はローカル認証を実行します。

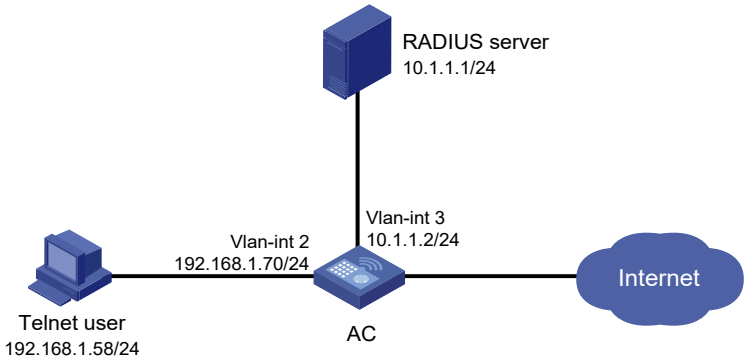


図 2-3 ネットワーク図

II. 設定手順

1)　AC を設定します。

Telnet ユーザに接続された VLAN インタフェース 2 に IP アドレスを割り当てます。

```
<AC> system-view
[AC] interface vlan-interface 2
[AC-Vlan-interface2] ip address 192.168.1.70 255.255.255.0
[AC-Vlan-interface2] quit
```

RADIUS サーバに接続された VLAN インタフェース 3 に IP アドレスを割り当てます。

```
[AC] interface vlan-interface 3
[AC-Vlan-interface3] ip address 10.1.1.2 255.255.255.0
[AC-Vlan-interface3] quit
```

Telnet サーバを有効にします。

```
[AC] telnet server enable
```

Telnet ユーザ用に、ユーザラインの scheme 認証を有効にします。

```
[AC] line vty 0 15
[AC-line-vty0-15] authentication-mode scheme
[AC-line-vty0-15] quit
```

一時的なユーザロールの許可のため、remote-then-local 認証を有効にします。

```
[AC] super authentication-mode scheme local
```

RADIUS scheme **radius** を作成し、RADIUS scheme view に移行します。

```
[AC] radius scheme radius
```

プライマリ認証サーバのアドレスを 10.1.1.1 に指定し、Switch とサーバ間の通信をセキュアにするため、scheme の専用の共有鍵を設定します。

```
[AC-radius-radius] primary authentication 10.1.1.1 key simple expert
```

RADIUS サーバに送信したユーザ名から ISP ドメイン名を除外します。

```
[AC-radius-radius] user-name-format without-domain
[AC-radius-radius] quit
```

ISP ドメイン **bbb** を作成し、ISP domain view に移行します。

```
[AC] domain bbb
```

ログインユーザでローカル認証を使用する ISP ドメイン **bbb** を設定します。

```
[AC-isp-bbb] authentication login local
```

ログインユーザでローカル許可を使用する ISP ドメイン **bbb** を設定します。

```
[AC-isp-bbb] authorization login local
```

ユーザロール認証のため、RADIUS scheme **radius** を ISP ドメインに適用します。

```
[AC-isp-bbb] authentication super radius-scheme radius
[AC-isp-bbb] quit
```

装置管理ユーザ **test** を作成し、local user view に移行します。

```
[AC] local-user test class manage
```

ユーザのサービスタイプを Telnet に設定します。

```
[AC-luser-manage-test] service-type telnet
```

ユーザのパスワードを **123456TESTplat&!**に設定します。

```
[AC-luser-manage-test] password simple 123456TESTplat&!
```

level-0 をユーザに割り当てます。

```
[AC-luser-manage-test] authorization-attribute user-role level-0
```

デフォルトユーザロール **network-operator** を削除します。

```
[AC-luser-manage-test] undo authorization-attribute user-role network-operator
[AC-luser-manage-test] quit
```

ユーザロール **network-admin** のローカル認証パスワードを **abcdef654321TESTplat&!** に設定します。

```
[AC] super password role network-admin simple abcdef654321TESTplat&!
```

```
[AC] quit
```

2) RADIUS サーバを設定します。

(詳細は省略します)

III. 設定の確認

1) AC に Telnet 接続を行い、ユーザ名 **test@bbb**、パスワード **123456TESTplat&!**を入力します。
2) 診断コマンドにアクセスできることを確認します。

```
<AC> telnet 192.168.1.70
Trying 192.168.1.70 ...
Press CTRL+K to abort
Connected to 192.168.1.59 ...

login: test@bbb
Password:
<AC>?
User view commands:
  ping         Ping function
  quit         Exit from current command view
  ssh2         Establish a secure shell client connection
  super        Switch to a user role
  system-view  Enter the System View
  telnet       Establish a telnet connection
  tracert      Tracert function

<AC>
```

3) ユーザロール network-admin を取得できることを確認します。

ユーザロール network-admin を取得するため、super password コマンドを使用します。システムはユーザ名とパスワードが表示されたとき、ユーザ名 **test@bbb**、パスワード **123456** を入力します。

```
<AC> super network-admin
Username: test@bbb
Password:
```

以下の出力はユーザロール network-admin を取得したことを示します。

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

#RADIUS サーバが応答しない場合、表示画面でローカル認証のパスワード **abcdef654321TESTplat&!**を入力します。

```
Invalid configuration or no response from the authentication server.
Change authentication mode to local.
Password:
User privilege role is network-admin, and only those commands that authorized to
the role can be used.
```

出力はユーザロール network-admin を取得したことを示します。

2.11 RBACのトラブルシューティング

本章では、一般的な RBAC の問題と解決方法について記載します。

2.11.1 ローカルユーザで許可していないコマンドにアクセスできる

I. 症状

ローカルユーザで割り当てられたユーザロールで許可していないコマンドが使用できます。

II. 分析

ローカルユーザには意図しないユーザロールが割り当てられている場合があります。たとえば、ローカルユーザを作成すると自動的にデフォルトのユーザロールも割り当てられています。

III. 解決策

1) **display local-user** コマンドを使用し、必要ないユーザロールがあるローカルユーザアカウントを確認し、それを削除します。

2.11.2 RADIUS ユーザによるログインが常に失敗する

I. 症状

以下の状況において RADIUS ユーザによって、ネットワークアクセス装置にログインできません。

- 本装置と RADIUS サーバ間の通信は正常です。
- すべての AAA 設定は正常です。

II. 分析

RBAC は少なくとも 1 つのユーザロールを持つログインユーザが必要です。もし RADIUS サーバがユーザロールを使用するログインユーザを許可していない場合、ユーザは装置にログインすることはできません。

III. 解決策

以下の方法で問題を解決します。

1) 以下のいずれかの方法を使用します。

- ユーザロールが RADIUS サーバに割り当てられていないとき、RADIUS ユーザがデフォルトユーザロールでログインできるようにするため、**role default-role enable** コマンドを設定します。
- ユーザロール許可属性を RADIUS サーバに追加してください。

目次

このセクションのページは**2-x-x** です。

3章 ログイン管理 3-1

3章 ログイン管理

初回の装置へのログインは、コンソールポートを使用した CLI ログインのみ行うことができます。2 回目以降はコンソールログインパラメータの変更やコンソール、Telnet、SSH、Web、SNMP のログイン方法に変更することができます。

表 3-1 ログイン方法の概要

ログイン方法		デフォルト設定、必要最低限の設定
CLIのログイン	コンソールポートからローカルにログイン	デフォルトでは、コンソールポートでのログインは有効、ユーザ名やパスワードの認証なし、ユーザロールはnetwork-adminです。 ログイン後、装置のセキュリティの対応を行うため、パスワードあるいは認証スキームモードを設定します。
	Telnet接続によるログイン	デフォルトではTelnet接続によるログインは無効です。 Telnet接続によるログインを行うため、以下の設定が必要です。 ● Telnetサーバ機能を有効にします。 ● レイヤ3インタフェースにIPアドレスを設定し、インタフェースとTelnetクライアント間で通信可能なことを確認します。 ● VTYログインユーザ用に認証モードを設定します。デフォルトではパスワード認証が使用されますが、パスワードは設定されていません。 ● VTYログインユーザにユーザロールを割り当てます。(デフォルトはnetwork-operator)
	SSH接続によるログイン	デフォルトではSSH接続によるログインは無効です。SSH接続によるログインを行うため、以下の設定が必要です。 ● SSHサーバ機能を有効にし、SSH属性を設定します。 ● レイヤ3インタフェースにIPアドレスを設定し、インタフェースとSSHクライアント間で通信可能なことを確認します。 ● VTYログインユーザ用に認証モードを設定します。デフォルトではパスワード認証が使用されます。 ● VTYログインユーザにユーザロールを割り当てます。(デフォルトはnetwork-operator)
Webインタフェースからのアクセス		デフォルトでWebインタフェースからのログインは無効です。 Webインタフェースによるログインを行うため、以下の設定が必要です。 ● レイヤ3インタフェースにIPアドレスを設定します。Webインタフェースと Webユーザホスト間で通信可能なことを確認します。 ● Webログインのローカルユーザアカウントを設定し、アカウントにユーザロールを割り当てます。デフォルトは network-operatorです。 ● ユーザにHTTPあるいはHTTPSサービスを割り当てます。デフォルトは設定されていません。
SNMPからのアクセス		デフォルトではSNMPによるログインは無効です。 SNMPによるログインを行うため、以下の設定が必要です。 ● レイヤ3インタフェースにIPアドレスを設定し、インタフェ

ログイン方法	デフォルト設定、必要最低限の設定
	ースとNMS間で通信可能なことを確認します。 ● SNMPの基本パラメータを設定します。

目次

このセクションのページは**2-x-x** です。

4章 コンソールポートによる最初のログイン 4-1

4章 コンソールポートによる最初のログイン

初回の装置へのログインは、コンソールポートを使用した CLI ログインのみ行うことができます。

コンソールポートからログインするには、PC などのコンソール端末を用意します。コンソール端末に HyperTerminal や PuTTY などの端末エミュレーションプログラムがあることを確認します。端末エミュレーションプログラムの使用方法については、各プログラムのユーザガイドを参照してください。

コンソールポートでログインする場合は以下の手順に従ってください。

1) PC のシリアルポートに D-sub 9 ピンメスコネクタを接続します。
2) コンソールケーブルの RJ-45 コネクタを装置のコンソールポートに接続します。

⚠ **重要：**

- 接続するポートを確認して間違ったコネクタに接続しないようにしてください。
- PC のシリアルポートはホットスワップ機能にサポートしていません。装置が電源 ON である場合、PC の電源を OFF にしてください。装置に接続する前に PC にコンソールケーブルを最初に接続してください。ケーブルを取り外すときは、最初に装置から取り外してください。

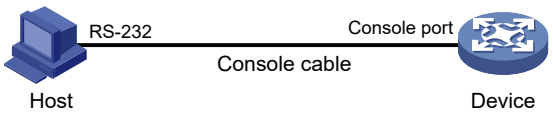


図 4-1 コンソールポートとの接続

3) PC が電源 OFF である場合、PC の電源を ON にしてください。
4) PC で端末エミュレーションソフトウェアを起動し、装置に接続する端末の設定を行います。通常、端末のコンソールポートのパラメータは以下となっています。

- 通信速度　　— 9600 bps
- フローコントロール — なし
- パリティ　　— なし
- ストップビット　— 1
- データビット　　— 8

5) 装置の電源を入れます。装置が問題なく POST（power-on self test）を終了すると、**Enter** を押すように指示されます。

デフォルトの user view のプロンプト<Switch>が表示されます。装置の設定や管理を行うため、コマンドを入力することができます。ヘルプ画面を表示する場合、クエスチョンマーク（?）を入力します。

目次

このセクションのページは**2-x-x** です。

5章 CLIによるログイン 5-1
5.1 CLI概要 5-1
5.1.1 ユーザライン 5-1
5.1.2 ログイン認証モード 5-2
5.1.3 ユーザロール 5-2
5.2 コンソールポートからのローカルログイン 5-3
5.2.1 コンソールログイン認証の設定 5-3
5.2.2 consoleユーザラインの共通設定 5-6
5.3 Telnetからのログイン 5-8
5.3.1 装置のTelnetログインの設定 5-8
5.3.2 装置からTelnetサーバへのTelnet接続 5-15
5.4 SSHからのログイン 5-15
5.4.1 SSHログインの設定 5-16
5.4.2 装置からSSHサーバへのSSH接続 5-18
5.5 CLIログインの表示と維持 5-18

5章 CLI によるログイン

初回の装置へのログインは、コンソールポートを使用した CLI ログインのみ行うことができます。装置の管理を容易にするため、コンソールポートや Telnet、SSH、Web、SNMP でログインすることができます。

CLI への不正アクセスを防止し、ユーザロールを管理するため、以下のことを行うことができます。

- ログイン認証の設定
- ユーザロールの割り当て
- コマンド許可の設定
- 無許可ログインのフィルタリングを行う ACL

この章では設定について方法記載し、ログイン認証、ユーザロール、共通ユーザライン設定を含む CLI ログイン方法について記載します。詳細は、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*2 基本機能*”の”*7 章 ログインユーザの制御*”を参照してください。

5.1 CLI概要

5.1.1 ユーザライン

装置は CLI セッションを管理し、ユーザのふるまいをモニタリングするため、ユーザライン（ユーザインタフェースと呼ばれます）を使用します。ユーザラインでのログイン認証、ユーザロールを含むアクセス管理の設定を行うことができます。ユーザがログインした後、ユーザラインに割り当てられた設定に従う必要があります。

ユーザは、表 5-1のようにログイン方法に依存した異なるユーザラインに割り当てられます。

表 5-1 CLI ログイン方法とユーザライン

ユーザライン	ログイン方法
AUXユーザライン	コンソールポート
Virtual type terminal （VTY）ユーザライン	TelnetあるいはSSH

I. ユーザラインの識別化

各ユーザラインは、識別化のため絶対値と相対値を持っています。

絶対値は、すべてのユーザライン間でユーザラインを一意に認識します。ユーザラインは、AUX と VTY ユーザラインで 0 から 1 ずつ増加するユーザライン番号で番号付けられます。**display line** コマンドでパラメータを指定しない場合、サポートされるユーザラインと絶対値を表示することができます。

相対値は同一タイプのすべてのユーザライン間でユーザラインを識別します。番号フォーマットは *interface type* + *number* です。すべてのユーザラインのタイプは 0 から 1 ずつ増加します。たとえば VTY ユーザラインの最初は VTY0 です。

II. ユーザラインの割り当て

装置は、ログイン方法に依存して、CLI ログインユーザにユーザラインを自動的に割り当てます。各ユーザラインは 1 度に 1 つのユーザにのみユーザラインを割り当てることができます。ユーザラインが有効でない場合、CLI ログインは拒否されます。

CLI ログインで、装置は、ログインタイプ用に、有効で空いているユーザラインから最も低い値を用います。たとえば 4 つの VTY インタフェース（0～3）が設定されている場合、VTY インタフェースの VTY0 と VTY3 は空いています。ユーザが装置に Telnet を行うとき、ユーザに VTY0 が割り当てられ、認証を行い、ユーザを管理するために VTY0 の設定を使用します。

5.1.2 ログイン認証モード

装置の CLI への不正アクセスを防ぐため、ログイン認証を設定することができます。

装置は以下のログイン認証モードをサポートしています。

- **None** – 認証なし。このモードはセキュリティの保護がありません。
- **Password** – パスワード認証が必要です。
- **Scheme** – ローカルあるいはリモートログイン認証を行うため、AAA モジュールを使用します。ログイン時にユーザ名、パスワードを使用する必要があります。

異なるログイン認証モードは、表 5-2のようにユーザラインで異なる設定が必要です。

表 5-2 異なるログイン認証で必要な設定

認証モード	操作
None	認証モードを**none**に設定します。
Password	1. 認証モードを **password** に設定します。 2. パスワードを設定します。
Scheme	1. 認証モードを **scheme** に設定します。 2. ISP domain view でログイン認証方法を設定します。詳細は、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*13 ユーザアクセスと認証*“の”*3 章AAA*“を参照してください。

5.1.3 ユーザロール

ログインするときユーザはユーザロールが割り当てられます。ユーザロールはユーザが実行できるコマンドを指定します。

装置はログイン認証モードとログイン方法をもとにしたユーザロールを割り当てます。

- もし None あるいは Password 認証が使用される場合、装置はユーザラインで作成されたユーザロールの設定に従ってユーザロールを割り当てます。

- もし Scheme 認証が使用される場合、以下のようにユーザロールを割り当てます。
  - 公開鍵あるいはパスワード公開鍵を使用する SSH ログインユーザの認証において、装置はユーザラインで設定されたユーザロールに従ってユーザロールを割り当てます。
  - 他のユーザにおいて、AAA モジュールで設定されたユーザロールに従ってユーザロールを割り当てます。リモート AAA 認証ユーザにおいて、もし AAA サーバがユーザにユーザロールを割り当てず、ユーザロール機能が無効である場合、ユーザはログインすることができません。

5.2 コンソールポートからのローカルログイン

図 5-1のように装置にログインし、管理するため、コンソールポートで端末を接続することができます。ログイン手順については、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*2 基本機能*”の”*2 章 コンソールポートによる最初のログイン*”を参照してください。

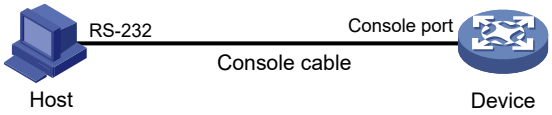


図 5-1 コンソールポートによるログイン

デフォルトでコンソールポートは有効で、認証を必要としません。装置のセキュリティの対応を行うため、パスワードあるいは認証スキームモードを設定します。そして初回に装置へログインした後、すぐに必要とされるようにユーザロールを割り当てます。

コンソールログインを設定するため、以下の作業が完了している必要があります。

操作	備考
（必須設定項目）コンソールログイン認証の設定: • None認証の設定 • Password認証の設定 • Scheme認証の設定	いずれか一つの認証モードが必要です。
（オプション設定項目）consoleユーザラインの共通設定	—

コンソールログインの設定は、ログイン中のユーザには適用しません。設定が行われた後、次にログインするユーザのみ適用されます。

5.2.1 コンソールログイン認証の設定

I. None 認証の設定

操作	コマンド	備考
1. system view に移行する	**system-view**	—

操作	コマンド	備考
2． AUX line view あるいは class view に移行する	● AUX line viewに移行する： **line aux** *first-number* [*last-number*] ● AUX line class viewに移行する： **line class aux**	どちらか一方を使用します。 User line viewでの設定はユーザラインのみ適用されます。 User line class viewでの設定はclassのすべてのユーザに適用されます。 どちらかの設定がデフォルトから変更された場合、他のviewのデフォルト設定よりも優先されます。 User line viewの設定がデフォルトから変更された場合、user line class viewでデフォルトから変更された設定よりも優先されます。 user line viewでの設定はオンラインユーザにすぐさま適用されます。 User line class viewでの設定は、設定が完了したのち、ログインしたユーザに適用されます。
3． None 認証モードを有効にする	**authentication-mode none**	デフォルト：**none** ⚠**注意：** 認証を無効にすると、ユーザは認証なしでラインまたはラインクラスを介して装置にログインできます。セキュリティ上の理由から、認証は慎重に無効にしてください。
4． ユーザロールを割り当てる	**user-role** *role-name*	デフォルト：**network-admin**

コンソールポートを使用して、次回ログインを行う場合、ユーザ名あるいはパスワードを必要としません。

II. Password 認証の設定

操作	コマンド	備考
1． system view に移行する	**system-view**	―
2． AUX line view あるいは class view に移行する	● AUX line viewに移行する： **line aux** *first-number* [*last-number*] ● AUX line class viewに移行する： **line class aux**	どちらか一方を使用します。 User line viewでの設定はユーザラインのみ適用されます。 User line class viewでの設定はclassのすべてのユーザに適用されます。 どちらかの設定がデフォルトから変更された場合、他のviewのデフォルト設定よりも優先されます。 User line viewの設定がデフォルトから変更された場合、user line class viewでデフォルトから変更された設定よりも優先されます。 user line viewでの設定はオンラインユーザにすぐさま適用されます。 User line class viewでの設定は、設定が完了したのち、ログインしたユーザに適用されます。

操作	コマンド	備考
3． Password 認証モードを有効にする	**authentication-mode password**	デフォルト：**none**
4． password を設定する	**set authentication password** { **hash** | **simple** } *password*	デフォルト：設定なし
5． ユーザロールを割り当てる	**user-role** *role-name*	デフォルト：**network-admin**

コンソールポートを使用して、次回ログインを行う場合、設定したログインパスワードが必要です。

III. Scheme 認証の設定

操作	コマンド	備考
1． system view に移行する	**system-view**	―
2． AUX line view あるいは class view に移行する	● AUX line viewに移行する：**line aux** *first-number* [*last-number*] ● AUX line class viewに移行する：**line class aux**	どちらか一方を使用します。 User line viewでの設定はユーザラインのみ適用されます。 User line class viewでの設定はclassのすべてのユーザに適用されます。 どちらかの設定がデフォルトから変更された場合、他のviewのデフォルト設定よりも優先されます。 User line viewの設定がデフォルトから変更された場合、user line class viewでデフォルトから変更された設定よりも優先されます。 user line viewでの設定はオンラインユーザにすぐさま適用されます。 User line class viewでの設定は、設定が完了したのち、ログインしたユーザに適用されます。
3． Scheme 認証を有効にする	**authentication-mode scheme**	デフォルト：**none** ⚠**重要：** Scheme認証を有効にする場合は、認証ユーザアカウントが使用可能であることを確認してください。使用可能な認証ユーザアカウントがない場合、次回にラインまたはラインクラスを使用して装置にログインすることはできません。

Scheme 認証を使用するため、以下の設定が完了している必要があります。

- ISP domain view でコンソールログイン方法を設定します。
- リモート認証を使用し、RADIUS スキームを設定します。
- ローカル認証を使用し、ローカルユーザと関連する設定を行います。

詳細は QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*13 ユーザアクセスと認証*“の”*3 章 AAA*“を参照してください。

コンソールポートを使用して、次回ログインを行う場合、設定したユーザ名、パスワードが必要です。

5.2.2 console ユーザラインの共通設定

console ユーザライン用のいくつかの共通の設定は、設定された後すぐに適用され、現在のセッションを中断してしまうことがあります。同一のログイン作業を再度行うことを防ぐため、console ユーザラインを変更する前に、コンソールログインとは別のログイン方法を使用します。

設定が完了した後、コンソールポートを経由してログインするため、装置で設定したコンソールポートに合うようにコンソールターミナルの設定を変更します。

以下に console ユーザラインの共通設定を示します。

操作	コマンド	備考
1. system view に移行する	**system-view**	―
2. AUX line view あるいは class view に移行する	● AUX line viewに移行する： **line aux** *first-number* [*last-number*] ● AUX line class viewに移行する： **line class aux**	どちらか一方を使用します。 User line viewでの設定はユーザラインのみ適用されます。 User line class viewでの設定はclassのすべてのユーザに適用されます。 どちらかの設定がデフォルトから変更された場合、他のviewのデフォルト設定よりも優先されます。 User line viewの設定がデフォルトから変更された場合、user line class viewでデフォルトから変更された設定よりも優先されます。 user line viewでの設定はオンラインユーザにすぐさま適用されます。 User line class viewでの設定は、設定が完了したのち、ログインしたユーザに適用されます。
3. ボーレートを設定する	**speed** *speed-value*	デフォルト：9600 bps このコマンドはconsole line class viewで設定できません。
4. パリティチェックモードを指定する	**parity** { **even** | **mark** | **none** | **odd** | **space** }	デフォルト：**none**（パリティチェックなし） このコマンドはconsole line class viewで設定できません。
5. ストップビットを設定する	**stopbits** { **1** | **1.5** | **2** }	デフォルト：**1** ストップビットは文字の最後を示します。ストップビットが多いと転送が遅くなります。 このコマンドはconsole line class viewで設定できません。

操作	コマンド	備考
6. データビットを設定する	**databits** { **7** | **8** }	デフォルト：**8** 文字コードタイプに依存します。たとえば7に設定されると標準ASCII文字が送信され、8に設定すると拡張ASCII文字が送信されます。 このコマンドはconsole line class viewで設定できません。
7. エスケープキーを設定する	**escape-key** { *character* | **default** }	デフォルト：CTRL+C
8. 端末タイプを設定する	**terminal type** { **ansi** | **vt100** }	デフォルト：ANSI 装置はANSIとvt100の2つの端末タイプをサポートします。端末で適した表示を保証するため、両方のタイプを設定し、装置と端末の両方のタイプをvt100に設定することを推奨します。 そうでなければコマンドラインが80文字超えてしまい、カーソル位置がエラーとなったり、異常な端末表示となる場合があります。
9. 画面に表示できる最大行数を設定する	**screen-length** *screen-length*	デフォルト：最大24行 出力の最大行を0とすると画面の表示は停止しません。
10. コマンド履歴バッファのサイズを設定する	**history-command max-size** *value*	デフォルト：10
11. ユーザラインのタイムアウトの時間を設定する	**idle-timeout** *minutes* [*seconds*]	デフォルト：10分 タイムアウト時間内に、ユーザラインで何も実行されないと自動的にユーザラインの接続が終了します。タイムアウト機能を無効にする場合、0に設定します。
12. ユーザが現在のユーザラインにログインしたとき、自動で実行されるコマンドを設定する	**auto-execute command** *command*	デフォルト：設定なし ⚠**注意**： このコマンドは慎重に使用してください。このコマンドをユーザラインで使用すると、このユーザラインで装置にログインしたユーザがシステムの設定に失敗する可能性があります。 ユーザが現在のユーザラインにログインしたとき、装置は自動で指定されたコマンドを実行します。コマンドが実行されたのち、ユーザの接続を切断します。 このコマンドはAUX line viewあるいはAUX line class viewでサポートしています。
13. 端末サービスを有効にする	**shell**	デフォルト：有効 AUX line viewでコマンドは**undo shell**サポートしていません。

5.3 Telnetからのログイン

装置のリモート管理を行うため、Telnet サーバを使用することができます。また他の装置を管理するため、装置を Telnet クライアントとして使用することができます。

デフォルトでは Telnet からのログインは無効です。Telnet を使用する場合、Telnet 以外の他のログイン方法を用いて、装置にログインしてください。

5.3.1 装置の Telnet ログインの設定

操作	備考
（必須設定項目）Telnetサーバの有効化	ー
（必須設定項目）Telnetからのログイン認証の設定 ● None認証の設定 ● Password認証の設定 ● Scheme認証の設定	いずれか一つの認証モードが必要です。
（オプション設定項目）Telnetサーバの共通設定	ー
（オプション設定項目）VTYユーザラインの共通設定	ー

I. Telnet サーバの有効化

操作	コマンド	備考
1． system view に移行する	**system-view**	ー
2． Telnet サーバを有効化する	**telnet server enable**	デフォルト：無効

II. None 認証の設定

操作	コマンド	備考
1． system view に移行する	**system-view**	ー

操作	コマンド	備考
2． VTY line view または VTY line class view に移行する	● VTY line viewに移行する：**line vty** *first-number* [*last-number*] ● VTY line class viewに移行する：**line class vty**	どちらか一方を使用します。 User line viewでの設定はユーザラインのみ適用されます。 User line class viewでの設定はclassのすべてのユーザに適用されます。 どちらかの設定がデフォルトから変更された場合、他のviewのデフォルト設定よりも優先されます。 User line viewの設定がデフォルトから変更された場合、user line class viewでデフォルトから変更された設定よりも優先されます。 user line viewでの設定はオンラインユーザにすぐさま適用されます。 User line class viewでの設定は、設定が完了したのち、ログインしたユーザに適用されます
3． None認証モードを有効にする	**authentication-mode none**	デフォルト：**password** ⚠**注意：** 認証を無効にすると、ユーザは認証なしでラインまたはラインクラスを介して装置にログインできます。セキュリティ上の理由から、認証は慎重に無効にしてください。 VTY line viewでは**protocol inbound**コマンドに関連します。 ● どちらかの設定がデフォルトから変更された場合、VTY line viewの設定が適用されます。 ● VTY line viewで両方の設定がデフォルトのままである場合、VTY line class viewの設定が適用されます。
4． （オプション設定項目）ユーザロールを割り当てる	**user-role** *role-name*	デフォルト：**network-operator**

以下のように次回 Telnet で装置にログインを行う場合、ユーザ名あるいはパスワードを必要としません。もしログインユーザ数が最大である場合、ログインに失敗し、"All user lines are used, Please try later!"のメッセージが表示されます。

```
<AC>
```

III. Password 認証の設定

操作	コマンド	備考
1． system view に移行する	**system-view**	ー
2． VTY line view または VTY line class view に移行する	● VTY line viewに移行する：**line vty** *first-number* [*last-number*] ● VTY line class viewに移行する：**line class vty**	どちらか一方を使用します。 User line viewでの設定はユーザラインのみ適用されます。 User line class viewでの設定はclassのすべてのユーザに適用されます。 どちらかの設定がデフォルトから変更された場合、他のviewのデフォルト設定よりも優先されます。 User line viewの設定がデフォルトから変更された場合、user line class viewでデフォルトから変更された設定よりも優先されます。 user line viewでの設定はオンラインユーザにすぐさま適用されます。 User line class viewでの設定は、ログイン中のユーザには適用しません。設定が完了したのち、ログインしたユーザに適用されます。
3． Password 認証モードを有効にする	**authentication-mode password**	デフォルト：**password** ⚠**注意：** Password認証を有効にする場合は、ラインまたはラインクラスの認証パスワードも設定する必要があります。認証パスワードが設定されていない場合、次回にラインまたはラインクラスを使用して装置にログインすることはできません。 VTY line viewでは**protocol inbound**コマンドに関連します。 ● どちらかの設定がデフォルトから変更された場合、VTY line viewの設定が適用されます。 ● VTY line viewで両方の設定がデフォルトのままである場合、VTY line class viewの設定が適用されます。
4． password の設定	**set authentication password** { **hash** | **simple** } *password*	デフォルト：設定なし
5． （オプション設定項目）ユーザロールを割り当てる	**user-role** *role-name*	デフォルト：**network-operator**

以下のように次回 Telnet で装置にログインを行う場合、パスワードが必要となります。もしログインユーザ数が最大である場合、ログインに失敗し、" All user lines are used, please try later!"のメッセージが表示されます。

```
Password:
<AC>
```

IV. Scheme 認証の設定

操作	コマンド	備考
1. system view に移行する	**system-view**	―
2. VTY line view または VTY line class view に移行する	● VTY line viewに移行する：**line vty** *first-number* [*last-number*] ● VTY line class viewに移行する：**line class vty**	どちらか一方を使用します。 User line viewでの設定はユーザラインのみ適用されます。 User line class viewでの設定はclassのすべてのユーザに適用されます。 どちらかの設定がデフォルトから変更された場合、他のviewのデフォルト設定よりも優先されます。 User line viewの設定がデフォルトから変更された場合、user line class viewでデフォルトから変更された設定よりも優先されます。 user line viewでの設定はオンラインユーザにすぐさま適用されます。 User line class viewでの設定は、ログイン中のユーザには適用しません。設定が完了したのち、ログインしたユーザに適用されます。

操作	コマンド	備考
3． Scheme 認証を有効にする	**authentication-mode scheme**	デフォルト：**password** ⚠**注意：** Scheme認証を有効にする場合は、認証ユーザアカウントが使用可能であることを確認します。使用可能な認証ユーザアカウントがない場合、次回にラインまたはラインクラスを使用して装置にログインすることはできません。 VTY line viewでは**protocol inbound**コマンドに関連します。 ● どちらかの設定がデフォルトから変更された場合、VTY line viewの設定が適用されます。 ● VTY line viewで両方の設定がデフォルトのままである場合、VTY line class viewの設定が適用されます。

Scheme 認証を行うため、以下の作業を完了してください。

- ISP domain view でログイン認証を設定してください。
- リモート認証を行うため、使用する RADIUS スキームの設定を行ってください。
- ローカル認証を行うため、ローカルユーザと関連する属性の設定を行ってください。

詳細は QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*13 ユーザアクセスと認証*“の”*3 章 AAA*“を参照してください。

以下のように次回 Telnet で装置にログインを行う場合、ユーザ名、パスワードが必要となります。もしログインユーザ数が最大である場合、ログインに失敗し、"All lines are used, please try later!"のメッセージが表示されます。

```
Login: admin
Password:
<AC>
```

V. Telnet サーバの共通設定

操作	コマンド	備考
1． system view に移行する	**system-view**	―
2． 出力 Telnet パケットに DSCP 値を設定する	● IPv4のTelnetサーバ **telnet server dscp** *dscp-value*	デフォルト：48 DSCP値はパケットの伝送優先度を示すために、IPv4 パケットの ToS フィールドで伝送されます。

操作	コマンド	備考
3． 同時に接続できる Telnet ユーザの最大数を設定する	**aaa session-limit telnet** *max-sessions*	デフォルト：32 オンライン中のTelnetユーザには影響しません。現在のオンライン中のTelnetユーザ数が、新しく設定した最大数以上である場合、オンラインユーザがログアウトするまで新規にログインすることができません。このコマンドの詳細はQX-W2300ACシリーズアクセスコントローラコマンドマニュアルの“*13 ユーザアクセスと認証*“の”*3章AAA*“を参照してください。

VI. VTY ユーザラインの共通設定

VTY ユーザラインにおいて、ユーザログインを行ったときに自動的に実行されるコマンドを指定することができます。指定したコマンドを実行し、操作を行った後、システムは自動的に Telnet セッションを切断します。この機能を設定する前に設定を保存し、異なるユーザラインによって CLI アクセスができることを確認してください。

一般的に、装置がTelnetユーザをX.X.X.Xのアドレスのホストにリダイレクトさせるため、**auto-execute command telnet** *X.X.X.X* コマンドを設定します。ユーザが X.X.X.X の Telnet 接続を切断したとき、現在の装置の接続が切断します。

以下に VTY ユーザラインの共通設定を示します。

操作	コマンド	備考
1． system view に移行する	**system-view**	―
2． VTY line view または VTY line class view に移行する	• VTY line viewに移行する：**line vty** *first-number* [*last-number*] • VTY line class viewに移行する：**line class vty**	どちらか一方を使用します。 User line viewでの設定はユーザラインのみ適用されます。 User line class viewでの設定はclassのすべてのユーザに適用されます。 どちらかの設定がデフォルトから変更された場合、他のviewのデフォルト設定よりも優先されます。 User line viewの設定がデフォルトから変更された場合、user line class viewでデフォルトから変更された設定よりも優先されます。 user line viewでの設定はオンラインユーザにすぐさま適用されます。 User line class viewでの設定は、ログイン中のユーザには適用されません。次にログインするユーザのみ適用されます。

操作	コマンド	備考
3. 端末サービスを有効にする	**shell**	デフォルト：有効
4. 指定したユーザラインでサポートするプロトコルを設定する	**protocol inbound** { **all** | **ssh** | **telnet** }	デフォルト：all 次回のログイン時に適用されます。 VTY line viewでは、**authentication-mode**コマンドに関連します。 ● VTY line viewの設定がデフォルトから変更された場合、VTY line viewの他の設定が適用されます。 ● VTY line viewで両方の設定がデフォルトである場合、VTY line class viewの設定が適用されます。
5. エスケープキーを設定する	**escape-key** { *character* | **default** }	デフォルト：CTRL+C
6. 端末タイプを設定する	**terminal type** { **ansi** | **vt100** }	デフォルト：ANSI
7. 画面に表示できる最大数を設定する	**screen-length** *screen-length*	デフォルト：24行 出力の最大行を0とすると画面の表示は停止しません。
8. コマンド履歴のバッファサイズを設定する	**history-command max-size** *value*	デフォルト：10 コマンド履歴のバッファは最大10のコマンドを保存します。
9. ユーザラインのタイムアウト時間を設定する	**idle-timeout** *minutes* [*seconds*]	デフォルト：10分 タイムアウト時間内に、ユーザラインで何も実行されないと自動的にユーザラインの接続が終了します。 タイムアウト機能を無効にする場合、0に設定します。
10. ユーザラインにログイン後、自動で実行されるコマンドを指定する	**auto-execute command** *command*	デフォルト：ユーザがユーザラインにログインした際に自動的に実行されるコマンドはなし ⚠ **重要**： ユーザラインにこのコマンドを実行すると、ユーザラインによる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あるいはAUX 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。

5.3.2 装置から Telnet サーバへの Telnet 接続

装置は Telnet クライアントとして Telnet サーバにログインすることができます。もし Telnet サーバが異なるサブネットにある場合、2 つの装置と Telnet サーバ間で通信できることを確認してください。



図 5-2 装置から Telnet サーバへの Telnet 接続

以下に装置から Telnet サーバへのログインの設定を示します。

操作	コマンド	備考
1． system view に移行する	**system-view**	—
2． （オプション設定項目） Telnet パケットの送信元 IPv4 アドレス/インタフェースを指定する	**telnet client source** { **interface** *interface-type interface-number* | **ip** *ip-address* }	デフォルト : 送信元IPv4アドレス/インタフェースは設定なし、送信元アドレスとして出力インタフェースのプライマリIPv4アドレスが使われます。
3． user view へ戻る	**quit**	—
4． Telnet サーバへのログインする	• IPv4 Telnet サーバへのログイン : **telnet** *remote-host* [*service-port*] [**source** { **interface** *interface-type interface-number* | **ip** *ip-address* } | **dscp** *dscp-value*] *	—

5.4 SSHからのログイン

SSH は、より強固なセキュリティを持ったログイン方法のアプローチです。強力な暗号化と認証機能によって IP スプーフィング攻撃、パスワード傍受なども防止することができます。詳細は QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*15 セキュリティ*”の”*5 章 SSH*”を参照してください。

装置のリモート管理を行うため、SSH クライアントを使用することができます。また SSH サーバの他の装置を管理するため、装置を SSH クライアントとして使用することができます。

デフォルトでは SSH からのログインは無効です。SSH を使用する場合、SSH 以外の他のログイン方法を用いて、初回に SSH ログインの設定を行う必要があります。

5.4.1 SSH ログインの設定

この章では SSH クライアント認証が password である場合の手順を示します。SSH、公開鍵認証の設定の詳細については、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*15 セキュリティ*”の”*4 章 公開鍵*”を参照してください。

以下に装置から SSH ログインの設定を示します。

操作	コマンド	備考
1． system view に移行する	**system-view**	―
2． ローカル鍵ペアを生成する	**public-key local create** { **dsa** | **ecdsa** [**secp192r1** | **secp256r1** | **secp384r1** | **secp521r1**] | **rsa** } [**name** *key-name*]	デフォルト：なし
3． SSH サーバを有効にする	**ssh server enable**	デフォルト：無効
4． VTY line view または VTY line class view に移行する	● VTY line viewに移行する：**line vty** *first-number* [*last-number*] ● VTY line class viewに移行する：**line class vty**	どちらか一方を使用します。 User line viewでの設定はユーザラインのみ適用されます。 User line class viewでの設定はclassのすべてのユーザに適用されます。 どちらかの設定がデフォルトから変更された場合、他のviewのデフォルト設定よりも優先されます。 User line viewの設定がデフォルトから変更された場合、user line class viewでデフォルトから変更された設定よりも優先されます。 user line viewでの設定はオンラインユーザにすぐさま適用されます。 User line class viewでの設定は、ログイン中のユーザには適用しません。設定が完了したのち、ログインしたユーザに適用されます。

操作	コマンド	備考
5. scheme 認証を有効にする	**authentication-mode scheme**	デフォルト：**password** ⚠**注意：** scheme 認証を有効にする場合は、認証ユーザアカウントが使用可能であることを確認します。使用可能な認証ユーザアカウントがない場合、次回にラインまたはラインクラスを使用して装置にログインすることはできません。 VTY line viewでは**protocol inbound**コマンドに関連します。 ● どちらかの設定がデフォルトから変更された場合、VTY line viewの設定が適用されます。 ● VTY line viewで両方の設定がデフォルトのままである場合、VTY line class viewの設定が適用されます。
6. （オプション設定項目）使用するプロトコルを指定する	**protocol inbound** { **all** | **ssh** | **telnet** }	デフォルト：**all** ログイン中のユーザには適用しません。次回のログイン時に適用されます。 VTY line viewでは、**authentication-mode**コマンドに関連します。 ● VTY line viewの設定がデフォルトから変更された場合、VTY line viewの他の設定が適用されます。 ● VTY line viewで両方の設定がデフォルトである場合、VTY line class viewの設定が適用されます。
7. system view から戻る	**quit**	―
8. （オプション設定項目）VTY ユーザラインの共通設定	QX-W2300ACシリーズアクセスコントローラオペレーションマニュアルの“*2 基本機能*”の”*2 章CLIによるログイン*”を参照してください。	―

操作	コマンド	備考
9.　（オプション設定項目） 現在のSSH ユーザの最大数を設定する	**aaa session-limit ssh** *max-sessions*	デフォルト：32 オンライン中のSSHユーザには影響しません。現在のオンライン中のSSHユーザ数が、新しく設定した最大数以上である場合、オンラインユーザがログアウトするまで新規にログインすることができません。このコマンドの詳細はQX-W2300ACシリーズアクセスコントローラコマンドマニュアルの“*13 ユーザアクセスと認証*“の”*3章 AAA*“を参照してください。

5.4.2 装置から SSH サーバへの SSH 接続

装置は SSH クライアントとして SSH サーバにログインすることができます。もし SSH サーバが異なるサブネットにある場合、2 つの装置と SSH サーバ間で通信できることを確認してください。



図 5-3 装置から SSH サーバへの SSH 接続

以下に user view で装置から SSH サーバへのログインの設定を示します。

操作	コマンド
IPv4 SSH サーバへのログイン	**ssh2** *server*

SSH サーバを動作させるためには、SSH クライアントの設定を行う必要があります。SSH クライアントの設定の詳細は、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*15 セキュリティ*”の”*5 章 SSH*”を参照してください。

5.5 CLIログインの表示と維持

display コマンドはすべての view で実行でき、他のコマンドは user view で実行できます。

操作	コマンド	備考
オンラインユーザ情報を表示する	**display users** [**all**]	—
ユーザラインを表示する	**display line** [*num1* | { **aux** | **vty** } *num2*] [**summary**]	—
送信元IPv4アドレス/インタフェースを表示する	**display telnet client**	—

操作	コマンド	備考
特定のユーザラインを解放する	**free line** { *num1* | { **aux** | **vty** } *num2* }	複数のユーザが同時に設定することができます。必要に応じて、このコマンドを使用して、ある接続を開放します。このコマンドで自分が使用している接続を開放することはできません。 user viewで使用可能です。
現在のユーザラインをロックする	**lock**	デフォルト：ロックされていません。
ユーザラインにメッセージを送信する	**send** { **all** | *num1* | { **aux** | **vty** } *num2* }	user viewで使用可能です。

目次

このセクションのページは**2-x-x** です。

6章 Webコンソールによるログイン 6-1
6.1 HTTPログインの設定 6-1
6.2 HTTPSログインの設定 6-2
6.3 Webログインの表示と維持 6-3
6.4 Webログインの設定例 6-3
6.4.1 HTTPログインの設定例 6-3

6章 Web コンソールによるログイン

装置は、HTTP および HTTPS をサポートする組み込みの Web サーバを提供します。Web ブラウザを使用して Web サーバにログインし、装置を設定できます。詳細は QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*5 ネットワーク接続*”の”*19 章 HTTP*”および QX-W2300AC シリーズアクセスコントローラコマンドマニュアルの“*5 ネットワーク接続*”の”*19 章 HTTP*”を参照してください。

Web コンソール機能はデフォルトでは使用できません。Web コンソールによるログインをしたい場合、最初にコンソールポートにてログインし、アクセスできるように設定する必要があります。

6.1 HTTPログインの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. HTTP サービスを有効にする	**ip http enable**	デフォルト：無効
3. （オプション設定項目）HTTP サービスのポート番号を設定する	**ip http port** *port-number*	デフォルト：80
4. （オプション設定項目）Web ユーザの接続のタイムアウトタイマを設定する	**web idle-timeout** *minutes*	デフォルト：10分
5. （オプション設定項目）オンライン HTTP ユーザの最大数を設定する	**aaa session-limit http** *max-sessions*	デフォルト：32 オンライン中のHTTPユーザには影響しません。現在のオンライン中のHTTPユーザ数が、新しく設定した最大数以上である場合、オンラインHTTPユーザがログアウトするまで新規にログインすることができません。詳細はQX-W2300ACシリーズアクセスコントローラコマンドマニュアルの“*13 ユーザアクセスと認証*“の”*3章 AAA*“を参照してください。
6. ローカルユーザを追加し、local user view に移行する	**local-user** *user-name* [**class manage**]	デフォルト：設定なし

操作	コマンド	補足
7. ローカルユーザのパスワードを設定する	**password** [{ **hash** | **simple** } *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。 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。 セキュリティのためローカルユーザのパスワードを設定してください。
8. ローカルユーザのユーザロールを設定する	**authorization-attribute user-role** *user-role*	デフォルト：network-operator
9. ローカルユーザのサービスタイプを指定する	**service-type http**	デフォルト：設定なし

6.2 HTTPSログインの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. HTTPS サービスを有効にする	**ip https enable**	デフォルト：無効
3. （オプション設定項目）HTTPS サービスのポート番号を設定する	**ip https port** *port-number*	デフォルト：443
4. （オプション設定項目）Web 接続のタイムアウトタイマを設定する	**web idle-timeout** *minutes*	デフォルト：10分
5. （オプション設定項目）オンライン HTTP ユーザの最大数を設定する	**aaa session-limit https** *max-sessions*	デフォルト：32 オンライン中のHTTPSユーザには影響しません。現在のオンライン中のHTTPSユーザ数が、新しく設定した最大数以上である場合、オンラインHTTPSユーザがログアウトするまで新規にログインすることができません。詳細はQX-W2300ACシリーズアクセスコントローラコマンドマニュアルの“*13 ユーザアクセスと認証*“の”*3章 AAA*“を参照してください。
6. ローカルユーザを追加し、local user view に移行する	**local-user** *user-name* [**class manage**]	デフォルト：設定なし

操作	コマンド	補足
7. ローカルユーザのパスワードを設定する	**password** [{ **hash** | **simple** } *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。 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。 セキュリティのためローカルユーザのパスワードを設定してください。
8. ローカルユーザのユーザロールを設定する	**authorization-attribute user-role** *user-role*	デフォルト：network-operator
9. ローカルユーザのサービスタイプを指定する	**service-type https**	デフォルト：設定なし

6.3 Webログインの表示と維持

すべての view で実行可能です。

操作	コマンド
オンラインWebユーザを表示する	**display web users**
HTTPサービスの設定と状態を表示する	**display ip http**
HTTPSサービスの設定と状態を表示する	**display ip https**
オンラインWebユーザをログオフする	**free web users** { **all** | **user-id** *user-id* | **user-name** *user-name* }

6.4 Webログインの設定例

6.4.1 HTTP ログインの設定例

I. ネットワーク要件

図 6-1に示すように IP ネットワークで通信可能な PC と AC を接続します。HTTP を使用して PC にログインします。



図 6-1 ネットワーク図

II. 設定手順

VLAN 100 を作成します。

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
```

VLAN-interface 100 を作成し、IP アドレス 192.168.100.99/24 をインタフェースに設定します。

```
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 192.168.100.99 24
[AC-Vlan-interface100] quit
```

admin と名付けたローカルユーザを作成し、パスワードを設定します。サービスタイプを HTTP、ユーザロールを network-admin に設定します。

```
[AC] local-user admin
[AC-luser-manage-admin] service-type http
[AC-luser-manage-admin] authorization-attribute user-role network-admin
[AC-luser-manage-admin] password simple hello12345
[AC-luser-manage-admin] quit
```

HTTP を有効にします。

```
[AC] ip http enable
```

III. 設定の確認

1) PC で IE ブラウザを起動し、アドレスバーに Device の IP アドレスを入力します。
2) ログインページでユーザ名、パスワード、verification code を入力します。English を選択し“Login”をクリックします。

認証に成功したのち、ホームページが表示されます。Device を設定することができます。

目次

このセクションのページは**2-x-x** です。

7章 ログインユーザの制御 7-1
7.1 Telnet/SSHログインの制御 7-1
7.1.1 設定手順 7-1
7.1.2 設定例 7-2
7.2 Webログインの制御 7-2
7.2.1 送信元IPアドレスベースのWebログインの制御 7-3
7.2.2 オンラインWebユーザのログオフ 7-3
7.2.3 設定例 7-3

7章 ログインユーザの制御

不正なアクセスを防ぐため ACL(Access Control List)を使用し、ユーザのふるまいを監視および制御を行うため、コマンドの許可、アカウンティングの設定を行います。ACL の詳細は QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*15 セキュリティ*”の”*1 章 ACL*”を参照してください。

7.1 Telnet/SSHログインの制御

Telnet、SSH ログインをフィルタするため、異なる条件で ACL を使用します。

- **標準 ACL（2000～2999）**－送信元 IP アドレスを使用します。
- **拡張 ACL（3000～3999）**－送信元 IP アドレス、宛先 IP アドレスを使用します。
- **L2 ACL（4000～4999）**－送信元 MAC アドレスを使用します。

適用する ACL が存在しないあるいは、ルールがない場合、ユーザはログイン制限が適用されません。ACL がある場合、ACL によって許可されたユーザのみが Telnet あるいは SSH によって装置にアクセスすることができます。

7.1.1 設定手順

以下に Telnet ログインを制御する設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	－
2． Telnet ログインをフィルタする ACL を適用する	**telnet server acl** { *advanced-acl-number* | *basic-acl-number* | **mac** *mac-acl-number* }	デフォルト：設定なし

以下に SSH ログインを制御する設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	－
2． SSH ログインをフィルタする ACL を適用する	**ssh server acl** { *advanced-acl-number* | *basic-acl-number* | **mac** *mac-acl-number* }	デフォルト：ACLはなし 詳細はQX-W2300ACシリーズアクセスコントローラコマンドマニュアルの“*15セキュリティ*”の”*6章 SSH*”を参照してください。

🕮 **メモ：**

本設定によるフィルタリングでは暗黙の deny が適用されます。

7.1.2 設定例

I. ネットワーク要件

図 7-1に装置が Host A と Host B からの Telnet パケットのみを許可するように設定します。

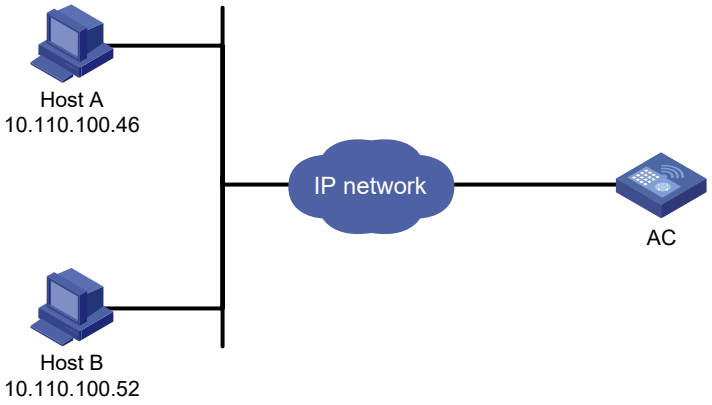


図 7-1 ネットワーク図

II. 設定手順

Host A、Host B からのパケットを許可する ACL を設定します。

```
<AC> system-view
[AC] acl basic 2000 match-order config
[AC-acl-ipv4-basic-2000] rule 1 permit source 10.110.100.52 0
[AC-acl-ipv4-basic-2000] rule 2 permit source 10.110.100.46 0
[AC-acl-ipv4-basic-2000] quit
```

Telnet ログインをフィルタするため ACL を適用します。

```
[AC] telnet server acl 2000
```

7.2 Webログインの制御

HTTP、HTTPS ログインをフィルタするため、送信元 IP アドレスによって標準 ACL（2000～2999）あるいは拡張 ACL(3000~3999)を使用します。

適用する ACL が存在しないあるいは、ルールがない場合、ユーザはログイン制限が適用されません。ACL がある場合、ACL によって許可されたユーザのみが HTTP、HTTPS によって装置にアクセスすることができます。

ログインしている疑わしい Web ユーザをログオフすることもできます。

7.2.1 送信元 IP アドレスベースの Web ログインの制御

Web ログイン要求にはユーザ名、パスワードが含まれます。セキュリティのため、装置は常に Web ログイン要求を転送するため HTTPS を使用します。以下の ACL で許可されたユーザのみが HTTP を通して装置にアクセスできます。

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

以下に送信元 IP アドレスベースの Web ログインを制御する設定を示します。

以下に Web ログインを制御する設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． Web ログインをフィルタする ACL を適用する	• **ip http acl** { *acl-number* | **name** *acl-name* } • **ip https acl** { *acl-number* | **name** *acl-name* }	デフォルト：設定なし
3． (オプション設定項目) TCP 接続を制御する ACL を適用する	• HTTPクライアントからのTCP接続を制御する **http acl** { *advanced-acl-number* | *basic-acl-number* } • HTTPSクライアントからのTCP接続を制御する **https acl** { *advanced-acl-number* | *basic-acl-number* }	デフォルト：すべてのHTTPクライアントとHTTPSクライアントが装置へのTCP接続を確立できます。

7.2.2 オンライン Web ユーザのログオフ

以下にオンライン Web ユーザをログオフする設定を示します。

操作	コマンド	補足
オンラインWebユーザをログオフする	**free web users** { **all** | **user-id** *user-id* | **user-name** *user-name* }	―

7.2.3 設定例

I. ネットワーク要件

図 7-2に示すように AC は HTTP サーバです。AC は Host B のみに HTTP サービスを提供するように設定します。

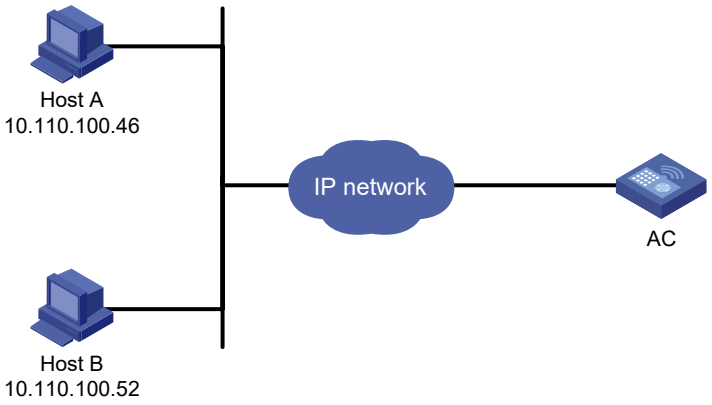


図 7-2 ネットワーク図

II. 設定手順

ACL を作成します。Host B からのパケットを許可するルール 1 を設定します。

```
< AC > system-view
[AC] acl basic 2030 match-order config
[AC-acl-ipv4-basic-2030] rule 1 permit source 10.110.100.52 0
```

Host B の Web ユーザが Device にアクセスできるように HTTP サービスを ACL に関連づけます。

```
[AC] ip http acl 2030
```

目次

このセクションのページは**2-x-x** です。

8章 FTP 8-1
8.1 FTPサーバの使用 8-1
8.1.1 認証および許可の設定 8-2
8.1.2 FTP接続の手動解放 8-3
8.1.3 FTPサーバの表示と維持 8-3
8.1.4 FTPサーバ設定例 8-3
8.2 FTPクライアントの使用 8-5
8.2.1 FTP接続の確立 8-5
8.2.2 FTPサーバのディレクトリの管理 8-6
8.2.3 FTPサーバの動作 8-6
8.2.4 別のユーザアカウントへの変更 8-7
8.2.5 FTP接続の維持とトラブルシューティング 8-8
8.2.6 FTP接続の終了 8-8
8.2.7 コマンドヘルプ情報の表示 8-8
8.2.8 FTPクライアントの表示と維持 8-8
8.2.9 FTPクライアント設定例 8-9

8章 FTP

FTP（File Transfer Protocol）は、IP ネットワークのサーバとクライアント間でファイルを共有するためのアプリケーションレイヤプロトコルです。FTP を利用することで、ファイルのアップグレードやダウンロードが可能です。

FTP はクライアント/サーバモデルで動作します。AC は FTP サーバあるいは FTP クライアントとして動作することができます。

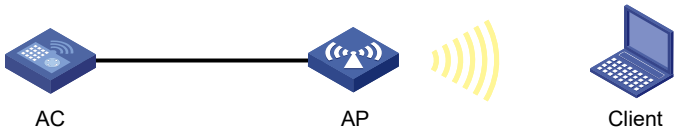


図 8-1 FTP アプリケーションのシナリオ

FTP は、2 つのモードでファイルを送信します。

- **Binary mode**– プログラムファイルの送信に使用します。たとえば、拡張子“**.bin**”、“**.btm**”のファイルです。
- **ASCII mode**– テキストファイルの送信に使用します。たとえば、拡張子“**.txt**”、“**.bat**”、“**.cfg**”のファイルです。

装置が FTP クライアントとして動作する場合、転送モードを設定することができます。デフォルトで binary モードを使用します。

装置が FTP サーバとして動作する場合、転送モードは FTP クライアントによって決定します。

FTP 動作モードは、以下のモードがあります。

- **Active mode（PORT）**– アクティブモードです。FTP サーバはデータ接続リクエストを初期化します。FTP クライアントがプライベートネットワークにあるなどのファイアウォール（Firewall）の内側にある場合、このモードでは使用できません。
- **Passive mode（PASV）**– パッシブモードです。FTP クライアントはデータ接続リクエストを初期化します。サーバ側が、クライアントからランダムポート（1024 以上）で接続することを許可していない場合、使用できません。

FTP 動作モードは、FTP クライアントのプログラムによって異なります。

8.1 FTPサーバの使用

装置を FTP サーバとして使用する場合、装置で FTP サーバを有効にし、認証と許可の設定を行ってください。ほかのコマンドはオプションです。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. FTP を有効にする	**ftp server enable**	デフォルト：無効

操作	コマンド	補足
3. （オプション設定項目）FTP サーバのアクセス管理を行うため ACL を使用する	**ftp server acl** { *advanced-acl-number* | *basic-acl-number* | **ipv6** { *advanced-acl-number* | *basic-acl-number* } }	デフォルト：設定なし
4. （オプション設定項目）idle-timeout タイマを設定する	**ftp timeout** *minutes*	デフォルト：30分 アイドルタイムアウト時間内にFTPサーバとFTPクライアント間で情報のやり取りがなければ、FTP接続は終了します。
5. （オプション設定項目）送信 FTP パケットの DSCP 値を設定する	**ftp server dscp** *dscp-value*	デフォルト：0
6. （オプション設定項目）現在のログインユーザの最大数を設定する	**aaa session-limit ftp** *max-sessions*	デフォルト：32 この変更はオンラインユーザに影響しません。FTPユーザの現在の数が新しい設定の値以上ならば、オンラインユーザがログアウトするまで、どの追加のFTPユーザもログインすることができません。詳細はQX-W2300ACシリーズアクセスコントローラコマンドマニュアルの“*13 ユーザアクセスと認証*“の”*3 章 AAA*“を参照してください。

8.1.1 認証および許可の設定

FTP サーバは、FTP クライアントを認証し、認証されたクライアントがアクセスできる用に許可されたディレクトリを設定する必要があります。

以下の認証モードが有効です。

- **ローカル認証**– 装置はローカルユーザ名データベースのクライアントのユーザ名とパスワードを確認し、もし一致している場合、認証が成功します。
- **リモート認証**– 装置は認証を行うため、クライアントのユーザ名とパスワードをリモート認証サーバに送信します。ユーザの名は、装置ではなくリモート認証サーバに設定されています。

以下の許可モードが有効です。

- **ローカル許可**– 装置は、ローカルに設定された許可の属性に従い、FTP クライアントのディレクトリを割り当てます。
- **リモート許可**– リモート許可サーバは装置で許可されるディレクトリを FTP クライアントに割り当てます。

認証と許可の詳細は、QX-W2300AC シリーズアクセスコントローラコマンドマニュアルの“*13 ユーザアクセスと認証*“の”*3 章 AAA*“を参照してください。

8.1.2 FTP 接続の手動解放

操作	コマンド
FTP接続を手動で開放する	• 指定したユーザ名を使用して確立したFTP接続を開放する： **free ftp user** *username* • 指定したIPアドレスを使用して確立したFTP接続を開放する： **free ftp user-ip** *client-address* [**port** *port-num*]

8.1.3 FTP サーバの表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
FTPサーバの設定とステータス情報を表示する	**display ftp-server**
オンラインFTPユーザの詳細情報を表示する	**display ftp-user**

8.1.4 FTP サーバ設定例

I. ネットワーク要件

- AC を FTP サーバとして設定します。
- FTP サーバにユーザ名 **abc**、パスワード **123456** のローカルユーザアカウントを作成します。
- ユーザアカウントは、FTP クライアントから FTP サーバにログインするために使用します。
- FTP クライアントから FTP サーバにファイル **temp.bin** をアップグレードします。
- FTP サーバから FTP クライアントにバックアップ用として設定ファイル **startup.cfg** をダウンロードします。

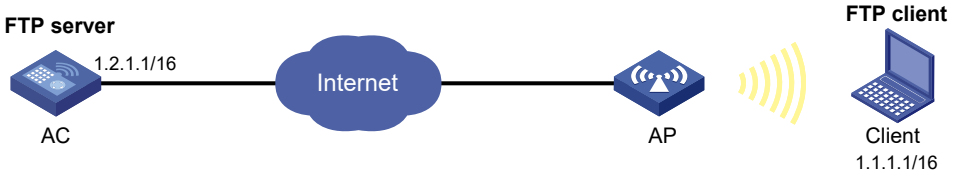


図 8-2 ネットワーク図

II. 設定手順

1) 図 8-2に示すように IP アドレスを設定し、AC と PC で互いに通信できることを確認します。（詳細は省略します。）
2) FTP サーバを設定します。

ローカルユーザアカウント **abc**、パスワード **123456** のローカルユーザを作成します。

```
<AC> system-view
[AC] local-user abc class manage
[AC-luser-abc] password simple 123456
```

ユーザにユーザロール network-admin を割り当てます。フラッシュメモリのルートディレクトリに作業ディレクトリを設定します。

```
[AC-luser-abc] authorization-attribute user-role network-admin work-directory flash:/
```

サービスタイプ FTP をユーザに割り当てます。

```
[AC-luser-abc] service-type ftp
[AC-luser-abc] quit
```

FTP ユーザを有効にします。

```
[AC] ftp server enable
[AC] quit
```

#ストレージスペースを確認し、空きスペースが不足している場合、未使用ファイルを削除して空き容量を増やします。

```
<AC> dir
Directory of flash:
     0      drw-           -  Jun 29 2016 18:30:38     logfile
     1      drw-           -  Jun 21 2016 14:51:38     diagfile
     2      drw-           -  Jun 21 2016 14:51:38     seclog
     3      -rw-        2943  Jul 02 2016 08:03:08     startup.cfg
     4      -rw-       63901  Jul 02 2016 08:03:08     startup.mdb
     5      -rw-         716  Jun 21 2016 14:58:02     hostkey
     6      -rw-         572  Jun 21 2016 14:58:02     serverkey
     7      -rw-     6541264  Aug 04 2016 20:40:49     backup.bin

473664 KB total (467080 KB free)
<AC> delete /unreserved flash:/backup.bin
```

3) FTP クライアントから FTP を実行します。

ローカルユーザアカウント **abc**、パスワード **123456** で FTP サーバ 1.2.1.1 にログインします。

```
c:\> ftp 1.2.1.1
Connected to 1.2.1.1.
220 FTP service ready.
User (1.2.1.1:(none)): abc
331 Password required for abc.
Password:
230 User logged in.
```

FTP 転送モードを ASCII モードに設定し、FTP サーバから PC にバックアップ用の設定ファイル **startup.cfg** をダウンロードします。

```
ftp> ascii
200 TYPE is now ASCII
```

```
ftp> get startup.cfg back-startup.cfg
```

FTP 転送モードを binary モードに設定し、AC へ **temp.bin** をアップロードします。

```
ftp> binary
200 TYPE is now 8-bit binary
ftp> put temp.bin
```

FTP からログアウトします。

```
ftp> bye
```

8.2 FTPクライアントの使用

8.2.1 FTP 接続の確立

FTP サーバにアクセスするため、FTP クライアントから FTP サーバに接続を確立する必要があります。

以下に IPv4 FTP 接続を確立する設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. （オプション設定項目）送信 FTP パケットの送信元IPアドレスを設定する	**ftp client source** { **interface** *interface-type interface-number* | **ip** *source-ip-address* }	デフォルト：送信元IPアドレスは、出力インタフェースのプライマリIPアドレスが使用されます。
3. user view へ戻る	**quit**	—
4. FTP サーバにログインする	• （方式1） user viewから直接FTPサーバにログインする： **ftp** [*ftp-server* [*service-port*] [**dscp** *dscp-value* | **source** { **interface** *interface-type interface-number* | **ip** *source-ip-address* } | **-d**] *] • （方式2） FTP client viewからFTPサーバにログインする： • **ftp** • **open** *server-address* [*service-port*]	**ftp**コマンドで指定された送信元IPアドレスは、**ftp client source**コマンドで指定されたアドレスより優先されます。

8.2.2 FTP サーバのディレクトリの管理

操作	コマンド
FTPサーバのディレクトリあるいはファイル情報を表示する	• FTPサーバのディレクトリあるいはファイルの詳細情報を表示する： **dir** [*remotefile* [*localfile*]] • FTPサーバのディレクトリ名あるいはファイル名を表示する： **ls** [*remotefile* [*localfile*]]
FTPサーバの作業ディレクトリを変更する	**cd** { *directory* | **..** | */* }
現在のディレクトリを終了して、上位レベルのディレクトリに移行する	**cdup**
FTPサーバの現在のディレクトリを表示する	**pwd**
FTPサーバにディレクトリを作成する	**mkdir** *directory*
リモートFTPサーバで指定した作業ディレクトリを削除する	**rmdir** *directory*

⚠ **注意**：

FTP サーバからディレクトリを削除する場合は注意が必要です。FTP サーバからディレクトリを削除する場合は、そのディレクトリが使用されていないことを確認してください。

8.2.3 FTP サーバの動作

FTP サーバにログインした後、以下の手順で、許可されたディレクトリからファイルのアップロードあるいはダウンロードすることができます。

1) FTP サーバのディレクトリとファイルの場所を表示するため **dir** コマンドあるいは **ls** コマンドを使用します。
2) 記憶領域の不要なファイルを削除します。
3) FTP 転送モードを設定します。FTP 転送モードは、テキストデータを転送する ASCII モードと、イメージデータを転送する binary モードの 2 つがあります。
4) **lcd** コマンドを使用して、FTP クライアントの作業ディレクトリを変更します。このディレクトリの下にファイルをダウンロードしたり、ダウンロードしたファイルを保存したりすることができます。
5) ファイルのアップロードあるいはダウンロードを行います。

以下に FTP client view で FTP サーバのファイルの動作を示します。

操作	コマンド	補足
FTPサーバのディレクトリあるいはファイル情報を表示する	• FTPサーバのディレクトリあるいはファイルの詳細情報を表示する： **dir** [*remotefile* [*localfile*]] • FTPサーバのディレクトリ名あるいはファイル名の情報を表示する： **ls** [*remotefile* [*localfile*]]	―
FTPサーバの指定したファイルを完全に削除する	**delete** *remotefile*	⚠**注意：** FTPサーバからファイルを完全に削除する場合は注意が必要です。FTPサーバからファイルを完全に削除する場合は、そのファイルが使用されていないことを確認してください。
FTP転送モードを設定する	• ASCIIIに設定する： **ascii** • バイナリに設定する： **binary**	デフォルト：binary
データ転送モードをpassiveに設定する	**passive**	デフォルト：passive
FTPクライアントの現在の作業ディレクトリを表示あるいは変更する	**lcd** [*directory* **|** */*]	―
FTPサーバにファイルをアップロードする	**put** *localfile* [*remotefile*]	―
FTPサーバからファイルをダウンロードする	**get** *remotefile* [*localfile*]	―
ローカルファイルをアップロードする	**newer** *remotefile*	―

8.2.4 別のユーザアカウントへの変更

FTP サーバにログインした後、FTP 接続を再確立しないで、ユーザ名を変更することができます。新しいユーザ名とパスワードを正しく入力してください。間違ったユーザ名とパスワードを入力すると接続は切断されます。

別のユーザアカウントに変更するため、user view で以下のコマンドを行います。

操作	コマンド
FTPサーバにログインした後別のユーザアカウントに変更する。	**user** *username* [*password*]

8.2.5 FTP 接続の維持とトラブルシューティング

操作	コマンド	補足
FTPサーバがサポートしているFTP関連コマンドを表示する	**rhelp**	―
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する	**rhelp** *protocol-command*	―
FTP動作の詳細情報の表示を有効あるいは無効にする	**verbose**	デフォルト：有効
FTPクライアントのデバッグを有効あるいは無効にする	**debug**	デフォルト：無効

8.2.6 FTP 接続の終了

操作	コマンド
FTP client viewを終了せずにFTPサーバとの接続を切断する	• **disconnect** • **close**
F TPサーバとの接続を切断し、user viewに戻る	• **bye** • **quit**

8.2.7 コマンドヘルプ情報の表示

以下にサーバにログインした後、ヘルプ情報を表示するコマンドを示します。

操作	コマンド
ヘルプ情報を表示する	• **help** [*command-name*] • **?** [*command-name*]

8.2.8 FTP クライアントの表示と維持

すべての view で **display** コマンドを実行します。

操作	コマンド
FTPクライアントで送信元IPアドレス情報を表示する	**display ftp client source**

8.2.9 FTP クライアント設定例

I. ネットワーク要件

図 8-3に示すように PC は FTP サーバとして動作します。ユーザ名 **abc**、パスワード **hello12345** のユーザアカウントは PC 上で作成されています。

- FTP クライアントとして AC が FTP サーバにログインします。
- FTP サーバから FTP クライアントに **temp.bin** ファイルをダウンロードします。
- バックアップ用として FTP クライアントから FTP サーバに設定ファイル **startup.cfg** をアップロードします。

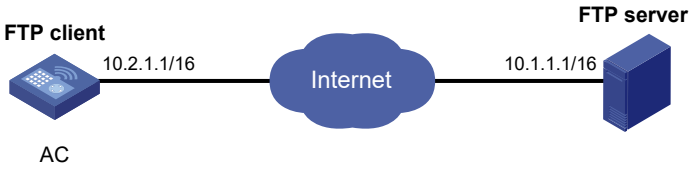


図 8-3 ネットワーク図

II. 設定手順

#図 8-3に示すように IP アドレスを設定し、AC と PC で互いに通信できることを確認します。（詳細は省略します。）

AC の記憶媒体の空き容量が十分あることを確認します。もし空き容量が十分でない場合、**delete /unreserved** *file-url* コマンドを使用し、不必要なファイルを削除してください。（詳細は省略します。）

ユーザ名 **abc**、パスワード **hello12345** を使用して、FTP サーバ 10.1.1.1 にログインします。

```
<AC> ftp 10.1.1.1
Press CTRL+C to abort.
Connected to 10.1.1.1 (10.1.1.1).
220 WFTPD 2.0 service (by Texas Imperial Software) ready for new user
User (10.1.1.1:(none)): abc
331 Give me your password, please
Password:
230 Logged in successfully
Remote system type is MSDOS.
ftp>
```

ファイル転送モードを設定します。

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

PC から AC にファイル **temp.bin** をダウンロードします。

```
ftp> get temp.bin
local: temp.bin remote: temp.bin
150 Connecting to port 47457
226 File successfully transferred
23951480 bytes received in 95.399 seconds (251.0 kbyte/s)
```

FTP 転送モードを ASCII モードに設定し、AC から PC にバックアップ用に設定ファイル **startup.cfg** をアップロードします。

```
ftp> ascii
200 TYPE is now ASCII
ftp> put startup.cfg back-startup.cfg
local: startup.cfg remote: back-startup.cfg
150 Connecting to port 47461
226 File successfully transferred
3494 bytes sent in 5.646 seconds (618.00 kbyte/s)
ftp> bye
221-Goodbye. You uploaded 2 and downloaded 2 kbytes.
221 Logout.
<AC>
```

目次

このセクションのページは**2-x-x** です。

9章 TFTP 9-1
9.1 IPv4 TFTPクライアントの設定 9-1

9章 TFTP

TFTP （Trivial File Transfer Protocol）は、FTP を簡略化したプロトコルです。TCP ベースの FTP と比較して TFTP は認証がないあるいはクライアントとサーバ間で複雑なやり取りを必要としないため、より簡単に使用することができます。TFTP は信頼性のあるネットワークで使用する場合に適しています。

装置は TFTP クライアント機能のみをサポートします。装置から TFTP サーバにファイルのアップロードあるいは TFTP サーバから装置にファイルのダウンロードを行うことができます。目的のディレクトリに、同一の名前のファイルがある状態でファイルをダウンロードした場合、既に存在しているファイルは削除され、ダウンロードされたファイルに上書きされます。ネットワークの切断などの理由によってファイルのダウンロードに失敗した場合、もとのファイルを復旧することはできません。そのため同一の名前がないことを確認した後、ファイルの転送を行います。



図 9-1 TFTP アプリケーションシナリオ

9.1 IPv4 TFTPクライアントの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. （オプション設定項目）TFTP サーバにアクセスするクライアントを管理するため ACL を使用する	**tftp-server acl** *acl-number*	デフォルト：設定なし
3. TFTP クライアントの送信元 IP アドレスを設定する	**tftp client source** { **interface** *interface-type interface-number* | **ip** *source-ip-address* }	デフォルト：送信元IPアドレスは、出力インタフェースのプライマリIPアドレスが使用されます。
4. user view へ戻る	**quit**	―
5. IPv4 ネットワークでファイルをダウンロードあるいはアップロードする	**tftp** *tftp-server* { **get** | **put** | **sget** } *source-filename* [*destination-filename*] [**dscp** *dscp-value* | **source** { **interface** *interface-type interface-number* | **ip** *source-ip-address* }] * [**-d**]	このコマンドで指定された送信元IPアドレスは、**tftp client source**コマンドで指定されたアドレスより優先されます。 このコマンドはuser viewで使用します。

目次

このセクションのページは**2-x-x** です。

10章 ファイルシステム管理 10-1
10.1 概要 10-1
10.1.1 ファイルシステム 10-1
10.1.2 ディレクトリ 10-1
10.1.3 ファイル 10-2
10.1.4 ディレクトリ、ファイル名の指定 10-3
10.2 ファイルシステムの管理の制限とガイドライン 10-4
10.3 ファイルシステムの管理 10-4
10.3.1 記憶媒体のフォーマット 10-4
10.3.2 記憶媒体の回復 10-5
10.4 ディレクトリの管理 10-5
10.4.1 ディレクトリ情報の表示 10-5
10.4.2 カレント作業ディレクトリの表示 10-5
10.4.3 カレント作業ディレクトリの変更 10-5
10.4.4 ディレクトリの作成 10-5
10.4.5 ディレクトリ名の変更 10-6
10.4.6 ディレクトリのアーカイブ（圧縮）/解凍 10-6
10.4.7 ディレクトリの削除 10-6
10.4.8 ディレクトリの動作モードの設定 10-6
10.5 ファイルの管理 10-7
10.5.1 ファイル情報の表示 10-7
10.5.2 テキストファイルの内容表示 10-7
10.5.3 ファイル名の変更 10-7
10.5.4 ファイルのコピー 10-8
10.5.5 ファイルの移動 10-8
10.5.6 ファイルの圧縮/解凍 10-8
10.5.7 ファイルのアーカイブ（圧縮）/解凍 10-8
10.5.8 ファイルの削除/回復 10-8
10.5.9 ごみ箱のファイルを削除する 10-9
10.5.10 ファイルの動作モードの設定 10-9

10章 ファイルシステム管理

10.1 概要

10.1.1 ファイルシステム

装置はフラッシュメモリと USB ディスクをサポートします。各ストレージメディアは 1 つのファイルシステムを有します。

I. 記憶媒体の命名ルール

フラッシュメモリ上のファイルシステム名は **flash:** です。

USB ディスク上のファイルシステム名は以下になります。

- 記憶媒体タイプ: usb
- シーケンス番号（A、B などの大文字の英字）
- 拡張スロット番号（0、1 などの数字）
- コロン（:）

たとえば、最初の USB ディスク上のファイルシステムの名前は usbA0:です。

⚠ **注意**：
ファイルシステム名は大文字と小文字が区別され、正しく入力する必要があります。

II. デフォルトファイルシステム

装置にログインしたのち、デフォルトではデフォルトファイルシステムで動作します。デフォルトファイルのファイルあるいはディレクトリを指定する場合、ファイルシステム名を指定する必要はありません。たとえば、デフォルトファイルシステムのルートディレクトリにカレントコンフィグレーションを保存する場合、すべての位置情報を指定する必要がありません。

10.1.2 ディレクトリ

ファイルシステムのディレクトリはツリー形状に構成されます。

I. ルートディレクトリ

ルートディレクトリはスラッシュ（/）で示します。たとえば、flash:/はフラッシュメモリのルートディレクトリを示します。

II. 作業ディレクトリ

作業ディレクトリはカレントディレクトリとも呼ばれます。

デフォルトの作業ディレクトリはフラッシュメモリのルートディレクトリです。

III. ディレクトリ命名ルール

ディレクトリの名前を指定する場合、以下のルールに従ってください。

- ディレクトリ名は、英字、数字、以下の文字を除く特殊文字を指定することができます。

  アスタリスク（*）、垂直バー（|）、スラッシュ（/）、バックスラッシュ（\）、クエスチョンマーク（?）、左アングルブラケット（<）、右アングルブラケット（>）、ダブルクォーテーションマーク（"）、コロン（:）
- ドット（.）で始まるディレクトリは隠しディレクトリです。システムがディレクトリを隠さないようにするため、ドット（.）で始まるディレクトリ名を指定しないでください。

IV. 共通使用ディレクトリ

装置はデフォルトのディレクトリがあります。システムは動作中に自動でディレクトリを作成します。以下のディレクトリがあります。

- **diagfile**—診断情報ファイルを記録します。
- **license**—ライセンスファイルを記録します。
- **apimage**—FIT-AP のソフトウェアを保管します。
- **logfile**—ログファイルを記録します。
- **seclog**—セキュリティログファイルを記録します。
- **versionInfo**—ソフトウェアのバージョン情報ファイルを記録します。

10.1.3 ファイル

I. ファイル命名ルール

ファイルの名前を指定する場合、以下のルールに従ってください。

- ファイル名は、名は、英字、数字、以下の文字を除く特殊文字を指定することができます。

  アスタリスク（*）、垂直バー（|）、スラッシュ（/）、バックスラッシュ（\）、クエスチョンマーク（?）、左アングルブラケット（<）、右アングルブラケット（>）、ダブルクォーテーションマーク（"）、コロン（:）
- ドット（.）で始まるファイルは隠しファイルです。システムがファイルを隠さないようにするため、ドット（.）で始まるファイル名を指定しないでください。

II. 共通使用ファイル

装置はデフォルトのファイルがあります。システムは動作中に自動でファイルを作成します。以下のファイルがあります。

- **.ipe file**—圧縮されたソフトウェアイメージの一括ファイル
- **.bin file**—ソフトウェアイメージファイル
- **.cfg file**—コンフィグレーションファイル
- **.mdb file**—バイナリ形式のコンフィグレーションファイル
- **.log file**—ログファイル
- **.mpcfg**—map-config 用サンプルコンフィグレーションファイル

III. 隠しファイルとディレクトリ

一部のシステムファイルとディレクトリは隠されています。システムの動作および機能の正常性のため、隠しファイルやディレクトリの変更や削除をしないでください。

10.1.4 ディレクトリ、ファイル名の指定

I. ディレクトリの指定

ディレクトリを指定する場合、絶対パスあるいは相対パスを使用することができます。たとえば、作業ディレクトリは **flash:/**です。図 10-1の test2 ディレクトリを指定する場合、以下の方法を使用することができます。

- flash:/test/test1/test2 （絶対パス）
- flash:/test/test1/test2/ （絶対パス）
- test/test1/test2 （相対パス）
- test/test1/test2/ （相対パス）



図 10-1 ディレクトリ階層の例

II. ファイルの指定

ファイルを指定する場合、以下の方法に従います。

- */filesystem*/*directory1*/*directory2*/…/*directoryn*/*filename* のフォーマットでファイルの絶対パスとファイル名を入力します。ここで *directoryn* はファイルが存在するディレクトリです。
- ファイルの相対パスとファイル名を入力します。

たとえば、作業ディレクトリは **flash:/**です。ファイル samplefile.cfg は、図 10-1の test2 ディレクトリにあります。ファイル samplefile.cfg を指定する場合、以下の方法を使用することができます。

- flash:/test/test1/test2/samplefile.cfg

- test/test1/test2/samplefile.cfg

10.2 ファイルシステムの管理の制限とガイドライン

ファイルシステムの障害を避けるため、ファイルシステムの操作中に記憶媒体の挿入、及び、取り外しを行わないでください。

記憶媒体のフォルダやファイルにアクセスしている間に記憶媒体を取り外した場合、装置は再インストールするときに記憶媒体を認識しない可能性があります。このような記憶媒体を再インストールする場合、以下の作業の 1 つを行ってください。

- ファイルあるいはディレクトリの絶対パスを使用してください。たとえば、フラッシュメモリのファイルシステムにあるファイル、ディレクトリを表示する場合、**dir flash:/**コマンドを使用してください。
- ファイルシステムのファイルあるいはディレクトリにアクセスする前に、ファイルシステムのルートディレクトリの作業ディレクトリを **cd** コマンドで変更してください。たとえば、フラッシュメモリのファイルシステムのルートディレクトリにあるファイルあるいはディレクトリを表示し、以下の処理を行ってください。

a) ファイルシステムのルートディレクトリに作業ディレクトリを、**cd flash:/**コマンドで変更してください。

b) **cd**コマンドを実行してください。

- 記憶媒体のファイルにアクセスしている場合は、ファイルを閉じてください。

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。

10.3 ファイルシステムの管理

10.3.1 記憶媒体のフォーマット

注意：
記憶媒体がフォーマットされた後、すべてのファイルとディレクトリは削除され、回復できません。記憶媒体にスタートアップコンフィグレーション ファイルが存在する場合は、必要に応じてバックアップしてください。

記憶媒体をフォーマットするとき、他のユーザがアクセスしていないことを確認してください。

user view で以下の操作を実行します。

操作	コマンド
記憶媒体をフォーマットする	**format** *medium-name*

10.3.2 記憶媒体の回復

記憶媒体のスペースが、何らかの異常な操作のためアクセスできない場合、記憶媒体のスペースを回復するために **fixdisk** コマンドを使用できます。

記憶媒体を復旧する前に、他のユーザが記憶媒体へアクセスしていないことを確認してください。そうでないと回復作業は失敗します。

user view で以下の操作を実行します。

操作	コマンド
記憶媒体を回復する	**fixdisk** *filesystem*

10.4 ディレクトリの管理

10.4.1 ディレクトリ情報の表示

user view で以下の操作を実行します。

操作	コマンド
ディレクトリの情報を表示する	**dir** [**/all**] [*file* | *directory* | **/all-filesystems**]

10.4.2 カレント作業ディレクトリの表示

user view で以下の操作を実行します。

操作	コマンド
カレント作業ディレクトリを表示する	**pwd**

10.4.3 カレント作業ディレクトリの変更

user view で以下の操作を実行します。

操作	コマンド
カレント作業ディレクトリを変更する	**cd** { *directory* | **..** | **/** }

10.4.4 ディレクトリの作成

user view で以下の操作を実行します。

操作	コマンド
ディレクトリを作成する	**mkdir** *directory*

10.4.5 ディレクトリ名の変更

user view で以下の操作を実行します。

操作	コマンド
ディレクトリ名を変更する	**rename** *source-directory dest-directory*

10.4.6 ディレクトリのアーカイブ（圧縮）/解凍

ディレクトリをアーカイブ（圧縮）/解凍する場合、ディレクトリの中にあるファイルもアーカイブ（圧縮）/解凍されます。アーカイブ（圧縮）されたディレクトリを表示する場合、ディレクトリの中にあるファイルも解凍されます。

user view で実行可能です。

操作	コマンド
ディレクトリをアーカイブする	**tar create** [**gz**] *archive-file dest-file* [**verbose**] **source** *source-directory* &<1-5>
ディレクトリを解凍する	**tar extract archive-file** *file* [**verbose**] [**screen** | **to** *directory*]
アーカイブされたディレクトリのリストを表示する	**tar list archive-file** *file*

10.4.7 ディレクトリの削除

user view で以下の操作を実行します。

操作	コマンド
ディレクトリを削除する	**rmdir** *directory*

注意：
ディレクトリを削除するには、まずディレクトリ内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。ごみ箱に移動した場合は、**rmdir** コマンドを実行してディレクトリを削除すると、完全に削除されます。**rmdir** コマンドを使用してディレクトリを削除する前に、ディレクトリとそのファイルおよびサブディレクトリが使用されていないことを確認する必要があります。

10.4.8 ディレクトリの動作モードの設定

ファイルシステムには、次のディレクトリの動作モードがあります。

- **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もたらす恐れのある操作についてシステムが警告を出します。
- **quiet**：どのような操作に対しても、システムは警告を出しません。

操作ミスによる望ましくない結果を避けるため、**alert** モードがよく使用されます。

以下にディレクトリの動作モードの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． ディレクトリの操作のプロンプトモードを設定する	**file prompt** { **alert** | **quiet** }	デフォルト：**alert** コマンドはファイルの動作モードも設定します。

10.5 ファイルの管理

コピー、ダウンロード、**save** コマンドを使用して、ファイルを作成することができます。ファイルのダウンロードの詳細は QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*2 基本機能*”の”*8 章 FTP*”および”*9 章 TFTP*”を参照してください。**save** コマンドについては QX-W2300AC シリーズアクセスコントローラコマンドマニュアルの“*2 基本機能*”の”*7 章 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。

10.5.1 ファイル情報の表示

user view で以下の操作を実行します。

操作	コマンド
ファイルの情報を表示する	**dir** [**/all**] [*file* | *directory* | **/all-filesystems**]

10.5.2 テキストファイルの内容表示

user view で以下の操作を実行します。

操作	コマンド
テキストファイルの内容を表示する	**more** *file-url*

10.5.3 ファイル名の変更

user view で以下の操作を実行します。

操作	コマンド
ファイル名を変更する	**rename** *source-file dest-file*

10.5.4 ファイルのコピー

user view で以下の操作を実行します。

操作	コマンド
ファイルをコピーする	**copy** *source-file* { *dest-file* | *dest-directory* } [**vpn-instance** **vpn-instance-name**] [**source interface** *interface-type interface-number*]

10.5.5 ファイルの移動

user view で以下の操作を実行します。

操作	コマンド
ファイルを移動する	**move** *source-file* { *dest-file* | *dest-directory* }

10.5.6 ファイルの圧縮/解凍

user view で以下の操作を実行します。

操作	コマンド
ファイルを圧縮する	**gzip** *file*
ファイルを解凍する	**gunzip** *file*

10.5.7 ファイルのアーカイブ（圧縮）/解凍

user view で実行可能です。

操作	コマンド
ファイルをアーカイブする	**tar create** [**gz**] *archive-file dest-file* [**verbose**] **source** *source-file*&<1-5>
ファイルを解凍する	**tar extract archive-file** *file* [**verbose**] [**screen** | **to** *directory*]
アーカイブされたファイルのリストを表示する	**tar list archive-file** *file*

10.5.8 ファイルの削除/回復

ファイルを完全に削除あるいは、再利用できるようにごみ箱に移動することができます。ごみ箱に移動したファイルは回復できますが、完全に削除したファイルは回復できません。

ごみ箱のファイルは、記憶媒体のスペースを使用します。ごみ箱のファイルを削除するには、**reset recycle-bin** コマンドを実行します。

user view で以下の操作を実行します。

操作	コマンド
ファイルをごみ箱に移す	**delete** *file*

操作	コマンド
ファイルをごみ箱から元に戻す	**undelete** *file*
ファイルを完全に削除する	**delete /unreserved** *file*

重要：

ごみ箱のファイルを削除するために **delete** コマンドを使用しないでください。**reset recycle-bin** コマンドを使用してください。

注意：

delete/unreserved *file* コマンドは、ファイルを完全に削除します。ファイルを復元できません。

10.5.9 ごみ箱のファイルを削除する

記憶媒体は**.trash** というごみ箱を使用します。ごみ箱のファイルを表示するには以下の方法を使用します。

- 記憶媒体に移動し、**dir /all .trash** コマンドを実行します。
- ごみ箱のフォルダに移動するため、**cd .trash** コマンドを実行し、**dir** コマンドを実行します。

user view でごみ箱のファイルを削除するには以下の操作を実行します。

操作	コマンド
カレントディレクトリ下で、ごみ箱でファイルを削除する	**reset recycle-bin** [**/force**]

注意：

ごみ箱内のファイルは、**undelete** コマンドを使用して復元できます。ごみ箱からファイルを削除すると、そのファイルは復元できません。ごみ箱からファイルを削除する前に、そのファイルが使用されていないことを確認してください。

10.5.10 ファイルの動作モードの設定

ファイルシステムには、次のファイルの動作モードがあります。

- **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もたらす恐れのある操作についてシステムが警告を出します。
- **quiet**：どのような操作に対しても、システムは警告を出しません。

以下にファイルの動作モードの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． ファイルの操作のプロンプトモードを設定する	**file prompt** { **alert** | **quiet** }	デフォルト：**alert** コマンドはディレクトリの動作モードも設定します。

目次

このセクションのページは **2-x-x** です。

11 章 コンフィグレーションファイル管理 11-1
11.1 概要 11-1
11.1.1 コンフィグレーションタイプ 11-1
11.1.2 次回の起動に使用するスタートアップコンフィグレーションファイルの冗長 . 11-2
11.1.3 コンフィグレーションファイルのフォーマット形式 11-2
11.1.4 スタートアップコンフィグレーションファイルの選択..... 11-2
11.1.5 コンフィグレーションファイルの内容とフォーマット..... 11-3
11.2 2 つのコンフィグレーション設定の差分表示..... 11-3
11.3 カレントコンフィグレーションの保存..... 11-4
11.4 次回の起動に使用するスタートアップコンフィグレーションファイルの設定 11-6
11.5 次回の起動で使用するスタートアップコンフィグレーションファイルの削除 11-7
11.6 コンフィグレーションファイルの表示と維持..... 11-7

11章 コンフィグレーションファイル管理

11.1 概要

コンフィグレーションファイルは、CLI あるいは Boot メニューから管理することができます。この章では CLI からコンフィグレーションファイルを管理する方法を記載します。

コンフィグレーションファイルには、装置のソフトウェア機能を設定するためのコマンドのセットが保存されます。設定はコンフィグレーションファイルに保存できるため、設定は再起動後にも適用されます。将来使用するために、コンフィグレーションファイルをホストにバックアップすることもできます。

11.1.1 コンフィグレーションタイプ

装置起動時に読み込まれた設定はスタートアップコンフィグレーションと呼ばれ、装置で動作している設定はカレントコンフィグレーションと呼ばれます。

以下にコンフィグレーションファイルの種類を示します。

I. デフォルトコンフィグレーション

初回起動時のコンフィグレーション設定で、装置固有のコンフィグレーション設定です。ファイルは”.ipe”の拡張子のパッケージファイルでリリースされ、変更できません。コンフィグレーションファイルあるいはスタートアップコンフィグレーションファイルが存在しない場合、デフォルトコンフィグレーションで起動します。

デフォルトコンフィグレーションの設定を表示するには、**display default-configuration** コマンドを使用します。装置に出荷時のデフォルトが付属していない場合、**display default-configuration** コマンドの出力は空になります。

II. スタートアップコンフィグレーション

ブートメニューあるいは CLI で指定されるコンフィグレーションファイルです。このファイルは次回の起動で使用するスタートアップコンフィグレーションファイルと呼ばれます。スタートアップコンフィグレーションで起動されたのち、カレントコンフィグレーションファイルと呼ばれます。システムの信頼性のため、メインとバックアップの 2 つの次回の起動で使用するスタートアップコンフィグレーションファイルを指定することができます。詳細は QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*2 基本機能*”の”*11 章 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。

- カレントコンフィグレーションと次回の起動で使用するスタートアップコンフィグレーションの設定を表示するには、**display startup** コマンドを使用します。詳細な設定を表示する場合、**more** コマンドを使用します。
- 次回の起動で使用するコンフィグレーションファイルの内容を表示するには、**display saved-configuration** コマンドを使用します。次回の起動で使用するコンフィグレーションファイルが保存されていない場合は表示されません。

III. カレントコンフィグレーション

カレントコンフィグレーションは稼働中の装置の現在の設定です。カレントコンフィグレーションはスタートアップコンフィグレーションと新しく設定したコンフィグレーションとなります。カレントコンフィグレーションは装置の一時的な記憶媒体に記録され、保存をしていない場合は、装置の電源 OFF/ON あるいは **reboot** コマンドを実行するときに削除されます。設定を削除しないようにするには、コンフィグレーションファイルにカレントコンフィグレーションを保存します。

カレントコンフィグレーションは **display current-configuration** コマンドを使用して表示することができます。表示されるパラメータはデフォルトコンフィグファイルのパラメータを含みません。

11.1.2 次回の起動に使用するスタートアップコンフィグレーションファイルの冗長

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バックアップのコンフィグレーションファイルを 1 つずつ指定することができます。

起動時、装置は以下の順番でスタートアップコンフィグレーションファイルの読み込みを行います。

1) 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で起動します。
2) 指定したメインスタートアップファイルがない、あるいは有効でない場合、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で起動します。
3) 指定したバックアップコンフィグレーションファイルがない、あるいは有効でない場合、装置はデフォルトのコンフィグレーションファイルで起動します。

11.1.3 コンフィグレーションファイルのフォーマット形式

コンフィグレーションファイルは、以下のフォーマット形式となります。

拡張子は、“.cfg”を使用する必要があります。“.cfg”ファイルはテキストファイルです。**more** コマンドで内容を表示することができます。“.cfg”で設定を保存したとき、装置は自動的に、同一ファイル名で拡張子が“.mdb”というバイナリデータを保存します。装置は”.mdb“の方が”.cfg“よりも速く読み込みます。

11.1.4 スタートアップコンフィグレーションファイルの選択

起動時、装置は以下の順番でコンフィグレーションファイルを識別します。

1) 装置は有効な“.cfg”の次回の起動で使用するコンフィグレーションファイルを検索します。
2) ファイルが見つかった場合は、“.cfg”と名前と内容が同じ“.mdb”ファイルを検索します。

3)　“.mdb”ファイルが見つかった場合は、その“.mdb”ファイルを起動で使用するコンフィグレーションファイルとします。見つからなかった場合は、“.cfg”ファイルを起動で使用するコンフィグレーションファイルとします。

本章で記載するコンフィグレーションファイルは、特に指定がない限り“.cfg”のコンフィグレーションファイルを示します。

11.1.5 コンフィグレーションファイルの内容とフォーマット

⚠ **重要**：

装置を起動するため、コンフィグレーションファイルは、装置で使用する規則とフォーマット形式に従う必要があります。起動時、コンフィグレーションファイルの読み込み失敗を防ぐため、装置で自動に作成されたコンフィグレーションファイルあるいは **save** コマンドを使用してください。もしコンフィグレーションファイルを編集する場合、装置で使われる規則とフォーマットにあわせてください。

相互に依存するコマンドのセットのいずれかで操作が失敗した場合、設定の復元またはロールバックが失敗することがあります。

コンフィグレーションファイルは以下の規則に従います。

- すべてのコマンドは省略されていない正しい形式のフォーマットで保存されます。
- コマンドラインに無効な文字は含まれません。

⚠ **重要**：

一部のコマンドライン(例えば、**sysname** コマンド)には疑問符 (?) または水平タブ (\t) を使用できません。システムが起動時に **sysname abc??** コマンドラインを含むコンフィグレーションファイルをロードした場合、システムはコマンドラインを無視し、デフォルトのシステム名を使用します。システムがそのコンフィグレーションファイルを使用して設定をロールバックまたは復元する場合、システム名はロールバックまたは復元されません。

- コマンドは view 毎にセクションに分かれて区別されています。通常は system view、interface view、protocol view、line view などの順番です。
- セクションは、1 行または複数行のブランク行またはコメント行（#）で区切られます。
- 最後に **return** が付きます。

11.2 2つのコンフィグレーション設定の差分表示

2 つのコンフィグレーションファイルで設定の差分を表示することができます。

比較を行うため次回の起動で使用するコンフィグレーションファイルを指定した場合、システムは以下の順番で次回の起動で使用するコンフィグレーションファイルを検索します。

1) 次回の起動で使用するメインコンフィグレーションファイルを検索します
2) 次回の起動で使用するメインコンフィグレーションファイルが有効でない、あるいは不正である場合、次回の起動で使用するバックアップコンフィグレーションファイルを検索します。

メインコンフィグレーションファイルとバックアップコンフィグレーションファイルの両方が有効でない、あるいは不正である場合、次回の起動で使用するコンフィグレーションファイルが存在しませんと表示します。

2 つのコンフィグレーションファイルの設定の差分を表示する方法を以下に示します。

すべての view で **display** コマンドを実行します。

操作	コマンド
指定された2つのコンフィグレーションファイルの差分を表示する	**display diff configfile** *file-name-s* **configfile** *file-name-d*
指定されたコンフィグレーションファイルとカレントコンフィグレーションファイルの差分を表示する	• 方法1： **display diff configfile** *file-name-s* **current-configuration** • 方法2： **display diff current-configuration configfile** *file-name-d*
指定されたコンフィグレーションファイルと次回の起動で使用するコンフィグレーションファイルの差分を表示する	• 方法1： **display diff configfile** *file-name-s* **startup-configuration** • 方法2： **display diff startup-configuration configfile** *file-name-d*
次回の起動で使用するコンフィグレーションファイルとカレントコンフィグレーションファイルの差分を表示する	• 方法1： **display diff current-configuration startup-configuration** • 方法2： **display current-configuration diff** • 方法3： **display diff startup-configuration current-configuration**

11.3 カレントコンフィグレーションの保存

カレント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するとき、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することができます。

次回に起動するコンフィグレーションファイルとしてファイルを指定する場合、以下に示すどちらかの方法で、カレントコンフィグレーションの保存を行ってください。

- **高速保存モード**–**safely** キーワードを使わないで **save** コマンドを使用します。より速くファイルを保存しますが、装置が再起動、または処理中に電源が切れた場合、カレントコンフィグレーションファイルを失う可能性があります。装置を再起動した後、新しいスタートアップコンフィグレーションファイルを指定してください。詳細は QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*2 基本機能*”の”*11 章 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。
- **セーフモード**–**safely** キーワードを使い **save** コマンドを使用します。高速ではありませんが、装置が再起動、または処理中に電源切れた場合でも、装置でコンフィグレーションファイルを保持することができます。

次の起動時の設定の紛失を防ぐために、装置が動作中の設定を保存している間は、誰も装置を再起動したり電源を再投入したりしないようにしてください。

拡張インタフェースカードをシステムから取り外すと、その設定はメモリに保持されますが、システム上で動作中の設定からは削除されます。交換用カードを取り付ける前に動作中の設定を保存すると、次回起動時のコンフィグレーションファイルからそのカードの設定が削除されます。

カードを取り外した後に動作中の設定を保存している場合は、次の手順を実行して次回起動時のコンフィグレーションファイルにカードの設定を復元します。

1) 交換用カードを取り付けます。
2) 交換用カードがオンラインになったら、**display current-configuration** コマンドを実行して、カードの設定がメモリから実行中の設定に自動的に復元されたことを確認します。
3) 実行中の設定を次回起動時のコンフィグレーションファイルに保存します。

⚠ **重要**：

設定の復元を成功させるには、カードを取り外した後にシステムが再起動していないことを確認します。

すべての view でカレントコンフィグレーションを保存する方法を以下に示します。

操作	コマンド	補足
指定したファイルに現在の設定を保存します、しかし、コンフィグレーションファイルは次回起動時にファイルとしてセットされません。	**save** *file-url*	―
現在の設定をコンフィグレーションファイルに保存し、 次回の起動に使用するスタートアップコンフィグレーションファイルに指定する	**save** [**safely**] [**backup** | **main**] [**force**]	この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設定を保存します。 信頼性のあるファイルの保存を行うため、**safety**パラメータを使用することを推奨します。 **force**パラメータを指定した場合、設定は次回の起動に使用されるコンフィグレーションファイルに保存されます。 **force**パラメータを指定しない場合、次回の起動に使用するスタートアップコンフィグレーションファイルを新規作成します。

⚠ **注意：**

起動中の設定を保存する場合は注意が必要です。この操作により、対象のコンフィグレーションファイルの設定が上書きされます。この操作を実行する場合は、システムによって表示されるメッセージを注意深く読み、操作がサービスに与える影響を十分に理解していることを確認してください。

11.4 次回の起動に使用するスタートアップコンフィグレーションファイルの設定

カレントコンフィグを“.cfg”コンフィグレーションファイルに保存するとき、**save** [**safely**] [**backup** | **main**] [**force**]コマンドを使用できます。“.cfg”コンフィグレーションファイルは、次回の起動で使用するメインとバックアップの両方のスタートアップコンフィグレーションファイルとして指定することができます。

また **startup saved-configuration** *cfgfile* [**backup** | **main**]コマンドを使用して次回の起動で使用するメインあるいはバックアップのスタートアップコンフィグレーションファイルを指定することができます。この作業を実行するために、以下のガイドラインに従ってください。

- メインもしくはバックアップのどちらも指定しない場合、このコマンドは次回の起動で使用するコンフィグレーションファイルをメインとして設定します。
- 次回の起動に使用するメインあるいはバックアップのスタートアップコンフィグレーションファイルを同一に設定することができますが、高可用性のため、スタートアップコンフィグレーションファイルを分けてください。
- 指定されたコンフィグファイルが有効であり、ルートディレクトリに保存されていることを確認してください。
- **undo startup saved-configuration** コマンドは次回の起動に使用するメインあるいはバックアップのスタートアップコンフィグレーションファイルを削除する代わりに NULL に変更します。

以下に、user view で、次回の起動に使用するスタートアップコンフィグレーションファイルを指定する設定を示します。

操作	コマンド	補足
次回の起動に使用するスタートアップコンフィグレーションファイルを指定する	**startup saved-configuration** *cfgfile* [**backup** | **main**]	デフォルト：設定なし **backup**あるいは**main**のいずれのキーワードも指定されない場合、次回の起動に使用するメインのスタートアップコンフィグレーションファイルとして保存されます。 設定を確認するには、すべてのviewで**display startup** コマンドと**display saved-configuration**を使用します。

11.5 次回の起動で使用するスタートアップコンフィグレーションファイルの削除

注意：
この作業を行うと、次回の起動で使用するスタートアップコンフィグレーションファイルを、装置から完全に削除します。削除を行う前に必要に応じてバックアップを行ってください。

次のいずれかの理由である場合、次回の起動時のスタートアップコンフィグレーションファイルを削除する必要があります。

- システムソフトをアップグレードさせた後、既存のコンフィグレーションファイルが、新しいシステムソフトウェアに合わない場合。
- コンフィグレーションファイルが破損している、あるいは不完全である場合。

メインとバックアップの次回の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た場合、次回の起動時にデフォルトコンフィグレーションで起動します。

メインとバックアップの両方の次回の起動で使用するスタートアップ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** コマンドを実行する必要があります。このコマンドを行う前は、ファイルを削除する代わりに、属性を削除します。

たとえば **reset saved-configuration backup** コマンドが行われると、バックアップの次回の起動で使用するスタートアップコンフィグレーションファイルの属性が NULL になり、ファイルが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場合、**reset saved-configuration main** コマンドを行う必要があります。

以下に user view で次回の起動時のスタートアップコンフィグレーションファイルを削除する操作を示します。

操作	コマンド	補足
次回の起動時のスタートアップコンフィグレーションファイルを削除する	**reset saved-configuration** [**backup** | **main**]	**backup**あるいは**main**の両方が指定されない場合、main のスタートアップコンフィグレーションファイルが削除されます。

11.6 コンフィグレーションファイルの表示と維持

すべての view で **display** コマンドを実行します。

操作	コマンド
カレントコンフィグレーションを表示する	**display current-configuration** [**configuration** [*module-name*] | **interface** [*interface-type* [*interface-number*]]]

操作	コマンド
カレント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の差分を表示する	**display current-configuration diff**
デフォルトコンフィグレーションを表示する	**display default-configuration**
2つのコンフィグレーションファイルの設定の差分を表示する	• **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** }
記憶媒体に保存されたコンフィグレーションファイルを表示する	**display saved-configuration**
今回および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表示する	**display startup**
現在のviewで有効な設定を表示する	**display this**
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	**reset saved-configuration** [**backup** | **main**]

目次

このセクションのページは**2-x-x** です。

12章 ソフトウェアアップグレード 12-1
12.1 概要 12-1
12.1.1 ソフトウェアタイプ 12-1
12.1.2 ソフトウェアファイル名の規則 12-1
12.1.3 Comwareイメージの冗長性と読み込み手順 12-2
12.1.4 システム起動プロセス 12-2
12.2 アップグレード方法 12-3
12.3 アップグレードの準備 12-3
12.4 スタートアップソフトウェアイメージの指定とアップグレードの完了 12-4
12.5 ソフトウェア設定の表示と維持 12-4
12.6 CLIによるソフトウェアアップグレード例 12-5

12章 ソフトウェアアップグレード

12.1 概要

ソフトウェアアップグレードは、新しい機能の追加や不具合を修正するために行います。

アップグレードを行う前に、新しいソフトウェアのリリースメモを確認して、装置とソフトウェアの互換性およびアップグレードが与える影響を確認してください。

12.1.1 ソフトウェアタイプ

以下にソフトウェアタイプを示します。

- **BootROM イメージ**－基本セグメントと拡張セグメントが含まれます。基本セグメントはシステムを起動する最小のコードです。拡張セグメントはハードウェア初期化を有効にし、システム管理メニューを提供します。装置が正常に起動しないときに、これらのメニューを使用してソフトウェアとスタートアップコンフィグレーションファイルあるいは管理ファイルを読み込むことができます。
- **Comware イメージ**– 以下に示すサブカテゴリのソフトウェアがあります。
  - **Boot イメージ**– Linux オペレーションのシステムカーネルを含む拡張子が“.bin”のファイルです。 プロセス管理、メモリ管理、ファイルシステム管理のプロセスを持っています。
  - **System ソフトウェアイメージ**– 装置が動作するのに必要最小限の機能を含む、拡張子が“.bin”のファイルです。装置管理、インタフェース管理、設定管理、ルーティング管理の機能を持っています。

読み込まれるソフトウェアイメージはカレントソフトウェアイメージと呼ばれます。次回起動時に指定したファイルで起動するソフトウェアイメージはスタートアップソフトウェアイメージと呼ばれます。

Boot ROM イメージ、Boot イメージ、System ソフトウェアイメージは、装置が起動するために必要です。イメージは拡張子“.ipe”の 1 つのパッケージファイル（Comware イメージ）にまとめられてリリースされます。Comware イメージをスタートアップソフトウェアイメージとして選択するとき、システムは自動的にファイルを解凍し、拡張子“.bin“のブートとシステムイメージをロードします。

12.1.2 ソフトウェアファイル名の規則

本章では、ブートイメージの名前に **boot.bin**、システムイメージの名前に **system.bin** を使用します。

12.1.3 Comware イメージの冗長性と読み込み手順

Comware イメージは、メインとバックアップの 2 セットを指定することができます。

スタートアップソフトウェアイメージの Boot イメージとシステムイメージは同一のバージョンにする必要があります。

システムは常にメインソフトウェアで起動を試みます。もしメインソフトウェアが存在しないあるいは無効である場合、システムはバックアップソフトウェアで起動を試みます。図 12-1に Comware イメージの読み込み手順の全体を示します。

メインソフトウェアとバックアップ Boot イメージが存在しないあるいは無効である場合、コンソールポートに接続し、Boot メニューから Boot イメージを読み込ませるため、電源の OFF/ON を行ってください。

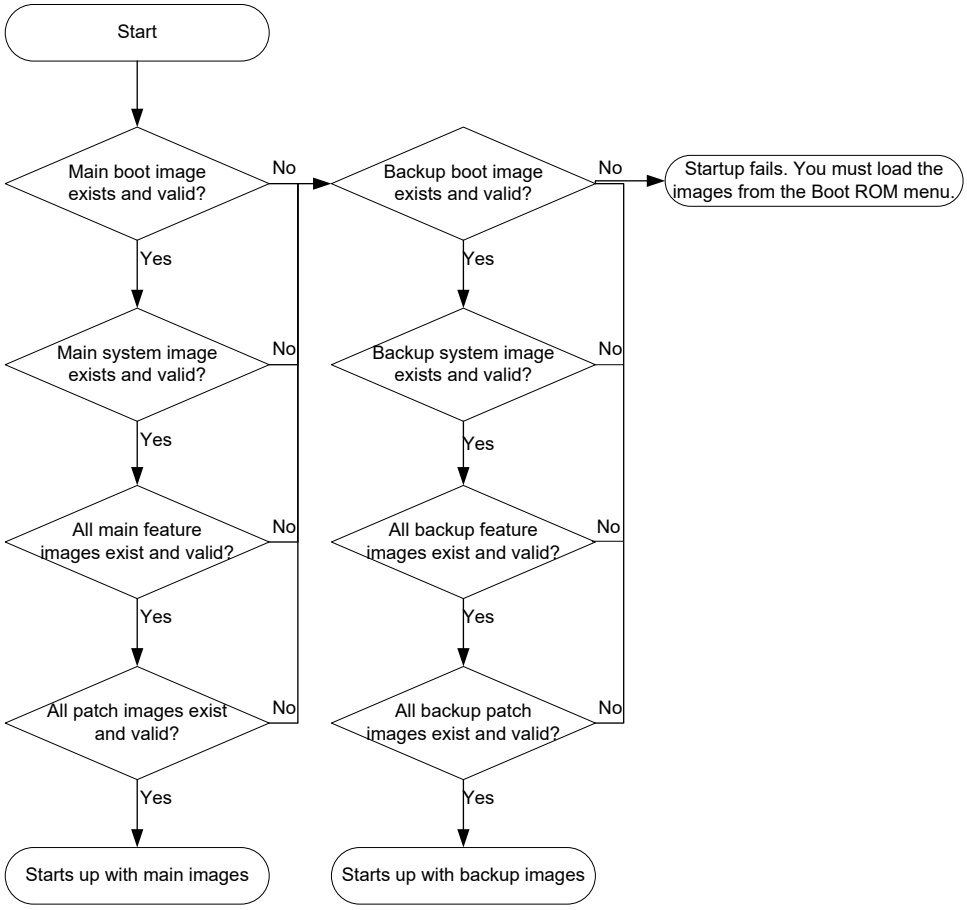


図 12-1 Comware イメージの読み込み手順の全体

12.1.4 システム起動プロセス

装置を起動したのち、ハードウェアを初期化するため Boot ROM イメージが起動します。その後、システム全体を動作させるためスタートアップシステムイメージが起動します。

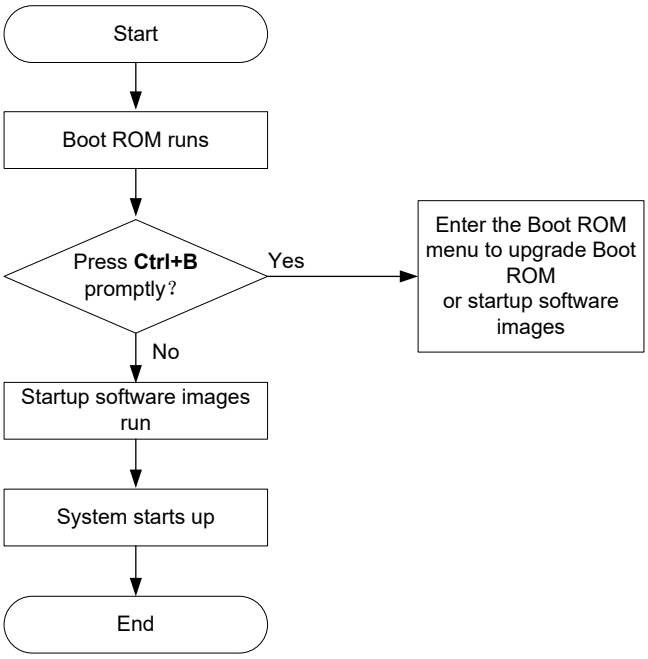


図 12-2 システム起動プロセス

12.2 アップグレード方法

アップグレード方法	ソフトウェアタイプ	補足
CLIからのアップグレード	• Boot ROMイメージ • Comwareイメージ	アップグレードを完了するため、再起動が必要となります。ネットワークサービスの中断が発生します。
Boot メニューからのアップグレード	• Boot ROMイメージ • Comwareイメージ	装置が正常に起動しないときに使用します。 最初にコンソールポートに接続し、装置の電源をONにします。その後Bootメニューにアクセスするため<CTRL+B>を押下します。 Bootメニューからのアップグレードの詳細はQX-W2300ACシリーズアクセスコントローラインスタレーションマニュアルを参照してください。

12.3 アップグレードの準備

1) 現在の Boot ROM バージョンとスタートアップソフトウェアバージョンを確認するため、**display version** コマンドを使用します。

2) アップグレードソフトウェアバージョンがネットワークに与える影響を確認するため、ソフトウェアアップグレードの以下のことを確認します。
   - □ ソフトウェアとハードウェアの互換性
   - □ ソフトウェアのアップグレードのバージョンとサイズ
   - □ 現在の Boot ROM イメージとアップグレードソフトウェアとの互換性
3) ソフトウェアのアップグレードに十分な記憶媒体を持っているかどうか確認するため、**dir** コマンドを使用します。記憶媒体に十分な空き容量がない場合、不要なファイルを **delete** コマンドで削除します。詳細は、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*2 基本機能*”の”*10 章 ファイルシステム管理*”を参照してください。
4) FTP あるいは TFTP を使用して、装置の記憶媒体のルートディレクトリにアップグレードソフトウェアファイルをダウンロードします。FTP、TFTP の設定や操作方法についての詳細は、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*2 基本機能*”の”*8 章 FTP*”および”*9 章 TFTP*”を参照してください。

12.4 スタートアップソフトウェアイメージの指定とアップグレードの完了

user view で以下の操作を実行します。

操作	コマンド	補足
1. メインあるいはバックアップのスタートアップイメージを指定する	• アプローチ1：**boot-loader file** *ipe-filename* { **backup** | **main** } • アプローチ2：**boot-loader file boot** *filename* **system** *filename* [**feature** *filename*&<1-30>] { **backup** | **main** }	🕮**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。
2. カレントコンフィグレーションを保存する	**save**	再起動によって設定が削除されないように行います。
3. 装置の再起動	**reboot**	
4. （オプション設定項目）ソフトウェアの設定を確認する	**display boot-loader**	カレントソフトウェアがスタートアップソフトウェアと同一であるか確認します。

12.5 ソフトウェア設定の表示と維持

すべての view で **display** コマンドを実行します。

操作	コマンド
カレントソフトウェアとスタートアップソフトウェアを表示する	**display boot-loader**
システムバージョン情報を表示する	**display version**

12.6 CLIによるソフトウェアアップグレード例

I. ネットワーク要件

AC にファイル **QX-W2300AC シリーズ-VABC.ipe** を使用してソフトウェアをアップグレードします。

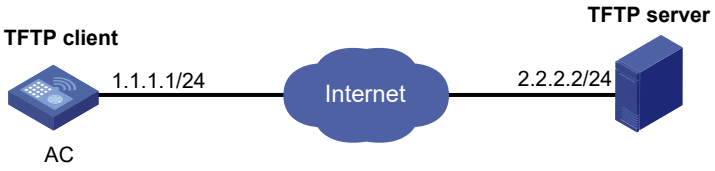


図 12-3 ネットワーク図

II. 設定手順

IP アドレスを設定し、装置と TFTP サーバが通信可能であることを確認します。（詳細は省略します。）

カレントソフトウェアの情報を表示します。

```
<AC> display version
```

TFTP を使用して TFTP サーバから装置の記憶媒体のルートディレクトリにソフトウェアファイル **QX-W2300AC シリーズ-VABC.ipe** をダウンロードします。この例ではフラッシュメモリを使用します。

```
<AC> tftp 2.2.2.2 get QX-W2300AC シリーズ-VABC.ipe
```

メインスタートアップソフトウェアとして **QX-W2300AC シリーズ-VABC.ipe** を指定します。

```
<AC> boot-loader file flash:/QX-W2300AC シリーズ-VABC.ipe main
```

スタートアップソフトウェアの設定を確認します。

```
<AC> display boot-loader
```

装置の再起動を行い、アップグレードを完了させます。

```
<AC> reboot
```

装置が正しいソフトウェアで動作しているか確認します。

```
<AC> display version
```

目次

このセクションのページは**2-x-x** です。

13章 Python 13-1
13.1 Pythonシェルへの移動 13-1
13.2 Pythonスクリプトの実行 13-1
13.3 Python使用例 13-1
13.3.1 ネットワーク要件 13-1

13章 Python

装置が Python シェルに入った後に表示される情報 (Python のバージョンを含む) は、装置モデルによって異なります。

Python とは汎用プログラミング言語の 1 つで、分かりやすい文法が特徴です。

Python インタプリタは以下の機能をサポートします。

- Python 2.7 コマンド。
- Python 2.7 標準 API。
- Comware 9 拡張 API。詳細は、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*2 基本機能*”の”*14 章 Comware 9 拡張 Python API*”を参照してください。
- Python スクリプト。Python スクリプトを作成し使用することができます。

13.1 Pythonシェルへの移動

Python コマンドと API を使用するには、Python シェルに移動する必要があります。

操作	コマンド
user viewからPythonシェルに移動する	**python**

13.2 Pythonスクリプトの実行

user view で Python スクリプトを実行します。

操作	コマンド
Pythonスクリプトを実行する	**python** *filename*

13.3 Python使用例

13.3.1 ネットワーク要件

Python スクリプトを使用して、次のタスクを実行します。

- 設定ファイル（**main.cfg** と **backup.cfg**）を装置にダウンロードします。
- 次回の起動時に、メインおよびバックアップ設定ファイルとして設定します。



図 13-1 ネットワーク図

I. 設定手順

PC 上のテキストエディタを使用して、Python スクリプト“**test.py**”を次のように編集します。

```
#!usr/bin/python
import comware

comware.Transfer('tftp', '192.168.1.26', 'main.cfg', ' flash:/main.cfg')
comware.Transfer('tftp', '192.168.1.26', 'backup.cfg', ' flash:/backup.cfg')
comware.CLI('startup saved-configuration flash:/main.cfg main ;startup
saved-configuration flash:/backup.cfg backup')
```

TFTP を使用して、スクリプトを装置にダウンロードします。

```
<AC> tftp 192.168.1.26 get test.py
```

スクリプトを実行します。

```
<AC> python flash:/test.py
<AC>startup saved-configuration flash:/main.cfg main
Please wait...... Done.
<AC>startup saved-configuration flash:/backup.cfg backup
Please wait...... Done.
```

II. 設定の確認

スタートアップ設定ファイルを表示します。

```
<AC> display startup
 Current startup saved-configuration file: flash:/startup.cfg
 Next main startup saved-configuration file: flash:/main.cfg
 Next backup startup saved-configuration file: flash:/backup.cfg
```

目次

このセクションのページは**2-x-x** です。

14章 Comware 9 拡張 Python API 14-1
14.1 channel 14-1
14.2 CLI 14-2
14.3 get_error 14-3
14.4 get_output 14-3
14.5 get_self_slot 14-4
14.6 get_slot_info 14-5
14.7 get_slot_range 14-5
14.8 get_standby_slot 14-6
14.9 Transfer 14-6

14章 Comware 9 拡張 Python API

Comware 9 拡張 Python API は、Python syntax と互換性があります。

14.1 channel

channel を使用して Comware 9 CLI コマンドを実行し、チャネルオブジェクトを作成します。

Syntax

channel(*command*='')

パラメータ

command: 実行するコマンドを指定します。複数のコマンドを入力するには、スペースとセミコロン (;) を区切り文字として使用します。user view 以外の view でコマンドを実行するには、コマンド実行前にその view へ移行する必要があります。たとえば、 **display interface brief | include UP** コマンドを実行するには、'**system-view ;display interface brief | include UP**' を実行しておく必要があります。

説明

この API は、Comware 9 コマンドのみをサポートします。Linux、Python、Tcl コマンドはサポートしません。

API は自動テストに使用されます。

チャネルによって返されるリストオブジェクトには、0 x 08 などの 16 進数の非表示文字が含まれている場合があります。16 進数の非表示文字を非表示にするには、代わりに CLI を使用するか、**for** ループを使用してチャネルの実行結果を出力します。

```
<Switch> python
>>> import comware
>>> c = comware.channel('display device')
>>> for value in c:
...  print value
...
display device
Slot No. Brd Type           Brd Status  Subslot  Sft Ver             Patch Ver
 1       Device-ABCDE        Master      0        Device-ABCDE-1234   None
<Switch>
```

戻り値

実行されたコマンドからリストオブジェクト形式で出力されます。

例

装置情報を表示します。

```
<Switch> python
>>> import comware
>>> comware.channel('display device')
```

出力例

```
['display device', 'Slot No. Brd Type       Brd Status  Subslot  Sft Ver       Patch
Ver', ' 1       Device-ABCDE       Master      0       Device-ABCDE-1234   None
', '< Switch>']
```

14.2 CLI

CLI を使用して、Comware 9 CLI コマンドの実行と CLI オブジェクトを作成します。

Syntax

CLI(*command*=‘’, *do_print*=True)

パラメータ

command: 実行するコマンドを指定します。複数のコマンドを実行するには、スペースとセミコロン (;) を区切り文字として使用します。user view 以外の view でコマンドを実行するには、コマンド実行前にその view へ移行する必要があります。たとえば、**local-user test class manage** コマンドを実行するには、’**system-view ;local-user test class manage**’を実行しておく必要があります。

do_print: コマンド実行時の出力を行うかどうかを指定します。

- **True**—行結果を表示します。この値がデフォルトです。
- **False**—実行結果を表示しません。

説明

この API は Comware コマンドのみをサポートします。Linux、Python、Tcl コマンドはサポートしません。

戻り値

CLI オブジェクト

例

ローカルユーザ **test** を追加します。

```
<AC> python
Python 2.7.3 (default)
[GCC 6.2.0] on linux2
Type "copyright", "credits" or "license" for more information.
>>> import comware
>>> comware.CLI('system-view ;local-user test class manage')
<AC>startup saved-configuration flash:/backup.cfg backup
Please wait...... Done.
```

出力例

```
<Switch> system-view
System View: return to User View with Ctrl+Z.
[Switch] local-user test class manage
New local user added.
<comware.CLI object at 0xb7f680a0>
```

14.3 get_error

get_error を使用して、ダウンロード時のエラー情報を取得します。

Syntax

Transfer.get_error()

戻り値

エラー情報(エラー情報がない場合は null)

例

ファイル **test.cfg** を TFTP サーバ 1.1.1.1 からダウンロードし、エラー情報を取得します。

```
<Switch> python
Python 2.7.3 (default)
[GCC 6.2.0] on linux2
Type "copyright", "credits" or "license" for more information.
>>> import comware
>>> c = comware.Transfer('tftp', '1.1.1.1', 'test.cfg', 'flash:/test.cfg',
user='', password='')
>>> c.get_error()
```

出力例

```
'Timeout was reached'
```

14.4 get_output

get_output を使用して、コマンド実行時の出力を得ることができます。

Syntax

CLI.get_output()

戻り値

コマンド実行時の出力

例

ローカルユーザを追加し、コマンドの出力を取得します。

<Switch> python

```
Python 2.7.3 (default)
[GCC 6.2.0] on linux2
Type "copyright", "credits" or "license" for more information.
>>> import comware
>>> c = comware.CLI('system-view ;local-user test class manage', False)
>>> c.get_output()
```

<Switch> python

```
Python 2.7.3 (default)
[GCC 6.2.0] on linux2
Type "copyright", "credits" or "license" for more information.
>>> import comware
>>> c = comware.CLI('system-view ;local-user test class manage', False)
>>> c.get_output()
```


出力例

```
['<Switch>system-view', 'System View: return to User View with Ctrl+Z.',
'[Switch]local-user test class manage', 'New local user added.']
```

14.5 get_self_slot

get_self_slot を使用して、マスタ装置のメンバ ID を取得します。

Syntax

get_self_slot()

戻り値

戻り値は常に [-1, -1] です。集中型装置にはアクティブな MPU はありません。

例

マスタ装置のメンバ ID またはアクティブ MPU のスロット番号を取得します。

<Switch> python

```
Python 2.7.3 (default)
[GCC 6.2.0] on linux2
Type "copyright", "credits" or "license" for more information.
>>> import comware
>>> comware.get_self_slot()
```

出力例

```
[-1,-1]
```

14.6 get_slot_info

get_slot_info を使用して、装置情報を取得します。

Syntax

get_slot_info(*global-slot-number*)

パラメータ

global-slot-number: カードのグローバルスロット番号を指定します。

戻り値

{'Slot': *slot-number*, 'Status': '*status*', 'Chassis': *chassis-number*, 'Role': '*role*', 'Cpu': *CPU-number* }形式の辞書オブジェクトです。*slot-number*、*chassis-number*、および *CPU-number* は 0 に固定されています。*status* は、装置のステータスを示します。*role* は、装置の役割を示します。

例

スロット情報を取得します。

```
<Switch> python
Python 2.7.3 (default)
[GCC 6.2.0] on linux2
Type "copyright", "credits" or "license" for more information.
>>> import comware
>>> comware.get_slot_info(1)
```

出力例

```
{'Slot': 1, 'Status': 'Normal', 'Chassis': 0, 'Role': 'Master', 'Cpu': 0}
```

14.7 get_slot_range

get_slot_range を使用して、サポートされているスロット番号の範囲を取得します。

Syntax

get_slot_range()

戻り値

{'MaxSlot': *max-slot-number*, 'MinSlot': *min-slot-number* }形式の辞書オブジェクトです。*max-slot-number* は最大スロット番号を示します。*min-slot-number* は最小スロット番号を示します。

例

サポートされているスロット番号の範囲を取得します。

```
<Switch> python
Python 2.7.3 (default)
[GCC 6.2.0] on linux2
Type "copyright", "credits" or "license" for more information.
>>> import comware
>>> comware.get_slot_range()
```

出力例

```
{'MaxSlot': 1, 'MinSlot': 1}
```

14.8 get_standby_slot

get_standby_slot を使用して、スタンバイ MPU のスロット番号を取得します。

Syntax

get_standby_slot()

戻り値

戻り値は常に[ ]です。集中型装置にはスタンバイ MPU はありません。

例

スタンバイ MPU のスロット番号を取得します。

```
<Switch> python
Python 2.7.3 (default)
[GCC 6.2.0] on linux2
Type "copyright", "credits" or "license" for more information.
>>> import comware
>>> comware.get_standby_slot()
Sample output
```

出力例

```
[ ]
```

14.9 Transfer

Transfer を使用して、サーバからファイルをダウンロードします。

Syntax

Transfer(*protocol*='', *host*='', *source*='', *dest*='',*login_timeout*=10, *user*='', *password*='')

パラメータ

protocol: ファイルのダウンロードに使用するプロトコルを指定します。

- **ftp**—FTP を使用します。

- **tftp**—TFTP を使用します。
- **http**—HTTP を使用します。

host: リモートサーバの IP アドレスを指定します。

source: リモートサーバからダウンロードするファイル名を指定します。

dest: ダウンロードするファイル名を指定します。

login_timeout: 操作のタイムアウトを秒単位で指定します。デフォルトは 10 です。

user: サーバにログインするためのユーザ名を指定します。

password: ログインパスワードを指定します。

戻り値

Transfer オブジェクト

例

TFTP サーバ 192.168.1.26 からファイル **test.cfg** をダウンロードします。

```
<Switch> python
Python 2.7.3 (default)
[GCC 6.2.0] on linux2
Type "copyright", "credits" or "license" for more information.
>>> import comware
>>>  comware.Transfer('tftp',  '192.168.1.26',  'test.cfg',  'flash:/test.cfg',
user='', password='')
```

出力例

```
<comware.Transfer object at 0xb7f700e0>
```

目次

このセクションのページは**2-x-x** です。

15章 Tcl 15-1
15.1 Tclを使用した装置設定 15-1
15.2 Tcl configuration view上でのComwareコマンド実行 15-2

15章 Tcl

Comware 9 は、内蔵のツールコマンド言語（Tcl、Tool command language）インタプリタを提供します。user view から、**tclsh** コマンドを使用して Tcl configuration view へ移動すると、以下のコマンドを使用できます。

- 全 Tcl 8.5 コマンド
- Comware コマンド（CLI コマンド）

Tcl configuration view と user view で設定した機能に違いはありません。user view と同等の方法で、Tcl configuration view 上で Comware コマンドを使用することができます。

たとえば、次のタスクを実行できます。

- **system-view** コマンドを使用して、system view に移動し、機能を設定します。
- **quit** コマンドを使用して、上位レベルの view に戻ります。

15.1 Tclを使用した装置設定

Tcl を使用して装置設定する場合、次のガイドラインおよび制限事項に従ってください。

- Tcl 環境変数を Comware コマンドに適用することができます。
- **Tcl** コマンド用のオンラインヘルプ情報は提供していません。
- **Tcl** コマンドではタブ補完機能は使用できません。
- **Tcl** コマンドが正しく実行されたか確認してください。**Tcl** コマンドの実行中に問題が発生した場合は、Telnet または SSH 経由でログインした場合は、プロセスを無効にすることができます。コンソールまたは AUX ポートからログインした場合は、装置を再起動する必要があります。QX シリーズでは、Telnet または SSH 経由でログインすることを推奨します。

以下に Tcl を使用した装置の設定手順を示します。

操作	コマンド
user viewからTcl configuration viewへ移動する	**tclsh**
Tclコマンドを実行する	Tclコマンドを実行する
Tcl configuration viewからuser viewへ戻る	**tclquit**

メモ：

- **tclquit** コマンドは Tcl configuration view 上では、**quit** コマンドと同等の機能です。
- Tcl configuration view 下位の view で Comware コマンドを使用した場合、上位の view に戻るためには **tclquit** コマンドは使用できません。この場合、**quit** コマンドを使用してください。

15.2 Tcl configuration view上でのComwareコマンド実行

Tcl configuration view 上で Comware コマンドを実行する場合、次の制限、ガイドラインに従ってください。

Comware コマンドでは、“**?**”によるオンラインヘルプとタブ補完機能を使用できます。詳細は QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*2 基本機能*”の”*1 章 CLI*”を参照してください。

- **cli** コマンドは **Tcl** コマンドのため、“**?** “によるオンラインヘルプとタブ補完機能を使用できません。
- 正しく実行された Comware コマンドは、コマンド履歴バッファに保存されます。保存されたコマンドを実行するには、上矢印キーまたは下矢印キーを使用します。
- 1 回の操作で複数の Comware コマンドを実行する手順を以下に示します。
  - 複数の Comware コマンドをセミコロンで区切って入力すると、入力された順序でコマンドが実行されます。例 **vlan 2;description Tech**
  - **cli** コマンドで複数の Comware コマンドを指定する場合、引用符で囲み、スペースとセミコロンで区切ります。例 **cli "vlan 2 ;description Tech"**
  - **cli** コマンドで 1 つの Comware コマンドを指定する場合、スペースとセミコロンで区切ります。例 **cli vlan 2 ;cli description Tech**

以下に Tcl configuration view での Comware コマンド実行の手順を示します。

操作	コマンド	補足
1. Tcl configuration view へ移動する	**tclsh**	–
2. Comware コマンドを直接実行する	Comwareコマンドを実行する	いずれかの方法を使用してください。 Comwareコマンドを直接実行した場合、**Tcl**コマンドとComwareコマンドが競合すると、**Tcl**コマンドが実行されます。 **cli**コマンドを使用してComwareコマンドを実行した場合、**Tcl**コマンドとComwareコマンドが競合すると、Comwareコマンドが実行されます。
3. **cli** コマンドを使用した Comware コマンドを実行する	**cli** *command*	

目次

このセクションのページは **2-x-x** です。

16 章 Auto Config..... 16-1
16.1 概要 16-1
16.2 Auto Config 作業リスト 16-1
16.3 ファイルサーバの設定 16-2
16.4 Auto Config に必要なファイルの準備 16-2
16.4.1 ホスト名ファイル 16-2
16.4.2 コンフィグレーションファイル 16-2
16.4.3 スクリプトファイル 16-3
16.5 DHCP サーバの設定 16-3
16.5.1 コンフィグレーションガイドライン 16-3
16.5.2 HTTP ファイルサーバ使用時の DHCP サーバの設定 16-4
16.5.3 TFTP ファイルサーバ使用時の DHCP サーバの設定 16-5
16.6 DNS サーバの設定 16-5
16.7 ゲートウェイの設定 16-5
16.8 Auto Config で使用するインタフェースの準備 16-6
16.9 Auto Config の開始と完了 16-6

16章 Auto Config

16.1 概要

Auto Config 機能は、スタートアップコンフィグレーションファイルを設定されていない状態で装置が起動するとき、自動でコンフィグレーションファイルを取得し、適用することを可能にします。Auto Config はネットワークの設定を簡略化とネットワーク管理を容易にすることで、メンテナンスの作業負荷を削減することができます。

Auto Config を実装するために、ネットワーク管理者はサーバにコンフィグレーションファイルを保存しておく必要があります。装置は自動でコンフィグレーションファイルを取得し、その設定を適用します。

図 16-1 に示すように、Auto Config は以下のサーバを要求します。

- DHCP サーバ
- ファイルサーバ（TFTP もしくは HTTP サーバ）
- （オプション）DNS サーバ

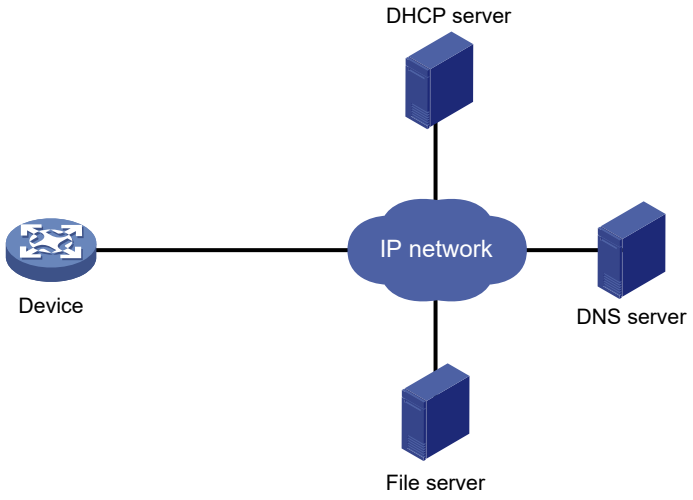


図 16-1 ネットワーク図

16.2 Auto Config作業リスト

作業リスト
（必須設定項目）ファイルサーバの設定
（必須設定項目）Auto Configに必要なファイルの準備
（必須設定項目）DHCPサーバの設定
（オプション設定項目）DNSサーバの設定
（オプション設定項目）ゲートウェイの設定
（必須設定項目）Auto Configで使用するインタフェースの準備
（必須設定項目）Auto Configの開始と完了

16.3 ファイルサーバの設定

装置が TFTP サーバからコンフィグレーション情報を取得できるように、ファイルサーバで TFTP サービスを開始します。

装置が HTTP サーバからコンフィグレーション情報を取得できるように、ファイルサーバで HTTP サービスを開始します。

16.4 Auto Configに必要なファイルの準備

装置は Auto Config のために、スクリプトファイルもしくはコンフィグレーションファイルを使用することができます。

- 装置が Auto Config のためにコンフィグレーションファイルを使用する場合、ファイルサーバにコンフィグレーションファイルを作成し、保存する必要があります。コンフィグレーションファイル名を割り当てるための DHCP サーバを設定していない場合、TFTP サーバでのホスト名ファイルの作成も必要になります。
- 装置が Auto Config のためにスクリプトファイルを使用する場合、ファイルサーバにスクリプトファイルを作成し、保存する必要があります。

16.4.1 ホスト名ファイル

ホスト名ファイルには、ホスト名－IP アドレスマッピングが含まれており、network.cfg と名付ける必要があります。

ホスト名ファイル内のすべてのマッピングエントリは **ip host** *host-name ip-address* フォーマットを使用する必要があります。各マッピングエントリは個別の行に記述する必要があります。例として、以下のように記述してください。

ip host host1 101.101.101.101

ip host host2 101.101.101.102

ip host client1 101.101.101.103

ip host client2 101.101.101.104

16.4.2 コンフィグレーションファイル

コンフィグレーションファイルの設定は以下に示すとおりです。

- 装置が、異なるコンフィグレーションを要求できるように、以下の作業を実行してください。
  - □ 各装置のコンフィグレーションファイルの名前を決定します。

    コンフィグレーションファイル名は“.cfg”拡張子を使用する必要があります。ファイル名識別子を例に挙げると、スペースを含まないコンフィグレーションファイル名を使用してください。

- □ ファイルサーバに装置のコンフィグレーションファイルを保存するために、設定した名前を使用します。
- 装置がすべてあるいは一部のコンフィグレーションを共有するために、ファイルサーバ上の“.cfg”ファイルには共通のコンフィグレーションを保存してください。
- TFTP ファイルサーバを使用する場合、TFTP ファイルサーバ上で device.cfg と名付けたデフォルトコンフィグレーションファイルを保存することができます。このファイルは、装置がほかに使用できるコンフィグレーションファイルを持たないときに使用されます。

Auto Config 処理中、装置は最初に専用のコンフィグレーションファイルの取得を行います。専用のコンフィグレーションファイルが見つからない場合、装置は共通のコンフィグレーションファイルの取得を行います。TFTP ファイルサーバが使用されている状態で共通のコンフィグレーションファイルが見つからない場合、装置はデフォルトコンフィグレーションファイルを使用します。

16.4.3 スクリプトファイル

スクリプトファイルは自動ソフトウェア更新と Auto Config で使用できます。装置は Python スクリプト（.py files）と Tcl スクリプト（.tcl files）をサポートします。Python スクリプトと Tcl スクリプトに関する詳細は、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*2 基本機能*”の “*13 章 Python*”と “*15 Tcl*”を参照してください。

以下にスクリプトファイルの設定を示します。

- 装置がすべてあるいは一部のコンフィグレーションを共有できるように、共通のコンフィグレーションを含むスクリプトファイルを作成します。
- その他の装置のために、個別のスクリプトを作成します。

16.5 DHCPサーバの設定

DHCP サーバは、Auto Config を必要とする装置に以下のアイテムを割り当てます。

- IP アドレス
- コンフィグレーションファイルもしくはスクリプトの経路

16.5.1 コンフィグレーションガイドライン

DHCP サーバを設定するとき、以下のガイドラインに従ってください。

- 異なるコンフィグレーションファイルを準備された各装置は、DHCP サーバ上で以下の作業を実行します。
  - □ DHCP アドレスプールを作成します。
  - □ スタティックアドレスバインディングを設定します。
  - □ コンフィグレーションファイルもしくはスクリプトファイルを指定します。

  アドレスプールは 1 つのコンフィグレーションファイルしか使用できないため、アドレスプールに対してスタティックアドレスバインディングを 1 つだけ指定できます。

- 同じコンフィグレーションファイルを準備された各装置は、以下の手法のいずれか 1 つを使用します。
  - 手法 1
    - 装置に DHCP アドレスプールを作成します。
    - アドレスプール内の各装置にスタティックアドレスバインディングを設定します。
    - 装置にコンフィグレーションファイルを指定します。
  - 手法 2
    - 装置に DHCP アドレスプールを作成します。
    - ダイナミックアロケーションにサブネットを指定します。
    - TFTP サーバを指定します。
    - 装置にコンフィグレーションファイルを指定します。
- サブネット上のすべての装置が同じコンフィグレーションファイルもしくはスクリプトファイルを共有する場合、DHCP サーバ上に以下の作業を実行します。
  - ダイナミックアドレスアロケーションを設定します。
  - 装置にコンフィグレーションファイルもしくはスクリプトファイルを指定します。

コンフィグレーションファイルは、装置に対する共通の設定のみ含むことができます。装置を起動させた後、コンフィグレーションを変更するために、装置管理機器に手法を提供することができます。

16.5.2 HTTP ファイルサーバ使用時の DHCP サーバの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. DHCP を有効にする	**dhcp enable**	デフォルト：無効
3. DHCP アドレスプールを作成し、DHCP address pool view に移行する	**dhcp server ip-pool** *pool-name*	デフォルト：設定なし
4. アドレスプールを設定する	• （手法1）アドレスプールにプライマリサブネットを指定する： **network** *network-address* [*mask-length* | **mask** *mask*] • （手法2）スタティックバインディングを設定する： **static-bind ip-address** *ip-address* [*mask-length* | **mask** *mask*] { **client-identifier** *client-identifier* | **hardware-address** *hardware-address* [**ethernet** | **token-ring**] }	いずれかの手法を使用します。 デフォルト：設定なし 多重スタティックバインディングを追加できます。 1つのIPアドレスは1つのクライアントにのみ設定できます。DHCPクライアントに対するバインディングを変更するためには、バインディングを取り除き、再設定する必要があります。
5. コンフィグレーションファイルもしくはスクリプトファイルの URL を指定する	**bootfile-name** *url*	デフォルト：設定なし

16.5.3 TFTP ファイルサーバ使用時の DHCP サーバの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. DHCP を有効にする	**dhcp enable**	デフォルト：無効
3. DHCP アドレスプールを作成し、DHCP address pool view に移行する	**dhcp server ip-pool** *pool-name*	デフォルト：設定なし
4. アドレスプールを設定する	• （手法1）アドレスプールにプライマリサブネットを指定する：**network** *network-address* [*mask-length* | **mask** *mask*] • （手法2）スタティックバインディングを設定する：**static-bind ip-address** *ip-address* [*mask-length* | **mask** *mask*] { **client-identifier** *client-identifier* | **hardware-address** *hardware-address* [**ethernet** | **token-ring**] }	いずれかの手法を使用します。 デフォルト：設定なし 多重スタティックバインディングを追加できます。 1つのIPアドレスは1つのクライアントにのみ設定できます。DHCPクライアントに対するばバインディングを変更するためには、バインディングを取り除き、再設定する必要があります。
5. TFTP サーバを指定する	• （手法1）TFTPサーバのIPアドレスを指定する：**tftp-server ip-address** *ip-address* • （手法2）TFTPサーバの名前を指定する：**tftp-server domain-name** *domain-name*	いずれかの手法を使用します。 デフォルト：設定なし 自身の名前でTFTPサーバを指定した場合、ネットワーク上でDNSサーバが要求されます。
6. コンフィグレーションファイル名を指定する	**bootfile-name** *bootfile-name*	デフォルト：設定なし

16.6 DNSサーバの設定

DNS サーバは以下の状況で必要になります。

- TFTP サーバがホスト名ファイルを持っていませんが、装置は以下の操作を実行する必要があります
  - ホスト名を取得するために IP アドレスを使用します。
  - TFTP サーバから *host name*.**cfg** フォーマットで名付けられたコンフィグレーションファイルを取得します。
- DHCP サーバが､DHCP 応答メッセージで TFTP サーバドメイン名を割り当てます。装置は TFTP サーバの IP アドレスを取得するためにドメイン名を使用する必要があります。

16.7 ゲートウェイの設定

Auto Config 装置と Auto Config のためのサーバが違うネットワークセグメントに存在する場合、以下の作業を実行する必要があります。

- ゲートウェイを配置し、装置がサーバと通信できることを確認します。
- DHCP リレーエージェント機能を設定します。
- UDP ヘルパー機能を設定します。

装置がブロードキャストパケットでファイルサーバに要求を送信するとき、UDP ヘルパーはブロードキャストパケットをユニキャストパケットに変換してファイルサーバに転送します。

16.8 Auto Configで使用するインタフェースの準備

装置は Auto Config のインタフェースを選択するために以下のステップを使用します。

1) レイヤ 2 の管理イーサネットインタフェースのステータスを識別します。ステータスが up の場合、装置は管理イーサネットインタフェースを使用します。
2) レイヤ 2 イーサネットインタフェースのステータスを識別します。1 つ以上のレイヤ 2 イーサネットインタフェースが up 状態の場合、装置はデフォルト VLAN の VLAN インタフェースを使用します。
3) up 状態のすべてのレイヤ 3 イーサネットインタフェースのインタフェースタイプをアルファベット順にソートし、それからインタフェース番号を昇順にソートします。最初のインタフェースタイプのインタフェースの間で最も小さなインタフェース番号によってインタフェースを使います。
4) up 状態のレイヤ 3 イーサネットインタフェースがない場合、装置は 30 秒間待機し、ステップ 1 に戻り再試行します。

Auto Config をすばやく行うために、各装置の管理イーサネットインタフェースだけをネットワークに接続してください。

16.9 Auto Configの開始と完了

1) Auto Config のために装置を起動します。

   装置がローカルで次回起動時のコンフィグレーションファイルを見つけない場合、コンフィグレーションファイルを取得するために Auto Config プロセスを開始します。1 度失敗した場合、装置は 30 秒待機し、その後自動的に再びプロセスを開始します。プロセスを止めるためには、<Ctrl+C>または<Ctrl+D>を押下してください。

   コンフィグレーションファイルを取得した後、装置は自動的にコンフィグレーションファイルを実行します。

2) カレントコンフィグレーションを保存するために **save** コマンドを使用します。

   装置はローカルで入手したコンフィグレーションファイルを保存しません。カレントコンフィグレーションを保存しない場合、装置は再起動後に再び Auto Config 機能を使用する必要があります。

save コマンドに関する詳細は、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*2 基本機能*”の”*11 章 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。

QX-W2300AC シリーズ アクセスコントローラ

オペレーションマニュアル

3. 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- 装置ハードニング

03- ハードウェアリソース管理

04- NTP

05- Information Center

目次

このセクションのページは**3-x-x** です。

1章 装置管理 1-1
1.1 装置管理作業リスト 1-1
1.2 装置名の設定 1-1
1.3 システムクロックの設定 1-1
1.3.1 システムクロックソースの設定 1-1
1.4 著作権情報表示の有効化 1-3
1.5 バナーの設定 1-3
1.5.1 バナーの種類 1-3
1.5.2 バナー入力モード 1-4
1.5.3 設定手順 1-5
1.6 装置の特定 1-5
1.6.1 LED の点滅開始 1-6
1.7 スケジュール自動実行の設定 1-6
1.7.1 設定の制限事項およびガイドライン 1-6
1.7.2 設定手順 1-7
1.7.3 スケジュール自動実行設定例 1-8
1.8 装置の再起動 1-11
1.8.1 CLIによる装置の即時再起動 1-12
1.8.2 装置のスケジュール再起動 1-12
1.9 診断およびトラブルシューティングのための動作中の統計情報の収集 1-12
1.10 装置管理の表示と維持 1-13

1章 装置管理

この章では装置の基本的なパラメータの設定、装置の管理について記載します。

この章の設定操作は、順番に関係なく実行できます。

1.1 装置管理作業リスト

作業リスト
（必須設定項目） 装置名の設定
（必須設定項目） システムクロックの設定
（オプション設定項目） 著作権情報表示の有効化
（オプション設定項目） バナーの設定
（オプション設定項目） スケジュール自動実行の設定
（オプション設定項目） 装置の再起動

1.2 装置名の設定

装置名あるいは、“ホスト名”はネットワークで装置を特定するのに使用されます。システムとしては、装置名は CLI のプロンプトに対応します。装置名が **NEC** の場合、プロンプトは<NEC>です。

以下に装置名を設定する方法を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． 装置名を設定する	**sysname** *sysname*	デフォルト：装置名

1.3 システムクロックの設定

1.3.1 システムクロックソースの設定

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。

システムクロックは、UTC 時間、タイムゾーン、サマータイムによって決まります。**display clock** コマンドを使用することで、システムクロックを表示できます。

装置は、ローカルに設定されたシステム時間を使用するか、NTP クロックソースから UTC 時間を取得し、システムクロックを計算することができます。

- **None**－ローカルシステムクロックです。CLI を用いて手動でシステムクロックを設定します。装置はシステム時間を維持するため、装置内部の水晶発振器によって生成

されたクロック周波数を使用します。装置の再起動を行うとローカルシステム時間はデフォルトに戻るため、再度コマンドを設定してください。

- **NTP**－NTP クロックソースです。装置が NTP のシステムクロックを使用したとき、手動でシステムクロックを変更できません。NTP についての詳細は、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“3 *システム管理*”の”*4 章 NTP*”を参照してください。

以下にローカルでシステムクロックソースを設定する方法を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． システムクロックのソースを指定する	**clock protocol none**	デフォルト：**ntp** コマンドを複数回実行した場合、最後に指定した設定が適用されます。
3． user view に戻る	**quit**	―
4． UTC 時間を設定する	**clock datetime** *time date*	⚠**注意**： このコマンドはシステム時刻を変更し、システム時刻に関連する機能(たとえば、スケジュールされたタスク)の実行や、装置と他の装置(たとえば、ログレポートと統計情報収集)との連携動作に影響を与えます。このコマンドを実行する前に、ご使用の環境への影響を確認してください。
5． system view に移行する	**system-view**	―
6． タイムゾーンを設定する	**clock timezone** *zone-name* { **add** | **minus** } *zone-offset*	デフォルト：UTC サマータイムを設定したのち、装置はシステム時間を再計算します。システムクロックを確認する場合**display clock**コマンドを使用します。ネットワークのすべての装置で同一のサマータイムを使用していることを確認してください。
7． （オプション設定項目）サマータイムを設定する	**clock summer-time** *name start-time start-date end-time end-date add-time*	デフォルト：無効 サマータイムを設定したのち、装置はシステム時間を再計算します。システムクロックを確認する場合**display clock**コマンドを使用します。ネットワークのすべての装置で同一のサマータイムを使用していることを確認してください。

以下に NTP でシステムクロックソースを設定する方法を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―

操作	コマンド	補足
2． システムクロックのソースを指定する	**clock protocol ntp**	デフォルト：**ntp** コマンドを複数回実行した場合、最後に指定した設定が適用されます。
3． タイムゾーンを設定する	**clock timezone** *zone-name* { **add** | **minus** } *zone-offset*	デフォルト：UTC サマータイムを設定したのち、装置はシステム時間を再計算します。システムクロックを確認する場合**display clock**コマンドを使用します。ネットワークのすべての装置で同一のサマータイムを使用していることを確認してください。
4． （オプション設定項目）サマータイムを設定する	**clock summer-time** *name start-time start-date end-time end-date add-time*	デフォルト：無効 サマータイムを設定したのち、装置はシステム時間を再計算します。システムクロックを確認する場合**display clock**コマンドを使用します。ネットワークのすべての装置で同一のサマータイムを使用していることを確認してください。

1.4 著作権情報表示の有効化

著作権情報の表示を有効にすると、以下の場合、著作権情報が表示されます。

- Telnet、SSH でログインします。
- コンソールポートから装置にログインした後に user view を終了します。この場合、装置は自動でコンソールセッションを再起動しようとします。

以下に著作権情報表示の有効化の手順を以下に示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． 著作権情報表示を有効にする	**copyright-info enable**	デフォルト：無効

1.5 バナーの設定

バナーはユーザが装置にログインしたときにシステムが表示するプロンプト情報です。

1.5.1 バナーの種類

装置は以下のバナーをサポートしています。

- **Legal** バナー – 認証情報とも呼ばれます。システムは著作権または権限情報を表示し、ユーザがログインする前にバナーを表示して、ユーザがログインするかどうか確認します。”Y”、または Enter キーを入力すると、ユーザはログインプロセスに入ります。”N”を入力すると、ユーザはログインプロセスを終了します。”Y”、”N”は、大文字でも小文字でもかまいません。
- **Message of the Day（MOTD）**バナー – 認証前に表示される welcome information です。legal バナーの後、login バナーの前に表示されます。
- **Login** バナー – ログイン認証時の welcome information です。パスワードと Scheme 認証が設定されている場合に表示されます。
- **incoming** バナー – Modem ダイヤルインユーザが user view に移行する際に表示されます。認証が必要な場合、認証にパスしたのちバナーが表示されます。
- **Shell** バナー – Modem 以外のユーザが user view に移行する際に表示されます。

1.5.2 バナー入力モード

バナーを設定する場合、1 行入力モードあるいは複数入力モードを使用します。

- 1 行入力モード

コマンドと同様に同一の行に入力します。入力テキストの開始および終了文字は同じにならなければなりませんが、バナー情報には含まれません。このとき、コマンドキーワードを含む入力テキストは 511 文字を超えないようにする必要があります。たとえば、ユーザが shell バナーの user view に移行した際に“Have a nice day.“と表示するように設定します。

```
<AC> system-view
[AC] header shell %Have a nice day.%
```

- 複数入力モード

バナーや区切り文字を 2002 文字まで入力可能です。バナーには改行を含むことができます。改行は 2 文字分としてカウントされます。

複数行を設定する場合以下のどちらかの方法を使用します。

□ **方法 1**– コマンドキーワードの後ろで直接 **Enter** を押し、設定の最後を"%"にします。Enter および"%"はバナー情報には含まれません。たとえば、ユーザが user view に移行した際に“Have a nice day. Please input the password.“と表示するように設定します。

```
<AC> system-view
[AC] header shell
Please input banner content, and quit with the character '%'.
Have a nice day.%
```

□ **方法 2**– 最初の行のコマンドキーワードの後ろに 1 文字入力し、**Enter** を押します。最初の行に入力した文字で設定を終了します。最初の行の文字および最後の文字はバナー情報には含まれません。たとえば、ユーザが user view に移行した際に“Have a nice day. Please input the password.“と表示するように設定します。

```
<AC> system-view
[AC] header shell A
Please input banner content, and quit with the character 'A'.
Have a nice day.A
```

□ **方法 3** – 最初の行のキーワードの後ろに複数の文字（最初と最後の文字は同じにしない）を入力し、**Enter** を押します。最初の行の最初の文字で設定を終了し

ます。最初の行の最初の文字および最後の文字はバナー情報には含まれません。たとえば、ユーザが user view に移行した際に“Have a nice day. Please input the password. “と表示するように設定します。

```
<AC> system-view
[AC] header shell AHave a nice day.
Please input banner content, and quit with the character 'A'.
A
```

1.5.3 設定手順

以下の手順に従ってバナーの設定を行います。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． バナーを設定する	• ログイン前の権限情報を設定する **header legal** *text* • ログイン前に表示されるバナーを設定する **header motd** *text* • ログイン認証時に表示されるバナーを設定する **header login** *text* • Modemダイヤルインユーザがuser viewに入るときに表示するバナーを設定する **header incoming** *text* • Modem以外のユーザがuser viewに入るときに表示するバナーを設定する **header shell** *text*	デフォルト：設定無し

1.6 装置の特定

🕮 **メモ：**

locator blink コマンドはソフトウェアバージョン 9.4.09 を含む以降のソフトウェアからサポートしています。

装置の特定について 本装置は **locator blink** コマンドを使用することで、指定した装置の LED を一定時間緑→赤の順に点滅させます。本機能は装置の位置を特定する際に役立ちます。

1.6.1 LED の点滅開始

🕮 **メモ：**

- **ap** *ap-name* パラメータを省略して実行した場合、コマンドを実行した装置の SYS LED が点滅します。
- **ap** *ap-name* パラメータを指定して実行した場合、指定した AP の電源 LED が点滅します。

user view で以下のコマンドを実行します。

操作	コマンド	補足
LED の点滅を開始する	**locator blink** *blink-time* [**ap** *ap-name*]	🕮 メモ： **ap** *ap-name* パラメータは、ソフトウェアバージョン9.6.05c を含む以降のソフトウェアからサポートしています。

1.7 スケジュール自動実行の設定

スケジュール自動実行機能は、管理者を妨げることなく、指定された時間に、指定されたコマンドまたはコマンド集合を自動的に実行します。

スケジュールされるコマンドは 1 回のみ、あるいは定期的に実行されます。1 回のみのスケジュールは設定ファイルに保存されません。装置が再起動したときに失われます。定期的なスケジュールは設定ファイルに保存され、指定時間に定期的に実行されます。

1.7.1 設定の制限事項およびガイドライン

スケジュール自動実行では、以下の制限事項およびガイドラインに従ってください。

- デフォルトのシステムクロックは、再起動時に常に復元されます。スケジュールを期待どおりに実行できるようにするには、システム時刻を再設定するか、装置を再起動した後に NTP を設定します。NTP の詳細については QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“3 *システム管理*”の”*4 章 NTP*”を参照してください。
- 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。
- スケジュール自動実行を行う場合、実行する view と command 引数をチェックしません。command 引数を正確に設定してください。自動実行の設定時には引数はチェックされません。
- **telnet** コマンド、**ftp** コマンド、**ssh2** コマンドおよび **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。
- 指定した自動実行時間になった後、バックグラウンドに指定されたコマンドを実行します。ログ、トラップ、デバッグなどの情報では表示されません。

1.7.2 設定手順

以下に 1 回のみのスケジュール自動実行を行う設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． job を作成する	**scheduler job** *job-name*	デフォルト：設定なし
3． job にコマンドを割り当てる	**command** *id command*	デフォルト：設定なし 複数のコマンドをjobに割り当てることができ、最も小さいIDから実行されます。
4． system view に戻る	**quit**	ー
5． スケジュールを作成する	**scheduler schedule** *schedule-name*	デフォルト：設定なし
6． スケジュールに job を割り当てる	**job** *job-name*	デフォルト：設定なし 複数のjobをスケジュールに割り当てることができ、同時に実行できます。
7． 1 回のみのスケジュールに実行時間テーブルを指定する	● 実行日と時間を指定する： **time at** *time date* ● 実行月日と時間を指定する： **time once at** *time* [**month-date** *month-day* | **week-day** *week-day*&<1-7>] ● 指定された遅延時間後にコマンドを自動実行する： **time once delay** *time*	デフォルト：設定なし いずれか1つのコマンドで設定します。 実行時間が指定された後、**clock datetime**コマンド、**clock summer-time**コマンド、**clock timezone**コマンドは既に設定された実行時間テーブルを変更しません。
8． (オプション設定項目) スケジュールログファイルのサイズ制限を設定する	**scheduler logfile size** *value*	デフォルト：16 KB スケジュールログファイルには、ジョブ内のコマンドの実行結果のログメッセージが格納されます。制限に達すると、新しいログメッセージを格納するために最も古いログメッセージが削除されます。ログファイルの残りの領域が1つのログメッセージに対して十分でない場合、システムはメッセージを切り捨て、余分な部分を格納しません。

以下に定期的なスケジュール自動実行を行う設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． job を作成する	**scheduler job** *job-name*	デフォルト：設定なし

操作	コマンド	補足
3． jobにコマンドを割り当てる	**command** *id command*	デフォルト：設定なし 複数のコマンドをjobに割り当てることができ、最も小さいIDから実行されます。
4． system viewに戻る	**quit**	ー
5． スケジュールを作成する	**scheduler schedule** *schedule-name*	デフォルト：設定なし
6． スケジュールにjobを割り当てる	**job** *job-name*	デフォルト：設定なし 複数のjobをスケジュールに割り当てることができ、同時に実行できます。
7． 定期的なスケジュールを指定する	● 指定された時間で定期的にスケジュールを実行する： **time repeating at** *time* [**month-date** [*month-day* | **last**] | **week-day** week-day&<1-7>] ● 指定された月日で定期的にスケジュールを実行する： **time repeating** [**at** *time* [*date*]] **interval** *interval-time*	デフォルト：設定なし いずれか1つのコマンドで設定します。 実行時間が指定された後、**clock datetime**コマンド、**clock summer-time**コマンド、**clock timezone**コマンドは既に設定された実行時間テーブルを変更しません。
8． (オプション設定項目)スケジュールログファイルのサイズ制限を設定する	**scheduler logfile size** *value*	デフォルト：16 KB スケジュールログファイルには、ジョブ内のコマンドの実行結果のログメッセージが格納されます。制限に達すると、新しいログメッセージを格納するために最も古いログメッセージが削除されます。ログファイルの残りの領域が1つのログメッセージに対して十分でない場合、システムはメッセージを切り捨て、余分な部分を格納しません。

1.7.3 スケジュール自動実行設定例

I. ネットワーク要件

図 1-1に示すように、AP 越しに PC から AC にアクセスします。AC は AP および PC に IP アドレスを付与する DHCP サーバとして動作します。AP は ap1 越しに AC と接続されます。

エネルギーを節約するため、以下のスケジュールを自動で実行します。

- 毎日 8:00 に ap1 を有効にします。
- 毎日 20:00 に ap1 を無効にします。

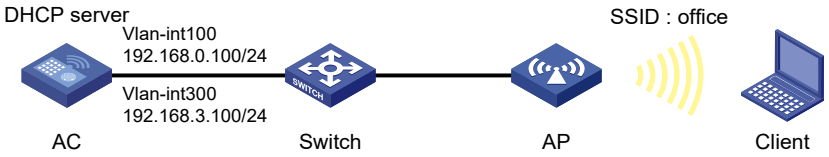


図 1-1 ネットワーク図

II. 設定手順

本章ではスケジュールの設定手順のみを示します。無線アクセスの設定については、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*6 WLAN アクセス*”の”*1 章 WLAN アクセス*”を参照してください。

system view に移行します。

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

ap1 を無効化する job を設定します。

```
[AC] scheduler job radio_disable
[AC-job-radio_disable] command 1 system-view
[AC-job-radio_disable] command 2 wlan ap ap1 model QX-W1110
[AC-job-radio_disable] command 3 radio 1
[AC-job-radio_disable] command 4 radio disable
[AC-job-radio_disable] quit
```

毎日 20:00 に無線を無効化する定期スケジュールを設定します。

```
[AC] scheduler schedule stop_radio
[AC-schedule-stop_radio] job radio_disable
[AC-schedule-stop_radio] time repeating at 20:00
[AC-schedule-stop_radio] quit
```

ap1 を有効化する job を設定します。

```
[AC] scheduler job radio_enable
[AC-job-radio_enable] command 1 system-view
[AC-job-radio_enable] command 2 wlan ap ap1 model QX-W1110
[AC-job-radio_enable] command 3 radio 1
[AC-job-radio_enable] command 4 radio enable
[AC-job-radio_enable] quit
```

毎日 8:00 に無線を有効化する定期スケジュールを設定します。

```
[AC] scheduler schedule start_radio
[AC-schedule-start_radio] job radio_enable
```

```
[AC-schedule-start_radio] time repeating at 8:00
[AC-schedule-start_radio] quit
```

III. 設定の確認

AP に関する情報を表示します。Admin State フィールドの値が up になっており、8:00～20:00 に up、それ以外の時間帯は down になっていることを確認します。

```
[AC] display wlan ap name ap1 verbose
AP name                          : ap1
AP ID                            : 1
AP group name                    : default-group
State                            : Run
Backup Type                      : NULL
Online time                      : 0 days 2 hours 18 minutes 10 seconds
System up time                   : 0 days 2 hours 19 minutes 11 seconds
Model                            : QX-W1110
Region code                      : JP
Region code lock                 : Disable
Serial ID                        : 210235A1BSC123000050
MAC address                      : 586a-b1fb-e2c0
IP address                       : 100.1.0.1
H/W version                      : Ver.C
S/W version                      : V700R001B64D003
Boot version                     : 7.01
Description                      : Not configured
Priority                         : 4
Echo interval                    : 10 seconds
Statistics report interval       : 50 seconds
Jumbo frame value                : 1500
MAC type                         : Local MAC & Split MAC
Tunnel mode                      : Local Bridging & 802.3 Frame & Native Frame
Discovery type                   : Unknown
Retransmission count             : 3
Retransmission interval          : 5 seconds
Firmware upgrade                 : Enabled
Sent control packets             : 3159
Received control packets         : 3159
Connection count                 : 1
Backup Ipv4                      : Not configured
Backup Ipv6                      : Not configured
Tunnel encryption                : Disabled
LED mode                         : Normal
Radio 1:
    Basic BSSID                  : 586a-b1fb-e2c0
    Admin state                  : Up
    Radio type                   : 802.11ac
    Antenna type                 : internal
    Client dot11ac-only          : Disabled
    Client dot11n-only           : Disabled
    Channel band-width           : 20/40/80MHz
    Secondary channel offset     : SCA
    Short GI for 20MHz           : Supported
    Short GI for 40MHz           : Supported
    Short GI for 80MHz           : Supported
    Short GI for 160MHz          : Not supported
    A-MSDU                       : Enabled
    A-MPDU                       : Enabled
    LDPC                         : Not Supported
    STBC                         : Supported
    Operational VHT-MCS Set:
        Mandatory                : Not configured
        Supported                : NSS1 0,1,2,3,4,5,6,7,8,9
                                   NSS2 0,1,2,3,4,5,6,7,8,9
```

```
        Multicast              : Not configured
    Operational HT MCS Set:
        Mandatory              : Not configured
        Supported              : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9,
                                 10, 11, 12, 13, 14, 15
        Multicast              : Not configured
    Channel                    : 149
    Max power                  : 20 dBm
    Operational rate:
        Mandatory              : 6, 12, 24 Mbps
        Multicast              : Auto
        Supported              : 9, 18, 36, 48, 54 Mbps
        Disabled               : Not configured
    Distance                   : 1 km
    ANI                        : Enabled
    Fragmentation threshold    : 2346 bytes
    Beacon interval            : 100 TU
    Protection threshold       : 2346 bytes
    Long retry threshold       : 4
    Short retry threshold      : 7
    Maximum rx duration        : 2000 ms
    Noise floor                : -102 dBm
```

1.8 装置の再起動

⚠ **注意**：

- ネットワークサービスに割り込んで再起動する可能性があります。
- 設定が消失するのを避けるため、装置を再起動する前に **save** コマンドでカレントコンフィグレーションを保存してください。**save** コマンドの詳細は、QX-W2300AC シリーズアクセスコントローラコマンドマニュアルの“*2 基本機能*”の”*7 章 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。
- システム起動時に使用されるコンフィグレーションファイルとスタートアップファイルを確認するには、**display startup** コマンドと **display boot-loader** コマンドを使用してください。スタートアップコンフィグレーションファイルあるいはソフトウェアイメージが異常である場合、装置は正常に起動しません。**display startup** コマンドと **display boot-loader** コマンドの詳細は QX-W2300AC シリーズアクセスコントローラコマンドマニュアルの“*2 基本機能*”の”*7 章 コンフィグレーションファイル管理*”および”*8 章ソフトウェアアップグレード*”を参照してください。

以下の方法で装置を再起動できます。

- CLI によるスケジュールリブートを行います。指定した時間に自動的に再起動させることができます。
- CLI による再起動を即時行うことができます。再起動中、装置は以下の処理を行います。
  - □ 装置内部のすべてのチップをリセットします。
  - □ スタートアップソフトウェアを確認するため、Boot ROM を使用します。圧縮されているイメージを解凍し、イメージを読み込みます。
- システムを初期設定します。
- 電源 ON/OFF による再起動を行います。この手順はデータの損失の可能性があり、推奨されません。

遠隔ホストから CLI により装置を再起動することができます。

データ保護のため、装置がファイルの操作を実行している間、装置の再起動を行わないでください。

1.8.1 CLI による装置の即時再起動

user view で以下のコマンドを実行します。

操作	コマンド
1． 装置を再起動する	**reboot** [**force**]

⚠ **注意**：

- 装置の再起動により、サービスが中断されることがあります。このコマンドを使用する前にご使用の環境への影響を確認してください。
- システムに障害が発生した場合、または正常に起動できなかった場合にのみ装置を再起動するには、**force** を使用します。強制的に装置を再起動すると、ファイルシステムが損傷する可能性があります。**force** を使用して装置を再起動する前にその影響を理解しておく必要があります。

1.8.2 装置のスケジュール再起動

装置はスケジュール再起動を 1 つのコマンドのみサポートします。もし **scheduler reboot at** コマンドあるいは **scheduler reboot delay** コマンドを複数回あるいは、両方のコマンドを設定した場合、最後に設定したコマンドが適用されます。

スケジュール再起動により装置を再起動する場合、user view で以下のコマンドを実行します。

操作	コマンド	補足
再起動時間と日付を指定し、スケジュール再起動機能を有効にする	**scheduler reboot at** *time* [*date*]	デフォルト：設定なし
再起動遅延時間を指定し、スケジュール再起動機能を有効にする	**scheduler reboot delay** *time*	デフォルト：設定なし

1.9 診断およびトラブルシューティングのための動作中の統計情報の収集

以下のいずれかの方法で、診断およびトラブルシューティングのために動作中の統計情報を収集できます。

- 個別の **display** コマンドで、機能別またはモジュール別に動作情報を収集します。
- 複数またはすべての機能およびハードウェアモジュールの動作情報を収集するには、**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、この機能は情報をファイルに保存する前に情報を自動的に圧縮します。ファイルの内容を表示するには、以下の手順を実行します。

1) **tar extract** コマンドを使用してファイルを抽出します。
2) **gunzip** コマンドを使用して、抽出されたファイルを解凍します。
3) **more** コマンドを使用して、解凍されたファイルの内容を表示します。

装置がこのコマンドを実行している間は、他のコマンドを実行しないでください。他のコマンドを実行すると、収集された動作情報に影響を与える可能性があります。

以下はすべての view で実行できます。

操作	コマンド
複数のモジュールの動作の統計情報を表示する	**display diagnostic-information** [**hardware** | **infrastructure** | **l2** | **l3** | **service**]

1.10 装置管理の表示と維持

すべての view で **display** コマンドを実行し、user view で **reset** コマンドを実行できます。

操作	コマンド
システムクロック、日時、タイムゾーン、サマータイムを表示する	**display clock**
複数のモジュールの動作の統計情報を表示する	**display diagnostic-information** [**hardware** | **infrastructure** | **l2** | **l3** | **service**]
スケジュール自動実行機能の設定状態を表示する	**display scheduler job** [*job-name*]
スケジュール自動実行機能のログ情報を表示する	**display scheduler logfile**
スケジュールリブート機能の設定状態を確認する	**display scheduler reboot**
スケジュール自動実行機能の情報を表示する	**display scheduler schedule** [*schedule-name*]
スケジュール自動実行機能のログ情報を削除する	**reset scheduler logfile**

目次

このセクションのページは**3-x-x** です。

2章 装置ハードニング 2-1
2.1 概要 2-1
2.2 パスワードリカバリ機能の無効化 2-1

2章 装置ハードニング

2.1 概要

すべての装置ハードニングはオプションです。

2.2 パスワードリカバリ機能の無効化

パスワードリカバリ機能は Boot ROM メニューから装置設定と 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の場合、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の場合、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、工場出荷コンフィグレーションに戻す必要があります。工場出荷コンフィグレーションに戻すことで、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。

次回起動時に使用するコンフィグレーションファイルにアクセスする不正なユーザからのアクセスを防ぐため、パスワードリカバリ機能を無効にできます。

以下にパスワードリカバリ機能を無効にする設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． パスワードリカバリ機能を無効にする	**undo password-recovery enable**	デフォルト：有効

目次

このセクションのページは**3-x-x** です。

3章 ハードウェアリソース管理..... 3-1
3.1 設定作業リスト..... 3-1
3.2 CPU使用率のモニタリング..... 3-1
3.2.1 CPU使用率アラームの設定..... 3-1
3.2.2 CPU使用率トラッキングの設定..... 3-2
3.3 メモリ使用率のモニタリング..... 3-3
3.3.1 メモリアラームしきい値の設定..... 3-3
3.4 検出間隔の設定..... 3-5
3.5 トランシーバのパラメータ表示..... 3-5
3.5.1 トランシーバの情報表示..... 3-5
3.5.2 トランシーバの診断..... 3-5
3.6 ハードウェアリソース管理の表示と維持..... 3-6

3章　ハードウェアリソース管理

この章では、CPU とメモリの使用状況のモニタリング、ファンの動作ステータスの表示、基本的な装置動作パラメータの設定など、日常的な装置ハードウェアリソース管理について説明します。

3.1　設定作業リスト

作業リスト
（オプション設定項目） CPU使用率のモニタリング
（オプション設定項目）メモリ使用率のモニタリング
（オプション設定項目） 検出間隔の設定
（オプション設定項目）トランシーバのパラメータ表示

3.2　CPU使用率のモニタリング

3.2.1　CPU 使用率アラームの設定

装置は 1 分間隔で CPU 使用率をサンプリングし、CPU 使用率のしきい値と比較して CPU 使用率のステータスを特定し、それに応じてアラームまたは通知を送信します。

装置は以下の CPU 使用率のしきい値をサポートしています。

- **Minor threshold**—CPU 使用率が Minor しきい値以上に増加しても、Severe しきい値未満の場合、CPU 使用率は Minor alarm 状態になります。CPU 使用率が Severe しきい値を超えるか、Minor alarm が削除されるまで、装置は定期的に Minor alarm を送信します。
- **Severe threshold**—CPU 使用率が Severe しきい値を超えると、CPU 使用率は Severe alarm 状態になります。装置は Severe alarm が削除されるまで定期的に Severe alarm を送信します。

CPU 使用率のアラームと通知を NETCONF、SNMP、および Information Center に送信して、NETCONF イベント、SNMP トラップと情報、およびログメッセージとしてカプセル化できます。NETCONF と SNMP の詳細は、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*17 ネットワーク管理と監視*”を参照してください。Information Center の詳細は、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“3 *システム管理*”の”*5 章 Information Center*”を参照してください。

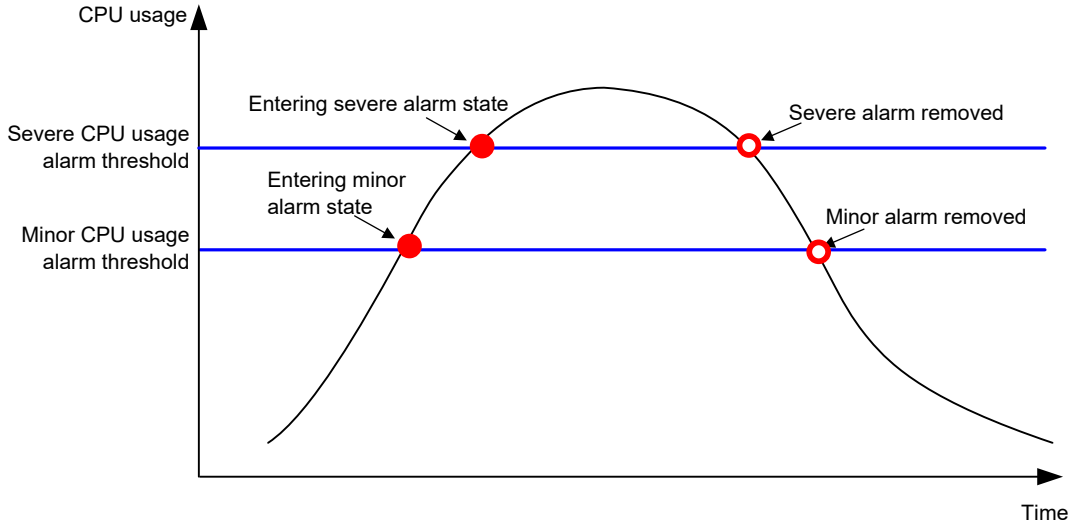


図 3-1 CPU アラームとアラーム削除通知

以下に CPU 使用率アラームの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. CPU 使用率のしきい値を設定する	**monitor cpu-usage threshold** *severe-threshold* [**minor-threshold** *minor-threshold*]	デフォルト：99%

3.2.2 CPU 使用率トラッキングの設定

CPU 使用率のトラッキングを有効にすると、システムは CPU 使用率を一定間隔でサンプリングし、そのサンプルをバッファに保存します。最近の CPU 使用率を表示するには、**display cpu-usage history** コマンドを使用します。

以下に CPU 使用率トラッキングの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. CPU 使用率トラッキングのサンプリング間隔を設定する	**monitor cpu-usage interval** *interval*	デフォルト：1分
3. CPU 使用率トラッキングを有効にする	**monitor cpu-usage enable**	デフォルト：有効

3.3 メモリ使用率のモニタリング

3.3.1 メモリアラームしきい値の設定

正しい動作を保証し、メモリ効率を向上させるために、システムはリアルタイムで空きメモリ領域の量を監視します。空きメモリ領域の量が Minor、Severe、または Critical のアラームしきい値に達すると、システムは影響を受けるサービスモジュールとプロセスにアラームを発行します。

システムは、メモリ不足状態が近づいていることを警告する早期警告を発行することもできます。

(ローメモリをサポートしていない装置の場合) **display memory** コマンドを使用して、メモリ使用状況情報を表示できます。

(ローメモリをサポートする装置の場合)システムは、空き低メモリ領域の量のみをモニタリングします。**display memory** コマンドを使用して、メモリ使用状況情報を表示できます。

(ローメモリをサポートするスロットを持つ装置の場合)ローメモリをサポートするスロットの場合、システムはローメモリ空き領域の量だけをモニタリングします。**display memory** コマンドを使用して、メモリ使用状況情報を表示できます。スロットの **LowMem** フィールドが表示されている場合、そのスロットは低メモリをサポートします。

表 3-1と図 3-2に示すように装置は以下のレベルのしきい値をサポートしています。

- Sufficient-memory しきい値
- Early-warning しきい値
- 通常状態しきい値
- Minor alarm しきい値
- Severe alarm しきい値
- Critical alarm しきい値

表 3-1 Memory alarm 通知と memory alarm-removed 通知

通知	トリガー状況	補足
Early-warning通知	空きメモリ容量が最初にEarly-warningしきい値以下に達した	Early-warning通知を作成、送信した後、装置は最初にEarly-warningがキャンセルされるまで追加でminor alarm通知を作成、送信しません。
Minor alarm通知	空きメモリ容量が最初にminor alarmしきい値以下に達した	minor alarm通知を作成、送信した後、装置は最初にminor alarmがキャンセルされるまで追加でminor alarm通知を作成、送信しません。
Severe alarm通知	空きメモリ容量が最初にsevere alarmしきい値以下に達した	severe alarm通知を作成、送信した後、装置は最初にsevere alarmがキャンセルされるまで追加でsevere alarm通知を作成、送信しません。
Critical alarm通知	空きメモリ容量が最初にcritical alarmしきい値以下に達した	critical alarm通知を作成、送信した後、装置は最初にcritical alarmがキャンセルされるまで追加でcritical alarm通知を作成、送信しません。
Critical alarm-removed 通知	空きメモリ容量が最初にsevere alarmしきい値以上に達した	ー

通知	トリガー状況	補足
Severe alarm-removed 通知	空きメモリ容量が最初に minor alarm しきい値以上に達した	ー
Minor alarm-removed 通知	空きメモリ容量が最初に normal alarm しきい値以上に達した	ー
Early-warning-removed 通知	空きメモリ容量が最初に sufficient-memory しきい値以上に達した	ー

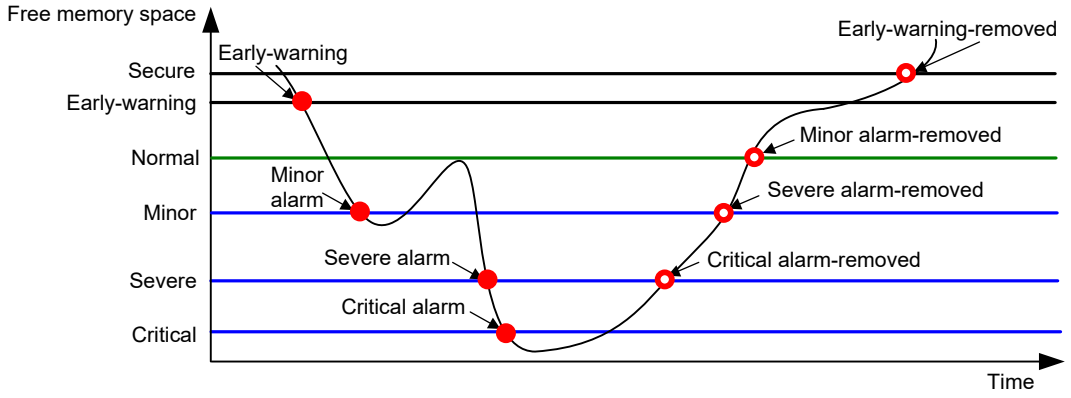


図 3-2 メモリ alarm 通知と alarm-removed 通知

以下にメモリアラームしきい値の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. 空きメモリしきい値を設定する	**memory-threshold** [**ratio**] **minor** *minor-value* **severe** *severe-value* **critical** *critical-value* **normal** *normal-value* [**early-warning** *early-warning-value* **secure** *secure-value*]	デフォルト： • **Minor alarm しきい値**– 512 MB • **Severe alarm しきい値**– 448 MB • **Critical alarm しきい値**– 384 MB • **Normal state しきい値**– 576 MB • **Early-warning しきい値**– 640 MB • **Sufficient-memory しきい値**– 704 MB

3.4 検出間隔の設定

特定の環境において、いくつかのプロトコルはポートをシャットダウンします。ポートがシャットダウンした後、装置は検出間隔タイマを開始します。検出間隔が経過した際にポートがまだダウンされている場合、物理的にポートを復旧させます。

以下に検出間隔を設定する方法を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． 検出間隔を設定する	**shutdown-interval** *time*	デフォルト：30秒

3.5 トランシーバのパラメータ表示

3.5.1 トランシーバの情報表示

搭載しているトランシーバ(SFP)のタイプ、コネクタの形状、送信するレーザーの中心波長、転送距離、ベンダ名などの情報を表示させることができます。

搭載しているトランシーバの表示を行うには、以下の手順に従って下さい。

操作	コマンド	補足
トランシーバの情報を表示する	**display transceiver interface** [*interface-type interface-number*]	―

3.5.2 トランシーバの診断

搭載しているトランシーバ(SFP)の状態確認やトラブルシューティングに役立つ診断機能を提供します。トランシーバモジュールが故障した場合や正常に動作していない場合、以下の機能を使用して状態を確認できます。

- アラーム情報の表示
  本装置は、トランシーバモジュールで発生しているアラームを表示します。これにより、ユーザは故障の原因を特定しやすくなります。
- デジタル診断パラメータの表示（デジタル診断機能）
  トランシーバモジュールのデジタル診断機能（DDM）によって監視されている、主要なパラメータの現在値を表示します。本装置から、温度、電圧、レーザーのバイアス電流、送信（TX）パワー、および受信（RX）パワーなどの状態を確認できます。

搭載しているトランシーバの診断を行うには、以下のコマンドを実行して下さい。

操作	コマンド	補足
トランシーバアラームを表示する	**display transceiver alarm interface** [*interface-type interface-number*]	―

操作	コマンド	補足
トランシーバモジュールのデジタル診断パラメータの現在地を表示する	**display transceiver diagnosis interface** [*interface-type interface-number*]	―

3.6 ハードウェアリソース管理の表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
CPU使用率の統計情報を表示する	**display cpu-usage**
CPU使用率のヒストリ統計情報を図で表示する	**display cpu-usage history** [**job** *job-id*]
ハードウェアについての情報を表示する	**display device** [**verbose**]
装置の製造情報を表示する	**display device manuinfo**
装置のメモリ使用率を表示する	**display memory**
装置のメモリ使用率のしきい値を表示する	**display memory-threshold**

目次

このセクションのページは **3-x-x** です。

4 章 NTP 4-1
4.1 概要 4-1
4.1.1 NTP の動作 4-1
4.1.2 NTP アーキテクチャ 4-2
4.1.3 運用モード 4-3
4.1.4 NTP セキュリティ 4-5
4.1.5 プロトコルと標準 4-7
4.2 設定の制限とガイドライン 4-7
4.3 設定作業リスト 4-7
4.4 NTP サービスの有効化 4-7
4.5 NTP 運用モードの設定 4-8
4.5.1 NTP クライアント/サーバモードの設定 4-8
4.5.2 NTP シンメトリックアクティブ/パッシブモードの設定 4-8
4.5.3 NTP ブロードキャストモードの設定 4-9
4.5.4 NTP マルチキャストモードの設定 4-9
4.6 NTP サービスアクセス制御権の設定 4-10
4.7 NTP 認証の設定 4-11
4.7.1 クライアント/サーバモードの NTP 認証の設定 4-11
4.7.2 シンメトリックアクティブ/パッシブモードの NTP 認証の設定 4-12
4.7.3 ブロードキャストモードの NTP 認証の設定 4-14
4.7.4 マルチキャストモードの NTP 認証の設定 4-16
4.8 NTP オプションパラメータの設定 4-18
4.8.1 NTP メッセージの送信元アドレスの指定 4-18
4.8.2 インタフェースでの NTP メッセージ処理の無効化 4-19
4.8.3 ダイナミックアソシエーションの最大数の設定 4-19
4.8.4 NTP パケットの DSCP 値の設定 4-20
4.9 NTP の表示と維持 4-20
4.10 NTP 設定例 4-20
4.10.1 NTP クライアント/サーバモードの設定例 4-20
4.10.2 NTP シンメトリックアクティブ/パッシブモードの設定例 4-22
4.10.3 NTP 認証を使用したクライアント/サーバモードの設定例 4-23

4章 NTP

NTP（Network Time Protocol）を使用して、あるいはシステムクロックを変更することで、ネットワークで動作させる前に、信頼されたシステムクロックと同期を取ります。システムメッセージのタイムスタンプとログは、システム時刻を使用しているため、ネットワーク管理、チャージシステム、監査、分散コンピューティングなどを含む、さまざまなアプリケーションは正確なシステムクロックが必要となります。

4.1 概要

NTP はネットワーク装置間のシステムクロックを動的に同期させるため、一般的に大規模ネットワークで使用されます。手動でシステムクロックを設定するよりも、高いクロック精度が保証されます。NTP を有効にする変更することで、装置間のシステムクロックを同期させ続けることができます。

NTP は UDP の上位プロトコルで、UDP ポート 123 を使用します。

🕮 **メモ：**

NTP は、レイヤ 3 イーサネットインタフェースでサポートします。

4.1.1 NTP の動作

図 4-1 に示すように、Device A と Device B の 2 つの Device 間でシステム時間を同期させる NTP の基本的なワークフローを示します。以下のように仮定します。

- システムクロックの同期を行う前に、Device A の時刻は 10:00:00 am で Device B の時刻は 11:00:00 am と設定されています。
- Device B は NTP サーバとして使用されます。Device A は Device B に同期化されます。
- NTP メッセージが Device A から Device B あるいは Device B から Device A に送信されるまで 1 秒かかります。
- Device B で NTP メッセージを処理するのに 1 秒かかります。

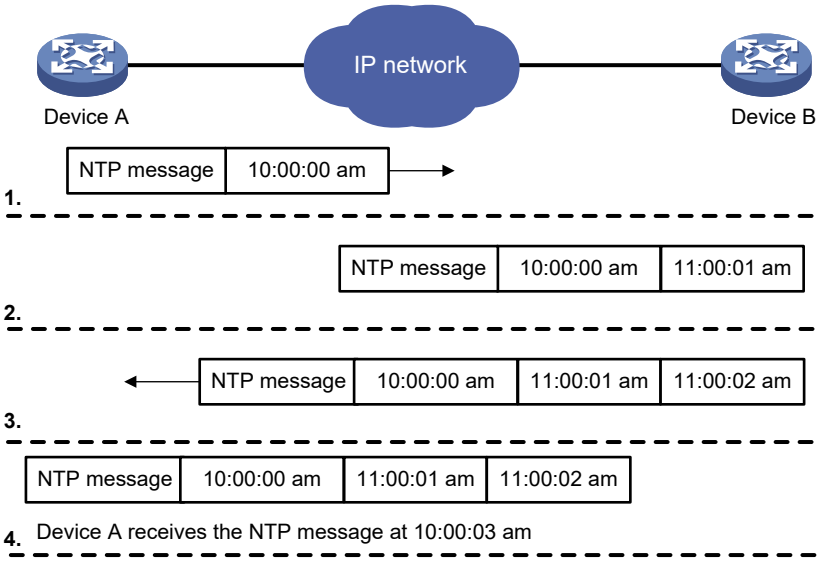


図 4-1 基本ワークフロー

以下に同期プロセスを示します。

1) Device A から Device B に NTP メッセージを送信します。メッセージは、Device A から発信されるときにタイムスタンプが与えられます。 タイムスタンプは 10:00:00 am （T1） です。
2) NTP メッセージが Device B に届くと、Device B によってタイムスタンプが与えられます。タイムスタンプは 11:00:01 am （T2） です。
3) NTP メッセージが Device B から発信されるときに、Device B はメッセージにタイムスタンプを与えます。タイムスタンプは 11:00:02 am （T3）です。
4) Device A が NTP メッセージを受信したとき、Device A の現地時刻は 10:00:03 am （T4）です。

Device A には以下の 2 つの重要なパラメータを計算するための情報があります。

- **NTP メッセージのラウンドトリップ遅延**：遅延＝（T4 － T1）－（T3 － T2）＝2 秒
- **Device A と Device B の間の時差**：オフセット＝（（T2 － T1）＋（T3 － T4））/2 ＝1 時間

これらのパラメータにもとづき、Device A の時計を Device B の時計に同期することができます。

上記は、NTP の動作メカニズムについての概要です。詳細については、関連するプロトコルと標準を参照してください。

4.1.2 NTP アーキテクチャ

NTP はクロックの正確さを定義するため、図 4-2 に示すように 1 から 16 の stratum（層）を使用します。stratum の値が小さいほど高い精度を持ちます。stratum 1 から 16 レベルのクロックは同期された時間で、stratum のレベル 16 のクロックは同期化されていないことを示します。

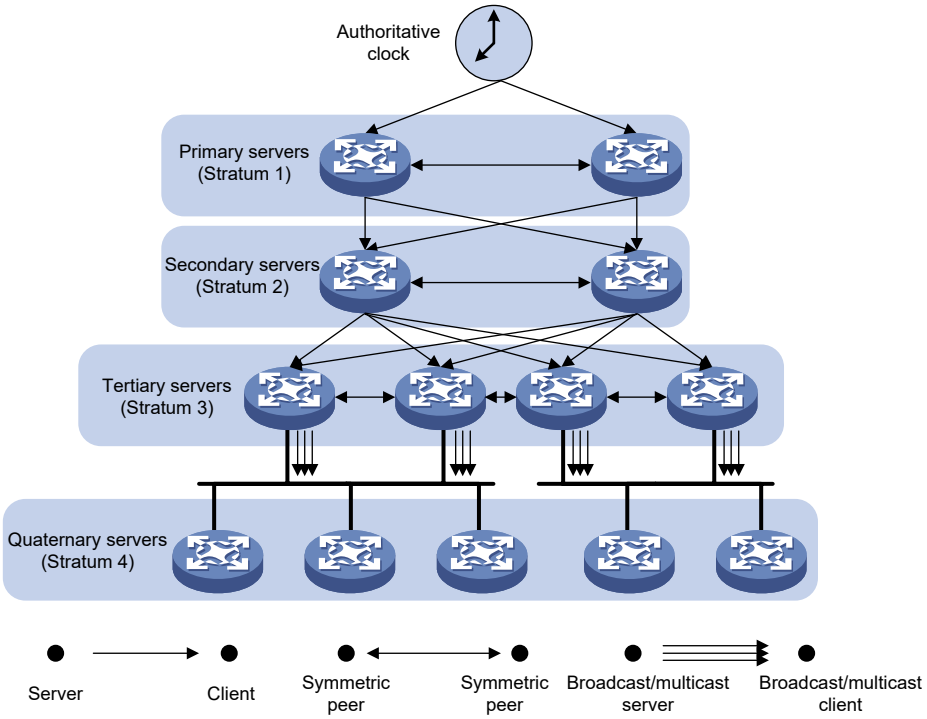


図 4-2 NTP アーキテクチャ

stratum レベル 1 の NTP サーバは、原子時計のような基準となるソースから時間を取得し、NTP サーバとして他の装置に時間を提供します。stratum レベル 2 のサーバは stratum レベル 1 のサーバなどから時間を取得します。

時間の正確性と有効性を保証するため、装置は複数の NTP サーバを指定することができます。装置は stratum のようなパラメータをもとにしてクロックソースとして最適な NTP サーバを選択します。装置が選択するクロックは参照ソースと呼ばれます。時計の選択の詳細は関連するプロトコルと標準を参照してください。

もしネットワークの装置がもっとも権威のあるサーバに同期することができない場合、以下の処理を行うことができます。

- ネットワークから相対的に精度のあるクロックを持つ装置を選択します。
- ネットワークのほかの装置と同期させるため、参照クロックとして相対的に精度のある装置のローカルクロックを使用します。

4.1.3 運用モード

NTP は以下の運用モードをサポートします。

- クライアント/サーバモード
- シンメトリックアクティブ/パッシブモード
- ブロードキャストモード
- マルチキャストモード

表 4-1 NTP 運用モード

モード	作業処理	原則	アプリケーションシナリオ
クライアント/サーバ	クライアントではNTPサーバのIPアドレスを指定します。 クライアントはクロック同期メッセージをNTPサーバに送信します。 メッセージを受信したサーバは自動的にサーバのモードで動作し、応答を返します。 クライアントはサーバに複数同期した場合、サーバからの応答を受信した後、最適なクロックを選択し、ローカルクロックを最適な参照ソースと同期させます。	クライアントはサーバと同期することができますが、サーバはクライアントと同期することができません。	図 4-2に示すように、このモードは高いstratumの装置が低いstratumの装置に同期します。
シンメトリックアクティブ/パッシブ	シンメトリックアクティブピア上で、シンメトリックパッシブピアのIPアドレスを指定します。 シンメトリックアクティブピアは周期的にシンメトリックパッシブピアにクロック同期メッセージを送信します。 シンメトリックパッシブピアは自動的にシンメトリックパッシブモードで動作し、応答を送信します。 シンメトリックアクティブピアがサーバに複数同期した場合、サーバからの応答を受信した後、最適なクロックを選択し、ローカルクロックを最適な参照ソースと同期させます。	シンメトリックアクティブピアとシンメトリックパッシブピアは互いに同期することができます。もし両方が同期された場合、低いstratumのピアが高いstratumのピアに同期します。	図 4-2に示すように、このモードはバックアップとして動作させるため、同じstratumの2つ以上のサーバ間で使われます。 高いstratumのすべてのサーバと通信できない場合、サーバは同じstratumのサーバと同期します。

モード	作業処理	原則	アプリケーションシナリオ
ブロードキャスト	サーバは周期的にブロードキャストアドレス255.255.255.255にクロック同期メッセージを送信します。 クライアントはサーバと同期するため、ブロードキャストメッセージに応答したサーバからブロードキャストメッセージを待ちます。 最初にブロードキャストメッセージを受信したとき、クライアントとサーバはネットワーク遅延を計算するため、メッセージの交換を開始します。ブロードキャストサーバのみがクロック同期メッセージを送信します。	ブロードキャストクライアントはブロードキャストサーバに同期することができますが、ブロードキャストサーバはブロードキャストクライアントに同期することができません。	ブロードキャストサーバはクロック同期メッセージを同じサブネットのクライアントに送信します。図 4-2に示すように、このモードは潜在的に1つあるいは少ないサーバで、多くのクライアントがある環境で使われます。 ブロードキャストモードは、ブロードキャストサーバのみがクロック同期メッセージを送信するため、クライアント/サーバモードやシンメトリックアクティブ/パッシブよりも精度が低くなります。
マルチキャスト	マルチキャストサーバは周期的にユーザが設定したマルチキャストアドレスにクロック同期メッセージを送信します。 クライアントはマルチキャストメッセージに応答したサーバからマルチキャストメッセージを待ちます。	マルチキャストクライアントはマルチキャストサーバに同期することができますが、マルチキャストサーバはマルチキャストクライアントに同期することができません。	マルチキャストサーバはクロック同期メッセージを同じあるいは異なるサブネットのクライアントに送信します マルチキャストモードは、クライアント/サーバモードやシンメトリックアクティブ/パッシブよりも精度が低くなります。

この章では、NTP サーバあるいはサーバとは、クライアント/サーバモードの NTP サーバとして動作する装置を示します。タイムサーバとは、NTP サーバ、NTP シンメトリックピア、ブロードキャストサーバ、マルチキャストサーバを含んだ、クロック同期を行うことができるすべての装置を示します。

4.1.4 NTP セキュリティ

クロック同期のセキュリティを向上させるため、装置は NTP サービスアクセス制御権と認証機能をサポートします。

I. NTP サービスアクセス制御権の設定

ACL を用いて NTP サービスアクセス制御権を設定することができます。アクセス制御権は以下となります。

- **Peer**ー時刻要求と NTP コントロールクエリ（アラーム、認証ステータス、時間サーバなどの情報）を受信し、ローカル装置が隣接装置に自身を同期させることを可能とします。
- **Server**ー時刻要求と NTP コントロールクエリを受信するが、ローカル装置が隣接装置に自身を同期させることを可能としません。
- **Synchronization**ーアドレスリストを通過したアドレスを持つシステムからの時刻要求のみ受信します。
- **Query**ー隣接装置からローカル装置への NTP コントロールクエリのみ受信します。

装置は以下のように NTP 要求を処理します。

- アクセス制御権が設定されていない場合、**peer** はローカル装置と隣接装置に与えられます。
- 隣接装置の IP アドレスが複数のアクセス制御権のための ACL にマッチし、**Permit** となる場合、もっとも制限の少ないアクセス制御権が隣接装置に与えられます。ACL にマッチしない、または **deny** となった場合、アクセス制御権は与えられません。
- アクセス制御権のために指定された ACL が作成されない場合、関連したアクセス制御権は与えられません。
- アクセス制御権のために指定された ACL が 1 つも作成されない場合、**peer** が与えられます。

この機能は、NTP を運用するシステムに最低限のセキュリティを提供します。より安全な方法としては NTP 認証があります。

II. NTP 認証

NTP 認証は、セキュリティのため、NTP メッセージを認証します。NTP メッセージが認証をパスしたとき、装置は、メッセージを受信し、クロック同期情報を取得します。もしパスしないとき、メッセージを廃棄します。この機能は、許可されていないサーバに同期をしないようにするために使われます。

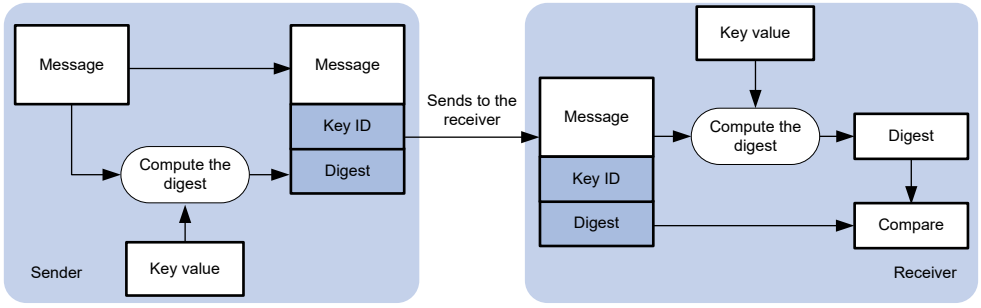


図 4-3 NTP 認証

図 4-3 に示すように NTP 認証は以下のように動作します。

1) Sender は、キーID によって識別されたキーに従って NTP メッセージを計算するため、MD5/HMAC アルゴリズムを使用します。NTP メッセージを計算したダイジェストとキーID を Receiver に送信します。
2) メッセージを受信すると Receiver は以下の処理を行います。

a) メッセージのキーIDに応じてキーを確認します。

b) ダイジェストを計算するため、MD5/HMACアルゴリズムを使用します。

c) NTPメッセージの計算したダイジェストとNTPメッセージに含まれているダイジェストと比較します。

- 計算したダイジェストと NTP メッセージに含まれているダイジェストが同一でない場合、Receiver はメッセージを廃棄します。
- 計算したダイジェストと NTP メッセージに含まれているダイジェストが同一であり、NTP アソシエーションを確立する必要がない場合、Receiver は応答パケットを提供します。 NTP アソシエーションの詳細は、本章の“*ダイナミックアソシエーションの最大数の設定*”を参照してください。
- 計算したダイジェストと NTP メッセージに含まれているダイジェストが同一で、NTP アソシエーションを確立する必要があるか、存在している場合、ローカル装置は Sender が認証 ID を許可しているかどうか確認します。Sender が認証 ID を許可している場合、Receiver はメッセージを受信します。Sender が認証 ID を許可していない場合、Receiver はメッセージを廃棄します。

4.1.5 プロトコルと標準

- RFC 1305, *Network Time Protocol (Version 3) Specification, Implementation and Analysis*
- RFC 5905, *Network Time Protocol Version 4: Protocol and Algorithms Specification*

4.2 設定の制限とガイドライン

以下の設定の制限とガイドラインに従って NTP を設定してください。

- アグリゲートメンバーポートで NTP を設定することはできません。
- 時間同期精度を保証するために、複数の reference source を指定することを推奨しません。reference source を複数指定した場合、頻繁にクロックが変更する、あるいは同期の失敗が発生する可能性があります。
- 正確な時刻同期のために、システム時刻と NTP クロック ソースの間の時間オフセットが 68 年未満であることを確認してください。

4.3 設定作業リスト

作業リスト
（必須設定項目） NTPサービスの有効化
（必須設定項目） NTP運用モードの設定
（オプション設定項目） NTPサービスアクセス制御権の設定
（オプション設定項目） NTP認証の設定
（オプション設定項目） NTPオプションパラメータの設定

4.4 NTPサービスの有効化

操作	コマンド	補足
1． system view に移行する	**system-view**	―

操作	コマンド	補足
2． NTP サービスを有効にする	**ntp-service enable**	デフォルト：無効

4.5 NTP運用モードの設定

この章は NTP 運用モードの設定方法について記載します。

4.5.1 NTP クライアント/サーバモードの設定

NTP クライアントを設定するとき、以下のガイドラインに従います。

- サーバは他の装置によって同期させる必要があります。あるいは NTP クライアントを同期する前に参照ソースとしてローカルクロックを使用する必要があります。そうでなければクライアントは NTP サーバに同期することができません。
- サーバの stratum レベルがクライアントと等しいあるいは高いレベルである場合クライアントはサーバに同期しません。
- **ntp-service unicast-server** コマンドを繰り返して設定することで複数のサーバを設定することができます。
- 装置がクライアント/サーバモードで動作するとき、クライアントの IP アドレスを指定します。

以下に NTP クライアントの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． 装置の NTP サーバを指定する	**ntp-service unicast-server** { *server-name* | *ip-address* } [**authentication-keyid** *keyid* | **priority** | **source** *interface-type interface-number* | **version** *number*] *	デフォルト：指定なし

4.5.2 NTP シンメトリックアクティブ/パッシブモードの設定

NTP シンメトリックアクティブピアを設定するとき、以下のガイドラインに従います。

- NTP を有効にするため、シンメトリックパッシブピアで **ntp-service enable** コマンドを実行してください。そうでなければシンメトリックパッシブピアはシンメトリックアクティブピアから NTP メッセージを処理しません。
- シンメトリックアクティブピアあるいはシンメトリックパッシブピアのどちらかあるいは、その両方は同期化された状態にする必要があります。そうでなければ同期化することができません。
- **ntp-service unicast-peer** コマンドを繰り返して設定することで複数のシンメトリックパッシブピアを設定することができます。
- シンメトリックアクティブ/パッシブモードで装置が動作するとき、シンメトリックパッシブピア用にシンメトリックアクティブピアの IP アドレスを指定します。

以下に NTP シンメトリックアクティブピアの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． シンメトリックパッシブピアを指定する	**ntp-service unicast-peer** { *peer-name* | *ip-address* } [**authentication-keyid** *keyid* | **priority** | **source** *interface-type interface-number* | **version** *number*] *	デフォルト：指定なし

4.5.3 NTP ブロードキャストモードの設定

ブロードキャストサーバは、ブロードキャストクライアントを同期する前に、他の装置によって同期させる必要があります。あるいは参照ソースとしてローカルクロックを使用する必要があります。そうでなければブロードキャストクライアントはブロードキャストサーバに同期させることができません。

ブロードキャストサーバとクライアントの両方でブロードキャストモードの NTP を設定します。

I. ブロードキャストクライアントの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． interface view に移行する	**interface** *interface-type interface-number*	NTPブロードキャストメッセージを受信するインタフェースに移行します。
3． 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装置を設定する	**ntp-service broadcast-client**	デフォルト：設定なし コマンドを実行した後、装置は指定したインタフェースからNTPブロードキャストメッセージを受信します。

II. ブロードキャストサーバの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． interface view に移行する	**interface** *interface-type interface-number*	NTPブロードキャストメッセージを送信するインタフェースに移行します。
3． NTP ブロードキャストサーバモードで動作するように装置を設定する	**ntp-service broadcast-server** [**authentication-keyid** *keyid* | **version** *number*] *	デフォルト：設定なし コマンドを実行した後、装置は指定したインタフェースからNTPブロードキャストメッセージを受信します。

4.5.4 NTP マルチキャストモードの設定

マルチキャストサーバは、マルチキャストクライアントを同期する前に、他の装置によって同期させる必要があります。あるいは参照ソースとしてローカルクロックを使用する必

要があります。そうでなければマルチキャストクライアントはマルチキャストサーバに同期させることができません。

マルチキャストサーバとクライアントの両方でマルチキャストモードの NTP を設定します。

I. マルチキャストクライアントの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． interface view に移行する	**interface** *interface-type interface-number*	NTPマルチキャストメッセージを受信するインタフェースに移行します。
3． 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装置を設定する	**ntp-service multicast-client** [*ip-address*]	デフォルト：設定なし コマンドを実行した後、装置は指定したインタフェースからNTPマルチキャストメッセージを受信します。

II. マルチキャストサーバの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． interface view に移行する	**interface** *interface-type interface-number*	NTPマルチキャストメッセージを送信するインタフェースに移行します。
3． NTP マルチキャストサーバモードで動作するように装置を設定する	**ntp-service multicast-server** [*ip-address*] [**authentication-keyid** *keyid* | **ttl** *ttl-number* | **version** *number*] *	デフォルト：設定なし コマンドを実行した後、装置は指定したインタフェースからNTPマルチキャストメッセージを送信します。

4.6 NTPサービスアクセス制御権の設定

アクセス制御権を設定するには、表 4-2 に記載されている制限とガイドラインに従ってください。

表 4-2 アクセス制御権を構成するための制限とガイドライン

アクセス制御権	時刻を同期できるかどうか (クライアントで設定できるかどうか)	他のデバイスの時刻を同期できるかどうか (タイム サーバで設定できるかどうか)	コントロール クエリを許可するかどうか
Peer	Yes	Yes	Yes
Server	Yes	No	Yes
Synchronization	Yes	No	No
Query	No	No	Yes

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． 隣接装置がローカル装置にアクセスするための NTP サービスアクセス制御権を設定する	**ntp-service** { **peer** | **query** | **server** | **synchronization** } **acl** *ipv4-acl-number*	デフォルト：peer

NTP サービスアクセス制御権をローカル装置に設定する前にアクセス制御権に関連した ACL を作成、設定してください。詳細は QX-W2300AC シリーズアクセスコントローラコマンドマニュアルの“*15 セキュリティ*”の”*1 章 ACL*”を参照してください。

4.7 NTP認証の設定

この章は NTP 認証の設定手順について記載します。

4.7.1 クライアント/サーバモードの NTP 認証の設定

サーバとクライアントで設定されたキーID、アルゴリズム、およびキーの値は同じにする必要があります。そうでなければ NTP 認証は失敗します。

以下にクライアントの NTP 認証の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． NTP 認証を有効にする	**ntp-service authentication enable**	デフォルト：無効
3． NTP 認証キーを設定する	**ntp-service authentication-keyid** *keyid* **authentication-mode** { **hmac-sha-1** | **hmac-sha-256** | **hmac-sha-384** | **hmac-sha-512** | **md5** } { **cipher** | **simple** } *string*	デフォルト：設定なし
4． 認証キーをトラステッドキーとして設定する	**ntp-service reliable authentication-keyid** *keyid*	デフォルト：設定なし
5． NTP サーバとキーを関連づける	**ntp-service unicast-server** { *server-name* | *ip-address* } **authentication-keyid** *keyid*	デフォルト：設定なし

以下にサーバの NTP 認証の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． NTP 認証を有効にする	**ntp-service authentication enable**	デフォルト：無効
3． NTP 認証キーを設定する	**ntp-service authentication-keyid** *keyid* **authentication-mode** { **hmac-sha-1** | **hmac-sha-256** | **hmac-sha-384** | **hmac-sha-512** | **md5** } { **cipher** | **simple** } *string*	デフォルト：設定なし

操作	コマンド	補足
4． 認証キーをトラステッドキーとして設定する	**ntp-service reliable authentication-keyid** *keyid*	デフォルト：設定なし

クライアントとサーバで異なる設定が実行されると、NTP 認証の結果は異なります。詳細を表 4-3 に示します。（ーは相違がないことを示します。）

以下に NTP 認証の結果を示します。

表 4-3 NTP 認証の結果

クライアント			サーバ		認証結果
NTP 認証を有効にする	キーをトラステッドキーとして設定する	NTP サーバにキーを関連づける	NTP 認証を有効にする	キーをトラステッドキーとして設定する	
Yes	Yes	Yes	Yes	Yes	認証は成功します。NTPメッセージは正常に送受信することができます。
Yes	Yes	Yes	Yes	No	認証は失敗します。NTPメッセージは正常に送受信することができません。
Yes	Yes	Yes	No	ー	認証は失敗します。NTPメッセージは正常に送受信することができません。
Yes	No	Yes	ー	ー	認証は失敗します。NTPメッセージは正常に送受信することができません。
Yes	ー	No	ー	ー	認証はありません。NTPメッセージは正常に送受信することができます。
No	ー	ー	ー	ー	認証はありません。NTPメッセージは正常に送受信することができます。

4.7.2 シンメトリックアクティブ/パッシブモードの NTP 認証の設定

アクティブピアとパッシブピアで設定されたキーID、アルゴリズム、およびキーの値は同じにする必要があります。そうでなければ NTP 認証は失敗します。ピアの装置がローカル装置でキーID を使用することができることを確認してください。

以下にアクティブピアの NTP 認証の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー

操作	コマンド	補足
2． NTP 認証を有効にする	**ntp-service authentication enable**	デフォルト：無効
3． NTP 認証キーを設定する	**ntp-service authentication-keyid** *keyid* **authentication-mode** { **hmac-sha-1** | **hmac-sha-256** | **hmac-sha-384** | **hmac-sha-512** | **md5** } { **cipher** | **simple** } *string*	デフォルト：設定なし
4． 認証キーをトラステッドキーとして設定する	**ntp-service reliable authentication-keyid** *keyid*	デフォルト：設定なし
5． パッシブピアとキーを関連づける	**ntp-service unicast-peer** { *ip-address* | *peer-name* } **authentication-keyid** *keyid*	デフォルト：設定なし

以下にパッシブピアの NTP 認証の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． NTP 認証を有効にする	**ntp-service authentication enable**	デフォルト：無効
3． NTP 認証キーを設定する	**ntp-service authentication-keyid** *keyid* **authentication-mode** { **hmac-sha-1** | **hmac-sha-256** | **hmac-sha-384** | **hmac-sha-512** | **md5** } { **cipher** | **simple** } *string*	デフォルト：設定なし
4． 認証キーをトラステッドキーとして設定する	**ntp-service reliable authentication-keyid** *keyid*	デフォルト：設定なし

アクティブピアとパッシブピアで異なる設定が実行されると、NTP 認証の結果は異なります。詳細を表 4-4 に示します。（ーは相違がないことを示します。）

以下に NTP 認証の結果を示します。

表 4-4 NTP 認証の結果

アクティブピア			パッシブピア		認証結果
NTP 認証を有効にする	キーをトラステッドキーとして設定する	パッシブピアにキーを関連づける	NTP 認証を有効にする	キーをトラステッドキーとして設定する	
アクティブピアとパッシブピアのstratumレベルは考慮しません。					
Yes	Yes	Yes	Yes	Yes	認証は成功します。NTPメッセージは正常に送受信することができます。
Yes	Yes	Yes	Yes	No	認証は失敗します。NTPメッセージは正常に送受信することができません。
Yes	Yes	Yes	No	―	認証は失敗します。NTPメッセージは正常に送受信することができません。

アクティブピア			パッシブピア		認証結果
NTP 認証を有効にする	キーをトラステッドキーとして設定する	パッシブピアにキーを関連づける	NTP 認証を有効にする	キーをトラステッドキーとして設定する	
Yes	―	No	Yes	―	認証は失敗します。NTPメッセージは正常に送受信することができません。
Yes	―	No	No	―	認証はありません。NTPメッセージは正常に送受信することができます。
No	―	―	Yes	―	認証は失敗します。NTPメッセージは正常に送受信することができません。
No	―	―	No	―	認証はありません。NTPメッセージは正常に送受信することができます。
アクティブピアはパッシブピアよりも高いstratumを持ちます。					
Yes	No	Yes	―	―	認証は失敗します。NTPメッセージは正常に送受信することができません。
パッシブピアはアクティブピアよりも高いstratumを持ちます。					
Yes	No	Yes	Yes	―	認証は失敗します。NTPメッセージは正常に送受信することができません。
Yes	No	Yes	No	―	認証はありません。NTPメッセージは正常に送受信することができます。

4.7.3 ブロードキャストモードの NTP 認証の設定

ブロードキャストクライアントとブロードキャストサーバで設定されたキーID、アルゴリズム、およびキーの値は同じにする必要があります。そうでなければ NTP 認証は失敗します。

以下にブロードキャストクライアントの NTP 認証の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. NTP 認証を有効にする	**ntp-service authentication enable**	デフォルト：無効
3. NTP 認証キーを設定する	**ntp-service authentication-keyid** *keyid* **authentication-mode** { **hmac-sha-1** | **hmac-sha-256** | **hmac-sha-384** | **hmac-sha-512** | **md5** } { **cipher** | **simple** } *string*	デフォルト：設定なし

操作	コマンド	補足
4． 認証キーをトラステッドキーとして設定する	**ntp-service reliable authentication-keyid** *keyid*	デフォルト：設定なし

以下にブロードキャストサーバの NTP 認証の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． NTP 認証を有効にする	**ntp-service authentication enable**	デフォルト：無効
3． NTP 認証キーを設定する	**ntp-service authentication-keyid** *keyid* **authentication-mode** { **hmac-sha-1** | **hmac-sha-256** | **hmac-sha-384** | **hmac-sha-512** | **md5** } { **cipher** | **simple** } *string*	デフォルト：設定なし
4． 認証キーをトラステッドキーとして設定する	**ntp-service reliable authentication-keyid** *keyid*	デフォルト：設定なし
5． interface view に移行する	**interface** *interface-type interface-number*	―
6． ブロードキャストサーバとキーを関連づける	**ntp-service broadcast-server authentication-keyid** *keyid*	デフォルト：設定なし

ブロードキャストクライアントとブロードキャストサーバで異なる設定が実行されると、NTP 認証の結果は異なります。詳細を表 4-5 に示します。（ーは相違がないことを示します。）

以下に NTP 認証の結果を示します。

表 4-5 NTP 認証の結果

ブロードキャストサーバ			ブロードキャストクライアント		認証の結果
NTP 認証を有効にする	キーをトラステッドキーとして設定する	ブロードキャストサーバとキーを関連づける	NTP 認証を有効にする	キーをトラステッドキーとして設定する	
Yes	Yes	Yes	Yes	Yes	認証は成功します。NTPメッセージは正常に送受信することができます。
Yes	Yes	Yes	Yes	No	認証は失敗します。NTPメッセージは正常に送受信することができません。
Yes	Yes	Yes	No	―	認証は失敗します。NTPメッセージは正常に送受信することができません。
Yes	No	Yes	Yes	―	認証は失敗します。NTPメッセージは正常に送受信することができません。

ブロードキャストサーバ			ブロードキャストクライアント		認証の結果
NTP 認証を有効にする	キーをトラステッドキーとして設定する	ブロードキャストサーバとキーを関連づける	NTP 認証を有効にする	キーをトラステッドキーとして設定する	
Yes	No	Yes	No	―	認証はありません。NTPメッセージは正常に送受信することができます。
Yes	―	No	Yes	―	認証は失敗します。NTPメッセージは正常に送受信することができません。
Yes	―	No	No	―	認証はありません。NTPメッセージは正常に送受信することができます。
No	―	―	Yes	―	認証は失敗します。NTPメッセージは正常に送受信することができません。
No	―	―	No	―	認証はありません。NTPメッセージは正常に送受信することができます。

4.7.4 マルチキャストモードの NTP 認証の設定

マルチキャストクライアントとマルチキャストサーバで設定されたキーID、アルゴリズム、およびキーの値は同じにする必要があります。そうでなければ NTP 認証は失敗します。ピアの装置がローカル装置でキーID を使用することができることを確認してください。

以下にマルチキャストクライアントの NTP 認証の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． NTP 認証を有効にする	**ntp-service authentication enable**	デフォルト：無効
3． NTP 認証キーを設定する	**ntp-service authentication-keyid** *keyid* **authentication-mode** { **hmac-sha-1** | **hmac-sha-256** | **hmac-sha-384** | **hmac-sha-512** | **md5** } { **cipher** | **simple** } *string*	デフォルト：設定なし
4． 認証キーをトラステッドキーとして設定する	**ntp-service reliable authentication-keyid** *keyid*	デフォルト：設定なし

以下にマルチキャストサーバの NTP 認証の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―

操作	コマンド	補足
2． NTP 認証を有効にする	**ntp-service authentication enable**	デフォルト：無効
3． NTP 認証を有効にする	**ntp-service authentication-keyid** *keyid* **authentication-mode** { **hmac-sha-1** | **hmac-sha-256** | **hmac-sha-384** | **hmac-sha-512** | **md5** } { **cipher** | **simple** } *string*	デフォルト：設定なし
4． 認証キーをトラステッドキーとして設定する	**ntp-service reliable authentication-keyid** *keyid*	デフォルト：設定なし
5． interface view に移行する	**interface** *interface-type interface-number*	―
6． マルチキャストサーバとキーを関連づける	**ntp-service multicast-server** [*ip-address*] **authentication-keyid** *keyid*	デフォルト：設定なし

マルチキャストクライアントとマルチキャストサーバで異なる設定が実行されると、NTP 認証の結果は異なります。詳細を表 4-6 に示します。（ーは相違がないことを示します。）

以下に NTP 認証の結果を示します。

表 4-6 NTP 認証の結果

マルチキャストサーバ			マルチキャストクライアント		認証の結果
NTP 認証を有効にする	キーをトラステッドキーとして設定する	マルチキャストサーバにキーを関連づける	NTP 認証を有効にする	キーをトラステッドキーとして設定する	
Yes	Yes	Yes	Yes	Yes	認証は成功します。NTPメッセージは正常に送受信することができます。
Yes	Yes	Yes	Yes	No	認証は失敗します。NTPメッセージは正常に送受信することができません。
Yes	Yes	Yes	No	―	認証は失敗します。NTPメッセージは正常に送受信することができません。
Yes	No	Yes	Yes	―	認証は失敗します。NTPメッセージは正常に送受信することができません。
Yes	No	Yes	No	―	認証はありません。NTPメッセージは正常に送受信することができます。
Yes	―	No	Yes	―	認証は失敗します。NTPメッセージは正常に送受信することができません。

マルチキャストサーバ			マルチキャストクライアント		認証の結果
NTP 認証を有効にする	キーをトラステッドキーとして設定する	マルチキャストサーバにキーを関連づける	NTP 認証を有効にする	キーをトラステッドキーとして設定する	
Yes	―	No	No	―	認証はありません。NTPメッセージは正常に送受信することができます。
No	―	―	Yes	―	認証は失敗します。NTPメッセージは正常に送受信することができません。
No	―	―	No	―	認証はありません。NTPメッセージは正常に送受信することができます。

4.8 NTPオプションパラメータの設定

この章はオプション作業設定項目について記載します。NTP セキュリティ、性能、信頼性を改善するために設定します。

4.8.1 NTP メッセージの送信元アドレスの指定

NTP メッセージの送信元 IP アドレスは、直接指定するか、送信元インタフェースを指定できます。 NTP メッセージの送信元インタフェースを指定すると、指定した送信元インタフェースのアドレスが NTP メッセージの送信元アドレスになります。

インタフェースの状態の変更によって、NTP 通信の失敗を引き起こすことを防ぐため、常にアップ状態であるインタフェースの IP アドレスを使用するように設定します。たとえば常にアップ状態であるインタフェースはループバックインタフェースです。装置のインタフェースの状態の変更によって、NTP メッセージを受信できるようにするため、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設定します。

装置が NTP リクエストに応答する場合、NTP 応答の送信元 IP アドレスは、NTP リクエストを受信したインタフェースの IP アドレスです。

以下に NTP メッセージの送信元インタフェースを指定するときのガイドラインを示します。

- **ntp-service unicast-server** コマンドあるいは **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-server** コマンドあるいは **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-service broadcast-server** コマンドあるいは **ntp-service multicast-server** コマンドが設定された場合、ブロードキャスト NTP メッセージあるいはマルチキャスト NTP メッセージの送信元インタフェースは、それぞれのコマンドで設定したインタフェースです。

以下に NTP メッセージの送信元アドレスの指定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. NTP メッセージの送信元アドレスを指定する	**ntp-service source** { *interface-type interface-number* | *ipv4-address* }	デフォルト：設定なし

4.8.2 インタフェースでの NTP メッセージ処理の無効化

NTP が有効なとき、デフォルトですべてのインタフェースは NTP メッセージを受信することができます。セキュリティのため、インタフェースで NTP メッセージを受信しないようにすることができます。

以下に NTP メッセージの受信をインタフェースで無効にする設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. interface view に移行する	**interface** *interface-type interface-number*	―
3. インタフェースで NTP メッセージの処理を無効にする	**undo ntp-service inbound enable**	デフォルト：有効

4.8.3 ダイナミックアソシエーションの最大数の設定

NTP は以下のアソシエーションタイプがあります。

- **スタティックアソシエーション** ― 手動で作成したアソシエーション
- **ダイナミックアソシエーション** ― NTP を動作する間、システムによって作成された一時的なアソシエーションです。12 分以内にメッセージの交換が行われない場合、ダイナミックアソシエーションは削除されます。

以下に設定される異なるアソシエーションモードを示します。

- **クライアント/サーバモード** ― NTP サーバを指定した後、システムはクライアントでスタティックアソシエーションを作成します。サーバはアソシエーション（スタティックあるいはダイナミック）を作成するのではなく、単に受信したメッセージに対して、受動的に応答します。
- **シンメトリックアクティブ/パッシブモード** ― シンメトリックアクティブピアでシンメトリックパッシブピアを指定した後、シンメトリックアクティブピア上でスタティックアソシエーションが作成され、シンメトリックパッシブピアでダイナミックアソシエーションが作成されます。
- **ブロードキャスト/マルチキャストモード** ― サーバでスタティックアソシエーションが作成され、クライアントでダイナミックアソシエーションが作成されます。

1 つの装置で、スタティックアソシエーション、ダイナミックアソシエーションを含み、共通で最大 128 のアソシエーションを作成することができます。

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。

以下にダイナミックアソシエーションの最大数の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． ダイナミックアソシエーションの最大数を設定する	**ntp-service max-dynamic-sessions** *number*	デフォルト：100

4.8.4 NTP パケットの DSCP 値の設定

パケットの DSCP 値は、パケットの優先度レベルを指定し、パケットの優先度に影響します。

以下に NTP パケットの DSCP 値の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． NTP パケットの DSCP 値を設定する	**ntp-service dscp** *dscp-value*	デフォルト：48

4.9 NTPの表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
IPv4 NTPアソシエーションを表示する	**display ntp-service sessions** [**verbose**]
NTPサービスステータスの情報を表示する	**display ntp-service status**
ローカル装置からプライマリ参照ソースに戻ったNTPサーバの概要情報を表示する	**display ntp-service trace**

4.10 NTP設定例

4.10.1 NTP クライアント/サーバモードの設定例

I. ネットワーク要件

図 4-4 に示すように設定します。

- AC の stratum レベル 2 のローカルクロックを参照ソースとして設定します。
- Switch をクライアントモードで動作し、AC を Switch の NTP サーバとして設定します。

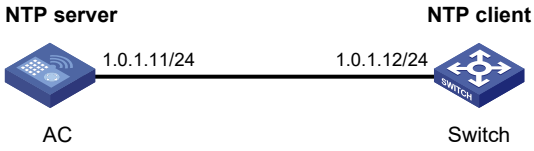


図 4-4 ネットワーク図

II. 設定手順

1) 図 4-4 に示すように各インタフェースの IP アドレスを設定します。(詳細は省略します。)
2) AC を設定します。

NTP サービスを有効にします。

```
<AC> system-view
[AC] ntp-service enable
```

参照ソースとして stratum レベル 2 のローカルクロックを指定します。

ntp-service refclock-master コマンドは QX-W2300AC シリーズではサポートしていません。

```
[AC] ntp-service refclock-master 2
```

3) Switch を設定します。

NTP サービスを有効にします。

```
<Switch> system-view
[Switch] ntp-service enable
```

Switch が AC に同期されるように、Switch の NTP サーバとして AC を指定します。

```
[Switch] ntp-service unicast-server 1.0.1.11
```

III. 設定の確認

Switch が AC に同期化され、Switch の stratum レベルが 3 であることを確認します。

```
[Switch] display ntp-service status
 Clock status: synchronized
 Clock stratum: 3
 System peer: 1.0.1.11
 Local mode: client
 Reference clock ID: 1.0.1.11
 Leap indicator: 00
 Clock jitter: 0.000977 s
 Stability: 0.000 pps
 Clock precision: 2^-23
 Root delay: 0.00383 ms
 Root dispersion: 16.26572 ms
 Reference time: d0c6033f.b9923965  Wed, Dec 29 2010 18:58:07.724
```

Switch と AC 間で NTP アソシエーションが確立されていることを確認します。

```
[Switch] display ntp-service sessions
       source           reference        stra reach poll  now offset  delay
disper
**************************************************************************
**
[12345]1.0.1.11         127.127.1.0         2     1    64   15    -4.0 0.0038
16.262
Notes:  1  source(master),  2  source(peer),  3  selected,  4  candidate,  5
configured.
 Total sessions: 1
```

4.10.2 NTP シンメトリックアクティブ/パッシブモードの設定例

I. ネットワーク要件

図 4-5 に示すように、設定します。

- 参照ソースとして AC のローカルクロックを stratum レベル 2 に設定します。
- シンメトリックアクティブモードで動作するように Switch を設定し、Switch のパッシブピアとして AC を指定します。

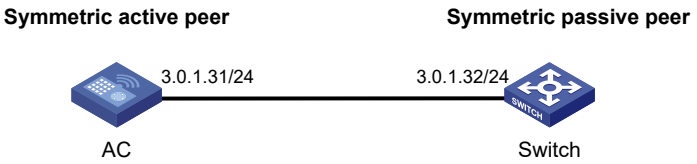


図 4-5 ネットワーク図

II. 設定手順

1) 図 4-5 に示すように各インタフェースの IP アドレスを設定します。(詳細は省略します。)
2) Switch を設定します。

NTP サービスを有効にします。

```
<Switch> system-view
[Switch] ntp-service enable
```

3) AC を設定します。

NTP サービスを有効にします。

```
<AC> system-view
[AC] ntp-service enable
```

参照ソースとして stratum レベル 2 のローカルクロックを設定します。

ntp-service refclock-master コマンドは QX-W2300AC シリーズではサポートしていません。

```
[AC] ntp-service refclock-master 2
```

シンメトリックパッシブピアとして Switch を設定します。

```
[AC] ntp-service unicast-peer 3.0.1.32
```

III. 設定の確認

Switch が AC に同期していることと、クロック stratum レベルが 3 であることを確認します。

```
[Switch] display ntp-service status
 Clock status: synchronized
 Clock stratum: 3
 System peer: 3.0.1.31
 Local mode: sym_passive
 Reference clock ID: 3.0.1.31
 Leap indicator: 00
 Clock jitter: 0.000916 s
 Stability: 0.000 pps
 Clock precision: 2^-23
 Root delay: 0.00609 ms
 Root dispersion: 1.95859 ms
 Reference time: 83aec681.deb6d3e5  Wed, Jan  8 2014 14:33:11.081
```

Switch と AC 間の IPv4 NTP アソシエーションが確立されていることを確認します。

```
[Switch] display ntp-service sessions
       source           reference        stra reach poll  now offset  delay
disper
**************************************************************************
**
   [12]3.0.1.31         127.127.1.0         2     62    64    34 0.4251 6.0882
1392.1
Notes:  1  source(master),  2  source(peer),  3  selected,  4  candidate,  5
configured.
 Total sessions: 1
```

4.10.3 NTP 認証を使用したクライアント/サーバモードの設定例

I. ネットワーク要件

- 図 4-6 に示すように、AC の stratum レベル 2 のローカルクロックは参照ソースとして使われます。
- Switch はクライアントモードで動作し、AC は Switch の NTP サーバとして使用されます。
- AC と Switch の両方で NTP 認証を設定します。

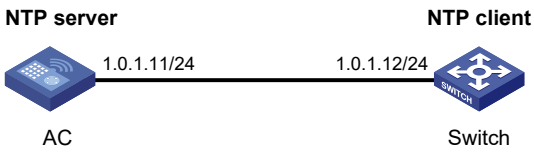


図 4-6 ネットワーク図

II. 設定手順

1) 図 4-6 に示すように各インタフェースの IP アドレスを設定します。(詳細は省略します。)
2) AC を設定します。

NTP サービスを有効にします。

```
<AC> system-view
[AC] ntp-service enable
```

参照ソースとして stratum レベル 2 のローカルクロックを指定します。

ntp-service refclock-master コマンドは QX-W2300AC シリーズはサポートしていません。

```
[AC] ntp-service refclock-master 2
```

3) Switch を設定します。

NTP サービスを有効にします。

```
<Switch> system-view
[Switch] ntp-service enable
```

Switch で NTP 認証を有効にします。

```
[Switch] ntp-service authentication enable
```

認証キーを設定し、プレーンテキストでキーを入力します。

```
[Switch] ntp-service authentication-keyid 42 authentication-mode md5 simple aNiceKey
```

キーをトラステッドキーとして指定します。

```
[Switch] ntp-service reliable authentication-keyid 42
```

Switch の NTP サーバとして Device A を指定し、キーID を 42 としてサーバと関連づけます。

```
[Switch] ntp-service unicast-server 1.0.1.11 authentication-keyid 42
```

Switch が AC のクロックの同期を行う前に、AC の NTP 認証を有効にします。

4) AC で NTP 認証を設定します。

NTP 認証を有効にします。

```
[AC] ntp-service authentication enable
```

認証キーを設定し、プレーンテキストでキーを入力します。

```
[AC] ntp-service authentication-keyid 42 authentication-mode md5 simple aNiceKey
```

キーをトラステッドキーとして指定します。

```
[AC] ntp-service reliable authentication-keyid 42
```

III. 設定の確認

Switch が AC に同期化され、Switch の stratum レベルが 3 であることを確認します。

[Switch] display ntp-service status

```
 Clock status: synchronized
 Clock stratum: 3
 System peer: 1.0.1.11
 Local mode: client
 Reference clock ID: 1.0.1.11
 Leap indicator: 00
 Clock jitter: 0.005096 s
 Stability: 0.000 pps
 Clock precision: 2^-23
 Root delay: 0.00655 ms
 Root dispersion: 1.15869 ms
 Reference time: d0c62687.ab1bba7d  Wed, Dec 29 2010 21:28:39.668
```

Switch と AC 間で NTP アソシエーションが確立されていることを確認します。

[Switch] display ntp-service sessions

```
       source           reference        stra reach poll  now offset  delay
disper
**************************************************************************
**
 [1245]1.0.1.11         127.127.1.0         2     1    64  519   -0.0 0.0065
0.0
Notes: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured.
 Total sessions: 1
```

目次

このセクションのページは **3-x-x** です。

5章 Information Center 5-1
5.1 概要 5-1
5.1.1 ログタイプ 5-1
5.1.2 ログレベル 5-1
5.1.3 ログの出力先 5-2
5.1.4 デフォルト出力ルール 5-2
5.1.5 Diagnosticログのデフォルト出力ルール 5-2
5.1.6 hiddenログのデフォルト出力ルール 5-3
5.1.7 ログフォーマット 5-3
5.2 Information Center設定作業リスト 5-5
5.3 Information Centerの有効化 5-5
5.4 ログ出力プロファイルの設定 5-6
5.5 各種出力先へのログ出力 5-6
5.5.1 コンソールへのログの出力 5-6
5.5.2 モニタ端末へのログの出力 5-7
5.5.3 ログホストへのログの出力 5-7
5.5.4 ログバッファへのログの出力 5-8
5.5.5 ログファイルへのログの保存 5-9
5.6 ログの最小記録期間の設定 5-10
5.7 情報の同期出力の設定 5-10
5.8 インタフェースでのリンクアップ/ダウンのログ情報生成の無効化 5-11
5.9 ログメッセージのSNMP notificationの送信の有効化 5-11
5.10 キープアライブログ送信の設定の有効化 5-12
5.11 Information Centerの表示と維持 5-12
5.12 設定例 5-13
5.12.1 コンソールへのログ出力の設定例 5-13
5.12.2 UNIXログホストへのログ出力の設定例 5-14
5.12.3 Linuxログホストへのログ出力の設定例 5-15

5章 Information Center

5.1 概要

Information Center は、送信元モジュールによって作成されたログを受信し、ユーザが定義した出力ルールに従って、異なる宛先にログを出力します。送信元モジュールに基づいて分類、フィルタリング、出力することができます。サポートされる送信元を表示するには、**info-center source ?**コマンドを使用します。

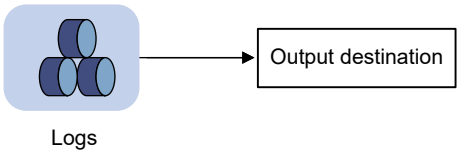


図 5-1 Information center の図

デフォルトで Information Center は有効です。Information Center が有効な場合、情報の分類や出力のため、システム性能にある程度影響を与えます。システムリソースが不十分である場合、リソースの消費を防ぐため Information Center を無効にしてください。

5.1.1 ログタイプ

ログは以下のタイプに分類されます。

- **Common ログ** － 共通なシステム情報の記録です。本章では、特に指定がない場合、ログは Common ログを示します。
- **Diagnostic ログ** － デバッグメッセージ記録です。
- **Hidden ログ** － 入力コマンドのような端末で表示されないログ情報です。
- **Custom ログ** － ベンダ固有情報の記録です。

5.1.2 ログレベル

ログは重要度により 0～7 の 8 つのレベルに分類されます。装置は指定されたレベル以上の重要度レベルを出力します。たとえば出力ルールを 6（informational）と設定した場合、0～6 までの重要度のログが出力されます。

表 5-1 ログレベル

重要度	レベル	説明
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。
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。

重要度	レベル	説明
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。
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。
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。
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。
6	Informational	情報メッセージです。たとえば、コマンドあるいはpingが実行されました。
7	Debugging	デバッグメッセージです。

5.1.3 ログの出力先

システムは、コンソール、モニタ端末、ログバッファ、ログホスト、ログファイルの宛先にログを出力します。ログの出力先は独立しており、Information Center を有効にした後、設定することができます。

5.1.4 デフォルト出力ルール

デフォルト出力ルールはログの送信元モジュールと出力先の重要度レベルを定義しています。出力ルールにマッチしたログが、出力先に出力されます。表 5-2にデフォルト出力ルールを示します。

表 5-2 デフォルト出力ルール

出力先	ログ送信元モジュール	出力装置	重要度
コンソール	サポートされるすべてのモジュール	有効	Debugging
モニタ端末	サポートされるすべてのモジュール	無効	Debugging
ログホスト	サポートされるすべてのモジュール	有効	Informational
ログバッファ	サポートされるすべてのモジュール	有効	Informational
ログファイル	サポートされるすべてのモジュール	有効	Informational

5.1.5 Diagnostic ログのデフォルト出力ルール

Diagnostic ログは Diagnostic ログファイルにのみ出力することができます。送信元モジュールと重要度でフィルタすることはできません。表 5-3に Diagnostic ログのデフォルト出力ルールを示します。

表 5-3 Diagnostic ログのデフォルト出力ルール

出力先	ログ送信元モジュール	出力装置	重要度
Diagnosticログファイル	サポートされるすべてのモジュール	有効	Debugging

5.1.6 hidden ログのデフォルト出力ルール

Hidden ログはログホスト、ログバッファ、ログファイルに出力することができます。表 5-4 に hidden ログのデフォルト出力ルールを示します。

表 5-4 hidden ログのデフォルト出力ルール

出力先	ログ送信元モジュール	出力装置	重要度
ログホスト	サポートされるすべてのモジュール	有効	Informational
ログバッファ	サポートされるすべてのモジュール	有効	Informational
ログファイル	サポートされるすべてのモジュール	有効	Informational

5.1.7 ログフォーマット

ログのフォーマットは出力先で異なります。表 5-5にログ情報の標準のログフォーマットを示します。このフォーマットは使用するツールによって異なります。

表 5-5 ログフォーマット

出力先	フォーマット	例
コンソール、モニタ端末、ログバッファ、ログファイル	Prefix Timestamp Sysname Module/Level/Mnemonic: Content	%Nov 24 14:21:43:502 2010 Sysname SHELL/5/SHELL_LOGIN: VTY logged in from 192.168.1.26
ログホスト	<PRI>Timestamp Sysname %%vvModule/Level/Mnemonic: Source; Content	<190>Nov 24 16:22:21 2010 Sysname %%10SYSLOG/6/SYSLOG_RESTART: -DevIP=1.1.1.1; System restarted ?-

表 5-6にログメッセージのフィールドの説明を示します。

表 5-6 ログフィールドの説明

フィールド	説明
Prefix (information type)	ログホスト以外の宛先へのログはタイムスタンプの前識別子があります。 ● パーセントの識別子（%）はinformational以上のレベルのログを示しています。 ● アスタリスク（*）の識別子はデバッグログを示します。 ● アスタリスク（^）の識別子はdiagnosticログを示します。

フィールド	説明
PRI (priority)	ログホストへのログはタイムスタンプの前にプライオリティの識別子があります。プライオリティは、facility*8+levelという式で計算されます。 ● **facility**はロギングファシリティ名です。16～23の値に対応したファシリティ名はlocal0～local7です。**info-center loghost**コマンドで設定されます。ログホストでログのソースを識別するのに使われます。対応するログソースのログをクエリやフィルタするのに使用します。 ● **level**は重要度（Severity）の範囲で0～7です。表 5-1に詳細を示します。
Timestamp	ログが作成されたときの時間を記録します。 ログホストとほかの宛先に送信したログは、異なる精度のタイムスタンプを持ちます。タイムスタンプのフォーマットは異なるコマンドで設定されます。詳細を表 5-7と表 5-8に示します。
Sysname （ホスト名あるいはホストのIPアドレス）	Sysnameはログが作成された装置のホスト名あるいはIPアドレスです。装置の名前を修正する場合は**sysname**コマンドを使用します。
%% (vendor ID)	このフィールドは、ベンダを識別するために使用します。出力先がログホストである場合のみ表示されます。
vv (version information)	このフィールドは、ログのバージョン識別子で、値は10です。出力先がログホストである場合のみ表示されます。
Module	このフィールドは、システム情報を作成するモジュールの名前を示します。system viewで**info-center source ?** コマンドを入力すると、モジュールの一覧を参照できます。
Level	ログのレベルを識別します。表 5-1に重要度のレベルの詳細を示します。
Mnemonic	ログの概要が記載されます。最大32文字の文字列です。
Source	ログの送信元を識別します。下記の値を含みます。 ● ログの送信者のIPアドレス
Content	ログの内容が記載されます。

表 5-7 タイムスタンプの精度と設定コマンド

アイテム	ログホスト	コンソール、モニタ端末、ログバッファ、ログファイル
精度	秒	ミリ秒
設定コマンド	**info-center timestamp loghost**	**info-center timestamp**

表 5-8 タイムスタンプパラメータの内容

パラメータ	内容	例
boot	時間はシステムが開始してからのミリ秒で記載された経過時間です。フォーマットはxxx.yyyです。xxxは上位32ビットでyyyは下位32ビットです。 ログホストを除いたすべての宛先に送信される出力先のログでサポートされます。	%0.109391473 Sysname FTPD/5/FTPD_LOGIN: User ftp (192.168.1.23) has logged in successfully. 0.109391473は**boot**フォーマットのタイムスタンプです。

パラメータ	内容	例
date	ログホストに出力されるログの現在日時と時間です。フォーマットはmmm dd hh:mm:ss yyyです。あるいはほかの宛先に出力されるログの現在日時と時間です。フォーマットはMMM DD hh:mm:ss:xxx YYYYです。 すべてのログでサポートされます。	%May 30 05:36:29:579 2019 Sysname FTPD/5/FTPD_LOGIN: User ftp (192.168.1.23) has logged in successfully. May 30 05:36:29:579 2019は**date**フォーマットのタイムスタンプです。
iso	ISO 8601で規定されたタイムスタンプです。ログホストへ送付するログのみサポートします。	<189>2019-05-30T06:42:44 Sysname %%10FTPD/5/FTPD_LOGIN(l): User ftp (192.168.1.23) has logged in successfully. 2019-05-30T06:42:44は**iso**フォーマットのタイムスタンプです。
none	タイムスタンプが含まれていません。 すべてのログでサポートされます。	% Sysname FTPD/5/FTPD_LOGIN: User ftp (192.168.1.23) has logged in successfully. タイムスタンプが含まれません
no-year-date	年またはミリ秒を除いた現在日付と時間です。フォーマットはMMM DD hh:mm:ssです。ログホストに送信されるログのみでサポートされます。	<189>May 30 06:44:22 Sysname %%10FTPD/5/FTPD_LOGIN: User ftp (192.168.1.23) has logged in successfully. May 30 06:44:22は**no-year-date**フォーマットのタイムスタンプです。

5.2 Information Center設定作業リスト

作業リスト
（必須設定項目）Information Centerの有効化
（オプション設定項目）ログ出力プロファイルの設定
（必須設定項目）各種出力先へのログ出力 以下の少なくとも1つの作業を実行します。 • コンソールへのログの出力 • モニタ端末へのログの出力 • ログホストへのログの出力 • ログバッファへのログの出力 • ログファイルへのログの保存
（オプション設定項目）ログの最小記録期間の設定
（オプション設定項目）情報の同期出力の設定
（オプション設定項目）インタフェースでのリンクアップ/ダウンのログ情報生成の無効化
（オプション設定項目）ログメッセージのSNMP notificationの送信の有効化

5.3 Information Centerの有効化

Information Center は有効化された後にのみログを出力できます。

以下に Information Center の有効化を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. Information Center を有効にする	**info-center enable**	デフォルト：有効

5.4 ログ出力プロファイルの設定

ログ出力プロファイルを作成してログホストにバインドした後、カプセル化形式、文字セットエンコーディング、タイムスタンプ形式、装置シリアル番号のログへの組み込みなど、ログホストのログ出力パラメータをカスタマイズできます。

ログ出力プロファイルは、宛先にバインドされている場合にのみ有効になります。現在、バインディングログ出力プロファイルをサポートしているログホストのみです。

以下にログ出力プロファイルの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. ログのタイムスタンプを設定する	**timestamp** { **date** [**with-milliseconds**] | **iso** [**with-milliseconds** | **with-timezone**] * | **no-year-date** | **none** }	デフォルト：**date**
3. ログの文字セットエンコーディングを指定する	**character-set** { **gb18030** | **utf-8** }	デフォルト：GB 18030

5.5 各種出力先へのログ出力

5.5.1 コンソールへのログの出力

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. コンソールへのログの出力ルールを設定する	**info-center source** { *module-name* | **default** } { **console** | **monitor** | **logbuffer** | **logfile** | **loghost** } { **deny** | **level** *severity* }	デフォルト出力ルールについての詳細は、本章の *"デフォルト出力ルール"* を参照してください。
3. （オプション設定項目）タイムスタンプのフォーマットを設定する	**info-center timestamp** { **boot** | **date** | **none** }	デフォルト：**date**
4. user view に戻る	**quit**	ー
5. （オプション設定項目）コンソールへのログの出力を有効にする	**terminal monitor**	デフォルト：コンソールでは有効、モニタ端末では無効です。

操作	コマンド	補足
6. 現在の端末でデバッグ情報の表示を有効にする	**terminal debugging**	デフォルト：無効 このコマンドは、コンソールへのデバッグ レベルのログメッセージの出力を有効にします。
7. （オプション設定項目）コンソールに出力されるログの重要度を設定する	**terminal logging level** *severity*	デフォルト：6（informational）

5.5.2 モニタ端末へのログの出力

AUX、VTY、TTY line を通して装置にログインしているモニタ端末です。

以下にモニタ端末へのログ出力の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. モニタ端末へのログの出力ルールを設定する	**info-center source** { *module-name* | **default** } { **console** | **monitor** | **logbuffer** | **logfile** | **loghost** } { **deny** | **level** *severity* }	デフォルト出力ルールについての詳細は、本章”の“*デフォルト出力ルール*”を参照してください。
3. （オプション設定項目）タイムスタンプのフォーマットを設定する	**info-center timestamp** { **boot** | **date** | **none** }	デフォルト：**date**
4. user view に戻る	**quit**	ー
5. モニタ端末へのログの出力を有効にする	**terminal monitor**	デフォルト：コンソールでは有効、モニタ端末では無効です。
6. 現在の端末でデバッグ情報の表示を有効にする	**terminal debugging**	デフォルト：無効 このコマンドは、モニタ端末へのデバッグ レベルのログメッセージの出力を有効にします。
7. （オプション設定項目）モニタ端末に出力されるログの重要度を設定する	**terminal logging level** *severity*	デフォルト：6（informational）

5.5.3 ログホストへのログの出力

操作	コマンド	補足
1. system view に移行する	**system-view**	ー

操作	コマンド	補足
2. ログホストへのログの出力ルールを設定する	**info-center source** { *module-name* **| default** } { **console | monitor | logbuffer | logfile | loghost** } { **deny | level** *severity* }	デフォルト出力ルールについての詳細は、本章の *"デフォルト出力ルール"* を参照してください。 システムは、ログホストへのログ出力を制御する設定を以下の順序で選択します。 a. ログホストに適用されるログ出力フィルタ。 b. **info-center source** コマンドを使用して、ログホストの出力先に設定されたログ出力ルール。
3. （オプション設定項目）出力ログの送信元 IP アドレスを指定する	**info-center loghost source** *interface-type interface-number*	デフォルト：ルータの出力インタフェースにマッチするプライマリIPアドレスです。
4. （オプション設定項目）タイムスタンプのフォーマットを設定する	**info-center timestamp loghost** { **date** [**with-milliseconds**] | **iso** [**with-milliseconds** | **with-timezone**] * | **no-year-date** | **none** }	デフォルト：**date**
5. ログホストを指定し、関連するパラメータを設定する	**info-center loghost** { *hostname* | *ipv4-address* } [**port** *port-number*] [**dscp** *dscp-value*] [**facility** *local-number*] [**filter** *filter-name*]	デフォルト：設定なし *port-number*引数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。異なる場合ログを受信できません。 装置は最大20のログホストをサポートします。

5.5.4 ログバッファへのログの出力

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. ログバッファの出力ルールを設定する	**info-center source** { *module-name* **| default** } { **console | monitor | logbuffer | logfile | loghost** } { **deny | level** *severity* }	デフォルト出力ルールについての詳細は、本章の *"デフォルト出力ルール"* を参照してください。
3. （オプション設定項目）タイムスタンプのフォーマットを設定する	**info-center timestamp** { **boot** | **date** | **none** }	デフォルト：**date**
4. ログバッファへの出力を有効にする	**info-center logbuffer**	デフォルト：有効
5. （オプション設定項目）ログバッファに保存できるバッファサイズの最大数を設定する	**info-center logbuffer size** *buffersize*	デフォルト：512

5.5.5 ログファイルへのログの保存

ログファイル機能により、ログファイルへのログ出力が可能になります。ログファイル機能により、ログファイルバッファからログファイルにログが保存されます。ログファイルにログを保存した後、システムはログファイルバッファをクリアします。

ログファイルバッファからログファイルへのログの保存は、次のいずれかの条件を満たした場合に実行されます。

- 指定した保存間隔が経過した場合
- 手動で即時保存を実行した場合
- ログファイルバッファが記録上限に達した場合

ログファイルは必要に応じて自動的に作成され、最大容量があります。ログファイルの容量制限は次のとおりです。

- 装置に使用可能なストレージ容量がない場合、または装置にストレージ容量があるがログファイルの空き容量がない場合、システムは最も古いログを新しいログに置き換えます。

以下に、ログファイルへのログの保存の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. ログファイルの出力ルールを設定する	**info-center source** { *module-name* | **default** } { **console** | **monitor** | **logbuffer** | **logfile** | **loghost** } { **deny** | **level** *severity* }	デフォルト出力ルールについての詳細は、本章の *"デフォルト出力ルール"* を参照してください。
3. ログファイル機能を有効にする	**info-center logfile enable**	デフォルト：有効
4. （オプション設定項目）ログファイルの最大記憶容量を設定する	**info-center logfile size-quota** *size*	デフォルト: ログ ファイルの最大サイズは 10 MB です。
5. （オプション設定項目）ログファイルを保存するディレクトリを指定する	**info-center logfile directory** *dir-name*	デフォルト：**flash:/logfile** 再起動を行うと設定は消去されます。
6. ログファイルにログファイルバッファのログを保存する	• ログファイルを記録する間隔を設定する：**info-center logfile frequency** *freq-sec* • 手動でログファイルを記録する：**logfile save**	デフォルト: ログファイルを記録する間隔は86400秒です。 すべてのviewで**logfile save**コマンドを実行できます。

🕮 **メモ：**

- **info-center logfile frequency** コマンドでログファイルをセーブする周期を著しく短くした場合、フラッシュメモリの書き込み可能回数の超過や、装置動作に影響を与える恐れがあります。したがって、通常はデフォルト値での使用を推奨します。
- ログファイルのサイズは、フラッシュメモリの空き容量を超えない範囲で設定する必要があります。通常はデフォルト値で使用することを推奨します。**info-center logfile size-quota** コマンドで設定を変更する場合、フラッシュメモリの空き容量を **dir** コマンドで確認してください。

5.6 ログの最小記録期間の設定

ログバッファにあるログの記録期間の最小値を設定することができます。この機能はログが指定した時間内のログが、新しいログによって上書きされることを防ぎます。

デフォルトでは、ログバッファあるいはログファイルが一杯になると、新しいログによって最も古いログが上書きされます。最小記録期間を設定した場合、システムはログを削除するかどうか決定するために、各ログの記録期間を確認します。システムクロックからログの発生時刻を引いた時間がログの記録期間となります。削除できるログがない場合、新しいログは保存されずに破棄されます。

- ログの記録期間が最小記録期間以下である場合、システムはそのログを削除しません。
- ログの記録期間が最小記録期間を超えている場合、システムはそのログを削除し、新しいログを保存します。

以下にログの最小記録期間の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. ログの最小記録期間を設定する	**info-center syslog min-age** *min-age*	デフォルト：設定なし

5.7 情報の同期出力の設定

システムログの出力が行われると設定の操作が中断されます。ログが出力される前に、以前に入力されたコマンドを見つける必要があります。

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するため、ログの出力後、以前に入力されたコマンドおよび、コマンドプロンプト（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）を表示させることができます。

以下に情報の同期出力の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. 情報の同期出力を設定する	**info-center synchronous**	デフォルト：無効

5.8 インタフェースでのリンクアップ/ダウンのログ情報生成の無効化

デフォルトでは、インタフェースのリンク状態が変わるときに、装置のすべてのインタフェースはリンクアップ/ダウンのログ情報を生成します。そのため、以下のような場合、指定したインタフェースの情報生成を無効にすることができます。

インタフェースの情報を監視するため、通常はデフォルトの有効にすることを推奨します。

- あるインタフェースの状態にのみ関係している場合です。この場合、ほかのインタフェースのリンクアップ/ダウンのログ情報を生成できないようにします。
- インタフェースのリンク状態が安定せず、不必要なログ情報が連続して生成される場合です。この場合、ほかのインタフェースのリンクアップ/ダウンのログ情報を生成できないようにします。

以下にインタフェースのリンクアップ/ダウンのログ情報の生成を無効の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. interface view に移行する	**interface** *interface-type interface-number*	―
3. インタフェースのリンクアップ/ダウンのログ情報の生成を無効にする	**undo enable log updown**	デフォルト : すべてのインタフェースは、インタフェースの状態が変化したとき、リンクアップ/ダウンのログ情報を生成します。

5.9 ログメッセージのSNMP notificationの送信の有効化

snmp-agent trap enable syslog コマンドを有効にすると、装置はシスログメッセージによる SNMP notification の送信を有効にします。

装置は SNMP notification をカプセル化し、SNMP モジュールとログバッファに送信します。

SNMP モジュールが受信した SNMP notification を正常に送信するため、装置で SNMP の設定を行ってください。SNMP の設定については、オペレーションマニュアルのセクション 19 *ネットワーク管理と監視 “SNMP”* を参照してください。

以下にシスログメッセージによる SNMP notification の送信を有効化の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. ログメッセージの SNMP notification の送信を有効にする	**snmp-agent trap enable syslog**	デフォルト：無効

5.10 キープアライブログ送信の設定の有効化

🕮 **メモ：**

この機能は、ソフトウェアバージョン 9.6.05c を含む以降のソフトウェアからサポートしています。

この機能を有効にすると、装置は設定された全てのログホストに対して定期的にキープアライブログを送信します。

キープアライブログを定期的に受信することにより、装置の運用状態を確認できるようにします。

以下にキープアライブログ送信の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. キープアライブログの送信間隔を設定する	**info-center loghost keep-alive interval** *seconds*	デフォルト：60秒
3. キープアライブログのレベルを設定する	**info-center loghost keep-alive level** *severity*	デフォルト: informational (レベル6)
4. キープアライブログに含めるカスタム情報を設定する	**info-center loghost keep-alive custom-info** *text*	デフォルト：設定なし
5. キープアライブログの送信を有効にする	**info-center loghost keep-alive enable**	デフォルト： ソフトウェアバージョンにより異なります。 ソフトウェアバージョン 9.6.05dを含む以前のソフトウェアでは有効です。 ソフトウェアバージョン 9.6.08cを含む以降のソフトウェアでは無効です。

5.11 Information Centerの表示と維持

すべての view で **display** コマンドを実行でき、user view で **reset** コマンドを実行できます。

操作	コマンド
各出力先の情報を表示する	**display info-center**
ログバッファの状態とログ情報を表示する	**display logbuffer** [**reverse**] [**level** *severity* | **size** *buffersize*] *
ログバッファの概要を表示する	**display logbuffer summary** [**level** *severity*]
ログファイルの設定を表示する	**display logfile summary**
ログ ファイル バッファの内容を表示する	**display logfile buffer**
ログバッファを削除する	**reset logbuffer**

5.12 設定例

5.12.1 コンソールへのログ出力の設定例

I. ネットワーク要件

warning 以上の重要度のレベルの FTP ログをコンソールに出力するように設定します。

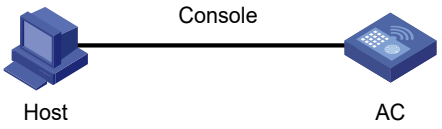


図 5-2 ネットワーク図

II. 設定手順

Information Center を有効にします。

```
<AC> system-view
[AC] info-center enable
```

コンソールへのログ出力を無効にします。

```
[AC] info-center source default console deny
```

それぞれのチャネルのデフォルトのシステム設定が異なるため、特定のチャネル（この例では **console**）では、必要に応じて、すべてのモジュールのログ情報の出力を無効にし、不要な情報が出力されないように出力ルールを設定します。

warning レベル以上の重要度の FTP ログをコンソールに出力するように設定します。

```
[AC] info-center source ftp console level warning
[AC] quit
```

コンソールでログの表示を有効にします。

```
<AC> terminal logging level 6
<AC> terminal monitor
The current terminal is enabled to display logs.
```

設定を行った後、FTP モジュールがログを生成した場合、Information Center は自動的にコンソールにログを送信し、ログを表示します。

5.12.2 UNIX ログホストへのログ出力の設定例

I. ネットワーク要件

AC が informational 以上の重要度のレベルの FTP ログを UNIX ログホストに出力するように設定します。



図 5-3 ネットワーク図

II. 設定手順

1) 設定を行う前に、AC とログホストが互いに通信可能であることを確認してください。（詳細は省略します。）
2) AC を設定します。

Information Center を有効にします。

```
<AC> system-view
[AC] info-center enable
```

ログホスト 1.2.0.1/16 を指定し、ロギングファシリティを **local4** に指定します。

```
[AC] info-center loghost 1.2.0.1 facility local4
```

ログホストへのログの出力を無効にします。

```
[AC] info-center source default loghost deny
```

不要な情報が出力されないようにするため、出力ルールを設定する前に、ログを出力するすべてのモジュールが、指定した宛先（この例では **loghost**）に出力しないようにします。

informational レベル以上の重要度の FTP ログをログホストに出力するように設定します。

```
[AC] info-center source ftp loghost level informational
```

3) ログホストを設定します。

ログホストの設定手順は、UNIX オペレーティング システムのベンダによって異なります。以下に例を示します。

a) rootユーザとしてログホストにログインします。

b) ディレクトリ/**var**/**log**/にサブディレクトリ**AC**を作成します。ディレクトリ**AC**にファイル**info.log**を作成し、**AC**からログを保存します。

```
# mkdir /var/log/AC
# touch /var/log/AC/info.log
```

c) ディレクトリ/**etc**/のファイル**syslog.conf**を編集し、以下の内容を追加します。

```
# AC configuration messages
local4.info /var/log/AC/info.log
```

この設定で、ホストがログを受信するために使用する **local4** はロギングファシリティの名前です。**info** は重要度のレベルです。UNIX システムは、**informational** の重要度のログ情報をファイル/**var/log/AC/info.log** に記録します。

🕮 **メモ：**

ファイル/**etc/syslog.conf** を編集するときのガイドラインを以下に示します。

- コメントは個別の行に記入し、# 記号で始めてください。
- ファイル名に不要なスペース等を入れないでください。
- ロギングファシリティ名とファイル/**etc/syslog.conf** が指定するログ情報の重要度は、**info-center loghost** コマンドと **info-center source** コマンドで AC に設定したものと一致しなければなりません。一致しないと、ログ情報は正しくログホストに出力されないことがあります。

---

d) **syslogd**のプロセスIDを表示して**syslogd**プロセスを強制終了し、-r オプション付きで**syslogd**を再起動し、新しい設定を有効にしてください。

```
# ps -ae | grep syslogd
147
# kill -HUP 147
# syslogd -r &
```

上記設定は、AC は関連するファイルに FTP ログ情報を保存できるようになります。

5.12.3 Linux ログホストへのログ出力の設定例

I. ネットワーク要件

AC が informational の重要度のレベルの FTP ログを Linux ログホスト 1.2.0.1/16 に出力するように設定します。



図 5-4 ネットワーク図

II. 設定手順

1) 設定を行う前に、AC とログホストが互いに通信可能であることを確認してください。（詳細は省略します。）
2) AC を設定します。

Information Center を有効にします。

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

```
[AC] info-center enable
```

ログホスト 1.2.0.1/16 を指定し、ロギングファシリティを **local5** に指定します。

```
[AC] info-center loghost 1.2.0.1 facility local5
```

ログホストにログの出力を無効にします。

```
[AC] info-center source default loghost deny
```

不要な情報が出力されないようにするため、出力ルールを設定する前に、ログを出力するすべてのモジュールが、指定した宛先（この例では **loghost**）に出力しないようにします。

informational レベル以上の重要度の FTP ログをログホストに出力するように設定します。

```
[AC] info-center source ftp loghost level informational
```

3)　ログホストを設定します。

ログホストの設定手順は、Linux オペレーティング システムのベンダによって異なります。以下に例を示します。

a)　rootユーザとしてログホストにログインします。

b)　ディレクトリ/**var**/**log**/にサブディレクトリACを作成します。ディレクトリACにファイル**info.log**を作成し、ACからログを保存します。

```
# mkdir /var/log/AC
# touch /var/log/ AC /info.log
```

c)　ディレクトリ/**etc**/のファイル**syslog.conf**を編集し、以下の内容を追加します。

```
# AC configuration messages
local5.info /var/log/AC/info.log
```

この設定で、ホストがログを受信するために使用する **local5** はロギングファシリティの名前です。**info** は重要度のレベルです。Linux システムは、**informational** の重要度のログ情報をファイル/**var**/**log**/**AC**/**info.log** に記録します。

🕮 **メモ：**

ファイル/**etc**/**syslog.conf** を編集するときのガイドラインを以下に示します。

- コメントは個別の行に記入し、# 記号で始めてください。
- ファイル名に不要なスペース等を入れないでください。
- ロギングファシリティ名とファイル/**etc**/**syslog.conf** が指定するログ情報の重要度は、**info-center loghost** コマンドと **info-center source** コマンドで AC に設定したものと一致しなければなりません。一致しないと、ログ情報は正しくログホストに出力されないことがあります。

---

d)　**syslogd**のプロセスIDを表示して**syslogd**プロセスを強制終了し、-r オプション付きで**syslogd**を再起動し、新しい設定を有効にしてください。

```
# ps -ae | grep syslogd
147
# kill -HUP 147
# syslogd -r &
```

上記設定は、AC は関連するファイルに FTP ログ情報を保存できるようになります。

QX-W2300AC シリーズ アクセスコントローラ

オペレーションマニュアル

4. 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
04-マネジメント Ethernet インタフェース

目次

このセクションのページは**4-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の設定 1-1
1.2 Nullインタフェースの設定 1-2
1.3 ループバックインタフェースとNULLインタフェースの表示と維持 1-2

1章 ループバックインタフェースと Null インタフェース

この章ではループバックインタフェースと Null インタフェースを設定する方法について記載します。

1.1 ループバックインタフェースの設定

ループバックインタフェースは、仮想的なインタフェースです。手動でコマンドによるシャットダウンをしない限り、ループバックインタフェースの物理レイヤ状態とリンクレイヤプロトコルは、常に UP しています。この利点によって以下のように広く使用されます。

- **装置が作成したパケットの送信元 IP アドレスとしてループバックアドレスの設定**
  - ループバックインタフェースアドレスは安定したユニキャストアドレスであるため、装置を識別するのに使用されます。
    - 認証ルールあるいはセキュリティサーバで、装置が作成したパケットの許可/禁止のルールを設定するとき、装置を識別するループバックインタフェースアドレスを送信元 IP アドレスとしたパケットを許可/禁止するようにルールを簡略化することができます。
    - ループバックインタフェースに IP アドレスを割り当て、送信元アドレスに使用した場合、ループバックインタフェースからピアまでのルートが届くことを確認してください。ループバックインタフェースに送信されるすべてのデータパケットは装置自体に送信されていると認識するため、装置はこのパケットを転送しません。
- **ダイナミックルーティングプロトコルのループバックインタフェースの使用** – ダイナミックルーティングプロトコル用にルータ ID を設定する際、ルータ ID として最も高いループバックインタフェースの IP アドレスを使用します。

description、**shutdown** コマンドの詳細は、QX-W2300AC シリーズアクセスコントローラコマンドマニュアルの“*4 インタフェース*”を参照してください。

以下にループバックインタフェースを設定する方法を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. ループバックインタフェースを作成し loopback interface view に移行する	**interface loopback** *interface-number*	—
3. ループバックインタフェースの説明を設定する	**description** *text*	デフォルト：*interface name* **Interface** (例 **LoopBack0 Interface**)
4. ループバックインタフェースを up にする	**undo shutdown**	デフォルト：up

1.2 Nullインタフェースの設定

NULL インタフェースは、論理的インタフェースで、常に UP しています。しかし、データパケットを転送したり、IP アドレスやリンクレイヤプロトコルを設定したりできません。NULL インタフェースをスタティックルートのネクストホップとして具体的なネットワークセグメントに指定した場合、ネットワークセグメントに送信されたパケットはすべて破棄されます。したがって、ACL を適用する代わりにパケットを NULL インタフェースに送信することで、不要なトラフィックをフィルタすることができます。

description コマンドの詳細は、QX-W2300AC シリーズアクセスコントローラコマンドマニュアルの“*4 インタフェース*”を参照してください。

以下に NULL インタフェースを設定する方法を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． null interface view に移行する	**interface null 0**	NULL 0インタフェースはデフォルト固定です。 NULLインタフェースは装置に一つだけサポートしています。NULLインタフェースは削除、作成することはできません。
3． NULL インタフェースの説明を設定する	**description** *text*	デフォルト：NULL0 Interface

1.3 ループバックインタフェースとNULLインタフェースの表示と維持

すべての view で **display** コマンドを実行し、user view で **reset** コマンドを実行できます。

操作	コマンド
指定したあるいはすべてのループバックインタフェースの情報を表示する	**display interface loopback** [*interface-number*] [**brief** [**description** | **down**]]
NULLインタフェースを表示する	**display interface null** [**0**] [**brief** [**description** | **down**]]
指定したあるいはすべてのループバックインタフェースの情報を削除する	**reset counters interface loopback** [*interface-number*]
NULLインタフェースを削除する	**reset counters interface null** [**0**]

目次

このセクションのページは**4-x-x** です。

2章 Ethernetインタフェース 2-1
2.1 Ethernetインタフェースの共通設定 2-1
2.1.1 Ethernetインタフェースの基本設定 2-1
2.1.2 ジャンボフレームの設定 2-2
2.1.3 Ethernetインタフェースのループバックテストの実行 2-2
2.1.4 統計情報のポーリング間隔の設定 2-3
2.1.5 ストーム抑制の設定 2-3
2.2 Ethernetインタフェースの表示および維持 2-4

2章 Ethernet インタフェース

装置は Ethernet インタフェース、コンソールインタフェースをサポートしています。サポートするインタフェースタイプと番号は、装置の種類により異なります。インタフェースタイプと番号については、*インスタレーションマニュアル*を参照してください。

この章では Ethernet インタフェースの設定方法について記載します。

2.1 Ethernetインタフェースの共通設定

2.1.1 Ethernet インタフェースの基本設定

Ethernet インタフェースは以下の通信モードの 1 つをサポートします。

- **全 2 重モード**－インタフェースはパケットを同時に送受信することができます。
- **半 2 重モード**－インタフェースはパケットを送受信のどちらか一方のみ行うことができます。
- **オートネゴシエーションモード**－インタフェースはピアと通信モードをネゴシエーションします。

Ethernet インタフェースは通信速度を設定することができ、ピアと通信速度を自動でネゴシエーションすることができます。

description、**shutdown** コマンドの詳細は、QX-W2300AC シリーズ アクセスコントローラコマンドマニュアルの“*4 インタフェース*”を参照してください。

speed 10000 コマンドをサポートするのは、EWPXM3XG03 拡張カードの Ethernet インタフェースだけです。

I. Ethernet インタフェースの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． Ethernet interface view に移行する	**interface** *interface-type interface-number*	―
3． 説明を設定する	**description** *text*	デフォルト：*interface-name* **Interface** たとえば“GigabitEthernet 1/0/1 Interface”です。
4． 通信モードを設定する	**duplex** { **auto** | **full** | **half** }	デフォルト：auto 1000BASE-Tを含むSFPトランシーバモジュールで動作するポート、1000Mbpsで動作するRJ-45ポートは、halfパラメータが未サポートです。
5． 通信速度を設定する	**speed** { **100** | **1000** | **10000** | **auto** }	デフォルト：auto
6． Ethernet インタフェースを有効にする	**undo shutdown**	デフォルト：up

2.1.2 ジャンボフレームの設定

Ethernet インタフェースは、ファイル転送のような高スループットのデータ交換において、標準の Ethernet フレームサイズよりも大きいフレームを受信する場合があります。これらのフレームはジャンボフレームと呼ばれます。

Ethernet インタフェースは、ジャンボフレームを以下の方法で処理します。

- Ethernet インタフェースでジャンボフレームの設定が無効（**undo jumboframe enable** コマンド）にされているとき、ジャンボフレームの処理を行わないで廃棄します。
- Ethernet インタフェースでジャンボフレームの設定が行われているとき、以下の処理を行います。
  - 指定したフレーム長でジャンボフレームを処理します。
  - 指定したフレーム長を超過したフレームは処理を行わないで廃棄します。

以下にジャンボフレームを設定する手順を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. Ethernet interface view に移行する	**interface** *interface-type interface-number*	—
3. ジャンボフレームを設定する	**jumboframe enable** [*size*]	デフォルト：4000バイト

2.1.3 Ethernet インタフェースのループバックテストの実行

注意：

インタフェースでループバックテストを有効にした場合、インタフェースはトラフィックデータを転送しません。

Ethernet リンクが正常に動作しているかを確認するために、本テストを実施します。

ループバックテストは以下のタイプに分けられます。

- **内部ループバックテスト** － Ethernet インタフェースに関連したスイッチングチップ内にあるすべての機能のテストを実行します。
- **外部ループバックテスト** － Ethernet インタフェースのハードウェアのテストを行います。外部ループバックテストを行うため、インタフェースにループバックプラグを挿入します。外部ループバックテストを行っている間、インタフェースはテストパケットを送信します。そこでプラグで折り返してインタフェースにループします。もしインタフェースがテストパケットを受信しない場合、インタフェースのハードウェアが故障しています。

I. 設定の制限とガイドライン

- **shutdown** および **loopback** コマンドは同時に設定することはできません。
- ループバックテスト実行中、Ethernet インタフェースは全二重モードで動作します。テスト終了後はもとの設定で動作します。

II. 設定手順

以下に Ethernet インタフェースのループバックテストの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Ethernet interface view に移行する	**interface** *interface-type interface-number*	―
3. ループバックテストを実行する	**loopback** { **external** | **internal** }	デフォルト : ループバックテストは実行されません。

2.1.4 統計情報のポーリング間隔の設定

統計情報ポーリング間隔を設定することで、パケットの統計情報を収集し、指定した間隔でパケットを分析できます。インタフェース トラフィック 統計情報をベースに、ネットワークの輻輳やサービスの中断を避けるためのトラフィック制御対策を迅速に行うことができます。

- ネットワークの輻輳が検出された場合、統計情報ポーリング間隔を 300 秒 (輻輳が悪化した場合は 30 秒) 未満に設定できます。その後、短時間でインタフェースのトラフィック分布を確認します。輻輳の原因となるデータパケットについては、トラフィック制御対策を講じます。
- ネットワーク帯域幅が十分で、サービスが正常に動作している場合は、統計情報ポーリング間隔を 300 秒より大きく設定できます。トラフィックパラメータの異常が発生したら、トラフィックパラメータの傾向をリアルタイムで観察できるように、統計情報ポーリング間隔を迅速に変更します。

最後の統計情報ポーリング間隔で収集されたインタフェース 統計情報を表示するには、**display interface** コマンドを使用します。インタフェース 統計情報を削除するには、**reset counters interface** コマンドを使用します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Ethernet interface view に移行する	**interface** *interface-type interface-number*	―
3. 統計情報のポーリング間隔を設定する	**flow-interval** *interval*	デフォルト : 300秒

2.1.5 ストーム抑制の設定

🕮 **メモ :**

この機能はソフトウェアバージョン 9.4.09 を含む以降のソフトウェアからサポートしています。

ストーム抑制機能を使用すると、特定タイプのトラフィック (ブロードキャスト、マルチキャスト、または未知のユニキャストトラフィック)のサイズがインタフェース上のしきい値を超えなくなります。インタフェース上のブロードキャスト、マルチキャスト、または未知のユニキャストトラフィックがこのしきい値を超えると、システムはトラフィックがこのしきい値を下回るまでパケットを廃棄します。

I. 設定の制限とガイドライン

pps または kbps で構成された抑制しきい値は、チップでサポートされているステップ値の倍数に変換される場合があります。その結果、有効な抑制しきい値が構成されているものと異なる場合があります。有効になる抑制しきい値については、装置のプロンプトを参照してください。

II. 設定手順

以下にストーム抑制の設定方法を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Ethernet interface view に移行する	**interface** *interface-type interface-number*	―
3. ブロードキャスト抑制を有効にし、ブロードキャスト抑制閾値を設定する	**broadcast-suppression** { *ratio* | **pps** *max-pps* | **kbps** *max-kbps* }	デフォルト：無効
4. マルチキャスト抑制を有効にし、マルチキャスト抑制閾値を設定する	**multicast-suppression** { *ratio* | **pps** *max-pps* | **kbps** *max-kbps* }	デフォルト：無効
5. 未知のユニキャスト抑制を有効にし、未知のユニキャスト抑制閾値を設定する	**unicast-suppression** { *ratio* | **pps** *max-pps* | **kbps** *max-kbps* }	デフォルト：無効

2.2 Ethernetインタフェースの表示および維持

すべての view で **display** コマンドを実行し、user view で **reset** コマンドを実行できます。

操作	コマンド
インタフェースのトラフィック統計情報を表示する	**display counters** { **inbound** | **outbound** } **interface** [*interface-type* [*interface-number*]]
最後のサンプリング間隔からのトラフィックレートの統計情報を表示する	**display counters rate** { **inbound** | **outbound** } **interface** [*interface-type* [*interface-number*]]
指定されたEthernetインタフェースあるいは全インタフェースの動作情報とステータス情報を表示する	**display interface** [**interface-type** [*interface-number*]] [**brief** [**description | down**]]
インタフェースの統計情報を削除する	**reset counters interface** [*interface-type* [*interface-number*]]

目次

このセクションのページは**4-x-x** です。

3章 Interface range 3-1
3.1 設定ガイドライン 3-1
3.2 設定手順 3-2
3.3 表示と維持 3-2

3章 Interface range

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にまとめて設定することができます。たとえば、複数のインタフェースをまとめてシャットダウンする場合、interface range view で **shutdown** コマンドを実行します。

interface range でインタフェースを設定するとき、**interface range** コマンドあるいは **interface range name** コマンドを使用して interface range を設定し、その view に移行する必要があります。

interface range コマンドを使用して設定した場合、interface range で指定した各インタフェースに反映されます。**interface range name** コマンドでは、繰り返し interface range を使用することはできません 。繰り返し設定する場合は、**interface range name** コマンドを使用します。

3.1 設定ガイドライン

interface range view で interface range を使用する際は、以下の点に注意してください。

- interface range view では、**interface range** コマンドで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有効です。
- **interface range** コマンドでインタフェースを設定する前に、**interface** *interface-type interface-number* コマンドで、そのインタフェースの view に移行できることを確認してください。
- リンクアグリゲーションのアグリゲートインタフェースとメンバポートを同じ interface range に設定しないでください。設定した場合、あるコマンドによってリンクアグリゲーションが失敗することがあります。
- interface range のインタフェースの最大数はシステムリソースに依存します。interface range でのインタフェースが多くなれば、実行時間も長くなります。interface range name を 1000 個以上の作成しないでください。
- interface range view でコマンドを実行した後、以下の状態のいずれか 1 つが発生することがあります。
  - システムがエラーメッセージを表示し、interface range view にとどまります。これは 1 つ以上のメンバインタフェースで実行が失敗したことを示します。
    - 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コマンドの実行に失敗した場合、他のメンバインタフェースで実行されません。
    - 最初に指定したインタフェースではないインタフェースで、コマンドの実行に失敗した場合、残りのメンバインタフェースでコマンドが適用されます。
  - システムが interface range view に移行します。以下のことを示します。
    - コマンドは system view と interface range view でサポートされます。
    - interface range view のメンバインタフェースでコマンドの実行に失敗した場合、システムは system view でコマンドを実行します。
    - システムは後続のメンバインタフェースでコマンドを実行しません。

各メンバインタフェースの interface view の設定を確認する場合、**display this** コマンドを使用することができます。また system view の設定が必要でない場合、**undo** コマンドで設定を削除することができます。

3.2 設定手順

Interface range の設定をするには以下の手順に従ってください。

操作	コマンド	補足
1． system view へ移行する	**system-view**	–
2． Interface range view へ移行する	• **interface range** { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-5> • **interface range name** *name* [**interface** { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-5>]	**interface range name**コマンドを使用すると interface rangeに名前を割り当てることができます。そしてinterface range viewに移行するためにinterface rangeを入力する代わりに名前を指定することができます。
3． （オプション設定項目）最初に指定したインタフェースで有効なコマンドを表示する	Interface range viewで”?”を入力する	―
4． インタフェースに設定を行う	有効なコマンドはインタフェースによって異なります。	―
5． （オプション設定項目）設定を確認する	**display this**	―

3.3 表示と維持

すべての view で **display** コマンドを実行します。

操作	コマンド
インタフェースレンジの情報を表示する	**display interface range** [**name** *name*]

目次

このセクションのページは **4-x-x** です。

4 章 マネジメント Ethernet インタフェース 4-1
4.1 マネジメント Ethernet インタフェース 4-1
4.1.1 マネジメント Ethernet インタフェースの基本設定 4-1

4章 マネジメント Ethernet インタフェース

4.1 マネジメントEthernetインタフェース

マネジメント Ethernet インタフェースは RJ-45 コネクタを使用します。PC に接続し、ソフトウェアのダウンロードやデバッグを行うために、接続します。またリモートからのシステム管理のために NMS に接続することができます。

マネジメント Ethernet インタフェースの詳細は、*QX-W2300AC シリーズ アクセスコントローラ インスタレーションマニュアル*を参照してください。

4.1.1 マネジメント Ethernet インタフェースの基本設定

マネジメント Ethernet インタフェースは、以下のように動作します。

- クラウドクラスタスタックに複数のマネジメント Ethernet インタフェースがある場合マスタ装置のマネジメント Ethernet インタフェースのみがマネジメントトラフィックを処理します。
- マスタ装置のマネジメント Ethernet インタフェースが故障した場合、メンバ装置のマネジメント Ethernet インタフェースはマネジメントトラフィックの処理を行います。
- マネジメント装置のマネジメント Ethernet インタフェースが回復した場合、マスタ装置が再度、マネジメントトラフックの処理を行います。
- マネジメント Ethernet インタフェースを使用して、AP との CAPWAP 接続はできません。

以下に、マネジメント Ethernet インタフェースの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． management Ethernet interface view に移行する。	**interface M-GigabitEthernet** *interface-number*	—
3． (オプション設定項目) インタフェースの説明を設定する	**description** *text*	デフォルト：設定なし
4． (オプション設定項目) 通信モードを設定する	**duplex { auto | full | half }**	デフォルト：auto
5． (オプション設定項目) 通信速度を設定する	**speed { 10 | 100 | 1000 | auto }**	デフォルト：auto
6． マネジメント Ethernet インタフェースを有効にする	**undo shutdown**	デフォルト：up

QX-W2300AC シリーズ アクセスコントローラ

オペレーションマニュアル

5. ネットワーク接続

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-リンクアグリゲーション

03-VLAN

04-ループ検出

05-STP

06-LLDP

07-レイヤ 2 フォワーディング

08-ARP

09-Gratuitous ARP

10-Proxy ARP

11-IP アドレス

12-DHCP 概要

13-DHCP サーバ

14-DHCP リレー

15-DHCP クライアント

16-BOOTP クライアント

17-DHCP スヌーピング

18-DNS

19-HTTP

20-IP パフォーマンスの最適化

21-NAT

22-IP ルーティングの基本

23-スタティックルーティング

24-デフォルトルーティング

25-マルチキャストの概要

26-IGMP スヌーピング

目次

このセクションのページは**5-x-x**です。

1章 MACアドレステーブル 1-1
1.1 概要 1-1
1.1.1 MACアドレスエントリの作成方法 1-1
1.1.2 MACアドレスエントリのタイプ 1-2
1.2 MACアドレス設定作業リスト 1-2
1.3 MACアドレスエントリの設定 1-3
1.3.1 設定ガイドライン 1-3
1.3.2 グローバルでのスタティック/ダイナミックMACアドレスエントリの追加/修正 .. 1-3
1.3.3 インタフェースでのスタティック/ダイナミックMACアドレスエントリの追加/修正1-4
1.3.4 ブラックホールMACアドレスエントリの追加/修正 1-4
1.4 MACアドレス学習の無効化 1-4
1.4.1 グローバルでのMACアドレス学習の無効化 1-4
1.4.2 インタフェースでのMACアドレス学習の無効化 1-5
1.5 ダイナミックMACアドレスエントリのエージングタイマの設定 1-5
1.6 インタフェースで学習可能なMACアドレス数の設定 1-6
1.7 インタフェースで学習可能なMACアドレスの上限到達後での未知のフレームの転送の設定 1-6
1.8 MACアドレスの移動の通知と抑制機能の有効化 1-7
1.9 MACアドレステーブルのSNMP通知の有効化 1-8
1.10 MACアドレステーブルの表示と維持 1-8
1.11 MACアドレステーブルの設定例 1-9
1.11.1 ネットワーク要件 1-9
1.11.2 設定手順 1-9
1.11.3 設定の確認 1-10

1章 MAC アドレステーブル

1.1 概要

Ethernet 装置は、フレームを転送するために MAC アドレステーブルを使用します。このテーブルは、宛先 MAC アドレス、出力インタフェース、VLAN ID を記載しています。フレームを転送した場合、装置は、最初に MAC アドレステーブルにフレームの MAC アドレスと一致するか検索します。

- エントリがある場合、出力インタフェースへパケットを転送します。
- エントリがない場合、装置はフレームが所属する VLAN にフレームをブロードキャストします。

1.1.1 MAC アドレスエントリの作成方法

MAC アドレステーブルのエントリは 2 つのソースから成り立ちます。装置によって自動的に学習されたエントリと、管理者によって手動で追加されたエントリから構成されます。

I. MAC アドレスの学習

通常、MAC アドレステーブルは装置の各インタフェースに入力された送信元 MAC アドレスを学習することによって自動的に MAC アドレステーブルを生成します。

装置は入力パケットの MAC アドレスを学習するため以下の処理を行います。

1) フレームの送信元 MAC アドレス（例：MAC-SOURCE）を確認します。
2) フレームの MAC アドレスに対応するエントリを MAC アドレステーブルから検索します。
   - □ MAC アドレスに対応するエントリがある場合、そのエントリを更新します。
   - □ MAC アドレスに対応するエントリがない場合、MAC-SOURCE と入力ポートのエントリに追加します。

この送信元 MAC アドレスの学習を行った後に MAC-SOURCE 宛のフレームを受信したとき、装置は以下の処理を行います。

1) MAC アドレステーブルから MAC-SOURCE を検索します。
2) エントリのポートからフレームを転送します。

装置は、不明な送信元 MAC アドレスのフレームを受信したとき、MAC アドレステーブルが完全に書き込まれるまで、毎回学習プロセスを行います。

II. MAC アドレスエントリの手動設定

装置が送信元 MAC アドレス学習を介して動的に MAC アドレスを学習するとき、装置は正規ユーザのフレームかハッカーからのフレームかを見分けることができません。これは潜在的にセキュリティに危険をもたらします。ホスト A がポート A に接続されていると

き、MAC アドレスエントリはホスト A の MAC アドレス（たとえば、MAC A）を学習します。不正なユーザがポート B への送信元 MAC アドレスとして MAC A のフレームを送信するとき、装置は以下の処理を行います。

1) 出力インタフェースとしてポート B の新しい MAC アドレスエントリを学習し、MAC A の古いエントリに上書きします。
2) ポート B から MAC A の宛先のフレームを不正ユーザに転送します。

その結果、不正なユーザはホスト A のデータを取得します。ポート A のセキュリティを強化するために、ホスト A をポート A と結合するため、スタティックエントリを手動で設定します。ホスト A のフレームは常にポート A に向けて送信されます。ホスト A の偽造した MAC アドレスを使っている他のホストはホスト A の宛先フレームを取得することができません。

1.1.2 MAC アドレスエントリのタイプ

MAC アドレステーブルには以下のタイプのエントリがあります。

- **スタティックエントリ** – スタティックエントリは、関連したインタフェースから特定の宛先 MAC アドレスによってフレームを転送するため、手動で設定されます。エージアウトしません。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されます。
- **ダイナミックエントリ** – 手動で設定されたダイナミックエントリ、または動的に学習したエントリです。エージアウトします。手動で設定されたダイナミックエントリと動的に学習したエントリの優先度は同じです。
- **ブラックホールエントリ** – 手動で設定され、エージアウトしません。ブラックホールエントリは特定の宛先 MAC アドレスでフレームをフィルタするために設定されます。たとえば、セキュリティに問題のある指定したユーザへのすべてのフレームを、ブラックホール MAC アドレスエントリとしてユーザの MAC アドレスを設定することができます。

スタティック、ブラックホール MAC アドレスエントリはダイナミック MAC アドレスに上書きすることができます。逆にダイナミック MAC アドレスは上書きすることができません。

1.2 MACアドレス設定作業リスト

この項で記載される設定項目はすべてオプション設定であり、設定する順番は関係ありません。必要に応じて設定を行ってください。

作業リスト
（オプション設定項目）MACアドレスエントリの設定 • グローバルでのスタティック/ダイナミックMACアドレスエントリの追加/修正 • インタフェースでのスタティック/ダイナミックMACアドレスエントリの追加/修正 • ブラックホールMACアドレスエントリの追加/修正
（オプション設定項目）MACアドレス学習の無効化
（オプション設定項目）ダイナミックMACアドレスエントリのエージングタイマの設定
（オプション設定項目）インタフェースで学習可能なMACアドレス数の設定
（オプション設定項目）インタフェースで学習可能なMACアドレスの上限到達後での未知のフレームの転送の設定

作業リスト
（オプション設定項目）MACアドレスの移動の通知と抑制機能の有効化
（オプション設定項目）MACアドレステーブルのSNMP通知の有効化

1.3 MACアドレスエントリの設定

1.3.1 設定ガイドライン

- 自動学習した MAC アドレスと異なる出力インタフェースで同じ MAC アドレスが存在する場合、ダイナミックエントリは適用されません。
- 設定を保存していない場合、手動で設定されたスタティック、ブラックホール MAC アドレスエントリは、再起動が行われると削除されます。手動で設定されたダイナミック MAC アドレスは設定を保存するあるいはしないに関わらず、削除されます。

送信元 MAC アドレスのフレームが、異なるタイプの MAC アドレスエントリとマッチするフレームは、別に処理されます

タイプ	説明
スタティックMACアドレスエントリ	フレームの入力インタフェースがエントリのインタフェースと同一かどうかにかかわらず、宛先MACアドレスにフレームを転送します。
ダイナミックMACアドレスエントリ	• そのエントリと異なるインタフェースから入力したフレームのMACアドレスを学習し、元のエントリに上書きします。 • そのエントリと異なるインタフェースから入力したフレームを転送し、エージングタイマをアップデートします。
ブラックホールMACアドレスエントリ	フレームを廃棄します。

1.3.2 グローバルでのスタティック/ダイナミック MAC アドレスエントリの追加/修正

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. MAC アドレスエントリを追加/変更する	**mac-address** { **dynamic** | **static** } *mac-address* **interface** *interface-type interface-number* **vlan** *vlan-id*	デフォルト : グローバルで設定されたMACアドレスエントリはありません。 VLANが作成され、VLANにインタフェースが割り当てられていることを確認してください。

1.3.3 インタフェースでのスタティック/ダイナミック MAC アドレスエントリの追加/修正

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. interface view に移行する	• interface viewに移行する：**interface** *interface-type interface-number* • aggregate interface viewに移行する：**interface bridge-aggregation** *interface-number*	ー
3. スタティック、ダイナミック MAC アドレスエントリを追加/変更する	**mac-address** { **dynamic** | **static** } *mac-address* **vlan** *vlan-id*	デフォルト：インタフェースで設定されたMACアドレスエントリはありません。VLANが作成され、VLANにインタフェースが割り当てられていることを確認してください。

1.3.4 ブラックホール MAC アドレスエントリの追加/修正

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. ブラックホール MAC アドレスエントリを追加/変更する	**mac-address blackhole** *mac-address* **vlan** *vlan-id*	デフォルト：設定されたブラックホールMACアドレスエントリはありません。VLANが作成されていることを確認してください。

1.4 MACアドレス学習の無効化

MAC アドレス学習はデフォルトで有効です。装置が攻撃者から攻撃をうけたとき、MAC アドレステーブルが満たされないようにするため、MAC アドレスの学習を無効にします。たとえば、攻撃者からの異なる送信元 MAC アドレスの大量のフレームを学習しないように装置で MAC アドレスの学習を無効にすることができます。

MAC アドレス学習を無効にしたのち、装置は早急に既存のダイナミック MAC アドレスエントリを削除します。

1.4.1 グローバルでの MAC アドレス学習の無効化

グローバルで MAC アドレス学習を無効にすると、すべてのインタフェースで MAC アドレス学習が無効になり、装置は MAC アドレス学習を行いません。

以下にグローバルでの MAC アドレス学習を無効にする設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． グローバルで MAC アドレス学習を無効にする	**undo mac-address mac-learning enable**	デフォルト：有効

1.4.2 インタフェースでの MAC アドレス学習の無効化

グローバルで MAC アドレス学習が有効であるとき、インタフェースごとに MAC アドレス学習を無効にすることができます。

以下にインタフェースでの MAC アドレス学習を無効にする設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． interface view に移行する	● interface viewに移行する：**interface** *interface-type interface-number* ● aggregate interface viewに移行する：**interface bridge-aggregation** *interface-number*	ー
3． インタフェースで MAC アドレス学習を無効にする	**undo mac-address mac-learning enable**	デフォルト：有効

1.5 ダイナミックMACアドレスエントリのエージングタイマの設定

装置の MAC アドレステーブルには、セキュリティとダイナミックエントリのリソースの浪費を防ぐために、エージングタイマがあります。もしエージングタイマが満了する前にダイナミック MAC アドレスエントリのアップデートが行われないと、装置はエントリを削除します。エージング機能は、MAC アドレステーブルを、最新のネットワークトポロジの変化に対応して即座にアップデートするためのものです。

エージングタイマは適切な時間に設定してください。トポロジの変更が少ない安定したネットワークではエージングタイマを長い時間にする必要があり、トポロジの変更が多いネットワークではエージングタイマを短い時間にする必要があります。

エージング間隔が長いと、有効期限切れのエントリを 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。また、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およ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。

不必要なエージングアウトからダイナミックエントリを防ぐために、エージングタイマの設定を長くするあるいはエージングタイマを無効にすることで安定したネットワークのブロードキャストを削減することができます。ネットワークのパフォーマンスを向上するだけでなく、思いがけない宛先にデータフレームを送信することを減らすことができるため、セキュリティも改善することができます。

以下に MAC アドレス学習のエージングタイマを設定する方法を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. 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する	**mac-address timer** { **aging** *seconds* | **no-aging** }	デフォルト：300秒 **no-aging**パラメータを使用した場合、エージングタイマを無効にします。

1.6 インタフェースで学習可能なMACアドレス数の設定

この機能は MAC アドレステーブルサイズを制限します。MAC アドレステーブルが大きくなって転送処理が低下することを防ぐためにポートまたはポートグループごとに学習可能な MAC アドレス数を制限することができます。

以下にインタフェースで学習可能な MAC アドレス数の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. interface view に移行する	• interface viewに移行する：**interface** *interface-type interface-number* • aggregate interface viewに移行する：**interface bridge-aggregation** *interface-number*	ー
3. インタフェースで学習可能な MAC アドレス数を設定する	**mac-address max-mac-count** *count*	デフォルト：設定なし

1.7 インタフェースで学習可能なMACアドレスの上限到達後での未知のフレームの転送の設定

この章では、未知のフレームは、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のことを示します。

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あるいは無効にすることができます。

以下にインタフェースで受信された未知のフレームの転送の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. interface view に移行する	• interface viewに移行する：**interface** *interface-type interface-number* • aggregate interface viewに移行する：**interface bridge-aggregation** *interface-number*	ー

操作	コマンド	補足
3． 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する	**mac-address max-mac-count enable-forwarding**	デフォルト：有効

1.8 MACアドレスの移動の通知と抑制機能の有効化

以下の状況である場合、インタフェース A で学習された MAC アドレスエントリの出力インタフェースがインタフェース B に変更します。

- インタフェース B が、送信元 MAC アドレスのパケットを受信します。
- インタフェース B がインタフェース A と同じ VLAN に所属しています。

この場合、MAC アドレスがインタフェース A からインタフェース B に移動し、MAC アドレスの移動が発生します。

MAC アドレスの移動の通知機能は、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ことのログを出力します。

2 つのインタフェース間で継続して MAC アドレスが移動した場合、レイヤ 2 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 **display mac-address mac-move** コマンドで MAC アドレスの移動情報を表示することができます。

インタフェースから MAC アドレスの移動が頻繁に移動することをシステムが検出するとき、インタフェースをダウンさせるため、インタフェースで MAC アドレスの移動の抑制を設定することができます。指定した抑制間隔の経過後、インタフェースは自動で UP 状態になります。あるいは手動でインタフェースを UP にすることができます。

以下に MAC アドレスの移動の通知を設定する手順を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． 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。	**mac-address notification mac-move** [**interval** *interval*]	デフォルト：無効 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。 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。

操作	コマンド	補足
3．（オプション設定項目）検出間隔内に送信元インタフェースから移動する MAC アドレスのしきい値と検出間隔を設定する	**mac-address notification mac-move suppression** { **interval** *interval* | **threshold** *threshold* }	デフォルト : 検出間隔内に送信元インタフェースから移動するMACアドレスのしきい値は3です。MACアドレスの抑制間隔は30秒です。
4．interface view に移行する	● interface viewに移行する：**interface** *interface-type interface-number* ● aggregate interface viewに移行する：**interface bridge-aggregation** *interface-number*	ー
5．MAC アドレスの移動の抑制機能を有効にする	**mac-address notification mac-move suppression**	デフォルト：無効

1.9 MACアドレステーブルのSNMP通知の有効化

MAC アドレステーブルの SNMP 通知を有効にしたのち、装置は NMS に重要なイベントを通知するため、SNMP モジュールに SNMP 通知を送信します。送信する通知の属性を決定するため、SNMP の送信パラメータを SNMP 通知に設定することができます。

MAC アドレステーブルの SNMP 通知を無効にした場合、装置は Information Center モジュールにログメッセージの送信を行います。MAC アドレステーブルモジュールのログメッセージを調査するため、出力ルールと宛先を設定することができます。SNMP 通知と Information Center の詳細は、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*17 ネットワーク管理と監視*”の”*4 章 SNMP*”、“3 *システム管理*”の”*5 章 Information Center*”を参照してください。

以下に MAC アドレステーブルの SNMP 通知の設定を示します。

操作	コマンド	補足
1．system view に移行する	**system-view**	ー
2．MAC アドレステーブルの SNMP 通知を有効にする	**snmp-agent trap enable mac-address**	デフォルト：無効

1.10 MACアドレステーブルの表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
MACアドレステーブル情報を表示する	**display mac-address** [*mac-address* [**vlan** *vlan-id*] | [[**dynamic** | **static**] [**interface** *interface-type interface-number*] | **blackhole**] [**vlan** *vlan-id*] [**count**]]
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する	**display mac-address aging-time**

操作	コマンド
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する	**display mac-address mac-learning** [**interface** *interface-type interface-number*]
MACアドレスの移動記録を表示する	**display mac-address mac-move**

1.11 MACアドレステーブルの設定例

1.11.1 ネットワーク要件

図 1-1に示すように、以下の要件を設定します。

- Host A （000f-e235-dc71）は AC のインタフェース GigabitEthernet 1/0/1 に接続され、VLAN1 に属しています。
- ネットワークで一度疑わしいふるまいをした Host B （000f-e235-abcd）は VLAN1 に属しています。

MAC アドレスの設定を以下に示します。

- MAC アドレス spoofing を防ぐため、AC の MAC アドレステーブルの Host A にスタティックエントリを追加します。
- Host B で定義されたすべてのフレームを廃棄するように、Host にブラックホール MAC アドレスエントリを追加します。
- 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。

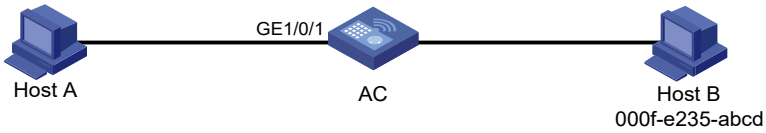


図 1-1 ネットワーク図

1.11.2 設定手順

VLAN1 に属している GigabitEthernet 1/0/1 に MAC アドレス 000f-e235-dc71 のスタティック MAC アドレスエントリを追加します。

```
<AC> system-view
[AC] mac-address static 000f-e235-dc71 interface gigabitethernet 1/0/1 vlan 1
```

VLAN1 に属している MAC アドレス 000f-e235-abcd にブラックホール MAC アドレスエントリを追加します。

```
[AC] mac-address blackhole 000f-e235-abcd vlan 1
```

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。

```
[AC] mac-address timer aging 500
```

1.11.3 設定の確認

GigabitEthernet 1/0/1 のスタティック MAC アドレスエントリを表示します。

```
[AC] display mac-address static interface gigabitethernet 1/0/1
MAC Address       VLAN ID    State           Port/NickName           Aging
000f-e235-dc71    1          Static          GE1/0/1                  N
```

ブラックホール MAC アドレスエントリを表示します。

```
[AC] display mac-address blackhole
MAC Address       VLAN ID    State           Port/NickName           Aging
000f-e235-abcd    1          Blackhole       N/A                     N
```

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。

```
[AC] display mac-address aging-time
MAC address aging time: 500s.
```

目次

このセクションのページは**5-x-x**です。

2章 リンクアグリゲーション 2-1
2.1 概要 2-1
2.1.2 アグリゲーショングループ、メンバポート、アグリゲートインタフェース 2-1
2.1.3 アグリゲーショングループのメンバポートの状態 2-1
2.1.4 オペレーショナルキー 2-1
2.1.5 コンフィグレーションタイプ 2-2
2.1.6 リンクアグリゲーションモード 2-2
2.1.7 スタティックモードのリンクアグリゲーションの動作 2-3
2.1.8 アグリゲーショングループの負荷分散 2-5
2.2 リンクアグリゲーション設定作業リスト 2-5
2.3 アグリゲーショングループの設定 2-5
2.3.1 アグリゲーショングループの設定 2-5
2.4 アグリゲートインタフェースの設定 2-6
2.4.1 アグリゲートインタフェースの説明の設定 2-6
2.4.2 アグリゲートインタフェースのシャットダウン 2-6
2.5 アグリゲーショングループのSelectedポートの最小と最大数の設定 2-7
2.6 リンクアグリゲーションのロードシェアリングモードの設定 2-8
2.7 リンクアグリゲーションの表示と維持 2-8
2.8 リンクアグリゲーションの設定例 2-9
2.8.1 スタティックアグリゲーション設定例 2-9
2.8.2 アグリゲーションロードシェアリング設定例 2-11

2章 リンクアグリゲーション

2.1 概要

リンクアグリゲーションは、複数のイーサネットインタフェースを束ねて、一つの論理インタフェースとして扱う機能です。図 2-1は、3 つイーサネットインタフェースを束ねて、一つの論理インタフェース（リンクアグリゲーション 1）として接続している例です。

これにより、装置間の接続帯域幅を拡大することができます。また、1 つのイーサネットインタフェースが故障した場合に、残ったイーサネットインタフェースで通信を継続する冗長性を確保できます。

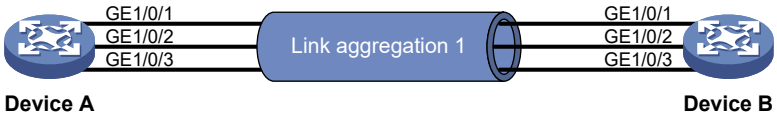


図 2-1 リンクアグリゲーション図

2.1.2 アグリゲーショングループ、メンバポート、アグリゲートインタフェース

アグリゲーショングループは、集約された Ethernet インタフェースのグループです。アグリゲーショングループには、アグリゲートインタフェースと呼ばれる論理的なインタフェースが作成されます。上位レイヤエンティティにリンクアグリゲーションを使用すると、以下のようになります。

アグリゲートインタフェースのレートは、Selected 状態のそのメンバポートのレートの合計と同一です。また通信モードは Selected 状態のメンバポートと同一です。

2.1.3 アグリゲーショングループのメンバポートの状態

アグリゲーショングループのメンバポートは、以下の状態のいずれかとなります。

- **Selected**：ユーザにトラフィックを送受信できます。
- **Unselected**：ユーザにトラフィックを送受信できません。

2.1.4 オペレーショナルキー

ポートを集約する際に、リンクアグリケーションは、通信速度、通信モードのような設定を含むポート属性にもとづいてオペレーショナルキーをそれぞれのポートに自動的に制御し割り当てます。

リンクアグリゲーショングループ内にある Selected 状態のすべてのメンバポートは、同じオペレーショナルキーを持っています。

2.1.5 コンフィグレーションタイプ

リンクアグリゲーショングループのメンバポートに設定するすべての設定は、グループのポートのアグリゲーション状態に影響を与える可能性があります。影響を与える設定は以下のコンフィグレーションタイプに分類されます。

I. 属性コンフィグレーション

Selected ポートになるためには、メンバポートはアグリゲートインタフェースとして同じ属性の設定を持つ必要があります。に属性の設定を示します。

表 2-1 属性の設定

機能	属性の設定
VLAN	VLAN属性設定 ● 許可されたVLAN ID ● PVID ● リンクタイプ(trunk、hybrid、access) ● VLANタグモード VLANについては、QX-W2300ACシリーズアクセスコントローラオペレーションマニュアルの“*5 ネットワーク接続*”の”*3章 VLAN*”を参照してください。

アグリゲートインタフェースで行われた属性コンフィグレーションは、すべてのメンバポートに自動的に同期されます。Selected ポートへの同期に失敗した場合、ポートは Unselected 状態になります。再度 Selected 状態になるには、アグリゲートインタフェースまたはメンバポートの属性設定を変更します。同期の失敗は、アグリゲートインタフェース上で作成された属性設定の変更には影響しません。アグリゲートインタフェースから同期された設定は、アグリゲートインタフェースが削除された後でもメンバポートに保持されます。

メンバポートの属性コンフィグレーションの変更は、メンバポートのアグリゲーション状態と実行中のサービスに影響する可能性があります。メンバポートの属性コンフィグレーション設定を変更しようとするたびに、警告メッセージが表示されます。

II. プロトコルコンフィグレーション

プロトコルコンフィグレーションは、アグリゲートインタフェースの変更があってもメンバポートのアグリゲーション状態に影響しません。プロトコルコンフィグレーションの例として、MAC アドレス学習があります。

アグリゲートインタフェースのプロトコルコンフィグレーションのみ適用します。メンバポートのプロトコルコンフィグレーションは、ポートがアグリゲーショングループから削除されるまで適用されません。

2.1.6 リンクアグリゲーションモード

リンクアグリゲーションは、ダイナミックモードとスタティックモードがあります。

- **スタティックアグリゲーションモード** — アグリゲーションが安定します。スタティックモードのアグリゲーショングループは、スタティックアグリゲーショングループと呼ばれます。メンバポートのアグリゲーション状態は対向先の影響を受けません。
- **ダイナミックアグリゲーションモード** — ダイナミックモードのアグリゲーショングループは、ダイナミックアグリゲーショングループと呼ばれます。ローカルシステムと対向先のシステムはメンバポートのアグリゲーション状態を自動的に管理します。管理者の管理負荷を削減することができます。

2.1.7 スタティックモードのリンクアグリゲーションの動作

I. リファレンスポートの選出

アグリゲーショングループでポートのアグリゲーション状態を設定するとき、システムはリファレンスポートとして自動でメンバポートを選出します。Selected ポートはリファレンスポートとして、同じオペレーショナルキーと属性コンフィグレーションを持つ必要があります。

メンバポートから、アグリゲートインタフェースとして同一の属性を持つ up 状態のリファレンスポートを選択します。

候補となるポートの優先順位は、以下の順番となります。

1) もっとも高いポート優先度
2) 全 2 重/高速
3) 全 2 重/低速
4) 半 2 重/高速
5) 半 2 重/低速

アグリゲートインタフェースと同じ属性コンフィグレーションを持つ候補のポートから、もっとも高い優先度レベルを持つポートがリファレンスポートとして選択されます。

- 同じ優先度を持つポートが複数あり、Selected ポートがある場合、Selected ポートが選ばれます。もし 1 つ以上の最初の Selected ポートがある場合、ポート番号が一番小さい Selected ポートが選択されます。
- 複数のポートに同じ優先度があり、Selected ポートがない場合、ポート番号が一番小さい Selected ポートが選択されます。

II. 各メンバポートのアグリゲーション状態の設定

スタティックアグリゲーショングループが Selected ポートの制限に達した後、グループに加入したポートは、Selected ポートのトラフィックの中断を防ぐため、Unselected 状態に置き換えられます。

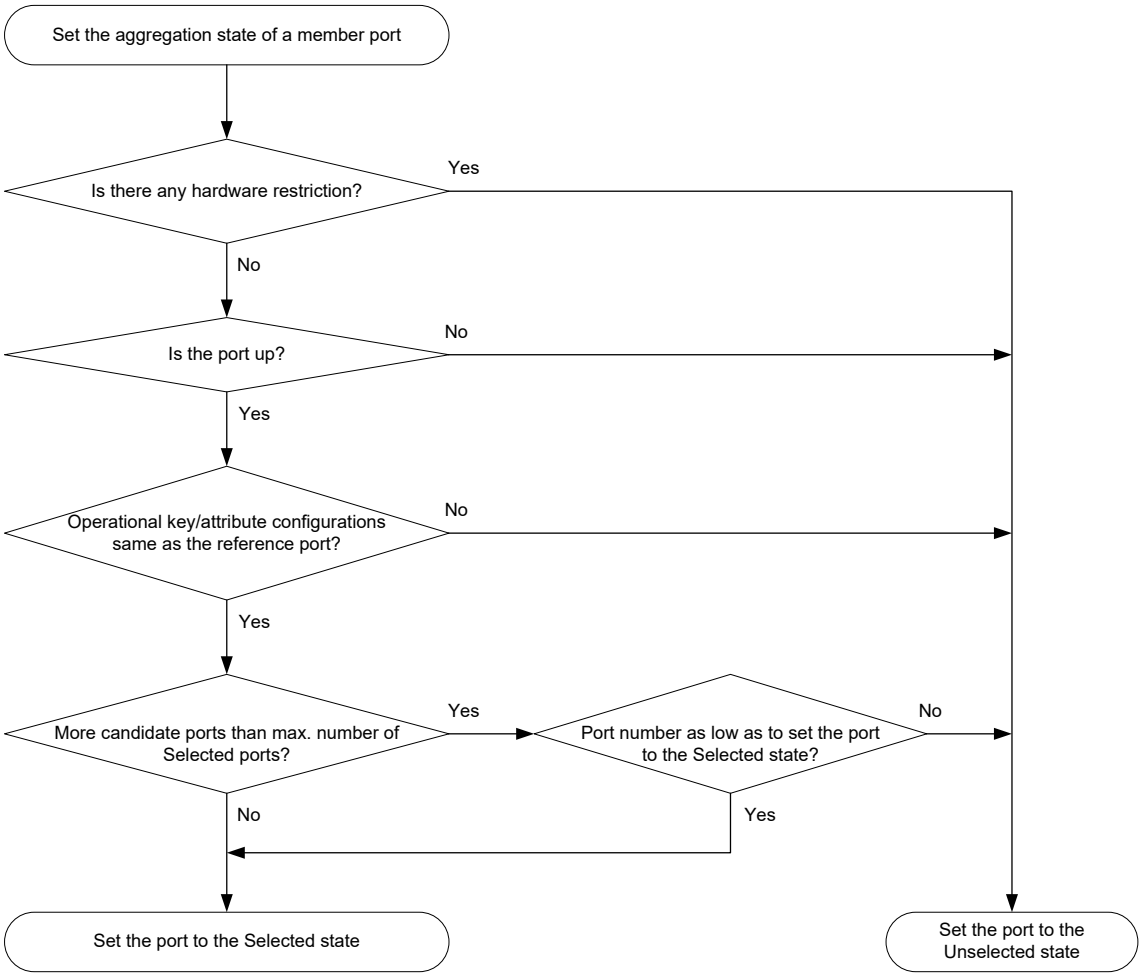


図 2-2 スタティックアグリゲーショングループのアグリゲーション状態の設定

Selected ポートの制限に到達したのち、新しいメンバポートのアグリゲーションの状態は以下の状態によって変わります。

- ポートと Selected ポートが同一の優先度を持つ場合、ポートは Unselected 状態に遷移します。このメカニズムによって既存の Selected ポートでトラフィックの中断を防ぎます。装置の再起動を行うとメンバポートのアグリゲーション状態の再計算が行われます。
- 以下の状態の場合、ポートは Selected 状態に遷移します。
  - □ ポートと Selected ポートが異なる優先度を持つ場合、ポートは少なくとも 1 つの Selected ポートの優先度よりも高い優先度を持ちます。
  - □ アグリゲートインタフェースとして同一の属性コンフィグレーションを持ちます。

オペレーショナルキーと属性コンフィグレーションを変更すると、リンクアグリゲーションメンバポートのアグリゲーションの状態に影響を及ぼす可能性があります。

2.1.8 アグリゲーショングループの負荷分散

リンクアグリゲーショングループにおいて、トラフィックは Selected ポートを通り、フローベースで負荷分散が行われます。ロードシェアリングモードは、以下の基準またはその組み合わせによってトラフィックフローが分散され、同じリンクにある同一フローのパケットを転送します。

- 送信に元あるいは宛先 IP アドレス
- 送信元あるいは宛先 MAC アドレス

2.2 リンクアグリゲーション設定作業リスト

作業リスト
（必須設定項目）アグリゲーショングループの設定
（オプション設定項目）アグリゲートインタフェースの設定 • アグリゲートインタフェースの説明の設定 • アグリゲートインタフェースのシャットダウン
（オプション設定項目）アグリゲーショングループのSelectedポートの最小と最大数の設定
（オプション設定項目）リンクアグリゲーションのロードシェアリングモードの設定

2.3 アグリゲーショングループの設定

2.3.1 アグリゲーショングループの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． アグリゲートインタフェースを作成し、aggregate interface view に移行する	**interface bridge-aggregation** *interface-number*	アグリゲートインタフェースを作成すると、スタティックアグリゲーショングループ番号が、自動的に同一番号で作成されます。
3． system view へ戻る	**quit**	ー
4． 指定されたアグリゲーショングループにインタフェースを割り当てる	1． Ethernet interface view に移行する： **interface** *interface-type interface-number* 2． 指定されたアグリゲーショングループにインタフェースを割り当てる： **port link-aggregation group** *group-id*	アグリゲーショングループに複数のインタフェースを割り当てる場合、このステップを繰り返してください。

2.4 アグリゲートインタフェースの設定

インタフェースで実行できる設定のほとんどは、アグリゲートインタフェースでも実行できます。

2.4.1 アグリゲートインタフェースの説明の設定

インタフェースの目的などを記載するように、管理者用にアグリゲートインタフェースの説明を記載することができます。

以下にアグリゲートインタフェースの説明を設定する方法を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. aggregate interface view に移行する	**interface bridge-aggregation** *interface-number*	―
3. アグリゲートインタフェースの説明を設定する	**description** *text*	デフォルト：*interface-name* **Interface**

2.4.2 アグリゲートインタフェースのシャットダウン

アグリゲートインタフェースをシャットダウンあるいはアップすると、対応するアグリゲーショングループの状態とリンク状態に以下のような影響があります。

- アグリゲートインタフェースがシャットダウンしたとき、アグリゲーショングループのすべての Selected ポートは Unselected になります。
- アグリゲートインタフェースをアップさせると、対応するアグリゲーショングループのポートの Selected 状態を再計算します。

以下にアグリゲートインタフェースをシャットダウンする方法を示します。

操作	コマンド
1. system view に移行する	**system-view**
2. aggregate interface view に移行する	**interface bridge-aggregation** *interface-number*
3. アグリゲートインタフェースをシャットダウンする	**shutdown**

注意：

shutdown コマンドは、インタフェースで確立されたすべてのリンクを切断します。ご使用の環境でこのコマンドを使用する場合は、このコマンドの影響を十分に認識しておく必要があります。

2.5 アグリゲーショングループのSelectedポートの最小と最大数の設定

重要：

スタティックアグリゲーショングループに Selected ポートの最小値と最大値を設定した場合、正しい接続を保証するために、対向先のアグリゲーショングループに同じ設定をしてください。

アグリゲートリンクの帯域幅は、Selected メンバポートを増やすことで増加させることができます。アグリゲートリンクの Selected ポートが不足することによる輻輳を防ぐため、アグリゲートインタフェースの Selected メンバポートの最小数を設定できます。

この最小数のしきい値はアグリゲーションメンバポートとアグリゲートインタフェースの両方の状態に影響します。

- 適切なメンバポートが最小数を下回ったとき、以下の処理が行われます。
  - すべてのメンバポートが Unselected ポートに変更します。
  - アグリゲートインタフェースのリンクがダウンします。
- Selected ポートに適切なメンバポートの数が最小数以上になったとき、以下の処理が行われます。
  - 適切なメンバポートが Selected ポートに変更します。
  - アグリゲートインタフェースのリンクがアップします。

アグリゲートグループの Selected ポートの最大数は、設定された最大数あるいはハードウェア性能のいずれか小さいほうで制限されます。

以下の処理を行うことで 2 つのポート間でバックアップを設定することができます。

- アグリゲートグループに 2 つのポートを割り当てます。
- アグリゲートグループの Selected ポートの最大数を 1 に設定します。

このように設定すると、1 つのメンバポートが Selected ポートになります。もう一方のメンバポートが Unselected ポートとなり、バックアップポートとして動作します。

アグリゲーショングループの場合、Selected ポートの最大数は、Selected ポートの最小数以上である必要があります。

以下に Selected ポートの最小と最大数の設定方法を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. aggregate interface view に移行する	**interface bridge-aggregation** *interface-number*	—
3. アグリゲーショングループの Selected ポートの最小数を設定する	**link-aggregation selected-port minimum** *number*	デフォルト：設定なし
4. アグリゲーショングループの Selected ポートの最大数を設定する	**link-aggregation selected-port maximum** *number*	デフォルト : ハードウェアの制限に依存します。

2.6 リンクアグリゲーションのロードシェアリングモードの設定

グローバルまたはグループ単位にロードシェアリングモードを設定できます。リンクアグリゲーショングループは、グループ単位のロードシェアリングモードを優先的に使用します。グループ単位のロードシェアリングモードが利用できない場合、グループはグローバルのロードシェアリングモードを使用します。

I. グローバルでのリンクアグリゲーションのロードシェアリングモードの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. グローバルでのロードシェアリングモードを設定する	**link-aggregation global load-sharing mode** { **destination-ip** | **destination-mac** | **destination-port** | **source-ip** | **source-mac** | **source-port** }	デフォルト : システムはパケットタイプに従い自動でロードシェアリングモードを選択します。

II. グループ単位でのロードシェアリングモードの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. aggregate interface view に移行する	**interface bridge-aggregation** *interface-number*	―
3. アグリゲーショングループのロードシェアリングモードを設定する	**link-aggregation load-sharing mode** { **destination-ip** | **destination-mac** | **source-ip** | **source-mac** } *	―

2.7 リンクアグリゲーションの表示と維持

display counters コマンド、**display counters rate** コマンドの詳細は、QX-W2300AC シリーズアクセスコントローラコマンドマニュアルの“*4 インタフェース*”を参照してください。

すべての view で **display** コマンドを実行し、user view で **reset** コマンドを実行できます。

操作	コマンド
グローバルあるいはグループのロードシェアリングモードを表示する	**display link-aggregation load-sharing mode interface** [**bridge-aggregation** *interface-number*]
アグリゲーションメンバポートのリンクアグリゲーションの詳細情報を表示する	**display link-aggregation member-port** [*interface-list* | **auto**]
すべてのアグリゲーショングループの概要を表示する	**display link-aggregation summary**
アグリゲーショングループの詳細情報を表示する	**display link-aggregation verbose** [**bridge-aggregation** [*interface-number*]] [**all-configuration**]
インタフェース トラフィックの統計情報を表示する	**display counters** { **inbound** | **outbound** } **interface** [**bridge-aggregation** [*interface-number*]]

操作	コマンド
最新の統計情報ポーリング間隔で、アップ状態のインタフェースのトラフィックレート統計情報を表示する	**display counters rate** { **inbound** | **outbound** } **interface** [**bridge-aggregation** [*interface-number*]]
アグリゲートインタフェース統計情報を削除する	**reset counters interface** [**bridge-aggregation** [*interface-number*]]

2.8 リンクアグリゲーションの設定例

2.8.1 スタティックアグリゲーション設定例

I. ネットワーク要件

図 2-3に示すように以下の要件を設定します。

- AC 1 と AC 2 の両方で、スタティックアグリゲーショングループを設定します。
- 片端で VLAN10 を有効にし、VLAN10 でアグリゲートリンクの対向先と通信します。
- 片端で VLAN20 を有効にし、VLAN20 でアグリゲートリンクの対向先と通信します。

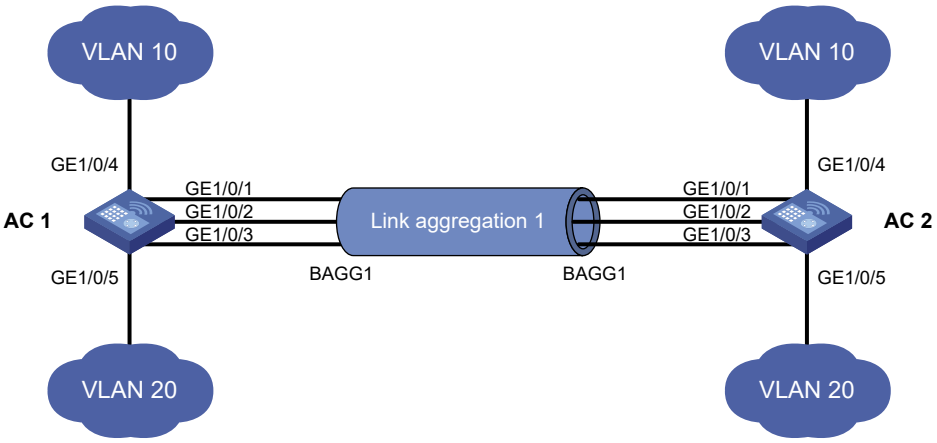


図 2-3 ネットワーク図

II. 設定手順

1)　AC 1 を設定します。

VLAN 10 を作成し、GigabitEthernet 1/0/4 に割り当てます。

```
<AC1> system-view
[AC1] vlan 10
[AC1-vlan10] port gigabitethernet 1/0/4
[AC1-vlan10] quit
```

VLAN 20 を作成し、GigabitEthernet 1/0/5 に割り当てます。

```
[AC1] vlan 20
[AC1-vlan20] port gigabitethernet 1/0/5
[AC1-vlan20] quit
```

アグリゲートインタフェース Bridge-Aggregation 1 を作成します。

```
[AC1] interface bridge-aggregation 1
[AC1-Bridge-Aggregation1] quit
```

GigabitEthernet 1/0/1～GigabitEthernet 1/0/3 にリングアグリゲーショングループ 1 を割り当てます。

```
[AC1] interface gigabitethernet 1/0/1
[AC1-GigabitEthernet1/0/1] port link-aggregation group 1
[AC1-GigabitEthernet1/0/1] quit
[AC1] interface gigabitethernet 1/0/2
[AC1-GigabitEthernet1/0/2] port link-aggregation group 1
[AC1-GigabitEthernet1/0/2] quit
[AC1] interface gigabitethernet 1/0/3
[AC1-GigabitEthernet1/0/3] port link-aggregation group 1
[AC1-GigabitEthernet1/0/3] quit
```

アグリゲートインタフェース Bridge-Aggregation 1 をトランクポートとして作成し、VLAN10、VLAN20 を割り当てます。

```
[AC1] interface bridge-aggregation 1
[AC1-Bridge-Aggregation1] port link-type trunk
[AC1-Bridge-Aggregation1] port trunk permit vlan 10 20
[AC1-Bridge-Aggregation1] quit
```

2)　AC 1 の設定と同様に AC 2 を設定します。（詳細は省略します。）

III. 設定の確認

Device A ですべてのアグリゲーショングループの詳細情報を表示します。

```
[AC1] display link-aggregation verbose
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected, I -- Individual
Port: A -- Auto port, M -- Management port, R -- Reference port
Flags:  A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
        D -- Synchronization, E -- Collecting, F -- Distributing,
        G -- Defaulted, H -- Expired
Role: P -- Primary, S -- Secondary

Aggregate Interface: Bridge-Aggregation1
Aggregation Mode: Static
Loadsharing Type: Shar
```

```
Management VLANs: None
  Port              Status  Priority Oper-Key  Role
  GE1/0/1(R)        S       32768    1         None
  GE1/0/2           S       32768    1         None
  GE1/0/3           S       32768    1         None
```

出力では、リンクアグリゲーション 1 がスタティックアグリゲーショングループで、3 つの Selected ポートがあることを示しています。

2.8.2 アグリゲーションロードシェアリング設定例

I. ネットワーク要件

図 2-4に示すように以下の要件を設定します。

- AC 1 と AC 2 の両方で、スタティックアグリゲーショングループ 1 と 2 を設定します。
- 片端で VLAN10 を有効にし、VLAN10 でアグリゲートリンクの対向先と通信します。
- 片端で VLAN20 を有効にし、VLAN20 でアグリゲートリンクの対向先と通信します。
- アグリゲーショングループメンバーポート間でトラフィックをロードシェアリングするようにリンクアグリゲーショングループ 1 および 2 を設定します。
  - 送信元 MAC アドレスに基づいてパケットをロードシャアリングするようにリンクアグリゲーショングループ 1 を設定します。
  - 宛先 MAC アドレスに基づいてパケットをロードシェアリングするようにリンクアグリゲーショングループ 2 を設定します。

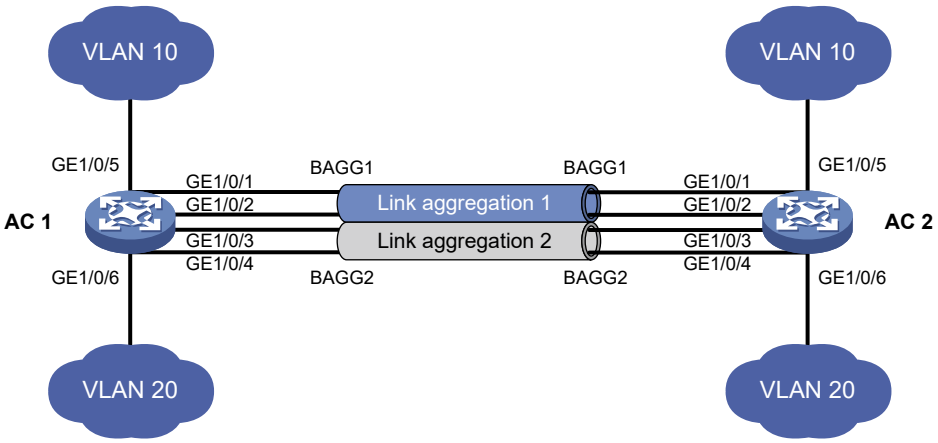


図 2-4 ネットワーク図

II. 設定手順

1)　AC 1 を設定します。

VLAN 10 を作成し、GigabitEthernet 1/0/5 に割り当てます。

```
<AC1> system-view
[AC1] vlan 10
```

```
[AC1-vlan10] port gigabitethernet 1/0/5
[AC1-vlan10] quit
```

VLAN 20 を作成し、GigabitEthernet 1/0/6 に割り当てます。

```
[AC1] vlan 20
[AC1-vlan20] port gigabitethernet 1/0/6
[AC1-vlan20] quit
```

アグリゲートインタフェース Bridge-Aggregation 1 を作成します。

```
[AC1] interface bridge-aggregation 1
```

送信元 MAC アドレスに基づいてパケットをロードシャアリングするようにアグリゲーションググループ 1 を設定します。

```
[AC1-Bridge-Aggregation1] link-aggregation load-sharing mode source-mac
[AC1-Bridge-Aggregation1] quit
```

GigabitEthernet 1/0/1 と GigabitEthernet 1/0/2 にリングアグリゲーショングループ 1 を割り当てます。

```
[AC1] interface gigabitethernet 1/0/1
[AC1-GigabitEthernet1/0/1] port link-aggregation group 1
[AC1-GigabitEthernet1/0/1] quit
[AC1] interface gigabitethernet 1/0/2
[AC1-GigabitEthernet1/0/2] port link-aggregation group 1
[AC1-GigabitEthernet1/0/2] quit
```

アグリゲートインタフェース Bridge-Aggregation 1 をトランクポートとして作成し、VLAN10 を割り当てます。

```
[AC1] interface bridge-aggregation 1
[AC1-Bridge-Aggregation1] port link-type trunk
[AC1-Bridge-Aggregation1] port trunk permit vlan 10
[AC1-Bridge-Aggregation1] quit
```

アグリゲートインタフェース Bridge-Aggregation 2 を作成します。

```
[AC1] interface bridge-aggregation 2
```

宛先 MAC アドレスに基づいてパケットをロードシャアリングするようにアグリゲーショングループ 2 を設定します。

```
[AC1-Bridge-Aggregation2] link-aggregation load-sharing mode destination-mac
[AC1-Bridge-Aggregation2] quit
```

GigabitEthernet 1/0/3 と GigabitEthernet 1/0/4 にリングアグリゲーショングループ 2 を割り当てます。

```
[AC1] interface gigabitethernet 1/0/3
```

```
[AC1-GigabitEthernet1/0/3] port link-aggregation group 2
[AC1-GigabitEthernet1/0/3] quit
[AC1] interface gigabitethernet 1/0/4
[AC1-GigabitEthernet1/0/4] port link-aggregation group 2
[AC1-GigabitEthernet1/0/4] quit
```

アグリゲートインタフェース Bridge-Aggregation 2 をトランクポートとして作成し、VLAN20 を割り当てます。

```
[AC1] interface bridge-aggregation 2
[AC1-Bridge-Aggregation2] port link-type trunk
[AC1-Bridge-Aggregation2] port trunk permit vlan 20
[AC1-Bridge-Aggregation2] quit
```

2)　AC 2 の設定と同様に Device B を設定します。（詳細は省略します。）

III. 設定の確認

AC 1 ですべてのアグリゲーショングループの詳細情報を表示します。

```
[AC1] display link-aggregation verbose
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected, I -- Individual
Port: A -- Auto port, M -- Management port, R -- Reference port
Flags:  A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
        D -- Synchronization, E -- Collecting, F -- Distributing,
        G -- Defaulted, H -- Expired
Role: P -- Primary, S -- Secondary

Aggregate Interface: Bridge-Aggregation1
Aggregation Mode: Static
Loadsharing Type: Shar
Management VLANs: None
  Port             Status  Priority Oper-Key  Role
  GE1/0/1(R)       S       32768    1         None
  GE1/0/2          S       32768    1         None

Aggregate Interface: Bridge-Aggregation2
Aggregation Mode: Static
Loadsharing Type: Shar
Management VLANs: None
  Port             Status  Priority Oper-Key  Role
  GE1/0/3(R)       S       32768    2         None
  GE1/0/4          S       32768    2         None
```

出力では以下を示します。

- リンクアグリゲーショングループ 1 とリンクアグリゲーショングループ 2 は、それぞれロードシェアドスタティックアグリゲーショングループです。
- 各アグリゲーショングループには 2 つの選択ポートが含まれています。

AC 1 でグループ単位の負荷分散モードをすべて表示します。

```
[AC1] display link-aggregation load-sharing mode interface

Bridge-Aggregation1 Load-Sharing Mode:
source-mac address
```

```
Bridge-Aggregation2 Load-Sharing Mode:
destination-mac address
```

出力では以下を示します。

- リンクアグリゲーショングループ 1 は送信元 MAC アドレスに基づいてパケットをロードシェアリングします。
- リンクアグリゲーショングループ 2 は宛先 MAC アドレスに基づいてパケットをロードシェアリングします。

目次

このセクションのページは**5-x-x** です。

3章 VLAN 3-1
3.1 概要 3-1
3.1.1 VLANフレームのカプセル化 3-1
3.1.2 プロトコルと標準 3-2
3.2 VLANの設定 3-2
3.2.1 制限とガイドライン 3-2
3.3 VLANインタフェースの設定 3-3
3.3.1 VLANインタフェースの基本設定 3-4
3.4 ポートベースVLANの設定 3-4
3.4.1 概要 3-4
3.4.2 アクセスポートVLANの設定 3-5
3.4.3 トランクポートVLANの設定 3-6
3.4.4 ハイブリッドポートVLANの設定 3-7
3.5 VLANの表示と維持 3-7
3.6 VLAN の設定例 3-8
3.6.1 ポートベースVLANの設定例 3-8

3章 VLAN

3.1 概要

VLAN（Virtual Local Area Network）テクノロジは、物理 LAN を複数の論理 LAN に分割することで、スイッチ内を仮想的なグループに分けます。次の利点があります。

- セキュリティー同じ VLAN 内のホストはレイヤ 2 で相互に通信できますが、レイヤ 2 の他の VLAN のホストから隔離され、直接通信できる範囲を限定します。
- ブロードキャストトラフィックの分離ーグループの範囲内でのみ直接通信するため、ブロードキャストフレームによる回線の混雑を緩和します。
- 柔軟性ーVLAN は、ワークグループごとに論理的に分割できます。 同じワークグループ内のホストは、物理的な場所に関係なく、ネットワーク構成を決めることができます。

図 3-1のように VLAN を使用して、LAN を小さく分割することで、ブロードキャストドメインの影響を少なくすることができます。

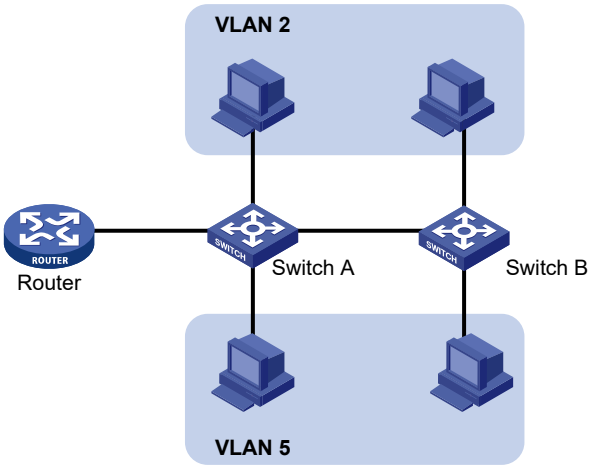


図 3-1 VLAN ネットワーク図

VLAN は物理的な要素からは制限を受けません。たとえば、特定のワークグループによって使用されるすべてのワークステーションとサーバは物理的な位置に関係なく、同じ LAN に接続することができます。異なる VLAN 間と通信するためにはルータやレイヤ 3 スイッチが必要となります。

3.1.1 VLAN フレームのカプセル化

異なる VLAN からイーサネットフレームを認識するため、図 3-2に示すように IEEE802.1Q では、宛先/送信元 MAC アドレス（DA&SA）フィールドと上位プロトコルタイプフィールドの間に 4byte の VLAN タグを追加しました。

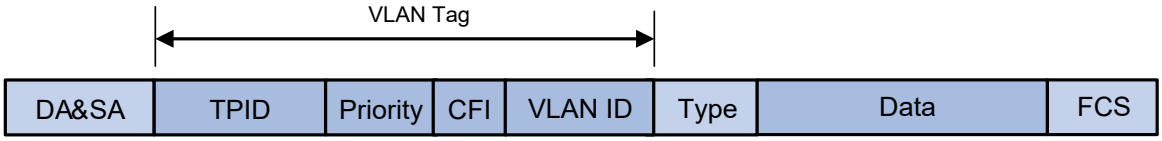


図 3-2 VLAN タグの位置とフォーマット

VLAN タグは以下のフィールドが含まれます。

- **TPID**– フレームに VLAN タグが付いているかどうかを識別するためのプロトコル識別子です。このフィールドは 16 ビット長です。デフォルトで TPID は 0x8100 で VLAN タグが付いています。
- **Priority**– フレームの 802.1p 優先度を示します。このフィールドは 3 ビット長です。
- **CFI**– 標準フォーマットを示すフィールドです。このフィールドは 1 ビット長です。パケットが異なるメディアを跨いで転送されるとき、MAC アドレスは標準フォーマットでカプセル化されます。以下の値が設定できます。
  - **0（デフォルト）**– MAC アドレスは標準フォーマットでカプセル化されます。
  - **1**– MAC アドレスは非標準フォーマットでカプセル化されます。
- **VLAN ID**– フレームが所属する VLAN を示します。このフィールドは 12 ビット長です。VLAN-ID の範囲は 0～4095 です。0 と 4095 はプロトコルによって予約されているので、実際に使える値は 1～4094 となります。

フレームを受信したとき、ネットワーク装置はフレームに VLAN タグが付いているか、そして VLAN タグの値を確認して処理を決定します。

イーサネットは Ethernet II、802.3/802.2 LLC、802.3/802.2 SNAP、802.3 raw などのカプセル化フォーマットをサポートしています。ここでは Ethernet II カプセル化フォーマットを使用しています。VLAN タグフィールドは VLAN を識別するために、これらのカプセル化フォーマットにも付与されます。詳細は関連するプロトコルと標準を参照してください。

複数のタグ付きフレームのために、装置はもっとも外側の VLAN タグに従って処理し、ペイロードとしてその内部の VLAN タグを送信します。

VLAN の詳細は QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*5 ネットワーク接続*”の”*3 章 VLAN*”を参照してください。

3.1.2 プロトコルと標準

IEEE 802.1Q, *IEEE Standard for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks*

3.2 VLANの設定

3.2.1 制限とガイドライン

VLAN を設定する場合、以下の制限とガイドラインに従ってください。

- デフォルト VLAN である VLAN1 は作成または削除できません。

- ダイナミック VLAN、あるいはアプリケーションで設定されている VLAN は **undo vlan** コマンドで削除することはできません。最初に各設定から VLAN の設定を削除してください。

以下に VLAN の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. （オプション設定項目）VLAN を作成し、view へ移行あるいは VLAN リストを作成する	**vlan** { *vlan-id-list* | **all** }	デフォルト： デフォルト VLAN（VLAN1）のみ
3. VLAN view に移行する	**vlan** *vlan-id*	VLANリストを作成した後、指定したVLANを設定するには、この操作を実行してください。
4. VLAN の名前を設定する	**name** *text*	デフォルト：**VLAN** *vlan-id* たとえばVLAN 100のVLAN名は**VLAN 0100**です。
5. VLAN の説明を設定する	**description** *text*	デフォルト：**VLAN** *vlan-id* *vlan-id*はVLANのIDです。 たとえばVLAN 100の説明は**VLAN 0100**です。

3.3 VLANインタフェースの設定

description、**shutdown** コマンドの詳細は、QX-W2300AC シリーズアクセスコントローラコマンドマニュアルの“*4 インタフェース*”を参照してください。

VLAN インタフェースが手動でシャットダウンされない場合、インタフェース状態には以下のガイドラインが適用されます。

- VLAN 内のすべてのポートがダウンしている場合、VLAN インタフェースはダウンしています。
- VLAN 内の 1 つ以上のポートがアップしている場合、VLAN インタフェースはアップしています。

このコマンドを使用して VLAN インタフェースをシャットダウンしても、VLAN インタフェースは DOWN (管理上) 状態のままです。この場合、VLAN インタフェースの状態は、VLAN 内のポートの状態の影響を受けません。

VLAN インタフェースのパラメータを設定する前に、このコマンドを使用して VLAN をシャットダウンし、設定がネットワークに影響を与えないようにします。VLAN インタフェースの設定が完了したら、**undo shutdown** コマンドを使用して設定を有効にします。

障害が発生した VLAN インタフェースをトラブルシューティングするには、インタフェースで **shutdown** コマンドを使用してから、**undo shutdown** コマンドを使用して回復するかどうかを確認します。

VLAN では、各 Ethernet インタフェースの状態は、VLAN インタフェースの状態に依存しません。

3.3.1 VLAN インタフェースの基本設定

VLANインタフェースを作成する前に、対応するVLANが作成されている必要があります。

以下に VLAN インタフェースの基本設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. VLAN インタフェースを作成し、VLAN interface view に移行する	**interface vlan-interface** *interface-number*	デフォルト：設定なし VLANが存在する場合、直接そのviewに移行します。
3. VLAN インタフェースに IP アドレスを割り当てる	**ip address** *ip-address* { *mask* | *mask-length* } [**sub**]	デフォルト：設定なし
4. VLAN インタフェースの説明を設定する	**description** *text*	デフォルト: VLANインタフェース名。 たとえば**Vlan-interface1 Interface**です。
5. （オプション設定項目）VLAN インタフェースをアップ状態にする	**undo shutdown**	デフォルト：**undo shutdown**

3.4 ポートベースVLANの設定

3.4.1 概要

ポートベース VLAN はポートに VLAN を割り当てます。VLAN を割り当てられたポートはその VLAN のトラフィックだけを転送します。

I. ポートリンクタイプ

ポートリンクタイプはアクセス、トランク、ハイブリッドに設定することができます。3つのリンクタイプは、異なる VLAN タグの処理方法を使用します。

- **アクセス**ーアクセスポートは 1 つの VLAN にのみ所属することができます。タグが付与されずにパケットを送信します。通常、PC が直接接続されるポートはアクセスポートに設定します。アクセスポートは、以下の場合に使用されます。
  - □ VLAN パケットをサポートしない端末に接続します。
  - □ VLAN を区別できない装置に接続します。
- **トランク**ートランクポートは複数の VLAN に所属することができ、複数の VLAN のトラフィックを送受信可能です。デフォルト VLAN（PVID）以外のトラフィックがトランクポートを通過するとき、そのトラフィックには VLAN タグが付与されます。トランクポートは通常、同じ VLAN を持つネットワーク装置と接続するのに使用されます。
- **ハイブリッド**ーハイブリッドポートは複数の VLAN からパケットを転送することができます。ハイブリッドポートに転送されたパケットのタグの状態はポートの設定に依存します。

II. PVID

PVID は、ポートのデフォルト VLAN です。ポートで受信されたタグなしパケットは PVID のポートから受信されたパケットとして認識されます。

ポートに PVID を設定する際は、以下の制限とガイドラインに従ってください。

- アクセスポートは 1 つの VLAN にのみ属しているため、その VLAN 以外へ PVID を変更することはできません。
- トランクまたはハイブリッドポートは複数の VLAN と PVID 設定をサポートします。
- アクセスポートで **undo vlan** コマンドで PVID を削除すると、ポートのタイプによって以下のいずれかの動作をします。
  - □ アクセスポートでは、PVID は VLAN1 になります。
  - □ トランクまたはハイブリッドポートでは、PVID の設定に影響はありません。

  トランクまたはハイブリッドポートでは存在しない VLAN を PVID として設定することができますが、アクセスポートではできません。
- ローカルとリモートで同じ PVID を設定することを推奨します。
- ポートで PVID からのパケットとタグなしパケットを廃棄しないように、ポートを PVID に割り当ててください。

III. 異なるリンクタイプの処理方法

アクション	アクセス	トランク	ハイブリッド
VLANタグなしフレームの入力フレーム処理	PVIDのタグを各フレームに付与します。	• PVIDがポートで許可されている場合、PVIDのタグを各フレームに付与します。 • PVIDがポートで許可されていない場合、フレームを廃棄します。	
VLANタグ付きフレームの入力フレーム処理	• PVIDのタグが付いたフレームのみ受信します。 • PVID以外のタグ付きフレームは破棄します。	• VLANがポートで許可されている場合、フレームを受信します。 • VLANがポートで許可されていない場合、フレームを廃棄します。	
出力フレーム処理	VLANのタグを外して送信します。	• PVIDのタグが付いたフレームはタグを外して送信します。 • PVID以外の許可されているVLANの場合、タグを付けたまま送信します。	PVIDを含めた**port hybrid vlan**コマンドの設定に従います。タグを付けたまま送信するか、タグを外して送信します。

3.4.2 アクセスポート VLAN の設定

VLAN view あるいは interface view でアクセスポートを VLAN に割り当てることができます。

アクセスポートを VLAN に割り当てる前に、対応する VLAN が作成されている必要があります。

I. VLAN view でのアクセス VLAN の設定方法

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． VLAN view 移行する	**vlan** *vlan-id*	ー
3． アクセスポートを VLAN に割り当てる	**port** *interface-list*	デフォルト：VLAN 1

II. interface view でのアクセス VLAN の設定方法

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． interface view に移行する	● Ethernet interface viewに移行する： **interface** *interface-type interface-number* ● aggregate interface viewに移行する： **interface bridge-aggregation** *interface-number*	ー
3． リンクタイプをアクセスに設定する	**port link-type access**	デフォルト：アクセス
4． （オプション設定項目）アクセスポートを VLAN に割り当てる	**port access vlan** *vlan-id*	デフォルト：VLAN1に属します。

3.4.3 トランクポート VLAN の設定

トランクポートは複数の VLAN に所属すことができます。トランクポート VLAN の設定は、interface view で VLAN に割り当てることができます。

VLAN にトランクポートを割り当てるとき、以下の制限とガイドラインに従ってください。

- ポートリンクタイプをトランクからハイブリッド（またはその逆）に直接変更することはできません。最初にリンクタイプをアクセスにしてから目的のタイプへ変更してください。
- PVID からのパケットを転送するために、トランクポートに PVID を設定した後に、**port trunk permit vlan** コマンドで PVID を許可する必要があります。

以下にトランクポートを VLAN に割り当てる設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． interface view に移行する	● interface viewに移行する： **interface** *interface-type interface-number* ● aggregate interface viewに移行する： **interface bridge-aggregation** *interface-number*	ー

操作	コマンド	補足
3. リンクタイプをトランクに設定する	**port link-type trunk**	デフォルト：アクセス
4. トランクポートで許可する VLAN を設定する	**port trunk permit vlan** { *vlan-id-list* | **all** }	デフォルト：vlan1のみ許可
5. （オプション設定項目）トランクポートの PVID を設定する	**port trunk pvid vlan** *vlan-id*	デフォルト： VLAN 1

3.4.4 ハイブリッドポート VLAN の設定

ハイブリッドポートは複数の VLAN に所属することができます。ハイブリッドポート VLAN の設定は、interface view で VLAN に割り当てることができます。ハイブリッドポートを VLAN に割り当てる前に、対応する VLAN が作成されている必要があります。

VLAN にハイブリッドポートを割り当てるとき、以下のガイドラインに従ってください。

- ポートリンクタイプをトランクからハイブリッド（またはその逆）に直接変更することはできません。最初にリンクタイプをアクセスにしてから目的のタイプへ変更してください。
- PVIDからのパケットを転送するためには、トランクポートにPVIDを設定した後に、**port hybrid vlan** コマンドで PVID を許可する必要があります。

以下にハイブリッドポートを VLAN に割り当てる設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. interface view に移行する	• interface viewに移行する：**interface** *interface-type interface-number* • aggregate interface viewに移行する：**interface bridge-aggregation** *interface-number*	ー
3. リンクタイプをハイブリッドに設定する	**port link-type hybrid**	デフォルト：アクセス
4. ハイブリッドポートで許可する VLAN を設定する	**port hybrid vlan** *vlan-id-list* { **tagged** | **untagged** }	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。
5. （オプション設定項目）ハイブリッドポートの PVID を設定する	**port hybrid pvid vlan** *vlan-id*	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。

3.5 VLANの表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
VLANインタフェース情報を表示する	**display interface vlan-interface** [*interface-number*] [**brief**]
VLAN情報を表示する	**display vlan** [*vlan-id1* [**to** *vlan-id2*] | **all** | **dynamic** | **reserved** | **static**]
VLANの概要情報を表示する	**display vlan brief**
装置のハイブリッドあるいはトランクポートを表示する	**display port** { **hybrid** | **trunk** }
VLANインタフェースの統計情報を削除する	**reset counters interface vlan-interface** [*interface-number*]

🕮 **メモ：**

reset counters interface コマンドの詳細は、QX-W2300AC シリーズアクセスコントローラコマンドマニュアルの“*4 インタフェース*”を参照してください。

3.6 VLAN の設定例

3.6.1 ポートベース VLAN の設定例

I. ネットワーク要件

図 3-3に示すように、設定します。

- Host A と Host C は部門 A に属しており、VLAN 100 が部門 A に割り当てられています。
- Host B と Host D は B 部門に属しており、VLAN 200 は B 部門に割り当てられています。

同じ部門のホストだけが相互に通信できるように、ポートベース VLAN を設定します。

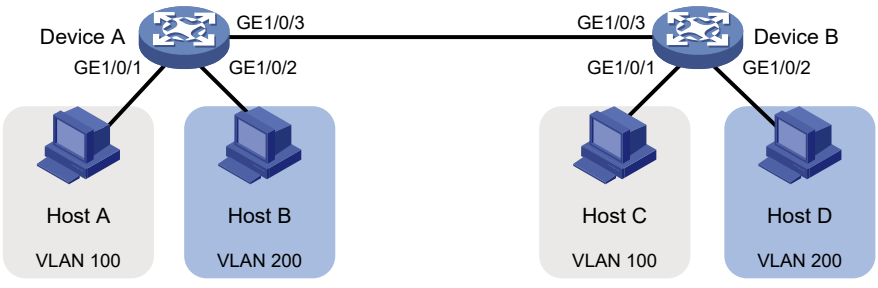


図 3-3 ネットワーク図

II. 設定手順

1)　Device A を設定します。

VLAN 100 を作成し、GigabitEthernet 1/0/1 を VLAN 100 に割り当てます。

```
<DeviceA> system-view
[DeviceA] vlan 100
[DeviceA-vlan100] port gigabitethernet 1/0/1
[DeviceA-vlan100] quit
```

VLAN 200 を作成し、GigabitEthernet 1/0/2 を VLAN 200 に割り当てます。

```
[DeviceA] vlan 200
[DeviceA-vlan200] port gigabitethernet 1/0/2
[DeviceA-vlan200] quit
```

GigabitEthernet 1/0/3 をトランクポートとして設定し、このポートを VLAN 100 および 200 に割り当てます。

```
[DeviceA] interface gigabitethernet 1/0/3
[DeviceA-GigabitEthernet1/0/3] port link-type trunk
[DeviceA-GigabitEthernet1/0/3] port trunk permit vlan 100 200
Please wait... Done.
```

2) Device A と同じ方法で Device B を設定します。(詳細は省略します。)
3) ホストを設定します。

a) Host A とHost C が同じ IP サブネット上になるように設定します。 たとえば、192.168.100.0/24 です。

b) Host B とHost D が同じ IP サブネットになるように設定します。 たとえば、192.168.200.0/24 です。

III. 設定の確認

Host A と Host C は相互に ping できるが、両方とも Host B と Host D に ping できないことを確認します。(詳細は省略します。)

Host B と Host D は相互に ping できるが、両方とも Host A と Host C に ping できないことを確認します。(詳細は省略します。)

Device A で VLAN 100 および 200 が正しく設定されていることを確認します。

[DeviceA-GigabitEthernet1/0/3] display vlan 100

```
VLAN ID: 100
 VLAN type: Static
 Route interface: Not configured
 Description: VLAN 0100
 Name: VLAN 0100
 Tagged ports:
    GigabitEthernet1/0/3
 Untagged ports:
    GigabitEthernet1/0/1
```

[DeviceA-GigabitEthernet1/0/3] display vlan 200

```
VLAN ID: 200
 VLAN type: Static
 Route interface: Not configured
 Description: VLAN 0200
 Name: VLAN 0200
 Tagged ports:
    GigabitEthernet1/0/3
 Untagged ports:
    GigabitEthernet1/0/2
```

目次

このセクションのページは**5-x-x** です。

4章 ループ検出 4-1
4.1 概要 4-1
4.1.1 ループ検出メカニズム 4-1
4.1.2 ループ検出間隔 4-2
4.1.3 ループ保護アクション 4-2
4.1.4 ポート状態自動回復 4-3
4.2 ループ検出設定作業リスト 4-3
4.3 ループ検出の有効化 4-3
4.3.1 グローバルでのループ検出の有効化 4-4
4.3.2 ポートでのループ検出の有効化 4-4
4.4 ループ保護アクションの設定 4-4
4.4.1 グローバルでのループ保護アクションの設定 4-4
4.4.2 Ethernetインタフェースでのループ保護アクションの設定 4-5
4.4.3 アグリゲートインタフェースでのループ保護アクションの設定 4-5
4.5 ループ検出間隔の設定 4-5
4.6 ループ検出の表示と維持 4-5
4.7 ループ検出設定例 4-6
4.7.1 ネットワーク要件 4-6
4.7.2 設定手順 4-6
4.7.3 設定の確認 4-8

4章 ループ検出

4.1 概要

不正なネットワークの接続あるいは設定は、レイヤ 2 のループを発生させます。ループができると送信されたデータがループ内を無限に巡り続け、回線が圧迫されて通信ができなくなり、ネットワーク機器が過負荷になって性能が低下するなどの、ネットワーク障害を引き起こす原因となります。

ループ検出機能は、ループが発生した場合、ネットワークの接続と設定に対応するように通知させるため、すぐさまログを作成します。ループ検出はネットワークの接続と設定をシャットダウンすることができます。ログは Information center で維持されます。詳細は QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“3 *システム管理*”の”*5 章 Information Center*”を参照してください。

4.1.1 ループ検出メカニズム

装置は検出フレームを送信し、装置のポートからフレームが戻るかどうかを確認することでループを検出します。検出した場合、装置はループされたリンクに接続されていると認識します。

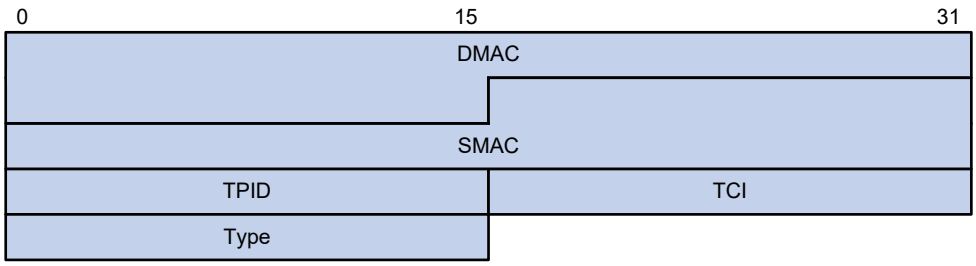


図 4-1 ループ検出のイーサネットフレームヘッダ

ループ検出のイーサネットフレームヘッダは以下のフィールドがあります。

- **DMAC** – フレームの宛先 MAC アドレスです。MAC アドレスは、マルチキャスト MAC アドレス 010F-E200-0007 です。ループ検出機能が有効で、この宛先 MAC アドレスのフレームを受信したとき、以下の処理を行います。
  - □ CPU にフレームを送信します。
  - □ フレームを最初に受信した VLAN にフラッドします。
- **SMAC** – フレームの送信元 MAC アドレスで、送信している装置の MAC アドレスです。
- **TPID** – VLAN タグのタイプで、0x8100 です。
- **TCI** – VLAN タグの情報で優先度と VLAN ID が含まれます。
- **Type** – プロトコルタイプで、0x8918 です。

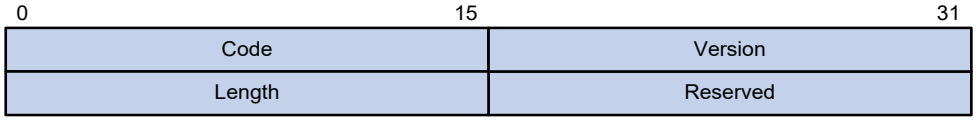


図 4-2 ループ検出の内部フレームヘッダ

ループ検出の内部フレームヘッダは以下のフィールドがあります。

- **Code** – プロトコルサブタイプで、0x0001 です。ループ検出プロトコルを含みます。
- **Version** – プロトコルバージョンで、0x0000 です。
- **Length** – フレーム長です。値は内部ヘッダを含みますが、イーサネットヘッダは含みません。
- **Reserved** – 予約されたフィールドです。

ループ検出のフレームは TLV（タイプ、長さ、値）としてカプセル化されます。

表 4-1 ループ検出でサポートされる TLV

TLV	説明	補足
End of PDU	PDUの最後	オプション
Device ID	送信装置のBridge MACアドレス	必須
Port ID	ポートを送信するPDUのID	オプション
Port Name	ポートを送信するPDU名	オプション
System Name	装置名	オプション
Chassis ID	ポートを送信するシャーシID	オプション
Slot ID	ポートを送信するスロットID	オプション
Sub Slot ID	ポートを送信するサブスロットID	オプション

4.1.2 ループ検出間隔

ループ検出は、ネットワークの変化に対して連続して対応します。ループ検出フレームは、指定された間隔（ループ検出間隔と呼ばれます）で、ポートにループが発生したかどうか、ループが取り除かれたかどうかを確認するために送信されます。

4.1.3 ループ保護アクション

装置がポートを検出したとき、ログを作成しますが、デフォルトでポートに何らかのアクションは実行しません。以下のアクションのうちの１つのアクションを行うように設定することができます。

- **Block** – ポートが MAC アドレスを学習することを無効にし、ポートに受信されるトラフィックをブロックします。
- **No-learning** – ポートが MAC アドレスを学習することを無効にします。
- **Shutdown** – 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。

4.1.4 ポート状態自動回復

block、**no-learning** ポートを設定した装置がポートでループを検出すると、アクションを開始しループ検出間隔の 3 倍の時間待ちます。もしポートでループを検出してからループ検出間隔の 3 倍の期間内にループ検出フレームを受信しない場合、以下の動作をします。

- 装置は自動的にポートを転送状態に設定します。
- ユーザにイベントを通知します。

loopback-detection action shutdown コマンドが使用されたとき、装置は以下の動作をします。

1) 装置は自動的にポートをシャットダウンします。
2) **shutdown-interval** コマンドで設定された検出タイマが満了したのち、装置は自動的にポートを転送状態に設定します。
3) 検出タイマが満了するときにループが検出されると、装置は再びポートをシャットダウンします。

この処理はループが削除されるまで繰り返されます。

🕮 **メモ：**

ループ検出フレームが負荷抑制機能などで削除されることによって、ループが継続していても誤って回復する場合があります。この現象を避けるためには、**shutdown** アクションを使用するか、手動でループを取り除いてください。

4.2 ループ検出設定作業リスト

作業リスト
（必須設定項目）ループ検出の有効化
（オプション設定項目）ループ保護アクションの設定
（オプション設定項目）ループ検出間隔の設定

4.3 ループ検出の有効化

ループ検出はグローバルあるいは指定されたポートで有効にすることができます。グローバルの設定は、指定された VLAN のすべてのポートに適用されます。ポートが指定された VLAN に属しているとき、ポート毎の設定は、個別のポートにのみ適用されます。ポートでの設定はグローバルでの設定より優先されます。

🕮 **メモ：**

ループ検出はネットワーク上の本装置よりも上位のスイッチで行なうことを推奨します。

4.3.1 グローバルでのループ検出の有効化

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. グローバルでループ検出を有効にする	**loopback-detection global enable vlan** { *vlan-id-list* | **all** }	デフォルト：無効 すべてのVLANで無効です。

4.3.2 ポートでのループ検出の有効化

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. Ethernet interface view あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	ー
3. ポートでループ検出を有効にする	**loopback-detection enable vlan** { *vlan-id-list* | **all** }	デフォルト：無効

4.4 ループ保護アクションの設定

ループ保護アクションはグローバルあるいは指定されたポートで有効にすることができます。グローバルの設定は、指定された VLAN のすべてのポートに適用されます。ポート毎の設定は、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場合、ポートをシャットダウンする際、ループ状態を解除するため、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が行われると、**display interface** コマンドの Current state フィールドが DOWN（Loopback detection down）と表示されます。

4.4.1 グローバルでのループ保護アクションの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. グローバルでループ保護アクションを設定する	**loopback-detection global action shutdown**	デフォルト：ループを検出したときアクションは実行しませんがログを出力します。

4.4.2 Ethernet インタフェースでのループ保護アクションの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． Ethernet interface view に移行する	**interface** *interface-type interface-number*	―
3． インタフェースでループ保護アクションを設定する	**loopback-detection action** { **block** | **no-learning** | **shutdown** }	デフォルト : ループを検出したときアクションは実行しませんがログを出力します。

4.4.3 アグリゲートインタフェースでのループ保護アクションの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． aggregate interface view に移行する	**interface bridge-aggregation** *interface-number*	―
3． アグリゲートインタフェースでループ保護アクションを設定する.	**loopback-detection action shutdown**	デフォルト : ループを検出したときアクションは実行しませんがログを出力します。

4.5 ループ検出間隔の設定

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。短い間隔では検出感度が上がりますが、より多くのリソースが消費されます。ループ検出間隔の設定を行うときには、システムのパフォーマンスとループ検出速度を考慮してください。

以下にループ検出間隔の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． ループ検出間隔を設定する	**loopback-detection interval-time** *interval*	デフォルト：30秒

4.6 ループ検出の表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
ループ検出の設定と状態を表示する	**display loopback-detection**

4.7 ループ検出設定例

4.7.1 ネットワーク要件

図 4-3に示すようなループ接続を行なった場合に、Device A がループを検出して自動的にポートのシャットダウンを行うようにループ検出の設定を行います。

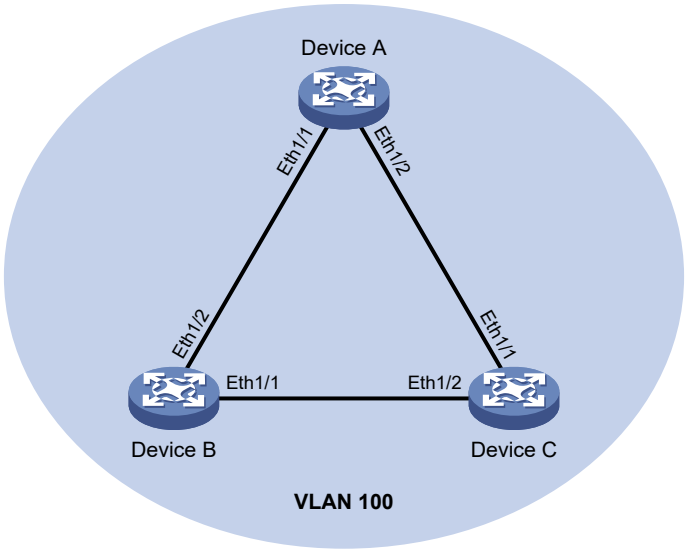


図 4-3 ネットワーク図

4.7.2 設定手順

1)　Device A を設定します。

VLAN 100 を作成し、グローバルにループ検出を設定します。

```
<DeviceA> system-view
[DeviceA] vlan 100
[DeviceA-vlan100] quit
[DeviceA] loopback-detection global enable vlan 100
```

GigabitEthernet 1/0/1、GigabitEthernet 1/0/2 をトランクポートとして設定し、VLAN 100 を割り当てます。

```
[DeviceA] interface GigabitEthernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-type trunk
[DeviceA-GigabitEthernet1/0/1] port trunk permit vlan 100
[DeviceA-GigabitEthernet1/0/1] quit
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port link-type trunk
```

```
[DeviceA-GigabitEthernet1/0/2] port trunk permit vlan 100
[DeviceA-GigabitEthernet1/0/2] quit
```

シャットダウンを行うループ保護アクションをグローバルで設定します。

```
[DeviceA] loopback-detection global action shutdown
```

ループ検出間隔を 35 秒に設定します。

```
[DeviceA] loopback-detection interval-time 35
```

2) Device B を設定します。

VLAN 100 を作成します。

```
<DeviceB> system-view
[DeviceB] vlan 100
[DeviceB–vlan100] quit
```

GigabitEthernet 1/0/1、GigabitEthernet 1/0/2 をトランクポートとして設定し、VLAN 100 を割り当てます。

```
[DeviceB] interface GigabitEthernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 100
[DeviceB-GigabitEthernet1/0/1] quit
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] port link-type trunk
[DeviceB-GigabitEthernet1/0/2] port trunk permit vlan 100
[DeviceB-GigabitEthernet1/0/2] quit
```

3) Device C を設定します。

VLAN 100 を作成します。

```
<DeviceC> system-view
[DeviceC] vlan 100
[DeviceC–vlan100] quit
```

GigabitEthernet 1/0/1、GigabitEthernet 1/0/2 をトランクポートとして設定し、VLAN 100 を割り当てます。

```
[DeviceC] interface GigabitEthernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] port link-type trunk
[DeviceC-GigabitEthernet1/0/1] port trunk permit vlan 100
[DeviceC-GigabitEthernet1/0/1] quit
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] port link-type trunk
[DeviceC-GigabitEthernet1/0/2] port trunk permit vlan 100
```

```
[DeviceC-GigabitEthernet1/0/2] quit
```

4.7.3 設定の確認

Device A のログを確認します。

```
[DeviceA]
%Feb 24 15:04:29:663 2013 DeviceA LPDT/4/LPDT LOOPED: Loopback exists on
GigabitEthernet1/0/1.
%Feb 24 15:04:29:667 2013 DeviceA LPDT/4/LPDT LOOPED: Loopback exists on
GigabitEthernet1/0/2.
%Feb 24 15:04:44:243 2013 DeviceA LPDT/5/LPDT RECOVERED: Loopback on
GigabitEthernet1/0/1 recovered.
%Feb 24 15:04:44:248 2013 DeviceA LPDT/5/LPDT RECOVERED: Loopback on
GigabitEthernet1/0/2 recovered.
```

出力内容は、以下のことを示します。

- Device A はループ検出間隔内に GigabitEthernet 1/0/1、GigabitEthernet 1/0/2 のポートでループを検出しました。
- Device A は自動的に GigabitEthernet 1/0/1、GigabitEthernet 1/0/2 をシャットダウンしました。

display loopback-detection コマンドを使用して Device A のループ検出の設定と情報を表示します。

```
[DeviceA] display loopback-detection
Loop detection is enabled.
Loop detection interval is 35 second(s).
No loopback is detected.
```

出力はシャットダウンアクションに従って、GigabitEthernet 1/0/1、GigabitEthernet 1/0/2 ポートがループから開放されたことを示しています。

Device A の GigabitEthernet 1/0/1 の状態を表示します。

```
[DeviceA] display interface gigabitethernet 1/0/1
GigabitEthernet1/0/1 current state: DOWN (Loop detection down)
...
```

出力は、GigabitEthernet 1/0/1 がループ検出アクションによってシャットダウンしていることを示しています。

Device A の GigabitEthernet 1/0/2 の状態を表示します。

```
[DeviceA] display interface gigabitethernet 1/0/2
GigabitEthernet1/0/2 current state: DOWN (Loop detection down)
...
```

出力は、GigabitEthernet 1/0/2 がループ検出アクションによってシャットダウンしていることを示しています。

目次

このセクションのページは **5-x-x** です。

5 章 STP 5-1
5.1 STP 5-1
5.1.1 STP のプロトコルパケット 5-1
5.1.2 STP の基本概念 5-3
5.1.3 STP アルゴリズムの計算プロセス 5-5
5.2 RSTP 5-12
5.3 PVST 5-13
5.4 MSTP 5-13
5.4.1 MSTP の特徴 5-14
5.4.2 MSTP の基本概念 5-14
5.4.3 MSTP の原理 5-18
5.4.4 装置での MSTP の実行 5-19
5.5 プロトコルと規格 5-19
5.6 スパニングツリー設定作業リスト 5-19
5.6.1 STP 設定作業リスト 5-20
5.6.2 RSTP 設定作業リスト 5-21
5.6.3 PVST 設定作業リスト 5-22
5.6.4 MSTP 設定作業リスト 5-23
5.7 動作モードの設定 5-23
5.7.1 設定手順 5-24
5.8 MST region の設定 5-24
5.9 Root Bridge と Secondary Root Bridge の設定 5-25
5.9.1 Root Bridge の設定 5-26
5.9.2 Secondary Root Bridge の設定 5-26
5.10 Bridge プライオリティの設定 5-26
5.11 MST region の最大ホップ数の設定 5-27
5.12 ネットワークダイアメータの設定 5-27
5.13 スパニングツリータイマの設定 5-28
5.13.1 設定の制限とガイドライン 5-28
5.13.2 設定手順 5-29
5.14 タイムアウトファクタの設定 5-29
5.15 BPDU 最大送出レートの設定 5-30
5.16 Edge ポートの設定 5-30
5.16.1 設定の制限とガイドライン 5-30
5.16.2 設定手順 5-30
5.17 Port Path Cost の設定 5-31
5.17.1 デフォルト Path Cost の計算時の基準指定 5-31
5.17.2 Path Cost の設定 5-32
5.18 Port priority の設定 5-33
5.19 Point-to-Point リンクの設定 5-33
5.19.1 設定の制限とガイドライン 5-34
5.19.2 設定手順 5-34
5.20 MSTP パケットのフォーマット設定 5-34
5.21 ポート遷移状態情報の出力の有効化 5-35
5.22 スパニングツリー機能の有効化 5-35

5.22.1 STP/RSTP/MSTP モードでのスパニングツリー機能の有効化 5-35
5.22.2 PVST モードでのスパニングツリー機能の有効化 5-36
5.23 mCheck 機能の設定 5-36
5.23.1 設定の制限とガイドライン 5-37
5.23.2 設定手順 5-37
5.24 Digest Snooping の設定 5-37
5.24.1 設定の制限とガイドライン 5-38
5.24.2 設定手順 5-38
5.24.3 Digest Snooping 設定例 5-39
5.25 No Agreement Check の設定 5-40
5.25.1 設定要件 5-41
5.25.2 設定手順 5-41
5.25.3 No Agreement Check 設定例 5-41
5.26 保護機能の設定 5-42
5.26.1 BPDU ガードの有効化 5-42
5.26.2 Root ガードの有効化 5-43
5.26.3 Loop ガードの有効化 5-44
5.26.4 ポート役割の制限機能 5-45
5.26.5 TC-BPDU ガードの有効化 5-45
5.26.6 PVST BPDU ガード機能の有効化 5-46
5.27 TC BPDU の検出または受信するイベントの記録 5-46
5.28 トポロジ変更イベントによる SNMP notification の有効化 5-47
5.29 スパニングツリーの表示と維持 5-47
5.30 スパニングツリー設定例 5-48
5.30.1 MSTP 設定例 5-48

5章 STP

スパニングツリーは、ループ検出時に物理的に通信しないインタフェースを設定することによりループを防止します。

STP は、狭義では、IEEE802.1d STP を意味しており、広義では IEEE802.1d STP と拡張されたスパニングツリープロトコル（RSTP（Rapid Spanning Tree Protocol）、MSTP（Multiple Spanning Tree Protocol）、PVST（Per-VLAN Spanning Tree）など）を含めたものを意味します。

5.1 STP

STP（Spanning Tree Protocol）は、IEEE の 802.1d で規定されている、LAN（local area network）の円環上（ループ状）に形成されたレイヤ 2 プロトコルにおいてデータトラフィックが永続的に流れ続けることを防止するプロトコルです。

STP が動作している装置は、ネットワークでループを検出します。ほかの装置と情報を交換し、ループがないツリー構成にループの構成を設定させ、特定のポートをブロックすることで、ループを防ぎます。

5.1.1 STP のプロトコルパケット

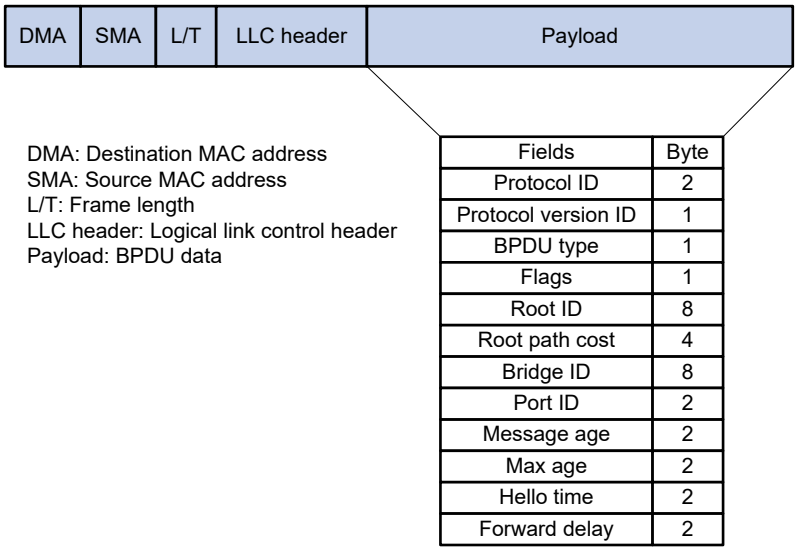
スパニングツリープロトコルでは、リンクレイヤパケットの BPDU（Bridge Protocol Data Units）を使用して、情報交換・状態の維持管理を行います。IEEE802.1d で規定される STP では、以下 2 種類の BPDU を使用します。STP が有効なネットワークの装置は BPDU を交換してスパニングツリーを確立します。BPDU はスパニングツリーの計算を行うために十分な情報を含みます。

STP は以下の BPDU のタイプを使用します。

- **Configuration BPDU** — スパニングツリーを構成しそのツリートポロジを維持するために使います。
- **TCN(Topology change notification) BPDU** — ネットワークトポロジの変更を通知するために使います。

I. Configuration BPDU

STP は、ネットワーク内の装置間で Configuration BPDU を交換することにより、ネットワークトポロジを構築し維持します。0 に Configuration BPDU の形式を示します。



Fields	Byte
Protocol ID	2
Protocol version ID	1
BPDU type	1
Flags	1
Root ID	8
Root path cost	4
Bridge ID	8
Port ID	2
Message age	2
Max age	2
Hello time	2
Forward delay	2

図 5-1 Configuration BPDU の形式

Configuration BPDU には、ネットワークトポロジを構築するための以下のデータが書き込まれています。

- **Protocol ID**－0x0000 で固定です（IEEE802.1d を表します）。
- **Protocol version ID**ースパニングツリープロトコルのバージョン ID。STP のプロトコルバージョンは 0x00 です。
- **BPDU type**ーBPDU のタイプ。Configuration BPDU の値は 0x00 です。
- **Flags**－BPDU の目的を表す 8 ビット領域。最低位ビットは TC（Topology Change）フラッグです。最高位ビットは TCA（Topology Change Acknowledge）フラッグです。他のすべてのビットは予約済みです。
- **Root ID**–Root Bridge の Priority と MAC アドレス。
- **Root path cost**– Root Bridge までの最短ルートのコスト。
- **Bridge ID**ーDesignated Bridge の Priority と MAC アドレス。
- **Port ID**– Designated Port の Priority とグローバルポート番号。
- **Message age**–ネットワーク内で転送された Configuration BPDU の経過時間。
- **Max age**–ネットワーク内で転送された Configuration BPDU の有効時間。
- **Hello time**– Configuration BPDU の転送間隔。
- **Forward delay**–ポートでの転送遅延。

装置は Root ID、Root path cost、Bridge ID、Port ID、Message age、Max age、Hello time、Forward delay を使用してスパニングツリーを計算します。

II. TCN BPDU

図 5-2 に TCN BPDU の形式を示します。

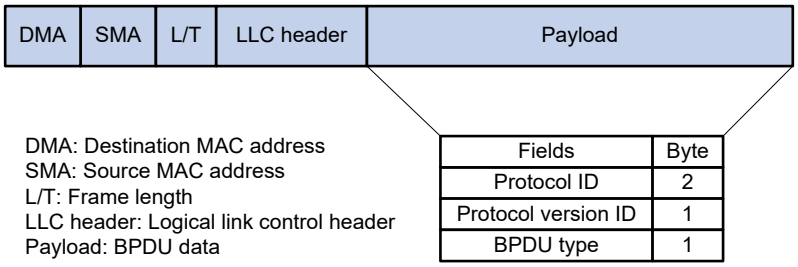


図 5-2 TCN BPDU の形式

TCN BPDU には以下のデータだ書き込まれています。

- **Protocol ID**－0x0000 で固定です（IEEE802.1d を表します）。
- **Protocol version ID**ースパニングツリープロトコルのバージョン ID。STP のプロトコルバージョンは 0x00 です。
- **BPDU type**－BPDU のタイプ。TCN BPDU の値は 0x80 です。

Bridge で以下の事象のいずれかが発生したとき、non-root Bridge は TCN BPDU を送信します。

- ポートが転送状態になり、かつ Bridge が Designated Port を少なくとも 1 つもつ場合。
- ポートが、転送状態もしくは学習状態からブロック状態になった場合。

ネットワークトポロジが変化すると、Non-root Bridge は Root Bridge に通知するために TCN BPDU を使用します。Root Bridge は Configuration BPDU 内の TC フラッグを設定し、他の装置にその TC フラッグを広告します。

5.1.2 STP の基本概念

I. Root bridge

STP のツリーは、1 つの Root ブリッジと複数の他のブリッジで構成されます。ほかのブリッジは“Leaf ノード”と呼ばれます。Root ブリッジはトポロジの変化に応じて変更することができます。

ネットワークの初期設定において、各装置は Root ブリッジとして Configuration BPDU を生成し、定期的に Configuration BPDU を送信します。ネットワークの収束後、Root ブリッジのみが定期的に Configuration BPDU を送信します。ほかの装置は、BPDU を転送するのみとなります。

II. Root port

Root Bridge 以外の装置において、Root Bridge への path cost が最も低い 1 つのポートが Root Port となります。Root Port は、Root Bridge の装置と通信を行うポートになります。なお、Root Bridge の装置には、Root Port はありません。

III. Designated bridge と Designated Port

分類	Designated bridge	Designated port
装置	ローカル装置に直接、接続されている装置でローカルの装置にBPDUの転送を行う	Designated bridgeがこのポートにBPDUを転送する
LAN	LANセグメントにBPDUを転送する	Designated bridge が、このLANセグメントにBPDUを転送する

図 5-3 に示すように、Device B と Device C は直接 LAN に接続されています。

もし Device A がポート A1 を経由して Device B に BPDU を転送する場合、Designated bridge と Designated port は以下のようになります。

- Device B の Designated bridge は Device A です。
- Device B の Designated port は Device A のポート A1 です。

もし Device B が LAN に BPDU を転送する場合は以下のようになります。Designated bridge と Designated port は以下のようになります。

- LAN の Designated bridge は Device B です。
- LAN の Designated port は Device B のポート B2 です。

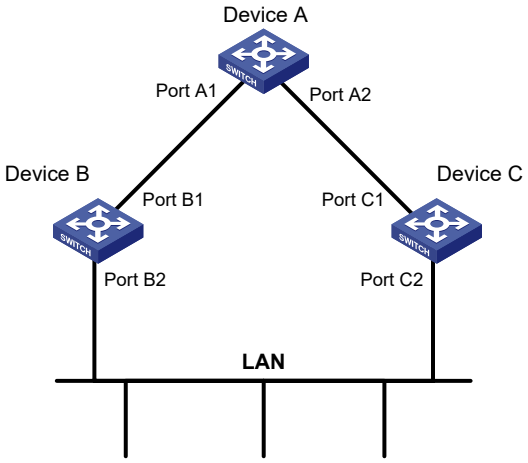


図 5-3 Designated bridge と Designated port

IV. Path cost

path cost は、STP でリンクを選択するのに使用される値です。STP はリンク間の path cost を比較し、最も path cost の小さいリンクを使ったトポロジを構成します。STP はループがないようにネットワークを構成させるため、冗長な STP のリンクをブロックします。

5.1.3 STP アルゴリズムの計算プロセス

スパニングツリーのアルゴリズムは以下の計算プロセスを使用しています。動作をわかりやすくするため、簡略化した処理の例をもとに説明します。

I. 計算プロセス

STP アルゴリズムは以下のプロセスを使用します。

1)　ネットワークの初期化

装置の初期化として、各ポートは以下の内容で Configuration BPDU を作成します。

- □　ポートを Designated port とします。
- □　装置自身を Root Bridge とします。
- □　Root Path Cost を 0 とします。
- □　Designated Bridge ID を自身の装置 ID とします。

2)　root bridge の選択

最初にネットワーク上の STP が有効な各装置は、自身が Root bridge として仮定し、Root Bridge を自身の Device ID とします。Configuration BPDU の交換を行うことによって、装置は自身の root bridge ID と、root bridge となる最も小さい root bridge ID の装置を選択するため、root bridge ID を比較します。

3)　root bridge でない root port と Designated port を選択します。

操作	説明
1	非root bridgeの装置は、最も優先度の高いConfiguration BPDUを受信したポートをroot portと認識します。表 5-1にConfiguration BPDUを選択する方法を記載します。
2	Configuration BPDUとroot portのpath costをもとにして、装置はほかのポートのDesignated PortのConfiguration BPDUを計算します。 ● Root Bridge IDをRoot Portで受信したConfiguration BPDUのRoot Bridge IDに書き換えます。 ● Root Port CostをRoot Portで受信するConfiguration BPDUのRoot Port CostにRoot PortのPath Costを加算した値に書き換えます ● Designated Bridge IDをその装置のBridge IDに書き換えます。 ● Designated Port IDを出力ポートのIDに書き換えます。
3	書き換えたConfiguration BPDUとそのポートで受信するConfiguration BPDUを比較することで、そのポートの役割が決まります。 ● 書き換えたConfiguration BPDUの優先度が高い場合、そのポートはDesignated Portになり、書き換えたConfiguration BPDUを定期的に送信します。 ● そのポートで受信するConfiguration BPDUの優先度が高い場合、そのポートからConfiguration BPDUを送出することを止め、対向装置からのConfiguration BPDUの受信だけを行います。

ネットワークのトポロジが安定している場合、root port と Designated Port はユーザのトラフィックのみを転送します。ほかのブロックされたポートは BPDU の受信のみを行い、BPDU やトラフィックの転送を行いません。

表 5-1 最も優先度の高い Configuration BPDU の選出

操作	アクション
1	ポートでConfiguration BPDUを受信し、装置はポートによって作成されたConfiguration BPDUと受信したConfiguration BPDUの優先度を比較します。 ● もし受信したConfiguration BPDUの優先度が低い場合、装置は受信したConfiguration BPDUを廃棄し、ポートで作成されたConfiguration BPDUを保存します。 ● もし受信したConfiguration BPDUの優先度が高い場合、受信したConfiguration BPDUの内容にもとづいてポートで作成したConfiguration BPDUの内容を書き換えます。
2	装置はすべてのConfiguration BPDUを比較し、最も優先度の高いConfiguration BPDUを選出します。

以下に Configuration BPDU の比較順序を示します。

a) Root Bridge ID が最も小さいConfiguration BPDUの優先度が最も高くなります。

b) すべてのConfiguration BPDU のRoot Bridge IDが同じ場合には、次にRoot Path Costを比較します。Configuration BPDUのRoot Path Costとその受信ポートのPath Costの加算値の最も小さいConfiguration BPDUの優先度が高くなります。たとえばConfiguration BPDUのroot path costと受信したポートのpath costがSとします。最も小さいSのConfiguration BPDUが最も高い優先度となります。

c) すべてのConfiguration BPDU のRoot Bridge IDとSが同じ場合、以下の領域を順に比較します。

- □ Designated Bridge ID
- □ Designated Port ID
- □ 受信したポートの ID

Designated Bridge ID、Designated Port ID あるいは受信したポートの ID の小さい Configuration BPDU が選択されます。

Root bridge のとき、ツリー構造のトポロジは、root port、Designated Port が選択されます。

II. STP アルゴリズム計算の例

図 5-4 に STP アルゴリズムの計算例を示します。

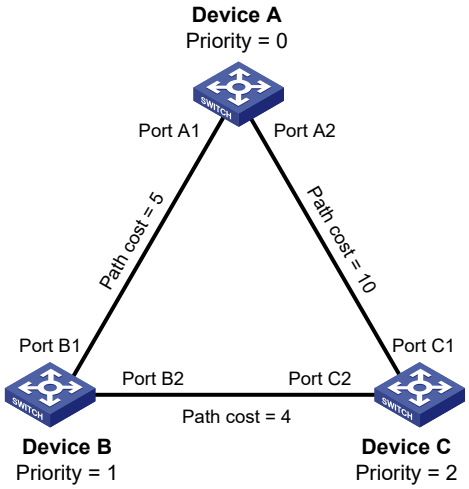


図 5-4 STP アルゴリズム

図 5-4 に示すように、Device A、Device B、Device C の優先度の値は、それぞれ 0、1、2 で、3 つの装置間のリンク path cost は、それぞれ 5、10、4 です。

1)　装置の初期状態

表 5-2 に示すように各 Configuration BPDU は root bridge ID、root path cost、designated bridge ID、Designated Port ID を含みます。

表 5-2 各装置の初期状態

装置	ポート名	ポートの Configuration BPDU
Device A	ポートA1	{0, 0, 0, Port A1}
	ポートA2	{0, 0, 0, Port A2}
Device B	ポートB1	{1, 0, 1, Port B1}
	ポートB2	{1, 0, 1, Port B2}
Device C	ポートC1	{2, 0, 2, Port C1}
	ポートC2	{2, 0, 2, Port C2}

2)　各装置の Configuration BPDU を比較します。

表 5-3 において、各 Configuration BPDU は root bridge ID、root path cost、designated bridge ID、designated port ID を含みます。

表 5-3 各装置の比較プロセスと結果

装置	比較プロセス	比較後のポートの Configuration BPDU
Device A	ポート A1 は以下の操作をします。 1. Device B の Configuration BPDU {1,0,1,ポート B1} を受信します。 2. ローカルポートの Configuration BPDU {0,0,0, ポート A1} が設定を受信したメッセージより優位であることを出します。 3. 受信した Configuration BPDU を破棄します。 ポート A2 は以下の操作をします。 1. Device C の Configuration BPDU {2,0,2, ポート C1} を受信します。 2. ローカルポートの Configuration BPDU {0,0,0, ポート A2} が受信した Configuration BPDU より優位であることをと検出します。 3. 受信した Configuration BPDU を破棄します。 Device A は、Device A の全ポートの Configuration BPDU のRoot Bridgeおよび designated Bridgeが Device A であることを検出するとそれ自体をRoot Bridgeとみなします。この場合、Device A は各ポートのConfiguration BPDU に対して何の変更も行わず、定期的に Configuration BPDU の送信をはじめます。	• ポートA1: {0, 0, 0,ポート A1} • ポートA2: {0, 0, 0,ポート A2}
Device B	ポート B1 は以下の操作をします。 1. Device A の Configuration BPDU {0,0,0, ポート A1} を受信します。 2. 受信した Configuration BPDU がローカルポートの Configuration BPDU {1, 0, 1,ポート B1} より優位であることを検出します。 3. ポート B1 の Configuration BPDU を更新します。 ポートB2 は以下の操作をします。 1. Device C の Configuration BPDU {2,0,2, ポート C2} を受信します。 2. ローカルポートの Configuration BPDU {1,0,1, ポート B2} が受信した Configuration BPDU より優位であることを検出します。 3. 受信した Configuration BPDU を破棄します。	• ポートB1: {0, 0, 0, ポート A1} • ポートB2: {1, 0, 1, ポート B2}

装置	比較プロセス	比較後のポートの Configuration BPDU
	Device B は以下の操作をします。 1. すべてのポートの Configuration BPDU を比較します。 2. ポート B1 の Configuration BPDU が最適な Configuration BPDU であると判断します。 3. ポート B1 を Root Port として使い、その Configuration BPDU は変更しません。 ポートB1 のConfiguration BPDU およびRoot Port のパス コスト にもとづき、ポートB2 の Configuration BPDUのdesignated {0,5,1, ポートB2} を計算します。Device B は計算した Configuration BPDU {0,5,1, ポートB2} とポートB2 のConfiguration BPDU を比較します。計算した Configuration BPDU が優位であれば ポートB2 はdesignated Portとなります。このポートの Configuration BPDUは計算したConfiguration BPDU に置き換えられ、定期的に送信されます。	• Root port (ポートB1): {0, 0, 0, ポートA1} • Designated port (ポート B2): {0, 5, 1, ポートB2}
Device C	ポートC1 は以下の操作をします。 1. Device A の Configuration BPDU{0,0,0, ポート A2}を受信します。 2. 受信した Configuration BPDU がローカル ポートの Configuration BPDU{2,0,2, ポート C1}より優位であることを検出します。 3. ポート C1 の Configuration BPDU を更新します。 ポートC2 は以下の操作をします。 1. メッセージが更新される前に、Device B のポート B2 の Configuration BPDU{1,0,1, ポート B2}を受信します。 2. 受信した Configuration BPDU がローカル ポートの Configuration BPDU{2,0,2, ポート C2}より優位であることを検出します。 3. ポート C2 の Configuration BPDU を更新します。	• ポートC1: {0, 0, 0, ポート A2} • ポートC2: {1, 0, 1, ポート B2}

装置	比較プロセス	比較後のポートの Configuration BPDU
	Device C は以下の操作をします。 1. すべてのポートの Configuration BPDU を比較します。 2. ポート C1 の Configuration BPDU が最適な Configuration BPDU であると判断します。 3. ポート C1 を Root Port として使い、その Configuration BPDU は変更しません。 ポートC1 のConfiguration BPDU およびRoot Port のパス コスト にもとづき、ポートC2 の Configuration BPDUのdesignated {0,10,2, ポートC2} を計算します。Device C は計算した Configuration BPDU {1,0,1, ポートB2} とポートC2 のConfiguration BPDU を比較します。計算した Configuration BPDU が優位であれば ポートC2 はdesignated Portとなります。このポートの Configuration BPDUは計算したConfiguration BPDU に置き換えられます。	• Root port (ポートC1): {0, 0, 0, ポートA2} • Designated port (ポートC2): {0, 10, 2, ポートC2}
	ポートC2 は以下の操作をします。 1. 更新された Device B の Configuration BPDU {0,5,1, ポート B2} を受信します。 2. 受信した Configuration BPDU がローカルポートの Configuration BPDU{0,10,2, ポート C2}より優位であることを検出します。 3. ポート C1 の Configuration BPDU を更新します。 ポート C1 は以下の操作をします。 1. Device A から定期的に Configuration BPDU {0,0,0, ポート A2}を受信します。 2. ローカルポートの Configuration BPDU と同じであることを検出します。 3. Configuration BPDU を更新します。	• ポートC1: {0, 0, 0, ポートA2} • ポートC2: {0, 5, 1, ポートB2}

装置	比較プロセス	比較後のポートの Configuration BPDU
	Device Cは、ポートC1のルートパスコスト(10) (受信したConfiguration BPDU(0)のルートパスコスト＋ポートC1のパスコスト(10))は、ポートC2のパスコスト(9)よりも大きいと判断し、ポートC2 のBPDU が最適なConfiguration BPDU と判断します。ポートC2 がルートポートとなり、そのメッセージは変更されません。 Configuration BPDUとルートポートのパスコストにもとづき、Device C は以下の操作をします。 1. ポート C1 の Designated Port の Configuration BPDU {0,9,2, ポート C1}を計算します。 2. それをポート C1 の Configuration BPDU {0,0,0, ポート A2}と比較します。 3. 計算された Configuration BPDU よりもローカルポートの Configuration BPDU が優位であることを検出し、ポート C1 はブロックされ、Configuration BPDU はそのまま変更しません。 ポートC1は、たとえば、Device Bと Device C の間のリンクが切断されるなど、STPの計算プロセスが新しく行われるまで、データを転送しません。	• Blocked port (ポートC1): {0, 0, 0, ポートA2} • Root port (ポートC2): {0, 5, 1, ポートB2}

表 5-3 に記述した比較プロセス後は、Device A を Root Bridge とするスパニングツリーが図 5-5 のように確立されます。

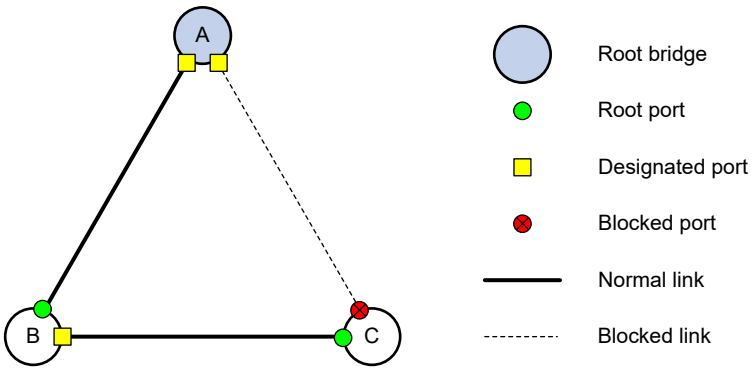


図 5-5 比較プロセス後のスパニングツリー

III. STP の Configuration BPDU 転送メカニズム

STP の Configuration BPDU は以下のガイドラインに従って転送されます。

- ネットワークの初期化をした際、各装置は自身を Root Bridge とみなします。Configuration BPDU を生成し、Hello タイムの間隔で Configuration BPDU を送信します。
- Configuration BPDU を受信した Root Port のプライオリティがポートの Configuration BPDU より高い場合、装置は以下の操作をします。
  - □ Configuration BPDU の有効時間を延ばします。
  - □ Configuration BPDU の時間を計るタイマをスタートさせます。
  - □ Designated Port から Configuration BPDU を送信します。
- Designated Port がローカルポートの Configuration BPDU と比較してプライオリティの低い Configuration BPDU を受信した場合、ローカルポートの Configuration BPDU を返信します。
- 通信ができなくなると、Root Port は、新しい Configuration BPDU を受信せず、古い Configuration BPDU はタイムアウトして破棄されます。 このとき、装置は装置自体をルートとする Configuration BPDU を生成し、その BPDU を送信します。これが新しいスパニング ツリーを計算する契機になり、ネットワークの接続を回復させます。

新しく計算された Configuration BPDU は、すぐにネットワーク内に広まらないため、トポロジの変更を検出していない古い Root Port や Designated Port は古い通信経路でデータの転送を継続します。 新しい Root Port や Designated Port が選出されてから、すぐにデータの転送を開始すると、ループが発生する可能性があります。

IV. STP タイマ

STP には、3 つの重要なパラメータがあります。

- Forward delay

装置の状態が遷移するときの遅延時間です。

リンク障害等が発生すると、STP トポロジは再構築されます。再構築後の Configuration BPDU は、ネットワーク内にすぐには広まらないため、新しく選出された Root Port や Designated Port がすぐにデータの転送をはじめてしまうと、ループが発生する可能性があります。

このため、新しく選出された Root Port または Designated Port は、forwarding ステートに遷移する前に Forward delay タイマの 2 倍の時間を必要とします。これにより、新しい Configuration BPDU をネットワークに広げることができます。

- Hello time

装置が周辺の装置に Hello パケットを送信する間隔です。通信が正常であることを確認するものです。

- Max age

装置の Configuration BPDU が時間切れになっていないかどうかを判断するのに使うパラメータです。 最大有効時間を越えた Configuration BPDU は破棄されます。

5.2 RSTP

RSTP は、新しく選出された Root Port あるいは Designated Port を forwarding 状態にするため、STP よりも高速なネットワークの収束を行います。

以下の場合、新しく選出された Root Port はすぐに forwarding 状態になります。

- 装置の古い Root Port がフォワーディングデータを止めた場合
- 上り方向の designated port が転送をはじめた場合

ほかの装置または共有 LAN セグメントではなくユーザ端末に直接接続した point-to-point リンクのポートあるいは Edge Port に接続されているとき、新しく選出された Designed Port は、直接接続された装置からハンドシェイクの応答を受信した後、即座に forwarding 状態になります。

5.3 PVST

STP または RSTP 対応の LAN では、すべてのブリッジはスパニングツリーを共有します。すべての VLAN からのトラフィックは、スパニングツリーによって転送されます。ループがあった場合、ポートは、VLAN でループをブロックすることができません。

PVST は各 VLAN にそれぞれのスパニングツリーを持たせることができます。スパニングツリーはリンクと帯域幅を増大することができます。各 VLAN が独立して STP または RSTP を動作するため、スパニングツリーは VLAN に対応するだけで動作します。

PVST は、Rapid PVST や PVST が動作するサードパーティ製の装置や NEC の装置と通信することができます。PVST が有効な NEC の装置は、PVST が有効な NEC の装置あるいは Rapid PVST が有効なサードパーティ製の装置と接続したとき、RSTP のように早急なネットワークの収束をサポートします。

ポートのリンクタイプによって送信する BPDU のタイプが異なります。

- アクセスポートは STP BPDU を送信します。
- トランクポートあるいはハイブリッドポートは、VLAN1 の STP BPDU を送信し、ほかの VLAN の PVST BPDU を送信します。

5.4 MSTP

MSTP は以下の STP、RSTP、PVST の制限を克服したものです。

- **STP の制限**–STP は、ポートの高速な状態遷移には対応できません。トポロジの変更が起こった際に、新しく選出された Root Port や Designed Port は、ほかの装置または共有 LAN セグメントではなくユーザ端末に直接接続した point-to-point リンクのポートあるいは Edge Port であっても、forwarding 状態に遷移する前に 2 倍の転送遅延時間を待たなければなりません。
- **RSTP の制限**– RSTP (rapid spanning tree protocol) は、STP よりも収束時間を早くしたにもかかわらず、STP 同様 VLAN 上の全ネットワークブリッジがスパニングツリーを共有するため、冗長リンクを VLAN 毎にブロックできない欠点があります。
- **PVST の制限**–各 VLAN はスパニングツリーを持つため、PVST BPDU の量は、トランクあるいはハイブリッドポートの VLAN の数に比例して増加します。トランクあるいはハイブリッドポートが多くの VLAN を許可しているとき、VLAN スパニングツリーを維持するリソースと計算を行うリソースの両方が劇的に増加します。複数の VLAN があるトランクあるいはハイブリッドポートでステータスの変更がある場合、装置の CPU は影響するスパニングツリーを再計算するために負担がかかります。その結果、ネットワークの性能が低下します。

5.4.1 MSTP の特徴

IEEE802.1s をもとに発展させた MSTP(multiple spanning tree protocol) は、STP、RSTP のデメリットを克服します。ネットワークを高速に収束させるだけでなく、VLAN ごとにデータフローがそれぞれのパスに転送されるので、冗長リンクのロードバランスができます。

MSTP には以下のような特徴があります。

- MSTP は、マッピング テーブルを使用し、MST インスタンスへの VLAN のマッピングを行います。MSTP は、複数の VLAN を 1 つの MST インスタンスにマッピングすることで、通信帯域やリソースの使用を節約できます。
- MSTP によりスイッチ ネットワークは複数の領域に分けられ、それぞれの領域が独立した複数のスパニング ツリーで構成されます。
- MSTP はループのあるネットワークをループのないツリー構造に変え、ネットワーク内でのループを回避します。さらに、MSTP はデータ転送用の冗長パスを複数提供し、データ転送プロセスにおける VLAN データのロードバランスを行います。
- MSTP は STP、RSTP と一部の PVST に互換性があります。

5.4.2 MSTP の基本概念

図 5-6 は 4 つの MST region から構成され、各 MST region は 4 つの MSTP 装置から構成されます。図 5-7 は MST region3 のネットワークトポロジを示します。

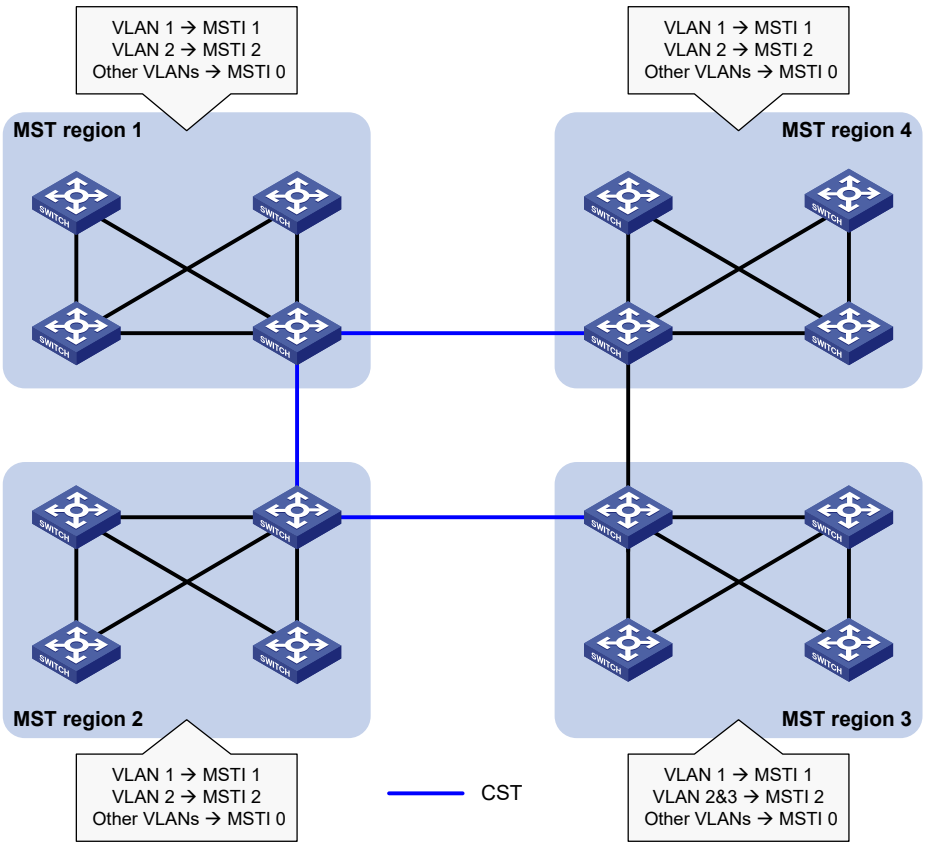


図 5-6 MSTP の基本概念

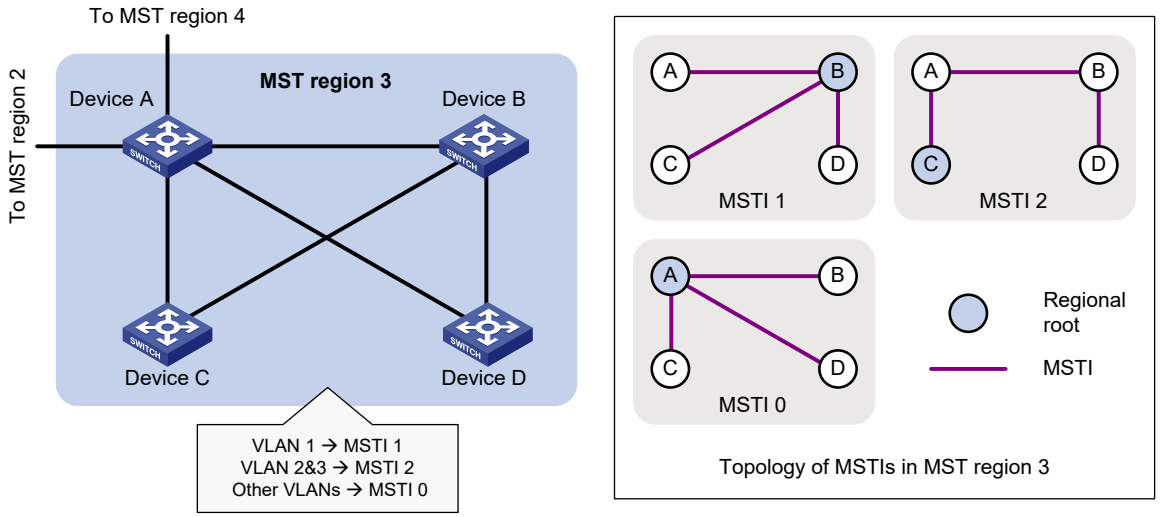


図 5-7 MST region 3 のネットワーク図とトポロジ

I. MST region

複数のスパニングツリーregion(MST region)は、スイッチネットワークの複数の装置と装置間のネットワーク セグメントで構成されています。これらの装置には、以下のような特性があります。

- すべて MSTP を有効にしています。
- 同じ region 名を持っています。
- VLAN-to-instance マッピングの設定が同じです。
- MSTP リビジョン レベルの設定が同じです。
- 物理的に相互にリンクしています。

複数の MST region はスイッチネットワークで使われます。同じ MST region に装置を割り当てることができます。図 5-6 は以下のようになっています。

- スイッチネットワークは MST region1～4 の 4 つの MST region から構成されます。
- 各 MST region のすべての装置は同じ MST region 設定を持ちます。

II. MSTI

MSTP により、複数のスパニングツリーを、ほかから独立したスパニング ツリーとして、1 つの MST region で生成でき、VLAN を指定するために各スパニングツリーでマッピングされます。それぞれのスパニング ツリーは 1 つの MST インスタンス (MSTI(Multiple Spanning Tree Instance)) とみなされます。

図 5-7 では、MSTI 1、MSTI 2、MSTI 0 の 3 つの MSTI があります。

III. VLAN-to-instance マッピングテーブル

VLAN-to-instance マッピング テーブルは VLAN と MST インスタンス間のマッピングの関係ついて、MST region ごとに記載されています。

図 5-7 では、MST region 3 の VLAN-to-instance マッピングテーブルは以下のようになっています。

- VLAN 1 は MSTI 1 にマッピングされています。
- VLAN 2 は MSTI 2 にマッピングされています。
- 残りは MSTI 0 にマッピングされています。

MSTP は、VLAN-to-instance マッピング テーブルを使ってロードバランスを行います。

IV. CST

CST は、スイッチ ネットワークのすべての MST region に接続する 1 つのスパニング ツリーです。MST region をそれぞれ装置とみなすと、CST はこれらの装置が STP または RSTP で計算したスパニング ツリーです。図 5-6 の青い線は CST を表しています。

V. IST

IST(Internal spanning tree)は、MST region で動作するスパニング ツリーです。特別な MSTI で MSTI0 と呼ばれます。デフォルトではすべての VLAN は MSTI0 にマッピングされています。図 5-6 では、MSTI 0 は MST region3 の IST です。

VI. CIST

CIST(common and internal spanning tree)はスイッチネットワークですべての装置に接続する 1 つのスパニングツリーです。CIST は、すべての MST region にある IST と CST で構成されます。図 5-6 では、すべての MST region と inter-region CST を加えた IST(MSTI 0)は、全体の CIST を構成します。

VII. Regional root

MST region 内の IST または MSTI の Root Bridge は、MST またはその MSTI の regional Root Bridge です。トポロジをベースに、MST region のそれぞれのスパニング ツリーが異なる region ルートを持つ場合があります。

図 5-7 の MST region3 では、以下のようになっています。

- MSTI1 の regional ルートは Device B です。
- MSTI2 の regional ルートは Device C です。
- MSTI0(IST)の regional ルートは Device A です。

VIII. 共通 root bridge

共通 Root Bridge は、CIST の root bridge です。

図 5-6 では、 MST Region 1 のスイッチが共通 Root Bridge です。

IX. ポートの役割

異なる MSTI で、ポートは異なる役割を行います。図 5-8 に示すように MST region は Device A、Device B、Device C、Device D があります。Device A のポート A1 とポート A2 は共通 Root Bridge に接続されています。Device B のポート B2、ポート B3 はループしています。Device C のポート C3、ポート C4 はほかの MST region に接続されています。Device D のポート D3 はホストに接続されています。

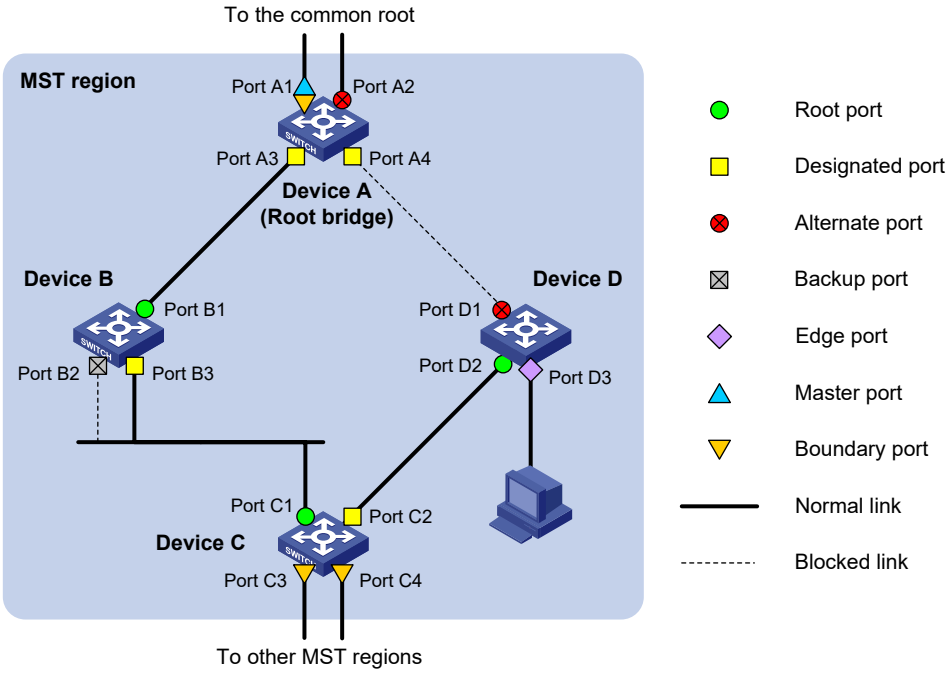


図 5-8 ポートの役割

MSTP では、以下のポートの計算を行っています。

- **Root ポート**–非 root bridge 用にデータを root bridge に転送します。root bridge は root port を持っていません。
- **Designated ポート**–データを下流方向のネットワークセグメントや装置に転送するポートです。
- **Alternate ポート**– Root ポートもしくは Master ポートの代替ポートです。Root ポートもしくは Master ポートがブロッキング状態になると、その代わりに Root ポートもしくは Master ポートになるポートです。
- **Backup ポート**–Designated ポートの代替ポートで、高速な切り替えのために使われます。Designated ポートがブロッキング状態になると、即座にその代わりに Designated ポートになり、データの転送を開始できます。
- **Edge ポート**–ネットワーク装置あるいはネットワークセグメントに接続されていないポートで、ユーザホストに直接接続されています。
- **Master ポート**–MST Region を共通 Root Bridge に接続するポートで、その MST Region における Root ポートでもあります。Master ポートから共通 Root Bridge へのパスは、最短パスとなります。Master ポートはいつも regional root にあるわけではありません。IST や CIST の Root ポートは Root Port で、ほかの MSTI の Master ポートです。
- **Boundary ポート**–MST Region の端点のポートで、ほかの MST Region や STP/RSTP で制御される装置と接続します。MSTP の計算を行うとき、MSTI の boundary port の役割は CIST の役割と同一です。Master ポートになるわけではありません。MSTI の Master ポートは CIST の root port です。

X. ポートの状態

MSTP では、ポートは以下のいずれかの状態になっています。

- **Forwarding**ーこの状態のポートは、BPDU の送受信が可能で、MAC アドレスを学習し、ユーザトラフィックを転送できます。
- **Learning**ーこの状態のポートは、BPDU の送受信が可能で、MAC アドレスを学習しますが、ユーザトラフィックを転送できません。
- **Discarding**ーこの状態のポートは、BPDU の受信のみ可能です。MAC アドレスの学習やユーザトラフィックを転送できません。

🕮 **メモ:**

MSTI が異なると、ポートの状態も異なります。

ポートの状態はポートの役割と排他的ではありません。表 5-4 にポートの役割とポート状態の関係を示します。“〇”はポートがこの状態に対応することを表し、 “×”はポートがこの状態に対応しないことを表します

表 5-4 ポートの役割とポート状態の関係

ポートの役割(右) ポートの状態(下)	Root port/master ポート	Designated ポート	Alternate ポート	Backup ポート
Forwarding	〇	〇	×	×
Learning	〇	〇	×	×
Discarding	〇	〇	〇	〇

5.4.3 MSTP の原理

MSTP はレイヤ 2 ネットワーク全体を複数の MST Region に分割します。MST Region 間で CST を生成し、各 MST Region 内に MSTI と呼ばれる複数のスパニングツリーを生成します。MSTI が 0 の MSTI は IST です。

MSTP では、STP と同様に、スパニングツリーを構成するための情報転送に BPDU を使用します。MSTP 用の BPDU との違いは、MSTP の BPDU に加えて、MSTI 用のパラメータを付加します。

I. CIST の構築

CIST の構築では、以下の処理が行われます

- 最も優先度の高い装置を、CIST の Root として選出します。
- 各 MST Region では IST が構築されます。
- MSTP はそれぞれの MST Region を 1 つの装置とみなして、ネットワークの CST を構築します。

構築された IST と CST で CIST が構成されます。

II. MSTI の構築

MST Region 内では、VLAN マッピングテーブルの情報によって VLAN グループごとの MSTI を構築します。それぞれの MSTI では、STP と同様にスパニングツリーを構成します。詳細は、本章の *“STP アルゴリズムの計算プロセス”* を参照してください。

MSTP では、VLAN パケットは以下のパスに沿って転送されます。

- MST region 内:パケットは対応する MSTI に沿って転送されます。
- MST region 間:パケットは CST に沿って転送されます。

5.4.4 装置での MSTP の実行

MSTP は STP および RSTP と互換性があります。STP および RSTP プロトコルパケットは、MSTP を実行している装置に認識され、スパニング ツリーの計算に使用されます。

基本的な MSTP 機能に加え、以下のような特別な機能を提供することで、管理を容易にします。

- Root bridge の保持
- Root bridge のバックアップ
- Root ガード
- BPDU ガード
- Loop ガード
- TC-BPDU ガード
- ポート役割制限
- TC-BPDU 転送制限機能

5.5 プロトコルと規格

MSTP は以下に示すプロトコルと規格に記載されています。

- IEEE 802.1d, *Media Access Control (MAC) Bridges*
- IEEE 802.1w, *Part 3: Media Access Control (MAC) Bridges–Amendment 2: Rapid Reconfiguration*
- IEEE 802.1s, *Virtual Bridged Local Area Networks–Amendment 3: Multiple Spanning Trees*
- IEEE 802.1Q-REV/D1.3*, Media Access Control (MAC) Bridges and Virtual Bridged Local Area Networks –Clause 13: Spanning tree Protocols*

5.6 スパニングツリー設定作業リスト

スパニングツリーを設定する前に、以下の作業を完了してください。

- 各 MST インスタンス内のそれぞれの装置で使用するプロトコル(STP、RSTP、MSTP、PVST)を定義してください。
- 装置の役割(Root Bridge または leaf node)を定義してください。

スパニングツリーを設定するとき、以下の制限とガイドラインに従ってください。

- スパニングツリーの設定は、サービスループバック、Smart Link と一緒に設定できません。
- system view で行った設定は全体に適用されます。Ethernet interface view で行った設定は、インタフェースでのみ適用されます。aggregate interface view で行った設定は、アグリゲートインタフェースでのみ適用されます。アグリゲーションメンバポートで行った設定は、アグリゲーショングループから取り除かれた後に有効になります。

- アグリゲートインタフェースでスパニングツリーを有効にした後、アグリゲートインタフェースでアルゴリズムの計算が行われます。アグリゲーションメンバポートでは行われません。スパニングツリーは、状態を有効にすることに加えて、対応するアグリゲートインタフェースに一致する各選択されたメンバポートの転送状態を有効にします。
- アグリゲーショングループのメンバポートはスパニングツリーの計算に関与しませんが、ポートは、アグリゲーショングループから取り除かれた後に、MSTP 計算に参加するために、その MSTP 設定を確保しています。

5.6.1 STP 設定作業リスト

作業リスト
root bridgeの設定: ● (必須設定項目) 動作モードの設定 ● (オプション設定項目) Root BridgeとSecondary Root Bridgeの設定 ● (オプション設定項目) Bridgeプライオリティの設定 ● (オプション設定項目) ネットワークダイアメータの設定 ● (オプション設定項目) スパニングツリータイマの設定 ● (オプション設定項目) タイムアウトファクタの設定 ● (オプション設定項目) BPDU最大送出レートの設定 ● (オプション設定項目) ポート遷移状態情報の出力の有効化 ● (必須設定項目) スパニングツリー機能の有効化
leaf nodeの設定: ● (必須設定項目) 動作モードの設定 ● (オプション設定項目) Bridgeプライオリティの設定 ● (オプション設定項目) タイムアウトファクタの設定 ● (オプション設定項目) BPDU最大送出レートの設定 ● (オプション設定項目) Port Path Costの設定 ● (オプション設定項目) Port priorityの設定 ● (オプション設定項目) ポート遷移状態情報の出力の有効化 ● (必須設定項目) スパニングツリー機能の有効化
(オプション設定項目) 保護機能の設定

5.6.2 RSTP 設定作業リスト

作業リスト
root bridgeの設定: ● (必須設定項目) 動作モードの設定 ● (オプション設定項目) Root BridgeとSecondary Root Bridgeの設定 ● (オプション設定項目) Bridgeプライオリティの設定 ● (オプション設定項目) ネットワークダイアメータの設定 ● (オプション設定項目) スパニングツリータイマの設定 ● (オプション設定項目) タイムアウトファクタの設定 ● (オプション設定項目) BPDU最大送出レートの設定 ● (オプション設定項目) Edgeポートの設定 ● (オプション設定項目) Point-to-Pointリンクの設定 ● (オプション設定項目) ポート遷移状態情報の出力の有効化 ● (必須設定項目) スパニングツリー機能の有効化
leaf nodeの設定: ● (必須設定項目) 動作モードの設定 ● (オプション設定項目) Bridgeプライオリティの設定 ● (オプション設定項目) タイムアウトファクタの設定 ● オプション設定項目) BPDU最大送出レートの設定 ● (オプション設定項目) Edgeポートの設定 ● (オプション設定項目) Port Path Costの設定 ● (オプション設定項目) Port priorityの設定 ● (オプション設定項目) Point-to-Pointリンクの設定 ● (オプション設定項目) ポート遷移状態情報の出力の有効化 ● (必須設定項目) スパニングツリー機能の有効化
(オプション設定項目) mCheck機能の設定
(オプション設定項目) 保護機能の設定

5.6.3 PVST 設定作業リスト

作業リスト
root bridgeの設定: • (必須設定項目) 動作モードの設定 • (オプション設定項目) Root BridgeとSecondary Root Bridgeの設定 • (オプション設定項目) Bridgeプライオリティの設定 • (オプション設定項目) ネットワークダイアメータの設定 • (オプション設定項目) スパニングツリータイマの設定 • (オプション設定項目) タイムアウトファクタの設定 • (オプション設定項目) BPDU最大送出レートの設定 • (オプション設定項目) Edgeポートの設定 • (オプション設定項目) Point-to-Pointリンクの設定 • (オプション設定項目) ポート遷移状態情報の出力の有効化 • (必須設定項目) スパニングツリー機能の有効化
leaf nodeの設定: • (必須設定項目) 動作モードの設定 • (オプション設定項目) Bridgeプライオリティの設定 • (オプション設定項目) タイムアウトファクタの設定 • (オプション設定項目) BPDU最大送出レートの設定 • (オプション設定項目) Edgeポートの設定 • (オプション設定項目) Port Path Costの設定 • (オプション設定項目) Port priorityの設定 • (オプション設定項目) Point-to-Pointリンクの設定 • (オプション設定項目) ポート遷移状態情報の出力の有効化 • (必須設定項目) スパニングツリー機能の有効化
(オプション設定項目) mCheck機能の設定
(オプション設定項目) 保護機能の設定
(オプション設定項目) TC BPDUの検出または受信するイベントの記録
(オプション設定項目) トポロジ変更イベントによるSNMP notificationの有効化

5.6.4 MSTP 設定作業リスト

作業リスト
root bridgeの設定: • (必須設定項目) 動作モードの設定 • (必須設定項目) MST regionの設定 • (オプション設定項目) Root BridgeとSecondary Root Bridgeの設定 • (オプション設定項目) Bridgeプライオリティの設定 • (オプション設定項目) MST regionの最大ホップ数の設定 • (オプション設定項目) ネットワークダイアメータの設定 • (オプション設定項目) スパニングツリータイマの設定 • (オプション設定項目) タイムアウトファクタの設定 • (オプション設定項目) BPDU最大送出レートの設定 • (オプション設定項目) Edgeポートの設定 • (オプション設定項目) Point-to-Pointリンクの設定 • (オプション設定項目) MSTPパケットのフォーマット設定 • (オプション設定項目) ポート遷移状態情報の出力の有効化 • (必須設定項目) スパニングツリー機能の有効化
leaf nodeの設定: • (必須設定項目) 動作モードの設定 • (必須設定項目) MST regionの設定 • (オプション設定項目) Bridgeプライオリティの設定 • (オプション設定項目) タイムアウトファクタの設定 • (オプション設定項目) BPDU最大送出レートの設定 • (オプション設定項目) Edgeポートの設定 • (オプション設定項目) Port Path Costの設定 • (オプション設定項目) Port priorityの設定 • (オプション設定項目) Point-to-Pointリンクの設定 • (オプション設定項目) MSTPパケットのフォーマット設定 • (オプション設定項目) ポート遷移状態情報の出力の有効化 • (必須設定項目) スパニングツリー機能の有効化
(オプション設定項目) mCheck機能の設定
(オプション設定項目) Digest Snoopingの設定
(オプション設定項目) No Agreement Checkの設定
(オプション設定項目) 保護機能の設定

5.7 動作モードの設定

スパニングツリーの動作モードは以下があります。

- **STP モード**–装置を STP で動作させます。スパニングツリーの情報交換のため、STP BPDU を送信します。ポートの対向装置が STP のみをサポートしている場合、このモードを選択します。
- **RSTP モード**–装置を RSTP で動作させます。スパニングツリーの情報交換のため、RSTP BPDU を送信します。ただし、対向装置が STP で動作していることを検知す

ると STP BPDU を送信します。対向装置が MSTP BPDU を受信していても、このモードのポートは MSTP モードに移行しません。

- **MSTP モード**–装置を MSTP で動作させます。スパニングツリーの情報交換のため、MSTP BPDU を送信します。ただし、対向装置が STP で動作していることを検知すると STP BPDU を送信します。対向装置が RSTP BPDU を受信していても、このモードのポートは RSTP モードに移行しません。
- **PVST モード**ー装置を PVST で動作させます。各 VLAN はスパニングツリーを維持します。スパニングツリーの容量は PVST が有効なポートと、PVST が有効な VLAN を掛け合わせた数になります。もしネットワークの容量がスパニングツリーの容量を超えるとき、装置の CPU に負荷がかかります。パケット転送が中断され、ネットワークが不安定になります。装置は最大 256 のスパニングツリー対応 VLAN をサポートします。

MSTP モードは、RSTP モードと互換性があり、RSTP モードは STP モードと互換性があります。

PVST モードの互換性はポートのリンクタイプに依存します。

- アクセスポートでは、PVST モードはすべての VLAN でほかのスパニングツリーと互換性があります。
- トランクポートあるいはハイブリッドポートでは、PVST モードは、VLAN1 でほかのスパニングツリーと互換性があります。

5.7.1 設定手順

以下に動作モードの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. 動作モードを設定する	**stp mode** { **mstp** | **pvst** | **rstp** | **stp** }	デフォルト：MSTP

5.8 MST regionの設定

スパニングツリーの装置が物理的に接続され、以下が同じ設定の場合、スパニングツリーの装置は同じ MST region に属します。

- フォーマットセレクタ(デフォルトは 0 です。設定できません。)
- MST region 名
- MST region revision レベル
- MST region の同一 VLAN-to-instance マッピングエントリ

MST region に関連したパラメータ(特に VLAN-to-instance マッピングテーブル)の設定は、MSTI に新しいスパニングツリーの計算の原因になり、ネットワークトポロジが不安定になる可能性があります。ネットワークトポロジが不安定になる可能性を減らすために、以下のいずれかの設定をしてから MST region の設定を適用してください。

- **active region-configuration** コマンドで MST region 関連のパラメータをアクティブにします。
- スパニングツリーが無効な状態では、**stp global enable** コマンドで MSTP を有効にします。

STP、RSTP、PVST モードでは MST region の設定は適用されません。

以下に MST region の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. MST region view に移行する	**stp region-configuration**	―
3. MST region 名を設定する	**region-name** *name*	デフォルト：装置のMACアドレス
4. VLAN-to-instance マッピングテーブルを作成する	• **instance** *instance-id* **vlan** *vlan-id-list* • **vlan-mapping modulo** *modulo*	どちらかの設定を使用します。 デフォルト：すべてのVLANがCIST(あるいはMSTI 0)にマッピングされています。
5. MST region の MSTP Revision レベルを設定する	**revision-level** *level*	デフォルト：0
6. (オプション設定項目) MST Region の設定がアクティブ化されていないことを表示する	**check region-configuration**	―
7. 手動で MST Region の設定を有効にする	**active region-configuration**	―

5.9 Root BridgeとSecondary Root Bridgeの設定

MSTP は、MSTP 計算でスパニングツリーの Root Bridge を指定できます。あるいは、Root Bridge あるいは Secondary Root Bridge として装置を指定することができます。

装置は、異なるスパニングツリーと独立しています。あるスパニングツリーの Root Bridge や Secondary Root Bridge は、別のスパニングツリーの Root Bridge や Secondary Root Bridge にすることができます。しかし 1 つの装置を同じスパニングツリーの Root Bridge や Secondary Root Bridge にすることはできません。

スパニングツリーは 1 つの Root Bridge のみ持ちます。もし同一時間に、スパニングツリーで複数の Root Bridge が選択された場合、最も小さい MAC アドレスの装置が選択されます。

インスタンスの Root Bridge が故障あるいはシャットダウンしたとき、以下のようになります。

- Secondary Root Bridge が指定されていれば、そのインスタンスを引き継ぐことができます。
- インスタンスに複数の Secondary Root Bridge を指定していた場合は、MSTP が MAC アドレスの最も小さい Secondary Root Bridge を新しい Root Bridge に指定します。
- Secondary Root Bridge が指定されていない場合、新しい Root Bridge を選出します。

装置のプライオリティの設定に関係なく、各スパニングツリーに 1 つの Root Bridge を指定することができます。装置を Root Bridge あるいは Secondary Root Bridge 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。

装置のプライオリティを 0 に設定し、Root Bridge に指定することもできます。装置のプライオリティの設定につきましては、本章の *"Bridge プライオリティの設定"* を参照してください。

5.9.1 Root Bridge の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. Root Bridge を設定する	• STP/RSTPモード: **stp root primary** • PVSTモード: **stp vlan** *vlan-id-list* **root primary** • MSTPモード: **stp** [**instance** *instance-list*] **root primary**	デフォルト：Root Bridgeとして機能しません。

5.9.2 Secondary Root Bridge の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. Secondary Root Bridge を設定する	• STP/RSTPモード: **stp root secondary** • PVSTモード: **stp vlan** *vlan-id-list* **root secondary** • MSTPモード: **stp** [**instance** *instance-list*] **root secondary**	デフォルト：Secondary Root Bridgeとして機能しません。

5.10 Bridgeプライオリティの設定

スパニングツリーでは、Bridge プライオリティのパラメータを用いて、Root Bridge を決定します。この際に使用する Bridge プライオリティの値を、以下のコマンドを使用して設定します。最も小さい値の Bridge プライオリティを設定することで、その装置を Root Bridge にすることができます。異なるスパニングツリーには異なる Bridge プライオリティを設定することができます。

Root Bridge の選出とき、スパニングツリーのすべての装置が、同じプライオリティの値である場合、最も小さい MAC アドレスの装置が Root Bridge として選択されます。Root bridge もしくは Secondary Root Bridge を指定した後、コマンドを使用してそのスイッチの Bridge Priority を変更することはできません。

以下に指定された MSTI の Bridge プライオリティの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー

操作	コマンド	補足
2． Bridge プライオリティを設定する	• STP/RSTPモード: **stp priority** *priority* • PVSTモード: **stp vlan** *vlan-id-list* **priority** *priority* • MSTPモード: **stp** [**instance** *instance-list*] **priority** *priority*	デフォルト：32768

5.11 MST regionの最大ホップ数の設定

MST Region における最大ホップ数は、MST Region の最大範囲を制限するために使用します。

Configuration BPDU には、残りホップ数を管理するためのフィールド（Remaining Hops 領域）があります。スパニングツリーの Root Bridge が送信する Configuration BPDU のこのフィールドは 、スパニングツリーを構成する装置を経由する度に、-1 します。フィールドの値が 0 である Configuration BPDU を受信した装置は、その BPDU を廃棄するため、MST Region のネットワークの最大範囲が制限できます。

この設定は Root Bridge のみ設定できます。MST region 内にある他のすべての装置は、Root Bridge で設定された値を使用します。

STP ネットワークサイズにもとづいて、MST Region の最大ホップ数を設定することができます。ルートブリッジの最大ホップ数の設定は、edge ポートの最大ホップ数よりも大きい値にすることを推奨します。

以下に MST region の最大ホップ数の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． MST Region の最大ホップ数を設定する	**stp max-hops** *hops*	デフォルト：20

5.12 ネットワークダイアメータの設定

ネットワークにおける任意の 2 台の装置を結ぶ最も遠いパス上にある装置の数を、ネットワークの大きさを示す 1 つの指標として設定します。ネットワークダイアメータが大きいと、ネットワークが大きいことを示します。

ネットワークダイアメータの設定に従って、装置は MSTP の Hello 時間、転送遅延、最大エージングタイマを適切な値に自動的に設定します。

STP、RSTP、MSTP モードでは、以下のようになります。

- 各 MST region は装置とみなされます。
- 設定したネットワーク ダイアメータは、CIST(あるいは Root Bridge)でのみ有効で、MSTI では無効です。

PVST モードでは、設定されたネットワークダイアメータは指定された VLAN の Root Bridge でのみ有効です。

以下にネットワークダイアメータの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. ネットワークダイアメータを設定する	• STP/RSTP/MSTPモード: **stp bridge-diameter** *diameter* • PVSTモード: **stp vlan** *vlan-id-list* **bridge-diameter** *diameter*	デフォルト：7

5.13 スパニングツリータイマの設定

設定可能なスパニングツリー関連タイマには、以下のタイマがあります。

- **Forward delay**–ポートが状態遷移に要する時間です。リンクに障害が発生すると、装置はスパニングツリーの再構築を行いますが、再構築されたスパニングツリーのBPDU がネットワーク全体に展開するまで時間を要します。そのため、Forward Delay、中間のポート状態(学習状態)を設定し、ルートポートと指定ポートが学習状態から転送状態に移行する時間を確保します。
- **Hello time**–リンク障害等を検出するために、Hello 時間に設定された間隔で Hello パケット(Configuration BPDU)を定期的に送信します。
- **Max age**–BPDU の有効期間を指定します。装置は、BPDU 内に記載されている最大エージングタイマ（Max Age）を経過した BPDU メッセージを廃棄します。最大エージングタイマは CIST を除いて MSTI に影響がありません。

スパニングツリーの状態変更が頻繁に発生するのを回避するには、Hello タイマ、Forward Delay、最大エージングタイマの設定を次式に満足するよう設定してください。

- 2 × (forward delay - 1 秒) ≧ max age
- Max age ≧ 2 × (hello time ＋ 1 秒)

スパニングツリーのタイマは手動ではなく自動で設定することを推奨します。ネットワークダイアメータの設定にもとづいて、自動的に計算します。ネットワークダイアメータがデフォルトである場合、スパニングツリーのタイマはデフォルト値となります。

Root Bridge に設定されるタイマは、ネットワーク全体のすべての装置で適用されます。

5.13.1 設定の制限とガイドライン

- ネットワークのダイアメータに応じて、Forward Delay の設定値は変更します。一般的に、ネットワークのダイアメータが大きい程、転送遅延は長く設定してください。転送遅延を極端に短く設定すると一時的に冗長パスが発生してしまい、転送遅延を極端に長くするとネットワーク接続が再開するまでの時間が長くなります。よって、一般的なネットワークにおいては、デフォルト値で使用することを推奨します。
- Hello タイマを適切に設定することで、リンク障害等を適切に検出しリンクの切り替えを行えます。Hello タイマを極端に短く設定すると、消費されるネットワークリソースが増えると共に装置での処理も大きくなります。また Hello タイマを極端に長く設定すると、リンク上でパケットロスが発生すると、装置はそれをリンク障害と認識

するためスパニングツリーの再構築が発生してしまいます。よって、一般的なネットワークにおいては、デフォルト値で使用することを推奨します。

- スパニングツリーの段数および構成する装置での処理能力に応じて、最大エージングタイマの設定値は変更します。極端に小さい設定を行うと、ネットワークの輻輳発生によってスパニングツリーの再構築が発生する可能性があります。また、極端に大きい設定を行うと、リンク障害を所定の時間内に検出し、スパニングツリーを再構築できなくなります。よって、一般的なネットワークにおいては、デフォルト値で使用することを推奨します。

5.13.2 設定手順

以下にスパニングツリータイマの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. forward delay timer を設定する	• STP/RSTP/MSTPモード: **stp timer forward-delay** *time* • PVSTモード: **stp vlan** *vlan-id-list* **timer forward-delay** *time*	デフォルト：15 秒
3. hello timer を設定する	• STP/RSTP/MSTP モード: **stp timer hello** *time* • PVSTモード: **stp vlan** *vlan-id-list* **timer hello** *time*	デフォルト：2秒
4. max age timer を設定する	• STP/RSTP/MSTPモード: **stp timer max-age** *time* • PVSTモード: **stp vlan** *vlan-id-list* **timer max-age** *time*	デフォルト： 20秒

5.14 タイムアウトファクタの設定

タイムアウトファクタは、以下の式で表されるタイムアウト時間を決めるために使用されるパラメータです。

タイムアウト時間 = タイムアウトファクタ × 3 × hello 時間

スパニングツリーの状態が安定しているとき、Root Bridge でない装置は hello パケット(configuration BPDU)を hello 間隔で下流の装置にリンクの故障を検知するため、転送します。もし通常、Hello タイマの 9 倍の時間、上位の装置から Hello パケットを受信しないと、上位の装置が故障しているとみなし、ネットワークのトポロジの再構築を開始します。

安定したネットワークにおいても、上位の装置処理能力がビジーのときに、ネットワークのトポロジの再構築が行われる可能性があります。この場合、Hello パケットの監視時間の倍数を多くして、タイムアウトするまでの時間を長くすることができます。通常はネットワークの安定性を保つために、タイムアウトファクタを 5、6、7 に設定することを推奨します。

以下にタイムアウトファクタの設定を示します。:

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. タイムアウトファクタを設定する	**stp timer-factor** *factor*	デフォルト：3

5.15 BPDU最大送出レートの設定

Hello タイマの時間内に送信可能な configuration BPDU の最大数を設定できます。ネットワークリソースの占有を回避するために設定します。

最大送出レートを高くすると、各 hello 時間内に多くの BPDU を送出しますが、多くのシステムリソースを消費します。一般的なネットワークでは、デフォルト値で使用することを推奨します。

以下に BPDU 最大送出レートの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Ethernet interface view あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	―
3. BPDU 最大送出レートを設定する	**stp transmit-limit** *limit*	デフォルト：10

5.16 Edgeポートの設定

Edge ポートとは、ほかの Ethernet スイッチや共有ネットワークセグメントに接続されず、ユーザ端末等に直接接続しているポートを指します。Edge ポートと設定することによって、接続装置が STP をサポートしていない場合には、ポートがリンクアップすると即座に Forwarding 状態に移行させることができます。

5.16.1 設定の制限とガイドライン

- BPDU ガード機能が無効であるとき、Edge ポートが別のポートから BPDU を受信した場合、Edge ポートは非 Edge ポートになります。Edge ポートに戻す場合、再度有効化を行う必要があります。
- ポートがユーザ端末に接続されている場合、Edge ポートとして設定し、BPDU ガードを有効にします。この機能によってネットワークのセキュリティを保持しながら forwarding 状態を早急に収束させることができます。
- ループガード、Edge ポートの機能を、ポートに同時に設定することはできません。

5.16.2 設定手順

以下に Edge ポートの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. Ethernet あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	—
3. edge port を設定する	**stp edged-port**	デフォルト：非Edgeポート

5.17 Port Path Costの設定

Path Cost は、ポートに接続するリンクの速度に関係するパラメータです。MSTP 対応の装置では、ポートは MSTI ごとに異なる Path Cost を持つことができます。Path Cost を適切に設定することで、VLAN トラフィックフローが別々の物理リンクで転送されるので、VLAN ごとのロードバランスが可能です。

装置は自動的にデフォルト Path Cost を計算でき、一方でユーザはポートの Path Cost を設定できます。

5.17.1 デフォルト Path Cost の計算時の基準指定

注意:
装置がデフォルト Path Cost を計算する際に使用する基準を変更した際は、デフォルトに Path Cost を戻してください。

Port Path Cost のデフォルト値には以下のモードがあります。以下の標準から選択できます。

- **dot1d-1998**–IEEE 802.1d-1998 で規定されている Port Path Cost の対応値を使用します。
- **dot1t**–IEEE 802.1t で規定されている Port Path Cost の対応値を使用します。
- **legacy**–QX シリーズ独自の Port Path Cost の対応値を使用します。

デフォルトの Path Cost を計算する際に、基準を設定する場合、以下のガイドラインに従ってください。

- アグリゲーションリンクの Path Cost の計算は、IEEE 802.1d-1998 の場合、アグリゲーションリンクのポートの数を考慮しません。IEEE 802.1t は、アグリゲーションリンクのポートの数を考慮にします。計算式は、Path Cost= 200,000,000/リンク速度 (100kbps 単位) で、リンク速度はアグリゲーションリンクがブロックされていないポートのリンク速度の合計です。
- IEEE 802.1d-1998 あるいは QX シリーズ独自の基準は、ポートあるいはインタフェースのリンク速度が 10Gbps を超えたとき、単一ポートあるいはアグリゲートインタフェースに設定可能な最も小さい値を指定してください。この基準にもとづいて転送する Path は、最適な Path にならない可能性があります。この問題に対応するため、以下のいずれかを行ってください。
  - □ デフォルト Path Cost 計算の基準として、**dot1t** を使用します。

□ ポートの Path Cost を手動で設定します。 Path Cost については、本章の *"Path Cost の設定"* を参照してください。

以下にデフォルト Path Cost を計算するときに装置に使用する基準を指定する方法を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Path Cost の計算基準を設定する	**stp pathcost-standard** { **dot1d-1998** | **dot1t** | **legacy** }	デフォルト：**legacy**

表 5-5 リンク速度と Path Cost 間のマッピング

リンク速度	ポートタイプ	Path Cost		
		IEEE 802.1d-1998	IEEE 802.1t	Legacy (QX シリーズ独自)
0	―	65535	200000000	200000
100 Mbps	単一ポート	19	200000	200
	集約リンク2ポート		100000	180
	集約リンク3ポート		66666	160
	集約リンク4ポート		50000	140
1000 Mbps	単一ポート	4	20000	20
	集約リンク2ポート		10000	18
	集約リンク3ポート		6666	16
	集約リンク4ポート		5000	14
10 Gbps	単一ポート	2	2000	2
	集約リンク2ポート		1000	1
	集約リンク3ポート		666	1
	集約リンク4ポート		500	1
20 Gbps	集約リンク2ポート	1	500	1
	集約リンク3ポート		333	1
	集約リンク4ポート		250	1
	集約リンク4ポート		50	1

5.17.2 Path Cost の設定

ポートの Path Cost を変更したとき、ポートの役割を再計算し、状態遷移を初期化します。

以下にポートの Path Cost の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Ethernet あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	―

操作	コマンド	補足
3. Path Cost を設定する	• STP/RSTPモード: **stp cost** *cost* • PVSTモード: **stp vlan** *vlan-id-list* **cost** *cost* • MSTPモード: **stp** [**instance** *instance-list*] **cost** *cost*	デフォルト：システムがPath Costを自動計算

5.18 Port priorityの設定

Root Port を選出する際、ポートの Port Priority が重要な役割を果たします。ほかのパラメータが同じ場合、Port Priority の高いポート（Port Priority 値が小さいポート）が Root Port に選出されます。

スパニングツリーでは異なる path ごとに異なる Port Priority を設定でき、スパニングツリーごとに役割を指定できます。そのため、VLAN 単位で異なる物理ポートを介してデータを流すことができるため、VLAN ベースでロードバランスが可能となります。正確なネットワーク要件にもとづいて Port Priority を設定することができます。

ポートの priority を変更したとき、システムはポートの役割を再計算し、状態遷移を開始します。

以下に port priority の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. Ethernet interface view あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	—
3. port priority を設定する	• STP/RSTPモード: **stp port priority** *priority* • PVSTモード: **stp vlan** *vlan-id-list* **port priority** *priority* • MSTPモード: **stp** [**instance** *instance-list*] **port priority** *priority*	デフォルト：128

5.19 Point-to-Pointリンクの設定

Point-to-Point リンクは、2 台の装置を直結するリンクです。2 つの Root Port や designated port が Point-to-Point リンクである場合、そのリンクの両端に Point-to-Point リンクと設定することで、ポート間で同期のためのパケットを使用して、即座に Forwarding 状態に移行させることができます。

5.19.1 設定の制限とガイドライン

- リンクアグリゲーションを設定している場合や全二重モードを設定している場合、Point-to-Point リンクとして設定することができます。NEC ではデフォルトの設定を使用し、リンクタイプを自動的に設定した値とすることを推奨します。
- MSTP あるいは PVST モードのポートに **stp point-to-point force-false** コマンドあるいは **stp point-to-point force-true** コマンドを設定した場合、設定はすべての VLAN あるいは MSTI に適用されます。
- 実際には Point-to-Point でないポートに対して、Point-to-Point の設定を行うと、一時的にループが発生する可能性がありますので、注意してください。

5.19.2 設定手順

以下に Point-to-Point リンクの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Ethernet あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	―
3. Point-to-Point リンクを設定する	**stp point-to-point** { **auto** | **force-false** | **force-true** }	デフォルト：**auto** autoではポートが自動的にリンクタイプを決定します。

5.20 MSTPパケットのフォーマット設定

ポートは以下のフォーマットで MSTP パケットの送受信を行うことができます。

- **dot1s** – IEEE802.1s で規定された形式です。
- **legacy** – QX シリーズ独自形式(IEEE802.1s ドラフト版で規定された形式）です。対向装置は、QX シリーズの製品のみです。

デフォルトの MSTP のパケットフォーマットは **auto** です。2 つの MSTP パケットのフォーマットを区別します。対向装置からの BPDU に合わせて、自動でフォーマットを選択し、送信します

ポートの MSTP パケットフォーマットをポートごとに設定できます。設定後、MSTP モードで動作しているときは、ポートは設定しているフォーマットのパケットのみ送受信し、同じフォーマットのパケットを送信する装置と通信します。

auto モードのポートはデフォルトで IEEE 802.1s MSTP パケットのみ送信します。ポートが legacy フォーマットの MSTP パケットを受信したときポートは **legacy** フォーマットのパケットのみ送信を行います。これは、ポートがパケットのフォーマットが頻繁に変更することを防ぎます。IEEE 802.1s MSTP パケットを送信するように設定するために、ポートをシャットダウンし、その後、ポートをアップ状態にします。

MSTI 数が 48 を超えたとき、ポートは IEEE 802.1s のみ送信することができます。

以下にポートへの MSTP パケットフォーマットの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Ethernet あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	―
3. MSTP パケットフォーマットを設定する	**stp compliance** { **auto** | **dot1s** | **legacy** }	デフォルト：**auto**

5.21 ポート遷移状態情報の出力の有効化

大規模なスパニングツリーネットワークでは、MSTI のポート状態の遷移に関する情報を出力できるように設定し、リアルタイムでポート状態をモニタリングできます。

以下にポート状態の遷移に関する情報を出力する設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. ポート遷移状態の情報を出力するように設定を有効にする	• STP/RSTPモード: **stp port-log instance 0** • PVSTモード: **stp port-log vlan** *vlan-id-list* • MSTPモード: **stp port-log** { **all** | **instance** *instance-list* }	デフォルト：有効

5.22 スパニングツリー機能の有効化

ほかのスパニングツリー機能に関連した設定を有効にする前に、装置でスパニングツリー機能を有効化にする必要があります。STP、RSTP、MSTP モードではスパニングツリー機能がグローバルと設定したポートで有効化されることを確認してください。PVST モードではスパニングツリー機能がグローバル、指定した VLAN および設定したポートで有効化されることを確認してください。

ポートでのスパニングツリーの計算と装置の CPU のリソースを節約するため、**undo stp enable** コマンドを使用して、ポートでスパニングツリー機能を無効にすることができます。スパニングツリー機能を無効にしたら、ループが発生していないことを確認してください。

5.22.1 STP/RSTP/MSTP モードでのスパニングツリー機能の有効化

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. スパニングツリー機能を有効にする	**stp global enable**	デフォルト：グローバルで無効

操作	コマンド	補足
3． Ethernet interface view あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	—
4． (オプション設定項目) ポートでスパニングツリー機能を有効にする	**stp enable**	デフォルト：すべてのポートで有効

5.22.2 PVST モードでのスパニングツリー機能の有効化

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． スパニングツリー機能を有効にする	**stp global enable**	デフォルト：グローバルで無効
3． VLAN でスパニングツリー機能を有効にする	**stp vlan** *vlan-id-list* **enable**	デフォルト：すべてのVLANで有効
4． Ethernet interface view あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	—
5． ポートでスパニングツリー機能を有効にする	**stp enable**	デフォルト：すべてのポートで有効

5.23 mCheck機能の設定

mCheck 機能はポート状態転送プロセスをユーザが設定できるようにする機能です。

MSTP、MSTP あるいは PVST が動作している装置のポートが STP で動作する装置に接続し STP BPDU を受信した場合、ポートは STP モードに自動的に変更します。しかし以下の場合は、ポートは自動的にもとのモードに戻ることができません。

- 対向の STP 装置がシャットダウンあるいは取り外された場合
- ローカルの装置が変更を検出できない場合

もとのモードで動作するようにポートの設定を強制的に変更するために、mCheck 機能の設定を行うことができます。

たとえば Device A、Device B、Device C が順に接続されています。Device A は STP が動作し、Device B はスパニングツリーが動作しておらず、Device C は RSTP、MSTP あるいは PVST で動作しています。このとき、Device C は、Device B によって透過的に転送された STP BPDU を受信するとき、受信したポートは STP モードに変更します。もし Device B が Device C と RSTP、MSTP あるいは PVST で動作するように設定された場合、Device B と Device C で相互に接続されているポートは mCheck を動作させる必要があります。

5.23.1 設定の制限とガイドライン

mCheck 機能は MSTP、RSTP あるいは PVST モードで動作する装置で適用されます。

5.23.2 設定手順

I. グローバルでの mCheck の実行

操作	コマンド
1. system view に移行する	**system-view**
2. mCheck を実行する	**stp global mcheck**

II. interface view での mCheck の実行

操作	コマンド
1. system view に移行する	**system-view**
2. Ethernet あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*
3. mCheck を実行する	**stp mcheck**

5.24 Digest Snoopingの設定

注意:

以下に示す状態において、グローバルで Digest Snooping を使用する場合、注意してください。

- VLAN-to-instance マッピングを変更するとき
- MST region の設定を復元するとき

VLAN-to-instance マッピングが隣り合う装置と異なる場合、ループあるいは通信断が発生します。

IEEE 802.1s で定義されているように、同じ region で接続された装置は、MST region 関連の設定が一致します。

- region 名
- リビジョンレベル
- VLAN-to-instance マッピング

MSTP 対応の装置は、BPDU パケットの configuration ID をチェックすることで、同じ MST region の装置かを識別します。configuration ID は、region 名、リビジョンレベル、設定ダイジェスト(16 バイト長、VLAN-to-instance マッピングにもとづく HMAC-MD5 アルゴリズムによる計算結果)で構成されています。

MSTP の実装はベンダによって異なり、プライベートキーを使用し計算される設定ダイジェストも異なるので、同じ MST region でも装置を提供するベンダが異なると、互いに通信することができません。

NEC の装置とほかのベンダの装置間で通信を行うには、同じ MST region で接続するポートで Digest snooping 機能を有効にします。

5.24.1 設定の制限とガイドライン

Digest snooping の設定を行うとき以下のガイドラインに従ってください。

- Digest snooping を有効にする前に、別のベンダの装置がスパニングツリーに接続され、動作していることを確認してください。
- Digest Snooping 機能が有効になっている場合、同じ region(in-the-same-region)チェックに設定ダイジェストの比較は行われないため、関連するポートでは VLAN-to-instance マッピングを同じにしなければなりません。
- Digest snooping 機能を適用するためには、グローバルと設定ポートの両方で Digest snooping 機能を有効にしてください。まず、関連するすべてのポートで Digest snooping 機能を有効にし、それからグローバルでも有効にすることを推奨します。これにより設定がすべてのポートに適用され、ネットワークへの影響を減らすことができます。
- ループを防ぐため、MST region の Edge ポートで Digest snooping を有効にしないでください。
- Digest snooping を有効にした後 、スパニングツリー機能を有効にしてください。ネットワークの動作が安定しているときは、トラフィックの中断を避けるため、Digest snooping を有効にしないでください。

5.24.2 設定手順

設定 Digest を計算するために秘密鍵を使用している他ベンダの装置が、NEC の装置に接続されている場合、NEC の装置でのみ Digest snooping の設定を有効にすることができます。

以下に Digest snooping の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Ethernet あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	―
3. インタフェースで Digest Snooping を有効にする	**stp config-digest-snooping**	デフォルト：無効
4. system view から戻る	**quit**	―
5. グローバルで Digest Snooping を有効にする	**stp global config-digest-snooping**	デフォルト：無効

5.24.3 Digest Snooping 設定例

I. ネットワーク要件

図 5-9 に示すように、Device A、Device B が Device C に接続されています。Device C はほかベンダの装置で、すべての装置は同じ region を使用しています。

3 つの装置が互いに通信できるように、Device C に接続されている Device A、Device B のポートで Digest snooping を有効にします。

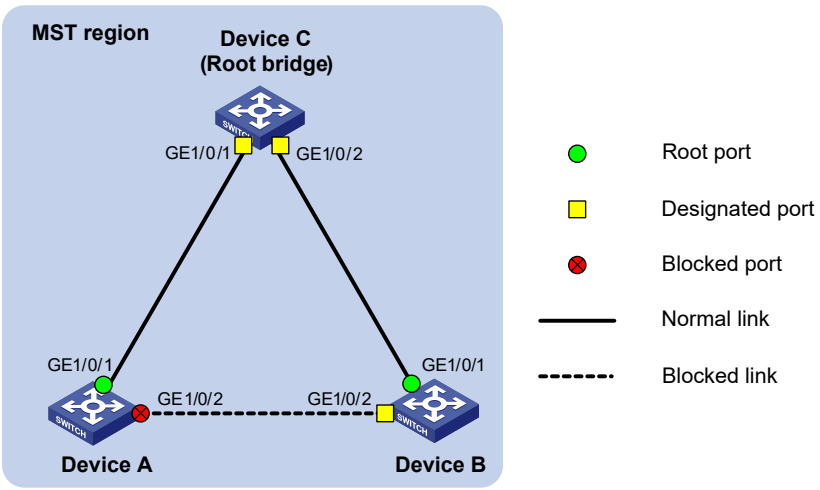


図 5-9 ネットワーク図

II. 設定手順

Device A の GigabitEthernet 1/0/1 で Digest snooping を有効にし、Device A のグローバルで Digest snooping を有効にします。

```
<DeviceA> system-view
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] stp config-digest-snooping
[DeviceA-GigabitEthernet1/0/1] quit
[DeviceA] stp global config-digest-snooping
```

Device B の GigabitEthernet 1/0/1 で Digest snooping を有効にし、Device B のグローバルで Digest snooping を有効にします。

```
<DeviceB> system-view
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] stp config-digest-snooping
[DeviceB-GigabitEthernet1/0/1] quit
```

```
[DeviceB] stp global config-digest-snooping
```

5.25 No Agreement Checkの設定

RSTP と MSTP の Designated Port の高速な状態遷移には、2 つのタイプのメッセージが使用されています。

- **Proposal** – Designated Port から送信される高速遷移リクエスト
- **Agreement** – 高速遷移リクエストの応答(acknowledge)パケット

RSTP、MSTP が動作している装置のポートが下流の装置から、agreement パケットを受信したときにのみ、Designated Port で高速遷移を実行できます。RSTP 装置と MSTP 装置の相違点は以下のとおりです。

- MSTP 装置は、下流装置の Root Port が上流の装置から agreement パケットを受信した後にのみ、agreement パケットを送信します。
- RSTP 装置は、下流装置の Root Port が上流の装置から agreement パケットを受信したかに関わらず、agreement パケットを送信します。

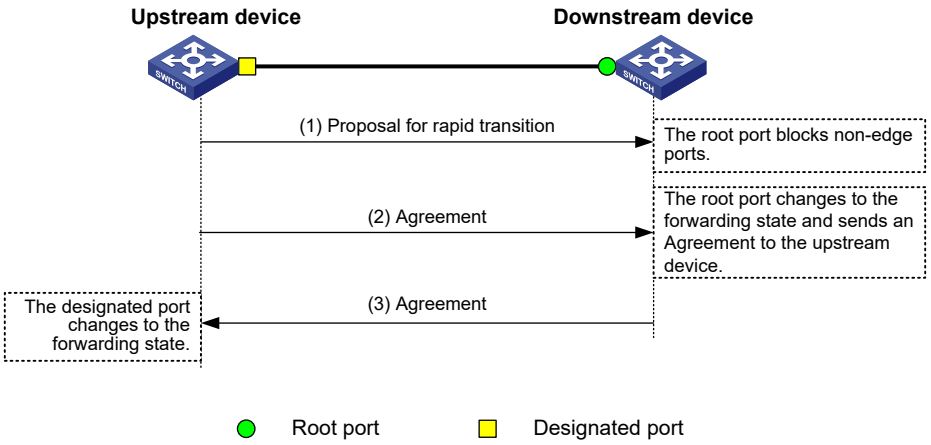


図 5-10 MSTP の designated port の高速状態遷移のメカニズム

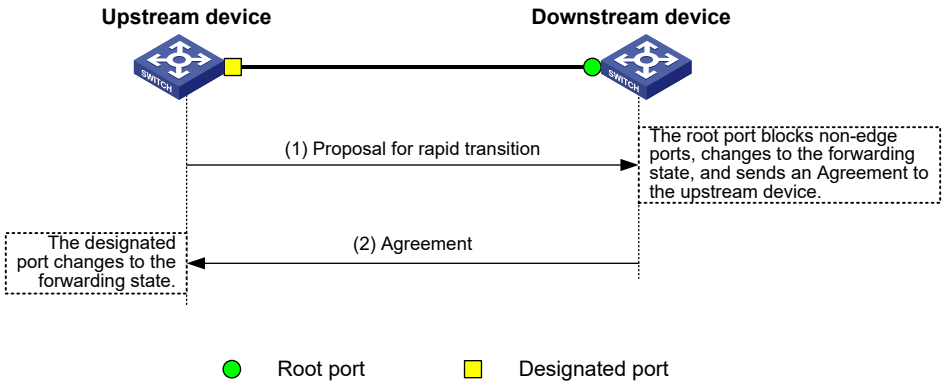


図 5-11 RSTP の designated port の高速状態遷移のメカニズム

上流装置がほかベンダの装置である場合、以下のように高速状態遷移の実行が制限される可能性があります。

- 上流装置が RSTP と類似の高速遷移メカニズムを使用している場合
- 下流装置が MSTP を使用し、RSTP モードをサポートしない場合

この場合、以下の事象が起こります。

1) 下流装置の Root Port は上流装置から agreement パケットを受信しません。
2) 上流装置に no agreement パケットを送信します。

その結果、上流装置の Designated Port は転送遅延の 2 倍の時間が経過した後、forwarding 状態に遷移します。

このような場合に下流装置のポートで No Agreement Check 機能を有効にすることで、高速状態遷移を実行できます。

5.25.1 設定要件

No Agreement Check 機能を設定する前に、以下の作業を行う必要があります。

- 装置は、スパニングツリーに対応している他ベンダの装置と point-to-point リンクによって接続しています。
- 2 台の装置で同じ region 名、リビジョンレベル、VLAN-to-instance マッピングを設定します。

5.25.2 設定手順

Root port で No Agreement Check 機能を有効にすることができます。

以下に No Agreement Check の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Ethernet interface view あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	―
3. No Agreement Check 機能を有効にする	**stp no-agreement-check**	デフォルト：無効

5.25.3 No Agreement Check 設定例

I. ネットワーク要件

図 5-12 に示すように、以下の要件に従います。

- Device A は、同じ region に属し、異なる MSTP を実装した他ベンダの装置に接続しています。

- ほかのベンダの装置(Device B)は Regional Root Bridge で、Device A は下流装置です。

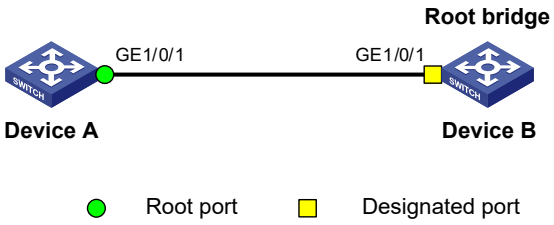


図 5-12 ネットワーク図

II. 設定手順

Device A の GigabitEthernet 1/0/1 で、No Agreement Check 機能を有効にします。

```
<DeviceA> system-view
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] stp no-agreement-check
```

5.26 保護機能の設定

スパニングツリーの装置は以下の保護機能をサポートしています。

- BPDU ガード
- Root ガード
- Loop ガード
- ポート役割の制限機能
- TC-BPDU ガード
- BPDU ドロップ機能
- PVST BPDU ガード

5.26.1 BPDU ガードの有効化

I. BPDU ガードの有効化について

アクセスレイヤ装置の場合、アクセスポートはユーザ端末 (PC など) またはファイルサーバに直接接続できます。アクセスポートは、迅速な移行を可能にするエッジポートとして設定されます。これらのポートが設定 BPDU を受信すると、システムは自動的にポートを非 Edge ポートとして設定し、新しいスパニングツリー計算プロセスを開始します。これにより、ネットワークトポロジが変更されます。通常の状態では、これらのポートは設定 BPDU を受信しません。ただし、誰かが悪意を持って設定 BPDU を使用して装置を攻撃すると、ネットワークが不安定になります。

スパニングツリープロトコルは、このような攻撃からシステムを保護する BPDU ガード機能を提供します。BPDU ガードが有効になっているポートが BPDU を受信すると、装置は次の操作を実行します。

- これらのポートをシャットダウンします。
- これらのポートがスパニングツリープロトコルによってシャットダウンされたことを NMS に通知します。

shutdown-interval コマンドで設定されたタイマの期限が切れると、装置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。このコマンドの詳細については、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“3 *システム管理*”の”*3 章 ハードウェアリソース管理*”を参照してください。

II. 制限とガイドライン

BPDU ガード機能は、システムビューまたは Edge ポートで設定できます。Edge ポートは、ポート固有の BPDU ガード設定を優先的に使用します。ポート固有の BPDU ガード設定が使用できない場合、Edge ポートはグローバル BPDU ガード設定を使用します。

グローバル BPDU ガードは、**stp edged-port** コマンドを使用して設定された Edge ポートでのみ有効になります。BPDU ガード機能を非 Edge ポートで有効にするには、ポート固有の BPDU ガード設定を使用します。

loopback { **external** | **internal** } コマンドを設定したポートでは、BPDU ガードは有効になりません。

以下にグローバル BPDU ガードの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. BPDU ガードを有効にする	**stp bpdu-protection**	デフォルト：無効

以下にインタフェース BPDU ガードの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Ethernet interface view あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	―
3. BPDU ガードを有効にする	**stp port bpdu-protection { enable | disable }**	デフォルト： グローバルのBPDUガードと同じです。Edgeポートには設定されません。

5.26.2 Root ガードの有効化

スパニングツリーの Root Bridge と secondary root bridge は、同一 MST region に割り当てられることを推奨します。特に CIST では、Root Bridge と secondary root bridge は、ネットワーク設計で、高帯域幅を持つ領域に配置されます。しかし設定ミスや攻撃により、不正な装置がより高い優先度を持った configuration BPDU を配信すると、本来意図され

るスパニングツリーのトポロジが構成されないだけでなく、ネットワークトポロジの変更が多発します。トラフィックが高帯域幅のリンクから低帯域幅のリンクに切り替えられてしまい、ネットワークを安定して使用できなくなります。

この状況を防止するための機能として、Root ガードをサポートします。

もし Root ガードが Root Bridge のポートで有効である場合、ポートはすべてのポートの designated port の役割を実行します。MSTI から高い優先度の configuration BPDU を受信した後、以下の操作をします。

- すぐさま MSTI の listening 状態にポートを切り替えます。
- 受信した configuration BPDU を転送しません。

この操作は、MSTI のポートに接続されたリンクを切断することと同一です。

もしポートが 2 倍の forwarding delay 内に高い優先度の BPDU を受信しない場合、もとの状態に戻ります。

ポートで、Loop ガード機能、Root ガード機能の設定は同時に設定することはできません。

Root ガードは、designated port で設定します。

以下に Root ガードの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Ethernet interface view あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	―
3. Root ガードを有効にする	**stp root-protection**	デフォルト：無効

5.26.3 Loop ガードの有効化

上流の装置から受信した BPDU に従って、Root ポートとほかの Blocking ポートの状態が決まります。しかしリンクの衝突あるいは片方向リンクの障害が発生すると、ポートは上流の装置から BPDU の受信に失敗する可能性があります。この場合ポートの役割を再選択します。

- 上流の BPDU の受信に失敗した Forwarding 状態のポートは designated ポートになります。
- Blocking ポートは Forwarding 状態に遷移します。

この結果、スイッチネットワークでリンクループが発生します。これらを防止するための機能として、Loop ガード機能をサポートします。

Loop ガード機能が有効なポートの初期状態は、各 MSTI で Discard 状態です。ポートが BPDU を受信したとき、正常状態になっても、そのポートを designated ポートとして Forwarding 状態に遷移しません。Blocking 状態でパケットを転送しないため、一時的なリンクのループを回避できます。

ユーザの端末を接続したポートで Loop ガードを無効にすることはできません。BPDU を受信できないため、すべての MSTI で discard 状態になったままとなります。

ポートで、Loop ガード機能、Root ガード機能、Edge ポート機能は同時に設定することはできません。

装置の Root ポートと、交代するポートで Loop ガードを設定します。

以下に Loop ガードの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Ethernet interface view あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	―
3. Loop ガードを有効にする	**stp loop-protection**	デフォルト：無効

5.26.4 ポート役割の制限機能

注意:
この機能を使用することで、スパニングツリーのトポロジの接続に影響する可能性がありますので、注意して設定してください。

ユーザアクセスネットワークの装置の bridge ID を変更すると、コアネットワークのスパニングツリーのトポロジが変更する可能性があります。この問題を回避するため、ポート役割の制限機能を有効にすることができます。この機能を有効にすることで、ポートが上位の BPDU を受信したとき、ルートポートではなく代理ポートになります。

この機能はユーザアクセスネットワークに接続するポートに設定してください。

以下にポート役割の制限機能の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Ethernet interface view あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	―
3. ポート役割の制限機能を有効にする	**stp role-restriction**	デフォルト：無効

5.26.5 TC-BPDU ガードの有効化

装置はトポロジ変更(TC)の BPDU(BPDU はトポロジ変更を装置に通知します)パケットを受信すると、転送アドレスエントリを削除します。しかし、悪意のユーザから偽装した TC-BPDU パケットの攻撃を受けた場合、装置は非常に短い時間内に大量の TC-BPDU パケットを受信することになります。頻繁に削除オペレーション（MAC アドレステーブルの更新）を実行すると、装置のリソースを浪費し、ネットワークの安定性に大きな被害をもたらす可能性があります。

TC-BPDU ガードを有効にすると、最初に TC-BPDU を受信した後、指定時間内(10 秒)の間に、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、装置は、一定の期間の満了後に、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オペレーションを行うことを防ぐことができます。NEC は TC-BPDU ガードを有効にすることを推奨します。

以下に TC-BPDU ガードの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. TC-BPDU ガードを有効にする	**stp tc-protection**	デフォルト：有効 無効にすることを推奨しません。
3. (オプション設定項目) 10 秒間に転送アドレスエントリを削除する最大数を設定する	**stp tc-protection threshold** *number*	デフォルト：6

5.26.6 PVST BPDU ガード機能の有効化

MSTP が有効な装置は PVST BPDU を認識できないため、データトラフィックとして PVST BPDU を転送します。別の独立したネットワークにある PVST が有効な装置で PVST BPDU を受信した場合、PVST の計算に失敗する可能性があります。PVST の計算を失敗させないため、MSTP が有効な装置で PVST BPDU ガード機能を有効にします。ポートで PVST BPDU を受信した場合、装置はポートをシャットダウンします。

以下に PVST BPDU ガード機能の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. PVST BPDU ガード機能を有効にする	**stp pvst-bpdu-protection**	デフォルト：無効

5.27 TC BPDUの検出または受信するイベントの記録

この機能により装置は TC BPDU を検出または受信したときにログを生成できます。この機能は、PVST モードにのみ適用されます。

以下に装置が TC BPDU を検出または受信するイベントを記録できるようにする設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. 装置が TC BPDU を受信または検出するイベントを記録できるようにする	**stp log enable tc**	デフォルト：装置はTC BPDU を検出または受信してもログを生成しません。

5.28 トポロジ変更イベントによるSNMP notificationの有効化

この機能を有効にすると、スパニングツリーのトポロジ変更イベントが発生した場合、装置はログを作成し、SNMP に通知します。

正常にイベントの notification を送信するため､装置で SNMP を設定する必要があります。SNMP の設定の詳細は、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*17 ネットワーク管理と監視*”の” *4 章 SNMP*”を参照してください。

snmp-agent trap enable stp tc コマンドを使用するとき、以下のガイドラインに従ってください。

- コマンドは PVST モードでのみ適用します。
- **snmp-agent trap enable stp** コマンドは、スパニングツリーのトポロジ変更が発生した場合、SNMP notification の送信を有効にします。

以下に新スパニングツリーのトポロジ変更イベントによる SNMP notification の送信の有効化の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． スパニングツリーのトポロジ変更イベントによる SNMP notification の送信を有効にする	**snmp-agent trap enable stp tc**	デフォルト： PVSTモードではすべてのVLANで無効です。

5.29 スパニングツリーの表示と維持

すべての view で **display** コマンドを実行し、user view で **reset** コマンドを実行できます。

操作	コマンド
STPのガード機能によってブロッキング状態にあるポートの表示する	**display stp abnormal-port**
ポートのBPDU統計情報を表示する	**display stp bpdu-statistics** [**interface** *interface-type interface-number* [**instance** *instance-list*]]
STPの保護機能によってダウンしているポートを表示する	**display stp down-port**
MSTIポートの役割計算の履歴を表示する	**display stp** [**instance** *instance-list* | **vlan** *vlan-id-list*] **history**
MSTIの全ポートで送受信されたTC/TCN BPDUの統計情報を表示する	**display stp** [**instance** *instance-list* **| vlan** *vlan-id-list*] **tc**
スパニングツリーの状態および統計情報を表示する	**display stp** [**instance** *instance-list* | **vlan** *vlan-id-list*] [**interface** *interface-list*] [**brief**]
有効なMST regionの設定情報を表示する	**display stp region-configuration**
MSTIのRoot Bridgeの情報を表示する	**display stp root**
スパニングツリーの統計情報をクリアする	**reset stp** [**interface** *interface-list*]

5.30 スパニングツリー設定例

5.30.1 MSTP 設定例

I. ネットワーク要件

図 5-13 に示すようにすべての装置は同じ MST region にあります。Device A、Device B はディストリビューション層にあり、Device C、AC はアクセス層にあります。

異なる VLAN のパケットが異なるスパニングツリーに転送されるように MSTP を設定します。

- VLAN10 のパケットは MSTI1 で転送されます。
- VLAN30 のパケットは MSTI3 で転送されます。
- VLAN40 のパケットは MSTI4 で転送されます。
- VLAN20 のパケットは MSTI0 で転送されます。

VLAN10 と VLAN30 はディストリビューション層の装置のみ、VLAN40 はアクセス層の装置のみで通信します。MSIT1 と MSTI3 の Root Bridge は Device A、Device B となり、MSTI4 の Root Bridge は Device C となります

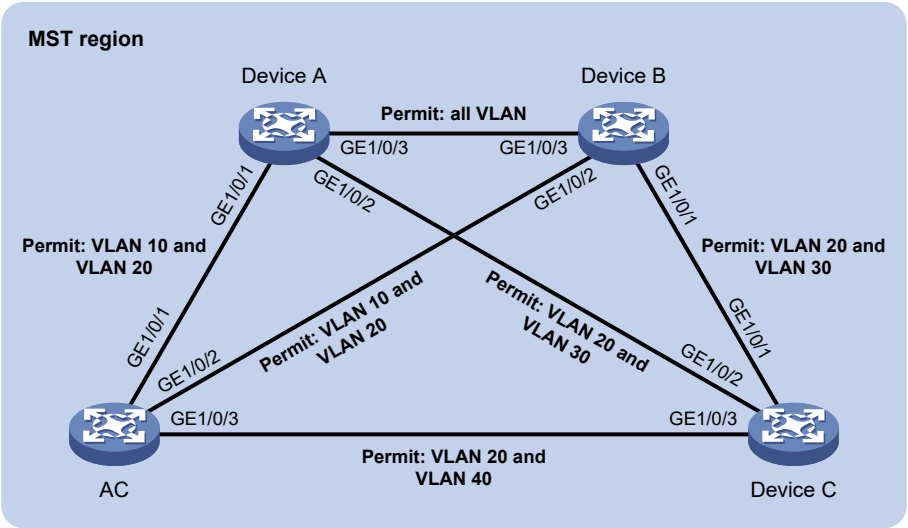


図 5-13 ネットワーク図

II. 設定手順

1) VLAN を作成し、VLAN メンバポートを設定します。(詳細は省略します)
   - □ Device A、Device B の両方で VLAN10、VLAN20、VLAN30 を作成します。
   - □ AC で VLAN10、VLAN20、VLAN40 を作成します。
   - □ Device C で VLAN20、VLAN30、VLAN40 を作成します。
   - □ 装置のポートをトランクポートに設定し、関連する VLAN を割り当てます。
2) Device A を設定します。

MST region view に移行し、region 名 **example** を設定します。

```
<DeviceA> system-view
[DeviceA] stp region-configuration
[DeviceA-mst-region] region-name example
```

VLAN10、VLAN30、VLAN40 をそれぞれ MSTI1、MSTI3、MSTI4 に割り当てます。

```
[DeviceA-mst-region] instance 1 vlan 10
[DeviceA-mst-region] instance 3 vlan 30
[DeviceA-mst-region] instance 4 vlan 40
```

MST region レベルを 0 とします。

```
[DeviceA-mst-region] revision-level 0
```

MST region の設定をアクティブにします。

```
[DeviceA-mst-region] active region-configuration
[DeviceA-mst-region] quit
```

MSTI1 の Root Bridge として Device A を設定します。

```
[DeviceA] stp instance 1 root primary
```

グローバルでスパニングツリーを有効にします。

```
[DeviceA] stp global enable
```

3) Device B を設定します。

MST region view に移行し、MST region 名 **example** を設定します。

```
<DeviceB> system-view
[DeviceB] stp region-configuration
[DeviceB-mst-region] region-name example
```

VLAN10、VLAN30、VLAN40 をそれぞれ MSTI1、MSTI3、MSTI4 に割り当てます。

```
[DeviceB-mst-region] instance 1 vlan 10
[DeviceB-mst-region] instance 3 vlan 30
[DeviceB-mst-region] instance 4 vlan 40
```

MST region レベルを 0 とします。

```
[DeviceB-mst-region] revision-level 0
```

MST region の設定をアクティブにします。

```
[DeviceB-mst-region] active region-configuration
[DeviceB-mst-region] quit
```

MSTI3 の Root Bridge として Device B を設定します。

```
[DeviceB] stp instance 3 root primary
```

グローバルでスパニングツリーを有効にします。

```
[DeviceB] stp global enable
```

4)　AC を設定します。

MST region view に移行し、MST region 名 **example** を設定します。

```
<AC> system-view
[AC] stp region-configuration
[AC-mst-region] region-name example
```

VLAN 10、VLAN 30、VLAN 40 をそれぞれ MSTI 1、MSTI 3、MSTI 4 に割り当てます。

```
[AC-mst-region] instance 1 vlan 10
[AC-mst-region] instance 3 vlan 30
[AC-mst-region] instance 4 vlan 40
```

MST region レベルを 0 とします。

```
[AC-mst-region] revision-level 0
```

MST region の設定をアクティブにします。

```
[AC-mst-region] active region-configuration
[AC-mst-region] quit
```

MSTI4 の Root Bridge として AC を設定します。

```
[AC] stp instance 4 root primary
```

グローバルでスパニングツリーを有効にします。

```
[AC] stp global enable
```

5)　Device C を設定します。

MST region view に移行し、MST region 名 **example** を設定します。

```
<DeviceC> system-view
[DeviceC] stp region-configuration
[DeviceC-mst-region] region-name example
```

VLAN10、VLAN30、VLAN40 をそれぞれ MSTI1、MSTI3、MSTI4 に割り当てます。

```
[DeviceC-mst-region] instance 1 vlan 10
[DeviceC-mst-region] instance 3 vlan 30
[DeviceC-mst-region] instance 4 vlan 40
```

MST region レベルを 0 とします。

```
[DeviceC-mst-region] revision-level 0
```

MST region の設定をアクティブにします。

```
[DeviceC-mst-region] active region-configuration
[DeviceC-mst-region] quit
```

グローバルでスパニングツリーを有効にします。

```
[DeviceC] stp global enable
```

III. 設定の確認

Device B が最も小さい Root Bridge ID を持っていると仮定します。結果として、Device B が MSTI 0 の Root Bridge となります。

ネットワークが安定したのち、**display stp brief** コマンドで、STP の概要情報を表示し、設定の確認を行います。

Device A のスパニングツリーの概要情報を表示します。

```
[DeviceA] display stp brief
 MST ID        Port                                        Role   STP State
Protection
 0             GigabitEthernet1/0/1                ALTE   DISCARDING    NONE
 0             GigabitEthernet1/0/2                DESI   FORWARDING    NONE
 0             GigabitEthernet1/0/3                ROOT   FORWARDING    NONE
 1             GigabitEthernet1/0/1                DESI   FORWARDING    NONE
 1             GigabitEthernet1/0/3                DESI   FORWARDING    NONE
 3             GigabitEthernet1/0/2                DESI   FORWARDING    NONE
 3             GigabitEthernet1/0/3                ROOT   FORWARDING    NONE
```

Device B のスパニングツリーの概要情報を表示します。

```
[DeviceB] display stp brief
 MST ID        Port                                        Role   STP State
Protection
 0             GigabitEthernet1/0/1                DESI   FORWARDING    NONE
 0             GigabitEthernet1/0/2                DESI   FORWARDING    NONE
 0             GigabitEthernet1/0/3                DESI   FORWARDING    NONE
 1             GigabitEthernet1/0/2                DESI   FORWARDING    NONE
 1             GigabitEthernet1/0/3                ROOT   FORWARDING    NONE
 3             GigabitEthernet1/0/1                DESI   FORWARDING    NONE
 3             GigabitEthernet1/0/3                DESI   FORWARDING    NONE
```

AC のスパニングツリーの概要情報を表示します。

```
[AC] display stp brief
 MST ID        Port                                        Role   STP State
Protection
 0             GigabitEthernet1/0/1                DESI   FORWARDING    NONE
 0             GigabitEthernet1/0/2                ROOT   FORWARDING    NONE
 0             GigabitEthernet1/0/3                DESI   FORWARDING    NONE
 1             GigabitEthernet1/0/1                ROOT   FORWARDING    NONE
 1             GigabitEthernet1/0/2                ALTE   DISCARDING    NONE
 4             GigabitEthernet1/0/3                DESI   FORWARDING    NONE
```

Device C のスパニングツリーの概要情報を表示します。

```
[DeviceC] display stp brief
 MST ID        Port                                        Role   STP State
Protection
 0             GigabitEthernet1/0/1                ROOT   FORWARDING    NONE
 0             GigabitEthernet1/0/2                ALTE   DISCARDING    NONE
 0             GigabitEthernet1/0/3                ALTE   DISCARDING    NONE
 3             GigabitEthernet1/0/1                ROOT   FORWARDING    NONE
 3             GigabitEthernet1/0/2                ALTE   DISCARDING    NONE
 4             GigabitEthernet1/0/3                ROOT   FORWARDING    NONE
```

出力情報から、図 5-14 のように VLAN の MSTI マッピングの設定を行っていることがわかります。

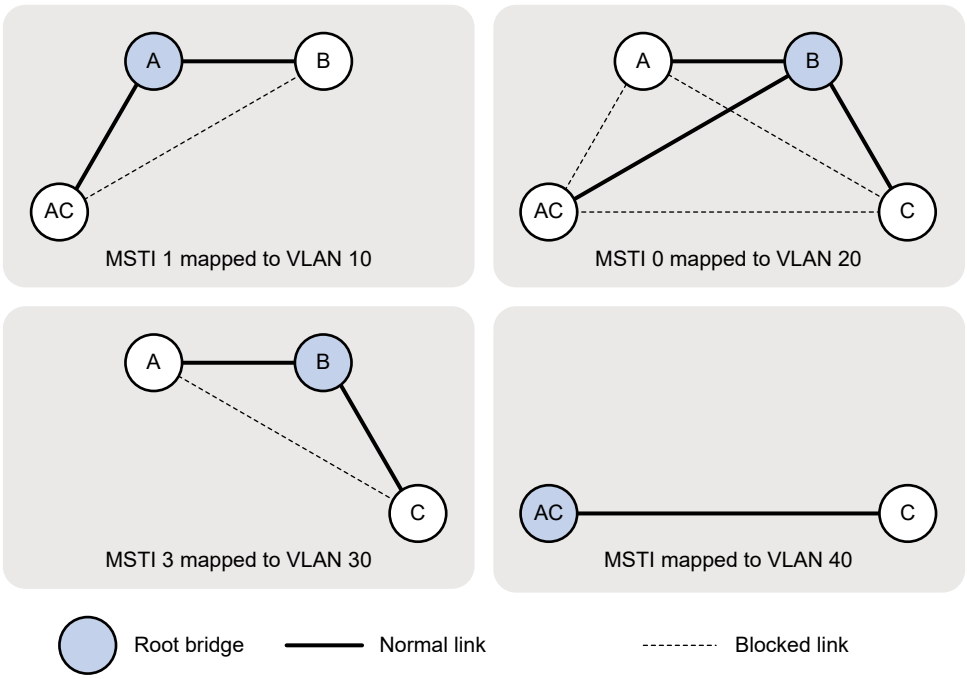


図 5-14 異なる VLAN への MSTI のマッピングの設定

目次

このセクションのページは**5-x-x** です。

6章 LLDP 6-1
6.1 概要 6-1
6.1.1 基本コンセプト 6-1
6.1.2 動作メカニズム 6-7
6.1.3 プロトコルと標準 6-8
6.2 LLDP設定作業リスト 6-8
6.3 LLDPの基本設定 6-9
6.3.1 LLDPの有効化 6-9
6.3.2 LLDP動作モードの設定 6-9
6.3.3 再初期化遅延時間の設定 6-9
6.3.4 LLDPポーリングの有効化 6-10
6.3.5 アドバタイズ可能なTLVの設定 6-10
6.3.6 管理アドレスTLVのアドバタイズの設定 6-12
6.3.7 LLDPフレーム送信パラメータの設定 6-13
6.3.8 LLDPフレームのカプセル化フォーマットの設定 6-14
6.4 LDPトラップおよびLLDP-MEDトラップの設定 6-14
6.5 LLDPの表示と維持 6-15
6.6 LLDPの設定例 6-15
6.6.1 LLDPの基本的な設定例 6-15

6章 LLDP

6.1 概要

異なるベンダが存在するネットワークのとき、標準の設定情報を交換するプラットフォームは、異なるベンダからの異なるタイプのネットワーク装置を相互に検出します。これにより設定を交換できることを保証します。

LLDP（Link Layer Discovery Protocol）は、IEEE802.1AB で規定されています。データリンクレイヤで直接装置に接続された装置間の装置情報を交換するプロトコルです。LLDP では、装置は LLDPDU（LLDP データユニット）にある TLV と呼ばれるタイプ（Type）長さ（Length）値（Value）の形式を利用して、ローカル装置情報を、直接接続された装置に送信します。ローカル装置情報はシステム機能、管理 IP アドレス、装置 ID、ポート ID を含みます。装置は LLDP 隣接装置から受信した LLDPDU の装置情報を標準 MIB に格納します。MIB についての詳細は、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*17 ネットワーク管理と監視*”の” *4 章 SNMP*”を参照してください。LLDP はレイヤ 2 のネットワークトポロジの変化をただちに検出し、識別するためにネットワーク管理システムを有効にします。

6.1.1 基本コンセプト

I. LLDP エージェント

LLDP が動作するところで LLDP エージェントはエンティティをマッピングします。複数の LLDP エージェントは同時にインタフェースで動作することができます。

LLDP エージェントは以下のタイプに分類されます。

- Nearest bridge エージェント
- Nearest customer bridge エージェント
- Nearest non-TPMR bridge エージェント

Two-port MAC Relay （TPMR）は 2 つの外部アクセスブリッジポートのブリッジタイプで、MAC ブリッジの機能をサポートします。TPMR は以下を除いて、すべてのフレームベースのメディアに独立したプロトコルに透過的です。

- 独立したプロトコル行き
- TPMR のリレー機能が転送しないように予約された MAC アドレス行き

LLDP は隣接エージェント間でパケットを交換し、隣接情報を作成、維持します。図 6-1 に LLDP エージェントの隣接関係を示します。LLDP はカスタマブリッジ（CB）とサービスブリッジ（SB）の 2 つのブリッジモードをもちます。

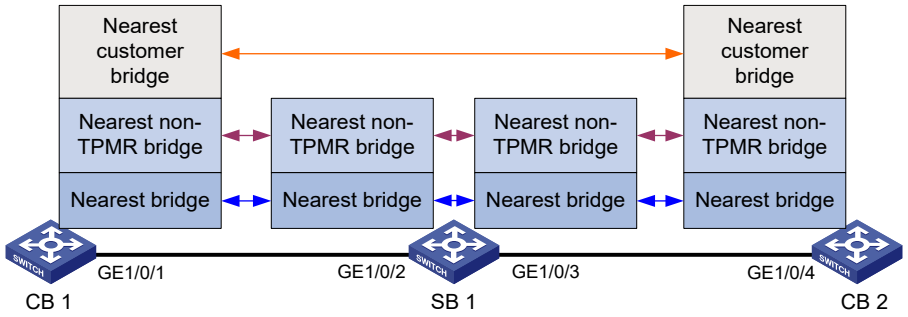


図 6-1 LLDP 隣接関係

II. LLDP フレームフォーマット

LLDP は LLDP フレームの装置情報を送信します。LLDP フレームは Ethernet II あるいは SNAP フレームでカプセル化されています。

- Ethernet II にカプセル化した LLDP フレーム

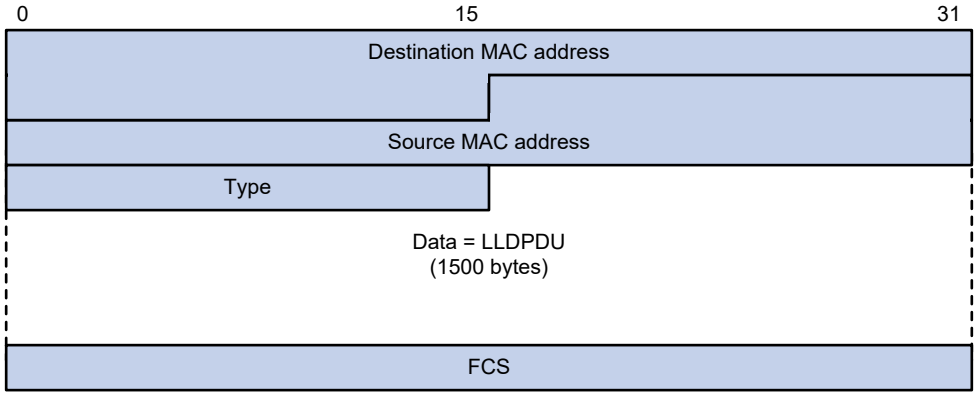


図 6-2 Ethernet II にカプセル化した LLDP フレーム

表 6-1 Ethernet II にカプセル化した LLDP フレームフィールド

フィールド	説明
Destination MAC address	LLDPフレームがアドバタイズしたMACアドレスです。 LLDPは異なるエージェントタイプ向けのLLDPフレームの宛先MACアドレスとして異なるマルチキャストアドレスを指定します。同一インタフェース上で異なるエージェントタイプで送受信したLLDPフレームを区別します。 • LLDPフレーム0x0180-C200-000Eはnearest bridge向けです。 • LLDPフレーム0x0180-C200-000はnearest customer bridge向けです。 • LLDPフレーム0x0180-C200-0003はnearest TPMR bridge向けです。
Source MAC address	送信ポートのMACアドレスです。
Type	上位レイヤプロトコルのEthernetタイプです。LLDPは0x88CCです。

フィールド	説明
Data	LLDPDUです。
FCS	フレームチェックシーケンスで、32ビットCRCの値が受信したEthernetフレームを確認するために使われます。

- SNAP にカプセル化した LLDP フレーム

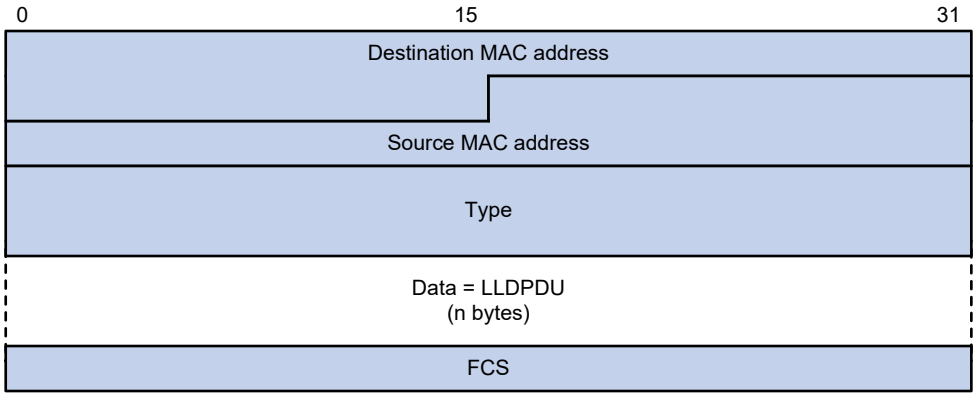


図 6-3 SNAP にカプセル化したフレーム

表 6-2 SNAP にカプセル化したフレームフィールド

フィールド	説明
Destination MAC address	LLDPフレームがアドバタイズしたマルチキャストのMACアドレスです。Ethernet2でカプセル化したLLDPフレームのMACアドレスと同一です。
Source MAC address	送信ポートのMACアドレスです。
Type	上位レイヤプロトコルのSNAPタイプです。LLDPは0xAAAA-0300-0000-88CCです。
Data	LLDPDUです。
FCS	フレームチェックシーケンスで、32ビットCRCの値が受信したEthernetフレームを確認するために使われます。

III. LLDPDU

LLDP は情報を交換するために LLDPDU を使用します。LLDPDU は複数の TLV（タイプ, 長さ,値）から構成されています。図 6-4で示すように、装置上の各 TLV をアドバタイズします。

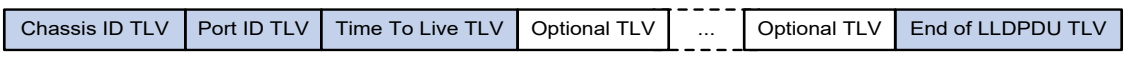


図 6-4 LLDPDU カプセルフォーマット

LLDPDU は、最大で 32 種類の TLV をもつことができます。ます。必須の TLV は、Chassis ID TLV、Port ID TLV、Time to Live TLV、End of LLDPDU TLV です。他の TLV はオプションです。

IV. TLV

TLV はタイプ、長さ、値のフィールドが含まれる情報の要素です。

LLDPDU TLV は以下のカテゴリに分類されます。

- 基本的な管理 TLV
- 組織規定された TLV （IEEE 802.1、IEEE 802.3）
- LLDP-MED（media endpoint discovery）関連の TLV

基本的な TLV は装置を管理するのに必要不可欠なカテゴリです。組織規定された TLV と LLDP-MED 関連の TLV は拡張された装置管理のために使用されます。標準あるいは他の組織によって定義され、LLDPDU のオプションです。

- 基本的な管理 TLV

表 6-3に基本的な管理 TLV タイプを示します。基本的な管理 TLV のいくつかは、各 LLDPDU に必須です。

表 6-3 基本的な管理 TLV

タイプ	説明	補足
Chassis ID	送信する装置のBridge MACアドレスを指定します。	必須
Port ID	送信ポートのIDを指定します。 ● LLDPDUがLLDP-MEDを含んでいる場合、Port ID TLVは送信ポートのMACアドレスです。 ● LLDPDUがLLDP-MEDを含んでいない場合、Port ID TLVはポート名です。	
Time to Live	受信する装置のTTLを指定します。	
End of LLDPDU	LLDPDUのTLVシーケンスの終端をマーキングします。	オプション
Port Description	送信するポートの説明を指定します。	
System Name	送信する装置の装置名を指定します。	
System Description	送信する装置の説明を指定します。	
System Capabilities	送信する装置の主な機能や有効な機能を識別します。	
Management Address	以下の要素を指定します。 ● ローカル装置の管理アドレスです。 ● インタフェース番号、アドレスに関連したOIDです。	

- IEEE 802.1 組織指定 TLV

表 6-4 IEEE 802.1 組織指定 TLV

タイプ	説明
Port VLAN ID	ポートのVLAN識別子（PVID） を指定します。
Port And Protocol VLAN ID	装置がプロトコルVLANをサポートしているかどうかを示します。サポートしている場合、プロトコルのVLAN IDです。
VLAN Name	ポートが属しているVLANの名前を示します。
Protocol Identity	ポートでサポートされるプロトコルを示します。

タイプ	説明
DCBX	Data center bridging exchangeプロトコルです。 🕮 メモ： DCBX TLVはサポートしていません。
EVB module	Edge Virtual Bridgingモジュールです。EVB TLV、CDCP TLVが含まれます。 🕮 メモ： EVB TLVをサポートしていません。
Link Aggregation	リンクアグリゲーションをサポートするポートかどうかを示します。もしサポートしている場合、リンクアグリゲーションが有効です。
Management VID	Management VLAN IDです。
VID Usage Digest	VLAN ID usage digestです。
ETS Configuration	Enhanced Transmission Selection configurationです。
ETS Recommendation	ETS recommendationです。
PFC	Priority-based Flow Controlです。
APP	Application protocolです。
QCN	Quantized Congestion Notificationです。

🕮 メモ：

本装置は Protocol identity TLV と VLAN ID usage digest TLV を受信することができますが、TLV を送信することはできません。

- IEEE 802.3 組織指定 TLV

表 6-5 IEEE 802.3 組織指定 TLV

タイプ	説明
MAC/PHY Configuration/Status	送信するポートの通信速度、通信モード、オートネゴシエーションのサポート状況、オートネゴシエーションの状態、現在の通信速度、現在の通信モードの状態を示します。
Power Via MDI	ポートの電源供給状態を示します。 • PoEタイプ（PSEあるいはPD） • PoEモード • PSE電源供給のサポート状況 • PSE電源供給の有効/無効状態 • PoEモードの管理可能/不可状態 • 電力供給タイプ • 電力ソース • 電力優先度 • PDが要求した電力 • PSEが割り当てた電力
Maximum Frame Size	ポートでサポートされる最大フレームサイズ（MTU）を示します。

タイプ	説明
Power Stateful Control	送信ポートで管理される電源状態制御を示します。 • PSE/PDの電源 • PSE/PDの優先度 • PSE/PDの電力
Energy-Efficient Ethernet	EEE（Energy Efficient Ethernet）を示します。

🕮 **メモ：**

Power Stateful Control TLV は IEEE802.3at Draft1.0 で定義されています。最近のバージョンでは Power Stateful Control TLV をサポートしていません。QX シリーズは Power Stateful Control TLV を受信したときのみ送信を行います。

LLDP-MED TLV は複数のアプリケーションを VoIP（voice over IP）の拡張されたアプリケーションに提供します。たとえば基本設定、ネットワークポリシー設定、アドレス、ディレクトリ管理などのアプリケーションです。LLDP-MED TLV は Ethernet で音声装置の費用効果、使用しやすさのソリューションを提供します。表 6-6に LLDP-MED TLV を示します。

表 6-6 LLDP-MED TLV

タイプ	説明
LLDP-MED Capabilities	LLDP-MED LEDをサポートするネットワークの装置がLLDP-MED LEDをアドバタイズすることを可能にします。
Network Policy	ポートのVLAN ID、VLANタイプ、指定アプリケーションのレイヤ2/レイヤ3の優先度を､ネットワーク装置あるいは端末装置がアドバタイズすることを可能にします。
Extended Power-via-MDI	ネットワーク装置あるいは端末装置が電源供給能力をアドバタイズすることを可能にします。TLVはPower Via MDI TLVの拡張です。
Hardware Revision	端末装置がハードウェアバージョンをアドバタイズすることを可能にします。
Firmware Revision	端末装置がファームウェアバージョンをアドバタイズすることを可能にします。
Software Revision	端末装置がソフトウェアバージョンをアドバタイズすることを可能にします。
Serial Number	端末装置がシリアル番号をアドバタイズすることを可能にします。
Manufacturer Name	端末装置がベンダ名をアドバタイズすることを可能にします。
Model Name	端末装置がモデル名をアドバタイズすることを可能にします。
Asset ID	端末装置がasset IDをアドバタイズすることを可能にします。一般的な使用方法として、ディレクトリ管理、価値のトラッキングを補助するためのエンドポイント用に指定されます。
Location Identification	位置をもとにしたアプリケーションの内容を使用するため、ネットワーク装置が端末装置の位置識別情報をアドバタイズすることを可能にします。

🕮 **メモ：**

- MAC/PHY configuration/status TLV がアドバタイズされない場合、LLDP-MED TLV をアドバタイズ可能でも LLDP-MED TLV は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 がアドバタイズ可能でもアドバタイズされません。

V. 管理アドレス

装置の管理アドレスは、ネットワークマネジメントシステムで使われ、トポロジ維持やネットワーク管理で装置を認識するために使われます。管理アドレスは、management address TLV にカプセル化されています。

6.1.2 動作メカニズム

I. LLDP 動作モード

LLDP エージェントは以下のモードを動作させることができます。

- **TxRx モード** – このモードの LLDP エージェントは LLDP フレームの送信、受信を行うことができます。
- **Tx モード** – このモードの LLDP エージェントは LLDP フレームの送信のみを行うことができます。
- **Rx モード** – このモードの LLDP エージェントは LLDP フレームの受信のみを行うことができます。
- **Disable モード** – このモードの LLDP エージェントは LLDP フレームの送信も受信も行うことができません。

LLDP エージェントの動作モードが別の動作モードに変更されるたびに LLDP は初期化されます。LLDP エージェントの動作モードが別の動作モードへ変更したとき、設定可能な再初期化遅延時間を設定することで LLDP が頻繁に初期化されるのを防ぐことができます。再初期化遅延時間を設定する場合、LLDP は LLDP 動作モードが変更したのち、指定された期間が終了するまで、再初期化を行いません。

II. LLDP フレームの送信

TxRx モードあるいは Tx モードで動作する LLDP エージェントは、定期的およびローカルの設定が変更されるときに、直接接続されている装置へ LLDP フレームを送信します。LLDP フレームがローカルの装置情報を頻繁に変更する際、ネットワークを占有してしまうことを防止するため、LLDP は LLDP フレームを制限するためトークバケットメカニズムを使用します。トークンバケットメカニズムの詳細は、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*16 QoS*”を参照してください。

LLDP は自動的に以下のいずれかのケースを用いて早急に LLDP フレームを送信することができます。

- 新しい LLDP フレームが受信され、ローカル装置に新しい装置情報をアドバタイズします。

- LLDP エージェントの LLDP 動作モードが Disable あるいは Rx から、TxRx あるいは Tx に変更したときに早急に LLDP フレームを送信します。

早急に LLDP フレームを送信するメカニズムでは、LLDP 隣接装置がローカル装置を発見できるように、指定した数の LLDP フレームが、設定可能なできるだけ早い送信間隔で連続して送信されます。装置は指定した数の LLDPDU を送信した後、送信間隔を通常に戻します。

III. LLDP フレームの受信

TxRx モードまたは Rx モードで動作している LLDP エージェントは、受信した LLDP フレームを受信するたびに TLV の有効性を確認します。TLV が有効である場合、LLDP エージェントは情報を保存し、エージングタイマを開始します。エージングタイマのデフォルトは LLDP フレームによってアドバタイズされる Time To Live TLV の TTL と同じ値です。LLDP エージェントが新しい LLDP フレームを受信したとき、エージングタイマは再スタートします。LLDP フレームでアドバタイズされた Time To Live TLV の TTL が 0 になったとき、保存されているすべての情報はエージアウトします。

6.1.3 プロトコルと標準

- IEEE 802.1AB-2005, *Station and Media Access Control Connectivity Discovery*
- IEEE 802.1AB-2009, *Station and Media Access Control Connectivity Discovery*
- ANSI/TIA-1057, *Link Layer Discovery Protocol for Media Endpoint Devices*
- DCB *Capability Exchange Protocol Specification Rev 1.00*
- DCB *Capability Exchange Protocol Base Specification Rev 1.01*
- IEEE Std 802.1Qaz-2011, *Media Access Control (MAC) Bridges and Virtual Bridged Local Area Networks-Amendment 18: Enhanced Transmission Selection for Bandwidth Sharing Between Traffic Classes*

6.2 LLDP設定作業リスト

作業リスト
LLDPの基本設定： • （必須設定項目） LLDPの有効化 • （オプション設定項目） LLDP動作モードの設定 • （オプション設定項目） 再初期化遅延時間の設定 • （オプション設定項目） LLDPポーリングの有効化 • （オプション設定項目） アドバタイズ可能なTLVの設定 • （オプション設定項目） 管理アドレスTLVのアドバタイズの設定 • （オプション設定項目） LLDPフレーム送信パラメータの設定 • （オプション設定項目） LLDPフレームのカプセル化フォーマットの設定
（オプション設定項目） LDPトラップおよびLLDP-MEDトラップの設定

6.3 LLDPの基本設定

6.3.1 LLDP の有効化

LLDP はポートで LLDP を有効にするには、ポートとグローバルの両方で有効にする必要があります。

以下に LLDP を有効化する設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． グローバルで LLDP を有効化する	**lldp global enable**	デフォルト：無効
3． interface view に移行する	**interface** *interface-type interface-number*	―
4． LLDP を有効化する	**lldp enable**	デフォルト：有効

6.3.2 LLDP 動作モードの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． interface view に移行する	**interface** *interface-type interface-number*	―
3． 動作モードを設定する	● Layer 2/Layer 3 Ethernet interface viewあるいは management Ethernet interface viewでの設定：**lldp** [**agent nearest-customer**] **admin-status** { **disable** | **rx** | **tx** | **txrx** } ● Layer 2 aggregate interface viewでの設定：**lldp agent nearest-customer admin-status** { **disable** | **rx** | **tx** | **txrx** }	デフォルト： nearest bridgeエージェント：txrxモードです。 nearest customer bridgeエージェント：disableです。 Ethernet interface viewでエージェントタイプが指定されていない場合、nearest bridgeエージェントで動作モードを設定します。 aggregate interface viewではnearest customer bridgeエージェントの動作モードのみを設定できます。

6.3.3 再初期化遅延時間の設定

ポートの LLDP 動作モードを変更した場合、ポートは遅延時間の経過後、プロトコル状態を初期化します。再初期化遅延時間を設定することで、ポートの LLDP 動作モードが頻繁に変更することを防ぐことができます。

以下に再初期化遅延時間の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―

操作	コマンド	補足
2． 再初期化遅延時間を設定する	**lldp timer reinit-delay** *delay*	デフォルト：2秒

6.3.4 LLDP ポーリングの有効化

LLDP ポーリングを有効にした装置はローカルの設定の変更を定期的に確認します。設定の変更を検出すると、装置は隣接装置へ変更を知らせるために LLDP フレームを送信します。

以下に LLDP ポーリングの有効化の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． interface view に移行する	**interface** *interface-type interface-number*	―
3． LLDP ポーリングの有効化を設定する	● Layer 2/Layer 3 Ethernet interface viewあるいは management Ethernet interface viewでの設定：**lldp** [**agent nearest-customer**] **check-change-interval** *interval* ● Layer 2 aggregate interface viewでの設定：**lldp agent nearest-customer check-change-interval** *interval*	デフォルト：無効

6.3.5 アドバタイズ可能な TLV の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． interface view に移行する	**interface** *interface-type interface-number*	―

操作	コマンド	補足
3. LLDPDU TLV を設定する（Layer 2 Ethernet interface view）	• **lldp tlv-enable** { **basic-tlv** { **all** | **port-description | system-capability | system-description | system-name | management-address-tlv** [*ip-address* | **interface loopback** *interface-number*] } | **dot1-tlv** { **all** | **port-vlan-id** | **link-aggregation | protocol-vlan-id** [*vlan-id*] | **vlan-name** [*vlan-id*] | **management-vid** [*mvlan-id*] } | **dot3-tlv** { **all | mac-physic | max-frame-size** } | **med-tlv** { **all** | **capability | inventory | power-over-ethernet | location-id** { **civic-address** *device-type country-code* { *ca-type ca-value* }&<1-10> | **elin-address** *tel-number* } } } • **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 | link-aggregation** } }	デフォルト： • Nearest bridgeエージェントはDCBX、location identification TLV, port VLAN ID TLV、protocol VLAN ID TLV、VLAN name TLV、management VLAN ID、Energy-Efficient Ethernet TLVを除いてすべてのLLDP TLVタイプを送信します。 • Nearest customer bridge エージェントはbasic TLV、IEEE 802.1 organizationally specific TLVを送信します。
4. LLDPDU TLV を設定する（Layer 3 Ethernet interface view）	• **lldp tlv-enable** { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [*ip-address* | **interface loopback** *interface-number*] } | **dot1-tlv** { **all** | **link-aggregation** } | **dot3-tlv** { **all** | **mac-physic** | **max-frame-size** } | **med-tlv** { **all** | **capability** | **inventory** | **power-over-ethernet** | **location-id** { **civic-address** *device-type country-code* { *ca-type ca-value* }&<1-10> | **elin-address** *tel-number* } } }	デフォルト： • Nearest bridgeエージェントは802.1 organizationally specific TLV setのLink aggregation TLV、サポートされているすべての802.3 organizationally specific TLV、network policy TLVを除くサポートされているすべての LLDP-MED TLVを送信します。
5. LLDPDU TLV を設定する（management Ethernet interface view）	• **lldp tlv-enable** { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [*ip-address*] } | **dot1-tlv** { **all** | **link-aggregation** } | **dot3-tlv** { **all** | **mac-physic** | **max-frame-size** } | **med-tlv** { **all** | **capability** | **inventory** | **power-over-ethernet** | **location-id** { **civic-address** *device-type country-code* { *ca-type ca-value* }&<1-10> | **elin-address** *tel-number* } } }	デフォルト： • Nearest bridgeエージェントは802.1 organizationally specific TLV setのLink aggregation TLV、サポートされているすべての802.3 organizationally specific TLV、サポートされているすべての LLDP-MED TLVを送信します。

操作	コマンド	補足
6. LLDPDU TLV を設定する（Layer 2 aggregate interface view）	• **lldp agent nearest-customer tlv-enable** { **basic-tlv** { **all** | **management-address-tlv** *[ip-address]* | **port-description** | **system-capability** | **system-description** | **system-name** } | **dot1-tlv** { **all** | **port-vlan-id** } } • **lldp tlv-enable dot1-tlv** { **protocol-vlan-id** [*vlan-id*] | **vlan-name** [*vlan-id*] | **management-vid** [*mvlan-id*] }	デフォルト： • Nearest customer bridgeエージェントはbasic TLV、IEEE802.1組織指定TLV（port VLAN ID TLV、protocol VLAN ID TLV、VLAN name TLV、management VLAN ID TLVのみ）を送信します • Nearest bridgeはアグリゲートインタフェースでサポートしていません。

6.3.6 管理アドレス TLV のアドバタイズの設定

LLDP は管理アドレス TLV の数値形式または string 形式でカプセル化します。

デフォルトでは、管理アドレス TLV は数値形式でカプセル化されています。隣接装置が管理アドレス TLV を string 形式でカプセル化している場合、管理アドレス TLV を string 形式でカプセル化することができます。これにより隣接装置と正常に通信することができます。

管理アドレス TLV のアドバタイズは、インタフェース単位で設定できます。装置は、インタフェースの管理アドレス TLV アドバタイズ設定を以下の順序で選択します。

1) インタフェースベース設定。**lldp tlv-enable** コマンドと **management-address-tlv** キーワードを使用して設定します。
2) インタフェースのデフォルト設定。
   デフォルト:
   - Nearest bridge エージェントと Nearest customer bridge エージェントは、管理アドレス TLV をアドバタイズします。

以下に管理アドレスのカプセル化フォーマットの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. interface view に移行する	**interface** *interface-type interface-number*	—

操作	コマンド	補足
3． LLDPDU 内の管理アドレスの設定、管理アドレスの送信を設定する	● Layer 2 Ethernet interface viewあるいはmanagement Ethernet interface viewでの設定： **lldp tlv-enable basic-tlv management-address-tlv** [*ip-address* | **interface loopback** *interface-number*] **lldp agent nearest-customer tlv-enable basic-tlv management-address-tlv** [*ip-address*] ● Layer 3 Ethernet interface viewでの設定： **lldp tlv-enable basic-tlv management-address-tlv** [*ip-address* | **interface loopback** *interface-number*] **lldp agent nearest-customer tlv-enable basic-tlv management-address-tlv** [*ip-address*] ● Layer 2 aggregate interface viewでの設定： **lldp agent nearest-customer tlv-enable basic-tlv management-address-tlv** [*ip-address*]	デフォルト：nearest bridgeエージェントとnearest customer bridgeエージェントはLLDPDUの管理アドレスを送信します。
4． 管理アドレス TLV のカプセル化フォーマットを string 形式として設定する	● Layer 2/Layer 3 Ethernet interface viewあるいはmanagement Ethernet interface viewでの設定： **lldp** [**agent nearest-customer**] **management-address-format string** ● Layer 2 aggregate interface viewでの設定： **lldp agent nearest-customer management-address-format string**	デフォルト：数値形式

6.3.7 LLDP フレーム送信パラメータの設定

LLDPDU でアドバタイズされる Time To Live TLV は、LLDPDU の装置情報の有効時間を決めて、隣接装置で保存されます。

TTL の乗数を設定することにより、隣接装置に送信する LLDPDU の 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 の乗数 × LLDP フレームの 送信間隔 ＋ 1

TTL は最大 65535 秒ということに注意してください。それより大きい場合、65535 秒に丸められます。

以下に LLDPDU に関するパラメータの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． TTL の乗数を設定する	**lldp hold-multiplier** *value*	デフォルト： 4
3． LLDP フレームの送信間隔を設定する	**lldp timer tx-interval** *interval*	デフォルト： 30秒

操作	コマンド	補足
4． 新しい隣接装置を検出したときの LLDP フレームの送信回数を設定する	**lldp fast-count** *count*	デフォルト： 4

6.3.8 LLDP フレームのカプセル化フォーマットの設定

LLDP フレームを処理する初期バージョンの LLDP は、両端で同じカプセル化フォーマットが必要です。初期バージョンの LLDP で動作する装置に隣接したローカル装置は、初期バージョンの LLDP で動作する装置と同じカプセル化フォーマットで設定してください。

以下に SNAP に LLDP フレームのカプセル化フォーマットの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． interface view に移行する	**interface** *interface-type interface-number*	―
3． SNAP に LLDPDU のカプセル化フォーマットを設定する	• Layer 2/Layer 3 Ethernet interface viewあるいは management Ethernet interface viewでの設定： **lldp** [**agent nearest-customer**] **encapsulation snap** • Layer 2 aggregate interface viewでの設定： **lldp agent nearest-customer encapsulation snap**	デフォルト： Ethernet II

6.4 LDPトラップおよびLLDP-MEDトラップの設定

LLDP トラップまたは LLDP-MED トラップは、ネットワーク管理システムに新しい隣接装置の検知やリンクの故障などのイベントを知らせるために使用されます。

LLDP のトラップ送信間隔を設定する前に、LLDP トラップおよび LLDP-MED トラップ送信間隔の以下の影響を理解しておく必要があります。

- 間隔の値が大きいと、トラップ送信頻度が低くなり、システムリソースの占有率が低くなります。これは、装置上のネットワークトポロジが頻繁に変更されるシナリオに適しています。ただし、間隔を大きすぎる値に設定しないでください。間隔の値が大きすぎると、ネットワーク管理システムが隣接の変更を時間的に識別できなくなり、装置上のネットワークトポロジが時間内に更新されなくなります。
- 間隔の値が小さいと、トラップ送信頻度が高くなります。これは、トポロジに依存するシナリオに適しています。ただし、間隔を小さすぎる値に設定しないでください。間隔の値が小さすぎると、ネットワーク管理システムは隣接ステータス情報を頻繁に更新します。これはシステムリソースを占有しすぎるだけでなく、装置上でネットワークトポロジ振動を引き起こします。

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。LLDP トラップまたは LLDP-MED トラップが有効になっている場合、装置は頻繁にトラップ情報を

ネットワーク管理システムに送信するため、システムの負荷が増加し、リソースが浪費されます。ネットワークの初期段階で LLDP トラップまたは LLDP-MED トラップを有効にしないことをお勧めします。

以下に LLDP トラップおよび LLDP-MED トラップの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. interface view に移行する	**interface** *interface-type interface-number*	―
3. LLDP-MED トラップの送信を有効にする	● Layer 2/Layer 3 Ethernet interface viewあるいは management Ethernet interface viewでの設定： **lldp notification med-topology-change enable**	デフォルト：無効
4. system view に戻る	**quit**	―
5. （オプション設定項目）LLDP トラップの送信間隔を設定する	**lldp timer notification-interval** *interval*	デフォルト：30秒

6.5 LLDPの表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
ローカルLLDP情報を表示する	**display lldp local-information** [**global** | **interface** *interface-type interface-number*]
隣接装置から受信したLLDP TLVの情報を表示する	**display lldp neighbor-information** [[[**interface** *interface-type interface-number*] [**verbose**]] | **list** [**system-name** *system-name*]]
LLDPの統計情報を表示する	**display lldp statistics** [**global** | [**interface** *interface-type interface-number*]]
ポートのLLDPのステータスを表示する	**display lldp status** [**interface** *interface-type interface-number*]
現在送信されているLLDP TLVのタイプを表示する	**display lldp tlv-config** [**interface** *interface-type interface-number*]

6.6 LLDPの設定例

6.6.1 LLDP の基本的な設定例

I. ネットワーク要件

図 6-5に示すように、Switch と AC 上で LLDP を設定して、NMS でリンクをモニタします。



図 6-5 ネットワーク図

II. 設定手順

1)　Switch を設定します。

グローバルで LLDP を有効にします。

```
<Switch> system-view
[Switch] lldp global enable
```

GigabitEthernet 1/0/1 で LLDP を有効にします。デフォルトではポートで LLDP が有効です。

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] lldp enable
```

GigabitEthernet 1/0/1 で LLDP の動作モードを Rx に設定します。

```
[Switch-GigabitEthernet1/0/1] lldp admin-status rx
[Switch-GigabitEthernet1/0/1] quit
```

GigabitEthernet 1/0/2 で LLDP を有効にします。デフォルトではポートで LLDP が有効です。

```
[Switch] interface gigabitethernet1/2
[Switch-GigabitEthernet1/0/2] lldp enable
```

GigabitEthernet 1/0/2 で LLDP の動作モードを Rx に設定します。

```
[Switch-GigabitEthernet1/0/2] lldp admin-status rx
[Switch-GigabitEthernet1/0/2] quit
```

2)　AC を設定します。

グローバルで LLDP を有効にします。

```
<AC> system-view
[AC] lldp global enable
```

GigabitEthernet 1/0/1 で LLDP を有効にします。デフォルトではポートで LLDP が有効です。

```
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] lldp enable
```

GigabitEthernet 1/0/1 で LLDP の動作モードを Tx に設定します。

```
[AC-GigabitEthernet1/0/1] lldp admin-status tx
[AC-GigabitEthernet1/0/1] quit
```

III. 設定の確認

Switch の GigabitEthernet 1/0/2 が次の条件を満たしていることを確認します。

- ポートが隣接装置に接続しています。
- ポートは Rx モードで動作し、LLDP フレームを受信できますが、LLDP フレームを送信することはできません。

[Switch] display lldp status

```
Global status of LLDP: Enable
Bridge mode of LLDP: customer-bridge
The current number of LLDP neighbors: 2
The current number of CDP neighbors: 0
LLDP neighbor information last changed time: 0 days, 0 hours, 4 minutes, 40 seconds
Transmit interval              : 30s
Fast transmit interval         : 1s
Transmit credit max            : 5
Hold multiplier                : 4
Reinit delay                   : 2s
Trap interval                  : 30s
Fast start times               : 4

LLDP status information of port 2 [GigabitEthernet1/0/2]:
LLDP agent nearest-bridge:
Port status of LLDP            : Enable
Admin status                   : Rx_Only
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    : 21
Number of received unknown TLV : 3

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    : 1
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    : 16
Number of received unknown TLV : 0
```

Switch と AC のリンクを切断します。

Switch の GigabitEthernet 1/0/2 が隣接装置と接続していないことを確認します。

[Switch] display lldp status

```
Global status of LLDP: Enable
The current number of LLDP neighbors: 1
```

```
The current number of CDP neighbors: 0
LLDP neighbor information last changed time: 0 days, 0 hours, 5 minutes, 20 seconds
Transmit interval              : 30s
Fast transmit interval         : 1s
Transmit credit max            : 5
Hold multiplier                : 4
Reinit delay                   : 2s
Trap interval                  : 30s
Fast start times               : 4

LLDP status information of port 2 [GigabitEthernet1/0/2]:
LLDP agent nearest-bridge:
Port status of LLDP            : Enable
Admin status                   : Rx_Only
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-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    : 1
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    : 16
Number of received unknown TLV : 0
```

目次

このセクションのページは**5-x-x** です。

7章 レイヤ2フォワーディング 7-1
7.1 標準のレイヤ2フォワーディング 7-1
7.2 標準のレイヤ2フォワーディングの表示と維持 7-1
7.3 高速レイヤ2フォワーディング 7-1
7.4 高速のレイヤ2フォワーディングの表示と維持 7-2

7章 レイヤ 2 フォワーディング

7.1 標準のレイヤ2フォワーディング

受信フレームの宛先インタフェースアドレスがレイヤ 3 MAC アドレスと一致しない場合、標準のレイヤ 2 フォワーディングはレイヤ 2 インタフェースを介してフレームを転送します。

装置はフレームの宛先 MAC アドレスを使用して、MAC アドレステーブルで一致を検索します。

- 一致が見つかった場合、装置は一致するエントリで送信インタフェースからフレームを転送します。
- 一致が見つからない場合、装置はフレームをフレームの VLAN 内のすべてのインタフェースにフラッディングします。

標準のレイヤ 2 フォワーディングはデフォルトで有効になっています。

7.2 標準のレイヤ2フォワーディングの表示と維持

すべての view で **display** コマンドを実行し、user view で **reset** コマンドを実行できます。

操作	コマンド
レイヤ2フォワーディング統計情報を表示する	**display mac-forwarding statistics** [**interface** *interface-type interface-number*]
レイヤ2フォワーディング統計情報を削除する	**reset mac-forwarding statistics**

7.3 高速レイヤ2フォワーディング

高速レイヤ 2 フォワーディングは、高速キャッシュとフローベースのテクノロジを使用してパケット転送の効率を向上させます。以下の項目を使用してフローを識別します。

- 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
- プロトコル番号
- 入力インタフェース
- 出力インタフェース
- Vlan ID

高速レイヤ 2 フォワーディングは、フローの最初のパケットの転送情報を取得することで、高速キャッシュにエントリを作成します。フローの後続のパケットは、エントリに基づいて転送されます。

高速レイヤ 2 フォワーディングはデフォルトで有効になっています。

7.4 高速のレイヤ2フォワーディングの表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
IPv 4 高速フォワーディングエントリを表示する	**display mac-forwarding cache ip** [*ip-address*]
フラグメントのIPv 4 高速フォワーディングエントリを表示する	**display mac-forwarding cache ip fragment** [*ip-address*]

目次

このセクションのページは**5-x-x** です。

8章 ARP 8-1
8.1 概要 8-1
8.1.1 ARPメッセージフォーマット 8-1
8.1.2 ARP動作メカニズム 8-2
8.1.3 ARPテーブル 8-3
8.2 スタティックARPエントリの設定 8-4
8.3 インタフェースで学習できるARPエントリの最大数の設定 8-4
8.4 ダイナミックARPエントリのエージングタイマの設定 8-5
8.5 ARPエントリチェックの有効化 8-5
8.6 ARPとインタフェースアドレスエントリ間のMAC整合性チェックの有効化 8-5
8.7 ARPロギング機能の有効化 8-6
8.8 ARPの表示と維持 8-6

8章 ARP

8.1 概要

ARP（Address Resolution Protocol）は、IP アドレスを基に MAC アドレス（物理アドレス）を調べる仕組みのことです。

8.1.1 ARP メッセージフォーマット

ARP は ARP 要求/応答メッセージの 2 つのメッセージタイプがあります。図 8-1に ARP 要求/応答メッセージのフォーマットを示します。図の数字はフィールド長を示します。

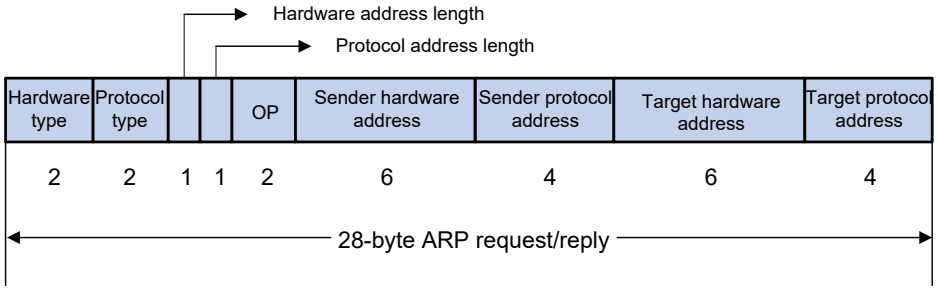


図 8-1 ARP メッセージフォーマット

- **Hardware type**– このフィールドはハードウェアアドレスタイプを指定します。1 は Ethernet を表します。
- **Protocol type**– このフィールドはマッピングされるプロトコルアドレスのタイプを指定します。16 進数で 0x0800 は IP を表します。
- **Hardware address length**、**protocol address length**– ハードウェアアドレスの長さと、プロトコルアドレスの長さをバイト単位で指定します。イーサネットアドレスに関して、Hardware address length の値は 6 です。IPv4 アドレスに関しては、protocol address length の値は 4 です。
- **OP**– このフィールド（Operation code）は ARP メッセージのタイプを指定します。1 は ARP 要求、2 は ARP 応答を表します。
- **Sender hardware address**– このフィールドはメッセージを送信する装置のハードウェアアドレスを指定します。
- **Sender protocol address**– このフィールドはメッセージを送信する装置のプロトコルアドレスを指定します。
- **Target hardware address**– このフィールドはメッセージが送られる装置のハードウェアアドレスを指定します。
- **Target protocol address**– このフィールドはメッセージが送られる装置のプロトコルアドレスを指定します。

8.1.2 ARP 動作メカニズム

図 8-2に示すように、Host A と Host B は同一サブネットにあります。Host A は Host B に以下のようにパケットを送信します。

1) Host A は Host B の ARP エントリが ARP テーブルにあるか検索します。もし ARP エントリがある場合、Host A は、ARP エントリの MAC アドレスを使用します。そしてデータリンクレイヤのフレームに IP パケットをカプセル化し、Host B にフレームを送信します。
2) もし Host B の ARP エントリがない場合、Host A はパケットをバッファし、ARP 要求をブロードキャストします。ARP リクエストのデータの内容は以下の情報が含まれます。
   - **送信元 IP アドレスと送信元 MAC アドレス** – Host A の IP アドレスと MAC アドレス
   - **宛先 IP アドレス** – Host B の IP アドレス
   - **宛先 MAC アドレス** – 値がすべて 0 の MAC アドレス

   サブネットのすべてのホストはブロードキャストリクエストを受信することができますが、パケットを処理するホスト（Host B）のみが ARP 要求を処理します。
3) Host B は自身の IP アドレスと ARP リクエストの宛先 IP アドレスを比較し、同一の場合、以下の処理を行います。
   a) 送信元IPアドレスと送信元MACアドレスをARPテーブルに追加します。
   b) ARP応答に自身のMACアドレスを挿入します。
   c) Host AにARP応答をユニキャストで送信します。
4) ARP 応答を受信した後、Host A は以下の処理を行います。
   a) Host BのMACアドレスをARPテーブルに追加します。
   b) 以降、送信するパケットにHost BのMACアドレスを追加し、Host Bにパケットを送信します。

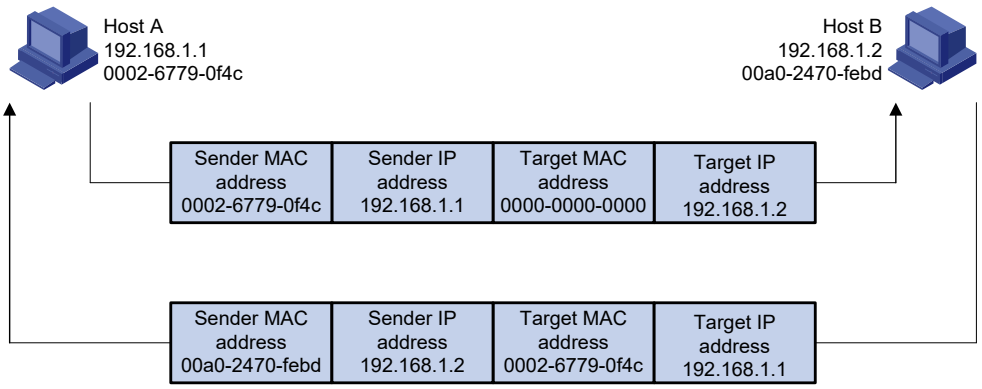


図 8-2 ARP アドレス解決プロセス

Host A と Host B が異なるサブネットにある場合、Host A は Host B に以下のようにパケットを送信します。

1) Host A は、宛先 IP アドレスをゲートウェイの IP アドレスにした ARP 要求をブロードキャストします。
2) ゲートウェイは、ARP 応答を行い、自身の MAC アドレスを Host A に送信します。

3) Host A はゲートウェイの MAC アドレスをパケットに挿入し、ゲートウェイにパケットを送信します。
4) ゲートウェイが Host B の ARP エントリがある場合、Host B にパケットを直接転送します。もし Host B の ARP エントリがない場合、宛先 IP アドレスを Host B の IP アドレスとして ARP 要求をブロードキャストします。
5) ゲートウェイが Host B の MAC アドレスを取得した後、Host B にパケットを送信します。

8.1.3 ARP テーブル

ARP テーブルはダイナミック、スタティックの ARP エントリがあります。

I. ダイナミック ARP エントリ

ダイナミックエントリは ARP によって自動的に作成、アップデートされます。エージングタイマが終了したとき、あるいは出力インタフェースがダウンしたとき、ダイナミックエントリは削除されます。ダイナミック ARP エントリはスタティック ARP エントリによって上書きされます。

II. スタティック ARP エントリ

スタティック ARP エントリは手動で設定され、維持します。スタティック ARP エントリはエージングせず、ダイナミック ARP エントリによって上書きされることもありません。

スタティック ARP エントリを使用することにより、通信のセキュリティを強化できます。スタティック ARP エントリで IP アドレスと MAC アドレスをマッピングすることにより、スタティック ARP エントリで指定された IP アドレスと MAC アドレスのマッピングが、攻撃パケットで変更されることはありません。

装置は以下のタイプのスタティック ARP エントリをサポートします。

- **ロングスタティック ARP エントリ**：IP アドレス、MAC アドレス、VLAN インタフェース、出力インタフェースから構成されます。パケットを転送するのに直接使用されます。
- **ショートスタティック ARP エントリ**：IP アドレス、MAC アドレスのみで構成されます。

  装置はターゲット IP アドレスがショートエントリの IP アドレスである ARP 要求を送信します。受信した ARP 応答の送信元 IP アドレスと MAC アドレスがショートスタティック ARP エントリと一致した場合、装置は以下の処理を行います。

  - ARP エントリを受信したインタフェースはショートスタティック ARP エントリを追加します。
  - IP パケットを転送するため、解決したショートスタティック ARP エントリを使用します。

固定の IP アドレス-MAC アドレスマッピングを使用してホストと通信する場合、装置は、ショートスタティック ARP エントリを設定します。固定の IP アドレス-MAC アドレスマッピングを使用して、指定した VLAN の指定したインタフェースを通してホストと通信する場合、装置はロングスタティック ARP エントリを設定します。

8.2 スタティックARPエントリの設定

スタティック ARP エントリは、装置が正常に動作するときに、適用されます。

解決済みのショートスタティック ARP エントリは、未解決となります。たとえば、解決した出力インタフェースがダウンあるいは対応する VLAN、VLAN インタフェースが削除したとき、解決済みのショートスタティック ARP エントリは、未解決となります。

未解決のロングスタティック ARP エントリはパケットの転送に使用することができません。ロングスタティック ARP エントリは以下の状態にある場合、未解決となります。

- 対応する VLAN インタフェースもしくは出力インタフェースがダウンしています。
- エントリの IP アドレスがローカル IP アドレスと衝突しています。
- インタフェースが同一サブネットの ARP エントリの IP アドレスを持っていません。

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。

以下にスタティック ARP エントリの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． スタティック ARP エントリを設定する	• ロングスタティックARPエントリを設定する：**arp static** *ip-address mac-address* [*vlan-id interface-type interface-number*] • ショートスタティックARPエントリを設定する：**arp static** *ip-address mac-address*	デフォルト：設定なし

8.3 インタフェースで学習できるARPエントリの最大数の設定

インタフェースは動的に ARP エントリを学習します。多すぎる ARP エントリを保持しないように、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。

ダイナミック ARP エントリの最大数をレイヤ 2 インタフェースと VLAN インタフェースの両方で設定することができます。レイヤ 2 インタフェースはダイナミック ARP エントリが最大値に到達しないときのみ ARP エントリを学習します。

以下にインタフェースで学習できるダイナミック ARP エントリの最大数の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． interface view に移行する	**interface** *interface-type interface-number*	―

操作	コマンド	補足
3． ダイナミック ARP エントリの最大数を設定する	**arp max-learning-num** *max-number*	デフォルト：272 *number* 引数に0を設定した場合、ダイナミックARPエントリの学習を行いません。

8.4 ダイナミックARPエントリのエージングタイマの設定

ARP テーブル上の各ダイナミック ARP エントリは有効期限があります。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 エントリが使用される度に、エージングタイマはアップデートされます。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。

以下にダイナミック ARP エントリのエージングタイマの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． ダイナミック ARP エントリのエージングタイムを設定する	**arp timer aging** { *aging-minutes* | **second** *aging-seconds* }	デフォルト：20分

8.5 ARPエントリチェックの有効化

ダイナミック ARP エントリチェック機能は、装置でマルチキャスト MAC アドレスを含むダイナミック ARP エントリのサポートを無効にします。装置は送信元がマルチキャスト MAC アドレスであるダイナミック ARP エントリを学習できません。マルチキャスト MAC アドレスを含むスタティック ARP エントリを手動で学習させることもできません。

ARP エントリチェックを無効にした場合、装置はマルチキャスト MAC アドレスの ARP エントリを学習することができます。手動でマルチキャスト MAC アドレスを含むスタティック ARP エントリを追加することができます。

以下に ARP エントリチェック機能の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． ARP エントリチェック機能を有効にする	**arp check enable**	デフォルト：有効

8.6 ARPとインタフェースアドレスエントリ間のMAC整合性チェックの有効化

不安定なネットワークでは、ユーザからのパケットの受信インタフェースが変わることがあります。MAC アドレスエントリのインタフェースはすぐに更新できますが、ARP エントリのインタフェースは更新できません。この場合、ARP エントリに一致するパケットは誤ったインタフェースから送信されます。この問題を解決するには、ユーザの ARP と

インタフェースアドレスエントリ間の MAC 整合性を定期的にチェックします。インタフェースが同じでない場合、ARP は ARP エントリの VLAN で ARP 要求を送信し、インタフェースを受信する ARP 応答でエントリを更新します。

MAC アドレスエントリを表示するには、**display mac-address** を使用します。このコマンドの詳細は、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*5 ネットワーク接続*”の”*1 章 MAC アドレステーブル*”を参照してください。

以下に ARP とインタフェースアドレスエントリ間の MAC 整合性チェックの有効化を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. ARP とインタフェースアドレスエントリ間の MAC 整合性チェックを有効にする	**arp mac-interface-consistency check enable**	デフォルト：無効

8.7 ARPロギング機能の有効化

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 アドレスでありません。
- ARP 応答の送信元 IP アドレスが受信インタフェースの IP と衝突しています。

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、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“3 *システム管理*”の”*5 章 Information Center*”を参照してください。

以下に ARP ロギング機能の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. ARP ロギング機能を有効にする	**arp check log enable**	デフォルト：無効

8.8 ARPの表示と維持

すべての view で **display** コマンドを実行でき、user view で **reset** コマンドが実行できます。

操作	コマンド
ARPエントリを表示する	**display arp** [[**all** | **dynamic** | **static**] | **vlan** *vlan-id* | **interface** *interface-type interface-number*] [**count** | **verbose**]
指定したIPアドレスのARPエントリを表示する	**display arp** *ip-address* [**verbose**]

操作	コマンド
ダイナミックARPエントリのエージングタイムを表示する	**display arp timer aging**
ARPテーブルからARPエントリを削除する	**reset arp** { **all** | **dynamic** | **interface** *interface-type interface-number* | **static** }

注意：

reset arp コマンドは、ARP テーブルから既存の ARP エントリを削除します。外部ユーザが LAN ユーザと迅速に通信できなくなる可能性があります。

目次

このセクションのページは**5-x-x** です。

9章 Gratuitous ARP 9-1
9.1 概要 9-1
9.1.1 Gratuitous ARPパケットの学習 9-1
9.1.2 Gratuitous ARPパケットの送信間隔の設定 9-1
9.2 設定手順 9-2
9.3 IP重複通知の有効化 9-2

9章 Gratuitous ARP

9.1 概要

GARP（Gratuitous ARP）は ARP パケットの 1 つであり、装置は以下の目的で Gratuitous ARP パケットを送信します。

- 他のネットワーク装置と、IP アドレスが重複していないかを確認できます。もし IP アドレスが既に使われていた場合、ARP 応答によって重複していることが通知されます。
- 他のネットワーク装置に MAC アドレス情報を通知して、ARP エントリを更新させます。

Gratuitous ARP パケットにおいて送信元 IP アドレスと宛先 IP アドレスは共に送信する装置の IP アドレスです。

9.1.1 Gratuitous ARP パケットの学習

Gratuitous ARP パケットの学習機能を有効にした場合、Gratuitous ARP パケットを受信すると、受信した Gratuitous ARP パケットの送信元 IP アドレスと MAC アドレスを使用して ARP エントリを作成あるいは更新します。

この機能を無効にした場合、ARP エントリの更新は行いますが、新しい ARP エントリは追加しません。ARP エントリは受信した Gratuitous ARP パケットをもとに ARP エントリを作成しないで、ARP テーブルを節約します。

9.1.2 Gratuitous ARP パケットの送信間隔の設定

定期的に Gratuitous ARP パケットを送信することにより、下流の装置の対応する ARP エントリあるいは MAC アドレスエントリを定期的に更新します。

この機能は以下の機能を実現します。

- ゲートウェイスプーフィングの防御

攻撃者がネットワーク上のホストに捏造した Gratuitous ARP パケットを送信するためにゲートウェイアドレスを使用したとき、ゲートウェイスプーフィングが発生します。ホストからゲートウェイ宛のトラフィックは代わりに攻撃者に送信されます。その結果ホストは外部のネットワークにアクセスできません。

ゲートウェイスプーフィングの攻撃を防ぐため、ゲートウェイが Gratuitous ARP パケットを送信する間隔を設定することができます。Gratuitous ARP パケットは、ホストが正しいゲートウェイの情報を学習できるように、ゲートウェイのプライマリ IP アドレスと手動で設定されたセカンダリ IP アドレスが含まれます。

- ARP エントリのエージアウトの防止

ネットワークのトラフィックが非常に多い、あるいはホストの CPU の使用率が高い場合、受信した ARP パケットは廃棄、あるいはすぐに処理されません。そのため、受信ホストのダイナミック ARP エントリはエージアウトします。ホストと対応する装置間のトラフィックは、ホストが ARP エントリを再作成するまで中断されます。

この問題を防ぐため、定期的に Gratuitous ARP パケットを送信するゲートウェイを有効にします。受信ホストはすぐに ARP エントリをアップデートすることができます。

9.2 設定手順

以下に Gratuitous ARP の設定を行うため、制限とガイドラインに従ってください。

- 最大 1024 のインタフェースで Gratuitous ARP パケットの送信間隔を設定できます。
- Gratuitous ARP パケットの送信間隔の設定は、以下の状態の場合に適用されます。
  - インタフェースのリンク状態がアップしています。
  - IP アドレスが割り当てられています。
- Gratuitous ARP パケットの送信間隔を変更する場合、設定は次の送信間隔から適用されます。
- 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る可能性があります。
  - 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
  - 複数のインタフェースで有効にされ、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、Gratuitous ARP パケットの送信間隔は設定された送信間隔よりも短くなります。

以下に Gratuitous ARP の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Gratuitous ARP パケット学習機能を有効にする	**gratuitous-arp-learning enable**	デフォルト：有効
3. 他のネットワークセグメントから ARP 要求を受信した際、Gratuitous ARP パケットの送信を有効にする	**gratuitous-arp-sending enable**	デフォルト：無効
4. interface view に移行する	**interface** *interface-type interface-number*	―
5. Gratuitous ARP パケットの定期的な送信を有効化し、送信間隔を設定する	**arp send-gratuitous-arp** [**interval** *interval*]	デフォルト：無効

9.3 IP重複通知の有効化

デフォルトで、受信装置が Gratuitous ARP パケットの送信者の IP アドレスを使用する場合、受信装置は gratuitous ARP 要求を送信します。重複に関する ARP 応答を受信したのち、エラーメッセージを表示します。

このコマンドを使用することで、Gratuitous ARP 応答あるいは要求を送信することなく、装置でエラーメッセージを表示することができます。

以下に IP 重複通知の有効化の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. IP 重複通知を有効にする	**arp ip-conflict log prompt**	デフォルト：無効

目次

このセクションのページは**5-x-x** です。

10章 Proxy ARP 10-1
10.1 一般的なProxy ARPの有効化 10-1
10.2 ローカルProxy ARPの有効化 10-1
10.3 Proxy ARPの表示と維持 10-1
10.4 一般的なProxy ARP設定例 10-2
10.4.1 ネットワーク要件 10-2
10.4.2 設定手順 10-2
10.4.3 設定の確認 10-3

10章 Proxy ARP

Proxy ARP が有効な装置で、別のネットワークの IP アドレスの ARP リクエストに応答します。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**－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**－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。

10.1 一般的なProxy ARPの有効化

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． interface view に移行する	**interface** *interface-type interface-number*	一般的なProxy ARPは、VLAN インタフェースでのみ使用できます。
3． 一般的な Proxy ARP を有効にする	**proxy-arp enable**	デフォルト：無効

10.2 ローカルProxy ARPの有効化

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． interface view に移行する	**interface** *interface-type interface-number*	ローカルProxy ARPは、VLAN インタフェースでのみ使用できます。
3． ローカル Proxy ARP を有効にする	**local-proxy-arp enable** [**ip-range** *startIP* **to** *endIP*]	デフォルト：無効

10.3 Proxy ARPの表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
一般的なProxy ARPの状態を表示する	**display proxy-arp** [**interface** *interface-type interface-number*]
ローカルProxy ARPの状態を表示する	**display local-proxy-arp** [**interface** *interface-type interface-number*]

10.4 一般的なProxy ARP設定例

10.4.1 ネットワーク要件

図 10-1に示すように、Client 1 と Client 2 は同一 IP プレフィックスとマスクを持ちますが、Switch によって異なるサブネットに分離されています。Client 1 は VLAN 10、Client 2 は VLAN 20 に所属しています。Client 1 と Client 2 のデフォルトゲートウェイは設定されていません。

2 つの Client で通信ができるように AC で一般的な Proxy ARP を設定します。

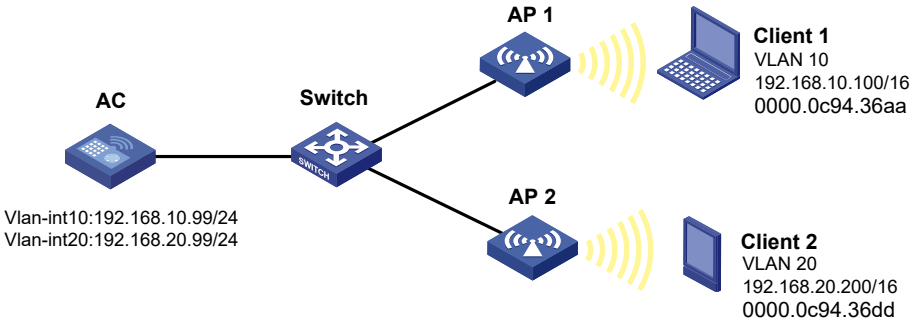


図 10-1 ネットワーク図

10.4.2 設定手順

VLAN 2 を作成します。

Create VLAN 10 and VLAN 20.

```
<AC> system-view
[AC] vlan 10
[AC-vlan10] quit
[AC] vlan 20
[AC-vlan20] quit
```

VLAN インタフェース 10 の IP アドレスを設定します。

```
[AC] interface vlan-interface 10
[AC-Vlan-interface10] ip address 192.168.10.99 255.255.255.0
```

VLAN インタフェース 10 で一般的な Proxy ARP を有効にします。

```
[AC-Vlan-interface10] proxy-arp enable
[AC-Vlan-interface10] quit
```

VLAN インタフェース 220 の IP アドレスを設定します。

```
[AC] interface vlan-interface 20
```

```
[AC-Vlan-interface20] ip address 192.168.20.99 255.255.255.0
```

VLAN インタフェース 20 で一般的な Proxy ARP を有効にします。

```
[AC-Vlan-interface20] proxy-arp enable
```

10.4.3 設定の確認

クライアント 1 とクライアント 2 で互いに ping ができるかどうか確認してください。

目次

このセクションのページは**5-x-x** です。

11章 IPアドレス 11-1
11.1 概要 11-1
11.1.1 IPアドレスクラス 11-1
11.1.2 特別なIPアドレス 11-2
11.1.3 サブネットとマスク 11-2
11.2 インタフェースへのIPアドレスの割り当て 11-3
11.2.1 設定ガイドライン 11-3
11.2.2 設定手順 11-4
11.3 IPアドレスの表示と維持 11-4

11章 IP アドレス

この章では IP アドレスの基本とインタフェースにアドレスを手動で割り当てる方法について記載します。ダイナミックに IP アドレスを割り当てる方法（BOOTP、DHCP）や PPP については記載しません。

11.1 概要

IP アドレスは、IPv4 ネットワークの各ホストを識別するため、32 ビットアドレスを使用します。たとえば、2 進数では 00001010000000010000000100000001 となります。IP アドレスをわかりやすくするために、32 ビットの整数値を 8 ビットずつ 4 つに分割し、ドット付きの 10 進数で IP アドレスを表します。先ほどの 32 ビットの 2 進数は、10.1.1.1 となります。

11.1.1 IP アドレスクラス

各 IP アドレスは以下のセクションに分類されます。

- **Net ID** – ネットワークを定義します。先頭の数ビットはネットワークを定義するアドレスです。クラスフィールドあるいはクラスビットで、IP アドレスのクラスを識別します。
- **Host ID** – ホストを定義します。

図 11-1に示すように、IP アドレスは 5 つのクラスに分類されます。IP アドレスがどのクラスに所属するのかは、下図の青い部分のアドレスによって決まります。最初の 3 つのクラスは一般的に使用されます。

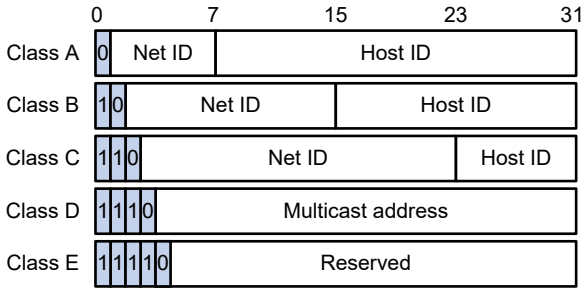


図 11-1 IP アドレスクラス

表 11-1 IP アドレスクラスと範囲

クラス	アドレス範囲	補足
A	0.0.0.0 ～ 127.255.255.255	0.0.0.0はブートストラップ時に一時的にホストが使用するため、有効な宛先アドレスにはなりません。127からはじまるアドレスはループバックテストのために予約されているため、このアドレス宛てのパケットは、入力パケットとしてローカルで処理されます。
B	128.0.0.0 ～ 191.255.255.255	ー
C	192.0.0.0 ～ 223.255.255.255	ー
D	224.0.0.0 ～ 239.255.255.255	マルチキャストアドレス
E	240.0.0.0 ～ 255.255.255.255	予約済みです。255.255.255.255はブロードキャストアドレスです。

11.1.2 特別な IP アドレス

以下の IP アドレスは特別な用途で使用されるため、ホストの IP アドレスに設定することができません。

- **Net ID がすべて 0 の IP アドレス** ー ローカルネットワークのホストを識別します。たとえば、IP アドレス 0.0.0.16 はローカルネットワークの Host ID が 16 のホストを示します
- **Host ID がすべて 0 の IP アドレス** ー ネットワークアドレスを示します。
- **Host ID がすべて 1 の IP アドレス** ー ディレクテッドブロードキャストを示します。たとえば、宛先アドレスが 192.168.1.255 のパケットは、ネットワーク 192.168.1.0 に属するすべてのホストにブロードキャストされます。

11.1.3 サブネットとマスク

サブネットは、Host ID のいくつかのビットを使用して Subnet ID を作成し、ネットワークをサブネットと呼ばれるより小さいネットワークに分割します。

Host ID と、Net ID と Subnet ID の組み合わせの境界を識別するために、サブネットマスクが使用されます。

各サブネットマスクは IP アドレスに関連する 32 ビットで構成されています。サブネットマスクは 1 と 0 で構成されています。1 が連続している部分で Net ID と Subnet ID の組み合わせを識別し、0 が連続している部分で Host ID を識別します。

サブネットとなるまえに、クラス A、B、C ネットワークは、それぞれ 255.0.0.0、255.255.0.0、255.255.255.0 のデフォルトマスク（ナチュラルマスクと呼ばれます）を使用します。

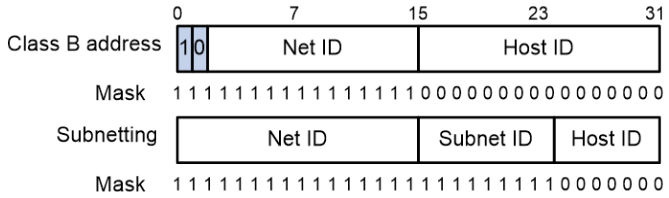


図 11-2 クラス B ネットワークのサブネット

サブネットを使用すると、ホストに割り当てるためのアドレスが減少します。従って、サブネットを使用することは、ある程度少ないホストを適用することになります。

たとえばクラス B ネットワークでは、1022 のサブネットを持つネットワークよりも、512 のサブネットを持つネットワークのほうが、多くのホストを収容することができます。

- **サブネットがないネットワーク** － 65534 個（$2^{16} - 2$）のホストを収容できます。（Host ID がすべて 1 のブロードキャストアドレスと、Host ID すべて 0 のネットワークアドレスを差し引きます。）
- **サブネットネットワーク** － Host-ID の最初の 9 ビットをサブネットに割り当てると、512 個（2^9）のサブネットができます。Host-ID に使用できるのは残りの 7 ビットだけとなり、各サブネットに 126 個（$2^7 - 2$）のホストを収容できます。従って、全部で 64512 個（512 × 126）のホストを収容できます。

11.2 インタフェースへのIPアドレスの割り当て

インタフェースは他のホストと通信するために IP アドレスが必要です。手動でインタフェースに IP アドレスを割り当てるか、BOOTP あるいは DHCP、PPP アドレスネゴシエーションによって IP アドレスを取得することができます。IP アドレスを取得する方法を変更した場合、新しい IP アドレスは古い IP アドレスに上書きします。

インタフェースは 1 つのプライマリアドレスと複数のセカンダリアドレスを持つことができます。

通常、インタフェースのプライマリアドレスを設定する必要があります。もしインタフェースが複数のサブネットに接続する場合、サブネットが、インタフェースを通して互いに通信できるようにインタフェースにプライマリとセカンダリ IP アドレスを設定します。

11.2.1 設定ガイドライン

インタフェースに IP アドレスを割り当てるとき以下のガイドラインに従ってください。

- インタフェースは 1 つのプライマリ IP アドレスのみを設定することができます。新しく IP アドレスを設定した場合、古いアドレスが上書きされます。
- BOOTP、DHCP により IP アドレスを取得する設定をしているインタフェースでは、セカンダリ IP アドレスを設定することはできません。
- インタフェースに設定するプライマリとセカンダリ IP アドレスは同じネットワークセグメントに存在することができます。しかし、装置上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にしなければなりません。

11.2.2 設定手順

以下にインタフェースへの IP アドレスの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． interface view に移行する	**interface** *interface-type interface-number*	―
3． インタフェースに IP アドレスを設定する	**ip address** *ip-address* { *mask* | *mask-length* } [**sub**]	デフォルト：設定なし

11.3 IPアドレスの表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
指定した、またはすべてのレイヤ3インタフェースの設定と統計情報を表示する	**display ip interface** [*interface-type* [*interface-number*]]
指定した、またはすべてのレイヤ3インタフェースの概要情報を表示する	**display ip interface** [*interface-type* [*interface-number*]] **brief**

目次

このセクションのページは**5-x-x** です。

12章 DHCPの概要 12-1
12.1 DHCPアドレスの割り当て 12-1
12.1.1 割り当てメカニズム 12-1
12.1.2 IPアドレスの割り当てプロセス 12-2
12.1.3 IPアドレスのリース延長 12-3
12.2 DHCPメッセージフォーマット 12-3
12.3 DHCPオプション 12-4
12.3.1 一般的なDHCPオプション 12-4
12.3.2 自己定義DHCPオプション 12-5
12.4 プロトコルと標準 12-8

12章 DHCP の概要

DHCP（Dynamic Host Configuration Protocol）は、ネットワークにおいて通信用の基本的な設定を自動的に行う機能を提供します。

図 12-1に示すように、一般的な DHCP の構成は、同一サブネットに DHCP サーバとクライアントがあります。

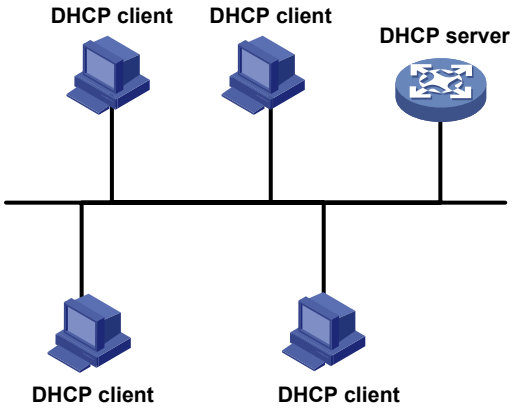


図 12-1 一般的な DHCP の構成

12.1 DHCPアドレスの割り当て

12.1.1 割り当てメカニズム

DHCP は以下の IP アドレスの割り当てメカニズムをサポートします。

- **手動割り当て** － ネットワーク管理者が WWW サーバなどのクライアントに IP アドレスを割り当てます。DHCP 割り当てられたアドレスをクライアントに伝送します。
- **自動割り当て** － DHCP がクライアントに永続的に使用可能な IP アドレスを割り当てます。
- **動的（ダイナミック）割り当て** － DHCP は、クライアントに一定期間（リース期間）使用可能な IP アドレスを割り当てます。ほとんどのクライアントがこの方法でアドレスを取得します。

12.1.2 IP アドレスの割り当てプロセス

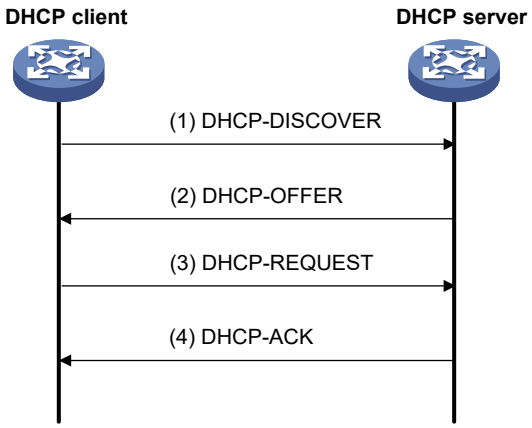


図 12-2 IP アドレスの割り当てプロセス

図 12-2に示すように DHCP サーバは以下の手順で DHCP クライアントに IP アドレスを割り当てます。

1) クライアントは DHCP-DISCOVER メッセージをブロードキャストし、DHCP サーバを特定します。
2) DHCP サーバは、DHCP-OFFER メッセージの中で IP アドレスなどの設定パラメータをクライアントに提供します。DHCP-OFFER の送信モードは DHCP-DISCOVER メッセージのフラグフィールドによって決定します。関連情報は、本章の *"DHCP メッセージフォーマット"* を参照してください。
3) クライアントが複数の DHCP-OFFER を受信した場合、クライアントは最初に受け取った DHCP-OFFER を受け入れ、正式に IP アドレスを要求するために DHCP-REQUEST メッセージをブロードキャストで送信します。(他の DHCP サーバから提供された IP アドレスは他のクライアントに提供することができます。)
4) すべての DHCP サーバが DHCP-REQUEST メッセージを受信します。しかし、クライアントによって選択されたサーバのみ以下の動作を行います。
   - □ サーバは、クライアントに IP アドレスが割り当てられていることを確認して DHCP-ACK メッセージを返します。
   - □ IP アドレスの割り当てを拒否して DHCP-NAK ユニキャストメッセージを返します。

クライアントは DHCP-ACK メッセージを受信した後、クライアントは割り当てられた IP アドレスを使用する前に、詳細を確認します。

- 割り当てられた IP アドレスが使用中であるかどうかを確認します。Gratuitous ARP パケットをブロードキャストで送信することによって、サーバから割り当てられた IP アドレスが使用中かどうかを調べます。一定時間内に応答がなければ、クライアントはこの IP アドレスを使用することができます。
- 割り当てられた IP アドレスがクライアントで使用している IP アドレスと同一サブネットにないかどうかを確認します。

そうでない場合、クライアントは DHCP-DECLINE メッセージをサーバに送信し、再度 IP アドレスを要求します。

12.1.3 IP アドレスのリース延長

DHCP サーバがクライアントに動的に割り当てた IP アドレスには、リース期間があります。リース期間が経過すると、その IP アドレスは DHCP から返還を要求（回収）されます。クライアントが再び IP アドレスを使用する場合は、リース期間を延長する必要があります。

リース期間の半分が経過したところで、DHCP クライアントはリース期間を延長するために DHCP サーバに DHCP-REQUEST ユニキャストメッセージを送信します。IP アドレスの使用状況に依存して、DHCP サーバは以下のメッセージの 1 つを返します。

- クライアントのリース期間が延長されていることを確認する DHCP-ACK ユニキャストを返します。
- 要求を拒否する DHCP-NAK ユニキャストメッセージを返します。

クライアントが応答を受信しない場合、クライアントはリース期間が 7/8 経過したところで、リースを延長するために別の DHCP-REQUEST メッセージをブロードキャストします。IP アドレスの使用状況に応じて、DHCP サーバはリース期間を延長されたことを示す DHCP-ACK ユニキャストあるいは DHCP-NAK ユニキャストメッセージを返します。

12.2 DHCPメッセージフォーマット

図 12-3に DHCP メッセージフォーマットを示します。DHCP フィールドのいくつかを異なる方法で使用します。カッコ内の数字は、各フィールドのサイズをバイト数で示したものです。

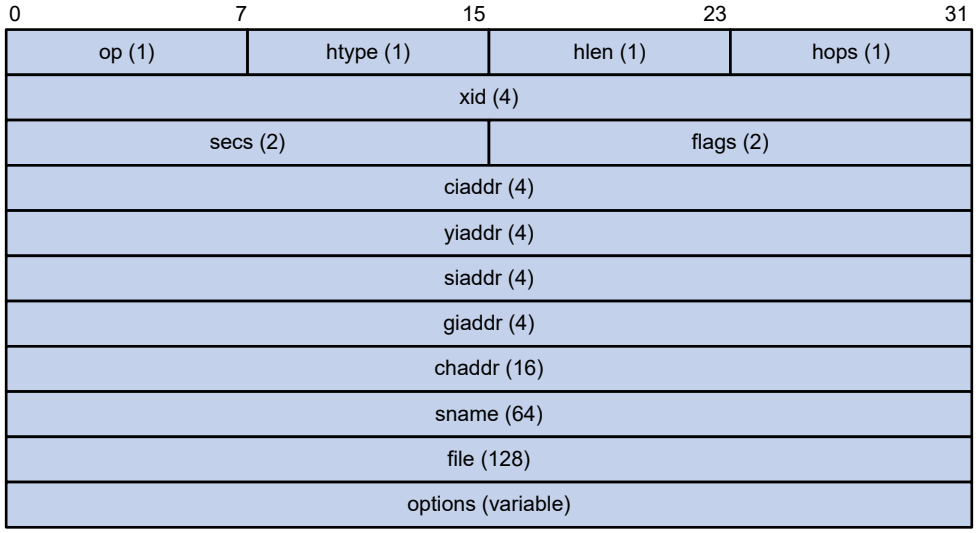


図 12-3 DHCP メッセージフォーマット

- **op**– オプションフィールドに定義されているメッセージタイプです。1 = REQUEST,2 = REPLY
- **htype, hlen**– DHCP クライアントのハードウェアアドレスのタイプと長さです。
- **hops**– 要求メッセージが伝送される（経由する）リレーエージェントの数です。

- **xid**– トランザクション ID で、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した数です。
- **secs**– クライアントがアドレスを取得または更新プロセスを始めてから経過した秒数です。このフィールドは予約されており 0 に設定されています。
- **flags**– 1 ビット目は BROADCAST（B）フラグです。このフラグが 0 に設定されていると、DHCP サーバは応答をユニキャストで返します。このフラグの設定値が 1 のときは、DHCP サーバはブロードキャストで応答を返します。フラグフィールドの残りのビットは、今後の使用のために予約されています。
- **ciaddr**– 有効で使用可能なクライアントの IP アドレスです。そうでなければ 0 に設定されています。（クライアントは、このフィールドを特定の IP アドレスを要求するために使いません。）
- **yiaddr**– DHCP サーバが DHCP クライアントに割り当てる IP アドレスです。
- **siaddr**– サーバの IP アドレスです。クライアントはここから設定パラメータを取得します。
- **giaddr**– 要求メッセージが最初に伝送されたリレーエージェントのゲートウェイ IP アドレスです。
- **chaddr**– クライアントの MAC アドレスです。
- **sname**– サーバのホスト名です。クライアントはここから設定パラメータを取得します。
- **file**– サーバからクライアントに対して定義されたブートファイル名（システムソフトウェアイメージと呼ばれます）、パス情報です。
- **options**– オプションの可変長パラメータです。メッセージタイプ、リース期間、DNS サーバの IP アドレスおよび WINS サーバの IP アドレスなどが含まれます。

12.3 DHCPオプション

DHCP メッセージは、BOOTP（Bootstrap Protocol）と同じメッセージフォーマットを使用しますが、DHCP は動的な IP アドレス割り当て情報と追加の設定情報をクライアントに送信するため、option フィールドを使用します。

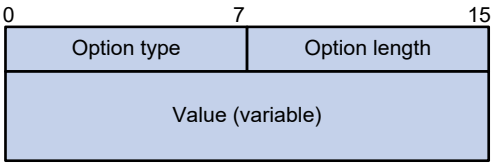


図 12-4 DHCP オプションフォーマット

12.3.1 一般的な DHCP オプション

以下に一般的な DHCP オプションを示します。

- **オプション 3** – ルータのオプションです。ゲートウェイアドレスを指定します。
- **オプション 6** – DNS サーバのオプションです。DNS サーバの IP アドレスを指定します。
- **オプション 33** – スタティックルートオプションです。ルーティングテーブルに追加する必要のあるクラスフルスタティックルート（クラスフルスタティックルートの宛先アドレス）のリストを指定します。クライアントはルーティングテーブルに追加

します。オプション 33 とオプション 121 の両方が存在する場合、オプション 33 は無視されます。

- **オプション 51** – IP アドレスのリースオプションです。
- **オプション 53** – DHCP メッセージタイプのオプションです。DHCP メッセージのタイプを識別します。
- **オプション 55** – パラメータ要求リストのオプションです。DHCP クライアントが、指定の設定パラメータを要求するために使用します。このオプションには、クライアントが要求したパラメータに対応する値が含まれます。
- **オプション 60** – ベンダクラスの識別オプションです。DHCP クライアントがベンダを識別するために使用します。DHCP サーバが、DHCP クライアントを区別し、指定された IP アドレスを割り当てるために使用します。
- **オプション 66** – TFTP サーバ名のオプションです。クライアントに割り当てる TFTP サーバを指定します。
- **オプション 67** – ブートファイル名のオプションです。クライアントに割り当てるブートファイル名を指定します。
- **オプション 121** – クラスレスルートオプションです。クラスレススタティックルート（スタティックルートの宛先ネットワークアドレスがクラスレス）のリストを指定します。クライアントがルーティングテーブルに追加するために要求します。オプション 33 とオプション 121 の両方が存在する場合、オプション 33 は無視されます。
- **オプション 150** – TFTP サーバの IP アドレスのオプションです。クライアントに割り当てる TFTP サーバの IP アドレスを指定します。

DHCP オプションについての詳細は、RFC2132、RFC3442 を参照してください。

12.3.2 自己定義 DHCP オプション

オプション 43、オプション 82、オプション 184 のようなオプションは、RFC2132 で定義されていません。

I. ベンダ指定オプション（オプション 43）

DHCP サーバとクライアントは、ベンダ指定の設定情報を交換するため、オプション 43 を使用します。

DHCP クライアントはオプション 43 を以下の情報を通して取得します。

- ACS の URL、ユーザ名、パスワードを含んだ自動設定パラメータ（ACS パラメータ）です。
- CPE によって DHCP サーバから取得され、ベンダ固有の設定とパラメータを選択するために ACS に送信されるサービスプロバイダ識別子です。
- PXE（Preboot Execution Environment）サーバからブートファイルあるいは、他のコントロール情報を取得するために使用する PXE サーバアドレスです。
- ブートファイルまたは他の制御情報を AC から取得するために AP によって使用される、AC のアドレスです。

1) オプション 43 のフォーマット

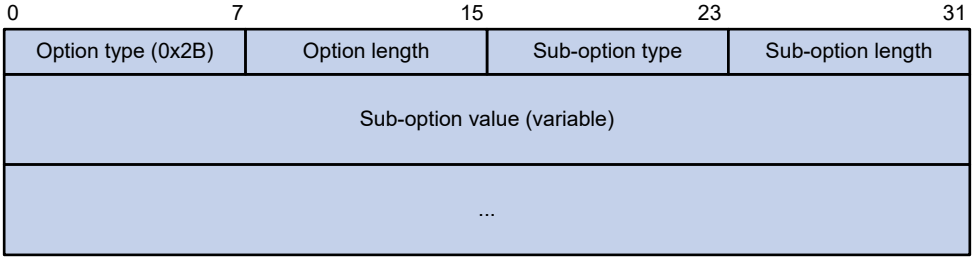


図 12-5 オプション 43 のフォーマット

図 12-5に示すように、ネットワーク設定パラメータは、異なるオプション 43 のサブオプションで送信されます。

- **サブオプションタイプ** ー サブオプションのタイプです。フィールド値は、0x01（ACS パラメータのサブオプション）、0x02（サービスプロバイダ識別子のサブオプション）または 0x80（PXE サーバアドレスのサブオプション）です。
- **サブオプション長** ー サブオプションタイプとサブオプション長フィールドを除くサブオプションの長さです。
- **サブオプション値** ー サブオプションによって値のフォーマットは変更します。

2)　サブオプションフィールドのフォーマット

- **ACS パラメータのサブオプションフィールド**– 図 12-6に示すように、ACS パラメータのサブオプションのフィールドは、ACS の URL、ユーザ名、パスワードです。それぞれの間はスペース（0x20）で分離されます。

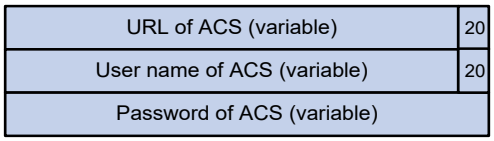


図 12-6 サブオプションフィールドのフォーマット

- **サービスプロバイダ識別子のサブオプションフィールド** ー サービスプロバイダ識別子のサブオプションフィールドは、サービスプロバイダ識別子を含みます。
- **PXE サーバアドレスのサブオプションフィールド** ー 図 12-7に示すように、PXE server type が 0 で、Server number がサブオプションに含まれる PXE サーバの数を示し、Server IP addresses が PXE サーバの IP アドレスを示します。

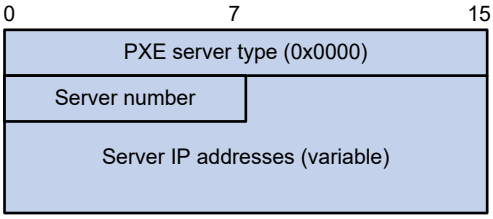


図 12-7 PXE サーバアドレスのサブオプションフィールド

II. リレーエージェントオプション（オプション 82）

オプション 82 は、オプションフィールドにおけるリレーエージェントのオプションです。DHCP クライアントの位置情報を記録します。DHCP リレーエージェントがクライアントの要求を受信すると、要求メッセージにオプション 82 を追加してサーバに送信します。

管理者は DHCP クライアントの位置を特定して、セキュリティ管理とアカウンティングを実行することができます。DHCP サーバは、クライアントの個別の設定ポリシーを提供するためにオプション 82 を使用します。

オプション 82 には、最大 255 のサブオプションがあります。少なくとも 1 つのサブオプションを定義する必要があります。オプション 82 は、サブオプション 1（Circuit ID）とサブオプション 2（Remote ID）の 2 つのサブオプションをサポートしています。オプション 82 は標準の定義がありません。ベンダによってパディングフォーマットは変わります。

- Circuit ID は以下に示すパディングフォーマットを持ちます。
  - **文字列パディングフォーマット** – ユーザが定義した文字列を含みます。
  - **標準（Normal）パディングフォーマット** – VLAN ID、クライアントの要求を受信したインタフェースのインタフェース番号を含みます。
  - **詳細（Verbose）パディングフォーマット** – ユーザ定義のアクセスノード識別子、VLAN ID、クライアントの要求を受信したインタフェースの番号、インタフェースのタイプを含みます。
- Remote ID は以下に示すパディングフォーマットを持ちます。
  - **文字列パディングフォーマット** – ユーザが定義した文字列を含みます。
  - **標準（Normal）パディングフォーマット** – DHCP リレーエージェントのインタフェースの要求を受信した DHCP snooping の MAC アドレスを含みます。
  - **システム名パディングフォーマット** – 装置のシステム名を含みます。装置のシステム名を設定する場合、system view で **sysname** コマンドを使用します。

III. オプション 184

オプション 184 は予約されているオプションです。パラメータを必要に応じて定義することができます。音声機能を持つ DHCP クライアントが DHCP サーバから音声パラメータを取得できるため、装置は音声関連パラメータを含むオプション 184 をサポートします。

オプション 184 は以下のサブオプションがあります。

- **サブオプション 1** – プライマリ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。プライマリネットワークコーリングプロセッサはネットワークコーリング制御ソースとして機能し、プログラムダウンロードサービスを提供します。オプ

ション 184 では、他のサブオプションを適用させるためには、サブオプション 1 を定義する必要があります。

- **サブオプション 2** － バックアップ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。プライマリプロセッサに到達できない場合、DHCP クライアントはバックアッププロセッサに接続します。
- **サブオプション 3** － 音声 VLAN ID、および DHCP クライアントがこの VLAN を音声 VLAN として適用するかどうかの結果を示します。
- **サブオプション 4** － IP アドレスとターゲットユーザの番号を含むフェイルオーバールートを指定します。SIP VoIP ユーザは、プライマリとバックアップの両方のコーリングプロセッサに到達できない場合に、この IP アドレスと番号を使用してターゲット SIP ユーザへの接続を直接確立します。

12.4 プロトコルと標準

- RFC 2131, *Dynamic Host Configuration Protocol*
- RFC 2132, *DHCP Options and BOOTP Vendor Extensions*
- RFC 1542, *Clarifications and Extensions for the Bootstrap Protocol*
- RFC 3046, *DHCP Relay Agent Information Option*
- RFC 3442, *The Classless Static Route Option for Dynamic Host Configuration Protocol (DHCP) version 4*

目次

このセクションのページは**5-x-x**です。

13章 DHCPサーバ 13-1
13.1 概要 13-1
13.1.1 DHCPアドレスプール 13-1
13.1.2 IPアドレス割り当て順序 13-3
13.2 DHCPサーバ設定作業リスト 13-3
13.3 DHCPサーバのアドレスプールの設定 13-3
13.3.1 設定作業リスト 13-3
13.3.2 DHCPアドレスプールの作成 13-4
13.3.3 DHCPアドレスプールのIPアドレス範囲の設定 13-4
13.3.4 DHCPクライアントのゲートウェイの設定 13-6
13.3.5 クライアントへのドメイン名サフィックスの設定 13-7
13.3.6 DHCPクライアントのDNSサーバの設定 13-7
13.3.7 DHCPクライアントのWINSサーバとNetBIOSノードタイプの設定 13-7
13.3.8 DHCPクライアントのBIMSサーバ情報の設定 13-8
13.3.9 DHCPクライアントのオートコンフィグレーションの設定ファイルの設定 13-8
13.3.10 DHCPクライアントのサーバの設定 13-9
13.3.11 DHCPクライアントのオプション184パラメータの設定 13-9
13.3.12 カスタマイズDHCPオプションの設定 13-10
13.4 DHCPの有効化 13-11
13.5 インタフェースでのDHCPサーバの有効化 13-11
13.6 インタフェースでのアドレスプールの適用 13-11
13.7 IPアドレス競合検出の設定 13-12
13.8 オプション82の処理モードの有効化 13-12
13.9 DHCPサーバが送信したDHCPパケットのDSCP値の設定 13-13
13.10 DHCPサーバのSNMP通知の設定 13-13
13.11 DHCPサーバの表示と維持 13-14
13.12 DHCPサーバ設定例 13-14
13.12.1 ダイナミックIPアドレスの割り当て設定例 13-15
13.12.2 プライマリ、セカンダリサブネット設定例 13-17
13.12.3 自己定義オプション設定例 13-19
13.13 DHCPサーバ設定のトラブルシューティング 13-21
13.13.1 症状 13-21
13.13.2 分析 13-21
13.13.3 解決策 13-21

13章 DHCP サーバ

13.1 概要

DHCP(Dynamic Host Configuration Protocol)サーバ機能とは、IP アドレスなどのネットワーク利用に必要な設定情報を、各クライアントに自動的に割り当てる機能です。これにより、各クライアントでネットワークの詳細な設定を行わなくても、ネットワークに接続することができます。

DHCP サーバは以下のようなネットワークに適しています。

- 手動の設定や集中管理が難しいネットワーク
- 同時にアクセスできる IP アドレス数が制限されているネットワーク
- 多くのホストで、固定の IP アドレスが必要でないネットワーク

13.1.1 DHCP アドレスプール

各 DHCP アドレスプールは、割り当て可能な IP アドレス、ネットワーク設定パラメータのグループを持っています。DHCP サーバは、アドレスプールから IP アドレスとほかのパラメータを選択し、DHCP クライアントに割り当てます。

I. アドレス割り当てメカニズム

必要に応じて以下のようにアドレス割り当てメカニズムの設定を行います。

- **スタティックアドレス割り当て** － DHCP アドレスプールの IP アドレスをクライアントの MAC アドレスあるいは ID に手動で割り当てます。クライアントが IP アドレスを要求したとき、DHCP サーバは、スタティックバインディングの IP アドレスをクライアントに割り当てます。
- **ダイナミックアドレス割り当て** － DHCP アドレスプールの IP アドレス範囲を設定します。DHCP クライアントからの要求を受信したとき、DHCP サーバは、ダイナミックにアドレスプールの IP アドレス範囲から IP アドレスを選択します。

アドレスプールの IP アドレス範囲を設定する場合、アドレスプールの 1 つのプライマリサブネットと複数のセカンダリサブネットを設定します。

DHCP サーバは最初にプライマリサブネットから IP アドレスを選択します。もしプライマリサブネットに割り当て可能な IP アドレスがない場合、DHCP サーバは、設定された順番でセカンダリサブネットから IP アドレスを選択します。

II. アドレスプール選択の原則

DHCP サーバは以下の原則に従い、アドレスプールを選択してクライアントに IP アドレスを割り当てます。

1) IP アドレスがクライアントの MAC アドレスあるいは ID にスタティックで割り当てられているアドレスプールがある場合は、DHCP サーバが、このアドレスプールを選択し、スタティックに割り当てられている IP アドレスとほかのパラメータをクライアントに割り当てます。
2) 受信インタフェースがアドレスプールに割り当てられている場合、DHCP サーバは、このアドレスプールを選択し、IP アドレスとほかのパラメータをクライアントに割り当てます。
3) 手動で設定したアドレスプールがなく、受信インタフェースに適用されるアドレスプールがない場合、DHCP サーバはクライアントの位置に依存して以下の方法でアドレスプールを選択します。
   - **クライアントとサーバが同一サブネットにある場合**－DHCP サーバは受信インタフェースの IP アドレスをすべてのアドレスプールのプライマリサブネットにマッチさせます。
     - マッチしたプライマリサブネットが複数ある場合、最長一致（ロンゲストマッチ）のルールでアドレスプールを選択します。
     - マッチしたプライマリサブネットがない場合、DHCP サーバはすべてのアドレスプールのセカンダリサブネットにマッチさせます。DHCP サーバは最長一致（ロンゲストマッチ）のルールでアドレスプールを選択します。
   - **クライアントとサーバが異なるサブネットにある場合**－DHCP サーバは DHCP リクエストの **giaddr** フィールドにある IP アドレスをすべてのアドレスプールのプライマリサブネットにマッチさせます。（DHCP リレーエージェントはクライアントとサーバの間にあります）
     - マッチしたプライマリサブネットが複数ある場合、最長一致（ロンゲストマッチ）のルールでアドレスプールを選択します。
     - マッチしたプライマリサブネットがない場合、DHCP サーバはすべてのアドレスプールのセカンダリサブネットにマッチさせます。DHCP サーバは最長一致（ロンゲストマッチ）のルールでアドレスプールを選択します。

たとえば、1.1.1.0/24 と 1.1.1.0/25 の 2 つのアドレスプールが設定可能ですが、DHCP サーバのインタフェースに適用されていないとします。

- 受信したインタフェースの IP アドレスが 1.1.1.1/25 である場合、DHCP サーバはアドレスプール 1.1.1.0/25 を選択します。アドレスプールに割り当て可能な IP アドレスがない場合、DHCP サーバはほかのプールを選択できず、アドレス割り当ては失敗します。
- 受信したインタフェースの IP アドレスが 1.1.1.130/25 である場合、DHCP サーバはアドレスプール 1.1.1.0/24 からクライアントの IP アドレスを選択します。

正しくアドレスの割り当てを行うため、以下のサブネットの 1 つでダイナミック割り当て用の IP アドレスを保持しておいてください。

- **クライアントとサーバが同一サブネットにある場合**－DHCP サーバのインタフェースが接続されているサブネット
- **クライアントとサーバが異なるサブネットにある場合**－クライアント側に面し、最初の DHCP リレーのインタフェースが接続されているサブネット

🕮 **メモ：**

ネットワークで最低 1 つの一致したプライマリのサブネットを設定してください。そうでない場合、最初にセカンダリサブネットを選択します。セカンダリサブネットで割り当て可能な IP アドレス数より多くの DHCP クライアントが存在する場合、すべての DHCP クライアントに IP アドレスの割り当てを行うことができません。

13.1.2 IP アドレス割り当て順序

DHCP サーバはクライアントの IP アドレスを以下の順序で選択します。

1) クライアントの MAC アドレスあるいは ID に手動で割り当てされている IP アドレスです。
2) クライアントに割り当てられていた IP アドレスです。
3) DHCP-DISCOVER メッセージ内のオプション 50 フィールドに設定されている IP アドレスです。

   オプション 50 は、DHCP-DISCOVER メッセージの要求した IP アドレスフィールドです。クライアントが取得したい IP アドレスを設定するために、クライアントにより追加されます。追加される内容は、ユーザが定義します。
4) 適切な DHCP アドレスプールで検出された､最初に割り当て可能な IP アドレスです。
5) 競合していた IP アドレスか、リース期間を過ぎた IP アドレスです。割り当て可能な IP アドレスがない場合、サーバは応答しません。

🕮 **メモ：**

- クライアントが別のサブネットに移動した場合､DHCP サーバは一度クライアントに割り当てた IP アドレスの代わりに、新しいサブネットにマッチする IP アドレスを割り当てます。
- 競合した IP アドレスは 1 時間経過したのち、ほかの DHCP クライアントに割り当てることができます。

13.2 DHCPサーバ設定作業リスト

作業リスト
（必須設定項目）DHCPサーバのアドレスプールの設定
（必須設定項目）DHCPの有効化
（必須設定項目）インタフェースでのDHCPサーバの有効化
（オプション設定項目）インタフェースでのアドレスプールの適用
（オプション設定項目）IPアドレス競合検出の設定
（オプション設定項目）オプション82の処理モードの有効化
（オプション設定項目）DHCPサーバが送信したDHCPパケットのDSCP値の設定
（オプション設定項目）DHCPサーバのSNMP通知の設定

13.3 DHCPサーバのアドレスプールの設定

13.3.1 設定作業リスト

作業リスト
（必須設定項目）DHCPアドレスプールの作成

作業リスト
少なくとも以下の作業の1つを実行します。 • DHCPアドレスプールのIPアドレス範囲の設定 • DHCPクライアントのゲートウェイの設定 • クライアントへのドメイン名サフィックスの設定 • DHCPクライアントのDNSサーバの設定 • DHCPクライアントのWINSサーバとNetBIOSノードタイプの設定 • DHCPクライアントのBIMSサーバ情報の設定 • DHCPクライアントのオートコンフィグレーションの設定ファイルの設定 • DHCPクライアントのサーバの設定 • DHCPクライアントのオプション184パラメータの設定 • カスタマイズDHCPオプションの設定

13.3.2 DHCP アドレスプールの作成

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. DHCP アドレスプールを作成し、その view に移行する	**dhcp server ip-pool** *pool-name*	デフォルト：設定なし

13.3.3 DHCP アドレスプールの IP アドレス範囲の設定

DHCP アドレスプールに、スタティックのアドレス割り当ておよびダイナミックアドレスの割り当ての両方を設定することができます。ダイナミックアドレスの割り当ては、1 つのプライマリサブネットに複数のセカンダリサブネットを設定することができます。

I. DHCP アドレスプールのプライマリサブネットと複数のセカンダリサブネットの設定

プライマリサブネットで割り当て可能な IP アドレスがないとき、DHCP サーバは、クライアントに要求するセカンダリサブネットの IP アドレスを割り当てることができます。

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を設定するとき、以下のガイドラインに従ってください。

- 各アドレスプールに 1 つのプライマリサブネットのみを設定することができます。**network** コマンドを使用して複数設定した場合、最後に行った設定が適用されます。
- 各アドレスプールで最大 32 のセカンダリサブネットを設定することができます。
- **forbidden-ip** コマンドで設定された IP アドレスは、現在のアドレスプールに割り当てすることができません。ほかのアドレスプールに割り当てすることができます。**dhcp server forbidden-ip** コマンドで設定した IP アドレスはアドレスプールに割り当てることができません。

以下に 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を設定する方法を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． DHCP アドレスプールを作成し、その view に移行する	**dhcp server ip-pool** *pool-name*	デフォルト：設定なし
3． プライマリサブネットを設定する	**network** *network-address* [*mask-length* | **mask** *mask*]	デフォルト：設定なし
4． （オプション設定項目）セカンダリサブネットを設定する	**network** *network-address* [*mask-length* | **mask** *mask*] **secondary**	デフォルト：設定なし
5． （オプション設定項目）system view に戻る	**quit**	―
6． （オプション設定項目）アドレスのリース期間を設定する	**expired** { **allow-hint** | { **day** *day* [**hour** *hour* [**minute** *minute* [**second** *second*]]] | **unlimited** } [**allow-hint**] }	デフォルト：1日
7． （オプション設定項目）ダイナミック割り当てから設定された IP アドレスを除外する	**forbidden-ip** *ip-address*&<1-8>	デフォルト：DHCP サーバの IP アドレスを除き、DHCPアドレスプールすべてのアドレスが割り当て可能です。 複数のアドレス範囲を除外する場合、このステップを繰り返します。
8． system view に戻る	**quit**	―
9． （オプション設定項目）グローバルにダイナミック割り当てから設定された IP アドレスを除外する	**dhcp server forbidden-ip** *start-ip-address* [*end-ip-address*]	デフォルト：DHCPサーバインタフェースのIPアドレスを除いて、DHCPアドレスプールすべてのアドレスが割り当て可能です。 複数のアドレス範囲を除外する場合、このステップを繰り返します。

II. DHCP アドレスプールのスタティック割り当ての設定

WWW サーバのような特定の DHCP クライアントは固定の IP アドレスが必要です。クライアントに固定の IP アドレスを提供する場合、MAC アドレスあるいはクライアントの ID を DHCP アドレスプールの IP アドレスにスタティックで割り当てることができます。

スタティック割り当てを設定するとき、以下のガイドラインに従ってください。

- 1 つの IP アドレスは 1 つの MAC アドレスあるいはクライアントの ID にのみ割り当てることができます。作成されたバインディングは変更することができません。DHCP クライアントのバインディングを変更する場合、最初に既存のバインディングを削除する必要があります。
- スタティックバインディングの IP アドレスは DHCP サーバインタフェースのアドレスにすることができません。そうでない場合、IP アドレスの競合が発生し、隣接のクライアントが正常に IP アドレスを取得することができません。
- 同一装置の複数インタフェースはスタティック IP アドレスを要求するため、DHCP を使用します。この場合、要求しているインタフェースを識別するため MAC アドレスよりもクライアントの ID を設定する必要があります。そうでない場合、IP アドレスの割り当てが失敗します。

以下にスタティックバインディングを設定する方法を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. DHCP アドレスプールを作成し、その view に移行する	**dhcp server ip-pool** *pool-name*	デフォルト：設定なし
3. スタティックバインディングを設定する	**static-bind ip-address** *ip-address* [*mask-length* | **mask** *mask*] { **client-identifier** *client-identifier* | **hardware-address** *hardware-address* [**ethernet** | **token-ring**] } [**description** *description-text*]	デフォルト：設定なし 複数のスタティックバインディングを設定する場合、このステップを繰り返します。
4. （オプション設定項目）アドレスのリース期間を設定する	**expired** { **allow-hint** | { **day** *day* [**hour** *hour* [**minute** *minute* [**second** *second*]]] | **unlimited** } [**allow-hint**] }	デフォルト：1日

13.3.4 DHCP クライアントのゲートウェイの設定

DHCP クライアントはほかのネットワークへのパケットをゲートウェイに送信します。DHCP サーバは DHCP クライアントにゲートウェイアドレスを割り当てることができます。

DHCP サーバで各アドレスプールにゲートウェイアドレスを設定することができます。最大 64 つのゲートウェイを DHCP address pool view あるいは secondary subnet view で設定することができます。

DHCP サーバは以下の方法でセカンダリサブネット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。

- address pool view と secondary subnet view の両方でゲートウェイアドレスを設定する場合、DHCP サーバは secondary subnet view で設定されたゲートウェイアドレスを設定します。
- ゲートウェイアドレスが address pool view で設定されているが、secondary subnet view にない場合、DHCP サーバは address pool view のゲートウェイアドレスを割り当てます。

以下に DHCP アドレスプールのゲートウェイを設定する方法を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. DHCP アドレスプールを作成し、その view に移行する	**dhcp server ip-pool** *pool-name*	デフォルト：設定なし
3. ゲートウェイを設定する	**gateway-list** *ip-address*&<1-64>	デフォルト：設定なし
4. （オプション設定項目）secondary subnet view に移行する	**network** *network-address* [*mask-length* | **mask** *mask*] **secondary**	ー
5. （オプション設定項目）ゲートウェイを設定する	**gateway-list** *ip-address*&<1-64>	デフォルト：設定なし

13.3.5 クライアントへのドメイン名サフィックスの設定

DHCP サーバの DHCP アドレスプールにドメイン名サフィックス（DNS）を設定することができます。このサフィックスを設定することで、クライアントはドメイン名の入力部分のみ必要となります。システムは名前解決のため、ドメイン名サフィックスを追加します。

以下に DHCP アドレスプールのドメイン名サフィックスの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. DHCP アドレスプールを作成し、その view に移行する	**dhcp server ip-pool** *pool-name*	デフォルト：設定なし
3. ドメイン名サフィックスを設定する	**domain-name** *domain-name*	デフォルト：設定なし

13.3.6 DHCP クライアントの DNS サーバの設定

インターネット上のホストがドメイン名を使用してアクセスする場合、DHCP クライアントは名前を解決するため、DNS（Domain Name System）サーバと通信する必要があります。DHCP アドレスプールで最大 8 つの DNS サーバを設定することができます。

以下に DHCP アドレスプールの DNS サーバの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. DHCP address pool view に移行する	**dhcp server ip-pool** *pool-name*	デフォルト：設定なし
3. DNS サーバを設定する	**dns-list** *ip-address*&<1-8>	デフォルト：設定なし

13.3.7 DHCP クライアントの WINS サーバと NetBIOS ノードタイプの設定

NetBIOS プロトコルを使用している Microsoft DHCP クライアントは、名前解決のために WINS（Windows Internet Naming Service）サーバと通信する必要があります。DHCP アドレスプールのクライアントに最大 8 つの WINS サーバを設定することができます。

クライアントが名前解決できるように、DHCP アドレスプールに NetBIOS ノードタイプを設定する必要があります。NetBIOS ノードタイプには以下の 4 つがあります。

- **b（ブロードキャスト）-ノード** – b-ノードクライアントは、ブロードキャストメッセージで宛先名を送信します。宛先はメッセージを受信後、クライアントに IP アドレスを返します。
- **p（ピアツー-ピア）-ノード** – P-ノードクライアントは WINS サーバにユニキャストメッセージで宛先名を送信します。WINS サーバは宛先の IP アドレスを返します。
- **m（ミックス）-ノード** – m-ノードクライアントは、宛先名をブロードキャストし、応答がない場合は、WINS サーバに宛先名をユニキャストして宛先 IP アドレスを取得します。

- **h（ハイブリッド）-ノード** – h-ノードクライアントは宛先名を WINS サーバにユニキャストし、応答がない場合は、宛先名をブロードキャストして宛先 IP アドレスを取得します。

以下にDHCPアドレスプールのWINSサーバとNetBIOSノードタイプの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． DHCP アドレスプールを作成し、その view に移行する	**dhcp server ip-pool** *pool-name*	デフォルト：設定なし
3． WINS サーバを設定する	**nbns-list** *ip-address*&<1-8>	b-ノードでは、オプション設定項目です。 デフォルト：設定なし
4． NetBIOS ノードタイプを設定する	**netbios-type** { **b-node** | **h-node** | **m-node** | **p-node** }	デフォルト：設定なし

13.3.8 DHCP クライアントの BIMS サーバ情報の設定

この設定は BIMS サーバの IP アドレス、ポート番号および共有キーをクライアントに提供します。DHCP クライアントは BIMS（branch intelligent management system）サーバから取得した設定ファイルを使用して、ソフトウェアの定期的なアップデートとバックアップを実行します。

以下に DHCP アドレスプールの BIMS サーバの IP アドレス、ポート番号、共有キーの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． DHCP アドレスプールを作成し、その view に移行する	**dhcp server ip-pool** *pool-name*	デフォルト：設定なし
3． BIMS サーバの IP アドレス、ポート番号、共有キーを設定する	**bims-server ip** *ip-address* [**port** *port-number*] **sharekey** { **cipher** | **simple** } *string*	デフォルト：設定なし

13.3.9 DHCP クライアントのオートコンフィグレーションの設定ファイルの設定

オートコンフィグレーションは装置がコンフィグレーションファイルなしで起動するとき、装置がサーバから自動でコンフィグレーションの設定を取得できることを有効にします。DHCP サーバ、DNS サーバ、TFTP サーバの協力が必要です。

コンフィグレーションファイルの取得を行うため DHCP サーバでパラメータを設定する際、以下のガイドラインに従ってください。

- 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 IP アドレスアドレスあるいは名前、コンフィグレーションファイル名を設定してください。

DHCPクライアントはコンフィグレーションファイルを取得するTFTPサーバと通信するため、取得したパラメータを使用します。

以下に DHCP アドレスプールのコンフィグレーションファイル名を設定する方法を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. DHCP アドレスプールを作成し、その view に移行する	**dhcp server ip-pool** *pool-name*	デフォルト：設定なし
3. TFTP サーバの IP アドレスあるいは名前を設定する	• TFTPサーバのIPアドレスを設定する：**tftp-server ip-address** *ip-address* • TFTPサーバの名前を設定する：**tftp-server domain-name** *domain-name*	IPアドレスあるいはTFTPサーバの名前を設定することができます。 デフォルト：設定なし
4. ブートファイル名を設定する	**bootfile-name** *bootfile-name*	デフォルト：設定なし

13.3.10 DHCP クライアントのサーバの設定

特定の DHCP クライアントは TFTP サーバのようなサーバから設定情報を取得する必要があります。サーバの IP アドレスを設定することができます。DHCP サーバはサーバの IP アドレスを DHCP クライアントに他の設定情報と共に送信します。

以下にサーバの IP アドレスの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. DHCP アドレスプールを作成し、その view に移行する	**dhcp server ip-pool** *pool-name*	デフォルト：設定なし
3. サーバの IP アドレスを設定する	**next-server** *ip-address*	デフォルト：設定なし

13.3.11 DHCP クライアントのオプション 184 パラメータの設定

音声サービスを備えた DHCP クライアントに音声サービスを割り当てるためには、DHCP サーバにオプション 184 を設定する必要があります。オプション 184 の詳細は、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*5 ネットワーク接続*”の”*12 章 DHCP の概要*”を参照してください。

以下に DHCP アドレスプールのオプション 184 パラメータの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. DHCP アドレスプールを作成し、その view に移行する	**dhcp server ip-pool** *pool-name*	デフォルト：設定なし

操作	コマンド	補足
3. プライマリネットワークコーリングプロセッサの IP アドレスを設定する	**voice-config ncp-ip** *ip-address*	デフォルト：設定なし このコマンドを設定した後、ほかのオプション184のパラメータが適用されます。
4. （オプション設定項目）バックアップサーバの IP アドレスを設定する	**voice-config as-ip** *ip-address*	デフォルト：設定なし
5. （オプション設定項目）音声 VLAN を設定する	**voice-config voice-vlan** *vlan-id* { **disable** | **enable** }	デフォルト：設定なし
6. （オプション設定項目）フェイルオーバーの IP アドレス、ダイヤル番号を設定する	**voice-config fail-over** *ip-address dialer-string*	デフォルト：設定なし

13.3.12 カスタマイズ DHCP オプションの設定

重要：
カスタマイズ DHCP オプションを設定するとき、DHCP の動作への影響を十分考慮して行ってください。

カスタマイズ DHCP オプションを設定すると、以下のことが可能になります。

- 新規に定義したオプションを追加します。
- オプション 43 のようなベンダ定義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。
- 予約されたオプションの設定コマンドの制限を超過させる場合、すべてのオプションを追加します。たとえば、**dns-list** コマンドを使用して、8 つを超える DNS サーバアドレスを設定することはできません。8 つを超える DNS サーバを設定する場合、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。

表 13-1 一般的な DHCP オプション

オプション	オプション名	対応コマンド	コマンドパラメータ
3	Router Option	**gateway-list**	**ip-address**
6	Domain Name Server Option	**dns-list**	**ip-address**
15	Domain Name	**domain-name**	**ascii**
44	NetBIOS over TCP/IP Name Server Option	**nbns-list**	**ip-address**
46	NetBIOS over TCP/IP Node Type Option	**netbios-type**	**hex**
66	TFTP server name	**tftp-server**	**ascii**
67	Boot file name	**bootfile-name**	**ascii**
43	Vendor Specific Information	—	**hex**

I. DHCP アドレスプールでのカスタマイズ DHCP オプション設定

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． DHCP アドレスプールを作成し、その view に移行する	**dhcp server ip-pool** *pool-name*	デフォルト：設定なし
3． カスタマイズ DHCP オプションを設定する	**option** *code* { **ascii** *ascii-string* | **hex** *hex-string* | **ip-address** *ip-address*&<1-8> }	デフォルト：設定なし 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。

13.4 DHCPの有効化

ほかの DHCP 設定を有効にする前に DHCP を有効にする必要があります。

以下に DHCP の有効化の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． DHCP を有効にする	**dhcp enable**	デフォルト：無効

13.5 インタフェースでのDHCPサーバの有効化

インタフェースで DHCP サーバを有効にする場合、この設定を行います。インタフェースで DHCP 要求を受信すると、DHCP サーバは DHCP アドレスプールから DHCP クライアントに IP アドレスとほかの設定パラメータを割り当てます。

以下にインタフェースでの DHCP サーバの有効化の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． interface view に移行する	**interface** *interface-type interface-number*	―
3． インタフェースで DHCP サーバを有効にする	**dhcp select server**	デフォルト：有効

13.6 インタフェースでのアドレスプールの適用

インタフェースに DHCP アドレスプールを適用する場合、この設定を行います。

インタフェースから DHCP 要求を受信すると、DHCP サーバは以下の方法でアドレスを割り当てます。

- DHCP 要求にスタティックバインディングがある場合、DHCP サーバはスタティックバインディングが含まれるアドレスプールからスタティックバインディング IP アドレスと設定パラメータをクライアントに割り当てます。
- DHCP 要求にスタティックバインディングがない場合、DHCP サーバはアドレスプールと設定パラメータのために適用されたアドレスプールを選択します。

以下にインタフェースにアドレスプールを適用する設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. interface view に移行する	**interface** *interface-type interface-number*	ー
3. インタフェースにアドレスプールを適用する	**dhcp server apply ip-pool** *pool-name*	デフォルト : 適用されていません。 アドレスプールがない場合、DHCPサーバはダイナミックアドレスの割り当てに失敗します。

13.7 IPアドレス競合検出の設定

IP アドレスを割り当てる前に、DHCP サーバは、ping パケットを送信して、割り当てるアドレスが使用中かどうかを調べます。

- DHCP サーバが設定した期間内に ping 応答を受信した場合、サーバは別の IP アドレスに ping を行います。
- 応答がない場合、指定数の ping パケットが送信されるまでサーバは IP アドレスに ping を行います。応答がない場合は、サーバは要求元のクライアントに IP アドレスを割り当てます。DHCP クライアントは gratuitous ARP パケットを送信して IP アドレスが競合しているかどうかを調べます。

以下に IP アドレス競合検出の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. （オプション設定項目）IP アドレス競合検出の ping パケットの最大数を設定する	**dhcp server ping packets** *number*	デフォルト：1 **0**に設定した場合、IPアドレスの競合検出を行いません。
3. （オプション設定項目）ping に対する応答の待機タイムアウトを設定する	**dhcp server ping timeout** *milliseconds*	デフォルト：500ms **0**に設定した場合、IPアドレスの競合検出を行いません。

13.8 オプション82の処理モードの有効化

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 DHCP 応答メッセージにオプション 82 を追加します。

DHCP サーバがオプション 82 を無視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。

オプション 82 のパラメータが正常に動作するために、DHCP サーバと DHCP リレーエージェントの両方でオプション 82 を処理するように有効にする必要があります。DHCP リレーエージェントでの有効にする設定については、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*5 ネットワーク接続*”の”*14 章 DHCP リレー*”を参照してください。

以下に DHCP サーバでのオプション 82 の処理モードの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. オプション 82 の処理モードを有効にする	**dhcp server relay information enable**	デフォルト：有効

13.9 DHCPサーバが送信したDHCPパケットのDSCP値の設定

パケットの DSCP 値は、パケットの優先度レベルを設定し、パケットの優先度に影響します。

以下に DHCP サーバが送信した DHCP パケットの DHCP 値の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. DHCP サーバが送信した DHCP パケットの DHCP 値を設定する	**dhcp dscp** *dscp-value*	デフォルト：56

13.10 DHCPサーバのSNMP通知の設定

下記の DHCP サーバイベントについて、SNMP 通知を設定することが可能です。

- DHCP アドレスプールが枯渇または回復した。
- DHCP アドレスプールの使用しきい値が超過した。
- IP アドレス割り当て使用率しきい値が超過した。

SNMP 通知は、SNMP モジュールに送信されます。SNMP 通知を正しく送信するには、SNMP も設定する必要があります。SNMP 設定の詳細については、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*17 ネットワーク管理と監視*”の”*4 章 SNMP*”を参照してください。

DHCP アドレスプール使用率しきい値違反の場合、DHCP モジュールはログメッセージもインフォメーションセンターに送信します。ログメッセージを正しく送信するには、インフォメーションセンターも設定する必要があります。インフォメーションセンター設定については、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“3 *システム管理*”の”*5 章 Information Center*”を参照してください。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー

操作	コマンド	補足
2. DHCP サーバの SNMP 通知を有効にする	**snmp-agent trap enable dhcp server** [**address-exhaust** | **allocated-ip** | **ip-in-use**]	デフォルト：有効
3. DHCP アドレスプール view に移行する	**dhcp server ip-pool** *pool-name*	ー

13.11 DHCPサーバの表示と維持

重要：

DHCP サーバの再起動あるいは、**reset dhcp server ip-in-use** コマンドが実行されると、すべてのリース情報を削除します。DHCP サーバは DHCP クライアントからのリース期間延長要求を拒否するので、クライアントは再度 IP アドレスを要求する必要があります。

すべての view で **display** コマンドを実行でき、user view で **reset** コマンドを実行できます。

操作	コマンド
IPアドレスの競合に関する情報を表示する	**display dhcp server conflict** [**ip** *ip-address*]
リース期限切れに関する情報を表示する	**display dhcp server expired** [**ip** *ip-address* | **pool** *pool-name*]
割り当て可能なIPアドレスに関する情報を表示する	**display dhcp server free-ip** [**pool** *pool-name*]
割り当てられたIPアドレス情報を表示する	**display dhcp server ip-in-use** [**ip** *ip-address* | **pool** *pool-name*]
DHCPサーバの統計情報を表示する	**display dhcp server statistics** [**pool** *pool-name*]
DHCPアドレスプールの情報を表示する	**display dhcp server pool** [*pool-name*]
IPアドレスの競合に関する情報を削除する	**reset dhcp server conflict** [**ip** *ip-address*]
リース期限切れに関する情報を削除する	**reset dhcp server expired** [**ip** *ip-address* | **pool** *pool-name*]
割り当てられたIPアドレス情報を削除する	**reset dhcp server ip-in-use** [**ip** *ip-address* | **pool** *pool-name*]
DHCPサーバの統計情報を削除する	**reset dhcp server statistics**

13.12 DHCPサーバ設定例

DHCP のネットワークの構築は以下のタイプがあります。

- 同一サブネット上の DHCP サーバと DHCP クライアントは、直接メッセージを交換できます。
- 異なるサブネット上の DHCP サーバと DHCP クライアントは、DHCP リレーエージェントを介して相互に通信します。

DHCP サーバの設定は、どちらのタイプでも同じです。

13.12.1 ダイナミック IP アドレスの割り当て設定例

I. ネットワーク要件

図 13-1に示すように、DHCP サーバ（AC）はサブネット 10.1.1.0/24 のクライアントに IP アドレスを割り当てます。10.1.1.0/24 はさらに 10.1.1.0/25 と 10.1.1.128/25 にサブネット化されます。

AC の DHCP サーバを、サブネット 10.1.1.0/25 の IP アドレスと、サブネット 10.1.1.128/25 の IP アドレスを DHCP クライアントに割り当てるよう設定します。

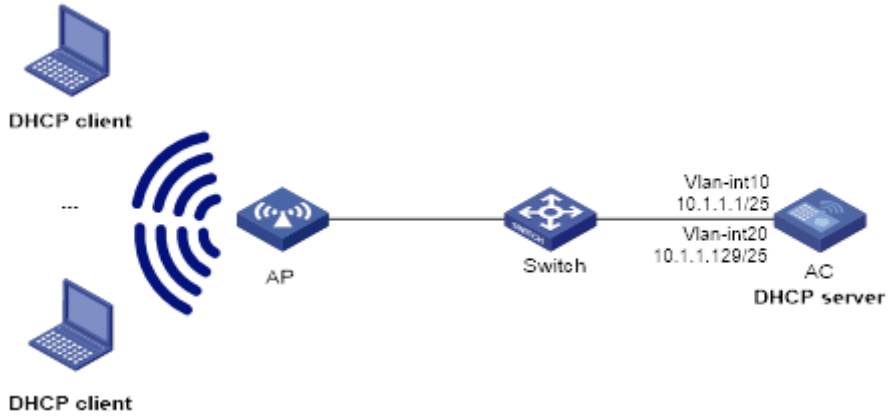


図 13-1 ネットワーク図

II. 設定手順

1)　VLAN インタフェースに IP アドレスを設定します。

VLAN 10 と VLAN 20 を作成します。

```
<AC> system-view
[AC] vlan 10
[AC-vlan10] quit
[AC] vlan 20
[AC-vlan20] quit
```

VLAN10 で AP に接続されるインタフェースに VLAN 10 を追加します。

```
[AC] interface gigabitethernet 1/0/2
[AC-GigabitEthernet1/0/2] port link-type trunk
[AC-GigabitEthernet1/0/2] port trunk permit vlan 10
```

```
[AC-GigabitEthernet1/0/2] port trunk pvid vlan 10
[AC-GigabitEthernet1/0/2] quit
```

VLAN インタフェース 10 と VLAN インタフェース 20 に IP アドレスをアサインします。

```
[AC] interface vlan-interface 10
[AC-Vlan-interface10] ip address 10.1.1.1 25
[AC-Vlan-interface10] quit
[AC] interface vlan-interface 20
[AC-Vlan-interface20] ip address 10.1.1.129 25
[AC-Vlan-interface20] quit
```

2) ワイヤレスサービスを設定します。

サービステンプレートを設定し、VLAN20 をサービステンプレートにバインドします。

```
[AC] wlan service-template service
[AC-wlan-st-service] ssid service
[AC-wlan-st-service] vlan 20
[AC-wlan-st-service] service-template enable
[AC-wlan-st-service] quit
```

AP を設定します。

```
[AC] wlan ap ap1 model QX- W1110
[AC-wlan-ap-ap1] serial-id 219801A28N819CE0002T
[AC-wlan-ap-ap1] radio 1
[AC-wlan-ap-ap1-radio-1] service-template service1
[AC-wlan-ap-ap1-radio-1] radio enable
[AC-wlan-ap-ap1-radio-1] return
```

3) DHCP サーバを設定します。

DHCP を有効にします。

```
[AC] dhcp enable
```

VLAN インタフェース 10、VLAN インタフェース 20 で DHCP サーバを有効にします。

```
[AC] interface vlan-interface 10
[AC-Vlan-interface10] dhcp select server
[AC-Vlan-interface10] quit
[AC] interface vlan-interface 20
[AC-Vlan-interface20] dhcp select server
[AC-Vlan-interface20] quit
```

サブネット 10.1.1.0/25 の AP に IP アドレスをアサインするための DHCP アドレスプール 1 を設定します。

```
[AC] dhcp server ip-pool 1
[AC-dhcp-pool-1] network 10.1.1.0 mask 255.255.255.128
[AC-dhcp-pool-1] quit
```

サブネット 10.1.1.128/25 の AP に IP アドレスをアサインするための DHCP アドレスプール 2 を設定します。

```
[AC] dhcp server ip-pool 2
[AC-dhcp-pool-2] network 10.1.1.128 mask 255.255.255.128
[AC-dhcp-pool-2] quit
```

III. 設定の確認

サブネット 10.1.1.0/25 の AP と 10.1.1.128/25 のクライアントが DHCP サーバから正しい IP アドレスを取得することを確認します。（詳細は省略します。）

DHCP サーバで AP とクライアントに割り当てられた IP アドレスを表示します。

```
[AC] display dhcp server ip-in-use
IP address       Client identifier/    Lease expiration      Type
                 Hardware address
10.1.1.3         0031-3865-392e-6262-  Jan 1 22:25:03 2015  Auto(C)
                 3363-2e30-3230-352d-
                 4745-302f-30
10.1.1.130       3030-3030-2e30-3030-  Jan 9 10:45:11 2015   Auto(C)
                 662e-3030-3033-2d45-
                 7568-6572-1e
10.1.1.131       3030-0020-fe02-3020-  Jan 9 10:45:11 2015   Auto(C)
                 7052-0201-2013-1e02
                 0201-9068-23
10.1.1.132       2020-1220-1102-3021-  Jan 9 10:45:11 2015   Auto(C)
                 7e52-0211-2025-3402
                 0201-9068-9a
10.1.1.133       2021-d012-0202-4221-  Jan 9 10:45:11 2015   Auto(C)
                 8852-0203-2022-55e0
                 3921-0104-31
```

13.12.2 プライマリ、セカンダリサブネット設定例

I. ネットワーク要件

図 13-2に示すように、DHCP サーバ（AC）は LAN 上のクライアントにダイナミックに IP アドレスを割り当てます。

DHCP サーバのアドレスプールにプライマリサブネット 10.1.1.0/24、セカンダリサブネット 10.1.2.0/24 を設定します。プライマリサブネットで割り当てるアドレスがないとき、DHCP サーバは、セカンダリサブネットの IP アドレスを選択します。

AC は以下のパラメータを割り当てます。

- サブネット 10.1.1.0/24 のクライアントにデフォルトゲートウェイ 10.1.1.254/24 を割り当てます。

- サブネット 10.1.2.0/24 のクライアントにデフォルトゲートウェイ 10.1.2.254/24 を割り当てます。

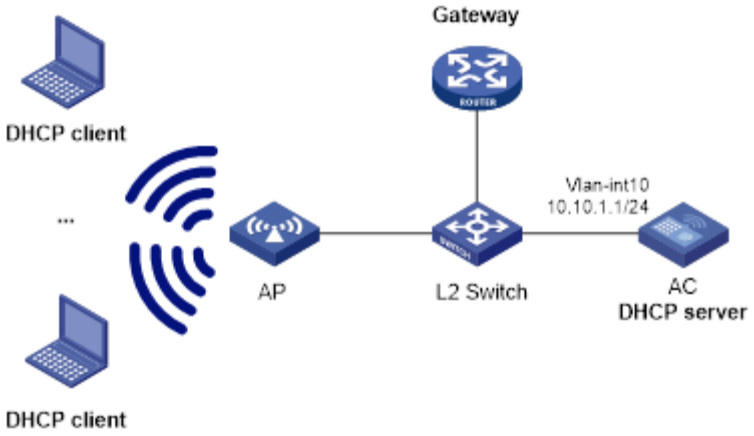


図 13-2 ネットワーク図

II. 設定手順

AC の基本設定を行います。詳細は、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*6 WLAN アクセス*”の”*1 章 WLAN アクセス*”を参照してください。

DHCP を有効にします。

```
<AC> system-view
[AC] dhcp enable
```

VLAN インタフェース 10 のプライマリ IP アドレス、セカンダリ IP アドレスを設定します。

```
[AC] interface vlan-interface 10
[AC-Vlan-interface10] ip address 10.1.1.1 24
[AC-Vlan-interface10] ip address 10.1.2.1 24 sub
```

VLAN インタフェース 10 で DHCP サーバを有効にします。

```
[AC-Vlan-interface10] dhcp select server
[AC-Vlan-interface10] quit
```

DHCP アドレスプール aa を作成します。

```
[AC] dhcp server ip-pool aa
```

ダイナミック割り当てのプライマリアドレス、ゲートウェイアドレスを設定します。

```
[AC-dhcp-pool-aa] network 10.1.1.0 mask 255.255.255.0
[AC-dhcp-pool-aa] gateway-list 10.1.1.254
```

ダイナミック割り当てのセカンダリサブネット、ゲートウェイアドレスを設定します。

```
[AC-dhcp-pool-aa] network 10.1.2.0 mask 255.255.255.0 secondary
```

```
[AC-dhcp-pool-aa-secondary] gateway-list 10.1.2.254
[AC-dhcp-pool-aa-secondary] quit
[AC-dhcp-pool-aa] quit
```

III. 設定の確認

プライマリサブネットで割り当て可能なアドレスがない場合、DHCP サーバはセカンダリサブネットから割り当てることを確認します（詳細は省略します）。

DHCP サーバが割り当てたプライマリ、セカンダリサブネット IP アドレスを表示します。

```
[AC] display dhcp server ip-in-use
IP address       Client identifier/    Lease expiration      Type
                 Hardware address
10.1.1.2         0031-3865-392e-6262-  Jan 14 22:25:03 2015  Auto(C)
                 3363-2e30-3230-352d-
                 4745-302f-30
10.1.2.2         3030-3030-2e30-3030-  Jan 14 22:25:03 2015  Auto(C)
                 662e-3030-3033-2d45-
                 7568-6572-1e
```

13.12.3 自己定義オプション設定例

I. ネットワーク要件

図 13-3に示すように DHCP クライアント（AC）は DHCP サーバ（Device）から、IP アドレスと ゼロタッチプロビジョニングを利用するためのオプション43情報を取得します。

DHCP サーバ(デバイス)に以下のように設定します。

- ゼロタッチプロビジョニングを利用するためのオプション43情報をDHCPオプショングループに設定します。この例では、ascii で” NEC,zerotouch,10.1.1.1,443”の文字列を設定します。
- DHCP ユーザクラスを作成し、ゼロタッチプロビジョニングを行う装置（option60に” NEC,”の文字列を含む）を条件として設定します。
- DHCP クライアントが取得する IP アドレスは、ネットワークセグメント 10.1.1.0/24 に属し、ゲートウェイアドレスと DNS サーバアドレスは 10.1.1.1 です。

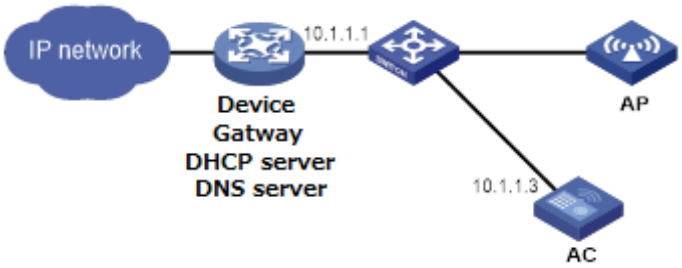


図 13-3 ネットワーク図

II. 設定手順

1)　デバイスの GigabitEthernet 1/0/1 に IP アドレスを指定します。

```
<Device> system-view
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] ip address 10.1.1.2 24
[Device-GigabitEthernet1/0/1] quit
```

2)　DHCP オプショングループ 1 を作成し、カスタマイズオプション 43 を設定します

```
[Device] dhcp option-group 1
[Device-dhcp-class-zero-touch] option 43 ascii NEC,zerotouch,10.1.1.1,443
[Device-dhcp-class-zero-touch] quit
```

3)　DHCP ユーザクラス zero-touch を作成し、条件を設定します。

```
[Device] dhcp class zero-touch
[Device-dhcp-option-group-1] if-match rule 1 option 60 ascii NEC, partial
[Device-dhcp-option-group-1] quit
```

4)　DHCP サーバを設定します。

DHCP を有効化します。

```
[Device] dhcp enable
```

GigabitEthernet 1/0/1 で DHCP を有効化します。

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] ip address dhcp select server
[Device-GigabitEthernet1/0/1] quit
```

ダイナミック割り当てのための DHCP アドレスプール 0 を設定します。

```
[Device] dhcp server ip-pool 0
```

10.1.1.0/24 をアサインするサブネットに指定します。

```
[Device-dhcp-pool-0] network 10.1.1.0 mask 255.255.255.0
```

#ゲートウェイアドレスと DNS サーバアドレスを 10.1.1.1 に指定します。

```
[Device-dhcp-pool-0] gateway-list 10.1.1.1
[Device-dhcp-pool-0] dns-list 10.1.1.1
```

DHCP ユーザクラス zero-touch に、DHCP オプショングループ 1 を指定します。

```
[Device-dhcp-pool-0] class zero-touch option-group 1
```

III. 設定の確認

AP がゼロタッチプロビジョニングに成功することを NetMeister で確認にします。（詳細は省略します。）

DHCP サーバで、アサインされた IP アドレスを表示します。

```
[Device] display dhcp server ip-in-use
```

13.13 DHCPサーバ設定のトラブルシューティング

13.13.1 症状

DHCP サーバから取得したクライアントの IP アドレスが別の IP アドレスと競合しています。

13.13.2 分析

サブネットの別のホストが同一 IP アドレスを持っている可能性があります。

13.13.3 解決策

1) クライアントのネットワークアダプタを無効にする、もしくはネットワークケーブルの接続を切断します。別のホストにあるクライアントの IP アドレスに ping を行い、同じ IP アドレスを使用しているホストがあるかを調べます。
2) ping に対する応答があれば、そのホストには IP アドレスが手動で設定されています。DHCP サーバで **dhcp server forbidden-ip** コマンドを実行して、ダイナミックな割り当てからその IP アドレスを除外します。
3) クライアントのネットワークアダプタを有効にする、もしくはネットワークケーブルを接続します。クライアントの IP アドレスを解放し、IP アドレスを再取得します。Windows の DHCP クライアントの場合、以下のように行います。
   a) DOS環境で**cmd**コマンドを実行し、コマンドプロンプトを起動します。
   b) **ipconfig /release**を実行してIPアドレスを放棄します。
   c) **ipconfig /renew**を実行し、IPアドレスの再取得を行います。

目次

このセクションのページは**5-x-x**です。

14章 DHCPリレー 14-1
14.1 概要 14-1
14.1.1 動作 14-1
14.1.2 DHCPリレーエージェントのオプション82のサポート 14-2
14.2 DHCPリレーエージェント設定作業リスト 14-3
14.3 DHCPの有効化 14-3
14.4 インタフェースでのDHCPリレーエージェントの有効化 14-3
14.5 リレーエージェントのDHCPサーバの指定 14-3
14.6 DHCPリレーエージェントセキュリティ機能の設定 14-4
14.6.1 DHCPリレーエージェントのリレーエントリの記録の有効化 14-4
14.6.2 ダイナミックリレーエントリの定期的な更新の有効化 14-4
14.7 DHCPリレーエージェントでのIPアドレスのリリース設定 14-5
14.8 オプション82の設定 14-5
14.9 DHCPリレーエージェントが送信したDHCPパケットのDSCPの設定 14-6
14.10 DHCPリレーエージェントの表示と維持 14-6
14.11 DHCPリレーエージェント設定例 14-7
14.11.1 DHCPリレーエージェント設定例 14-7
14.12 DHCPリレーエージェントのトラブルシューティング 14-8
14.12.1 症状 14-8
14.12.2 分析 14-8
14.12.3 解決策 14-8

14章 DHCP リレー

14.1 概要

DHCP リレーエージェントは、DHCP クライアントが別のサブネット上の DHCP サーバから IP アドレスを取得できるようにします。この機能は、異なるサブネット上の DHCP クライアントが同一の DHCP サーバに通信でき、集中管理が行いやすくなることで、コストの節減にもなります。図 14-1に DHCP リレーエージェントの標準的な構成を示します。

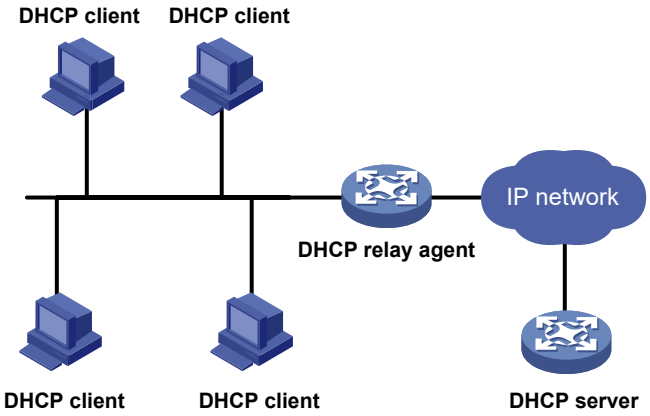


図 14-1 DHCP リレーエージェント構成

14.1.1 動作

DHCP サーバと DHCP クライアントは、DHCP リレーエージェントの有無に関わらず、同様の方法で互いに相互に通信します。相互接続の詳細は、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*5 ネットワーク接続*”の”*12 章 DHCP の概要*”を参照してください。以下に、DHCP リレーエージェントに関連した手順を示します。

1) DHCP クライアントから DHCP-DISCOVER または DHCP-REQUEST ブロードキャストメッセージを受信すると、DHCP リレーエージェントはメッセージを以下のように処理します。
   a) メッセージの**giaddr**フィールドにIPアドレスを入力します。
   b) メッセージを指定したDHCPサーバにユニキャストで転送します。
2) **giaddr** フィールドにもとづいて、DHCP サーバは IP アドレスおよびその他の設定パラメータをリレーエージェントに返信します。
3) リレーエージェントはそれらの情報をクライアントへ転送します。

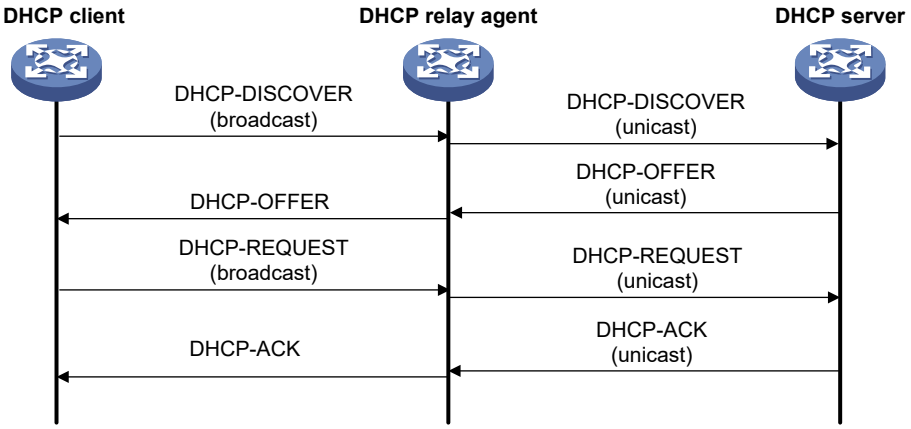


図 14-2 DHCP リレーエージェントの動作

14.1.2 DHCP リレーエージェントのオプション 82 のサポート

オプション 82 は DHCP クライアントの位置情報を記録します。オプション 82 は以下の作業を行います。

- セキュリティとアカウンティングのため、DHCP クライアントの位置を示します。
- DHCP クライアントに指定した範囲の IP アドレスを割り当てます。

詳細は、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*5 ネットワーク接続*”の”*12 章 DHCP の概要*”を参照してください。

DHCP リレーエージェントがオプション 82 をサポートしている場合、表 14-1に示されている処理方法に従って、DHCP 要求を処理します。

DHCP サーバからの返答にオプション 82 が含まれている場合は、DHCP リレーエージェントがクライアントに応答を転送する前にオプション 82 を取り除きます。

表 14-1 DHCP リレーエージェントのオプション 82 の処理方法

クライアントの要求メッセージに含まれるオプション	処理方法	DHCP リレーエージェントの動作
Option 82	Drop	メッセージを廃棄します。
	Keep	オプション82を変更せずにメッセージを転送します。
	Replace	元のオプション82を設定されたパディング形式、パディングの内容、コードタイプに従って、新しいオプション82に置き換えてからメッセージを転送します。
No Option 82	–	設定されたパディング形式、パディングの内容、コードタイプに従って、元のオプション82に追加し、メッセージを転送します。

14.2 DHCPリレーエージェント設定作業リスト

作業リスト
（必須設定項目）DHCPの有効化
（必須設定項目）インタフェースでのDHCPリレーエージェントの有効化
（必須設定項目）リレーエージェントのDHCPサーバの指定
（オプション設定項目）DHCPリレーエージェントセキュリティ機能の設定
（オプション設定項目）DHCPリレーエージェントでのIPアドレスのリリース設定
（オプション設定項目）オプション82の設定
（オプション設定項目）DHCPリレーエージェントが送信したDHCPパケットのDSCPの設定

14.3 DHCPの有効化

ほかの DHCP リレーエージェントの設定を有効にするために、DHCP を有効にしてください。

以下に DHCP の有効化の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． DHCP を有効にする	**dhcp enable**	デフォルト：無効

14.4 インタフェースでのDHCPリレーエージェントの有効化

DHCP リレーエージェントが有効なとき、インタフェースは DHCP サーバに受信した DHCP 要求を転送します。

DHCP リレーエージェントのインタフェースの IP アドレスが含まれる IP アドレスプールは DHCP サーバに設定する必要があります。そうでない場合、DHCP リレーエージェントに接続される DHCP クライアントは IP アドレスを取得できません。

以下にインタフェースでの DHCP リレーエージェントの有効化の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． interface view に移行する	**interface** *interface-type interface-number*	―
3． DHCP リレーエージェントを有効にする	**dhcp select relay**	デフォルト：DHCPが有効にされたとき、インタフェースはDHCPサーバモードで動作します。

14.5 リレーエージェントのDHCPサーバの指定

可用性を向上するため、DHCP リレーエージェントでいくつかの DHCP サーバを指定することができます。インタフェースがクライアントから要求メッセージを受信したとき、リレーエージェントはすべての DHCP サーバに要求メッセージを転送します。

リレーエージェントで DHCP サーバアドレスを指定するとき、以下のガイドラインに従ってください。

- 指定された DHCP サーバアドレスは、リレーエージェントインタフェースの IP アドレスと異なるサブネットにする必要があります。そうでなければクライアントは IP アドレスの取得に失敗します。
- 最大 8 つの DHCP サーバを指定することができます。

以下にリレーエージェントに DHCP サーバアドレスの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. interface view に移行する	**interface** *interface-type interface-number*	―
3. リレーエージェントに DHCP サーバアドレスを指定する	**dhcp relay server-address** *ip-address*	デフォルト：指定なし

14.6 DHCPリレーエージェントセキュリティ機能の設定

14.6.1 DHCP リレーエージェントのリレーエントリの記録の有効化

DHCP から IP アドレスを取得した後、クライアントの IP アドレスと MAC アドレスバインディング情報（リレーエントリ）を自動的に記録することができます。

いくつかのセキュリティ機能は、受信パケットを確認するため、記録されたリレーエントリを使用し、エントリにマッチしないパケットをブロックします。ブロックすることで、不正なホストがリレーエージェントを通して外部ネットワークにアクセスできないようにします。

以下に DHCP リレーエージェントのリレーエントリの記録を有効にする設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. DHCP リレーエージェントのリレーエントリの記録を有効にする	**dhcp relay client-information record**	デフォルト：無効

14.6.2 ダイナミックリレーエントリの定期的な更新の有効化

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、以下の情報を使用します。

- リレーエントリの IP アドレス
- DHCP リレーインタフェースの MAC アドレス

DHCP リレーエージェントは DHCP サーバからの受信に従って、リレーエントリを保持します。

- 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リレーエントリを削除します。そして 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。

以下にダイナミックリレーエントリの定期的な更新の有効化の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. ダイナミックリレーエントリの定期的な更新を有効にする	**dhcp relay client-information refresh enable**	デフォルト：有効

14.7 DHCPリレーエージェントでのIPアドレスのリリース設定

クライアントの IP アドレスをリリースするためにリレーエージェントを設定します。リレーエージェントは DHCP-RELEASE メッセージをサーバに送信し、リレーエントリを削除します。DHCP-RELEASE メッセージを受信した DHCP サーバは IP アドレスをリリースします。

以下に IP アドレスをリリースするために DHCP リレーエージェントの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. IP アドレスをリリースするために DHCP リレーエージェントを設定する	**dhcp relay release ip** *ip-address*	このコマンドでは、DHCPリレーエージェントでリレーエントリが記録されたIPアドレスのみリリースすることができます。

14.8 オプション82の設定

オプション 82 を設定するとき、以下のガイドラインに従ってください。

- オプション 82 をサポートするため、関連する DHCP サーバと DHCP リレーエージェントの設定を実行してください。
- 要求メッセージの処理方法が replace である場合、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。要求メッセージの処理方法が keep あるいは drop である場合、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。
- オプション 82 のサブオプション 1 が設定されている場合、ノードの装置名（**sysname**）でパディングされている場合、装置名はスペースを含んではいけません。スペースが含まれている場合、DHCP リレーエージェントはオプション 82 の追加、更新に失敗します。

以下にオプション 82 の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. interface view に移行する	**interface** *interface-type interface-number*	―
3. オプション 82 を動作できるようにリレーエージェントで有効にする	**dhcp relay information enable**	デフォルト：無効
4. （オプション設定項目）オプション 82 が含まれる要求メッセージの処理方法を設定する	**dhcp relay information strategy** { **drop** | **keep** | **replace** }	デフォルト：**replace**
5. （オプション設定項目）サーキット ID サブオプションのパディング内容とコードタイプを設定する	**dhcp relay information circuit-id** { **string** *circuit-id* | { **normal** | **verbose** [**node-identifier** { **mac** | **sysname** | **user-defined** *node-identifier* }] } [**format** { **ascii** | **hex** }] }	デフォルト：サーキットIDサブオプションのパディング内容は**normal**で、コードタイプは**hex**です。
6. （オプション設定項目）リモート ID サブオプションのパディング内容とコードタイプを設定する	**dhcp relay information remote-id** { **normal** [**format** { **ascii** | **hex** }] | **string** *remote-id* | **sysname** }	デフォルト：リモートIDサブオプションのパディング内容は**normal**で、コードタイプは**hex**です。

14.9 DHCPリレーエージェントが送信したDHCPパケットのDSCPの設定

パケットの DSCP は、パケットの優先度レベルを指定し、パケットの優先度に影響します。

以下にDHCP リレーエージェントが送信したDHCP パケットのDSCP の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. DHCP リレーエージェントが送信した DHCP パケットのDSCP を設定する	**dhcp dscp** *dscp-value*	デフォルト：56

14.10 DHCPリレーエージェントの表示と維持

すべての view で **display** コマンドを実行でき、user view で **reset** コマンドを実行できます。

操作	コマンド
インタフェース上のDHCPリレーエージェントのDHCPサーバ情報を表示する	**display dhcp relay server-address** [**interface** *interface-type interface-number*]
DHCPリレーエージェントのオプション82の設定情報を表示する	**display dhcp relay information** [**interface** *interface-type interface-number*]

操作	コマンド
DHCPリレーエージェントのリレーエントリを表示する	**display dhcp relay client-information** [**interface** *interface-type interface-number* | **ip** *ip-address*]
DHCPリレーエージェントのパケット統計情報を表示する	**display dhcp relay statistics** [**interface** *interface-type interface-number*]
DHCPリレーエージェントのリレーエントリを削除する	**reset dhcp relay client-information** [**interface** *interface-type interface-number* | **ip** *ip-address*]
DHCPリレーエージェントのパケット統計情報を削除する	**reset dhcp relay statistics** [**interface** *interface-type interface-number*]

14.11 DHCPリレーエージェント設定例

14.11.1 DHCP リレーエージェント設定例

I. ネットワーク要件

図 14-3に示すように、DHCP クライアントが別のサブネット上にある DHCP サーバから IP アドレスと設定パラメータを取得するため、Switch A に DHCP リレーエージェントを設定します。

DHCP リレーエージェントとサーバは異なるサブネットにあり、互いに通信できるようにするため、スタティックあるいはダイナミックルーティングを設定します。

クライアントとサーバ間の通信を行うため、DHCP サーバで設定を行います。DHCP サーバの設定については、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*5 ネットワーク接続*”の”*13 章 DHCP サーバ*”を参照してください。

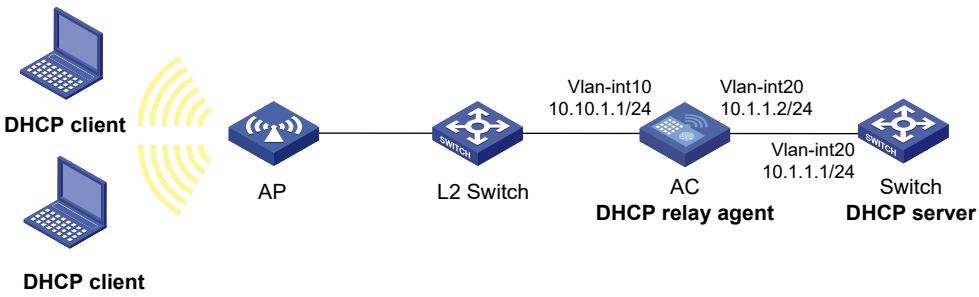


図 14-3 ネットワーク図

II. 設定手順

インタフェースの IP アドレスを指定します。（詳細は省略します。）

AC の基本設定を行います。詳細は、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*6 WLAN アクセス*”の”*1 章 WLAN アクセス*”を参照してください。

DHCP を有効にします。

```
<AC> system-view
[AC] dhcp enable
```

VLAN インタフェース 10 で DHCP リレーエージェントを有効にします。

```
[AC] interface vlan-interface 10
[AC-Vlan-interface10] dhcp select relay
```

リレーエージェントで DHCP サーバの IP アドレスを指定します。

```
[AC-Vlan-interface10] dhcp relay server-address 10.1.1.1
```

III. 設定の確認

DHCP クライアントが DHCP リレーエージェントを通して DHCP サーバから IP アドレスとほかのネットワークパラメータを取得できることを確認します（詳細は省略します）。

DHCP リレーエージェントによって転送された DHCP パケットの統計情報を表示します。

```
[AC] display dhcp relay statistics
```

DHCP リレーエージェントの記録を有効にしている場合、リレーエントリを表示します。

```
[AC] display dhcp relay client-information
```

14.12 DHCPリレーエージェントのトラブルシューティング

14.12.1 症状

DHCP クライアントが、DHCP リレーエージェントを通して設定パラメータを取得することができません。

14.12.2 分析

DHCP リレーエージェントあるいは DHCP サーバの設定に問題が発生している可能性があります。

14.12.3 解決策

問題を切り分けるため、デバッグを有効にし、DHCP リレーエージェントで **display** コマンドを実行します。デバッグ情報とインタフェース状態の情報を確認してください。

以下の項目を確認してください。

- DHCP サーバと DHCP リレーエージェントで DHCP が有効になっているかどうか確認してください。
- DHCP サーバが DHCP クライアントと同じサブネットでアドレスプールを持っているかどうか確認してください。
- DHCP サーバと DHCP リレーエージェントが互いに通信可能であることを確認してください。
- DHCP クライアントに接続される DHCP リレーエージェントのインタフェースで、DHCP サーバのアドレスが正しく設定されているかどうか確認してください。

目次

このセクションのページは**5-x-x** です。

15章 DHCPクライアント 15-1
15.1 インタフェースでのDHCPクライアントの有効化 15-1
15.2 アドレス重複検出の有効化 15-1
15.3 DHCPクライアントが送信するDHCPパケットのDSCPの設定 15-2
15.4 DHCPクライアントの表示と維持 15-2

15章 DHCP クライアント

装置は DHCP クライアントが有効である場合、DHCP サーバから IP アドレスを含む設定パラメータを取得できます。DHCP クライアントの設定は VLAN インタフェースでのみサポートします。

15.1 インタフェースでのDHCPクライアントの有効化

インタフェースで DHCP クライアントを有効にするため、以下のガイドラインに従ってください。

- IP アドレス要求の失敗数がシステムで定義した値に到達した場合、DHCP クライアントが有効なインタフェースはデフォルトの IP アドレスを使用します。
- インタフェースは何度も IP アドレスを取得することができますが、古い設定が新しい設定に上書きされ、新しい設定が適用されます。
- DHCP クライアントが有効になった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。
- DHCP サーバから割り当てられた IP アドレスが装置上のほかのインタフェースの IP アドレスとネットワークセグメントを共有していた場合、インタフェースは割り当てられた IP アドレスを使用しません。その代わり、DHCP サーバから新しい IP アドレスを要求します。

以下にインタフェースでの DHCP クライアントの有効化の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. interface view に移行する	**interface** *interface-type interface-number*	―
3. インタフェースで DHCP クライアントを有効にする	**ip address dhcp-alloc**	デフォルト：無効

15.2 アドレス重複検出の有効化

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。

以下にアドレス重複検出の有効化の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. アドレス重複検出を有効にする	**dhcp client dad enable**	デフォルト：有効

15.3 DHCPクライアントが送信するDHCPパケットのDSCPの設定

パケットの DSCP は、パケットの優先度レベルを指定し、パケットの優先度に影響します。

以下に DHCP クライアントが送信した DHCP パケットの DSCP の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． DHCP クライアントが送信する DHCP パケットの DSCP を設定する	**dhcp client dscp** *dscp-value*	デフォルト：56

15.4 DHCPクライアントの表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
DHCPクライアント情報を表示する	**display dhcp client** [**verbose**] [**interface** *interface-type interface-number*]

目次

このセクションのページは**5-x-x**です。

16章 BOOTPクライアント..... 16-1
16.1 BOOTPアプリケーション 16-1
16.2 動的IPアドレスの取得 16-1
16.3 プロトコルと標準 16-1
16.4 インタフェースでBOOTPを使用したIPアドレスの取得の設定 16-2
16.5 BOOTPクライアントの表示と維持 16-2

16章 BOOTP クライアント

BOOTP（ブートストラッププロトコル）は、コンピュータネットワークに接続されたクライアントが、IP アドレスやホスト名、サブネットマスク等を自動的に取得するためのプロトコルです。

BOOTP クライアントの設定は VLAN インタフェースでのみサポートします。

16.1 BOOTPアプリケーション

BOOTP クライアントとして指定したインタフェースは BOOTP を使用して BOOTP サーバから情報（IP アドレスなど）を入手することができます。

BOOTP を使用するため、管理者は各 BOOTP クライアントに対し BOOTP パラメータファイルを BOOTP サーバ上に用意する必要があります。パラメータファイルには、BOOTP クライアントの IP アドレス、MAC アドレスなどの情報が含まれます。BOOTP クライアントが BOOTP サーバに要求を送信すると、BOOTP サーバは BOOTP パラメータファイルを検索し、対応する設定情報を返信します。

一般的に BOOTP は安定した環境で使用します。ネットワーク環境が頻繁に変わる場合、DHCP が適しています。

DHCP サーバは BOOTP クライアントと相互に対応しています。そのため、BOOTP クライアントの IP アドレスを変更する場合、BOOTP サーバを使用しないで DHCP サーバを使用することができます。DHCP サーバは、IP アドレス割り当てシーケンスに基づいて BOOTP クライアントに IP アドレスを割り当てます。

16.2 動的IPアドレスの取得

BOOTP クライアントは以下のように BOOTP サーバから動的に IP アドレスを取得します。

1) BOOTP クライアントは自身の MAC アドレスを含めた、BOOTP 要求をブロードキャストします。
2) BOOTP サーバは、BOOTP 要求を受信するとクライアントの MAC アドレスに対応する IP アドレスの情報を検索します。
3) BOOTP サーバは BOOTP クライアントに BOOTP 応答を返信します。
4) BOOTP クライアントは受信した応答から IP アドレスを取得します。

DHCP サーバは BOOTP サーバの代わりに動的に IP アドレスを取得することができます。

16.3 プロトコルと標準

- RFC 951, *Bootstrap Protocol (BOOTP)*
- RFC 2132, *DHCP Options and BOOTP Vendor Extensions*
- RFC 1542, *Clarifications and Extensions for the Bootstrap Protocol*

16.4 インタフェースでBOOTPを使用したIPアドレスの取得の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． interface view に移行する	**interface** *interface-type interface-number*	―
3． インタフェースで BOOTP を使用した IP アドレスの取得を設定する	**ip address bootp-alloc**	デフォルト：設定なし

16.5 BOOTPクライアントの表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
BOOTPクライアント情報を表示する	**display bootp client** [**interface** *interface-type interface-number*]

目次

このセクションのページは **5-x-x** です。

17 章 DHCP スヌーピング 17-1
17.1 概要 17-1
17.1.1 トラステッドポートと非トラステッドポートのアプリケーション 17-1
17.1.2 DHCP snooping でのオプション 82 のサポート 17-2
17.2 DHCP snooping 設定作業リスト 17-3
17.3 DHCP snooping の基本機能の設定 17-3
17.4 オプション 82 の設定 17-4
17.5 DHCP snooping の表示と維持 17-5
17.6 DHCP snooping 設定例 17-5
17.6.1 DHCP snooping の基本機能の設定例 17-5

17章 DHCP スヌーピング

17.1 概要

DHCP スヌーピング（DHCP snooping）は、DHCP サーバと DHCP クライアント間でやりとりされる DHCP メッセージを監視して動的な IP ソースフィルタリングを行う機能です。本機能を利用することで、DHCP サーバを用いたネットワーク環境において、正当な DHCP クライアントにだけ IP 通信を許可することができる DHCP セキュリティ機能です。

セキュリティの目的から DHCP クライアントの IP アドレスと MAC アドレスバインディング（DHCP snooping エントリと呼ばれます）を記録します。

DHCP snooping は DHCP サーバと DHCP リレーエージェント間では動作しません。

DHCP snooping は許可された DHCP サーバからのみ IP アドレスを取得することができるように、トラステッド（trusted）ポートと非トラステッド（untrusted）ポートを定義します。

- **トラステッド（Trusted）** – DHCP メッセージを正常に転送し、DHCP クライアントが承認された DHCP サーバから IP アドレスを取得できることを確実にします。
- **非トラステッド（Untrusted）** – 不正な DHCP サーバからの IP アドレスの割り当てを防ぐため、受信した DHCP-ACK パケットまたは DHCP-OFFER パケットを廃棄します。

DHCP snooping は DHCP snooping エントリを作成するため、トラステッドポートから受信した DHCP-ACK メッセージと、DHCP-REQUEST メッセージを読み込みます。DHCP snooping エントリはクライアントの MAC アドレスと IP アドレス、DHCP クライアントに接続するポート、VLAN 情報を含みます。

DHCP snooping エントリを使用するため、以下の機能が必要となります。

- **ARP attack detection** – 承認されたクライアントからの ARP パケットかどうか、DHCP Snooping エントリにもとづいて決定します。この機能は、不正なクライアントからの ARP 攻撃を防ぐことができます。詳細は、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*15 セキュリティ*”の”*10 章 ARP アタックプロテクション*”を参照してください。

17.1.1 トラステッドポートと非トラステッドポートのアプリケーション

DHCP サーバに接続されているポートをトラステッドポートとして設定し、他のポートを非トラステッドポートとして設定します。

図 17-1 に示すように、DHCP サーバに接続している DHCP snooping 装置のポートをトラステッドポートとして設定します。トラステッドポートは DHCP サーバからクライアントに応答メッセージを転送します。許可されていない DHCP サーバに接続されている非トラステッドポートは入力した DHCP 応答メッセージを廃棄します。

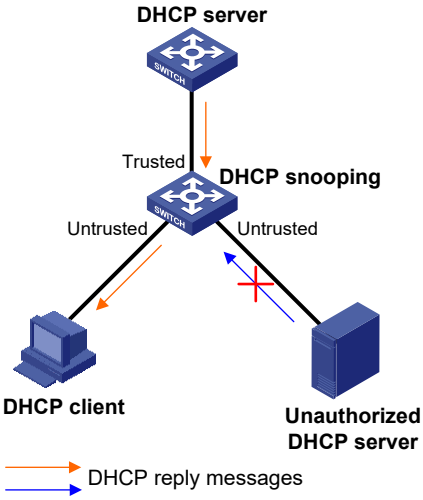


図 17-1 トラステッドポートと非トラステッドポート

図 17-2 に示すようなカスケードネットワーク構成では、DHCP サーバに面しているポートはトラステッドポートとして設定する必要があります。システムリソースを節約するため、直接 DHCP クライアントに接続されている非トラステッドポートのみが、DHCP snooping エントリを記録することができます。

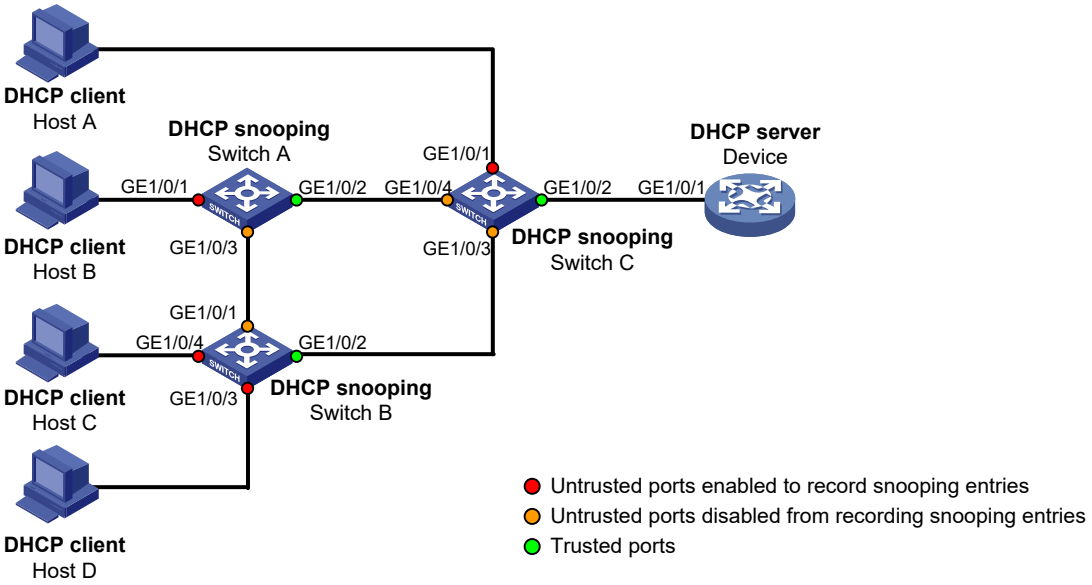


図 17-2 カスケードネットワーク構成のトラステッドポートと非トラステッドポート

17.1.2 DHCP snooping でのオプション 82 のサポート

オプション 82 は DHCP クライアントの位置情報を記録します。管理者はセキュリティとアカウンティングのため、DHCP クライアントを特定することができます。オプション 82

の詳細は、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*5 ネットワーク接続*”の”*12 章 DHCP の概要*”を参照してください。

DHCP snooping は表 17-1 に示すように、DHCP 要求メッセージのオプション 82 を処理するため、DHCP リレーエージェントと同様の処理を行います。DHCP サーバからの応答にオプション 82 が含まれている場合は、クライアントに応答を転送する前に DHCP Snooping 装置がオプション 82 を取り除きます。応答にオプション 82 が含まれていない場合、そのまま転送します。

表 17-1 DHCP snooping の動作

クライアントの要求メッセージに含まれるオプション	処理方法	DHCP Snooping の動作
Option 82	Append	オプション82を変更せずにメッセージを転送します。
	Drop	メッセージを破棄します。
	Keep	オプション82を変更せずにメッセージを転送します。
	Replace	もとのオプション82を設定されたパディング形式、パディングの内容、コードタイプに従って、新しいオプション82に置き換えてからメッセージを転送します。
No Option 82	ー	設定されたパディング形式、パディングの内容、コードタイプに従って、もとのオプション82に追加し、メッセージを転送します。

17.2 DHCP snooping設定作業リスト

アグリゲーショングループに接続されているレイヤ 2 Ethernet インタフェースに DHCP snooping を設定する場合、アグリゲーショングループからインタフェースを削除するまで設定は適用されません。

作業リスト
（必須設定項目） DHCP snoopingの基本機能の設定
（オプション設定項目） オプション82の設定

17.3 DHCP snoopingの基本機能の設定

DHCP snooping の基本機能の設定を行うとき、以下のガイドラインに従ってください。

- 許可された DHCP サーバに接続されているポートをトラステッドポートとして指定し、DHCP クライアントが確実に有効な IP アドレスを取得できるようにします。トラステッドポートと、DHCP クライアントに接続されているポートは同じ VLAN 内になければなりません。
- レイヤ 2 Ethernet インタフェースとアグリゲートインタフェースは、トラステッドポートとして指定できます。アグリゲートインタフェースの詳細は、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*5 ネットワーク接続*”の”*2 章 リンクアグリゲーション*”を参照してください。

- アグリゲーショングループに追加された Ethernet インタフェースで DHCP snooping の設定を行う場合、アグリゲーショングループからインタフェースが削除されるまで設定内容は適用されません。

以下に DHCP snooping の基本機能の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． DHCP snooping を有効にする	**dhcp snooping enable**	デフォルト：無効
3． interface view に移行する	**interface** *interface-type interface-number*	インタフェースはDHCPサーバに接続する必要があります。
4． トラステッドポートとしてポートを指定する	**dhcp snooping trust**	デフォルト：DHCP snooping が有効になった後、すべてのポートは非トラステッドポートとなります。
5． system view に戻る	**quit**	―
6． interface view に移行する	**interface** *interface-type interface-number*	インタフェースはDHCPクライアントに接続する必要があります。
7． （オプション設定項目） DHCP snooping エントリの記録を有効にする	**dhcp snooping binding record**	デフォルト：DHCP snooping が有効になった後、DHCP snoopingエントリの記録は無効です。

17.4 オプション82の設定

オプション 82 を設定するとき、以下のガイドラインに従ってください。

- アグリゲーショングループに追加された Ethernet インタフェースでオプション 82 の設定を行う場合、アグリゲーショングループからインタフェースが削除されるまで設定内容は適用されません。
- オプション 82 をサポートする場合、DHCP サーバと DHCP snooping 装置の両方でオプション 82 を設定する必要があります。DHCP サーバのオプション 82 の設定の詳細は、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*5 ネットワーク接続*”の”*13 章 DHCP サーバ*”を参照してください。
- オプション 82 がノードの装置名でパディングされる場合、装置名にスペースを含めることはできません。含まれている場合、DHCP Snooping が有効になっている装置はメッセージを破棄します。**sysname** コマンドを使用して装置名を指定することができます。コマンドの詳細は、QX-W2300AC シリーズアクセスコントローラコマンドマニュアルの“*3 システム管理*”の”*1 章 装置管理*”を参照してください。

以下にオプション 82 をサポートする DHCP snooping の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． interface view に移行する	**interface** *interface-type interface-number*	―
3． オプション 82 をサポートする DHCP snooping を有効にする	**dhcp snooping information enable**	デフォルト：無効

操作	コマンド	補足
4.　（オプション設定項目）オプション 82 が含まれている要求メッセージの処理方法を設定する	**dhcp snooping information strategy** { **append** | **drop** | **keep** | **replace** }	デフォルト：**replace**
5.　（オプション設定項目）サーキット ID サブオプションのパディング内容とコードタイプを設定する	**dhcp snooping information circuit-id** { [**vlan** *vlan-id*] **string** *circuit-id* | { **normal** | **verbose** [**node-identifier** { **mac** | **sysname** | **user-defined** *node-identifier* }] } [**format** { **ascii** | **hex** }] }	デフォルト：パディング内容は**normal**、サーキットIDサブオプションは**hex**です。
6.　（オプション設定項目）リモート ID サブオプションのパディング内容とコードタイプを設定する	**dhcp snooping information remote-id** { **normal** [**format** { **ascii** | **hex** }] | [**vlan** *vlan-id*] { **string** *remote-id* | **sysname** } }	デフォルト：パディング内容は**normal**、リモートIDサブオプションは**hex**です。

17.5 DHCP snoopingの表示と維持

すべての view で **display** コマンドを実行でき、user view で **reset** コマンドを実行できます。

操作	コマンド
DHCP snoopingエントリを表示する	**display dhcp snooping binding** [**ip** *ip-address* [**vlan** *vlan-id*]] [**verbose**]
DHCP Snooping装置でオプション82の設定に関する情報を表示する	**display dhcp snooping information** { **all** | **interface** *interface-type interface-number* }
DHCP Snooping装置のDHCPパケット統計情報を表示する	**display dhcp snooping packet statistics**
トラステッドポートの情報を表示する	**display dhcp snooping trust**
DHCP snoopingエントリを削除する	**reset dhcp snooping binding** { **all** | **ip** *ip-address* [**vlan** *vlan-id*] }
DHCP Snooping装置のDHCPパケット統計情報を削除する	**reset dhcp snooping packet statistics**

17.6 DHCP snooping設定例

17.6.1 DHCP snooping の基本機能の設定例

I. ネットワーク要件

図 17-3 に示すように設定します。

- GigabitEthernet 1/0/1 をトラステッドポートとして DHCP サーバに接続します。
- ほかのポートは非トラステッドポートとして設定します。

- DHCP サーバから応答を転送するため、許可されている DHCP サーバにのみ接続するように設定します。トラステッドポートから受信した DHCP-REQUEST メッセージと DHCP-ACK メッセージを確認することで、DHCP snooping がクライアントの IP-MAC バインディングを記録するようにします。

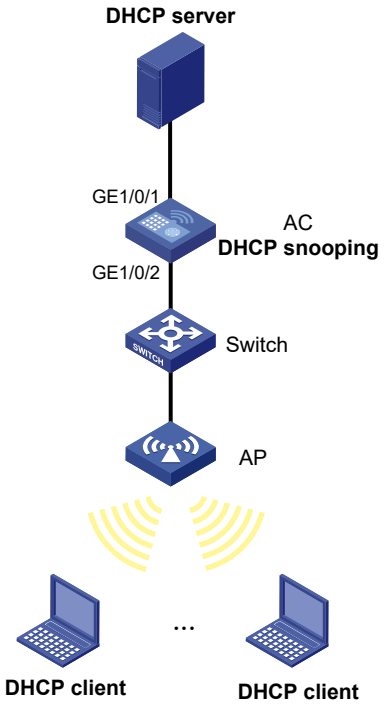


図 17-3 ネットワーク図

II. 設定手順

AC で WLAN アクセスの設定を行います。WLAN アクセスの設定については、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*6 WLAN アクセス*”の”*1 章 WLAN アクセス*”を参照してください。（詳細は省略します。）

DHCP snooping を有効にします。

```
<AC> system-view
[AC] dhcp snooping enable
```

トラステッドポートとして GigabitEthernet 1/0/1 を設定します。

```
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] dhcp snooping trust
[AC-GigabitEthernet1/0/1] quit
```

GigabitEthernet 1/0/2 でクライアントの IP-MAC バインディングを記録することを有効にします。

```
[AC] interface gigabitethernet 1/0/2
[AC-GigabitEthernet1/0/2] dhcp snooping binding record
[AC-GigabitEthernet1/0/2] quit
```

III. 設定の確認

DHCP クライアントは許可された DHCP サーバからのみ IP アドレスと他の設定パラメータを取得できることを確認します。（詳細は省略します。）

クライアントの記録された DHCP snooping エントリを表示します。

```
[AC] display dhcp snooping binding
```

目次

このセクションのページは **5-x-x** です。

18 章 DNS 18-1
18.1 概要 18-1
18.1.1 スタティックドメイン名解決 18-1
18.1.2 DNS サーバベースのダイナミックドメイン名解決 18-1
18.1.3 DNS プロキシ 18-3
18.2 DNS 設定作業リスト 18-4
18.3 IPv4 DNS クライアントの設定 18-4
18.3.1 DNS クライアントのドメイン名解決 18-4
18.3.2 スタティックドメイン名解決の設定 18-4
18.3.3 DNS サーバベースのダイナミックドメイン名解決の設定 18-5
18.4 DNS プロキシの設定 18-5
18.4.1 DNS プロキシの有効化 18-5
18.4.2 DNS サーバアドレスの指定 18-6
18.5 送信される DNS パケットの DSCP 値の設定 18-6
18.6 IPv4 DNS の表示と維持 18-6
18.7 IPv4 DNS 設定例 18-7
18.7.1 スタティックドメイン名解決の設定例 18-7
18.7.2 ダイナミックドメイン名解決の設定例 18-8
18.7.3 DNS プロキシの設定例 18-11
18.8 IPv4 DNS 設定のトラブルシューティング 18-13
18.8.1 症状 18-13
18.8.2 解決策 18-13

18章 DNS

18.1 概要

DNS（Domain Name System）は、DNS サーバから DNS プロトコルを介してホスト名を IP アドレスにマッピングできる分散データベースです。各固有の IP アドレスには、ホスト名を関連付けることができます。

ドメイン名－IP アドレスのマッピングは DNS エントリと呼ばれます。

DNS サービスには、スタティックとダイナミックの 2 種類があります。ユーザが名前を指定したのち、装置はスタティックの名前解決のデータベースで IP アドレスを調べます。有効な IP アドレスがない場合、ダイナミック（動的）な名前を解決するために DNS サーバに問い合わせを行います。これは、スタティック（静的）な名前解決のときよりも時間がかかります。そこで効率化のために、よく照会される名前と IP アドレスのマッピングがローカルのスタティックな名前解決のデータベーステーブルに保存されています。

18.1.1 スタティックドメイン名解決

スタティックドメイン名解決は、ドメイン名と IP アドレスの間にマッピングを手動でマッピングを作成します。たとえば、Telnet などのアプリケーションを使用する際に、装置のスタティックドメイン名解決のマッピングを作成することができます。

18.1.2 DNS サーバベースのダイナミックドメイン名解決

I. 解決手段

1) ユーザプログラムは、DNS クライアントの解決者にネームクエリを送信します。
2) DNS の解決者は、ローカルでドメイン名を適合させるためにキャッシュを調べます。適合するものがあれば、それに対応する IP アドレスを返送します。適合するものがなければ、DNS サーバにネームクエリを送信します。
3) DNS サーバはドメイン名を適合させるために名前解決のデータベースを調べます。適合するものがなければ、他のより高レベルの DNS サーバにネームクエリを送信します。このプロセスは、結果（成功、もしくは失敗）が返ってくるまで続けられます。
4) DNS サーバから応答を受信した後、DNS クライアントはユーザプログラムに解決結果を返信します。

図 18-1 に、ユーザプログラム、DNS クライアントおよび DNS サーバ間の関係を示しています。

解決者（Resolver）とキャッシュ（Cache）は DNS クライアントによって構成されます。通常、ユーザプログラムと DNS クライアントは同じ装置あるいは異なる装置で動作しますが、DNS サーバと DNS クライアントが異なる装置間で動作します。

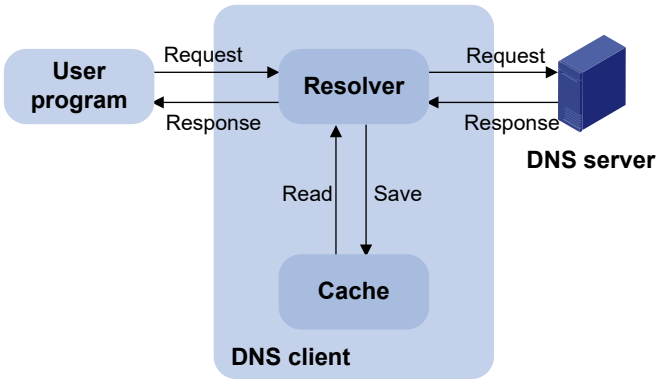


図 18-1 ダイナミックドメイン名解決

ダイナミックドメイン名解決は、DNS クライアントがダイナミックドメイン名のキャッシュに、DNS エントリを格納するようにします。有効期間内に度重なるクエリ用に DNS 要求を DNS サーバに送信する必要はありません。有効期間が満了したとき、DNS サーバからのエントリが最新であることを確認するため、DNS エントリを削除します。DNS サーバはマッピングの有効な期間を決定します。DNS クライアントは DNS 応答からエージング情報を取得します。

II. DNS サフィックス

DNS クライアントは、通常、ユーザによって定義することのできるサフィックスのリストを保持します。それは解決する名前が完全に一致しないときに使用します。解決者は不明な部分を提供することができます。

たとえば、ユーザは example.com のためのサフィックスとして **com** を設定することができます。これによって、ユーザは、**example** を入力するだけで example.com の IP アドレスを取得することができます。解決者は DNS サーバに名前を通過させる前に、サフィックスとデリミタ（区切り記号）を付加します。

名前解決は、ユーザが入力したドメインネームにもとづくクエリを処理します。

- ユーザがドット（.）なしでドメイン名を入力した場合（たとえば example）、解決者は、ホスト名と認識し、処理する前にホスト名に DNS サフィックスを追加します。すべての DNS の検索に失敗した場合、解決者は、IP アドレスのクエリのためにユーザが入力したドメイン名（たとえば example）を使用します。
- 文字の間にドメイン名にドット（.）がある場合（たとえば www. example）、解決者は、最初に DNS の検索を行うために、このドメイン名を直接使用します。DNS の検索に失敗した場合、解決者は、他の DNS を検索するために DNS サフィックスを追加します。
- ドメイン名の末尾にドット（.）がある場合（たとえば、example.com.）、解決者は、ドメイン名を FQDN（Fully Qualified Domain Name、完全修飾ドメイン名）と認識し、クエリが正常に処理されたかエラーが発生したか、結果が解決者から返信されます。このため、ドメイン名末尾のドット（.）は終端記号と認識されます。

装置は、スタティック DNS サービスおよびダイナミック DNS サービスをサポートしています。

DNS サーバでドメイン名にエイリアスが設定されている場合、そのエイリアスをホストの IP アドレスに変換できます。

18.1.3 DNS プロキシ

図 18-2 に示すように、DNS プロキシは以下のように動作します。

- DNS クライアント（DNS client）は DNS プロキシ（DNS proxy）に DNS 要求を送信します。
- DNS プロキシから指定された DNS サーバ（DNS server）に転送されます。DNS サーバからの応答は DNS プロキシを通して DNS クライアントに送信されます。

DNS プロキシは、ネットワーク管理を容易にします。DNS サーバのアドレスが変更された場合、DNS プロキシの設定を変更するだけで、各 DNS クライアントの設定を変更する必要がなくなります。

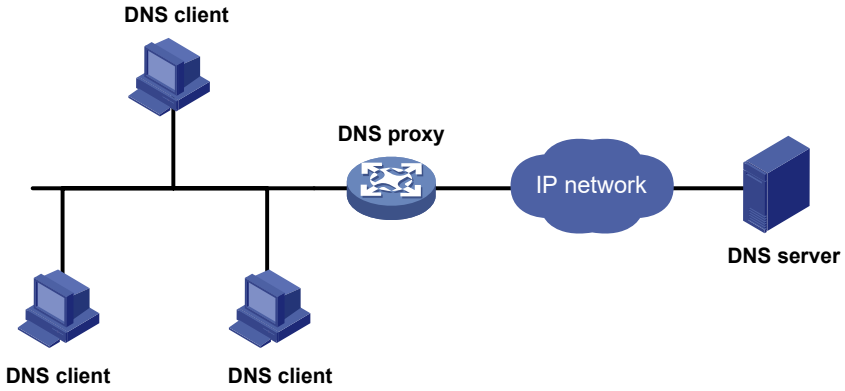


図 18-2 DNS プロキシアプリケーション

DNS プロキシは以下のように動作します。

1) DNS クライアントは DNS プロキシを DNS サーバと認識し、DNS プロキシに DNS 要求を送信します。つまり、要求の宛先アドレスは DNS プロキシの IP アドレスです。
2) DNS プロキシは、要求を受信すると、ローカルスタティックドメイン名解決テーブルおよびダイナミックドメイン名解決テーブルを検索します。要求された情報がテーブル内にあれば、DNS プロキシはクライアントに DNS 応答を返します。
3) 要求された情報が見つからない場合、DNS プロキシは以下のように要求を転送します。

a) 一致するドメイン名ルールが存在する場合、プロキシはそのルールにバインドされたDNSサーバグループ内のDNSサーバに要求を転送します。

b) 一致するDNSサーバグループが存在せず、DNSサーバが指定されている場合、DNSプロキシはドメイン名解決のためにDNSサーバに要求を送信します。

4) DNS サーバから応答を受け取ると、DNS プロキシは IP アドレス－ドメイン名のマッピングを記録し、応答を DNS クライアントに転送します。

DNS サーバが存在しない、あるいは、指定された DNS サーバへのルートがない場合、DNS プロキシは DNS 要求を転送しません。

18.2 DNS設定作業リスト

作業リスト
（必須設定項目） IPv4 DNSクライアントの設定
（オプション設定項目） DNSプロキシの設定
（オプション設定項目） 送信されるDNSパケットのDSCP値の設定

18.3 IPv4 DNSクライアントの設定

18.3.1 DNS クライアントのドメイン名解決

以下の方法を使用して、DNS クライアントでドメイン名とアドレスのマッピングを作成できます。

- **スタティックドメイン名解決の設定** – ドメイン名で少数の装置にアクセスする場合、またはネットワークに使用可能な DNS サーバがない場合は、この方法を使用します。ネットワーク管理者は、ドメイン名とアドレスのマッピングを手動で設定または維持する必要があります。
- **ダイナミックドメイン名解決の設定** – ドメイン名で多数の装置にアクセスし、ネットワークに使用可能な DNS サーバがある場合は、この方法を使用します。ダイナミックドメイン名解決には、DNS サーバベースのドメイン名解決と DNS サーバグループベースのドメイン名解決が含まれます。

DNS クライアントは、以下の順序でドメイン名を解決します。

1) 解決済みのローカルに保存された DNS マッピング
2) スタティックドメイン名解決
3) DNS サーバベースのドメイン名解決

これらの方法をすべて使用した後でドメイン名を解決できない場合、解決は失敗します。

18.3.2 スタティックドメイン名解決の設定

スタティックドメイン名解決は、IPv4 アドレスの代わりにホスト名を使用してホストに接続する Telnet のようなアプリケーションを提供します。

スタティックドメイン名解決の設定を行うとき、以下のガイドラインに従ってください。

- 各ホスト名は 1 つの IPv4 アドレスのみ割り当てられます。既にホスト名に割り当てられた IPv4 アドレスがある場合、最後に行われた設定が適用されます。
- IPv4 DNS エントリを最大 1024 まで設定することができます。

以下にスタティックドメイン名解決の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	–
2. スタティック名前解決テーブルでホスト名と IPv4 アドレスの間のマッピングを設定する	**ip host** *host-name ip-address*	デフォルト：設定なし

18.3.3 DNS サーバベースのダイナミックドメイン名解決の設定

ダイナミックドメイン名解決を使用する場合、正しいサーバに DNS クエリを送信できるように DNS サーバを設定します。DNS サーバは DHCP を通して動的に取得した設定よりも、手動の設定が優先されます。複数設定を行った場合、最初に行った設定が優先されます。最初に最も高い優先度の DNS サーバにドメイン名解決リクエストを送信します。DNS サーバからの応答がない場合、順番に、2 番目の優先度のドメイン名解決リクエストが DNS サーバに送信されます。

加えて、取得したドメイン名を、システムが自動で追加するように DNS サフィックスを設定することができます。DNS サフィックスは DHCP を通して動的に取得した設定よりも、手動での設定が優先されます。複数設定を行った場合、最初に行った設定が優先されます。DNS 解決者は最初に最も高い優先度のサフィックスを使用します。名前解決に失敗した場合、順番に、2 番目の優先度のサフィックスを使用します。

I. 設定ガイドライン

ダイナミックドメイン名解決の設定を行うとき、以下のガイドラインに従ってください。

- DNS サーバは最大 6 台まで設定することができます。
- DNS サフィックスは最大 16 まで設定できます。

II. 設定手順

以下にダイナミックドメイン名解決の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. DNS サーバの IP アドレスを設定する	• system viewのDNSサーバアドレスを指定する **dns server** ip-address • interface viewのDNSサーバアドレスを指定する **interface** *interface-type interface-number* **dns server** *ip-address*	デフォルト：設定なし
3. （オプション設定項目） ドメイン名のサフィックスを設定する	**dns domain** *domain-name*	デフォルト：設定なし 定義済みのドメイン名のみ解決します。

18.4 DNSプロキシの設定

18.4.1 DNS プロキシの有効化

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. DNS プロキシを有効にする	**dns proxy enable**	デフォルト：無効

18.4.2 DNS サーバアドレスの指定

複数の DNS サーバを指定することができます。DNS プロキシは最も高い優先度の DNS サーバに要求を転送します。もし DNS サーバから応答がない場合、2 番目以降の優先度の DNS サーバに要求を転送します。

以下に DNS サーバアドレスの指定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. DNS サーバのアドレスを指定する	• system viewのDNSサーバアドレスを指定する **dns server** *ip-address* • interface viewのDNSサーバアドレスを指定する **interface** *interface-type interface-number* **dns server** *ip-address*	デフォルト：指定なし

18.5 送信されるDNSパケットのDSCP値の設定

パケットの DSCP は、パケットの優先度レベルを指定し、パケットの優先度に影響します。DSCP が高いほど、優先度が高くなります。

以下に出力される DNS パケットの DSCP の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. 出力される DNS パケットの DSCP 値を設定する	**dns dscp** *dscp-value*	デフォルト：0 この設定はDNSクライアント、DNSプロキシの装置で有効です。

18.6 IPv4 DNSの表示と維持

すべての view で **display** コマンドを実行でき、user view で **reset** コマンドを実行できます。

操作	コマンド
ドメイン名解決テーブルを表示する	**display dns host** [**ip**]
IPv4 DNSサーバ情報を表示する	**display dns server** [**dynamic**]
DNSサフィックスを表示する	**display dns domain** [**dynamic**]
ダイナミックドメイン名キャッシュの情報を削除する	**reset dns host** [**ip**]

18.7 IPv4 DNS設定例

18.7.1 スタティックドメイン名解決の設定例

I. ネットワーク要件

図 18-3 に示すように、AC は IP アドレスよりも、覚えやすいドメイン名を使用して、Host にアクセスします。

ドメイン名 host.com で IP アドレス 10.1.1.2 のホストにアクセスできるように、AC にスタティックドメイン名解決の設定を行います。

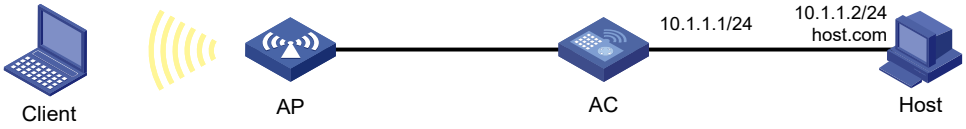


図 18-3 ネットワーク図

II. 設定手順

AC で WLAN アクセスの設定を行ってください。詳細は QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*6 WLAN アクセス*”の”*1 章 WLAN アクセス*”を参照してください。（詳細は省略します。）

ホスト名 host.com と IP アドレス 10.1.1.2 のマッピングを設定します。

```
<AC> system-view
[AC] ip host host.com 10.1.1.2
```

ping host.com コマンドを使用します。Device がスタティックドメイン名解決により、host.com に対応する IP アドレスの 10.1.1.2 を取得できることを確認します。

```
[AC] ping host.com
Ping host.com (10.1.1.2): 56 data bytes, press CTRL_C to break
56 bytes from 10.1.1.2: icmp_seq=0 ttl=255 time=1.000 ms
56 bytes from 10.1.1.2: icmp_seq=1 ttl=255 time=1.000 ms
56 bytes from 10.1.1.2: icmp_seq=2 ttl=255 time=1.000 ms
56 bytes from 10.1.1.2: icmp_seq=3 ttl=255 time=1.000 ms
56 bytes from 10.1.1.2: icmp_seq=4 ttl=255 time=2.000 ms

--- Ping statistics for host.com ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.000/1.200/2.000/0.400 ms
```

18.7.2 ダイナミックドメイン名解決の設定例

I. ネットワーク要件

図 18-4 に示すように、AC を以下のように設定します。

- IP アドレスよりも、覚えやすいドメイン名を使用して Host にアクセスします。
- ダイナミック DNS を使用し、DNS Server に IP アドレスの要求を行います。

DNS Server の IP アドレスは 2.1.1.2/16 で、ドメインは com で、IP アドレス 3.1.1.1/16 とドメイン名 host のマッピングは com に保存されます。

DNS client として動作する AC でダイナミック DNS、DNS サフィックス com を設定します。AC は、AC がドメイン名 host.com と IP アドレス 3.1.1.1/16 で Host にアクセスできるように設定します。

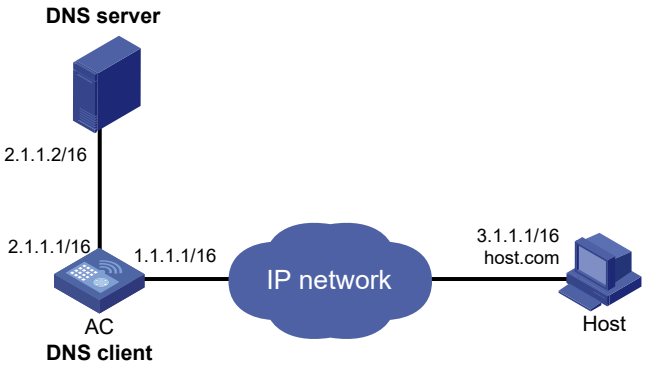


図 18-4 ネットワーク図

設定を行う前に、以下を確認してください。

- AC とホストは相互に通信可能であることを確認してください。
- インタフェースの IP アドレスが、図 18-4 に示すように設定されていることを確認してください。

設定は DNS サーバによって異なります。以下の設定は、Windows 2008 R2 サーバで行われています。

II. 設定手順

1) AC で WLAN アクセスの設定を行ってください。詳細は QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*6 WLAN アクセス*”の”*1 章 WLAN アクセス*”を参照してください。
2) DNS server を設定します。

a) “Start” > “Programs” > “Administrative Tools” > “DNS”を選択します。図 18-5に示すようにDNS serverの設定ページが表示されます。

b) “Forward Lookup Zones”を右クリックし、“New zone”を選択します。指示に従って、新しいゾーンcomを作成します。

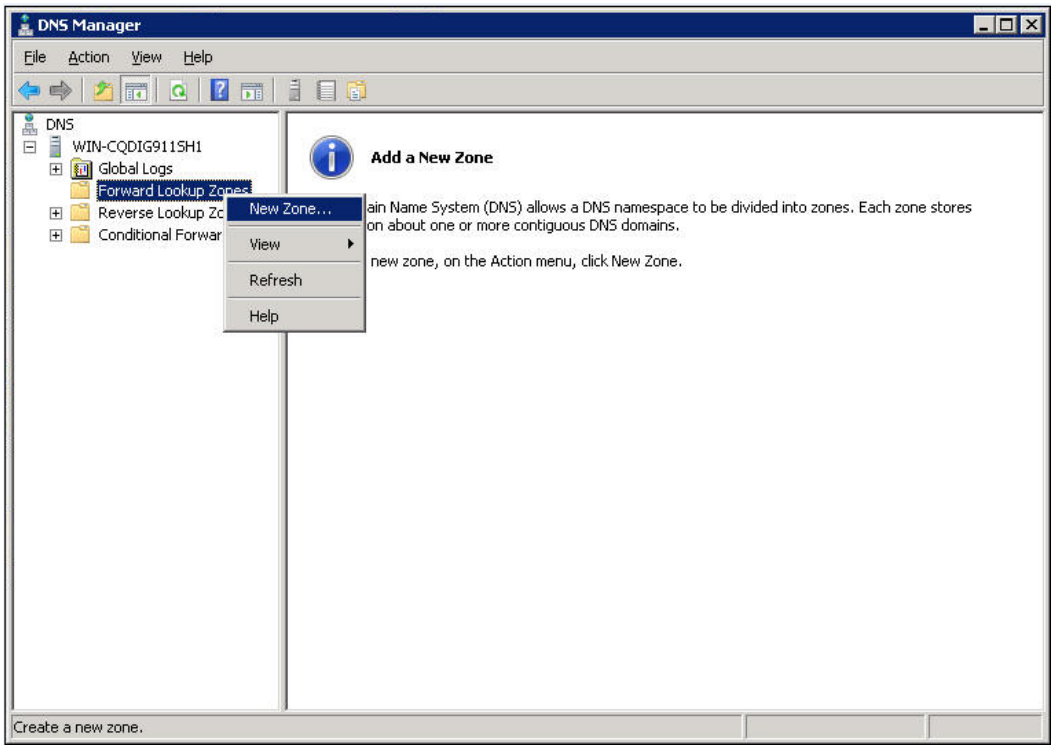


図 18-5 ゾーンの作成

c) DNS server設定ページで、ゾーンcomを右クリックし、“New Host”を選択します。

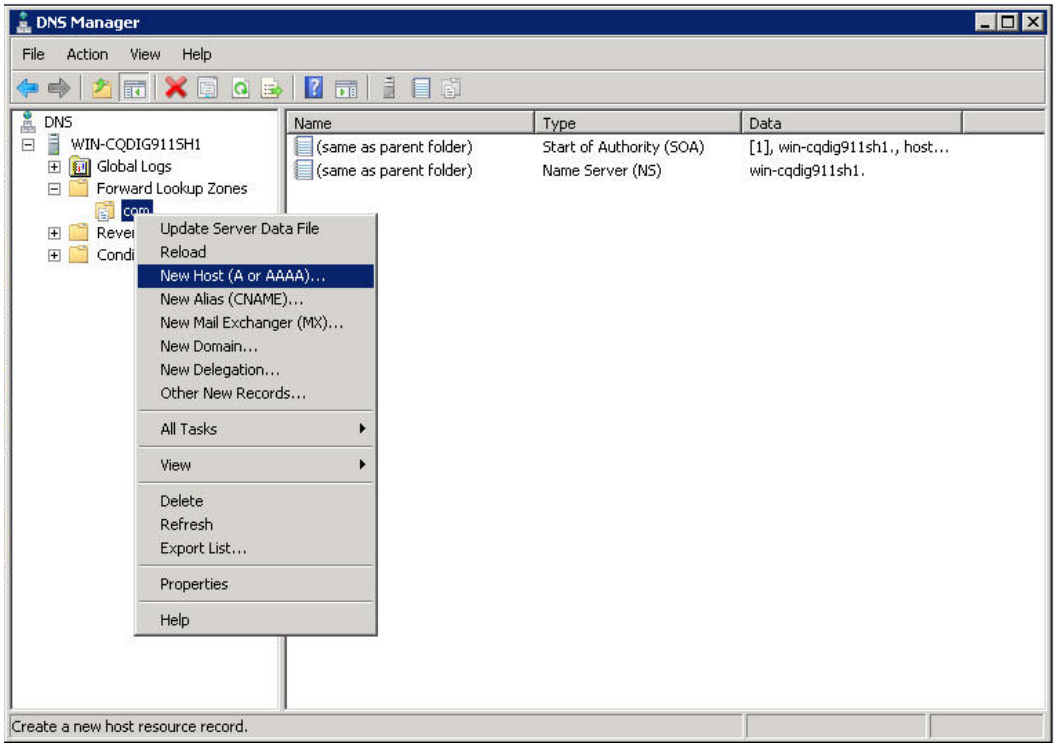


図 18-6 ホストの追加

d)　ダイアログボックスで、ホスト名host、IPアドレス3.1.1.1を入力します。

e)　“Add Host”をクリックします。IPアドレスとホスト名間のマッピングが作成されます。

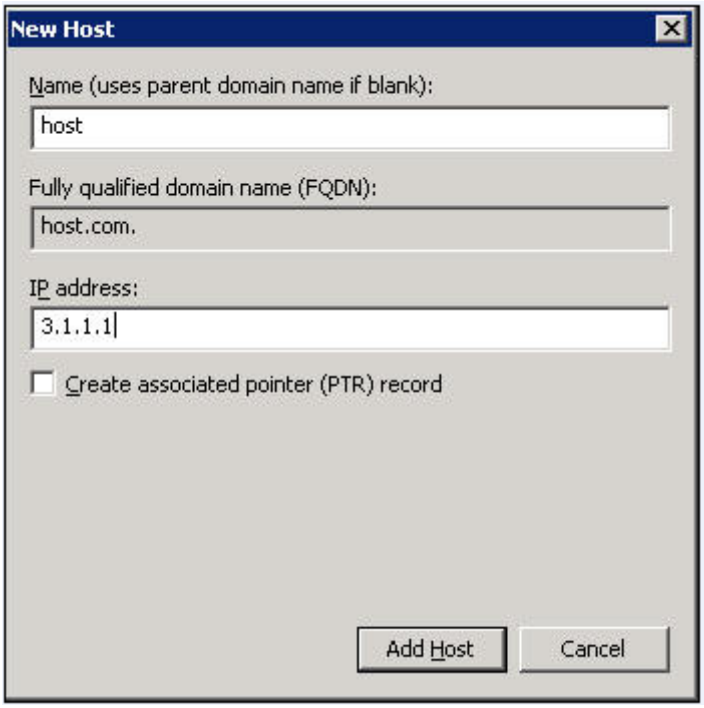


図 18-7 IP アドレスとホスト名間のマッピングの作成

3) DNS client を設定します。

IP アドレスとして 2.1.1.2 を指定します。

```
<AC> system-view
[AC] dns server 2.1.1.2
```

#ドメイン名のサフィックスとして com を設定します。

```
[AC] dns domain com
```

III. 設定の確認

Device で **ping** host コマンドを使用します。Device と host 間の通信が正常であり、ドメイン名 host.com に対応する宛先 IP アドレスが 3.1.1.1 であることを確認します。

18.7.3 DNS プロキシの設定例

I. ネットワーク要件

図 18-8 に示すように DNS client と DNS Server 間で DNS パケットを転送する DNS プロキシとして AC を設定します。DNS Server の IP アドレスは 4.1.1.1 です。

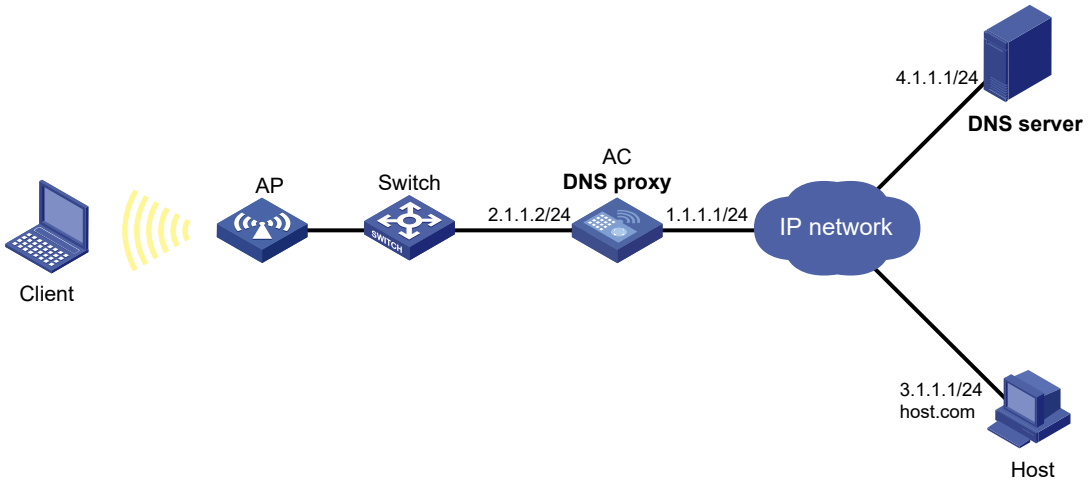


図 18-8 ネットワーク図

II. 設定手順

設定を行う前に、以下のことを確認してください。

- AC と DNS Server、Host の間が互いに通信可能であることを確認してください。
- インタフェースの IP アドレスが、図 18-8 に示すように設定されていることを確認してください

1) AC で WLAN アクセスの設定を行ってください。詳細は QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*6 WLAN アクセス*”の”*1 章 WLAN アクセス*”を参照してください。（詳細は省略します。）

2) DNS サーバを設定します。

この設定は DNS サーバによって異なります。Windows サーバを DNS サーバとして使用する場合、本章の *“ダイナミックドメイン名解決の設定例”* を参照してください。

3) DNS proxy を設定します。

DNS Server の IP アドレスとして、4.1.1.1 を指定します。

```
<AC> system-view
[AC] dns server 4.1.1.1
```

DNS プロキシを有効にします。

```
[AC] dns proxy enable
```

4) DNS client を設定し、DNS Server の IP アドレスとして、2.1.1.2 を指定します。（詳細は省略します。）

III. 設定の確認

AC 機能上で DNS プロキシが有効であることを確認します。

```
C:\Users\ss> ping host.com
Ping host.com (3.1.1.1): 56 data bytes, press CTRL_C to break
56 bytes from 3.1.1.1: icmp_seq=0 ttl=255 time=1.000 ms
```

```
56 bytes from 3.1.1.1: icmp_seq=1 ttl=255 time=1.000 ms
56 bytes from 3.1.1.1: icmp_seq=2 ttl=255 time=1.000 ms
56 bytes from 3.1.1.1: icmp_seq=3 ttl=255 time=1.000 ms
56 bytes from 3.1.1.1: icmp_seq=4 ttl=255 time=2.000 ms

--- Ping statistics for host.com ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.000/1.200/2.000/0.400 ms
```

18.8 IPv4 DNS設定のトラブルシューティング

18.8.1 症状

ダイナミックドメイン名解決を有効にした後、ユーザが正しい IP アドレスを取得することができません。

18.8.2 解決策

1) **display dns host ip** コマンドを使用して、指定されたドメイン名がキャッシュにあることを確認してください。
2) 定義済みのドメイン名がない場合、ダイナミックドメイン名解決を有効にし、DNS クライアントと DNS サーバ間の通信が可能なことを確認してください。
3) キャッシュに特定のドメイン名はあっても、IP アドレスが正しくない場合、DNS クライアントが DNS サーバの正しい IP アドレスであることを確認してください。
4) DNS サーバのドメイン名と IP アドレス間のマッピングが正しいことを確認してください。

目次

このセクションのページは**5-x-x** です。

19章 HTTP 19-1
19.1 HTTP 19-1
19.2 制限とガイドライン 19-1
19.3 HTTPサービスの設定 19-1
19.4 HTTPSサービスの設定 19-1
19.5 HTTPの表示と維持 19-3

19章 HTTP

19.1 HTTP

この装置は、HTTP 1.0、HTTP 1.1、および HTTPS をサポートする組み込み Web サーバを提供します。

Hypertext Transfer Protocol (HTTP) は、インターネット上の Web ページ情報を転送するために使用されます。TCP/IP プロトコルスタックで TCP を使用するアプリケーションレイヤプロトコルです。

Hypertext Transfer Protocol Secure (HTTPS) は HTTP をベースとしており、HTTP よりも安全です。SSL を使用して、クライアントとサーバ間で交換されるデータの完全性とセキュリティを確保します。証明書ベースのアクセスコントロールポリシーを定義して、合法的なクライアントのみに HTTPS サービスの使用を許可できます。

19.2 制限とガイドライン

装置のセキュリティを向上させるため、HTTP サービスを有効にすると、HTTPS サービスが自動的に有効になります。HTTP サービスが有効になっている場合、HTTPS サービスを無効にすることはできません。

19.3 HTTPサービスの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. HTTP サービスを有効にする	**ip http enable**	デフォルト：無効
3. （オプション設定項目）HTTP サービスのポート番号を指定する	**ip http port** *port-number*	デフォルト：80
4. （オプション設定項目）HTTP サービスに ACL を適用する	**ip http acl** { *acl-number* | **name** *acl-name* }	デフォルト：設定なし

19.4 HTTPSサービスの設定

装置は以下の HTTPS サービスモードをサポートしています。

- **簡易モード**– 装置で HTTPS サービスを有効にすると、装置は簡易モードで動作します。装置は自己署名証明書 (装置自体によって生成および署名される証明書) とデフォルトの SSL 設定を使用します。HTTPS サービスに関連付けられた SSL サーバポリシーはありません。ただし、証明書が信頼できる CA によって発行されていないため、ブラウザは自己署名証明書を信頼しません。HTTPS を使用して装置にアクセス

すると、ブラウザはセキュリティリスクメッセージを表示します。セキュリティリスクに寛容な場合は、メッセージを無視してアクセスを続行できます。

- **セキュアモード**– 装置は CA によって署名されたローカル証明書と、一連のユーザ定義のセキュリティ保護設定を使用して、セキュリティを確保します。装置をセキュアモードで動作させるには、以下のタスクを実行する必要があります。
  - □ PKI ドメイン関連のパラメータを設定します。
  - □ CA 証明書を取得し、CA にローカル証明書を要求します。
  - □ SSL サーバポリシーを設定し、ポリシーを HTTPS サービスに関連付けます。
  - □ 装置で HTTPS サービスを有効にします。

⚠ **重要**:

セキュアモードを使用するには、最初に公式のサードパーティ CA から SSL 用のローカル証明書を購入する必要があります。NEC は装置の認証局によって署名された CA 証明書を提供しません。

簡易モードは簡単に設定できますが、安全ではありません。安全モードは安全ですが、設定が複雑です。

SSL、自己署名証明書、ローカル証明書、および PKI の詳細は、QX-W シリーズ Web 認証(ポータル認証) オペレーションマニュアルの”*3 章 PKI 設定*”を参照してください。

I. 制限とガイドライン

- 別の SSL サーバポリシーを HTTPS サービスに関連付けるには、以下のタスクを実行する必要があります。
  - □ 新しい SSL サーバポリシーを関連付ける前に、HTTP サービスと HTTPS サービスを無効にします。
  - □ アソシエーションの後で、HTTP サービスと HTTPS サービスを再度有効にします。

  必要なタスクを完了できなかった場合、新しい SSL サーバポリシーは有効になりません。
- SSL サーバポリシーを HTTPS サービスに関連付けた後に HTTP サービスが自己署名証明書を使用するには、以下の手順を実行する必要があります。

a) HTTPサービスとHTTPSサービスを無効にします。

b) HTTPサービスとHTTPSサービスを再度有効にします。

- HTTPS サービスを有効にすると、SSL ハンドシェイク ネゴシエーションプロセスがトリガーされます。
  - □ 装置にローカル証明書がある場合、SSL ハンドシェイク ネゴシエーションは成功し、HTTPS サービスが起動します。
  - □ 装置にローカル証明書がない場合、証明書適用プロセスが開始されます。証明書適用プロセスに時間がかかるため、SSL ハンドシェイク ネゴシエーションが失敗し、HTTPS サービスが開始されない場合があります。この問題を解決するには、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。
- 証明書ベースのアクセスコントロールポリシーを使用して HTTPS アクセスを制御するには、以下のタスクを実行する必要があります。
  - □ 証明書ベースのアクセスコントロールポリシーの許可ルールを 1 つ以上設定します。

必要なタスクを完了できなかった場合、HTTPS クライアントはログインできません。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. HTTPS サービスを有効にする	**ip https enable**	デフォルト：無効
3. （オプション設定項目）HTTPS サービスポート番号を指定する	**ip https port** *port-number*	デフォルト：443
4. （オプション設定項目）HTTPS サービスに ACL を適用する	**ip https acl** {*acl-number* | **name** *acl-name* }	デフォルト：設定なし

19.5 HTTPの表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
HTTPサービス設定およびステータス情報を表示する	**display ip http**
HTTPSサービスの設定およびステータス情報を表示する	**display ip https**

目次

このセクションのページは **5-x-x** です。

20 章 IP パフォーマンスの最適化 20-1
20.1 ダイレクトブロードキャスト転送の有効化 20-1
20.1.1 設定手順 20-1
20.1.2 設定例 20-1
20.2 インタフェースの MTU サイズの設定 20-2
20.3 TCP path MTU discovery の設定 20-3
20.4 TCP バッファサイズの設定 20-4
20.5 TCP タイマの設定 20-4
20.6 ICMP エラーパケットの送信設定 20-5
20.7 ICMP エラーメッセージのレートリミットの設定 20-6
20.8 IP パフォーマンスの最適化の表示と維持 20-7

20章 IP パフォーマンスの最適化

装置の設定を最適化することで、IP パフォーマンス全体を最適にすることができます。この章では設定を最適化するための、さまざまな技術について記載します。

ルータという用語は、ルーティング対応装置を指します。

20.1 ダイレクトブロードキャスト転送の有効化

この処理により、インタフェース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を転送できます。

ダイレクトブロードキャストパケットは、特定の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の宛先 IP アドレスでは、ネットワーク ID によって宛先ネットワークを識別され、ホスト ID はすべて 1 で構成されます。

20.1.1 設定手順

以下に、インタフェースで、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の転送を有効にする設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. interface view に移行する	**interface** *interface-type interface-number*	―
3. 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の転送を有効にする	**ip forward-broadcast**	デフォルト：無効

20.1.2 設定例

I. ネットワーク要件

図 20-1 に示すように、Host のデフォルトゲートウェイは AC の VLAN インタフェース 3 の IP アドレス 1.1.1.2/24 です。

Server が Host から IP アドレス 2.2.2.255 にダイレクトブロードキャストを受信できるようにするため、VLAN インタフェース 2 が直接接続されたネットワークへのブロードキャストを転送できるように有効にします。

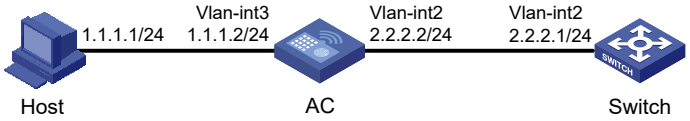


図 20-1 ネットワーク図

II. 設定手順

1)　VLAN インタフェース 2、VLAN インタフェース 3 の IP アドレスを設定します。

```
<AC> system-view
[AC] interface vlan-interface 3
[AC-Vlan-interface3] ip address 1.1.1.2 24
[AC-Vlan-interface3] quit
[AC] interface vlan-interface 2
[AC-Vlan-interface2] ip address 2.2.2.2 24
```

2)　VLAN インタフェース 2 で直接接続されたネットワークのダイレクトブロードキャストの転送を有効にします。

```
[AC -Vlan-interface2] ip forward-broadcast
```

3)　Switch を設定します。

ホストへのスタティックルートを設定します。

```
<Switch> system-view
[Switch] ip route-static 1.1.1.1 24 2.2.2.2
```

VLAN インタフェース 2 の IP アドレスを設定します。

```
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ip address 2.2.2.1 24
```

VLAN インタフェース 2 で直接接続されたネットワークのダイレクトブロードキャストの受信を有効にします。

```
[Switch-Vlan-interface2] ip forward-broadcast
```

設定を行った後、ホストでサブネットに直接接続されたブロードキャストアドレス 2.2.2.255 に ping を行った場合、Switch の VLAN インタフェース 2 は ping パケットを受信できます。Switch で **ip forward-broadcast** コマンドの設定を削除した場合、インタフェースは ping パケットを受信することができません。

20.2 インタフェースのMTUサイズの設定

IPv4 パケットが出力インタフェースの MTU サイズを超えたとき、装置は以下のどちらかの処理を行います。

- 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。

以下にインタフェースの MTU サイズの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． interface view に移行する	**interface** *interface-type interface-number*	―
3． インタフェースの MTU サイズを設定する	**ip mtu** *mtu-size*	デフォルト：設定なし

20.3 TCP path MTU discoveryの設定

⚠ **重要**：

TCP 経路のすべての装置は **ip unreachables enable** コマンドを使用して、ICMP エラーメッセージの送信を有効にする必要があります。

TCP path MTU discovery（RFC1191）は、TCP 接続の送信元と宛先間の経路 MTU を探索します。以下のように動作します。

1) TCP 送信元の装置はフラグメント禁止（DF）ビットを設定して、パケットを送信します。
2) ルータは、出力インタフェースで MTU サイズを超過したパケットを廃棄します。出力インタフェースの MTU サイズが含まれた ICMP エラーメッセージを送信します。
3) ICMP エラーメッセージを受信した TCP 送信元の装置は、TCP 接続の現在の経路 MTU を計算します。
4) TCP 送信元の装置は、MSS よりも小さい TCP セグメントの次のパケットを送信します。（MSS ＝ 経路 MTU － IP ヘッダ長 － TCP ヘッダ長）

MSS が 32 バイトよりも小さい状態で、もし TCP 送信元の装置が ICMP エラーメッセージを受信する場合、TCP 送信元の装置はパケットをフラグメントします。

RFC1191 をサポートしていないルータから ICMP エラーメッセージを受信した場合、出力インタフェースの MTU は 0 に設定されます。ICMP エラーメッセージを受信した際、TCP 送信元の装置は、RFC1191 に記載されているように TCP MSS を計算するため、MTU テーブルから、現在の経路 MTU よりも小さい経路 MTU を選択します。MTU テーブルは、68、296、508、1006、1280、1492、2002、4352、8166、17914、32000、65535 バイトの MTU 値を含んでいます。最小 TCP MSS の値はシステムで 32 バイトと決められているため、実際の最小 MTU は 72 バイトです。

TCP path MTU discovery を有効にした後、すべての新しい TCP 接続は、経路 MTU を見つけます。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、経路 MTU を使用します。

経路上で最小リンク MTU が増加したとき、送信元の装置の経路 MTU を増加させることができるように、経路 MTU は以下に示すエージングメカニズムを使用します。

- TCP 送信元の装置が ICMP エラーメッセージを受信したとき、経路 MTU を減少させ、経路 MTU のエージングタイマを開始します。
- エージングタイマが終了した後、送信元の装置は、RFC1191 に記載されているように、MTU テーブルで大きい値の MSS を使用します。
- ICMP エラーメッセージを 2 分以内に受信しない場合、送信元の装置は、TCP 3WAY ハンドシェイクでネゴシエートできる最大の MSS の値まで MSS を増加させます。

以下に TCP path MTU discovery の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. TCP path MTU discovery を有効にする	**tcp path-mtu-discovery** [**aging** *age-time* | **no-aging**]	デフォルト：無効

20.4 TCPバッファサイズの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. TCP 受信/送信バッファのサイズの設定をする	**tcp window** *window-size*	デフォルト：64KB

20.5 TCPタイマの設定

以下の TCP タイマを設定することができます。

- **SYN wait timer** – SYN パケットを送信したのち、TCP は SYN wait タイマを開始します。SYN wait タイマ間隔以内に応答パケットを受信しない場合、TCP 接続は確立しません。
- **FIN wait timer** – TCP 接続が FIN_WAIT_2 状態に変更されるとき、FIN wait タイマを開始します。タイマ間隔以内に FIN パケットを受信しない場合、TCP 接続は終了します。FIN パケットを受信した場合、TCP 接続状態は TIME_WAIT に変わります。FIN パケットを受信しない場合、タイマを再スタートします。タイマが満了した場合、接続は切断されます。

以下に TCP タイマの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. TCP タイマを設定する	• TCP SYN waitタイマを設定する： **tcp timer syn-timeout** *time-value* • TCP FIN waitタイマを設定する： **tcp timer fin-timeout** *time-value*	デフォルト： • TCP SYN waitタイマ：75秒 • TCP FIN waitタイマ：675秒

20.6 ICMPエラーパケットの送信設定

ICMP エラーパケットには、リダイレクトパケット、タイムアウトパケット、宛先到達不能パケットの 3 種類のパケットがあります。この機能は ICMP エラーメッセージの送信を有効にします。パケット タイプ フィールドの詳細は、RFC792 を参照してください。

- ICMP リダイレクトメッセージ

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します。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、以下のルールで、ホストに ICMP リダイレクトパケットを送信します。

- 受信と送信が同じインタフェースです。
- パケット送信元 IP アドレスとパケット受信インタフェースの IP アドレスは同じセグメント上にあります。
- 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。

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。

- ICMP タイムアウトパケット

装置は以下のルールで ICMP タイムアウトパケット(パケットタイプフィールドが 11 に設定されている)を送信します。

- 以下の場合、装置は送信元に ICMP TTL Expired の ICMP エラーパケット(パケットタイプフィールドが 0 に設定されている)を送信します。
  - 受信パケットが装置へのパケットではありません。
  - 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(パケットタイプフィールドを 1 に設定されている)を送信します。

- ICMP 宛先到達不能パケット

装置は以下のルールで ICMP 宛先不能パケット(パケットタイプフィールドが 3 に設定されている)を送信します。

- 以下の場合、装置は ICMP Network Unreachable の ICMP エラーパケットを送信元に送信します。
  - パケットを転送するためのルートがありません。
  - ルーティングテーブルにデフォルトルートが存在しません。
- 以下の場合、装置は ICMP Protocol Unreachable の ICMP エラーパケットを送信元に送信します。
  - 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。

🕮 **メモ：**

DHCP 対応の装置が ICMP エコー要求を送信しないで、ICMP エコー返答を受信する場合、装置はどのようなプロトコルの ICMP 到達不能のエラーパケットも送信元に送信しません。DHCP を有効にするには、**dhcp enable** コマンドを使用します。このコマンドの詳細は、QX-W2300AC シリーズアクセスコントローラコマンドマニュアルの“5 ネットワーク接続”の” 12 章 DHCP 共通” を参照してください。

- 以下の場合、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。
  - UDP 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一致していません。
- 以下の場合、装置は ICMP Source Route Failed の ICMP エラーパケットを送信元に送信します。
  - パケットの送信元が、Strict Source Routing を使用しています。
  - 中継装置が、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。
- 以下の場合、装置は ICMP Fragmentation Needed and DF-set の ICMP エラーパケットを送信元に送信します。
  - パケット転送とき、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。

以下に ICMP エラーパケットの送信の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． ICMP エラーパケットの送信を有効にする	● ICMPリダイレクトパケットの送信を有効にする：**ip redirects enable** ● ICMPタイムアウトパケットの送信を有効にする：**ip ttl-expires enable** ● ICMP宛先到達不能パケットの送信を有効にする：**ip unreachables enable**	デフォルト：無効

多くの ICMP パケットを送信するとネットワークトラフィックが増加します。多くの ICMP エラーによる悪意のあるパケットを受信した場合、装置のパフォーマンスが下がります。

このような問題を防止するために、装置は ICMP エラーパケットを送信しないように設定を無効にすることができます。ICMP タイムアウトパケットの送信が無効のとき、装置は ICMP TTL Expired メッセージの ICMP エラーパケットを送信しません。ICMP Fragment Reassembly Timeout の ICMP エラーパケットは正常に送信します。

20.7 ICMPエラーメッセージのレートリミットの設定

ネットワークの混雑状態を引き起こす可能性のある短い期間内に、過度の ICMP エラーメッセージを送信することを避けるため、ICMP エラーメッセージの送信レートを制限することができます。トークンバケット（bucket）アルゴリズムは、1 つの ICMP エラーメッセージを示す 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の最大数に達するまで、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に、トークンはバケットから取り除かれます。バケットが空のときに、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。

以下に ICMP エラーメッセージのレートリミットの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． ICMP エラーメッセージの間隔とトークンバケットサイズを設定する	**ip icmp error-interval** *milliseconds* [*bucketsize*]	デフォルト：100ミリ秒間隔で最大10トークンが配置されます。 ICMPレートリミットを無効にするには、間隔を0ミリ秒に設定します。

20.8 IPパフォーマンスの最適化の表示と維持

すべての view で **display** コマンドを実行でき、user view で **reset** コマンドを実行できます。

操作	コマンド
RawIP接続の概要情報を表示する	**display rawip**
RawIP接続の詳細情報を表示する	**display rawip verbose**
TCP接続の概要情報を表示する	**display tcp**
TCP接続の詳細情報を表示する	**display tcp verbose**
UCP接続の概要情報を表示する	**display udp**
TCP接続の詳細情報を表示する	**display udp verbose**
IPパケットの統計情報を表示する	**display ip statistics**
TCPトラフィックの統計情報を表示する	**display tcp statistics**
UCPトラフィックの統計情報を表示する	**display udp statistics**
ICMPの統計情報を表示する	**display icmp statistics**
IPパケットの統計情報を削除する	**reset ip statistics**
TCPトラフィックの統計情報を削除する	**reset tcp statistics**
UDPトラフィックの統計情報を削除する	**reset udp statistics**

目次

このセクションのページは **5-x-x** です。

21 章 NAT 21-1
21.1 NAT の基本概念 21-1
21.2 基本的な NAT 操作メカニズム 21-1
21.3 NAT アプリケーション 21-2
21.3.1 従来の NAT 21-2
21.3.2 Twice NAT 21-2
21.3.3 双方向 NAT 21-2
21.3.4 NAT ヘアピン 21-2
21.3.5 NAT DNS マッピング 21-3
21.4 NAT 制御 21-4
21.5 NAT 変換方式 21-4
21.5.1 スタティック NAT 21-4
21.5.2 ダイナミック NAT 21-4
21.5.3 NAT サーバ 21-5
21.5.4 ポートブロックベース NAT 21-6
21.6 NAT エントリ 21-7
21.6.1 NAT セッションエントリ 21-7
21.6.2 EIM エントリ 21-8
21.6.3 NO-PAT エントリ 21-8
21.6.4 ポートブロックベースのエントリ 21-8
21.7 NAT ALG 21-8
21.8 制限とガイドライン 21-9
21.9 NAT タスクの概要 21-9
21.10 NAT 設定作業リスト 21-9
21.11 スタティック NAT の設定 21-10
21.11.1 制限とガイドライン 21-10
21.11.2 前提条件 21-10
21.11.3 送信 1 対 1 スタティック NAT の設定 21-10
21.11.4 送信 net-to-net スタティック NAT の設定 21-11
21.11.5 受信 1 対 1 スタティック NAT の設定 21-12
21.11.6 受信 net-to-net スタティック NAT の設定 21-13
21.12 ダイナミック NAT の設定 21-14
21.12.1 制限とガイドライン 21-14
21.12.2 前提条件 21-14
21.12.3 送信ダイナミック NAT の設定 21-14
21.12.4 受信ダイナミック NAT の設定 21-16
21.13 NAT サーバマッピングの設定 21-17
21.13.1 NAT サーバマッピングについて 21-17
21.13.2 インタフェースでの一般的な NAT サーバマッピングの設定 21-18
21.13.3 インタフェースでのロードシェアリング NAT サーバマッピングの設定 21-19
21.13.4 インタフェースでの ACL ベース NAT サーバマッピングの設定 21-20
21.14 ポートブロックベース NAT の設定 21-21
21.14.1 ポートブロックベース NAT について 21-21
21.14.2 制限とガイドライン 21-21

21.14.3 スタティックポートブロックマッピングの設定 21-21
21.14.4 ダイナミックポートブロックマッピングの設定 21-22
21.14.5 ポートブロックのグローバル共有の有効化 21-23
21.15 NAT DNS マッピングの設定 21-23
21.16 NAT ALG の設定 21-23
21.17 NAT ログの設定 21-24
21.17.1 NAT セッションログの設定 21-24
21.18 TCP SYN および SYN ACK パケットのタイムスタンプ削除の有効化 21-25
21.19 NAT の表示と維持 21-25
21.20 NAT の設定例 21-26
21.20.1 送信 1 対 1 スタティック NAT の設定例 21-26
21.20.2 送信ダイナミック NAT の設定例 21-28

21章 NAT

NAT (Network Address Translation) は、IP パケットヘッダ内の IP アドレスを別の IP アドレスに変換します。通常、NAT はゲートウェイで設定され、プライベートホストが外部ネットワークにアクセスし、外部ホストが Web サーバなどのプライベートネットワークリソースにアクセスできるようにします。

21.1 NATの基本概念

NAT の基本概念について説明します。

- **NAT 装置**ーNAT が設定された装置です。通常、NAT は内部ネットワークと外部ネットワークを接続するエッジ装置に設定されます。
- **NAT インタフェース**ーNAT が設定されたインタフェースです。
- **NAT ルール**ーアドレス変換の実行方法を定義するルールです。ルールのプライオリティは、ルールリスト上の位置によって決まります。ルールリストの前の方にある NAT ルールは、パケット一致のプライオリティが高くなります。
- **NAT アドレス**ーアドレス変換に使用されるパブリック IP アドレスで、外部ネットワークから到達可能です。NAT アドレスは手動で割り当てることも、ダイナミックに取得することもできます。
- **NAT エントリ**ープライベート IP アドレスとパブリック IP アドレス間のマッピングを保存します。詳細は、本章の“*NAT エントリ*”を参照してください。
- **Easy IP** ーインタフェースの IP アドレスを NAT アドレスとして使用します。インタフェースの IP アドレスは、手動で割り当てることも、DHCP で取得することもできます。

21.2 基本的なNAT操作メカニズム

図 21-1 に基本的な NAT の動作メカニズムを示します。

1) ホストからサーバへの要求を受信すると、NAT はプライベート送信元アドレス 192.168.1.3 をパブリックアドレス 20.1.1.1 に変換し、NAT 処理されたパケットを転送します。NAT は、2 つのアドレスのマッピングを NAT テーブルに追加します。
2) サーバからの応答を受信すると、NAT は宛先パブリックアドレスをプライベートアドレスに変換し、パケットをホストに転送します。

NAT 操作は端末 (ホストとサーバ) に対して透過的です。NAT はプライベートネットワークを外部ユーザから隠し、内部ホストの IP アドレスが 20.1.1.1 であることを示します。

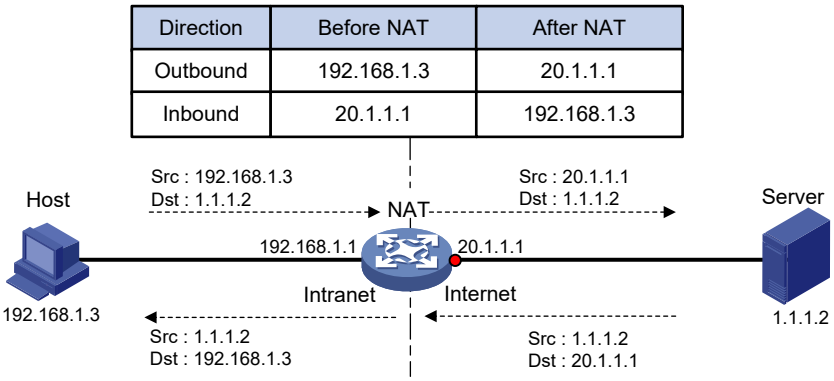


図 21-1 基本的な NAT 動作

21.3 NATアプリケーション

21.3.1 従来の NAT

従来の NAT は、パブリックネットワークに接続するインタフェースで設定します。送信パケットの送信元 IP アドレスと受信パケットの宛先 IP アドレスを変換します。

21.3.2 Twice NAT

Twice NAT は、受信インタフェースの宛先 IP アドレスと送信インタフェースの送信元 IP アドレスを変換します。受信インタフェースと送信インタフェースは両方とも NAT インタフェースです。

Twice NAT を使用すると、重複するアドレスを持つ VPN が相互にアクセスできます。

21.3.3 双方向 NAT

NAT は、受信インタフェース上の受信パケットおよび送信インタフェース上の送信パケットの送信元および宛先 IP アドレスを変換します。

双方向 NAT は、内部 IP アドレスと外部 IP アドレスが重複している場合に、内部ユーザから外部ネットワークリソースへのアクティブアクセスをサポートします。

21.3.4 NAT ヘアピン

NAT ヘアピンを使用すると、内部ホストは NAT を介して相互にアクセスできます。パケットの送信元および宛先 IP アドレスは、内部ネットワークに接続されたインタフェースで変換されます。

NAT ヘアピンには、P 2 P モードと C/S モードがあります。

- **P 2 P**－内部ホストが NAT を介して相互にアクセスできるようにします。内部ホストは、最初にパブリックアドレスを外部サーバに登録します。そして、登録された IP アドレスを用いてホスト間の通信を行います。
- **C/S**－内部ホストが NAT アドレスを使用して内部サーバにアクセスできるようにします。内部サーバに送信されるパケットの宛先 IP アドレスは、NAT サーバ設定と一致することによって変換されます。送信元 IP アドレスは、送信ダイナミック NAT エントリまたは送信スタティック NAT エントリの照合によって変換されます。

21.3.5 NAT DNS マッピング

DNS サーバは通常、パブリックネットワーク上にあります。パブリックネットワーク上のユーザが内部サーバにアクセスできるように、パブリックネットワークに接続する NAT インタフェースに NAT サーバ機能を設定できます。NAT サーバは、パブリック IP アドレスとポート番号を内部サーバのプライベート IP アドレスとポート番号にマッピングします。パブリックユーザは、サーバのドメイン名またはパブリック IP アドレスを使用して内部サーバにアクセスできます。

ユーザがプライベートネットワークにいる場合、サーバのドメイン名を使用して内部サーバにアクセスすることはできません。これは、DNS 応答にサーバのパブリック IP アドレスが含まれているためです。この場合、NAT DNS マッピングを設定して問題を解決できます。

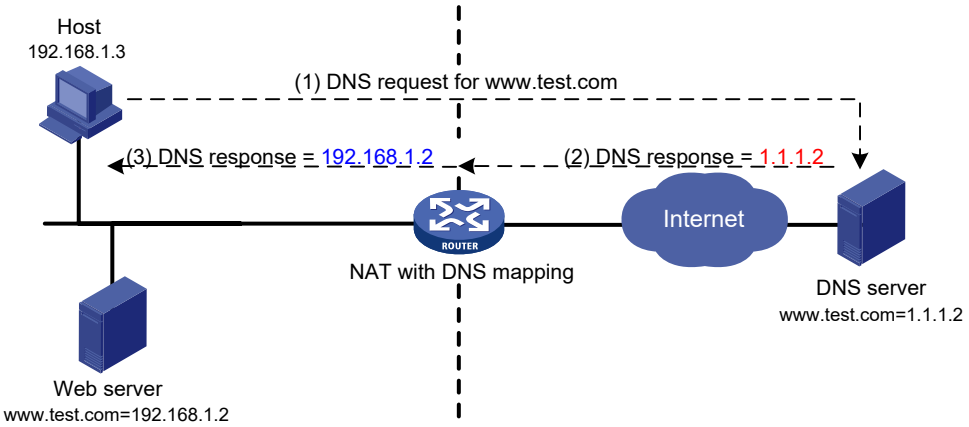


図 21-2 NAT DNS マッピング

図 21-2 に示すように、NAT DNS マッピングは以下のように機能します。

1) ホストは、内部 Web サーバのドメイン名を含む DNS 要求を送信します。
2) DNS 応答を受信すると、NAT 装置は応答のドメイン名を使用して DNS マッピングルックアップを実行します。NAT DNS マッピングは、ドメイン名を内部サーバのパブリック IP アドレス、パブリックポート番号、およびプロトコルタイプにマッピングします。
3) 一致が見つかった場合、NAT は引き続きパブリックアドレス、パブリックポート番号、およびプロトコルタイプを NAT サーバ設定と比較します。NAT サーバ設定は、

パブリック IP アドレスとポート番号を内部サーバのプライベート IP アドレスとポート番号にマッピングします。

4) 一致が見つかった場合、NAT は応答のパブリック IP アドレスを Web サーバのプライベート IP アドレスに変換します。
5) 内部ホストは DNS 応答を受信し、Web サーバのプライベート IP アドレスを取得します。

21.4 NAT制御

ACL を使用して NAT 制御を実装できます。ACL の一致基準には、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、トランスポート層プロトコル、および VPN インスタンスが含まれます。ACL によって許可されたパケットだけが NAT によって処理されます。

21.5 NAT変換方式

21.5.1 スタティック NAT

スタティック NAT では、プライベートアドレスとパブリックアドレスの間に固定マッピングが作成されます。内部ユーザから外部ネットワークへの接続、および外部ユーザから内部ネットワークへの接続がサポートされます。スタティック NAT は、通常の通信に適用されます。

21.5.2 ダイナミック NAT

ダイナミック NAT はアドレスプールを使用してアドレスを変換します。これは、多数の内部ユーザが外部ネットワークにアクセスするシナリオに適用されます。

I. NO-PAT

NO-PAT（Not Port Address Translation） は、プライベート IP アドレスを IP パブリックアドレスに変換します。パブリック IP アドレスは、解放されるまで別の内部ホストで使用できません。

NO-PAT は、すべての IP パケットをサポートします。

II. PAT

PAT（Port Address Translation） は、プライベート IP アドレスと送信元ポートをパブリック IP アドレスと一意のポートにマッピングすることで、複数のプライベート IP アドレスを 1 つのパブリック IP アドレスに変換します。PAT は、TCP パケット、UDP パケット、および ICMP 要求パケットをサポートします。

Direction	Before NAT	After NAT
Outbound	192.168.1.2:1111	20.1.1.1:1001
Outbound	192.168.1.2:2222	20.1.1.1:1002
Outbound	192.168.1.3:1111	20.1.1.1:1003

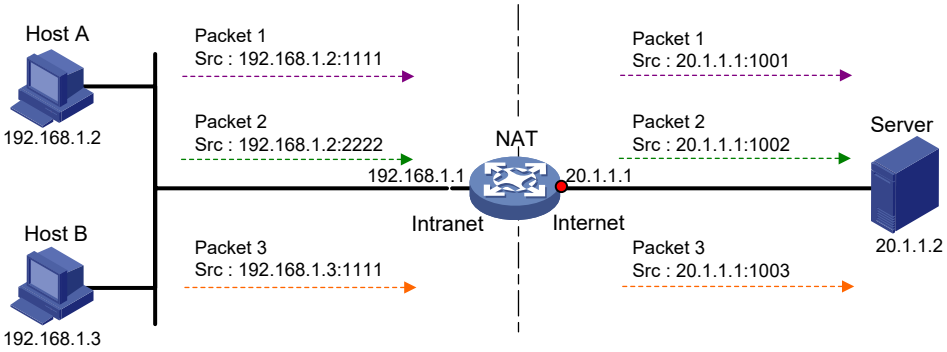


図 21-3 PAT 動作

図 21-3 に示すように、PAT は 3 つのパケットの送信元 IP アドレスを同じ IP パブリックアドレスに変換し、それぞれのポート番号を異なるポート番号に変換します。PAT は応答を受信すると、その応答の宛先アドレスとポート番号を変換し、ターゲットホストに転送します。

PAT では、以下のマッピングがサポートされています。

- **Endpoint-Independent Mapping（EIM）**–同じ送信元 IP 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 を使用すると、外部ホストから内部ホストの変換済み IP アドレスおよびポートへの接続を開始できます。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（APDM）**–同じ送信元 IP およびポートから異なる宛先 IP アドレスおよびポートへのパケットに対して、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への接続を開始できます。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。

21.5.3 NAT サーバ

NAT サーバ機能は、パブリックアドレスとポート番号を内部サーバのプライベート IP アドレスとポート番号にマッピングします。この機能により、プライベートネットワーク内のサーバは外部ユーザにサービスを提供できます。

図 21-4 に、NAT サーバの動作を示します。

1) ホストから要求を受信すると、NAT はパブリック宛先 IP アドレスとポート番号を内部サーバのプライベート IP アドレスとポート番号に変換します。
2) サーバからの応答を受信すると、NAT はプライベート送信元 IP アドレスとポート番号をパブリック IP アドレスとポート番号に変換します。

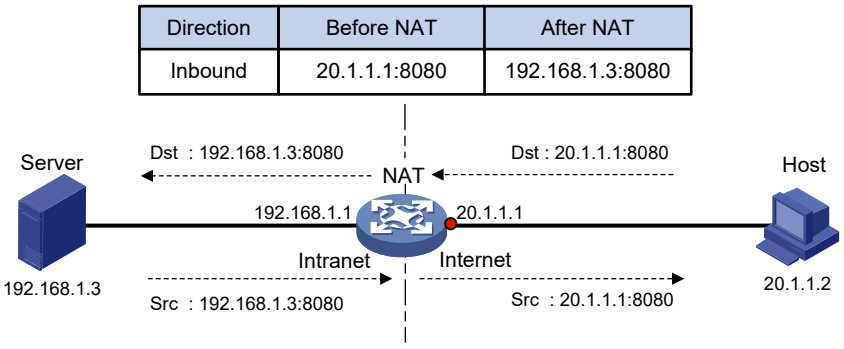


図 21-4 NAT サーバの動作

21.5.4 ポートブロックベース NAT

ポートブロックベース NAT は、ポート範囲に基づく PAT 変換です。複数のプライベート IP アドレスを 1 つのパブリック IP アドレスにマッピングし、プライベート IP アドレスごとに異なるポートブロックを使用します。たとえば、内部ホストのプライベート IP アドレス 10.1.1.1 は、パブリック IP アドレス 202.1.1.1 およびポートブロック 10001~10256 にマッピングされます。内部ホストがパブリックホストにアクセスする場合、送信元 IP アドレス 10.1.1.1 は 202.1.1.1 に変換され、送信元ポートはポートブロック 10001~10256 のポートに変換されます。

ポートブロックベース NAT には、スタティックマッピングとダイナミックマッピングがあります。

I. スタティックポートブロックマッピング

NAT ゲートウェイは、アドレス変換の前にスタティックポートブロックマッピングを計算します。このマッピングは、プライベート IP アドレスとポートブロックを持つパブリック IP アドレスの間で行われます。

内部ユーザが外部ネットワークへの接続を開始すると、システムは以下の操作を実行します。

- ユーザのプライベート IP アドレスに基づいてスタティックマッピングを検索し、マッピングのパブリック IP アドレスとポートブロックを取得します。
- ポートブロック内のパブリックポート番号を選択します。
- プライベート IP アドレスをパブリック IP アドレスに変換し、選択したパブリックポート番号を割り当てます。

NAT ゲートウェイは、プライベート IP アドレス、パブリック IP アドレス、ポート範囲、およびポートブロックサイズを使用して、スタティックマッピングを計算します。

1) ポート範囲をポートブロックサイズで割り、各パブリック IP アドレスで使用可能なポートブロック数を取得します。
   この値はマッピングの基本番号です。
2) 各ブロックの開始ポート番号の昇順でポートブロックをソートします。
3) プライベート IP アドレスとパブリック IP アドレスを別々に昇順でソートします。
4) プライベート IP アドレスの最初のベース番号を、最初のパブリック IP アドレスとそのポートブロックに昇順でマッピングします。

たとえば、各パブリック IP アドレスの使用可能なポートブロックの数は **m** です。最初の **m** 個のプライベート IP アドレスは、最初のパブリック IP アドレスと **m** 個のポートブロックに昇順でマッピングされます。次の **m** 個のプライベート IP アドレスは、2 番目の IP アドレスと **m** 個のポートブロックに昇順でマッピングされます。他のスタティックポートブロックマッピングも同様に作成されます。

II. ダイナミックポートブロックマッピング

内部ユーザが外部ネットワークへの接続を開始すると、ダイナミックポートブロックベース NAT は以下のように動作します。

1) ACL を使用して変換制御を実装します。ACL 許可ルールに一致するパケットだけを処理します。
2) 内部ユーザのプライベート IP アドレスからパブリック IP アドレスおよびポートブロックへのマッピングを作成します。
3) プライベート IP アドレスをパブリック IP アドレスに変換し、プライベート IP アドレスからの後続の接続用に、選択したポートブロック内のポートに送信元ポートを変換します。
4) プライベート IP アドレスからのすべての接続が切断されると、ポートブロックを取り消し、ダイナミックポートブロックマッピングを削除します。

ダイナミックポートブロックマッピングは、ポートブロック拡張をサポートします。プライベートアドレスのポートブロック内のポートがすべて占有されている場合、ダイナミックポートブロックマッピングは送信元ポートを拡張ポートブロック内のポートに変換します。

21.6 NATエントリ

21.6.1 NAT セッションエントリ

NAT は、セッションの NAT セッションエントリを作成し、セッションの最初のパケットのアドレスマッピングを作成します。

NAT セッションエントリには、インタフェースや変換方式などの拡張 NAT 情報が含まれます。セッションの後続のパケットは、このエントリを使用して変換されます。

- 後続のパケットの方向が最初に変換されたパケットの方向と同じ場合、NAT は最初のパケットと同じように送信元アドレスと宛先アドレスの変換を実行します。
- 後続のパケットの方向が逆方向の場合、NAT は逆アドレス変換を実行します。たとえば、最初のパケットの送信元アドレスが変換されると、後続のパケットの宛先アドレスも変換されます。

セッション管理モジュールは、NAT セッションエントリの更新とエージングを維持します。セッション管理の詳細は、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*15 セキュリティ*”の”*7 章 接続制限*”を参照してください。

21.6.2 EIM エントリ

EIM が NAT 装置に設定されている場合、PAT モードでは最初に NAT セッションエントリが作成され、次に EIM エントリが作成されます。EIM エントリは 3 タプルエントリで、プライベートアドレス/ポートをパブリックアドレス/ポートにマッピングします。EIM エントリにより、以下のことが保証されます。

- 同じ送信元 IP およびポートから送信される後続の新しい接続は、最初の接続と同じ変換を使用します。
- 外部ホストから開始された新しい接続のアドレスを、EIM エントリに基づいて NAT アドレスとポート番号に変換します。

関連するすべての NAT セッションエントリが期限切れになると、EIM エントリが期限切れになります。

21.6.3 NO-PAT エントリ

NO-PAT エントリは、プライベートアドレスをパブリックアドレスにマッピングします。同じ送信元 IP から送信される後続の接続にも、同じマッピングが適用されます。

関連するすべての NAT セッションエントリが期限切れになると、NO-PAT エントリが期限切れになります。

21.6.4 ポートブロックベースのエントリ

ポートブロックベースのエントリは、プライベート IP アドレスをパブリック IP アドレスとポートブロックにマッピングします。

ポートブロックベースのエントリには、スタティックおよびダイナミックポートブロックマッピングが含まれます。これらのマッピングの詳細は、本章の“*ポートブロックベース NAT*”の“*スタティックポートブロックマッピング*”および“*ダイナミックポートブロックマッピング*”を参照してください。

21.7 NAT ALG

NAT ALG (Application Level Gateway) 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、接続を確立します。

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 がデータ接続確立のためにアドレスとポート情報を変換する必要があります。

21.8 制限とガイドライン

一般的な制限とガイドラインは以下の通りです。

- 変換する IP アドレスを識別する ACL を設定します。一致基準には、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、およびトランスポート層プロトコルおよび VPN インスタンスが含まれます。ACL の詳細は、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*15 セキュリティ*”の”*1 章 ACL*”を参照してください。
- すべての変換方式を実行する場合、NAT ルールは以下の降順でソートされます。

a) NATサーバ

b) スタティックNAT

c) NATスタティックポートブロックマッピング

d) ダイナミックNATおよびNATダイナミックポートブロックマッピング

ダイナミックNATおよびNATダイナミックポートブロックマッピングは、IPv4パケットで有効になります。ダイナミックNATルールおよびNATダイナミックポートブロックマッピングルールの一致順序は、プライオリティ値によって決まります。プライオリティ値が同じ場合、ルールは使用するACLに基づいて一致します。

21.9 NATタスクの概要

NAT ルールの適用範囲に基づいて、インタフェースベースの NAT を設定できます。インタフェースベースの NAT の場合は、インタフェースで NAT ルールを設定します。

21.10 NAT設定作業リスト

作業リスト
（必須設定項目）インタフェースでの変換方式の設定 • スタティックNATの設定 • ダイナミックNATの設定 • インタフェースでの一般的なNATサーバマッピングの設定 • インタフェースでのロードシェアリングNATサーバマッピングの設定 • インタフェースでのACLベースNATサーバマッピングの設定 • ポートブロックベースNATの設定
（オプション設定項目）NAT DNSマッピングの設定
（オプション設定項目） NAT ALGの設定
（オプション設定項目） NATログの設定
（オプション設定項目） TCP SYNおよびSYN ACKパケットのタイムスタンプ削除の有効化

21.11 スタティックNATの設定

21.11.1 制限とガイドライン

通常、双方向 NAT を実装するには、受信スタティック NAT を送信ダイナミック NAT、NAT サーバ、または送信スタティック NAT とともに設定します。

21.11.2 前提条件

スタティック NAT を設定する前に、以下の作業を実行する必要があります。

- 変換する IP アドレスを識別する ACL を設定します。ACL の詳細は、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*15 セキュリティ*”の”*1 章 ACL*”を参照してください。
- 受信スタティック NAT のルートを手動で追加します。宛先アドレスとして *local-ip* または local-network を使用し、ネクストホップとして *global-ip*、グローバルネットワーク内のアドレス、または出力インタフェースに直接接続されたネクストホップを使用します。

21.11.3 送信 1 対 1 スタティック NAT の設定

I. 送信 1 対 1 スタティック NAT について

プライベート IP アドレスからパブリック IP アドレスへのアドレス変換の場合は、外部ネットワークに接続されたインタフェースで送信 1 対 1 スタティック NAT を設定します。

- 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、送信元 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。

II. 制限とガイドライン

1 つのプライベート IP アドレスに対して複数の送信 1 対 1 スタティックマッピングが使用可能な場合、装置は以下のルールで一致順序を決定します。

- プライオリティ値が小さいマッピングほどプライオリティが高くなります。
- マッピングにプライオリティ値がない場合、またはプライオリティ値が同じ場合、マッピングの ACL によって一致順序が決定されます。
  - 名前付き ACL を持つマッピングは、番号付き ACL を持つマッピングよりもプライオリティが高くなります。
  - 名前付き ACL を持つマッピングは、ACL 名の英数字順で照合されます。
  - 番号付き ACL を持つマッピングは、ACL 番号の降順で照合されます。

III. 設定手順

以下に送信 1 対 1 スタティック NAT の設定手順を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. 送信スタティック NAT の 1 対 1 マッピングを設定する	**nat static outbound** *local-ip global-ip* [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } [**reversible**]] [**rule** *rule-name*] [**priority** *priority*]	―
3. (オプション設定項目) 送信 1 対 1 マッピング NAT ルールを再配置して、プライオリティを調整する	**nat static outbound rule move** *nat-rule-name1* { **after** | **before** } *nat-rule-name2*	デフォルト : マッピングルールのプライオリティは、ルールリスト上の位置によって決まります。ルールリストの前の方にあるNATルールは、パケット一致のプライオリティが高くなります。
4. interface view に移行する	**interface** *interface-type interface-number*	―
5. インタフェースでスタティック NAT を有効にする	**nat static enable**	デフォルト : 無効

21.11.4 送信 net-to-net スタティック NAT の設定

I. 送信 net-to-net スタティック NAT について

プライベートネットワークからパブリックネットワークへのアドレス変換の場合は、外部ネットワークに接続されているインタフェース上で送信net-to-netスタティックNATを設定します。

- 送信パケットの送信元 IP 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 IP 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。
- 受信パケットの宛先 IP 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 IP 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。

II. 制限とガイドライン

プライベート IP ネットワーク内のアドレスを変換するために複数の送信 net-to-net スタティックマッピングが使用可能な場合、装置は以下のルールで一致順序を決定します。

- プライオリティ値が小さいマッピングほどプライオリティが高くなります。
- マッピングにプライオリティ値がない場合、またはプライオリティ値が同じ場合、マッピングの ACL によって一致順序が決定されます。
  - 名前付き ACL を持つマッピングは、番号付き ACL を持つマッピングよりもプライオリティが高くなります。
  - 名前付き ACL を持つマッピングは、ACL 名の英数字順で照合されます。
  - 番号付き ACL を持つマッピングは、ACL 番号の降順で照合されます。

III. 設定手順

以下に送信 net-to-net スタティック NAT の設定手順を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―

操作	コマンド	補足
2. 送信スタティック NAT の net-to-net マッピングを設定する	**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*]	—
3. interface view に移行する	**interface** *interface-type interface-number*	—
4. インタフェースでスタティック NAT を有効にする	**nat static enable**	デフォルト：無効

21.11.5 受信 1 対 1 スタティック NAT の設定

I. 受信 1 対 1 スタティック NAT について

パブリック IP アドレスからプライベート IP アドレスへのアドレス変換では、受信 1 対 1 スタティック NAT を設定します。

- 受信パケットの送信元 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。
- 送信パケットの宛先 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。

II. 制限とガイドライン

1 つのパブリック IP アドレスを変換するために複数の受信 1 対 1 スタティックマッピングが使用可能な場合、装置は以下のルールで一致順序を決定します。

- プライオリティ値が小さいマッピングほどプライオリティが高くなります。
- マッピングにプライオリティ値がない場合、またはプライオリティ値が同じ場合、マッピングの ACL によって一致順序が決定されます。
  - 名前付き ACL を持つマッピングは、番号付き ACL を持つマッピングよりもプライオリティが高くなります。
  - 名前付き ACL を持つマッピングは、ACL 名の英数字順に照合されます。
  - 番号付き ACL を持つマッピングは、ACL 番号の降順に照合されます。

III. 設定手順

以下に受信 1 対 1 スタティック NAT の設定手順を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. 受信スタティック NAT の 1 対 1 マッピングを設定する	**nat static inbound** *global-ip local-ip* [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } [**reversible**]] [**rule** *rule-name*] [**priority** *priority*]	—

操作	コマンド	補足
3. (オプション設定項目) 受信 1 対 1 マッピング NAT ルールを再配置して、プライオリティを調整する	**nat static inbound rule move** *nat-rule-name1* { **after** | **before** } *nat-rule-name2*	デフォルト : ルールのプライオリティはルールリスト上の位置によって決まります。ルールリストの前の方にあるNATルールは、パケット一致の優先度が高くなります。
4. interface view に移行する	**interface** *interface-type interface-number*	—
5. インタフェースでスタティック NAT を有効にする	**nat static enable**	デフォルト：無効

21.11.6 受信 net-to-net スタティック NAT の設定

I. 受信 net-to-net スタティック NAT について

パブリックネットワークからプライベートネットワークへのアドレス変換の場合は、受信 net-to-net スタティック NAT を設定します。

- 受信パケットの送信元 IP 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 IP 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。
- 送信パケットの宛先 IP 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 IP 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。

II. 制限とガイドライン

パブリックネットワーク内のアドレスを変換するために複数の受信 net-to-net スタティックマッピングが使用可能な場合、装置は以下のルールで一致順序を決定します。

- プライオリティ値が小さいマッピングほどプライオリティが高くなります。
- マッピングにプライオリティ値がない場合、またはプライオリティ値が同じ場合、マッピングの ACL によって一致順序が決定されます。
  - 名前付き ACL を持つマッピングは、番号付き ACL を持つマッピングよりもプライオリティが高くなります。
  - 名前付き ACL を持つマッピングは、ACL 名の英数字順で照合されます。
  - 番号付き ACL を持つマッピングは、ACL 番号の降順で照合されます。

III. 設定手順

以下に受信 net-to-net スタティック NAT の設定手順を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. 受信スタティック NAT の net-to-net マッピングを設定する	**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*]	—

操作	コマンド	補足
3． interface view に移行する	**interface** *interface-type interface-number*	—
4． インタフェースでスタティック NAT を有効にする	**nat static enable**	デフォルト：無効

21.12 ダイナミックNATの設定

21.12.1 制限とガイドライン

複数の受信または送信ダイナミック NAT ルールを設定できます。装置は以下のガイドラインに従って一致順序を決定します。

- プライオリティ値が小さい NAT ルールはプライオリティが高くなります。
- NAT ルールにプライオリティ値がない場合、またはプライオリティ値が同じ場合、ルール内の ACL によって一致順序が決定されます。
  - 名前付き ACL を持つ NAT ルールは、番号付き ACL を持つ NAT ルールよりもプライオリティが高くなります。
  - 名前付き ACL を持つ NAT ルールは、ACL 名の英数字順で照合されます。
  - 番号付き ACL を持つ NAT ルールは、ACL 番号の降順で照合されます。
- ACL が設定されていない NAT ルールのプライオリティは最も低くなります。

21.12.2 前提条件

ダイナミック NAT を設定する前に、以下の作業を実行する必要があります。

- 変換する IP アドレスを識別する ACL を設定します。ACL の詳細は、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*15 セキュリティ*”の”*1 章 ACL*”を参照してください。
- Easy IP 機能を有効にするかどうかを決定します。インタフェースの IP アドレスを NAT アドレスとして使用する場合は、Easy IP を設定します。
- アドレス変換用のパブリック IP アドレスプールを決定します。
- ポート番号を変換するかどうかを決定します。IP アドレスだけを変換するには NO-PAT を使用し、IP アドレスとポート番号の両方を変換するには PAT を使用します。

21.12.3 送信ダイナミック NAT の設定

I. 送信ダイナミック NAT について

プライベート IP アドレスをパブリック IP アドレスに変換するには、外部ネットワークに接続されたインタフェースで送信ダイナミック NAT を設定します。

II. 設定手順

以下に送信ダイナミック NAT の設定手順を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. NAT アドレスグループを作成し、その view に移行する	**nat address-group** *group-id*	ー
3. アドレスグループにアドレス範囲を追加する	**address** *start-address end-address*	デフォルト：設定なし 1つのアドレスグループに複数のアドレス範囲を追加できます。 アドレス範囲は重複してはいけません。
4. system view に戻る	**quit**	ー
5. interface view に移行する	**interface** *interface-type interface-number*	ー
6. 送信ダイナミック NAT を設定する	• NO-PATを設定する **nat outbound** [*ipv4-acl-number* | **name** *ipv4-acl-name*] **address-group** *group-id* **no-pat** [**reversible**] [**rule** *rule-name*] [**priority** *priority*] • PATを設定する **nat outbound** [*ipv4-acl-number* | **name** *ipv4-acl-name*] [**address-group** *group-id*] [**port-preserved**] [**rule** *rule-name*] [**priority** *priority*]	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。 **address-group**: このキーワードを指定しない場合、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が実装されています。 **no-pat reversible**: これらのキーワードを指定すると、逆アドレス変換が有効になります。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。宛先アドレスは、一致するNO-PATエントリ内のプライベートIPアドレスに変換されます。
7. (オプション設定項目) 送信ダイナミック NAT ルールを再配置して、プライオリティを調整	**nat outbound rule move** *nat-rule-name1* { **after** | **before** } *nat-rule-name2*	デフォルト：ルールのプライオリティはルールリスト上の位置によって決まります。ルールリストの前の方にあるNATルールは、パケット一致の優先度が高くなります。

21.12.4 受信ダイナミック NAT の設定

I. 制限とガイドライン

受信ダイナミック NAT だけを設定しないでください。通常、受信ダイナミック NAT は、双方向 NAT を実装するために、送信ダイナミック NAT、NAT サーバ、または送信スタティック NAT とともに機能します。

ルートの自動追加には時間がかかるため、手動でルートを作成することを推奨します。

II. 設定手順

以下に受信ダイナミック NAT の設定手順を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. NAT アドレスグループを作成し、その view に移行する	**nat address-group** *group-id*	
3. アドレスグループにアドレス範囲を追加する	**address** *start-address end-address*	デフォルト：設定なし 1つのアドレスグループに複数のアドレス範囲を追加できます。 アドレス範囲は重複してはいけません。
4. system view に戻る	**quit**	―
5. interface view に移行する	**interface** *interface-type interface-number*	―

操作	コマンド	補足
6. 受信ダイナミック NAT を設定する	**nat inbound** { *ipv4-acl-number* | **name** *ipv4-acl-name* } **address-group** *group-id* [**no-pat** [**reversible**] [**add-route**]] [**rule** *rule-name*] [**priority** *priority*]	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。 **no-pat reversible**: これらのキーワードを指定すると、逆アドレス変換が有効になります。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。宛先アドレスは、一致するNO-PATエントリ内のプライベートIPアドレスに変換されます。 **add-route**: このキーワードを使用すると、受信ダイナミックNATルールが一致したときに、プライベートアドレス宛てのルートを装置が自動的に追加できます。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。この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。
7. (オプション設定項目) 送信ダイナミック NAT ルールを再配置して、プライオリティを調整する	**nat inbound rule move** *nat-rule-name1* { **after** | **before** } *nat-rule-name2*	デフォルト : ルールのプライオリティはルールリスト上の位置によって決まります。ルールリストの前の方にあるNATルールは、パケット一致のプライオリティが高くなります。

21.13 NATサーバマッピングの設定

21.13.1 NAT サーバマッピングについて

通常、NAT サーバ機能は、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、プライベートネットワーク内のサーバが外部ユーザにサービスを提供できるようにします。パブリック IP アドレスとポート番号を内部サーバのプライベート IP アドレスとポート番号にマッピングします。

NAT サーバ機能を実装するには、以下のサーバマッピングを設定します。

- **共通NATサーバマッピング**－内部サーバのプライベートIPアドレスとポート番号を、パブリック IP アドレスとポート番号にマッピングします。この方法では、外部ホストは、指定されたパブリック IP アドレスを使用して内部サーバにアクセスできます。
- **ロードシェアリング NAT サーバマッピング**－複数の内部サーバを内部サーバグループに追加して、これらのサーバが外部ホストに対して同じサービスを提供できるよう

にできます。NAT 装置は、サーバの重みと接続数に基づいて 1 つの内部サーバを選択し、外部ホストから内部サーバグループのパブリックアドレスへの要求に応答します。

- **ACL ベースの NAT サーバマッピング**――一般的な NAT サーバマッピングの拡張です。共通 NAT サーバマッピングは、内部サーバのプライベート IP アドレスを単一のパブリック IP アドレスにマッピングします。ACL ベースの NAT サーバマッピングは、内部サーバのプライベート IP アドレスを ACL で定義された一連のパブリック IP アドレスにマッピングします。パケットの宛先アドレスが ACL の許可ルールと一致する場合、宛先アドレスは内部サーバのプライベート IP アドレスに変換されます。

21.13.2 インタフェースでの一般的な NAT サーバマッピングの設定

以下にインタフェースでの一般的な NAT サーバマッピングの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． interface view に移行する	**interface** *interface-type interface-number*	―

操作	コマンド	補足
3. 一般的な NAT サーバマッピングを設定する	• 1つもしくは存在しないパブリックポートでの単一パブリックアドレス **nat server** [**protocol** *pro-type*] **global** { *global-address* | **current-interface** | **interface** *interface-type interface-number* } [*global-port*] **inside** *local-address* [*local-port*] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* }] [**reversible**] [**rule** *rule-name*] • 連続するパブリックポートでの単一のパブリックアドレス **nat server protocol** *pro-type* **global** { *global-address* | **current-interface** | **interface** *interface-type interface-number* } *global-port*1 *global-port*2 **inside** { { *local-address* | *local-address*1 *local-address*2 } *local-port* | *local-address local-port*1 *local-port*2 } [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* }] [**rule** *rule-name*] • 1つもしくは存在しないパブリックポートでの連続パブリックアドレス **nat server protocol** *pro-type* **global** *global-address*1 *global-address*2 [*global-port*] **inside** { *local-address* | *local-address*1 *local-address*2 } [*local-port*] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* }] [**rule** *rule-name*] • 単一パブリックポートでの連続パブリックアドレス **nat server protocol** *pro-type* **global** *global-address*1 *global-address*2 *global-port* **inside** *local-address local-port*1 *local-port*2 [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* }] [**rule** *rule-name*]	1つのインタフェースに複数のNATサーバマッピングを設定できます。

21.13.3 インタフェースでのロードシェアリング NAT サーバマッピングの設定

負荷分散型 NAT サーバマッピングを設定する場合、ユーザが同じパブリックアドレスとパブリックポートで内部サーバ上の同じサービスにアクセスするようにする必要があります。このため、以下のマッピングの値 *N* が内部サーバグループ内のサーバ数以下であることを確認してください。

- 1 つのパブリックアドレスと *N* 個の連続するパブリックポート番号が、1 つの内部サーバグループにマッピングされます。

- *N* 個の連続するパブリックアドレスと 1 つのパブリックポート番号が、1 つの内部サーバグループにマッピングされます。

以下にインタフェースでのロードシェアリングNATサーバマッピングの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. NAT アドレスグループを作成し、その view に移行する	**nat address-group** *group-id*	デフォルト：設定なし
3. 内部サーバをグループに追加する	**inside ip** *inside-ip* **port** *port-number* [**weight** *weight-value*]	1つのグループに複数の内部サーバを追加できます。
4. system view に戻る	**quit**	―
5. interface view に移行する	**interface** *interface-type interface-number*	―
6. ロードシェアリング NAT サーバマッピングを設定する	**nat server protocol** *pro-type* **global** { { *global-address* | **current-interface** | **interface** *interface-type interface-number* } { *global-port* | *global-port*1 *global-port*2 } | *global-address*1 *global-address*2 *global-port* } **inside server-group** *group-id* [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* }] [**rule** *rule-name*]	1つのインタフェースに複数のロードシェアリングNATサーバマッピングを設定できます。

21.13.4 インタフェースでの ACL ベース NAT サーバマッピングの設定

複数の ACL ベースの NAT サーバマッピングが設定されている場合、装置は以下のルールを使用して一致順序を決定します。

- プライオリティ値が小さいマッピングほどプライオリティが高くなります。
- マッピングにプライオリティ値がない場合、またはプライオリティ値が同じ場合、マッピングの ACL によって一致順序が決定されます。
  - 名前付き ACL を持つマッピングは、番号付き ACL を持つマッピングよりもプライオリティが高くなります。
  - 名前付き ACL を持つマッピングは、ACL 名の英数字順で照合されます。
  - 番号付き ACL を持つマッピングは、ACL 番号の降順で照合されます。

以下にインタフェースでのロードシェアリングNATサーバマッピングの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. interface view に移行する	**interface** *interface-type interface-number*	―
3. ACL ベースの NAT サーバマッピングを設定する	**nat server global { ipv4-acl-number | name** *ipv4-acl-name* **} inside** *local-address* **[** *local-port* **] [rule** *rule-name* **] [priority** *priority* **]**	1つのインタフェースに複数のNATサーバマッピングを設定できます。

操作	コマンド	補足
4. ACL ベースの NAT サーバマッピングのプライオリティを調整する	**nat server rule move** *nat-rule-name1* { **after** | **before** } *nat-rule-name2*	デフォルト : マッピングルールのプライオリティは、ルールリスト上の位置によって決まります。ルールリストの前の方にあるNATルールは、パケット一致のプライオリティが高くなります。

21.14 ポートブロックベースNATの設定

21.14.1 ポートブロックベース NAT について

ポートブロックベースの NAT は、送信アドレス変換を提供し、パブリック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。

21.14.2 制限とガイドライン

ダイナミックポートブロックマッピングを設定するには、NAT アドレスグループでポートブロックパラメータを設定する必要があります。

21.14.3 スタティックポートブロックマッピングの設定

以下にスタティックポートブロックマッピングの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. NAT ポートブロックグループを作成し、その view に移行する	**nat port-block-group** *group-id*	―
3. プライベート IP アドレス範囲をポートブロックグループに追加する	**local-ip-address** *start-address end-address*	複数のプライベートIPアドレス範囲を1つのポートブロックグループに追加できますが、重複することはできません。
4. パブリック IP アドレス範囲をポートブロックグループに追加する	**global-ip-pool** *start-address end-address*	1つのポートブロックグループに複数のパブリックIPアドレス範囲を追加できますが、それらを重複させることはできません。
5. パブリック IP アドレスのポート範囲を設定する	**port-range** *start-port-number end-port-number*	デフォルト：1~65535
6. ポートブロックサイズを設定する	**block-size** *block-size*	デフォルト：256

操作	コマンド	補足
7. system view に戻る	**quit**	―
8. interface view に移行する	**interface** *interface-type interface-number*	―
9. インタフェースにスタティック送信ポートブロックマッピングルールを設定する	**nat outbound port-block-group** *group-id* [**rule** *rule-name*]	デフォルト：設定なし 1つのインタフェースに複数のポートブロックマッピングルールを設定できます。
10. (オプション設定項目) PAT マッピングモードを設定する	**a)** system viewに戻る **quit** **b)** **nat mapping-behavior endpoint-independent** [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* }]	デフォルト：Address and Port-Dependent Mapping

21.14.4 ダイナミックポートブロックマッピングの設定

以下にダイナミックポートブロックマッピングの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. (オプション設定項目) PAT マッピングモードを設定する	**nat mapping-behavior endpoint-independent** [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* }]	デフォルト：Address and Port-Dependent Mapping
3. NAT アドレスグループを作成し、その view に移行する	**nat address-group** *group-id*	―
4. NAT アドレスグループにパブリック IP アドレス範囲を追加する	**address** *start-address end-address*	1つのアドレスグループに複数のパブリックIPアドレス範囲を追加できます。 アドレスグループ内のIPアドレス範囲は重複してはいけません。
5. (オプション設定項目) パブリック IP アドレスのポート範囲を設定する	**port-range** *start-port-number end-port-number*	デフォルト：1~65535 この設定はPAT変換モードでのみ有効です。
6. ポートブロックパラメータを設定する	**port block block-size** *block-size* [**extended-block-number** *extended-block-number*]	デフォルト：設定なし この設定は、PAT変換モードでのみ有効です。
7. system view に戻る	**quit**	―
8. interface view に移行する	**interface** *interface-type interface-number*	―
9. 送信ダイナミック NAT の PAT を設定する	**nat outbound** [*ipv4-acl-number* | **name** *ipv4-acl-name*] [**address-group** *group-id*] [**port-preserved**] [**rule** *rule-name*] [**priority** *priority*]	デフォルト：設定なし **port-preserved**キーワードは、ダイナミックポートブロックマッピングでは有効になりません。

21.14.5 ポートブロックのグローバル共有の有効化

I. ポートブロックのグローバル共有の有効化について

複数のインタフェースにダイナミック NAT ポートブロックマッピングが設定されている場合、インタフェースは同じ IP アドレスからのパケットに対して異なるポートブロックマッピングを作成することがあります。このコマンドを使用すると、同じ IP アドレスからのパケットの変換に同じポートブロックマッピングを使用するようにインタフェースを設定できます。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. ポートブロックのグローバル共有を有効にする	**nat port-block global-share enable**	デフォルト：無効

21.15 NAT DNSマッピングの設定

I. 制限とガイドライン

NAT DNS マッピングは、NAT サーバと連携して機能します。NAT DNS マッピングは、内部サーバのドメイン名を内部サーバのパブリック IP アドレス、パブリックポート番号、およびプロトコルタイプにマッピングします。NAT サーバは、パブリック IP およびポートを内部サーバのプライベート IP およびポートにマッピングします。

II. 設定手順

以下に NAT DNS マッピングの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
1. NAT DNS マッピングを設定する	**nat dns-map domain** *domain-name* **protocol** *pro-type* { **interface** *interface-type interface-number* | **ip** *global-ip* } **port** global-port	複数のNAT DNSマッピングを設定できます。

21.16 NAT ALGの設定

以下に NAT ALG の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー

操作	コマンド	補足
2. 1 つのプロトコルまたはすべてのプロトコルに対して NAT ALG を設定する	**nat alg** { **all** | **dns** | **ftp** | **h323** | **icmp-error** | **ils** | **mgcp** | **nbt** | **pptp** | **rsh** | **rtsp** | **sccp** | **sip** | **sqlnet** | **tftp** | **xdmcp** }	デフォルト：NAT ALGはDNS、FTP、ICMPエラーメッセージ、RTSP、およびPPTPに対して有効になっており、サポートされている他のプロトコルに対しては無効になっています。

21.17 NATログの設定

21.17.1 NAT セッションログの設定

I. NAT セッションログについて

NAT セッションログは、変換情報やアクセス情報などの NAT セッション情報を記録します。

NAT 装置は、以下のイベントの NAT セッションログを生成します。

- NAT セッションの確立。
- NAT セッションの削除。このイベントは、プライオリティの高い設定の追加、設定の削除、ACL の変更を行った場合、NAT セッションが期限切れになった場合、または NAT セッションを手動で削除した場合に発生します。
- アクティブな NAT セッションログ。

II. 設定手順

以下に NAT セッションログの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. NAT ログを有効にする	**nat log enable** [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* }]	デフォルト：無効
3. NAT セッションログを有効にする	• NATセッション確立イベントの場合： **nat log flow-begin** • NATセッション削除イベントの場合： **nat log flow-end** • アクティブNATフローの場合： **nat log flow-active** *time-value*	デフォルト：無効

21.18 TCP SYNおよびSYN ACKパケットのタイムスタンプ削除の有効化

I. TCP SYN および SYN ACK パケットのタイムスタンプ削除について

この機能が設定されている場合、ダイナミックアドレス変換後に、TCP SYN および SYN ACK パケットからタイムスタンプが削除されます。

nat inbound または **nat outbound** を使用して PAT モードがインタフェースに設定され、tcp_timestams および tcp_tw_recycle 機能が TCP サーバに設定されている場合、TCP 接続が確立されないことがあります。この問題を解決するには、tcp_tw_recycle 機能をシャットダウンするか、**nat timestamp delete** コマンドを設定します。

II. 設定手順

以下に NAT 応答リダイレクションの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
1. TCP SYN および SYN ACK パケットのタイムスタンプ削除を有効にする	**nat timestamp delete**	デフォルト：無効

21.19 NATの表示と維持

すべての view で **display** コマンドを実行でき、user view で **reset** コマンドを実行できます。

操作	コマンド
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。	**display nat alg**
すべてのNAT設定情報を表示します。	**display nat all**
NATアドレスグループ情報を表示します。	**display nat address-group** [*group-id*]
NAT DNSマッピング設定を表示します。	**display nat dns-map**
NAT EIMエントリに関する情報を表示します。	**display nat eim** [**protocol** { **tcp** | **udp** }]
受信ダイナミックNATコンフィグレーションを表示します。	**display nat inbound**
NATログ設定を表示します。	**display nat log**
NAT NO-PATエントリに関する情報を表示します。	**display nat no-pat**
送信ダイナミックNATコンフィグレーションを表示します。	**display nat outbound**
NATサーバマッピングを表示します。	**display nat server**

操作	コマンド
内部サーバグループの設定を表示します。	**display nat server-group** [*group-id*]
NATセッションを表示します。	**display nat session** [{ **source-ip** *source-ip* | **destination-ip** *destination-ip* } *] [**verbose**]
スタティックNATマッピングを表示します。	**display nat static**
NAT統計情報を表示します。	**display nat statistics** [**summary**]
NAT 444に対するスタティック送信ポートブロックマッピングルールを表示します。	**display nat outbound port-block-group**
NATポートブロックグループコンフィグレーションを表示します。	**display nat port-block-group** [*group-id*]
NATポートブロックマッピングを表示します。	**display nat port-block** { **dynamic** | **static** }
アドレスグループのポートブロック使用状況を表示します。	**display nat port-block-usage** [**address-group** *group-id*]
NATカウント統計情報のクリア	**reset nat count statistics** { **all** | **dynamic** | **server** | **static** | **static-port-block** }
NATセッションをクリアします。	**reset nat session** [**protocol** { **tcp** | **udp** }]

21.20 NATの設定例

21.20.1 送信 1 対 1 スタティック NAT の設定例

I. ネットワーク要件

図 21-5 に示すように、10.110.10.8/24 のクライアントがインターネットにアクセスできるようにスタティック NAT を設定します。

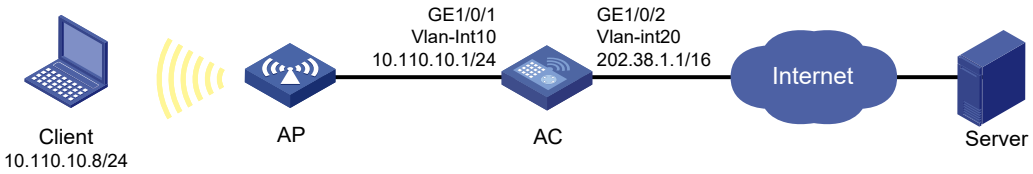


図 21-5 ネットワーク図

II. 設定手順

インタフェースに IP アドレスを割り当てます。(詳細は省略します。)

プライベートアドレス 10.110.10.8 とパブリックアドレス 202.38.1.100 の間に 1 対 1 のスタティック NAT マッピングを設定します。

```
<AC>system-view
[AC] nat static outbound 10.110.10.8 202.38.1.100
```

VLAN インタフェース 20 でスタティック NAT を有効にします。

```
[AC] interface vlan-interface 20
[AC-Vlan-interface20] nat static enable
```

III. 設定の確認

10.110.10.8/24 のクライアントがインターネット上のサーバにアクセスできることを確認します。(詳細は省略します。)

スタティック NAT の設定を確認します。

```
[AC] display nat static
Static NAT mappings:
  Totally 1 outbound static NAT mappings.
  IP-to-IP:
    Local IP     : 10.110.10.8
    Global IP    : 202.38.1.100
    Config status: Active

Interfaces enabled with static NAT:
  Totally 1 interfaces enabled with static NAT.
  Interface: Vlan-interface20
    Config status: Active
```

NAT セッション情報を表示します。

```
[AC] display nat session verbose
Initiator:
  Source      IP/port: 10.110.10.8/42496
  Destination IP/port: 202.38.1.111/2048
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: Vlan-interface10
Responder:
  Source      IP/port: 202.38.1.111/42496
  Destination IP/port: 202.38.1.100/0
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: Vlan-interface20
State: ICMP_REPLY
Application: INVALID
Start time: 2012-08-16 09:30:49  TTL: 27s
Initiator->Responder:            5 packets        420 bytes
Responder->Initiator:            5 packets        420 bytes

Total sessions found: 1
```

21.20.2 送信ダイナミック NAT の設定例

I. ネットワーク要件

図 21-6 に示すように、企業はプライベートサブネットアドレス 192.168.0.0/16 と、2 つのパブリック IP アドレス 202.38.1.2 および 202.38.1.3 を持っています。サブネット 192.168.1.0/24 上の内部ユーザだけがインターネットにアクセスできるように、送信ダイナミック NAT を設定します。

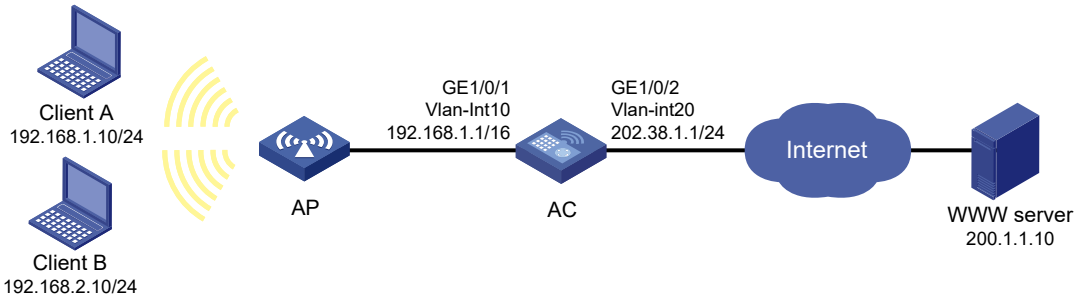


図 21-6 ネットワーク図

II. 設定手順

#インタフェースに IP アドレスを割り当てます。(詳細は省略します。)

アドレスグループ 0 を設定し、アドレス 202.38.1.2 および 202.38.1.3 をグループに追加します。

```
<AC> system-view
[AC] nat address-group 0
[AC-address-group-0] address 202.38.1.2 202.38.1.3
[AC-address-group-0] quit
```

ACL 2000 を設定し、サブネット 192.168.1.0/24 からのパケットだけを通過させるルールを作成します。

```
[AC] acl basic 2000
[AC-acl-ipv4-basic-2000] rule permit source 192.168.1.0 0.0.0.255
[AC-acl-ipv4-basic-2000] quit
```

VLAN インタフェース 20 で送信ダイナミック PAT を有効にします。ACL ルールで許可されたパケットの送信元 IP アドレスは、アドレスグループ 0 のアドレスに変換されます。

```
[AC] interface vlan-interface 20
[AC-Vlan-interface20] nat outbound 2000 address-group 0
```

III. 設定の確認

Client A は WWW サーバにアクセスできますが、Client B はアクセスできないことを確認します。(詳細は省略します。)

すべての NAT 設定と統計情報を表示します。

[AC] display nat all

```
NAT address group information:
  Totally 1 NAT address groups.
  Address group ID: 0
    Port range: 1-65535
    Address information:
      Start address         End address
      202.38.1.2            202.38.1.3

NAT outbound information:
  Totally 1 NAT outbound rules.
  Interface: Vlan-interface20
    ACL: 2000
    Address group: 0
    Port-preserved: N    NO-PAT: N         Reversible: N
    Config status: Active

NAT logging:
  Log enable          : Disabled
  Flow-begin          : Disabled
  Flow-end            : Disabled
  Flow-active         : Disabled
  Port-block-assign   : Disabled
  Port-block-withdraw : Disabled
  Alarm               : Disabled
  NO-PAT IP usage     : Disabled

NAT mapping behavior:
  Mapping mode : Address and Port-Dependent
  ACL          : ---
  Config status: Active

NAT ALG:
  DNS         : Enabled
  FTP         : Disabled
  H323        : Disabled
  ICMP-ERROR  : Enabled
  ILS         : Disabled
  MGCP        : Disabled
  NBT         : Disabled
  PPTP        : Enabled
  RTSP        : Enabled
  RSH         : Disabled
  SCCP        : Disabled
  SIP         : Disabled
  SQLNET      : Disabled
  TFTP        : Disabled
  XDMCP       : Disabled
```

Client A が WWW サーバにアクセスしたときに生成される NAT セッション情報を表示します。

[AC] display nat session verbose

```
Initiator:
  Source      IP/port: 192.168.1.10/52992
  Destination IP/port: 200.1.1.10/2048
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
```

```
  Protocol: ICMP(1)
  Inbound interface: Vlan-interface10
Responder:
  Source      IP/port: 200.1.1.10/4
  Destination IP/port: 202.38.1.3/0
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: Vlan-interface20
State: ICMP_REPLY
Application: INVALID
Start time: 2012-08-15 14:53:29  TTL: 12s
Initiator->Responder:            1 packets         84 bytes
Responder->Initiator:            1 packets         84 bytes

Total sessions found: 1
```

目次

このセクションのページは**5-x-x** です。

22章 IPルーティングの基本 22-1
22.1 ルーティングテーブル 22-1
22.2 ルートの優先度 22-2
22.3 ルーティングテーブルの表示と維持 22-2

22章 IP ルーティングの基本

IP ルーティングはルーティングテーブルをもとにルータ上で IP パケットの転送を行います。この章では、ユニキャストルーティングプロトコルについて説明します。マルチキャストルーティングプロトコルの詳細については、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*5 ネットワーク接続*”の”*25 章 マルチキャストの概要*”を参照してください。

この章の“ルータ”は、アクセスコントローラ、アクセスコントローラモジュールを示します。

22.1 ルーティングテーブル

RIB (routing information base)はルート再帰、ルート再分配、ルート拡張情報を含んだグローバルルーティングテーブルと関連する情報が含まれます。ルータはルーティングテーブルから最適なルートを選択し、FIB (forwarding information base)テーブルに格納します。ルータはパケットを転送するために FIB テーブルを使用します。

表 22-1にルートのカテゴリを示します。

表 22-1 ルートのカテゴリ

基準	カテゴリ
宛先	• **ネットワークルート**—宛先がネットワークです。サブネットマスクは32ビット未満です。 • **ホストルート**—宛先がホストです。サブネットマスクは32ビットです。
宛先が直接接続されているかどうか	• **ダイレクトルート**—宛先が直接接続されています。 • **インダイレクトルート**—宛先が直接接続されていません。
作成元	• **ダイレクトルート**—ダイレクトルートがインタフェースのデータリンクプロトコルによって検出されました。インタフェースルートと呼ばれます。 • **スタティックルート**—管理者によって手動で設定されたルートです。 • **ダイナミックルート**—ルーティングプロトコルによって自動に検出されたルートです。

ルーティングテーブルの概要を表示する場合、**display ip routing-table** コマンドを使用します。

```
<AC> display ip routing-table

Destinations : 19        Routes : 19

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
0.0.0.0/32          Direct 0    0            127.0.0.1       InLoop0
```

```
1.1.1.0/24          Direct 0    0           1.1.1.1         GE1/0/1
1.1.1.0/32          Direct 0    0           1.1.1.1         GE1/0/1
1.1.1.1/32          Direct 0    0           127.0.0.1       InLoop0
1.1.1.255/32        Direct 0    0           1.1.1.1         GE1/0/1
2.2.2.0/24          Static 60   0           12.2.2.2        Vlan1
80.1.1.0/24         Static 10   0           80.1.1.1        Vlan10
...
```

ルーティングエントリは以下の項目が含まれます。

- **Destination**(宛先アドレス)—宛先ホストあるいはネットワークの IP アドレスです。
- **Mask**(ネットワークマスク)—IP アドレスのマスク長です。
- **Pre**(プリファレンス)—ルートの優先度です。同一宛先へのルートがある場合、最も高い優先度を持つルートが最適なルートとなります。
- **Cost**(コスト)— 宛先へのルートが複数あり、同一優先度である場合、最も小さいコストの値を持つルートが最適なルートとなります。
- **NextHop**(ネクストホップ)— ネクストホップの IP アドレスを示します。
- **Interface**(インタフェース)—IP パケットの転送に使用する出力先のインタフェースを示します。

22.2 ルートの優先度

スタティックルーティング、ダイナミックルーティングを含むルーティングプロトコルは、デフォルトで優先度を持ちます。同一宛先に複数のルートがある場合、ルータは最適なルートとして最も高い優先度を持つルートを選択します。

ダイレクトルートのプリファレンスは 0 で、変更できません。各スタティックルートとダイナミックルーティングプロトコルのプリファレンスを設定することができます。表 22-2にルートタイプとデフォルトのプリファレンスを示します。値が小さいほど優先度が高くなります。

表 22-2 ルートタイプとデフォルトルートプリファレンス

ルートタイプ	プリファレンス
Direct route	0
Multicast static route	1
Unicast static route	60
Unknown(信用されていない送信元からのルート)	256

22.3 ルーティングテーブルの表示と維持

すべての view で **display** コマンドを実行でき、user view で **reset** コマンドを実行できます。

操作	コマンド
ルーティングテーブルの情報を表示する	**display ip routing-table** [**verbose**]
標準IPv4 ACLで許可されているルーティング情報を表示する	**display ip routing-table acl** *acl-number* [**verbose**]

操作	コマンド
指定した宛先アドレスへのルート情報を表示する	**display ip routing-table** *ip-address* [*mask* | *mask-length*] [**longer-match**] [**verbose**]
指定した範囲内の宛先アドレスを持つルート情報を表示する	**display ip routing-table** *ip-address1* **to** *ip-address2* [**verbose**]
IPプレフィックスリストで許可されているルーティング情報を表示する	**display ip routing-table prefix-list** *prefix-list-name* [**verbose**]
ルートのルーティングプロトコルを表示する	**display ip routing-table protocol** *protocol* [**inactive** | **verbose**]
IPv4ルーティングテーブルの統計情報を表示する	**display ip routing-table** [**all-routes**] [**prefix**] **statistics**
IPv4ルーティングテーブルの統計情報を削除する	**reset ip routing-table statistics protocol** { *protocol* | **all** }

目次

このセクションのページは**5-x-x** です。

23章 スタティックルーティング 23-1
23.1 スタティックルートの設定 23-1
23.2 フローティングスタティックルートの設定 23-2
23.3 スタティックルートの表示と維持 23-2
23.4 基本的なスタティックルートの設定例 23-3

23章 スタティックルーティング

スタティックルートはマニュアル設定する必要があります。ネットワークの構成が簡単であれば、ネットワークを適切に動作させるため、スタティックルートの設定を行うことで問題なく運用が可能です。

ただし、スタティックルートはネットワークの変化に適応できません。ネットワーク障害やトポロジーの変化が起きた場合、宛先との通信ができなくなります。ネットワーク管理者がスタティックルートを修正する必要があります。

23.1 スタティックルートの設定

スタティックルートの設定を行う前に以下の設定が完了していることを確認してください。

- 関係するインタフェースの物理パラメータの設定
- 関係するインタフェースのリンクレイヤの設定
- 関係するインタフェースの IP アドレスの設定

以下にスタティックルートの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. スタティックルートを設定する	**ip route-static** *dest-address* { *mask-length* | *mask* } { *interface-type interface-number* [*next-hop-address* [**nexthop-index** *index-string*]] | *next-hop-address* [**nexthop-index** *index-string*] [**recursive-lookup** { **host-route** | **longest-match** }] } [**permanent** | **track** *track-entry-number*] [**preference** *preference*] [**tag** *tag-value*] [**recursive-lookup**] [**description** *text*]	デフォルト：設定なし **recursive-lookup host-route**キーワードと**recursive-lookup**キーワードの両方を指定することはできません。
3. （オプション設定項目）スタティックルートのデフォルトプリファレンスを設定する	**ip route-static default-preference** *default-preference*	デフォルト：60

操作	コマンド	補足
4．（オプション設定項目）デフォルトルートを含むすべてのルートを削除する	**delete static-routes all**	1つのスタティックルートを削除するには、**undo ip route-static**コマンドを使用します。 ⚠**注意**： このコマンドを実行すると、ネットワーク通信が中断され、パケット転送が失敗する場合があります。コマンドを実行する前に、ネットワークへの潜在的な影響を十分に理解していることを確認してください。

23.2 フローティングスタティックルートの設定

ルートバックアップを実装し、ネットワークの信頼性を向上させるには、次の作業を実行します。

デバイス上に宛先アドレスへのスタティックルートまたはダイナミックルートがすでに存在する場合は、優先度の低い別のスタティックルートをバックアップルートとして設定し、ネットワークの信頼性を向上させることができます。このバックアップスタティックルートはフローティングスタティックルートと呼ばれ、プライマリルートで障害が発生した場合にのみアクティブ化されます。プライマリルートが障害から回復すると、フローティングスタティックルートは非アクティブになり、データ転送はプライマリルートに切り替わります。

フローティングスタティックルートは、次のいずれかの方法で設定できます。

- 同じ宛先アドレスへの複数のスタティックルート用に異なる優先順位を設定します。優先順位の低いルートは、自動的にフローティングスタティックルートになります。
- デバイス上に宛先アドレスへのルートがすでに存在する場合は、同じ宛先アドレスに優先順位の低いスタティックルートを設定します。

フローティングスタティックルートを設定する場合は、ルートの優先順位の値をプライマリルートの優先順位の値より大きくする必要があります。詳細については、 スタティックルートの設定 を参照してください。

23.3 スタティックルートの表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
スタティックルート情報を表示する	**display ip routing-table protocol static** [**inactive** | **verbose**]

23.4 基本的なスタティックルートの設定例

I. ネットワーク要件

図 23-1に示すように、各ホストと AC 間で相互接続できるように、Switch と AC にスタティックルートを設定します。

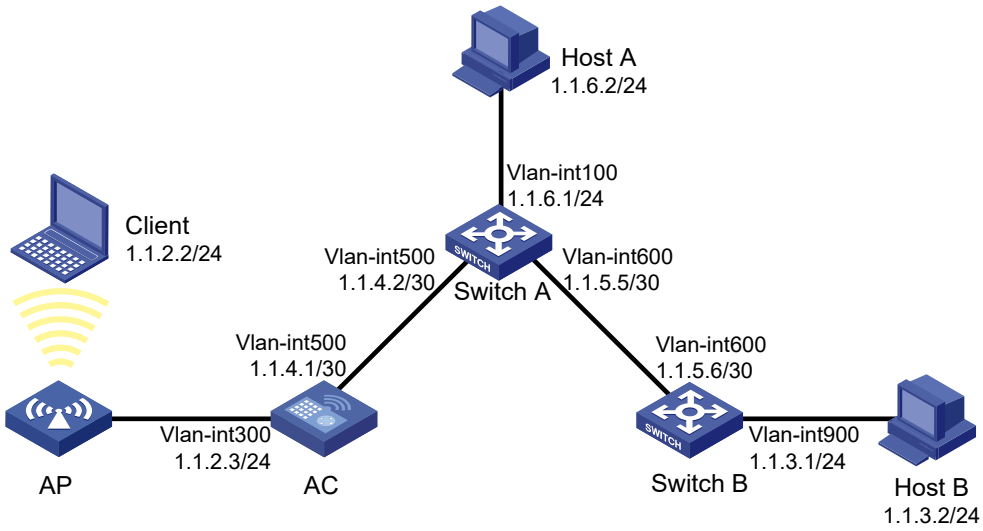


図 23-1 ネットワーク図

II. 設定手順

1)　インタフェースの IP アドレスを設定します。（詳細は省略します）
2)　スタティックルートを設定します。

AC にデフォルトルートを設定します。

```
<AC> system-view
[AC] ip route-static 0.0.0.0 0.0.0.0 1.1.4.2
```

Switch A に 2 つのスタティックルートを設定します。

```
<SwitchA> system-view
[SwitchA] ip route-static 1.1.2.0 255.255.255.0 1.1.4.1
[SwitchA] ip route-static 1.1.3.0 255.255.255.0 1.1.5.6
```

Switch B にデフォルトルートを設定します。

```
<SwitchB> system-view
[SwitchB] ip route-static 0.0.0.0 0.0.0.0 1.1.5.5
```

3)　Client、Host A、Host B にそれぞれ 1.1.2.3、1.1.6.1、1.1.3.1 のデフォルトゲートウェイアドレスを設定します。（詳細は省略します）

III. 設定の確認

AC のスタティックルートを表示します。

```
[AC] display ip routing-table protocol static

Summary Count : 1

Static Routing table Status : <Active>
Summary Count : 1

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
0.0.0.0/0           Static 60   0            1.1.4.2         Vlan500

Static Routing table Status : <Inactive>
Summary Count : 0
```

Switch A のスタティックルートを表示します。

```
[SwitchA] display ip routing-table protocol static

Summary Count : 2

Static Routing table Status : <Active>
Summary Count : 2

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
1.1.2.0/24          Static 60   0            1.1.4.1         Vlan500

Static Routing table Status : <Inactive>
Summary Count : 0
```

Host A で **ping** コマンドを使用し、Client への接続を確認します。（2 つのホストは Windows 2000 以上で動作していると仮定します。）

```
C:\Documents and Settings\Administrator>ping 1.1.2.2

Pinging 1.1.2.2 with 32 bytes of data:

Reply from 1.1.2.2: bytes=32 time=1ms TTL=126
Reply from 1.1.2.2: bytes=32 time=1ms TTL=126
Reply from 1.1.2.2: bytes=32 time=1ms TTL=126
Reply from 1.1.2.2: bytes=32 time=1ms TTL=126

Ping statistics for 1.1.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

Host A で **tracert** コマンドを使用し、Client への接続を確認します。

```
C:\Documents and Settings\Administrator>tracert 1.1.2.2

Tracing route to 1.1.2.2 over a maximum of 30 hops

  1    <1 ms    <1 ms    <1 ms  1.1.6.1
  2    <1 ms    <1 ms    <1 ms  1.1.4.1
  3     1 ms    <1 ms    <1 ms  1.1.2.2

Trace complete.
```

目次

このセクションのページは**5-x-x** です。

24章 デフォルトルート 24-1

24章 デフォルトルート

デフォルトルートはルーティングテーブルの指定したルーティングエントリにマッチしないパケットを転送するのに使用されます。デフォルトルートが設定されていない場合、ルーティングエントリにマッチしないパケットは廃棄されます。

デフォルトルートは以下の方法で設定することができます。

- ネットワーク管理者が宛先アドレスとマスクを 0.0.0.0 に設定します。詳細は QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*5 ネットワーク接続*”の”*23 章 スタティックルーティング*”を参照してください。

目次

このセクションのページは **5-x-x** です。

25 章 マルチキャストの概要 25-1
25.1 マルチキャストの導入 25-1
25.1.1 情報通信技術 25-1
25.1.2 マルチキャストの機能 25-3
25.1.3 マルチキャストの利点とアプリケーション 25-4
25.2 マルチキャストモデル 25-5
25.2.1 ASM モデル 25-5
25.2.2 SFM モデル 25-5
25.2.3 SSM モデル 25-5
25.3 マルチキャストアドレス 25-6
25.3.1 IP マルチキャストアドレス 25-6
25.3.2 イーサネットマルチキャスト MAC アドレス 25-8
25.4 マルチキャストプロトコル 25-9
25.4.1 レイヤ 3 マルチキャストプロトコル 25-10
25.4.2 レイヤ 2 マルチキャストプロトコル 25-11
25.5 マルチキャストパケット転送メカニズム 25-12
25.6 IP マルチキャストアーキテクチャ 25-12
25.7 マルチキャストの一般的な表記方法 25-13

25章 マルチキャストの概要

25.1 マルチキャストの導入

ユニキャストおよびブロードキャストと共存する技術として、マルチキャスト技術はポイントツーマルチポイントデータ送信の問題を効果的に対処します。ネットワーク上で効率の高いポイントツーマルチポイントデータ送信を行うことで、マルチキャストはネットワーク帯域幅を大きく節約し、ネットワーク負荷を低減します。

マルチキャスト技術により、ネットワークオペレータは新しい付加価値のあるサービスを容易に提供することが可能となります。たとえば、Web キャスティング、Web TV、遠隔学習、遠隔医療、Web ラジオ、リアルタイムビデオカンファレンスなどの他に、帯域幅や時間が重要な情報サービスです。

25.1.1 情報通信技術

情報通信技術はユニキャスト、ブロードキャスト、マルチキャストを含みます。

I. ユニキャスト

ユニキャストでは、情報を必要とする各ホスト（Receiver）へ情報送信元（Source）から情報のコピーが個別に送信されます。

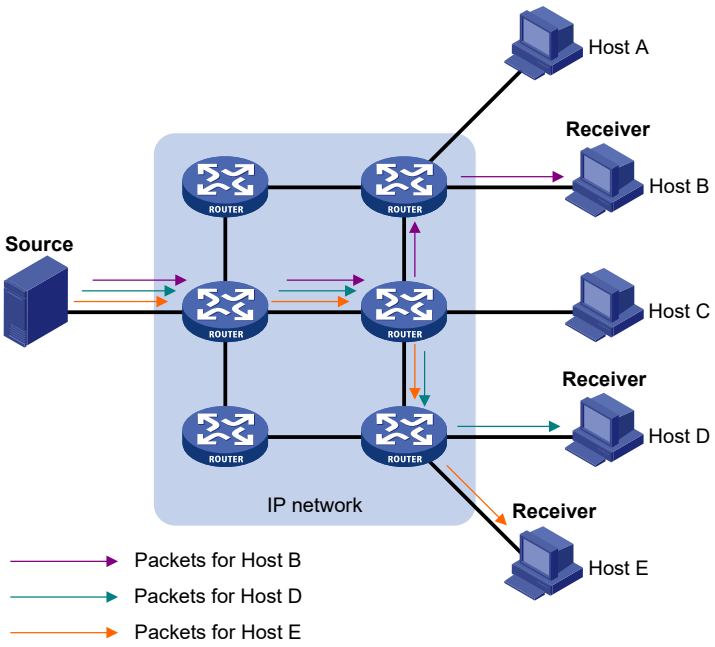


図 25-1 ユニキャスト通信

図 25-1 において、Host B と Host D と Host E は情報を必要とします。個別の通信チャネルは情報送信元から各ホストに対して確立する必要があります。

ユニキャスト通信では、ネットワーク上のトラフィックは情報を必要とするホストの数に比例します。非常に多くのユーザが情報を必要とする場合、情報送信元は各ユーザに同じ情報のコピーを送信する必要があります。これは情報送信元とネットワーク帯域幅に相当な負荷をかけることになります。

ユニキャスト通信は情報のバッチ送信には適していません。

II. ブロードキャスト

ブロードキャストでは、情報を必要としていないホストがあったとしても、情報送信元からネットワーク上のすべてのホストに情報が送信されます。

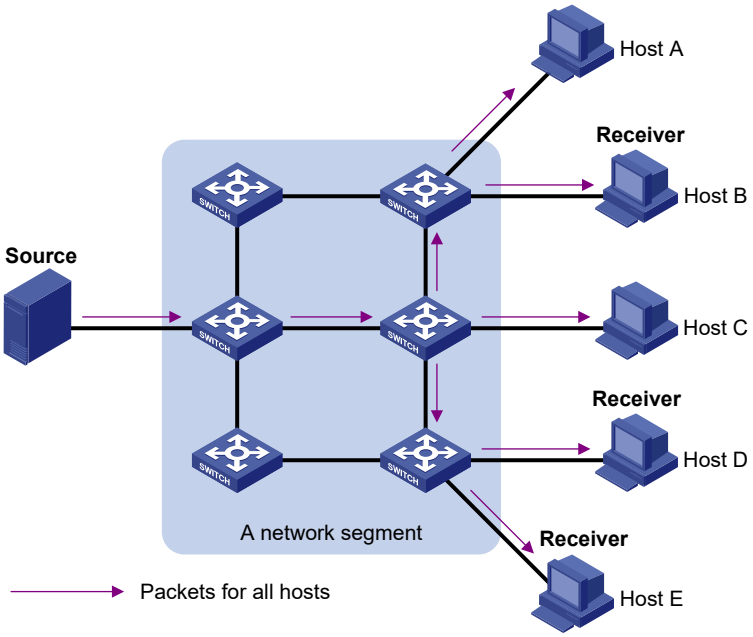


図 25-2 ブロードキャスト通信

図 25-2 に示すように、Host B と Host D と Host E は情報を必要とします。情報が同一ネットワーク上にブロードキャストされた場合、Host A と Host C も情報を受信してしまいます。これにより、情報セキュリティの問題に加えて、同一ネットワーク上でトラフィックフラッディングも発生してしまいます。

特定のホストにデータを送信する場合、ブロードキャストは効率的ではありません。ブロードキャストの送信は多くのネットワークリソースを浪費します。

III. マルチキャスト

マルチキャストはネットワークリソースの消費を最小限に抑えてポイントツーマルチポイント送信を実現することができます。ネットワーク上のいくつかのホストがマルチキャスト情報を必要とした場合、情報の送信者あるいはマルチキャスト送信元は情報のコピー

を 1 つだけ送信します。マルチキャストルーティングプロトコルによってマルチキャスト配信ツリーが構成され、ツリーが分岐するノードでのみパケットがコピーされます。

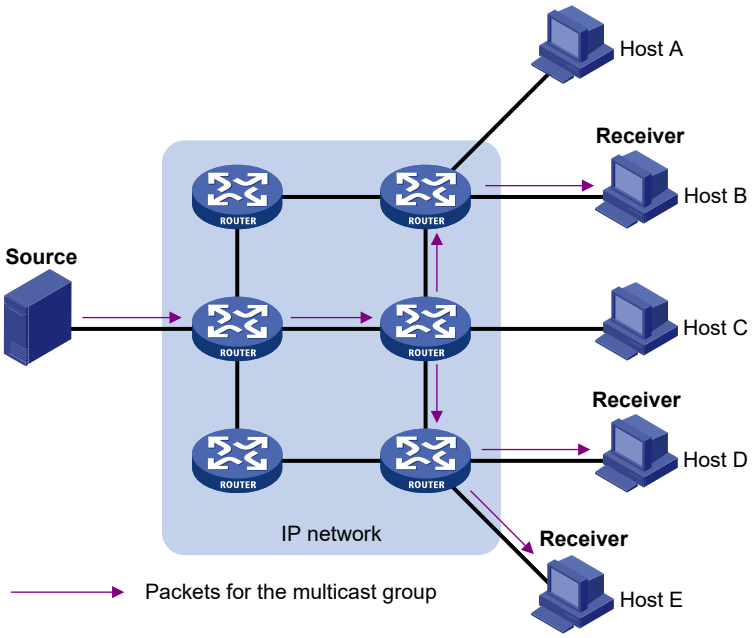


図 25-3 マルチキャスト通信

マルチキャスト送信元（Source）は情報のコピーを 1 つだけマルチキャストグループへ送信します。情報の受信者である Host B、Host D、Host E は、マルチキャストグループに参加する必要があります。ネットワーク上のルータはグループメンバの配置にもとづいて情報を複製して転送します。最終的に、情報は Host B と Host D と Host E に正確に送信されます。

要約すると、マルチキャストの利点を以下に示します。

- **ユニキャストからの利点** － ユニキャストに対しては、マルチキャストトラフィックは送信元から可能な限り遠いノードに流れてから複製、配信されるため、ホストの数が増加した場合でも送信元とネットワークの負荷を増やすことはありません。
- **ブロードキャストからの利点** － ブロードキャストに対しては、必要としている受信者だけにマルチキャストデータが送信されるので、マルチキャストは合理的にネットワーク帯域幅を使用し、ネットワークセキュリティを強化します。さらに、ブロードキャストの配信は同一ネットワークに限定されますが、マルチキャストの配信は同一ネットワークに限定されません。

25.1.2 マルチキャストの機能

- マルチキャストグループは IP マルチキャストアドレスによって識別されて配置されるマルチキャストレシーバです。ホストはマルチキャストグループ宛に送信されたマルチキャストデータを受信できるようになる前に、マルチキャストグループのメンバになるためにマルチキャストグループに参加します。通常、マルチキャスト送信元はマルチキャストグループに参加する必要はありません。
- マルチキャスト送信元は情報の送信者です。マルチキャスト送信元は同時に複数のマルチキャストグループにデータを送信することができます、そして、複数のマルチキ

ャスト送信元は同時に同一のマルチキャストグループにデータを送信することができます。

- グループメンバは動的です。ホストは、いつでもマルチキャストグループに参加あるいは離脱することができます。マルチキャストグループは、地理的な制約を受けません。
- レイヤ 3 マルチキャストをサポートするルータまたはレイヤ 3 スイッチは、マルチキャストルータまたはレイヤ 3 マルチキャスト装置と呼ばれます。マルチキャストルーティング機能の提供に加えて、マルチキャストルータはグループメンバに所属しているスタブサブネットのマルチキャストグループメンバを管理することもできます。マルチキャストルータ自身は、マルチキャストグループメンバになることができます。

マルチキャストの概念をより良く理解するために、マルチキャスト配信を TV 番組の配信に例えることができます。

表 25-1 TV 番組の配信とマルチキャスト通信の比較

TV 番組の配信	マルチキャスト配信
TV 局がチャンネルを介して TV 番組を放送します。	マルチキャスト送信元がマルチキャストグループにマルチキャストデータを送信します。
ユーザが TV をチャンネルに合わせます。	レシーバがマルチキャストグループに参加します。
チャンネルを介してTV 局から放送される TV 番組の視聴をユーザが開始します。	送信元からマルチキャストグループに送信されたマルチキャストデータをレシーバが受信し始めます。
ユーザが TV の電源を切るか、他のチャンネルに合わせます。	レシーバがマルチキャストグループから離脱するか、他のグループに参加します。

25.1.3 マルチキャストの利点とアプリケーション

I. マルチキャストの利点

- **効率の向上** － 情報送信元サーバとネットワーク装置の CPU 負荷を低減します。
- **最適なパフォーマンス** － 冗長なトラフィックを低減します。
- **配信アプリケーション** － 最小限のネットワークリソースで、ポイントツーマルチポイントアプリケーションを可能にします。

II. マルチキャストアプリケーション

- マルチメディアとストリーミングアプリケーションがあります。たとえば Web TV、Web ラジオ、リアルタイムビデオ/オーディオ会議などがあります。
- 通信教育や遠隔医療などの研修および協力運用の通信があります。
- データウェアハウスと財務アプリケーション（株価情報）があります。
- その他のポイントツーマルチポイントデータ配信アプリケーションがあります。

25.2 マルチキャストモデル

レシーバ（受信者）がマルチキャスト送信元をどのように扱うかによって、ASM（any-source multicast）、SFM（source-filtered multicast）、SSM（source-specific multicast）の 3 つのマルチキャストモデルがあります。

25.2.1 ASM モデル

ASM モデルでは、すべてのマルチキャスト送信元はマルチキャストグループへ情報を送信できます。レシーバ（受信者）がグループアドレスによって識別されたマルチキャストグループに参加し、そのマルチキャストグループ宛てのマルチキャスト情報を取得することができます。このモデルでは、レシーバ（受信者）はあらかじめマルチキャスト送信元の位置を認識していません。

25.2.2 SFM モデル

SFM モデルは ASM モデルから派生しています。マルチキャスト送信元の観点からは、2 つのモデルは同じマルチキャストメンバシップのアーキテクチャです。

SFM モデルは ASM モデルの機能拡張版です。SFM モデルでは、上位レイヤソフトウェアが受信したマルチキャストの送信元アドレスをチェックし、指定した送信元からのマルチキャストトラフィックを許可または拒否します。これにより、レシーバ（受信者）は一部のマルチキャスト送信元からのみマルチキャストデータを受信することができます。レシーバ（受信者）の観点からは、マルチキャスト送信元がすべて有効というわけではありません。マルチキャスト送信元はフィルタされます。

25.2.3 SSM モデル

SSM モデルは、マルチキャストレシーバが、必要となるマルチキャスト送信元を指定することができる転送サービスを提供します。

SSM モデルと ASM モデルの根本的な違いは、SSM モデルではレシーバ（受信者）が何らかの方法でマルチキャスト送信元の位置を既に知っていることです。これは SSM モデルと ASM モデルの主な相違点です。さらに、SSM モデルでは ASM /SFM モデルの場合とは異なるマルチキャストアドレス範囲を使用します。レシーバと指定のマルチキャスト送信元の間に専用のマルチキャスト転送パスが確立されます。

25.3 マルチキャストアドレス

25.3.1 IP マルチキャストアドレス

I. IPv4 マルチキャストアドレス

IANA（Internet Assigned Numbers Authority）は IPv4 マルチキャストにクラス D アドレス（224.0.0.0～239.255.255.255）を割り当てました。

表 25-2 クラス D IP アドレスブロックと説明

アドレスブロック	説明
224.0.0.0 ～ 224.0.0.255	予約されている永久的なグループアドレスです。IPアドレス 224.0.0.0 は予約されており、その他のIPアドレスはルーティングプロトコルによって、そしてトポロジ検索、プロトコルの維持管理などに使用できます。一般的な永久グループアドレスの一覧は表 25-3に示されています。このブロックアドレス宛のパケットは、IPヘッダのTTL （Time to Live） 値に関わらず、ローカルサブネットを越えて転送されることはありません。
224.0.1.0 ～ 238.255.255.255	グローバルスコープグループアドレスです。このブロックには2種類の指定グループアドレスがあります。 ● **232.0.0.0/8** － SSMグループアドレス ● **233.0.0.0/8** － Glopグループアドレス
239.0.0.0 ～ 239.255.255.255	管理スコープのマルチキャストアドレスです。これらのアドレスはグローバルにではなくローカルに一意とみなされ、異なる組織が管理しているドメインで衝突を起こすことなく再利用できます。詳細はRFC2365を参照してください。

🕮 **メモ：**

“Glop”は、異なる自律システム（AS）間でマルチキャストアドレスを割り当てるメカニズムです。233.0.0.0 の中間の 2 バイトに AS の数字を入力することで、その AS に 255 のマルチキャストアドレスが得られます。詳細については、RFC2770 を参照してください。

表 25-3 一般的な予約済みマルチキャストグループアドレス

アドレス	説明
224.0.0.1	ホストとルータを含む、サブネット上のすべてのシステムです。
224.0.0.2	サブネット上のすべてのマルチキャストルータです。
224.0.0.3	未割り当てです。
224.0.0.4	DVMRP（Distance Vector Multicast Routing Protocol）ルータです。
224.0.0.5	OSPF（Open Shortest Path First）ルータです。
224.0.0.6	OSPF指定ルータおよびバックアップ指定ルータです。
224.0.0.7	ST（Shared Tree）ルータです。
224.0.0.8	STホストです。
224.0.0.9	RIPv2（Routing Information Protocol version 2）ルータです。
224.0.0.11	モバイルエージェントです。

アドレス	説明
224.0.0.12	DHCP（Dynamic Host Configuration Protocol）サーバまたはリレーエージェントです。
224.0.0.13	すべてのPIM（Protocol Independent Multicast）ルータです。
224.0.0.14	RSVP（Resource Reservation Protocol）のカプセル化です。
224.0.0.15	すべてのCBT（Core-Based Tree）ルータです。
224.0.0.16	指定されたSBM（Subnetwork Bandwidth Management）です。
224.0.0.17	すべてのSBMです。
224.0.0.18	VRRP（Virtual Router Redundancy Protocol）です。

II. IPv6 マルチキャストアドレス

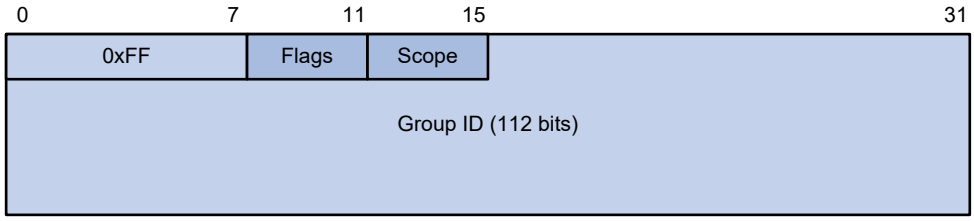


図 25-4 IPv6 マルチキャストフォーマット

以下に IPv6 マルチキャストアドレスのフィールドの説明を示します。

- **0xFF** ー 上位 8 ビットは 11111111 です。
- **Flags** ー 4 ビットのフラグフィールドです。



図 25-5 Flags フィールドフォーマット

表 25-4 フラグフィールドの説明

ビット	説明
0	予約済みです。常に0です。
R	• 0の場合、RPアドレスが埋め込まれていないIPv6マルチキャストアドレスであることを示します。 • 1の場合、RPアドレスが埋め込まれているIPv6マルチキャストアドレスであることを示します。（PビットとTビットも1にセットされます）
P	• 0の場合、ユニキャストプレフィックスにもとづかないIPv6マルチキャストアドレスであることを示します。 • 1の場合、ユニキャストプレフィックスにもとづくIPv6マルチキャストアドレスであることを示します。（Tビットも1にセットされます）
T	• 0の場合、IANAによって永続的に割り当てられた既知のIPv6マルチキャストアドレスであることを示します。 • 1の場合、一時的あるいはダイナミックに使用される（非永続的な）IPv6マルチキャストアドレスであることを示します。

- **Scope** – 4 ビットの IPv6 マルチキャストアドレスの有効範囲を示すフィールドです。

表 25-5 Scope フィールドの値

値	意味
0、F	予約済み
1	インタフェースローカル
2	リンクローカル
3	サブネットローカル
4	アドミンローカル
5	サイトローカル
6、7、9 ～ D	未割り当て
8	組織ローカル
E	グローバル

- **Group ID** – 112 ビットで IPv6 マルチキャストグループを識別します。Scope フィールドが定義する範囲で IPv6 マルチキャストグループを一意に識別します。

25.3.2 イーサネットマルチキャスト MAC アドレス

イーサネットマルチキャストレイヤアドレスは、データリンク MAC で同じマルチキャストグループに属する受信者を識別します。

I. IPv4 マルチキャスト MAC アドレス

IANA によって定義されているように、IPv4 マルチキャスト MAC アドレスの上位 24 ビットは 0x01005E、25 ビット目は 0x0、および下位 23 ビットはマルチキャスト IPv4 アドレスの低位 23 ビットです。

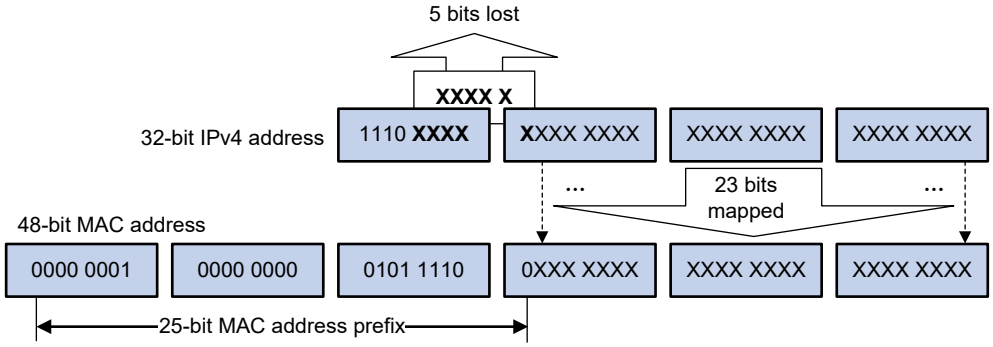


図 25-6 IPv4 アドレスと MAC アドレスのマッピング

IPv4 マルチキャストアドレスの上位 4 ビットは 1110 で固定です。IPv4 アドレスと MAC アドレスのマッピングで使用され、IPv4 マルチキャストアドレスの 5 ビットは失われます。その結果、32 個のマルチキャスト IPv4 アドレスは同じ MAC アドレスにマッピングされます。そのため、レイヤ 2 マルチキャスト転送においては、他の IPv4 マルチキャス

トグループに宛てたマルチキャストデータを受け取る場合があります。そのような冗長データは上位層によってフィルタする必要があります。

II. IPv6 マルチキャスト MAC アドレス

IPv6 マルチキャスト MAC アドレスの上位 16 ビットは 0x3333 です。下位 32 ビットはマルチキャスト IPv6 アドレスの下位 32 ビットにマッピングされます。これは IPv4 アドレスから MAC アドレスのマッピングと同じように、IPv6 から MAC アドレスのマッピングが重複する問題があります。

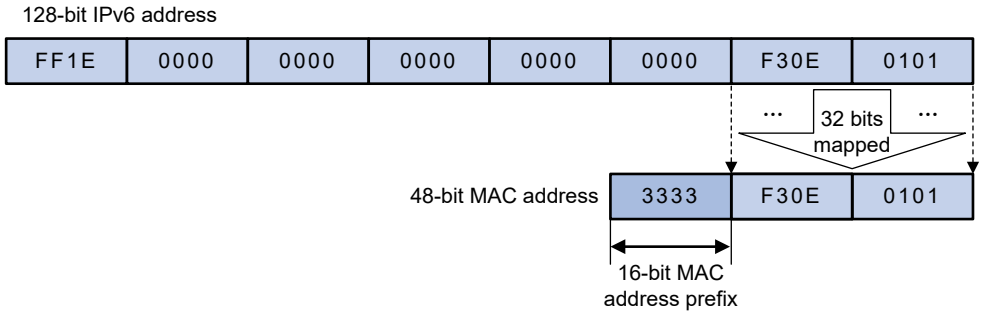


図 25-7 IPv6 アドレスと MAC アドレスのマッピング例

25.4 マルチキャストプロトコル

注意：

装置はレイヤ 3 マルチキャストプロトコルと以下に示すレイヤ 2 マルチキャストプロトコルをサポートしていません。

- マルチキャスト VLAN
- IPv6 マルチキャスト VLAN
- PIM snooping
- IPv6 PIM snooping

マルチキャストプロトコルは以下のカテゴリに分けられます。

- レイヤ 3、レイヤ 2 マルチキャストプロトコル
  - □ ネットワークレイヤで動作する IP マルチキャストのレイヤ 3 マルチキャスト

    レイヤ 3 マルチキャストプロトコル － IGMP、MLD、PIM、IPv6 PIM、MSDP、MBGP、IPv6 MBGP
  - □ データリンクレイヤで動作する IP マルチキャストのレイヤ 2 マルチキャスト

    レイヤ 2 マルチキャストプロトコル － IGMP snooping、MLD snooping、PIM snooping、IPv6 PIM snooping、マルチキャスト VLAN、IPv6 マルチキャスト VLAN
- IPv4、IPv6 マルチキャストプロトコル
  - □ **IPv4 ネットワーク** － IGMP snooping、PIM snooping、マルチキャスト VLAN、IGMP、PIM、MSDP、MBGP

- **IPv6 ネットワーク** – MLD snooping、IPv6 PIM snooping、IPv6 マルチキャスト VLAN、MLD、IPv6 PIM、IPv6 MBGP

この章ではレイヤ 2、レイヤ 3 マルチキャストプロトコルの一般的なアプリケーションと機能について記載します。レイヤ 2 マルチキャストプロトコルに関する詳細は、関連する章を参照してください。

25.4.1 レイヤ 3 マルチキャストプロトコル

レイヤ 3 マルチキャストプロトコルには、マルチキャストグループ管理プロトコルやマルチキャストルーティングプロトコルがあります。

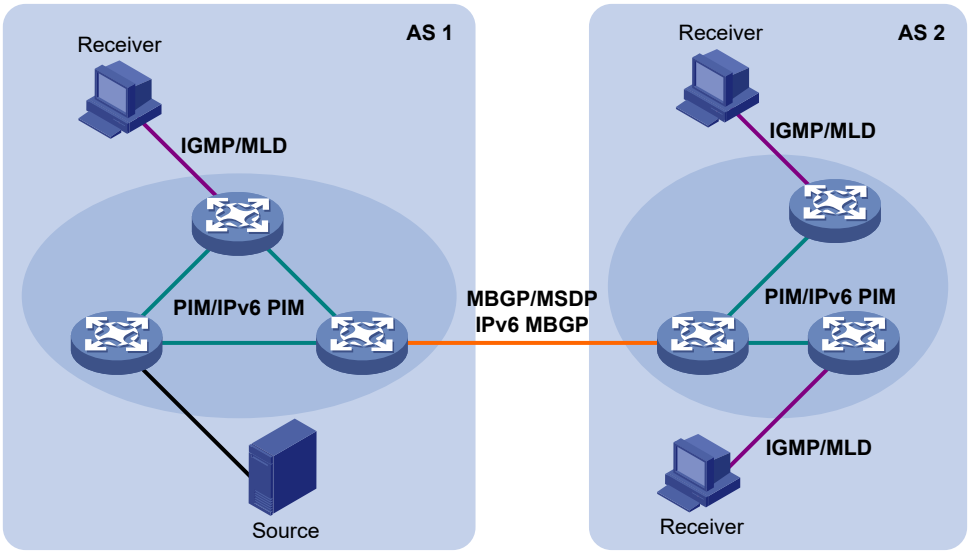


図 25-8 レイヤ 3 マルチキャストプロトコルの位置

- マルチキャストグループ管理プロトコル

通常は、IGMP（internet group management protocol）、MLD（multicast listener discovery protocol）はマルチキャストグループ管理プロトコルです。通常、これらのプロトコルは、ホストとレイヤ 3 マルチキャスト装置の間でグループメンバシップを確立して維持するメカニズムを定義します。

- マルチキャストルーティングプロトコル

マルチキャストルーティングプロトコルはレイヤ 3 マルチキャスト装置上で動作し、マルチキャストルートを確立して維持します。そして、マルチキャストパケットを正確に効率よく転送します。マルチキャストルートは、データ送信元から複数のレシーバまでループのないデータ転送パス（マルチキャスト配信ツリーとして知られます。）を構成します。

ASM モデルでは、マルチキャストルートにはドメイン内ルートとドメイン間ルートが含まれます。

- ドメイン内マルチキャストルーティングプロトコルは、マルチキャスト送信元を検出し、AS 内でマルチキャスト配信ツリーを構築して、マルチキャストデータを受信者に配信します。さまざまな成熟したドメイン内マルチキャストルーティングプロトコルの中で、PIM が最も広く使用されています。転送メカニズムに基

づいて、PIM にはデンスモード (多くの場合、PIM-DM と呼ばれる) とスパースモード (多くの場合、PIM-SM と呼ばれる) があります。

- ドメイン間マルチキャストルーティングプロトコルは、2 つの AS 間でマルチキャスト情報を配信するために使用されます。これまでのところ、成熟したソリューションには Multicast Source Discovery Protocol (MSDP) と MBGP が含まれています。MSDP は異なる AS 間でマルチキャスト送信元情報を伝播します。MBGP は、異なる AS 間でマルチキャストルーティング情報を交換するための MP-BGP を拡張したものです。

SSM モデルでは、マルチキャストルートはドメイン内ルートとドメイン間ルートに分けられません。受信者はマルチキャスト送信元の位置を知っているため、PIM-SM を介して確立されたチャネルはマルチキャスト情報の転送で十分です。

25.4.2 レイヤ 2 マルチキャストプロトコル

レイヤ 2 マルチキャストプロトコルには、IGMP Snooping、MLD Snooping、PIM Snooping、IPv6 PIM Snooping、マルチキャスト VLAN、IPv6 マルチキャスト VLAN があります。

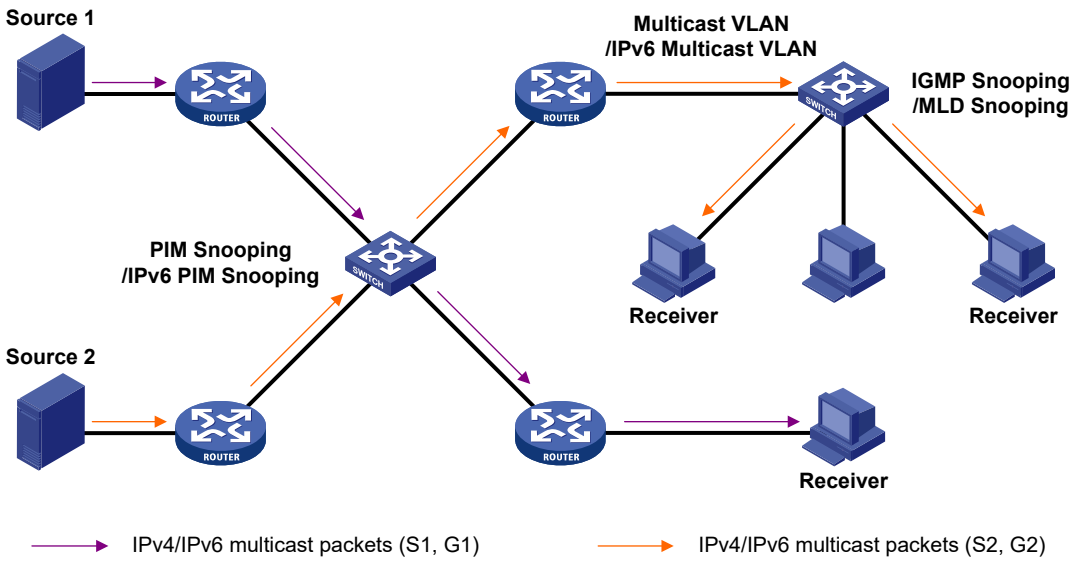


図 25-9 レイヤ 2 マルチキャストプロトコルの位置

- IGMP snooping、MLD snooping

IGMP Snooping および MLD Snooping はレイヤ 2 装置で動作するマルチキャスト構成メカニズムです。ホストとレイヤ 3 マルチキャスト装置の間で交換される IGMP または MLD メッセージをモニタ、解析することによって、マルチキャストグループを管理、制御します。このメカニズムはレイヤ 2 ネットワークでマルチキャストデータのフラッディングを制御するのに効率的です。

- PIM snooping、IPv6 PIM snooping

PIM Snooping および IPv6 PIM Snooping はレイヤ 2 装置で動作します。IGMP snooping または MLD snooping と連携して、受信した PIM メッセージを解析します。次に PIM snooping ルーティングエントリや IPv6 PIM snooping ルーティングエントリに、指定し

たマルチキャストデータに関連するポートのみを追加します。これによって、マルチキャストデータは、関連するポートに対してのみ転送します。

- マルチキャスト VLAN、IPv6 マルチキャスト VLAN

異なる VLAN に同一グループのマルチキャストレシーバが存在するところで、マルチキャストネットワークのレイヤ 2 装置でマルチキャスト VLAN、IPv6 マルチキャスト VLAN が動作します。これらのプロトコルでは、レイヤ 3 マルチキャスト装置はレイヤ 2 装置のマルチキャスト VLAN または IPv6 マルチキャスト VLAN へマルチキャストデータのコピーを 1 つだけ送信します。これにより、レイヤ 3 装置上のネットワーク帯域幅の浪費や余分な負荷を回避します。

25.5 マルチキャストパケット転送メカニズム

マルチキャストモデルでは、通常、マルチキャストグループの受信ホストはネットワーク上の異なる領域に配置されます。これらは同じマルチキャストグループアドレスによって識別されます。これらの受信者にマルチキャストパケットを配信するために、マルチキャスト送信元はマルチキャストデータを、宛先アドレスとしてマルチキャストグループアドレスを持つ IP パケットにカプセル化します。転送パス上のマルチキャストルータは、受信インタフェースが複数の送信インタフェースを介して受信するマルチキャストパケットを転送します。ユニキャストモデルと比較して、マルチキャストモデルは以下の点でより複雑です。

- ネットワーク上でのマルチキャストパケット伝送を保証するために、マルチキャスト転送をガイドするために異なるルーティングテーブルが使用されます。これらのルーティングテーブルには、ユニキャストルーティングテーブル、マルチキャスト用のルーティングテーブル(たとえば、MBGP ルーティングテーブル)、およびスタティックマルチキャストルーティングテーブルが含まれます。
- 異なるインタフェースで受信した異なるピアからの同じマルチキャスト情報を処理するために、マルチキャスト装置は各マルチキャストパケットに対して RPF チェックを実行します。RPF チェックの結果によって、パケットが転送されるか破棄されるかが決まります。RPF チェックメカニズムは、ほとんどのマルチキャストルーティングプロトコルがマルチキャスト転送を実装するための基礎となります。

25.6 IPマルチキャストアーキテクチャ

IP マルチキャストは以下の問題を解決します。

- マルチキャスト送信元はどこに情報を送信するべきか？（マルチキャストアドレッシング）
- ネットワーク上にはどんなレシーバ（受信者）が存在するか？（ホストレジストレーション）
- レシーバが受信する必要があるマルチキャストデータのマルチキャスト送信元（送信元）がどこにいるのか？（マルチキャスト送信元ディスカバリ）
- 情報がどのようにしてレシーバ（受信者）に転送されるのか？（マルチキャストルーティング）

IP マルチキャストはエンドツーエンドサービスの 1 つです。マルチキャストアーキテクチャには以下の 4 つのパートがあります。

- **アドレッシングメカニズム** － マルチキャスト送信元はマルチキャストアドレスを介してレシーバのグループへ情報を送信します。
- **ホストレジストレーション** － レシーバホストはマルチキャストグループへの参加と離脱を動的に行うことができます。このメカニズムはグループメンバシップ管理の基礎になります。
- **マルチキャストルーティング** － マルチキャスト送信元からレシーバへマルチキャストデータを配信するために、マルチキャスト配信ツリー（ネットワーク上でのマルチキャストデータの転送パスツリー）が構築されます。
- **マルチキャストアプリケーション** － ビデオ会議などのマルチキャストアプリケーションをサポートするソフトウェアシステムを、マルチキャスト送信元とレシーバホスト（受信者）にインストールする必要があります。そして、TCP/IP スタックはマルチキャストデータの送受信をサポートする必要があります。

25.7 マルチキャストの一般的な表記方法

マルチキャストでは一般的に 2 つの表記法が使用されます。

- **(*, G)** － RPT（rendezvous point tree）または、あらゆるマルチキャスト送信元がマルチキャストグループ G へ送信したマルチキャストパケットを表します。（*）はあらゆるマルチキャスト送信元、（G）は特定のマルチキャストグループを表します。
- **(S, G)** － SPT（shortest path tree）または、マルチキャスト送信元 S がマルチキャストグループ G へ送信したマルチキャストパケットを表します。（S）は特定のマルチキャスト送信元、（G）は特定のマルチキャストグループを表します。

目次

このセクションのページは **5-x-x** です。

26 章 IGMP スヌーピング 26-1
26.1 概要 26-1
26.1.1 IGMP snooping のポート 26-1
26.1.2 IGMP snooping の動作 26-3
26.2 プロトコルと標準 26-5
26.3 IGMP snooping 設定作業リスト 26-5
26.4 IGMP snooping の基本機能の設定 26-5
26.4.1 IGMP snooping の有効化 26-6
26.4.2 IGMP snooping のバージョンの設定 26-6
26.4.3 IGMP snooping 転送エントリの最大数の設定 26-7
26.4.4 IGMP last member クエリ間隔の設定 26-7
26.5 IGMP snooping ポート機能の設定 26-8
26.5.1 ダイナミックポートのエージングタイマの設定 26-8
26.5.2 スタティックポートの設定 26-9
26.5.3 シミュレーティッドメンバホストの設定 26-9
26.5.4 fast-leave 処理の有効化 26-10
26.6 IGMP snooping クエリの設定 26-11
26.6.1 設定要件 26-11
26.6.2 IGMP snooping クエリアの有効化 26-11
26.6.3 IGMP クエリと response のパラメータの設定 26-12
26.7 IGMP メッセージのパラメータの設定 26-13
26.7.1 設定要件 26-13
26.7.2 IGMP メッセージの送信元 IP アドレスの設定 26-13
26.7.3 IGMP メッセージの 802.1p 優先度の設定 26-14
26.8 IGMP snooping ポリシーの設定 26-15
26.8.1 マルチキャストグループポリシーの設定 26-15
26.8.2 未知のマルチキャストデータ廃棄機能の有効化 26-16
26.8.3 IGMP report 抑制機能の有効化 26-17
26.8.4 ポートで参加可能なマルチキャストグループの最大数の設定 26-17
26.8.5 マルチキャストグループ置き換え機能の有効化 26-18
26.9 送信 IGMP プロトコルパケットの DSCP 値の設定 26-18
26.10 IGMP snooping の表示と維持 26-19
26.11 IGMP snooping 設定例 26-20
26.11.1 ネットワーク要件 26-20
26.11.2 設定手順 26-20
26.11.3 設定の確認 26-22
26.12 IGMP snooping のトラブルシューティング 26-22
26.12.1 レイヤ 2 マルチキャスト転送ができない 26-22
26.12.2 マルチキャストグループポリシーが動作しない 26-22

26章 IGMP スヌーピング

26.1 概要

IGMP snooping はマルチキャスト転送時のネットワークへの負荷を軽減するためのメカニズムです。図 26-1 に示すように、IGMP snooping を有効にしない場合、マルチキャストパケットはすべてのポートにフラッディングされます。IGMP snooping を有効にすると、既知のマルチキャストグループからのマルチキャストパケットは、Receiver レシーバへのみ転送されます。IGMP snooping を有効にすることで、不要なマルチキャストトラフィックのフラッディングを抑止し、ネットワークを効率的に利用することができます。

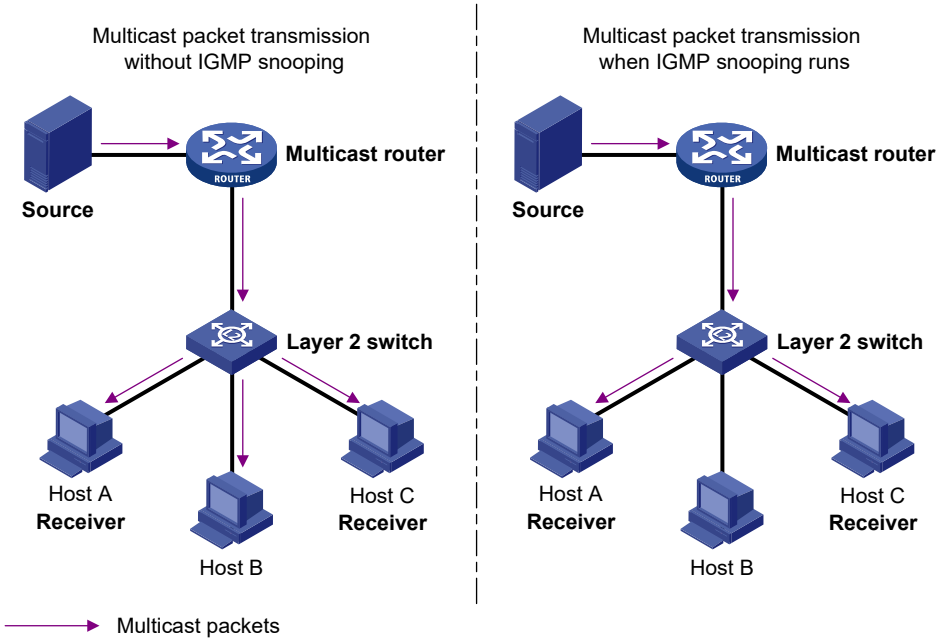


図 26-1 IGMP snooping を有効にする前と有効にした後のマルチキャストパケットの転送

26.1.1 IGMP snooping のポート

図 26-2 に示すように、IGMP snooping は Device A と Device B で動作し、Host A と Host C がマルチキャストグループのホストとするレシーバです。IGMP snooping のポートはメンバポートとルータポートに分類されます。

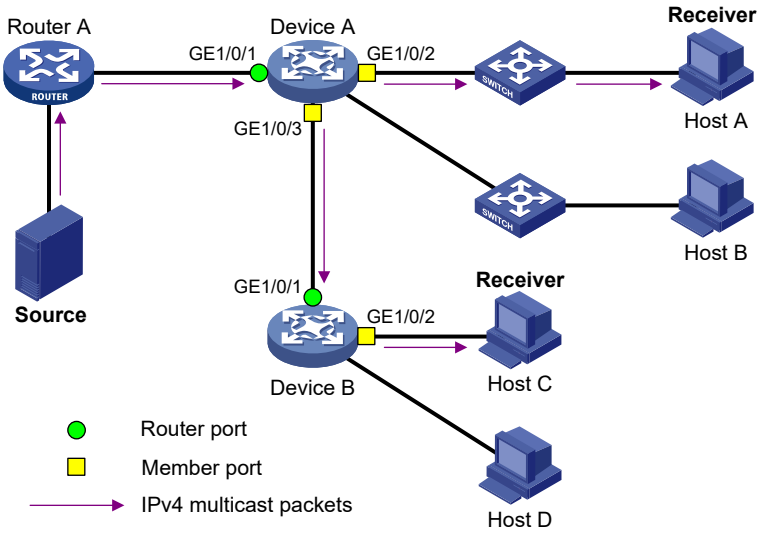


図 26-2 IGMP snooping 関連ポート

I. ルータポート

IGMP snooping のレイヤ 2 装置で、レイヤ 3 マルチキャストへのポートはルータポートと呼ばれます。図 26-2 では、Device A の GigabitEthernet 1/0/1 と Device B の GigabitEthernet 1/0/1 がルータポートです。

ルータポートは以下のタイプがあります。

- **ダイナミックルータポート**－ポートで 0.0.0.0 以外の送信元アドレスの IGMP general クエリを受信する、あるいは PIM Hello メッセージを受信した場合、ダイナミックルータポートリストにポートを追加します。同時にポートのタイマを開始します。タイマが満了する前にメッセージを受信しない場合、ポートはダイナミックルータポートリストからポートを削除します。
- **スタティックルータポート**－ポートがルータポートとしてスタティックに設定された場合、スタティックルータポートリストにポートを追加します。スタティックルータポートはエージアウトしません。手動でのみ削除することができます。

IGMP snooping のルータポートをレイヤ 3 インタフェースのルーテッドインタフェースと混同しないでください。IGMP snooping のルータポートはレイヤ 2 インタフェースです。

II. メンバポート

IGMP snooping のレイヤ 2 装置で、マルチキャストレシーバへのポートはメンバポートと呼ばれます。図 26-2 では、Device A の GigabitEthernet 1/0/2 と GigabitEthernet 1/0/3、Device B の GigabitEthernet 1/0/2 がメンバポートです。

メンバポートは以下のタイプがあります。

- **ダイナミックメンバポート**－ポートが IGMP report をした場合、出力インタフェースとして関連づけられたダイナミック IGMP snooping 転送エントリに追加されます。同時にポートのタイマを開始します。タイマが満了する前にメッセージを受信しない場合、ポートはダイナミック転送エントリからからポートを削除します。

- **スタティックメンバポート**－ポートがメンバポートとしてスタティックに設定された場合、出力インタフェースとして関連づけられたスタティック IGMP snooping 転送エントリに追加されます。スタティックメンバポートはエージアウトしません。手動でのみ削除することができます。

特に指定しない限り、この章でのルータポートとメンバポートは、スタティックルータポート、ダイナミックルータポートと、スタティックメンバポート、ダイナミックメンバポートを含みます。

26.1.2 IGMP snooping の動作

この章のポートはダイナミックポートです。スタティックポートの設定、削除方法については、本章の *“スタティックポートの設定”* を参照してください。

IGMP メッセージのタイプは、general クエリ、IGMP report、leave message を含みます。IGMP snooping が有効なレイヤ 2 装置は、受信した IGMP メッセージによってそれぞれ異なる動作をします。

I. General クエリ

IGMP クエリアは、アクティブなマルチキャストグループメンバが存在するかどうかを調べるために、ローカルサブネット上のすべてのホストとルータへ IGMP general クエリを定期的に送信します。

IGMP クエリアから IGMP general クエリを受信すると、装置はメッセージを受信したポートと同じ VLAN に属する、受信したポート以外のすべてのポートへ IGMP general クエリを転送します。受信ポートに対しては以下を実施します。

- 受信ポートがルータポートリストに存在するルータポートの場合、装置はこのルータポートのエージングタイマを再起動します。
- 受信ポートがルータポートリストに存在しない場合、装置はその受信ポートをルータポートリストに追加し、このルータポートのエージングタイマを開始します。

II. IGMP report

ホストは以下の目的により IGMP report を IGMP クエリアへ送信します。

- ホストがマルチキャストグループメンバである場合、IGMP クエリに応答します。
- マルチキャストグループ membership を適用します。

IGMP report を受信すると、装置は VLAN 内のすべてのルータポートからそれを転送し、報告されたマルチキャストグループのアドレスを解決します。そして、転送テーブルを検索します。

- 報告されたグループの転送テーブルエントリが存在しない場合、装置はエントリを作成して、受信したポートを転送エントリにダイナミックメンバポートとして追加します。そして、そのポートでメンバポートエージングタイマを起動します。
- 報告されたグループの転送テーブルエントリは存在するが、そのグループの発信ポートリストにポートが含まれていない場合、装置はポートをダイナミックメンバポートとして転送エントリに追加します。そのポートのメンバポートエージングタイマを起動します。

- 報告されたグループの転送テーブルエントリが存在し、転送エントリに受信ポートが含まれている場合、装置はそのポートのメンバポートエージングタイマをリセットします。

IGMP snooping が有効な装置でマルチキャストグループポリシーの設定がある際、ユーザがマルチキャストプログラムを要求したとき、ユーザのホストは IGMP report を初期化します。この IGMP report を受信した後、装置は IGMP report のマルチキャストグループアドレスを解決し、IGMP report の ACL によるフィルタリングを実行します。ACL のフィルタリングにパスした場合、出力インタフェースとして受信したポートの IGMP snooping 転送エントリを作成し、転送エントリにポートを追加します。パスしない場合、装置は IGMP report を廃棄します。ユーザはマルチキャストグループに加入できず、マルチキャストプログラムを要求することができないことを示します。

装置は IGMP report の抑制を行わないため、非ルータポートを通して IGMP report の転送を行いません。

III. Leave message

IGMPv1 ホストがマルチキャストグループを離脱する場合、ホストは IGMP leave メッセージを送信しません。レシーバホストに接続されているポートのエージングタイマが終了するまで、装置はホストに対応するメンバポートの転送エントリを転送テーブルから削除しません。この場合、ポートのマルチキャストグループのエージングタイマが終了したときのみ関連する転送エントリの出力インタフェースリストからポートを削除します。

IGMPv2 ホストあるいは IGMPv3 ホストがマルチキャストグループを離脱する場合、マルチキャストルータに IGMP leave メッセージを送信します。

装置がダイナミックメンバポートで IGMP leave メッセージを受信した場合、そのグループの転送テーブルエントリが存在するかどうかを確認します。

- 転送テーブルエントリが存在しない場合、装置は IGMP leave メッセージを破棄します。
- 転送テーブルエントリが存在するが転送エントリに受信ポートがない場合、装置は IGMP leave メッセージを破棄します。
- 転送テーブルエントリが存在し、転送エントリに受信ポートがある場合、装置は leave メッセージを VLAN 内のすべてのルータポートに転送します。装置は転送エントリから即座にポートを破棄しないかわりに、ポートに対してエージングタイマを設定します。

ホストから IGMP leave メッセージを受信したのち、IGMP クエリアはメッセージからマルチキャストグループのアドレスを解決します。そして leave メッセージを受信したポートからマルチキャストグループに IGMP group-specific クエリを送信します。

IGMP group-specific クエリを受信すると、装置は VLAN 内のすべてのルータポートとマルチキャストグループのすべてのメンバポートから IGMP group-specific クエリを転送します。直接接続されたレシーバから IGMP レポートの応答を待ちます。leave メッセージを受信したダイナミックメンバポートのため、装置は以下のアクションを実行します。

- メンバポートのエージングタイマが切れる前に、装置はそのポートのエージングタイマを再起動します。
- 装置はエージングタイマが終了すると、マルチキャストグループの転送テーブルエントリからポートを削除します。

26.2 プロトコルと標準

RFC 4541, *Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches*

26.3 IGMP snooping設定作業リスト

作業リスト
IGMP snoopingの基本機能の設定 • （必須設定項目）IGMP snoopingの有効化 • （オプション設定項目）IGMP snoopingのバージョンの設定 • （オプション設定項目）IGMP snooping転送エントリの最大数の設定 • （オプション設定項目）IGMP last member クエリ間隔の設定
IGMP snoopingポート機能の設定 • （オプション設定項目）ダイナミックポートのエージングタイマの設定 • （オプション設定項目）スタティックポートの設定 • （オプション設定項目）シミュレーティッドメンバホストの設定 • （オプション設定項目）fast-leave処理の有効化
IGMP snooping クエリの設定 • （オプション設定項目）IGMP snoopingクエリアの有効化 • （オプション設定項目）IGMP クエリとresponseのパラメータの設定
IGMPメッセージのパラメータの設定 • （オプション設定項目）IGMPメッセージの送信元IPアドレスの設定 • （オプション設定項目）IGMPメッセージの802.1p優先度の設定
IGMP snooping ポリシーの設定 • （オプション設定項目）マルチキャストグループポリシーの設定 • （オプション設定項目）未知のマルチキャストデータ廃棄機能の有効化 • （オプション設定項目）IGMP report抑制機能の有効化 • （オプション設定項目）ポートで参加可能なマルチキャストグループの最大数の設定 • （オプション設定項目）マルチキャストグループ置き換え機能の有効化
（オプション設定項目）送信IGMPプロトコルパケットのDSCP値の設定

IGMP snooping において、アグリゲートインタフェース上での設定は、そのメンバポートの設定に干渉しないし、アグリゲーション計算にも参加しません。アグリゲートグループのメンバポートでの設定は、アグリゲートグループから離脱するまで有効になりません。

26.4 IGMP snoopingの基本機能の設定

IGMP snooping の基本機能の設定をする前に、以下の作業を完了させてください。

- 対応する VLAN を設定してください。
- IGMP snooping のバージョンを定義してください。
- IGMP snooping 転送エントリの最大数を定義してください。

- IGMP last member クエリの間隔を定義してください。

26.4.1 IGMP snooping の有効化

IGMP snooping を有効にするとき、以下のガイドラインに従ってください。

- VLAN で IGMP snooping を有効にする前に、グローバルで有効にしてください。
- VLAN 用の IGMP snooping は、VLAN のメンバポートでのみ動作します。

以下に IGMP snooping の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. IGMP snooping をグローバルで有効にし、IGMP-snooping view に移行する	**igmp-snooping**	デフォルト：無効
3. system view に戻る	**quit**	ー
4. VLAN view に移行する	**vlan** *vlan-id*	ー
5. VLAN で IGMP snooping を有効にする	**igmp-snooping enable**	デフォルト：無効

26.4.2 IGMP snooping のバージョンの設定

IGMP snooping のバージョン異なると、IGMP メッセージの異なるバージョンを処理することができます。

- IGMPv2 snooping は IGMPv1 と IGMPv2 のメッセージを処理することができますが、IGMPv3 メッセージは処理することはできず、VLAN 上にフラッディングされてしまいます。
- IGMPv3 snooping は IGMPv1、IGMPv2、IGMPv3 メッセージを処理することができます。

IGMPv3 snooping を IGMPv2 snooping に変更する場合、装置は以下のことを行います。

- ダイナミックに追加されたすべての IGMP snooping 転送エントリを削除します。
- IGMPv3 snooping スタティック（* , G）の転送エントリは維持します。
- IGMPv3 snooping スタティック(S , G)の転送エントリは削除します。IGMP snooping が IGMPv3 snooping に切り替わったとき復元されます。

スタティック IGMP snooping 転送エントリの詳細については、本章の *“スタティックポートの設定”* を参照してください。

以下に IGMP snooping のバージョンの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. VLAN view に移行する	**vlan** *vlan-id*	ー
3. IGMP snooping のバージョンを指定する	**igmp-snooping version** *version-number*	デフォルト：2

26.4.3 IGMP snooping 転送エントリの最大数の設定

IGMP snooping 転送テーブルの最大エントリ数をグローバルに設定できます。この最大エントリ数はダイナミックエントリ、スタティックを含みます。装置の転送エントリ数が上限に達すると、装置は、いくつかのエントリがタイムアウトするか、手動で削除されるまで、転送エントリを生成することができません。新しいエントリを作成するため、手動でエントリを削除することを推奨します。

以下に IGMP snooping 転送エントリの最大数の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． IGMP-snooping view に移行する	**igmp-snooping**	―
3． IGMP snooping 転送エントリの最大数を設定する	**entry-limit** *limit*	デフォルト：4294967295

26.4.4 IGMP last member クエリ間隔の設定

グループの IGMP group-specific クエリを受信すると、レシーバホストは参加した各マルチキャストグループのタイマを起動します。このタイマは、0 から最大応答時間（ホストは、受信した IGMP クエリの Max Response Time フィールドから最大応答時間の値を取得します）の範囲でランダムな値に初期化されます。タイマ値が経過して 0 になったときに、ホストは対応するマルチキャストグループに IGMP report を送信します。

IGMP クエリの最大応答時間を適切に設定すると、ホストは速やかにクエリに応答できます。また、対応するタイマの期限が多数のホストで同時に切れたときに同時に送信する report によってネットワーク上で発生する IGMP トラフィックのバーストを回避することもできます。

I. 設定の制限とガイドライン

IGMP last member クエリの間隔を設定する場合、以下の制限とガイドラインに従ってください。

- fast-leave 処理が有効なポートから IGMP leave メッセージを受信した場合、装置は IGMP group-specific クエリを送信しません。
- IGMP-snooping view のすべての VLAN、あるいは VLAN view の VLAN でグローバルに IGMP last member クエリの間隔を設定することができます。VLAN で行った設定はグローバルで行った設定よりも優先されます。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． IGMP-snooping view に移行する	**igmp-snooping**	―
3． IGMP last-member クエリの送信間隔を設定する	**last-member-query-interval** *interval*	デフォルト：1秒

II. VLAN での IGMP last member クエリの間隔の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． IGMP-snooping view に移行する	**vlan** *vlan-id*	―
3． IGMP last-member クエリの送信間隔を設定する	**igmp-snooping last-member-query-interval** *interval*	デフォルト：1秒

26.5 IGMP snoopingポート機能の設定

IGMP snooping ポート機能の設定をする前に、以下の作業を完了させてください。

- VLAN で IGMP snooping を有効にしてください。
- ダイナミックルータポートのエージングタイマを定義してください。
- ダイナミックメンバポートのエージングタイマを定義してください。
- マルチキャストグループとマルチキャスト送信元アドレスを定義してください。

26.5.1 ダイナミックポートのエージングタイマの設定

ダイナミックポートのエージングタイマを設定するとき、以下のガイドラインに従ってください。

- マルチキャストグループメンバシップが頻繁に変更される場合は、メンバポートのエージングタイマに比較的小さな値を設定します。マルチキャストグループメンバシップがほとんど変更されない場合は、メンバポートのエージングタイマに比較的大きな値を設定します。
- ダイナミックポートのエージングタイマの設定は、VLAN view の現在の VLAN あるいは IGMP-snooping view のすべての VLAN のどちらかに設定することができます。もし VLAN view と IGMP-snooping view の両方に設定がある場合、VLAN view の設定が適用されます。

I. グローバルでのダイナミックポートのエージングタイマの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． IGMP-snooping view に移行する	**igmp-snooping**	―
3． グローバルでのダイナミックルータポートのエージングタイマを設定する	**router-aging-time** *interval*	デフォルト：260秒
4． グローバルでのダイナミックメンバポートのエージングタイマを設定する	**host-aging-time** *interval*	デフォルト：260秒

II. VLAN でのダイナミックポートのエージングタイマの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. VLAN view に移行する	**vlan** *vlan-id*	―
3. VLAN でのダイナミックルータポートのエージングタイマを設定する	**igmp-snooping router-aging-time** *interval*	デフォルト：260秒
4. VLAN でのダイナミックメンバポートのエージングタイマを設定する	**igmp-snooping host-aging-time** *interval*	デフォルト：260秒

26.5.2 スタティックポートの設定

以下のタイプのスタティックポートを設定することができます。

- **スタティックメンバポート**－マルチキャストグループのスタティックメンバポートを設定するとき、ポートに接続されるすべてのホストはグループのマルチキャストデータを受信することができます。

  設定を完了した、あるいは取り消したとき、ポートは IGMP report や leave メッセージを送信しません。スタティックメンバポートは IGMP クエリに応答しません。
- **スタティックルータポート**－マルチキャストグループのスタティックルータポートを設定するとき、ポートで受信されたグループのすべてのマルチキャストデータは転送されます。

以下にスタティックポートの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Layer 2 Ethernet interface view あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	―
3. ポートをスタティックポートに設定する	• ポートをスタティックメンバポートに設定する：**igmp-snooping static-group** *group-address* [**source-ip** *source-address*] **vlan** *vlan-id* • ポートをスタティックルータポートに設定する：**igmp-snooping static-router-port vlan** *vlan-id*	デフォルト：設定なし

26.5.3 シミュレーティッドメンバホストの設定

ポートでシミュレーティッドメンバホストを設定したとき、以下の方法により独立したホストと同等になります。

- 設定が完了したとき、unsolicited IGMP report を送信します。
- IGMP report として IGMP general クエリに応答します。
- 設定を削除したとき、IGMP leave メッセージを送信します。

シミュレーティッドホストの IGMP のバージョンと IGMP snooping バージョンが同一であることを確認してください。スタティックメンバポートと異なり、シミュレーティッドメンバホストとして設定されたポートはダイナミックメンバポートと同様にエージアウトします。

以下にシミュレーティッドメンバホストの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Layer 2 Ethernet interface view あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	―
3. ポートをシミュレーティッドメンバホストとして設定する	**igmp-snooping host-join** *group-address* [**source-ip** *source-address*] **vlan** *vlan-id*	デフォルト：設定なし

26.5.4 fast-leave 処理の有効化

ポートが leave メッセージを受信するとき、装置は fast-leave 処理機能によって、IGMP leave メッセージを迅速に転送エントリからポートを削除することができます。

I. 設定の制限とガイドライン

IGMP snooping fast-leave 処理機能を設定するとき、以下の設定の制限とガイドラインに従ってください。

- 複数のホストが接続しているポートでは fast-leave 処理機能を有効にしないでください。そうでないと同じマルチキャストグループにあるポートに接続された他のレシーバのホストはマルチキャストデータを受信することができません。
- IGMP snooping fast-leave 処理機能は、ポートあるいはグローバルのどちらかに設定することができます。もしポートとグローバルの両方に設定がある場合、ポートの設定が適用されます。

II. グローバルでの IGMP snooping fast-leave 処理機能の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. IGMP-snooping view に移行する	**igmp-snooping**	―
3. グローバルで IGMP snooping fast-leave 処理機能を設定する	**fast-leave** [**vlan** *vlan-list*]	デフォルト：無効

III. ポートでの IGMP snooping fast-leave 処理機能の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―

操作	コマンド	補足
2. Layer 2 Ethernet interface view あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	—
3. ポートで IGMP snooping fast-leave 処理機能を設定する	**igmp-snooping fast-leave** [**vlan** *vlan-list*]	デフォルト：無効

26.6 IGMP snooping クエリの設定

この項では IGMP snooping クエリの設定方法について記載します。

26.6.1 設定要件

IGMP snooping クエリを設定する前に、以下の作業を完了してください。

- VLAN で IGMP snooping を有効にしてください。
- IGMP general クエリの送信間隔を定義してください。
- IGMP last-member クエリの送信間隔を定義してください。
- IGMP general クエリの最大応答時間を定義してください。

26.6.2 IGMP snooping クエリアの有効化

この機能は、データリンクレイヤでマルチキャスト転送エントリを確立し、維持するために、装置が IGMP general クエリを定期的に送信します。レイヤ 3 マルチキャスト装置がないネットワークで IGMP snooping クエリアを設定することができます。

IGMP snooping クエリアを有効にするとき、IGMP が動作するマルチキャストネットワークで IGMP snooping クエリアを有効にしないでください。IGMP Snooping クエリアは IGMP クエリアの選択に関与しませんが、小さい送信元 IP アドレスで IGMP general クエリを送信するので IGMP クエリアの選択に影響を与える可能性があります。

以下に VLAN で IGMP snooping クエリアを有効にする設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. VLAN view に移行する	**vlan** *vlan-id*	—
3. IGMP snooping クエリアを有効にする	**igmp-snooping querier**	デフォルト：無効

26.6.3 IGMP クエリと response のパラメータの設定

注意：

IGMP general クエリ間隔は IGMP general クエリの最大応答時間よりも大きいことを確認してください。そうしないとマルチキャストグループメンバが誤って削除されてしまう可能性があります。

VLAN ベースのネットワークの実際の状況にもとづいて、IGMP general クエリ の送信間隔 を調整することができます。

IGMP クエリ（general クエリ または group-specific クエリ）を受信すると、レシーバホストは参加した各マルチキャストグループの report delay タイマを起動します。このタイマは、0 から最大応答時間（ホストは、受信した IGMP クエリの Max Response Time フィールドから最大応答時間の値を取得します）の範囲でランダムな値に初期化されます。タイマ値が経過して 0 になったときに、ホストは対応するマルチキャストグループに IGMP report を送信します。

IGMP クエリの最大応答時間を適切に設定すると、ホストは速やかにクエリに応答できます。また、対応するタイマの期限が多数のホストで同時に切れたときに同時に送信する report によってネットワーク上で発生する IGMP トラフィックのバーストを回避することもできます。

IGMP クエリと応答のパラメータは、VLAN view で現在の view あるは IGMP-snooping view ですべての VLAN で設定できます。もし VLAN view と IGMP-snooping view の 2 つの設定がある場合、VLAN view で設定された設定が適用されます。

I. グローバルでの IGMP クエリと response のパラメータの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. IGMP-snooping view に移行する	**igmp-snooping**	―
3. IGMP general クエリの最大応答時間を設定する	**max-response-time** *seconds*	デフォルト：10秒
4. IGMP last-member クエリ間隔を設定する	**last-member-query-interval** *interval*	デフォルト：1秒

II. VLAN での IGMP クエリと response のパラメータの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. VLAN view に移行する	**vlan** *vlan-id*	―
3. IGMP general クエリの送信間隔を設定する	**igmp-snooping query-interval** *interval*	デフォルト：125秒
4. IGMP general クエリの最大応答時間を設定する	**igmp-snooping max-response-time** *interval*	デフォルト：10秒
5. IGMP last-member クエリ間隔を設定する	**igmp-snooping last-member-query-interval** *interval*	デフォルト：1秒

26.7 IGMPメッセージのパラメータの設定

この章では IGMP メッセージのパラメータの設定について記載します。

26.7.1 設定要件

VLAN で IGMP メッセージのパラメータを設定する前に、以下の作業を完了してください。

- VLAN で IGMP snooping を有効にしてください。
- IGMP general クエリの送信元 IP アドレスを定義してください。
- IGMP group-specific クエリの送信元 IP アドレスを定義してください。
- IGMP report の送信元 IP アドレスを定義してください。
- IGMP leave message の送信元 IP アドレスを定義してください。
- IGMP メッセージの 802.1p 優先度を定義してください。

26.7.2 IGMP メッセージの送信元 IP アドレスの設定

送信元 IP アドレスが 0.0.0.0 である IGMP クエリをポートで受信すると、装置はそのポートをダイナミックルータポートとして設定しません。これによって、マルチキャスト転送エントリがデータリンクレイヤで正しく作成されずに、最終的にマルチキャストトラフィック転送エラーが発生する可能性があります。

この問題を防ぐため、IGMP snooping クエリアとして動作する装置によって送信された IGMP クエリの送信元 IP アドレスとしてオール 0 以外の IP アドレスを設定することができます。IGMP クエリの送信元アドレスを変更するとサブネット内の IGMP クエリアの選定に影響する可能性があります。

シミュレーティッドメンバホストあるいは IGMP snooping のプロキシーによって IGMP report あるいは IGMP leave message の送信元 IP アドレスを変更することができます。

以下に VLAN での IGMP メッセージの送信元 IP アドレスの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． VLAN view に移行する	**vlan** *vlan-id*	―
3． IGMP general クエリの送信元 IP アドレスを設定する	**igmp-snooping general-query source-ip** *ip-address*	デフォルト：現在のVLANインタフェースのIPアドレスです。 現在のVLANインタフェースにIPアドレスがない場合、0.0.0.0です。

操作	コマンド	補足
4． IGMP group-specific クエリの送信元 IP アドレスを設定する	**igmp-snooping special-query source-ip** *ip-address*	デフォルト：以下のいずれかとなります。 ● VLANのIGMP snoopingクエリアがIGMP general クエリを受信したとき、IGMP group-specific クエリの送信元IPアドレスはIGMP general クエリの送信元IPアドレスです。 ● VLANのIGMP snoopingクエリアがIGMP general クエリを受信していない場合、IGMP group-specific クエリの送信元IPアドレスは現在のVLANインタフェースのIPアドレスです。 ● VLANのIGMP snoopingクエリアがIGMP general クエリを受信しておらず、現在のVLANインタフェースにIPアドレスが設定されていない場合、送信元IPアドレスは0.0.0.0です。
5． IGMP reports の送信元 IP アドレスを設定する	**igmp-snooping report source-ip** *ip-address*	デフォルト：現在のVLANインタフェースのIPアドレスです。 現在のVLANインタフェースにIPアドレスがない場合、0.0.0.0です。
6． IGMP leave メッセージの送信元 IP アドレスを設定する	**igmp-snooping leave source-ip** *ip-address*	デフォルト：現在のVLANインタフェースのIPアドレスです。 現在のVLANインタフェースにIPアドレスがない場合、0.0.0.0です。

26.7.3 IGMP メッセージの 802.1p 優先度の設定

装置の出力ポートで混雑が発生すると、802.1p 優先度が高い順から IGMP メッセージを転送します。装置によって作成あるいは転送される IGMP メッセージに高い 802.1p 優先度を割り当てることができます。

IGMP-snooping view のすべての VLAN あるいは VLAN view の現在の VLAN で IGMP メッセージの優先度を設定することができます。VLAN view での設定は IGMP-snooping view での設定よりも優先されます。

I. グローバルでの IGMP メッセージの 802.1p 優先度の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	―

操作	コマンド	補足
2． IGMP-snooping view に移行する	**igmp-snooping**	―
3． IGMP メッセージの 802.1p 優先度を設定する	**dot1p-priority** *priority*	デフォルト：設定なし

II. VLAN での IGMP メッセージの 802.1p 優先度の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． VLAN view に移行する	**vlan** *vlan-id*	―
3． IGMP メッセージの 802.1p 優先度を設定する	**igmp-snooping dot1p-priority** *priority*	デフォルト：6

26.8 IGMP snooping ポリシーの設定

IGMP snooping ポリシーの設定をする前に、以下の作業を完了させてください。

- VLAN で IGMP snooping を有効にしてください。
- マルチキャストグループポリシーに使用する ACL を定義してください。
- ポートが追加できるマルチキャストグループの最大数を定義してください。

26.8.1 マルチキャストグループポリシーの設定

マルチキャストグループを指定する ACL とオプションのソースにもとづいて IGMP report をフィルタします。受信ホストが加入するマルチキャストグループを管理するために使用されます。

I. 設定の制限とガイドライン

マルチキャストグループポリシーの設定を行うとき、以下の設定の制限とガイドラインに従ってください。

- この設定はポートがダイナミックに追加するマルチキャストグループに適用されます。
- マルチキャストグループポリシーは、ポートあるいはグローバルのどちらかに設定することができます。もしポートとグローバルの両方に設定がある場合、ポートの設定が適用されます。

II. グローバルでのマルチキャストグループポリシーの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． IGMP-snooping view に移行する	**igmp-snooping**	―

操作	コマンド	補足
3. グローバルでマルチキャストグループポリシーを設定する	**group-policy** *acl-number* [**vlan** *vlan-list*]	デフォルト：設定なし

III. ポートでのマルチキャストグループポリシーの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Layer 2 Ethernet interface view あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	―
3. ポートでマルチキャストグループポリシーを設定する	**igmp-snooping group-policy** *acl-number* [**vlan** *vlan-list*]	デフォルト：設定なし

26.8.2 未知のマルチキャストデータ廃棄機能の有効化

この機能はすべての未知のマルチキャストデータを廃棄します。未知のマルチキャストデータとは、IGMP snooping 転送テーブルにエントリが存在しないマルチキャストデータのことです。装置にルータポートがない場合、未知のマルチキャストデータを廃棄します。

この機能はすべての未知のマルチキャストデータを廃棄します。この機能を無効にした場合、装置は未知のマルチキャストパケットをデータが存在する VLAN にフラッディングします。

I. 設定制限とガイドライン

未知のマルチキャストデータ廃棄機能を有効にするとき、以下の制限とガイドラインに従ってください。

- 未知のマルチキャストデータ廃棄機能を、IGMP-snooping view ですべての VLAN に対してグローバルに、もしくは VLAN view で現在の VLAN に対して有効にできます。
- 未知のマルチキャストデータの廃棄が有効になっている場合でも、装置は受信ルータポート以外のルータポートから未知のマルチキャストデータを転送します。

II. VLAN での未知のマルチキャストデータ廃棄機能の有効化

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. VLAN view に移行する	**vlan** *vlan-id*	―
3. 未知のマルチキャストデータ廃棄機能を VLAN で有効にする	**igmp-snooping drop-unknown**	デフォルト：無効 未知のマルチキャストデータはフラッディングします。

26.8.3 IGMP report 抑制機能の有効化

この機能はマルチキャストグループ用に、直接接続されているレイヤ 3 装置に最初の IGMP report のみを転送します。以降の同じマルチキャストグループからの IGMP report を廃棄します。

以下に IGMP report 抑制機能を有効にする設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. IGMP-snooping view に移行する	**igmp-snooping**	―
3. IGMP report 抑制機能を有効にする	**report-aggregation**	デフォルト：有効

26.8.4 ポートで参加可能なマルチキャストグループの最大数の設定

ポートトラフィックを調整するため、ポートで参加可能なマルチキャストグループの最大数を設定することができます。

I. 設定の制限とガイドライン

ポートで参加可能なマルチキャストグループの最大数を設定するとき、以下の設定の制限とガイドラインに従ってください。

- この設定はダイナミックにマルチキャストグループに加入されたポートのみ適用します。
- ポートが参加したマルチキャストグループの数が設定されている最大数に達したときは、そのポートに残るすべての転送エントリを IGMP snooping 転送テーブルから削除します。このポートに接続されたホストは、最大数になる前に、再度マルチキャストグループに参加することができます。

II. 設定手順

以下にポートで参加可能なマルチキャストグループの最大数の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Layer 2 Ethernet interface view あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	―
3. ポートで参加可能なマルチキャストグループの最大数を設定する	**igmp-snooping group-limit** *limit* [**vlan** *vlan-list*]	デフォルト：設定なし

26.8.5 マルチキャストグループ置き換え機能の有効化

この機能は、グループのメンバ数が上限を超えたとき、装置が既存のマルチキャストグループを新規に追加されたマルチキャストグループに置き換える機能です。この機能は一般的にチャンネルスイッチアプリケーションで使われます。この機能が無効の場合、装置は新しいグループの IGMP report を廃棄し、ユーザが新しいチャンネルに変更することができません。

I. 設定の制限とガイドライン

マルチキャストグループ置き換え機能を有効にしたとき、以下の設定の制限とガイドラインに従ってください。

- この設定はダイナミックにマルチキャストグループに加入されたポートのみ適用します。
- マルチキャストグループ置き換え機能は、インタフェースあるいはグローバルのどちらかに設定することができます。もしインタフェースとグローバルの両方に設定がある場合、インタフェースの設定が適用されます。

II. グローバルでのマルチキャストグループ置き換え機能の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. IGMP-snooping view に移行する	**igmp-snooping**	—
3. グローバルでマルチキャストグループ置き換え機能を有効にする	**overflow-replace** [**vlan** *vlan-list*]	デフォルト：無効

III. ポートでのマルチキャストグループ置き換え機能の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. Layer 2 Ethernet interface view あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	—
3. ポートでマルチキャストグループ置き換え機能を有効にする	**igmp-snooping overflow-replace** [**vlan** *vlan-list*]	デフォルト：無効

26.9 送信IGMPプロトコルパケットのDSCP値の設定

DSCP 値は、パケット送信の優先順位を決定します。DSCP 値が大きいほど、優先順位が高くなります。

I. 設定手順

以下に送信 IGMP プロトコルパケットの DSCP 値の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． IGMP-snooping view に移行する	**igmp-snooping**	―
3． 送信 IGMP プロトコルパケットの DSCP 値を設定する	**dscp** *dscp-value*	デフォルト：48

26.10 IGMP snoopingの表示と維持

すべての view で **display** コマンドを実行でき、user view で **reset** コマンドを実行できます。

操作	コマンド
IGMP snoopingステータスを表示する	**display igmp-snooping** [**global** | **vlan** *vlan-id*]
ダイナミックIGMP snooping転送エントリの情報を表示する	**display igmp-snooping group** [*group-address* | *source-address*] * [**vlan** *vlan-id*] [**interface** *interface-type interface-number* | **verbose**]
スタティックIGMP snooping転送エントリの情報を表示する	**display igmp-snooping static-group** [*group-address* | *source-address*] * [**vlan** *vlan-id*] [**verbose**]
ダイナミックルータポートの情報を表示する	**display igmp-snooping router-port** [**vlan** *vlan-id*] [**verbose**]
スタティックルータポートの情報を表示する	**display igmp-snooping static-router-port** [**vlan** *vlan-id*]
IGMP snoopingによって学習されたIGMPメッセージの統計情報を表示する	**display igmp-snooping statistics**
レイヤ2 IPマルチキャストグループエントリの情報を表示する	**display l2-multicast ip forwarding** [**group** *group-address* | **source** *source-address*] * [**vlan** *vlan-id*]
レイヤ2 IPマルチキャストグループの情報を表示する	**display l2-multicast ip** [**group** *group-address* **| source** *source-address*] * [**vlan** *vlan-id*]
レイヤ2 MACマルチキャストグループエントリの情報を表示する	**display l2-multicast mac forwarding** [*mac-address*] [**vlan** *vlan-id*]
レイヤ2 MACマルチキャストグループの情報を表示する	**display l2-multicast mac** [*mac-address*] [**vlan** *vlan-id*]
指定されたマルチキャストグループのダイナミックIGMP snooping転送エントリを削除する	**reset igmp-snooping group** { *group-address* [*source-address*] | **all** } [**vlan** *vlan-id*]
ダイナミックルータポートを削除する	**reset igmp-snooping router-port** { **all** | **vlan** *vlan-id*]
IGMP snoopingによって学習されたIGMPメッセージの統計情報を削除する	**reset igmp-snooping statistics**

26.11 IGMP snooping設定例

26.11.1 ネットワーク要件

図 26-33 に示すように、

- Source はマルチキャストグループ 244.1.1.1 にマルチキャストトラフィックを送信します。
- Client はマルチキャストグループの受信ホストです。
- Source と Client 間のルートは通信可能です。

Client が Source からマルチキャストトラフィックを受信できるように AC を設定します。

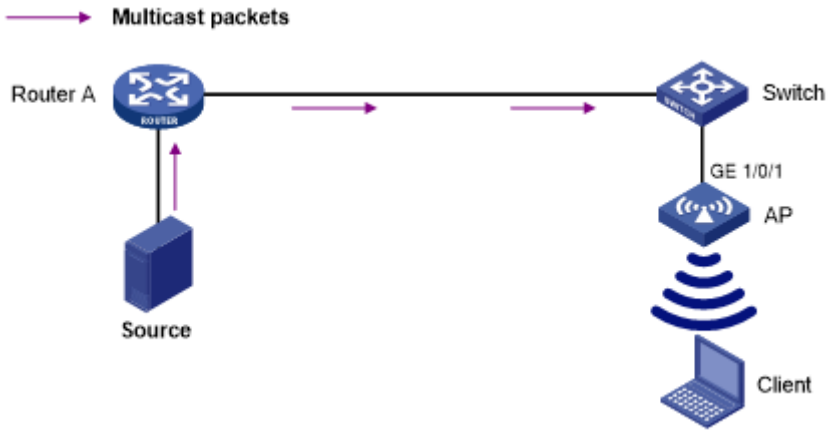


図 26-3 ネットワーク図

26.11.2 設定手順

I. Router A の設定

IP マルチキャストルーティングをグローバルで有効にします。また、AC と接続したポートで PIM-SM と IGMP を有効にします。（詳細は省略します。）

II. AC の設定

1)　WLAN サービスの設定

VLAN 100 を作成します。

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
```

サービステンプレート 1 を作成し、サービステンプレートに SSID を Multicast に設定します。

```
[AC] wlan service-template 1
[AC-wlan-st-1] ssid Multicast
```

VLAN 100 をサービステンプレート 1 に設定し、サービステンプレートを有効にします。

```
[AC-wlan-st-1] vlan 100
[AC-wlan-st-1] service-template enable
[AC-wlan-st-1] quit
```

ap と名付けたモデル QX-W1110 の AP を作成し、AP のシリアル ID を 219801A0CNC138011454 に設定します。

```
[AC] wlan ap ap model QX-W1110
[AC-wlan-ap-ap] serial-id 219801A0CNC138011454
```

サービステンプレート 1 を radio 1 に設定し、ap に対して radio 1 を有効にします。

```
[AC-wlan-ap-ap] radio 1
[AC-wlan-ap-ap-radio-1] service-template 1
[AC-wlan-ap-ap-radio-1] radio enable
[AC-wlan-ap-ap-radio-1] quit
[AC-wlan-ap-ap]quit
```

2)　IGMP snooping のグローバルでの設定

IGMP snooping をグローバルで有効にします。

```
[AC] igmp-snooping
[AC-igmp-snooping] quit
```

VLAN 100 で IGMP snooping を有効にし、IGMP snooping バージョン 3 を指定します。

```
[AC] vlan 100
[AC-vlan100] igmp-snooping enable
[AC-vlan100] igmp-snooping version 3
[AC-vlan100] quit
```

3)　イーサネットインタフェースの設定

アクセスコントローラで GigabitEthernet 1/0/2 をトランクポートとして設定し、ポートを VLAN 100 に割り当てます。

```
[AC] interface GigabitEthernet 1/0/2
[AC-GigabitEthernet1/0/2] port link-type trunk
[AC-GigabitEthernet1/0/2] port trunk permit vlan 100
[AC-GigabitEthernet1/0/2] quit
```

III. Client の設定

Client が、SSID が Multicast の WLAN サービスにアクセスし、マルチキャストグループ 244.1.1.1 に対してマルチキャストトラフィックを要求するように設定します。（詳細は省略します。）

26.11.3 設定の確認

AC 上で VLAN 100 に対してエントリを転送するダイナミック IGMP snooping の情報を表示します。

```
[AC] display igmp-snooping group vlan 100 verbose
Total 1 entries.

VLAN 100: Total 1 entries.
  (0.0.0.0, 224.1.1.1)
    Attribute: local port
    FSM information: normal
    Host slots (0 in total):
    Host ports (1 in total):
      WLAN-BSS1/0/20                          (00:03:23)
```

出力は、AC 上の WLAN-BSS 1/0/20 がマルチキャストグループ 244.1.1.1 に参加したことを示します。

26.12 IGMP snoopingのトラブルシューティング

26.12.1 レイヤ 2 マルチキャスト転送ができない

I. 症状

装置でレイヤ 2 マルチキャスト転送ができません。

II. 解決策

1) IGMP snooping 情報を表示するため **display igmp-snooping** コマンドを使用します。
2) IGMP snooping が有効になっていない場合、グローバルで **igmp-snooping** コマンドを使用して IGMP snooping を有効にし、VLAN view で **igmp-snooping enable** コマンドを使用して IGMP snooping を有効にしてください。
3) グローバルで IGMP snooping が有効で、対応する VLAN で IGMP snooping が無効になっている場合、対応する VLAN の VLAN view 上で **igmp-snooping enable** コマンドを使用して IGMP snooping を有効にしてください。
4) 問題が解決しない場合、NEC に問い合わせてください。

26.12.2 マルチキャストグループポリシーが動作しない

I. 症状

マルチキャストポリシーによって許可されていないマルチキャストグループから、ホストがマルチキャストデータを受信できません。

II. 解決策

1) **display acl** コマンドで ACL ルールの設定を確認してください。実行するマルチキャストグループポリシーに ACL ルールが一致していることを確認してください。
2) **display this** コマンドを IGMP snooping view または対応するポートの interface view で使用して、マルチキャストグループポリシーが正しく適用されているかどうかを確認してください。適用されていない場合、**group-policy** または **igmp-snooping group-policy** コマンドでマルチキャストグループポリシーを正しく適用してください。
3) **display igmp-snooping** コマンドを使用して、未知のマルチキャストデータ廃棄機能が有効になっているかどうか確認してください。有効になっていない場合、**igmp-snooping drop-unknown** コマンドを使用して未知のマルチキャストデータ廃棄機能を有効にしてください。
4) 問題が解決しない場合、NEC に問い合わせてください。

QX-W2300AC シリーズ アクセスコントローラ

オペレーションマニュアル

6.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**6-x-x** です。

1章 WLANアクセス 1-1
1.1 WLANアクセスの概要 1-1
1.1.1 スキャニング 1-1
1.1.2 関連づけ 1-3
1.2 SSIDにもとづくアクセス制御 1-3
1.3 ホワイトリスト、ブラックリストにもとづくアクセス制御 1-4
1.4 ACLにもとづくアクセス制御 1-5
1.5 設定の制限とガイドライン 1-5
1.6 設定作業リスト 1-5
1.7 領域コードの指定 1-6
1.8 無線サービスの設定 1-8
1.8.1 サービステンプレートの設定 1-8
1.8.2 サービステンプレートに対する記述の設定 1-8
1.8.3 SSIDの設定 1-8
1.8.4 サービス テンプレートの無線に関連付けられたクライアントの最大数の設定 1-9
1.8.5 サービステンプレートの有効化 1-9
1.8.6 無線に対するサービステンプレートの設定 1-9
1.8.7 APが指定されたサービステンプレートをAPグループから引き継がないための設定 1-10
1.9 クライアントデータ転送の設定 1-11
1.9.1 クライアントトラフィック転送モードの指定 1-11
1.9.2 クライアントのトラフィック転送の有効化 1-11
1.9.3 クライアントデータフレームに対するカプセル化フォーマットの設定 1-12
1.9.4 APが未知のクライアントからのトラフィックを処理する方法の設定 1-12
1.10 クライアント管理の設定 1-12
1.10.1 ACまたはAPでのクライアントの関連づけの有効化 1-12
1.10.2 クイックアソシエーションの有効化 1-13
1.10.3 クライアント情報報告先のWebサーバの指定 1-13
1.10.4 クライアントのVLANの割り当て方式の指定 1-14
1.10.5 ローミング後のクライアントの許可VLANの選択の設定 1-14
1.10.6 クライアント再認証を行う前のアイドル時間の設定 1-14
1.11 クライアントメンテナンスの設定 1-15
1.11.1 クライアントアイドルタイムアウトの設定 1-15
1.11.2 クライアントkeepaliveの設定 1-15
1.11.3 無線リンク品質テストの実行 1-16
1.11.4 NAS IDの設定 1-16
1.12 クライアントアクセス制御の設定 1-18
1.12.1 ホワイトリストへのクライアントの追加 1-18
1.12.2 スタティックブラックリストへのクライアントの追加 1-18
1.12.3 ダイナミックブラックリストの設定 1-18
1.12.4 ACLにもとづくアクセス制御の設定 1-19
1.13 APの特定ブロードキャストプローブ要求への応答の有効化 1-20
1.14 APへのコンフィグレーションファイルの設定 1-21
1.15 WLANアクセスのSNMP notificationの有効化 1-22

1.16 WLANアクセスの表示と維持 1-22
1.17 WLANアクセスの設定例 1-23
1.17.1 WLANアクセスの設定例 1-23
1.17.2 ホワイトリストの設定例 1-25
1.17.3 スタティックブラックリストの設定例 1-26
1.17.4 ACLの設定例 1-26

1章 WLAN アクセス

本章では WLAN アクセスの設定方法について記述します。

1.1 WLANアクセスの概要

無線クライアントは、スキャニング、リンクレイヤ認証、関連づけ、WLAN 認証プロセスが完了したときのみ WLAN にアクセスすることができます。

データリンクレイヤ認証に関する詳細は、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*8 WLAN セキュリティ*”の”*1 章 WLAN セキュリティ*”を参照してください。

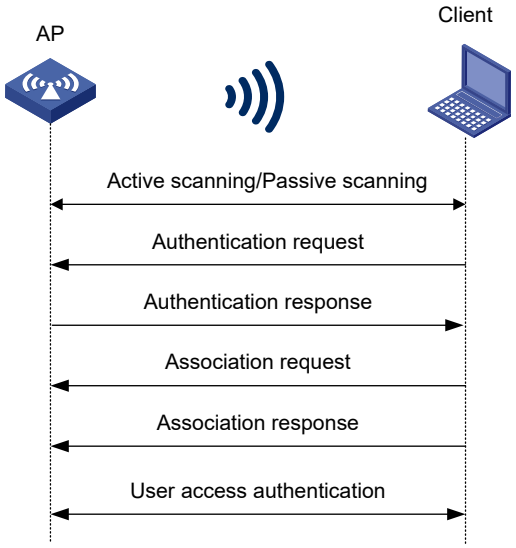


図 1-1 WLAN アクセスプロセス

1.1.1 スキャニング

I. アクティブスキャニング

無線クライアントは、プローブ要求を送信することで、定期的に周辺の無線ネットワークをスキャンします。無線クライアントは、受信したプローブ応答からネットワーク情報を取得します。プローブ要求が SSID を運ぶか否かにもとづき、アクティブスキャニングは以下のタイプに分類できます。

- すべての無線ネットワークのアクティブスキャニング
  - 図 1-2に示すように、クライアントは無線ネットワークをスキャンするために、サポートされた各々のチャネル上で定期的にプローブ要求を送信します。プロー

ブ要求を受信した AP は、プローブ応答を送信します。これにより、入手可能な無線ネットワーク情報を運びます。クライアントは、最適 AP と関連づけられます。

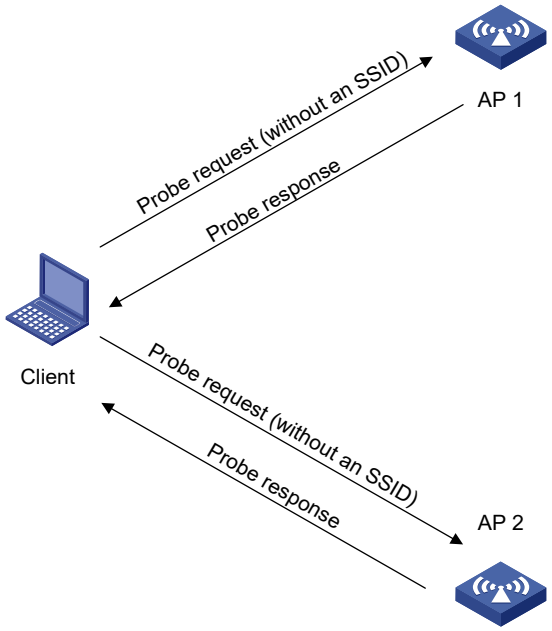


図 1-2 WLAN アクセスプロセス

- 特定の無線ネットワークのアクティブスキャニング
  - 無線クライアントが SSID を設定される、もしくは SSID に関連づけられる場合、図 1-3に示すように、クライアントは指定された SSID を運ぶプローブ要求を定期的に送信します。特定の SSID で無線サービスを提供できる AP がプローブ要求を受信したとき、AP はプローブ応答を送信します。

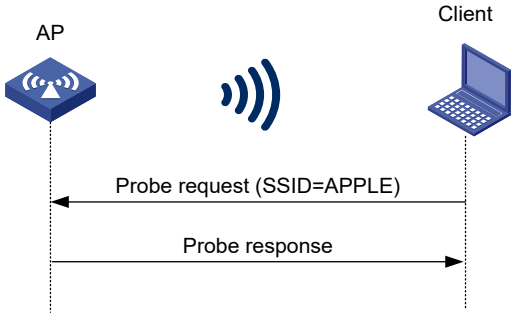


図 1-3 特定の無線ネットワークのスキャニング

II. パッシブスキャニング

- 図 1-4に示すように、クライアントは周辺の無線ネットワークに関する情報を入手するために、サポートされたチャネル上で AP によって送信されたビーコンフレームを受信します。クライアントは認証のために AP を選択します。パッシブスキャニングは電力消費を抑えたいときに使用します。

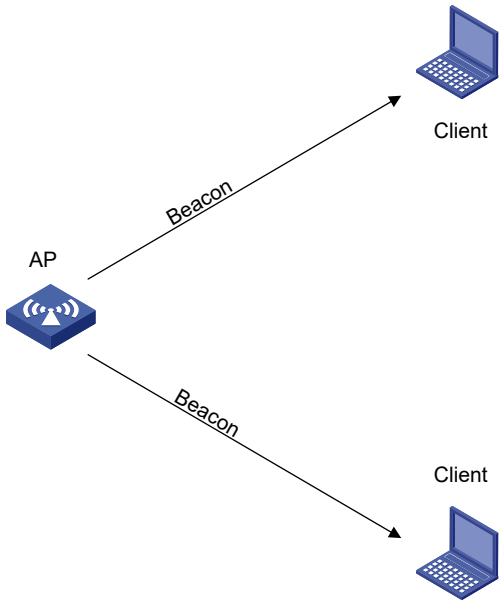


図 1-4 パッシブスキャニング

1.1.2 関連づけ

クライアントは、データリンクレイヤ認証を通過したあと、関連づけられた AP に対して関連づけ要求を送信します。関連づけ要求を受信すると、AP は無線クライアントによってサポートされた容量を決定し、クライアントに対して関連づけ応答を送信します。これにより、クライアントは AP に関連づけられます。

1.2 SSIDにもとづくアクセス制御

図 1-5に示すように、SSID にもとづくアクセス制御では、ssida を Client1 と Client2 の許可された SSID として設定し、ssidb を Client3 の許可された SSID として設定します。

クライアントが認証に合格すると、サーバは関連するユーザプロファイルを AC に送信します。AC は、クライアントの関連付けられた SSID が許可された SSID であるかどうかを調べます。許可された SSID の場合、クライアントは WLAN へのアクセスを許可されます。許可されていない SSID の場合、AC はクライアントをログオフします。

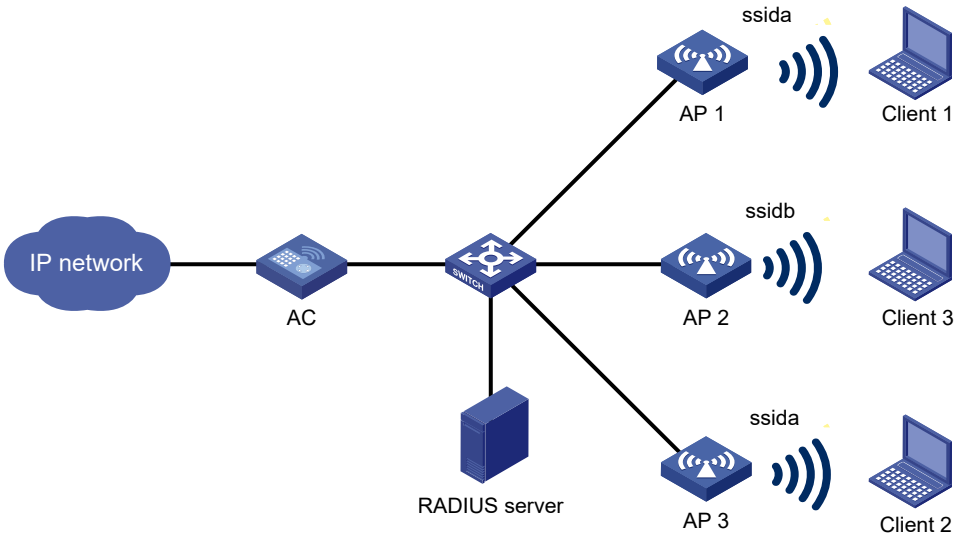


図 1-5 SSID にもとづくアクセス制御

1.3 ホワイトリスト、ブラックリストにもとづくアクセス制御

WLAN クライアントからのフレームをフィルタリングし、クライアントアクセス制御を実行するために、ホワイトリストとブラックリストを設定することができます。

- **ホワイトリスト**－WLAN にアクセスすることを許可されたすべてのクライアントの MAC アドレスを含みます。ホワイトリスト内に存在しないクライアントからのフレームは破棄されます。ホワイトリストは手動で設定されます。
- **スタティックブラックリスト**－WLAN にアクセスすることを禁止されたクライアントの MAC アドレスを含みます。スタティックブラックリストは手動で設定されます。
- **ダイナミックブラックリスト**－WLAN にアクセスすることを禁止されたクライアントの MAC アドレスを含みます。AP は、WIPS が設定された場合、あるいは URL リダイレクションが WLAN MAC 認証クライアントのために URL リダイレクションが有効である場合、リストに WLAN にアクセスすることを禁止されたクライアントの MAC アドレスを追加します。

WIPS に関する詳細は、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*8 WLAN セキュリティ*”の”*2 章 WIPS*”を参照してください。

WLAN MAC 認証クライアントの詳細は、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*13 ユーザアクセスと認証*“の”*1 章 WLAN アクセス認証*“を参照してください。

AP が関連づけ要求を受信し、AC に追加モバイルメッセージを送信すると、AC はクライアントを許可するかどうか判断するために、以下の操作を実行します。

1)　ホワイトリストを捜索します。

- クライアント MAC アドレスがホワイトリスト内のいずれのエントリとも一致しない場合、クライアントは拒否されます。
- クライアント MAC アドレスがホワイトリスト内のエントリと一致する場合、クライアントは許可されます。

2)　ホワイトリストエントリが存在しない場合、スタティック、ダイナミックブラックリストを捜索します。

- クライアント MAC アドレスがいずれかのブラックリスト内のエントリと一致する場合、クライアントは拒否されます。
- クライアント MAC アドレスがいずれのブラックリスト内のエントリとも一致しない場合、もしくはブラックリストエントリが存在しない場合、クライアントは許可されます。

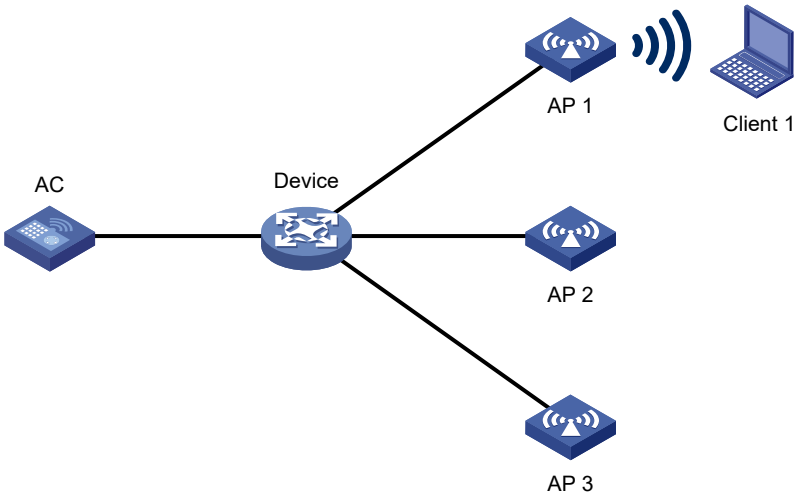


図 1-6 ホワイトリスト、ブラックリストにもとづくアクセス制御

1.4 ACLにもとづくアクセス制御

ACL にもとづくアクセスコントロールと、ホワイトリストおよびブラックリストベースのアクセスコントロールの両方を同じ装置に設定しないでください。

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。

AP View の設定は、サービステンプレート View の設定よりも優先されます。

この機能は、レイヤ 2 ACL だけをサポートし、一致基準として送信元 MAC アドレスだけを使用できます。

1.5 設定の制限とガイドライン

設定の優先順位は AP view、AP group view、global configuration view の順番で優先します。

1.6 設定作業リスト

作業リスト
（オプション設定項目）領域コードの指定

作業リスト
（必須設定項目）無線サービスの設定 ● （必須設定項目）サービステンプレートの設定 ● （オプション設定項目）サービステンプレートに対する記述の設定 ● （必須設定項目）SSIDの設定 ● （オプション設定項目）サービス テンプレートの無線に関連付けられたクライアントの最大数の設定 ● （必須設定項目）サービステンプレートの有効化 ● （必須設定項目）無線に対するサービステンプレートの設定 ● （オプション設定項目）APが指定されたサービステンプレートをAPグループから引き継がないための設定
（オプション設定項目）クライアントデータ転送の設定 ● （オプション設定項目）クライアントトラフィック転送モードの指定 ● （オプション設定項目）クライアントのトラフィック転送の有効化 ● （オプション設定項目）クライアントデータフレームに対するカプセル化フォーマットの設定 ● （オプション設定項目）APが未知のクライアントからのトラフィックを処理する方法の設定
（オプション設定項目）クライアント管理の設定 ● （オプション設定項目）ACまたはAPでのクライアントの関連づけの有効化 ● （オプション設定項目）クイックアソシエーションの有効化 ● （オプション設定項目）クライアント情報報告先のWebサーバの指定 ● （オプション設定項目）クライアントのVLANの割り当て方式の指定 ● （オプション設定項目）ローミング後のクライアントの許可VLANの選択の設定 ● （オプション設定項目）クライアント再認証を行う前のアイドル時間の設定
（オプション設定項目）クライアントメンテナンスの設定 ● （オプション設定項目）クライアントアイドルタイムアウトの設定 ● （オプション設定項目）クライアントkeepaliveの設定 ● （オプション設定項目）無線リンク品質テストの実行 ● （オプション設定項目）NAS IDの設定
（オプション設定項目）クライアントアクセス制御の設定 ● （オプション設定項目）ホワイトリストへのクライアントの追加 ● （オプション設定項目）スタティックブラックリストへのクライアントの追加 ● （オプション設定項目）ダイナミックブラックリストの設定 ● （オプション設定項目）ACLにもとづくアクセス制御の設定
（オプション設定項目）APの特定ブロードキャストプローブ要求への応答の有効化
（オプション設定項目）APへのコンフィグレーションファイルの設定
（オプション設定項目）WLANアクセスのSNMP notificationの有効化

1.7 領域コードの指定

領域コードは、使用可能周波数、使用可能チャネル、伝送電力レベルなどの性質を決定します。AP を設定する前に、有効な領域コードを設定してください。

領域コードの変更により引き起こされる規制違反を防止するために、領域コードをロックしてください。

I. AP view での領域コードの指定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP view に移行する	**wlan ap** *ap-name* [**model** *model-name*]	—
3. 領域コードを指定する	**region-code** *code*	デフォルト：APは、AP group view の設定を使用します。AP group view に領域コードが存在しない場合、APはglobal configuration view の設定を使用します。
4. 領域コードをロックする	**region-code-lock enable**	デフォルト：APは、AP group view の設定を使用します。AP group view に領域コードが存在しない場合、APはglobal configuration view の設定を使用します。

II. AP group view での領域コードの指定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP group view に移行する	**wlan ap-group** *group-name*	—
3. 領域コードを指定する	**region-code** *code*	デフォルト：APはglobal configuration view の設定を使用します。
4. 領域コードをロックする	**region-code-lock enable**	デフォルト：APはglobal configuration view の設定を使用します。

III. グローバル領域コードの指定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP group view に移行する	**wlan global-configuration**	—
3. 領域コードを指定する	**region-code** *code*	デフォルト：領域コードはJPです。
4. 領域コードをロックする	**region-code-lock enable**	デフォルト：設定なし

1.8 無線サービスの設定

1.8.1 サービステンプレートの設定

サービステンプレートは、SSID や認証方法のような無線サービス認証方式を定義します。

以下にサービステンプレートの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. サービステンプレートを作成する	**wlan service-template** *service-template-name*	デフォルト：設定なし
3. VLAN をサービステンプレートに結びつける	**vlan** *vlan-id*	デフォルト：VLAN 1

1.8.2 サービステンプレートに対する記述の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. service template view に移行する	**wlan service-template** *service-template-name*	—
3. サービステンプレートに対して記述を設定する	**description** *text*	デフォルト：設定なし

1.8.3 SSID の設定

AP は、クライアントが検出できるようにビーコン フレームで SSID をブロードキャストします。BSS が利用できない場合、またはクライアントに BSS を検出させたくない場合は、SSID ステルスを有効にできます。SSID ステルスが有効のとき、BSS は SSID をビーコンフレーム内に隠し、ブロードキャストプローブ要求に応答しません。クライアントは、WLAN にアクセスするために、指定された SSID とともにプローブ要求を送信しなければなりません。この機能により、WLAN は攻撃から保護されます。

AP に関連付けられているクライアントの数が上限に達すると、AP はビーコンフレーム内の SSID を自動的に隠し、他のクライアントは AP を検出して関連付けることができません。これらのクライアントが AP を検出するために、SSID ブロードキャスト機能を設定できます。ただし、これらのクライアントは AP に関連付けることができません。

以下に SSID の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. service template view に移行する	**wlan service-template** *service-template-name*	—

操作	コマンド	補足
3. サービステンプレートに SSID を設定する	**ssid** *ssid-name*	デフォルト：設定なし NECは、サービステンプレートに対して独自のSSIDを設定することを推奨します。
4. （オプション設定項目）ビーコンフレーム内で SSID ステルスを有効にする	**beacon ssid-hide**	デフォルト：無効

⚠ **注意：**

6GHz 帯の SSID で SSID ステルスを有効にすると接続できない端末があります。
6GHz 帯で利用するサービステンプレートでは SSID ステルスを有効にしないでください。

1.8.4 サービス テンプレートの無線に関連付けられたクライアントの最大数の設定

このタスクを実行して、無線に関連付けられているクライアント数を制限し、過負荷を回避します。この機能が設定されている場合、新しいクライアントは WLAN にアクセスできず、無線で最大数に達すると SSID は非表示になります。

以下にサービス テンプレートの無線に関連付けられたクライアントの最大数の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. service template view に移行する	**wlan service-template** *service-template-name*	—
3. サービステンプレートの無線で関連付けられるクライアントの最大数を設定する	**client max-count** *max-number*	デフォルト：設定なし

1.8.5 サービステンプレートの有効化

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. service template view に移行する	**wlan service-template** *service-template-name*	—
3. サービステンプレートを有効にする	**service-template enable**	デフォルト：無効

1.8.6 無線に対するサービステンプレートの設定

無線に対してサービステンプレートを設定する場合、AP はサービステンプレート内で定義された無線サービスを提供できる BSS を作成します。

無線に対してサービステンプレートを設定する場合、以下の作業を実行することができます。

- BSS に関連づけられたクライアントが、VLAN グループ内のすべての VLAN に対して均等に割り当てられるように、無線に VLAN グループを結びつけます。
- ネットワークアクセスサーバを識別するために、無線に NAS ポート ID もしくは NAS ID を結びつけます。
- AP がビーコンフレーム内に SSID を隠せるようにします。

I. radio view での無線に対するサービステンプレートの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP view に移行する	**wlan ap** *ap-name* [**model** *model-name*]	—
3. radio view に移行する	**radio** *radio-id*	—
4. 無線に対してサービステンプレートを設定する	**service-template** *service-template-name* [**vlan** *vlan-id* | **vlan-group** *vlan-group-name*] [**ssid-hide**] [**nas-port-id** *nas-port-id*] [**nas-id** *nas-id*]	デフォルト：AP group viewの設定が使用されます。 無線に対して最大16のサービステンプレートを設定することができます。

II. AP group radio view での無線に対するサービステンプレートの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP group view に移行する	**wlan ap-group** *group-name*	—
3. AP model view に移行する	**ap-model** *ap-model*	
4. radio view に移行する	**radio** *radio-id*	—
5. 無線に対してサービステンプレートを設定する	**service-template** *service-template-name* [**vlan** *vlan-id* | **vlan-group** *vlan-group-name*] [**ssid-hide**] [**nas-port-id** *nas-port-id*] [**nas-id** *nas-id*]	デフォルト：設定なし 無線に対して最大16のサービステンプレートを設定することができます。

1.8.7 AP が指定されたサービステンプレートを AP グループから引き継がないための設定

デフォルトでは、AP グループ内の AP は、AP グループに設定されたサービステンプレートを引き継ぎ、BSS を作成します。

本設定により、AP が、指定されたサービステンプレートを AP グループから引き継がないように設定することができます。

以下に AP が指定されたサービステンプレートを AP グループから引き継がないための設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP view に移行する	**wlan ap** *ap-name* [**model** *model-name*]	—

操作	コマンド	補足
3. radio view に移行する	**radio** *radio-id*	—
4. AP が指定されたサービステンプレートを AP グループから引き継がないように設定する	**inherit exclude service-template** *service-template-name*	デフォルト：設定なし

1.9 クライアントデータ転送の設定

1.9.1 クライアントトラフィック転送モードの指定

AC (中央転送モード) または AP (ローカル転送モード) は、クライアントトラフィックを転送できます。AP でクライアントトラフィックを転送すると、AC の転送負荷が解放されます。

トラフィック転送を指定する前に、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。

AC を使用してクライアントトラフィックを転送する設定で有効にするには、クライアントトラフィック転送が有効になっていることを確認します。

AC をトラフィック転送として指定する場合は、AC でクライアントの関連づけが有効になっていることを確認します。

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。

以下にクライアントトラフィック転送モードの指定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. service template view に移行する	**wlan service-template** *service-template-name*	—
3. クライアントトラフィックを転送するように AP を設定する	**client forwarding-location** { **ac** | **ap** }	デフォルト : APはクライアントデータ トラフィックを転送します。

1.9.2 クライアントのトラフィック転送の有効化

"*クライアントトラフィック転送モードの指定*"で AC（中央転送モード）を指定する場合、クライアントのトラフィック転送を有効にする必要があります。

以下にクライアントのトラフィック転送の有効化の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. クライアントのトラフィック転送を有効にする	**wlan client forwarding enable**	デフォルト：有効

1.9.3 クライアントデータフレームに対するカプセル化フォーマットの設定

"*クライアントトラフィック転送モードの指定*"で AC（中央転送モード）を指定する場合、AP はデータフレームをクライアントから AC に対して CAPWAP トンネルを通して送信します。クライアントデータフレームに対して、カプセル化フォーマットを 802.3 または 802.11 に設定できます。フォーマットを 802.3 に設定することで、AC がフレームフォーマット変換を実行する必要がなくなるため、NEC は 802.3 の設定を推奨します。

クライアントデータフレームに対するカプセル化フォーマットの設定手順は以下の通りです。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. service template view に移行する	**wlan service-template** *service-template-name*	—
3. クライアントデータフレームに対してカプセル化フォーマットを設定する	**client frame-format** { **dot3** | **dot11** }	デフォルト : クライアントデータフレームは、802.3フォーマット内でカプセル化されます。

1.9.4 AP が未知のクライアントからのトラフィックを処理する方法の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. service template view に移行する	**wlan service-template** *service-template-name*	—
3. AP が未知のクライアントからのトラフィックを処理する方法を設定する	**unknown-client** { **deauthenticate** | **drop** }	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を認証しません。

1.10 クライアント管理の設定

1.10.1 AC または AP でのクライアントの関連づけの有効化

AC でクライアントの関連づけを有効にする場合、管理フレームが CAPWAP トンネルを通じて AC に送信されます。これにより、安全性が保証され、管理が容易になります。AC と AP 間のネットワークが複雑なとき、NEC は AP でのクライアントの関連づけを推奨します。

クライアントの関連づけが AP で有効な場合、レイヤ 3 ローミングはサポートされません。**service-template** コマンドを使用する場合、同一のサービステンプレートを使用し、カバーエリアが重なる AP は、同一の VLAN を指定しなければなりません。

以下に AC または AP でクライアントの関連づけを有効にする設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—

操作	コマンド	補足
2. service template view に移行する	**wlan service-template** *service-template-name*	—
3. AC または AP でクライアントの関連づけを有効にする	**client association-location** { **ac** | **ap** }	デフォルト： AC

1.10.2 クイックアソシエーションの有効化

ロードバランスまたはバンドナビゲーションを有効にすることで、クライアント関連づけ効率に影響がでる可能性があります。遅延が許されないサービス、あるいはロードバランス、帯域幅のナビゲーションが必要ない環境では、サービステンプレートに対するすばやい関連づけを有効にすることができます。

この機能により、WLAN 内でロードバランスまたはバンドナビゲーションが有効な場合でも、装置がサービステンプレートに関連づけられたクライアント上で、ロードバランスまたはバンドナビゲーションを実行するのを無効にできます。

以下にクイックアソシエーションを有効にする設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. service template view に移行する	**wlan service-template** *service-template-name*	—
3. クイックアソシエーションを有効にする	**quick-association enable**	デフォルト：無効

1.10.3 クライアント情報報告先の Web サーバの指定

指定した Web サーバに対し、HTTP を使用してクライアントの情報を報告します。報告されたクライアント情報は、クライアントの MAC アドレス、紐付けされた AP、紐付いた時間を含みます。Web サーバは、サーバのホスト名、ポート番号、経路が指定された場合に限りクライアント情報を承認します。

クライアント情報報告先の Web サーバの指定方法は以下の通りです。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. Web サーバのホスト名とポート番号を指定する	**wlan web-server host** *host-name* **port** *port-number*	デフォルト：設定なし
3. Web サーバの経路を指定する	**wlan web-server api-path** *path*	デフォルト：設定なし
4. 1 度に報告するクライアントエントリの最大数を設定する	**wlan web-server max-client-entry** *number*	デフォルト：10

1.10.4 クライアントの VLAN の割り当て方式の指定

クライアントが初回にオンラインになったとき、無線はクライアントにランダムな VLAN を割り当てます。クライアントが再度オンラインになったとき、割り当て方式に依存してクライアントに VLAN を割り当てます。

- **スタティック割り当て**－クライアントは前回に割り当てられた VLAN を引き継ぎます。IP アドレスのリース期間が期限切れでない場合、クライアントは同一の IP アドレスを使用します。この方式は IP アドレス数を削減するのに役立ちます。
- **ダイナミック割り当て**－クライアントに VLAN が再度割り当てられます。すべての VLAN にクライアントがバランスよく振り分けられます。
- **互換性のあるスタティック割り当て**－クライアントは、Comware 5 と Comware 7 の AC 間のローミング時に割り当てられた VLAN を継承します。

以下にクライアントの VLAN の割り当て方式の指定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. service template view に移行する	**wlan service-template** *service-template-name*	—
3. クライアントの VLAN の割り当て方式を指定する	**client vlan-alloc** { **dynamic** | **static** | **static-compatible** }	デフォルト：ダイナミック

1.10.5 ローミング後のクライアントの許可 VLAN の選択の設定

移動する可能性のあるグループでは、すべての AC はこの機能を設定することを推奨します。

クライアントのローミングが行われた後、通常、クライアントの VLAN は変更されません。

クライアントが別の AP にローミングした後、QMC で設定されたセキュリティ警告が開始した場合、ユーザを適切に隔離するため許可 VLAN が適用されます。

この機能は 802.1X、MAC アドレス認証のクライアントのみ適用します。

以下にローミング後のクライアントの許可 VLAN の選択の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. service template view に移行する	**wlan service-template** *service-template-name*	—
3. ローミング後のクライアントの許可 VLAN の選択を設定する	**client preferred-vlan authorized**	デフォルト：有効

1.10.6 クライアント再認証を行う前のアイドル時間の設定

再認証の失敗を削減するため、クライアントに再認証を行う前のアイドル時間を設定します。

WLAN MAC アドレス認証のクライアントで URL リダイレクションが有効である場合、AP は MAC アドレス認証にパスしたクライアントをログオフします。次回の MAC アドレス認証の施行時、クライアントは MAC アドレス認証にパスし、WLAN にアクセスすることができます。アイドル時間が設定されている場合、AP はクライアントをログオフしたのち、ダイナミックブラックリストにクライアントを追加し、指定したアイドル時間後にクライアントのエントリがエージアウトします。

以下にクライアント再認証を行う前のアイドル時間の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. クライアント再認証を行う前のアイドル時間を設定する	**wlan client reauthentication-period** [*period-value*]	デフォルト：設定なし

1.11 クライアントメンテナンスの設定

1.11.1 クライアントアイドルタイムアウトの設定

クライアントアイドルタイムアウトタイマが終了する前に、関連づけられた AP に対して、オンラインのクライアントが任意の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。

I. AP view でのクライアントアイドルタイムアウトの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP view に移行する	**wlan ap** *ap-name* [**model** *model-name*]	—
3. クライアントアイドルタイムアウトタイマを設定する	**client idle-timeout** *timeout*	デフォルト：APは、AP group view の設定を使用します。

II. AP group view でのクライアントアイドルタイムアウトの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP group view に移行する	**wlan ap-group** *group-name*	—
3. クライアントアイドルタイムアウトタイマを設定する	**client idle-timeout** *timeout*	デフォルト：300秒

1.11.2 クライアント keepalive の設定

クライアント keepalive の設定機能により、AP はクライアントがオンラインかどうか識別するために、クライアントに対して指定された間隔で keepalive パケットを送信するこ

とができます。keepalive が 3 回送信される間隔以内に AP で応答を受信しない場合、クライアントをログオフします。

I. AP view でのクライアント keepalive の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP view に移行する	**wlan ap** *ap-name* [**model** *model-name*]	—
3. クライアント keepalive を有効にする	**client keep-alive enable**	デフォルト：APは、AP group view の設定を使用します。
4. （オプション設定項目）クライアント keepalive 間隔を設定する	**client keep-alive interval** *interval*	デフォルト：APは、AP group view の設定を使用します。

II. AP group view でのクライアント keepalive の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP group view に移行する	**wlan ap-group** *group-name*	—
3. クライアント keepalive を有効にする	**client keep-alive enable**	デフォルト：無効
4. （オプション設定項目）クライアント keepalive 間隔を設定する	**client keep-alive interval** *interval*	デフォルト： 300秒

1.11.3 無線リンク品質テストの実行

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、サポートされている各レートで空のデータフレームをクライアントに送信します。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。

無線リンク品質テストのタイムアウトは 10 秒です。タイムアウトになる前に無線リンクテストが完了しない場合、テスト結果を取得できません。

I. 設定手順

操作	コマンド	補足
1. 無線リンク品質テストを実行する	● user view: **wlan link-test** *mac-address*	—

1.11.4 NAS ID の設定

NAS port ID（Network Access Server Port IDentifier）は、クライアントのネットワークアクセスサーバを独自に識別し、クライアントトラフィックの送信元を区別します。

無線にサービステンプレートが設定された状態で NAS ID あるいは NAS port ID を指定する場合、無線はサービステンプレートに対して NAS ID あるいは NAS port ID を使用します。

I. AP view での NAS ID の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. クライアントの NAS port ID の形式を設定する	**wlan nas-port-id format** { **2** | **4** }	デフォルト：2
3. AP view に移行する	**wlan ap** *ap-name* [**model** *model-name*]	—
4. NAS ID を設定する	**nas-id** *nas-id*	デフォルト：APはAP group view の設定を使用します。AP group view にNAS IDが存在しない場合、APはglobal configuration view の設定を使用します。
5. NAS port ID を設定する	**nas-port-id** *nas-port-id*	デフォルト：APはAP group view の設定を使用します。AP group view にNAS port IDが存在しない場合、APはglobal configuration view の設定を使用します。
6. NAS VLAN ID を設定し、AC で RADIUS 要求の VLAN ID にカプセル化することを有効にする	**nas-vlan** *vlan-id*	デフォルト：設定なし RADIUSサーバに送信される認証要求はNAS VLAN IDフィールドがありません。 他ベンダのセキュリティアカウント管理サーバ（SAM、Security Accounting Management）がRADIUSサーバとして使用している場合、NAS VLAN IDを設定してください。

II. AP group view での NAS ID の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. クライアントの NAS port ID の形式を設定する	**wlan nas-port-id format** { **2** | **4** }	デフォルト：2
3. AP group view に移行する	**wlan ap-group** *group-name*	—
4. NAS ID を設定する	**nas-id** *nas-id*	デフォルト： APはglobal configuration view の設定を使用します。
5. NAS port ID を設定する	**nas-port-id** *nas-port-id*	デフォルト：APはglobal configuration view の設定を使用します。

III. グローバル NAS ID の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. クライアントの NAS port ID の形式を設定する	**wlan nas-port-id format** { **2** | **4** }	デフォルト：2
3. global configuration view に移行する	**wlan global-configuration**	—
4. グローバル NAS ID を設定する	**nas-id** *nas-id*	デフォルト：設定なし
5. NAS port ID を設定する	**nas-port-id** *nas-port-id*	デフォルト：設定なし

1.12 クライアントアクセス制御の設定

1.12.1 ホワイトリストへのクライアントの追加

最初のクライアントをホワイトリストに追加するとき、システムは、すべてのオンラインのクライアントを切断するかどうか尋ねます。ホワイトリストを設定するために、設定画面で“Y”を入力してください。

以下にホワイトリストへのクライアントの追加を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. ホワイトリストにクライアントを追加する	**wlan whitelist mac-address** *mac-address*	デフォルト：設定なし

1.12.2 スタティックブラックリストへのクライアントの追加

ホワイトリストとスタティック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。

以下にスタティックブラックリストへのクライアントの追加を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. スタティックブラックリストにクライアントを追加する	**wlan static-blacklist mac-address** *mac-address*	デフォルト：設定なし

1.12.3 ダイナミックブラックリストの設定

AC あるいは AP でダイナミックブラックリストを設定することができます。

AC でダイナミックブラックリストを設定した場合、AC に接続されたすべての AP はダイナミックブラックリストにあるクライアントを拒否します。

AP でダイナミックブラックリストを設定した場合、AP はダイナミックブラックリストにあるクライアントを拒否することができますが、クライアントは AC に接続された別の AP と関連し続けることができます。多くのクライアントが存在する環境では AC でダイナミックブラックリストを設定することを推奨します。

その後、ダイナミックブラックリストに追加されたエントリは設定されたエージングタイマの間、拒否されます。

ホワイトリスト、ブラックリストの両方が設定されている場合、ホワイトリストの設定が適用されます。

以下にダイナミックブラックリストの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. ダイナミックブラックリストを設定する	• APでダイナミックブラックリストを設定する：**wlan dynamic-blacklist active-on-ap** • ACでダイナミックブラックリストを設定する：**undo wlan dynamic-blacklist active-on-ap**	デフォルト：APでダイナミックブラックリストが設定されています。
3. ダイナミックブラックリストのエージングタイマを設定する	**wlan dynamic-blacklist lifetime** *lifetime*	デフォルト：300秒

1.12.4 ACL にもとづくアクセス制御の設定

クライアントが指定された ACL にもとづいて WLAN にアクセスできるようにします。ACL にもとづくアクセス制御と、ホワイトリストおよびブラックリストの両方を同じ装置に設定しないでください。

AP View の設定は、サービステンプレート View の設定よりも優先されます。

この機能は、レイヤ 2 ACL だけをサポートし、一致基準として送信元 MAC アドレスだけを使用できます。

リモート AP 機能を有効にし、ACL に **permit-remote-ap** を指定した場合、AC は許可ルールに一致するオンラインクライアントのキャッシュエントリを AP と同期します。AP がリモート状態になった場合、キャッシュエントリ内のクライアントだけがネットワークにアクセスできます。

以下に ACL にもとづくアクセス制御の設定を示します。

I. サービステンプレート View での ACL にもとづくアクセス制御の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. service template view に移行する	**wlan service-template** *service-template-name*	—
3. ACL にもとづくアクセス制御を設定する	**access control acl** *acl-number* [**permit-remote-ap**]	デフォルト：設定なし

II. AP View での ACL にもとづくアクセス制御の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP view に移行する	**wlan ap** *ap-name* [**model** *model-name*]	—
3. ACL にもとづくアクセス制御を設定する	**access control acl** *acl-number* [**permit-remote-ap**]	デフォルト：設定なし

1.13 APの特定ブロードキャストプローブ要求への応答の有効化

ブロードキャストプローブ要求は、いずれの SSID も運びません。ブロードキャストプローブ要求を受信すると、AP はサービス情報を運ぶプローブ応答で応答します。

デフォルトでは、AP はすべてのブロードキャストプローブ要求に応答するため、ネットワークセキュリティが脅かされ、AP のパフォーマンスが低下する可能性があります。ただし、ブロードキャストプローブ要求への応答を無効にすると、クライアントが時間内に最適な AP にローミングできなくなり、クライアントアクセスに影響する可能性があります。

このタスクを実行すると、強い信号強度を持つ特定の周波数帯域からのブロードキャスト要求に AP が応答できるようになります。

I. AP view での AP のブロードキャストプローブ要求への応答の無効化

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP view に移行する	**wlan ap** *ap-name* [**model** *model-name*]	—
3. AP でブロードキャストプローブ要求への応答を無効にする	**broadcast-probe reply** { **disable** | **enable** [**rssi-threshold** *rssi-value*] } [**frequency-band** { **2.4** | **5** }]	デフォルト：APは、AP group view の設定を使用します。

II. AP group view での AP のブロードキャストプローブ要求への応答の無効化

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP group view に移行する	**wlan ap-group** *group-name*	—
3. AP でブロードキャストプローブ要求への応答を無効にする	**broadcast-probe reply** { **disable** | **enable** [**rssi-threshold** *rssi-value*] } [**frequency-band** { **2.4** | **5** }]	デフォルト：APは、すべてのブロードキャストプローブ要求に応答します。

1.14 APへのコンフィグレーションファイルの設定

🕮 **メモ：**

- AP へのコンフィグ設定は **remote-configuration** を使用することを推奨します。**remote-configuration** コマンドの詳細は、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*7 AP 管理*”の”*1 章 AP 管理*”を参照してください。
- **remote-configuration** を有効にした場合、**remote-configuration** で設定可能なコマンドがデフォルト値として適用されます。**remote-configuration** で設定できないコマンドを設定したい場合に限り、**map-configuration** の併用をご検討ください。また、**remote-configuration** と **map-configuration** の両方に同じ機能を有するコマンド設定がある場合、AP へのコンフィグ適用が正常におこなわれません。

AC から AP の設定を行う場合、**map-configuration** コマンドを使用してコンフィグレーションファイルを AP に設定できます。コンフィグレーションファイルは手動で作成し、予め FTP などによって AC の **flash:/**内に保存しておく必要があります。

AC の **flash:/**には予め下記の 3 つのサンプルコンフィグファイルが保存されています。

- **Trunk.mpcfg** – AP の G1/0/1 または G1/0/2 を trunk ポートとし permit-vlan all で運用する場合に使用します。
- **LAG.mpcfg** – AP の G1/0/1 および G1/0/2 を LAG ポートとして運用する場合に使用します。
- **LAG_Trunk.mpcfg** – AP の G1/0/1 および G1/0/2 を LAG ポートとし、さらに trunk ポートの permit-vlan all で運用する場合に使用します。

各サンプルコンフィグファイルの内容は **more** *file-name* コマンドでも確認可能です。

🕮 **メモ：**

- サンプルコンフィグでは特定の **Vlan** の作成は設定されておりません。
- サンプルコンフィグをそのまま使用する場合、wlan ap view で **remote-configuration enable** を使用し、任意の **vlan** を設定して下さい。

AC までの CAPWAP トンネルが稼働した後、コンフィグレーションファイルが適用されます。AP を再起動すると、コンフィグレーションファイルは失効します。

コンフィグレーションファイルの内容は、正しいフォーマットで入力されたコマンド完全なコマンドにする必要があり、省略したコマンドを使用することはできません。

AP がコンフィグレーションファイルを使用して設定される場合、AC までの CAPWAP トンネルが確立可能なネットワークである必要があります。

クラウドクラスタを形成する際、Master 装置と Standby 装置が切り替わる場合に備え、各メンバ AC にコンフィグレーションファイルを保存してください。**map-configuration** コマンドはマスタ AC にのみ適用できます。**map-configuration** コマンドを実行するときにパスを指定する場合、Master 装置のファイルにパスが通じていることを確認してください。

以下に AP へのコンフィグレーションファイルの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—

操作	コマンド	補足
2. AP view に移行する	**wlan ap** *ap-name* [**model** *model-name*]	—
3. AP で使用するコンフィグレーションファイルを設定する	**map-configuration** *filename*	デフォルト：設定なし ACのストレージメディアに使用するコンフィグレーションファイルが格納されていることを確認してください。

1.15 WLANアクセスのSNMP notificationの有効化

SNMP notification の通知機能は重要な WLAN アクセスに関するイベントを NMS に通知するため、SNMP notification を作成します。NMS は設定された出力ルールにしたがって notification を出力する方法を決定します。SNMP notification の詳細は、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*17 ネットワーク管理と監視*”の” *4 章 SNMP*”を参照してください。

以下に WLAN アクセスの SNMP notification の有効化を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. WLAN アクセスの SNMP notification を有効にする	• クライアントアクセスにSNMP通知を有効にする **snmp-agent trap enable wlan client** • クライアント監査にSNMP通知を有効にする **snmp-agent trap enable wlan client-audit**	デフォルト：無効

1.16 WLANアクセスの表示と維持

すべての view で **display** コマンドを実行し、user view で **reset** コマンドを実行できます。

操作	コマンド
ブラックリストエントリを表示する	**display wlan blacklist** { **dynamic** | **static** }
basic service set (BSS) 情報を表示する	**display wlan bss** { **all** | **ap** *ap-name* | **bssid** *bssid* } [**verbose**]
クライアント情報を表示する	**display wlan client** [**ap** *ap-name* [**radio** *radio-id*] | **mac-address** *mac-address* | **service-template** *service-template-name* | **frequency-band** { **2.4** | **5** | **6** }] [**verbose**] 📖 メモ：**frequency-band 6** のパラメータはソフトウェアバージョン9.6.05cを含む以降のソフトウェアからサポートしています。
APに対する領域コード情報を表示する	**display wlan region-code ap** { **all** | **name** *ap-name* }
サービステンプレート情報を表示する	**display wlan service-template** [*service-template-name*] [**verbose**]

操作	コマンド
クライアントの統計情報を表示する	**display wlan statistics client** [**mac-address** *mac-address*]
クライアント接続履歴を表示する	**display wlan statistics connect-history service-template** *service-template-name* }
サービステンプレートの統計情報を表示する	**display wlan statistics service-template** *service-template-name*
ホワイトリストエントリを表示する	**display wlan whitelist**
クライアントをログオフする	**reset wlan client** { **all** | **mac-address** *mac-address* }
クライアントのステータス情報を表示する	**display wlan client status** [**mac-address** *mac-address*] [**verbose**]
指定されたクライアントまたはすべてのクライアントをダイナミックブラックリストから削除する	**reset wlan dynamic-blacklist** [**mac-address** *mac-address*]
クライアントの統計情報を削除する	**reset wlan statistics client** { **all** | **mac-address** *mac-address* }
サービステンプレートの統計情報を削除する	**reset wlan statistics service-template** *service-template-name*

1.17 WLANアクセスの設定例

1.17.1 WLAN アクセスの設定例

I. ネットワーク要件

図 1-7に示すように、スイッチは AP とクライアントに IP アドレスを割り当てるための DHCP サーバとして動作します。AP は、無線サービスに SSID trade-off を提供します。

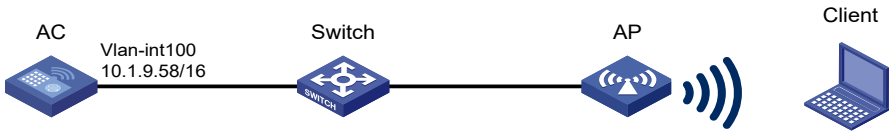


図 1-7 ネットワーク図

II. 設定手順

1)　VLAN 100 を作成します。

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
```

2)　VLAN-interface 100 を作成し、IP アドレスに VLAN-interface 100 を割り当てます。

```
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 10.1.9.58 16
```

3) 手動 AP ap1 を作成し、AP モデルとシリアル ID を指定します。

```
[AC] wlan ap ap1 model QX-W1110
[AC-wlan-ap-ap1] serial-id 219801A28N819CE0002T
```

4) サービステンプレートを作成し、AP 無線にサービステンプレートを設定します。

サービステンプレート service1 を作成します。サービステンプレートに SSID として trade-off を設定し、VLAN 100 を設定します。サービステンプレートを有効にします。

```
<AC> system-view
[AC] wlan service-template service1
[AC-wlan-st-service1] ssid trade-off
[AC-wlan-st-service1] vlan 100
[AC-wlan-st-service1] service-template enable
[AC-wlan-st-service1] quit
```

radio 1 に対してサービステンプレート service1 を設定します。

```
[AC] wlan ap ap1
[AC-wlan-ap-ap1] radio 1
[AC-wlan-ap-ap1-radio-1] radio enable
[AC-wlan-ap-ap1-radio-1] service-template service1
```

III. 設定の確認

SSID が trade-off か検証し、サービステンプレートを有効にします。

```
[AC] display wlan service-template verbose
Service template name           : service1
Description                     : Not configured
SSID                            : trade-off
SSID-hide                       : Disabled
User-isolation                  : Disabled
Service template status         : Enabled
Maximum clients per BSS         : 64
Frame format                    : Dot3
Seamless roam status            : Disabled
Seamless roam RSSI threshold    : 0
Seamless roam RSSI gap          : 0
VLAN ID                         : 100
AKM mode                        : Not configured
Security IE                     : Not configured
Cipher suite                    : Not configured
TKIP countermeasure time        : 0 s
PTK life time                   : 43200 s
GTK rekey                       : Enabled
GTK rekey method                : Time-based
GTK rekey time                  : 86400 s
GTK rekey client-offline        : Disabled
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                : 4096
Max MAC-auth users              : 4096
802.1X re-authenticate          : Enabled
Authorization fail mode         : Online
Accounting fail mode            : Online
Authorization                   : Permitted
Key derivation                  : N/A
PMF status                      : Disabled
Hotspot policy number           : Not configured
Forwarding policy status        : Disabled
Forwarding policy name          : Not configured
FT status                       : Disabled
QoS trust                       : Port
QoS priority                    : 0
BTM status                      : Disabled
```

クライアントを AP に関連づけます。（詳細は省略します。）

クライアントが WLAN にアクセスできるか確認します。

```
[AC] display wlan client service-template service1
Total number of clients: 3

MAC address     Username            APID/RID  IP address                VLAN ID
0023-8933-223b  N/A                  1024/1    3.0.0.3                    100
```

1.17.2 ホワイトリストの設定例

I. ネットワーク要件

図 1-8に示すように、MAC アドレスが 0000-000f-1211 のクライアントのみが WLAN へのアクセスを許可されるように、ホワイトリストを設定します。

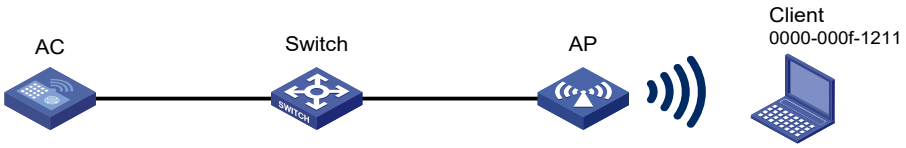


図 1-8 ネットワーク図

II. 設定手順

#ホワイトリストに MAC アドレス 0000-000f-1211 を追加します。

```
<AC> system-view
[AC] wlan whitelist mac-address 0000-000f-1211
```

III. 設定の確認

MAC アドレス 0000-000f-1211 がホワイトリストにあるか確認します。

```
[AC] display wlan whitelist
Total number of clients: 1
 MAC addresses:
  0000-000f-1211
```

1.17.3 スタティックブラックリストの設定例

I. ネットワーク要件

図 1-9に示すように、MAC アドレスが 0000-000f-1211 のクライアントのみが WLAN へのアクセスを拒否されるように、スタティックブラックリストを設定します。

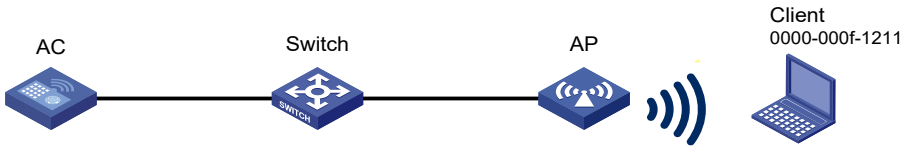


図 1-9 ネットワーク図

II. 設定手順

スタティックブラックリストに MAC アドレス 0000-000f-1211 を追加します。

```
<AC> system-view
[AC] wlan static-blacklist mac-address 0000-000f-1211
```

III. 設定の確認

MAC アドレス 0000-000f-1211 がスタティックブラックリストにあるか確認します。

```
[AC] display wlan blacklist static
Total number of clients: 1
 MAC addresses:
  0000-000f-1211
```

1.17.4 ACL の設定例

図 1-10に示すように、Client 1 および Client 2 と同じ OUI を持つクライアントが WLAN にアクセスできるように、ACL ベースのアクセス制御を設定します。

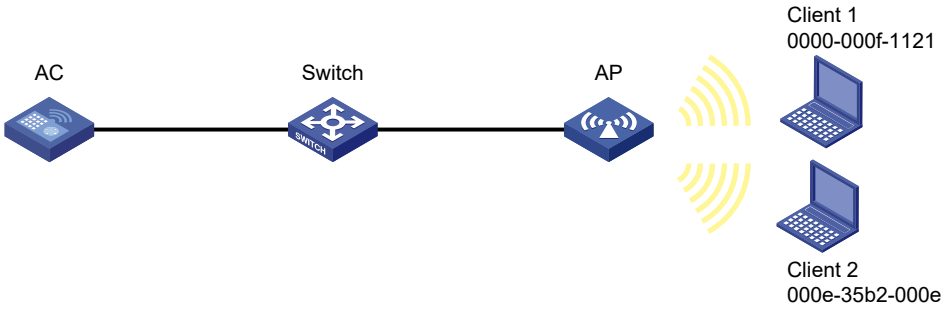


図 1-10 ネットワーク図

I. 設定手順

レイヤ 2 ACL 4000 を作成し、Client 1 と Client 2 と同じ OUI を持つクライアントを許可する ACL ルールを作成します。

```
<Switch> system-view
[Switch] acl mac 4000
[Switch-acl-mac-4000] rule 0 permit source-mac 0000-000f-1121 ffff-ffff-ffff
[Switch-acl-mac-4000] rule 1 permit source-mac 000e-35b2-000e ffff-ff00-0000
[Switch-acl-mac-4000] quit
```

ACL 4000 をサービステンプレート service 1 に設定します。

```
[Switch] wlan service service1
[Switch-wlan-st-service1] access-control acl 4000
```

II. 設定の確認

display wlan client コマンドを実行して、Client 1 および Client 2 と同じ OUI を持つクライアント (Client 2 を含む) だけが WLAN にアクセスできることを確認します。

```
[AC] display wan client
Total number of clients: 2

MAC address    Username          AP name       RID   IPv4 address        VLAN
0000-000f-1121 N/A               ap            1     192.168.100.12      1
           00e-35b2-000e N/A            ap          1     192.168.100.13     1
```

QX-W2300AC シリーズ アクセスコントローラ

オペレーションマニュアル

7.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
02-コンフィグレーションプロファイルの設定

目次

このセクションのページは **7-x-x** です。

1 章 AP 管理 1-1
1.1 概要 1-1
1.1.1 管理可能な AP モデルと動作モード 1-1
1.1.2 CAPWAP トンネル 1-1
1.1.3 APDB 1-5
1.1.4 プロトコルと基準 1-5
1.2 制約事項とガイドライン 1-5
1.3 AP 管理設定の操作リスト 1-6
1.4 CAPWAP トンネルの確立 1-6
1.4.1 CAPWAP トンネル確立を設定するための前提条件 1-6
1.4.2 手動 AP の作成 1-7
1.4.3 自動 AP の管理 1-8
1.4.4 AC に対する AP 接続優先度の設定 1-9
1.4.5 ユニキャスト検出要求のみ応答する AC の設定 1-9
1.5 AP グループの設定 1-10
1.6 AP のソフトウェアのアップグレード 1-11
1.6.1 ソフトウェアアップグレードの設定 1-11
1.6.2 AP モデルのソフトウェアとハードウェアのバージョンマッピングの設定 1-12
1.6.3 AC が AP イメージファイルを取得するための優先ロケーションの指定 1-12
1.6.4 オンライン AP へのイメージファイルの展開 1-13
1.7 AP の給電モードの設定 1-14
1.7.1 AP の給電モードの仕様 1-14
1.7.2 設定手順 1-15
1.8 リモート設定の割り当て設定 1-15
1.8.1 オンライン AP との設定の同期 1-15
1.9 CAPWAP トンネルの設定 1-16
1.9.1 AP に対する制御トンネルの keepalive 時間の設定 1-16
1.9.2 AP に対するデータトンネルの keepalive 時間の設定 1-17
1.9.3 CAPWAP パケットの最大フラグメントサイズの設定 1-18
1.9.4 CAPWAP トンネルの TCP MSS の設定 1-18
1.10 region コードの設定 1-19
1.10.1 region コードの指定 1-19
1.11 AC 要求の再送信の設定 1-20
1.12 AP のメンテナンス 1-20
1.12.1 AP のリセット 1-20
1.12.2 手動 AP の名前変更 1-20
1.12.3 AP のファイルシステムの管理 1-21
1.12.4 統計情報レポート間隔の設定 1-21
1.12.5 LED 照明モードの設定 1-22
1.12.6 AP への設定ファイルの展開 1-22
1.13 AP 管理の高度な機能の設定 1-23
1.13.1 リモート AP の設定 1-23
1.14 AC のメンテナンス 1-24
1.14.1 タイムゾーン同期の有効化 1-24

1.14.2 APDB ユーザスクリプトのロード 1-24
1.15 SNMP 通知の設定 1-25
1.15.1 SNMP 通知の有効化 1-25
1.15.2 SNMP トラップをトリガーするためのオンライン AP 数の閾値の設定 1-25
1.16 AP 管理の表示と維持 1-26
1.16.1 AP 接続レコードの表示とクリア 1-26
1.16.2 AP 管理情報の表示とクリア 1-26
1.16.3 すべての AP または指定された AP のリブートログのクリア 1-27
1.16.4 CAPWAP トンネル情報の表示とクリア 1-27
1.16.5 クラウドラスタの統計情報の表示とクリア 1-27
1.17 AP 管理の設定例 1-27
1.17.1 DHCP を通した CAPWAP トンネル確立の設定例 1-27
1.17.2 DNS を通した CAPWAP トンネル確立の設定例 1-31
1.17.3 自動 AP の設定例 1-35
1.17.4 AP group の設定例 1-38

1章 AP 管理

1.1 概要

数多くの AP（Access Point）を管理するのは、時間を浪費しコストもかかります。AP＋AC 適合ネットワーク構築により、AC は数多くの AP を有する CAPWAP（Control And Provisioning of Wireless Access Points）トンネルを確立でき、集約した AP の管理と保守が可能となります。

1.1.1 管理可能な AP モデルと動作モード

QX-W2300AC シリーズアクセスコントローラで管理可能な AP モデルと動作モードを表 1-1 に示します。

表 1-1 QX-W2300AC でサポートしている AP モデルと動作モード

FIT/Anchor-FIT AP モデル アクセスコントローラ	QX-W1010 QX-W1020 QX-W1030	QX-W1110 QX-W1120 QX-W1130	QX-W1210 QX-W1230	QX-W1240
QX-W2300AC	FIT	Anchor-FIT	Anchor-FIT (v9.6.05c 以降でサポート)	Anchor-FIT (v9.4.13 以降でサポート)

1.1.2 CAPWAP トンネル

CAPWAP は、AP と AC の通信方法を定義します。CAPWAP は、AP と AC 間に包括的なカプセル化とトランスポート構造を提供します。CAPWAP は UDP を使用し、IPv4 をサポートします。

図 1-1 に示すように、AC と AP は、データパケットを転送するためにデータトンネルを確立します。また、制御パケットを転送するために、制御トンネルを確立します。

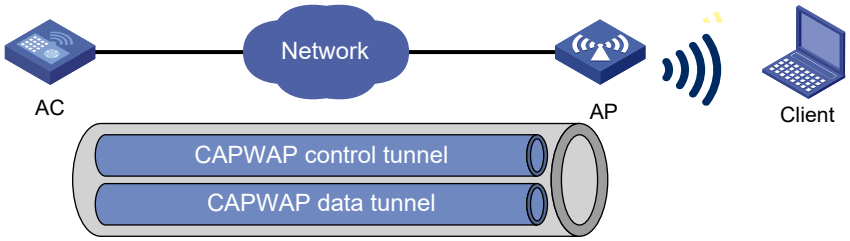


図 1-1 CAPWAP トンネル

I. AP 検出

使用するコンフィグレーションファイルが設定されていない状態で、AP は自動的に VLAN-interface1 を作成し、インタフェース上で DHCP クライアント、DHCPv6 クライアント、DNS 機能を使用可能にします。その後、DHCP サーバから自身の IP アドレスを取得し、以下の手法を用いて AC を検出します。

- DHCP オプション

a) APは、Option 138、Option 43およびオプション52からACのIPv4アドレスを取得します。IPv4アドレスは降順で使用します。

- DNS

a) APはDHCPサーバからドメイン名のサフィックスを取得します。

b) APは、取得したサフィックスをホスト名に追加します。

c) DNSサーバは、ドメイン名をIPアドレスに変換します。

DNS に関する詳細は、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*5 ネットワーク接続*”の”*18 章 DNS*”を参照してください。

- ブロードキャスト

  AP は AC を検出するために、IP アドレス 255.255.255.255 に対してブロードキャスト検出要求を送信します。

- IPv4 マルチキャスト

  AP は AC を検出するために、IPv4 アドレス 224.0.1.140 に対してマルチキャスト検出要求を送信します。

DHCPv4 オプション、ブロードキャスト/IPv4 マルチキャスト、IPv4 DNS の方式が降順で使用されます。

AP は、検出した AC の 1 つとの CAPWAP トンネルを確立するまで AC 検出を停止しません。

II. DHCP オプション

1) Option 43

Option 43 は、大文字と小文字を区別しない 16 進数形式でのみ設定できます。PXE サーバアドレスサブオプションと ACS パラメータサブオプションが含まれています。

- PXE サーバアドレスサブオプション。
  - 1 つの AC IPv4 アドレス (たとえば、2.2.2.2) を指定する場合は、DHCP サーバの DHCP アドレスプール view で Option 43 hex 800700000102020202 を指定する必要があります。
  - 80: 固定値、長さ 1 バイト

- 07: 後続のフィールドの長さ。この例では、後続のフィールドの長さは 7 バイトです。
- 0000: 固定値
- 01: AC IPv 4 アドレスの数。この例では、IPv 4 アドレスを 1 つ指定しています。
- 02020202: 16 進数形式の AC IPv 4 アドレス。最大 16 個の IPv 4 アドレスを指定でき、IPv 4 アドレス間にスペースは使用できません。
- 6.6.6.2 と 6.6.6.3 のように 2 つの AC IPv 4 アドレスを指定する場合、DHCP サーバの DHCP アドレスプール view で Option 43 の 16 進数 800 b 0000020606060606060603 を指定する必要があります。

- ACS パラメータサブオプション。

1 つの AC IPv 4 アドレス (たとえば、2.2.2.2) を指定する場合は、DHCP サーバの DHCP アドレスプール view で Option 43 hex 010402020202 を指定する必要があります。

- 01: 固定値、1 バイト長。
- 04: 後続のフィールドの長さ。この例では、後続のフィールドの長さは 4 バイトです。
- 02020202: 16 進数形式の AC IPv 4 アドレス。最大 16 個の IPv 4 アドレスを指定でき、IPv 4 アドレス間にスペースは使用できません。
- 6.6.6.2 と 6.6.6.3 のように 2 つの AC IPv 4 アドレスを指定する場合は、DHCP サーバの DHCP アドレスプール view でオプション 43 の 16 進数 01080606060206060603 を指定する必要があります。

2) Option 138

Option 138 は、16 進形式と IP 形式で設定できます。16 進形式では、Option 138 に PXE サーバアドレスサブオプションと ACS パラメータサブオプションが含まれます。16 進形式のサブオプションのフィールドは、Option 43 と同じです。

- 1 つの AC IPv 4 アドレス (たとえば、192.168.0.100) を指定する場合は、DHCP サーバの DHCP アドレスプール view で Option 138 ip-address 192.168.0.100 を指定する必要があります。

最大 8 つの IPv 4 アドレスを指定でき、スペースで区切る必要があります。

- 6.6.6.2 と 6.6.6.3 のように、2 つの AC IPv 4 アドレスを指定する場合は、DHCP サーバの DHCP アドレスプール view で Option 138 ip-address 6.6.6.2 6.6.6.3 を指定する必要があります。

3) Option 52

Option 52 は、大文字と小文字を区別しない 16 進数形式でのみ設定できます。

III. CAPWAP トンネル確立

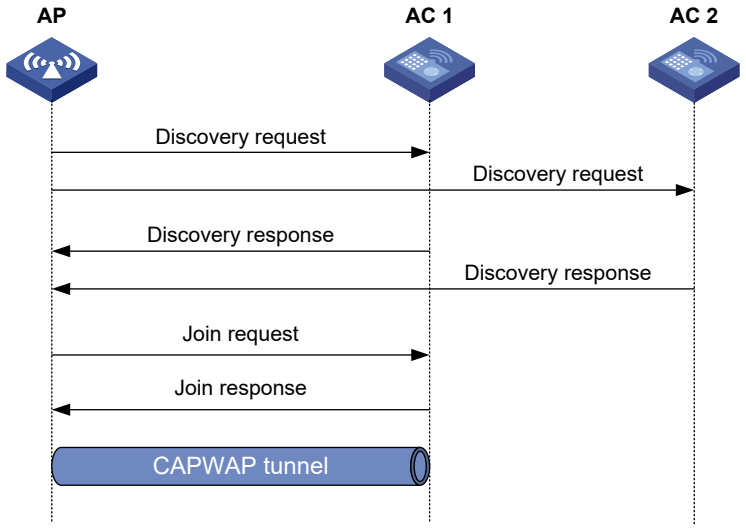


図 1-2 CAPWAP トンネルの確立

図 1-2 に示すように、AP と AC は、以下の手順で CAPWAP トンネルを確立します。

1) AP は AC を検出するために、各 AC に対して検出要求を送信します。
2) 検出要求を受信したあと、各 AC は、自身のローカル設定と要求内の情報にもとづき、検出応答を送信するかどうか決定します。

a) 検出要求がユニキャストパケットかどうかを識別します。

- **ユニキャストパケット**－AC はステップ B に進みます。
- **ブロードキャストあるいはマルチキャストパケット**－ユニキャスト検出要求のみ応答する機能が無効の場合、AC はステップ B に進みます。ユニキャスト検出要求のみ応答する機能が有効の場合、AC は検出応答を送信しません。

b) 検出要求で指定されたAPモデルで手動APの設定があるかどうかを識別します。

- 手動 AP の設定が存在する場合、AC は AP に検出応答を送信します。検出応答には、AP で手動設定があるかどうかの情報、AP の接続優先度、AC の負荷状態が含まれます。
- 手動 AP の設定が存在する場合、AC はステップ C に進みます。

c) 自動APが有効かどうかを識別します。

- 自動 AP が有効の場合、AC は AP に検出応答を送信します。検出応答には、自動 AP の有効化機能の状態、AP の接続優先度、AC の負荷状態が含まれます。
- 自動 AP が無効の場合、AP は検出応答を送信しません。

3) 検出応答を受信すると、AP は下記の順に条件を比較し、最適な AC を選択します。

- 1. AP に関する情報を保存している AC
- 2. 自動 AP 機能が有効な AC
- 3. AP 接続の優先度が高い AC
- 4. 管理している AP 数が少ない AC
- 5. 最も早く応答する AC

4) AP は、最適な AC に対して参加要求を送信します。
5) 参加要求を受信したあと、AC は AP に対してアクセスサービスを提供するかどうかを決定するために、要求内の情報を調査し、参加応答を送信します。
6) 参加応答を受信したあと、AP は応答内のリザルトコードを調査します。

- リザルトコードが失敗と表示された場合、AP は AC との CAPWAP トンネルを確立しません。
- リザルトコードが成功と表示された場合、AP は AC との CAPWAP トンネルを確立します。

1.1.3 APDB

AC の APDB（Access Point Information Database）は以下の AP 情報を記録します。

- AP のモデル名
- ハードウェアバージョン、ソフトウェアバージョンの対応表
- AP モデル名でサポートされる無線情報
  - 無線数
  - 無線タイプ
  - 有効なアンテナタイプ
  - 最大出力電力

APDB に対応する AP モデル情報が含まれるときのみ、AC は AP と CAPWAP トンネルを確立することができます。

APDB のデータを管理するため、システムスクリプトとユーザスクリプトを使用することができます。システムスクリプトは AC のソフトウェアによってリリースされます。AC が起動するたびに自動で読み込まれます。新しい AP モデルを追加する場合、AC ソフトウェアバージョンをアップグレードするか、*ユーザスクリプトを作成して AC にロードします*(「APDB ユーザスクリプトのロード」 を参照) 。

1.1.4 プロトコルと基準

- RFC 5415, *Control And Provisioning of Wireless Access Points (CAPWAP) Protocol Specification*
- RFC 5416, *Control and Provisioning of Wireless Access Points (CAPWAP) Protocol Binding for IEEE 802.11*
- RFC 5417, *Control And Provisioning of Wireless Access Points (CAPWAP) Access Controller DHCP Option*

1.2 制約事項とガイドライン

次の方法を使用して AP を設定できます。

- AP view で 1 つずつ AP を設定します。
- AP グループに AP を割り当て、AP group view で AP グループを設定します。
- グローバル設定 view ですべての AP 設定を表示します。

AP の場合、これらの view で同じパラメータに対して行った設定は、AP view、AP group view、グローバル設定 view の降順で有効になります。

大規模なネットワーク展開の場合は、AP group view で AP を設定することをお勧めします。

マネジメント Ethernet ポートを使用して、AP との CAPWAP 接続はできません。

1.3 AP管理設定の操作リスト

操作リスト
1.（必須設定項目）CAPWAPトンネルの確立 手動AP作成か、自動APの管理のいずれかを選択します （選択設定項目）手動APの作成 （選択設定項目） 自動APの管理 （オプション設定項目）ACに対するAP接続優先度の設定 （オプション設定項目）ユニキャスト検出要求のみ応答するACの設定
2.（オプション設定項目）APグループの設定
3.（オプション設定項目）APのソフトウェアのアップグレード
4.（オプション設定項目）リモート設定の割り当て設定
5.（オプション設定項目）CAPWAPトンネルの設定 （オプション設定項目）APに対する制御トンネルのkeepalive時間の設定 （オプション設定項目）APに対するデータトンネルのkeepalive時間の設定 （オプション設定項目）CAPWAPパケットの最大フラグメントサイズの設定 （オプション設定項目）CAPWAPトンネルのTCP MSSの設定
6.（オプション設定項目）regionコードの設定
7.（オプション設定項目）AC要求の再送信の設定
9.（オプション設定項目）APのメンテナンス （オプション設定項目）APのリセット （オプション設定項目）手動APの名前変更 （オプション設定項目）APのファイルシステムの管理 （オプション設定項目）統計情報レポート間隔の設定 （オプション設定項目）LED照明モードの設定 （オプション設定項目）APへの設定ファイルの展開
10.（オプション設定項目）AP管理の高度な機能の設定 （オプション設定項目）リモートAPの設定
11.（オプション設定項目）1.14 ACのメンテナンス （オプション設定項目）タイムゾーン同期の有効化 （オプション設定項目）APDB ユーザスクリプトのロード
12.（オプション設定項目）SNMP通知の設定 （オプション設定項目）SNMP通知の有効化 （オプション設定項目）SNMPトラップをトリガーするためのオンラインAP数の閾値の設定

1.4 CAPWAPトンネルの確立

1.4.1 CAPWAP トンネル確立を設定するための前提条件

AP を管理する前に、次のタスクを完了します。

- DHCP サーバに DHCP アドレスプールを作成し、IP アドレスを AP に割り当てます。
- AP 検出に DHCP オプションを使用する場合は、DHCP サーバ上の DHCP アドレスプールにオプション 138、オプション 43、オプション 52 を設定します。

- AP 検出に DNS を使用する場合は、DHCP サーバ上の DHCP アドレスプールに DNS サーバの IP アドレスと AC ドメイン名サフィックスを設定します。次に、DNS サーバ上でドメイン名と AC IP アドレスのマッピングを設定します。
- AP と AC が相互に到達できることを確認します。

DHCP と DNS の詳細については、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*5 ネットワーク接続*”を参照してください。

1.4.2 手動 AP の作成

使用している AP のモデル、シリアル ID、および手動 AP アドレスに基づいて、AC に MAC を作成できます。AP は、手動 AP 設定を保存する AC を使用して CAPWAP トンネルを確立することを優先します。

以下に手動 AP の設定手順を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． 手動 AP view に移行する	物理AP viewに移行する： **wlan ap** *ap-name* [**model** *model-name*]	デフォルト：設定なし APを作成するときは、モデル名を指定しなければなりません。
3． AP に対してシリアル ID または MAC アドレスを指定する	APに対してシリアルIDを指定する： **serial-id** *serial-id* APに対してMACアドレスを指定する： **mac-address mac-address**	いずれかのコマンドを使用します。
4． （オプション設定項目） AP に対して記述を設定する	**description** *text*	デフォルト：設定なし

1.4.3 自動 AP の管理

自動 AP 機能を使用すると、手動 AP 設定なしで AP を AC に接続できます。この機能により、WLAN に多数の AP を展開するときに設定が簡素化されます。

I. 制約事項とガイドライン

不正な AP が AC に関連付けられないようにするには、必要なすべての AP が AC に関連付けられた後で自動 AP 機能を無効にします。

次の理由により、自動 AP をオンラインになった後で手動 AP に変換する必要があります。

- 自動 AP は、手動 AP に変換された場合にのみ、AC の再起動または CAPWAP トンネルの終了時に AC と再関連付けできます。
- 手動 AP に変換された場合にのみ、自動 AP を個別に設定できます。

II. タスクの概要

自動 AP を設定するには、次のタスクを実行します。

- 自動 AP 機能の有効化
- (オプション) 自動 AP から手動 AP への変換

III. 前提条件

自動 AP のリモート認証を設定する前に、AC で認証ドメインとユーザスキームを指定し、RADIUS サーバで AAA アカウントを作成します。認証ドメインと AAA スキームの詳細については、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*13 ユーザアクセスと認証*“の”*3 章 AAA*“を参照してください。

IV. 自動 AP 機能の有効化

操作	コマンド	補足
1． system view に移行する	**system-view**	—

操作	コマンド	補足
2． 自動 AP 機能を有効にする	**wlan auto-ap enable**	デフォルト：無効

V. 自動 AP から手動 AP への変換

自動 AP を手動 AP に変換するために本操作を実行します。

以下に自動 AP パーシステンスの設定手順を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． 自動 AP パーシステンスを設定する	オンライン自動APを手動APに変換する： **wlan auto-ap persistent** { **all** | **name** *auto-ap-name* [*new-ap-name*] } 自動APがオンラインになったあと、自動的に自動APを手動APに変換する： **wlan auto-persistent enable**	いずれかのコマンドを使用します。 すでにオンラインの自動APに対しては、**wlan auto-persistent enable** コマンドは適用しません。

1.4.4 AC に対する AP 接続優先度の設定

AC は、検出応答内に AP 接続優先度を記載します。また AP は、より接続優先度の高い AC との CAPWAP トンネルを優先して確立します。以下のどちらかの状態が存在します。

- 複数の AC は手動 AP の設定があります。
- AC に手動 AP の設定がないが、複数の AC で自動 AP 機能が有効です。

I. AP view での AP 接続優先度の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP view または AP group view に移行する	AP viewに移行する。 **wlan ap** *ap-name* AP group viewに移行する。 **wlan ap-group** group-name	—
3． AP 接続優先度を設定する	**priority** *priority*	AP viewでは、AP は AP group viewの設定を使用します。 デフォルト:4

1.4.5 ユニキャスト検出要求のみ応答する AC の設定

AP は、検出した AC に対してユニキャスト、マルチキャスト、ブロードキャスト検出要求を送信できます。本機能により、AC はユニキャスト検出要求に対してのみ応答することができるようになります。

以下に AC にユニキャスト検出要求のみに応答させる設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. ユニキャスト検出要求に対してのみ応答する AC を設定する	**wlan capwap discovery-policy unicast**	デフォルト：ACは、ユニキャスト、マルチキャスト、ブロードキャスト検出要求に応答できます。

1.5 APグループの設定

I. このタスクについて

この機能を使用すると、複数の AP をバッチで設定して、設定のワークロードを軽減できます。

AP グループ内の AP は、グループの設定を使用します。デフォルトでは、すべての物理 AP はシステム定義の AP グループ default-group に属します。システム定義の AP グループは削除できません。

AP 名、シリアル ID、MAC アドレス、および IP アドレスによる AP グループ化ルールを設定して、指定した AP グループに AP を追加できます。これらのグループ化ルールの優先順位は降順です。グループ化ルールと一致しない AP は、デフォルトの AP グループに追加されます。

II. 制約事項とガイドライン

AP は、1 つの AP グループにのみ追加できます。

AP を含む AP グループは削除できません。グループ化ルールがあるが、AP を含まない AP グループは削除できます。

AP グループ化ルールを設定する場合は、次の制限とガイドラインに従ってください。

- 異なる AP グループに対して同じグループ化ルールを作成することはできません。作成すると、最新の設定が有効になります。
- デフォルトの AP グループのグループ化ルールは作成できません。
- AP グループまたは異なる AP グループの IPv 4 アドレスによる AP グループ化ルールは、互いに重複することはできません。
- AP グループは、IPv4 アドレスによる最大 32 の AP グループ化ルールをサポートします。

III. 設定手順

操作	コマンド	補足
1. system view に移行する	system-view	—
2. AP view または AP group view を入力する	AP viewに移行する。 **wlan ap** *ap-name* AP group viewに移行する。 **wlan ap-group** group-name	—
3. (オプション)AP グループの説明を設定する	**description** *text*	デフォルト：なし

操作	コマンド	補足
4. AP グループ化ルールを作成し、必要に応じて設定する	AP名でAPグループ化ルールを作成する。 **ap** *ap-name-list* シリアルIDでAPグループ化ルールを作成する。 **serial-id** *serial-id* MACアドレスによるAPグループ化ルールを作成する。 **mac-address** *mac-address* IPv 4アドレスによるAPグループ化ルールを作成する。 **if-match ip** *ip-address* { *mask-length* | *mask* }	
5. system view に移行する	quit	ー
6. (オプション) AP 再グループ化ルールを作成する	**wlan re-group** { **ap** *ap-name* | **ap-group** *source-group-name* | **mac-address** *mac-address* | **serial-id** *serial-id* } *group-name*	デフォルト：なし

1.6 APのソフトウェアのアップグレード

1.6.1 ソフトウェアアップグレードの設定

ソフトウェアのアップグレード機能が有効である場合、AC は CAPWAP トンネルの確立中に AP ソフトウェアバージョンを確認します。ソフトウェアのアップグレード機能が無効である場合、AC は AP のソフトウェアバージョンを調査せず、AP を有する CAPWAP トンネルを直接確立します。

1) AP は AC にソフトウェアバージョン、AP モデル情報を通知します。
2) AC は受信した AP のソフトウェアバージョンを確認します。
   - □ バージョンが同一である場合、AC は AP と CAPWAP トンネルを確立します。
   - □ バージョンが異なる場合、AC は AP に AP ソフトウェアバージョンの不一致を通知するメッセージを送信します。
3) 不一致を通知するメッセージを受信すると、AP は AC からソフトウェアバージョンを要求します。
4) AP からリクエストを受信したあと、AC は AP にソフトウェアバージョンを割り当てます。
5) AP はソフトウェアバージョンをアップグレードし、AC との CAPWAP トンネルを再確立します。

I. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—

操作	コマンド	補足
2． AP view/AP group view/global コンフィグレーション view に移行する	AP viewに移行する **wlan ap** *ap-name* AP group viewに移行する **wlan ap-group** *group-name* グローバルコンフィグレーションviewに移行する **wlan global-configuration**	—
3． ソフトウェアアップグレードを設定する	**firmware-upgrade** { **disable** | **enable** }	デフォルト： ● AP viewに設定が無い場合、AP group viewの設定を使用します。 ● AP group viewに設定が存在しない場合、APはグローバルコンフィグレーションviewの設定を使用します。 ● グローバルコンフィグレーション viewでは、ソフトウェアアップグレード機能が有効になっています。

1.6.2 AP モデルのソフトウェアとハードウェアのバージョンマッピングの設定

ソフトウェアアップグレード用の AP モデルのソフトウェアバージョンとハードウェアバージョン間のマッピングを設定するには、次のタスクを実行します。

このタスクは、APDB に格納されている AP モデルの AP ソフトウェアバージョンが、AP モデルに期待するソフトウェアバージョンと一致しない場合にのみ実行します。APDB 内の各 AP モデルの AP ソフトウェアバージョンを表示するには、display wlan ap-model コマンドを使用します。

I. 設定手順

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP モデルのソフトウェアバージョンとハードウェアバージョンのマッピングを設定する	**wlan apdb model-name** *hardware-version software-version*	デフォルト：APDB ユーザスクリプトに格納されているソフトウェアバージョン

1.6.3 AC が AP イメージファイルを取得するための優先ロケーションの指定

AP が CAPWAP トンネルの確立中にソフトウェアバージョンを要求した場合、AC は AP に AP イメージファイルを割り当てます。AC が AP イメージファイルを取得するための AC の RAM またはローカルフォルダとして、優先する場所を指定できます。AC が優先ロケーションから AP イメージファイルを取得できない場合、AC は他のロケーションから AP イメージファイルを取得します。AP イメージファイルが存在しない場合、AC はイメ

ージファイルの取得に失敗し、AP にソフトウェアバージョンを割り当てることができません。

I. 設定の制限とガイドライン

AC は、.ipe AP イメージファイルのみを AP に割り当てることができます。

ローカルフォルダを指定する場合は、AC がデフォルトのファイルシステムとして CF またはフラッシュカードを使用し、AP イメージファイルが AC 上のファイルシステムのルートディレクトリに保存されていることを確認します。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AC が AP イメージファイルを取得するための優先ロケーションを指定する	**wlan image-load filepath** { **local** | **ram** }	デフォルトでは、ACは、APにソフトウェアバージョンを割り当てるときに、RAMに保存されているAPイメージファイルを優先します。

1.6.4 オンライン AP へのイメージファイルの展開

この機能を使用すると、すべてのオンライン AP のイメージをアップグレードできます。アップグレードを有効にするには、アップグレード後に AP を再起動します。

🕮 **メモ：**

この機能のサポートは、AP モデルによって異なります。

設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. すべてのオンライン AP にイメージファイルを展開する。	**wlan ap-image-deploy** { **all** | **ap-group** *group-name* | **name** *ap-name* }	—

1.7 APの給電モードの設定

🕮 **メモ：**

- AP の給電モードの設定は、ソフトウェアバージョン 9.4.09 を含む以降のソフトウェアでサポートします。
- この機能が設定できるのは QX-W1200 シリーズのみです。

1.7.1 AP の給電モードの仕様

10G Ethernet インタフェースの最大リンク速度と USB インタフェースの利用を制限することにより、消費電力を 25W 以下に制限し PoE+(802.3at)給電での動作を可能にします。

- PoE++(802.3bt)もしくは AC アダプタによる給電の場合は、**high** を設定します
- PoE+(802.3at)による給電の場合は、**middle** または **low** を設定します。

表 1-2 に AP の給電モード設定時の動作仕様を示します。

表 1-2 AP の給電モードの動作仕様

動作仕様 / AP の給電モード	装置の消費電力制限	10G Ethernet インタフェース最大リンク速度	USB インタフェース利用制限
high	制限なし	制限なし	制限なし (QX-W1230 は使用不可)
middle	25W	5Gbps	使用不可
low	25W	2.5Gbps	使用不可

1.7.2 設定手順

🕮 **メモ：**

- 10G Ethernet インタフェースの通信速度が "**10000**" または "**5000**" の固定設定の場合、AP の給電モード設定 "**low**" を設定することはできません。
- 10G Ethernet インタフェースの通信速度が "**10000**" の固定設定の場合、AP の給電モード設定 "**middle**" と "**low**" を設定することはできません。
- AP の給電モード設定 "**middle**" または "**low**" が設定されている場合、10G Ethernet インタフェースの通信速度、通信モードを変更することはできません。
- AP の給電モード設定による USB インタフェースの利用制限は "**usb**" コマンドの設定よりも優先されます。
- AP の給電モードを異なるモードに変更する場合、AutoNegotiation をやり直すため 10G Ethernet インタフェースがリンクダウンします。

I. AP view での AP の給電モードの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP view に移行する	**wlan ap** *ap-name*	—
3. AP の給電モードを設定する	**power-level default { high | middle | low }**	デフォルト：AP group viewの設定を使用します。

II. AP group view での AP の給電モードの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP group view に移行する	**wlan ap-group** *group-name*	—
3. AP model view に移行する	**ap-model** *ap-model*	—
4. AP の給電モードを設定する	**power-level default { high | middle | low }**	デフォルト：high

1.8 リモート設定の割り当て設定

AP の設定を行う場合、map-configuration コマンドを使用して設定ファイルを AP に展開します。ただし、展開前に関連コマンドを設定ファイルに書き込んでおく必要があります。なお、この処理は時間がかかるため、展開する AP の数が多いネットワークには適用できません。

1.8.1 オンライン AP との設定の同期

I. このタスクについて

この機能により、AC は VLAN、リンク集約、ポート分離の変更などの AP 設定をオンライン AP に直接同期できます。

II. 制約事項とガイドライン

⚠ **注意**：
この機能は、オンライン AP 上のすべての VLAN、LAG、およびポート設定 (ポートアイソレート設定を除く) をクリアし、AC 上の設定を AP に発行します。慎重に使用してください。これらの設定のいずれかをクリアできない場合は、AC で設定の競合が発生しています。AC の設定を確認する必要があります。

この機能は、リモート設定割り当てとリモート設定同期の両方が設定されている場合にのみ有効です。リモート設定割り当てのみが設定されている場合、AC は指定された AP または AP グループに VLAN 設定のみを割り当てます。

リモート設定割り当てを有効にすると、AP はオンラインになった後、AC に VLAN、リンク集約、およびポート設定を自動的に要求します。

リモート設定同期は、リモート設定割り当てが有効になっている場合にのみ有効になります。

ベストプラクティスとして、AC でリモート設定同期とマップ設定コマンドの両方を使用しないでください。AC で両方を使用する必要がある場合は、展開する設定ファイルの VLAN、LAG、ポートアイソレートの設定が AC の設定と競合しないようにしてください。

III. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP view または AP group view に移行する	AP viewに移行する。 **wlan ap** *ap-name* AP group viewに移行する。 **wlan ap-group** *group-name* **ap-model** *ap-model*	—
3. リモート設定割り当てを有効にする	**remote-configuration enable**	デフォルト：無効
4. リモート設定同期を有効にする	**remote-configuration synchronize**	デフォルト：無効

1.9 CAPWAP トンネルの設定

1.9.1 AP に対する制御トンネルの keepalive 時間の設定

AP は、CAPWAP トンネルが正しく動作しているかどうか確認するために、指定されたエコー間隔で AC にエコー要求を送信します。AC は、エコー応答を送信することで応答します。AC が keepalive 時間以内にエコー要求を受信しない場合、AP の接続が終了します。

制御トンネルの keepalive 時間は、”**echo-interval**”と” **echo-count**”の積です。AC の場合、最小キープアライブ時間は 120 秒です。計算値が 120 より小さい場合、システムはキープアライブ時間を 120 秒に設定します。

🕮 **メモ：**

エコー間隔を 0 秒に設定すると、AP はエコー要求を送信できなくなります。AC と AP 間の通信を正しく行うには、エコー間隔を 0 秒に設定しないでください。

I. AP view での AP に対する keepalive 時間の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP view /AP グループ view に移行する	AP viewに移行する。 **wlan ap** *ap-name* AP group viewに移行する。 **wlan ap-group** *group-name*	—
3． AP がエコー要求を送信する間隔を設定する	**echo-interval** *interval*	デフォルト： ・APはAP group viewの設定を使用します。 ・AP group viewでは、エコー間隔は10秒です。
4． エコー要求の再送試行回数の最大値を設定する	**echo-count** *count*	デフォルト： ・APはAP group viewの設定を使用します。 ・AP group viewでは、エコー要求送信の最大試行回数は3回です。

1.9.2 AP に対するデータトンネルの keepalive 時間の設定

AP は AC との CAPWAP トンネルが確立されると、指定した keepalive 時間で AC にデータトンネルの keepalive パケットを送信します。

I. AP view での AP に対する keepalive 時間の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP view または AP group view に移行する	AP viewに移行する。 **wlan ap** *ap-name* AP group viewに移行する。 **wlan ap-group** *group-name* **ap-model** *ap-model*	—
3． AP がエコー要求を送信する間隔を設定する	**keepalive-interval** *interval*	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、データトンネルキープアライブ間隔は10秒です。

1.9.3 CAPWAP パケットの最大フラグメントサイズの設定

AP がインターネットを経由して AC と接続している場合、中継装置でパケットの廃棄を防ぐことができます。

最大フラグメントサイズの変更はオンライン中の AP でのみ適用されます。

I. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP view または AP group view に移行する	AP viewに移行する。 **wlan ap** *ap-name* AP group viewに移行する。 **wlan ap-group** *group-name* **ap-model** ap-model	—
3. CAPWAP 制御、データパケットの最大フラグメントサイズを設定する	**fragment-size** { **control** *control-size* | **data** *data-size* }	デフォルト： ・APはAP group viewの設定を使用します。 ・AP group viewでは、CAPWAP制御パケットとデータパケットの最大フラグメントサイズは、それぞれ1450バイトと1500バイトです。

1.9.4 CAPWAP トンネルの TCP MSS の設定

I. TCP MSS の概要

CAPWAP トンネルを経由して転送された SYN パケットの MSS（Maximum Segment Size）オプションの値を設定します。

MSS オプションは送信側が受信したもっとも大きいセグメントの受信側を通知します。TCP 接続の確立を行う間、各端末間で MSS を通知します。TCP セグメントのサイズが受信側の MSS 以上である場合、TCP はフラグメントを行わずに TCP セグメントを送信します。TCP セグメントのサイズが受信者の MSS 未満である場合、受信側の MSS にもとづいてセグメントを分割します。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. CAPWAP トンネルの TCP MSS を設定する	**wlan tcp mss** *value*	デフォルト：1460バイト

1.10 regionコードの設定

1.10.1 region コードの指定

I. このタスクについて

region コードは、使用可能な周波数、使用可能なチャネル、送信電力レベルなどの特性を決定します。AP を設定する前に、有効な region コードを設定します。

region コードの変更による規制違反を防ぐには、region コードをロックすることができます。

II. 設定手順

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP view,AP group view またはグローバル設定 view に移行する	AP viewに移行する。 **wlan ap** ap-name AP group viewに移行する。 **wlan ap-group** *group-name* **ap-model** *ap-model* グローバルコンフィグレーションviewに移行する。 **wlan global-configuration**	—
3． region コードを設定する	**region-code** *code*	デフォルト： ・AP viewでは、APはAP group viewの設定を使用します。APグループview regionコードが存在しない場合、APはグローバル設定viewの設定を使用します。 ・AP group viewでは、APはグローバル設定viewの設定を使用します。 ・グローバル設定viewでは、regionコードはJPとして指定されます。
4． (オプション)region コードをロックする。	**region-code-lock enable**	デフォルト： ・AP viewでは、APはAPグループviewで設定を使用します。AP group viewに領域コードが存在しない場合、APはグローバル設定viewで設定を使用します。 ・AP group viewでは、APはグローバル設定viewの設定を使用します。 ・グローバル設定viewでは、regionコードはロックされていません。

1.11 AC要求の再送信の設定

AC は、AP 要求の再送信の試行が最大数に達するまで、あるいは応答が受信されるまで、AP に送信された要求を再送信間隔で送信します。

I. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP view,または、AP group view に移行する	AP viewに移行する。 wlan ap ap-name AP group viewに移行する。 wlan ap-group *group-name*	—
3. 要求再伝送の最大試行回数を設定する	**retransmit-count** *value*	デフォルト： APはAP group viewの設定を使用します。 AP group viewでは、要求再送信の最大試行回数は3回です。
4. AC 要求が再伝送される間隔を設定する	**retransmit-interval** *interval*	デフォルト： APはAP group viewの設定を使用します。 AP group viewでは、再送信間隔は5秒です。

1.12 APのメンテナンス

1.12.1 AP のリセット

すべての AP または指定した AP をリセットするには、user view で次のコマンドを実行します。

操作	コマンド
すべてのAPもしくは指定されたAPをリセットする	**reset wlan ap** { **all** | **ap-group** *group-name* | **model** *model-name* | **name** *ap-name* | **native** }

1.12.2 手動 AP の名前変更

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. 手動 AP の名前を変更する	**wlan rename-ap** *ap-name new-ap-name*	—

1.12.3 AP のファイルシステムの管理

AP が AC と CAPWAP トンネルを確立した後、AC で次のタスクを実行して AP のファイルを管理できます。

- AP のファイル情報を表示します。
- AP からファイルを削除します。
- AC から AP にイメージファイルをダウンロードします。

I. 制約事項とガイドライン

この機能は、マスタ AC でのみ有効です。

II. 設定手順

操作	コマンド	補足
1. AP 上のファイルまたはファイルフォルダに関する情報を表示する	**display wlan ap name** *ap-name* **files**	—
2. system view に移行する	**system-view**	—
3. AP view に移行する	**wlan ap** *ap-name*	—
4. AP 上のファイルを管理する	**delete file** *filename* **download file** *file-name*	—

1.12.4 統計情報レポート間隔の設定

AP が統計情報を報告する間隔を変更するには、次のタスクを実行します。統計情報を使用して、AP 上の無線の動作状態を監視できます。

I. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP view/AP group view/global 設定 view に移行する	AP viewに移行する **wlan ap** *ap-name* AP group viewに移行する **wlan ap-group** *group-name* グルーバルコンフィグレーションviewに移行する wlan global-configuration	—
3. 統計情報レポート間隔を設定する	**statistics-interval** *interval*	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に設定が存在しない場合、APはグローバル設定viewで設定を使用します。 ・AP group viewでは、APはグローバル設定viewで設定を使用します。 ・グローバル設定viewでは、統計情報レポート間隔は50秒です。

1.12.5 LED 照明モードの設定

AP の LED を次のモードで点滅するように設定できます。

- quiet:すべての LED がオフになります。
- awake:すべての LED が 1 分に 1 回点滅します。このモードのサポートは AP モデルによって異なります。
- always-on:すべての LED が点灯します。このモードのサポートは AP モデルによって異なります。
- normal:このモードでの LED の点滅方法は AP モデルによって異なります。このモードでは、AP の実行ステータスを識別できます。

I. 制約事項とガイドライン

AP group view で LED 照明モードを awake または always-on に設定した場合、設定は指定した LED 照明モードをサポートするメンバ AP でのみ有効になります。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP view/AP group view に移行する	AP viewに移行する。 **wlan ap** *ap-name* AP group viewに移行する。 **wlan ap-group** *group-name*	ー
3. LED の点灯モードを設定する	**led-mode** { **always-on** | **awake** | **normal** | **quiet** }	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、LED照明モードは**normal**です。

1.12.6 AP への設定ファイルの展開

設定ファイルを更新する場合、または設定ファイルを必要とする機能を設定する場合は、設定ファイルを AP に展開します。たとえば、ローカル転送モードで AP のユーザプロファイルを設定するには、関連コマンドを設定ファイルに記述してから、設定ファイルを AP に展開する必要があります。設定ファイルは、AC への CAPWAP トンネルが Run 状態のときに有効になります。AP の再起動後は存続しません。

I. 制約事項とガイドライン

設定ファイルが AC の記憶媒体に保存されていることを確認します。設定ファイルの内容は、完全なコマンドである必要があります。設定ファイルは、FTP または Web インタフェースから AC にアップロードできます。ベストプラクティスとして、Web インタフェースから設定ファイルをアップロードします。

オンライン AP の設定ファイルを編集し、設定ファイルをすぐに有効にするには、次のいずれかのタスクを実行します。

- undo map-configuration コマンドを実行し、次に map-configuration filename コマンドを実行して設定ファイルを AP に展開します。
- AP が再びオンラインになるように、AP から AC を切断します。

II. 設定手順

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP view/AP group view に移行する	AP viewに移行する。 **wlan ap** *ap-name* AP group viewに移行する。 **wlan ap-group group-name** ap-model ap-model	ー
3． 設定ファイルを AP に展開する	**map-configuration** *filename*	デフォルト： 設定ファイルはAPに展開されません。

1.13 AP管理の高度な機能の設定

1.13.1 リモート AP の設定

AP と AC 間のトンネルが接続されていないとき、AP はクライアントに対してサービスの提供を停止します。本機能により AP は、AP と AC 間のトンネルが接続されていないとき、AP でクライアントアクセスサービスを有効にします。

リモート AP は、ローカル転送モード内で作動する AP でのみ有効です。

AC と AP 間のトンネルが復元されると、AC を有するクライアントは認証者として再認証を必要とします。

リモート AP はテレコミュニケーション、スモールブランチ、SOHO ソリューションに適用可能です。

I. 設定手順

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP view/AP group view に移行する	**wlan ap** *ap-name* **wlan ap-group** *group-name*	—
3． リモート AP を設定する	**hybrid-remote-ap** { **disable** | **enable** }	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、リモートAPは無効です。

1.14 ACのメンテナンス

1.14.1 タイムゾーン同期の有効化

この機能を使用すると、AP はアソシエーションとアソシエーション以降の特定の間隔で AC からの時刻とタイムゾーンの情報を同期できます。

I. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. タイムゾーンの同期を有効にする	**wlan timezone-sync enable**	デフォルト：有効

1.14.2 APDB ユーザスクリプトのロード

このタスクでは、AC ソフトウェアをアップグレードせずに、新しい AP モデルを APDB に追加できます。

I. 制約事項とガイドライン

ユーザスクリプトが有効であることを確認します。無効なスクリプトはロード失敗の原因となります。

ユーザスクリプト内の AP モデルは、システムスクリプト内の AP モデルとは異なる必要があります。

AC で複数のユーザスクリプトをロードすると、最後にロードされたユーザスクリプトによって古いユーザスクリプトが上書きされます。

次の条件が存在する場合にユーザスクリプトをリロードするには、関連する AP モデルを削除するか、**wlan apdb** コマンドを使用して元のソフトウェアバージョンを復元する必要があります。

- 古いユーザスクリプトにモデルがリストされている手動 AP またはオンライン自動 AP が存在する。
- 古いユーザスクリプトにリストされている AP モデルの AP が AP グループに追加されている。
- 古いユーザスクリプトには、ソフトウェアバージョンがすでに設定されている AP モデルが含まれている。

AC リブート後に AP モデル設定が失われないようにするには、名前を変更するときにユーザスクリプトをリロードするか、ファイルシステムのユーザスクリプトを削除する必要があります。

ユーザスクリプトを置き換える場合、新しいユーザスクリプトに古いスクリプトの AP モデル設定が含まれていないと、古いユーザスクリプトの AP モデル設定は AC リブート時に失われます。この場合、新しいユーザスクリプトをリロードする必要があります。

II. 設定手順

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． APDB ユーザスクリプトをロードする	**wlan apdb file** *user.apdb*	デフォルト：ユーザスクリプトはACにロードしない

1.15 SNMP通知の設定

1.15.1 SNMP 通知の有効化

重大な WLAN イベントを NMS に報告するには、SNMP 通知を有効にします。WLAN イベント通知を正しく送信するには SNMP も設定する必要があります。

I. 設定手順

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． SNMP 通知を有効にする	AP管理のためのSNMP通知を有効にする。 **snmp-agent trap enable wlan ap** CAPWAPのSNMP通知を有効にします。 **snmp-agent trap enable wlan capwap**	デフォルト：無効

1.15.2 SNMP トラップをトリガーするためのオンライン AP 数の閾値の設定

SNMP 通知とこのコマンドが設定されている場合、ライセンスで許可されている AP の数に対するオンライン AP の数が、指定された閾値を超えると、AC は SNMP モジュールに過負荷トラップを送信します。閾値を超えると、AP がオンラインになるたびに、AC は SNMP 回復トラップを送信します。オンライン AP の数が閾値を下回ると、AC は SNMP モジュールに回復トラップを送信します。

I. 制限事項とガイドライン

閾値を 100 に設定すると、オンライン AP の数がライセンスで許可されている AP の数を超えないため、AC は過負荷トラップを送信しません。

II. 設定手順

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． SNMP トラップをトリガーするためのオンライン AP 量の閾値を設定する	**wlan trap ap-number threshold** *percent*	デフォルト：100

1.16 AP管理の表示と維持

1.16.1 AP 接続レコードの表示とクリア

操作	コマンド
ACに接続されているすべてのAPもしくは指定したAPの情報を表示する	**display wlan ap** { **all** | **name** *ap-name* } **connection-record**
ACに接続されているすべてのAPもしくは指定したAPの情報をクリアする ※user viewで実行します。	**reset wlan ap** { **all** | **name** *ap-name* } **connection-record**

1.16.2 AP 管理情報の表示とクリア

操作	コマンド
すべてのAPもしくは指定したAPに関する情報を表示する	**display wlan ap** { **all** | **name** *ap-name* } [**verbose**]
すべてのAPもしくは指定したAPのアドレス情報を表示する	**display wlan ap** { **all** | **name** *ap-name* } **address**
すべてのAPまたは指定されたAPのAPグループ情報を表示する	**display wlan ap** { **all** | **name** *ap-name* } **group**
APオンライン期間を表示する	**display wlan ap** { **all** | **name** *ap-name* } **online-time**
すべてのAPまたは指定されたAPの実行中の設定を表示する	**display wlan ap** { **all** | **name** *ap-name* } **running-configuration** [**verbose**]
指定したAPの再起動ログを表示する	**display wlan ap reboot-log name** *ap-name*
APのregionコード情報を表示する	**display wlan ap** { **all** | **name** *ap-name* } **region-code**
APの関連付けに失敗した記録を表示する	**display wlan ap association-failure-record**
APの関連付けに失敗した記録を削除する。	**reset wlan ap statistics association-failure-record**
APイメージのダウンロードに関する情報を表示する	**display wlan ap statistics image-download [failed | in-progress | succeeded]**
APイメージのダウンロードに関する情報を削除する	**reset wlan ap statistics image-download** { **all** | **failed** | **in-progress** | **succeeded** }
オンラインAP数量レコードを表示する	**display wlan ap statistics online-record** [**datetime** *date time* [**count** count]]
オンラインAP数量レコードを削除する	**reset wlan ap statistics online-record**
APの合計オンライン期間を表示する	**display wlan ap** { **all** | **name** *ap-name* } **total-online-duration**

操作	コマンド
すべてのAP groupもしくは指定したAP groupに関する情報を表示する	**display wlan ap-group** [**brief** | **name** *group-name*]
APモデル情報を表示する	**display wlan ap-model** { **all** | **name** *model-name* }

1.16.3 すべての AP または指定された AP のリブートログのクリア

操作	コマンド
すべてのAPまたは指定されたAPのリブートログをクリアする ※user viewで実行します。	**reset wlan ap reboot-log** { **all** | **name** *ap-name* }

1.16.4 CAPWAP トンネル情報の表示とクリア

操作	コマンド
CAPWAP機能の設定ステータスを表示する	**display wlan ap all feature capwap**
CAPWAPトンネル接続断の統計情報を削除する	**reset wlan ap statistics tunnel-down-record**

1.16.5 クラウドラスタの統計情報の表示とクリア

操作	コマンド
マスタ、スタンバイが切り替わる際のフラグビットの状態を表示する	**display wlan ap all feature capwap**
マスタとスタンバイのリンクの切り替えの統計情報を削除する	**reset wlan ap statistics tunnel-down-record**

1.17 AP管理の設定例

1.17.1 DHCP を通した CAPWAP トンネル確立の設定例

I. ネットワーク要件

図 1-3 に示すように、AP が DHCP Option 43 を通して DHCP サーバから自身の IP アドレスと AC の IP アドレスを取得できるように設定します。AP は、AC との CAPWAP トンネルを確立するために、AC の IP アドレスを使用します。

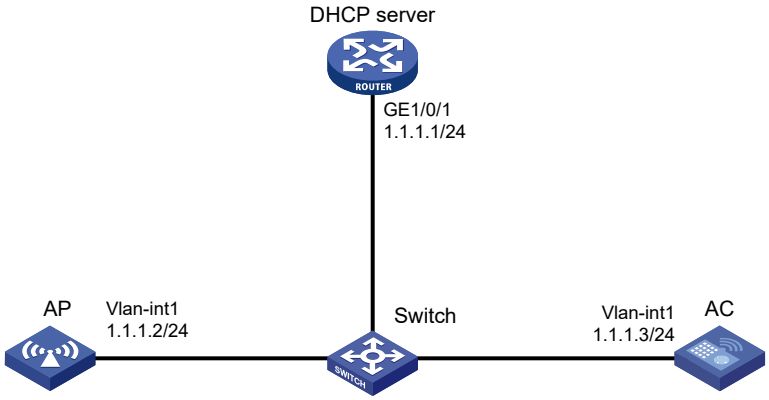


図 1-3 ネットワーク図

II. 設定手順

1)　DHCP サーバを設定します。

DHCP を有効にします。

```
<DHCP server> system-view
[DHCP server] dhcp enable
```

DHCP address pool 1 を設定します。

```
[DHCP server] dhcp server ip-pool 1
[DHCP server-dhcp-pool-1] network 1.1.1.0 mask 255.255.255.0
```

address pool 0 に AC の IP アドレスを指定するために Option 43 を設定します。右端のバイト 01010103（1.1.1.3）は AC の IP アドレスを示します。

```
[DHCP server-dhcp-pool-1] option 43 hex 800700000101010103
[DHCP Server-dhcp-pool-1] quit
[DHCP Server] quit
```

2)　AC を設定します。

AC 上の VLAN-interface 1 の IP アドレスに 1.1.1.3/24 を設定します。

```
<AC> system-view
[AC] interface vlan-interface 1
[AC-Vlan-interface1] ip address 1.1.1.3 24
[AC-Vlan-interface1] quit
```

QX-W1020 を有する AP 名が ap1 の AP を作成し、シリアル ID を 210235A1BSC123000050 に設定します。

```
[AC] wlan ap ap1 model QX-W1020
[AC-wlan-ap-ap1] serial-id 210235A1BSC123000050
[AC-wlan-ap-ap1] quit
```

#AP を始動させます。AP は以下の操作を実行します。

- DHCP サーバから自身の IP アドレス 1.1.1.2 を取得します。
- Option 43 を通して AC の IP アドレスを取得します。
- AC との CAPWAP トンネルを確立します。

III. 設定の確認

以下の情報を検証します。

- AP は、DHCP を通して AC の IP アドレスを取得します。
- AP と AC が、確立された CAPWAP トンネルを有します。
- AP は稼働状態です。

[AC] display wlan ap name ap1 verbose

```
AP name                          : ap1
AP ID                            : 1
AP group name                    : default-group
State                            : Run
Backup type                      : Master
Ready-for-Switchover             : Not ready
Online time                      : 0 days 1 hours 25 minutes 12 seconds
System up time                   : 0 days 2 hours 22 minutes 12 seconds
Model                            : QX-W1020
Region code                      : JP
Region code lock                 : Disable
Serial ID                        : 219801A0CNC138011454
MAC address                      : 0AFB-423B-893C
IP address                       : 1.1.1.2
UDP control port number          : 18313
UDP data port number             : N/A
H/W version                      : Ver.C
S/W version                      : E2321
Boot version                     : 1.01
USB state                        : N/A
Power Level                      : N/A
PowerInfo                        : N/A
Description                      : wtp1
Priority                         : 4
Echo interval                    : 10 seconds
Statistics report interval       : 50 seconds
Fragment size (data)             : 1500
Fragment size (control)          : 1450
MAC type                         : Local MAC & Split MAC
Tunnel mode                      : Local Bridging & 802.3 Frame & Native Frame
CWPCAP data-tunnel status        : Up
Discovery type                   : DHCP
Retransmission count             : 3
Retransmission interval          : 5 seconds
Firmware upgrade                 : Enabled
Sent control packets             : 1
Received control packets         : 1
Echo requests                    : 147
Lost echo responses              : 0
Average echo delay               : 3
Last reboot reason               : User soft reboot
Latest IP address                : 10.1.0.2
Current AC IP                    : N/A
Tunnel down reason               : Request wait timer expired
Connection count                 : 1
Backup Ipv4                      : Not configured
Backup Ipv6                      : Not configured
Tunnel encryption                : Disabled
Data-tunnel encryption           : Disabled
Data-tunnel encryption state     : Not encrypted
LED mode                         : Normal
Remote configuration             : Enabled Radio 1:
Radio 1:
```

```
    Basic BSSID               : 7848-59f6-3940
    Admin state               : Up
    Radio type                : 802.11ac
    Antenna type              : internal
    Client dot11ac-only       : Disabled
    Client dot11n-only        : Disabled
    Channel band-width        : 20/40/80MHz
    Active band-width         : 20/40/80MHz
    Secondary channel offset  : SCB
    Short GI for 20MHz        : Supported
    Short GI for 40MHz        : Supported
    Short GI for 80MHz        : Supported
    Short GI for 160MHz       : Not supported
    mimo                      : Not Config
    Green-Energy-Management   : Disabled
    A-MSDU                    : Enabled
    A-MPDU                    : Enabled
    LDPC                      : Not Supported
    STBC                      : Supported
    Operational VHT-MCS Set:
        Mandatory             : Not configured
        Supported             : NSS1 0,1,2,3,4,5,6,7,8,9
                                NSS2 0,1,2,3,4,5,6,7,8,9
        Multicast             : Not configured
    Operational HT MCS Set:
        Mandatory             : Not configured
        Supported             : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9,
                                10, 11, 12, 13, 14, 15
        Multicast             : Not configured
    Channel                   : 44(auto)
    Channel usage(%)          : 15
    Max power                 : 20 dBm
    Operational rate:
        Mandatory             : 6, 12, 24 Mbps
        Multicast             : Auto
        Supported             : 9, 18, 36, 48, 54 Mbps
        Disabled              : Not configured
    Distance                  : 1 km
    ANI                       : Enabled
    Fragmentation threshold   : 2346 bytes
    Beacon interval           : 100 TU
    Protection threshold      : 2346 bytes
    Long retry threshold      : 4
    Short retry threshold     : 7
    Maximum rx duration       : 2000 ms
    Noise Floor               : -102 dBm
    Smart antenna             : Enabled
    Smart antenna policy      : Auto
    Protection mode           : rts-cts
    Continuous mode           : N/A
    HT protection mode        : No protection
Radio 2:
    Basic BSSID               : 7848-59f6-3950
    Admin state               : Down
    Radio type                : 802.11b
    Antenna type              : internal
    Client dot11n-only        : Disabled
    Channel band-width        : 20/40MHz
    Secondary channel offset  : SCN
    Short GI for 20MHz        : Supported
    Short GI for 40MHz        : Supported
    A-MSDU                    : Enabled
    A-MPDU                    : Enabled
    LDPC                      : Not Supported
    STBC                      : Supported
    Operational HT MCS Set:
        Mandatory             : Not configured
        Supported             : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9,
                                10, 11, 12, 13, 14, 15, 16, 17,
                                18, 19, 20, 21, 22, 23, 24, 25,
```

```
                                  26, 27, 28, 29, 30, 31
    Multicast                   : Not configured
Channel                         : 5(auto)
Channel usage(%)                : 0
Max power                       : 20 dBm
Preamble type                   : Short
Operational rate:
    Mandatory                   : 1, 2, 5.5, 11 Mbps
    Multicast                   : Auto
    Supported                   : 6, 9, 12, 18, 24, 36, 48, 54 Mbps
    Disabled                    : Not configured
Distance                        : 1 km
ANI                             : Enabled
Fragmentation threshold         : 2346 bytes
Beacon interval                 : 100 TU
Protection threshold            : 2346 bytes
Long retry threshold            : 4
Short retry threshold           : 7
Maximum rx duration             : 2000 ms
Noise Floor                     : 0 dBm
Smart antenna                   : Enabled
Smart antenna policy            : Auto
Protection mode                 : rts-cts
Continuous mode                 : N/A
HT protection mode              : No protection
```

1.17.2 DNS を通した CAPWAP トンネル確立の設定例

I. ネットワーク要件

図 1-4 に示すように、AP が DNS を通して AC の IP アドレスを取得できるように設定します。

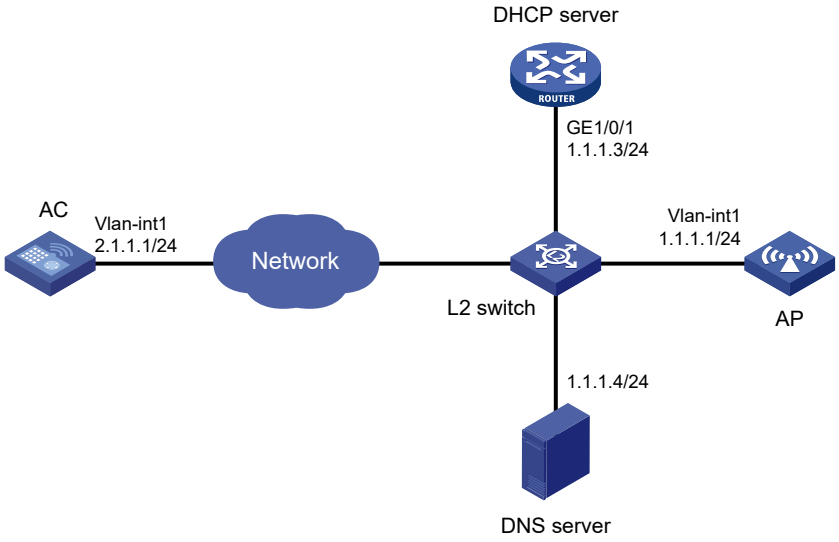


図 1-4 ネットワーク図

II. 設定手順

1)　DHCP サーバを設定します。

```
<DHCP server> system-view
[DHCP server] dhcp enable
[DHCP server] dhcp server ip-pool 1
[DHCP server-dhcp-pool-1] network 1.1.1.0 mask 255.255.255.0
[DHCP server-dhcp-pool-1] domain-name abc
[DHCP server-dhcp-pool-1] dns-list 1.1.1.4
[DHCP server-dhcp-pool-1] gateway-list 1.1.1.2
[DHCP server-dhcp-pool-1] quit
[DHCP server] quit
```

2) ドメイン名（host.abc）と IP アドレス 2.1.1.1/24 の間のマッピングを設定します。詳細は、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*5 ネットワーク接続*”の”*11 章 IP アドレス*”を参照してください。（詳細は省略します。）
3) AC を設定します。

VLAN-interface の IP アドレスを 2.1.1.1/24 に設定します。

```
<AC> system-view
[AC] interface vlan-interface 1
[AC-Vlan-interface1] ip address 2.1.1.1 24
[AC-Vlan-interface1] quit
```

ap 1 と名づけた AP を作成し、モデルとシリアル ID を指定します。

```
[AC] wlan ap ap1 model QX-W1020
[AC-wlan-ap-ap1] serial-id 210235A1BSC123000050
```

AP を起動させます。

```
[AC-wlan-ap-ap1] quit
```

AP は以下の操作を実行します。

- DHCP サーバから、自身の IP アドレス 1.1.1.1、AC のドメイン名サフィックス、DNS サーバの IP アドレスを取得します。
- ドメイン名サフィックスをホスト名に追加します。
- ドメイン名を IP アドレスに変換するように DNS クライアントに知らせます。
- AC との CAPWAP トンネルを確立するために、AC の IP アドレスを使用します。

III. 設定の確認

#以下の操作を検証します。

- AP と AC が、確立された CAPWAP トンネルを有します。
- AP の状態が、稼働(Run)となっている。
- AP は、DNS を通して AC の IP アドレスを取得します。

```
[AC] display wlan ap name ap1 verbose
AP name                         : ap1
AP ID                           : 1
AP group name                   : default-group
State                           : Run
```

```
Backup Type                     : Master
Online time                     : 0 days 1 hours 25 minutes 12 seconds
System up time                  : 0 days 2 hours 22 minutes 12 seconds
Model                           : QX-W1020
Region code                     : JP
Region code lock                : Disable
Serial ID                       : 210235A1BSC123000050
MAC address                     : 0AFB-423B-893C
IP address                      : 1.1.1.1
UDP port number                 : 18313
H/W version                     : Ver.C
S/W version                     : E2321
Boot version                    : 1.01
USB state                       : N/A
Power level                     : N/A
Power info                      : N/A
Description                     : wtp1
Priority                        : 4
Echo interval                   : 10 seconds
Echo count                      : 3 counts
Keepalive interval              : 10 seconds
Discovery-response wait-time    : 2 seconds
Statistics report interval      : 50 seconds
Jumbo frame value               : Disabled
Fragment size (data)            : 1500
Fragment size (control)         : 1450
MAC type                        : Local MAC & Split MAC
Tunnel mode                     : Local Bridging & 802.3 Frame & Native Frame
CWPCAP data-tunnel status       : Up
Discovery type                  : DNS
Retransmission count            : 3
Retransmission interval         : 5 seconds
Firmware upgrade                : Enabled
Sent control packets            : 1
Received control packets        : 1
Echo requests                   : 147
Lost echo responses             : 0
Average echo delay              : 3
Last reboot reason              : User soft reboot
Latest IP address               : 10.1.0.2
Current AC IP                   : N/A
Tunnel down reason              : Request wait timer expired
Connection count                : 1
Backup Ipv4                     : Not configured
Backup Ipv6                     : Not configured
Tunnel encryption               : Disabled
Data-tunnel encryption          : Disabled
Data-tunnel encryption state    : Not encrypted
LED mode                        : Normal
Radio 1:
    Basic BSSID                 : 7848-59f6-3940
    Admin state                 : Up
    Radio type                  : 802.11ac
    Antenna type                : internal
    Client dot11ac-only         : Disabled
    Client dot11n-only          : Disabled
    Channel band-width          : 20/40/80MHz
    Operating bandwidth         : 20/40/80MHz
    Secondary channel offset    : SCB
    Short GI for 20MHz          : Supported
    Short GI for 40MHz          : Supported
    Short GI for 80MHz          : Supported
    Short GI for 160MHz         : Not supported
    mimo                        : Not Config
    Green-Energy-Management     : Disabled
    A-MSDU                      : Enabled
    A-MPDU                      : Enabled
    LDPC                        : Not Supported
    STBC                        : Supported
    Operational VHT-MCS Set:
```

```
        Mandatory             : Not configured
        Supported             : NSS1 0,1,2,3,4,5,6,7,8,9
                                NSS2 0,1,2,3,4,5,6,7,8,9
        Multicast             : Not configured
    Operational HT MCS Set:
        Mandatory             : Not configured
        Supported             : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9,
                                10, 11, 12, 13, 14, 15
        Multicast             : Not configured
    Channel                   : 44(auto)
    Max power                 : 20 dBm
    Operational rate:
        Mandatory             : 6, 12, 24 Mbps
        Multicast             : Auto
        Supported             : 9, 18, 36, 48, 54 Mbps
        Disabled              : Not configured
    Distance                  : 1 km
    ANI                       : Enabled
    Fragmentation threshold   : 2346 bytes
    Beacon interval           : 100 TU
    Protection threshold      : 2346 bytes
    Long retry threshold      : 4
    Short retry threshold     : 7
    Maximum rx duration       : 2000 ms
    Noise Floor               : -102 dBm
    Smart antenna             : Enabled
    Smart antenna policy      : Auto
    Protection mode           : rts-cts
    Continuous mode           : N/A
    HT protection mode        : No protection
Radio 2:
    Basic BSSID               : 7848-59f6-3950
    Admin state               : Down
    Radio type                : 802.11n(2.4GHz)
    Antenna type              : internal
    Client dot11n-only        : Disabled
    Channel band-width        : 20/40MHz
    Secondary channel offset  : SCN
    Short GI for 20MHz        : Supported
    Short GI for 40MHz        : Supported
    A-MSDU                    : Enabled
    A-MPDU                    : Enabled
    LDPC                      : Not Supported
    STBC                      : Supported
    Operational HT MCS Set:
        Mandatory             : Not configured
        Supported             : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9,
                                10, 11, 12, 13, 14, 15 16, 17,
                                18, 19, 20, 21, 22, 23, 24, 25,
                                26, 27, 28, 29, 30, 31
        Multicast             : Not configured
    Channel                   : 5(auto)
    Channel usage(%)          : 0
    Max power                 : 20 dBm
    Preamble type             : Short
    Operational rate:
        Mandatory             : 1, 2, 5.5, 11 Mbps
        Multicast             : Auto
        Supported             : 6, 9, 12, 18, 24, 36, 48, 54 Mbps
        Disabled              : Not configured
    Distance                  : 1 km
    ANI                       : Enabled
    Fragmentation threshold   : 2346 bytes
    Beacon interval           : 100 TU
    Protection threshold      : 2346 bytes
    Long retry threshold      : 4
    Short retry threshold     : 7
    Maximum rx duration       : 2000 ms
    Noise Floor               : 0 dBm
    Smart antenna             : Enabled
```

```
                Smart antenna policy      : Auto
    Protection mode             : rts-cts
    Continuous mode             : N/A
    HT protection mode          : No protection
```

1.17.3 自動 AP の設定例

I. ネットワーク要件

図 1-5 に示すように、AC 上で自動 AP 機能を有効にします。AP は、DHCP Option 43 を通して AC の IP アドレスを取得し、AC との CAPWAP トンネルを確立します。

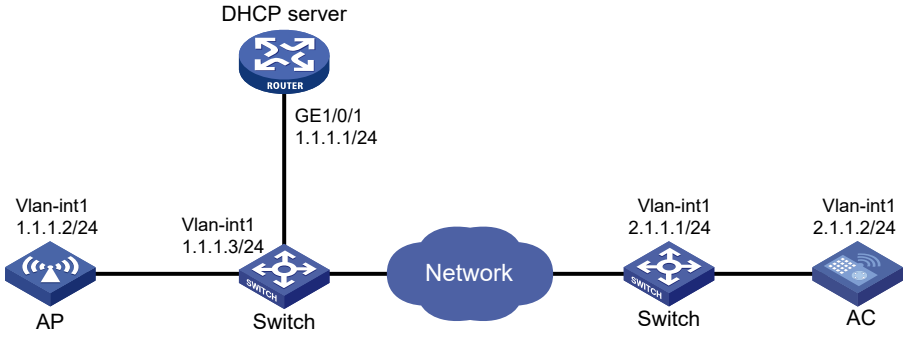


図 1-5 ネットワーク図

II. 設定手順

1)　DHCP サーバを設定します。

DHCP サーバを有効にします。

```
<DHCP server> system-view
[DHCP server] dhcp enable
```

DHCP address pool 1 を設定します。

```
[DHCP server] dhcp server ip-pool 1
[DHCP server-dhcp-pool-1] network 1.1.1.0 mask 255.255.255.0
```

address pool 0 内で AC の IP アドレスを指定するために Option 43 を設定します。右端のバイト 02010102 （2.1.1.2）は AC の IP アドレスを示します。

```
[DHCP server-dhcp-pool-1] option 43 hex 800700000102010102
[DHCP server-dhcp-pool-1] gateway-list 1.1.1.3
[DHCP server-dhcp-pool-1] quit
[DHCP server] quit
```

2)　AC を設定します。

AC 上で VLAN-interface 1 の IP アドレスを 2.1.1.2/24 に設定します。

```
<AC> system-view
[AC] interface vlan-interface 1
[AC-Vlan-interface1] ip address 2.1.1.2 24
[AC-Vlan-interface1] quit
```

#ネクストホップアドレスを 2.1.1.1 としたデフォルトルートを設定します。

```
[AC] ip route-static 0.0.0.0 0 2.1.1.1
```

自動 AP を有効にします。

```
[AC] wlan auto-ap enable
```

III. 設定の確認

#AP が AC との CAPWAP トンネルを確立したか検証します。

```
[AC] display wlan ap name 0011-2200-0101 verbose
AP name                         : 0011-2200-0101
AP ID                           : 1
AP group name                   : default-group
State                           : Run
Backup type                     : Master
Ready-for-Switchover            : Not ready
Online time                     : 0 days 1 hours 25 minutes 12 seconds
System up time                  : 0 days 2 hours 22 minutes 12 seconds
Model                           : QX-W1020
Region code                     : JP
Region code lock                : Disable
Serial ID                       : 219801A0CNC138011454
MAC address                     : 0011-2200-0101
IP address                      : 1.1.1.2
UDP control port number         : 18313
UDP data port number            : N/A
H/W version                     : Ver.C
S/W version                     : E2321
Boot version                    : 1.01
USB state                       : N/A
Power Level                     : N/A
PowerInfo                       : N/A
Description                     : wtp1
Priority                        : 4
Echo interval                   : 10 seconds
Echo count                      : 3 counts
Keepalive interval              : 10 seconds
Discovery-response wait-time    : 2 seconds
Statistics report interval      : 50 seconds
Fragment size (data)            : 1500
Fragment size (control)         : 1450
MAC type                        : Local MAC & Split MAC
Tunnel mode                     : Local Bridging & 802.3 Frame & Native Frame
CWPCAP data-tunnel status       : Up
Discovery type                  : DHCP
Retransmission count            : 3
Retransmission interval         : 5 seconds
Firmware upgrade                : Enabled
Sent control packets            : 1
Received control packets        : 1
Echo requests                   : 147
Lost echo responses             : 0
Average echo delay              : 3
Last reboot reason              : User soft reboot
```

```
Latest IP address              : 10.1.0.2
Current AC IP                  : N/A
Tunnel down reason             : Request wait timer expired
Connection count               : 1
Backup Ipv4                    : Not configured
Backup Ipv6                    : Not configured
Tunnel encryption              : Disabled
Data-tunnel encryption         : Disabled
Data-tunnel encryption state   : Not encrypted
LED mode                       : Normal
Remote configuration           : Enabled
Radio 1:
    Basic BSSID                : 7848-59f6-3940
    Admin state                : Up
    Radio type                 : 802.11ac
    Antenna type               : internal
    Client dot11ac-only        : Disabled
    Client dot11n-only         : Disabled
    Channel band-width         : 20/40/80MHz
    Active band-width          : 20/40/80MHz
    Secondary channel offset   : SCB
    Short GI for 20MHz         : Supported
    Short GI for 40MHz         : Supported
    Short GI for 80MHz         : Supported
    Short GI for 160MHz        : Not supported
    mimo                       : Not Config
    Green-Energy-Management    : Disabled
    A-MSDU                     : Enabled
    A-MPDU                     : Enabled
    LDPC                       : Not Supported
    STBC                       : Supported
    Operational VHT-MCS Set:
        Mandatory              : Not configured
        Supported              : NSS1 0,1,2,3,4,5,6,7,8,9
                                 NSS2 0,1,2,3,4,5,6,7,8,9
        Multicast              : Not configured
    Operational HT MCS Set:
        Mandatory              : Not configured
        Supported              : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9,
                                 10, 11, 12, 13, 14, 15
        Multicast              : Not configured
    Channel                    : 44(auto)
    Channel usage(%)           : 15
    Max power                  : 20 dBm
    Operational rate:
        Mandatory              : 6, 12, 24 Mbps
        Multicast              : Auto
        Supported              : 9, 18, 36, 48, 54 Mbps
        Disabled               : Not configured
    Distance                   : 1 km
    ANI                        : Enabled
    Fragmentation threshold    : 2346 bytes
    Beacon interval            : 100 TU
    Protection threshold       : 2346 bytes
    Long retry threshold       : 4
    Short retry threshold      : 7
    Maximum rx duration        : 2000 ms
    Noise Floor                : -102 dBm
    Smart antenna              : Enabled
    Smart antenna policy       : Auto
    Protection mode            : rts-cts
    Continuous mode            : N/A
    HT protection mode         : No protection
Radio 2:
    Basic BSSID                : 7848-59f6-3950
    Admin state                : Down
    Radio type                 : 802.11b
    Antenna type               : internal
    Client dot11n-only         : Disabled
    Channel band-width         : 20MHz
```

```
    Active band-width          : 20MHz
    Secondary channel offset   : SCN
    Short GI for 20MHz         : Supported
    Short GI for 40MHz         : Supported
    A-MSDU                     : Enabled
    A-MPDU                     : Enabled
    LDPC                       : Not Supported
    STBC                       : Supported
    Operational HT MCS Set:
        Mandatory              : Not configured
        Supported              : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9,
                                 10, 11, 12, 13, 14, 15
        Multicast              : Not configured
    Channel                    : 5(auto)
    Channel usage(%)           : 0
    Max power                  : 20 dBm
    Preamble type              : Short
    Operational rate:
        Mandatory              : 1, 2, 5.5, 11 Mbps
        Multicast              : Auto
        Supported              : 6, 9, 12, 18, 24, 36, 48, 54 Mbps
        Disabled               : Not configured
    Distance                   : 1 km
    ANI                        : Enabled
    Fragmentation threshold    : 2346 bytes
    Beacon interval            : 100 TU
    Protection threshold       : 2346 bytes
    Long retry threshold       : 4
    Short retry threshold      : 7
    Maximum rx duration        : 2000 ms
    Noise Floor                : 0 dBm
    Smart antenna              : Enabled
    Smart antenna policy       : Auto
    Protection mode            : rts-cts
    Continuous mode            : N/A
    HT protection mode         : No protection
```

1.17.4 AP group の設定例

I. ネットワーク要件

図 1-6 に示すように、AP group を設定し、AP 1 を AP group group 1 に、AP 2、AP 3、AP 4 を AP group group 2 に追加します。

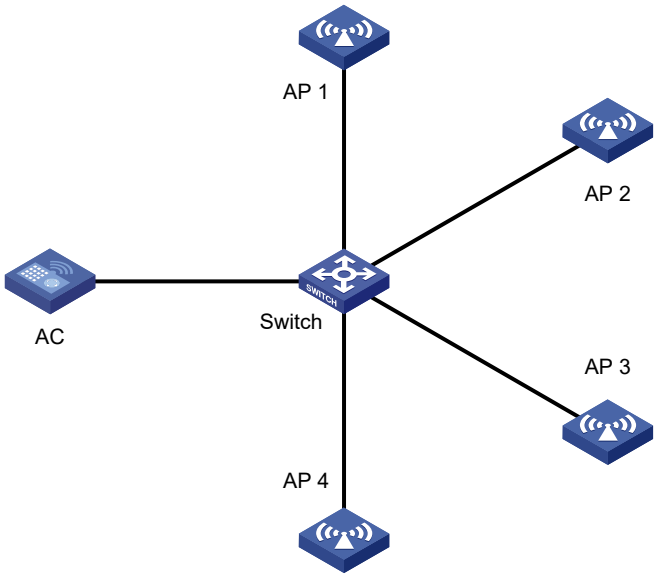


図 1-6 ネットワーク図

II. 設定手順

1) 各 AP が、DHCP サーバから各自の AP の IP アドレスと AC の IP アドレスを入手するように設定します。（詳細は省略します。）
2) 手動 AP を設定します。（詳細は省略します。）
3) AP group を設定します。

AP group group 1 を作成します。

```
<System> system-view
[System] wlan ap-group group1
```

AP group group 2 を作成します。

```
<System> system-view
[System] wlan ap-group group2
```

#AP 1 を AP group group 1 を追加します。

```
[System] wlan ap-group group1
[System-wlan-ap-group-group1] ap ap1
```

#AP 2、AP 3、AP 4 を AP group group 2 に追加します。

```
[System] wlan ap-group group2
[System-wlan-ap-group-group2] ap ap2 ap3 ap4
```

III. 設定の確認

#AP 1 が AP group group1 内に存在し、AP 2、AP 3、AP 4 が AP group group 2 内に存在することを検証します。

[System-wlan-ap-group-group2] display wlan ap-group

```
Total number of AP groups: 3
AP group name       : default-group
Description         : Not configured
AP model            : Not configured
APs                 : Not configured

AP group name       : group1
Description         : Not configured
AP model            : QX-W1020
AP grouping rules:
  AP name           : ap1
  Serial ID         : Not configured
  MAC address       : Not configured
  IPv4 address      : Not configured
  IPv6 address      : Not configured
APs                 : ap1 (AP name)

AP group name       : group2
Description         : Not configured
AP model            : QX-W1020
AP grouping rules:
  AP name           : ap2, ap3, ap4
  Serial ID         : Not configured
  MAC address       : Not configured
  IPv4 address      : Not configured
  IPv6 address      : Not configured
APs                 : ap2 (AP name), ap3 (AP name), ap4 (AP name)
```

目次

このセクションのページは **7-x-x** です。

2 章 コンフィグレーションプロファイルの設定 2-1
2.1 概要 2-1
2.2 設定作業リスト 2-1
2.3 コンフィグレーションプロファイルの作成 2-1
2.4 コンフィグレーションプロファイルの関連付け 2-2
2.5 コンフィグレーションプロファイルの設定 2-3
2.5.1 コンソールポートからのログイン設定 2-3
2.5.2 装置の Telnet ログインの設定 2-4
2.5.3 Ethernet インタフェースの設定 2-6
2.5.4 ポートアイソレーションの設定 2-7
2.5.5 リンクアグリゲーションの設定 2-7
2.5.6 VLAN の設定 2-8
2.5.7 IP アドレスの設定 2-10
2.5.8 DHCP クライアントの設定 2-11
2.5.9 DHCP サーバの設定 2-11
2.5.10 DHCP リレーエージェントの設定 2-13
2.5.11 スタティックルーティングの設定 2-14
2.5.12 ACL の設定 2-14
2.5.13 QoS の設定 2-16
2.5.14 ローカルユーザの設定 2-17
2.6 設定例 2-18
2.6.1 コンフィグレーションプロファイルの設定例 2-18

2章 コンフィグレーションプロファイルの設定

🕮 メモ：

コンフィグレーションプロファイルの設定は、ソフトウェアバージョン 9.6.05c 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 概要

コンフィグレーションプロファイルは、AC のコンフィグレーションプロファイルで指定された設定を、AP または AP グループ内の AP がオンラインになったときに展開します。

2.2 設定作業リスト

操作
（必須設定項目）コンフィグレーションプロファイルの作成
（必須設定項目）コンフィグレーションプロファイルとAPまたはAPグループの関連付け
（オプション設定項目）CLIによるログインの設定
（オプション設定項目）Ethernetインタフェースの設定
（オプション設定項目）ポートアイソレーションの設定
（オプション設定項目）リンクアグリゲーションの設定
（オプション設定項目）VLANの設定
（オプション設定項目）IPアドレスの設定
（オプション設定項目）DHCPクライアントの設定
（オプション設定項目）DHCPサーバの設定
（オプション設定項目）スタティックルーティングの設定
（オプション設定項目）ACLの設定
（オプション設定項目）QoSの設定
（オプション設定項目）ローカルユーザの設定

2.3 コンフィグレーションプロファイルの作成

I. 概要

AC でコンフィグレーションプロファイルを作成し、プロファイルを 1 つまたは複数の AP に関連付けることができます。その後、AC はプロファイルで指定された設定を、関連付けられた AP がオンラインになったときに自動的に展開します。

コンフィグレーションプロファイルを作成するときは、AP モデル名を指定する必要があります。AC は、AP モデルに基づいてプロファイルのデフォルト設定を生成します。

II. 設定手順

以下にコンフィグレーションプロファイルの作成手順を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． コンフィグレーションプロファイルを作成し、その View に移行する	**configuration profile** *profile-name* [**model** *model-name*]	設定なし

2.4 コンフィグレーションプロファイルの関連付け

メモ：

- **configuration-profile** と **remote-configuration** を同じ AP に対して設定しないでください。
- コンフィグレーションプロファイルで設定できないコマンドを設定したい場合に限り、**map-configuration** の併用をご検討ください。また、**configuration-profile** と **map-configuration** の両方に同じ機能を有するコマンド設定がある場合、AP へのコンフィグ適用が正常におこなわれません。

既存のコンフィグレーションプロファイルと AP または AP グループの関連付ける場合、**configuration-profile** コマンドを使用します。AP または AP グループ内の AP がオンラインになると、AC はプロファイル内の設定を AP に自動的に展開します。

コンフィグレーションプロファイルと AP または AP グループの関連付けを解除するには、**undo configuration-profile** コマンドを実行します。また、**undo configuration-profile** コマンドを実行すると、AP または AP グループ内の AP の設定が工場出荷時のデフォルトに復元されます。

I. AP view でのコンフィグレーションプロファイルの関連付け

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP view に移行する	**wlan ap** *ap-name*	—
3． コンフィグレーションプロファイルを関連付ける	**configuration-profile** *profile-name* [**model** *model-name*]	設定なし

II. AP group view でのコンフィグレーションプロファイルの関連付け

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP group view に移行する	**wlan ap-group** *group-name*	—
3． AP model view に移行する	**ap-model** *group-name*	—
4． コンフィグレーションプロファイルを関連付ける	**configuration-profile** *profile-name* [**model** *model-name*]	設定なし

2.5 コンフィグレーションプロファイルの設定

2.5.1 コンソールポートからのログイン設定

コンソールポートからのログイン設定の詳細は、オペレーションマニュアルのセクション 2 *基本機能“CLI によるログイン”の“コンソールポートからのローカルログイン”*を参照してください。

コンフィグレーションプロファイル View での、コンソールポートからのログイン設定の手順を以下に示します。

I. None 認証の設定

操作	コマンド	備考
1． system view に移行する	**system-view**	―
2． コンフィグレーションプロファイルを作成し、その View に移行する	**configuration profile** *profile-name* [**model** *model-name*]	設定なし
3． console line view あるいは class view に移行する	● console line viewに移行する： **line console** *first-number* [*last-number*] ● console line class viewに移行する： **line class console**	どちらか一方を使用します。 User line viewでの設定はユーザラインのみ適用されます。 User line class viewでの設定はclassのすべてのユーザに適用されます。
4． None 認証モードを有効にする	**authentication-mode** *none*	デフォルト：製品モデルにより異なります。 QX-W1000シリーズは**none**。 QX-W1100シリーズは**password**。 QX-W1200しりーずは**password**。

II. Password 認証の設定

操作	コマンド	備考
1． system view に移行する	**system-view**	―
2． コンフィグレーションプロファイルを作成し、その View に移行する	**configuration profile** *profile-name* [**model** *model-name*]	設定なし

操作	コマンド	備考
3. console line view あるいは class view に移行する	● console line viewに移行する： **line console** *first-number* [*last-number*] ● console line class viewに移行する： **line class console**	どちらか一方を使用します。 User line viewでの設定はユーザラインのみ適用されます。 User line class viewでの設定はclassのすべてのユーザに適用されます。
4. Password 認証モードを有効にする	**authentication-mode password**	デフォルト：**none**
5. password を設定する	**set authentication password** { **hash** | **simple** } *password*	デフォルト：製品モデルにより異なります。 QX-W1000シリーズはパスワード設定なし。 QX-W1100シリーズはqx_admin。 QX-W1200シリーズはqx_admin。

III. Scheme 認証の設定

操作	コマンド	備考
1. system view に移行する	**system-view**	―
2. コンフィグレーションプロファイルを作成し、その View に移行する	**configuration profile** *profile-name* [**model** *model-name*]	設定なし
3. console line view あるいは class view に移行する	● console line viewに移行する： **line console** *first-number* [*last-number*] ● console line class viewに移行する： **line class console**	どちらか一方を使用します。 User line viewでの設定はユーザラインのみ適用されます。 User line class viewでの設定はclassのすべてのユーザに適用されます。
4. Scheme 認証を有効にする	**authentication-mode** *scheme*	デフォルト：製品モデルにより異なります。 QX-W1000シリーズは**none**。 QX-W1100シリーズは**password**。 QX-W1200シリーズは**password**。

2.5.2 装置の Telnet ログインの設定

装置の Telnet ログイン設定の詳細は、オペレーションマニュアルのセクション 2 *基本機能“CLI によるログイン”の“Telnet からのログイン”*を参照してください。

コンフィグレーションプロファイル View での、Telnet ログイン設定の手順を以下に示します。

I. Telnet サーバの有効化

操作	コマンド	備考
1． system view に移行する	**system-view**	―
2． コンフィグレーションプロファイルを作成し、その View に移行する	**configuration profile** *profile-name* [**model** *model-name*]	設定なし
3． Telnet サーバを有効化する	**telnet server enable**	デフォルト：無効

II. None 認証の設定

操作	コマンド	備考
1． system view に移行する	**system-view**	―
2． コンフィグレーションプロファイルを作成し、その View に移行する	**configuration profile** *profile-name* [**model** *model-name*]	設定なし
3． VTY line view または VTY line class view に移行する	● VTY line viewに移行する： **line vty** *first-number* [*last-number*] ● VTY line class viewに移行する： **line class vty**	どちらか一方を使用します。 User line viewでの設定はユーザラインのみ適用されます。 User line class viewでの設定はclassのすべてのユーザに適用されます。
4． None 認証モードを有効にする	**authentication-mode none**	デフォルト：**password**

III. Password 認証の設定

操作	コマンド	備考
1． system view に移行する	**system-view**	―
2． コンフィグレーションプロファイルを作成し、その View に移行する	**configuration profile** *profile-name* [**model** *model-name*]	設定なし
3． VTY line view または VTY line class view に移行する	● VTY line viewに移行する： **line vty** *first-number* [*last-number*] ● VTY line class viewに移行する： **line class vty**	どちらか一方を使用します。 User line viewでの設定はユーザラインのみ適用されます。 User line class viewでの設定はclassのすべてのユーザに適用されます。
4． Password 認証モードを有効にする	**authentication-mode password**	デフォルト：**password**

操作	コマンド	備考
5. password の設定	**set authentication password** { **hash** | **simple** } *password*	デフォルト：製品モデルにより異なります。 QX-W1000シリーズはパスワード設定なし。 QX-W1100シリーズはqx_admin。 QX-W1200シリーズはqx_admin。

IV. Scheme 認証の設定

操作	コマンド	備考
1. system view に移行する	**system-view**	―
2. コンフィグレーションプロファイルを作成し、その View に移行する	**configuration profile** *profile-name* [**model** *model-name*]	設定なし
3. VTY line view または VTY line class view に移行する	● VTY line viewに移行する：**line vty** *first-number* [*last-number*] ● VTY line class viewに移行する：**line class vty**	どちらか一方を使用します。 User line viewでの設定はユーザラインのみ適用されます。 User line class viewでの設定はclassのすべてのユーザに適用されます。
4. Scheme 認証を有効にする	**authentication-mode scheme**	デフォルト：**password**

2.5.3 Ethernet インタフェースの設定

Ethernet インタフェースの詳細は、オペレーションマニュアルのセクション 4 *インタフェース "Ethernet インタフェース"* を参照してください。

コンフィグレーションプロファイル View での Ethernet インタフェースの設定手順を以下に示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. コンフィグレーションプロファイルを作成し、その View に移行する	**configuration profile** *profile-name* [**model** *model-name*]	設定なし
3. Ethernet interface view に移行する	**interface** *interface-type interface-number*	―
4. Ethernet インタフェースを有効にする	**undo shutdown**	デフォルト：有効

2.5.4 ポートアイソレーションの設定

コンフィグレーションプロファイル View での、ポートアイソレーション設定の手順を以下に示します。

I. Ethernet インタフェースのポートアイソレーションの設定

操作	コマンド	備考
1. system view に移行する	**system-view**	―
2. コンフィグレーションプロファイルを作成し、その View に移行する	**configuration profile** *profile-name* [**model** *model-name*]	設定なし
3. Ethernet interface view に移行する	**interface** interface-type interface-number	―
4. ポートアイソレーションを有効にする	**port-isolate enable**	デフォルト：有効

II. アグリゲートインタフェースのポートアイソレーション設定

操作	コマンド	備考
1. system view に移行する	**system-view**	―
2. コンフィグレーションプロファイルを作成し、その View に移行する	**configuration profile** *profile-name* [**model** *model-name*]	設定なし
3. アグリゲートインタフェースを作成し、aggregate interface view に移行する	**interface bridge-aggregation** *interface-number*	―
4. ポートアイソレーションを有効にする	**port-isolate enable**	デフォルト：無効

2.5.5 リンクアグリゲーションの設定

リンクアグリゲーションの詳細は、オペレーションマニュアルのセクション 5 *ネットワーク接続“リンクアグリゲーション”*を参照してください。

コンフィグレーションプロファイル View での、リンクアグリゲーション設定の手順を以下に示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―

操作	コマンド	補足
2． コンフィグレーションプロファイルを作成し、その View に移行する	**configuration profile** *profile-name* [**model** *model-name*]	設定なし
3． アグリゲートインタフェースを作成し、aggregate interface view に移行する	**interface bridge-aggregation** *interface-number*	アグリゲートインタフェースを作成すると、スタティックアグリゲーショングループ番号が、自動的に同一番号で作成されます。
4． system view へ戻る	**quit**	―
5． 指定されたアグリゲーショングループにインタフェースを割り当てる	1． Ethernet interface view に移行する： **interface** *interface-type interface-number* 2． 指定されたアグリゲーショングループにインタフェースを割り当てる： **port link-aggregation group** *group-id*	アグリゲーショングループに複数のインタフェースを割り当てる場合、このステップを繰り返してください。

2.5.6 VLAN の設定

VLAN の詳細は、オペレーションマニュアルのセクション 5 *ネットワーク接続　"VLAN"* を参照してください。

コンフィグレーションプロファイル View での、VLAN 設定の手順を以下に示します。

I. VLAN の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． コンフィグレーションプロファイルを作成し、その View に移行する	**configuration profile** *profile-name* [**model** *model-name*]	設定なし
3． VLAN を作成し、view へ移行あるいは VLAN リストを作成する	**vlan** { *vlan-id1* [**to** *vlan-id2*] | **all** }	デフォルト： デフォルト VLAN（VLAN1）のみ
4． VLAN view に移行する	**vlan** *vlan-id*	VLANリストを作成した後、指定したVLANを設定するには、この操作を実行してください。

II. VLAN インタフェースの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	―

操作	コマンド	補足
2. コンフィグレーションプロファイルを作成し、その View に移行する	**configuration profile** *profile-name* [**model** *model-name*]	設定なし
3. VLAN インタフェースを作成し、VLAN interface view に移行する	**interface vlan-interface** *interface-number*	デフォルト：設定なし VLANが存在する場合、直接そのviewに移行します。
4. VLAN インタフェースを有効にする	**undo shutdown**	デフォルト：有効

III. interface view でのアクセス VLAN の設定方法

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. コンフィグレーションプロファイルを作成し、その View に移行する	**configuration profile** *profile-name* [**model** *model-name*]	設定なし
3. interface view に移行する	● Ethernet interface viewに移行する： **interface** *interface-type interface-number* ● aggregate interface viewに移行する： **interface bridge-aggregation** *interface-number*	ー
4. リンクタイプをアクセスに設定する	**port link-type access**	デフォルト：アクセス
5. アクセスポートを VLAN に割り当てる	**port access vlan** *vlan-id*	デフォルト：VLAN1に属します。

IV. トランクポート VLAN の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. コンフィグレーションプロファイルを作成し、その View に移行する	**configuration profile** *profile-name* [**model** *model-name*]	設定なし
3. interface view に移行する	● interface viewに移行する： **interface** *interface-type interface-number* ● aggregate interface viewに移行する： **interface bridge-aggregation** *interface-number*	ー
4. リンクタイプをトランクに設定する	**port link-type trunk**	デフォルト：アクセス

操作	コマンド	補足
5. トランクポートで許可する VLAN を設定する	**port trunk permit vlan** { *vlan-id-list* | **all** }	デフォルト：vlan1のみ許可
6. トランクポートの PVID を設定する	**port trunk pvid vlan** *vlan-id*	デフォルト： VLAN 1

V. ハイブリッドポート VLAN の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. コンフィグレーションプロファイルを作成し、その View に移行する	**configuration profile** *profile-name* [**model** *model-name*]	設定なし
3. interface view に移行する	● interface viewに移行する：**interface** *interface-type interface-number* ● aggregate interface viewに移行する：**interface bridge-aggregation** *interface-number*	ー
4. リンクタイプをハイブリッドに設定する	**port link-type hybrid**	デフォルト：アクセス
5. ハイブリッドポートで許可する VLAN を設定する	**port hybrid vlan** *vlan-id-list* { **tagged** | **untagged** }	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。
6. ハイブリッドポートの PVID を設定する	**port hybrid pvid vlan** *vlan-id*	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。

2.5.7 IP アドレスの設定

コンフィグレーションプロファイル View での、IP アドレス設定の手順を以下に示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. コンフィグレーションプロファイルを作成し、その View に移行する	**configuration profile** *profile-name* [**model** *model-name*]	設定なし
3. VLAN インタフェースを作成し、VLAN interface view に移行する	**interface vlan-interface** *interface-number*	デフォルト：設定なし VLANが存在する場合、直接そのviewに移行します。
4. VLAN インタフェースに IP アドレスを割り当てる	**ip address** *ip-address* { *mask* | *mask-length* } [sub]	デフォルト：設定なし

2.5.8 DHCP クライアントの設定

DHCP クライアントの詳細は、オペレーションマニュアルのセクション 5 *ネットワーク接続 "DHCP クライアント"* を参照してください。

コンフィグレーションプロファイル View での、DHCP クライアント設定の手順を以下に示します。

I. インタフェースでの DHCP クライアントの有効化

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. コンフィグレーションプロファイルを作成し、その View に移行する	**configuration profile** *profile-name* [**model** *model-name*]	設定なし
3. VLAN インタフェースを作成し、VLAN interface view に移行する	**interface vlan-interface** *interface-number*	デフォルト：設定なし VLANが存在する場合、直接そのviewに移行します。
4. VLAN インタフェースに IP アドレスを割り当てる	**ip address dhcp-alloc**	デフォルト：無効

2.5.9 DHCP サーバの設定

DHCP サーバの詳細は、オペレーションマニュアルのセクション 5 *ネットワーク接続 "DHCP サーバ"* を参照してください。

コンフィグレーションプロファイル View での、DHCP サーバ設定の手順を以下に示します。

I. DHCP アドレスプールの作成

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. コンフィグレーションプロファイルを作成し、その View に移行する	**configuration profile** *profile-name* [**model** *model-name*]	設定なし
3. DHCP アドレスプールを作成し、その view に移行する	**dhcp server ip-pool** *pool-name*	デフォルト：設定なし

II. DHCP アドレスプールの IP アドレス範囲の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	ー

操作	コマンド	補足
2． コンフィグレーションプロファイルを作成し、その View に移行する	**configuration profile** *profile-name* [**model** *model-name*]	設定なし
3． DHCP アドレスプールを作成し、その view に移行する	**dhcp server ip-pool** *pool-name*	デフォルト：設定なし
4． プライマリサブネットを設定する	**network** *network-address* [*mask-length* | **mask** *mask*]	デフォルト：設定なし
5． （オプション設定項目） ゲートウェイを設定する	**gateway-list** *ip-address*&<1-64>	デフォルト：設定なし
6． DNS サーバを設定する	**dns-list** *ip-address*&<1-8>	デフォルト：設定なし
7． （オプション設定項目） アドレスのリース期間を設定する	**expired** { **day** *day* [**hour** *hour* [**minute** *minute* [**second** *second*]]] | **unlimited** }	デフォルト：1日
8． （オプション設定項目）アドレスプールの動的割り当てから設定された IP アドレスを除外する	**forbidden-ip** *ip-address*&<1-8>	デフォルト：DHCPアドレスプールすべてのアドレスが割り当て可能です。 複数のアドレス範囲を除外する場合、このステップを繰り返します。

III. DHCP の有効化

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． コンフィグレーションプロファイルを作成し、その View に移行する	**configuration profile** *profile-name* [**model** *model-name*]	設定なし
3． DHCP を有効にする	**dhcp enable**	デフォルト：無効

IV. インタフェースでの DHCP サーバの有効化

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． コンフィグレーションプロファイルを作成し、その View に移行する	**configuration profile** *profile-name* [**model** *model-name*]	設定なし
3． interface view に移行する	**interface** *interface-type interface-number*	―
4． インタフェースで DHCP サーバを有効にする	**dhcp select server**	デフォルト：有効

V. インタフェースでのアドレスプールの適用

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. コンフィグレーションプロファイルを作成し、その View に移行する	**configuration profile** *profile-name* [**model** *model-name*]	設定なし
3. interface view に移行する	**interface** *interface-type interface-number*	ー
4. インタフェースにアドレスプールを適用する	**dhcp server apply ip-pool** *pool-name*	デフォルト：適用されていません。

2.5.10 DHCP リレーエージェントの設定

DHCP リレーエージェントの詳細は、オペレーションマニュアルのセクション 5 *ネットワーク接続 “DHCP リレー”* を参照してください。

コンフィグレーションプロファイル View での、DHCP リレーエージェント設定の手順を以下に示します。

I. DHCP の有効化

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. コンフィグレーションプロファイルを作成し、その View に移行する	**configuration profile** *profile-name* [**model** *model-name*]	設定なし
3. DHCP アドレスプールを作成し、その view に移行する	**dhcp server ip-pool** *pool-name*	デフォルト：設定なし

II. インタフェースでの DHCP リレーエージェントの有効化

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. コンフィグレーションプロファイルを作成し、その View に移行する	**configuration profile** *profile-name* [**model** *model-name*]	設定なし
3. interface view に移行する	**interface** *interface-type interface-number*	ー
4. DHCP リレーエージェントを有効にする	**dhcp select relay**	デフォルト：DHCPが有効にされたとき、インタフェースはDHCPサーバモードで動作します。

III. リレーエージェントの DHCP サーバの指定

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． コンフィグレーションプロファイルを作成し、その View に移行する	**configuration profile** *profile-name* [**model** *model-name*]	設定なし
3． interface view に移行する	**interface** *interface-type interface-number*	―
4． リレーエージェントに DHCP サーバアドレスを指定する	**dhcp relay server-address** *ip-address*	デフォルト：指定なし

2.5.11 スタティックルーティングの設定

スタティックルーティングの詳細は、オペレーションマニュアルのセクション 5 *ネットワーク接続 “スタティックルーティング”* を参照してください。

コンフィグレーションプロファイル View での、スタティックルーティング設定の手順を以下に示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． コンフィグレーションプロファイルを作成し、その View に移行する	**configuration profile** *profile-name* [**model** *model-name*]	設定なし
3． スタティックルートを設定する	**ip route-static** *dest-address* { *mask-length* | *mask* } *next-hop-address*	デフォルト：設定なし

2.5.12 ACL の設定

ACL の詳細は、オペレーションマニュアルのセクション 15 *セキュリティ “ACL”* を参照してください。

コンフィグレーションプロファイル View での、ACL 設定の手順を以下に示します。

I. 標準 ACL の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． コンフィグレーションプロファイルを作成し、その View に移行する	**configuration profile** *profile-name* [**model** *model-name*]	設定なし

操作	コマンド	補足
3． 標準 IPv4 ACL を作成し、その view に移行する	● **acl basic** { *acl-number* | **name** *acl-name* } ● **acl number** *acl-number* [**name** *acl-name*] [**match-order** { **auto** | **config** }]	デフォルト：設定なし *acl-number*の設定範囲は2000～2999です。
4． （オプション設定項目） ルールの番号づけステップを設定する	**step** *step-value*	デフォルト：5
5． ルールを作成/修正する	**rule** [*rule-id*] { **deny** | **permit** } [**fragment** | **source** { *source-address source-wildcard* | **any** } | **time-range** *time-range-name*] *	デフォルト：設定なし
6． （オプション設定項目） ルールの説明を設定する	**rule** *rule-id* **comment** *text*	デフォルト：設定なし

II. 拡張 ACL の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． コンフィグレーションプロファイルを作成し、その View に移行する	**configuration profile** *profile-name* [**model** *model-name*]	設定なし
3． 拡張 IPv4 ACL を作成し、その view に移行する	● **acl advanced** { *acl-number* | **name** *acl-name* } ● **acl number** *acl-number* [**name** *acl-name*] [**match-order** { **auto** | **config** }]	デフォルト：設定なし *acl-number*の設定範囲は3000～3999です。
4． （オプション設定項目） ルールの番号付けステップを設定する	**step** *step-value*	デフォルト：5
5． ルールを作成/修正する	**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** } | **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* } | **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
6． （オプション設定項目） ルールの説明を設定する	**rule** *rule-id* **comment** *text*	デフォルト：設定なし

III. L2 ACL の設定

操作	コマンド	補足
7． system view に移行する	**system-view**	―
1． L2 ACL を作成し、その view に移行する	● **acl mac** { *acl-number* | **name** *acl-name* } ● **acl number** *acl-number* [**name** *acl-name*] [**match-order** { **auto** | **config** }]	デフォルト：設定なし *acl-number*の設定範囲は4000～4999です。
2． （オプション設定項目） ルールの番号付けステップを設定する	**step** *step-value*	デフォルト：5
3． ルールを作成/修正する	**rule** [*rule-id*] { **deny** | **permit** } [**cos** *dot1p* | **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
4． （オプション設定項目） ルールの説明を設定する	**rule** *rule-id* **comment** *text*	デフォルト：設定なし

IV. インタフェースへの ACL 適用

🕮 **メモ：**

- Ethernet インタフェース、アグリゲートインタフェースに適用した ACL は、Layer2 通信パケットに対してのみ動作します。
- VLAN インタフェースに適用した ACL は、Layer3 通信パケットに対してのみ動作します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． コンフィグレーションプロファイルを作成し、その View に移行する	**configuration profile** *profile-name* [**model** *model-name*]	設定なし
3． interface view に移行する	**interface** *interface-type interface-number*	―
4． インタフェースに ACL を適用する	**packet-filter [mac] { acl-number | name** *acl-name* **} { inbound | outbound }**	デフォルト：指定なし

2.5.13 QoS の設定

QoS の詳細は、オペレーションマニュアルのセクション 16 *QoS“プライオリティマッピング”*を参照してください。

コンフィグレーションプロファイル View での、QoS 設定の手順を以下に示します。

I. プライオリティマッピングのパケットプライオリティを信用するインタフェースの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. コンフィグレーションプロファイルを作成し、その View に移行する	**configuration profile** *profile-name* [**model** *model-name*]	設定なし
3. interface view に移行する	**interface** *interface-type interface-number*	―
4. パケットプライオリティタイプの信用を設定する	**qos trust** { **dot1p** | **dscp** }	デフォルト：ポートプライオリティを信用する

II. インタフェースのポートプライオリティの変更

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. コンフィグレーションプロファイルを作成し、その View に移行する	**configuration profile** *profile-name* [**model** *model-name*]	設定なし
3. interface view に移行する	**interface** *interface-type interface-number*	―
4. ポートプライオリティを設定する	**qos priority** *priority-value*	デフォルト：0

2.5.14 ローカルユーザの設定

ローカルユーザの詳細は、オペレーションマニュアルのセクション 13 *ユーザアクセスと認証 “AAA”* を参照してください。

コンフィグレーションプロファイル View での、ローカルユーザ設定の手順を以下に示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. コンフィグレーションプロファイルを作成し、その View に移行する	**configuration profile** *profile-name* [**model** *model-name*]	設定なし
3. ローカルユーザ（装置管理ユーザ）を追加し、local user view に移行する	**local-user** *user-name* **class manage**	デフォルト：設定なし。 最大16の装置管理ユーザを作成できます。
4. （オプション設定項目）ローカルユーザのパスワードを設定する	**password** { **cipher** | **simple** } *string*	デフォルト：設定なし

操作	コマンド	補足
5. ローカルユーザのサービスタイプを指定する	装置管理ユーザ： **service-type { ftp | { telnet | terminal } }**	デフォルト：設定なし
6. （オプション設定項目） ローカルユーザの許可属性を設定する	**authorization-attribute** { **acl** *acl-number* | **idle-cut** *minutes* | **user-profile profile-name** | **user-role** *role-name* | **vlan** *vlan-id* | **work-directory** *directory-name* }	デフォルト：以下に示します。 • FTPユーザはNASのルートディレクトリがありますが、アクセス許可がありません。 • network-operatorユーザロールは、network-adminまたはレベル15ユーザによって作成されるローカルユーザに割り当てられます。

2.6 設定例

2.6.1 コンフィグレーションプロファイルの設定例

I. ネットワーク要件

図 2-1 に示すように、コンフィグレーションプロファイルを AP に適用し、FIT-AP のコンフィグを設定します。

FIT-AP に適用するコンフィグレーションプロファイルには、以下の設定を行います。

- VLAN 10、20 を作成します
- VLAN-Interface 1 を作成し、固定 IP アドレス(10.1.1.2/24)を割り当てます。
- デフォルトゲートウェイ 10.1.1.254 を割り当てます。
- GigabitEthernet 1/0/1 をトランクポートとして設定し、VLAN1，VLAN10,VLAN20 を割り当てます。

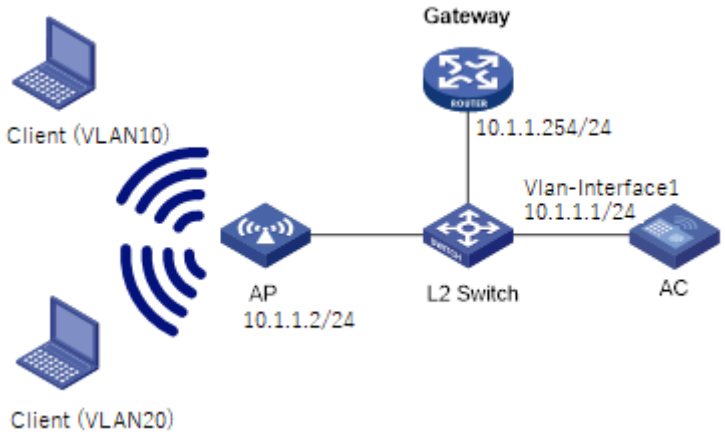


図2-1 ネットワーク図

II. 設定手順

1)　コンフィグレーションプロファイル CP1 を作成します。

```
<AC> system-view
[AC] configuration profile CP1 model QX-W1030
[AC-config-profile-CP1]
```

2)　コンフィグレーションプロファイルに、コンフィグを設定します。

VLAN 10、VLAN 20 を作成します。

```
[AC-config-profile-CP1] vlan 10
[AC-config-profile-CP1-vlan10] quit
[AC-config-profile-CP1] vlan 20
[AC-config-profile-CP1-vlan20] quit
```

#VLAN-Interface 1 を作成し、IP アドレスを割り当てます。

```
[AC-config-profile-CP1] interface vlan-interface 1
[AC-config-profile-CP1-Vlan-interface1] ip address 10.1.1.2 24
[AC-config-profile-CP1-Vlan-interface1] quit
```

#デフォルトルートを設定します。

```
[AC-config-profile-CP1] ip route-static 0.0.0.0 0.0.0.0 10.1.1.254
```

#GigabitEthernet 1/0/1 をトランクポートとして設定し、VLAN1 と VLAN10 と VLAN20 を割り当てます。

```
[AC-config-profile-CP1] interface GigabitEthernet 1/0/1
[AC-config-profile-CP1-GigabitEthernet1/0/1] port link-type trunk
[AC-config-profile-CP1-GigabitEthernet1/0/1] port trunk permit vlan 1 10 20
[AC-config-profile-CP1-GigabitEthernet1/0/1] quit
[AC-config-profile-CP1] quit
```

3)　AP 名が ap1 の手動 AP を作成し、コンフィグレーションプロファイルを関連付けます。

#AP ap1 を AP モデル QX-W1030 を指定して作成し、シリアル ID を設定します

```
[AC] wlan ap ap1 model QX-W1030
[AC-wlan-ap-ap1] serial-id 210235A1BSC123000050
```

#AP ap1 にコンフィグレーションプロファイル CP1 を関連付けます。

```
[AC-wlan-ap-ap1] configuration-profile CP1
```

III. 設定の確認

#以下の情報を検証します。(詳細は省略します。)

- AP と AC が通信できること

- Client(VLAN10)が通信できること
- Client(VLAN20)が通信できること

QX-W2300AC シリーズ アクセスコントローラ

オペレーションマニュアル

8.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概要 1-1
1.2 Pre-RSNAメカニズム 1-1
1.2.1 オープンシステム認証 1-1
1.2.2 共有鍵認証 1-2
1.3 RSNAメカニズム 1-3
1.3.1 認証 1-3
1.3.2 鍵管理 1-3
1.3.3 暗号化方式 1-8
1.4 管理フレームの保護 1-9
1.5 ダイナミックWEPメカニズム 1-11
1.6 プロトコルと標準 1-11
1.7 WLANセキュリティ設定作業リスト 1-12
1.8 セキュリティ機能の設定 1-13
1.8.1 AKMモードの設定 1-13
1.8.2 暗号化規格の設定 1-13
1.8.3 WPA3セキュリティモードの設定 1-13
1.8.4 暗号化方式の設定 1-14
1.8.5 PSKの設定 1-15
1.8.6 KDFの設定 1-15
1.8.7 GTKアップデートの設定 1-16
1.8.8 PTKアップデートの設定 1-16
1.8.9 TKIP MIC failureホールドタイムの設定 1-17
1.8.10 WEP鍵の設定 1-17
1.8.11 管理フレーム保護の設定 1-18
1.8.12 ダイナミックWEPメカニズムの有効化 1-19
1.8.13 Enhanced Openシステム認証の設定 1-19
1.8.14 移行モードでの推奨サービステンプレートの指定 1-20
1.8.15 WPA3-SAEのSAE交換時のPWE生成方式の設定 1-21
1.8.16 WLANセキュリティのSNMP notificationの有効化 1-21
1.9 WLANセキュリティの表示と維持 1-21
1.10 WLANセキュリティの設定例 1-22
1.10.1 共有鍵認証設定例 1-22
1.10.2 WPA-PSK(TKIP)設定例 1-24
1.10.3 WPA2-PSK(AES)＋MACアドレス認証設定例 1-26
1.10.4 802.1X AKM設定例 1-29
1.10.5 管理フレーム保護設定例 1-32
1.10.6 ダイナミックWEPメカニズム設定例 1-35
1.10.7 WPA3エンタープライズ(192bitセキュリティなし)設定例 1-38
1.10.8 WPA3パーソナル設定例 1-41

1章 WLAN セキュリティ

1.1 WLAN概要

オリジナルの IEEE802.11 は Pre-RSNA（Pre Robust Security Network Association）メカニズムを使用します。このメカニズムは鍵露出（key exposure）、トラフィック妨害（traffic interception）、改変（tampering）などの攻撃に対してセキュリティ上で脆弱性があります。WLAN セキュリティを拡張させるため、IEEE802.11i（RSNA メカニズム）が導入されました。WLAN のセキュリティを向上させるため、必要に応じて Pre-RSNA あるいは RSNA のどちらかを選択することができます。

IEEE802.11i は WLAN データトラフィックのみを暗号化します。暗号化されていない WLAN 管理フレームは機密性、確実性、完全性への攻撃に対して無防備となります。IEEE802.11w は 802.11i フレームワークをもとにして管理フレームの保護を行うことで、偽造された認証されていないフレームや分離されたフレームを使用した攻撃を防ぐことができます。

1.2 Pre-RSNAメカニズム

⚠ **重要**：
WEP は設定した暗号化キーが固定であり、解読される危険性があるため、よりセキュリティ強度の高い AES の利用を推奨します。

Pre-RSNA メカニズムは、認証にオープンシステムと共有鍵アルゴリズムを使用し、データの暗号に WEP を使用します。WEP（Wired Equivalent Privacy）は機密性を保持するためストリーム暗号として RC4 を使用します。鍵は 40 ビット（WEP40）、104 ビット（WEP104）、128 ビット（WEP128）をサポートしています。

1.2.1 オープンシステム認証

オープンシステム認証はデフォルトでもっとも簡単な認証アルゴリズムです。オープンシステム認証を使用して認証を要求するクライアントは認証にパスすることができます。

オープンシステム認証は以下のプロセスを使用します。

1) クライアントは AP に認証を要求します。
2) クライアントが認証にパスしたのち、AP はクライアントに認証の応答を送信します。

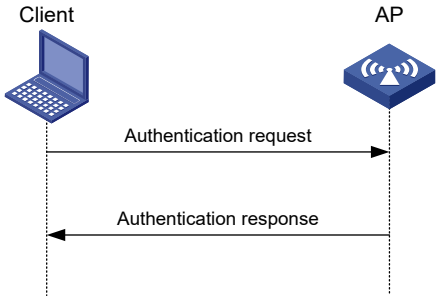


図 1-1 オープンシステム認証のプロセス

1.2.2 共有鍵認証

共有鍵認証は、認証を行うため AP とクライアントの WEP 鍵を使用します。

共有鍵認証は以下のプロセスを使用します。

1) クライアントは AP に認証要求を送信します。
2) AP はランダムに作成したチャレンジテキスト（乱数）をクライアントに送信します。
3) クライアントはチャレンジテキストを暗号化するためクライアントの WEP 鍵を使用し、AP に暗号化したチャレンジテキストを送信します。
4) AP はチャレンジテキストを復号化するため、AP の WEP 鍵を使用します。もとのチャレンジテキストと復号化したチャレンジテキストを比較します。2 つのチャレンジテキストが一致した場合、クライアントは認証にパスします。一致しない場合、クライアントは認証に失敗します。

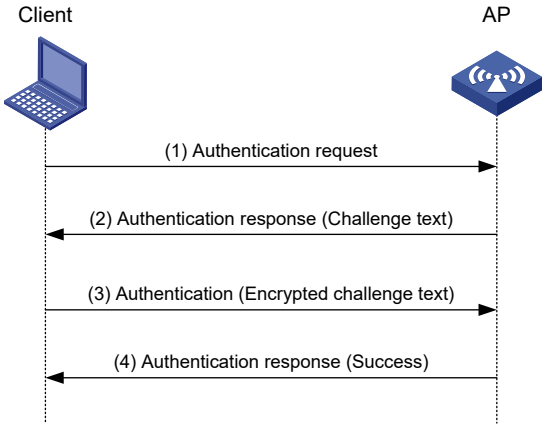


図 1-2 共有鍵の認証プロセス

1.3 RSNAメカニズム

重要：
RSNA はリンクレイヤの認証を行うため、オープンシステム認証が必要です。

RSNA メカニズムは WPA（Wi-Fi Protected Access）、RSN（Robust Security Network）セキュリティモードが含まれます。RSNA は以下の機能を提供します。

- ユーザの完全性を認証し、鍵を動的に作成し、鍵のアップデートを行うため、802.1X、PSK（Pre-Shared Key）AKM（Authentication and key management）を使用します。
  - **802.1X**－802.1X はユーザの認証を行います。802.1X は認証を行う際に PMK（pairwise master key）を作成します。クライアントと AP は PTK（pairwise transient key）を作成するために PMK を使用します。
  - **PSK**－PSK は PMK を作成するために使用します。クライアントと AP は PTK を作成するために PMK を使用します。
- データを暗号化するため、TKIP（Temporal key integrity Protocol）、CCMP（Counter Mode CBC-MAC Protocol）を使用します。

1.3.1 認証

802.1X 認証は PSK 認証よりもセキュリティの強度が強くなります。

PSK 認証は AP とクライアントの両方で設定するため、同一の PSK が必要となります。PSK の完全性は 4-WAY ハンドシェイクを行う間に行われます。PTK の交換が成功した場合、クライアントは認証にパスします。

1.3.2 鍵管理

鍵管理は PTK、GTK（group temporary key）の作成方法およびアップデート方法について定義しています。PTK はユニキャストで使用されます。GTK はマルチキャスト、ブロードキャストで使用されます。

I. PTK、GTK

- PTK の構造



  - EAPOL-KCK（Extensible Authentication Protocol over LAN - Key Confirmation Key）は EAPOL-Key フレームの完全性を確認するために使用します。
  - EAPOL-KEK（Key Encryption Key）は EAPOL-Key フレームの鍵データを暗号化するために使用します。
  - TK（Temporal Key）はユニキャストパケットを暗号化するために使用します。

- GTK には TK に加えてほかのフィールドが含まれます。TK はマルチキャストパケット、ブロードキャストパケットを暗号化するために使用します。

II. EAPOL-Key パケット

IEEE802.11i プロトコルは鍵の交換を行う際、EAPOL-Key を使用します。

Descriptor type (1 byte)	
Key information (2 bytes)	Key length (2 bytes)
Key replay counter (8 bytes)	
Key nonce (32 bytes)	
EAPOL Key IV (16 bytes)	
Key RSC (8 bytes)	
Reserved (8 bytes)	
Key MIC (16 bytes)	
Key data length (2 bytes)	Key data (n bytes)

図 1-3 EAPOL-Key の構造

表 1-1 EAPOL-Key フィールドの説明

フィールド	説明
Descriptor type	ネットワークタイプを指定します。 ● WPAネットワーク ● RSNネットワーク
Key information	鍵情報は表 1-2に示します。
Key length	鍵の長さです。
Key replay counter	リプライ攻撃を防ぐため、GTKアップデートの総数を記録します。APの交換が開始されたときにフィールドを0に設定し、連続したEAPOL-Keyフレームの値を増加させます。 クライアントは、以前に記録したフィールドの値より大きい場合、最新のEAPOL-Keyフレームからフィールドを記録します。以下の場合、EAPOL-Keyフレームを再送します。 ● クライアントで受信したフィールドの値が、保存されているフィールドの値と等しいあるいは小さい場合 ● APで受信されたフィールドが、APで記録されているフィールドと異なる場合 再送回数が最大数を超過した場合、APはクライアントを切断します。
Key nonce	PTKを作成するために使用するランダム値です。
EAPOL Key IV	TKIPを暗号化します。 このフィールドは暗号化タイプがCCMPでない場合のみ有効です。
Key RSC	リプライ攻撃を防ぐため、マルチキャストパケットあるいはブロードキャストパケットの総数を記録します。 各マルチキャストパケットあるいはブロードキャストパケットの転送を行うとAPは、このフィールドの値を増加します。
Reserved	予約されたフィールドです。

フィールド	説明
Key MIC	メッセージの完全性のチェックです。
Key data length	鍵データの長さです。
Key data	GTK、PMKID（pairwise master key identifier）などの転送されるデータです。



図 1-4 Key information の構造

表 1-2 Key information の説明

フィールド	説明
Key Descriptor Version	3ビットの鍵のバージョンです。 ● **1**－非CCMP鍵です。 ● **2**－CCMP鍵です。
Key Type	1ビットの鍵のタイプです。 ● **0**－マルチキャスト交換鍵です。 ● **1**－ユニキャスト交換鍵です。
Reserved	2ビットのフィールドが予約されています。 送信側でこのフィールドを0にした場合、受信側はこのフィールドを無視します。
Install	1ビットの鍵のインストレーションフィールドです。 鍵のタイプが1である場合、このフィールドは0あるいは1となります。 ● **0**－APはTKをインストールするためにクライアントに要求しません。 ● **1**－APはTKをインストールするためにクライアントに要求します。 鍵のタイプが0である場合、送信側はこのフィールドを0に設定し、受信側はこのフィールドを無視します。
Key Ack	1ビットの鍵のAcknowledgmentフィールドです。 値が1の場合、APはクライアントからAcknowledgmentを要求することを示します。
Key MIC	メッセージの完全性をチェックします。 このフィールドが1の場合、作成されたMIC（message integrity check）はEAPOL-keyフレームの鍵MICフィールドに含まれています。
Secure	1ビットの鍵の状態です。値が1の場合、鍵が既に作成されていることを示します。
Error	1ビットのMICチェックの状態です。 値が1の場合、MICが失敗したことを示します。 Requestフィールドが1の場合、クライアントは、このフィールドを1に設定します。
Request	1ビットのリクエストです。MICの改ざんレポートの4-WAYハンドシェイクあるいはマルチキャストハンドシェイクを初期化するため、クライアントがAPに要求するために使用されます。

フィールド	説明
Encrypted Key Data	1ビットの鍵データの暗号化状態です。値が1の場合、鍵データは暗号化されていることを示します。
Reserved	3ビットの予約されたフィールドです。 送信側でこのフィールドを0にした場合、受信側はこのフィールドを無視します。

III. WPA 鍵の交換

WPA は PTK をネゴシエートするため、4-WAY ハンドシェイクの EAPOL-key パケットを使用し、GTK をネゴシエートするため、2-WAY ハンドシェイクの EAPOL-key パケットを使用します。

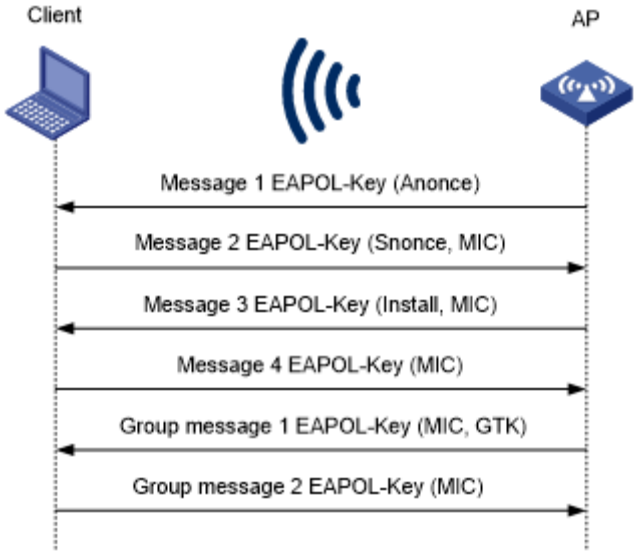


図 1-5 WPA 鍵交換プロセス

WPA 鍵交換は以下のプロセスを用います。

1) AP は ANonce のランダム値が含まれる EAPOL-key メッセージ 1 をクライアントに送信します。
2) クライアントは以下の処理を行います。
   a) KDF（key derivation function）によって PTK を作成するため、ランダム値 SNonce、ANonce、PMK を使用します。
   b) MIC を作成するため PTK の KCK を使用します。
   c) SNonce、MIC が含まれる EAPOL-key メッセージ 2 を返します。
3) AP は以下の処理を行います。
   a) KDF（key derivation function）によって PTK を作成するため、ランダム値 SNonce、ANonce、PMK を使用します。
   b) MIC を作成するため PTK の KCK を使用します。
   c) 受信した MIC とローカルに保存されている MIC を比較します。

d) 2 つの MIC が同一である場合、PTK インストレーションリクエストタグ、MIC が含まれる EAPOL-key メッセージ 3 を返します。

4) クライアントは以下の処理を行います。

a) 受信した MIC とローカルに保存されている MIC を比較します。

b) 2 つの MIC が同一である場合、PTK をインストールし、MIC が含まれる EAPOL-key メッセージ 4 を返します。

5) AP は以下の処理を行います。

a) 受信した MIC とローカルに保存されている MIC を比較します。

b) 2 つの MIC が同一である場合、PTK をインストールし、GMK によって GTK を作成し、KDF によって AP の MAC アドレスを作成します。

c) GTK、MIC が含まれる EAPOL-key グループメッセージ 1 を返します。

6) クライアントは以下の処理を行います。

a) 2 つの MIC が同一である場合、GTK をインストールします。

b) MIC が含まれる EAPOL-key グループメッセージ 2 を返します。

7) AP は以下の処理を行います。

a) 受信した MIC とローカルに保存されている MIC を比較します。

b) 2 つの MIC が同一である場合、GTK をインストールします。

IV. RSN 鍵交換

RSN は PTK と GTK をネゴシエートするため、4-WAY ハンドシェイクの EAPOL-Key パケットを使用します。

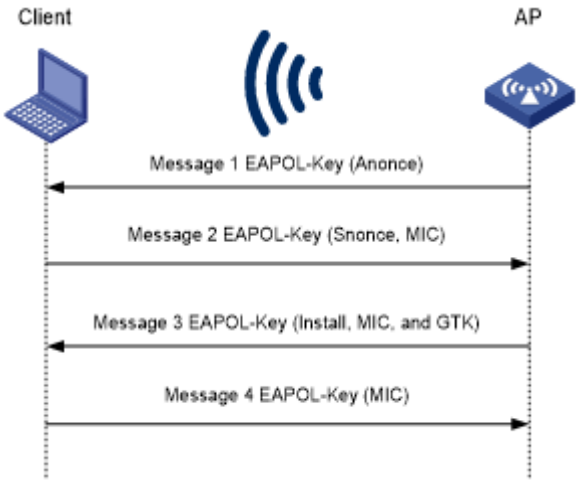


図 1-6 RSN 鍵交換のプロセス

RSN 鍵交換は以下のプロセスを用います。

1) AP は ANonce のランダム値が含まれる EAPOL-key メッセージ 1 をクライアントに送信します。

2) クライアントは以下の処理を行います。

a) KDF によって PTK を作成するため、ランダム値 SNonce、ANonce、PMK を使用します。

b) MIC を作成するため PTK の KCK を使用します。

c) SNonce、MIC が含まれる EAPOL-key メッセージ 2 を返します。

3) AP は以下の処理を行います。

a) KDF（key derivation function）によって PTK を作成するため、ランダム値 SNonce、ANonce、PMK を使用します。

b) MIC を作成するため PTK の KCK を使用します。

c) 受信した MIC とローカルに保存されている MIC を比較します。

d) 2 つの MIC が同一である場合、ランダム GMK によって GTK を作成し、KDF によって AP の MAC アドレスを作成します。

e) 鍵インストレーションリクエストタグ、MIC、GTK が含まれる EAPOL-key メッセージ 3 を返します。

4) クライアントは以下の処理を行います。

a) 受信した MIC とローカルに保存されている MIC を比較します。

b) 2 つの MIC が同一である場合、PTK、GTK をインストールします。

c) MIC が含まれる EAPOL-key メッセージ 4 を返します。

5) AP は以下の処理を行います。

a) 受信した MIC とローカルに保存されている MIC を比較します。

b) 2 つの MIC が同一である場合、PTK、GTK をインストールします。

V. 鍵アップデート

鍵アップデートは WLAN セキュリティを拡張します。鍵アップデートには PTK アップデート、GTK アップデートがあります。

- PTK アップデート– 4-WAY ハンドシェイク交換を使用してユニキャスト鍵をアップデートします。
- GTK アップデート– 2-WAY ハンドシェイク交換を使用してマルチキャスト鍵をアップデートします。

1.3.3 暗号化方式

I. TKIP

TKIP と WEP は RC4 アルゴリズムを使用します。ハードウェアの変更を行うことなくソフトウェアのアップデートを行うことで WEP から TKIP に暗号化方式を変更することができます。TKIP は WEP に比べて以下の利点があります。

- TKIP は暗号セキュリティを拡張するため、長い IV（initialization vectors）を提供します。WEP の暗号化と比べ、TKIP 暗号化は 128 ビットの RC4 暗号アルゴリズムを使用し、IV の長さは 24 ビットから 48 ビットに増加されています。
- TKIP はスタティックに鍵が割り当てられることを防ぐため、ダイナミック鍵交換を行います。TKIP のダイナミック鍵は簡単に解読することはできません。
- TKIP は MIC、Countermeasure（対策）を提供します。パケットが改ざんされた場合、MIC（message integrity check）に失敗します。2 つのパケットが一定の期間、MIC に失敗した場合、AP は攻撃を防ぐためサービスの提供を停止するため、自動で Countermeasure（対策）を行います。

II. CCMP

CCMP は AES（Advanced Encryption Standard）暗号化アルゴリズムの CCM（Counter-Mode/CBC-MAC）をもとにしています。

CCMP はダイナミック鍵交換と管理方式が含まれます。各クライアントはダイナミックに鍵方式をネゴシエートすることができます。CCMP 暗号化方式のセキュリティを強化するため、定期的にアップデートすることができます。暗号化処理を行う間、CCMP は各暗号化パケットで異なる PN（packet number）を使用するため、48 ビット長の PN を使用します。これによって WLAN セキュリティを向上させています。

1.4 管理フレームの保護

管理フレームの保護サービスは、非認証、分離、強固な管理アクションフレームなどの強固な管理フレームを保護します。管理フレームはユニキャストフレームを暗号化する際に PTK を使用し、秘密性、完全性、リプレイ保護を提供します。BIP（Broadcast Integrity Protocol）を使用し、ブロードキャスト管理フレーム、マルチキャスト管理フレームの秘密性、リプレイ保護を提供します。

AP、クライアントが管理フレームの保護を行う場合、セキュリティを向上させるため SA（security association）クエリメカニズムが使用されます。SA クエリはアクティブ SA クエリ、パッシブ SA クエリがあります。

- アクティブ SA クエリ

図 1-7に示すようにアクティブ SA クエリは以下のプロセスを使用します。

a) クライアントはAPにアソシエーションあるいは再送アソシエーションリクエストを送信します。

b) リクエストを受信すると、APはすぐにリクエストが許可されません。すぐに許可されず、後程に関連づけができることをクライアントに通知するため、リプライを送信します。リプライにはアソシエーションのコールバック時間が含まれます。

c) クライアントの状態を確認するため、APはSAクエリリクエストを送信します。
   - □ AP がタイムアウト時間以内に SA クエリのリプライを受信した場合、AP はクライアントがオンラインであるとみなします。
   - □ AP がタイムアウト時間以内に SA クエリのリプライを受信しない場合、別の SA クエリリクエストを送信します。AP が再送タイムアウト時間以内に SA クエリのリプライを受信した場合、AP はクライアントがオンラインであるとみなします。アソシエーションのコールバックのタイムアウト時間まで、クライアントからア

ソシエーションリクエストあるいは再送アソシエーションリクエストに対して応答しません。

- AP が再送タイムアウト時間以内に SA クエリのリプライを受信しない場合、AP はクライアントがオフラインであるとみなします。そしてクライアントが再送アソシエーションを行うことを許可します。

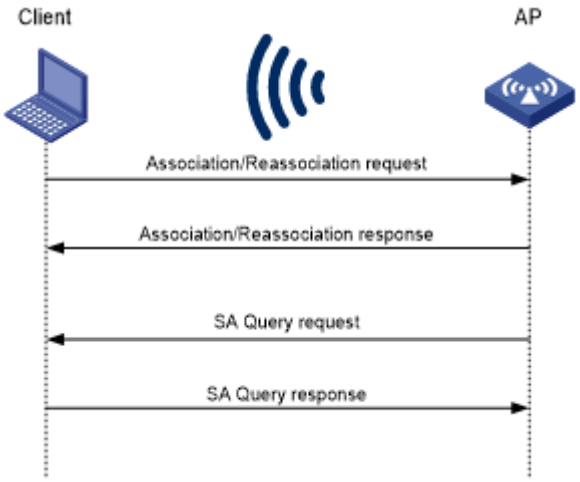


図 1-7 アクティブ SA クエリのプロセス

- パッシブ SA クエリ

図 1-8に示すようにパッシブ SA クエリは以下のプロセスを使用します。

a) クライアントは暗号化されていないdisassociationフレームあるいはdeauthenticationフレームを受信すると、SAクエリプロセスを開始します。

b) クライアントはAPにSAクエリリクエストを送信します。

c) APはクライアントにSAクエリリプライを送信します。

- クライアントがリプライを受信した場合、クライアントは AP がオンラインであることを認識し、disassociation フレームあるいは deauthentication フレームの処理を行いません。
- クライアントがリプライを受信しない場合、クライアントは AP がオフラインであることを認識し、AP との関連づけを解除します。

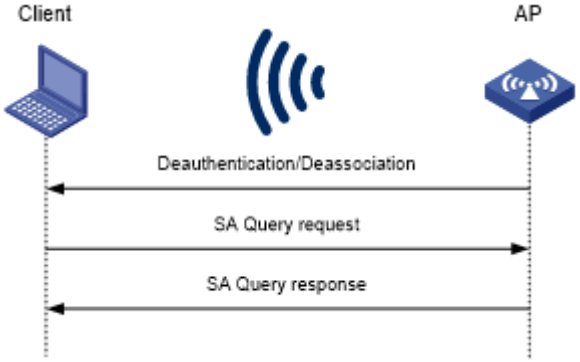


図 1-8 パッシブ SA クエリのプロセス

1.5 ダイナミックWEPメカニズム

⚠ **重要**：

ダイナミック WEP メカニズムはリンクレイヤの認証を行う際にオープンシステム認証を使用します。

WEP は設定した暗号化キーが固定であり、解読される危険性があるため、よりセキュリティ強度の高い AES の利用を推奨します。

IEEE802.11 は、各ユーザがプライベート WEP 鍵の使用することを保証するため、ダイナミック WEP メカニズムを提供します。ユニキャスト通信においては、802.1X 認証を行う間にクライアントとサーバ間で交換が行われた WEP 鍵を使用します。マルチキャスト通信においては、設定された WEP 鍵を使用します。WEP 鍵を設定しない場合、AP はブロードキャスト通信、マルチキャスト通信を行うため WEP 鍵をランダムに作成します。

クライアントが 802.1X 認証にパスしたのち、AP はユニキャスト WEP 鍵、マルチキャストとブロードキャスト WEP 鍵、鍵の ID が含まれる RC4-EAPOL パケットをクライアントに送信します。ユニキャスト WEP 鍵の ID は 4 です。

1.6 プロトコルと標準

- IEEE Standard for Information technology－ *Telecommunications and information exchange between systems－ Local and metropolitan area networks－ Specific requirements－ 2004*
- WI-FI Protected Access－ *Enhanced Security Implementation Based On IEEE P802.11i Standard-Aug 2004*
- Information technology－ *Telecommunications and information exchange between systems－ Local and metropolitan area networks－ Specific requirements－ 802.11, 1999*
- IEEE Standard for Local and metropolitan area networks *"Port-Based Network Access Control" 802.1X™-2004*
- 802.11i IEEE Standard for Information technology－ *Telecommunications and information exchange between systems－ Local and metropolitan area networks－ Specific requirements*
- 802.11w IEEE Standard for Information technology－ *Telecommunications and information exchange between systems－ Local and metropolitan area networks－ Specific requirements*

1.7 WLANセキュリティ設定作業リスト

注意：

- RSNA はリンクレイヤ認証を行うため、オープンシステム認証が必要です。
- ダイナミック WEP メカニズムはユーザアクセスの認証を行うため、802.1X 認証が必要です。
- AKM モード、暗号化規格、暗号化方式は RSNA ネットワークで設定する必要があります。
- 管理フレームの保護は、RSNA メカニズムを使用し、CCMP 暗号化方式、RSN 暗号化規格が設定されているネットワークでのみ有効です。

重要：

WEP は設定した暗号化キーが固定であり、解読される危険性があるため、よりセキュリティ強度の高い AES の利用を推奨します。

Pre-RSNA メカニズムの設定作業リストを以下に示します。

作業リスト
（必須設定項目）暗号化方式の設定
（必須設定項目）WEP鍵の設定

RSNA メカニズムの設定作業リストを以下に示します。

作業リスト
（必須設定項目）AKMモードの設定
（必須設定項目）暗号化規格の設定
（必須設定項目）WPA3セキュリティモードの設定
（必須設定項目）暗号化方式の設定
（オプション設定項目）PSKの設定
（オプション設定項目）KDFの設定
（オプション設定項目）GTKアップデートの設定
（オプション設定項目）PTKアップデートの設定
（オプション設定項目）TKIP MIC failureホールドタイムの設定
（オプション設定項目）WEP鍵の設定
（オプション設定項目）管理フレーム保護の設定

🕮 **メモ：**

- WEP 鍵が設定されている場合、ダイナミック WEP メカニズムはマルチキャスト WEP 鍵、ブロードキャスト WEP 鍵として設定された WEP 鍵を使用します。ネゴシエートされたユニキャスト WEP の ID は 4 で、暗号化方式長の設定を使用します。
- WEP 鍵が設定されていない場合、マルチキャスト、ブロードキャストの両方のダイナミック WEP 鍵の長さは 104 ビットです。ネゴシエートされたユニキャスト WEP の ID は 4 です。作成されたマルチキャスト WEP 鍵、ブロードキャスト WEP 鍵の ID は 1 です。

1.8 セキュリティ機能の設定

1.8.1 AKM モードの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. WLAN service template view に移行する	**wlan service-template** *service-template-name*	—
3. security IE を設定する	**akm mode** { **dot1x** | **psk** }	デフォルト：設定なし

1.8.2 暗号化規格の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. WLAN service template view に移行する	**wlan service-template** *service-template-name*	—
3. security IE を設定する	**security-ie** { **rsn** | **wpa** }	デフォルト：設定なし

🕮 **メモ：**

暗号化規格に WPA2 または WPA3 を使用する場合は RSN、WPA を使用する場合は WPA を設定します。

1.8.3 WPA3 セキュリティモードの設定

WPA 3 は、次のセキュリティモードをサポートしています。

- **WPA3-SAE**：SAE(Simultaneous Authentication of Equals) を使用します。これは、WPA 2-Personal の PSK を置き換えて、より堅牢なパスワードベースの認証を提供します。これにより、個々のユーザの保護が向上します。
- **WPA 3-Enterprise**：192 ビットの最小強度セキュリティプロトコルと暗号化ツールを使用して、機密データの保護を強化するオプションモードを提供します。暗号化ツ

ールの適切な組み合わせが使用されるようにし、WPA 3 ネットワーク内で一貫したセキュリティのベースラインを設定します。

I. 制限事項とガイドライン

WPA 3-Enterprise を使用するには、cipher スイートを GCMP に、セキュリティ IE を RSN に設定します。

WPA 3-SAE を使用するには、cipher スイートを CCMP に、セキュリティ IE を RSN に設定します。

WPA 3 セキュリティモードを指定する場合は、管理フレーム保護を有効にすることをお勧めします。

一部のクライアントは、一時的に WPA 3 エンタープライズセキュリティモードを使用してオンラインになった場合、WPA 3-SAE セキュリティモードを使用してオンラインにできなくなります。このような問題が発生した場合、クライアントは WPA 3-SAE セキュリティモードを使用して再試行できます。

WPA 3 セキュリティモードを設定せず、802.11r FT または拡張オープンシステム認証を同時に有効にします。有効にすると、サービステンプレートを有効にできません。802.11r の詳細については、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*10 WLAN ローミング*” の”*10 章 拡張ローミング*“を参照してください。

以下に WPA3 セキュリティモードを有効にする設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. WLAN service template view に移行する	**wlan service-template** *service-template-name*	—
3. WPA3 セキュリティモードを有効にする	**wpa3** { **enterprise** | **personal** { **mandatory** | **optional** } }	デフォルト：無効

1.8.4 暗号化方式の設定

重要：

WEP は設定した暗号化キーが固定であり、解読される危険性があるため、よりセキュリティ強度の高い AES の利用を推奨します。

暗号化方式には以下があります。

- WEP (WEP40、WEP104、WEP128)
- CCMP
- GCMP
- TKIP

クライアントアソシエーションの障害を回避するため、CCMP、GCMP、または TKIP が設定されている場合は WEP 40 または WEP 104 を設定しないことを推奨します。

以下に暗号化方式の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. WLAN service template view に移行する	**wlan service-template** *service-template-name*	ー
3. 暗号化方式を設定する	**cipher-suite** { **ccmp** | **gcmp** | **tkip** | **wep40** | **wep104** | **wep128** }	デフォルト：設定なし WEP128とCCMPの両方を設定することはできません。 WEP128とTKIPの両方を設定することはできません。 WEP128とGCMPの両方を設定することはできません。

メモ：

暗号化方式に AES を使用する場合は CCMP を設定します。

1.8.5 PSK の設定

AKM モードが PSK の場合、PSK を設定する必要があります。

以下に PSK の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. WLAN service template view に移行する	**wlan service-template** *service-template-name*	ー
3. PSK を設定する	**preshared-key** { **pass-phrase** | **raw-key** } { **cipher** | **simple** } *string*	デフォルト：設定なし

1.8.6 KDF の設定

KDF は PTK と GTK を作成するため RSNA ネットワークで使用します。KDF には HMAC-SHA1、HMAC-SHA256 が含まれます。HMAC-SHA256 アルゴリズムは HMAC-SHA1 よりもセキュリティの強度が強くなります。

以下に KDF の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. WLAN service template view に移行する	**wlan service-template** *service-template-name*	ー
3. KDF を設定する	**key-derivation** { **sha1** | **sha256** | **sha1-and-sha256** }	デフォルト：HMAC-SHA1

1.8.7 GTK アップデートの設定

AKM、暗号化規格、暗号化方式が設定されている場合、鍵交換を行っている間、システムは GTK を作成します。鍵のセキュリティを拡張するため、以下のアップデートモードにもとづいて GTK をアップデートします。

- **Time-based**– 指定した間隔で GTK がアップデートされます。
- **Packet-based**– 指定したパケット数が送信された後、GTK がアップデートされます。
- **Offline-triggered**– BSS（basic service set）のクライアントがオフラインになったとき、GTK がアップデートされます。

以下に GTK アップデートの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. WLAN service template view に移行する	**wlan service-template** *service-template-name*	―
3. GTK のアップデートを有効にする	**gtk-rekey enable**	デフォルト：無効
4. （オプション設定項目）GTK アップデートのモードを設定する	**gtk-rekey method** { **packet-based** [*packet*] | **time-based** [*time*] }	デフォルト：GTKは86400秒ごとにアップデートされます。**packet-based**モードのデフォルトのパケット数は10000000です。
5. （オプション設定項目）Offline-triggered モードの GTK アップデートを有効にする	**gtk-rekey client-offline enable**	デフォルト：無効

1.8.8 PTK アップデートの設定

AKM、暗号化規格、暗号化方式が設定されている場合、鍵交換を行っている間、システムは PTK を作成します。PTK ライフタイムが終了したのち、PTK をアップデートします。

PTK アップデートを有効にするには、高速 BSS 移行 (FT) を設定しないでください。両方の機能が設定されている場合、FTP 更新は有効になりません。

以下に PTK アップデートの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. WLAN service template view に移行する	**wlan service-template** *service-template-name*	―
3. PTK アップデートを有効にする	**ptk-rekey enable**	デフォルト：無効
4. PTK ライフタイムを設定する	**ptk-lifetime** *time*	デフォルト：43200秒

1.8.9 TKIP MIC failure ホールドタイムの設定

TKIP を設定したのち、TKIP MIC failure ホールドタイムを設定することができます。AP は MIC failure ホールドタイム以内に 2 つの MIC の失敗が検出された場合、60 秒の間、すべてのクライアントとのアソシエーションを解除します。

以下に TKIP MIC failure ホールドタイムの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. WLAN service template view に移行する	**wlan service-template** *service-template-name*	―
3. TKIP MIC failure ホールドタイムを設定する	**tkip-cm-time** *time*	デフォルト：0 APは対応しません。

1.8.10 WEP 鍵の設定

重要：

WEP は設定した暗号化キーが固定であり、解読される危険性があるため、よりセキュリティ強度の高い AES の利用を推奨します。

WEP 鍵は、Pre-RSNA ネットワークのすべてのパケットおよび RSNA ネットワークのマルチキャストパケットを暗号化するために使用します。WEP 鍵が設定されていない場合、以下の対応となります。

- **Pre-RSNA ネットワークのパケット**：暗号化されません。
- **RSNA ネットワークのマルチキャストパケット**：暗号化するために交換された GTK を使用します。

以下に WEP 鍵の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. WLAN service template view に移行する	**wlan service-template** *service-template-name*	―
3. WEP 鍵を設定する	**wep key** *key-id* { **wep40** | **wep104** | **wep128** } { **pass-phrase** | **raw-key** } { **cipher** | **simple** } *string*	デフォルト：設定なし
4. （オプション設定項目）WEP 鍵を適用する	**wep key-id** { **1** | **2** | **3** | **4** }	デフォルト：1 ダイナミックWEPメカニズムが有効の場合、WEP鍵を適用しないでください。

1.8.11 管理フレーム保護の設定

🕮 **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。

管理フレーム保護は、RSNA メカニズムを使用するネットワークでのみ適用されます。管理フレーム保護は暗号化規格に RSN、暗号化方式に CCMP を設定します。

管理フレーム保護が無効の場合、ネットワークはすべてのクライアントで有効となりますが、管理フレーム保護は実行されません。管理フレーム保護が有効な場合、ネットワークアクセスおよび管理フレーム保護の有効性は管理フレーム保護のモードによって変わります。

- **Optional モード**－すべてのクライアントはネットワークへのアクセスが有効です。管理フレーム保護は、管理フレーム保護がサポートされているクライアントでのみ実行されます。
- **Mandatory モード**－ ネットワークアクセスと管理フレーム保護は管理フレーム保護がサポートされているクライアントでのみ実行されます。

以下に管理フレーム保護の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. WLAN service template view に移行する	**wlan service-template** *service-template-name*	―
3. 管理フレーム保護を有効にする	**pmf** { **optional** | **mandatory** }	デフォルト：無効
4. (オプション設定項目) KDF を設定する	**key-derivation { sha1 | sha256 | sha1-and-sha256 }**	デフォルト：HMAC-SHA1
5. SA クエリリクエストの送信間隔を設定する	**pmf saquery retrytimeout** *timeout*	デフォルト：200ミリ秒
6. SA クエリリクエストの最大試行回数を設定する	**pmf saquery retrycount** *count*	デフォルト：4
7. アソシエーション復帰時間を設定する	**pmf association-comeback** *time*	デフォルト：1秒

1.8.12 ダイナミック WEP メカニズムの有効化

⚠ **重要：**
WEP は設定した暗号化キーが固定であり、解読される危険性があるため、よりセキュリティ強度の高い AES の利用を推奨します。

ダイナミック WEP メカニズムは 802.1X 認証モードを使用する必要があります。

以下にダイナミック WEP メカニズムを有効にする設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. WLAN service template view に移行する	**wlan service-template** *service-template-name*	—
3. ダイナミック WEP メカニズムを有効にする	**wep mode dynamic**	デフォルト：無効

1.8.13 Enhanced Open システム認証の設定

🕮 **メモ：**
この機能は、ソフトウェアバージョン 9.6.08c を含む以降のソフトウェアからサポートしています。

I. Enhanced Open システム認証について

Enhanced Open システム認証は、Opportunistic Wireless Encryption (OWE) を使用して、OWE 対応クライアントのデータパケットを暗号化するためのキーをネゴシエーションし、セキュリティパフォーマンスが強化されたオープンシステム認証を提供します。

II. 制限とガイドライン

この機能を有効にする前に、WPA3 セキュリティモード、FT、管理フレーム保護、暗号化規格、暗号化方式、および KDF がデフォルト設定になっていることを確認してください。

この機能を有効にすると、次の操作が実行されます。

- 暗号化規格を RSN として指定します。
- CCMP として暗号化方式を指定します。
- 管理フレーム保護を有効にします。
- KDF として HMAC-SHA256 または HMAC-SHA384 を指定します。

III. 設定手順

以下に Enhanced Open システム認証を有効にする設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. WLAN service template view に移行する	**wlan service-template** *service-template-name*	―
3. Enhanced Open システム認証を有効にする	**enhanced-open enable**	デフォルト：無効

1.8.14 移行モードでの推奨サービステンプレートの指定

🕮 **メモ：**

この機能は、ソフトウェアバージョン 9.6.08c を含む以降のソフトウェアからサポートしています。

I. 移行モードでの推奨サービステンプレートについて

オープン WLAN から Enhanced Open WLAN への移行時には、OWE 非対応および OWE 対応のクライアントに対応するために、両方のタイプの WLAN が存在する可能性があります。この場合、OWE 対応クライアントがオープン WLAN にアクセスしようとした場合、または OWE 非対応クライアントが拡張オープン WLAN にアクセスしようとした場合、対応する AP はアクセス要求を拒否します。

この機能により、クライアントは適合する適切な WLAN に高速アクセスできます。

II. 制限とガイドライン

オープンサービステンプレートと Enhanced Open サービステンプレートの両方でこの機能を設定し、これらを相互の推奨テンプレートとして指定します。

サービステンプレートとその推奨サービステンプレートを同じ無線に設定します。

Enhanced Open サービステンプレートの SSID 非表示を有効にします。

III. 設定手順

以下に Enhanced Open システム認証を有効にする設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. WLAN service template view に移行する	**wlan service-template** *service-template-name*	―
3. 移行モードでの推奨サービステンプレートを設定する	**enhanced-open transition-mode service-template** *service-template-name*	デフォルト：設定なし このコマンドを複数回実行した場合、最後の設定が反映されます。

1.8.15 WPA3-SAE の SAE 交換時の PWE 生成方式の設定

WPA3-SAE は、Hunting-and-Pecking (HnP) と Hash-to-Element (H2E) を使用した PWE の生成をサポートしています。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。

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、クライアントは WLAN 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 キーワードを指定します。

以下に WPA-SAE の SAE 交換時の PWE 生成方式の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. WLAN service template view に移行する	**wlan service-template** *service-template-name*	―
3. WPA3-SAE の SAE 交換時の PWE 生成方式を設定する	**akm sae pwe { both-h2e-hnp | h2e | hnp }**	デフォルト：both-h2e-hnp

1.8.16 WLAN セキュリティの SNMP notification の有効化

SNMP notification を有効にすることで、WLAN セキュリティに関する重要なイベントを NMS に通知します。NMS は設定された出力ルールにしたがって notification を出力する方法を決定します。

SNMP notification についての詳細は、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*17 ネットワーク管理と監視*”の” *4 章 SNMP*”を参照してください。

以下に WLAN セキュリティに関する SNMP notification の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. WLAN セキュリティに関する SNMP notification を有効にする	**snmp-agent trap enable wlan usersec**	デフォルト：無効

1.9 WLANセキュリティの表示と維持

すべての view で display コマンドを実行できます。

操作	コマンド
WLANサービステンプレート情報を表示する	**display wlan service-template** [*service-template-name*] [**verbose**]
クライアント情報を表示する	**display wlan client** [**ap** *ap-name* [**radio** *radio-id*] | **mac-address** *mac-address* | **service-template** *service-template-name*] [**verbose**]

詳細は QX-W2300AC シリーズアクセスコントローラコマンドマニュアルの“*6 WLAN アクセス*”の”*1 章 WLAN アクセス*”を参照してください。

1.10 WLANセキュリティの設定例

1.10.1 共有鍵認証設定例

I. ネットワーク要件

重要：

WEP は設定した暗号化キーが固定であり、解読される危険性があるため、よりセキュリティ強度の高い AES の利用を推奨します。

図 1-9に示すように Switch は AP とクライアントに IP アドレスを割り当てるため、DHCP サーバとして動作します。クライアントが WEP 鍵 12345 を使用してネットワークにアクセスできるように、共有鍵認証を設定します。

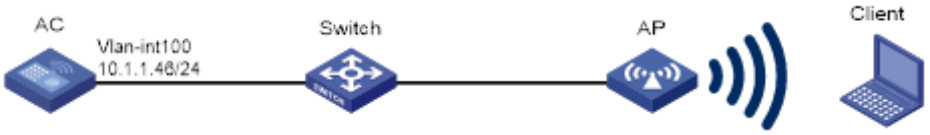


図 1-9 ネットワーク図

II. 設定手順

WLAN サービステンプレート service1 を作成します。

```
<AC> system-view
[AC] wlan service-template service1
```

サービステンプレートの SSID サービスを指定します。

```
[AC-wlan-st-service1] ssid service
```

サービステンプレート service1 の暗号化方式を WEP40 に設定します。プレーンテキストで共有鍵を 12345 に指定します。鍵を ID 2 に割り当てます。

```
[AC-wlan-st-service1] cipher-suite wep40
[AC-wlan-st-service1] wep key 2 wep40 pass-phrase simple 12345
[AC-wlan-st-service1] wep key-id 2
```

サービステンプレート service1 を有効にします。

```
[AC-wlan-st-service1] service-template enable
[AC-wlan-st-service1] quit
```

AP 名 ap1 の AP を作成し、モデル名、シリアル番号を指定します。

```
[AC] wlan ap ap1 model QX-W1110
[AC-wlan-ap-ap1] serial-id 2219801A28N819CE0002T
```

サービステンプレート service1 を AP の radio 1 に割り当て、radio 1 を有効にします。

```
[AC-wlan-ap-ap1] radio 1
[AC-wlan-ap-ap1-radio-1] service-template service1
[AC-wlan-ap-ap1-radio-1] radio enable
[AC-wlan-ap-ap1-radio-1] return
```

III. 設定の確認

WLAN サービステンプレートが正常に設定されていることを確認するため、**display wlan service-template** コマンドを使用します。

```
<AC> display wlan service-template service1 verbose
Service template name         : service1
Description                   : Not configured
SSID                          : service
SSID-hide                     : Disabled
User-isolation                : Disabled
Service template status       : Enabled
Maximum clients per BSS       : 64
Frame format                  : Dot3
Seamless roam status          : Disabled
Seamless roam RSSI threshold  : 50
Seamless roam RSSI gap        : 20
VLAN ID                       : 1
AKM mode                      : Not configured
Security IE                   : Not configured
Cipher suite                  : WEP40
WEP key ID                    : 2
TKIP countermeasure time      : 0
PTK lifetime                  : 43200 sec
PTK rekey                     : Enabled
GTK rekey                     : Enabled
GTK rekey method              : Time-based
GTK rekey time                : 86400 sec
GTK rekey client-offline      : Enabled
WPA3 status                   : Disabled
PPSK                          : Disabled
PPSK Fail Permit              : 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                  : Not configured
802.1X handshake              : Disabled
802.1X handshake secure       : Disabled
802.1X domain                 : Not configured
MAC-auth domain               : Not configured
Max 802.1X users per BSS      : 4096
Max MAC-auth users per BSS    : 4096
```

```
802.1X re-authenticate        : Disabled
Authorization fail mode       : Online
Accounting fail mode          : Online
Authorization                 : Permitted
Key derivation                : N/A
PMF status                    : Disabled
Hotspot policy number         : Not configured
Forwarding policy status      : Disabled
Forwarding policy name        : Not configured
Forwarder                     : AC
FT status                     : Disabled
QoS trust                     : Port
QoS priority                  : 0
BTM status                    : Disabled
```

1.10.2 WPA-PSK(TKIP)設定例

I. ネットワーク要件

図 1-10に示すようにSwitchはAPとクライアントにIPアドレスを割り当てるため、DHCPサーバとして動作します。

- WPA-PSK(TKIP)を設定します。
- ネットワークにアクセスするため、クライアントは共有鍵 12345678 を使用します。

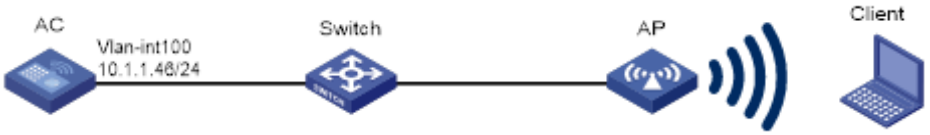


図 1-10 ネットワーク図

II. 設定手順

1) サービステンプレート service1 を作成します。

```
<AC> system-view
[AC] wlan service-template service1
```

2) サービステンプレートの SSID サービスを指定します。

```
[AC-wlan-st-service1] ssid service
```

3) サービステンプレート service1 の WLAN セキュリティを設定します。

AKM モードとして PSK を設定し、プレーンテキストで共有鍵 12345678 を指定します。

```
[AC-wlan-st-service1] akm mode psk
[AC-wlan-st-service1] preshared-key pass-phrase simple 12345678
```

WPA(TKIP)のために、暗号化規格に RSN、暗号化方式に TKIP を指定します。

```
[AC-wlan-st-service1] cipher-suite tkip
[AC-wlan-st-service1] security-ie rsn
```

4) サービステンプレート service1 を有効にします。

```
[AC-wlan-st-service1] service-template enable
[AC-wlan-st-service1] quit
```

5) AP 名 ap1 の AP を作成し、モデル名、シリアル番号を指定します。

```
[AC] wlan ap ap1 model QX-W1110
[AC-wlan-ap-ap1] serial-id 219801A28N819CE0002T
```

6) サービステンプレート service1 を AP の radio 1 に割り当て、radio 1 を有効にします。

```
[AC-wlan-ap-ap1] radio 1
[AC-wlan-ap-ap1-radio-1] service-template service1
[AC-wlan-ap-ap1-radio-1] radio enable
[AC-wlan-ap-ap1-radio-1] return
```

III. 設定の確認

WLAN サービステンプレートが正常に設定されていることを確認するため、**display wlan service-template** コマンドを使用します。

```
<AC> display wlan service-template service1 verbose
Service template name         : service1
Description                   : Not configured
SSID                          : service
SSID-hide                     : Disabled
User-isolation                : Disabled
Service template status       : Enabled
Maximum clients per BSS       : 64
Frame format                  : Dot3
Seamless roam status          : Disabled
Seamless roam RSSI threshold  : 50
Seamless roam RSSI gap        : 20
VLAN ID                       : 1
AKM mode                      : PSK
Security IE                   : RSN
Cipher suite                  : TKIP
TKIP countermeasure time      : 0
PTK lifetime                  : 43200 sec
PTK rekey                     : Enabled
GTK rekey                     : Enabled
GTK rekey method              : Time-based
GTK rekey time                : 86400 sec
GTK rekey client-offline      : Enabled
WPA3 status                   : Disabled
PPSK                          : Disabled
PPSK Fail Permit              : 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                  : Not configured
802.1X handshake              : Disabled
802.1X handshake secure       : Disabled
802.1X domain                 : Not configured
MAC-auth domain               : Not configured
Max 802.1X users per BSS      : 4096
Max MAC-auth users per BSS    : 4096
802.1X re-authenticate        : Disabled
Authorization fail mode       : Online
Accounting fail mode          : Online
```

```
Authorization                 : Permitted
Key derivation                : N/A
PMF status                    : Disabled
Hotspot policy number         : Not configured
Forwarding policy status      : Disabled
Forwarding policy name        : Not configured
Forwarder                     : AC
FT status                     : Disabled
QoS trust                     : Port
QoS priority                  : 0
BTM status                    : Disabled
```

1.10.3 WPA2-PSK(AES)＋MAC アドレス認証設定例

I. ネットワーク要件

図 1-11に示すように、Switch は AP とクライアントに IP アドレスを割り当てるため、DHCP サーバとして動作します。

- ログイン名 abc、パスワード 123 を使用して、クライアントがネットワークにアクセスできるように WPA2-PSK(AES)と MAC アドレス認証を設定します。
- ネットワークにアクセスするため、クライアントは共有鍵 12345678 を使用します。

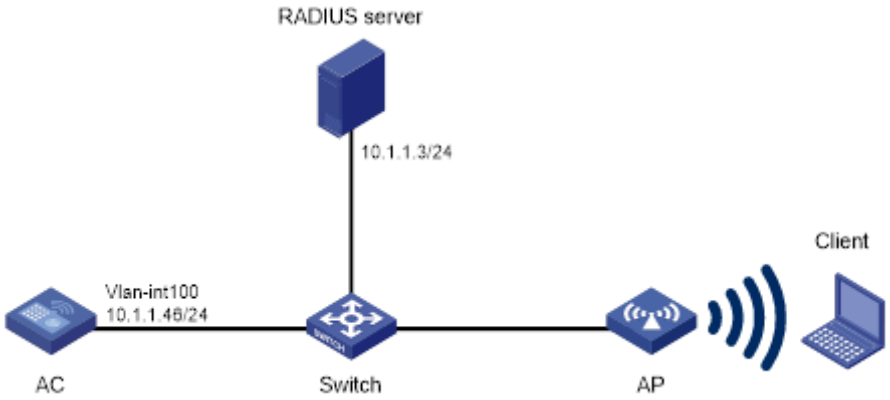


図 1-11 ネットワーク図

II. 設定手順

1) RADIUS サーバでユーザ名 abc、パスワード 123 を設定し、RADIUS サーバと AC が互いに通信可能なことを確認します。（詳細は省略します。）
2) WLAN サービステンプレート service1 を作成します。サービステンプレートの SSID サービスを指定します。

```
<AC> system-view
[AC] wlan service-template service1
[AC-wlan-st-service1] ssid service
```

3) サービステンプレート service1 の WLAN セキュリティを設定します。

AKM モードとして PSK を設定し、プレーンテキストで共有鍵 12345678 を指定します。

```
[AC-wlan-st-service1] akm mode psk
```

```
[AC-wlan-st-service1] preshared-key pass-phrase simple 12345678
```

WPA2(AES)のために、暗号化規格に RSN、暗号化方式に CCMP を設定します。

```
[AC-wlan-st-service1] cipher-suite ccmp
[AC-wlan-st-service1] security-ie rsn
```

MAC アドレス認証を設定します。

```
[AC-wlan-st-service1] client-security authentication-mode mac
```

4) サービステンプレート service1 を有効にします。

```
[AC-wlan-st-service1] service-template enable
[AC-wlan-st-service1] quit
```

5) RADIUS スキームを設定します。

RADIUS スキーム radius1 を作成し、RADIUS scheme view に移行します。

```
[AC] radius scheme radius1
```

プライマリ認証サーバ、アカウンティングサーバを指定します。

```
[AC-radius-radius1] primary authentication 10.1.1.3 1812
[AC-radius-radius1] primary accounting 10.1.1.3 1813
```

プレーンテキストで認証サーバ、アカウンティングサーバの共有鍵 12345678 を設定します。

```
[AC-radius-radius1] key authentication simple 12345678
[AC-radius-radius1] key accounting simple 12345678
```

RADIUS サーバの設定にもとづいて、RADIUS サーバにユーザ名を送信するように設定します。

- RADIUS サーバに送信するユーザ名からドメイン名を除外します。

```
[Device-radius-rs1] user-name-format without-domain
[Device-radius-rs1] quit
```

- RADIUS サーバに送信するユーザ名にドメイン名を含めます。

```
[Device-radius-rs1] user-name-format with-domain
[Device-radius-rs1] quit
```

6) ISP ドメイン dom1 を作成し、ISP ドメインの RADIUS スキームを設定します。

```
[AC] domain dom1
[AC-isp-dom1] authentication lan-access radius-scheme radius1
[AC-isp-dom1] authorization lan-access radius-scheme radius1
[AC-isp-dom1] accounting lan-access radius-scheme radius1
[AC-isp-dom1] quit
```

7) ISP ドメイン dom1 を設定し、ユーザ名 abc、パスワード 123 を指定します。

```
[AC] mac-authentication domain dom1
[AC] mac-authentication user-name-format fixed account abc password simple 123
```

8) AP 名 ap1 の AP を作成し、モデル名、シリアル番号を指定します。

```
[AC] wlan ap ap1 model QX-W1110
[AC-wlan-ap-ap1] serial-id 219801A28N819CE0002T
```

9) サービステンプレート service1 を AP の radio 1 に割り当て、radio 1 を有効にします。

```
[AC-wlan-ap-ap1] radio 1
[AC-wlan-ap-ap1-radio-1] service-template service1
[AC-wlan-ap-ap1-radio-1] radio enable
[AC-wlan-ap-ap1-radio-1] return
```

🕮 メモ：

AAA、RADIUS コマンドの詳細は、QX-W2300AC シリーズアクセスコントローラコマンドマニュアルの“*13 ユーザアクセスと認証*“の”*3 章 AAA*“を参照してください。

III. 設定の確認

WLAN サービステンプレートが正常に設定されていることを確認するため、**display wlan service-template** コマンドを使用します。

```
<AC> display wlan service-template service1 verbose
Service template name         : service1
Description                   : Not configured
SSID                          : service
SSID-hide                     : Disabled
User-isolation                : Disabled
Service template status       : Enabled
Maximum clients per BSS       : 64
Frame format                  : Dot3
Seamless roam status          : Disabled
Seamless roam RSSI threshold : 50
Seamless roam RSSI gap        : 20
VLAN ID                       : 1
AKM mode                      : PSK
Security IE                   : RSN
Cipher suite                  : CCMP
TKIP countermeasure time      : 0 sec
PTK lifetime                  : 43200 sec
PTK rekey                     : Enabled
GTK rekey                     : Enabled
GTK rekey method              : Time-based
GTK rekey time                : 86400 sec
GTK rekey client-offline      : Enabled
WPA3 status                   : Disabled
PPSK                          : Disabled
PPSK Fail Permit              : Enabled
User authentication mode      : MAC
Intrusion protection          : Disabled
Intrusion protection mode     : Temporary-block
Temporary block time          : 180 sec
Temporary service stop time   : 20 sec
Fail VLAN ID                  : Not configured
802.1X handshake              : Disabled
802.1X handshake secure       : Disabled
802.1X domain                 : Not configured
MAC-auth domain               : Not configured
Max 802.1X users per BSS      : 4096
```

```
Max MAC-auth users per BSS    : 4096
802.1X re-authenticate        : Disabled
Authorization fail mode       : Online
Accounting fail mode          : Online
Authorization                 : Permitted
Key derivation                : N/A
PMF status                    : Disabled
Hotspot policy number         : Not configured
Forwarding policy status      : Disabled
Forwarding policy name        : Not configured
Forwarder                     : AC
FT status                     : Disabled
QoS trust                     : Port
QoS priority                  : 0
BTM status                    : Disabled
```

1.10.4 802.1X AKM 設定例

I. ネットワーク要件

図 1-12に示すように、Switch は AP とクライアントに IP アドレスを割り当てるため、DHCP サーバとして動作します。

- ログイン名 abcdef、パスワード 123456 を使用して、クライアントがネットワークにアクセスできるように 802.1X 認証を設定します。
- AKM モードとして 802.1X を設定します。

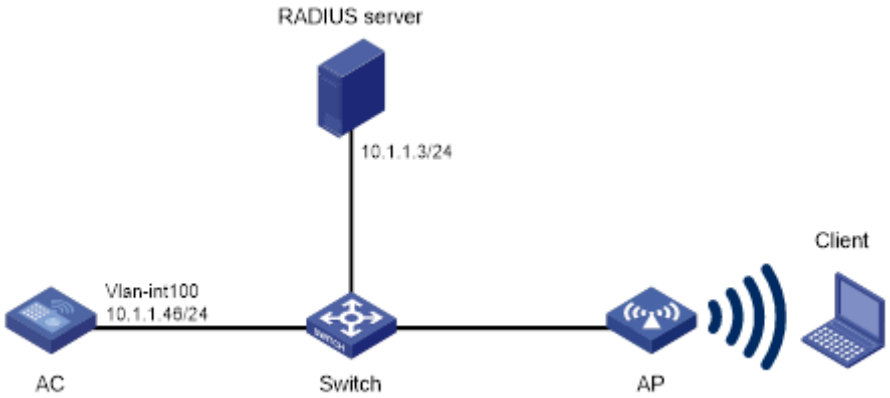


図 1-12 ネットワーク図

II. 設定手順

1) RADIUS サーバでユーザ名 abcdef、パスワード 123456 を設定し、RADIUS サーバと AC が互いに通信可能なことを確認します。（詳細は省略します。）
2) 802.1X クライアントを設定します。

```
<AC> system-view
[AC] dot1x
[AC] dot1x authentication-method eap
```

3) WLAN サービステンプレート service1 を作成します。

```
[AC] wlan service-template service1
```

4) サービステンプレートの SSID サービスを指定します。

```
[AC-wlan-st-service1] ssid service
```

5) サービステンプレート service1 の WLAN セキュリティを設定します。

AKM モードとして 802.1X を設定します。

```
[AC-wlan-st-service1] akm mode dot1x
```

暗号化方式に CCMP、暗号化規格に WPA を指定します。

```
[AC-wlan-st-service1] cipher-suite ccmp
[AC-wlan-st-service1] security-ie wpa
```

802.1X 認証モードを設定します。

```
[AC-wlan-st-service1] client-security authentication-mode dot1x
```

6) サービステンプレート service1 を有効にします。

```
[AC-wlan-st-service1] service-template enable
[AC-wlan-st-service1] quit
```

7) RADIUS スキームを設定します。

RADIUS スキーム radius1 を作成し、RADIUS scheme view に移行します。

```
[AC] radius scheme radius1
```

プライマリ認証サーバ、アカウンティングサーバを指定します。

```
[AC-radius-radius1] primary authentication 10.1.1.3 1812
[AC-radius-radius1] primary accounting 10.1.1.3 1813
```

プレーンテキストで認証サーバ、アカウンティングサーバの共有鍵 12345 を設定します。

```
[AC-radius-radius1] key authentication simple 12345
[AC-radius-radius1] key accounting simple 12345
```

RADIUS サーバの設定にもとづいて、RADIUS サーバにユーザ名を送信するように設定します。

- RADIUS サーバに送信するユーザ名からドメイン名を除外します。

```
[Device-radius-rs1] user-name-format without-domain
[Device-radius-rs1] quit
```

- RADIUS サーバに送信するユーザ名にドメイン名を含めます。

```
[Device-radius-rs1] user-name-format with-domain
[Device-radius-rs1] quit
```

8) ISP ドメイン dom1 を作成し、ISP ドメインの RADIUS スキームを設定します。

```
[AC] domain dom1
[AC-isp-dom1] authentication lan-access radius-scheme radius1
[AC-isp-dom1] authorization lan-access radius-scheme radius1
```

```
[AC-isp-dom1] accounting lan-access radius-scheme radius1
[AC-isp-dom1] quit
```

9) ISP ドメイン dom1 をデフォルトの ISP ドメインとして設定します。

```
[AC] domain default enable dom1
```

10) AP 名 ap1 の AP を作成し、モデル名、シリアル番号を指定します。

```
[AC] wlan ap ap1 model QX-W1110
[AC-wlan-ap-ap1] serial-id 219801A28N819CE0002T
```

11) サービステンプレート service1 を AP の radio 1 に割り当て、radio 1 を有効にします。

```
[AC-wlan-ap-ap1] radio 1
[AC-wlan-ap-ap1-radio-1] service-template service1
[AC-wlan-ap-ap1-radio-1] radio enable
[AC-wlan-ap-ap1-radio-1] return
```

🕮 メモ：

AAA、RADIUS コマンドの詳細は、QX-W2300AC シリーズアクセスコントローラコマンドマニュアルの“*13 ユーザアクセスと認証*“の”*3 章 AAA*“を参照してください。

III. 設定の確認

WLAN サービステンプレートが正常に設定されていることを確認するため、**display wlan service-template** コマンドを使用します。

```
<AC> display wlan service-template service1 verbose
Service template name         : service1
Description                   : Not configured
SSID                          : service
SSID-hide                     : Disabled
User-isolation                : Disabled
Service template status       : Enabled
Maximum clients per BSS       : 64
Frame format                  : Dot3
Seamless roam status          : Disabled
Seamless roam RSSI threshold : 50
Seamless roam RSSI gap        : 20
VLAN ID                       : 1
AKM mode                      : dot1x
Security IE                   : WPA
Cipher suite                  : CCMP
TKIP countermeasure time      : 0
PTK lifetime                  : 43200 sec
PTK rekey                     : Enabled
GTK rekey                     : Enabled
GTK rekey method              : Time-based
GTK rekey time                : 86400 sec
GTK rekey client-offline      : Enabled
WPA3 status                   : Disabled
PPSK                          : Disabled
PPSK Fail Permit              : Enabled
User authentication mode      : 802.1X
Intrusion protection          : Disabled
Intrusion protection mode     : Temporary-block
```

```
Temporary block time          : 180 sec
Temporary service stop time   : 20 sec
Fail VLAN ID                  : Not configured
802.1X handshake              : Disabled
802.1X handshake secure       : Disabled
802.1X domain                 : Not configured
MAC-auth domain               : Not configured
Max 802.1X users per BSS      : 4096
Max MAC-auth users per BSS    : 4096
802.1X re-authenticate        : Disabled
Authorization fail mode       : Online
Accounting fail mode          : Online
Authorization                 : Permitted
Key derivation                : N/A
PMF status                    : Disabled
Hotspot policy number         : Not configured
Forwarding policy status      : Disabled
Forwarding policy name        : Not configured
Forwarder                     : AC
FT status                     : Disabled
QoS trust                     : Port
QoS priority                  : 0
BTM status                    : Disabled
```

1.10.5 管理フレーム保護設定例

I. ネットワーク要件

図 1-13に示すように、Switch は AP とクライアントに IP アドレスを割り当てるため、DHCP サーバとして動作します。

- クライアントがネットワークにアクセスできるように PSK の鍵 12345678 を設定します。
- 暗号化規格に RSN、暗号化方式に CCMP を使用し、管理フレーム保護を設定します。

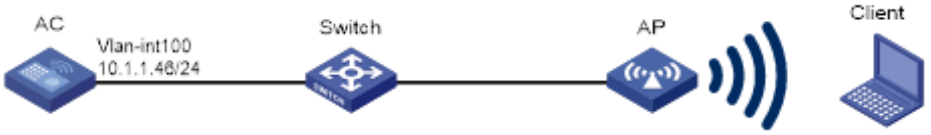


図 1-13 ネットワーク図

II. 設定手順

1) WLAN サービステンプレート service1 を作成します。

```
<AC> system-view
[AC] wlan service-template service1
```

2) サービステンプレートの SSID サービスを指定します。

```
[AC-wlan-st-service1] ssid service
```

3) 管理フレーム保護を設定します。

optional モードで管理フレーム保護を有効にします。

```
[AC-wlan-st-service1] pmf optional
```

KDF を sha1-and-sha256 に設定します。

```
[AC-wlan-st-service1] key-derivation sha1-and-sha256
```

4) RSNA メカニズムを設定します。

AKM モードとして PSK を設定し、プレーンテキストで鍵 12345678 を指定します。

```
[AC-wlan-st-service1] akm mode psk
[AC-wlan-st-service1] preshared-key pass-phrase simple 12345678
```

暗号化方式に CCMP、暗号化規格に RSN を指定します。

```
[AC-wlan-st-service1] cipher-suite ccmp
[AC-wlan-st-service1] security-ie rsn
```

5) サービステンプレート service1 を有効にします。

```
[AC-wlan-st-service1] service-template enable
[AC-wlan-st-service1] quit
```

6) AP 名 ap1 の AP を作成し、モデル名、シリアル番号を指定します。

```
[AC] wlan ap ap1 model QX-W1110
[AC-wlan-ap-ap1] serial-id 219801A28N819CE0002T
```

7) サービステンプレート service1 を AP の radio 1 に割り当て、radio 1 を有効にします。

```
[AC-wlan-ap-ap1] radio 1
[AC-wlan-ap-ap1-radio-1] service-template service1
[AC-wlan-ap-ap1-radio-1] radio enable
[AC-wlan-ap-ap1-radio-1] return
```

III. 設定の確認

WLAN サービステンプレートが正常に設定されていることを確認するため、**display wlan service-template** コマンドを使用します。

```
<AC> display wlan service-template service1 verbose
Service template name         : service1
Description                   : Not configured
SSID                          : service
SSID-hide                     : Disabled
User-isolation                : Disabled
Service template status       : Enabled
Maximum clients per BSS       : 64
Frame format                  : Dot3
Seamless roam status          : Disabled
Seamless roam RSSI threshold  : 50
Seamless roam RSSI gap        : 20
VLAN ID                       : 1
Customer Vlan                 : 4294967295
AKM mode                      : PSK
Security IE                   : RSN
Cipher suite                  : CCMP
TKIP countermeasure time      : 0
PTK lifetime                  : 43200 sec
PTK rekey                     : Enabled
GTK rekey                     : Enabled
GTK rekey method              : Time-based
```

```
GTK rekey time                : 86400 sec
GTK rekey client-offline      : Enabled
WPA3 status                   : Disabled
PPSK                          : Disabled
PPSK Fail Permit              : 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                  : Not configured
802.1X handshake              : Disabled
802.1X handshake secure       : Disabled
802.1X domain                 : Not configured
MAC-auth domain               : Not configured
Max 802.1X users per BSS      : 4096
Max MAC-auth users per BSS    : 4096
802.1X re-authenticate        : Disabled
Authorization fail mode       : Online
Accounting fail mode          : Online
Authorization                 : Permitted
Key derivation                : SHA1-AND-SHA256
PMF status                    : Optional
Hotspot policy number         : Not configured
Forwarding policy status      : Disabled
Forwarding policy name        : Not configured
Forwarder                     : AC
FT status                     : Disabled
QoS trust                     : Port
QoS priority                  : 0
BTM status                    : Disabled
```

802.11w クライアントがオンラインになったのち、管理フレーム保護の交換結果を確認するため、**display wlan client verbose** コマンドを使用します。

```
<AC> display wlan client verbose
Total number of clients: 1

MAC address                          : 5250-0012-0411
IPv4 address                         : 135.3.2.1
IPv6 address                         : N/A
Username                             : 11w
AID                                  : 1
AP ID                                : 1
AP name                              : ap1
Radio ID                             : 1
Channel                              : 36
SSID                                 : service
BSSID                                : 1111-2222-3333
VLAN ID                              : 1
Sleep count                          : 147
Power save mode                      : Active
Wireless mode                        : 802.11a
Channel bandwidth                    : 20MHz
SM power save                        : Disabled
Short GI for 20MHz                   : Not supported
Short GI for 40MHz                   : Not supported
STBC RX capability                   : Not supported
STBC TX capability                   : Not supported
LDPC RX capability                   : Not supported
Block Ack                            : TID 0  In
Support HT-MCS set                   : 0, 1, 2, 3, 4, 5, 6, 7,
                                       8, 9, 10, 11, 12, 13, 14,
                                       15
Supported rates                      : 1, 2, 5.5, 6, 9, 11,
                                       12, 18, 24, 36, 48, 54 Mbps
QoS mode                             : WMM
```

```
Listen interval                  : 10
RSSI                             : 46
Rx/Tx rate                       : 39/65
Authentication method            : Open system
Security mode                    : RSN
AKM mode                         : 802.1X
Cipher suite                     : CCMP
User authentication mode         : 802.1X
Authorization ACL ID             : N/A
Authorization user profile       : N/A
Roam status                      : N/A
Key derivation                   : SHA1
PMF status                       : Enabled
Forwarding policy name           : N/A
Online time                      : 0days 0hours 2minutes 56seconds
FT status                        : Inactive
BTM status                       : Disabled
```

1.10.6 ダイナミック WEP メカニズム設定例

I. ネットワーク要件

重要：

WEP は設定した暗号化キーが固定であり、解読される危険性があるため、よりセキュリティ強度の高い AES の利用を推奨します。

図 1-14に示すように、Switch は AP とクライアントに IP アドレスを割り当てるため、DHCP サーバとして動作します。

- ログイン名 abcdef、パスワード 123456 を使用して、クライアントがネットワークにアクセスできるように 802.1X 認証を設定します。
- ダイナミック WEP メカニズムを設定します。

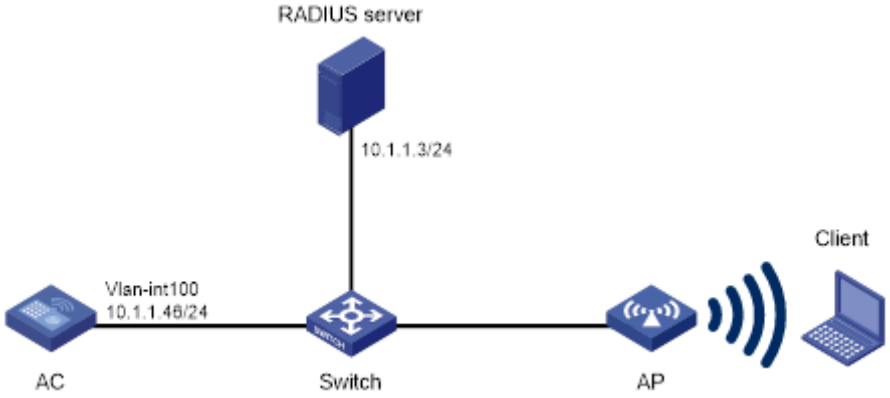


図 1-14 ネットワーク図

II. 設定手順

1) RADIUS サーバでユーザ名 abcdef、パスワード 123456 を設定し、RADIUS サーバと AC が互いに通信可能なことを確認します。（詳細は省略します。）
2) 802.1X クライアントを設定します。（詳細は省略します。）
3) WLAN サービステンプレート service1 を作成します。

```
<AC> system-view
[AC] wlan service-template service1
```

4) サービステンプレートの SSID サービスを指定します。

```
[AC-wlan-st-service1] ssid service
```

5) ダイナミック WEP メカニズムを有効にします。

```
[AC-wlan-st-service1] wep mode dynamic
```

6) 802.1X 認証モードを設定します。

```
[AC-wlan-st-service1] client-security authentication-mode dot1x
```

7) サービステンプレート service1 を有効にします。

```
[AC-wlan-st-service1] service-template enable
[AC-wlan-st-service1] quit
```

8) RADIUS スキームを設定します。

RADIUS スキーム radius1 を作成し、RADIUS scheme view に移行します。

```
[AC] radius scheme radius1
```

プライマリ認証サーバ、アカウンティングサーバを指定します。

```
[AC-radius-radius1] primary authentication 10.1.1.3 1812
[AC-radius-radius1] primary accounting 10.1.1.3 1813
```

プレーンテキストで認証サーバ、アカウンティングサーバの共有鍵 12345 を設定します。

```
[AC-radius-radius1] key authentication simple 12345
[AC-radius-radius1] key accounting simple 12345
```

RADIUS サーバの設定にもとづいて、RADIUS サーバにユーザ名を送信するように設定します。

- RADIUS サーバに送信するユーザ名からドメイン名を除外します。

```
[Device-radius-rs1] user-name-format without-domain
[Device-radius-rs1] quit
```

- RADIUS サーバに送信するユーザ名にドメイン名を含めます。

```
[Device-radius-rs1] user-name-format with-domain
[Device-radius-rs1] quit
```

9) ISP ドメイン dom1 を作成し、ISP ドメインの RADIUS スキームを設定します。

```
[AC] domain dom1
[AC-isp-dom1] authentication lan-access radius-scheme radius1
[AC-isp-dom1] authorization lan-access radius-scheme radius1
[AC-isp-dom1] accounting lan-access radius-scheme radius1
```

```
[AC-isp-dom1] quit
```

10) ISP ドメイン dom1 をデフォルトの ISP ドメインとして設定します。

```
[AC] domain default enable dom1
```

11) AP 名 ap1 の AP を作成し、モデル名、シリアル番号を指定します。

```
[AC] wlan ap ap1 model QX-W1110
[AC-wlan-ap-ap1] serial-id 219801A28N819CE0002T
```

12) サービステンプレート service1 を AP の radio 1 に割り当て、radio 1 を有効にします。

```
[AC-wlan-ap-ap1] radio 1
[AC-wlan-ap-ap1-radio-1] service-template service1
[AC-wlan-ap-ap1-radio-1] radio enable
[AC-wlan-ap-ap1-radio-1] return
```

🕮 メモ：

AAA、RADIUS コマンドの詳細は、QX-W2300AC シリーズアクセスコントローラコマンドマニュアルの“*13 ユーザアクセスと認証*“の”*3 章 AAA*“を参照してください。

III. 設定の確認

WLAN サービステンプレートが正常に設定されていることを確認するため、**display wlan service-template** コマンドを使用します。

```
<AC> display wlan service-template service1 verbose
Service template name          : service1
Description                    : Not configured
SSID                           : service
SSID-hide                      : Disabled
User-isolation                 : Disabled
Service template status        : Enabled
Maximum clients per BSS        : 64
Frame format                   : Dot3
Seamless roam status           : Disabled
Seamless roam RSSI threshold   : 50
Seamless roam RSSI gap         : 20
VLAN ID                        : 1
AKM mode                       : Not configured
Security IE                    : Not configured
Cipher suite                   : WEP104
WEP key ID                     : 1
TKIP countermeasure time       : 0
PTK lifetime                   : 43200 sec
PTK rekey                      : Enabled
GTK rekey                      : Enabled
GTK rekey method               : Time-based
GTK rekey time                 : 86400 sec
GTK rekey client-offline       : Enabled
WPA3 status                    : Disabled
PPSK                           : Disabled
PPSK Fail Permit               : Enabled
User authentication mode       : 802.1X
Intrusion protection           : Disabled
Intrusion protection mode      : Temporary-block
Temporary block time           : 180 sec
```

```
Temporary service stop time  : 20 sec
Fail VLAN ID                 : Not configured
802.1X handshake             : Disabled
802.1X handshake secure      : Disabled
802.1X domain                : Not configured
MAC-auth domain              : Not configured
Max 802.1X users per BSS     : 4096
Max MAC-auth users per BSS   : 4096
802.1X re-authenticate       : Disabled
Authorization fail mode      : Online
Accounting fail mode         : Online
Authorization                : Permitted
Key derivation               : N/A
PMF status                   : Disabled
Hotspot policy number        : Not configured
Forwarding policy status     : Disabled
Forwarding policy name       : Not configured
Forwarder                    : AC
FT status                    : Disabled
QoS trust                    : Port
QoS priority                 : 0
BTM status                   : Disabled
```

1.10.7 WPA3 エンタープライズ(192bit セキュリティなし)設定例

I. ネットワーク要件

図 1-16に示すようにSwitchはAPとクライアントにIPアドレスを割り当てるため、DHCPサーバとして動作します。

- WPA 3 エンタープライズを 192bit セキュリティなしで使用するために管理フレーム保護を設定します。
- ネットワークにアクセスするため、クライアントは共有鍵 12345678 を使用します。

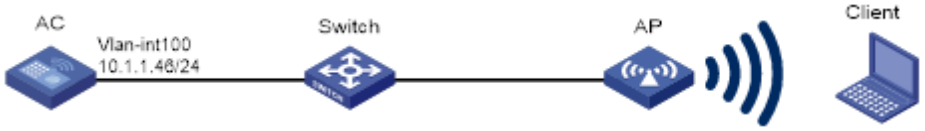


図 1-15 ネットワーク図

II. 設定手順

1) サービステンプレート service1 を作成します。

```
<AC> system-view
[AC] wlan service-template service1
```

2) サービステンプレートの SSID サービスを指定します。

```
[AC-wlan-st-service1] ssid wpa3_test
```

3) サービステンプレート service1 の WLAN セキュリティを設定します。

AKM モードとして 802.1X を設定します。

```
[AC-wlan-st-service1] akm mode dot1x
```

暗号化方式に CCMP、暗号化規格に RSN を指定します。

```
[AC-wlan-st-service1] cipher-suite ccmp
[AC-wlan-st-service1] security-ie rsn
```

802.1X 認証モードを設定します。

```
[AC-wlan-st-service1] client-security authentication-mode dot1x
```

802.1X 認証ドメインとして dom1 を設定します。

```
[AC-wlan-st-service1] dot1x domain dom1
```

4) 管理フレーム保護(192bit セキュリティなし WPA3 エンタープライズ)を設定します。

```
[AC-wlan-st-service1] pmf mandatory
```

KDF を sha1-and-sha256 に設定します。

```
[AC-wlan-st-service1] key-derivation sha1-and-sha256
```

5) サービステンプレート service1 を有効にします。

```
[AC-wlan-st-service1] service-template enable
[AC-wlan-st-service1] quit
```

6) RADIUS スキームを設定します。

RADIUS スキーム radius1 を作成し、RADIUS scheme view に移行します。

```
[AC] radius scheme radius1
```

プライマリ認証サーバ、アカウンティングサーバを指定します。

```
[AC-radius-radius1] primary authentication 10.1.1.3 1812
[AC-radius-radius1] primary accounting 10.1.1.3 1813
```

プレーンテキストで認証サーバ、アカウンティングサーバの共有鍵 12345 を設定します。

```
[AC-radius-radius1] key authentication simple 12345
[AC-radius-radius1] key accounting simple 12345
```

RADIUS サーバの設定にもとづいて、RADIUS サーバにユーザ名を送信するように設定します。

- RADIUS サーバに送信するユーザ名からドメイン名を除外します。

```
[Device-radius-rs1] user-name-format without-domain
[Device-radius-rs1] quit
```

- RADIUS サーバに送信するユーザ名にドメイン名を含めます。

```
[Device-radius-rs1] user-name-format with-domain
[Device-radius-rs1] quit
```

7) ISP ドメイン dom1 を作成し、ISP ドメインの RADIUS スキームを設定します。

```
[AC] domain dom1
[AC-isp-dom1] authentication lan-access radius-scheme radius1
[AC-isp-dom1] authorization lan-access radius-scheme radius1
[AC-isp-dom1] accounting lan-access radius-scheme radius1
[AC-isp-dom1] quit
```

8) AP 名 ap1 の AP を作成し、モデル名、シリアル番号を指定します。

```
[AC] wlan ap ap1 model QX-W1020
[AC-wlan-ap-ap1] serial-id 219801A0CNC138011454
```

9) サービステンプレート service1 を AP の radio 1 に割り当て、radio 1 を有効にします。

```
[AC-wlan-ap-ap1] radio 1
[AC-wlan-ap-ap1-radio-1] service-template service1
[AC-wlan-ap-ap1-radio-1] radio enable
[AC-wlan-ap-ap1-radio-1] return
```

III. 設定の確認

 # display wlan service-template verbose コマンドを使用します。

```
<AC>dis wlan service-template service1 verbose
Service template name                                : service1
Description                                          : Not configured
SSID                                                 : wpa3_test
SSID-hide                                            : Disabled
User-isolation                                       : Disabled
Service template status                              : Enabled
Maximum clients per BSS                              : Not configured
VLAN ID                                              : 1
Customer Vlan                                        : 4294967295
AKM mode                                             : PSK
Security IE                                          : RSN
Cipher suite                                         : CCMP
TKIP countermeasure time                             : 0 sec
PTK lifetime                                         : 43200 sec
PTK rekey                                            : Enabled
GTK rekey                                            : Enabled
GTK rekey method                                     : Time-based
GTK rekey time                                       : 86400 sec
GTK rekey client-offline                             : Disabled
WPA3 status                                          : Disabled
Enhance-open status                                  : Disabled
Enhanced-open transition-mode service-template       : N/A
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                                         : Not configured
802.1X handshake                                     : Disabled
802.1X handshake secure                              : Disabled
802.1X domain                                        : Not configured
MAC-auth domain                                      : Not configured
Max 802.1X users per BSS                             : 512
Max MAC-auth users per BSS                           : 512
802.1X re-authenticate                               : Disabled
Authorization fail mode                              : Online
Accounting fail mode                                 : Online
Authorization                                        : Permitted
Key derivation                                       : SHA1
PMF status                                           : Mandatory
Hotspot policy number                                : Not configured
Forwarding policy status                             : Disabled
Forwarding policy name                               : Not configured
Forwarder                                            : AP
FT status                                            : Disabled
QoS trust                                            : Port
```

```
QoS priority                                : 0
```

1.10.8 WPA3 パーソナル設定例

I. ネットワーク要件

図 1-16に示すようにSwitchはAPとクライアントにIPアドレスを割り当てるため、DHCPサーバとして動作します。

- WPA3 を設定します。
- ネットワークにアクセスするため、クライアントは共有鍵 12345678 を使用します。

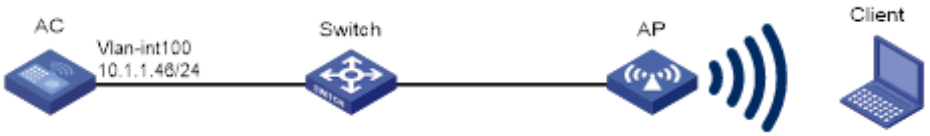


図 1-16 ネットワーク図

II. 設定手順

1) サービステンプレート service1 を作成します。

```
<AC> system-view
[AC] wlan service-template service1
```

2) サービステンプレートの SSID サービスを指定します。

```
[AC-wlan-st-service1] ssid wpa3_test
```

3) サービステンプレート service1 の WLAN セキュリティを設定します。

AKM モードとして PSK を設定し、プレーンテキストで共有鍵 12345678 を指定します。

```
[AC-wlan-st-service1] akm mode psk
[AC-wlan-st-service1] preshared-key pass-phrase simple 12345678
```

暗号化方式に CCMP、暗号化規格に RSN を指定します。

```
[AC-wlan-st-service1] cipher-suite ccmp
[AC-wlan-st-service1] security-ie rsn
```

4) WPA3 の設定を personal に設定し、WPA3 セキュリティモードを optional に設定します。

```
[AC-wlan-st-service1] wpa3 personal optional
```

5) 管理フレーム保護を設定します。

optional モードで管理フレーム保護を有効にします。

```
[AC-wlan-st-service1] pmf optional
```

KDF を sha1-and-sha256 に設定します。

```
[AC-wlan-st-service1] key-derivation sha1-and-sha256
```

6) サービステンプレート service1 を有効にします。

```
[AC-wlan-st-service1] service-template enable
[AC-wlan-st-service1] quit
```

7) AP 名 ap1 の AP を作成し、モデル名、シリアル番号を指定します。

```
[AC] wlan ap ap1 model QX-W1020
[AC-wlan-ap-ap1] serial-id 219801A0CNC138011454
```

8) サービステンプレート service1 を AP の radio 1 に割り当て、radio 1 を有効にします。

```
[AC-wlan-ap-ap1] radio 1
[AC-wlan-ap-ap1-radio-1] service-template service1
[AC-wlan-ap-ap1-radio-1] radio enable
[AC-wlan-ap-ap1-radio-1] return
```

III. 設定の確認

クライアントが APに接続されていることを確認するため、**display wlan client verbose** コマンドを使用します。

```
<AC> display wlan client verbose
Total number of clients: 1

 MAC address                          : 88e8-7fec-c042
 IPv4 address                         : 192.168.1.140
 IPv6 address                         : N/A
 Username                             : N/A
 AID                                  : 1
 AP ID                                : 2
 AP name                              : test1
 Radio ID                             : 1
 SSID                                 : wpa3_test
 BSSID                                : 9ce8-9525-f192
 VLAN ID                              : 1
 Sleep count                          : 0
 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                   : Not supported
 STBC TX capability                   : Not supported
 LDPC RX capability                   : Supported
 Beamformee STS capability            : 2
 Number of Sounding Dimensions        : 1
 SU beamformee capability             : 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                      : 20
 RSSI                                 : 0
 Rx/Tx rate                           : 0/0 Mbps
```

```
Speed                              : N/A
Authentication method              : Open system
Security mode                      : RSN
AKM mode                           : PSK
Cipher suite                       : CCMP
User authentication mode           : Bypass
WPA3 status                        : Enabled
Authorization CAR                  : N/A
Authorization ACL ID               : N/A
Authorization user profile         : N/A
Roam status                        : N/A
Key derivation                     : SHA256
PMF status                         : Enabled
Forwarding policy name             : Not configured
Online time                        : 0days 0hours 0minutes 4seconds
FT status                          : Inactive
```

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 概要 2-1
2.2 攻撃検出 2-1
2.2.1 フラッドアタックの検出 2-1
2.2.2 不正パケットの検出 2-2
2.2.3 なりすまし攻撃の検出 2-4
2.2.4 Weak IVの検出 2-5
2.2.5 Omerta攻撃の検出 2-5
2.2.6 ブロードキャストアソシエーション解除/認証取り消し攻撃の検出 2-5
2.2.7 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 2-5
2.2.8 パワーセーブ攻撃の検出 2-5
2.2.9 禁止チャネルの検出 2-6
2.2.10 ソフトAPの検出 2-6
2.2.11 Windowsブリッジの検出 2-6
2.2.12 未暗号化装置の検出 2-6
2.2.13 ホットスポット攻撃の検出 2-6
2.2.14 APなりすまし攻撃の検出 2-6
2.2.15 HT-グリーンフィールドAPの検出 2-7
2.2.16 ハニーポットAPの検出 2-7
2.2.17 MITM攻撃の検出 2-7
2.2.18 無線ブリッジの検出 2-7
2.2.19 アソシエーション/再アソシエーションDoS攻撃の検出 2-7
2.2.20 APフラッド攻撃の検出 2-8
2.2.21 装置エントリ攻撃の検出 2-8
2.3 シグネチャにもとづいたユーザ定義の攻撃の検出 2-8
2.4 装置の種別 2-8
2.4.1 APの種別 2-8
2.4.2 クライアント種別 2-12
2.5 対策 2-13
2.6 WIPS設定作業リスト 2-13
2.7 WIPS有効化 2-14
2.7.1 radio viewでのWIPSの有効化 2-15
2.7.2 AP group radio viewでのWIPSの有効化 2-15
2.8 無線攻撃検出の設定 2-15
2.8.1 フラッド攻撃検出の設定 2-15
2.8.2 不正パケット検出の設定 2-16
2.8.3 装置エントリ攻撃検出の設定 2-17
2.8.4 その他の攻撃に対する検出設定 2-18
2.8.5 RSSIにもとづいた無線装置検出の設定 2-20
2.8.6 WIPSに関連付けられていないクライアント検出の有効化 2-20
2.8.7 攻撃検知ポリシーの適用 2-20
2.9 シグネチャにもとづいた攻撃検出の設定 2-21
2.9.1 シグネチャ設定 2-21
2.9.2 シグネチャポリシーの設定 2-22

2.9.3 シグネチャポリシーの適用 2-22
2.10 装置種別の設定 2-22
2.10.1 分類ポリシーの設定 2-22
2.10.2 手動AP分類ポリシーの設定 2-24
2.10.3 分類ポリシーの適用 2-24
2.11 対策の設定 2-25
2.11.1 対策ポリシーの設定 2-25
2.11.2 対策ポリシーの適用 2-26
2.12 アラーム無視装置リストの設定 2-27
2.13 OUIの設定 2-27
2.14 WIPSの表示と維持 2-27
2.15 WIPS設定例 2-28
2.15.1 装置の分類の設定例 2-28
2.15.2 不正パケットとフラッド攻撃の検出例 2-31
2.15.3 シグネチャベースのユーザ定義攻撃検出設定例 2-35

2章 WIPS

2.1 概要

無線侵入防止システム（WIPS）は、802.11 プロトコルに対応したレイヤ 2 プロトコルの検出および防御機能です。

WIPS はチャネルを監視し、分析データを処理することで、ネットワークの安全性を脅かす行為、サービスを妨害する行為、または性能に影響を与える無線機器や動作を検出します。さらに、不正な無線機器に対する対抗措置を提供し、無線ネットワークに包括的なセキュリティ対策を提供します。

WIPS は、センサと AC で構成されます。WIPS は以下の機能を提供します。

- WIPS 機能を有効にした AP をセンサと呼び。センサは無線チャネルを監視し、収集した情報を簡易処理した後、AC へ送信して総合分析を行います。
- AC は攻撃元を分析し、対抗措置を実施するとともに、ログを出力します。

2.2 攻撃検出

WIPS は、無線区間の 802.11 フレームを解析して攻撃を検出し、通知します。

2.2.1 フラッドアタックの検出

AP が、短期間に同じタイプのフレームを多数受信した場合、フラッドアタック攻撃を受けている可能性があります。AP の機能不全を防止するため、WIPS は周期的に受信パケット統計を調査し、フラッドアタックが疑われる場合には、アラームを発生します。WIPS は、以下のフラッドアタックを検出することができます。

- **認証要求フラッドアタック**

多数のクライアントの認証要求を模倣することにより、AP の認証テーブルは、容量をオーバーします。

- **プローブ要求/アソシエーション要求/再アソシエーション要求フラッドアタック**

多数のクライアントのプローブ要求/アソシエーション要求/再アソシエーション要求を模倣することにより、AP のアソシエーションテーブルは、容量をオーバーします。

- **EAPOL-Start フラッドアタック**

多数のクライアントの IEEE802.1X で定義された EAPOL-start フレームを模倣することにより、AP のリソースを消費します。

- **ブロードキャスト/ユニキャスト認証取り消し（Deauthentication）フラッドアタック**

クライアントは、AP からのなりすまし認証取り消し（Deauthentication）フレームを受信すると、AP への接続を切断します。この攻撃で、急速に複数のクライアントの無線サービスを終わらせることができます。

- **ブロードキャスト/ユニキャスト アソシエーション解除フラッドアタック**

クライアントは、AP からのなりすましアソシエーション解除フレームを受信すると、AP への接続を切断します。この攻撃により、複数クライアントの無線サービスが急速に終了させられる恐れがあります。

- **RTS/CTS フラッドアタック**

大量の RTS/CTS フレームで RF 帯域を予約し、RF 帯域を共有する他の無線装置が送信を抑止するように強制します。この攻撃はバーチャルなキャリアメカニズムの脆弱性を利用します。

- **ブロック ACK フラッドアタック**

大量のブロック ACK フレームにより、ブロック ACK 動作を中断させます。

- **ヌルデータ フラッドアタック**

なりすましのヌルデータをクライアントから AP に送信します。AP は、クライアントがパワーセーブモードであると判断し、クライアントのためにフレームをバッファ処理します。バッファ処理されたフレームの保存時間が期限切れになった場合、AP はフレームを廃棄します。これにより、クライアントと AP との通信が中断されます。

- **ビーコン フラッドアタック**

多数の擬似 AP を模倣するビーコンフレームは、クライアントの関連付けを中断させます。

- **EAPOL-logoff フラッドアタック**

IEEE802.1X 標準は、LAN（EAPOL）上で拡張認証プロトコルを使って、認証プロトコルを定義します。クライアントは、APによってセッションを終わらせるためにEAPOL-logoffフレームを送る必要があります。EAPOL-logoff フレームは認証されておらず、攻撃者は、クライアントを分離するために EAPOL-logoff フレームを偽ることができます。

- **EAP-success/failure フラッドアタック**

802.1X 認証を使用している WLAN において、認証成功/失敗を通知するために、AP は EAP-success/EAP-failure フレームをクライアントに送信します。攻撃者は、認証プロセスを混乱させるために、AP の MAC アドレスに偽装した EAP-success/EAP-failure フレームをクライアントに送ることができます。

2.2.2 不正パケットの検出

WIPS は、フレームが表 2-1示した条件と一致している場合、不正フレームと判定し、アラームとログを発生します。WIPS は 16 種類の不正パケットを検出することができます。

表 2-1 不正フレーム条件

検出タイプ	適用フレーム	一致条件
無効なIE長検出	全管理フレーム	IE長が802.11プロトコルに準拠していません。
重複IE検出	全管理フレーム	重複IE。このタイプの検出はベンダで定義されたIEに適用可能ではありません。
冗長IE検出	全管理フレーム	IEはフレームに必要なIEではなく、予約されたIEでもありません。
無効パケット長検出	全管理フレーム	パケットペイロードが解決された後の残IE長は、ゼロではありません。

検出タイプ	適用フレーム	一致条件
異常なIBSSとESS設定検出	• ビーコンフレーム • プローブ応答フレーム	IBSSとESSの両方が1に設定されています。
不正な認証要求フレーム検出	認証要求フレーム	• 認証アルゴリズム番号が802.11プロトコルに対応せず、3より大きいです。 • 認証トランザクションシーケンス番号は0です。 • 認証トランザクションシーケンス番号が1で且つ、ステータスコードが0ではありません。 • 認証トランザクションシーケンス番号が4より大きいです。
不正なアソシエーション要求フレーム検出	アソシエーション要求フレーム	フレーム長が0です。
不正なHT IE検出	• ビーコンフレーム • プローブ応答フレーム • アソシエーション応答フレーム • 再アソシエーション要求フレーム	• HT capabilities IEのSMパワーセーブ値が2です。 • HT capabilities IEの二次チャネルオフセット値が2です。
継続時間超過検出	• 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, CTS, ACK フレーム	パケットの継続時間の値が指定したしきい値を超えています。
不正なプローブ応答フレーム検出	プローブ応答フレーム	フレームはメッシュフレームではなく、そのSSID長が0です。
無効な認証取り消し（Deauthentication）コード検出	認証取り消し（Deauthentication） フレーム	理由コードが0、または、67～65535の範囲内にあります。
無効なアソシエーション解除コード検出	アソシエーション解除フレーム	理由コードが0、または、67～65535の範囲内にあります。
SSIDデータ長超過検出	• 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 • アソシエーション要求フレーム	SSIDデータ長が32より大きいです。
FATA-Jack 検出	認証フレーム	認証アルゴリズム番号が2です。

検出タイプ	適用フレーム	一致条件
無効ソースアドレス検出	全管理フレーム	• TO DSは1であり、フレームがクライアントによってAPに送信されたことを示しています。 • フレームのソースMACアドレスが、マルチキャストまたはブロードキャストアドレスです。
EAPOL key長超過検出	EAPOL-Keyフレーム	TO DSが1、かつ、キー長が0より大きいです。

2.2.3 なりすまし攻撃の検出

なりすまし攻撃では、攻撃者はネットワークを脅かすために別の装置になりすましてフレームを送ります。WIPS は以下のなりすまし攻撃の検出をサポートします。

- **フレームなりすまし**

偽 AP は、許可された AP になりすまして、ビーコン、または、プローブ応答フレームを送信し、クライアントが偽 AP に参加するよう誘導します。

- **AP MAC アドレスなりすまし**

許可された AP になりすましたクライアントは、認証取り消し（Deauthentication）、または、アソシエーション解除フレームを他のクライアントに送ります。

これにより、クライアントがオフラインになり、WLAN の正常な動作に影響を与える可能性があります。

- **クライアント MAC アドレスなりすまし**

偽 AP は、許可されたクライアントになりしまし、許可された AP に参加することができます。

I. フレームなりすまし攻撃の検出

WIPS は、フレーム受信時刻とタイムスタンプを使用して AP の起動時間を計算します。計算された AP の起動時間が WIPS に記録された起動時間と異なる場合、WIPS は、なりすまし攻撃であると判断します。

II. AP MAC アドレスなりすまし攻撃の検出

WIPS は、送信側の MAC アドレスを調査します。送信側の MAC アドレスが、すでに AP MAC アドレステーブルに存在している場合、WIPS は、なりすまし攻撃であると判断します。

III. クライアント MAC アドレスなりすまし攻撃の検出

WIPS は、送信側の MAC アドレスを調査します。送信側の MAC アドレスが、すでにクライアント MAC アドレステーブルに存在している場合、WIPS は、なりすまし攻撃であると判断します。

2.2.4 Weak IV の検出

WEP セキュリティプロトコルで使用されている RC4 暗号化アルゴリズムで特定の IV を使用する場合、WEP キーがクラックされる可能性が高くなります。この特定の IV を Weak IV といいます。WIPS は、各 WEP パケットの IV を検出することで、この種の攻撃を防ぎます。

2.2.5 Omerta 攻撃の検出

Omerta は 802.11 のプロトコルをベースにした DoS 攻撃ツールです。このツールは、クライアントを分離するために、理由コード 0x01 のアソシエーション解除フレームを送信します。理由コード 0x01 は、未知の分離理由です。WIPS は、各アソシエーション解除フレームの理由コードを検出することによって、Omerta 攻撃を検出します。

2.2.6 ブロードキャストアソシエーション解除/認証取り消し攻撃の検出

攻撃者は、全クライアントを正当な AP からログオフさせるためのブロードキャスト アソシエーション解除/認証取り消し（Deauthentication）フレームを送信するために、正当な AP になりすまします。

2.2.7 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

複数の帯域幅を使用できるラジオにおいて、40MHz 帯域幅モードを使用禁止(40Mhz チャネル幅非互換)のクライアントが接続されて通信をしている場合、そのクライアントの通信が完了するまで、同じラジオに接続されている他のクライアントは通信を開始できず、ネットワークスループットと効率に影響を与えます。

WIPS は、クライアントが送信するプローブ要求フレームを検出することによって、そのようなクライアントを検出します。

2.2.8 パワーセーブ攻撃の検出

攻撃者は、クライアントの MAC アドレスになりすまして、パワーセーブのフレームを AP に送信します。AP はクライアントのフレームをキャッシュします。攻撃を受けたクライアントは、パワーセーブモードであると AP に判断されているため、データフレームを受信できません。キャッシングされたフレームのエージングタイマが満了すると、AP はフレームを破棄してしまいます。WIPS は、パワーセーブ ON フレームとパワーセーブ OFF フレームの比率を決定することでパワーセーブ攻撃を検出します。

2.2.9 禁止チャネルの検出

許可チャネルリストを設定し、禁止チャネル検出を有効にすると、WIPS は許可チャネルリストにないチャネルを禁止チャネルであると判断します。

2.2.10 ソフト AP の検出

ソフト AP とは、AP として機能し、無線サービスを提供するクライアントを指します。攻撃者は、ソフト AP を介して内部ネットワークにアクセスし、さらに攻撃を開始することができます。WIPS は、装置がクライアントと AP 間の役割を切り替える間隔を検出することにより、ソフト AP を検出します。WIPS は、接続していないクライアントのソフト AP 検出を実行しません。

2.2.11 Windows ブリッジの検出

有線ネットワークに接続された無線クライアントが有線 NIC を介して Windows ブリッジを確立すると、クライアントは外部 AP を内部ネットワークとブリッジすることができます。これにより、内部ネットワークにセキュリティ上の問題が発生する可能性があります。WIPS は、接続したクライアントから送信されるデータフレームを分析して、Windows ブリッジを検出します。

2.2.12 未暗号化装置の検出

暗号化していないフレームを送信する認証 AP またはクライアントは、セキュリティ問題をネットワークにもたらす可能性があります。WIPS は、認証 AP またはクライアントから送信されたフレームを分析することによって、暗号化していない装置を検出します。

2.2.13 ホットスポット攻撃の検出

攻撃者は、ホットスポットと同じ SSID を持つ不正な AP を設定して、クライアントが接続するよう誘導します。クライアントが不正な AP に接続した場合、攻撃者はクライアント情報を取得するためにさらに攻撃を開始します。

WIPS がホットスポット攻撃を検出できるように、ホットスポット情報を設定できます。

2.2.14 AP なりすまし攻撃の検出

AP なりすまし攻撃では、正規 AP と同じ BSSID と ESSID を持つ悪意のある AP に、クライアントを接続するように誘導します。次に、このなりすまし AP は、ホットスポット攻撃を開始するか、検出システムをだまします。

WIPS は、AP が送信するビーコンフレーム間隔を検出することによって、AP なりすまし攻撃を検出します。

2.2.15 HT-グリーンフィールド AP の検出

HT-グリーンフィールドモードで動作する AP は、802.11a/b/g 装置と通信できないため、衝突、エラー、再送信を引き起こす可能性があります。 WIPS は、AP によって送信されたビーコンフレームまたはプローブ応答フレームを分析することによって HT-グリーンフィールド AP を検出します。

2.2.16 ハニーポット AP の検出

ハニーポット AP 攻撃では、攻撃者は悪意のある AP を設定してクライアントが接続するよう誘導します。 悪意のある AP の SSID は、正規 AP の SSID に似ています。 クライアントがハニーポット AP に接続した場合、ハニーポット AP は、ポートスキャンや偽認証などのさらなる攻撃を開始して、クライアント情報を取得します。

WIPS は外部 AP の SSID を検出してハニーポット AP を検出します。外部 AP の SSID と正規 AP の SSID との類似性が指定されたしきい値に達すると、WIPS はアラームを発生します。

2.2.17 MITM 攻撃の検出

MITM 攻撃では、攻撃者は不正 AP を設定し、クライアントが接続するように誘導します。次に、不正 AP は、許可 AP に接続するクライアントの MAC アドレスになりすまします。クライアントと認可 AP が通信するとき、不正 AP はクライアントと認可 AP の両方からパケットをキャプチャします。不正 AP はフレームを修正し、フレーム情報を取得する可能性があります。 WIPS は、許可 AP から切り離され、ハニーポット AP に接続したクライアントを検出することによって、MITM 攻撃を検出します。

2.2.18 無線ブリッジの検出

攻撃者は、無線ブリッジを経由して、内部のネットワークに侵入するかもしれません。WIPS は、無線ブリッジを検出するとアラームを発生します。無線ブリッジがメッシュネットワークにある場合、WIPS はメッシュリンクを記録します。

2.2.19 アソシエーション/再アソシエーション DoS 攻撃の検出

アソシエーション/再アソシエーション DoS 攻撃では、多くのクライアントになりすましたアソシエーション要求を AP に送信することにより、AP のアソシエーションテーブル

をオーバーさせます。テーブル登録が上限に達すると、AP は正規のクライアントの要求を処理することができません。

2.2.20 AP フラッド攻撃の検出

WIPS は WLAN 内の AP 数を検出し、AP 数が指定したしきい値を超えた場合、AP フラッド攻撃のアラームを発生します。

2.2.21 装置エントリ攻撃の検出

攻撃者は、無効なパケットを WIPS に送信して処理コストを増加させることができます。WIPS は学習された装置エントリを定期的に調べ、装置エントリの学習を制限するかどうかを決定します。指定した間隔内に学習された AP またはクライアントエントリの数がしきい値を超えると、WIPS はアラームを発生して新しいエントリの学習を停止します。

2.3 シグネチャにもとづいたユーザ定義の攻撃の検出

WIPS は、シグネチャにもとづいたユーザ定義の攻撃検出を提供します。シグネチャには、パケットの識別方法と、一致するパケットを取得するアクションが含まれています。センサは、検出されたパケットをシグネチャと照合し、パケットがシグネチャと一致した場合、シグネチャで定義されたアクションを実行します。

シグネチャには、フレームタイプ、MAC アドレス、シリアル ID、SSID 長、SSID、フレームパターンにもとづいて定義できる最大 6 つのサブシグネチャを含めることができます。 パケットは、シグネチャ内のすべてのサブシグネチャと一致する場合にのみ、シグネチャと一致したことになります。

2.4 装置の種別

2.4.1 AP の種別

表 2-2に示すように、WIPS はあらかじめ決められた分類ポリシーに応じて、検出された AP を分類します。

表 2-2 AP の種別

種別	説明	分類ルール
許可されたAP	WLANで許可されているAP	• 許可APとして設定されています • 許可APリストに該当します • 許可APとしてユーザ定義のAP分類ルールによって分類されます • 無線サービスを提供し、禁止装置リストに該当しません
不正AP	WLANで使用できないAP	• 禁止装置リストに該当します • OUIコンフィグファイルには該当しません。 • 不正APとして設定されています • ユーザ定義のAP分類ルールによって不正APに分類されます
設定ミスのAP	WLANで使用できるが誤ったコンフィグのAP	• 設定が誤っているAPとして設定されています • ユーザ定義のAP分類ルールによって誤って設定されたAPとして分類されます
外部AP	隣接するWLANにあるAP	• 外部APとして設定されています • ユーザ定義のAP分類ルールによって外部APとして分類されます
アドホック	アドホックモードで動作するAP。 WIPSはビーコンフレームを確認してアドホックAPを検出します。	–
メッシュAP	WLANメッシュネットワーク内のAP	WIPSはビーコンフレームを通じてメッシュAPを識別します。
潜在的な不正AP	不正APであると考えられるAP。	ワイヤレス設定が間違っていて、次のいずれのリストにも記載されていません。 • 許可装置リスト。 • 禁止装置リスト。 • 信頼できるOUIリスト。 APの有線ポートがネットワークに接続されている場合、APは不正APです。

種別	説明	分類ルール
潜在的外部AP	外部APの可能性があるAP。	● ワイヤレスサービスの設定が間違っています。 ● 有線ポートがネットワークに接続されていません。 ● 次のリストには含まれていません。 1. 許可装置リスト。 2. 禁止装置リスト。 3. 信頼できる OUI リスト。
未分類AP	分類を特定できないPA	ー

検出された AP は以下の手順に従って分類されます。

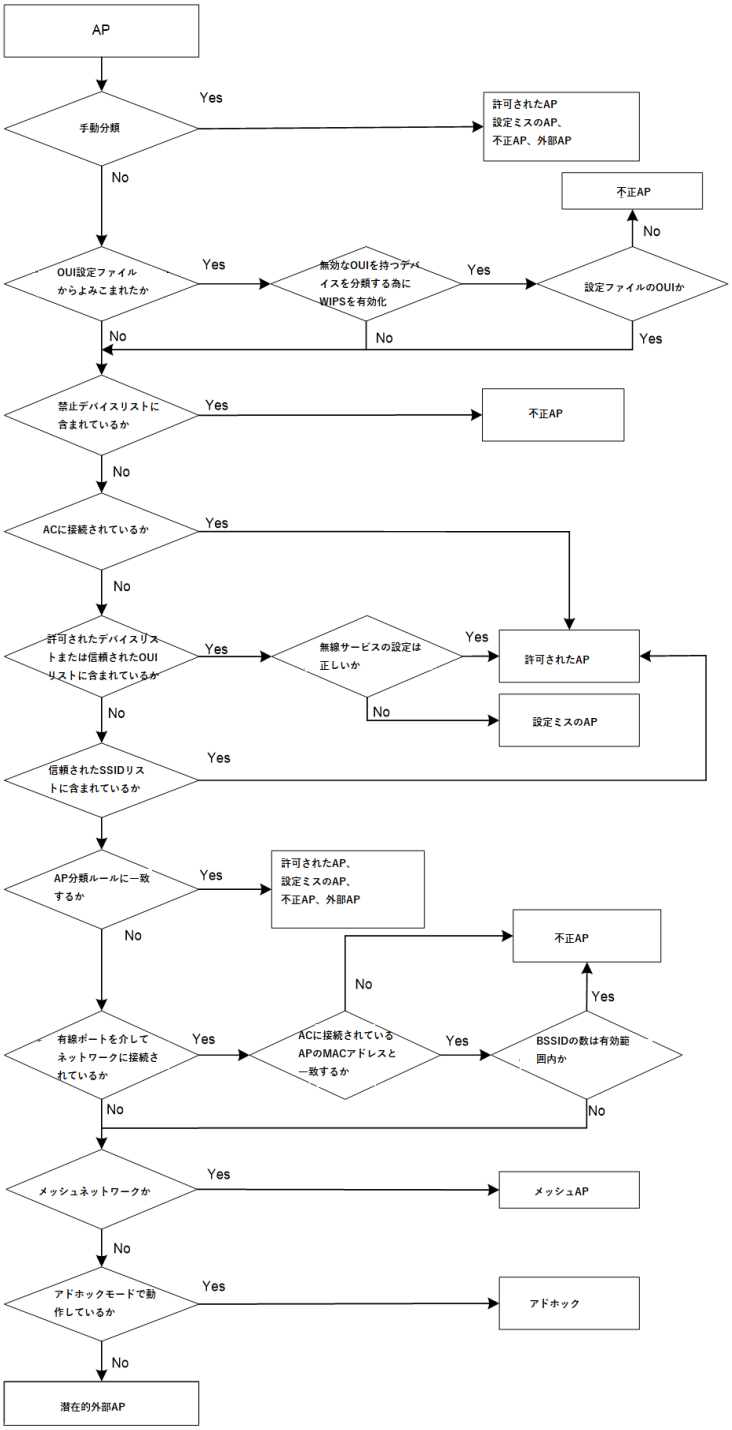


図 2-1 AP 分類フロー

🕮 メモ：

AP 分類フローでは、NEC 装置のみが有線ネットワーク接続の検出をサポートします。

2.4.2 クライアント種別

表 2-3に示すように、WIPS はあらかじめ決められた分類ポリシーに応じて、検出されたクラオアントを分類します。

表 2-3 クライアント種別

種別	説明	分類ルール
許可クライアント	WLANで許可されているクライアント	● 禁止装置リストに該当し、許可APに接続しています。 ● 認証に成功し、許可APに接続しています。
無許可クライアント	WLANで使用できないクライアント	● 禁止装置リストに該当します。 ● 不正APに接続しています。 ● OUIコンフィグファイルに該当しません。
関連付けが不正なクライアント	無許可APに接続しているクライアント	許可装置リストに該当するが、無許可APに接続しています。誤接続したクライアントは、セキュリティ脅威をネットワークにもたらす可能性があります。
未分類クライアント	種別を特定できないクライアント	―

検出されたクライアントは以下の手順に従って分類されます。

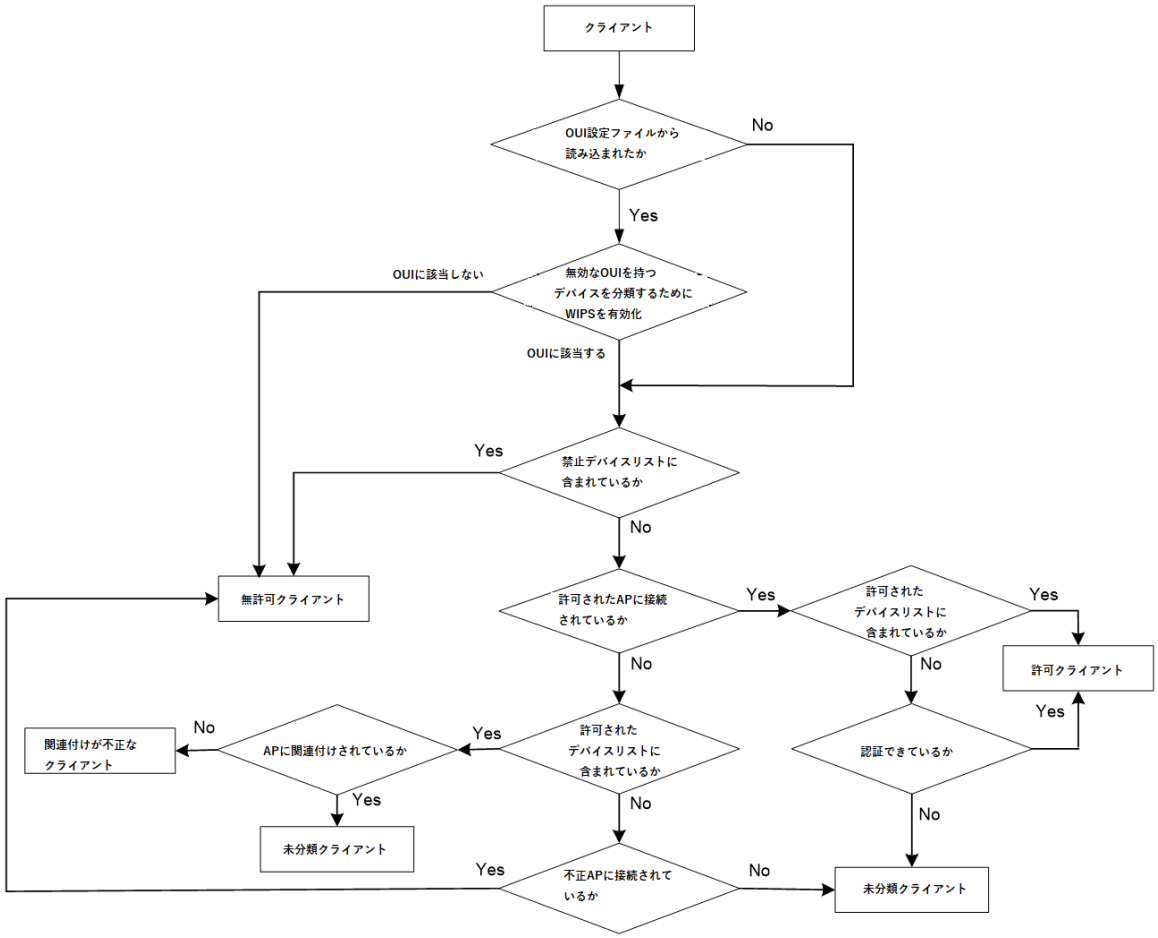


図 2-2 クライアントの分類フロー

2.5 対策

WLAN は不正装置からの攻撃の影響を受けやすく、攻撃によりセキュリティ上の問題が引き起こされる可能性があります。WIPS では、不正装置に対する対策を実行できます。

2.6 WIPS設定作業リスト

作業リスト
（必須設定項目）WIPS有効化

作業リスト
（オプション設定項目）無線攻撃検出の設定 • フラッド攻撃検出の設定 • 不正パケット検出の設定 • 装置エントリ攻撃検出の設定 • その他の攻撃に対する検出設定 RSSIにもとづいた無線装置検出の設定 • WIPSに関連付けられていないクライアント検出の有効化 • 攻撃検知ポリシーの適用
（オプション設定項目）シグネチャにもとづいた攻撃検出の設定 • シグネチャ設定 • シグネチャポリシーの設定 • シグネチャポリシーの適用
（オプション設定項目）装置種別の設定 • 分類ポリシーの設定 • 手動AP分類ポリシーの設定 • 分類ポリシーの適用 （オプション設定項目）対策の設定 • 対策ポリシーの設定 • 対策ポリシーの適用
（オプション設定項目）アラーム無視装置リストの設定
（オプション設定項目）OUIの設定

2.7 WIPS有効化

🕮 **メモ：**

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。

WIPS センサとして動作させるために、AP の radio で WIPS を有効にします。

WIPS は、ワイヤレスネットワークを複数の仮想セキュリティドメイン（VSD）に分割し、それぞれに異なるポリシーを適用することができます。

AP の radio で WIPS を有効にする前に、AP を VSD に追加する必要があります。

2.7.1 radio view での WIPS の有効化

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. AP view に移行する	**wlan ap** *ap-name* [**model** *model-name*]	APを作成するときは、モデル名を指定する必要があります。
3. AP を VSD に追加する	**wips virtual-security-domain** *vsd-name*	デフォルト：設定なし
4. radio view に移行する	**radio** *radio-id*	ー
5. WIPS を有効にする	**wips enable**	デフォルト：無効

2.7.2 AP group radio view での WIPS の有効化

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. AP view に移行する	**wlan ap-group** *group-name*	ー
3. AP を VSD に追加する	**wips virtual-security-domain** *vsd-name*	デフォルト：設定なし
4. AP model view に移行する	**ap-model** *ap-model*	ー
5. radio view に移行する	**radio** *radio-id*	ー
6. WIPS を有効にする	**wips enable**	デフォルト：無効

2.8 無線攻撃検出の設定

無線攻撃検出を設定する場合、最初に攻撃検出ポリシーを作成し、指定した攻撃検出を許可する必要があります。

2.8.1 フラッド攻撃検出の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. WIPS view に移行する	**wips**	ー
3. 攻撃検出ポリシーを作成し、その view に移行する	**detect policy** *policy-name*	デフォルト：設定なし
4. アソシエーション要求用フラッド攻撃検出を設定する	**flood association-request** [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *	デフォルト：無効
5. 認証要求用フラッド攻撃検出を設定する	**flood authentication** [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *	デフォルト：無効
6. ビーコン用フラッド攻撃検出を設定する	**flood beacon** [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *	デフォルト：無効

操作	コマンド	補足
7. ブロック ACK 用フラッド攻撃検出を設定する	**flood block-ack** [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *	デフォルト：無効
8. RTS 用フラッド攻撃検出を設定する	**flood rts** [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *	デフォルト：無効
9. CTS 用フラッド攻撃検出を設定する	**flood cts** [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *	デフォルト：無効
10. 認証取り消し（Deauthentication）用フラッド攻撃検出を設定する	**flood deauthentication** [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *	デフォルト：無効
11. アソシエーション解除用フラッド攻撃検出を設定する	**flood disassociation** [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *	デフォルト：無効
12. EAPOL-start 用フラッド攻撃検出を設定する	**flood eapol-start** [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *	デフォルト：無効
13. ヌルデータ用フラッド攻撃検出を設定する	**flood null data** [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *	デフォルト：無効
14. プローブ要求用フラッド攻撃検出を設定する	**flood probe-request** [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *	デフォルト：無効
15. 再アソシエーション要求用フラッド攻撃検出を設定する	**flood reassociation-request** [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *	デフォルト：無効
16. EAPOL-logoff 用フラッド攻撃検出を設定する	**flood eapol-logoff** [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*]*	デフォルト：無効
17. EAP-failure 用フラッド攻撃検出を設定する	**flood eap-failure** [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *	デフォルト：無効
18. EAPOL-success 用フラッド攻撃検出を設定する	**flood eap-success** [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *	デフォルト：無効

2.8.2 不正パケット検出の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. WIPS view に移行する	**wips**	―
3. 攻撃検出ポリシーを作成し、その view に移行する	**detect policy** *policy-name*	デフォルト：設定なし
4. 重複 IE 検出を設定する	**malformed duplicated-ie** [**quiet** *quiet-value*]	デフォルト：無効
5. FATA-Jack 検出を設定する	**malformed fata-jack** [**quiet** *quiet-value*]	デフォルト：無効
6. 異常な IBSS と ESS 設定検出を設定する	**malformed illegal-ibss-ess** [**quiet** *quiet-value*]	デフォルト：無効

操作	コマンド	補足
7. 無効ソースアドレス検出を設定する	**malformed invalid-address-combination** [**quiet** *quiet-value*]	デフォルト：無効
8. 不正アソシエーション要求フレーム検出を設定する	**malformed invalid-assoc-req** [**quiet** *quiet-value*]	デフォルト：無効
9. 不正認証要求フレーム検出を設定する	**malformed invalid-auth** [**quiet** *quiet-value*]	デフォルト：無効
10. 無効な認証取り消し（Deauthentication）コード検出を設定する	**malformed invalid-deauth-code** [**quiet** *quiet-value*]	デフォルト：無効
11. 無効なアソシエーション解除コード検出を設定する	**malformed invalid-disassoc-code** [**quiet** *quiet-value*]	デフォルト：無効
12. 無効な IE 長検出を設定する	**malformed invalid-ie-length** [**quiet** *quiet-value*]	デフォルト：無効
13. 不正な HT IE 検出を設定する	**malformed invalid-ht-ie** [**quiet** *quiet-value*]	デフォルト：無効
14. 無効なパケット長検出を設定する	**malformed invalid-pkt-length** [**quiet** *quiet-value*]	デフォルト：無効
15. 継続時間超過検出を設定する	**malformed large-duration** [**quiet** *quiet-value* | threshold value]	デフォルト：無効
16. 不正なプローブ応答フレーム検出を設定する	**malformed null-probe-resp** [**quiet** *quiet-value*]	デフォルト：無効
17. EAPOL key 長超過検出を設定する	**malformed overflow-eapol-key** [**quiet** *quiet-value*]	デフォルト：無効
18. SSID データ長超過検出を設定する	**malformed overflow-ssid** [**quiet** *quiet-value*]	デフォルト：無効
19. 冗長 IE 検出を設定する	**malformed redundant-ie** [**quiet** *quiet-value*]	デフォルト：無効

2.8.3 装置エントリ攻撃検出の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. WIPS view に移行する	**wips**	ー
3. 攻撃検出ポリシーを作成し、その view に移行する	**detect policy** *policy-name*	デフォルト：設定なし
4. クライアントエントリの学習レートを設定する	**client-rate-limit** [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *	デフォルト：統計収集間隔は60秒、待機時間は1200秒、学習するクライアントエントリのしきい値は1024です。

操作	コマンド	補足
5. クライアントエントリタイマを設定する	**client-timer inactive** *inactive-value* **aging** *aging-value*	デフォルト : 非アクティブ時間は300秒、エージングタイマは600秒です。 非アクティブ時間内にクライアントがパケット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。クライアントがエージングタイマ内にフレームを送受信しない場合、WIPSはそのエントリを削除します。
6. AP エントリの学習レートを設定する	**ap-rate-limit** [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *	デフォルト : 統計収集間隔は60秒、待機時間は1200秒、学習するAPエントリのしきい値は512です。
7. AP エントリタイマを設定する	**ap-timer** [**inactive** *inactive-value* **aging** *aging-value*]	デフォルト : APの非アクティブ時間は300秒、エージングタイマは600秒です。 APが非アクティブ時間内にパケット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。 APがエージングタイマ内にフレームを送受信しない場合、WIPSはそのエントリを削除します。

2.8.4 その他の攻撃に対する検出設定

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. WIPS view に移行する	**wips**	ー
3. 攻撃検出ポリシーを作成し、その view に移行する	**detect policy** *policy-name*	デフォルト：設定なし
4. ライアント MAC アドレスなりすまし攻撃検出を設定する	**client-spoofing** [**quiet** *quiet-value*]	デフォルト：無効
5. AP MAC アドレスなりすまし攻撃検出を設定する	**ap-spoofing** [**quiet** *quiet-value*]	デフォルト：無効
6. weak IV 検出を設定する	**weak-iv** [**quiet** *quiet-value*]	デフォルト：無効
7. Omerta 攻撃検出を設定する	**omerta** [**quiet** *quiet-value*]	デフォルト：無効
8. ブロードキャスト アソシエーション解除攻撃検出を設定する	**disassociation-broadcast** [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *	デフォルト：無効

操作	コマンド	補足
9. ブロードキャスト 認証取り消し（Deauthentication）攻撃検出を設定する	**deauthentication-broadcast** [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *	デフォルト：無効
10. 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設定する	**ht-40mhz-intolerance** [**quiet** *quiet-value*]	デフォルト：無効
11. パワーセーブ攻撃検出を設定する	**power-save** [**interval** *interval-value* | **minoffpacket** *packet-value* | **onoffpercent** *percent-value* | **quiet** *quiet-value*] *	デフォルト：無効
12. 許可チャネルリストを設定する	**permit-channel** *channel-id-list*	デフォルト：設定なし
13. 禁止チャネル検出を設定する	**prohibited-channel** [**quiet** *quiet-value*]	デフォルト：無効
14. Windows ブリッジ検出を設定する	**windows-bridge** [**quiet** *quiet-value*]	デフォルト：無効
15. 未暗号許可 AP 検出を設定する	**unencrypted-authorized-ap** [**quiet** *quiet-value*]	デフォルト：無効
16. 未暗号許可クライアント検出を設定する	**unencrypted-trust-client** [**quiet** *quiet-value*]	デフォルト：無効
17. ソフト AP 検出を設定する	**soft-ap** [**convert-time** *time-value*]	デフォルト：無効
18. AP なりすまし攻撃検出を設定する	**ap-impersonation** [**quiet** *quiet-value*]	デフォルトで：無効
19. HT-グリーンフィールドモード AP 検出を設定する	**ht-greenfield** [**quiet** *quiet-value*]	デフォルト：無効
20. アソシエーション/再アソシエーション DoS 攻撃検出を設定する	**association-table-overflow** [**quiet** *quiet-value*]	デフォルト：無効
21. 無線ブリッジ検出を設定する	**wireless-bridge** [**quiet** *quiet-value*]	デフォルト：無効
22. AP フラッド攻撃検出を設定する	**ap-flood** [**apnum** *apnum-value* | **exceed** *exceed-value* | **quiet** *quiet-value*] *	デフォルト：無効
23. ハニーポット AP 検出を設定する	**honeypot-ap** [**similarity** **similarity-value** | **quiet** *quiet-value*] *	デフォルト：無効
24. MITM 攻撃検出を設定する	**man-in-the-middle** [**quiet** *quiet-value*]	デフォルト：無効
25. チャネル変更検出を設定する	**ap-channel-change** [**quiet** *quiet-value*]	デフォルト：無効
26. ランダム 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 を設定する	**random-mac-scan enable**	デフォルト: ランダム MAC アドレスを使用する Apple 端末のアラームをトリガーされます。
27. WIPS view に戻る	**quit**	ー
28. コンフィグファイルからホットスポット情報をインポートする	**import hotspot** *file-name*	デフォルト: ホットスポット情報はインポートされません。

操作	コマンド	補足
29．攻撃検出ポリシーを作成し、その view に移行する	**detect policy** *policy-name*	デフォルト：設定なし
30．ホットスポット攻撃検出を設定する	**hotspot-attack** [**quiet** *quiet-value*]	デフォルト：無効

2.8.5 RSSI にもとづいた無線装置検出の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． WIPS view に移行する	**wips**	―
3． 攻撃検出ポリシーview に移行する	**detect policy** *policy-name*	―
4． クライアントまたは AP の RSSI しきい値を設定する	**rssi-threshold** { **ap** *ap-rssi-value* | **client** *client-rssi-value* }	デフォルト：設定なし
5． 無線装置検出の RSSI 差のしきい値を設定する	**rssi-change-threshold** *threshold-value*	デフォルト：設定なし

2.8.6 WIPS に関連付けられていないクライアント検出の有効化

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． WIPS view に移行する	**wips**	―
3． 攻撃検出ポリシーview に移行する	**detect policy** *policy-name*	―
4． 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 を有効にする	**detect dissociate-client enable**	デフォルト：WIPSは関連付けられていないクライアントを検出しません。

2.8.7 攻撃検知ポリシーの適用

操作	コマンド	補足
5． system view に移行する	**system-view**	―
6． WIPS view に移行する	**wips**	―
7． VSD を作成し、その view に移行する	**virtual-security-domain** *vsd-name*	デフォルト：設定なし
8． VSD に攻撃検出ポリシーを適用する	**apply detect policy** *policy-name*	デフォルト：設定なし VSDに適用される攻撃検出ポリシーは、VSD内のすべての無線に適用されます。

2.9 シグネチャにもとづいた攻撃検出の設定

2.9.1 シグネチャ設定

WIPS は、検出されたパケットを設定済みシグネチャと昇順 ID で一致するまで照合します。

シグネチャに対して 1 つまたは複数のサブシグネチャを設定できます。 パケットは、シグネチャのすべてのサブシグネチャと一致する場合にのみ、シグニチャと一致したとみなします。

以下にシグネチャ設定をする手順を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. WIPS view に移行する	**wips**	ー
3. シグネチャを作成し、その view に移行する	**signature rule** *rule-id*	デフォルト：設定なし
4. フレームのフレームタイプに一致するサブシグネチャを設定する	**frame-type** { **control** | **data** | **management** [**frame-subtype** { **association-request** | **association-response** | **authentication** | **beacon** | **deauthentication** | **disassociation** | **probe-request** }] }	デフォルト：設定なし
5. フレームの MAC アドレスに一致するサブシグネチャを設定する	**mac-address** { **bssid** | **destination** | **source** } *mac-address*	デフォルト：設定なし
6. フレームのシーケンス番号に一致するサブシグネチャを設定する	**seq-number** *seq-value1* [**to** *seq-value2*]	デフォルト：設定なし
7. フレームの SSID 長に一致するサブシグネチャを設定する	**ssid-length** *length-value1* [**to** *length-value2*]	デフォルト：設定なし
8. フレームの SSID に一致するサブシグネチャを設定する	**ssid** [**case-sensitive**] [**not**] { **equal** | **include** } *string*	デフォルト：設定なし
9. フレームの指定ビットに一致するサブシグネチャを設定する	**pattern** *pattern-number* **offset** *offset-value* **mask** *hex-value value1* [**to** *value2*] [**from-payload**]	デフォルト：設定なし
10. 論理 AND 関係にあるサブシグネチャを設定する	**match all**	デフォルト：サブシグネチャは論理OR関係にあります。パケットは、シグネチャのサブシグネチャのいずれかと一致する場合、シグネチャと一致します。 このコマンドを設定すると、パケットはシグネチャのすべてのサブシグネチャと一致する場合にのみ、シグネチャと一致します。

2.9.2 シグネチャポリシーの設定

シグネチャを適用するには、シグネチャをシグネチャポリシーに割り当てます。

以下にシグネチャポリシーの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. WIPS view に移行する	**wips**	ー
3. シグネチャポリシーを作成し、その view に移行する	**signature policy** *policy-name*	デフォルト：設定なし
4. 指定シグネチャをシグネチャポリシーに割り当てる	**apply signature rule** *rule-id*	デフォルト：設定なし
5. WIPS でシグネチャに一致するパケットの検出を有効にする	**detect signature** [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *	デフォルト：有効 統計収集間隔は60秒、待機時間は600秒、学習するAPエントリのしきい値は50です。

2.9.3 シグネチャポリシーの適用

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. WIPS view に移行する	**wips**	ー
3. VSD を作成し、その view に移行する	**virtual-security-domain** *vsd-name*	デフォルト：設定なし
4. 指定シグネチャポリシーを VSD に適用する	**apply signature policy** *policy-name*	デフォルト：設定なし

2.10 装置種別の設定

無線装置種別設定では、最初に分類ポリシーを作成し、指定装置の種別を設定しなければなりません。

2.10.1 分類ポリシーの設定

以下の方法のいずれかで、WIPS による装置の分類が可能です。

- **自動分類**－装置の MAC アドレス、OUI、SSID を指定リストに追加することにより、WIPS は自動的に装置を分類します。また、WIPS は、ユーザ定義の AP 分類ルールを使用して、AP を分類することもできます。
- **手動分類**－装置種別を手動で指定します。手動分類は AP のみ適用可能です。

自動分類と手動分類の両方を設定した場合、手動分類が有効になります。

🕮 **メモ：**

AP を指定する場合は、BSSID(無線の MAC アドレス)を指定してください。

I. 自動装置分類の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. WIPS view に移行する	**wips**	ー
3. 分類ポリシーを作成し、その view に移行する	**classification policy** *policy-name*	デフォルト：設定なし
4. WIPS で無効 OUI 装置を悪意のある装置に分類する	**invalid-oui-classify illegal**	デフォルト：設定なし
5. 許可装置リストへ MAC アドレスを追加する	**trust mac-address** *mac-address*	デフォルト：設定なし
6. 許可 OUI リストへ OUI を追加する	**trust oui** *oui*	デフォルト：設定なし このコマンドは、APの分類のみに適用されます。
7. 許可 SSID リストへ SSID を追加する	**trust ssid** *ssid-name*	デフォルト：設定なし
8. スタティック禁止装置リストへ MAC アドレスを追加する	**block mac-address** *mac-address*	デフォルト：設定なし
9. 指定 AP 分類ルールを分類ポリシーに割り当てる	**apply ap-classification rule** *rule-id* { **authorized-ap** | { { **external-ap** | **misconfigured-ap** | **rogue-ap** } [**severity-level** *level*] } }	デフォルト：設定なし

II. AP 分類ルールの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. WIPS view に移行する	**wips**	ー
3. AP 分類ルールを作成し、その view に移行する	**ap-classification rule** *rule-id*	デフォルト：設定なし
4. AP の RSSI と一致する AP 分類ルールを設定する	**rssi** *value1* [**to** *value2*]	デフォルト：設定なし
5. AP の無線サービスの SSID と一致する AP 分類ルールを設定する	**ssid** [**case-sensitive**] [**not**] { **equal** | **include** } *ssid-string*	デフォルト：設定なし
6. AP の動作時間と一致する AP 分類ルールを設定する	**up-duration** *value1* [**to** *value2*]	デフォルト：設定なし

操作	コマンド	補足
7. APの接続クライアント数と一致するAP分類ルールを設定する	**client-online** *value1* [**to** *value2*]	デフォルト：設定なし
8. APを検出するセンサ数と一致するAP分類ルールを設定する	**discovered-ap** *value1* [**to** *value2*]	デフォルト：設定なし
9. APが使用するセキュリティモードと一致するAP分類ルールを設定する	**security** { **equal** | **include** } { **clear** | **wep** | **wpa** | **wpa2** }	デフォルト：設定なし
10. APが使用する認証モードと一致するAP分類ルールを設定する	**authentication** { **equal** | **include** } { **802.1x** | **none** | **other** | **psk** }	デフォルト：設定なし
11. APのOUI情報と一致するAP分類ルールを設定する	**oui** *oui-info*	デフォルト：設定なし
12. AP分類ルールの基準を論理AND関係になるように設定する	**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。 このコマンドを設定すると、AP分類ルールのすべての基準に一致する場合にのみ、APはAP分類ルールに一致します。

2.10.2 手動 AP 分類ポリシーの設定

操作	コマンド	補足
1. system viewに移行する	**system-view**	―
2. WIPS viewに移行する	**wips**	―
3. 分類ポリシーを作成し、その viewに移行する	**classification policy** *policy-name*	デフォルト：設定なし
4. 指定されたAPカテゴリを設定する	**manual-classify mac-address** *mac-address* { **authorized-ap** | **external-ap** | **misconfigured-ap** | **rogue-ap** }	デフォルト：設定なし

2.10.3 分類ポリシーの適用

操作	コマンド	補足
1. system viewに移行する	**system-view**	―
2. WIPS viewに移行する	**wips**	―
3. VSD viewに移行する	**virtual-security-domai**n *vsd-name*	デフォルト：設定なし

操作	コマンド	補足
4. VSD に分類ポリシーを適用する	**apply classification policy** *policy-name*	デフォルト：設定なし VSDに適用される分類ポリシーは、VSD内のすべての無線に適用されます。

2.11 対策の設定

不正装置に対策を行うには、まず対策ポリシーを作成し、WIPS を有効にする必要があります。

2.11.1 対策ポリシーの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. WIPS view に移行する	**wips**	ー
3. 対策ポリシーを作成し、その view に移行する	**countermeasure policy** *policy-name*	デフォルト：設定なし
4. WIPS の外部 AP 対策を有効にする	**countermeasure external-ap**	デフォルト：無効
5. WIPS の未設定 AP 対策を有効にする	**countermeasure misconfigured-ap**	デフォルト：無効
6. WIPS の誤接続クライアント対策を有効にする	**countermeasure misassociation-client**	デフォルト：無効
7. WIPS の潜在的外部 AP 対策を有効にする	**countermeasure potential-external-ap**	デフォルト：無効
8. WIPS の潜在的許可 AP 対策を有効にする	**countermeasure potential-authorized-ap**	デフォルト：無効
9. WIPS の潜在的不正 AP 対策を有効にする	**countermeasure potential-rogue-ap**	デフォルト：無効
10. WIPS の不正 AP 対策を有効にする	**countermeasure rogue-ap**	デフォルト：無効
11. WIPS の無許可クライアント対策を有効にする	**countermeasure unauthorized-client**	デフォルト：無効
12. WIPS の未分類 AP 対策を有効にする	**countermeasure uncategorized-ap**	デフォルト：無効
13. WIPS の未分類クライアント対策を有効にする	**countermeasure uncategorized-client**	デフォルト：無効
14. WIPS の指定装置対策を有効にする	**countermeasure mac-address** *mac-address* [**except-authorized-ap**]	デフォルト：無効
15. WIPS のアドホック装置対策を有効にする	**countermeasure adhoc**	デフォルト：無効

操作	コマンド	補足
16. 認証取り消しアタックをブロードキャストする装置対策を有効にする	**countermeasure attack deauth-broadcast**	デフォルト：無効
17. アソシエーション解除アタックをブロードキャストする装置対策を有効にする	**countermeasure attack disassoc-broadcast**	デフォルト：無効
18. WIPS のハニーポット AP 対策を有効にする	**countermeasure attack honeypot-ap**	デフォルト：無効
19. WIPS ホットスポット攻撃の対策を有効にする	**countermeasure attack hotspot-attack**	デフォルト：無効
20. 40MHz 帯域幅モードが無効の装置対策を有効にする	**countermeasure attack ht-40-mhz-intolerance**	デフォルト：無効
21. 不正パケットを送信する装置対策を有効にする	**countermeasure attack malformed-packet**	デフォルト：無効
22. WIPS の MITM 攻撃対策を有効にする	**countermeasure attack man-in-the-middle**	デフォルト：無効
23. WIPS の Omerta 攻撃対策を有効にする	**countermeasure attack omerta**	デフォルト：無効
24. WIPS のパワーセーブ攻撃対策を有効にする	**countermeasure attack power-save**	デフォルト：無効
25. WIPS のソフト AP 対策を有効にする	**countermeasure attack soft-ap**	デフォルト：無効
26. 未暗号化のフレームを送信する許可クライアント対策を有効にする	**countermeasure attack unencrypted-trust-client**	デフォルト：無効
27. Weak IV を使用する装置対策を有効にする	**countermeasure attack weak-iv**	デフォルト：無効
28. Windows ブリッジ攻撃対策を有効にする	**countermeasure attack windows-bridge**	デフォルト：無効
29. WIPS の全検出攻撃対応対策を有効にする	**countermeasure attack all**	デフォルト：無効
30. WIPS の全攻撃検出用センサの攻撃対応対策を有効にする	**select sensor all**	デフォルト：最後に攻撃検出したセンサのみが、攻撃対策を行います。

2.11.2 対策ポリシーの適用

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. WIPS view に移行する	**wips**	ー
3. VSD を作成し、その view に移行する	**virtual-security-domain** *vsd-name*	デフォルト：設定なし

操作	コマンド	補足
4. VSD に対策ポリシーを適用する	**apply countermeasure policy** *policy-name*	デフォルト：設定なし VSDに適用される対策ポリシーは、VSD内のすべての無線に適用されます。

2.12 アラーム無視装置リストの設定

アラーム無視装置リストに該当する無線装置の場合、WIPS は、監視のみを行い、アラームを発生しません。

以下にアラーム無視装置リストの設定手順を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. WIPS view に移行する	**wips**	―
3. アラーム無視装置リストに MAC アドレスを追加する	**ignorelist mac-address** *mac-address*	デフォルト：設定なし

2.13 OUIの設定

Organizationally Unique Identifier (OUI) は、装置の MAC アドレスの最初の 3 バイトであり、装置のベンダを識別するために使用されます。

装置の起動後、デフォルトの OUI 設定ファイル内の OUI が OUI ライブラリに自動的にインポートされます。

以下のように、OUI ライブラリを手動で設定することもできます。

- OUI 設定ファイルから OUI ライブラリに OUI をインポートするには、**import oui** コマンドを使用します。
  インポートされた OUI、更新された OUI、既存の OUI、およびインポートに失敗した OUI の数が表示されます。

以下に OUI のインポートを示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. WIPS view に移行する	**wips**	―
3. OUI 設定ファイルから OUI ライブラリに OUI をインポートする	**import oui** ***file-name***	―

2.14 WIPSの表示と維持

すべての view で **display** コマンドを実行し、user view で **reset** コマンドを実行できます。

操作	コマンド
全センサに関する情報を表示する	**display wips sensor**
センサが収集した攻撃検出情報を表示する	**display wips statistics** [**receive** | **virtual-security-domain** *vsd-name*]
不正な装置に対してWIPSが実行した対策に関する情報を表示する	**display wips virtual-security-domain** *vsd-name* **countermeasure record**
VSDで検出された無線装置情報を表示する	**display wips virtual-security-domain** *vsd-name* **device** [**ap** [**adhoc** | **authorized** | **external** | **misconfigured** | **potential-authorized** | **potential-external** | **potential-rogue** | **rogue**] | **client** [[**dissociative-client**] [**authorized** | **misassociation** | **unauthorized** | **uncategorized**]] | **mac-address** *mac-address*] [**verbose**]
検出したNAT設定クライアント情報を表示する	**display wlan nat-detect [mac-address** *mac-address* **]**
全センサ受信情報を削除する	**reset wips statistics**
VSDの学習されたAPエントリまたはクライアントエントリを削除する	**reset wips virtual-security-domain** *vsd-name* { **ap** { **all** | **mac-address** *mac-address* } | **client** { **all** | **mac-address** *mac-address* } | **all** }
不正な装置に対してWIPSが実行した対策に関する情報を削除する	**reset wips virtual-security-domain** *vsd-name* **countermeasure record**
検出したNAT設定気裏慰安と情報を消去する	**reset wlan nat-detect**

2.15 WIPS設定例

2.15.1 装置の分類の設定例

I. ネットワーク要件

図 2-3に示すように、センサはスイッチ経由で AC と接続します。AP1 と AP2 は SSID abc を設定してクライアントに無線サービスを提供します。以下のタスクを実行してください。

- Radio の通信状況の影響を受けずに WIPS 検出を行うためにセンサ用 AP を用意します。
- 無線装置種別を設定して、静的禁止装置リストに MAC アドレス 000f-1c35-12a5 を追加し、許可 SSID リストに SSID abc を追加します。

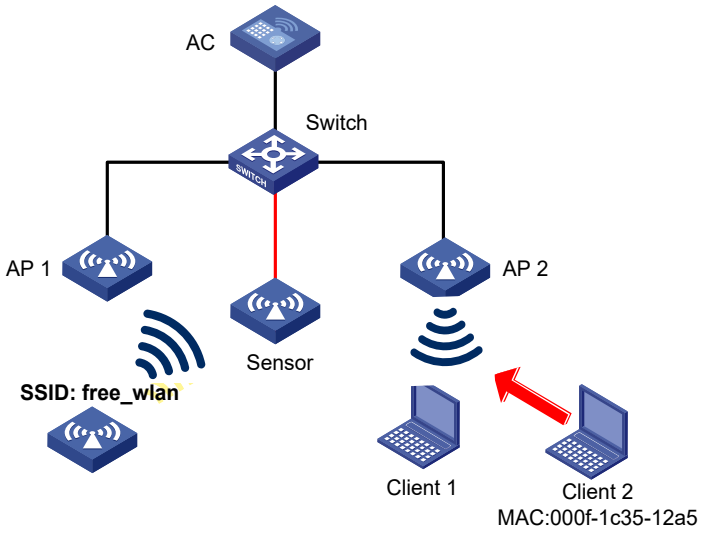


図 2-3 ネットワーク図

II. 設定手順

AC の無線サービスを設定します。（詳細は省略します。）

無線サービスの設定については、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*6 WLAN アクセス*”の”*1 章 WLAN アクセス*”を参照してください。

VSD vsd1 を作成します。

```
<AC> system-view
[AC] wips
[AC-wips] virtual-security-domain vsd1
[AP-wips-vsd-vsd1] quit
[AC-wips] quit
```

AP Sensor を作成し、この AP 用 WIPS を有効にします。

```
[AC] wlan ap Sensor model QX-W1110
[AC-wlan-ap-Sensor] serial-id 219801A28N819CE0002T
[AC-wlan-ap-Sensor] radio 1
[AC-wlan-ap-Sensor-radio-1] radio enable
[AC-wlan-ap-Sensor-radio-1] wips enable
[AC-wlan-ap-Sensor-radio-1] quit
```

AP Sensor を VSD vsd1 に追加します。

```
[AC-wlan-ap-Sensor] wips virtual-security-domain vsd1
[AC-wlan-ap-Sensor] quit
```

分類ポリシーclass1 を作成し、禁止装置リストにクライアント 2 の MAC アドレスを追加します。

```
[AC] wips
[AC-wips] classification policy class1
[AC-wips-cls-class1] block mac-address 000f-1c35-12a5
[AC-wips-cls-class1] trust ssid abc
[AC-wips-cls-class1] quit
```

分類ポリシーclass1 を VSD vsd1 に適用します。

```
[AC-wips] virtual-security-domain vsd1
[AC-wips-vsd-vsd1] apply classification policy class1
[AC-wips-vsd-vsd1] quit
```

対策ポリシーprotect を作成し、無許可クライアントや潜在的外部 AP 用対策を行うように WIPS を有効にします。

```
[AC-wips] countermeasure policy protect
[AC-wips-cms-protect] countermeasure unauthorized-client
[AC-wips-cms-protect] countermeasure potential-external-ap
[AC-wips-cms-protect] quit
```

対策ポリシーprotect を VSD vsd1 に適用します。

```
[AC-wips] virtual-security-domain vsd1
[AC-wips-vsd-vsd1] apply countermeasure policy protect
[AC-wips-vsd-vsd1] quit
[AC-wips] quit
```

III. 設定の確認

VSD vsd1 の無線装置分類情報を表示します。

```
[AC] display wips virtual-security-domain vsd1 device
Total 3 detected devices in virtual-security-domain vsd1

Class: Auth - authorization; Ext - extern; Mis - mistake;
       Unauth - unauthorized; Uncate - uncategorized;
       (A) - associate; (C) - config; (P) - potential

MAC address    Type   Class    Duration    Sensors Channel Status
000f-e200-5829 AP     Auth     00h 10m 24s 1       11      Active
000f-e228-2528 AP     Auth     00h 10m 04s 1       11      Active
000f-e223-1616 AP     Ext(P)   00h 10m 46s 1       11      Active
000f-1c35-12a5 Client Unauth   00h 10m 02s 1       11      Active
000f-e201-0102 Client Auth     00h 10m 02s 1       11      Active
```

この例は、MAC アドレス 000f-e223-1616 を持つ AP が潜在的外部 AP として分類され、MAC アドレス 000f-1c35-12a5 を持つクライアントが無許可クライアントとして分類されることを示します。

WIPS が装置に対して行った対策情報を表示します。

```
[AC] display wips virtual-security-domain vsd1 countermeasure record
Total 2 times countermeasure, current 2 countermeasure record in
virtual-security-domain vsd1

Class: Auth - authorization; Ext - extern; Mis - mistake;
       Unauth - unauthorized; Uncate - uncategorized;
       (A) - associate; (C) - config; (P) - potential

MAC address    Type   Class    Sensor name          Radio ID   Time
000f-e200-5829 AP     Auth     Sensor               1          2014-06-03/09:30:25
000f-e228-2528 AP     Auth     Sensor               1          2014-06-03/19:31:56
000f-e223-1616 AP     Ext(P)   Sensor               1          2014-06-03/10:30:36
000f-1c35-12a5 Client Unauth   Sensor               1          2014-06-03/09:13:26
000f-e201-0102 Client Auth     Sensor               1          2014-06-03/09:33:46
```

この例は、WIPS が MAC アドレス 000f-1c35-12a5 を持つ無許可クライアントと MAC アドレス 000f-e223-1616 を持つ潜在的外部 AP に対して対策を取ったことを示します。

2.15.2 不正パケットとフラッド攻撃の検出例

I. ネットワーク要件

図 2-4に示すように、センサとして 2 つの AP をスイッチ経由で AC と接続してください。センサ 1 とセンサ 2 を VSD VSD_1 に追加してください。重複 IE の不正パケット、または、ビーコンフラッド攻撃を検出した場合にアラームを発生するように、不正パケットとフラッド攻撃用 WIPS を有効にします。

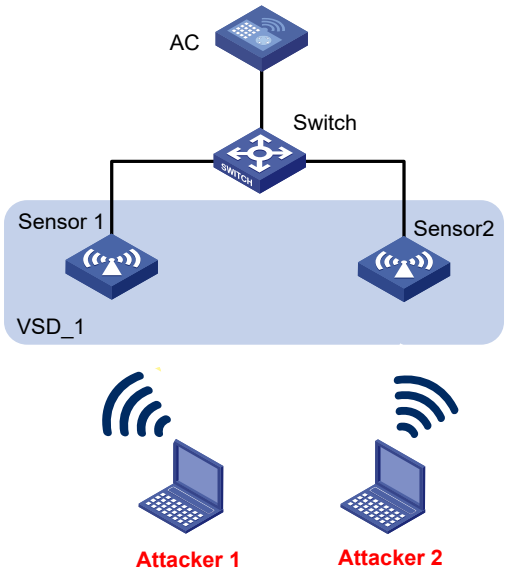


図 2-4 ネットワーク図

II. 設定手順

AC の無線サービスを設定します。（詳細は省略します。）

無線サービスの設定については、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*6 WLAN アクセス*”の”*1 章 WLAN アクセス*”を参照してください。

AP sensor1 を作成し、この AP 用 WIPS を有効にします。

```
<AC> system-view
[AC] wlan ap sensor1 model QX-W1110
[AC-wlan-ap-sensor1] serial-id 219801A28N819CE0002T
[AC-wlan-ap-sensor1] radio 1
[AC-wlan-ap-sensor1-radio-1] radio enable
[AC-wlan-ap-sensor1-radio-1] wips enable
[AC-wlan-ap-sensor1-radio-1] return
```

AP sensor2 を作成し、この AP 用 WIPS を有効化します。

```
<AC> system-view
[AC] wlan ap sensor2 model QX-W1110
[AC-wlan-ap-sensor2] serial-id 219801A28N819CE0002T
[AC-wlan-ap-sensor2] radio 1
[AC-wlan-ap-sensor2-radio-1] radio enable
[AC-wlan-ap-sensor2-radio-1] wips enable
[AC-wlan-ap-sensor2-radio-1] quit
[AC-wlan-ap-sensor2] quit
```

VSD VSD_1 を作成します。

```
[AC] wips
[AC-wips] virtual-security-domain VSD_1
[AP-wips-vsd-VSD_1] quit
```

攻撃検出ポリシーdtc1 を作成します。

```
[AC-wips] detect policy dtc1
```

重複 IE の不正パケット検出を有効にし、待機時間を 50 秒に設定します。

```
[AC-wips-dtc-dtc1] malformed duplicated-ie quiet 50
```

ビーコンフラッド攻撃検出を有効にし、統計間隔、しきい値、待機時間を 100 秒、200、50 秒に設定します。

```
[AC-wips-dtc-dtc1] flood beacon interval 100 quiet 50 threshold 200
[AC-wips-dtc-dtc1] quit
```

攻撃検出ポリシーdtc1 を VSD VSD_1 に適用します。

```
[AC-wips] virtual-security-domain VSD_1
[AC-wips-vsd-VSD_1] apply detect policy dtc1
```

```
[AC-wips-vsd-VSD_1] quit
[AC-wips] quit
```

AP sensor1 を VSD VSD_1 に追加します。

```
[AC] wlan ap sensor1
[AC-wlan-ap-sensor1] wips virtual-security-domain VSD_1
[AC-wlan-ap-sensor1] quit
```

AP sensor2 を VSD VSD_1 に追加します。

```
[AC] wlan ap sensor2
[AC-wlan-ap-sensor2] wips virtual-security-domain VSD_1
[AC-wlan-ap-sensor2] return
```

III. 設定の確認

WIPS が、WLAN で何も攻撃を検出していない状態でパケット統計情報を表示してください。この例では、不正パケットもフラッド攻撃メッセージも存在していないことを示します。

```
<AC> 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 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 sig rule messages: 0
Information from sensor 2
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 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 sig rule messages: 0
```

WIPS が、ビーコンフラッド攻撃と重複 IE の不正パケットを検出した状態でパケット統計を表示してください。この例では、重複 IE の不正パケット 28、ビーコンフラッド攻撃メッセージ 18 を検出したことを示します。

<AC> 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: 18
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 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 sig rule messages: 0
Information from sensor 2
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 duplicated-ie messages: 28
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 sig rule messages: 0
```

2.15.3 シグネチャベースのユーザ定義攻撃検出設定例

I. ネットワーク要件

図 2-5に示すように、AP1 と AP2 に SSID abc を設定し、クライアントに無線サービスを提供します。SSID が abc ではないビーコンフレームを検出した場合、アラームを発生するシグネチャ設定を行ったセンサ用 WIPS を有効にします。

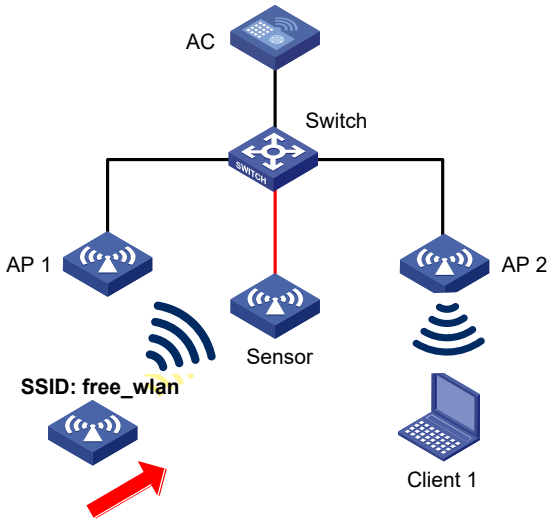


図 2-5 ネットワーク図

II. 設定手順

AC の無線サービスを設定します。（詳細は省略します。）

無線サービスの設定については、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*6 WLAN アクセス*”の”*1 章 WLAN アクセス*”を参照してください。

AP sensor1 を作成し、この AP 用 WIPS を有効にします。

```
<AC> system-view
[AC] wlan ap sensor1 model QX-W1110
[AC-wlan-ap-sensor1] serial-id 219801A28N819CE0002T
[AC-wlan-ap-sensor1] radio 1
[AC-wlan-ap-sensor1-radio-1] radio enable
[AC-wlan-ap-sensor1-radio-1] wips enable
[AC-wlan-ap-sensor1-radio-1] quit
[AC-wlan-ap-sensor1 ] quit
```

VSD vsd1 を作成します。

```
[AC] wips
[AC-wips] virtual-security-domain vsd1
[AC-wips] quit
```

AP sensor1 を VSD vsd1 に追加します。

```
[AC] wlan ap sensor1
[AC-wlan-ap-sensor1] wips virtual-security-domain vsd1
[AC-wlan-ap-sensor1] quit
```

シグネチャ 1 を作成し、ビーコンフレームでかつ SSID が abc ではないフレームと一致するというサブシグネチャを設定します。

```
[AC] wips
[AC-wips] signature rule 1
[AC-wips-sig-rule-1] frame-type management frame-subtype beacon
[AC-wips-sig-rule-1] ssid not equal abc
[AC-wips-sig-rule-1] quit
```

シグネチャポリシーsig1 を作成し、シグネチャ 1 をシグネチャポリシーsig1 に割り当てます。

```
[AC-wips] signature policy sig1
[AC-wips-sig-sig1] apply signature rule 1
```

シグネチャと一致したパケットを検出するように WIPS を有効にし、統計収集間隔、待機時間、アラームしきい値を、それぞれ 5 秒、60 秒、60 に設定します。

```
[AC-wips-sig-sig1] detect signature interval 5 quiet 60 threshold 60
[AC-wips-sig-sig1] quit
```

シグネチャポリシーsig1 を VSD vsd1 に適用します。

```
[AC] wips
[AC-wips] virtual-security-domain vsd1
[AP-wips-vsd-vsd1] apply signature policy sig1
[AP-wips-vsd-vsd1] quit
```

III. 設定の確認

センサが SSID free_wlan の無線サービスを検出したときに、AC がセンサからアラームを受信していることを確認します。

```
WIPS/5/WIPS_SIGNATURE: -VSD=vsd1-RuleID=1; Signature rule matched.
```

センサから収集した攻撃検出情報を表示してください。この例では、シグネチャと一致したパケットを 26 パケット検出したことを示します。

```
[AC] display wips statistics receive
Information from sensor
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 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 sig rule messages: 26
```

QX-W2300AC シリーズ アクセスコントローラ

オペレーションマニュアル

9. 無線管理

本マニュアルは以下に示す章で構成されています。

01-無線管理の設定

02- WLAN 無線ロードバランスの設定

03- WLAN ロードバランスの設定

04- WLAN 無線リソース計測の設定

05-バンドナビゲーションの設定

06- WLAN RRM の設定

07-チャネルスキャンの設定

08-スペクトル管理の設定

目次

このセクションのページは **9-x-x** です。

1 章 無線管理の設定 1-1
1.1 概要 1-1
1.1.1 無線モード 1-1
1.1.2 チャネル 1-1
1.1.3 伝送電力 1-2
1.1.4 伝送速度 1-2
1.1.5 MCS 1-2
1.1.6 VHT-MCS 1-5
1.1.7 HE-MCS 1-9
1.2 設定の制限とガイドライン 1-14
1.3 設定作業リスト 1-14
1.4 無線の有効化/無効化 1-15
1.4.1 すべての無線の有効化/無効化 1-15
1.4.2 radio view での無線の有効化/無効化 1-15
1.4.3 AP group view での無線の有効化/無効化 1-15
1.5 無線モードの指定 1-16
1.6 基本的な無線機能の設定 1-17
1.6.1 作動チャネルの指定 1-17
1.6.2 ブラックリスト、ホワイトリストのチャネル選択の設定 1-18
1.6.3 アンテナタイプの設定 1-18
1.6.4 最大伝送電力の設定 1-19
1.6.5 電力ロックの設定 1-20
1.6.6 伝送速度の設定 1-21
1.6.7 ビーコン間隔の設定 1-22
1.6.8 衝突回避モードの指定 1-23
1.6.9 RTS しきい値の設定 1-24
1.6.10 フラグメンテーションしきい値の設定 1-25
1.6.11 ハードウェア再伝送の最大数の設定 1-26
1.6.12 AP に関連づけるクライアントの最大数の設定 1-27
1.6.13 802.11b クライアント拒否の設定 1-27
1.6.14 802.11g 保護の設定 1-28
1.6.15 ANI の設定 1-29
1.6.16 プリアンプルタイプの設定 1-30
1.6.17 最大伝送距離の設定 1-30
1.6.18 無線連続モードの有効化 1-31
1.6.19 オンデマンドでのチャネル使用率の測定 1-32
1.6.20 チャネル使用率アラーム閾値の設定 1-32
1.7 802.11n 機能の設定 1-33
1.7.1 A-MPDU アグリゲーション方式の指定 1-33
1.7.2 A-MSDU アグリゲーション方式の指定 1-34
1.7.3 ショート GI の設定 1-35
1.7.4 LDPC の設定 1-36
1.7.5 STBC の設定 1-36
1.7.6 MCS インデックスの設定 1-37
1.7.7 802.11n/ac/ax クライアント限定アクセスの設定 1-39

1.7.8 802.11n 帯域幅モードの設定 1-40
1.7.9 エネルギ節約機能の設定 1-41
1.7.10 802.11n 保護の設定 1-41
1.8 802.11ac/ax 機能の設定 1-43
1.8.1 NSS の設定 1-43
1.8.2 802.11ac/ax クライアント限定アクセスの設定 1-45
1.8.3 802.11ac/ax 帯域幅モードの設定 1-46
1.8.4 TxBF の設定 1-47
1.8.5 OFDMA の設定 1-48
1.8.6 BSS カラーリングの設定 1-49
1.8.7 TWT ネゴシエーションの設定 1-50
1.9 802.11be 機能の設定 1-52
1.9.1 NSS の設定 1-52
1.9.2 802.11be 帯域幅モードの設定 1-54
1.9.3 MRU の設定 1-55
1.9.4 preamble puncturing 機能の設定 1-56
1.10 6GHz 帯の無線の設定 1-58
1.10.1 6GHz 帯の無線モードの指定 1-58
1.10.2 6GHz 帯無線サービス検出の設定 1-59
1.10.3 マルチ BSSID の設定 1-60
1.10.4 サービステンプレートの設定 1-60
1.10.5 サービステンプレートの有効化 1-63
1.10.6 無線に対するサービステンプレートの設定 1-64
1.11 スマートアンテナ機能の設定 1-64
1.12 無線管理の表示および管理 1-65
1.13 無線管理の設定例 1-66
1.13.1 基本無線機能の設定例 1-66
1.13.2 6GHz 帯の無線(Enhanced Open)の設定例 1-69
1.13.3 6GHz 帯の無線(WPA3 パーソナル)の設定例 1-71
1.13.4 6GHz 帯の無線(WPA3 エンタープライズ 192bit セキュリティあり)の設定例 .. 1-73
1.13.5 6GHz 帯の無線(WPA3 エンタープライズ 192bit セキュリティなし)の設定例 .. 1-76

1章 無線管理の設定

1.1 概要

RF（Radio Frequency）は、300kHz～300GHz の範囲内で電気的に振動する割合を示します。WLAN は、2.4GHz 帯（2.4GHz～2.4835GHz）と 5 GHz 帯（5.150GHz～5.350GHz、および 5.470～5.730GHz）の無線周波数を伝送メディアとして使用します。

“無線周波数”もしくはその略語“RF”は、無線コミュニケーションの“無線”に対する同義語としても使用されます。

1.1.1 無線モード

IEEE 基準では、802.11a、802.11b、802.11g、802.11n、802.11ac、802.11ax を定義しています。

表 1-1 802.11 基準の比較

IEEE 基準	周波数帯	最大速度
802.11a	5GHz	54Mbps
802.11b	2.4GHz	11Mbps
802.11g	2.4GHz	54Mbps
802.11n	2.4GHz or 5GHz	600Mbps
802.11ac	5GHz	6900Mbps
802.11gac	2.4GHz	1600Mbps
802.11ax	5GHz	9600Mbps
802.11gax	2.4GHz	2294Mbps

🕮 **メモ：**

- 802.11ac を 2.4GHz で使用するモードを 802.11gac と定義します。
- 802.11ax を 2.4GHz で使用するモードを 802.11gax と定義します。
- 特に指定が無い場合、文中に登場する“802.11ac”には 802.11gac が含まれます。
- 特に指定が無い場合、文中に登場する“802.11ax”には 802.11gax が含まれます。
- 到達範囲は、ご利用の環境(電波状況、パソコン性能、遮蔽物など)により異なります。

1.1.2 チャネル

チャネルとは、特定の帯域幅をもつ周波数の範囲のことです。2.4GHz 帯の中には、指定された 14 のチャネルがあります。各チャネルに対する帯域幅は 20MHz で、2 チャネル間は 5MHz 離れています。14 チャネル中、4 グループは重複のないチャネルとして存在し、もっとも一般的に使用されるのはチャネル 1、6、11 です。

5GHz 帯はより高い速度を供給でき、干渉に対してより耐性があります。5GHz 帯には、指定された 19 の重複しないチャネルが存在します。そのチャネルは 20MHz の帯域幅を有し、20MHz の間隔をおいて配置されます。

1.1.3 伝送電力

伝送電力は、無線装置の信号強度を表します。無線は、伝送電力が高いほどより広範囲のエリアをカバーできますが、隣接する装置により多くの干渉をもたらします。信号強度は、伝送距離が大きくなるにつれて減衰します。

1.1.4 伝送速度

伝送速度は、無線装置が通信する速度について言及します。伝送速度は、無線モード、拡散方式、コーディング方式、変調方式により変わります。異なる無線モードにサポートされた速度を以下に示します。

- **802.11a**－6Mbps、9Mbps、12Mbps、18Mbps、24Mbps、36Mbps、48Mbps、54Mbps
- **802.11b**－1Mbps、2Mbps、5.5Mbps、11Mbps
- **802.11g**－1Mbps、2Mbps、5.5Mbps、6Mbps、9Mbps、11Mbps、12 Mbps、18Mbps、24Mbps、36Mbps、48Mbps、54Mbps
- **802.11n**－802.11n 無線に対する速度は、チャネル帯域幅により変化します。詳細は、MCS を参照してください。
- **802.11ac**－802.11ac 無線に対する速度は、チャネル帯域幅および NSS（Number of Spatial Streams）により変化します。詳細は、MCS を参照してください。
- **802.11gac**－2.4GHz 帯で作動し、802.11ac と互換性があります。伝送帯域と NSS（number of spatial streams）によって変わります。詳細は VHT-MCS を参照してください。
- **802.11ax**－802.11ax に対する速度は、チャネル帯域幅および NSS（Number of Spatial Streams）により変化します。詳細は、オペレーションマニュアルのセクション 2 *WLAN “無線管理の設定”* の *“HE-MCS”* を参照してください。
- **802.11gax**－2.4GHz 帯で作動し、802.11ax と互換性があります。伝送帯域と NSS（number of spatial streams）によって変わります。詳細は、HE-MCS を参照してください。

1.1.5 MCS

IEEE 802.11n-2009 内で定義される MCS（Modulation and Coding Scheme）は、変調方式、コーディング、および NSS を決定する値です。

I. MCS タイプ

802.11 n MCS は、次のタイプに分類されます。

- Mandatory MCS-AP で必須となる MCS。802.11 n AP に関連付けるには、クライアントが AP の Mandatory MCS をサポートしている必要があります。

- Supported MCS- Mandatory MCS 以外に AP でサポートされる MCS。クライアントが Mandatory MCS と Supported MCS の両方をサポートする場合、クライアントはサポートされるレートを使用して AP と通信できます。
- Multicast MCS-AP がマルチキャストフレームを送信するレートの MCS。

II. MCS パラメータ

MCS は MCS インデックスにより指定され、MCS インデックスは 0～76 の整数で示されます。MCS パラメータは、MCS インデックスからデータ速度までをマッピングしたものです。

表 1-2～表 1-9 は、20 MHz と 40 MHz の両方に対する MCS パラメータの例を示します。

帯域幅モードが 20 MHz のとき、0～15 の MCS インデックスは AP に対して必須であり、0～7 の MCS インデックスはクライアントに対して必須です。

表 1-2 表 2 MCS パラメータ （20 MHz, NSS=1）

MCS インデックス	NSS	変調方式	データ速度（Mbps）	
			800 ns GI	400 ns GI
0	1	BPSK	6.5	7.2
1	1	QPSK	13.0	14.4
2	1	QPSK	19.5	21.7
3	1	16-QAM	26.0	28.9
4	1	16-QAM	39.0	43.3
5	1	64-QAM	52.0	57.8
6	1	64-QAM	58.5	65.0
7	1	64-QAM	65.0	72.2

表 1-3 MCS パラメータ （20 MHz, NSS=2）

MCS インデックス	NSS	変調方式	データ速度（Mbps）	
			800 ns GI	400 ns GI
8	2	BPSK	13.0	14.4
9	2	QPSK	26.0	28.9
10	2	QPSK	39.0	43.3
11	2	16-QAM	52.0	57.8
12	2	16-QAM	78.0	86.7
13	2	64-QAM	104.0	115.6
14	2	64-QAM	117.0	130.0
15	2	64-QAM	130.0	144.4

表 1-4 MCS パラメータ （20 MHz, NSS=3）

MCS インデックス	NSS	変調方式	データ速度（Mbps）	
			800 ns GI	400 ns GI
16	3	BPSK	19.5	21.7
17	3	QPSK	39.0	43.3
18	3	QPSK	58.5	65.0
19	3	16-QAM	78.0	86.7
20	3	16-QAM	117.0	130.0
21	3	64-QAM	156.0	173.3
22	3	64-QAM	175.5	195.0
23	3	64-QAM	195.0	216.7

表 1-5 MCS パラメータ （20 MHz, NSS=4）

MCS インデックス	NSS	変調方式	データ速度（Mbps）	
			800 ns GI	400 ns GI
24	4	BPSK	26.0	28.9
25	4	QPSK	52.0	57.8
26	4	QPSK	78.0	86.7
27	4	16-QAM	104.0	115.6
28	4	16-QAM	156.0	173.3
29	4	64-QAM	208.0	231.1
30	4	64-QAM	234.0	260.0
31	4	64-QAM	260.0	288.9

表 1-6 MCS パラメータ （40 MHz, NSS=1）

MCS インデックス	NSS	変調方式	データ速度（Mbps）	
			800 ns GI	400 ns GI
0	1	BPSK	13.5	15.0
1	1	QPSK	27.0	30.0
2	1	QPSK	40.5	45.0
3	1	16-QAM	54.0	60.0
4	1	16-QAM	81.0	90.0
5	1	64-QAM	108.0	120.0
6	1	64-QAM	121.5	135.0
7	1	64-QAM	135.0	150.0

表 1-7 MCS パラメータ （40 MHz, NSS=2）

MCS インデックス	NSS	変調方式	データ速度（Mbps）	
			800 ns GI	400 ns GI
8	2	BPSK	27.0	30.0
9	2	QPSK	54.0	60.0
10	2	QPSK	81.0	90.0
11	2	16-QAM	108.0	120.0
12	2	16-QAM	162.0	180.0
13	2	64-QAM	216.0	240.0
14	2	64-QAM	243.0	270.0
15	2	64-QAM	270.0	300.0

表 1-8 MCS パラメータ （40 MHz, NSS=3）

MCS インデックス	NSS	変調方式	データ速度（Mbps）	
			800 ns GI	400 ns GI
16	3	BPSK	40.5	45.0
17	3	QPSK	81.0	90.0
18	3	QPSK	121.5	135.0
19	3	16-QAM	162.0	180.0
20	3	16-QAM	243.0	270.0
21	3	64-QAM	324.0	360.0
22	3	64-QAM	364.5	405.0
23	3	64-QAM	405.0	450.0

表 1-9 MCS パラメータ （40 MHz, NSS=4）

MCS インデックス	NSS	変調方式	データ速度（Mbps）	
			800 ns GI	400 ns GI
24	4	BPSK	54.0	60.0
25	4	QPSK	108.0	120.0
26	4	QPSK	162.0	180.0
27	4	16-QAM	216.0	240.0
28	4	16-QAM	324.0	360.0
29	4	64-QAM	432.0	480.0
30	4	64-QAM	486.0	540.0
31	4	64-QAM	540.0	600.0

🕮 **メモ：**

- MCS データ速度については IEEE 802.11n-2009 を参照してください。
- MCS インデックスのサポートは、デバイスモデルによって異なります。

1.1.6 VHT-MCS

802.11ac は、無線データ速度を示すために、VHT-MCS（Very High Throughput Modulation and Coding Scheme）インデックスを使用します。

I. VHT-MCS タイプ

802.11 ac VHT-MCS は、次のタイプに分類されます。

- Mandatory VHT-MCS—AP の必須 VHT-MCS。802.11 ac AP と関連付けるには、クライアントが AP の Mandatory VHT-MCS をサポートする必要があります。
- Supported VHT-MCS—Mandatory VHT-MCS 以外に AP でサポートされる VHT-MCS。クライアントが Mandatory VHT-MCS と Supported VHT-MCS の両方をサポートしている場合、クライアントはサポートされているレートを使用して AP と通信できます。
- Multicast VHT-MCS—AP がマルチキャストフレームを送信するレートの VHT-MCS。

II. VHT-MCS のパラメータ

VHT-MCS は VHT-MCS インデックスにより識別され、VHT-MCS インデックスは 0～9 の整数で表されます。VHT-MCS パラメータは、VHT-MCS インデックスからデータ速度までをマッピングしたものです。

802.11ac は 20 MHz、40 MHz、80MHz、160 MHz の帯域幅モードをサポートし、最大で 8 つの空間ストリームをサポートします。802.11gac は 20 MHz、40 MHz の帯域幅モードをサポートします。

表 1-10～表 1-21 は、AP にサポートされた VHT-MCS パラメータを示します。

表 1-10 VHT-MCS パラメータ （20 MHz, NSS=1）

VHT-MCS インデックス	変調方式	データ速度（Mbps）	
		800 ns GI	400 ns GI
0	BPSK	6.5	7.2
1	QPSK	13.0	14.4
2	QPSK	19.5	21.7
3	16-QAM	26.0	28.9
4	16-QAM	39.0	43.3
5	64-QAM	52.0	57.8
6	64-QAM	58.5	65.0
7	64-QAM	65.0	72.2
8	256-QAM	78.0	86.7
9	無効		

表 1-11 VHT-MCS パラメータ （20 MHz, NSS=2）

VHT-MCS インデックス	変調方式	データ速度（Mbps）	
		800 ns GI	400 ns GI
0	BPSK	13.0	14.4
1	QPSK	26.0	28.9
2	QPSK	39.0	43.3
3	16-QAM	52.0	57.8
4	16-QAM	78.0	86.7
5	64-QAM	104.0	115.6
6	64-QAM	117.0	130.0
7	64-QAM	130.0	144.4
8	256-QAM	156.0	173.3
9	無効		

表 1-12 VHT-MCS パラメータ （20 MHz, NSS=3）

VHT-MCS インデックス	変調方式	データ速度（Mbps）	
		800 ns GI	400 ns GI
0	BPSK	19.5	21.7
1	QPSK	39.0	43.3
2	QPSK	58.5	65.0
3	16-QAM	78.0	86.7
4	16-QAM	117.0	130.0
5	64-QAM	156.0	173.3
6	64-QAM	175.5	195.0
7	64-QAM	195.0	216.7
8	256-QAM	234.0	260.0
9	256-QAM	260.0	288.9

表 1-13 VHT-MCS パラメータ （20 MHz, NSS=4）

VHT-MCS インデックス	変調方式	データ速度（Mbps）	
		800 ns GI	400 ns GI
0	BPSK	26.0	28.9
1	QPSK	52.0	57.8
2	QPSK	78.0	86.7
3	16-QAM	104.0	115.6

VHT-MCS インデックス	変調方式	データ速度（Mbps）	
		800 ns GI	400 ns GI
4	16-QAM	156.0	173.3
5	64-QAM	208.0	231.1
6	64-QAM	234.0	260.0
7	64-QAM	260.0	288.9
8	256-QAM	312.0	346.7
9	無効		

表 1-14 VHT-MCS パラメータ （40 MHz, NSS=1）

VHT-MCS インデックス	変調方式	データ速度（Mbps）	
		800 ns GI	400 ns GI
0	BPSK	13.5	15.0
1	QPSK	27.0	30.0
2	QPSK	40.5	45.0
3	16-QAM	54.0	60.0
4	16-QAM	81.0	90.0
5	64-QAM	108.0	120.0
6	64-QAM	121.5	135.0
7	64-QAM	135.0	150.0
8	256-QAM	162.0	180.0
9	256-QAM	180.0	200.0

表 1-15 VHT-MCS パラメータ （40 MHz, NSS=2）

VHT-MCS インデックス	変調方式	データ速度（Mbps）	
		800 ns GI	400 ns GI
0	BPSK	27.0	30.0
1	QPSK	54.0	60.0
2	QPSK	81.0	90.0
3	16-QAM	108.0	120.0
4	16-QAM	162.0	180.0
5	64-QAM	216.0	240.0
6	64-QAM	243.0	270.0
7	64-QAM	270.0	300.0
8	256-QAM	324.0	360.0
9	256-QAM	360.0	400.0

表 1-16 VHT-MCS パラメータ （40 MHz, NSS=3）

VHT-MCS インデックス	変調方式	データ速度（Mbps）	
		800 ns GI	400 ns GI
0	BPSK	40.5	45.0
1	QPSK	81.0	90.0
2	QPSK	121.5	135.0
3	16-QAM	162.0	180.0
4	16-QAM	243.0	270.0
5	64-QAM	324.0	360.0
6	64-QAM	364.5	405.0
7	64-QAM	405.0	450.0
8	256-QAM	486.0	540.0

VHT-MCS インデックス	変調方式	データ速度（Mbps）	
		800 ns GI	400 ns GI
9	256-QAM	540.0	600.0

表 1-17 VHT-MCS パラメータ （40 MHz, NSS=4）

VHT-MCS インデックス	変調方式	データ速度（Mbps）	
		800 ns GI	400 ns GI
0	BPSK	54.0	60.0
1	QPSK	108.0	120.0
2	QPSK	162.0	180.0
3	16-QAM	216.0	240.0
4	16-QAM	324.0	360.0
5	64-QAM	432.0	480.0
6	64-QAM	486.0	540.0
7	64-QAM	540.0	600.0
8	256-QAM	648.0	720.0
9	256-QAM	720.0	800.0

表 1-18 VHT-MCS パラメータ （80 MHz, NSS=1）

VHT-MCS インデックス	変調方式	データ速度（Mbps）	
		800 ns GI	400 ns GI
0	BPSK	29.3	32.5
1	QPSK	58.5	65.0
2	QPSK	87.8	97.5
3	16-QAM	117.0	130.0
4	16-QAM	175.5	195.0
5	64-QAM	234.0	260.0
6	64-QAM	263.0	292.5
7	64-QAM	292.5	325.0
8	256-QAM	351.0	390.0
9	256-QAM	390.0	433.3

表 1-19 VHT-MCS パラメータ （80 MHz, NSS=2）

VHT-MCS インデックス	変調方式	データ速度（Mbps）	
		800 ns GI	400 ns GI
0	BPSK	58.5	65.0
1	QPSK	117.0	130.0
2	QPSK	175.5	195.0
3	16-QAM	234.0	260.0
4	16-QAM	351.0	390.0
5	64-QAM	468.0	520.0
6	64-QAM	526.5	585.0
7	64-QAM	585.0	650.0
8	256-QAM	702.0	780.0
9	256-QAM	780.0	866.7

表 1-20 VHT-MCS パラメータ （80 MHz, NSS=3）

VHT-MCS インデックス	変調方式	データ速度（Mbps）	
		800 ns GI	400 ns GI
0	BPSK	87.8	97.5
1	QPSK	175.5	195.0
2	QPSK	263.3	292.5
3	16-QAM	351.0	390.0
4	16-QAM	526.5	585.0
5	64-QAM	702.0	780.0
6	無効		
7	64-QAM	877.5	975.0
8	256-QAM	1053.0	1170.0
9	256-QAM	1170.0	1300.0

表 1-21 VHT-MCS パラメータ （80 MHz, NSS=4）

VHT-MCS インデックス	変調方式	データ速度（Mbps）	
		800 ns GI	400 ns GI
0	BPSK	117.0	130.0
1	QPSK	234.0	260.0
2	QPSK	351.0	390.0
3	16-QAM	468.0	520.0
4	16-QAM	702.0	780.0
5	64-QAM	936.0	1040.0
6	64-QAM	1053.0	1170.0
7	64-QAM	1170.0	1300.0
8	256-QAM	1404.0	1560.0
9	256-QAM	1560.0	1733.3

🕮 **メモ：**

VHT-MCS データ速度については IEEE 802.11ac-2013 を参照してください。

1.1.7 HE-MCS

802.11ax は、無線データ速度を示すために、HE-MCS（High Efficiency Modulation and Coding Scheme）インデックスを使用します。

I. HE-MCS のタイプ

802.11 ax HE-MCS は、次のタイプに分類されます。

- Mandatory HE-MCS—AP に必須の HE-MCS。802.11 ax AP と関連付けるには、クライアントが AP に必須の HE-MCS をサポートする必要があります。
- Supported HE-MCS—Mandatory HE-MCS 以外に、AP でサポートされる HE-MCS。クライアントが Mandatory HE-MCS と Supported HE-MCS の両方をサポートしている場合、クライアントはサポートされているレートを使用して AP と通信できます。
- Multicast HE-MCS—AP がマルチキャストフレームを送信するレートの HE-MCS。

II. HE-MCS のパラメータ

HE-MCS は、0～11 の整数で表される HE-MCS インデックスによって識別されます。HE-MCS パラメータは、HE-MCS インデックスからデータ速度までをマッピングしたものです。

802.11ax は、20 MHz、40 MHz、80 MHz、および 160 MHz の帯域幅モードをサポートし、最大 8 つの空間ストリームをサポートします。802.11gax は、20MHz および 40MHz の帯域幅モードをサポートします。

表 1-22～表 1-33 に、AP でサポートされている HE-MCS パラメータを示します。

表 1-22 HE-MCS パラメータ（20 MHz, NSS =1）

HE-MCS インデックス	NSS	変調方式	データ速度（Mbps）	
			1600 ns GI	800 ns GI
0	1	BPSK	8.0	8.6
1	1	QPSK	16.0	17.2
2	1	QPSK	24.0	25.8
3	1	16-QAM	33.0	34.4
4	1	16-QAM	49.0	51.6
5	1	64-QAM	65.0	68.8
6	1	64-QAM	73.0	77.4
7	1	64-QAM	81.0	86.0
8	1	256-QAM	98.0	103.2
9	1	256-QAM	108.0	114.7
10	1	1024-QAM	122.0	129.0
11	1	1024-QAM	135.0	143.4

表 1-23 HE-MCS パラメータ（20 MHz, NSS =2）

HE-MCS インデックス	NSS	変調方式	データ速度（Mbps）	
			1600 ns GI	800 ns GI
0	2	BPSK	16.0	17.2
1	2	QPSK	32.0	34.4
2	2	QPSK	48.0	51.6
3	2	16-QAM	66.0	68.8
4	2	16-QAM	98.0	103.2
5	2	64-QAM	130.0	137.6
6	2	64-QAM	146.0	154.8
7	2	64-QAM	162.0	172.0
8	2	256-QAM	196.0	206.4
9	2	256-QAM	216.0	229.4
10	2	1024-QAM	244.0	258.0
11	2	1024-QAM	270.0	286.8

表 1-24 HE-MCS パラメータ（20 MHz, NSS =3）

HE-MCS インデックス	NSS	変調方式	データ速度（Mbps）	
			1600 ns GI	800 ns GI
0	3	BPSK	24.0	25.8
1	3	QPSK	48.0	51.6
2	3	QPSK	72.0	77.4
3	3	16-QAM	99.0	103.2

HE-MCS インデックス	NSS	変調方式	データ速度（Mbps）	
			1600 ns GI	800 ns GI
4	3	16-QAM	147.0	154.8
5	3	64-QAM	195.0	206.4
6	3	64-QAM	219.0	232.2
7	3	64-QAM	243.0	258.0
8	3	256-QAM	294.0	309.6
9	3	256-QAM	324.0	344.1
10	3	1024-QAM	366.0	387.0
11	3	1024-QAM	405.0	430.2

表 1-25 HE-MCS パラメータ（20 MHz, NSS =4）

HE-MCS インデックス	NSS	変調方式	データ速度（Mbps）	
			1600 ns GI	800 ns GI
0	4	BPSK	32.0	34.4
1	4	QPSK	64.0	68.8
2	4	QPSK	96.0	103.2
3	4	16-QAM	132.0	137.6
4	4	16-QAM	196.0	206.4
5	4	64-QAM	260.0	275.2
6	4	64-QAM	292.0	309.6
7	4	64-QAM	324.0	344.0
8	4	256-QAM	392.0	412.8
9	4	256-QAM	432.0	458.8
10	4	1024-QAM	488.0	516.0
11	4	1024-QAM	540.0	573.6

表 1-26 HE-MCS パラメータ（40 MHz, NSS =1）

HE-MCS インデックス	NSS	変調方式	データ速度（Mbps）	
			1600 ns GI	800 ns GI
0	1	BPSK	16.0	17.2
1	1	QPSK	33.0	34.4
2	1	QPSK	49.0	51.6
3	1	16-QAM	65.0	68.8
4	1	16-QAM	98.0	103.2
5	1	64-QAM	130.0	137.6
6	1	64-QAM	146.0	154.9
7	1	64-QAM	163.0	172.1
8	1	256-QAM	195.0	206.5
9	1	256-QAM	217.0	229.4
10	1	1024-QAM	244.0	258.1
11	1	1024-QAM	271.0	286.8

表 1-27 HE-MCS パラメータ（40 MHz, NSS =2）

HE-MCS インデックス	NSS	変調方式	データ速度（Mbps）	
			1600 ns GI	800 ns GI
0	2	BPSK	32.0	34.4
1	2	QPSK	66.0	68.8
2	2	QPSK	98.0	103.2

HE-MCS インデックス	NSS	変調方式	データ速度（Mbps）	
			1600 ns GI	800 ns GI
3	2	16-QAM	130.0	137.6
4	2	16-QAM	196.0	206.4
5	2	64-QAM	260.0	275.2
6	2	64-QAM	292.0	309.8
7	2	64-QAM	326.0	344.2
8	2	256-QAM	390.0	413.0
9	2	256-QAM	434.0	458.8
10	2	1024-QAM	488.0	516.2
11	2	1024-QAM	542.0	573.6

表 1-28 HE-MCS パラメータ（40 MHz, NSS =3）

HE-MCS インデックス	NSS	変調方式	データ速度（Mbps）	
			1600 ns GI	800 ns GI
0	3	BPSK	48.0	51.6
1	3	QPSK	99.0	103.2
2	3	QPSK	147.0	154.8
3	3	16-QAM	195.0	206.4
4	3	16-QAM	294.0	309.6
5	3	64-QAM	390.0	412.8
6	3	64-QAM	438.0	464.7
7	3	64-QAM	489.0	516.3
8	3	256-QAM	585.0	619.5
9	3	256-QAM	651.0	688.2
10	3	1024-QAM	732.0	774.3
11	3	1024-QAM	813.0	860.4

表 1-29 HE-MCS パラメータ（40 MHz, NSS =4）

HE-MCS インデックス	NSS	変調方式	データ速度（Mbps）	
			1600 ns GI	800 ns GI
0	4	BPSK	64.0	68.8
1	4	QPSK	132.0	137.6
2	4	QPSK	196.0	206.4
3	4	16-QAM	260.0	275.2
4	4	16-QAM	392.0	412.8
5	4	64-QAM	520.0	550.4
6	4	64-QAM	584.0	619.6
7	4	64-QAM	652.0	688.4
8	4	256-QAM	780.0	826.0
9	4	256-QAM	868.0	917.6
10	4	1024-QAM	976.0	1032.4
11	4	1024-QAM	1084.0	1147.2

表 1-30 HE-MCS パラメータ（80 MHz, NSS =1）

HE-MCS インデックス	NSS	変調方式	データ速度（Mbps）	
			1600 ns GI	800 ns GI
0	1	BPSK	34.0	36.0
1	1	QPSK	68.0	72.1

HE-MCS インデックス	NSS	変調方式	データ速度（Mbps）	
			1600 ns GI	800 ns GI
2	1	QPSK	102.0	108.1
3	1	16-QAM	136.0	144.1
4	1	16-QAM	204.0	216.2
5	1	64-QAM	272.0	288.2
6	1	64-QAM	306.0	324.4
7	1	64-QAM	340.0	360.3
8	1	256-QAM	408.0	432.4
9	1	256-QAM	453.0	480.4
10	1	1024-QAM	510.0	540.4
11	1	1024-QAM	567.0	600.5

表 1-31 HE-MCS パラメータ（80 MHz, NSS =2）

HE-MCS インデックス	NSS	変調方式	データ速度（Mbps）	
			1600 ns GI	800 ns GI
0	2	BPSK	68.0	72.0
1	2	QPSK	136.0	144.2
2	2	QPSK	204.0	216.2
3	2	16-QAM	272.0	288.2
4	2	16-QAM	408.0	432.4
5	2	64-QAM	544.0	576.4
6	2	64-QAM	612.0	648.8
7	2	64-QAM	680.0	720.6
8	2	256-QAM	816.0	864.8
9	4	256-QAM	906.0	960.8
10	4	1024-QAM	1020.0	1080.8
11	4	1024-QAM	1134.0	1201.0

表 1-32 HE-MCS パラメータ（80 MHz, NSS =3）

HE-MCS インデックス	NSS	変調方式	データ速度（Mbps）	
			1600 ns GI	800 ns GI
0	3	BPSK	102.0	108.0
1	3	QPSK	204.0	216.3
2	3	QPSK	306.0	324.3
3	3	16-QAM	408.0	432.3
4	3	16-QAM	612.0	648.6
5	3	64-QAM	816.0	864.6
6	3	64-QAM	918.0	973.2
7	3	64-QAM	1020.0	1080.9
8	3	256-QAM	1224.0	1297.2
9	4	256-QAM	1359.0	1441.2
10	4	1024-QAM	1530.0	1621.2
11	4	1024-QAM	1701.0	1801.5

表 1-33 HE-MCS パラメータ（80 MHz, NSS =4）

HE-MCS インデックス	NSS	変調方式	データ速度（Mbps）	
			1600 ns GI	800 ns GI
0	4	BPSK	136.0	144.0

HE-MCS インデックス	NSS	変調方式	データ速度（Mbps）	
			1600 ns GI	800 ns GI
1	4	QPSK	272.0	288.4
2	4	QPSK	408.0	432.4
3	4	16-QAM	544.0	576.4
4	4	16-QAM	816.0	864.8
5	4	64-QAM	1088.0	1152.8
6	4	64-QAM	1224.0	1297.6
7	4	64-QAM	1360.0	1441.2
8	4	256-QAM	1632.0	1729.6
9	4	256-QAM	1812.0	1921.6
10	4	1024-QAM	2040.0	2161.6
11	4	1024-QAM	2268.0	2402.0

🕮 **メモ：**

- すべての HE-MCS データ速度については、IEEE802.11ax を参照してください。
- HE-MCS のサポートは、AP モデルによって異なります。

1.2 設定の制限とガイドライン

次の方法を使用して無線を設定できます。

- AP の無線ビューで 1 つずつ無線を設定します。
- AP グループに AP を割り当て、AP グループの無線ビューで AP グループの無線を設定します。
- グローバル設定ビューですべての無線を設定表示します。

設定の優先順位は radio view、AP group radio view、global configuration view の順番で優先します。

1.3 設定作業リスト

操作	補足
無線の有効化/無効化	
無線モードの指定	
基本的な無線機能の設定	
802.11n機能の設定	
802.11be機能の設定	
802.11ac/ax機能の設定	
6GHz帯の無線の設定	
スマートアンテナ機能の設定	

1.4 無線の有効化/無効化

1.4.1 すべての無線の有効化/無効化

⚠ **注意**：
すべての無線を無効にした場合、ワイヤレスサービスが終了します。無効にする場合は影響を十分に考慮して行ってください。

この機能は手動 AP とオンライン自動 AP でのみ適用します。

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． すべての無線を有効あるいは無効にする	**wlan radio** { **enable** | **disable** }	デフォルト：無線はradio viewあるいはAP group radio viewで有効にしない限り無効です。

1.4.2 radio view での無線の有効化/無効化

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP を作成し、AP view へ移行する	**wlan ap** *ap-name* [**model** *model-name*]	デフォルト：設定なし APを作成するときは名前とモデルを指定する必要があります。
3． radio view へ移行する	**radio** *radio-id*	—
4． 無線を有効あるいは無効にする	**radio** { **enable** | **disable** }	デフォルト：**wlan radio enable**コマンドがsystem viewで実行されている場合、有効です。実行されていない場合、AP group radio viewの設定を使用します。

1.4.3 AP group view での無線の有効化/無効化

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP グループを作成し、AP group view を入力する	**wlan ap-group** *group-name*	デフォルト：デフォルトAPグループ（default-group）が存在し、デフォルトAPグループは削除することができません。
3． AP model view へ移行する	**ap-model** *ap-model*	—

操作	コマンド	補足
4． radio view へ移行する	**radio** *radio-id*	—
5． 無線を有効にする	**radio** { **enable** | **disable** }	デフォルト：**wlan radio enable**コマンドがsystem viewで実行されていない場合、無効です。

1.5 無線モードの指定

⚠ **注意**：

有効化した無線モードを修正すると、関連したすべてのクライアントがログオフになります。

🕮 **メモ**：

- 有効化した無線モードを修正すると、関連したすべてのクライアントがログオフになります。QX-W1100 シリーズは Raido3 で 802.11a、ac、an も指定できますが設定した場合 Raido3 が無効になります。
- QX-W1120 は Radio3 で 802.11gax を設定することができません。Radio 3 を 802.11a、ac、an のいずれかに設定することで、Radio 2 を 802.11gax に設定することができます。

無線モードに応じてチャネルと伝送電力をサポートします。無線モードを変更するとき、システムはチャネルと電力パラメータを自動で無線に適用します。

I. radio view での無線モードの指定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP を作成し、AP view へ移行する	**wlan ap** *ap-name* [**model** *model-name*]	デフォルト：設定なし APを作成するときは名前とモデルを指定する必要があります。
3． radio view へ移行する	**radio** *radio-id*	—
4． 無線モードを指定する	**type** { **dot11a** | **dot11ac** | **dot11an** | **dot11ax** | **dot11b** | **dot11g** | **dot11gac** | **dot11gax** | **dot11gn** }	デフォルト：無線はAP group viewの設定を使用します。

II. AP group view での無線モードの指定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP グループを作成し、AP group view を入力する	**wlan ap-group** *group-name*	デフォルト：デフォルトAPグループ（default-group）が存在し、デフォルトAPグループは削除することができません。

操作	コマンド	補足
3． AP model view へ移行する	**ap-model** *ap-model*	—
4． radio view へ移行する	**radio** *radio-id*	—
5． 無線モードを指定する	**type** { **dot11a** | **dot11ac** | **dot11an** | **dot11ax** | **dot11b** | **dot11g** | **dot11gac** | **dot11gax** | **dot11gn** }	デフォルト：APモデルにより異なります。

1.6 基本的な無線機能の設定

1.6.1 作動チャネルの指定

無線装置と非無線装置の両方からのインタフェースを削減するためにこのタスクを実行します。

無線チャネルを選択するため、手動もしくはシステムで自動に設定することができます。

レーダー信号が無線の作動チャネル上で検出されると、以下の事象のいずれかが発生します。

- チャネルが手動で指定されている場合、無線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、静止タイマが起動します。静止時間内にレーダー信号が検出されなければ、無線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、無線はチャネルを変更します。
- チャネルが自動的に割り当てられている場合、無線はチャネルを変更します。

I. radio view での作動チャネルの指定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP を作成し、AP view へ移行する	**wlan ap** *ap-name* [**model** *model-name*]	デフォルト：設定なし APを作成するときは名前とモデルを指定する必要があります。
3． radio view へ移行する	**radio** *radio-id*	—
4． 作動チャネルを指定する	**channel** { *channel-number* | **auto** { **lock** | **unlock** } }	デフォルト：無線はAP group viewの設定を使用します。

II. AP group view での作動チャネルの指定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP グループを作成し、AP group view を入力する	**wlan ap-group** *group-name*	デフォルト：デフォルトAPグループ（default-group）が存在し、デフォルトAPグループは削除することができません。

操作	コマンド	補足
3． AP model view へ移行する	**ap-model** *ap-model*	—
4． radio view へ移行する	**radio** *radio-id*	—
5． 作動チャネルを指定する	**channel** { *channel-number* | **auto** { **lock** | **unlock** } }	デフォルト：ACは無線に対して自動でチャネルを選択し、ロックしません。

1.6.2 ブラックリスト、ホワイトリストのチャネル選択の設定

この機能を行うと、AP で自動チャネルを使用するとき、ブラックリストのチャネルを選択しない、あるいはホワイトリストのチャネルのみ選択することができます。同一 AP でブラックリストとホワイトリストのチャネルの両方を設定することはできません。

I. radio view でのブラックリスト、ホワイトリストのチャネル選択の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP を作成し、AP view へ移行する	**wlan ap** *ap-name* [**model** *model-name*]	—
3． radio view へ移行する	**radio** *radio-id*	—
4． ブラックリスト、ホワイトリストのチャネル選択を設定する	**channel auto-select** { **blacklist** | **whitelist** } *channel-number*	デフォルト：無線はAP group viewの設定を使用します。

II. AP group view でのブラックリスト、ホワイトリストのチャネル選択の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP グループを作成し、AP group view を入力する	**wlan ap-group** *group-name*	—
3． radio view へ移行する	**radio** *radio-id*	—
4． ブラックリスト、ホワイトリストのチャネル選択を設定する	**channel auto-select** { **blacklist** | **whitelist** } *channel-number*	デフォルト：設定なし

1.6.3 アンテナタイプの設定

🕮 **メモ：**

AP にサポートされたアンテナタイプは、装置モデルにより変わります。

AP がサードパーティ（第三者）製のアンテナを使用する場合、AP が使用するアンテナのタイプに設定しなければなりません。

伝送電力が適切な範囲内で保証するようにアンテナタイプを設定したあと、アンテナゲインは自動で変更します。

I. radio view でのアンテナタイプの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP を作成し、AP view へ移行する	**wlan ap** *ap-name* [**model** *model-name*]	デフォルト：設定なし APを作成するときはAP名とモデルを指定する必要があります。
3． radio view へ移行する	**radio** *radio-id*	—
4． アンテナタイプを設定する	**antenna type** *antenna-type*	デフォルト：無線はAP group viewの設定を使用します。

II. AP group view でのアンテナタイプの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP グループを作成し、AP group view を入力する	**wlan ap-group** *group-name*	デフォルト：デフォルトAPグループ（default-group）が存在し、デフォルトAPグループは削除することができません。
3． AP model view へ移行する	**ap-model** *ap-model*	—
4． radio view へ移行する	**radio** *radio-id*	—
5． アンテナタイプを設定する	**antenna type** *antenna-type*	デフォルト：装置モデルによって異なります。

1.6.4 最大伝送電力の設定

最大伝送電力が、無線にサポートされた伝送電力範囲内であることを確認します。無線にサポートされた伝送電力範囲は、カントリーコード、チャネル、AP モデル、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、無線に対するこれらの特性を変更する場合、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を超える可能性があります。範囲を超えた場合、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。

電力ロックを有効にする場合、ロックされた電力が最大伝送電力になります。電力ロックに関する詳細な情報については、本章の *“電力ロックの設定”* を参照してください。

I. radio view での最大伝送電力の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—

操作	コマンド	補足
2． AP を作成し、AP view へ移行する	**wlan ap** *ap-name* [**model** *model-name*]	デフォルト：設定なし APを作成するときは名前とモデルを指定する必要があります。
3． radio view へ移行する	**radio** *radio-id*	—
4． 最大伝送電力を設定する	**max-power** *radio-power*	デフォルト：無線はAP group viewの設定を使用します。

II. AP group view での最大伝送電力の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP グループを作成し、AP group view を入力する	**wlan ap-group** *group-name*	デフォルト：デフォルトAPグループ（default-group）が存在し、デフォルトAPグループは削除することができません。
3． AP model view へ移行する	**ap-model** *ap-model*	—
4． radio view へ移行する	**radio** *radio-id*	—
5． 最大伝送電力を設定する	**max-power** *radio-power*	デフォルト：無線はサポートされた最大伝送電力を使用します。

1.6.5 電力ロックの設定

電力ロックを有効にする場合、現在の電力はロックされ、最大伝送電力となります。ロックされた電力は、AC を再始動したのちも適用されます。

電力ロックを有効にした無線が、ロックされた電力より低い電力を供給する新たなチャネルに切り替わる場合、新規のチャネルによってサポートされた最大電力が適用されます。

I. radio view での電力ロックの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP を作成し、AP view へ移行する	**wlan ap** *ap-name* [**model** *model-name*]	デフォルト：設定なし APを作成するときは名前とモデルを指定する必要があります。
3． radio view へ移行する	**radio** *radio-id*	—
4． 電力ロックを設定する	**power-lock** { **disable** | **enable** }	デフォルト：無線はAP group viewの設定を使用します。

II. AP group view での電力ロックの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP グループを作成し、AP group view を入力する	**wlan ap-group** *group-name*	デフォルト：デフォルトAP グループ（default-group）が存在し、デフォルトAPグループは削除することができません。
3． AP model view へ移行する	**ap-model** *ap-model*	—
4． radio view へ移行する	**radio** *radio-id*	—
5． 電力ロックを設定する	**power-lock** { **disable** | **enable** }	デフォルト：無効

1.6.6 伝送速度の設定

伝送速度は以下のタイプに分類されます。

- **禁止速度**—AP により使用できない速度です。
- **必須速度**—AP と関連づけ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です。
- **サポート速度**—AP がサポートする速度です。クライアントが AP と関連づけられたたあと、クライアントは AP と接続するために、サポートされた速度より高い速度を選択することができます。多くのインタフェース、再伝送、あるいはパケット廃棄を検出したとき、AP は自動的に伝送速度を低減します。また少ないインタフェース、再伝送、パケット廃棄を検出したとき、自動的に伝送速度を増加します。
- **マルチキャスト速度**—AP 伝送マルチキャストとブロードキャストが伝送する速度です。マルチキャスト速度は必須速度から選択する必要があります。

I. radio view での伝送速度の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP を作成し、AP view へ移行する	**wlan ap** *ap-name* [**model** *model-name*]	デフォルト：設定なし APを作成するときは名前とモデルを指定する必要があります。
3． radio view へ移行する	**radio** *radio-id*	—
4． 無線に伝送速度を設定する	**rate** { **multicast** { **auto** | *rate-value* } | { **disabled** | **mandatory** | **supported** } *rate-value* }	デフォルト：無線はAP group viewの設定を使用します。

II. AP group view での伝送速度の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—

操作	コマンド	補足
2. AP グループを作成し、AP group view を入力する	**wlan ap-group** *group-name*	デフォルト：デフォルトAPグループ（default-group）が存在し、デフォルトAPグループは削除することができません。
3. AP model view へ移行する	**ap-model** *ap-model*	—
4. radio view へ移行する	**radio** *radio-id*	—
5. 無線に伝送速度を設定する	**rate** { **multicast** { **auto** | *rate-value* } | { **disabled** | **mandatory** | **supported** } *rate-value* }	デフォルト： ● 802.11a/802.11an/802.11ac/802.11ax無線： • **禁止速度**：なし • **必須速度**：6、12、24 • **マルチキャスト速度**：必須速度から選択します。 • **サポート速度**：9、18、36、48、54 ● 802.11b 無線： • **禁止速度**：なし • **必須速度**：1、2 • **マルチキャスト速度**：必須速度から選択します。 • **サポート速度**：5.5、11 ● 802.11g/802.11gn/802.11gac/802.11gax無線： • **禁止速度**：なし • **必須速度**：1、2、5.5、11 • **マルチキャスト速度**：必須速度から選択します。 • **サポート速度**：9、12、18、24、36、48、54

1.6.7 ビーコン間隔の設定

AP が、指定された間隔でビーコンフレームをブロードキャストできるように、ビーコン間隔を設定します。小さなビーコン間隔により、クライアントは AP を容易に検出することができますが、より多くのシステムリソースを消費します。

I. radio view でのビーコン間隔の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP を作成し、AP view へ移行する	**wlan ap** *ap-name* [**model** *model-name*]	デフォルト：設定なし APを作成するときは名前とモデルを指定する必要があります。
3． radio view へ移行する	**radio** *radio-id*	—
4． ビーコン間隔を設定する	**beacon-interval** *interval*	デフォルト：無線はAP group viewの設定を使用します。

II. AP group view でのビーコン間隔の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP グループを作成し、AP group view へ移行する	**wlan ap-group** *group-name*	デフォルト：デフォルトAP グループ（default-group）が存在し、デフォルトAPグループは削除することができません。
3． AP model view へ移行する	**ap-model** *ap-model*	—
4． radio view へ移行する	**radio** *radio-id*	—
5． ビーコン間隔を設定する	**beacon-interval** *interval*	デフォルト：100 TU

1.6.8 衝突回避モードの指定

無線装置は半二重モードで作動し、データの送受信を同時に行うことはできません。802.11 により、衝突を回避するために、無線装置は RTS（Request to Send）パケットもしくは CTS（Clear to Send）パケットを送信できるようになります。

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、クライアントにデータを送信する前に、RTS パケットを送信します。RTS パケットを受信したあと、クライアントは CTS パケットを AP に送信します。CTS パケット受信後、AP はデータの送信を開始します。また、その RTS パケットもしくは CTS パケットを検出した別の装置が、指定された時間内にデータを送信することはありません。

🕮 **メモ：**

802.11b 無線は RTS/CTS モードのみサポートします。

- **CTS-to-self**－AP は、クライアントにデータを送信する前に、CTS パケットを送信します。この CTS パケットには、AP 自体の MAC アドレスが宛先 MAC アドレスとして付随されています。CTS-to-self パケット受信後、AP はデータの送信を開始します。また、その CTS-to-self パケットを受信した別の装置が、指定された時間内にデータ

を送信することはありません。CTS-to-self モードにより伝送時間は減少しますが、隠れたノード問題を引き起こす可能性があります。

無線リソース効率を保証するために、以下の条件が満たされるときに限り衝突回避が適用されます。

- 送信されるパケットが、RTS しきい値 2346 バイトより長い場合。
- 802.11g 保護もしくは 802.11n 保護が有効な場合。802.11g 保護もしくは 802.11n 保護に関する詳細な情報は、本章の *"802.11g 保護の設定"* と *"802.11n 保護の設定"* を参照してください。

I. radio view での衝突回避モードの指定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP view へ移行する	**wlan ap** *ap-name* [**model** *model-name*]	—
3. radio view へ移行する	**radio** *radio-id*	—
4. 衝突回避モードを指定する	**protection-mode** { **cts-to-self** | **rts-cts** }	デフォルト：無線はAP group viewの設定を使用します。

II. AP group view での衝突回避モードの指定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP group view へ移行する	**wlan ap-group** *group-name*	—
3. AP model view へ移行する	**ap-model** *ap-model*	—
4. radio view へ移行する	**radio** *radio-id*	—
5. 衝突回避モードを指定する	**protection-mode** { **cts-to-self** | **rts-cts** }	デフォルト：CTS-to-selfモード

1.6.9 RTS しきい値の設定

802.11 により、無線装置は衝突回避のために RTS パケットもしくは CTS パケットを送信できるようになります。しかし、過度な RTS パケットや CTS パケットはシステムリソースの過剰消費の原因となり、伝送効率を低下させます。この問題を解決するために、RTS しきい値を設定することができます。このシステムは、パケットが RTS しきい値より大きい場合に限り衝突回避を実行します。

低密度 WLAN 内では、ネットワークの処理能力と効率を向上させるために RTS しきい値を増加させます。

高密度 WLAN 内では、ネットワーク内の衝突を減少させるために RTS しきい値を低下させます。

I. radio view での RTS しきい値の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—

操作	コマンド	補足
2． AP view へ移行する	**wlan ap** *ap-name* [**model** *model-name*]	—
3． radio view へ移行する	**radio** *radio-id*	—
4． RTS しきい値を設定する	**protection-threshold** size	デフォルト：無線はAP group viewの設定を使用します。

II. AP group view での RTS しきい値の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP group view へ移行する	**wlan ap-group** *group-name*	—
3． AP model view へ移行する	**ap-model** *ap-model*	—
4． radio view へ移行する	**radio** *radio-id*	—
5． RTS しきい値を設定する	**protection-threshold** *size*	デフォルト： 2346 バイト

1.6.10 フラグメンテーションしきい値の設定

フラグメンテーションのしきい値より大きいフレームは、伝送の前にフラグメントされます。フラグメンテーションのしきい値より小さいフレームは、フラグメントされずに伝送されます。

多くのインタフェースを有する WLAN 内では、ネットワーク処理能力と効率を向上させるために、フラグメンテーションのしきい値を低く設定してください。

I. radio view でのフラグメンテーションしきい値の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP view へ移行する	**wlan ap** *ap-name* [**model** *model-name*]	—
3． radio view へ移行する	**radio** *radio-id*	—
4． フラグメンテーションしきい値を設定する	**fragment-threshold** size	デフォルト：無線はAP group viewの設定を使用します。

II. AP group view でのフラグメンテーションしきい値の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP group view へ移行する	**wlan ap-group** *group-name*	—
3． AP model view へ移行する	**ap-model** *ap-model*	—
4． radio view へ移行する	**radio** *radio-id*	—
5． フラグメンテーションしきい値を設定する	**fragment-threshold** *size*	デフォルト： 2346バイト

1.6.11 ハードウェア再伝送の最大数の設定

無線ネットワークにおいて、ユニキャストフレームは Acknowledgement を必要とします。装置がパケットに対する Acknowledgement の受信に失敗した場合、装置はパケットを再伝送します。

装置が Acknowledgement の受信に失敗しつづけ、フレーム再伝送の最大値に達した場合、装置はパケットを破棄し上位レイヤに伝送失敗のプロトコルを通知します。

ハードウェア再伝送の最大数の値を、大きいフレームと小さいフレームに対して異なる値で設定することができます。大きいフレームとは、RTS しきい値より大きいフレームを示し、小さいフレームとは、RTS しきい値以下のフレームを示します。

大きいフレームの伝送には、大きなバッファサイズと長い時間が必要となります。なぜなら、システムは大きなフレームを伝送する前に、衝突回避を実行しなければならないからです。したがって、システムバッファと伝送時間を節約するために、大きなフレームに対するハードウェア再伝送の最大数を小さくすることができます。

I. radio view でのフレーム再伝送の最大数の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP view へ移行する	**wlan ap** *ap-name* [**model** *model-name*]	—
3． radio view へ移行する	**radio** *radio-id*	—
4． 小さいフレームに対するフレーム再伝送の最大数を設定する	**short-retry threshold** *count*	デフォルト：無線はAP group viewの設定を使用します。
5． 大きいフレームに対するフレーム再伝送の最大数を設定する	**long-retry threshold** *count*	デフォルト：無線はAP group viewの設定を使用します。

II. AP group view でのフレーム再伝送の最大数の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP group view へ移行する	**wlan ap-group** *group-name*	—
3． AP model view へ移行する	**ap-model** *ap-model*	—
4． radio view へ移行する	**radio** *radio-id*	—
5． 小さいフレームに対するフレーム再伝送の最大数を設定する	**short-retry threshold** *count*	デフォルト：7
6． 大きいフレームに対するフレーム再伝送の最大数を設定する	**long-retry threshold** *count*	デフォルト：4

1.6.12 AP に関連づけるクライアントの最大数の設定

クライアントの数が AP 上で最大になると、AP は新たなクライアントの許可を停止します。これにより、AP に過負荷がかかることを防ぎます。

I. radio view での AP に関連づけるクライアントの最大数の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP を作成し、AP view へ移行する	**wlan ap** *ap-name* [**model** *model-name*]	デフォルト：設定なし APを作成するときは名前とモデルを指定する必要があります。
3． radio view へ移行する	**radio** *radio-id*	—
4． AP に関連づけるクライアントの最大数を設定する	**client max-count** *max-number*	デフォルト：無線はAP group viewの設定を使用します。

II. AP group view での AP に関連づけるクライアントの最大数の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP グループを作成し、AP group view へ移行する	**wlan ap-group** *group-name*	デフォルト：デフォルトAPグループ（default-group）が存在し、デフォルトAPグループは削除することができません。
3． AP model view へ移行する	**ap-model** *ap-model*	—
4． radio view へ移行する	**radio** *radio-id*	—
5． AP に関連づけるクライアントの最大数を設定する	**client max-count** *max-number*	デフォルト：設定なし （各APの最大接続数）

1.6.13 802.11b クライアント拒否の設定

低速度の 802.11b クライアントの影響を軽減し、無線データ伝送の速度をあげるために、802.11g 無線、802.11gn 無線、802.11gac 無線、802.11gax 無線に 802.11b クライアントにアクセスするのを禁止するように設定できます。

I. radio view での 802.11b クライアント拒否の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP を作成し、AP view へ移行する	**wlan ap** *ap-name* [**model** *model-name*]	デフォルト：設定なし APを作成するときは名前とモデルを指定する必要があります。
3． radio view へ移行する	**radio** *radio-id*	—

操作	コマンド	補足
4． 802.11b クライアント拒否を設定する	**client dot11b-forbidden** { **disable** | **enable** }	デフォルト：無線はAP group viewの設定を使用します。

II. AP group view での 802.11b クライアント拒否の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP グループを作成し、AP group view へ移行する	**wlan ap-group** *group-name*	デフォルト：デフォルトAP グループ（default-group）が存在し、デフォルトAPグループは削除することができません。
3． AP model view へ移行する	**ap-model** *ap-model*	—
4． radio view へ移行する	**radio** *radio-id*	—
5． 802.11b クライアント拒否を設定する	**client dot11b-forbidden** { **disable** | **enable** }	デフォルト：無効

1.6.14 802.11g 保護の設定

重要：

- この機能は、802.11g 無線と 802.11n（2.4GHz）、802.11gac 無線、802.11gax 無線にのみ適用されます。
- ソフトウェアバージョン 9.6.05c を含む以降のソフトウェアでは、802.11gbe 無線でこの機能を使用できます。

802.11b と 802.11g のクライアントの両方が WLAN 内に存在しているとき、両者は異なる変調モードを使用するため伝送衝突が生じる可能性があります。802.11g 保護を設定することにより、そのような衝突を回避することができます。また、メディアに対するアクセスを遅らせるように 802.11b クライアントに知らせるために、802.11g、802.11n、802.11gac、802.11gax、802.11abe 装置が RTS/CTS パケットまたは CTS-to-self パケットを送信できるようになります。RTS/CTS または CTS-to-self に関する詳細は、本書の *“衝突回避モードの指定”* を参照してください。

802.11g、802.11n、802.11gac、802.11gbe 装置は、チャネル上で 802.11b 信号を検出したときに限り、データを送信する前に RTS/CTS パケットもしくは CTS-to-self パケットを送信します。

802.11g 保護は、802.11b クライアントが 802.11g、802.11n（2.4 GHz）、802.11gac、802.11gax、802.11gbe AP に関連づけされたとき、自動的に適用されます。

I. radio view での 802.11g 保護の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—

操作	コマンド	補足
2． AP view へ移行する	**wlan ap** *ap-name* [**model** *model-name*]	—
3． radio view へ移行する	**radio** *radio-id*	—
4． 802.11g 保護を設定する	**dot11g protection** { **disable** | **enable** }	デフォルト：無線はAP group viewの設定を使用します。

II. AP group view での 802.11g 保護の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP group view へ移行する	**wlan ap-group** *group-name*	—
3． AP model view へ移行する	**ap-model** *ap-model*	—
4． radio view へ移行する	**radio** *radio-id*	—
5． 802.11g 保護を設定する	**dot11g protection** { **disable** | **enable** }	デフォルト：無効

1.6.15 ANI の設定

ANI（Adaptive Noise Immunity）は、周辺環境からの干渉を減少させるために、無線装置が環境にもとづいた騒音防止レベルを調整できるようにします。

I. radio view での ANI の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP を作成し、AP view へ移行する	**wlan ap** *ap-name* [**model** *model-name*]	デフォルト：設定なし APを作成するときは名前とモデルを指定する必要があります。
3． radio view へ移行する	**radio** *radio-id*	—
4． ANI を設定する	**ani** { **disable** | **enable** }	デフォルト：無線はAP group viewの設定を使用します。

II. AP group view での ANI の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP グループを作成し、AP group view へ移行する	**wlan ap-group** *group-name*	デフォルト：デフォルトAP グループ（default-group）が存在し、デフォルトAPグループは削除することができません。
3． AP model view へ移行する	**ap-model** *ap-model*	—
4． radio view へ移行する	**radio** *radio-id*	—
5． ANI を設定する	**ani** { **disable** | **enable** }	デフォルト：有効

1.6.16 プリアンプルタイプの設定

重要：
プリアンプルタイプの設定機能は、802.11b 無線、802.11g 無線、802.11gn 無線に対してのみ適用されます。

プリアンプルは、送信側と受信側の間で伝送信号を同期させるためのパケットヘッダ内のビットのセットです。short プリアンプルはネットワーク性能を改善し、long プリアンプルは初期モデルのすべての無線装置との互換性を保証します。

I. radio view でのプリアンプルタイプの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP を作成し、AP view へ移行する	**wlan ap** *ap-name* [**model** *model-name*]	デフォルト：設定なし APを作成するときは名前とモデルを指定する必要があります。
3． radio view へ移行する	**radio** *radio-id*	—
4． プリアンプルタイプを設定する	**preamble** { **long** | **short** }	デフォルト：無線はAP group viewの設定を使用します。

II. AP group view でのプリアンプルタイプの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP グループを作成し、AP group view へ移行する	**wlan ap-group** *group-name*	デフォルト：デフォルトAP グループ（default-group）が存在し、デフォルトAPグループは削除することができません。
3． AP model view へ移行する	**ap-model** *ap-model*	—
4． radio view へ移行する	**radio** *radio-id*	—
5． プリアンプルタイプを設定する	**preamble** { **long** | **short** }	デフォルト：**short**

1.6.17 最大伝送距離の設定

無線信号の強さは、伝送距離が大きくなるにつれて徐々に低下します。無線信号の最大伝送距離は、周辺の環境や外部アンテナの使用の有無に依存します。

- **外部アンテナ不使用**—約 300m。
- **外部アンテナ使用**—30km～50km

- **障害のあるエリア**—35m～50m

I. radio view での最大伝送距離の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP を作成し、AP view へ移行する	**wlan ap** *ap-name* [**model** *model-name*]	デフォルト：設定なし APを作成するときは名前とモデルを指定する必要があります。
3． radio view へ移行する	**radio** *radio-id*	—
4． 最大伝送距離を設定する	**distance** *distance*	デフォルト：無線はAP group viewの設定を使用します。

II. AP group view での最大伝送距離の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP グループを作成し、AP group view へ移行する	**wlan ap-group** *group-name*	デフォルト：デフォルトAP グループ（default-group）が存在し、デフォルトAPグループは削除することができません。
3． AP model view へ移行する	**ap-model** *ap-model*	—
4． radio view へ移行する	**radio** *radio-id*	—
5． 最大伝送距離を設定する	**distance** *distance*	デフォルト：1km

1.6.18 無線連続モードの有効化

この機能は、ネットワークテストにのみ使用されます。それ以外の状況では使用しないでください。

この機能を使用すると、指定したレートで継続的にデータパケットを送信できます。機能が有効になっている場合は、送信レートの変更以外の操作は行わないでください。

802.11 a、802.11 b、802.11 g 無線の場合は、送信レートを設定します。802.11 n 無線の場合は、送信レートまたは MCS インデックスを設定します。802.11 ac または 802.11 gac 無線の場合は、送信レート、MCS インデックス、または VHT-MCS インデックスを設定します。

I. radio view での無線連続モードの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP を作成し、AP view へ移行する	**wlan ap** *ap-name* [**model** *model-name*]	デフォルト：設定なし APを作成するときは名前とモデルを指定する必要があります。

操作	コマンド	補足
3． radio view へ移行する	**radio** *radio-id*	—
4． 無線連続モードを設定する	continuous-mode { mcs mcs-index | nss nss-index vht-mcs vhtmcs-index | rate rate-value }	デフォルト：無効

II. AP group view での無線連続モードの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP グループを作成し、AP group view へ移行する	**wlan ap-group** *group-name*	デフォルト：デフォルトAPグループ（default-group）が存在し、デフォルトAPグループは削除することができません。
3． AP model view へ移行する	**ap-model** *ap-model*	—
4． radio view へ移行する	**radio** *radio-id*	—
5． 無線連続モードを設定する	continuous-mode { mcs mcs-index | nss nss-index vht-mcs vhtmcs-index | rate rate-value }	デフォルト：無効

1.6.19 オンデマンドでのチャネル使用率の測定

この機能は、AP でサポートされるチャネルと、スキャニングを行った後、チャネルの使用率を表示します。

以下にオンデマンドでのチャネル使用率を測定する手順を示します。

操作	コマンド
1． system view に移行する	**system-view**
2． AP view へ移行する	**wlan ap** *ap-name* [**model** *model-name*]
3． radio view へ移行する	**radio** *radio-id*
4． オンデマンドでのチャネル使用率を測定する	**channel-usage measure**

1.6.20 チャネル使用率アラーム閾値の設定

チャネル使用率がしきい値を超えると、装置は info-center にアラームを報告します。

以下にチャネル使用率アラームしきい値を設定する手順を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP を作成し、AP view へ移行する	**wlan ap** *ap-name* [**model** *model-name*]	デフォルト：設定なし APを作成するときは名前とモデルを指定する必要があります。

操作	コマンド	補足
3． radio view へ移行する	**radio** *radio-id*	—
4． チャネル使用率アラームのしきい値を設定する	**channel-usage threshold** *threshold*	デフォルト：90%。

1.7 802.11n機能の設定

🕮 **メモ：**

- 802.11n に対するサポートは装置のモデルに依存します。
- 802.11 n 機能は、802.11 an、802.11 gn、802.11 ac、802.11 gac、802.11 ax、および 802.11 gax 無線にのみ適用されます。

⚠ **重要：**

AP に対して 802.11n 機能を設定するとき、別のユーザが同じ AP に対して 802.1n 機能を設定している場合、設定は失敗します。

IEEE 802.11n は、高品質の無線サービスを提供し、WLAN が Ethernet と同じネットワークパフォーマンスを実現できるように定義されました。802.11n は、物理レイヤと MAC（Media Access Control）レイヤを最適化することにより、WLAN の処理能力と伝送速度を向上させます。

802.11n の物理レイヤは、OFDM にもとづいています。802.11n は、物理レイヤでの高い処理能力を実現するために、MIMO（Multiple Input Multiple Output）、40MHz 帯域幅、ショート GI（Guard Interval）、STBC（Space-Time Block Coding）、および LDPC（Low-Density Parity Check）を使用します。また、802.11n は、MAC レイヤでの伝送効率を向上させるために、A-MPDU、A-MSDU、および BA（Block Acknowledgment）を使用します。

1.7.1 A-MPDU アグリゲーション方式の指定

MPDU(MAC Protocol Data Unit) は、802.11 形式のデータフレームです。MPDU 集約は、複数の MPDU を 1 つの集約 MPDU (A-MPDU) に集約して、追加情報、ACK フレーム、および物理層コンバージェンス設定手順 (PLCP) ヘッダーのオーバーヘッドを削減します。これにより、ネットワークスループットとチャネル効率が向上します。

A-MPDU 内のすべての MPDU は、同じ QoS 優先順位、送信元アドレス、宛先アドレスである必要があります。

I. radio view での A-MPDU アグリゲーション方式の指定

操作	コマンド	補足
1． system view に移行する	**system-view**	—

操作	コマンド	補足
2． AP を作成し、AP view へ移行する	**wlan ap** *ap-name* [**model** *model-name*]	デフォルト：設定なし APを作成するときは名前とモデルを指定する必要があります。
3． radio view へ移行する	**radio** *radio-id*	—
4． A-MPDU アグリゲーション方式を指定する	**a-mpdu** { **disable** | **enable** }	デフォルト：無線はAP group viewの設定を使用します。

II. AP group view での A-MPDU アグリゲーション方式の指定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP グループを作成し、AP group view へ移行する	**wlan ap-group** *group-name*	デフォルト：デフォルトAPグループ（default-group）が存在し、デフォルトAPグループは削除することができません。
3． AP model view へ移行する	**ap-model** *ap-model*	—
4． radio view へ移行する	**radio** *radio-id*	—
5． A-MPDU アグリゲーション方式を指定する	**a-mpdu** { **disable** | **enable** }	デフォルト： 有効

1.7.2 A-MSDU アグリゲーション方式の指定

I. radio view での A-MSDU アグリゲーション方式の指定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP を作成し、AP view へ移行する	**wlan ap** *ap-name* [**model** *model-name*]	デフォルト：設定なし APを作成するときは名前とモデルを指定する必要があります。
3． radio view へ移行する	**radio** *radio-id*	—
4． A-MSDU アグリゲーション方式を指定する	**a-msdu** { **disable** | **enable** }	デフォルト：無線はAP group viewの設定を使用します。

II. AP group view での A-MSDU アグリゲーション方式の指定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP グループを作成し、AP group view へ移行する	**wlan ap-group** *group-name*	デフォルト：デフォルトAPグループ（default-group）が存在し、デフォルトAPグループは削除することができません。

操作	コマンド	補足
3． AP model view へ移行する	**ap-model** *ap-model*	—
4． radio view へ移行する	**radio** *radio-id*	—
5． A-MSDU アグリゲーション方式を指定する	**a-msdu** { **disable** | **enable** }	デフォルト：有効

1.7.3 ショート GI の設定

802.11 OFDM は、伝送するためフレームをデータブロックにフラグメントします。また、データブロック伝送が互いに干渉せず、伝送遅延の影響を受けづらくなることを保障するため、802.11 OFDM は GI を使用します。

802.11a/g に使用される GI は 800ns です。802.11n は 400ns のショート GI をサポートします。ショート GI により、データ速度は 10%向上します。

20MHz 帯域幅モードと 40MHz 帯域幅モードのどちらもショート GI をサポートします。

I. radio view でのショート GI の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP を作成し、AP view へ移行する	**wlan ap** *ap-name* [**model** *model-name*]	デフォルト：設定なし APを作成するときは名前とモデルを指定する必要があります。
3． radio view へ移行する	**radio** *radio-id*	—
4． ショート GI を設定する	**short-gi** { **disable** | **enable** }	デフォルト：無線はAP group viewの設定を使用します。

II. AP group view でのショート GI の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP グループを作成し、AP group view へ移行する	**wlan ap-group** *group-name*	デフォルト：デフォルトAP グループ（default-group）が存在し、デフォルトAPグループは削除することができません。
3． AP model view へ移行する	**ap-model** *ap-model*	—
4． radio view へ移行する	**radio** *radio-id*	—
5． ショート GI を設定する	**short-gi** { **disable** | **enable** }	デフォルト：有効

1.7.4 LDPC の設定

802.11n は、S/N 比（信号対雑音比）と伝送品質を向上させるために、LDPC（Low-Density Parity Check）機能を導入します。LDPC は、両端が LDPC をサポートするときに限り適用されます。

I. radio view での LDPC の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP を作成し、AP view へ移行する	**wlan ap** *ap-name* [**model** *model-name*]	デフォルト：設定なし APを作成するときは名前とモデルを指定する必要があります。
3． radio view へ移行する	**radio** *radio-id*	—
4． LDPC を設定する	**ldpc** { **disable** | **enable** }	デフォルト：無線はAP group viewの設定を使用します。

II. AP group view での LDPC の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP グループを作成し、AP group view へ移行する	**wlan ap-group** *group-name*	デフォルト：デフォルトAPグループ（default-group）が存在し、デフォルトAPグループは削除することができません。
3． AP model view へ移行する	**ap-model** *ap-model*	—
4． radio view へ移行する	**radio** *radio-id*	—
5． LDPC を設定する	**ldpc** { **disable** | **enable** }	デフォルト：無効

1.7.5 STBC の設定

STBC（Space-Time Block Coding）機能により、データ伝送の信頼性を向上させることができます。また、STBC 機能は、クライアントに対して高い伝送速度を要求しません。

I. radio view での STBC の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP を作成し、AP view へ移行する	**wlan ap** *ap-name* [**model** *model-name*]	デフォルト：設定なし APを作成するときは名前とモデルを指定する必要があります。
3． radio view へ移行する	**radio** *radio-id*	—
4． STBC を設定する	**stbc** { **disable** | **enable** }	デフォルト：無線はAP group viewの設定を使用します。

II. AP group view での STBC の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP グループを作成し、AP group view へ移行する	**wlan ap-group** *group-name*	デフォルト：デフォルトAPグループ（default-group）が存在し、デフォルトAPグループは削除することができません。
3． AP model view へ移行する	**ap-model** *ap-model*	—
4． radio view へ移行する	**radio** *radio-id*	—
5． STBC を設定する	**stbc** { **disable** | **enable** }	デフォルト：有効

1.7.6 MCS インデックスの設定

802.11n AP に対して MCS インデックスを設定するとき、以下の制限とガイドラインに従ってください。

- 802.11n クライアントは、ユニキャストフレームを送信するために、MCS インデックスと一致した速度を使用します。802.11a/b/g クライアントは、ユニキャストフレームを送信するために、802.11a/b/g 速度を使用します。
- マルチキャスト MCS インデックスを設定しない場合、802.11n クライアントと AP は、マルチキャストフレームを送信するために、802.11a/b/g マルチキャスト速度を使用します。マルチキャスト MCS インデックスを設定する場合、以下のケースのいずれかが発生します。
  - □ すべてのクライアントが 802.11n クライアントの場合、AP とクライアントはマルチキャストフレームを送信するために、マルチキャスト MCS インデックスと一致する速度を使用します。
  - □ 802.11a/b/g クライアントが存在する場合、AP とクライアントはマルチキャストフレームを送信するために、802.11a/b/g マルチキャスト速度を使用します。
- 最大必須 MCS インデックスあるいはサポート MCS インデックスを設定するとき、実際に範囲を指定します。たとえば、最大必須 MCS インデックスを 5 に設定する場合、0～5 の MCS インデックスに一致する速度が 802.11n 必須速度として設定されます。

I. radio view での MCS インデックスの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP を作成し、AP view へ移行する	**wlan ap** *ap-name* [**model** *model-name*]	デフォルト：設定なし APを作成するときは名前とモデルを指定する必要があります。
3． radio view へ移行する	**radio** *radio-id*	—

操作	コマンド	補足
4. 最大必須 MCS インデックスを設定する	**dot11n mandatory maximum-mcs** *index*	デフォルト： ● 最大サポートMCSインデックスが設定されている場合、最大必須MCSインデックスは設定されません。 ● 最大サポートMCSインデックスが設定されていない場合、無線はAP group viewの設定を使用します。
5. 最大サポート MCS インデックスを設定する	**dot11n support maximum-mcs** *index*	デフォルト： ● 最大必須MCSインデックスが設定されている場合、最大サポートMCSインデックスは76です。 ● 最大必須MCSインデックスが設定されていない場合、無線はAP group viewの設定を使用します。 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することはできません。
6. マルチキャスト MCS インデックスを設定する	**dot11n multicast-mcs** *index*	デフォルト： ● 最大サポートMCSインデックスまたは最大必須MCSインデックスが設定されている場合、マルチキャストMCSインデックスは設定されません。 ● 最大サポートMCSインデックスと最大必須MCSインデックスのどちらも設定されていない場合、無線はAP group viewの設定を使用します。 マルチキャストMCSインデックスは、最大必須MCSインデックスより大きくすることはできません。

II. AP group view での MCS インデックスの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP グループを作成し、AP group view へ移行する	**wlan ap-group** *group-name*	デフォルト：デフォルトAPグループ（default-group）が存在し、デフォルトAPグループは削除することができません。

操作	コマンド	補足
3． AP model view へ移行する	**ap-model** *ap-model*	—
4． radio view へ移行する	**radio** *radio-id*	—
5． 最大必須 MCS インデックスを設定する	**dot11n mandatory maximum-mcs** *index*	デフォルト：設定なし
6． 最大サポート MCS インデックスを設定する	**dot11n support maximum-mcs** *index*	デフォルト： 76 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することはできません。
7． マルチキャスト MCS インデックスを設定する	**dot11n multicast-mcs** *index*	デフォルト：設定なし マルチキャストMCSインデックスは、最大必須MCSインデックスより大きくすることはできません。

1.7.7 802.11n/ac/ax クライアント限定アクセスの設定

低速の 802.11a/b/g クライアントの影響を減らし、無線データ通信を加速するために、802.11n/ac/ax クライアントにのみアクセスできるように AP を設定することができます。

I. radio view での 802.11n/ac/ax クライアント限定アクセスの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP を作成し、AP view へ移行する	**wlan ap** *ap-name* [**model** *model-name*]	デフォルト：設定なし APを作成するときは名前とモデルを指定する必要があります。
3． radio view へ移行する	**radio** *radio-id*	—
4． 802.11n/ac/ax クライアント限定アクセスを設定する	**client dot11n-only** { **disable** | **enable** }	デフォルト：無線はAP group viewの設定を使用します。

II. AP group view での 802.11n/ac/ax クライアント限定アクセスの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP グループを作成し、AP group view へ移行する	**wlan ap-group** *group-name*	デフォルト：デフォルトAPグループ（default-group）が存在し、デフォルトAPグループは削除することができません。
3． AP model view へ移行する	**ap-model** *ap-model*	—
4． radio view へ移行する	**radio** *radio-id*	—

操作	コマンド	補足
5. 802.11n/ac/ax クライアント限定アクセスを設定する	**client dot11n-only** { **disable** | **enable** }	デフォルト：無効

1.7.8 802.11n 帯域幅モードの設定

802.11n は 802.11a/b/g のチャネル構造を使用しますが、データを送信するための 20MHz のチャネルにおけるサブチャネルの数は 52 まで増加します。これにより、データ通信速度は向上します。

802.11n は、2 つの隣接した 20MHz のチャネルに対して、40MHz のチャネル（一方は 1 次チャネル、もう一方は 2 次チャネル）を形成することを義務づけます。これは、データ転送速度を 2 倍にする簡単な方法を提供します。

無線のための帯域幅は帯域幅モード設定とチップ機能により変化します。

I. radio view での 802.11n 帯域幅モードの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP を作成し、AP view へ移行する	**wlan ap** *ap-name* [**model** *model-name*]	デフォルト：設定なし APを作成するときは名前とモデルを指定する必要があります。
3. radio view へ移行する	**radio** *radio-id*	—
4. 802.11n 帯域幅モードを設定する	**channel band-width** { **20** | **40** [**auto-switch**] }	デフォルト：無線はAP group viewの設定を使用します。 802.11gn無線のみ**auto-switch**パラメータをサポートします。

II. AP group view での 802.11n 帯域幅モードの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP グループを作成し、AP group view へ移行する	**wlan ap-group** *group-name*	デフォルト：デフォルトAPグループ（default-group）が存在し、デフォルトAPグループは削除することができません。
3. AP model view へ移行する	**ap-model** *ap-model*	—
4. radio view へ移行する	**radio** *radio-id*	—

操作	コマンド	補足
5. 802.11n 帯域幅モードを設定する	**channel band-width** { **20** | **40** [**auto-switch**] }	デフォルト：802.11an無線のデフォルトは40MHzです。 802.11gn無線のデフォルトは20MHzです。 802.11gn無線のみ**auto-switch**パラメータをサポートします。

1.7.9 エネルギ節約機能の設定

エネルギ節約機能を有効にしたあと、無線に関連づけられたクライアントが存在しない場合、無線の MIMO モードは自動的に 1x1 に変更されます。これにより電力の消費を抑えることができます。

I. radio view でのエネルギ節約機能の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP を作成し、AP view へ移行する	**wlan ap** *ap-name* [**model** *model-name*]	デフォルト：設定なし APを作成するときは名前とモデルを指定する必要があります。
3. radio view へ移行する	**radio** *radio-id*	—
4. エネルギ節約機能を設定する	**green-energy-management** { **disable** | **enable** }	デフォルト：無線はAP group viewの設定を使用します。

II. AP group view でのエネルギ節約機能の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP グループを作成し、AP group view へ移行する	**wlan ap-group** *group-name*	デフォルト：デフォルトAPグループ（default-group）が存在し、デフォルトAPグループは削除することができません。
3. AP model view へ移行する	**ap-model** *ap-model*	—
4. radio view へ移行する	**radio** *radio-id*	—
5. エネルギ節約機能を設定する	**green-energy-management** { **disable** | **enable** }	デフォルト：無効

1.7.10 802.11n 保護の設定

802.11n と 802.11n 以外のクライアントの両方が WLAN 内に存在しているとき、両者は異なる変調モードを使用するため伝送衝突が生じる可能性があります。802.11n 保護はそのような衝突を避けることができます。802.11n 保護により、802.11n 機器は 802.11n 以

外のクライアントに対してメディアへのアクセスを延期するよう知らせるために、RTS/CTS または CTS-to-self パケットを送信することができるようになります。RTS/CTS または CTS-to-self に関する詳細は、本章の *“衝突回避モードの指定”* を参照してください。

802.11n 機器は、チャネルの上で 802.11n 以外の信号が検出された場合に限り、データを送信する前に RTS/CTS または CTS-to-self パケットを送信します。

802.11n 保護は、802.11n 以外のクライアントが 802.11n AP と関連づけられたとき、自動的に適用されます。

🕮 **メモ：**

- 802.11n 装置は、802.11n 装置と 802.11ac/ax/be 装置を指します。
- この機能は、ソフトウェアバージョン 9.6.05c を含む以降のソフトウェアでは 802.11abe と 802.11gbe の無線タイプの Radio での使用をサポートしています。

I. radio view での 802.11n 保護の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP view へ移行する	**wlan ap** *ap-name* [**model** *model-name*]	—
3． radio view へ移行する	**radio** *radio-id*	—
4． 802.11n 保護を設定する	**dot11n protection** { **disable** | **enable** }	デフォルト：無線はAP group viewの設定を使用します。

II. AP group view での 802.11n 保護の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP group view へ移行する	**wlan ap-group** *group-name*	—
3． AP model view へ移行する	**ap-model** *ap-model*	—
4． radio view へ移行する	**radio** *radio-id*	—
5． 802.11n 保護を設定する	**dot11n protection** { **disable** | **enable** }	デフォルト：無効

1.8 802.11ac/ax機能の設定

🕮 **メモ：**

802.11ac/ax 装置に対するサポートは、装置モデルに依存します。

⚠ **重要：**

AP に対して 802.11ac/ax 機能を設定するとき、別のユーザが同じ AP に対して 802.11ac/ax 機能を設定している場合、設定は失敗します。

1.8.1 NSS の設定

802.11ac/ax AP に対して NSS を設定するときは、以下の制限とガイドラインに従ってください。

- AP が NSS をサポートする場合、AP は NSS に対するすべての VHT-MCS/HE-MCS インデックスをサポートします。
- 802.11ac/ax クライアントは、ユニキャストフレームを送信するために、NSS に対して VHT-MCS/HE-MCS インデックスと一致した速度を使用します。また、802.11ac/ax 以外のクライアントは、ユニキャストフレームを送信するために、802.11a/b/g/n 速度を使用します。
- マルチキャスト NSS を送信しない場合、802.11ac/ax クライアントと AP は、マルチキャストフレームを送信するために 802.11a/b/g/n マルチキャスト速度を使用します。NSS を設定し、VHT-MCS/HE-MCS インデックスを指定した場合、以下のケースのうちいずれかが発生します。
  - すべてのクライアントが 802.11ac/ax クライアントである場合、AP とクライアントはマルチキャストフレームを送信するために、VHT-MCS/HE-MCS インデックスと一致した速度を使用します。
  - 802.11ac/ax 以外のクライアントが存在する場合、AP とクライアントはマルチキャストフレームを送信するために、802.11a/b/g/n マルチキャスト速度を使用します。
  - 最大必須 NSS または最大サポート NSS を設定するとき、実際に範囲を指定します。たとえば、最大必須 NSS を 5 に設定する場合、1～5 までの NSS に対して VHT-MCS/HE-MCS インデックスと一致する速度が、802.11ac/ax 必須速度として設定されます。

🕮 **メモ：**

サポートされる最大 NSS を最大必須 NSS より小さくすることはできません。
マルチキャスト NSS を最大必須 NSS より大きくすることはできません。

I. radio view での NSS の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—

操作	コマンド	補足
2． AP を作成し、AP view へ移行する	**wlan ap** *ap-name* [**model** *model-name*]	デフォルト：設定なし APを作成するときは名前とモデルを指定する必要があります。
3． radio view へ移行する	**radio** *radio-id*	—
4． 最大必須 NSS を設定する	● 802.11ac **dot11ac mandatory maximum-nss** *nss-number* ● 802.11ax **dot11ax mandatory maximum-nss** *nss-number*	デフォルト： ● 最大サポートNSSが設定されている場合、最大必須NSSは設定されません。 ● 最大サポートNSSが設定されていない場合、無線はAP group viewの設定を使用します。
5． 最大サポート NSS を設定する	● 802.11ac **dot11ac support maximum-nss** *nss-number* ● 802.11ax **dot11ax support maximum-nss** *nss-number*	デフォルト： ● 最大必須NSSが設定されている場合、最大サポートNSSは8です。 ● 最大必須NSSが設定されていない場合、無線はAP group viewの設定を使用します。
6． マルチキャスト NSS の設定と VHT-MCS/HE-MCS インデックスを指定する	● 802.11ac **dot11ac multicast-nss** *nss-number* **vht-mcs** *index* ● 802.11ax **dot11ax multicast-nss** *nss-number* **he-mcs** *index*	デフォルト： ● 最大サポートNSSまたは最大必須NSSが設定されている場合、マルチキャストNSSは設定されません。 ● 最大サポートNSSと最大必須NSSのどちらも設定されていない場合、無線はAP group viewの設定を使用します。

II. AP group view での NSS の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP グループを作成し、AP view へ移行する	**wlan ap-group** *group-name*	デフォルト：デフォルトAPグループ（default-group）が存在し、デフォルトAPグループは削除することができません。
3． AP model view へ移行する	**ap-model** *ap-model*	—
4． radio view へ移行する	**radio** *radio-id*	—

操作	コマンド	補足
5. 最大必須 NSS を設定する	• 802.11ac **dot11ac mandatory maximum-nss** *nss-number* • 802.11ax **dot11ax mandatory maximum-nss** *nss-number*	デフォルト：設定なし
6. 最大サポート NSS を設定する	• 802.11ac **dot11ac support maximum-nss** *nss-number* • 802.11ax **dot11ax support maximum-nss** *nss-number*	デフォルト： 8
7. マルチキャスト NSS の設定と VHT-MCS/HE-MCS インデックスを指定する	• 802.11ac **dot11ac multicast-nss** *nss-number* **vht-mcs** *index* • 802.11ax **dot11ax multicast-nss** *nss-number* **he-mcs** *index*	デフォルト：設定なし

1.8.2 802.11ac/ax クライアント限定アクセスの設定

低速 802.11a/b/g/n クライアントの影響を低減し、無線データ伝送を加速させるために、AP が 802.11ac/ax クライアントのみを許可するように設定することができます。

I. radio view での 802.11ac/ax クライアント限定アクセスの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP を作成し、AP view へ移行する	**wlan ap** *ap-name* [**model** *model-name*]	デフォルト：設定なし APを作成するときは名前とモデルを指定する必要があります。
3. radio view へ移行する	**radio** *radio-id*	—
4. 802.11ac/ax クライアント限定アクセスを設定する	• 802.11acクライアント限定アクセス **client dot11ac-only** { **disable** | **enable** } • 802.11axクライアント限定アクセス **client dot11ax-only** { **disable** | **enable** }	デフォルト：無線はAP group viewの設定を使用します。

II. AP group view での 802.11ac/ax クライアント限定アクセスの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—

操作	コマンド	補足
2． AP グループを作成し、AP group view へ移行する	**wlan ap-group** *group-name*	デフォルト：デフォルトAP グループ（default-group）が存在し、デフォルトAPグループは削除することができません。
3． AP model view へ移行する	**ap-model** *ap-model*	—
4． radio view へ移行する	**radio** *radio-id*	—
5． 802.11ac/ax クライアント限定アクセスを設定する	● 802.11acクライアント限定アクセス **client dot11ac-only** { **disable** | **enable** } ● 802.11axクライアント限定アクセス **client dot11ax-only** { **disable** | **enable** }	デフォルト： 無効

1.8.3 802.11ac/ax 帯域幅モードの設定

802.11ac/ax は 802.11n のチャネル構造を使用し、最大帯域幅を 40MHz から 160MHz まで増大させます。802.11ac/ax は、2 つの隣接した 20MHz のチャネルに対して 40MHz のチャネルを関連づけることができ、2 つの隣接した 40MHz チャネルに対して、80MHz のチャネルを形成することを関連づけることができます。また、2 つの隣接した 80MHz チャネルに対して、160MHz のチャネルを形成することを関連づけることができます。

🕮 **メモ：**

- 802.11gac は 80MHz、40MHz 帯域幅モードをサポートします。
- 160MHz は QX-W1130 と QX-W1200 シリーズでサポートします。

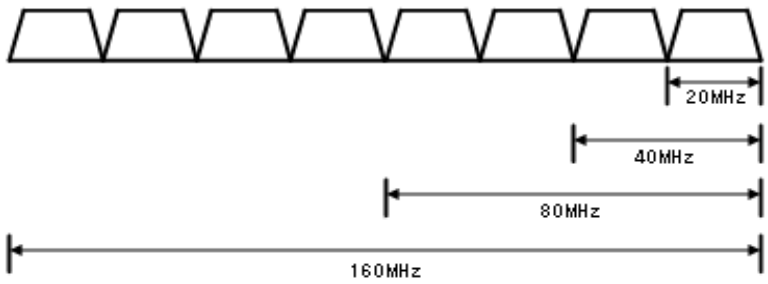


図 1-1 802.11ac/ax 帯域幅モード

II. radio view での 802.11ac/ax 帯域幅モードの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—

操作	コマンド	補足
2． AP を作成し、AP view へ移行する	**wlan ap** *ap-name* [**model** *model-name*]	デフォルト：設定なし APを作成するときは名前とモデルを指定する必要があります。
3． radio view へ移行する	**radio** *radio-id*	—
4． 802.11ac/ax 帯域幅モードを設定する	● 802.11ac/ax帯域幅モードを設定する： **channel band-width** { **20** | **40** | **80** | **160** } ● 802.11gac/gax帯域幅モードを設定する： **channel band-width** { **20** | **40** [**auto-switch**] }	デフォルト：無線はAP group viewの設定を使用します。

III. AP group view での 802.11ac/ax 帯域幅モードの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP グループを作成し、AP group view へ移行する	**wlan ap-group** *group-name*	デフォルト：デフォルトAPグループ（default-group）が存在し、デフォルトAPグループは削除することができません。
3． AP model view へ移行する	**ap-model** *ap-model*	—
4． radio view へ移行する	**radio** *radio-id*	—
5． 802.11ac/ax 帯域幅モードを設定する	● 802.11ac/ax帯域幅モードを設定する： **channel band-width** { **20** | **40** | **80** | **160** } ● 802.11gac/gax帯域幅モードを設定する： **channel band-width** { **20** | **40** [**auto-switch**] }	デフォルト： 802.11ac/ax帯域幅モード：80 802.11gac/gax帯域幅モード：20

1.8.4 TxBF の設定

🕮 **メモ：**

TxBF のサポートは、装置モデルに依存します。

TxBF（Transmit beamforming）は、クライアントに意図した RF 信号に焦点を合わせるため、AP がチャネル情報にもとづいて送信するパラメータを適合させます。この機能は RF 信号の品質を向上させます。TxBF はシングルユーザ TxBF とマルチユーザ TxBF があります。

- **シングルユーザ TxBF**－意図した 1 クライアントへの信号を向上します。シングルユーザ TxBF はクライアントが広範囲にわたっている、品質が低いネットワーク、信号の減衰に対して厳しい WLAN に適しています。

- **マルチユーザ TxBF**－802.11ac wave2 の一部です。マルチユーザ TxBF は干渉と伝送遅延を縮小させるため、AP が意図したクライアントに異なる RF 信号の焦点を合わせます。

I. radio view での 802.11ac 帯域幅モードの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP を作成し、AP view へ移行する	**wlan ap** *ap-name* [**model** *model-name*]	デフォルト：設定なし APを作成するときは名前とモデルを指定する必要があります。
3. radio view へ移行する	**radio** *radio-id*	—
4. シングルユーザ TxBF を設定する	**su-txbf** { **disable** | **enable** }	デフォルト：無線はAP group viewの設定を使用します。
5. マルチユーザ TxBF を設定する	**mu-txbf** { **disable** | **enable** }	デフォルト：無線はAP group viewの設定を使用します。

II. AP group view での 802.11ac 帯域幅モードの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP グループを作成し、AP group view へ移行する	**wlan ap-group** *group-name*	デフォルト：デフォルトAP グループ（default-group）が存在し、デフォルトAPグループは削除することができません。
3. AP model view へ移行する	**ap-model** *ap-model*	—
4. radio view へ移行する	**radio** *radio-id*	—
5. シングルユーザ TxBF を設定する	**su-txbf** { **disable** | **enable** }	デフォルト：無効
6. マルチユーザ TxBF を設定する	**mu-txbf** { **disable** | **enable** }	デフォルト：有効 マルチユーザTxBFはシングルユーザTxBFが無効である場合のみ有効になります。

1.8.5 OFDMA の設定

メモ：
この機能は QX-W1100 シリーズおよび QX-W1200 シリーズの AP でサポートしています。

I. OFDMA について

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

II. radio view での設定方法

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP を作成し、AP view へ移行する	**wlan ap** *ap-name* [**model** *model-name*]	デフォルト：設定なし APを作成するときは名前とモデルを指定する必要があります。
3. radio view へ移行する	**radio** *radio-id*	—
4. ダウンリンク OFDMA を設定する	**dl-ofdma** { **disable** | **enable** }	デフォルト：AP group radio viewの設定を使用
5. アップリンク OFDMA を設定する	**ul-ofdma** { **disable** | **enable** }	デフォルト：AP group radio viewの設定を使用

III. AP group view での設定方法

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP グループを作成し、AP group view へ移行する	**wlan ap-group** *group-name*	デフォルト：デフォルトAPグループ（default-group）が存在し、デフォルトAPグループは削除することができません。
3. AP model view へ移行する	**ap-model** *ap-model*	—
4. radio view へ移行する	**radio** *radio-id*	—
5. ダウンリンク OFDMA を設定する	**dl-ofdma** { **disable** | **enable** }	デフォルト：無効
6. アップリンク OFDMA を設定する	**ul-ofdma** { **disable** | **enable** }	デフォルト：無効

1.8.6 BSS カラーリングの設定

🕮 **メモ：**
この機能は QX-W1100 シリーズおよび QX-W1200 シリーズの AP でサポートしています。

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 802.11ax 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。

I. radio view での設定手順

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP を作成し、AP view へ移行する	**wlan ap** *ap-name* [**model** *model-name*]	デフォルト：設定なし APを作成するときは名前とモデルを指定する必要があります。
3． radio view へ移行する	**radio** *radio-id*	—
4． BSS カラーリングを設定する	**bss-color** { **disable** | **enable** }	デフォルト：AP group radio viewの設定を使用

II. AP group view での設定方法

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP グループを作成し、AP group view へ移行する	**wlan ap-group** *group-name*	デフォルト：デフォルトAPグループ（default-group）が存在し、デフォルトAPグループは削除することができません。
3． AP model view へ移行する	**ap-model** *ap-model*	—
4． radio view へ移行する	**radio** *radio-id*	—
5． BSS カラーリングを設定する	**bss-color** { **disable** | **enable** }	デフォルト：無効

1.8.7 TWT ネゴシエーションの設定

🕮 **メモ：**

この機能は QX-W1100 シリーズおよび QX-W1200 シリーズの AP でサポートしています。

TWT(Trget Wake Time) ネゴシエーションを使用すると、クライアントと AP はサービス期間中にのみデータパケットを交換し、クライアントの休止状態をスケジュールして、クライアントの電力消費量と無線リソースの競合を減らすことができます。

TWT ネゴシエーションを有効にすると、クライアントはサービス期間、TWT 間隔、および最初のスリープ状態解除時間(クライアントによって計算される)を含むネゴシエーション要求を AP に送信します。このような要求を受信すると、AP は応答を送信します。クライアントはスケジュールに従って起動し、その AP からのトリガーフレームを待機します。トリガーフレームを受信すると、クライアントはサービス期間に入り、その AP とのデータパケットの交換を開始します。サービス期間が終了すると、データパケットの交換が完了していなくても、クライアントは休止モードに入ります。

I. 制限とガイドライン

無線は、最大 8 台のクライアントに TWT サービスを提供できます。8 つのクライアントの TWT ネゴシエーション要求に応答した後、無線は他のクライアントからの要求を拒否します。

本機能は、802.11ax、802.11gax、802.11eax、802.11be、802.11abe、802.11gbe で有効です。他の無線タイプに変更すると、設定が削除されます。

II. radio view での設定方法

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP を作成し、AP view へ移行する	**wlan ap** *ap-name* [**model** *model-name*]	デフォルト：設定なし APを作成するときは名前とモデルを指定する必要があります。
3． radio view へ移行する	**radio** *radio-id*	—
4． TWT ネゴシエーションを設定する	**twt negotiate** { **disable** | **enable** }	デフォルト：AP group radio viewの設定を使用

III. AP group view での設定方法

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP グループを作成し、AP group view へ移行する	**wlan ap-group** *group-name*	デフォルト：デフォルトAPグループ（default-group）が存在し、デフォルトAPグループは削除することができません。
3． AP model view へ移行する	**ap-model** *ap-model*	—
4． radio view へ移行する	**radio** *radio-id*	—
5． TWT ネゴシエーションを設定する	**twt negotiate** { **disable** | **enable** }	デフォルト： APモデルにより異なります。

1.9 802.11be機能の設定

🕮 **メモ：**

- QX-W1240 は 802.11be (draft)に対応しています。
- 802.11be 機能の設定はソフトウェアバージョン 9.4.09 を含む以降のソフトウェアでサポートしています。

1.9.1 NSS の設定

802.11be クライアントがオンラインになると、システムは NSS に対応する EHT-MCS インデックスで表される MCS を使用して、クライアントのユニキャストデータを送信します。

- マルチキャスト NSS が設定されていない場合、システムはマルチキャストレートまたはマルチキャスト MCS を使用して、802.11be クライアントと AP の間でマルチキャスト データを送信します。
- マルチキャスト NSS が設定され、すべてのクライアントが 802.11be クライアントである場合、AP とクライアントは EHT-MCS インデックスで表される MCS を使用してマルチキャスト データを送信します。
- マルチキャスト NSS は最大必須 NSS の値以下であることを確認してください。
- 最大必須 NSS はサポートされる最大 NSS の値 以下であることを確認してください。

I. radio view での NSS の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP を作成し、AP view へ移行する	**wlan ap** *ap-name* [**model** *model-name*]	デフォルト：設定なし APを作成するときは名前とモデルを指定する必要があります。
3. radio view へ移行する	**radio** *radio-id*	—
4. 最大必須 NSS を設定する	**dot11be mandatory maximum-nss** *nss-number*	デフォルト：AP group radio viewの設定を使用
5. 最大サポート NSS を設定する	**dot11be support maximum-nss** *nss-number*	デフォルト： AP group radio viewの設定を使用
6. マルチキャスト NSS の設定と EHT-MCS インデックスを指定する	**dot11be multicast-nss** *nss-number* **eht-mcs** *index*	デフォルト：AP group radio viewの設定を使用

II. AP group radio view での NSS の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP グループを作成し、AP group view へ移行する	**wlan ap-group** *group-name*	デフォルト：デフォルトAPグループ（default-group）が存在し、デフォルトAPグループは削除することができません。

操作	コマンド	補足
3． AP model view へ移行する	**ap-model** *ap-model*	—
4． radio view へ移行する	**radio** *radio-id*	—
5． 最大必須 NSS を設定する	**dot11be mandatory maximum-nss** *nss-number*	デフォルト：設定なし
6． 最大サポート NSS を設定する	**dot11be support maximum-nss** *nss-number*	デフォルト： 8
7． マルチキャスト NSS の設定と EHT-MCS インデックスを指定する	**dot11be multicast-nss** *nss-number* **eht-mcs** *index*	デフォルト：設定なし

1.9.2 802.11be 帯域幅モードの設定

🕮 **メモ：**

- QX-W1240 は、320MHz 帯域幅モードをサポートしていません。
- QX-W1210 と QX-W1230 の 320MHz 帯域幅モードの設定は、ソフトウェアバージョン 9.6.05c を含む以降のソフトウェアからサポートしています。

802.11be は、チャネル帯域幅を最大 160 MHz から最大 320 MHz に拡張します。802.11be は、隣接するチャネルをマージすることでより大きな帯域幅チャネルを得る 802.11n からのチャネル帯域幅割り当て方式を採用しています。802.11be では、隣接する 2 つの 20 MHz チャネルをマージして 40 MHz チャネルを形成し、80 MHz および 160 MHz チャネルも同じ方法でマージできます。

プロトコル仕様によると、動作周波数帯域幅は 2/2 に分割されます。前半の位置はプライマリチャネルによって決定され、後半の位置はセカンダリチャネルによって決定されます。プライマリチャネルは、すべての制御および管理フレームと同様にデータフレームの送信に使用され、セカンダリチャネルはプライマリチャネルにバンドルされ、データフレームの送信にのみ使用されます。channel コマンドを使用してプライマリチャネルを設定し、動作周波数帯域幅を 320/160 MHz に設定すると、secondary-channel パラメータを使用してセカンダリ 160/80 MHz 周波数帯域幅を指定できます。その他の場合、セカンダリチャネルはシステムによって自動的に選択されます。

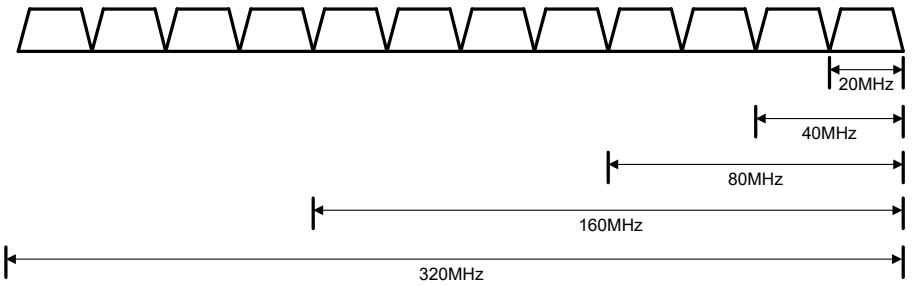


図 1-2 802.11be 帯域幅モード

II. radio view での 802.11be 帯域幅モードの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP を作成し、AP view へ移行する	**wlan ap** *ap-name* [**model** *model-name*]	デフォルト：設定なし APを作成するときは名前とモデルを指定する必要があります。
3． radio view へ移行する	**radio** *radio-id*	—
4． 帯域幅モードを設定する(6GHz 帯の Radio)	802.11be帯域幅モードを設定する **channel band-width** { **20** | **40** | **80** | **160** | **320** }	デフォルト：AP group radio viewの設定を使用
5． 帯域幅モードを設定する(5GHz 帯の Radio)	802.11abe帯域幅モードを設定する	デフォルト：AP group radio viewの設定を使用

操作	コマンド	補足
	channel band-width { **20** | **40** | **80** | **160** }	
6. 帯域幅モードを設定する(2.4GHz 帯の Radio)	802.11gbe帯域幅モードを設定する **channel band-width** { **20** | **40** [**auto-switch**] }	デフォルト：AP group radio viewの設定を使用

III. AP group radio view での 802.11be 帯域幅モードの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP グループを作成し、AP group view へ移行する	**wlan ap-group** *group-name*	デフォルト：デフォルトAPグループ（default-group）が存在し、デフォルトAPグループは削除することができません。
3. AP model view へ移行する	**ap-model** *ap-model*	—
4. radio view へ移行する	**radio** *radio-id*	—
5. 帯域幅モードを設定する(6GHz 帯の Radio)	802.11be帯域幅モードを設定する **channel band-width** { **20** | **40** | **80** | **160** | **320** }	デフォルト： 160MHz
6. 帯域幅モードを設定する(5GHz 帯の Radio)	802.11abe帯域幅モードを設定する **channel band-width** { **20** | **40** | **80** | **160** }	デフォルト： 80 MHz
7. 帯域幅モードを設定する(2.4GHz 帯の Radio)	802.11gbe帯域幅モードを設定する **channel band-width** { **20** | **40** [**auto-switch**] }	デフォルト： 20 MHz

1.9.3 MRU の設定

Multiple Resource Unit (MRU) は、主にマルチユーザシナリオで、スペクトルリソースの使用率を向上させるために使用される手法です。

従来の技術では、各ユーザが使用できるリソースユニット (RU) は 1 つだけです。MRU の機能を導入することにより、ユーザは複数の RU を使用できます。同じ帯域幅で 2 人のユーザに同時にデータを送信する場合、MRU 技術は、1 つの STA が同時に複数の RU リソースを占有することを可能にし、スペクトルリソースの利用率を向上させ、遅延を削減します。

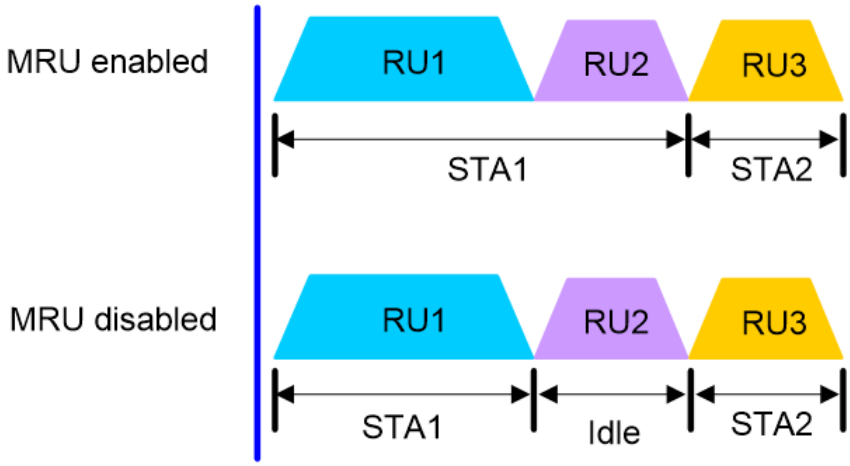


図 1-3 MRU

このコマンドは Radio type が 802.11be、802.11gbe、および 802.11abe の無線でのみ使用することができます。Radio type が 802.11be、802.11gbe、802.11abe 以外のモードに切り替わると、このコマンドは無効になります。

MRU の設定方法は以下の通りです。

II. radio view での MRU の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP を作成し、AP view へ移行する	**wlan ap** *ap-name* [**model** *model-name*]	デフォルト：設定なし APを作成するときは名前とモデルを指定する必要があります。
3． radio view へ移行する	**radio** *radio-id*	—
4． MRU を設定する	mru { **disable** | **enable** }	デフォルト：無効

1.9.4 preamble puncturing 機能の設定

🕮 **メモ：**

QX-W1240 は、320MHz 帯域幅モードをサポートしていません。

preamble puncturing 機能を使用すると、非連続チャネルを使用したデータ送信が可能になり、主にチャネル干渉を使用するシナリオでチャネルの使用効率が向上します。

図 1-4 のように、preamble puncturing 機能がサポートされていない場合は、80 MHz チャネルでデータを送信する場合、チャネル 56 で干渉が検出され、チャネル帯域幅は 20 MHz に減少します。

図 1-5 のように、preamble puncturing 機能がサポートされている場合は、80 MHz チャネル全体の干渉部分 (channel 56) が puncturing およびシールドされ、残りのチャネル 52、

60、および 64 がまとめられて情報を送信し続けます。AP は引き続き 80 MHz 帯域幅モードで動作しますが、干渉されたチャネルは Null 状態になります。つまり、実際の送信中はアイドル状態になります。

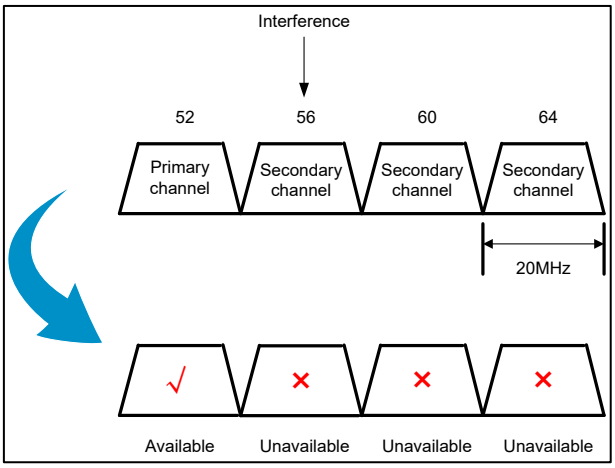


図 1-4 preamble puncturing 機能がサポートされていない場合

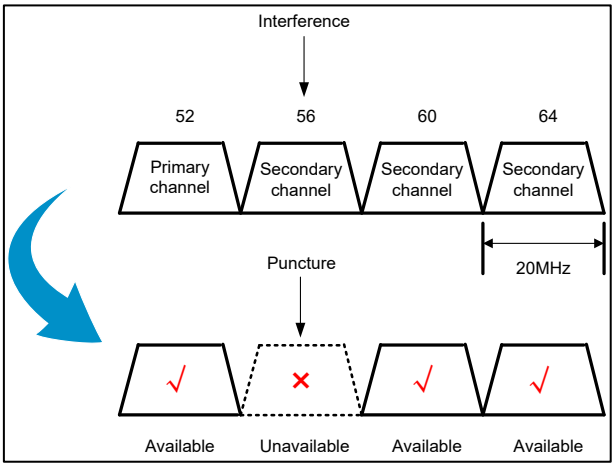


図 1-5 preamble puncturing 機能 がサポートされている場合

静的 preamble puncturing は、ソフトウェアが帯域幅モードとプライマリチャネルの場所に基づいて puncturing の位置を指定します。

このコマンドは 80 MHz、160 MHz、320 MHz の帯域幅モードに適用することができます。

このコマンドは Radio type が 802.11be、802.11abe、802.11gbe の無線でのみ使用することができます。Radio type が 802.11be、802.11abe、802.11gbe 以外のモードに切り替わると、このコマンドは無効になります。

preamble puncturing の設定方法は以下の通りです。

II. radio view での preamble puncturing の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP を作成し、AP view へ移行する	**wlan ap** *ap-name* [**model** *model-name*]	デフォルト：設定なし APを作成するときは名前とモデルを指定する必要があります。
3． radio view へ移行する	**radio** *radio-id*	—
4． preamble puncturing を設定する	pre-puncture static **{ disable | enable }**	デフォルト：無効

1.10 6GHz帯の無線の設定

🕮 **メモ：**

6GHz 帯の無線の設定は、ソフトウェアバージョン 9.4.09 を含む以降のソフトウェアでサポートしています。

1.10.1 6GHz 帯の無線モードの指定

🕮 **メモ：**

QX-W1240 は 802.11be (draft)に対応しています。

6GHz 帯の無線モードを指定する方法は以下の通りです。

I. radio view での 6GHz 帯の無線モードの指定方法

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP view に移行する	**wlan ap** *ap-name* **[model** *model-name* **]**	—
3． radio view へ移行する	**radio** *radio-id*	—
4． 6GHz 帯の無線モードを指定する	**type { dot11be | dot11eax }**	デフォルト：AP group viewの設定を使用します。

II. AP group radio view での 6GHz 帯の無線モードの指定方法

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP group view に移行する	**wlan ap-group** *group-name*	—
3． AP model view に移行する	**ap-model** *ap-model*	—
4． radio view へ移行する	**radio** *radio-id*	—
5． 6GHz 帯の無線モードを指定する	**type { dot11be | dot11eax }**	デフォルト：dot11be

1.10.2 6GHz 帯無線サービス検出の設定

I. 5GHz、2.4GHz 無線を使用した 6GHz 無線サービス検出

🕮 **メモ：**

6GHz 帯無線サービス検出を使用するためには、6GHz 帯無線を使用する AP の Radio2 または Radio3 を有効化し、サービステンプレートをバインドする必要があります。

6GHz 帯無線サービス検出を有効にすると、6GHz 帯無線をサポートするクライアントは AP の 2.4GHz または 5GHz 無線から送信されたパケットを読み取り、伝送された 6GHz 帯の無線サービスの情報を取得することができます。この機能を使用する場合は、AP の 2.4GHz または 5GHz 無線が有効になっていることを確認してください。

6GHz 帯無線サービス検出の設定方法は以下の通りです。

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． global configuration view へ移行する	**wlan global-configuration**	—
3． 6GHz 帯ワイヤレスサービス検出機能を有効にする	**wlan out-band 6g-discovery enable**	デフォルト：有効

II. 6GHz 無線を使用した 6GHz 無線サービス検出

🕮 **メモ：**

この機能は、ソフトウェアバージョン 9.6.05c を含む以降のソフトウェアからサポートしています。

この機能を有効にすると、6GHz 無線で有効になっている無線サービスの情報を、以下のいずれかのフレームを 6GHz 無線から送信することで検出できるようにします。

- **fils** モードでは、FILS(Fast Initial Link Setup）discovery フレームを使用して 6GHz の無線サービスを検出します。FILS discovery フレームは圧縮ビーコンフレームであり、SSID、BSSID、およびチャネルなどの重要な情報のみを含みます。この方法が構成されていると、AP の 6GHz 無線は 20 ミリ秒の間隔で FILS discovery フレームをブロードキャストします。無線サービスの検出方法を指定せずにこの機能を有効にした場合、fils モードが使用されます。
- **upr** モードでは、UPR(Unsolicited Probe Response)フレームを使用して 6GHz 無線サービスを検出します。UPR フレームはビーコンフレームと同じ詳細情報を含みます。この方法が構成されていると、AP の 6GHz 無線は 20 ミリ秒の間隔で UPR をブロードキャストします。

6GHz 無線を使用した 6GHz 帯無線サービス検出の設定方法は以下の通りです。

操作	コマンド	補足
1． system view に移行する	**system-view**	—

操作	コマンド	補足
2． global configuration view へ移行する	**wlan global-configuration**	—
3． 6GHz 帯ワイヤレスサービス検出機能を設定する	**wlan in-band 6g-discovery { enable | mode { fils | upr } }**	デフォルト：無効

1.10.3 マルチ BSSID の設定

🕮 **メモ：**

マルチ BSSID の設定は、ソフトウェアバージョン 9.6.05c を含む以降のソフトウェアからサポートしています。

この機能を有効にすると、AP は 1 つのビーコンフレームまたはプローブ応答に複数の BSSID に関する情報を含めて送信します。この機能は 6 GHz 帯無線を使用するときに有効にしてください。

マルチ BSSID の設定方法は以下の通りです。

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． global configuration view へ移行する	**wlan global-configuration**	—
3． マルチ BSSID を有効にする	**wlan multiple-bssid enable**	デフォルト：無効

1.10.4 サービステンプレートの設定

🕮 **メモ：**

- 6GHz 帯無線での **wpa3 personal optional** コマンドを設定したサービステンプレートの使用は、ソフトウェアバージョン 9.6.05c を含む以降のソフトウェアからサポートしています。
- 6GHz 帯無線での **wpa3-enterprise-only-mode** コマンド、**wpa3-enterprise-transition-mode** コマンドを設定したサービステンプレートの使用は、ソフトウェアバージョン 9.6.05c を含む以降のソフトウェアからサポートしています。
- 6GHz 帯無線での **enhanced-open enable** コマンドを設定したサービステンプレートの使用は、ソフトウェアバージョン 9.6.08c を含む以降のソフトウェアからサポートしています。

6GHz 帯の無線は、次の機能が有効になっているサービステンプレートのみ設定することができます。次のいずれかのサービステンプレートを設定します。

- Enhanced Open システム認証を有効にしてください。有効にするには、**enhanced-open enable** コマンを使用します。

- WPA3 パーソナルセキュリティモードを有効にしてください。有効にするには、次のいずれかのコマンドを設定します。
  - **wpa3 personal mandatory** コマンドを使用します。WPA3-SAE の SAE 交換時の PWE 生成方式として H2E モードを設定してください。H2E モードを設定するには、**akm sae pwe h2e** コマンドを使用します。なお、ソフトウェアバージョン 9.6.05c を含む以降のソフトウェアでは **akm sae pwe h2e** コマンドが設定されていないサービステンプレートを 6GHz 帯の無線に設定できますが、内部では H2E モードとして動作します。
  - **wpa3 personal optional** コマンドを使用します。**akm sae pwe** コマンドの設定は不要です。6GHz 帯の無線に設定すると、内部では **wpa3 personal mandatory**、H2E モード(**akm sae pwe h2e**)として動作します。
- WPA3 エンタープライズ 192bit セキュリティモードを有効にしてください。有効にするには、**wpa3 enterprise** コマンドを使用します。暗号化規格を RSN に設定し、暗号化方式を GCMP に設定する必要があります。
- 192bit セキュリティなしの WPA3 エンタープライズセキュリティモードを有効にしてください。有効にするには、次のいずれかのコマンドを設定します。
  - **wpa3 enterprise-only-mode** コマンドを設定します。
  - **wpa3 enterprise-transition-mode** コマンドを設定します。6GHz 帯の無線に設定すると、内部では **wpa3 enterprise-only-mode** として動作します。

I. Enhanced Open システム認証の設定

🕮 **メモ：**

6GHz 帯の無線での Enhanced Open システム認証(**enhanced-open enable**)の利用は、ソフトウェアバージョン 9.6.08c を含む以降のソフトウェアからサポートしています。

Enhanced Open システム認証では、Opportunistic Wireless Encryption (OWE) を使用して、OWE 対応クライアントのデータパケットを暗号化するためのキーをネゴシエートし、セキュリティパフォーマンスを強化したオープンシステム認証を提供します。

この機能を有効にする前に、WPA3 セキュリティモード、FT、管理フレーム保護、暗号化規格、暗号化方式、KDF がデフォルト設定になっていることを確認してください。

この機能を有効にすると、次の操作が実行されます。

- セキュリティ IE を RSN として指定します。
- 暗号スイートを CCMP として指定します。
- 管理フレーム保護を有効にします。
- HMAC-SHA256 および HMAC-SHA384 アルゴリズムを KDF として指定します。

Enhanced Open システム認証の設定方法は以下の通りです。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. service-template view へ移行する	**wlan service-template** *service-template-name*	—
3. Enhanced Open システム認証機能を有効にする	**enhanced-open enable**	デフォルト：無効

II. WPA3 パーソナルモードの設定

WPA3-SAE では、WPA2-Personal の PSK に代わる Simultaneous Authentication of Equals (SAE) を使用して、より堅牢なパスワードベースの認証を提供します。これにより、個々のユーザの保護が向上します。6GHz 帯の無線は、WPA3 パーソナル mandatory モードのみをサポートします。

WPA3-SAE は、Hunting-and-Pecking (HnP) と Hash-to-Element (H2E) を使用した PWE の生成方式をサポートしています。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。

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、クライアントはワイヤレスネットワークにアクセスできません。6GHz 帯の無線は H2E 方法のみをサポートします。

WPA3-SAE を使用するには、暗号スイートを CCMP に設定し、セキュリティ IE を RSN に設定します。

一部のクライアントは、一時的に WPA3 エンタープライズセキュリティモードを使用してオンラインになった場合、WPA3-SAE セキュリティモードを使用してオンラインになることができません。このような問題が発生した場合、クライアントは WPA3-SAE セキュリティモードを使用して再試行できます。

WPA3 セキュリティモードを設定し、同時に 802.11r FT を有効にしないでください。その場合、サービステンプレートを有効にすることができなくなります。

WPA3 パーソナルモードの設定方法は以下の通りです。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. service-template view へ移行する	**wlan service-template** *service-template-name*	—
3. WPA3 パーソナルモードを設定する	**wpa3 personal { mandatory | optional }**	デフォルト：無効
4. WPA3-SAE の SAE 交換時の PWE 生成方式を設定する	**akm sae pwe h2e**	—
5. 暗号化規格として RSN を設定する	**security-ie rsn**	デフォルト：設定なし
6. 暗号化方式として CCMP を設定する	**cipher-suite ccmp**	デフォルト：設定なし
7. 管理フレーム保護機能を有効にする	**pmf { optional | mandatory }**	デフォルト：無効
8. KDF を設定する	**key-derivation { sha1 | sha256 | sha1-and-sha256 }**	デフォルト：sha1

III. WPA3 エンタープライズ 192bit セキュリティモードの設定

WPA3 エンタープライズの 192bit セキュリティモードは、**wpa3 enterprise** コマンドで有効にします。暗号化規格を RSN に設定し、暗号化方式を GCMP に設定する必要があります。

WPA3 エンタープライズ 192bit セキュリティモードの設定方法は以下の通りです。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. service-template view へ移行する	**wlan service-template** *service-template-name*	—
3. WPA3 エンタープライズモードを設定する	**wpa3 enterprise**	デフォルト：無効
4. 暗号化規格として RSN を設定する	**security-ie rsn**	デフォルト：設定なし
5. 暗号化方式として GCMP を設定する	**cipher-suite gcmp**	デフォルト：設定なし
6. 管理フレーム保護機能を有効にする	**pmf { optional | mandatory }**	デフォルト：無効
7. KDF を設定する。	**key-derivation { sha1 | sha256 | sha1-and-sha256 }**	デフォルト：sha1

IV. 192bit セキュリティなしの WPA3 エンタープライズの設定

192bit セキュリティなしの WPA3 エンタープライズは、**wpa3 enterprise-only-mode** コマンドもしくは **wpa3 enterprise-transition-mode** コマンドで有効にします。暗号化規格を RSN に設定し、暗号化方式を CCMP に設定する必要があります。

192bit セキュリティなしの WPA3 エンタープライズの設定方法は以下の通りです。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. service-template view へ移行する	**wlan service-template** *service-template-name*	—
3. WPA3 エンタープライズモードを設定する	**wpa3 { enterprise-only-mode | enterprise-transition-mode }**	デフォルト：無効
4. 暗号化規格として RSN を設定する	**security-ie rsn**	デフォルト：設定なし
5. 暗号化方式として CCMP を設定する	**cipher-suite ccmp**	デフォルト：設定なし

1.10.5 サービステンプレートの有効化

サービステンプレートの設定方法は以下の通りです。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. service-template view へ移行する	**wlan service-template** service-template-name	—
3. サービステンプレートを有効にする	**service-template enable**	デフォルト：無効

1.10.6 無線に対するサービステンプレートの設定

I. radio view での無線に対するサービステンプレートの設定方法

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP view に移行する	**wlan ap** *ap-name* **[model** *model-name* **]**	—
3. radio view へ移行する	**radio** *radio-id*	—
4. 無線に対してサービステンプレートを設定する	**service-template** *service-template-name*	デフォルト：AP group viewの設定を使用します。

II. AP group radio view での無線に対するサービステンプレートの設定方法

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP group view に移行する	**wlan ap-group** *group-name*	—
3. AP model view に移行する	**ap-model** *ap-model*	—
4. radio view へ移行する	**radio** *radio-id*	—
5. 無線に対してサービステンプレートを設定する	**service-template** *service-template-name*	デフォルト：設定なし

1.11 スマートアンテナ機能の設定

🕮 **メモ**：

この機能に対するサポートは装置モードに依存します。

⚠ **重要**：

この機能は、802.11n と 802.11ac/ax 無線に対してのみ適用されます。

スマートアンテナ機能により、AP は信号品質と安定性を向上させるために、クライアント位置とチャネル情報にもとづいたアンテナパラメータを自動的に適用可能になります。

無線が、以下のスマートアンテナモードのいずれかで作動するように設定することができます。

- **自動モード**－音声パケットとビデオパケットに対しては高可用性モードを使用します。また、別のパケットに対しては高処理能力モードを使用します。
- **高可用性モード**－安定した帯域幅を要求する WLAN に適用されます。このモードは、雑音とインタフェースの影響を低減し、クライアントに対して帯域幅を保証します。
- **高処理能力モード**－ハイパフォーマンスを要求する WLAN に適用されます。このモードは、信号強度と関連づけ機能を強化します。

I. radio view でのスマートアンテナ機能の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP を作成し、AP view へ移行する	**wlan ap** *ap-name* [**model** *model-name*]	デフォルト：設定なし APを作成するときは名前とモデルを指定する必要があります。
3． radio view へ移行する	**radio** *radio-id*	—
4． スマートアンテナ機能の有効化	**smart antenna enable**	デフォルト：無線はAP group viewの設定を使用します。
5． スマートアンテナモードを指定する	**smart-antenna policy** { **auto** | **high-availability** | **high-throughput** }	デフォルト：無線はAP group viewの設定を使用します。

II. AP group view でのスマートアンテナ機能の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP を作成し、AP view へ移行する	**wlan ap-group** *group-name*	デフォルト：デフォルトAPグループ（default-group）が存在し、デフォルトAPグループは削除することができません。
3． AP model view へ移行する	**ap-model** *ap-model*	—
4． radio view へ移行する	**radio** *radio-id*	—
5． スマートアンテナ機能の有効化	**smart antenna enable**	デフォルト：無効
6． スマートアンテナモードを指定する	**smart-antenna policy** { **auto** | **high-availability** | **high-throughput** }	デフォルト：自動モード

1.12 無線管理の表示および管理

すべての view で **display** コマンドを実行できます。

操作	コマンド
連続モードに関する情報を表示	display wlan ap { all | name ap-name } continuous-mode
AP無線の情報を表示する	**display wlan ap** { **all** | **name** ap-name } **radio** [**frequency-band** { **5** | **2.4** }]
無線チャネルの情報を表示する	**display wlan ap** { **all** | **name** *ap-name* } **radio channel**
無線タイプの情報を表示する	**display wlan ap** { **all** | **name** *ap-name* } **radio type**
無線の統計情報を表示する	display wlan statistics ap { all | name ap-name } radio

reset コマンドは、user view でのみ実行できます。

操作	コマンド
無線の統計情報を削除する	**reset wlan** statistics **ap** { **all** | **name** *ap-name* } **radio**

1.13 無線管理の設定例

1.13.1 基本無線機能の設定例

I. ネットワーク要件

図 1-6 に示すように、手動 AP を作成し、無線モード、作動チャネル、最大伝送電力に対してそれぞれ 802.11gn、channel 11、19 dBm を設定します。

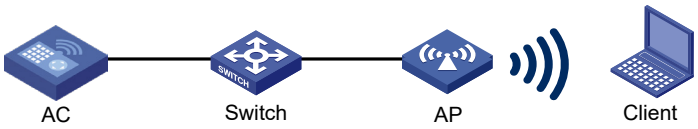


図 1-6 ネットワーク図

II. 設定手順

AP 名が ap1 の手動 AP を作成し、モデル名、シリアル ID を指定します。

```
<AC> system-view
[AC] wlan ap ap1 model QX-W1020
[AC-wlan-ap-ap1] serial-id 219801A0CNC138011454
```

radio 2 の radio view に移行します。

```
[AC-wlan-ap-ap1] radio 2
```

無線モードを dot11gn に設定します。

```
[AC-wlan-ap-ap1-radio-2] type dot11gn
```

radio 2 の作動チャネルを channel 11 に設定します。

```
[AC-wlan-ap-ap1-radio-2] channel 11
```

最大伝送電力を 19 dBm に設定します。

```
[AC-wlan-ap-ap1-radio-2] max-power 19
```

radio 2 を有効にします。

```
[AC-wlan-ap-ap1-radio-2] radio enable
```

III. 設定の確認

すべての無線の情報を表示します。

[AC] display wlan ap all verbose

```
Total number of APs: 1
Total number of connected APs: 1
Total number of connected manual APs: 1
Total number of connected auto APs: 0
Total number of connected common APs: 1
Total number of connected WTUs: 0
Total number of inside APs: 0
Maximum supported APs: 6144
Remaining APs: 6144
Total AP licenses: 128
local AP licenses: 0
Server AP licenses: 0
Remaining local AP licenses: 127
Sync AP licenses: 0

AP name                         : ap1
AP ID                           : 1
AP group name                   : default-group
State                           : Run
Backup type                     : Master

Online time                     : 0 days 1 hours 25 minutes 12 seconds
System up time                  : 0 days 2 hours 22 minutes 12 seconds
Model                           : QX-W1020
Region code                     : CN
Region code lock                : Disable
Serial ID                       : 219801A0CNC138011454
MAC address                     : 0AFB-423B-893C
IP address                      : 192.168.1.50
UDP port number                 : 65488
H/W version                     : Ver.C
S/W version                     : V700R001B49D001
Boot version                    : 1.01
USB state                       : N/A
Power level                     : N/A
Power info                      : N/A
Description                     : Not configured
Priority                        : 4
Echo interval                   : 10 seconds
Echo count                      : 3 counts
Keepalive interval              : 10 seconds
discovery-response wait-time    : 2 seconds
Statistics report interval      : 50 seconds
Fragment size (data)            : 1500
Fragment size (control)         : 1450
MAC type                        : Local MAC & Split MAC
Tunnel mode                     : Local Bridging & 802.3 Frame & Native Frame
CAPWAP data-tunnel status       : Down
Discovery type                  : Static Configuration
Retransmission count            : 3
Retransmission interval         : 5 seconds
Firmware upgrade                : Enabled
Sent control packets            : 1
Received control packets        : 1
Echo requests                   : 147
Lost echo responses             : 0
Average echo delay              : 3
Last reboot reason              : User soft reboot
Latest IP address               : 10.1.0.2
Current AC IP                   : N/A
Tunnel down reason              : Request wait timer expired
Connection count                : 1
Backup Ipv4                     : Not configured
Backup Ipv6                     : Not configured
```

```
Tunnel encryption             : Disabled
LED mode                      : Normal
Remote configuration          : Enabled
Radio 1:
    Basic BSSID               : 7848-59f6-3940
    Admin state               : Up
    Radio mode                : 802.11ax
    Antenna type              : internal
    Client dot11ac-only       : Disabled
    Client dot11n-only        : Disabled
    Channel band-width        : 20/40/80MHz
    Active band-width         : 20/40/80MHz
    Secondary channel offset  : SCB
    Short GI for 20MHz        : Supported
    Short GI for 40MHz        : Supported
    Short GI for 80MHz        : Supported
    Short GI for 160MHz       : Not supported
    mimo                      : Not Config
    Green-Energy-Management   : Disabled
    A-MSDU                    : Enabled
    A-MPDU                    : Enabled
    LDPC                      : Not Supported
    STBC                      : Supported
    Operational VHT-MCS Set:
        Mandatory             : Not configured
        Supported             : NSS1 0,1,2,3,4,5,6,7,8,9
                                NSS2 0,1,2,3,4,5,6,7,8,9
        Multicast             : Not configured
    Operational HT MCS Set:
        Mandatory             : Not configured
        Supported             : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9,
                                10, 11, 12, 13, 14, 15
        Multicast             : Not configured
    Channel                   : 44(auto)
    Channel usage(%)          : 0
    Max power                 : 20 dBm
    Operational rate:
        Mandatory             : 6, 12, 24 Mbps
        Multicast             : Auto
        Supported             : 9, 18, 36, 48, 54 Mbps
        Disabled              : Not configured
    Distance                  : 1 km
    ANI                       : Enabled
    Fragmentation threshold   : 2346 bytes
    Beacon interval           : 100 TU
    Protection threshold      : 2346 bytes
    Long retry threshold      : 4
    Short retry threshold     : 7
    Maximum rx duration       : 2000 ms
    Noise Floor               : -102 dBm
    Protection mode           : rts-cts
    Continuous mode           : N/A
    MU-TxBF                   : Enabled
    SU-TxBF                   : Enabled
    Continuous mode           : N/A
    Client dot11ax-only       : Disabled
    Operational HE-MCS Set:
        Mandatory             : Not configured
        Supported             : NSS1 0,1,2,3,4,5,6,7,8,9,10,11
                                NSS2 0,1,2,3,4,5,6,7,8,9,10,11
        Multicast             : Not configured
    OFDMA random access RUs   : Not Supported
    Channel Width Set         : 0x02
    DL-OFDMA                  : Enabled
    UL-OFDMA                  : Enabled
    UL-MU-MIMO                : Disabled
    BSS-COLOR                 : Enabled
    TWT negotiation           : Disabled
    HT protection mode        : No protection
Radio 2:
```

```
    Basic BSSID               : 7848-59f6-3950
    Admin state               : Up
    Radio mode                : 802.11n(2.4GHz)
    Antenna type              : internal
    Client dot11n-only        : Disabled
    Channel band-width        : 20MHz
    Active band-width         : 20MHz
    Secondary channel offset  : SCN
    Short GI for 20MHz        : Supported
    Short GI for 40MHz        : Supported
    A-MSDU                    : Enabled
    A-MPDU                    : Enabled
    LDPC                      : Not Supported
    STBC                      : Supported
    Operational HT MCS Set:
        Mandatory             : Not configured
        Supported             : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9,
                                10, 11, 12, 13, 14, 15
        Multicast             : Not configured
    Channel                   : 11
    Channel usage(%)          : 0
    Max power                 : 19 dBm
    Preamble type             : Short
    Operational rate:
        Mandatory             : 1, 2, 5.5, 11 Mbps
        Multicast             : Auto
        Supported             : 6, 9, 12, 18, 24, 36, 48, 54 Mbps
        Disabled              : Not configured
    Distance                  : 1 km
    ANI                       : Enabled
    Fragmentation threshold   : 2346 bytes
    Beacon interval           : 100 TU
    Protection threshold      : 2346 bytes
    Long retry threshold      : 4
    Short retry threshold     : 7
    Maximum rx duration       : 2000 ms
    Noise Floor               : -105 dBm
    Smart antenna             : Enabled
    Smart antenna policy      : Auto
    Protection mode           : rts-cts
    Continuous mode           : N/A
    HT protection mode        : No protection
```

1.13.2 6GHz 帯の無線(Enhanced Open)の設定例

🕮 メモ：

6GHz 帯の無線での Enhanced Open システム認証(**enhanced-open enable**)の利用は、ソフトウェアバージョン 9.6.08c を含む以降のソフトウェアからサポートしています。

I. ネットワーク要件

図 1-7 に示すように、AP 上の無線 1(6GHz 帯)にクライアントが接続して通信できるように設定します。

- 6GHz 帯の無線サービス検出を有効にします。
- AP 上の無線 1(6GHz 帯)に、サービステンプレート service を設定します。サービステンプレートは Enhanced Open システム認証を設定します。
- AP 上の無線 2 に、6GHz 帯の無線サービスを検出するためのサービステンプレート radio2 を設定します。

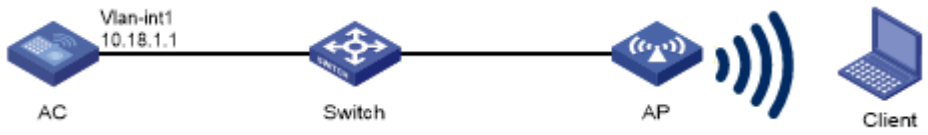


図 1-7 ネットワーク図

II. 設定手順

#6GHz 帯無線サービスの検出を有効にします。

```
<AC> system-view
[AC] wlan global-configuration
[AC-wlan-global-configuration] wlan out-band 6g-discovery enable
[AC-wlan-global-configuration] quit
```

#サービステンプレート service を作成します。

```
[AC] wlan service-template service
```

#サービステンプレートの SSID を指定します。

```
[AC-wlan-st-service] ssid service
```

#enhanced open システム認証を有効にします。

```
[AC-wlan-st-service] enhanced-open enable
```

#サービステンプレート service を有効にします。

```
[AC-wlan-st-service] service-template enable
[AC-wlan-st-service] quit
```

#サービステンプレート radio2 を作成します。

```
[AC] wlan service-template radio2
```

#サービステンプレートの SSID を指定します。

```
[AC-wlan-st-radio2] ssid radio2
```

#サービステンプレート radio2 を有効にします。

```
[AC-wlan-st-radio2] service-template enable
[AC-wlan-st-radio2] quit
```

AP 名が ap1 の手動 AP を作成し、モデル名、シリアル ID を指定します。

```
[AC] wlan ap ap1 model QX-W1240
[AC-wlan-ap-ap1] serial-id 219801A5B1234567890
```

#サービステンプレート service を ap1 の radio 1 に割り当て、radio 1 を有効にします。

```
[AC] wlan ap ap1
```

```
[AC-wlan-ap-ap1] radio 1
[AC-wlan-ap-ap1-radio-1] radio enable
[AC-wlan-ap-ap1-radio-1] service-template service
[AC-wlan-ap-ap1-radio-1] quit
```

#サービステンプレート radio2 を ap1 の radio 2 に割り当て、radio 2 を有効にします。

```
[AC-wlan-ap-ap1] radio 2
[AC-wlan-ap-ap1-radio-2] radio enable
[AC-wlan-ap-ap1-radio-2] service-template radio2
[AC-wlan-ap-ap1-radio-2] return
```

III. 設定の確認

クライアントが SSID に接続できることを確認します。（詳細は省略します。）

1.13.3 6GHz 帯の無線(WPA3 パーソナル)の設定例

I. ネットワーク要件

図 1-8 に示すように、AP 上の無線 1(6GHz 帯)にクライアントが接続して通信できるように設定します。

- 6GHz 帯の無線サービス検出を有効にします。
- AP 上の無線 1(6GHz 帯)に、サービステンプレート service を設定します。サービステンプレートは WPA3 パーソナルを設定します。
- AP 上の無線 2 に、6GHz 帯の無線サービスを検出するためのサービステンプレート radio2 を設定します。

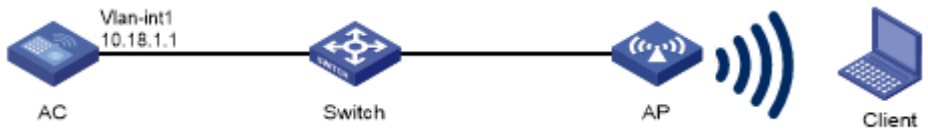


図 1-8 ネットワーク図

II. 設定手順

#6GHz 帯無線サービスの検出を有効にします。

```
<AC> system-view
[AC] wlan global-configuration
[AC-wlan-global-configuration] wlan out-bound 6g-discovery enable
```

```
[AC-wlan-global-configuration] quit
```

#サービステンプレート service を作成します。

```
[AC] wlan service-template service
```

#サービステンプレートの SSID を指定します。

```
[AC-wlan-st-service] ssid service
```

#AKM モードとして PSK を設定し、プレーンテキストで共有鍵 12345678 を指定します。

```
[AC-wlan-st-service1] akm mode psk
[AC-wlan-st-service1] preshared-key pass-phrase simple 12345678
```

暗号化方式に CCMP、暗号化規格に RSN を指定します。

```
[AC-wlan-st-service1] cipher-suite ccmp
[AC-wlan-st-service1] security-ie rsn
```

WPA3 の設定を personal に設定し、管理フレーム保護を設定します。

- WPA3 セキュリティモードを mandatory に設定し、mandatory モードで管理フレーム保護を有効にします。

```
[AC-wlan-st-service] wpa3 personal mandatory
[AC-wlan-st-service] pmf mandatory
```

- WPA3 セキュリティモードを optional に設定し、optional モードで管理フレーム保護を有効にします。

📖メモ：6GHz 帯の無線での wpa3 personal optional の利用は、ソフトウェアバージョン 9.6.05c 以降のソフトウェアからサポートしています。

```
[AC-wlan-st-service] wpa3 personal optional
[AC-wlan-st-service] pmf optional
```

KDF を sha1-and-sha256 に設定します。

```
[AC-wlan-st-service] key-derivation sha1-and-sha256
```

WPA3-SAE の SAE 交換時の PWE 生成方式として H2E 方式を設定します。

📖メモ : ソフトウェアバージョン 9.6.05c 含む以降のソフトウェアではこの設定は省略可能です。必要に応じて設定してください。

```
[AC-wlan-st-service] akm sae pwe h2e
```

#サービステンプレート service を有効にします。

```
[AC-wlan-st-service] service-template enable
[AC-wlan-st-service] quit
```

#サービステンプレート radio2 を作成します。

```
[AC] wlan service-template radio2
```

#サービステンプレートの SSID を指定します。

```
[AC-wlan-st-radio2] ssid radio2
```

#サービステンプレート radio2 を有効にします。

```
[AC-wlan-st-radio2] service-template enable
[AC-wlan-st-radio2] quit
```

AP 名が ap1 の手動 AP を作成し、モデル名、シリアル ID を指定します。

```
[AC] wlan ap ap1 model QX-W1240
[AC-wlan-ap-ap1] serial-id 219801A5B1234567890
```

#サービステンプレート service を ap1 の radio 1 に割り当て、radio 1 を有効にします。

```
[AC] wlan ap ap1
[AC-wlan-ap-ap1] radio 1
[AC-wlan-ap-ap1-radio-1] radio enable
[AC-wlan-ap-ap1-radio-1] wlan service-template service
[AC-wlan-ap-ap1-radio-1] quit
```

#サービステンプレート radio2 を ap1 の radio 2 に割り当て、radio 2 を有効にします。

```
[AC-wlan-ap-ap1] radio 2
[AC-wlan-ap-ap1-radio-2] radio enable
[AC-wlan-ap-ap1-radio-2] wlan service-template radio2
[AC-wlan-ap-ap1-radio-2] return
```

III. 設定の確認

クライアントが SSID に接続できることを確認します。（詳細は省略します。）

1.13.4 6GHz 帯の無線(WPA3 エンタープライズ 192bit セキュリティあり)の設定例

I. ネットワーク要件

図 1-9 に示すように、AP 上の無線 1(6GHz 帯)にクライアントが接続して通信できるように設定します。

- 6GHz 帯の無線サービス検出を有効にします。
- AP 上の無線 1(6GHz 帯)に、サービステンプレート service を設定します。サービステンプレートは WPA3 エンタープライズ (192bit セキュリティあり)を設定します。
- AP 上の無線 2 に、6GHz 帯の無線サービスを検出するためのサービステンプレート radio2 を設定します。

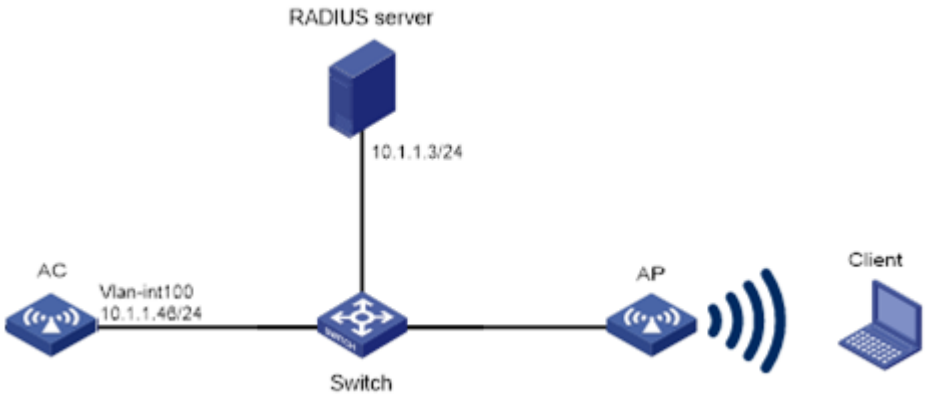


図 1-9 ネットワーク図

II. 設定手順

#6GHz 帯無線サービスの検出を有効にします。

```
<AC> system-view
[AC] wlan global-configuration
[AC-wlan-global-configuration] wlan out-bound 6g-discovery enable
[AC-wlan-global-configuration] quit
```

#サービステンプレート service を作成します。

```
[AC] wlan service-template service
```

#サービステンプレートの SSID を指定します。

```
[AC-wlan-st-service] ssid service
```

AKM モードとして 802.1X を設定します。

```
[AC-wlan-st-service1] akm mode dot1x
```

暗号化方式に GCMP、暗号化規格に RSN を指定します。

```
[AC-wlan-st-service1] cipher-suite gcmp
[AC-wlan-st-service1] security-ie rsn
```

WPA3 の設定を enterprise に設定します。

```
[AC-wlan-st-service1] wpa3 enterprise
```

mandatory モードで管理フレーム保護を有効にします。

```
[AC-wlan-st-service1] pmf mandatory
```

KDF を sha1-and-sha256 に設定します。

```
[AC-wlan-st-service1] key-derivation sha1-and-sha256
```

802.1X 認証モードを設定します。

```
[AC-wlan-st-service1] client-security authentication-mode dot1x
```

802.1X 認証ドメインとして dom1 を設定します。

```
[AC-wlan-st-service1] dot1x domain dom1
```

#サービステンプレート service を有効にします。

```
[AC-wlan-st-service] service-template enable
[AC-wlan-st-service] quit
```

#サービステンプレート radio2 を作成します。

```
[AC] wlan service-template radio2
```

#サービステンプレートの SSID を指定します。

```
[AC-wlan-st-radio2] ssid radio2
```

#サービステンプレート radio2 を有効にします。

```
[AC-wlan-st-radio2] service-template enable
[AC-wlan-st-radio2] quit
```

RADIUS スキーム radius1 を作成し、RADIUS scheme view に移行します。

```
[AC] radius scheme radius1
```

プライマリ認証サーバ、アカウンティングサーバを指定します。

```
[AC-radius-radius1] primary authentication 10.1.1.3 1812
[AC-radius-radius1] primary accounting 10.1.1.3 1813
```

プレーンテキストで認証サーバ、アカウンティングサーバの共有鍵 12345 を設定します。

```
[AC-radius-radius1] key authentication simple 12345
[AC-radius-radius1] key accounting simple 12345
```

#dot1x を設定します。

```
[AC] dot1x
[AC] dot1x authentication-method eap
```

ISP ドメイン dom1 を作成し、ISP ドメインの RADIUS スキームを設定します。

```
[AC] domain dom1
[AC-isp-dom1] authentication lan-access radius-scheme radius1
[AC-isp-dom1] authorization lan-access radius-scheme radius1
[AC-isp-dom1] accounting lan-access radius-scheme radius1
[AC-isp-dom1] quit
```

AP 名が ap1 の手動 AP を作成し、モデル名、シリアル ID を指定します。

```
[AC] wlan ap ap1 model QX-W1240
```

```
[AC-wlan-ap-ap1] serial-id 219801A5B1234567890
```

#サービステンプレート service を ap1 の radio 1 に割り当て、radio 1 を有効にします。

```
[AC] wlan ap ap1
[AC-wlan-ap-ap1] radio 1
[AC-wlan-ap-ap1-radio-1] radio enable
[AC-wlan-ap-ap1-radio-1] wlan service-template service
[AC-wlan-ap-ap1-radio-1] quit
```

#サービステンプレート radio2 を ap1 の radio 2 に割り当て、radio 2 を有効にします。

```
[AC-wlan-ap-ap1] radio 2
[AC-wlan-ap-ap1-radio-2] radio enable
[AC-wlan-ap-ap1-radio-2] wlan service-template radio2
[AC-wlan-ap-ap1-radio-2] return
```

III. 設定の確認

クライアントが SSID に接続できることを確認します。（詳細は省略します。）

1.13.5 6GHz 帯の無線(WPA3 エンタープライズ 192bit セキュリティなし)の設定例

🕮 **メモ**：

- 6GHz 帯無線での **wpa3-enterprise-only-mode** コマンド、**wpa3-enterprise-transition-mode** コマンドを設定したサービステンプレートの使用は、ソフトウェアバージョン 9.6.05c を含む以降のソフトウェアからサポートしています。

I. ネットワーク要件

図 1-10 に示すように、AP 上の無線 1(6GHz 帯)にクライアントが接続して通信できるように設定します。

- 6GHz 帯の無線サービス検出を有効にします。
- AP 上の無線 1(6GHz 帯)に、サービステンプレート service を設定します。サービステンプレートは WPA3 エンタープライズ (192bit セキュリティなし)を設定します。
- AP 上の無線 2 に、6GHz 帯の無線サービスを検出するためのサービステンプレート radio2 を設定します。

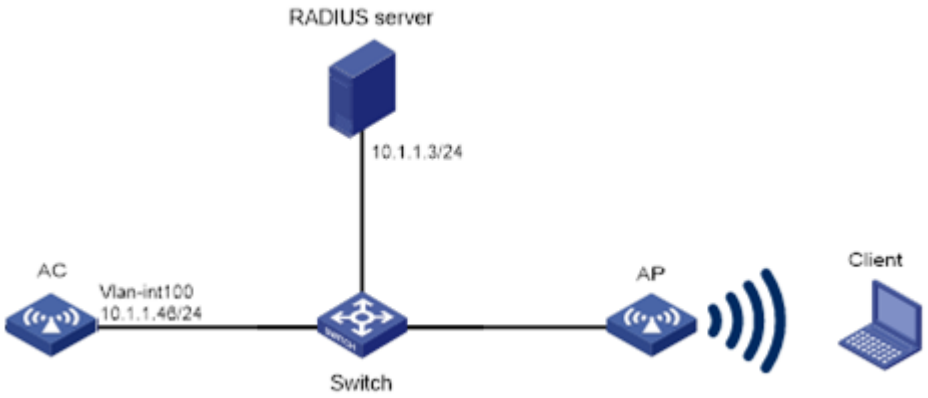


図 1-10 ネットワーク図

II. 設定手順

#6GHz 帯無線サービスの検出を有効にします。

```
<AC> system-view
[AC] wlan global-configuration
[AC-wlan-global-configuration] wlan out-band 6g-discovery enable
[AC-wlan-global-configuration] quit
```

#サービステンプレート service を作成します。

```
[AC] wlan service-template service
```

#サービステンプレートの SSID を指定します。

```
[AC-wlan-st-service] ssid service
```

AKM モードとして 802.1X を設定します。

```
[AC-wlan-st-service] akm mode dot1x
```

暗号化方式に CCMP、暗号化規格に RSN を指定します。

```
[AC-wlan-st-service] cipher-suite ccmp
[AC-wlan-st-service] security-ie rsn
```

WPA3 エンタープライズの 192bit セキュリティなしモードを設定します。

- wpa3 enterprise-only-mode を設定します。

```
[AC-wlan-st-service] wpa3 enterprise-only-mode
```

- wpa3 enterprise-transition-mode を設定します。

```
[AC-wlan-st-service] wpa3 enterprise-transition-mode
```

802.1X 認証モードを設定します。

```
[AC-wlan-st-service] client-security authentication-mode dot1x
```

802.1X 認証ドメインとして dom1 を設定します。

```
[AC-wlan-st-service] dot1x domain dom1
```

#サービステンプレート service を有効にします。

```
[AC-wlan-st-service] service-template enable
[AC-wlan-st-service] quit
```

#サービステンプレート radio2 を作成します。

```
[AC] wlan service-template radio2
```

#サービステンプレートの SSID を指定します。

```
[AC-wlan-st-radio2] ssid radio2
```

#サービステンプレート radio2 を有効にします。

```
[AC-wlan-st-radio2] service-template enable
[AC-wlan-st-radio2] quit
```

RADIUS スキーム radius1 を作成し、RADIUS scheme view に移行します。

```
[AC] radius scheme radius1
```

プライマリ認証サーバ、アカウンティングサーバを指定します。

```
[AC-radius-radius1] primary authentication 10.1.1.3 1812
[AC-radius-radius1] primary accounting 10.1.1.3 1813
```

プレーンテキストで認証サーバ、アカウンティングサーバの共有鍵 12345 を設定します。

```
[AC-radius-radius1] key authentication simple 12345
[AC-radius-radius1] key accounting simple 12345
```

#dot1x を設定します。

```
[AC] dot1x
[AC] dot1x authentication-method eap
```

ISP ドメイン dom1 を作成し、ISP ドメインの RADIUS スキームを設定します。

```
[AC] domain dom1
[AC-isp-dom1] authentication lan-access radius-scheme radius1
[AC-isp-dom1] authorization lan-access radius-scheme radius1
[AC-isp-dom1] accounting lan-access radius-scheme radius1
[AC-isp-dom1] quit
```

AP 名が ap1 の手動 AP を作成し、モデル名、シリアル ID を指定します。

```
[AC] wlan ap ap1 model QX-W1240
[AC-wlan-ap-ap1] serial-id 219801A5B1234567890
```

#サービステンプレート service を ap1 の radio 1 に割り当て、radio 1 を有効にします。

```
[AC] wlan ap ap1
[AC-wlan-ap-ap1] radio 1
[AC-wlan-ap-ap1-radio-1] radio enable
[AC-wlan-ap-ap1-radio-1] service-template service
[AC-wlan-ap-ap1-radio-1] quit
```

#サービステンプレート radio2 を ap1 の radio 2 に割り当て、radio 2 を有効にします。

```
[AC-wlan-ap-ap1] radio 2
[AC-wlan-ap-ap1-radio-2] radio enable
[AC-wlan-ap-ap1-radio-2] service-template radio2
[AC-wlan-ap-ap1-radio-2] return
```

III. 設定の確認

クライアントが SSID に接続できることを確認します。（詳細は省略します。）

目次

このセクションのページは **9-x-x** です。

2 章 WLAN 無線ロードバランスの設定 2-1
2.1 概要 2-1
2.1.1 ネットワークスキーム 2-1
2.1.2 無線ロードバランスのモードとタイプ 2-1
2.2 制限とガイドライン 2-2
2.3 WLAN 無線ロードバランシングタスクの概要 2-2
2.4 WLAN 無線ロードバランシングの有効化 2-3
2.5 無線ロードバランシングパラメータの設定 2-3
2.6 5GHz 無線ロードバランス機能 2-3
2.7 WLAN radio load balancing 設定の例 2-4
2.7.1 WLAN 無線ロードバランシングの設定 2-4

2章 WLAN 無線ロードバランスの設定

2.1 概要

WLAN 無線ロードバランスは、同じ AC で管理されている AP 上の無線間でクライアントの負荷を動的に分散します。これにより、高密度 WLAN のクライアントに対してワイヤレスサービス品質と適切な帯域幅が保証されます。

2.1.1 ネットワークスキーム

図 2-1 に示すように、AP 1 と AP 2 は同じ AC によって管理され、それぞれ Radio1 と Radio2 が有効になっており、無線ロードバランシングが有効になっています。

AP 1 の Radio1 と Radio2 が最大負荷に達した状態で、Client6 が AP 1 に接続しようとすると、AC は Client6 を AP2 に誘導します。

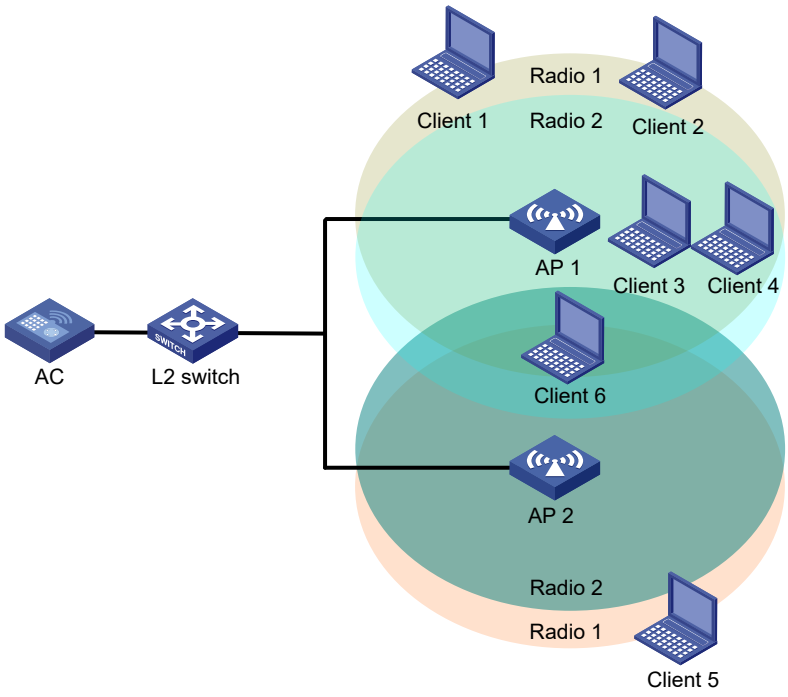


図 2-1 ネットワーク図

2.1.2 無線ロードバランスのモードとタイプ

装置は、セッションモードの無線ロードバランスと次の無線ロードバランスタイプをサポートしています。

- **セッションギャップしきい値ベース**－装置は、次の条件が満たされた場合に無線ロードバランスを実行します。
  - 無線に関連付けられたクライアントの数が、セッションしきい値に達した場合
  - クライアント数が最も少ない無線と無線の間のセッションギャップが、セッションギャップしきい値に達した場合

- 帯域比率ベース:デバイス－次のシナリオで無線ロードバランスを実行します。

  シナリオ 1
  - クライアントが 5 GHz 無線との関連付けを要求します。
  - 5 GHz 無線に関連付けられたオンラインクライアントの数がセッションしきい値に達します。
  - 5 GHz のすべてのネイバ無線に関連付けられたクライアントの数に無線重量の値を乗じた値と、2.4 GHz のすべてのネイバ無線に関連付けられたクライアントの数に無線重量の値を乗じた値との比率が帯域比よりも大きいか、または無線の負荷が同じタイプのすべての無線の平均負荷よりも高くなっています。

  シナリオ 2
  - クライアントが 2.4 GHz 無線との関連付けを要求します。
  - 2.4 GHz 無線に関連付けられたオンラインクライアントの数がセッションしきい値に達しました。
  - 5 GHz のすべてのネイバ無線に関連付けられたクライアントの数に無線重量の値を乗じた値と、2.4 GHz のすべてのネイバ無線に関連付けられたクライアントの数に無線重量の値を乗じた値との比率が、帯域比以下か同等であるか、または無線の負荷が同じタイプのすべての無線の平均負荷以下か同等である。

注意：
クライアントのネイバ無線は、クライアントから要求を受信するすべての無線を指します。

2.2 制限とガイドライン

クライアントが WLAN へのアクセスを要求すると、システムは同じ AC によって管理され、クライアントによって検出可能な AP の無線間でのみ無線ロードバランスを実行します。

2.3 WLAN無線ロードバランシングタスクの概要

操作リスト
1.（必須設定項目）WLAN無線ロードバランシングの有効化
2.（オプション設定項目）無線ロードバランシングパラメータの設定
3.（オプション設定項目）5GHz無線ロードバランス機能

2.4 WLAN無線ロードバランシングの有効化

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. WLAN 無線ロードバランスを有効にする	**wlan radio-load-balance enable** [**mode session** *value* [**gap** *gap-value* | **band-ratio** *5g-proportion 2.4g-proportion*] [**report-time** *time*]]	デフォルト：無効

2.5 無線ロードバランシングパラメータの設定

次のパラメータは、無線ロードバランシングの計算に影響します。

- 無線ロードバランシングの RSSI しきい値ークライアントの RSSI が指定されたしきい値よりも低い場合、無線はクライアントのアソシエーション要求を無視します。
- アソシエーション要求に対する拒否の最大数ー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。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. RSSI しきい値を設定する	**wlan radio-load-balance rssi-threshold** *rssi-threshold*	デフォルト：30
3. アソシエーション要求に対する拒否の最大数を設定する	**wlan radio-load-balance access-denial** *access-denial*	デフォルト：3

2.6 5GHz無線ロードバランス機能

🕮 **メモ：**

- この機能は QX-W1010 および QX-W1110 では利用できません。

この機能を有効にすると、5GHz 無線は次の 2 つの条件が満たされた場合に、ビーコンフレームの SSID を非表示にします。

- 5GHz 無線に関連付けられたクライアントの数が、しきい値に達した場合
- 同じ AP 内の 2 つの 5GHz 無線の間のセッションギャップが、しきい値に達した場合

5GHz 無線に関連付けられているクライアントの数がセッションしきい値を下回ると、5GHz 無線はビーコンフレームの SSID の非表示を停止します。

2 つの 5GHz 無線で同一の SSID で動作させる環境で、ネットワークに多数のクライアントが存在する場合は、この機能を有効にすることを推奨します。

SSID を非表示にするための過負荷状態の 5GHz 無線の設定手順は以下のとおりです。

操作	コマンド	補足
4. system view に移行する	**system-view**	—
5. AP view または AP group view に移行する	• AP viewに移行する **wlan ap** *ap-name* • AP group viewに移行する **wlan ap-group** *group-name*	—
6. 5 GHz 無線ロードバランスを有効にする	**wlan radio-load-balance overload-5g ssid-hide** [**session** *value* [**gap** *gap-value*]] }	デフォルト： AP viewでは、APはAP group viewの設定を使用します。 AP group viewでは、有効です。

2.7 WLAN radio load balancing 設定の例

2.7.1 WLAN 無線ロードバランシングの設定

ネットワーク要件

図 2-2 に示すように、AP 1 と AP 2 は AC によって管理され、クライアントは AP を検出できます。Client1 は AP 1 に関連付けられ、Client2～Client4 は AP 2 に関連付けられます。

次の条件が満たされている場合、AP を設定して、AP 1 と AP 2 の無線で無線ロードバランシングを実行します。

- AP の無線のセッション数が 3 に達する。
- 無線とセッション数が最も少ない無線とのセッションギャップが 2 に達する。

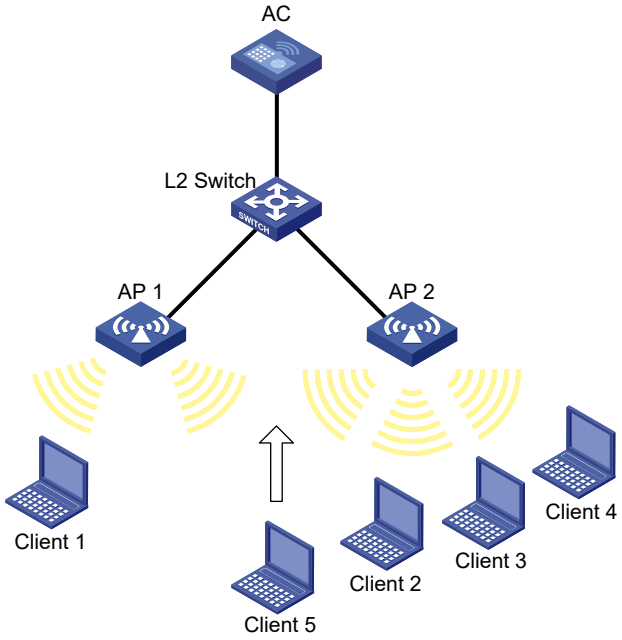


図 2-2 ネットワーク図

設定手順

#無線サービステンプレート 1 を作成し、その SSID を rlb に設定する。

```
<AC> system-view
[AC] wlan service-template 1
[AC-wlan-st-1] ssid rlb
[AC-wlan-st-1] service-template enable
[AC-wlan-st-1] quit
```

#AP テンプレート ap 1 を作成し、モデルとシリアル ID を指定する。

```
[AC] wlan ap ap1 WA1020
[AC-wlan-ap-ap1] serial-id 219801A28N819CE0002T
```

#サービステンプレート 1 を AP 1 の無線 2 にバインドする。

```
[AC-wlan-ap-ap1] radio2
[AC-wlan-ap-ap1-radio2] service-template 1
[AC-wlan-ap-ap1-radio2] radio enable
[AC-wlan-ap-ap1-radio2] quit
[AC-wlan-ap-ap1] quit
```

#AP テンプレート ap 2 を作成し、モデルとシリアル ID を指定する。

```
[AC] wlan ap ap2 WA1020
[AC-wlan-ap-ap2] serial-id 219801A28N819CE0002T
```

#サービステンプレート 1 を AP 2 の無線 2 にバインドする。

```
[AC-wlan-ap-ap2] radio2
[AC-wlan-ap-ap2-radio2] service-template 1
[AC-wlan-ap-ap2-radio2] radio enable
[AC-wlan-ap-ap2-radio2] quit
[AC-wlan-ap-ap2] quit
```

#WLAN 無線ロードバランシングを有効にし、セッションしきい値とセッションギャップしきい値をそれぞれ 3 と 2 に設定する。

```
[AC] wlan radio-load-balamce enable mode session 3 gap 2
```

#RSSI しきい値を 30 に設定する。

```
[AC] wlan radio-load-balance rssi-threshold 30
```

設定の確認

#次の条件が満たされている場合に、AC が AP 1 および AP 2 の無線で無線ロードバランシングを実行することを確認します。

- AP 2 の無線 2 のセッション数が 3 に達します。
- AP 2 の無線 2 と AP 1 の無線 2 のセッションギャップが 2 に達します。(詳細は省略します)

#display wlan client コマンドを使用して、AP 1 の Radio2 と AP 2 の Radio2 がロードバランスされていることを確認します。(詳細は省略します)

目次

このセクションのページは **9-x-x** です。

3 章 WLAN ロードバランスの設定 3-1
3.1 概要 3-1
3.1.1 実行必須条件 3-1
3.1.2 動作メカニズム 3-2
3.1.3 ロードバランスモード 3-2
3.1.4 ロードバランスタイプ 3-4
3.2 設定作業リスト 3-4
3.3 WLAN ロードバランスの設定 3-5
3.3.1 制限とガイドライン 3-5
3.3.2 WLAN ロードバランスの有効化 3-5
3.3.3 ロードバランスモードの設定 3-5
3.3.4 ロードバランスパラメータの設定 3-5
3.4 WLAN ロードバランスに対する SNMP 通知の有効化 3-6
3.5 WLAN ロードバランスの表示と維持 3-6
3.6 無線ベース WLAN ロードバランスの設定例 3-7
3.6.1 セッションモードロードバランスの設定 3-7
3.6.2 トラフィックモードロードバランスの設定 3-9
3.6.3 帯域幅モードロードバランスの設定 3-10
3.7 ロードバランスグループベース WLAN ロードバランスの設定例 3-12
3.7.1 セッションモードロードバランスの設定 3-12
3.7.2 トラフィックモードロードバランスの設定 3-14
3.7.3 帯域幅モードロードバランスの設定 3-17

3章 WLAN ロードバランスの設定

本章では、AP は有効な無線をひとつだけ持つと仮定します。

3.1 概要

WLAN ロードバランス機能は、密集した WLAN において無線サービスの品質とクライアントの帯域幅を保証するため、AP を経由したクライアントの負荷を動的に分散させます。

3.1.1 実行必須条件

WLAN ロードバランスを特定の AP 間で実行するために、AP は同じ AC に管理されなければなりません。同じ AC で管理することで、クライアントは AP を検出することができます。図 3-1 に示すように、ロードバランスは、同じ AC で管理された AP 1、AP 2、AP 3 上で有効化されます。AP 3 は最大ロードに達します。Client 5 が AP 3 と関連づけようとしたとき、AC はそのアソシエーション要求を拒否し、AP 1 か AP 2 に要求を送るように Client 5 に指示します。しかし、Client 5 が AP 3 しか発見できない場合、Client 5 は AP 3 に対してアソシエーション要求を送信し続けます。AP 3 が Client 5 を拒否する回数が、指定した拒絶の最大数に達した場合、AP 3 は Client 5 のアソシエーション要求を承認します。

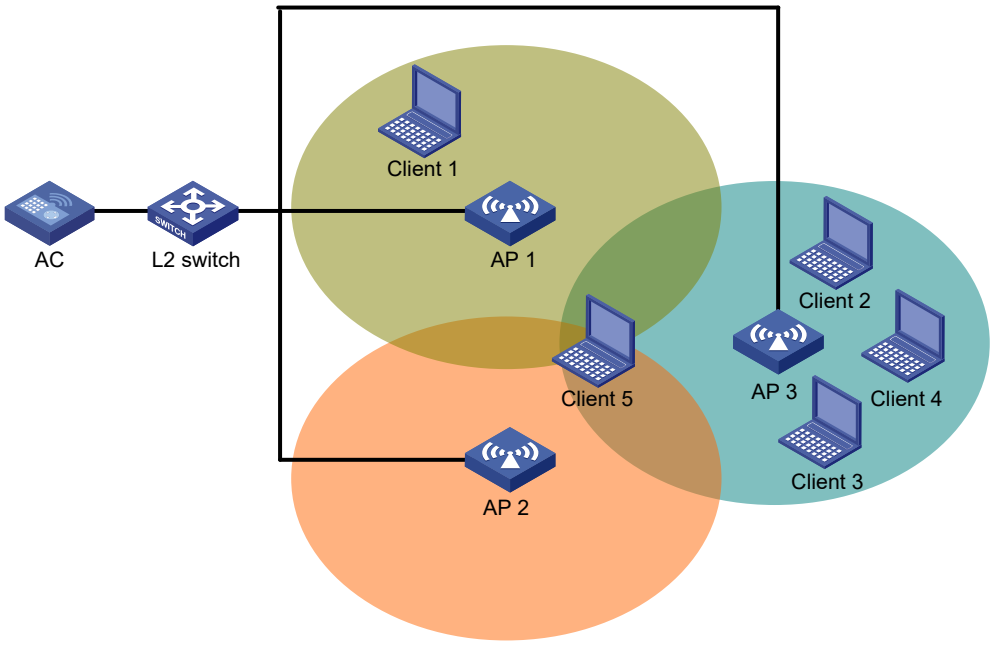


図 3-1 実行必須条件

3.1.2 動作メカニズム

AC は、以下の条件が満たされたときロードバランスを実行します。

- AP の負荷がしきい値に到達した
- AP と最も軽い負荷の AP との間の負荷のギャップが、しきい値に到達した

負荷と AP に対する負荷のギャップがそれぞれのしきい値に達すると、AP はクライアントのアソシエーション要求を拒否します。AP がクライアントを拒否する回数が、指定した拒絶の最大数に達した場合、AP はクライアントのアソシエーション要求を承認します。

3.1.3 ロードバランスモード

AC は、セッションモード、トラフィックモード、帯域幅モードロードバランスをサポートします。以下の条件が満たされたとき、AC は特定のモードのロードバランスを実行します。

- 指定したセッション/トラフィック/帯域幅しきい値に達した
- 指定したセッション/トラフィック/帯域幅ギャップしきい値に達した

I. セッションモードロードバランス

図 3-2 に示すように、Client 1 は AP 1 に関連づき、Client 2～Client 4 は AP 2 に関連づいています。セッションしきい値とセッションギャップしきい値を、それぞれ 3 と 2 に設定したと仮定します。Client 5 が AP 2 と関連づけようとしたとき、セッションしきい値とセッションギャップしきい値がともに最大値に達するため、AP 2 はその要求を拒否します。

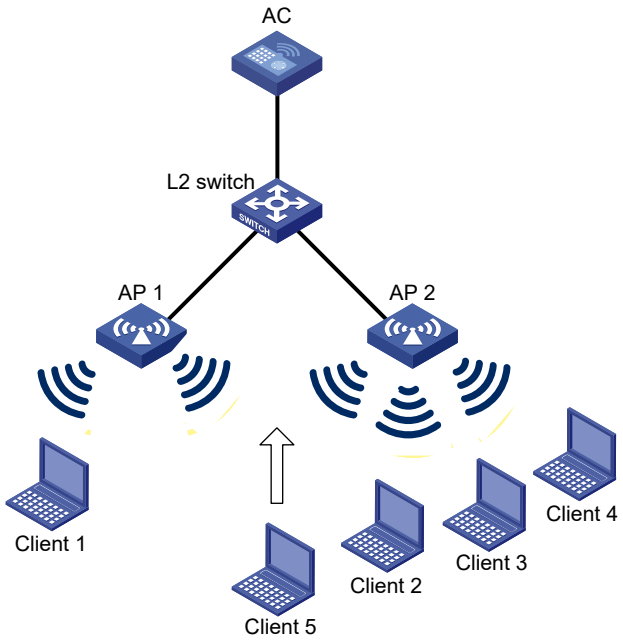


図 3-2 セッションモードロードバランス

II. トラフィックモードロードバランス

図 3-3 に示すように、Client 1 は AP 1 に関連付き、Client 2 は AP 2 に関連付いています。AP 1 のトラフィックと、AP1 と AP 2 のトラフィックギャップが、それぞれのしきい値に達するとき、AP 1 は Client 3 からのアソシエーション要求を拒否します。

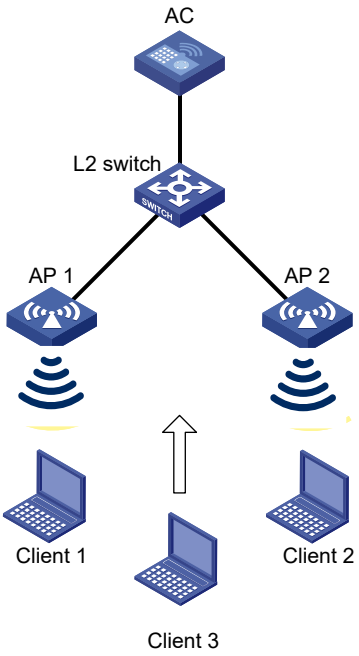


図 3-3 トラフィックモードロードバランス

III. 帯域幅モードロードバランス

図 3-4 に示すように、Client 1 は AP 1 に関連付き、Client 2 は AP 2 に関連付いています。AP 1 の帯域幅と、AP 1 と AP 2 の帯域幅ギャップが、それぞれのしきい値に達するとき、AP 1 は Client 3 からの要求を拒否します。

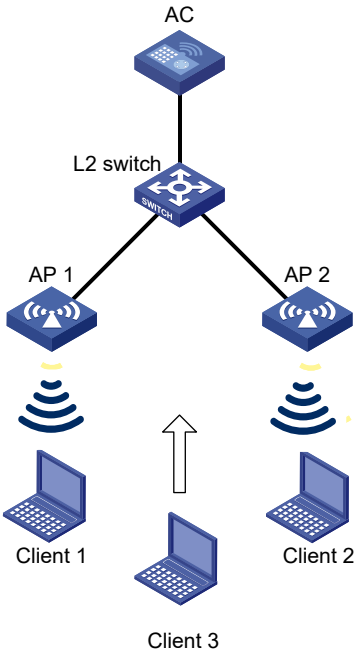


図 3-4 帯域幅モードロードバランス

3.1.4 ロードバランスタイプ

AC は以下のロードバランスタイプをサポートします。

- **無線ベース**－AC は、AP の隣接レポートに基づいたロードバランスに参加する AP を決定します。AP の隣接レポートは、AP に検出された各クライアントの MAC アドレスと RSSI 値を記録します。AC は、以下の条件のいずれかが満たされたときに、AP がロードバランスに参加すると決定します。
  - クライアントが AP とのアソシエーションを要求し、クライアントの RSSI が RSSI しきい値より低いと AP が検出した場合。
  - クライアントの RSSI が RSSI しきい値に達するが、クライアントは AP とのアソシエーションを要求しないと AP が検出した場合。

3.2 設定作業リスト

作業リスト	補足
（必須設定項目） WLANロードバランスの有効化	—
（必須設定項目） ロードバランスモードの設定	—
（オプション設定項目） ロードバランスパラメータの設定	—
（オプション設定項目） WLANロードバランスに対するSNMP通知の有効化	—

3.3 WLANロードバランスの設定

3.3.1 制限とガイドライン

クライアントが WLAN へのアクセスを要求すると、システムは同じ AC によって管理され、クライアントが検出できる AP 間でのみロードバランシングを実行します。

3.3.2 WLAN ロードバランスの有効化

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． WLAN ロードバランスを有効にする	**wlan load-balance enable**	デフォルト：無効

3.3.3 ロードバランスモードの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． ロードバランスモードを設定にする	• セッションモードロードバランスを設定する：**wlan load-balance mode session** *value* [**gap** *gap-value*] • トラフィックモードロードバランスを設定する：**wlan load-balance mode traffic** *value* [**gap** *gap-value*] • 帯域幅モードロードバランスを設定する：**wlan load-balance mode bandwidth** *value* [**gap** *gap-value*]	デフォルト：セッションモードロードバランスが使用されます。

3.3.4 ロードバランスパラメータの設定

以下のパラメータはロードバランスの計算に影響を与えます。

- **ロードバランス RSSI しきい値**ークライアントの RSSI が、指定した RSSI しきい値より低いと AP が検出した場合、AP は以下のいずれかの操作を実行します。
  - □ 複数の AP がクライアントを検出できる場合、AP はクライアントがアソシエーションを要求したときのみロードバランスに参加します。
  - □ 単独の AP のみがクライアントを検出できる場合、クライアントが AP と関連付く機会をよりもてるように拒絶最大数を 1 まで小さくします。

- **アソシエーション要求に対する拒絶最大数**－AP がクライアントを拒否する回数が、指定した拒絶最大数に達する場合、AP はクライアントにアソシエーション要求を承認します。

ロードバランスパラメータの設定手順は以下のとおりです。

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． RSSI しきい値を設定する	**wlan load-balance rssi-threshold** *rssi-threshold*	デフォルト： 25
3． アソシエーション要求に対する拒絶最大数を設定する	**wlan load-balance access-denial** *access-denial*	デフォルト：10

3.4 WLANロードバランスに対するSNMP通知の有効化

NMS に WLAN ロードバランスの重要なイベントを報告するために、SNMP 通知を WLAN ロードバランスに対して有効にします。WLAN ロードバランスイベント通知が正確に送信されるためには、“ネットワーク管理とモニタリングコンフィグレーションガイド”に記述されるように、SNMP の設定もしなければなりません。

SNMP 通知を WLAN ロードバランスに対して有効にする手順は以下のとおりです。

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． WLAN ロードバランスに対して SNMP 通知を有効にする	**snmp-agent trap enable wlan load-balance**	デフォルト：無効

3.5 WLANロードバランスの表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
ロードバランスグループ情報を表示する	**display wlan load-balance group** { *group-id* | **all** }
サービステンプレートにバインドされている無線のロードバランス情報を表示する	**display wlan load-balance status service-template** *template-name* { **client** *mac-address* | **group** *group-id* }

3.6 無線ベースWLANロードバランスの設定例

3.6.1 セッションモードロードバランスの設定

I. ネットワーク要件

図 3-5 に示すように、AP 1 と AP 2 は AC により管理され、クライアントは AP を検出できます。

以下の条件が満たされたとき、AC が AP 1 と AP 2 上でセッションモードロードバランスを実行するように設定します。

- 1 つの AP 上のセッション数が 3 に達する場合。
- AP 間のセッションギャップが 2 に達する場合。

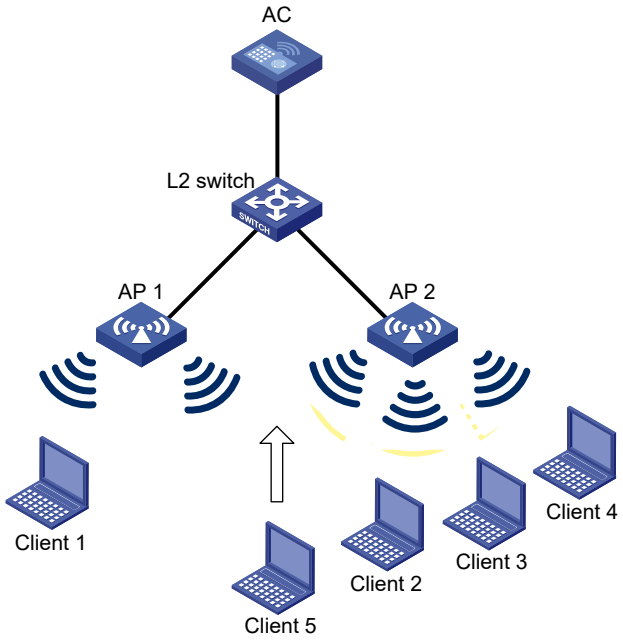


図 3-5 ネットワーク図

II. 設定手順

サービステンプレート 1 を作成し、SSID を session-balance に設定します。

```
<AC> system-view
[AC] wlan service-template 1
[AC-wlan-st-1] ssid session-balance
[AC-wlan-st-1] service-template enable
[AC-wlan-st-1] quit
```

AP template ap1 を作成し、AP モデル名とシリアル ID を指定します。

```
[AC] wlan ap ap1 model QX-W1020
[AC-wlan-ap-ap1] serial-id 210235A29G007C000020
```

サービステンプレート 1 を AP 1 の radio 2 に設定します。

```
[AC-wlan-ap-ap1] radio 2
[AC-wlan-ap-ap1-radio-2] service-template 1
[AC-wlan-ap-ap1-radio-2] radio enable
[AC-wlan-ap-ap2-radio-2] quit
[AC-wlan-ap-ap2] quit
```

AP template ap2 を作成し、AP モデル名とシリアル ID を指定します。

```
[AC] wlan ap ap2 model QX-W1020
[AC-wlan-ap-ap2] serial-id 210235A29G007C000021
```

サービステンプレート 1 を AP 2 の radio 2 に設定します。

```
[AC-wlan-ap-ap2] radio 2
[AC-wlan-ap-ap2-radio-2] service-template 1
[AC-wlan-ap-ap2-radio-2] radio enable
[AC-wlan-ap-ap2-radio-2] quit
[AC-wlan-ap-ap2] quit
```

ロードバランスモードをセッションモードに設定し、セッションしきい値とセッションギャップしきい値をそれぞれ 3 と 2 に設定します。

```
[AC] wlan load-balance mode session 3 gap 2
```

WLAN ロードバランスを有効にします。

```
[AC] wlan load-balance enable
```

III. 設定の確認

以下の条件が満たされるとき、AC が AP 1 と AP 2 に対してセッションモードロードバランスを実行することを確認します。

- 1 つの AP 上でのセッション数が 3 に達する場合。
- AP 間のセッションギャップが 2 に達する場合。（詳細は省略します。）

display wlan client コマンドを使用し、AP 1 と AP 2 がロードバランスされるか確認します。（詳細は省略します。）

3.6.2 トラフィックモードロードバランスの設定

I. ネットワーク要件

図 3-6 に示すように、AP 1 と AP 2 は AC により管理され、クライアントは AP を検出できます。各 AP に対する最大帯域幅は 150Mbps です。

以下の条件が満たされたとき、AC が AP 1 と AP 2 上でトラフィックモードロードバランスを実行するように設定します。

- 1 つの AP のトラフィックが 30Mbps（最大帯域幅の 20%）に達する場合。
- AP 間のトラフィックギャップが 15Mbps（最大帯域幅の 10%）に達する場合。

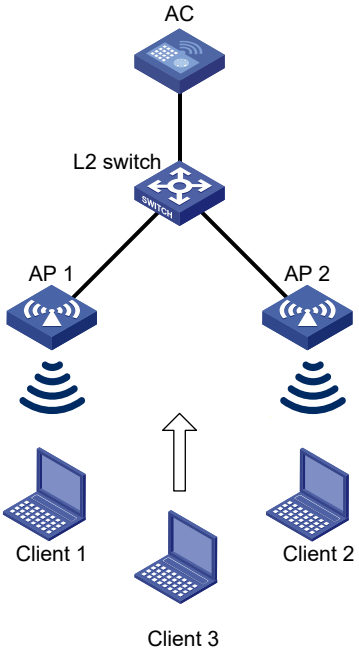


図 3-6 ネットワーク図

II. 設定手順

サービステンプレート 1 を作成し、SSID を traffic-balance に設定します。

```
<AC> system-view
[AC] wlan service-template 1
[AC-wlan-st-1] ssid traffic-balance
[AC-wlan-st-1] service-template enable
[AC-wlan-st-1] quit
```

AP template ap1 を作成し、AP モデル名とシリアル ID を指定します。

```
[AC] wlan ap ap1 model QX-W1020
[AC-wlan-ap-ap1] serial-id 210235A29G007C000020
```

サービステンプレート 1 を AP 1 の radio 2 に設定します。

```
[AC-wlan-ap-ap1] radio 2
[AC-wlan-ap-ap1-radio-2] service-template 1
[AC-wlan-ap-ap1-radio-2] radio enable
[AC-wlan-ap-ap1-radio-2] quit
[AC-wlan-ap-ap1] quit
```

AP template ap2 を作成し、AP モデル名とシリアル ID を指定します。

```
[AC] wlan ap ap2 model QX-W1020
[AC-wlan-ap-ap2] serial-id 210235A29G007C000021
```

サービステンプレート 1 を AP 2 の radio 2 に設定します。

```
[AC-wlan-ap-ap2] radio 2
[AC-wlan-ap-ap2-radio-2] service-template 1
[AC-wlan-ap-ap2-radio-2] radio enable
[AC-wlan-ap-ap2-radio-2] quit
[AC-wlan-ap-ap2] quit
```

ロードバランスモードをトラフィックモードに設定し、トラフィックしきい値とトラフィックギャップしきい値をそれぞれ 20%と 10%に設定します。

```
[AC] wlan load-balance mode traffic 20 gap 10
```

WLAN ロードバランスを有効にします。

```
[AC] wlan load-balance enable
```

III. 設定の確認

以下の条件が満たされるとき、AC が AP 1 と AP 2 に対してトラフィックモードロードバランスを実行することを確認します。

- 1 つの AP のトラフィックが 30Mbps に達する場合。
- AP 間のトラフィックギャップが 15Mbps に達する場合。（詳細は省略します。）

display wlan client コマンドを使用し、AP 1 と AP 2 がロードバランスされるか確認します。（詳細は省略します。）

3.6.3 帯域幅モードロードバランスの設定

I. ネットワーク要件

図 3-7 に示すように、AP 1 と AP 2 は AC により管理され、クライアントは AP を発見できます。

以下の条件が満たされたとき、AC が AP 1 と AP 2 上で帯域幅モードロードバランスを実行するように設定します。

- 1 つの AP の帯域幅が 12Mbps に達する場合。
- AP 間の帯域幅ギャップが 3Mbps に達する場合。

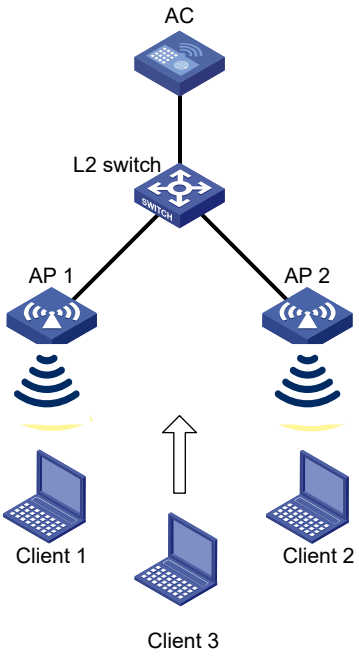


図 3-7 ネットワーク図

II. 設定手順

サービステンプレート 1 を作成し、SSID を bandwidth-balance に設定します。

```
<AC> system-view
[AC] wlan service-template 1
[AC-wlan-st-1] ssid bandwidth-balance
[AC-wlan-st-1] service-template enable
[AC-wlan-st-1] quit
```

AP template ap1 を作成し、AP モデル名とシリアル ID を指定します。

```
[AC] wlan ap ap1 model QX-W1020
[AC-wlan-ap-ap1] serial-id 210235A29G007C000020
```

サービステンプレート 1 を AP 1 の radio 2 に設定します。

```
[AC-wlan-ap-ap1] radio 2
[AC-wlan-ap-ap1-radio-2] service-template 1
[AC-wlan-ap-ap1-radio-2] radio enable
[AC-wlan-ap-ap1-radio-2] quit
```

```
[AC-wlan-ap-ap1] quit
```

AP template ap2 を作成し、AP モデル名とシリアル ID を指定します。

```
[AC] wlan ap ap2 model QX-W1020
[AC-wlan-ap-ap2] serial-id 210235A29G007C000021
```

サービステンプレート 1 を AP 2 の radio 2 に設定します。

```
[AC-wlan-ap-ap2] radio 2
[AC-wlan-ap-ap2-radio-2] service-template 1
[AC-wlan-ap-ap2-radio-2] radio enable
[AC-wlan-ap-ap2-radio-2] quit
[AC-wlan-ap-ap2] quit
```

ロードバランスモードを帯域幅モードに設定し、帯域幅しきい値と帯域幅ギャップしきい値をそれぞれ 12 Mbps と 3 Mbps に設定します。

```
[AC] wlan load-balance mode bandwidth 12 gap 3
```

WLAN ロードバランスを有効にします。

```
[AC] wlan load-balance enable
```

III. 設定の確認

以下の条件が満たされるとき、AC が AP 1 と AP 2 に対して帯域幅モードロードバランスを実行することを確認します。

- 1 つの AP の帯域幅が 12 Mbps に達する場合。
- AP 間の帯域幅ギャップが 3 Mbps に達する場合。（詳細は省略します。）

display wlan client コマンドを使用し、AP 1 と AP 2 がロードバランスされるか確認します。（詳細は省略します。）

3.7 ロードバランスグループベースWLANロードバランスの設定例

3.7.1 セッションモードロードバランスの設定

I. ネットワーク要件

図 3-8 に示すように、AP 1、AP 2、AP 3 は AC により管理され、クライアントは AP を発見できます。

以下の条件が満たされたとき、AC が AP 1 の radio 2 と AP 2 の radio 2 上でセッションモードロードバランスを実行するように設定します。

- 1 つの無線上のセッション数が 3 に達する場合。
- 無線間のセッションギャップが 2 に達する場合。

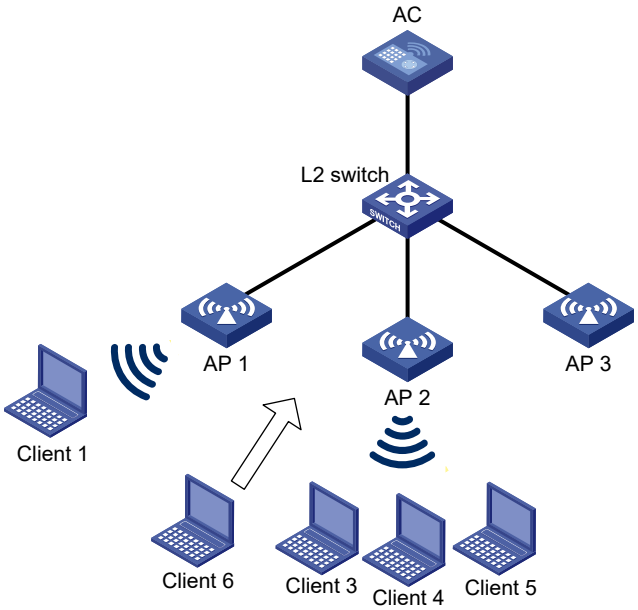


図 3-8 ネットワーク図

II. 設定手順

サービステンプレート 1 を作成し、SSID を session-balance に設定します。

```
<AC> system-view
[AC] wlan service-template 1
[AC-wlan-st-1] ssid session-balance
[AC-wlan-st-1] service-template enable
[AC-wlan-st-1] quit
```

AP template ap1 を作成し、AP モデル名とシリアル ID を指定します。

```
[AC] wlan ap ap1 model QX-W1020
[AC-wlan-ap-ap1] serial-id 210235A29G007C000020
```

サービステンプレート 1 を AP 1 の radio 2 に設定します。

```
[AC-wlan-ap-ap1] radio 2
[AC-wlan-ap-ap1-radio-2] service-template 1
[AC-wlan-ap-ap1-radio-2] radio enable
[AC-wlan-ap-ap1-radio-2] quit
[AC-wlan-ap-ap1] quit
```

AP template ap2 を作成し、model と serial ID を指定します。

```
[AC] wlan ap ap2 model QX-W1020
[AC-wlan-ap-ap2] serial-id 210235A29G007C000021
```

サービステンプレート 1 を AP 2 の radio 2 に設定します。

```
[AC-wlan-ap-ap2] radio 2
[AC-wlan-ap-ap2-radio-2] service-template 1
[AC-wlan-ap-ap2-radio-2] radio enable
[AC-wlan-ap-ap2-radio-2] quit
[AC-wlan-ap-ap2] quit
```

AP template ap3 を作成し、AP モデル名とシリアル ID を指定します。

```
[AC] wlan ap ap3 model QX-W1020
[AC-wlan-ap-ap3] serial-id 210235A29G007C000022
```

サービステンプレート 1 を AP 3 の radio 2 に設定します。

```
[AC-wlan-ap-ap3] radio 2
[AC-wlan-ap-ap3-radio-2] service-template 1
[AC-wlan-ap-ap3-radio-2] radio enable
[AC-wlan-ap-ap3-radio-2] quit
[AC-wlan-ap-ap3] quit
```

ロードバランスモードをセッションモードに設定し、セッションしきい値とセッションギャップしきい値をそれぞれ 3 と 2 に設定します。

```
[AC] wlan load-balance mode session 3 gap 2
```

WLAN ロードバランスを有効にします。

```
[AC] wlan load-balance enable
```

III. 設定の確認

以下の条件が満たされるとき、AC が AP 1 の radio 2 と AP 2 の radio 2 に対してセッションモードロードバランスを実行することを確認します。

- 1 つの無線上でのセッション数が 3 に達する場合。
- 無線間のセッションギャップが 2 に達する場合。（詳細は省略します。）

display wlan client コマンドを使用し、AP 1 と AP 2 がロードバランスされるか確認します。（詳細は省略します。）

3.7.2 トラフィックモードロードバランスの設定

I. ネットワーク要件

図 3-9 に示すように、AP 1、AP 2、AP 3 は AC により管理され、クライアントは AP を検出できます。

以下の条件が満たされたとき、AC が AP 1 の radio 2 と AP 2 の radio 2 上でトラフィックモードロードバランスを実行するように設定します。

- 1 つの無線のトラフィックが 30Mbps（最大帯域幅の 20%）に達する場合。
- 無線間のトラフィックギャップが 15Mbps（最大帯域幅の 10%）に達する場合。

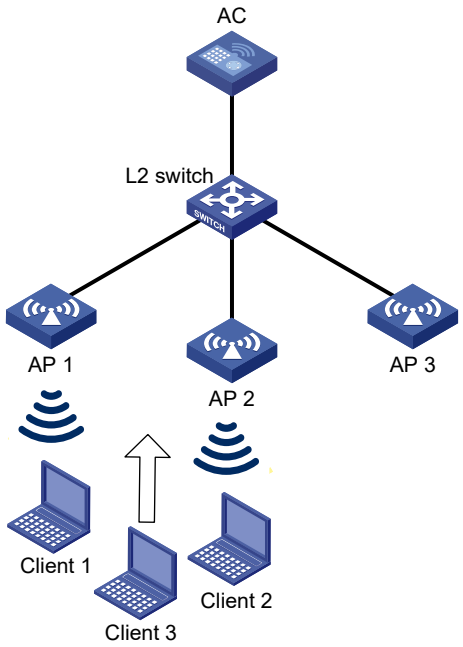


図 3-9 ネットワーク図

II. 設定手順

サービステンプレート 1 を作成し、SSID を traffic-balance に設定します。

```
<AC> system
[AC] wlan service-template 1
[AC-wlan-st-1] ssid traffic-balance
[AC-wlan-st-1] service-template enable
[AC-wlan-st-1] quit
```

AP template ap1 を作成し、AP モデル名とシリアル ID を指定します。

```
[AC] wlan ap ap1 model QX-W1020
[AC-wlan-ap-ap1] serial-id 210235A29G007C000020
```

サービステンプレート 1 を AP 1 の radio 2 に設定します。

```
[AC-wlan-ap-ap1] radio 2
[AC-wlan-ap-ap1-radio-2] service-template 1
[AC-wlan-ap-ap1-radio-2] radio enable
[AC-wlan-ap-ap1-radio-2] quit
```

```
[AC-wlan-ap-ap1] quit
```

AP template ap2 を作成し、model と serial ID を指定します。

```
[AC] wlan ap ap2 model QX-W1020
[AC-wlan-ap-ap2] serial-id 210235A29G007C000021
```

サービステンプレート 1 を AP 2 の radio 2 に設定します。

```
[AC-wlan-ap-ap2] radio 2
[AC-wlan-ap-ap2-radio-2] service-template 1
[AC-wlan-ap-ap2-radio-2] radio enable
[AC-wlan-ap-ap2-radio-2] quit
[AC-wlan-ap-ap2] quit
```

AP template ap3 を作成し、model と serial ID を指定します。

```
<AC> system-view
[AC] wlan ap ap3 model QX-W1020
[AC-wlan-ap-ap3] serial-id 210235A29G007C000022
```

サービステンプレート 1 を AP 3 の radio 2 に設定します。

```
[AC-wlan-ap-ap3] radio 2
[AC-wlan-ap-ap3-radio-2] service-template 1
[AC-wlan-ap-ap3-radio-2] radio enable
[AC-wlan-ap-ap3-radio-2] quit
[AC-wlan-ap-ap3] quit
```

#ロードバランスモードをトラフィックモードに設定し、トラフィックしきい値とトラフィックギャップしきい値をそれぞれ 20%と 10%に設定します。

```
[AC] wlan load-balance mode traffic 20 gap 10
```

WLAN ロードバランスを有効にします。

```
[AC] wlan load-balance enable
```

III. 設定の確認

#以下の条件が満たされるとき、AC が AP 1 の radio 2 と AP 2 の radio 2 に対してトラフィックモードロードバランスを実行することを確認します。

- 1 つの無線でのトラフィックが 30Mbps に達する場合。
- 無線間のトラフィックギャップが 15Mbps に達する場合。（詳細は省略します。）

display wlan client コマンドを使用し、AP 1 と AP 2 がロードバランスされるか確認します。（詳細は省略します。）

3.7.3 帯域幅モードロードバランスの設定

I. ネットワーク要件

図 3-10 に示すように、AP 1、AP 2、AP 3 は AC により管理され、クライアントは AP を発見できます。

以下の条件が満たされたとき、AC が AP 1 の radio 2 と AP 2 の radio 2 上で帯域幅モードロードバランスを実行するように設定します。

- 1 つの無線の帯域幅が 12Mbps に達する場合。
- 無線間の帯域幅ギャップが 3Mbps に達する場合。

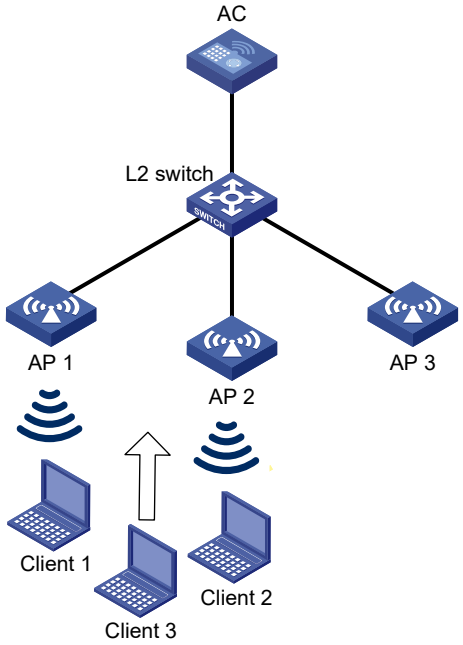


図 3-10 ネットワーク図

II. 設定手順

サービステンプレート 1 を作成し、SSID を bandwidth-balance に設定します。

```
<AC> system
[AC] wlan service-template 1
[AC-wlan-st-1] ssid bandwidth-balance
[AC-wlan-st-1] service-template enable
[AC-wlan-st-1] quit
```

AP template ap1 を作成し、AP モデル名とシリアル ID を指定します。

```
[AC] wlan ap ap1 model QX-W1020
[AC-wlan-ap-ap1] serial-id 210235A29G007C000020
```

サービステンプレート 1 を AP 1 の radio 2 に設定します。

```
[AC-wlan-ap-ap1] radio 2
[AC-wlan-ap-ap1-radio-2] service-template 1
[AC-wlan-ap-ap1-radio-2] radio enable
[AC-wlan-ap-ap1-radio-2] quit
[AC-wlan-ap-ap1] quit
```

AP template ap2 を作成し、model と serial ID を指定します。

```
[AC] wlan ap ap2 model QX-W1020
[AC-wlan-ap-ap2] serial-id 210235A29G007C000021
```

サービステンプレート 1 を AP 2 の radio 2 に設定します。

```
[AC-wlan-ap-ap2] radio 2
[AC-wlan-ap-ap2-radio-2] service-template 1
[AC-wlan-ap-ap2-radio-2] radio enable
[AC-wlan-ap-ap2-radio-2] quit
[AC-wlan-ap-ap2] quit
```

AP template ap3 を作成し、model と serial ID を指定します。

```
[AC] wlan ap ap3 model QX-W1020
[AC-wlan-ap-ap3] serial-id 210235A29G007C000022
```

サービステンプレート 1 を AP 3 の radio 2 に設定します。

```
[AC-wlan-ap-ap3] radio 2
[AC-wlan-ap-ap3-radio-2] service-template 1
[AC-wlan-ap-ap3-radio-2] radio enable
[AC-wlan-ap-ap3-radio-2] quit
[AC-wlan-ap-ap3] quit
```

ロードバランスモードを帯域幅モードに設定し、帯域幅しきい値と帯域幅ギャップしきい値をそれぞれ 12 Mbps と 3 Mbps に設定します。

```
[AC] wlan load-balance mode bandwidth 12 gap 3
```

WLAN ロードバランスを有効にします。

```
[AC] wlan load-balance enable
```

III. 設定の確認

#以下の条件が満たされるとき、AC が AP 1 の radio 2 と AP 2 の radio 2 に対して帯域幅モードロードバランスを実行することを確認します。

- 1 つの無線の帯域幅が 12 Mbps に達する場合。

- 無線間の帯域幅ギャップが 3 Mbps に達する場合。（詳細は省略します。）

display wlan client コマンドを使用し、AP 1 と AP 2 がロードバランスされるか確認します。（詳細は省略します。）

目次

このセクションのページは **9-x-x** です。

4 章 WLAN 無線リソースの計測の設定 4-1
4.1 概要 4-1
4.1.1 802.11k 計測 4-1
4.2 設定作業リスト 4-2
4.3 無線リソース計測の有効化 4-2
4.3.1 radio view での無線リソース計測の有効化 4-2
4.3.2 AP group view での無線リソース計測の有効化 4-2
4.4 計測期間と計測間隔の設定 4-3
4.4.1 radio view での計測期間と計測間隔の設定 4-3
4.4.2 AP group radio view での計測期間と計測間隔の設定 4-3
4.5 クライアント無線リソース計測性能に対するマッチモードの設定 4-3
4.5.1 radio view でのクライアント無線リソース計測性能に対するマッチモードの設定 4-4
4.5.2 AP group radio view でのクライアント無線リソース計測性能に対するマッチモードの設定 4-4
4.6 WLAN 無線リソース計測の表示と維持 4-4
4.7 無線リソース計測の設定例 4-5
4.7.1 ネットワーク要件 4-5
4.7.2 設定手順 4-5
4.7.3 設定の確認 4-6

4章 WLAN 無線リソースの計測の設定

4.1 概要

WLAN 無線リソース計測は、チャネル品質と無線性能を計測します。WLAN 無線リソース計測により、クライアントと AP は無線環境を学習可能になり、また、スペクトル、電力、帯域幅などの無線リソースをより効果的に使用可能になります。

4.1.1 802.11k 計測

802.11k 計測は、2.4GHz 帯と 5GHz 帯の両方のチャネルを計測します。表 4-1 は、802.11k 計測がサポートする計測の一覧です。

表 4-1 802.11k 計測

タイプ		内容
無線計測	Beacon	ビーコン、計測パイロットパケット、プローブ応答のRCPI（Received Channel Power Indicator）とRSNI（Received Signal to Noise Indicator）を計測します。
	Frame	伝送されたフレームの数と伝送されたフレームに対する平均RCPIを計測します。
	Station statistics	送受信されたフラグメント総計、マルチキャストフレーム総計、失敗総計、リトライ総計、ACK失敗総計を計測します。
	Transmit stream	特定の伝送ストリームのフレームを計測します。
	Channel load	チャネル使用を計測します。
	Location	要求者と要求されたものの相対的な位置を計測します。
	Noise histogram	異なるデシベル範囲での雑音分布を計測します。
Link measurement		リンク冗長性とクライアントに対する伝送電力を計測します。
Neighbor measurement		チャネルとネイバAPのBSSIDを計測します。

802.11k 計測は、以下の手順で作動します。

1) AP は、802.11k 計測要求を送信できるとクライアントに通知するために、ビーコン、プローブ応答、アソシエーション応答、または再アソシエーション応答内で無線計測フィールドを 1 に設定します。
これらの応答フレームは、AP がサポートする計測タイプのクライアントに通知するために、AP の計測性能も運びます。
AP は、クライアントがすばやく AP を検出できるように、計測パイロットフレームを定期的に送信します。計測パイロットフレームはビーコンよりも頻繁に送信され、運ぶ情報はより少ないです。
2) クライアントから計測要求を受信すると、AP は要求された計測を実行し、クライアントにレポートを送信します。
AP は、クライアントに定期的に計測要求を送信し、クライアントから計測報告を収集することもできます。

4.2 設定作業リスト

作業リスト
（必須設定項目）無線リソース計測の有効化
（オプション設定項目）計測期間と計測間隔の設定
（オプション設定項目） クライアント無線リソース計測性能に対するマッチモードの設定

4.3 無線リソース計測の有効化

4.3.1 radio view での無線リソース計測の有効化

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP view に移行する	**wlan ap** *ap-name* [**model** *model-name*]	—
3． radio view に移行する	**radio** *radio-id*	—
4． 計測タイプを有効にする	**measure** { **all** | **link** | **neighbor** | **radio** | **spectrum** | **tpc** } { **enable** | **disable** }	デフォルト：AP group view内の設定が使用されます。
5． 無線リソース測定を有効にする	**resource-measure enable**	デフォルト：AP group view内の設定が使用されます。
6． スペクトル管理を有効にする	**spectrum-management enable**	デフォルト：AP group view内の設定が使用されます。

4.3.2 AP group view での無線リソース計測の有効化

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP group view に移行する	**wlan ap-group** *group-name*	—
3． AP model view に移行する	**ap-model** *ap-model*	—
4． AP group radio view に移行する	**radio** *radio-id*	—
5． 計測タイプを有効にする	**measure** { **all** | **link** | neighbor | **radio** | **spectrum** | **tpc** } { **enable** | **disable** }	デフォルト：無効 **spectrum**、**tpc**パラメータは5GHz帯のみサポートします。
6． 無線リソース測定を有効にする	**resource-measure enable**	デフォルト：無効 リンク、ネイバ、または無線測定を有効にする場合は、無線リソース測定を有効にする必要があります。

操作	コマンド	補足
7. スペクトル管理を有効にする	**spectrum-management enable**	デフォルト：無効 スペクトルまたはTPC測定は、スペクトル管理を有効にした後でのみ有効になります。

4.4 計測期間と計測間隔の設定

無線リソース計測が AP に対して有効なとき、AP は計測期間の情報を運ぶ計測要求を、指定された間隔でクライアントに送信します。

4.4.1 radio view での計測期間と計測間隔の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP view に移行する	**wlan ap** *ap-name* [**model** *model-name*]	—
3. radio view に移行する	**radio** *radio-id*	—
4. 計測期間を設定する	**measure-duration** *time*	デフォルト：AP group view内の設定が使用されます。
5. 計測間隔を設定する	**measure-interval** *value*	デフォルト：AP group view内の設定が使用されます。

4.4.2 AP group radio view での計測期間と計測間隔の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP group view に移行する	**wlan ap-group** *group-name*	—
3. AP model view に移行する	**ap-model** *ap-model*	—
4. AP group radio view に移行する	**radio** *radio-id*	—
5. 計測期間を設定する	**measure-duration** *time*	デフォルト： 500TU
6. 計測間隔を設定する	**measure-interval** *value*	デフォルト：30秒

4.5 クライアント無線リソース計測性能に対するマッチモードの設定

本機能により、クライアントは事前に定義されたマッチ基準に基づいて AP と関連付けることができます。無線リソース計測性能は、AP とクライアントにサポートされた無線リ

ソース計測タイプに言及します。装置は、クライアントの無線リソース計測性能に対して以下のマッチモードをサポートします。

- **ALL**－クライアントは、すべての無線リソース計測性能が AP の無線リソース計測性能と一致する場合に限り、AP とのアソシエーションが許可されます。
- **None**－クライアントの無線リソース計測性能はチェックされません。
- **Partial**－クライアントは、無線リソース計測性能の 1 つが AP の任意の無線リソース計測性能と一致する場合に限り、AP とのアソシエーションが許可されます。

4.5.1 radio view でのクライアント無線リソース計測性能に対するマッチモードの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP view に移行する	**wlan ap** *ap-name* [**model** *model-name*]	—
3. radio view に移行する	**radio** *radio-id*	—
4. クライアントの無線リソース計測性能に対してマッチモードを設定する	**rm-capability mode** { **all** | **none** | **partial** }	デフォルト：AP group view内の設定が使用されます。

4.5.2 AP group radio view でのクライアント無線リソース計測性能に対するマッチモードの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP group view に移行する	**wlan ap-group** *group-name*	—
3. AP model view に移行する	**ap-model** *ap-model*	—
4. AP group radio view に移行する	**radio** *radio-id*	—
5. クライアントの無線リソース計測性能に対してマッチモードを設定する	**rm-capability mode** { **all** | **none** | **partial** }	デフォルト：none

4.6 WLAN無線リソース計測の表示と維持

すべての view で **display** コマンドを実行します。

操作	コマンド
クライアント計測報告を表示する	**display wlan measure-report ap** *ap-name* **radio** *radio-id* [**client mac-address** *mac-address*]

4.7 無線リソース計測の設定例

4.7.1 ネットワーク要件

図 4-1 に示すように、以下の条件を満たすように無線リソース計測を設定します。

- クライアントは、すべての無線リソース計測性能が AP の無線リソース計測性能と一致したときのみオンラインになります。
- クライアントはすべてのタイプの計測を実行できます。

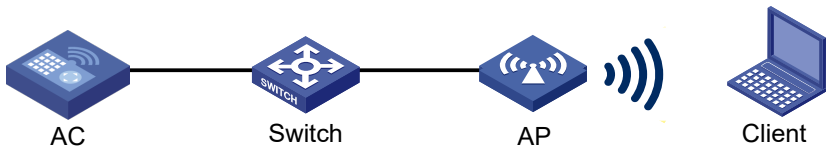


図 4-1 ネットワーク図

4.7.2 設定手順

サービステンプレート 1 を作成します。

```
<AC> system-view
[AC] wlan service-template 1
```

SSID resource-measure を設定し、サービステンプレート 1 を有効にします。

```
[AC-wlan-st-1] ssid resource-measure
[AC-wlan-st-1] service-template enable
[AC-wlan-st-1] quit
```

手動 AP ap1 を作成し、AP モデル名とシリアル ID を指定します。

```
[AC] wlan ap ap1 model QX-W1020
[AC-wlan-ap-ap1] serial-id 219801A0CNC138011454
```

radio 1 の radio view に移行します.

```
[AC-wlan-ap-ap1] radio 1
```

無線リソース計測を有効にします。

```
[AC-wlan-ap-ap1-radio-1] resource-measure enable
```

すべての計測機能を有効にします。

```
[AC-wlan-ap-ap1-radio-1] measure all enable
```

クライアントの無線リソース計測性能に対するマッチモードを All に設定します。

```
[AC-wlan-ap-ap1-radio-1] rm-capability mode all
```

radio 1 にサービステンプレートを設定し、無線を有効にします。

```
[AC-wlan-ap-ap1-radio-1] service-template 1
[AC-wlan-ap-ap1-radio-1] radio enable
[AC-wlan-ap-ap1-radio-1] quit
[AC-wlan-ap-ap1] quit
```

4.7.3 設定の確認

クライアントがオンラインになることを検証します。

```
[AC] display wlan client
Total number of clients: 1

MAC address       Username             AP name  IP address          VLAN ID
00ee-bd44-557f      N/A                AP1      1.1.1.1             1
```

#クライアントからの計測報告を表示します。

```
[AC] display wlan measure-report ap ap1 radio 1
Total number of clients: 1

Client MAC address                              : 00ee-bd44-557f
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
```

目次

このセクションのページは**9-x-x** です。

5章 バンドナビゲーションの設定 5-1
5.1 概要 5-1
5.2 設定作業リスト 5-1
5.3 設定必須要件 5-1
5.4 バンドナビゲーションの設定 5-2
5.4.1 グローバルでのバンドナビゲーションの有効化 5-2
5.4.2 APに対するバンドナビゲーションの有効化 5-2
5.4.3 バンドナビゲーションに対するロードバランスの設定 5-2
5.4.4 バンドナビゲーションパラメータの設定 5-3
5.5 バンドナビゲーションの設定例 5-3

5章 バンドナビゲーションの設定

5.1 概要

AP は、バンドナビゲーションを行うことで、デュアルバンド（2.4GHz と 5GHz）クライアントの優先的な 5GHz 無線使用を可能にします。これにより、混雑しやすい 2.4GHz バンドでの無線負荷を分散でき、ネットワーク性能が向上します。

図 5-1に示すように、バンドナビゲーションは WLAN 内で有効化されます。Client 1 は 5GHz 無線に関連づけられ、Client 2 は 2.4GHz 無線に関連づけられます。デュアルバンドクライアントの Client 3 が 2.4GHz 無線への関連づけを要求したとき、AP は Client 3 を拒否し、5GHz 無線を使用するように指示します。

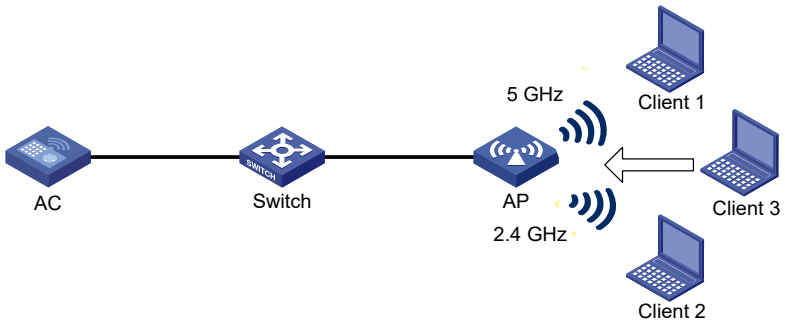


図 5-1 バンドナビゲーション

5.2 設定作業リスト

作業リスト
バンドナビゲーションの設定 • （必須設定項目）グローバルでのバンドナビゲーションの有効化 • （必須設定項目）APに対するバンドナビゲーションの有効化 • （オプション設定項目）バンドナビゲーションに対するロードバランスの設定 • （オプション設定項目）バンドナビゲーションパラメータの設定

5.3 設定必須要件

5GHz 無線と 2.4GHz 無線の両方が有効化され、無線が同じサービステンプレートに設定されていることを確認してください。

5.4 バンドナビゲーションの設定

5.4.1 グローバルでのバンドナビゲーションの有効化

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． バンドナビゲーションをグローバルに有効化する	**wlan band-navigation enable**	デフォルト：無効

5.4.2 AP に対するバンドナビゲーションの有効化

バンドナビゲーションは、グローバルおよび AP の両者に有効なときにのみ、AP に対して適用します。

I. AP に対するバンドナビゲーションの有効化

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP view に移行する	**wlan ap** *ap-name*	—
3． AP に対してバンドナビゲーションを有効にする	**band-navigation enable**	デフォルト：APはAP group viewの設定を使用します。

II. AP group に対するバンドナビゲーションの有効化

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP group view に移行する	**wlan ap-group** *group-name*	—
3． AP に対してバンドナビゲーションを有効にする	**band-navigation enable**	デフォルト：有効

5.4.3 バンドナビゲーションに対するロードバランスの設定

AP は、以下の条件が満たされるとき、クライアントの 5GHz の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 無線と、関連づけられたクライアント数が最小の無線とのクライアント数のギャップが、指定したしきい値に達した場合。

バンドナビゲーションに対するロードバランスの設定手順は以下のとおりです。

操作	コマンド	補足
1． system view に移行する	**system-view**	—

操作	コマンド	補足
2. バンドナビゲーションに対してロードバランスを設定する	**wlan band-navigation balance session** *session* [**gap** *gap*]	デフォルト：無効

5.4.4 バンドナビゲーションパラメータの設定

以下のパラメータはバンドナビゲーションに影響を与えます。

- **5GHz アソシエーション要求に対する拒絶の最大数**－5GHz 無線がクライアントを拒否する回数が、指定した最大数に達した場合、無線はクライアントのアソシエーション要求を承認します。
- **バンドナビゲーション RSSI しきい値**－クライアントは複数の無線に検出される可能性があります。クライアントの RSSI がバンドナビゲーション RSSI しきい値より小さい場合、5GHz 無線はクライアントのアソシエーション要求を拒否します。
- **クライアント情報エージングタイマ** AP は、クライアントからアソシエーション要求を受信すると、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終了する前に AP がクライアントからプローブ要求やアソシエーション要求を受信しない場合、AP はクライアントの情報を削除します。

クライアントのアソシエーションとシステムリソースの効率の両方を保証するために、適切なクライアント情報エージングタイマを設定してください。

バンドナビゲーションパラメータの設定手順は以下のとおりです。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. 5GHz アソシエーション要求に対する拒絶の最大数を設定する	**wlan band-navigation balance access-denial** *access-denial*	デフォルト：1
3. バンドナビゲーション RSSI しきい値を設定する	**wlan band-navigation rssi-threshold** *rssi-threshold*	デフォルト：15
4. クライアント情報エージングタイマを設定する	**wlan band-navigation aging-time** *aging-time*	デフォルト： 180秒

5.5 バンドナビゲーションの設定例

I. ネットワーク要件

図 5-2に示すように、5GHz 無線と 2.4GHz 無線の両方が AP 上で有効化されています。バンドナビゲーションを設定し、無線の負荷を分散させるためにとロードバランスを設定します。

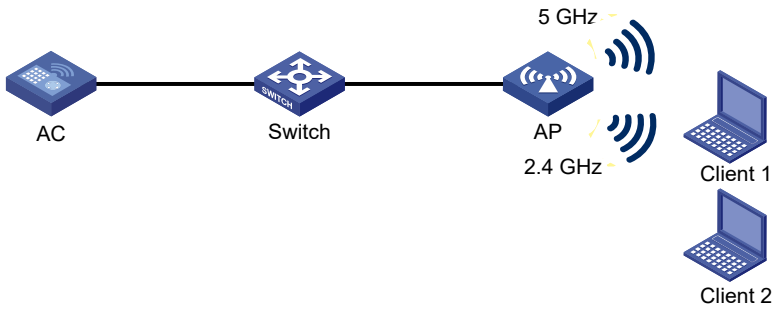


図 5-2 ネットワーク図

II. 設定手順

サービステンプレート 1 を作成し、SSID を band-navigation に設定します。

```
<AC> system-view
[AC] wlan service-template 1
[AC-wlan-st-1] ssid band-navigation
[AC-wlan-st-1] service-template enable
[AC-wlan-st-1] quit
```

AP template ap1 を作成し、AP モデル名とシリアル ID を指定します。

```
[AC] wlan ap ap1 model QX-W1020
[AC-wlan-ap-ap1] serial-id 210235A29G007C000020
```

radio 1 の radio view に移行し、radio 1 が 802.11n （5 GHz）モード内で作動するように設定します。

```
[AC-wlan-ap-ap1] radio 1
[AC-wlan-ap-ap1-radio-1] type dot11an
```

サービステンプレート 1 を AP 1 の radio 1 に設定し、radio 1 を有効にします。

```
[AC-wlan-ap-ap1-radio-1] service-template 1
[AC-wlan-ap-ap1-radio-1] radio enable
[AC-wlan-ap-ap1-radio-1] quit
```

radio 3 の radio view に移行し、radio 3 は 802.11n （2.4 GHz） モード内で作動するように設定します。

```
[AC-wlan-ap-ap1] radio 3
[AC-wlan-ap-ap1-radio-3] type dot11gn
```

サービステンプレート 1 を AP 1 の radio 3 に設定し、radio 3 を有効にします。

```
[AC-wlan-ap-ap1-radio-3] service-template 1
[AC-wlan-ap-ap1-radio-3] radio enable
```

```
[AC-wlan-ap-ap1-radio-3] quit
[AC-wlan-ap-ap1] quit
```

バンドナビゲーションをグローバルに有効化します。

```
[AC] wlan band-navigation enable
```

AP 1 に対してバンドナビゲーションを有効化します。

```
[AC] wlan ap ap1 model QX-W1020
[AC-wlan-ap-ap1] band-navigation enable
[AC-wlan-ap-ap1] quit
```

バンドナビゲーションに対してロードバランスを有効化し、クライアント数のしきい値とクライアント数のギャップしきい値をそれぞれ 5 と 2 に設定します。

```
[AC] wlan band-navigation balance session 5 gap 2
```

5GHz アソシエーション要求に対する拒絶の最大数を 3 に設定します。

```
[AC] wlan band-navigation balance access-denial 3
```

#バンドナビゲーション RSSI しきい値を 30 に設定します。

```
[AC] wlan band-navigation rssi-threshold 30
```

クライアント情報エージングタイマ 160 秒に設定します。

```
[AC] wlan band-navigation aging-time 160
```

III. 設定の確認

1) デュアルバンドクライアントが AP に関連づけを要求したときに、5GHz 無線に関連付くことを確認します。
2) 以下の条件を満たすとき、デュアルバンドクライアントが 2.4GHz 無線に関連付くことを確認します。

- 5GHz 無線上のクライアント数が 5 に達した場合。（詳細は省略します。）
- 5GHz 無線と 2.4GHz 無線とのクライアント数ギャップが 2 に達した場合。（詳細は省略します。）

目次

このセクションのページは**9-x-x** です。

6章 WLAN RRMの設定 6-1
6.1 概要 6-1
6.1.1 動的周波数選択（DFS） 6-1
6.1.2 送信電力制御（TPC） 6-2
6.1.3 帯域幅自動調整 6-3
6.2 制約事項とガイドライン:WLAN RRM 設定 6-3
6.3 WLAN RRM設定作業リスト 6-4
6.4 DFSの設定 6-4
6.4.1 設定の制限とガイドライン 6-4
6.4.2 DFS設定作業リスト 6-4
6.4.3 auto-DFSの有効化 6-5
6.4.4 定期auto-DFSの設定 6-6
6.4.5 スケジュールauto-DFSの実行 6-6
6.4.6 オンデマンドDFSの設定 6-8
6.4.7 DFSトリガーパラメータの設定 6-9
6.4.8 RRM抑制グループの設定 6-10
6.5 TPCの設定 6-10
6.5.1 TPC設定作業リスト 6-11
6.5.2 設定の制限とガイドライン 6-11
6.5.3 auto-TPCの有効化 6-11
6.5.4 オンデマンドTPCの実行 6-11
6.5.5 死角検出の設定 6-12
6.5.6 auto-TPCの電力キャリブレーション間隔の設定 6-14
6.5.7 TPCモードの設定 6-14
6.5.8 TPCトリガーパラメータの設定 6-15
6.5.9 最小送信電力の設定 6-16
6.5.10 最大送信電力の設定 6-17
6.5.11 RRM抑制グループの設定 6-18
6.6 帯域幅自動調整の設定 6-18
6.6.1 帯域幅自動調整の設定作業リスト 6-18
6.6.2 帯域幅自動調整の有効化 6-18
6.6.3 帯域幅自動調整間隔の設定 6-19
6.7 無線ベースラインの設定 6-20
6.8 無線スキャニングの有効化 6-20
6.9 WLAN RRMのSNMP通知の有効化 6-21
6.10 2.4GHzの無線チャネル最適化の設定 6-22
6.10.1 設定の制限とガイドライン 6-22
6.10.2 2.4GHzの無線チャネル最適化の設定 6-22
6.11 高密度シナリオでシャットダウンできるAPの除外 6-24
6.12 WLAN RRMの表示および管理 6-24
6.13 WLAN RRMの設定例 6-25
6.13.1 定期auto-DFSの設定例 6-25
6.13.2 スケジュールauto-DFSの設定例 6-26
6.13.3 定期TPCの設定例 6-28

6.13.4 帯域幅自動調整の設定例..... 6-30

6章 WLAN RRM の設定

6.1 概要

WLAN RRM（Radio Resource Management）は、インテリジェントで拡張性のある無線管理機能を提供します。RRM により、AC は関連する無線を監視し、無線リソースの監視、動的周波数選択（DFS）、送信電力制御（TPC）を実行できます。これにより、WLAN が環境変化に適応し、最適な無線リソース状態を維持することができます。

6.1.1 動的周波数選択（DFS）

同じチャネル上の 2 つの隣接する無線が信号の衝突を引き起こしたり、レーダー信号や電子レンジなどの他の無線発信源が無線の動作を妨害する可能性があります。DFS はこれらの問題を解決することができます。

DFS を使用することで、AC は同一チャネルの干渉および他の無線発信源からの干渉を回避するために、リアルタイムで各無線に最適なチャネルを選択します。

DFS を決定する要因は以下の通りです。

- **エラーコード等級**－物理層エラーコード等級および CRC エラーです。
- **干渉**－すべての無線信号が無線サービスに及ぼす影響です。
- **干渉状態**－DFS は、チャネル使用率のしきい値と干渉率のしきい値の両方に到達または超過した場合にトリガーされますが、受信したサービス トラフィックはサービス トラフィックのしきい値に到達できません。
  - **チャネル使用率しきい値**－パケットの送受信に使用されるチャネルリソースの割合。
  - **干渉率しきい値**－使用されるチャネルリソースの合計に対する干渉によって使用されるチャネルリソースの割合。
  - **サービストラフィックしきい値**－合計受信トラフィックに対する受信サービストラフィックの割合。
- **再送信**－AC からの ACK メッセージを受信しない場合の無線によるデータ再送信です。
- **ノイズしきい値**－現在動作しているチャネルで AC によって検出されたノイズ。

AC は、以下のプロセスを使用し新しい無線チャネルを選択します。

1) 現在のチャネルを検出し、DFS のいずれかのしきい値に達した場合に最適なチャネルを選択します。
2) 古いチャネルと新しいチャネルとの品質を比較します。新しいチャネルと古いチャネルとの間の品質ギャップが許容レベルを超えるまで、無線では新しいチャネルを使用しません。

図 6-1に DFS の例を示します。BSS1、BSS3、および BSS5 のチャネルの品質が DFS しきい値に達すると、AC はそれらについて新しいチャネルを選択します。これにより、ワイヤレスサービスの品質が保証されます。

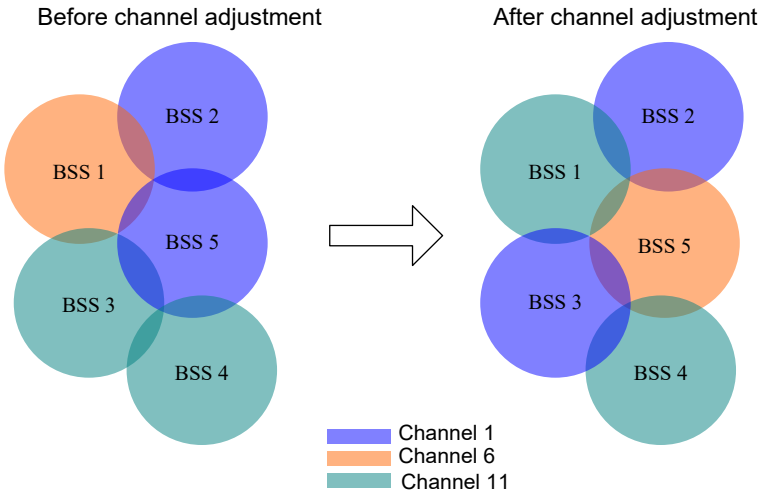


図 6-1 動的周波数選択（DFS）

6.1.2 送信電力制御（TPC）

TPC により、AC はリアルタイム WLAN 条件に基づいてアクセスポイントの送信電力を動的に制御できます。これは、無線間のチャネル干渉を回避しながら、要求された RF の適用範囲を達成することができます。

TPC を決定する要因は以下の通りです。

- **隣接番号しきい値**
- **電力検出用無線機**－電力検出を実行する近隣無線機
- **電力調整しきい値**

1) TPC が有効になると、無線機は送信電力を次のように調整します。
- 無線の隣接数がしきい値に達していない場合、無線は最大送信電力を使用します。
- 無線の隣接数がしきい値に達すると、2)のステップに移行します。

2) ほかの無線の隣接通知に記録されている無線の RSSI を降順でランク付けます。
3) 近接要因によって指定された RSSI を電力調整しきい値と比較し、以下のアクションの 1 つを実行します。
- RSSI がしきい値を超過した場合、無線の送信電力を減少させます。
- RSSI がしきい値を下回った場合、無線の送信電力を増加させます。

無線の TPC 計算に参加できる無線には、次のタイプがあります。

- **All-channel 無線**－無線を検出する管理可能な無線をすべて含めます。All-channel 無線に基づく TPC は、信号カバレッジをより適切に制御できます。
- **Overlapping-channel 無線**－無線の送信チャネルと重複するチャネルで無線を検出する管理可能な無線が含まれます。Overlapping-channel 無線に基づく TPC は、干渉を増やすことなく信号カバレッジを拡張できます。

図 6-2に示すように、各 AP は 1 つの無線のみが有効になっています。AP4 が加入すると、AP1 のデフォルトの最大近隣番号である 3 に達します。AP1 のすべての隣接者の中で、AP4 の信号強度が 3 番目であるため、AP4 が電力検出用 AP になります。AP1 の電力がデフォルト電力調整しきい値よりも低いことを AP4 が検出すると、AP1 はその送信電力を増加させます。AP1 の電力がデフォルト電力調整しきい値より高いことを AP4 が検出すると、AP1 は送信電力を減少させます。

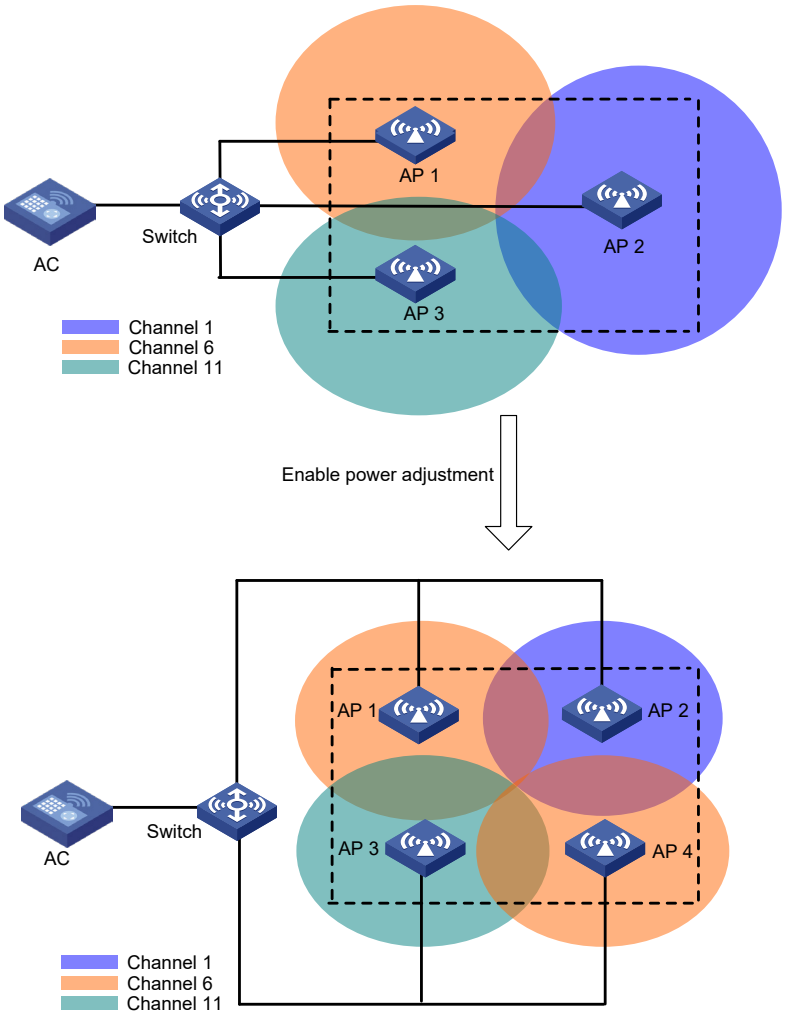


図 6-2 送信電力制御

6.1.3 帯域幅自動調整

802.11 n および 802.11 ac では、隣接するチャネルを組み合わせてデータ伝送速度を向上させることができます。ただし、この方法では、信号干渉が発生しやすいため、データ伝送の安定性が低下する可能性があります。

自動帯域幅調整により、AC は自動帯域幅調整間隔に達したときにチャネル品質検出を開始し、帯域幅調整を行うかどうかを判断できます。周辺 AP の数が多い場合は干渉を減らすために無線の帯域幅を減らし、数が少ない場合は伝送レートを増やすために帯域幅を増やします。

6.2 制約事項とガイドライン:WLAN RRM 設定

次の方法を使用して AP を設定できます。

- AP view で 1 つずつ AP 設定をする。

- AP group view で AP グループを作成して、AP を割当てる。
- グローバル view ですべての AP を設定する。

これらの view で同じパラメータに対して行った変更は、AP view→AP group view→グローバル view の降順で有効になります。

6.3 WLAN RRM設定作業リスト

作業リスト
DFSの設定
TPCの設定
帯域幅自動調整の設定
無線ベースラインの設定
無線スキャニングの有効化
WLAN RRMのSNMP通知の有効化

6.4 DFSの設定

AC は以下の DFS 方式をサポートします。

- **定期 auto-DFS**－AC は自動的にチャネルキャリブレーション間隔で無線の DFS を実行します。
- **スケジュール auto-DFS**－AC は時間範囲の指定した時間で DFS を実行します。干渉が大きい時、動作中の無線サービスへの影響を避ける場合、この方式を使用します。
- **オンデマンド DFS**－AC はチャネルキャリブレーション間隔時間を待った後、すべての無線の DFS を実行します。AC で無線の DFS を実行する際に、この方式を行う必要があります。

6.4.1 設定の制限とガイドライン

DFS を設定する際は、次の制限とガイドラインに従ってください。

DFS を動作させるには、無線のチャネルを自動で選択し、**channel auto unlock** コマンドを使用して、チャネルのロックを解除してください。

6.4.2 DFS 設定作業リスト

作業リスト
1. auto-DFSの有効化
2.必要に応じて次のタスクを選択します。 ・定期auto-DFSの設定 ・スケジュールauto-DFSの実行 ※定期auto-DFSの設定と、スケジュールauto-DFSの実行を同時に設定することはできません。
3. （オプション設定項目）オンデマンドDFSの設定
4. （オプション設定項目）DFSトリガーパラメータの設定

作業リスト
5.（オプション設定項目）RRM抑制グループの設定

6.4.3 auto-DFS の有効化

定期的 auto-DFS またはスケジュール auto-DFS を使用するには、auto-DFS 機能を有効にする必要があります。

RRM view、AP group の RRM view、またはグローバル設定 view で auto-DFS を有効にできます。RRM view、AP group の RRM view、グローバル設定 view での設定の優先順位は降順です。

I. グローバル設定 view での設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. グローバル設定 view に移行する	**wlan global-configuration**	—
3. auto-DFS を有効にする	**calibrate-channel self-decisive enable** { **2.4g** | **5g** | **6g** | **all** }	デフォルト：無効 **6g**パラメータはソフトウェアバージョン9.4.09を含む以降のソフトウェアでサポートです。

II. RRM view での設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP を作成し、AP view へ移行する	**wlan ap** *ap-name*	—
3. radio view に移行する	**radio** *radio-id*	—
4. RRM view に移行する	**rrm**	—
5. auto-DFS を有効にする	**calibrate-channel self-decisive enable**	デフォルト：AP group viewの設定が使用されます。

III. AP group の RRM view での設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP group view に移行する	**wlan ap-group** *group-name*	—
3. AP model view に移行する	**ap-model** *model-name*	—
4. radio view に移行する	**radio** *radio-id*	—
5. RRM view に移行する	**rrm**	—
6. auto-DFS を有効にする	**calibrate-channel self-decisive enable**	デフォルト：無効 AP group viewで設定されていない場合、APはグローバル設定viewの設定を使用します。

6.4.4 定期 auto-DFS の設定

I. RRM view での auto-DFS の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． （オプション設定項目）チャネルキャリブレーションを設定する	**wlan rrm calibration-channel interval** *minutes*	デフォルト： 23分
3． AP を作成し、AP view へ移行する	**wlan ap** *ap-name* [**model** *model-name*]	—
4． radio view に移行する	**radio** *radio-id*	—
5． RRM view に移行する	**rrm**	—
6． 定期的に auto-DFS を実行するように設定する	**calibrate-channel mode periodic**	デフォルト：AP group viewの設定が使用されます。

II. AP group RRM view での auto-DFS の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． （オプション設定項目）チャネルキャリブレーション間隔を設定する	**wlan rrm calibration-channel interval** *minutes*	デフォルト： 23分
3． AP group view に移行する	**wlan ap-group** *group-name*	—
4． AP model view に移行する	**ap-model** *model-name*	—
5． radio view に移行する	**radio** *radio-id*	—
6． RRM view に移行する	**rrm**	—
7． 定期的に auto-DFS を実行するように設定する	**calibrate-channel mode periodic**	デフォルト：有効

6.4.5 スケジュール auto-DFS の実行

スケジュール auto-DFS を設定する場合、チャネルレポート、隣接レポートを生成するため統計情報を取得するタイムレンジを設定する必要があります。

I. RRM view でのスケジュール auto-DFS の実行方法

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． タイムレンジを設定する	**time-range** *time-range-name* { *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
3． スケジュール自動実行機能の job を作成する	**scheduler job** *job-name*	デフォルト：設定なし

操作	コマンド	補足
4. jobにコマンドを割り当てる	**command 1 system-view** **command 2 wlan ap** *ap-name* [**model** *model-name*] **command 3 radio** *radio-id* **command 4 rrm** **command 5 calibrate-channel pronto**	デフォルト：設定なし
5. system viewに戻る	**quit**	ー
6. 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に移行する	**scheduler schedule** *schedule-name*	デフォルト：設定なし
7. スケジュールにjobを割り当てる	**job** *job-name*	デフォルト：設定なし
8. スケジュールにユーザロールを割り当てる	**user-role** *role-name*	デフォルト：スケジュールの作成者がスケジュールに割り当てられています。
9. 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する	**time at** *time date*	いずれかの1つを設定します。 デフォルト：設定なし
10. 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する	**time once at** *time* [**month-date** *month-day* | **week-day** *week-day*&<1-7>]	
11. スケジュール自動実行機能の実行日と時間を指定する	**time once delay** *time*	
12. system viewに戻る	**quit**	—
13. AP viewに移行する	**wlan ap** *ap-name*	—
14. radio viewに移行する	**radio** *radio-id*	—
15. RRM viewに移行する	**rrm**	—
16. auto-DFSを有効にする	**calibrate-channel self-decisive enable**	デフォルト：無効
17. スケジュールauto-DFSを設定する	**calibrate-channel mode scheduled**	デフォルト：AP group viewの設定が使用されます。

II. AP group RRM view でのスケジュール auto-DFS の実行方法

操作	コマンド	補足
1. system viewに移行する	**system-view**	—
2. タイムレンジを設定する	**time-range** *time-range-name* { *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
3. スケジュール自動実行機能のjobを作成する	**scheduler job** *job-name*	デフォルト：設定なし

操作	コマンド	補足
4. jobにコマンドを割り当てる	**command 1 system-view** **command 2 wlan ap** *ap-name* [**model** *model-name*] **command 3 radio** *radio-id* **command 4 rrm** **command 5 calibrate-channel pronto**	デフォルト：設定なし
5. system viewに戻る	**quit**	ー
6. 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に移行する	**scheduler schedule** *schedule-name*	デフォルト：設定なし
7. スケジュールにjobを割り当てる	**job** *job-name*	デフォルト：設定なし
8. スケジュールにユーザロールを割り当てる	**user-role** *role-name*	デフォルト：スケジュールの作成者がスケジュールに割り当てられています。
9. 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する	**time at** *time date*	いずれかの1つを設定します。 デフォルト：設定なし
10. 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する	**time once at** *time* [**month-date** *month-day* | **week-day** *week-day*&<1-7>]	
11. スケジュール自動実行機能の実行日と時間を指定する	**time once delay** *time*	
12. system viewに戻る	**quit**	—
13. AP group viewに移行する	**wlan ap-group** *group-name*	—
14. AP model viewに移行する	**ap-model** *model-name*	—
15. radio viewに移行する	**radio** *radio-id*	—
16. RRM viewに移行する	**rrm**	—
17. auto-DFSを有効にする	**calibrate-channel self-decisive enable**	デフォルト：無効
18. スケジュールauto-DFSを設定する	**calibrate-channel mode scheduled**	デフォルト：AP group viewの設定が使用されます。

6.4.6 オンデマンド DFS の設定

⚠ **注意：**
この機能はシステムリソースを消費します。慎重に使用してください。

I. すべての AP でオンデマンド DFS の実行方法

操作	コマンド	補足
1. system viewに移行する	**system-view**	—

操作	コマンド	補足
2. すべての AP の無線に対してワンタイム DFS を実行する	ソフトウェアバージョン 9.4.05のソフトウェア **wlan calibrate-channel pronto ap all** ソフトウェアバージョン 9.4.09を含む以降のソフトウェア **wlan calibrate-channel pronto ap** { **all** | **ap-group** *group-name* } { **2.4g** | **5g** | **6g** | **all** }	—
3. （オプション設定項目）キャリブレーション間隔を設定する	**wlan rrm calibration-channel interval** *minutes*	デフォルト： 23分

6.4.7 DFS トリガーパラメータの設定

注意：
正確なチャネル調整のため、DFS が有効になっているすべての無線で同じ DFS トリガーパラメータを設定することを推奨します。

I. RRM view での DFS トリガーパラメータの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP を作成し、AP view に移行する	**wlan ap** *ap-name* [**model** *model-name*]	—
3. radio view に移行する	**radio** *radio-id*	—
4. RRM view に移行する	**rrm**	—
5. CRC エラーしきい値を設定する	**crc-error-threshold** *percent*	デフォルト：AP group viewの設定が使用されます。
6. 干渉しきい値を設定する	**interference-threshold** *percent*	デフォルト：AP group viewの設定が使用されます。
7. 許容レベルを設定する	**tolerance-level** *percent*	デフォルト：AP group viewの設定が使用されます。

II. AP group RRM view での DFS トリガーパラメータの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP group view に移行する	**wlan ap-group** *group-name*	—
3. AP model view に移行する	**ap-model** *model-name*	—
4. radio view に移行する	**radio** *radio-id*	—
5. RRM view に移行する	**rrm**	—

操作	コマンド	補足
6． CRC エラーしきい値を設定する	**crc-error-threshold** *percent*	デフォルト : グローバル設定ビューの設定が使用されます。
7． 干渉しきい値を設定する	**interference-threshold** *percent*	デフォルト : グローバル設定ビューの設定が使用されます。
8． 許容レベルを設定する	**tolerance-level** *percent*	デフォルト : グローバル設定ビューの設定が使用されます。

6.4.8 RRM 抑制グループの設定

頻繁なチャネルまたは電力の調整が無線サービスに影響しないようにする場合、指定した無線を RRM 抑制グループに追加します。RRM 抑制グループ内の無線機に関する、チャネルまたは電力の変更が行われるたびに、チャネルまたは電力抑制タイマを開始します。チャネルまたは電力抑制タイマの時間が切れるまでは、無線のチャネルまたは電力は変更されません。

オンデマンド DFS を実行すると、チャネルタイマの時間切れに関係なく、キャリブレーション間隔が終了すると DFS が実行されます。

以下に RRM 抑制グループを設定する手順を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． RRM 抑制グループを作成し、RRM holddown group view に移行する	**wlan rrm-calibration-group** *group-id*	デフォルト：設定なし
3． （オプション設定項目）RRM 抑制グループの説明を設定する	**description** *text*	デフォルト：設定なし
4． 無線を RRM グループに追加する	**ap** *ap-name* **radio** *radio-id*	デフォルト：設定なし
5． （オプション設定項目）チャネル抑制タイマを設定する	**channel holddown-time** *minutes*	デフォルト： 720分

6.5 TPCの設定

AC は以下の TPC 方式をサポートします。

- **定期 auto-TPC**－AC は自動的に電力キャリブレーション間隔で無線の TPC を実行します。
- **オンデマンド TPC**－AC は電力キャリブレーション間隔時間を待った後、すべての無線の TPC を実行します。AC で無線の TPC を実行する際に、この方式を行う必要があります。

6.5.1 TPC 設定作業リスト

作業リスト
1. auto-TPCの有効化
2.オンデマンドTPCの実行
3. （オプション設定項目）auto-TPCの電力キャリブレーション間隔の設定
4. （オプション設定項目）TPCモードの設定
5. （オプション設定項目）TPCトリガーパラメータの設定
6. （オプション設定項目）最小送信電力の設定
7. （オプション設定項目）RRM抑制グループの設定

6.5.2 設定の制限とガイドライン

TPC を有効にする前に **power-lock enable** コマンドを設定して電力がロックされていないことを確認してください。

6.5.3 auto-TPC の有効化

RRM view、AP group の RRM view、またはグローバル設定 view で auto-TPC を有効にできます。RRM view、AP group の RRM view、グローバル設定 view での設定の優先順位は降順です。

I. グローバル設定 view での設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. グローバル設定 view に移行する	**wlan global-configuration**	—
3. auto-TPC を有効にする	**calibrate-power self-decisive enable** { **2.4g** | **5g** | **6g** | **all** }	デフォルト：無効 **6g**パラメータはソフトウェアバージョン9.4.09を含む以降のソフトウェアでサポートです。

6.5.4 オンデマンド TPC の実行

⚠ **注意**：
この機能はシステムリソースを消費します。慎重に使用してください。

I. オンデマンド TPC の設定方法

操作	コマンド	補足
1. system view に移行する	**system-view**	—

操作	コマンド	補足
2. すべての AP の無線に対してオンデマンド TPC を有効にする	ソフトウェアバージョン 9.4.05のソフトウェア **wlan calibrate-power pronto ap all** ソフトウェアバージョン 9.4.09を含む以降のソフトウェア **wlan calibrate-power pronto ap** { **all** | **ap-group** *group-name* } { **2.4g** | **5g** | **6g** | **all** }	—

6.5.5 死角検出の設定

🕮 **メモ：**

この機能はソフトウェアバージョン 9.4.09 を含む以降のソフトウェアからサポートしています。

この機能により、AC は無線信号カバレッジに死角 (または弱い信号領域) が存在するかどうかを判断できます。死角が検出された場合、AC は auto-TPC を実行するときに対応する AP の送信電力を増加させます。

AC は、次の条件を満たす場合に、無線のカバレッジに死角があると判断します。

- 無線に関連付けられた弱い信号クライアントの数が、しきい値に達するか、または超えている場合。
- 無線に関連付けられた弱い信号クライアントの割合がしきい値に達するか、それを超えている場合。

AC は、次の条件が満たされた場合に、クライアントが弱信号クライアントであると判断します。

- クライアントの弱信号パケット数がしきい値に達するか、またはしきい値を超えた場合。
- クライアントの弱信号パケットの割合がしきい値に達するか、それを超えた場合。

パケットの RSSI が RSSI しきい値より低い場合、そのパケットは弱い信号パケットと見なされます。

I. radio View での死角検出の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP を作成し、AP view に移行する	**wlan ap** *ap-name* [**model** *model-name*]	—
3. radio view に移行する	**radio** *radio-id*	—
4. 死角検出を有効にする	**calibrate-power coverage { disable | enable }**	デフォルト：AP group viewの設定が使用されます。

II. AP group radio View での死角検出の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP group view に移行する	**wlan ap-group** *group-name*	—
3． AP model view に移行する	**ap-model** *model-name*	—
4． radio view に移行する	**radio** *radio-id*	—
5． 死角検出を有効にする	**calibrate-power coverage { disable | enable }**	デフォルト： Global configuration viewの設定が使用されます。

III. global configuration View での死角検出の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． global configuration view に移行する	**wlan global-configuration**	—
3． 死角検出を有効にする	**calibrate-power coverage enable { 2.4g | 5g | 6g | all }**	デフォルト：無効 6gパラメータは、ソフトウェアバージョン7.2.75を含む以降のソフトウェアでサポートです。
4． （オプション設定項目）2.4GHz 無線の弱信号クライアント数のしきい値を設定する	**calibrate-power 2.4g coverage weak-signal-client threshold** *counts*	デフォルト：3
5． （オプション設定項目）5GHz 無線の弱信号クライアント数のしきい値を設定する	**calibrate-power 5g coverage weak-signal-client threshold** *counts*	デフォルト：3
6． （オプション設定項目）6GHz 無線の弱信号クライアント数のしきい値を設定する	**calibrate-power 6g coverage weak-signal-client threshold** *counts*	デフォルト：3 このコマンドは、ソフトウェアバージョン7.2.75を含む以降のソフトウェアでサポートです。
7． （オプション設定項目）2.4GHz 無線の弱信号クライアント割合のしきい値を設定する。	**calibrate-power 2.4g coverage weak-signal-client ratio** *percent*	デフォルト：25%
8． （オプション設定項目）5GHz 無線の弱信号クライアント割合のしきい値を設定する。	**calibrate-power 5g coverage weak-signal-client ratio** *percent*	デフォルト：25%
9． （オプション設定項目）6GHz 無線の弱信号クライアント割合のしきい値を設定する。	**calibrate-power 6g coverage weak-signal-client ratio** *percent*	デフォルト：25% このコマンドは、ソフトウェアバージョン7.2.75を含む以降のソフトウェアでサポートです。
10． （オプション設定項目）2.4GHz 無線の弱信号パケット数のしきい値を設定する	**calibrate-power 2.4g coverage weak-signal-packet threshold** *packets*	デフォルト：5

操作	コマンド	補足
11.（オプション設定項目）5GHz 無線の弱信号パケット数のしきい値を設定する	**calibrate-power 5g coverage weak-signal-packet threshold** *packets*	デフォルト：5
12.（オプション設定項目）6GHz 無線の弱信号パケット数のしきい値を設定する	**calibrate-power 6g coverage weak-signal-packet threshold** *packets*	デフォルト：5 このコマンドは、ソフトウェアバージョン7.2.75を含む以降のソフトウェアでサポートです。
13.（オプション設定項目）2.4GHz 無線の弱信号パケット割合のしきい値を設定する	**calibrate-power 2.4g coverage weak-signal-packet ratio** *percent*	デフォルト：20%
14.（オプション設定項目）5GHz 無線の弱信号パケット割合のしきい値を設定する	**calibrate-power 5g coverage weak-signal-packet ratio** *percent*	デフォルト：20%
15.（オプション設定項目）6GHz 無線の弱信号パケット割合のしきい値を設定する	**calibrate-power 6g coverage weak-signal-packet ratio** *percent*	デフォルト：20% このコマンドは、ソフトウェアバージョン7.2.75を含む以降のソフトウェアでサポートです。
16.（オプション設定項目）2.4GHz 無線の弱信号パケットと判別する RSSI しきい値を設定する	**calibrate-power 2.4g coverage rssi-threshold** *rssi*	デフォルト：20
17.（オプション設定項目）5GHz 無線の弱信号パケットと判別する RSSI しきい値を設定する	**calibrate-power 5g coverage rssi-threshold** *rssi*	デフォルト：25
18.（オプション設定項目）6GHz 無線の弱信号パケットと判別する RSSI しきい値を設定する	**calibrate-power 6g coverage rssi-threshold** *rssi*	デフォルト：25 このコマンドは、ソフトウェアバージョン7.2.75を含む以降のソフトウェアでサポートです。

6.5.6 auto-TPC の電力キャリブレーション間隔の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2.（オプション設定項目）電力キャリブレーション間隔を設定する	**wlan rrm calibration-power interval** *minutes*	デフォルト：11分

6.5.7 TPC モードの設定

AC は density、coverage、custom の TPC モードをサポートします。AP 間の影響を避ける場合、density モードを使用してください。信号の適用範囲を増加させる場合、coverage

モードを使用してください。density、coverage の 2 つのネットワーク要件に適合しない場合、電力調整の設定をカスタマイズさせるため、custom モードを使用してください。

density、coverage の 2 つのモードでは、電力調整の設定を変更することができません。

I. RRM view での TPC モードの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP view に移行する	**wlan ap** *ap-name*	—
3． radio view に移行する	**radio** *radio-id*	—
4． RRM view に移行する	**rrm**	—
5． TPC モードを設定する	**calibrate-power mode** { **coverage** | **custom** | **density** }	デフォルト：AP group viewの設定が使用されます。

II. AP group RRM view での TPC モードの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP group view に移行する	**wlan ap-group** *group-name*	—
3． AP model view に移行する	**ap-model** *model-name*	—
4． radio view に移行する	**radio** *radio-id*	—
5． RRM view に移行する	**rrm**	—
6． TPC モードを設定する	**calibrate-power mode** { **coverage** | **custom** | **density** }	デフォルト：custom

6.5.8 TPC トリガーパラメータの設定

⚠ **注意**：
正確な電力調整のために、TPC が有効になっているすべての無線で同じ TPC パラメータを設定することを推奨します。

近接ファクタ、電力調整しきい値によって無線の TPC が決まります。近接ファクタは検出された無線の品質を定義し、電力調整しきい値との比較に使用される RSSI のランク付けに使われます。必要に応じて近接ファクタを設定してください。

I. RRM view での TPC トリガーパラメータの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP view に移行する	**wlan ap** *ap-name*	—
3． radio view に移行する	**radio** *radio-id*	—
4． RRM view に移行する	**rrm**	—

操作	コマンド	補足
5. 隣接番号のしきい値を設定し、電力検出用無線機を指定する	**adjacency-factor** *neighbor*	デフォルト：AP group viewの設定が使用されます。
6. 電力調整のしきい値を設定する	**calibrate-power threshold** *value*	デフォルト：AP group RRM viewの設定が使用されます。

II. AP group RRM view での TPC トリガーパラメータの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP group view に移行する	**wlan ap-group** *group-name*	—
3. AP model view に移行する	**ap-model** *model-name*	—
4. radio view に移行する	**radio** *radio-id*	—
5. RRM view に移行する	**rrm**	—
6. 隣接番号のしきい値を設定し、電力検出用無線機を指定する	**adjacency-factor** *neighbor*	デフォルト: グローバル設定ビューの設定が使用されます。
7. 電力調整のしきい値を設定する	**calibrate-power threshold** *value*	デフォルト: グローバル設定ビューの設定が使用されます。

6.5.9 最小送信電力の設定

この機能を使用することにより、TPC が実行された後も無線機を検出することができます。

I. RRM view での最小送信電力の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP を作成し、AP view に移行する	**wlan ap** *ap-name*	—
3. radio view に移行する	**radio** *radio-id*	—
4. RRM view に移行する	**rrm**	—
5. 最小送信電力を設定する	**calibrate-power min** *tx-power*	デフォルト：AP group viewの設定が使用されます。

II. AP group RRM view での最小送信電力の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP group view に移行する	**wlan ap-group** *group-name*	—
3. AP model view に移行する	**ap-model** *model-name*	—

操作	コマンド	補足
4． radio view に移行する	**radio** *radio-id*	—
5． RRM view に移行する	**rrm**	—
6． 最小送信電力を設定する	**calibrate-power min** *tx-power*	デフォルト： グローバル設定ビューの設定が使用されます。

III. Global Configuration view での最小送信電力の設定

🕮 **メモ：**

この機能はソフトウェアバージョン 9.4.09 を含む以降のソフトウェアからサポートしています。

以下に、最大送信電力を設定する手順を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． global configuration view に移行する	**wlan global-configuration**	—
3． 2.4GHz 無線の最大送信電力を設定する	**calibrate-power 2.4g min** *tx-power*	デフォルト：6dBm
4． 5GHz 無線の最大送信電力を設定する	**calibrate-power 5g min** *tx-power*	デフォルト：11dBm
5． 6GHz 無線の最大送信電力を設定する	**calibrate-power 6g min** *tx-power*	デフォルト：11dBm

6.5.10 最大送信電力の設定

🕮 **メモ：**

この機能はソフトウェアバージョン 9.4.09 を含む以降のソフトウェアからサポートしています。

auto-TPC で設定できる無線の最大送信電力を調整することができます。

最大送信電力は、最小送信電力の設定値よりも小さくすることはできません。

以下に、最大送信電力を設定する手順を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． global configuration view に移行する	**wlan global-configuration**	—
3． 2.4GHz 無線の最大送信電力を設定する	**calibrate-power 2.4g max** *tx-power*	デフォルト：2.4GHz無線でサポートされる最大電力
4． 5GHz 無線の最大送信電力を設定する	**calibrate-power 5g max** *tx-power*	デフォルト：5GHz無線でサポートされる最大電力

操作	コマンド	補足
5． 6GHz 無線の最大送信電力を設定する	**calibrate-power 6g max** *tx-power*	デフォルト: 6GHz無線でサポートされる最大電力

6.5.11 RRM 抑制グループの設定

頻繁なチャネルまたは電力の調整が無線サービスに影響しないようにする場合、指定した無線を RRM 抑制グループに追加します。RRM 抑制グループ内の無線機に関する、チャネルまたは電力の変更が行われるたびに、チャネルまたは電力抑制タイマを開始します。チャネルまたは電力抑制タイマの時間が切れるまでは、無線のチャネルまたは電力は変更されません。

オンデマンド TPC を実行すると、電力抑制タイマの時間切れに関係なく、キャリブレーション間隔が終了すると TPC が実行されます。

I. RRM 抑制グループの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． RRM 抑制グループを作成し、RRM holddown group view に移行する	**wlan rrm-calibration-group** *group-id*	デフォルト：設定なし
3． （オプション設定項目）RRM 抑制グループの説明を設定する	**description** *text*	デフォルト：設定なし
4． 無線を RRM グループに追加する	**ap name** *ap-name* **radio** *radio-id*	デフォルト：設定なし
5． （オプション設定項目）電力抑制タイマを設定する	**power holddown-time** *minutes*	デフォルト： 60分

6.6 帯域幅自動調整の設定

6.6.1 帯域幅自動調整の設定作業リスト

作業リスト
1. 帯域幅自動調整の有効化
2. （オプション設定項目） 帯域幅自動調整間隔の設定

6.6.2 帯域幅自動調整の有効化

帯域幅自動調整機能は 5GHz 帯および 6GHz 帯でのみ有効です。

I. グローバル設定 view での帯域幅自動調整の有効化

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． グローバル設定 view に移行する	**wlan global-configuration**	—
3． auto-TPC を有効にする	**calibrate-bandwidth self-decisive enable** { **5g** | **6g** | **all** }	デフォルト：無効 **5g**、**6g**、**all**パラメータはソフトウェアバージョン9.4.09を含む以降のソフトウェアでサポートです。

II. radio view での帯域幅自動調整の有効化

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP を作成し、AP view に移行する	**wlan ap** *ap-name*	—
3． radio view に移行する	**radio** *radio-id*	—
4． rrm view に移行する	**rrm**	—
5． 帯域幅自動調整を有効にする	**calibrate-bandwidth self-decisive enable**	デフォルト：AP group viewの設定が使用されます。

III. AP group radio view での帯域幅自動調整の有効化

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP group view に移行する	**wlan ap-group** *group-name*	—
3． AP model view に移行する	**ap-model** *model-name*	—
4． radio view に移行する	**radio** *radio-id*	—
5． rrm view に移行する	**rrm**	—
6． 帯域幅自動調整を有効にする	**calibrate-bandwidth self-decisive enable**	デフォルト：Global configuration viewの設定が使用されます。

6.6.3 帯域幅自動調整間隔の設定

帯域幅自動調整が有効の場合、AC は帯域幅自動調整間隔に達するとチャネル品質検出を開始し、帯域幅調整を実行するかどうかを決定します。

I. 帯域幅自動調整間隔の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． （オプション設定項目）帯域幅自動調整間隔を設定する	**wlan rrm-calibration-bandwidth interval** *minutes*	デフォルト：13分

6.7 無線ベースラインの設定

無線ベースラインは無線の動作チャネル、転送レートやほかの無線属性を保存します。

現在の無線の設定を保存することで無線ベースラインを作成し、必要な設定を使用するためのベースラインを適用することができます。

無線ベースラインは AC のファイルシステムに“.csv”ファイルとして保存されます。

以下のいずれかの状態の場合、無線ベースラインを無線に適用することができません。

- 無線がダウンしています。
- サービステンプレートが無線に関連付けられていません。あるいはサービステンプレートが無効です。
- ベースラインのチャネルが不正です。
- 無線が手動で指定されたチャネルを使用しています。
- 無線の動作チャネル、送信電力がロックされています。
- 無線のチャネル、電力抑制タイマが終了していません。
- ベースラインのチャネルが指定したチャネルギャップに一致していません。
- 無線のベースラインの送信電力が指定した最小送信電力より小さいです。
- 無線のベースラインの送信電力が指定した最大送信電力より大きいです。
- ベースラインの無線モード、ロケーション識別子、帯域幅が無線の無線モード、ロケーション識別子、帯域幅に一致していません。

以下に無線ベースラインを設定する手順を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. 現在の無線の設定を保存するベースラインを作成する	**wlan rrm baseline save name** *baseline-name* { **ap** *ap-name* **radio** *radio-id* | **ap-group** *group-name* **ap-model** *ap-model* **radio** *radio-id* | **global** }	—
3. ベースラインを適用する	**wlan rrm baseline apply name** *baseline-name*	—
4. （オプション設定項目）無線ベースラインを削除する	**wlan rrm baseline remove name** *baseline-name*	—

6.8 無線スキャニングの有効化

この機能は、WLAN 環境をスキャンするため、AP で有効にします。指定した間隔で AC に収集した統計情報を通知します。AC はチャネルレポートと隣接レポートを作成するため、統計情報を使用します。

チャネルレポートと隣接レポートを表示する場合、**display wlan rrm-status ap** コマンドを使用します。

定期 auto-DFS、スケジュール auto-DFS、定期 auto-TPC、スケジュール auto-TPC が設定されている場合、この機能は自動的に有効になります。

I. RRM view でのクライアントチャネル機能一致モード設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP view に移行する	**wlan ap** *ap-name*	—
3． radio view に移行する	**radio** *radio-id*	—
4． RRM view に移行する	**rrm**	—
5． 無線スキャニングを有効にする	**scan-only enable**	デフォルト：AP group viewの設定が使用されます。

II. RRM view でのクライアントチャネル機能一致モード設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP group view に移行する	**wlan ap-group** *group-name*	—
3． AP model view に移行する	**ap-model** *model-name*	—
4． radio view に移行する	**radio** *radio-id*	—
5． RRM view に移行する	**rrm**	—
6． 無線スキャニングを有効にする	**scan-only enable**	デフォルト：無効

6.9 WLAN RRMのSNMP通知の有効化

重要な WLAN RRM イベントを NMS に報告するには、WLAN RRM の SNMP 通知を有効にする必要があります。WLAN RRM イベント通知を正しく送信するには、SNMP を設定する必要があります。SNMP の詳細は、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*17 ネットワーク管理と監視*”の”*4 章 SNMP*”を参照してください。

I. WLAN RRM の SNMP 通知有効化設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． WLAN RRM の SNMP 通知を有効にする	**snmp-agent trap enable wlan rrm**	デフォルト：無効

6.10 2.4GHzの無線チャネル最適化の設定

🕮 **メモ：**
この機能はソフトウェアバージョン 9.4.09 を含む以降のソフトウェアからサポートしています。

6.10.1 設定の制限とガイドライン

異なるベンダの AP を使用した高密度展開では、これらの AP を統一した方法で管理できず、異なるチャネルグループを使用する可能性があるため、2.4 GHz 無線に対して重大な干渉が発生する可能性があります。これは、ユーザーエクスペリエンスに大きな影響を与えます。

この機能を使用すると、AC は、auto DFS でサードパーティ製 AP の近隣無線で最も使用されるチャネルグループを採用できます。この操作により、異なるベンダの AP 間のチャネル間干渉を最大限に減らすことができます。

装置は、(1、6、11)、(1、7、13)、(2、7、12)、(3、8、13)、 (4、9、14)のチャネルグループの検出をサポートしています。

周辺の無線には、次のタイプがあります。

- **Managed neighbor**– 同じ **AC** で管理されている **AP** 無線を検出した場合
- **Unmanaged neighbor**– 別の **AC** で管理されている **AP** 無線を検出した場合

この機能を有効にすると、次の条件がすべて満たされた場合、装置は自動 DFS 中に 2.4 GHz 無線のチャネル最適化を実行します。

- 周辺の合計数が設定されたしきい値に達するか、それを超えた場合
- 管理対象外の周辺の比率（管理対象外の周辺/周辺の合計）が設定されたしきい値に達した場合か、それを超えた場合
- 単一のチャネルグループ（管理対象外の周辺/周辺の合計）の管理対象外の周辺の比率が設定されたしきい値に達した場合か、それを超えた場合

6.10.2 2.4GHz の無線チャネル最適化の設定

I. Global configuration view での 2.4GHz の無線チャネル最適化の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. Global configuration view に移行する	**global configuration view**	—
3. 2.4 GHz 無線のチャネル最適化を有効にする	**calibrate-channel 2.4g channel-set-optimization enable**	デフォルト：有効
4. （オプション設定項目）周辺の数のしきい値を設定する	**calibrate-channel 2.4g channel-set-optimization neighbor-threshold** *count*	デフォルト： 10

操作	コマンド	補足
5．（オプション設定項目）周辺の数の比率のしきい値を設定する	**calibrate-channel 2.4g channel-set-optimization neighbor-threshold percent** *count*	デフォルト：50%
6．（オプション設定項目）単一のチャネルグループの管理対象外の周辺の比率のしきい値を設定する	**calibrate-channel 2.4 g channel-set-optimization neighbor-unmanaged-threshold percent-per-set** *percent*	デフォルト： 10%

II. RRM view での 2.4GHz の無線チャネル最適化の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP view に移行する	**wlan ap** *ap-name*	—
3． radio view に移行する	**radio** *radio-id*	—
4． RRM view に移行する	**rrm**	—
5． 2.4 GHz 無線のチャネル最適化を有効にする	**calibrate-channel channel-set-optimization** { **disable** | **enable** }	デフォルト：AP group viewの設定が使用されます。
6．（オプション設定項目）周辺の数のしきい値を設定する	**calibrate-channel channel-set-optimization neighbor-threshold** *count*	デフォルト：AP group viewの設定が使用されます。
7．（オプション設定項目）管理対象外の周辺の比率のしきい値を設定する	**calibrate-channel-set-optimization neighbor-unmanaged-threshold percent-per-set** *percent*	デフォルト：AP group viewの設定が使用されます。
8．（オプション設定項目）単一のチャネルグループの管理対象外の周辺の比率のしきい値を設定する	**calibrate-channel-set-optimization neighbor-unmanaged-threshold percent-per-set** *percent*	デフォルト：AP group viewの設定が使用されます。

III. AP group RRM view での 2.4GHz の無線チャネル最適化の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP group RRM view に移行する	**wlan ap-group** *group-name*	—
3． AP model view に移行する	**ap-model** *model-name*	—
4． radio view に移行する	**radio** *radio-id*	—
5． RRM view に移行する	**rrm**	—
6． 2.4 GHz 無線のチャネル最適化を有効にする	**calibrate-channel channel-set-optimization** { **disable** | **enable** }	デフォルト： Global configuration viewの設定が使用されます。
7．（オプション設定項目）周辺の数のしきい値を設定する	**calibrate-channel channel-set-optimization neighbor-threshold** *count*	デフォルト： Global configuration viewの設定が使用されます。

操作	コマンド	補足
8.　（オプション設定項目）管理対象外の周辺の比率のしきい値を設定する	**calibrate-channel-set-optimization neighbor-unmanaged-threshold percent-per-set** *percent*	デフォルト： Global configuration viewの設定が使用されます。
9.　（オプション設定項目）単一のチャネルグループの管理対象外の周辺の比率のしきい値を設定する	**calibrate-channel-set-optimization neighbor-unmanaged-threshold percent-per-set** *percent*	デフォルト： Global configuration viewの設定が使用されます。

6.11 高密度シナリオでシャットダウンできるAPの除外

🕮 **メモ：**

この機能はソフトウェアバージョン 9.4.09 を含む以降のソフトウェアからサポートしています。

高密度シナリオでは、チャネルリソースが限られているため、隣接 AP 間で AP 間干渉が避けられない場合があります。密度が高いほど、干渉が大きくなります。

高密度シナリオでチャネル調整によって干渉を削減できない場合は、このタスクを実行して、シャットダウンできる AP をフィルタで除外できます。フィルタ処理後、**display wlan rrm high-density filter history** コマンドを実行して、フィルタで除外した AP を表示し、手動で AP を無効にします。

I. 高密度シナリオでシャットダウンできる AP の除外設定

操作	コマンド	補足
1.　system view に移行する	**system-view**	—
2.　密度シナリオでシャットダウンできる AP を除外する	**wlan rrm high-density filter** { **all** | **ap-group** *group-name* } { **2.4g** | **5g** | **6g** | **all** }	—

6.12 WLAN RRMの表示および管理

すべての view で **display** コマンドを実行できます

操作	コマンド
無線ベースラインの情報を表示する	**display wlan rrm baseline** { **all** | **name** *baseline-name* } [**verbose**]
無線ベースラインの直近のアプリケーション結果を表示する	**display wlan rrm baseline apply-result**
チャネルと電力調整履歴を表示する	**display wlan rrm-history ap** { **all** | **name** *ap-name* }

操作	コマンド
WLAN RRMを情報表示する	**display wlan rrm-status ap** { **all** | **name** *ap-name* }
RRM抑制グループの情報を表示する	**display wlan rrm-calibration-group** { **all** | *group-id* }

6.13 WLAN RRMの設定例

6.13.1 定期 auto-DFS の設定例

I. ネットワーク要件

図 6-3に示すように、チャネル調整トリガー条件が満たされたときに AP の無線用のチャネルを調整するように auto-DFS を設定します。頻繁なチャネル調整を避けるために、AP1 の無線 1 を RRM 抑制グループに追加します。

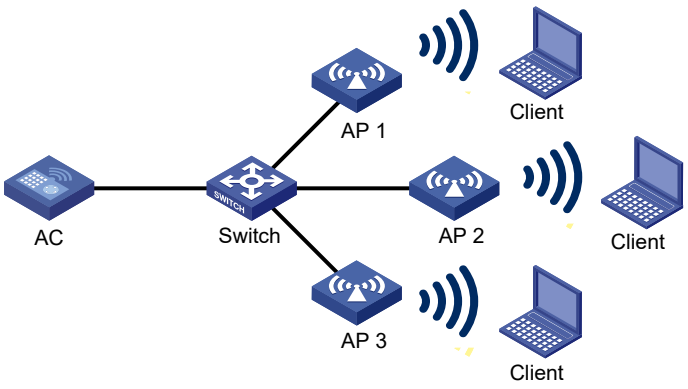


図 6-3 ネットワーク図

II. 設定手順

AC と各 AP の間に CAPWAP トンネルを確立します。詳細については、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*7 AP 管理*”の”*1 章 AP 管理*”を参照してください。（詳細は省略します。）

AP1 で auto-DFS を有効にします。

```
<AC> system-view
[AC] wlan ap ap1 model QX-W1020
[AC-wlan-ap-ap1] radio 1
[AC-wlan-ap-ap1-radio-1] rrm
[AC-wlan-ap-ap1-radio-1-rrm] calibrate-channel self-decisive enable
```

```
[AC-wlan-ap-ap1-radio-1-rrm] calibrate-channel mode periodic
```

DFS トリガーパラメータを設定します。

```
[AC-wlan-ap-ap1-radio-1-rrm] crc-error-threshold 20
[AC-wlan-ap-ap1-radio-1-rrm] tolerance-level 20
[AC-wlan-ap-ap1-radio-1-rrm] quit
[AC-wlan-ap-ap1-radio-1] quit
[AC-wlan-ap-ap1] quit
```

RRM 抑制グループ 10 を作成します。

```
[AC] wlan rrm-calibration-group 10
```

AP1 の無線 1 を RRM 抑制グループ 10 に追加します。

```
[AC-wlan-rc-group-10] ap name ap1 radio 1
```

チャネル抑制タイマを 600 分に設定します。

```
[AC-wlan-rc-group-10] channel holddown-time 600
```

AP 1 と同じ方法で、AP 2 と AP 3 の auto-DFS を設定します。（詳細は省略します。）

III. 設定の確認

display wlan rrm-status ap all コマンドを実行します。チャネル調整トリガー条件を満たし較正間隔に達することで、AP の無線用のチャネルが変更されることを確認します。（詳細は省略します。）

display wlan rrm-history ap all コマンドを使用して、チャネル調整の理由を表示します。（詳細は省略します）

最初の DFS から 600 分以内に、AP 1 の無線 1 のチャネルが変更されていないことを確認します。（詳細は省略します）

6.13.2 スケジュール auto-DFS の設定例

I. ネットワーク要件

図 6-4に示すように、チャネル調整トリガー条件が満たされたときに AP の無線用のチャネルを調整するようにスケジュール auto-DFS を設定します。

0:05～23:50 の測定結果を使用して翌日の 5:00 にチャネル設定を行います。

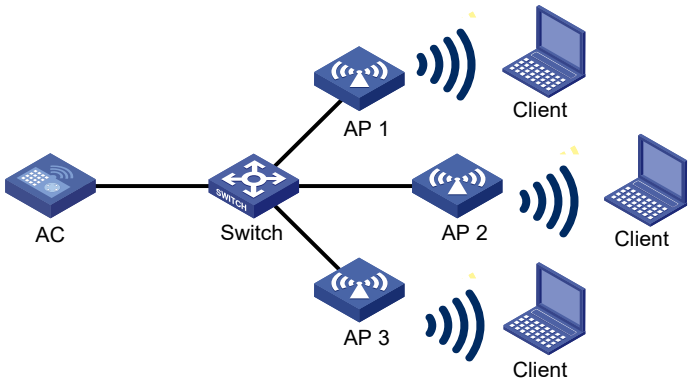


図 6-4 ネットワーク図

II. 設定手順

AC と各 AP の間に CAPWAP トンネルを確立します。詳細については、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*7 AP 管理*”の”*1 章 AP 管理*”を参照してください。（詳細は省略します。）

タイムレンジを作成します。

```
<AC> system-view
[AC] time-range time1 from 0:05 to 23:50 daily
```

job を作成し、job にコマンドを割り当てます。

```
[AC] scheduler job calibratechannel
[AC-job-calibratechannel] command 1 system-view
[AC-job-calibratechannel] command 2 wlan ap ap1
[AC-job-calibratechannel] command 3 radio 1
[AC-job-calibratechannel] command 4 rrm
[AC-job-calibratechannel] command 5 calibrate-channel pronto
[AC-job-calibratechannel] quit
```

スケジュールを作成し、スケジュールに job を割り当てます。

```
[AC] scheduler schedule schedule1
[AC-schedule-schedule1] job calibratechannel
```

スケジュールに実行日時(毎日 5 時)を設定します。

```
[AC-schedule-schedule1] time repeating at 5:00
[AC-schedule-schedule1] quit
```

AP1 で auto-DFS を有効にし、スケジュール auto-DFS を設定します。

```
[AC] wlan ap ap1
```

```
[AC-wlan-ap-ap1] radio 1
[AC-wlan-ap-ap1-radio-1] rrm
[AC-wlan-ap-ap1-radio-1-rrm] calibrate-channel self-decisive enable
[AC-wlan-ap-ap1-radio-1-rrm] calibrate-channel mode scheduled
```

ap1 にタイムレンジ time1 の間、チャネルのモニタリングを実行するように設定します。

```
[AC-wlan-ap-ap1-radio-1-rrm] calibrate-channel monitoring time-range time1
```

auto-DFS の属性は変更せず初期値を使用します。

III. 設定の確認

display wlan rrm-status ap all コマンドを実行します。チャネル調整トリガー条件を満たし較正間隔に達することで、AP の無線用のチャネルが変更されることを確認します。（詳細は省略します。）

display wlan rrm-history ap all コマンドを使用して、チャネル調整の理由を表示します。（詳細は省略します）

6.13.3 定期 TPC の設定例

I. ネットワーク要件

図 6-5に示すように、auto-TPC を設定し、隣接番号のしきい値を 3 に設定すると、AP 4 が参加したときに AC が auto-TPC を実行できるようになります。頻繁な電力調整を避けるために、AP1 の無線 1 を RRM 抑制グループに追加します。

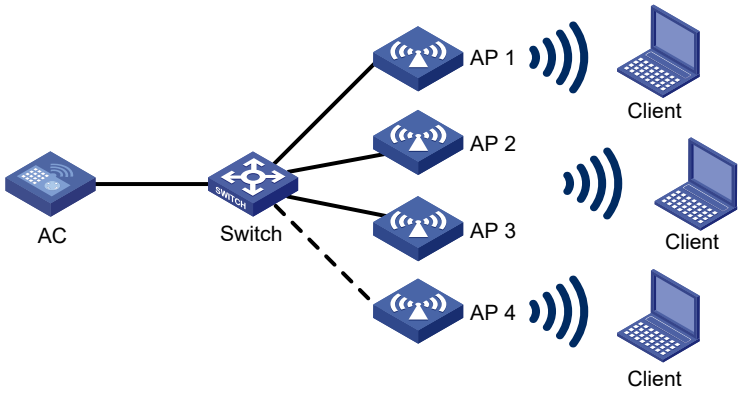


図 6-5 ネットワーク図

II. 設定手順

#AC と各 AP の間に CAPWAP トンネルを確立します。詳細については、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*7 AP 管理*”の”*1 章 AP 管理*”を参照してください。（詳細は省略します。）

AP1 で auto-TPC を有効にします。

```
<AC> system-view
[AC] wlan ap ap1 model QX-W1020
[AC-wlan-ap-ap1] radio 1
[AC-wlan-ap-ap1-radio-1] rrm
[AC-wlan-ap-ap1-radio-1-rrm] calibrate-power self-decisive enable
```

TPC トリガーパラメータを設定します。

```
[AC-wlan-ap-ap1-radio-1-rrm] adjacency-factor 3
[AC-wlan-ap-ap1-radio-1-rrm] calibrate-power threshold 80
[AC-wlan-ap-ap1-radio-1-rrm] calibrate-power min 1
[AC-wlan-ap-ap1-radio-1-rrm] quit
[AC-wlan-ap-ap1-radio-1] quit
[AC-wlan-ap-ap1] quit
```

RRM 抑制グループ 10 を作成します。

```
[AC] wlan rrm-calibration-group 10
```

AP1 の無線 1 を RRM 抑制グループ 10 に追加します。

```
[AC-wlan-rc-group-10] ap name ap1 radio 1
```

電力抑制タイマを 100 分に設定します。

```
[AC-wlan-rc-group-10] power holddown-time 100
```

AP 1 と同じ方法で、AP 2、AP 3、および AP 4 に auto-TPC を設定します。（詳細は省略します）

III. 設定の確認

AP4 の無線機が電力検出用無線機であり、このステップで AP の名前を使用してその無線機を参照すると仮定します。

次の情報を確認するには、**display wlan rrm-status ap all** コマンドを使用します。

- AP1 の電力が電力調整しきい値よりも低いことを AP4 が検出すると、AP1 は送信電力を増加させることを確認します。
- AP1 の電力が電力調整しきい値より高いことを AP4 が検出すると、AP1 は送信電力を減少させることを確認します。
- AP1 の調整された電力は、最小送信電力（この例では 1dBm）より低くはないことを確認します。

最初の TPC から 100 分以内に、AP1 の無線 1 の電力が変更されないことを確認します。

6.13.4 帯域幅自動調整の設定例

I. ネットワーク要求

図 6-6に示すように、帯域幅自動調整を設定して周辺 AP の数に応じて、自動的に帯域幅が調整されるようにします。

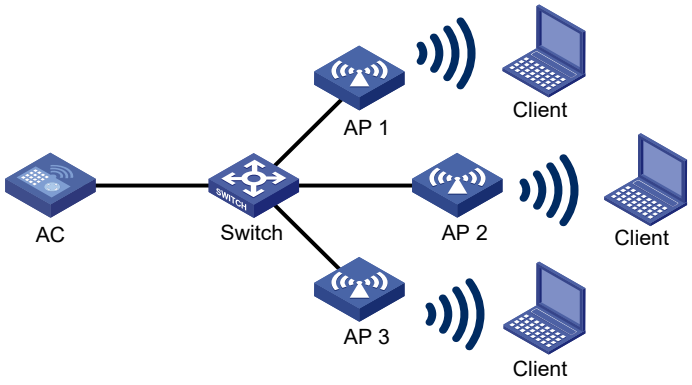


図 6-6 ネットワーク図

II. 設定手順

帯域幅自動調整を有効にします。

```
<AC> system-view
[AC] wlan global-configuration
[AC-wlan-global-configuration] calibrate-bandwidth self-decisive enable
[AC-wlan-global-configuration] quit
```

帯域幅自動調整間隔を 10 分に設定します。

```
[AC] wlan rrm calibration-bandwidth interval 10
```

III. 設定の確認

display wlan rrm-history ap all コマンドを使用して、帯域幅自動調整の履歴を表示します。（詳細は省略します）

目次

このセクションのページは **9-x-x** です。

7 章 チャネルスキャンの設定 7-1
7.1 概要 7-1
7.1.1 基本概念 7-1
7.1.2 動作メカニズム 7-1
7.2 チャネルスキャンの設定 7-2
7.3 チャネルスキャン設定の作業リスト 7-2
7.3.1 スキャン期間の設定 7-2
7.3.2 最大サービス期間の設定 7-3
7.3.3 サービスアイドルタイムアウトの設定 7-3
7.3.4 チャネルスキャンブラックリスト・ホワイトリストの設定 7-4
7.3.5 連続サービスの抑制 7-5
7.3.6 チャネルレポートおよびネイバレポートの送信の設定 7-5
7.4 チャネルスキャンの設定例 7-6
7.4.1 相対的な優先転送の設定例 7-6
7.4.2 絶対的な優先転送の設定例 7-7

7章 チャネルスキャンの設定

7.1 概要

チャネルスキャンにより、AP はチャネルをスキャンし無線パケットをキャプチャすることができます。AC は、インタフェース、エラービットレート、無線信号強度などの無線サービス情報を得るために、キャプチャした無線パケットを分析します。チャネルスキャンにより、WLAN RRM と WIPS に対してデータが提供され、無線サービス品質が向上します。

7.1.1 基本概念

- **スキャン期間**－AP は、スキャン期間内でチャネルのスキャンのみ行い、無線サービスは提供しません。
- **サービス期間**－AP は、サービス期間内で以下の方法のいずれかで働きます。
  - AP は無線サービスの提供のみを行い、チャネルのスキャンはしません。
  - AP は、スキャン期間と同じ期間、動作チャネルのスキャンと無線サービスの提供を同時に行います。その後、AP は無線サービスの提供のみ行います。

7.1.2 動作メカニズム

AP は、AP が無線サービスを提供するかどうかにかかわらず、スキャン期間の間にチャネルスキャンリスト上の各チャネルを順番にスキャンします。AP が無線サービスを提供しない場合、AP はスキャン期間を継続的に開始します。AP が無線サービスを提供する場合、AP はサービス期間とスキャン期間のどちらか一方を開始します。

図 7-1 は、AP がチャネル 6 で動作し、チャネルスキャンリストがチャネル 1、6、11 を含むときのチャネルスキャンの仕組みを示します。

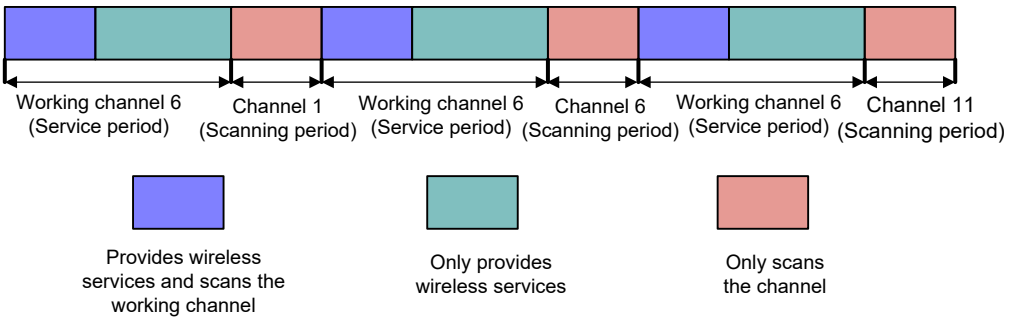


図 7-1 チャネルスキャンメカニズム

7.2 チャネルスキャンの設定

以下の方法で AP を設定できます：

- AP view で 1 つずつ AP を構成する。
- AP を AP group に割り当て、AP group view で AP group を構成する。
- グローバル設定ビューですべての AP を構成する。

AP の場合、同じパラメータの設定は、AP view、AP group view、グローバル設定 view の降順で有効になります。

7.3 チャネルスキャン設定の作業リスト

作業リスト
スキャン期間の設定
最大サービス期間の設定
サービスアイドルタイムアウトの設定
（オプション設定項目）チャネルスキャンブラックリスト・ホワイトリストの設定
（オプション設定項目）連続サービスの抑制
（オプション設定項目）チャネルレポートおよびネイバレポートの送信の設定

7.3.1 スキャン期間の設定

I. radio view でのスキャン期間の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP view に移行する	**wlan ap** *ap-name*	—
3． radio view に移行する	**radio** *radio-id*	—
4． スキャン期間を設定する	**scan scan-time** *scan-time*	デフォルト： AP group radio viewの設定を使用します。

II. AP group view でのスキャン期間の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP group view に移行する	**wlan ap-group** *group-name*	—
3． AP model view に移行する	**ap-model** *ap-model*	—
4． radio view に移行する	**radio** *radio-id*	—
5． スキャン期間を設定する	**scan scan-time** *scan-time*	デフォルト： 100ミリ秒

7.3.2 最大サービス期間の設定

スキャン品質とサービス品質の両方を保証するために、最大サービス期間を設定できます。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の有無に関わらずスキャン期間を開始します。無線サービス品質を保証するため、AP がサービス期間を制限しないように設定できます。AP はサービスアイドルタイムアウトが終了するまでスキャン期間を開始しません。

I. radio view での最大サービス期間の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP view に移行する	**wlan ap** *ap-name*	—
3. radio view に移行する	**radio** *radio-id*	—
4. 最大サービス期間を設定する	**scan max-service-time** { *max-service-time* | **no-limit** }	デフォルト： AP group radio viewの設定を使用します。

II. AP group view での最大サービス期間の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP group view に移行する	**wlan ap-group** *group-name*	—
3. AP model view に移行する	**ap-model** *ap-model*	—
4. radio view に移行する	**radio** *radio-id*	—
5. スキャン期間を設定する	**scan max-service-time** { *max-service-time* | **no-limit** }	デフォルト： no-limit

7.3.3 サービスアイドルタイムアウトの設定

サービス期間の間、たとえ指定されたサービスアイドルタイムアウトが終了しても、現在のサービス期間がスキャン期間を超過するまで、AP は新たなスキャン期間を開始しません。

I. radio view でのサービスアイドルタイムアウトの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP view に移行する	**wlan ap** *ap-name*	—
3. radio view に移行する	**radio** *radio-id*	—
4. サービスアイドルタイムアウトを設定する	**scan idle-time** *idle-time*	デフォルト： AP group radio viewの設定を使用します。サービスアイドルタイムアウトは最大サービス期間よりも大きくすることはできません。

II. AP group view でのービスアイドルタイムアウトの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP group view に移行する	**wlan ap-group** *group-name*	—
3. AP model view に移行する	**ap-model** *ap-model*	—
4. radio view に移行する	**radio** *radio-id*	—
5. スキャン期間を設定する	**scan idle-time** *idle-time*	デフォルト： 100ミリ秒

7.3.4 チャネルスキャンブラックリスト・ホワイトリストの設定

ブラックリストのチャネルをスキャンしない、あるいはホワイトリストのチャネルのみをスキャンするようにAPを設定します。ブラックリストとホワイトリストの両方を同じAPに設定することはできません。

I. radio view でのブラックリスト・ホワイトリストの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP view に移行する	**wlan ap** *ap-name*	—
3. radio view に移行する	**radio** *radio-id*	—
4. 特定のチャネルをブラックリストに指定する	**scan channel blacklist** *channel-list*	デフォルト： AP group radio viewの設定を使用します。
5. 特定のチャネルをホワイトリストに指定する	**scan channel whitelist** *channel-list*	デフォルト： AP group radio viewの設定を使用します。

II. AP group radio view でのブラックリスト・ホワイトリストの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP group view に移行する	**wlan ap-group** *group-name*	—
3. AP model view に移行する	**ap-model** *ap-model*	—
4. radio view に移行する	**radio** *radio-id*	—
5. 特定のチャネルをブラックリストに指定する	**scan channel blacklist** *channel-list*	デフォルト： 設定なし
6. 特定のチャネルをホワイトリストに指定する	**scan channel whitelist** *channel-list*	デフォルト： 設定なし

7.3.5 連続サービスの抑制

AP が継続的なサービスを提供する場合、最大サービス期間は制限されず、サービスアイドルタイムアウトタイマが経過しない限り、AP はスキャン期間を開始しません。

完全なチャネルレポートとネイバレポートを収集するために、AP は AP の起動中に一定期間、継続的なサービスを自動的に抑制します。通常の AP 動作中は、必要に応じて継続的なサービスを抑制できます。サービス抑制期間中、AP はチャネルを代替的にスキャンし、無線アクセスサービスを提供します。収集されたチャネルレポートとネイバレポートは、チャネルと電力を自動的に調整するためのベースとなります。

サービス抑止時間は、継続サービスの自動・手動抑止時に wlan radio continuous-service suppression-time コマンドで設定する。

I. 制限事項とガイドライン

この機能を設定する前に、継続的サービスが有効になっていることを確認してください。

パケット損失によるサービスへの影響を回避するためのベストプラクティスとして、ネットワークメンテナンス中は継続的サービスを抑制してください。

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． 連続サービスを抑止する	**wlan radio continuous-service suppression**	—
3． 連続サービス抑止時間を設定する	**wlan radio continuous-service suppression-time** *time*	デフォルト：10分

7.3.6 チャネルレポートおよびネイバレポートの送信の設定

I. チャネルレポートの送信の設定

自動チャネル調整、自動電力調整、および無線リソース測定のために AC の負荷が高い場合は、チャネルレポートの送信を一時的に無効にして、ワイヤレスアクセスサービスを保証できます。チャネルレポートの送信を無効にすると、自動チャネル調整、自動電力調整、および無線リソース測定は使用できなくなります。

チャネルレポートの送信を無効にした後、AP がチャネルレポートを送信する間隔を調整して、AC の負荷を軽減できます。適切なレポート間隔を設定します。レポート間隔が小さいと、AC 負荷が高くなります。レポート間隔が大きいと、自動チャネル調整と自動電源調整に影響します。

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP によるチャネルレポートの送信を無効にする	**wlan channel-report disable**	デフォルト：有効
3． （オプション設定項目）AP がチャネルレポートを送信する間隔を設定する	**wlan channel-report interval** *interval*	デフォルト：300秒

II. ネイバレポート送信の設定

自動チャネル調整、自動電力調整、および無線リソース測定のために AC 負荷が高い場合は、ネイバレポート送信を一時的に無効にして、無線アクセスサービスを確保できます。ネイバレポート送信を無効にすると、自動チャネル調整、自動電力調整、および無線リソース測定は使用できなくなります。

ネイバレポート送信を無効にした後、AP がネイバレポートを送信する間隔を調整して、AC の負荷を軽減できます。適切なレポート間隔を設定します。レポート間隔が小さいと、AC 負荷が高くなります。レポート間隔が大きいと、自動チャネル調整と自動電源調整に影響します。

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． APによるチャネルレポートの送信を無効にする	**wlan neighbor-report disable**	デフォルト：有効
3． （オプション設定項目）APがチャネルレポートを送信する間隔を設定する	**wlan neighbor-report interval** *interval*	デフォルト：300秒

7.4 チャネルスキャンの設定例

7.4.1 相対的な優先転送の設定例

I. ネットワーク要件

図 7-2 に示すように、チャネルスキャンを設定し、チャネルスキャンと無線サービス品質を保証するために AP 1 に最大サービス期間を設定します。

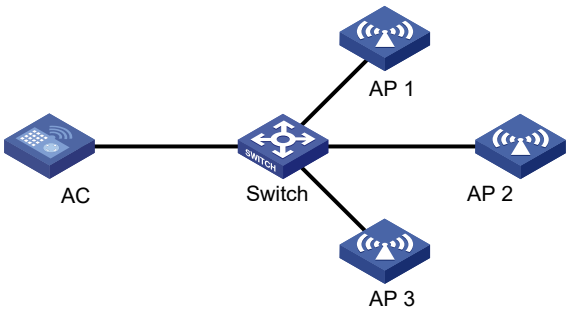


図 7-2 ネットワーク図

II. 設定手順

手動 AP を作成し、AP モデル名とシリアル ID を指定します。

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

```
[AC] wlan ap ap1 model QX-W1020
[AC-wlan-ap-ap1] serial-id 219801A0CNC138011454
```

radio 1 の radio view を有効にします。

```
[AC-wlan-ap-ap1] radio 1
```

スキャン期間を 200 ミリ秒に設定します。

```
[AC-wlan-ap-ap1-radio-1] scan scan-time 200
```

最大サービス期間を 5000 ミリ秒に設定します。

```
[AC-wlan-ap-ap1-radio-1] scan max-service-time 5000
```

サービスアイドルタイムアウトを 100 ミリ秒に設定します。

```
[AC-wlan-ap-ap1-radio-1] scan idle-time 100
```

7.4.2 絶対的な優先転送の設定例

I. ネットワーク要件

図 7-3 に示すように、チャネルスキャンを設定し、無線サービス品質を保証するために AP 1 に対してサービス期間を制限しないようにします。

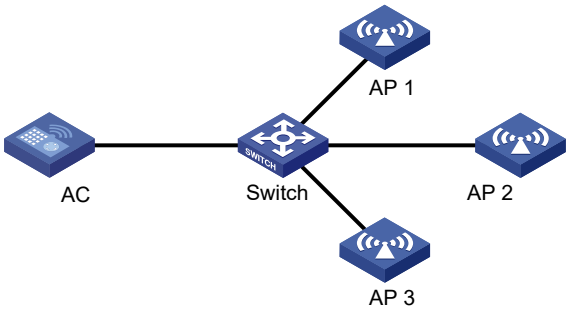


図 7-3 ネットワーク図

II. 設定手順

手動 AP を作成し、AP モデル名とシリアル ID を指定します。

```
<AC> system-view
[AC] wlan ap ap1 model QX-W1020
[AC-wlan-ap-ap1] serial-id 219801A0CNC138011454
```

radio 1 の radio view を有効にします。

```
[AC-wlan-ap-ap1] radio 1
```

スキャン期間を 100 ミリ秒に設定します。

```
[AC-wlan-ap-ap1-radio-1] scan scan-time 100
```

無線がサービス期間を制限しないように設定します。

```
[AC-wlan-ap-ap1-radio-1] scan max-service-time no-limit
```

サービスアイドルタイムアウトを 100 ミリ秒に設定します。

```
[AC-wlan-ap-ap1-radio-1] scan idle-time 100
```

目次

このセクションのページは**9-x-x** です。

8章 スペクトル管理の設定 8-1
8.1 概要 8-1
8.2 スペクトル管理の設定作業リスト 8-1
8.3 スペクトル管理の設定 8-1
8.3.1 スペクトル管理の有効化 8-1
8.3.2 電力制約モードの設定 8-2
8.3.3 チャネルスイッチモードの設定 8-3
8.3.4 送信電力機能一致モードの設定 8-3
8.3.5 チャネル機能一致モードの設定 8-4
8.4 スペクトル管理の設定例 8-5
8.4.1 スペクトル管理の設定例 8-5

8章 スペクトル管理の設定

8.1 概要

802.11h で定義されているスペクトル管理は、5GHz 帯での運用の規制要件を満たすために 5GHz WLAN に適用されます。802.11h では、5GHz 帯で動作するクライアントは他の無線デバイスの干渉を避けるために送信電力を制御する必要があります。スペクトル管理により、無線機は関連するクライアントに許可された最大送信電力を通知し、その電力およびチャネルが規制上の要件を満たさない場合には、関連付けを拒否することができます。

8.2 スペクトル管理の設定作業リスト

作業リスト
スペクトル管理の有効化
（オプション設定項目）電力制約モードの設定
（オプション設定項目）チャネルスイッチモードの設定
（オプション設定項目）送信電力機能一致モードの設定
（オプション設定項目）チャネル機能一致モードの設定

8.3 スペクトル管理の設定

8.3.1 スペクトル管理の有効化

スペクトル管理機能は 5GHz 帯でのみ有効です。

I. radio view でのスペクトル管理の有効化

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP を作成し、AP view に移行する	**wlan ap** *ap-name*	—
3． radio view に移行する	**radio** *radio-id*	—
4． スペクトル管理を有効にする	**spectrum-management enable**	デフォルト：AP group viewの設定が使用されます。

II. AP group radio view でのスペクトル管理の有効化

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP group view に移行する	**wlan ap-group** *group-name*	—

操作	コマンド	補足
3． AP model view に移行する	**ap-model** *model-name*	—
4． radio view に移行する	**radio** *radio-id*	—
5． スペクトル管理を有効にする	**spectrum-management enable**	デフォルト：無効

8.3.2 電力制約モードの設定

電力制約モードの設定は 5GHz 帯でのみ有効です。

この機能を使用することで、無線が関連するクライアントの送信電力を制限して、他の無線デバイスへの干渉を回避できます。無線からの電力制約値を含むビーコンフレームまたはプローブ応答を受信すると、クライアントはその新しいローカル最大送信電力を使用してトラフィックを送信します。新しいローカル最大送信電力は、チャネルに対して指定された最大送信電力レベルから電力制約値を差し引いたものとなります。

無線リソース管理の詳細については、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*9 無線管理*”の”*4 章 WLAN 無線リソースの計測の設定*”を参照してください。

無線には次の電力制約モードを設定できます。

- **Manual**－電力制約値を指定します。
- **Auto**－自動的に電力制約値を計算します。

I. radio view での電力制約モードの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP を作成し、AP view に移行する	**wlan ap** *ap-name*	—
3． radio view に移行する	**radio** *radio-id*	—
4． 電力制約モードを設定する	**power-constraint mode** { **auto** [**anpi-interval** *anpi-interval-value*] | **manual** *power-constraint* }	デフォルト：AP group viewの設定が使用されます。 電力制約モードは、スペクトル管理または無線リソース測定を有効にする場合にのみ利用することができます。

II. AP group radio view での電力制約モードの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP group view に移行する	**wlan ap-group** *group-name*	—
3． AP model view に移行する	**ap-model** *model-name*	—
4． radio view に移行する	**radio** *radio-id*	—

操作	コマンド	補足
5. 電力制約モードを設定する	**power-constraint mode** { **auto** [**anpi-interval** *anpi-interval-value*] | **manual** *power-constraint* }	デフォルト：Auto 電力制約モードは、スペクトル管理または無線リソース測定を有効にする場合にのみ利用することができます。

8.3.3 チャネルスイッチモードの設定

この機能を使用することにより、無線が新しいチャネルに変更されたときに、無線が関連付けられたクライアントにチャネルスイッチアナウンスメントを送信することができます。アナウンスメントには、新しいチャネル番号と、クライアントがフレームの送信を続行できるかどうかに関する情報が含まれています。

I. radio view でのチャネルスイッチモードの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP を作成し、AP view に移行する	**wlan ap** *ap-name*	—
3. radio view に移行する	**radio** *radio-id*	—
4. チャネルスイッチモードを設定する	**channel-switch mode** { **continuous** | **suspend** }	デフォルト：AP group viewの設定が使用されます。

II. AP group radio view でのチャネルスイッチモードの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP group view に移行する	**wlan ap-group** *group-name*	—
3. AP model view に移行する	**ap-model** *model-name*	—
4. radio view に移行する	**radio** *radio-id*	—
5. チャネルスイッチモードを設定する	**channel-switch mode** { **continuous** | **suspend** }	デフォルト： suspend オンラインクライアントは、チャネル切り替え中にフレームの送信を停止します。

8.3.4 送信電力機能一致モードの設定

この機能を使用することにより、クライアントは定義済みの一致基準に基づいて無線に関連付けることができます。送信電力機能は、クライアントおよび無線機が現在のチャネルでフレームを送信できる最小電力および最大電力を指します。

デバイスは、次のクライアント電力機能の一致モードをサポートしています。

- **All**－クライアントは、それぞれの送信電力機能が各無線の送信電力機能と一致する場合にのみ、無線に関連付けることができます。
- **None**－クライアントの送信電力機能はチェックされません。

- **Partial**－クライアントは、その送信電力機能の 1 つが無線機の送信電力機能と一致する限り、無線機に関連付けることができます。

無線リソース管理の詳細については、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*9 無線管理*”の”*4 章 WLAN 無線リソースの計測の設定*”を参照してください。

I. radio view での送信電力機能一致モード設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP を作成し、AP view に移行する	**wlan ap** *ap-name*	—
3． radio view に移行する	**radio** *radio-id*	—
4． 送信電力機能一致モードを設定する	**power-capability mode** { **all** | **none** | **partial** }	デフォルト：AP group viewの設定が使用されます。 送信電力機能一致モードは、スペクトル管理または無線リソース測定を有効にした場合にのみ利用することができます。

II. AP group radio view での送信電力機能一致モード設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP group view に移行する	**wlan ap-group** *group-name*	—
3． AP model view に移行する	**ap-model** *model-name*	—
4． radio view に移行する	**radio** *radio-id*	—
5． 送信電力機能一致モードを設定する	**power-capability mode** { **all** | **none** | **partial** }	デフォルト：設定なし 送信電力機能一致モードは、スペクトル管理または無線リソース測定を有効にした場合にのみ利用することができます。

8.3.5 チャネル機能一致モードの設定

この機能を使用することにより、クライアントは定義済みの一致基準に基づいて無線に関連付けることができます。チャネル機能は、クライアントおよび無線がそれぞれサポートするチャネルを指します。

このデバイスは、次のクライアントチャネル機能一致モードを提供します。

- **All**－クライアントは、サポートされている各チャネルが無線でサポートされているチャネルのそれぞれと一致する場合にのみ、無線に関連付けることができます。
- **None**－チャネル機能のチェックはされません。
- **Partial**－サポートされているチャネルのいずれかがサポートされているラジオのチャネルと一致する限り、クライアントはラジオに関連付けることができます。

I. radio view でのクライアントチャネル機能一致モード設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP を作成し、AP view に移行する	**wlan ap** *ap-name*	—
3． radio view に移行する	**radio** *radio-id*	—
4． クライアントチャネル機能一致モードを設定する	**channel-capability mode** { **all** | **none** | **partial** }	デフォルト：AP group viewの設定が使用されます。

II. AP group radio view でのクライアントチャネル機能一致モード設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP group view に移行する	**wlan ap-group** *group-name*	—
3． AP model view に移行する	**ap-model** *model-name*	—
4． radio view に移行する	**radio** *radio-id*	—
5． チャネル機能一致モードを設定する	**channel-capability mode** { **all** | **none** | **partial** }	デフォルト：設定なし

8.4 スペクトル管理の設定例

8.4.1 スペクトル管理の設定例

I. ネットワーク要求

図 8-1に示すように、スペクトル管理を設定してクライアントの送信電力を制限し、チャネル切り替え中にクライアントがフレームを送信し続けるようにします。

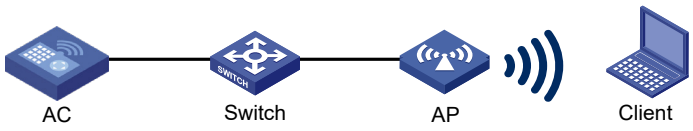


図 8-1 ネットワーク図

II. 設定手順

スペクトル管理を有効にします。

```
<AC> system-view
[AC] wlan ap officeap model QX-W1020
```

```
[AC-wlan-ap-officeap] radio 1
[AC-wlan-ap-officeap-radio-1] spectrum-management enable
```

チャネル機能一致モードを all に設定します。

```
[AC-wlan-ap-officeap-radio-1] channel-capability mode all
```

送信電力機能一致モードを all に設定します。

```
[AC-wlan-ap-officeap-radio-1] power-capability mode all
```

電力制約モードを手動に設定し、電源制約値を 5 dBm に設定します。

```
[AC-wlan-ap-officeap-radio-1] power-constraint mode manual 5
```

チャネルスイッチモードを continuous に設定します。

```
[AC-wlan-ap-officeap-radio-1] channel-switch mode continuous
```

III. 設定の確認

display wlan client コマンドを実行して、クライアントが正常に無線と関連付けられていることを確認します。（詳細は省略します）

QX-W2300AC シリーズ アクセスコントローラ

オペレーションマニュアル

10.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

02-拡張ローミング

03-モビリティグループ

目次

このセクションのページは **10-x-x** です。

1章 WLANローミング 1-1
1.1 概要 1-1
1.2 WLANローミングメカニズム 1-1
1.3 レイヤ3ローミング 1-1
1.4 ローミングエントリエージングタイムの設定 1-2
1.5 AC内ローミングの設定例 1-3

1章 WLAN ローミング

1.1 概要

WLAN ローミングは、クライアントがローミングプロセス中に IP アドレスと許可情報を保持しながら、同じ ESS 内のワイヤレスサービス間をシームレスにローミングできます。

1.2 WLANローミングメカニズム

図 1-1に示すように、クライアントは以下のように AP1 から AP2 にローミングします。

1) クライアントは AP1 からオンラインになり、AC はクライアントのローミングエントリを作成します。
   エントリは初期 SSID を関連付け、PMKID、認証方法、セキュリティモード、およびローミング VLAN に記録します。
2) クライアントは AP2 にローミングします。AC はローミングエントリを調べます。
3) クライアントは再認証を実行し、AP2 からオンラインになります。

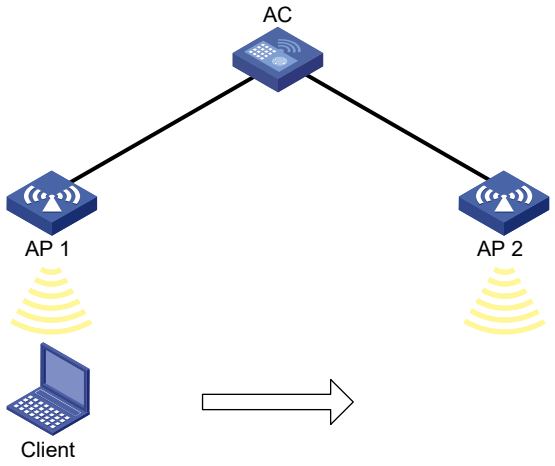


図 1-1 WLAN ローミングメカニズム

1.3 レイヤ3ローミング

図 1-2に示すように、クライアントは特別な設定なしで異なる VLAN の AP 間をローミングできます。ローミング手順については、本章の *“WLAN ローミングメカニズム”* を参照してください。

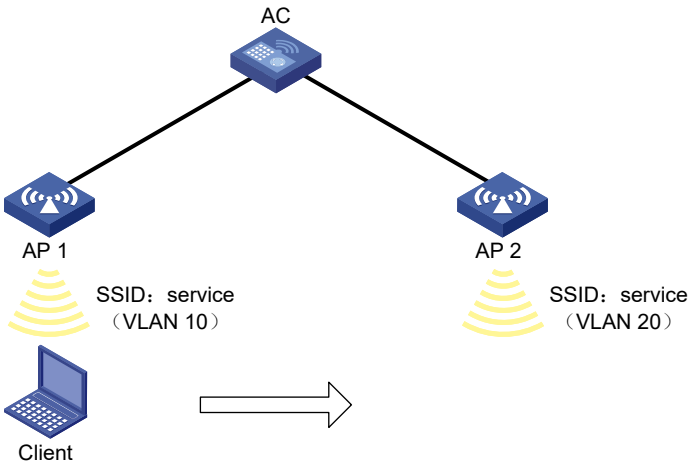


図 1-2 レイヤ 3 ローミング

1.4 ローミングエントリエージングタイムの設定

クライアントローミングエントリは、クライアント PMK、VLAN、およびその他の許可情報を記録します。切断されたクライアントがローミングエントリの期限が切れる前に AP に接続した場合、クライアントはエントリに記録された許可を継承し、高速ローミングを実現できます。

切断されたクライアントがエントリの期限が切れる前にオンラインになれない場合、システムはエントリを削除します。

エージングタイムは AC 内ローミングエントリでのみ使用でき、AC 間ローミングエントリには適用されません。

制約事項とガイドライン

ローミングエントリエージングタイムを 0 に設定すると、クライアントがオフラインになった時点で、システムはクライアントのローミングエントリを削除できます。高速ローミングはできません。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. service template view に移行にする	**wlan service-template** *service-template-name*	—
3. ローミングエントリエージングタイムを設定する	**client cache aging-time** *aging-time*	デフォルト：180秒

1.5 AC内ローミングの設定例

I. ネットワーク要件

図 1-3に示すように、AC 内ローミングを設定して、クライアントが AP1 から AP2 にローミングできるようにします。2 つの AP は同じ AC によって管理されます。

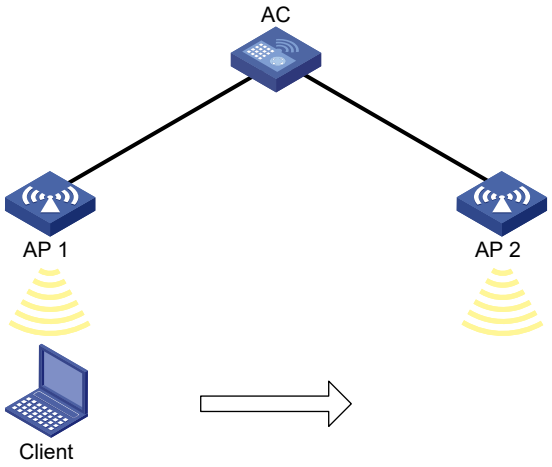


図 1-3 ネットワーク図

II. 設定手順

サービステンプレート **service** を作成し、SSID を 1 に設定し、サービステンプレートを有効にします。

```
<AC> system-view
[AC] wlan service-template service
[AC-wlan-st-service] ssid 1
[AC-wlan-st-service] service-template enable
[AC-wlan-st-service] quit
```

手動 AP **ap1** を作成し、AP モデルとシリアル ID を指定します。

```
[AC] wlan ap ap1 model QX-W1110
[AC-wlan-ap-ap1] serial-id 219801A28N819CE0002T
```

AP1 の radio1 に対してサービステンプレートを設定します。

```
[AC-wlan-ap-ap1] radio 1
[AC-wlan-ap-ap1-radio-1] radio enable
[AC-wlan-ap-ap1-radio-1] service-template service
[AC-wlan-ap-ap1-radio-1] quit
[AC-wlan-ap-ap1] quit
```

#手動 AP **ap2** を作成し、AP モデルとシリアル ID を指定します。

```
[AC] wlan ap ap2 model QX- W1110
[AC-wlan-ap-ap2] serial-id 219801A28N819CE0003T
```

AP2 の radio1 に対してサービステンプレートを設定します。

```
[AC-wlan-ap-ap2] radio 1
[AC-wlan-ap-ap2-radio-1] radio enable
[AC-wlan-ap-ap2-radio-1] service-template service
[AC-wlan-ap-ap2-radio-1] quit
[AC-wlan-ap-ap2] quit
```

III. 設定確認

クライアントが AP 1 からオンラインになるようにします。（詳細は省略します。）

クライアントが AP1 に関連付けられ、ローミングステータスは **N/A** であることを確認します。これは、クライアントがローミングを行っていないことを示します。

```
[AC] display wlan client verbose
Total number of clients: 1

MAC address                          : 9cd3-6d9e-6778
IPv4 address                         : 10.1.1.114
IPv6 address                         : N/A
Username                             : N/A
AID                                  : 1
AP ID                                : 1
AP name                              : ap1
Radio ID                             : 1
Channel                              : 36
SSID                                 : 1
BSSID                                : 000f-e200-4444
VLAN ID                              : 1
Sleep count                          : 242
Wireless mode                        : 802.11ac
Channel bandwidth                    : 80MHz
SM power save                        : Enabled
SM power save mode                   : Dynamic
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                   : Not supported
STBC TX capability                   : Not supported
LDPC RX capability                   : Not supported
SU beamformee capability             : Not supported
MU beamformee capability             : Not supported
Beamformee STS capability            : N/A
Block Ack                            : TID 0 In
Supported VHT-MCS set                : NSS1 0, 1, 2, 3, 4, 5, 6, 7, 8
                                       NSS2 0, 1, 2, 3, 4, 5, 6, 7, 8
Supported HT MCS set                 : 0, 1, 2, 3, 4, 5, 6, 7,
                                       8, 9, 10, 11, 12, 13, 14,
                                       15, 16, 17, 18, 19, 20,
                                       21, 22, 23
Supported rates                      : 6, 9, 12, 18, 24, 36,
                                       48, 54 Mbps
QoS mode                             : WMM
Listen interval                      : 10
RSSI                                 : 62
```

```
Rx/Tx rate                          : 130/11
Authentication method               : Open system
Security mode                       : PRE-RSNA
AKM mode                            : Not configured
Cipher suite                        : N/A
User authentication mode            : Bypass
Authorization ACL ID                : 3001(Not effective)
Authorization user profile          : N/A
Authorization CAR                   : N/A
Roam status                         : N/A
Key derivation                      : SHA1
PMF status                          : Enabled
Forward policy name                 : Not configured
Online time                         : 0days 0hours 1minutes 13seconds
FT status                           : Inactive
```

クライアントを AP2 にローミングします。（詳細は省略します。）

クライアントが AP2 に関連付けられ、ローミングステータスが **Intra-AC roam** であることを確認します。

[AC] display wlan client verbose

```
Total number of clients: 1

MAC address                         : 9cd3-6d9e-6778
IPv4 address                        : 10.1.1.114
IPv6 address                        : N/A
Username                            : N/A
AID                                 : 1
AP ID                               : 2
AP name                             : ap2
Radio ID                            : 1
Channel                             : 36
SSID                                : 1
BSSID                               : 000f-e203-7777
VLAN ID                             : 1
Sleep count                         : 242
Wireless mode                       : 802.11ac
Channel bandwidth                   : 80MHz
SM power save                       : Enabled
SM power save mode                  : Dynamic
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                  : Not supported
STBC TX capability                  : Not supported
LDPC RX capability                  : Not supported
SU beamformee capability            : Not supported
MU beamformee capability            : Not supported
Beamformee STS capability           : N/A
Block Ack                           : TID 0 In
Supported VHT-MCS set               : NSS1 0, 1, 2, 3, 4, 5, 6, 7, 8
                                      NSS2 0, 1, 2, 3, 4, 5, 6, 7, 8
Supported HT MCS set                : 0, 1, 2, 3, 4, 5, 6, 7,
                                      8, 9, 10, 11, 12, 13, 14,
                                      15, 16, 17, 18, 19, 20,
                                      21, 22, 23
Supported rates                     : 6, 9, 12, 18, 24, 36,
                                      48, 54 Mbps
QoS mode                            : WMM
Listen interval                     : 10
RSSI                                : 62
Rx/Tx rate                          : 130/11
Authentication method               : Open system
Security mode                       : PRE-RSNA
AKM mode                            : Not configured
Cipher suite                        : N/A
```

```
User authentication mode          : Bypass
Authorization ACL ID              : 3001(Not effective)
Authorization user profile        : N/A
Authorization CAR                 : N/A
Roam status                       : Intra-AC roam
Key derivation                    : SHA1
PMF status                        : Enabled
Forward policy name               : Not configured
Online time                       : 0days 0hours 5minutes 13seconds
FT status                         : Inactive
```

目次

このセクションのページは **10-x-x** です。

2章 拡張ローミング 2-1
2.1 拡張ローミング 2-1
2.2 802.1X高速ローミング 2-1
2.2.1 802.1X高速ローミングメカニズム 2-1
2.2.2 制限とガイドライン: 802.1 X高速転送設定 2-2
2.3 MAC高速ローミング 2-2
2.3.1 MAC高速ローミングメカニズム 2-2
2.3.2 制限とガイドライン: MAC高速転送 2-3
2.3.3 MAC認証されたAC内ローミングクライアントの高速接続の有効化 2-3
2.4 802.11rの設定 2-4
2.4.1 802.11r 2-4
2.4.2 802.11rの設定 2-5
2.4.3 モビリティドメインIDの設定 2-6
2.4.4 Over-the-air FTとPSK認証設定例 2-6
2.4.5 Over-the-air FTと802.1X認証設定例 2-10
2.5 802.11vの設定 2-14
2.5.1 802.11v 2-14
2.5.2 制限とガイドライン: 802.11v 設定 2-15
2.5.3 BTMの有効化 2-15
2.5.4 BTMアソシエーション解除の設定 2-15
2.5.5 802.11vの設定例 2-16
2.6 802.11kの設定 2-18
2.7 協調ローミング 2-18
2.7.1 協調ローミング 2-18
2.7.2 制限とガイドライン:協調ローミング設定 2-18
2.7.3 クライアントanti-stickyの設定 2-19
2.7.4 協調ローミングの表示と維持 2-19
2.8 802.11r設定例 2-20
2.8.1 Over-the-DS FTとPSK認証設定例 2-20
2.8.2 Over-the-DS FTと802.1X認証設定 2-24

2章 拡張ローミング

2.1 拡張ローミング

WLAN は、以下の拡張ローミングテクノロジーをサポートしています。

- **802.1X 高速ローミング**－ ユーザは再認証されることなく、新しい AP または無線からオンラインになることができます。RSN+802.1X 認証を使用する場合にのみ適用できます。
- **MAC 高速ローミング**－ ユーザは再認証されずに新しい AP または無線からオンラインになることができます。MAC アドレス認証を使用する場合にのみ適用されます。
- **802.11 r**－ ローミング遅延を短縮してクライアントの切断率を下げ、サービス品質を向上させます。
- **802.11 v**－ 802.11 v クライアントが最適な AP に接続してサービス品質を向上させるのに役立ちます。
- **協調ローミング**－ IEEE 802.11k、IEEE 802.11r、および IEEE 802.11v を使用して、ESS でのクライアントのシームレスなローミングをサポートします。

2.2 802.1X高速ローミング

2.2.1 802.1X 高速ローミングメカニズム

図 2-1に示すように、802.1X 高速ローミングは以下のように動作します。

1) クライアントは RSN+802.1X 認証を通過した後、AP1 からオンラインになります。AP 1 はクライアントのローミングエントリを作成します。
   802.1X 認証の詳細は、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*8 WLAN セキュリティ*”の”*1 章 WLAN セキュリティ*”を参照してください。
2) クライアントは AP2 にローミングします。AP はクライアントのローミングエントリを調べ、クライアントが AP と同じ PMKID を伝送している場合は 802.1X 高速転送をトリガします。
   システムはキャッシュされた PMK を使用して鍵 ネゴシエーションを実行し、クライアントは再認証なしで AP2 と関連付けることができます。

🕮 **メモ：**

システムは、以下の方法を使用して PMKID をキャッシュすることをサポートしています。

- **Sticky Key Caching (SKC)** －クライアントの 802.1 X 認証中に生成された PMKID を直接キャッシュします。
- **Opportunistic Key Caching (OKC)** －現在関連付けられている BSSID、クライアント MAC アドレス、およびキャッシュされた PMK を使用して PMKID を生成します。

どちらの方法も、手動による操作なしで 802.1X 高速ローミングをサポートします。

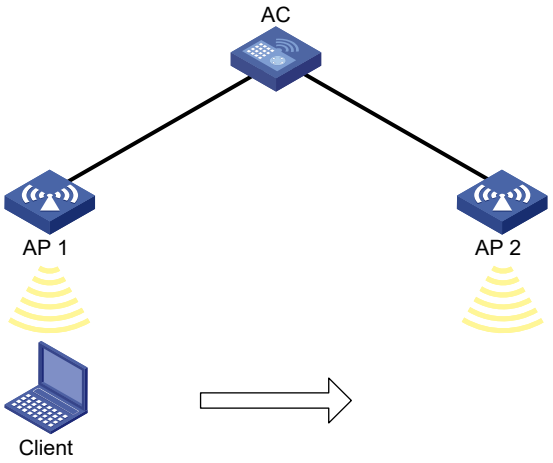


図 2-1 802.1X 高速ローミング

2.2.2 制限とガイドライン: 802.1 X 高速転送設定

802.1X 高速ローミングは、同じ AC によって管理される AP 間のローミングのみをサポートします。

2.3 MAC高速ローミング

2.3.1 MAC 高速ローミングメカニズム

図 2-2に示すように、MAC 高速ローミングは以下のように動作します。

1) クライアントは MAC アドレス認証を通過した後、AP1 からオンラインになります。AP1 はクライアントのローミングエントリを作成します。
MAC アドレス認証の詳細は、 QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*8 WLAN セキュリティ*”の”*1 章 WLAN セキュリティ*”を参照してください。
2) クライアントは AP2 にローミングします。AP2 はクライアントのローミングエントリを調べ、高速接続が有効な場合は MAC アドレス認証をトリガします。
クライアントは再認証されずに AP2 からオンラインになります。

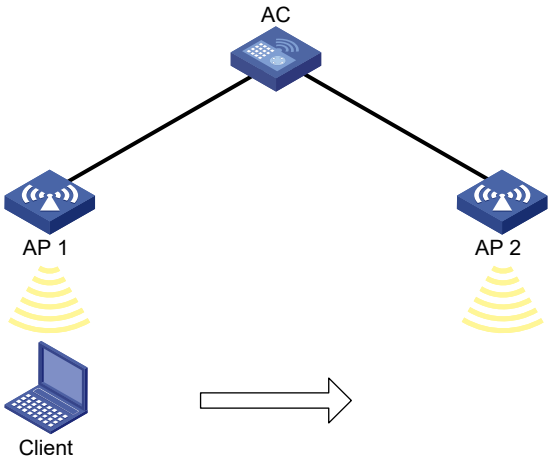


図 2-2 MAC 高速ローミング

2.3.2 制限とガイドライン: MAC 高速転送

802.1X 高速ローミングは、同じ AC で管理されている AP 間のローミングのみをサポートします。

2.3.3 MAC 認証された AC 内ローミングクライアントの高速接続の有効化

AC で一度認証された MAC アドレス認証ローミングクライアントが、再認証なしで AC に接続されたすべての AP からオンラインになることができます。

認証ロケーションとアソシエーションロケーションの両方が AC 上にある MAC アドレス認証無線クライアントにのみ適用されます。

MAC アドレス認証を使用し、専用の設定を必要とする AC 間ローミングクライアントの表示ローミング状態に影響します。

- クライアントが AC 間をローミングした場合、そのローミング状態は **display wlan client verbose** コマンドの出力で **N/A** になります。
- AC 間ローミングクライアントが異なる VLAN に属している場合は、同じローミンググループ内のすべての AC のアップストリームポートで、これらの VLAN からのトラフィックの通過が許可されていることを確認する必要があります。

サービステンプレートで設定する前に、そのサービステンプレートを無効にする必要があります。

以下に MAC 認証された AC 内ローミングクライアントの高速接続の有効化を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. Service template view に移行する	**wlan service-template** *service-template-name*	—

操作	コマンド	補足
3． MAC 認証された AC 内ローミングクライアントの高速接続を有効にする	**mac-authentication fast-connect enable**	デフォルト：有効

2.4 802.11rの設定

2.4.1 802.11r

802.11r FT（fast BSS transition）により、クライアントが同一 ESS 内の別の BSS にローミングする際、遅延が短縮されます。802.11r FT では、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 は無線メッセージ交換方式をサポートしており、クライアントはプレ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。

I. Over-the-air FT

図 2-3に示すように、クライアントは AP1 に関連付いています。Over-the-air FT を使用した AC 内ローミングは以下の手順で実行されます。

1) クライアントは AP1 に関連付いています。
2) クライアントは AP2 に FT 認証要求を送信します。
3) AP2 は FT 認証応答をクライアントに送信します。
4) クライアントは AP2 に再関連付け要求を送信します。
5) AP2 はクライアントに再関連付け応答を送信します。
6) クライアントは AP2 にローミングします。

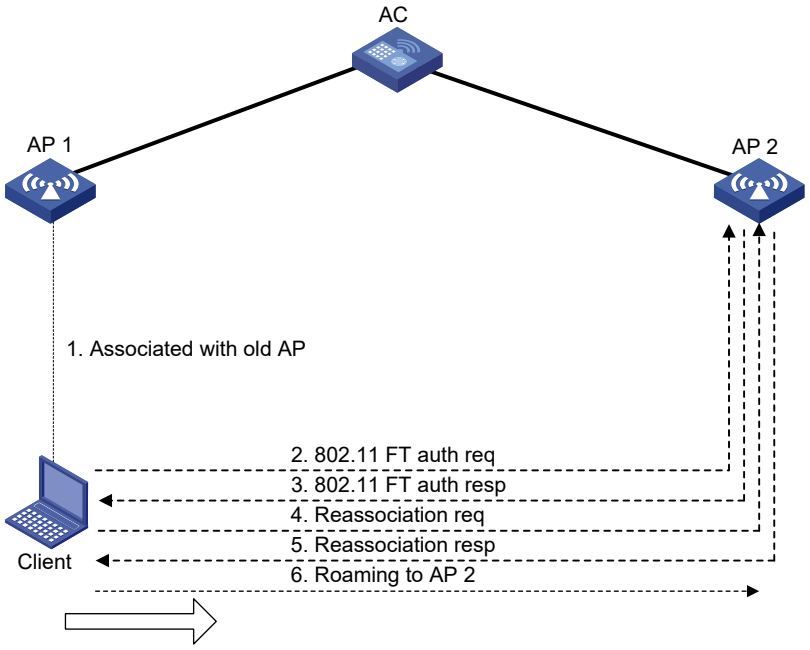


図 2-3 Over-the-air FT を使用した AC 内ローミング

2.4.2 802.11r の設定

802.11r を設定する際、以下の制限とガイドラインに従ってください。

- FT をサポートしていないクライアントが WLAN にアクセスできるようにするには、SSID 名が同じ 2 つのサービステンプレートを作成し、一方のサービステンプレートで FT を有効にし、もう一方では FT を無効にしてください。
- 定期再認証タイマが終了するたびにクライアントがオンラインになることを防ぐために、FT と 802.1X 定期再認証を同じサービステンプレートに対して有効にしないでください。
- PTK アップデートは FT を使用して WLAN にアクセスしているクライアントにはサポートされません。
- FT を使用するには、AKM モードも指定する必要があります。
- 802.11r を使用するには、AP から送信されるビーコンおよびプローブ応答に RSN IE が搭載されていること、Cipher スイートが CCMP であること、およびローカル認証が使用されていないことを確認します。
- 802.11r は、現在のソフトウェアバージョンでは AC 内ローミングのみをサポートしています。
- 802.11r は、AC に関連付けられたクライアントでのみ有効です。
- 802.11r を設定するには、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ます。
- 802.11r FT を有効にしないで、WPA 3 セキュリティモードを設定するか、拡張オープンシステム認証を同時に有効にします。有効にすると、サービステンプレートを有効にできません。

802.11r の設定方法を以下に示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． Service template view に移行する	**wlan service-template** *service-template-name*	―
3． FT を有効にする	**ft enable**	デフォルト：無効 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。
4． （オプション設定項目）再関連付けタイムアウトタイマを設定する	**ft reassociation-timeout** *timeout*	デフォルト：20秒 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。

🕮 **メモ：**

認証機能の詳細は、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*8 WLAN セキュリティ*”の”*1 章 WLAN セキュリティ*”を参照してください。

2.4.3 モビリティドメイン ID の設定

クライアントが異なる AP 間を移動するときに、クライアントのアクセス時間を短縮するには、この機能を設定します。

この機能を設定すると、クライアントは、2 つの AP が同じモビリティドメイン ID を持つ場合に限り、802.11r FT(fast BSS transition) を介して異なる AP 間をローミングできます。

クライアントが、FT が有効なっていてもモビリティグループに含まれていない AP 間を移動する場合、クライアントは AP 間の FT ローミングを使用する場合があります。ただし、AP は同じモビリティグループに属していないため、ローミングは失敗します。次に、クライアントはアソシエーションを使用して新しい AP に切り替えます。

AP に異なるモビリティドメイン ID を設定することで、クライアントは AP 間の FT ローミングを試行せずに新しい AP に直接関連付けができるようになります。その結果、AP 間の FT ローミング処理が省略されるため、サービス切り替え時間が短縮されます。

サービステンプレートを有効にする前に、この機能を設定します。この機能は、FT が有効の場合にだけ有効です。

モビリティドメイン ID の設定方法を以下に示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． Service template view に移行する	**wlan service-template** *service-template-name*	―
3． モビリティドメイン ID を設定する	**ft mobility-domain-id** *mobility-domain-id*	デフォルト：設定なし

2.4.4 Over-the-air FT と PSK 認証設定例

I. ネットワーク要件

図 2-4に示すように、クライアントが AP1 と AP2 間でローミングできるように Over-the-air FT を使用した AC 内ローミングを設定します。認証および鍵管理モードを PSK に設定します。

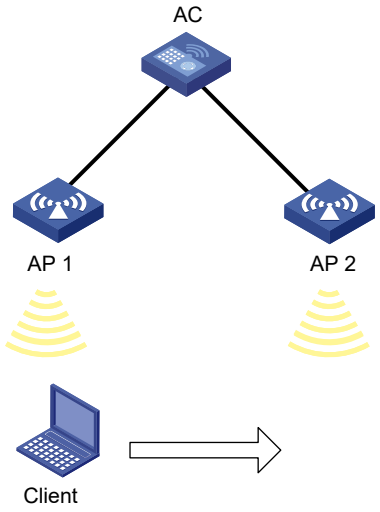


図 2-4 ネットワーク図

II. 設定手順

サービステンプレート **acstname** を作成します。

```
<AC> system-view
[AC] wlan service-template acstname
```

SSID を **service** に設定します。

```
[AC-wlan-st-acstname] ssid service
```

認証および鍵管理モードを **PSK** に設定し、単純な文字列 **12345678** を PSK として設定します。

```
[AC-wlan-st-acstname] akm mode psk
[AC-wlan-st-acstname] preshared-key pass-phrase simple 12345678
```

ビーコンおよびプローブ応答で RSN IE を有効にします。

```
[AC-wlan-st-acstname] cipher-suite ccmp
[AC-wlan-st-acstname] security-ie rsn
```

FT を有効にします。

```
[AC-wlan-st-acstname] ft enable
```

再関連付けタイムアウトタイマを 50 秒に設定します。

```
[AC-wlan-st-acstname] ft reassociation-timeout 50
```

サービステンプレートを有効にします。

```
[AC-wlan-st-acstname] service-template enable
[AC-wlan-st-acstname] quit
```

AP1 を作成し、AP の radio1 にサービステンプレート **acstname** を設定します。

```
[AC] wlan ap 1 model QX-W1110
[AC-wlan-ap-1] serial-id 219801A28N819CE0002T
[AC-wlan-ap-1] radio 1
[AC-wlan-ap-1-radio-1] service-template acstname
[AC-wlan-ap-1-radio-1] radio enable
[AC-wlan-ap-1-radio-1] quit
[AC-wlan-ap-1] quit
```

AP2 を作成し、AP の radio1 にサービステンプレート **acstname** を設定します。

```
[AC] wlan ap 2 model QX-W1110
[AC-wlan-ap-2] serial-id 219801A28N819CE0003T
[AC-wlan-ap-2] radio 1
[AC-wlan-ap-2-radio-1] service-template acstname
[AC-wlan-ap-2-radio-1] radio enable
[AC-wlan-ap-2-radio-1] quit
[AC-wlan-ap-2] quit
```

III. 設定確認

以下の情報を確認します。

- RSN IE が有効。
- AKM モードが **PSK**。
- Cipher スイートが **CCMP**。
- FT 状態が **Active**。

```
[AC] display wlan client verbose
Total number of clients: 1

MAC address                          : fc25-3f03-8361
IPv4 address                         : 10.1.1.114
IPv6 address                         : N/A
Username                             : N/A
AID                                  : 1
AP ID                                : 1
AP name                              : 1
Radio ID                             : 1
SSID                                 : service
BSSID                                : 000f-e266-7788
VLAN ID                              : 1
Sleep count                          : 242
Wireless mode                        : 802.11ac
Channel bandwidth                    : 80MHz
SM power save                        : Enabled
SM power save mode                   : Dynamic
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                   : Not supported
STBC TX capability                   : Not supported
LDPC RX capability                   : Not supported
```

```
SU beamformee capability          : Not supported
MU beamformee capability          : Not supported
Beamformee STS capability         : N/A
Block Ack                         : TID 0 In
Supported VHT-MCS set             : NSS1 0, 1, 2, 3, 4, 5, 6, 7, 8
                                    NSS2 0, 1, 2, 3, 4, 5, 6, 7, 8
Supported HT MCS set              : 0, 1, 2, 3, 4, 5, 6, 7,
                                    8, 9, 10, 11, 12, 13, 14,
                                    15, 16, 17, 18, 19, 20,
                                    21, 22, 23
Supported rates                   : 6, 9, 12, 18, 24, 36,
                                    48, 54 Mbps
QoS mode                          : WMM
Listen interval                   : 10
RSSI                              : 62
Rx/Tx rate                        : 130/11
Authentication method             : Open system
Security mode                     : RSN
AKM mode                          : PSK
Encryption cipher                 : CCMP
User authentication mode          : Bypass
Authorization ACL ID              : 3001(Not effective)
Authorization user profile        : N/A
Authorization CAR                 : N/A
Roam status                       : N/A
Key derivation                    : SHA1
PMF status                        : Enabled
Forward policy name               : Not configured
Online time                       : 0days 0hours 1minutes 13seconds
FT status                         : Active
BTM status                        : Disabled
```

クライアントを AP2 のカバレッジに移動します（詳細は省略します）。

認証方式が **FT** で、ローミング状態が **Intra-AC roam** であることを確認します。

[AC] display wlan client verbose

```
Total number of clients: 1

MAC address                       : fc25-3f03-8361
IPv4 address                      : 10.1.1.114
IPv6 address                      : N/A
Username                          : N/A
AID                               : 1
AP ID                             : 2
AP name                           : 2
Radio ID                          : 1
SSID                              : service
BSSID                             : 000f-e211-2233
VLAN ID                           : 1
Sleep count                       : 242
Wireless mode                     : 802.11ac
Channel bandwidth                 : 80MHz
SM power save                     : Enabled
SM power save mode                : Dynamic
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                : Not supported
STBC TX capability                : Not supported
LDPC RX capability                : Not supported
SU beamformee capability          : Not supported
MU beamformee capability          : Not supported
Beamformee STS capability         : N/A
Block Ack                         : TID 0 In
Supported VHT-MCS set             : NSS1 0, 1, 2, 3, 4, 5, 6, 7, 8
                                    NSS2 0, 1, 2, 3, 4, 5, 6, 7, 8
Supported HT MCS set              : 0, 1, 2, 3, 4, 5, 6, 7,
```

```
                                    8, 9, 10, 11, 12, 13, 14,
                                    15, 16, 17, 18, 19, 20,
                                    21, 22, 23
Supported rates                   : 6, 9, 12, 18, 24, 36,
                                    48, 54 Mbps
QoS mode                          : WMM
Listen interval                   : 10
RSSI                              : 62
Rx/Tx rate                        : 130/11
Authentication method             : FT
Security mode                     : RSN
AKM mode                          : PSK
Encryption cipher                 : CCMP
User authentication mode          : Bypass
Authorization ACL ID              : 3001(Not effective)
Authorization user profile        : N/A
Authorization CAR                 : N/A
Roam status                       : Intra-AC roam
Key derivation                    : SHA1
PMF status                        : Enabled
Forward policy name               : Not configured
Online time                       : 0days 0hours 5minutes 13seconds
FT status                         : Active
BTM status                        : Disabled
```

2.4.5 Over-the-air FT と 802.1X 認証設定例

I. ネットワーク要件

図 2-4に示すように、クライアントが AP1 と AP2 間でローミングできるように Over-the-air FT を使用した AC 内ローミングを設定します。認証および鍵管理モードを 802.1X に設定します。

II. 設定手順

サービステンプレート **acstname** を作成します。

```
<AC> system-view
[AC] wlan service-template acstname
```

SSID を **service** に設定します。

```
[AC-wlan-st-acstname] ssid service
```

akm モードを 802.1X に設定します。

```
[AC-wlan-st-acstname] akm mode dot1x
```

ビーコンおよびプローブ応答で RSN IE を有効にします。

```
[AC-wlan-st-acstname] cipher-suite ccmp
[AC-wlan-st-acstname] security-ie rsn
```

クライアントに対する認証モードを 802.1X に設定します。

```
[AC-wlan-st-acstname] client-security authentication-mode dot1x
[AC-wlan-st-acstname] dot1x domain imc
```

FT を有効にします。

```
[AC-wlan-st-acstname] ft enable
```

サービステンプレートを有効にします。

```
[AC-wlan-st-acstname] service-template enable
[AC-wlan-st-acstname] quit
```

802.1X 認証モードを EAP に設定します。

```
[AC] dot1x authentication-method eap
```

RADIUS スキーム **imcc** を作成します。

```
[AC] radius scheme imcc
```

プライマリ認証とアカウンティングサーバの IP アドレスを **10.1.1.3** に設定します。

```
[AC-radius-imcc] primary authentication 10.1.1.3
[AC-radius-imcc] primary accounting 10.1.1.3
```

認証とアカウンティングサーバとパケットを交換できるように、AC に共有鍵 **12345678** を設定します。

```
[AC-radius-imcc] key authentication simple 12345678
[AC-radius-imcc] key accounting simple 12345678
```

RADIUS サーバに送信するユーザ名から ISP ドメイン名を外すように設定します。

```
[AC-radius-imcc] user-name-format without-domain
[AC-radius-imcc] quit
```

ISP ドメイン **imc** を作成し、RADIUS スキーム **imcc** を認証、許可、アカウンティングに使用するためにドメインを設定します。

```
[AC] domain imc
[AC-isp-imc] authentication lan-access radius-scheme imcc
[AC-isp-imc] authorization lan-access radius-scheme imcc
[AC-isp-imc] accounting lan-access radius-scheme imcc
[AC-isp-imc] quit
```

AP1 を作成し、AP の radio1 にサービステンプレート **acstname** を設定します。

```
[AC] wlan ap 1 model QX-W1110
[AC-wlan-ap-1] serial-id 219801A28N819CE0002T
[AC-wlan-ap-1] radio 1
[AC-wlan-ap-1-radio-1] service-template acstname
[AC-wlan-ap-1-radio-1] radio enable
[AC-wlan-ap-1-radio-1] quit
[AC-wlan-ap-1] quit
```

AP2 を作成し、AP の radio1 にサービステンプレート **acstname** を設定します。

```
[AC] wlan ap 2 model QX-W1110
[AC-wlan-ap-2] serial-id 219801A28N819CE0003T
[AC-wlan-ap-2] radio 1
[AC-wlan-ap-2-radio-1] service-template acstname
[AC-wlan-ap-2-radio-1] radio enable
[AC-wlan-ap-2-radio-1] quit
[AC-wlan-ap-2] quit
```

III. 設定確認

以下の情報を確認します。

- RSN IE が有効。
- AKM モードが **802.1X**。
- Cipher スイートが **CCMP**。
- FT 状態が **Active**。

```
[AC] display wlan client verbose
Total number of clients: 1

MAC address                          : fc25-3f03-8361
IPv4 address                         : 10.1.1.114
IPv6 address                         : N/A
Username                             : N/A
AID                                  : 1
AP ID                                : 1
AP name                              : 1
Radio ID                             : 1
SSID                                 : service
BSSID                                : 000f-e266-7788
VLAN ID                              : 1
Sleep count                          : 242
Wireless mode                        : 802.11ac
Channel bandwidth                    : 80MHz
SM power save                        : Enabled
SM power save mode                   : Dynamic
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                   : Not supported
STBC TX capability                   : Not supported
LDPC RX capability                   : Not supported
SU beamformee capability             : Not supported
MU beamformee capability             : Not supported
Beamformee STS capability            : N/A
Block Ack                            : TID 0 In
Supported VHT-MCS set                : NSS1 0, 1, 2, 3, 4, 5, 6, 7, 8
                                       NSS2 0, 1, 2, 3, 4, 5, 6, 7, 8
Supported HT MCS set                 : 0, 1, 2, 3, 4, 5, 6, 7,
                                       8, 9, 10, 11, 12, 13, 14,
                                       15, 16, 17, 18, 19, 20,
                                       21, 22, 23
Supported rates                      : 6, 9, 12, 18, 24, 36,
                                       48, 54 Mbps
QoS mode                             : WMM
Listen interval                      : 10
```

```
RSSI                                : 62
Rx/Tx rate                          : 130/11
Authentication method               : Open system
Security mode                       : RSN
AKM mode                            : 802.1X
Encryption cipher                   : CCMP
User authentication mode            : 802.1X
Authorization ACL ID                : 3001(Not effective)
Authorization user profile          : N/A
Authorization CAR                   : N/A
Roam status                         : N/A
Key derivation                      : SHA1
PMF status                          : Enabled
Forward policy name                 : Not configured
Online time                         : 0days 0hours 1minutes 13seconds
FT status                           : Active
BTM status                          : Disabled
```

クライアントを AP2 のカバレッジに移動します（詳細は省略します）。

認証方法が **FT** で、ローミング状態が **Intra-AC roam** であることを確認します。

[AC] display wlan client verbose

```
Total number of clients: 1

MAC address                         : fc25-3f03-8361
IPv4 address                        : 10.1.1.114
IPv6 address                        : N/A
Username                            : N/A
AID                                 : 1
AP ID                               : 2
AP name                             : 2
Radio ID                            : 1
SSID                                : service
BSSID                               : 000f-e211-2233
VLAN ID                             : 1
Sleep count                         : 242
Wireless mode                       : 802.11ac
Channel bandwidth                   : 80MHz
SM power save                       : Enabled
SM power save mode                  : Dynamic
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                  : Not supported
STBC TX capability                  : Not supported
LDPC RX capability                  : Not supported
SU beamformee capability            : Not supported
MU beamformee capability            : Not supported
Beamformee STS capability           : N/A
Block Ack                           : TID 0 In
Supported VHT-MCS set               : NSS1 0, 1, 2, 3, 4, 5, 6, 7, 8
                                      NSS2 0, 1, 2, 3, 4, 5, 6, 7, 8
Supported HT MCS set                : 0, 1, 2, 3, 4, 5, 6, 7,
                                      8, 9, 10, 11, 12, 13, 14,
                                      15, 16, 17, 18, 19, 20,
                                      21, 22, 23
Supported rates                     : 6, 9, 12, 18, 24, 36,
                                      48, 54 Mbps
QoS mode                            : WMM
Listen interval                     : 10
RSSI                                : 62
Rx/Tx rate                          : 130/11
Authentication method               : FT
Security mode                       : RSN
AKM mode                            : 802.1X
Encryption cipher                   : CCMP
User authentication mode            : 802.1X
```

```
Authorization ACL ID                : 3001(Not effective)
Authorization user profile          : N/A
Authorization CAR                   : N/A
Roam status                         : Intra-AC roam
Key derivation                      : SHA1
PMF status                          : Enabled
Forward policy name                 : Not configured
Online time                         : 0days 0hours 5minutes 13seconds
FT status                           : Active
BTM status                          : Disabled
```

2.5 802.11vの設定

2.5.1 802.11v

802.11v は BSS 移行管理 (BTM) を定義しており、接続中の AP の信号強度が低い場合や、より信号強度の優れた 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。

図 2-5に示すように、BTM は以下のように動作します。

1) 現在関連付けられている AP の RSSI が低すぎるか、クライアントがより適切な AP を検出した場合、クライアントは関連付けられている AP に BTM query を送信します。BTM query を受信すると、AP は BTM request で応答します。
   BTM request には、推奨される BSS に関する情報が含まれます。
2) BTM request を受信すると、クライアントは現在接続している AP から切断して推奨される AP にローミングするかどうかを決定します。
3) クライアントがローミングを実行することを決定すると、BTM response を AP に送信します。クライアントがアソシエーション解除タイマの期限内に現在の BSS から移行できない場合、AP はクライアントに Disassociation request を送信し、クライアントをログオフします。

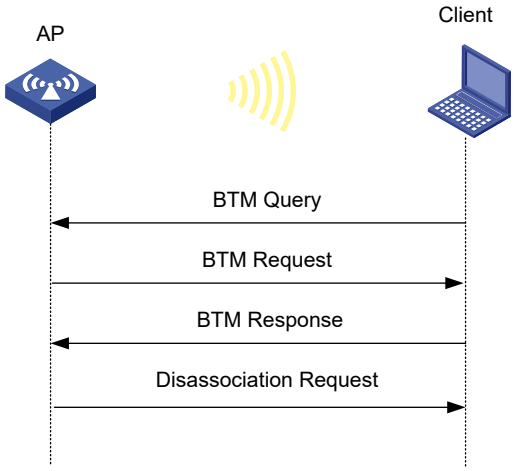


図 2-5 BSS 移行

2.5.2 制限とガイドライン: 802.11v 設定

802.11v は、現在のソフトウェアバージョンでは AC 内ローミングのみをサポートしています。

2.5.3 BTM の有効化

BTM を設定する際、以下の制限とガイドラインに従ってください。

- 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。
- BTM がすべてのクライアントで有効になるようにするには、**bss transition-management disassociation** コマンドを使用して BTM の関連付けを有効にします。

以下に BTM の有効化を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. Service template view に移行する	**wlan service-template** *service-template-name*	—
3. BTM を有効にする	**bss transition-management enable**	デフォルト：無効

2.5.4 BTM アソシエーション解除の設定

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 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。強制 BTM のアソシエーション解除が設定されている場合、AP はクライアントのアソシエーション解除タイマが期限切れになる前に、現在の BSS を離れることができなかった場合、クライアントを強制的にログオフします。

強制的な BTM のアソシエーションを解除すると、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。

BTM のアソシエーションを有効にするには、まず BTM を有効にします。

以下に BTM アソシエーション解除の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． Service template view に移行する	**wlan service-template** *service-template-name*	—
3． BTM アソシエーション解除を有効にし、強制解除を設定する	**bss transition-management disassociation** { **forced** | **recommended** } [**timer** *time*]	デフォルト：**recommended** アソシエーション解除のタイムアウトは90秒です。

2.5.5 802.11v の設定例

I. ネットワーク要件

図 2-6に示すように、AP に 802.11v を設定して、クライアントを最適な AP に誘導します。

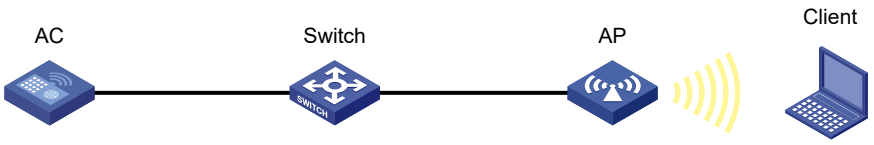


図 2-6 ネットワーク図

II. 設定手順

サービス テンプレート **service** を作成します。

```
<AC> system-view
[AC] wlan service-template service
```

SSID を **service** に設定します。

```
[AC-wlan-st-service] ssid service
```

BTM を有効にします。

```
[AC-wlan-st-service] bss transition-management enable
```

BTM アソシエーション解除タイムアウトを 45 秒に指定します。

```
[AC-wlan-st-service] bss transition-management disassociation recommended timer 45
```

サービス テンプレートを有効にします。

```
[AC-wlan-st-service] service-template enable
[AC-wlan-st-service] quit
```

AP **ap1** を作成し、AP モデルとシリアル ID を指定して AP が BSS 候補情報を取得できるようにし、サービス テンプレート **service** を AP **ap1** の radio1 に設定します。

```
[AC] wlan ap ap1 model QX-W1110
[AC-wlan-ap-ap1] serial-id 219801A28N819CE0002T
[AC-wlan-ap-ap1] radio 1
[AC-wlan-ap-ap1-radio-1] service-template service
[AC-wlan-ap-ap1-radio-1] radio enable
[AC-wlan-ap-ap1-radio-1] quit
[AC-wlan-ap-ap1] quit
```

III. 設定の確認

BTM が有効になっていることを確認します。

```
[AC] display wlan service-template service verbose
Service template name         : service
Description                   : Not configured
SSID                          : service
SSID-hide                     : Disabled
User-isolation                : Disabled
Service template status       : Disabled
Maximum clients per BSS       : Not configured
Frame format                  : Dot3
Seamless roam status          : Disabled
Seamless roam RSSI threshold : 50
Seamless roam RSSI gap        : 20
VLAN ID                       : 1
AKM mode                      : Not configured
Security IE                   : Not configured
Cipher suite                  : Not configured
TKIP countermeasure time      : 0 sec
PTK lifetime                  : 43200 sec
PTK rekey                     : Enabled
GTK rekey                     : Enabled
GTK rekey method              : Time-based
GTK rekey time                : 86400 sec
GTK rekey client-offline      : Disabled
WPA3 status                   : Disabled
PPSK                          : Disabled
PPSK Fail Permit              : 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                  : Not configured
802.1X handshake              : Disabled
802.1X handshake secure       : Disabled
802.1X domain                 : Not configured
MAC-auth domain               : Not configured
Max 802.1X users per BSS      : 512
Max MAC-auth users per BSS    : 512
802.1X re-authenticate        : Disabled
Authorization fail mode       : Online
Accounting fail mode          : Online
Authorization                 : Permitted
Key derivation                : SHA1
PMF status                    : Disabled
```

```
Hotspot policy number        : Not configured
Forwarding policy status     : Disabled
Forwarding policy name       : Not configured
Forwarder                    : AC
FT status                    : Disabled
QoS trust                    : Port
QoS priority                 : 0
BTM status                   : Enabled
```

クライアントがオンラインになったことを確認します。

```
<AC> display wlan client
Total number of clients: 3

MAC address    Username            AP name               R IP address      VLAN
4581-61ac-885a N/A                  ap1                   1 192.168.66.230  1
```

AP がクライアントに最適な AP を推奨してから 45 秒後に、クライアントがログオフされたことを確認します（詳細は省略します）。

2.6 802.11kの設定

オペレーションマニュアルのセクション 9 無線管理の“*WLAN 無線リソースの計測の設定*”の”*802.11k 計測*”を参照してください。

2.7 協調ローミング

2.7.1 協調ローミング

協調ローミングは、IEEE 802.11k、IEEE 802.11r、および IEEE 802.11v を使用して、ESS で無線クライアントの AP および無線クライアントガイド付きローミングを提供するために、NEC によって定義されています。

- 802.11k はビーコン無線測定を定義しており、2.4 GHz と 5 GHz の両方のチャネルでチャネル品質とリソースパフォーマンスを監視できます。
- 802.11r は、クライアントのローミング中の伝送遅延を短縮し、切断率を減らしてローミングサービスの品質を向上させる Fast BSS Transition (FT) を定義しています。
- 802.11v は、802.11v クライアントを最適な AP に導く BSS Transition Management (BTM) を定義し、アクセスサービスの品質を向上させます。

協調ローミングは、AP を使用して 802.11v クライアントの信号強度を監視することもサポートしており、クライアントをより優れたサービスに積極的に導くことができます。

2.7.2 制限とガイドライン:協調ローミング設定

現在のソフトウェアバージョンでは、協調ローミングは AC 内ローミングのみをサポートしています。

協調ローミングを使用するには、AP が Wi-Fi 6 をサポートしていることを確認します。

2.7.3 クライアント anti-sticky の設定

クライアント anti-sticky を設定すると、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。

ACL ベースのクライアントの sticky 対策は、クライアントの sticky 対策が有効になっている場合にのみ有効になります。

1 つの無線にバインドできる ACL ルールは 1 つだけです。

display wlan client verbose コマンドを使用してクライアント RSSI を表示し、RSSI に基づいて ACL ベースのクライアント anti-sticky を設定できます。

I. ap view でのクライアント anti-sticky の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． ap view に移行する	**wlan ap** *ap-name*	―
3． radio view に移行する	**radio** *radio-id*	―
4． クライアント anti-sticky を設定する	**sacp anti-sticky** { **disable** | **enable** [**rssi** *rssi-value*] [**interval** *interval*] [**forced-logoff**] }	デフォルト：AP group viewの設定を使用します。

II. ap group view でのクライアント anti-sticky の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． ap group view に移行する	**wlan ap-group** *group-name*	―
3． ap model-view に移行する	**ap-model** *ap-model*	―
4． radio view に移行する	**radio** *radio-id*	―
5． クライアント anti-sticky を設定する	**sacp anti-sticky** { **disable** | **enable** [**rssi** *rssi-value*] [**interval** *interval*] [**forced-logoff**] }	デフォルト：有効

2.7.4 協調ローミングの表示と維持

すべての view で display コマンドを実行できます。

操作	コマンド
指定したAPまたはすべてのAPの実行中の設定を表示する	**display wlan ap** { **all** | **name** *ap-name* } **running-configuration** [**verbose**]
クライアント情報を表示する	**display wlan client** [**ap** *ap-name* [**radio** *radio-id*] | **mac-address** *mac-address* | **service-template** *service-template-name* | **frequency-band** { **2.4** | **5** }] [**verbose**]
サービステンプレート情報を表示する	**display wlan service-template** [*service-template-name*] [**verbose**]

メモ：

display wlan service-template および **display wlan client** コマンドの詳細は、QX-W2300AC シリーズアクセスコントローラコマンドマニュアルの“*6 WLAN アクセス*”の”*1 章 WLAN アクセス*”を参照してください。

2.8 802.11r設定例

2.8.1 Over-the-DS FT と PSK 認証設定例

I. ネットワーク要件

図 2-7に示すように、クライアントが AP1 と AP2 間でローミングできるように Over-the-DS FT を使用した AC 内ローミングを設定します。akm(authentication and key management)モードを PSK に設定します。

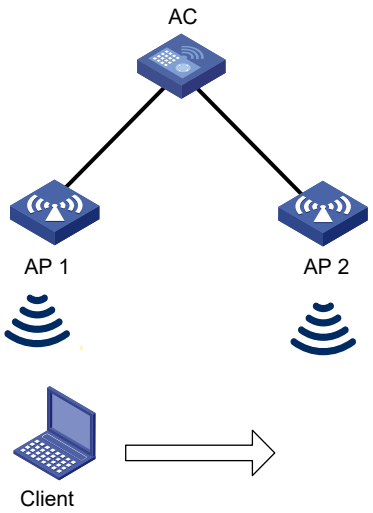


図 2-7 ネットワーク図

II. 設定手順

サービステンプレート **acstname** を作成します。

```
<AC> system-view
[AC] wlan service-template acstname
```

SSID を **service** に設定します。

```
[AC-wlan-st-acstname] ssid service
```

akm モードを PSK に設定し、事前共有鍵を 12345678 に設定します。

```
[AC-wlan-st-acstname] akm mode psk
[AC-wlan-st-acstname] preshared-key pass-phrase simple 12345678
```

cipher スイートを CCMP に設定し、セキュリティ IE を RSN に設定します。

```
[AC-wlan-st-acstname] cipher-suite ccmp
[AC-wlan-st-acstname] security-ie rsn
```

FT を有効にします。

```
[AC-wlan-st-acstname] ft enable
```

再関連付けタイムアウトタイマを 50 秒に設定します。

```
[AC-wlan-st-acstname] ft reassociation-timeout 50
```

FT の方法を Over-the-DS に設定します。

```
[AC-wlan-st-acstname] ft method over-the-ds
```

サービステンプレートを有効にします。

```
[AC-wlan-st-acstname] service-template enable
[AC-wlan-st-acstname] quit
```

AP1 の radio2 に対してサービステンプレート **acstname** を設定します。

```
[AC] wlan ap 1
[AC-wlan-ap-1] radio 2
[AC-wlan-ap-1-radio-2] service-template acstname
[AC-wlan-ap-1-radio-2] radio enable
[AC-wlan-ap-1-radio-2] quit
[AC-wlan-ap-1] quit
```

AP2 の radio2 に対してサービステンプレート **acstname** を設定します。

```
[AC] wlan ap 2
[AC-wlan-ap-2] radio 2
[AC-wlan-ap-2-radio-2] service-template acstname
[AC-wlan-ap-2-radio-2] radio enable
[AC-wlan-ap-2-radio-2] quit
[AC-wlan-ap-2] quit
```

III. 設定確認

サービステンプレートが正しく設定されていることを確認します。

```
[AC] display wlan service-template acstname verbose
Service template name        : acstname
SSID                         : service
```

```
SSID-hide                     : Disabled
User-isolation                : Disabled
Service template status       : Enabled
Maximum clients per BSS       : Not configured
Frame format                  : Dot3
Seamless-roam                 : Disabled
Seamless-roam RSSI threshold : 50
Seamless-roam RSSI gap        : 20
VLAN ID                       : 1
AKM mode                      : PSK
Security IE                   : RSN
Cipher suite                  : CCMP
TKIP countermeasure time      : 0 sec
PTK lifetime                  : 43200 sec
GTK rekey                     : Enabled
GTK rekey method              : Time-based
GTK rekey time                : 86400 sec
GTK rekey client-offline      : Disabled
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                  : Not configured
802.1X handshake              : Disabled
802.1X handshake secure       : Disabled
802.1X domain                 : Not configured
MAC-auth domain               : Not configured
Max 802.1X users              : 4096
Max MAC-auth users            : 4096
802.1X re-authenticate        : Disabled
Authorization fail mode       : Online
Accounting fail mode          : Online
Authorization                 : Permitted
Key derivation                : SHA1
PMF status                    : Disabled
Hotspot policy number         : Not configured
Forward policy                : Not configured
Forwarder                     : AC
FT Status                     : Enable
FT Method                     : over-the-ds
FT Reassociation Deadline     : 50 sec
QoS trust                     : Port
QoS priority                  : 0
```

ローミング状態が N/A で、FT 状態が Active であることを確認します。

[AC] display wlan client verbose

```
Total number of clients: 1

MAC address                          : fc25-3f03-8361
IPv4 address                         : 10.1.1.114
IPv6 address                         : N/A
Username                             : N/A
AID                                  : 1
AP ID                                : 1
AP name                              : 1
Radio ID                             : 2
SSID                                 : service
BSSID                                : 000f-e266-7788
VLAN ID                              : 1
Power save mode                      : Active
Wireless mode                        : 802.11gn
Channel bandwidth                    : 20MHz
SM power save                        : Enabled
SM power save mode                   : Static
Short GI for 20MHz                   : Not supported
Short GI for 40MHz                   : Not supported
STBC RX capability                   : Supported
STBC TX capability                   : Not supported
```

```
Support HT-MCS set                : 0, 1, 2, 3, 4, 5, 6, 7
QoS mode                          : WMM
Listen interval                   : 20
RSSI                              : 0
Rx/Tx rate                        : 65/65
Authentication method             : Open system
Security mode                     : RSN
AKM mode                          : PSK
Encryption cipher                 : CCMP
User authentication mode          : Bypass
Authorization ACL ID              : N/A
Authorization user profile        : N/A
Roam status                       : N/A
Key derivation                    : SHA256
PMF status                        : N/A
Forward policy                    : N/A
Online time                       : 0hr 0min 41sec
FT status                         : Active
```

クライアントを AP2 にローミングさせます（詳細は省略します）。

認証方式が FT で、ローミング状態が Intra-AC roam であることを確認します。

[AC] display wlan client verbose

```
Total number of clients: 1

 MAC address                      : fc25-3f03-8361
 IPv4 address                     : 10.1.1.114
 IPv6 address                     : N/A
 Username                         : N/A
 AID                              : 1
 AP ID                            : 2
 AP name                          : 2
 Radio ID                         : 2
 SSID                             : service
 BSSID                            : 000f-e211-2233
 VLAN ID                          : 1
 Power save mode                  : Active
 Wireless mode                    : 802.11gn
 Channel bandwidth                : 20MHz
 SM power save                    : Enabled
 SM power save mode               : Static
 Short GI for 20MHz               : Not supported
 Short GI for 40MHz               : Not supported
 STBC RX capability               : Supported
 STBC TX capability               : Not supported
 Support HT-MCS set               : 0, 1, 2, 3, 4, 5, 6, 7
 QoS mode                         : WMM
 Listen interval                  : 20
 RSSI                             : 0
 Rx/Tx rate                       : 0/0
 Authentication method            : FT
 Security mode                    : RSN
 AKM mode                         : PSK
 Encryption cipher                : CCMP
 User authentication mode         : Bypass
 Authorization ACL ID             : N/A
 Authorization user profile       : N/A
 Roam status                      : Intra-AC roam
 Key derivation                   : SHA256
 PMF status                       : N/A
 Forward policy                   : N/A
 Online time                      : 0hr 0min 27sec
 FT status                        : Active
```

2.8.2 Over-the-DS FT と 802.1X 認証設定

I. ネットワーク要件

図 2-7に示すように、クライアントが AP1 と AP2 間でローミングできるように Over-the-DS FT を使用した AC 内ローミングを設定します。akm モードを 802.1X に設定します。

II. 設定手順

サービステンプレート **acstname** を作成します。

```
<AC> system-view
[AC] wlan service-template acstname
```

SSID を **service** に設定します。

```
[AC-wlan-st-acstname] ssid service
```

akm モードを 802.1X に設定します。

```
[AC-wlan-st-acstname] akm mode dot1x
```

cipher スイートを CCMP に設定し、セキュリティ IE を RSN に設定します。

```
[AC-wlan-st-acstname] cipher-suite ccmp
[AC-wlan-st-acstname] security-ie rsn
```

クライアントに対する認証モードを 802.1X に設定します。

```
[AC-wlan-st-acstname] client-security authentication-mode dot1x
[AC-wlan-st-acstname] dot1x domain imc
```

FT を有効にします。

```
[AC-wlan-st-acstname] ft enable
```

FT の方法を Over-the-DS に設定します。

```
[AC-wlan-st-acstname] ft method over-the-ds
```

サービステンプレートを有効にします。

```
[AC-wlan-st-acstname] service-template enable
[AC-wlan-st-acstname] quit
```

802.1X 認証モードを EAP に設定します。

```
[AC] dot1x authentication-method eap
```

RADIUS スキーム **imcc** を作成します。

```
[AC] radius scheme imcc
```

プライマリ認証とアカウンティングサーバの IP アドレスを **10.1.1.3** に設定します。

```
[AC-radius-imcc] primary authentication 10.1.1.3
[AC-radius-imcc] primary accounting 10.1.1.3
```

認証とアカウンティングサーバとパケットを交換できるように、AC に共有鍵 **12345678** を設定します。

```
[AC-radius-imcc] key authentication simple 12345678
[AC-radius-imcc] key accounting simple 12345678
```

RADIUS サーバに送信するユーザ名から ISP ドメイン名を外すように設定します。

```
[AC-radius-imcc] user-name-format without-domain
[AC-radius-imcc] quit
```

ISP ドメイン **imc** を作成し、RADIUS スキーム **imcc** を認証、許可、アカウンティングに使用するためにドメインを設定します。

```
[AC] domain imc
[AC-isp-imc] authentication lan-access radius-scheme imcc
[AC-isp-imc] authorization lan-access radius-scheme imcc
[AC-isp-imc] accounting lan-access radius-scheme imcc
[AC-isp-imc] quit
```

AP1 の radio2 に対してサービステンプレート **acstname** を設定します。

```
[AC] wlan ap 1
[AC-wlan-ap-1] radio 2
[AC-wlan-ap-1-radio-2] service-template acstname
[AC-wlan-ap-1-radio-2] radio enable
[AC-wlan-ap-1-radio-2] quit
[AC-wlan-ap-1] quit
```

AP2 の radio2 に対してサービステンプレート **acstname** を設定します。

```
[AC] wlan ap 2
[AC-wlan-ap-2] radio 2
[AC-wlan-ap-2-radio-2] service-template acstname
[AC-wlan-ap-2-radio-2] radio enable
[AC-wlan-ap-2-radio-2] quit
[AC-wlan-ap-2] quit
```

III. 設定確認

サービステンプレートが正しく設定されたことを確認します。

```
[AC] display wlan service-template acstname verbose
```

```
Service template name         : stname
SSID                          : service
SSID-hide                     : Disabled
User-isolation                : Disabled
Service template status       : Enabled
Maximum clients per BSS       : Not configured
Frame format                  : Dot3
Seamless-roam                 : Disabled
Seamless-roam RSSI threshold : 50
Seamless-roam RSSI gap        : 20
VLAN ID                       : 1
AKM mode                      : 802.1X
Security IE                   : RSN
Cipher suite                  : CCMP
TKIP countermeasure time      : 0 sec
PTK lifetime                  : 43200 sec
GTK rekey                     : Enabled
GTK rekey method              : Time-based
GTK rekey time                : 86400 sec
GTK rekey client-offline      : Disabled
User authentication mode      : 802.1X
Intrusion protection          : Disabled
Intrusion protection mode     : Temporary-block
Temporary block time          : 180 sec
Temporary service stop time   : 20 sec
Fail VLAN ID                  : Not configured
802.1X handshake              : Disabled
802.1X handshake secure       : Disabled
802.1X domain                 : imc
MAC-auth domain               : Not configured
Max 802.1X users              : 4096
Max MAC-auth users            : 4096
802.1X re-authenticate        : Disabled
Authorization fail mode       : Online
Accounting fail mode          : Online
Authorization                 : Permitted
Key derivation                : SHA1
PMF status                    : Disabled
Hotspot policy number         : Not configured
Forward policy                : Not configured
Forwarder                     : AC
FT Status                     : Enable
FT Method                     : over-the-ds
FT Reassociation Deadline     : 20 sec
QoS trust                     : Port
QoS priority                  : 0
```

ローミング状態が N/A で、FT 状態が Active であることを確認します。

[AC] display wlan client verbose

```
Total number of clients: 1

MAC address                       : fc25-3f03-8361
IPv4 address                      : 10.1.1.114
IPv6 address                      : N/A
Username                          : w2
AID                               : 1
AP ID                             : 1
AP name                           : 1
Radio ID                          : 2
SSID                              : service
BSSID                             : 000f-e266-7788
VLAN ID                           : 1
Power save mode                   : Active
Wireless mode                     : 802.11gn
Channel bandwidth                 : 20MHz
SM power save                     : Enabled
SM power save mode                : Static
Short GI for 20MHz                : Not supported
Short GI for 40MHz                : Not supported
```

```
STBC RX capability                : Supported
STBC TX capability                : Not supported
Support HT-MCS set                : 0, 1, 2, 3, 4, 5, 6, 7
QoS mode                          : WMM
Listen interval                   : 20
RSSI                              : 0
Rx/Tx rate                        : 0/0
Authentication method             : Open system
Security mode                     : RSN
AKM mode                          : 802.1X
Encryption cipher                 : CCMP
User authentication mode          : 802.1X
Authorization ACL ID              : N/A
Authorization user profile        : N/A
Roam status                       : N/A
Key derivation                    : SHA256
PMF status                        : N/A
Forward policy                    : N/A
Online time                       : 0hr 0min 7sec
FT status                         : Active
```

クライアントを AP2 にローミングします（詳細は省略します）。

認証方法が FT で、ローミング状態が Intra-AC roam であることを確認します。

[AC] display wlan client verbose

```
Total number of clients: 1

MAC address                       : fc25-3f03-8361
IPv4 address                      : 10.1.1.114
IPv6 address                      : N/A
Username                          : w2
AID                               : 1
AP ID                             : 2
AP name                           : 2
Radio ID                          : 2
SSID                              : service
BSSID                             : 000f-e211-2233
VLAN ID                           : 1
Power save mode                   : Active
Wireless mode                     : 802.11gn
Channel bandwidth                 : 20MHz
SM power save                     : Enabled
SM power save mode                : Static
Short GI for 20MHz                : Not supported
Short GI for 40MHz                : Not supported
STBC RX capability                : Supported
STBC TX capability                : Not supported
Support HT-MCS set                : 0, 1, 2, 3, 4, 5, 6, 7
QoS mode                          : WMM
Listen interval                   : 20
RSSI                              : 0
Rx/Tx rate                        : 0/0
Authentication method             : FT
Security mode                     : RSN
AKM mode                          : 802.1X
Encryption cipher                 : CCMP
User authentication mode          : 802.1X
Authorization ACL ID              : N/A
Authorization user profile        : N/A
Roam status                       : Intra-AC roam
Key derivation                    : SHA256
PMF status                        : N/A
Forward policy                    : N/A
Online time                       : 0hr 0min 7sec
FT status                         : Active
```

目次

このセクションのページは **10-x-x** です。

3章 モビリティグループ 3-1
3.1 モビリティグループ 3-1
3.2 用語 3-1
3.3 モビリティグループメカニズム 3-1
3.3.1 IADTPトンネルの確立 3-2
3.4 制限とガイドライン 3-3
3.5 モビリティグループのSNMP通知の有効化 3-4
3.6 モビリティグループの設定例 3-4

3章 モビリティグループ

3.1 モビリティグループ

モビリティグループには複数のメンバ装置が含まれており、これらの装置間でクライアントは IP または許可を変更せずにローミングできます。モビリティグループは、クライアントがローミングできる規模を拡大します。

🕮 **メモ：**

- AC 間でローミングする場合は、モビリティグループを設定してください。モビリティグループの設定をしていない場合の、AC 間ローミング動作は未サポートです。
- 異なる機種、異なるソフトウェアバージョンの組み合わせでのモビリティグループ動作は未サポートです。

3.2 用語

- **IACTP（Inter Access Controller Tunneling Protocol）**

IACTP は、AC 間の安全な通信のための一般的なパケットカプセル化と通信メカニズムで、QX 独自のプロトコルです。ローミング・サービスを提供している AC 間では、IACTP トンネル上で制御メッセージとクライアント情報を交換しています。

- **Home AC**

Home AC は、無線クライアントが最初に接続する AP を管理する AC です。

- **Foreign AC**

Foreign AC は、クライアントが相互 AC ローミングの後に接続する AC です。

- **モビリティグループ**

モビリティグループはクライアントがローミングできる複数の AP を管理する AC を含むグループです。

3.3 モビリティグループメカニズム

モビリティグループを使用すると、異なる AC によって管理されている AP 間でクライアントをローミングできます。これらの AC は同じモビリティグループに属し、相互に IADTP トンネルを確立している必要があります。

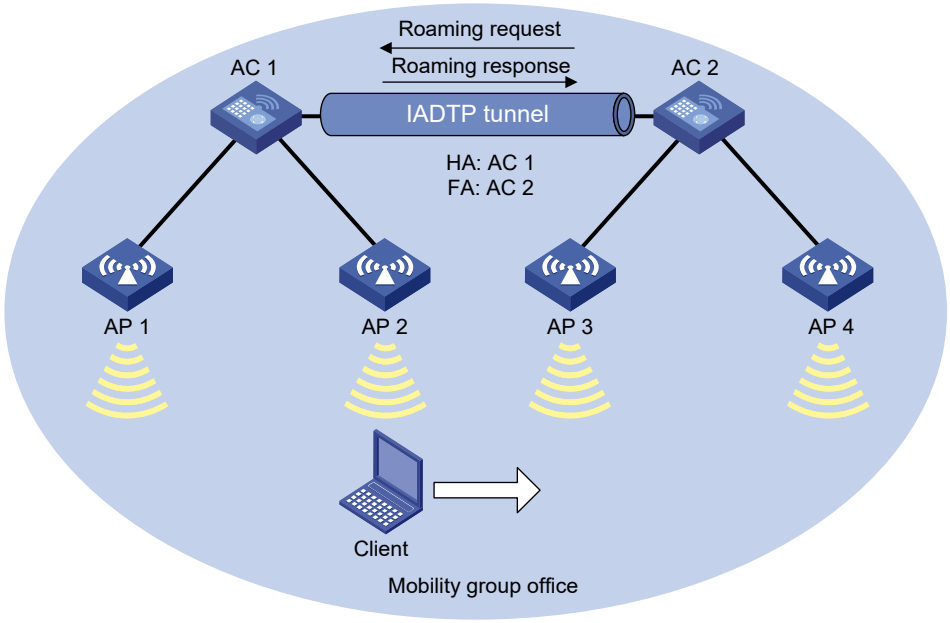


図 3-1 モビリティグループのメカニズム

図 3-1に示すように、AC 間ローミングでは以下の手順を使用します。

1) クライアントは AP2 からオンラインになります。AC1 はクライアントのローミングエントリを作成し、IADTP トンネルを介して情報を AC2 に送信します。
2) クライアントは AP3 にローミングします。AC2 は、クライアントのローミングエントリを調べ、高速ローミングを実行するかどうかを判断します。
クライアントが RSN+802.1 X 認証を使用し、AC と同じ PMKID を伝送する場合、高速ローミングが使用され、クライアントは再認証なしで AP3 と関連付けることができます。そうでない場合、クライアントは AP3 と関連付ける前に再認証する必要があります。
3) クライアントは AP3 と関連付けます。AC2 はローミング要求を AC1 に送信します。
4) AC1 はローミング要求を確認し、以下のいずれかの操作を実行します。
   - 要求が無効な場合、ローミングの失敗を示すローミング応答を AC2 に送信します。AC2 はクライアントをログオフします。
   - ローミングトレースとローミングアウト情報を保存し、要求が有効な場合はローミングの成功を示すローミング応答を AC2 に送信します。AC2 はクライアントのローミングイン情報を保存します。

3.3.1 IADTP トンネルの確立

モビリティグループ内のデバイスは、クライアントとして動作して接続要求を開始したり、サーバとして動作して接続要求を待ち受けて応答したりできます。

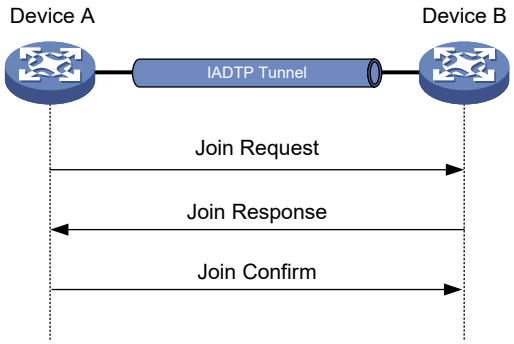


図 3-2 IADTP トンネルの確立

図 3-2に示すように、2 つの装置は以下の手順を使用して IADTP トンネルを確立します。

1) Device A は Device B に参加要求を送信します。
2) 参加要求を受信すると、Device B はローカル設定とパケットコンテンツを使用して、Device A が同じモビリティグループに属しているかどうかを識別します。
   - 同じモビリティグループに属している場合、Device B は成功を表す結果コードを含む参加応答を返します。
   - これらが異なるモビリティグループに属している場合、Device B は失敗を表す結果コードを含む参加応答を返します。
3) 参加応答を受信すると、Device A は応答内の結果コードを調べます。
   - 結果コードが失敗を表している場合、Device A はパケットを返しません。
   - 結果コードが成功を表している場合、Device A は Device B に結合確認を送信します。
4) 結合確認を受信すると、Device B は Device A との IADTP トンネルを確立します。

3.4 制限とガイドライン

以下の方法で AP を設定できます。

- AP view で AP を 1 つずつ設定します。
- AP グループに AP を割り当て、AP group view で AP グループを設定します。
- グローバル設定 view ですべての AP を設定します。

AP の場合、同じパラメータに対してこれらの view で行った設定は、AP view、AP group view、グローバル設定 view の降順で有効になります。

AP がクライアント認証装置として設定されているサービステンプレートの場合、WLAN ローミングはサポートされません。QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*13 ユーザアクセスと認証*“の”*1 章 WLAN アクセス認証*“を参照してください。

異なる VLAN の RSN+802.1X クライアントがモビリティグループ内の装置間をローミングするには、メンバ装置のアップリンクインタフェースですべてのクライアント VLAN が許可されていることを確認します。

3.5 モビリティグループのSNMP通知の有効化

重大なモビリティグループイベントを NMS に通知するために、WLAN ローミングの SNMP 通知を有効にしてください。モビリティグループイベントを正しく通知するために、装置で SNMP も設定する必要があります。SNMP 設定の詳細は、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*17 ネットワーク管理と監視*”の”*4 章 SNMP*”を参照してください。

以下にモビリティグループの SNMP 通知の有効化を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． モビリティグループの SNMP 通知を有効にする	**snmp-agent trap enable wlan mobility**	デフォルト：無効

3.6 モビリティグループの設定例

I. ネットワーク要件

図 3-3に示すように、異なる AC によって管理されている AP2 から AP3 にクライアントがローミングできるように、モビリティグループを設定します。

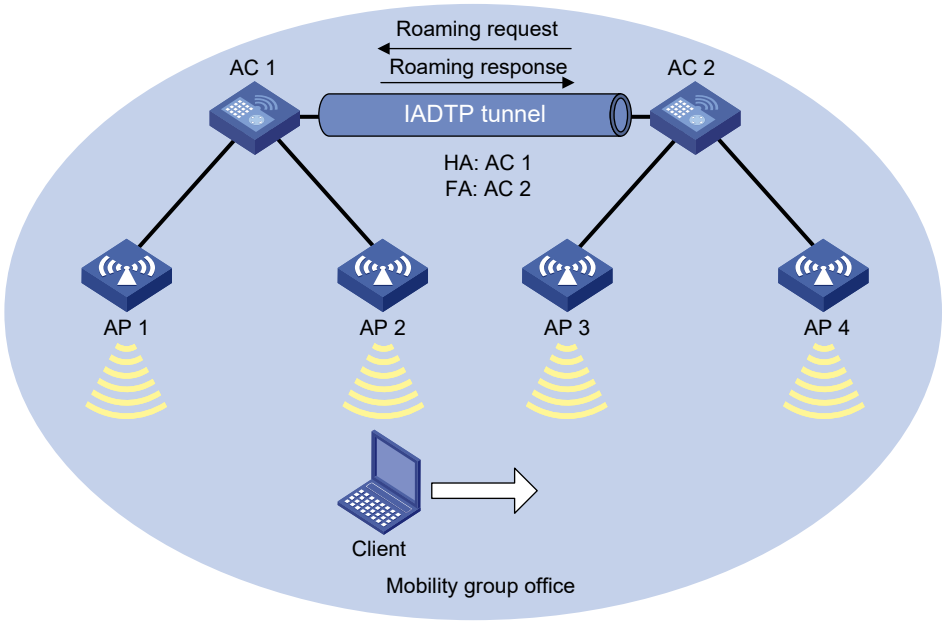


図 3-3 ネットワーク図

II. 設定手順

1)　AC1 を設定します。

サービステンプレート **service** を作成し、SSID を **office** に設定してサービステンプレートを有効にします。

```
<AC1> system-view
[AC1] wlan service-template service
[AC1-wlan-st-service] ssid office
[AC1-wlan-st-service] service-template enable
[AC1-wlan-st-service] quit
```

手動 AP **ap1** を作成し、AP モデルとシリアル ID を指定します。

```
[AC1] wlan ap ap1 model QX-W1110
[AC1-wlan-ap-ap1] serial-id 219801A28N819CE0002T
```

AP1 の radio1 に対してサービステンプレートを設定します。

```
[AC1-wlan-ap-ap1] radio 1
[AC1-wlan-ap-ap1-radio-1] radio enable
[AC1-wlan-ap-ap1-radio-1] service-template service
[AC1-wlan-ap-ap1-radio-1] quit
[AC1-wlan-ap-ap1] quit
```

手動 AP **ap2** を作成し、AP モデルとシリアル ID を指定します。

```
[AC1] wlan ap ap2 model QX-W1110
[AC1-wlan-ap-ap2] serial-id 219801A28N819CE0003T
```

AP2 の radio1 に対してサービステンプレートを設定します。

```
[AC1-wlan-ap-ap2] radio 1
[AC1-wlan-ap-ap2-radio-1] radio enable
[AC1-wlan-ap-ap2-radio-1] service-template service
[AC1-wlan-ap-ap2-radio-1] quit
[AC1-wlan-ap-ap2] quit
```

モビリティグループ **office** を作成します。

```
[AC1] wlan mobility group office
```

IADTP トンネルの IP アドレスタイプを IPv4 で指定します。

```
[AC1-wlan-mg-office] tunnel-type ipv4
```

IADTP トンネルを確立する送信元 IP アドレスを 10.1.4.22 に指定します。

```
[AC1-wlan-mg-office] source ip 10.1.4.22
```

AC2 をモビリティグループに追加します。

```
[AC1-wlan-mg-office] member ip 10.1.4.23
```

モビリティグループを有効にします。

```
[AC1-wlan-mg-office] group enable
```

```
[AC1-wlan-mg-office] quit
```

2)　AC2 を設定します。

サービステンプレート **service** を作成し、SSID を **office** に設定してサービステンプレートを有効にします。

```
<AC2> system-view
[AC2] wlan service-template service
[AC2-wlan-st-service] ssid office
[AC2-wlan-st-service] service-template enable
[AC2-wlan-st-service] quit
```

手動 AP **ap3** を作成し、AP モデルとシリアル ID を指定します。

```
[AC2] wlan ap ap3 model QX-W1110
[AC2-wlan-ap-ap3] serial-id 219801A28N819CE0004T
```

AP3 の radio1 に対してサービステンプレートを設定します。

```
[AC2-wlan-ap-ap3] radio 1
[AC2-wlan-ap-ap3-radio-1] radio enable
[AC2-wlan-ap-ap3-radio-1] service-template service
[AC2-wlan-ap-ap3-radio-1] quit
[AC2-wlan-ap-ap3] quit
```

手動 AP **ap4** を作成し、AP モデルとシリアル ID を指定します。

```
[AC2] wlan ap ap4 model QX-W1110
[AC2-wlan-ap-ap4] serial-id 219801A28N819CE0005T
```

AP4 の radio1 に対してサービステンプレートを設定します。

```
[AC2-wlan-ap-ap4] radio 1
[AC2-wlan-ap-ap4-radio-1] radio enable
[AC2-wlan-ap-ap4-radio-1] service-template service
[AC2-wlan-ap-ap4-radio-1] quit
[AC2-wlan-ap-ap4] quit
```

モビリティグループ **office** を作成します。

```
[AC2] wlan mobility group office
```

IADTP トンネルの IP アドレスタイプを IPv4 で指定します。

```
[AC2-wlan-mg-office] tunnel-type ipv4
```

IADTP トンネルを確立する送信元 IP アドレスを 10.1.4.23 に指定します。

```
[AC2-wlan-mg-office] source ip 10.1.4.23
```

AC2 をモビリティグループに追加します。

```
[AC2-wlan-mg-office] member ip 10.1.4.22
```

モビリティグループを有効にします。

```
[AC2-wlan-mg-office] group enable
[AC2-wlan-mg-office] quit
```

III. 設定の確認

AC1 にモビリティグループが作成されていることを確認します。

```
[AC1] display wlan mobility group
Mobility group name: office
 Tunnel type: IPv4
 Source IPv4: 10.1.4.22
 Source IPv6: Not configured
 Authentication method: Not configured
 Mobility group status: Enabled
 Member entries: 1
 IP address                              State          Online time
 10.1.4.23                               Up             00hr 00min 12sec
```

AC 2 にモビリティグループが作成されたことを確認します。

```
[AC2] display wlan mobility group
Mobility group name: office
 Tunnel type: IPv4
 Source IPv4: 10.1.4.23
 Source IPv6: Not configured
 Authentication method: Not configured
 Mobility group status: Enabled
 Member entries: 1
 IP address                              State          Online time
 10.1.4.22                               Up             00hr 00min 05sec
```

AP2 でクライアントをオンラインにしてから、クライアントを AP3 にローミングさせます。(詳細は省略します)

クライアントのローミング情報を AC1 に表示して、クライアントが AP2 からオンラインになり、AP3 にローミングされたことを確認します。

```
[AC1] display wlan mobility roam-track mac-address 9cd3-6d9e-6778
Total entries: 2
BSSID          Created at          Online time      AC IP address  RID  AP name
000f-e203-8889  2016-06-14 11:12:28  00hr 06min 56sec  10.1.4.23      1    ap3
000f-e203-7777  2016-06-14 11:11:28  00hr 03min 30sec  127.0.0.1      1    ap2
```

AC1 でクライアントが AC2 にローミングされたことを確認します。

```
<AC1> display wlan mobility roam-out
Total entries: 1
MAC address     BSSID           VLAN ID  Online time       FA IP address
9cd3-6d9e-6778  000f-e203-8889  1        00hr 01min 59sec  10.1.4.23
```

AC2 でクライアントが AP3 と関連付けられ、ローミングステータスが **Inter-AC roam** であることを確認します。

```
<AC2> display wlan client verbose
Total number of clients: 1

MAC address                         : 9cd3-6d9e-6778
IPv4 address                        : 10.1.1.114
```

```
IPv6 address                        : N/A
Username                            : N/A
AID                                 : 1
AP ID                               : 3
AP name                             : ap3
Radio ID                            : 1
Channel                             : 36
SSID                                : 1
BSSID                               : 000f-e203-8889
VLAN ID                             : 1
Sleep count                         : 242
Wireless mode                       : 802.11ac
Channel bandwidth                   : 80MHz
SM power save                       : Enabled
SM power save mode                  : Dynamic
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                  : Not supported
STBC TX capability                  : Not supported
LDPC RX capability                  : Not supported
SU beamformee capability            : Not supported
MU beamformee capability            : Not supported
Beamformee STS capability           : N/A
Block Ack                           : TID 0 In
Supported VHT-MCS set               : NSS1 0, 1, 2, 3, 4, 5, 6, 7, 8
                                      NSS2 0, 1, 2, 3, 4, 5, 6, 7, 8
Supported HT MCS set                : 0, 1, 2, 3, 4, 5, 6, 7,
                                      8, 9, 10, 11, 12, 13, 14,
                                      15, 16, 17, 18, 19, 20,
                                      21, 22, 23
Supported rates                     : 6, 9, 12, 18, 24, 36,
                                      48, 54 Mbps
QoS mode                            : WMM
Listen interval                     : 10
RSSI                                : 62
Rx/Tx rate                          : 130/11
Authentication method               : Open system
Security mode                       : PRE-RSNA
AKM mode                            : Not configured
Cipher suite                        : N/A
User authentication mode            : Bypass
Authorization ACL ID                : 3001(Not effective)
Authorization user profile          : N/A
Authorization CAR                   : N/A
Roam status                         : Inter-AC roam
Key derivation                      : SHA1
PMF status                          : Enabled
Forward policy name                 : Not configured
Online time                         : 0days 0hours 5minutes 13seconds
FT status                           : Inactive
```

クライアントが AC1 から AC2 にローミングされたことを確認します。

```
<AC2> display wlan mobility roam-in
Total entries: 1
MAC address     BSSID           VLAN ID  HA IP address
9cd3-6d9e-6778  000f-e203-8889  1        10.1.4.22
```

QX-W2300AC シリーズ アクセスコントローラ

オペレーションマニュアル

11. WLAN トラフィック最適化

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 **11-x-x** です。

1章 ユーザアイソレーション 1-1
1.1 概要 1-1
1.2 SSIDベースユーザアイソレーション 1-1
1.2.1 中央転送モードのユーザアイソレーションメカニズム 1-1
1.2.2 ローカル転送モードのユーザアイソレーションメカニズム 1-2
1.3 VLANベースユーザアイソレーション 1-3
1.3.1 中央転送モードのユーザアイソレーションメカニズム 1-3
1.3.2 ローカル転送モードのユーザアイソレーションメカニズム 1-5
1.4 SSIDベースのユーザアイソレーションの有効化 1-7
1.5 VLANベースのユーザアイソレーションの設定 1-7
1.5.1 制限とガイドライン 1-7
1.5.2 設定手順 1-8
1.6 ユーザアイソレーションの表示と維持 1-8
1.7 ユーザアイソレーションの設定例 1-9
1.7.1 SSIDベースのユーザアイソレーションの設定例（中央転送モード） 1-9
1.7.2 SSIDベースのユーザアイソレーションの設定例（ローカル転送モード） 1-10
1.7.3 VLANベースのユーザアイソレーションの設定例（中央転送モード） 1-11
1.7.4 VLANベースのユーザアイソレーションの設定例（ローカル転送モード） 1-12

1章 ユーザアイソレーション

1.1 概要

ユーザアイソレーション(user isolation)機能は、ワイヤレスユーザのセキュリティを改善します。

ユーザアイソレーションが AP で有効化されると、同一 VLAN もしくは同一 SSID のワイヤレスユーザはレイヤ 2 で相互に接続できなくなります。AP はこれらのユーザに対し、レイヤ 2 ユニキャスト、マルチキャスト、ブロードキャストパケットを転送しません。

ユーザアイソレーションは以下のタイプがあります。

- **SSID ベースユーザアイソレーション**－同一 VLAN の同一 SSID を使用する無線ユーザを隔離します。
- **VLAN ベースユーザアイソレーション**－同一 VLAN の無線ユーザを隔離します。

1.2 SSIDベースユーザアイソレーション

SSID ベースユーザアイソレーションはローカル転送モードと中央転送モードの両方に適用します。

SSID ベースユーザアイソレーションのサービスを有効にしたとき、装置は、同一 VLAN のサービスを経由してネットワークにアクセスするすべての無線ユーザを隔離します。

1.2.1 中央転送モードのユーザアイソレーションメカニズム

図 1-1に示すように、AC はクライアントのトラフィックを中央で転送します。サービス service を使用して Client 1～Client 3 は AP1～AP3 を通して WLAN にアクセスします。Client 1、Client 2 は VLAN 100 に所属しています。Client 2 は VLAN 200 に所属しています。ユーザアイソレーションサービスを行うため、AC でユーザアイソレーションを有効にします。

- Client 1 は VLAN 100 のブロードキャストあるいはマルチキャストパケットを送信します。AC がパケットを受信すると、WLAN の各 AP にパケットを転送しません。AC は Switch の有線ポートのみパケットを転送します。
- Client 1 は VLAN 100 の Client 2 にユニキャストパケットを送信します。AC がパケットを受信すると、AP 2 に転送しないでパケットを廃棄します。

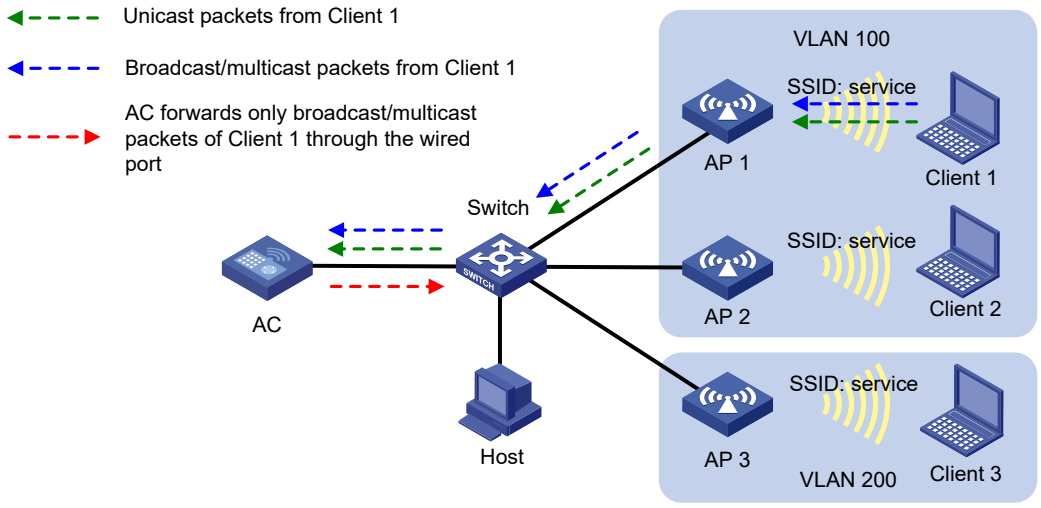


図 1-1 パケット転送パス

1.2.2 ローカル転送モードのユーザアイソレーションメカニズム

このメカニズムは同一 AP の無線クライアントを隔離します。

図 1-2に示すように、APはクライアントのローカルトラフィックの転送を行います。Client 1～Client 4 はサービス service を使用して、AP1～AP3 を通して WLAN にアクセスします。Client 1～Client 3 は VLAN 100 に所属しています。Client 4 は VLAN 200 に所属しています。AP1 でユーザアイソレーションサービスを行うため SSID ベースのユーザアイソレーションを有効にします。

- Client 1 は VLAN 100 のブロードキャストあるいはマルチキャストパケットを送信します。
  - AP1 がパケットを受信すると、ユーザアイソレーションが有効のため、Client 2 にパケットを転送しません。AP は AP2、AP3、Host が含まれる同一 VLAN の無線装置に優先を経由してのみパケットを転送します。
  - AP2がパケットを受信すると、ユーザアイソレーションがAP2で無効であるため、Client 3 にパケットを転送します。
  - AP3 がパケットを受信すると、Client 1 と Client 4 は異なる VLAN に所属しているため、Client 4 にパケットを転送しません。
- Client 1 は VLAN 100 の Client 2 にユニキャストパケットを送信します。AP 1 がパケットを受信すると、Client 2 に転送しないでパケットを廃棄します。

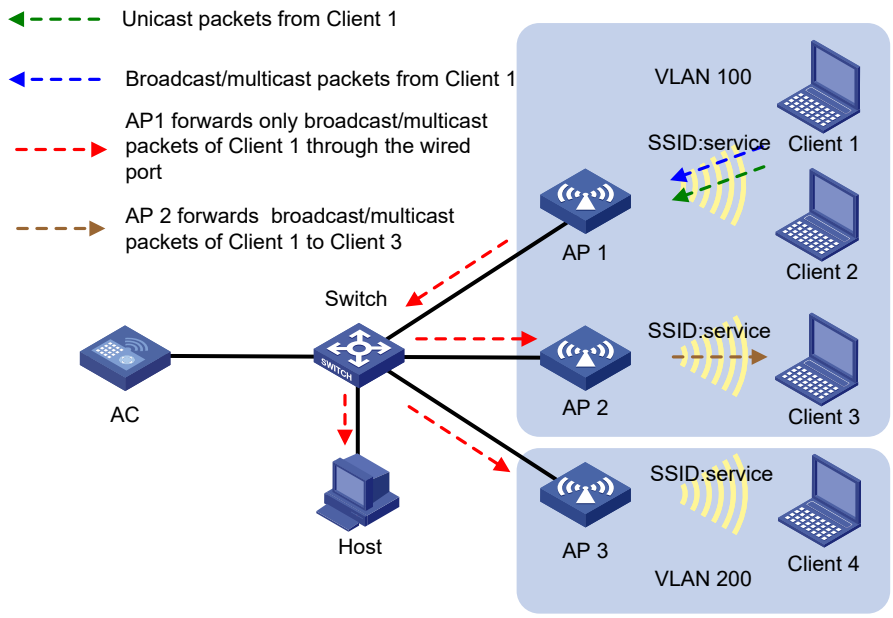


図 1-2 パケット転送パス

1.3 VLANベースユーザアイソレーション

VLAN ベースユーザアイソレーションはローカル転送モードと中央転送モードの両方に適用します。

転送モード	受信したユニキャストパケット	受信したブロードキャストキャストパケット、マルチキャストパケット
中央転送	APはパケットを廃棄します。	ACはVLANの有線ユーザに有線ポートのみパケットを転送します。VLANの無線ユーザにはパケットを転送しません。
ローカル転送	FITモードのAPはパケットを廃棄します。	FITモードのAPは有線ポートを通してVLANのユーザにパケットを転送します。 しかしAPはVLANのローカル無線ユーザにパケットを転送しません。

1.3.1 中央転送モードのユーザアイソレーションメカニズム

I. 無線ユーザから受信したパケット

図 1-3に示すように、AC は Client のトラフィックを中央で転送します。VLAN 100 の AC でユーザアイソレーションを有効にします。

- Client 1 は VLAN 100 のブロードキャストあるいはマルチキャストパケットを送信します。AC がパケットを受信すると、WLAN の各 AP にパケットを転送しません。AC は Switch の有線ポートにパケットを転送します。Switch は Host と Server にパケットを転送します。

- Client 1 は VLAN 100 の Client 3 にユニキャストパケットを送信します。AC がパケットを受信すると、AP 2 に転送しないでパケットを廃棄します。

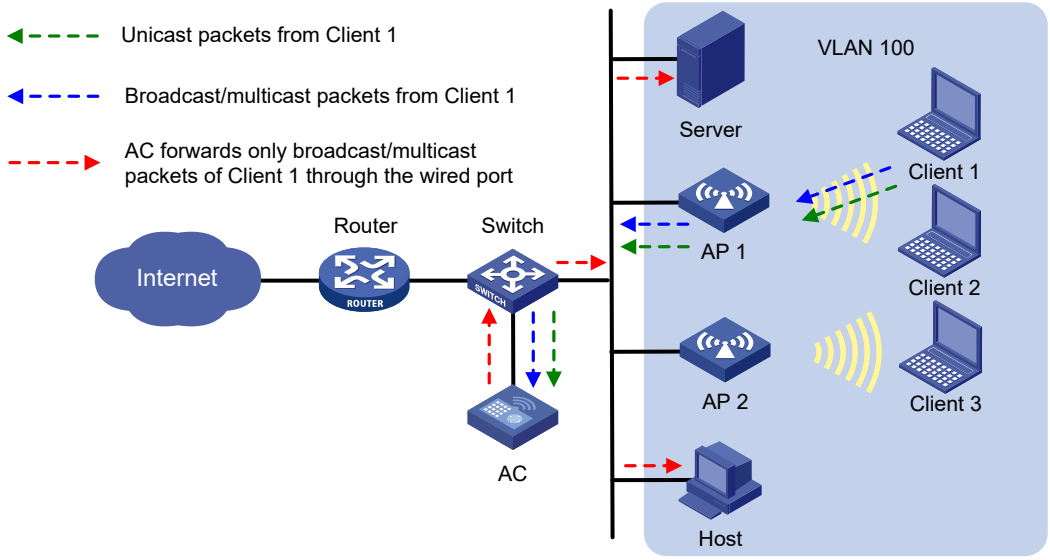


図 1-3 パケット転送パス

II. 有線ユーザから受信したパケット

図 1-4に示すように、AC は Client のトラフィックを中央で転送します。VLAN 100 の AC でユーザアイソレーションを有効にします。

- Host は VLAN 100 のブロードキャストあるいはマルチキャストパケットを送信します。サーバ、AC がパケットを受信することができます。AC がパケットを受信すると、WLAN の各 AP にパケットを転送しないで廃棄します。
- Host は VLAN 100 の Client 3 にユニキャストパケットを送信します。AC がパケットを受信すると、AP 2 に転送しないでパケットを廃棄します。

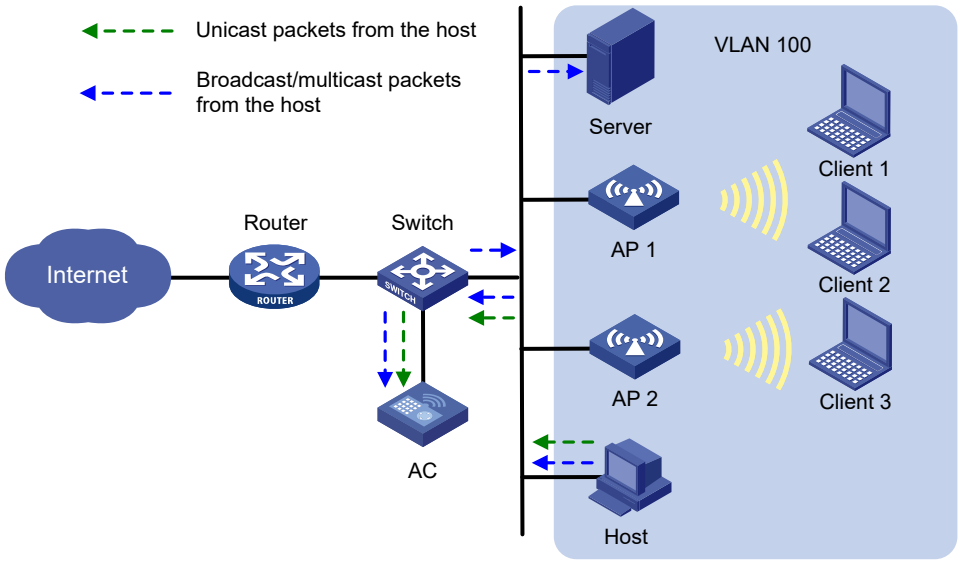


図 1-4 パケット転送パス

1.3.2 ローカル転送モードのユーザアイソレーションメカニズム

I. 無線ユーザから受信したパケット

図 1-5に示すように、AP1 はクライアントのローカルトラフィックの転送を行います。VLAN 100 の AP1 でユーザアイソレーションを有効にします。

- Client 1 は VLAN 100 のブロードキャストあるいはマルチキャストパケットを送信します。
  - AP1 がパケットを受信すると、有線ポートを経由して VLAN 100 の Server、AP2、Host にパケットを転送します。しかし、AP1 はユーザアイソレーションが有効のため、Client 2 にパケットを転送しません。
  - AP2 がパケットを受信すると、ユーザアイソレーションが AP2 で無効であるため、Client 3 にパケットを転送します。
- Client 1 は VLAN 100 の Client 3 にユニキャストパケットを送信します。AP 1 がパケットを受信すると、AP 2 に転送しないでパケットを廃棄します。

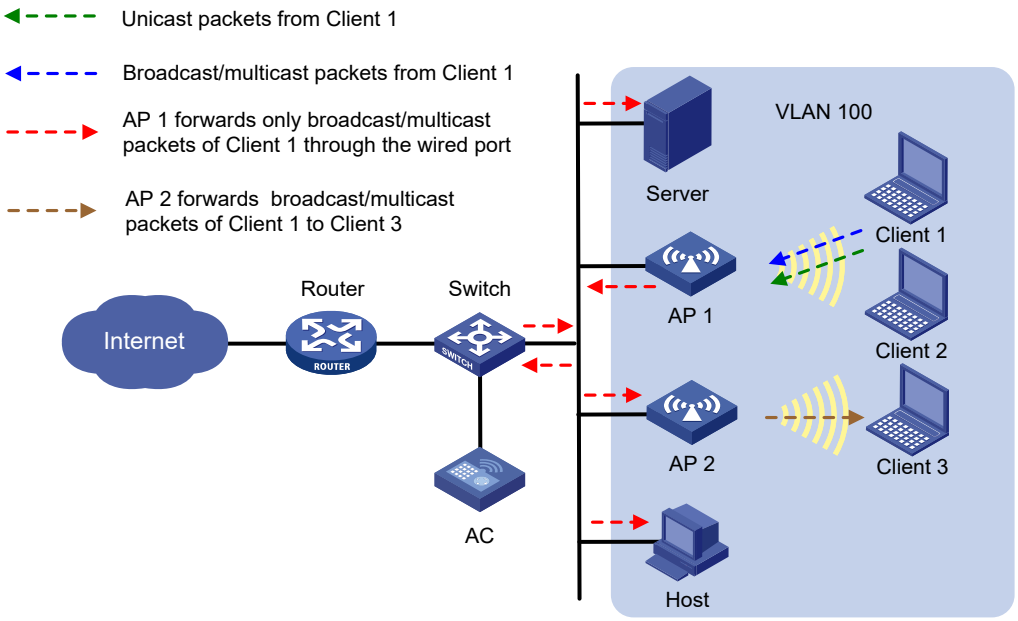


図 1-5 パケット転送パス

II. 有線ユーザから受信したパケット

図 1-6に示しように、AP1 はクライアントのローカルトラフィックの転送を行います。VLAN100 の AP1 でユーザアイソレーションを有効にします。

- Host は VLAN 100 のブロードキャストあるいはマルチキャストパケットを送信します。サーバ、AC、AP1、AP2 がパケットを受信することができます。
  - AP1 がパケットを受信すると、Client 1、Client 2 にパケットを転送しないで廃棄します。
  - AP2 がパケットを受信すると、ユーザアイソレーションが AP2 で無効であるため、Client 3 にパケットを転送します。
- Host は VLAN 100 の Client 1 にユニキャストパケットを送信します。AP 1 がパケットを受信すると、Client 1 に転送しないでパケットを廃棄します。

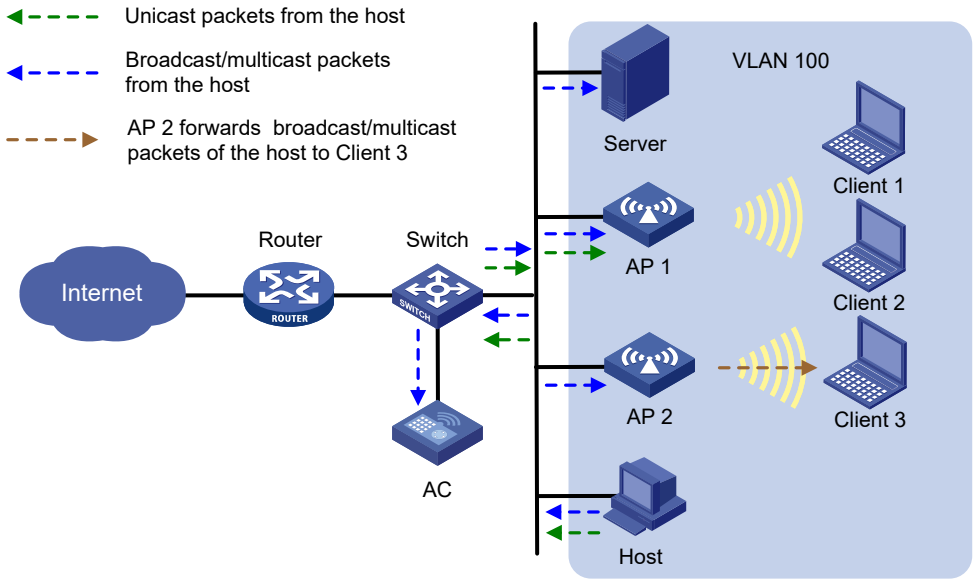


図 1-6 パケット転送パス

1.4 SSIDベースのユーザアイソレーションの有効化

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. service template view に移行する	**wlan service-template** *service-template-name*	—
3. ユーザアイソレーションを有効化する	**user-isolation enable**	デフォルト：無効

1.5 VLANベースのユーザアイソレーションの設定

1.5.1 制限とガイドライン

VLAN ベースのユーザアイソレーションを設定するとき、以下の制限とガイドラインに従ってください。

- VLAN のユーザが外部ネットワークにアクセスできるようにするには、VLAN ベースのユーザアイソレーションを有効にする前に、VLAN ゲートウェイ 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。
- VLAN ベースのユーザアイソレーションを中央転送モードとローカル転送モードの両方に適用します。
  - 中央転送モードでは、AC に直接この機能を設定します
  - ローカル転送モードでは、AC 上で AP グループを設定するか、AC から AP への設定ファイルの展開ができます。AC から AP に設定ファイルを展開する場合は、1.5.2 I. の後に、AC で **map-configuration** コマンドを使用してユーザアイソレーションコンフィグレーションを含むコンフィグレーションファイルを AP に展開

する必要があります。詳細は QX-W2300AC シリーズアクセスコントローラコマンドマニュアルの“*6 WLAN アクセス*”の”*1 章 WLAN アクセス*”を参照してください。

1.5.2 設定手順

VLAN ベースのユーザアイソレーションの設定手順は以下の通りです。

I. 集中型転送モードまたはローカル転送モードで AP に設定ファイルを展開する

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． （オプション設定項目）VLAN リストで許可された MAC アドレスリストを設定する	**user-isolation vlan** *vlan-list* **permit-mac** *mac-list*	デフォルト：設定なし 装置は、許可されたMACアドレスのユーザから送信されたユニキャスト、マルチキャスト、ブロードキャストトラフィックを転送できます。また、他のユーザから送信されたユニキャストトラフィックを転送できます。
3． VLAN リストのユーザアイソレーションを有効にする	**user-isolation vlan** *vlan-list* **enable** [**permit-unicast**]	デフォルト：無効 指定されたVLANのすべてのユーザのユニキャストトラフィックを許可するには**permit-unicast**パラメータを指定します。
4． （オプション設定項目）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とマルチキャストトラフィックを許可する	**user-isolation permit-broadcast**	デフォルト : ユーザアイソレーションが有効の場合、装置はトラフィックを転送しません。

1.6 ユーザアイソレーションの表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
1つのVLANあるいはすべてのVLANでユーザアイソレーションの統計情報を表示する	**display user-isolation statistics** [**vlan** *vlan-id*]
1つのVLANあるいはすべてのVLANでユーザアイソレーションの統計情報を削除する	**reset user-isolation statistics** [**vlan** *vlan-id*]

1.7 ユーザアイソレーションの設定例

1.7.1 SSID ベースのユーザアイソレーションの設定例（中央転送モード）

I. ネットワーク要件

図 1-7に示すように、Client 1、Client2 はインタネットに接続するため、同一 SSID を使用します。AC は Client のトラフィックを中央で転送します。

クライアントがインタネットにアクセスを行う際、クライアント間での通信を隔離するように、AC でユーザアイソレーションを設定します。

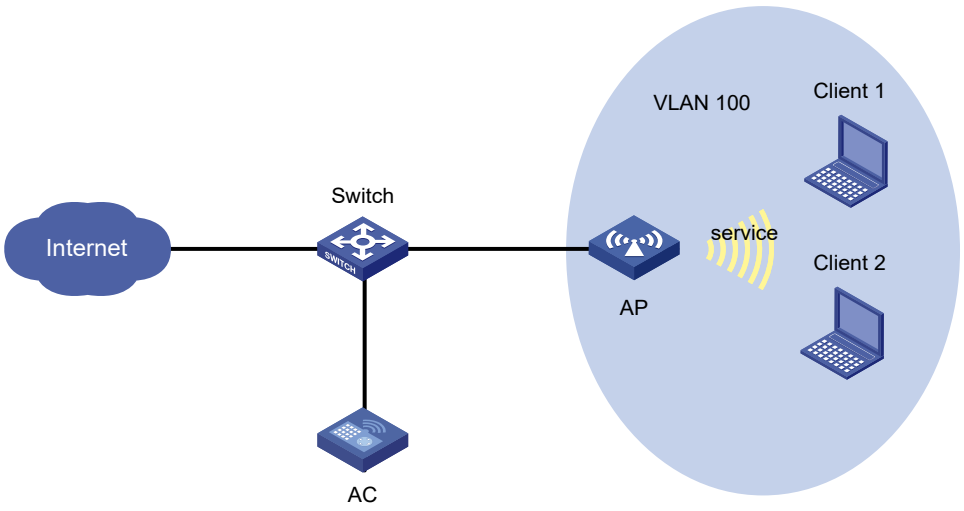


図 1-7 ネットワーク図

II. 設定手順

サービステンプレート service を通してインタネットにアクセスするため、Client 1、Client 2 を設定します。（詳細は省略します。）

サービステンプレート service で SSID ベースのユーザアイソレーションを有効にします。

```
<AC> system-view
[AC] wlan service-template service
[AC-wlan-st-service] user-isolation enable
[AC-wlan-st-service] quit
```

III. 設定の確認

Client 1、Client2 はインタネットに接続でき、互いに Client 間で通信ができないことを確認します。（詳細は省略します。）

1.7.2 SSID ベースのユーザアイソレーションの設定例（ローカル転送モード）

I. ネットワーク要件

図 1-8に示すように、Client 1、Client2 はインタネットに接続するため、同一 SSID を使用します。AC は Client のトラフィックをローカルで転送します。

クライアントがインタネットにアクセスを行う際、クライアント間での通信を隔離するように、AC1 でユーザアイソレーションを設定します。

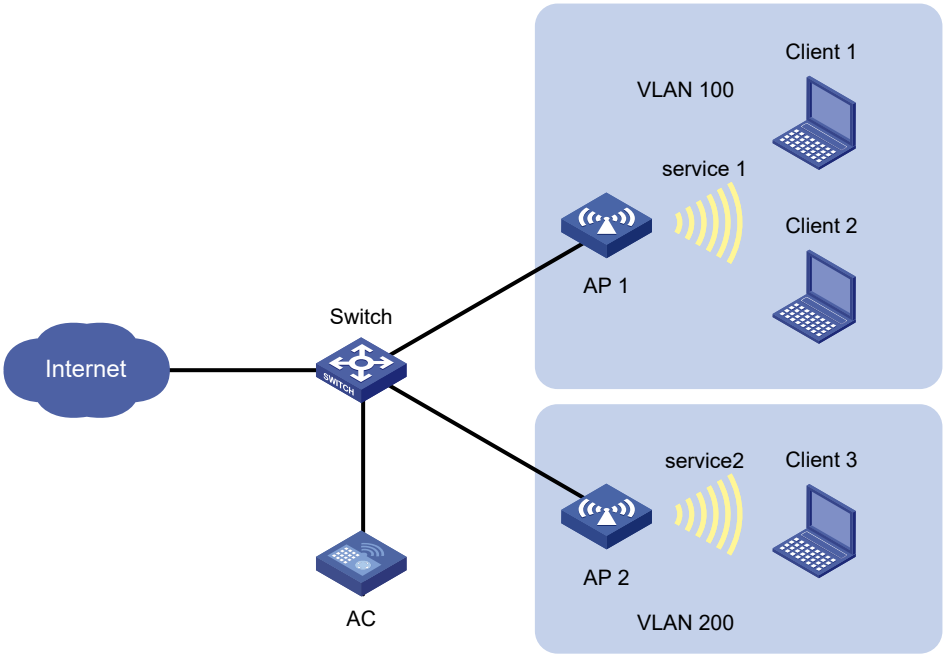


図 1-8 ネットワーク図

II. 設定手順

サービステンプレート service1 を通してインタネットにアクセスするため、Client 1、Client 2 を設定します。Client のローカルトラフィックの転送を行うため、AP を設定します。（詳細は省略します。）

サービステンプレート service1 で SSID ベースのユーザアイソレーションを有効にします。

```
<AC> system-view
[AC] wlan service-template service1
[AC-wlan-st-service1] user-isolation enable
[AC-wlan-st-service1] quit
```

III. 設定の確認

Client 1、Client2 はインタネットにアクセスするためサービス service1 を使用することができ、互いに Client 間で通信ができないことを確認します。（詳細は省略します。）

1.7.3 VLAN ベースのユーザアイソレーションの設定例（中央転送モード）

I. 設定の確認

図 1-9に示すように、AC は Client のトラフィックを中央で転送します。Router は VLAN2 の装置のゲートウェイとして動作します。

AC で VLAN 2 のユーザアイソレーションを設定します。Client 1、Client 2、Host、Server がインタネットにアクセスできるようにするため、許可する MAC アドレスを設定するため、ゲートウェイに MAC アドレスを追加します。

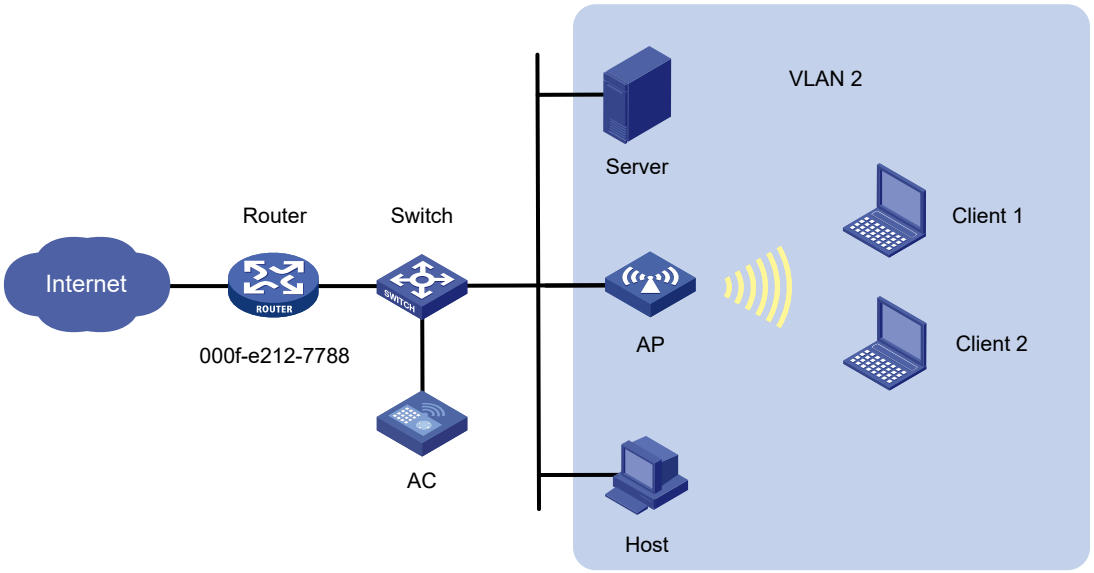


図 1-9 ネットワーク図

II. 設定手順

WLAN を通してインタネットにアクセスするため、Client 1、Client 2 を設定します。（詳細は省略します。）

許可する MAC アドレスのリストにゲートウェイの MAC アドレスを割り当てます。

```
<AC> system-view
[AC] user-isolation vlan 2 permit-mac 000f-e212-7788
```

VLAN 2 で VLAN ベースユーザアイソレーションを有効にします。

```
[AC] user-isolation vlan 2 enable
```

III. 設定の確認

Client 1、Client 2、Host、Server がインタネットにアクセスできることを確認します。（詳細は省略します。）

1.7.4 VLAN ベースのユーザアイソレーションの設定例（ローカル転送モード）

図 1-10に示すように、AC は Client のトラフィックをローカルで転送します。Router は VLAN100 の装置のゲートウェイとして動作します。ゲートウェイの MAC アドレスは 000f-e212-7788 です。

AP1 で VLAN 100 のユーザアイソレーションを設定します。Client 1、Client 2 がインタネットにアクセスできるようにするため、許可する MAC アドレスを設定するため、ゲートウェイに MAC アドレスを追加します。

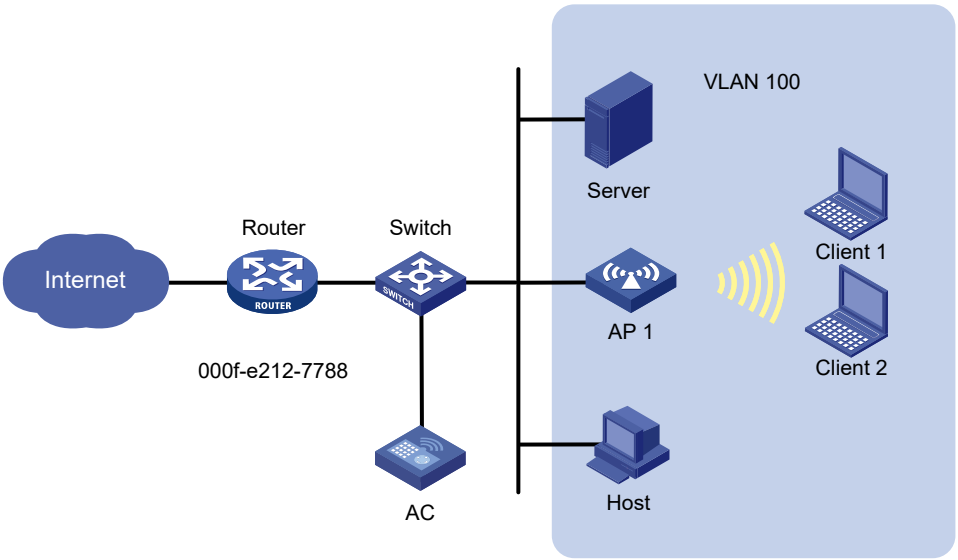


図 1-10 ネットワーク図

I. 設定手順

WLAN を通してインタネットにアクセスするため、Client 1、Client 2 を設定します。（詳細は省略します。）

コンフィグレーションファイル” apcfg.txt”を作成し、コンフィグレーションファイルにユーザアイソレーションコマンドを追加します。

ユーザアイソレーションを有効にする前に、許可する MAC アドレスリストにゲートウェイの MAC アドレスを追加するため、以下のコマンドを記載する必要があります。

```
system-view
user-isolation vlan 100 permit-mac 000f-e212-7788
user-isolation vlan 100 enable
```

AC にコンフィグレーションファイル apcfg.txt をアップロードします。(詳細は省略します。)

AP1 にコンフィグレーションファイル apcfg.txt を送信します。

```
<AC> system-view
[AC] wlan ap ap1 model QX-W1020
[AC-wlan-ap-ap1] map-configuration apcfg.txt
```

II. 設定の確認

VLAN100 の Client 1、Client 2 がインタネットにアクセスできることを確認します。(詳細は省略します。)

QX-W2300AC シリーズ アクセスコントローラ

オペレーションマニュアル

12. WLAN アドバンスド機能

本マニュアルは以下に示す章で構成されています。

01- WLAN 最適化の設定

02- WLAN メッシュの設定

03- IoT 機能の設定

04- HotSpot2.0 の設定

目次

このセクションのページは **12-x-x** です。

1章 WLAN最適化の設定 1-1
1.1 概要 1-1
1.2 制限事項とガイドライン 1-1
1.3 APトリガのクライアント再関連付けの設定 1-1
1.4 APのトラフィックスケジューリングモードの設定 1-2
1.5 隠れ端末保護の設定 1-3
1.6 ブロードキャストおよびマルチキャストパケット制御の設定 1-4
1.7 ブロードキャストおよびマルチキャストのパケットレート制御の設定 1-5
1.8 APアップリンクブロードキャストおよびマルチキャストパケットパケットのレート制限の設定 1-6
1.9 クライアント高速キープアライブの設定 1-7

1章 WLAN 最適化の設定

1.1 概要

WLAN 導入時の適切なチャネル選択と送信パワー制御は、良好なパフォーマンスのために重要です。しかし、通常の WLAN ネットワークでは、重複しないチャネル数に対し、WLAN デバイス数は常に増加するため、チャネル重複,衝突,干渉は容易に発生します。

WLAN 最適化機能は、WLAN の品質と安定性の向上に役立ちます。

1.2 制限事項とガイドライン

特定の WLAN を最適化するために固定された組み合わせはありません。

コマンドの効果と WLAN のパフォーマンスに基づいて機能を選択し調整する必要があります。

WLAN の全体的なパフォーマンスは、ネットワークアーキテクチャ、チャネルと送信パワーによって決まります。従って、WLAN 最適化機能は WLAN の性能を著しく向上させることはできません。

1.3 APトリガのクライアント再関連付けの設定

I. AP トリガのクライアント再関連付けについて

クライアントは、クライアントのメーカーが定義した信号強度より低い場合にのみ、別の AP にローミングを行います。そのため、クライアントは良好なネットワークとサービス品質を得ることができません。

この機能を使用すると、クライアントの信号強度が指定された RSSI しきい値よりも低い場合に、AP は、認証解除フレームをクライアントに送信します。その後、クライアントは AP と再接続するか、別の AP にローミングします。

II. 設定手順

radio view での AP トリガのクライアント再関連付けの設定方法を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． AP を作成し、その view に移行する	**wlan ap** *ap-name*	―
3． radio view に移行する	**radio** *radio-id*	―

操作	コマンド	補足
4. AP トリガのクライアント再関連付けを設定する	**option client reconnect** { **disable** | **enable** [**rssi** *rssi-value*] [**interval** *interval*] }	デフォルト：AP group viewの設定を使用します。

AP group radio view での AP トリガのクライアント再関連付けの設定方法を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP グループを作成し、その view に移行する	**wlan ap-group** *group-name*	—
3. AP model view に移行する	**ap-model** *ap-model*	—
4. radio view に移行する	**radio** *radio-id*	—
5. AP トリガのクライアント再関連付けを設定する	**option client reconnect** { **disable** | **enable** [**rssi** *rssi-value*] [**interval** *interval*] }	デフォルト：無効

1.4 APのトラフィックスケジューリングモードの設定

🕮 **メモ：**

- この機能はソフトウェアバージョン 9.6.05c を含む以降のソフトウェアからサポートしています。

AP にフロー調整モードを設定すると、AC はチャネル利用状況、最大速度、クライアント数などの要因に基づいて利用可能な総帯域幅を計算します。その後、AC は指定したスケジューリングモードに基づいて AP に関連付けられたクライアントに利用可能な帯域幅を割り当てます。

- バランスモード: 帯域幅をクライアント間で均等に割り当てます。公平性を確保する必要があるオフィス環境などでの使用に適しています。
- クイックスピードモード: クライアントが自分のトラフィックに基づいて帯域幅を競います。高トラフィックのクライアントのパフォーマンスを確保する必要がある、少数のクライアントのシナリオで、このモードを使用することをお勧めします。
- インテリジェントモード: クライアントに帯域幅を均等に割り当て、アイドリングクライアントの余剰帯域幅を大きなトラフィックのクライアントにアルゴリズム計算に基づいて再割り当てできます。多くのクライアントと多数のアイドリングクライアントがいる環境でこのモードを使用すると、帯域幅の使用率が向上します。

I. 設定手順

radio view でのトラフィックスケジューリングモードの設定方法を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP を作成し、その view に移行する	**wlan ap** *ap-name*	—
3. radio view に移行する	**radio** *radio-id*	—

操作	コマンド	補足
4. トラフィックスケジューリングモードを設定する	**rrop flow-schedule mode** { **balanced** | **quick-speed** | **intelligent** [**channel-usage-threshold** *threshold-value* | **max** *max-value* | **min** *min-value*] }	デフォルト：AP group viewの設定を使用します。

AP group radio view でのトラフィックスケジューリングモードの設定方法を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. AP グループを作成し、その view に移行する	**wlan ap-group** *group-name*	―
3. AP model view に移行する	**ap-model** *ap-model*	―
4. radio view に移行する	**radio** *radio-id*	―
5. トラフィックスケジューリングモードを設定する	**rrop flow-schedule mode** { **balanced** | **quick-speed** | **intelligent** [**channel-usage-threshold** *threshold-value* | **max** *max-value* | **min** *min-value*] }	デフォルト：quick-speed

1.5 隠れ端末保護の設定

I. 隠れ端末保護について

この機能を使用すると、クライアントは隠れ端末からの干渉を避けるために、フレームを転送する前に 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。

II. 制限とガイドライン

この機能は 802.11g、802.11n、802.11ac、802.11ax のクライアントにのみ適用できます。

III. 設定手順

radio view での隠れたノード保護の設定方法を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. AP を作成し、その view に移行する	**wlan ap** *ap-name*	―
3. radio view に移行する	**radio** *radio-id*	―
4. 隠れ端末保護を設定する	**option client hide-node-protection** { **disable** | **enable** }	デフォルト：AP group viewの設定を使用します。

AP group radio view での AP トリガのクライアント再関連付けの設定方法を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP グループを作成し、その view に移行する	**wlan ap-group** *group-name*	—
3. AP model view に移行する	**ap-model** *ap-model*	—
4. radio view に移行する	**radio** *radio-id*	—
5. 隠れ端末保護を設定する	**option client hide-node-protection** { **disable** | **enable** }	デフォルト：無効

1.6 ブロードキャストおよびマルチキャストパケット制御の設定

I. ブロードキャストおよびマルチキャストパケット制御について

無線リソースを節約し、転送パフォーマンスを向上させるには、次の作業を実行します。

IPv4 ネットワークで基本的なブロードキャストおよびマルチキャストパケットを制御します。本機能を有効にすると、AP は ARP ブロードキャストパケットに応答し、DHCP ブロードキャストパケットを廃棄し、他のパケットを正常に処理します。

II. 設定手順

AP view でのブロードキャストおよびマルチキャストパケット制御の設定方法を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP を作成し、その view に移行する	**wlan ap** *ap-name*	—
3. ブロードキャストおよびマルチキャストパケットのパケット制御を設定する	**rrop anti-bmc network { disable | ipv4-simple enable }**	デフォルト：AP group viewの設定を使用します。

AP group view でのブロードキャストおよびマルチキャストパケット制御の設定方法を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP グループを作成し、その view に移行する	**wlan ap-group** *group-name*	—

操作	コマンド	補足
3. ブロードキャストおよびマルチキャストパケットのパケット制御を設定する	**rrop anti-bmc network { disable | ipv4-simple enable }**	デフォルト：ソフトウェアバージョンにより異なります。 ソフトウェアバージョン7.2.50を含む以前のソフトウェアでは有効です。 ソフトウェアバージョン7.2.52を含む以降のバージョンでは無効です。

1.7 ブロードキャストおよびマルチキャストのパケットレート制御の設定

I. ブロードキャストおよびマルチキャストのパケットレート制御について

無線リソースを節約し、転送パフォーマンスを向上させるには、次の作業を実行します。

AP は、ブロードキャストまたはマルチキャストパケットを無線インターフェイス経由で転送するレートを制限します。

II. 設定手順

AP view でのブロードキャスト、マルチキャストのパケットレート制限の設定方法を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP を作成し、その view に移行する	**wlan ap** *ap-name*	—
3. ブロードキャストまたはマルチキャストパケットのパケットレート制限を有効化する	**rrop anti-bmc { broadcast | multicast } rate-limit { disable | enable }**	デフォルト：AP group viewの設定を使用します。
4. ブロードキャストまたはマルチキャストパケットのパケットレート制限値を設定する	**rrop anti-bmc { broadcast | multicast } rate-limit pps** *max-pps*	デフォルト：AP group viewの設定を使用します。

AP group view でのブロードキャスト、マルチキャストのパケットレート制限の設定方法を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP グループを作成し、その view に移行する	**wlan ap-group** *group-name*	—
3. ブロードキャストまたはマルチキャストパケットのパケットレート制限を有効化する	**rrop anti-bmc { broadcast | multicast } rate-limit { disable | enable }**	デフォルト：無効

操作	コマンド	補足
4. ブロードキャストまたはマルチキャストパケットのパケットレート制限値を設定する	**rrop anti-bmc { broadcast | multicast } rate-limit pps** *max-pps*	ブロードキャスト：無制限 マルチキャスト：無制限

1.8 APアップリンクブロードキャストおよびマルチキャストパケットパケットのレート制限の設定

🕮 **メモ：**

AP アップリンクブロードキャストおよびマルチキャストパケットパケットのレート制限の設定は、ソフトウェアバージョン 9.4.09 を含む以降のソフトウェアからサポートしています。

I. ブロードキャストおよびマルチキャストパケット制御について

多数のクライアントからブロードキャスト パケットおよびマルチキャスト パケットを受信すると、AP の動作に影響を及ぼすおそれがあります。この問題を解決するために、AP が各クライアントから受信するブロードキャスト パケットとマルチキャスト パケットのレートを制限することができます。この機能を設定すると、AP はレート制限のしきい値を超える過剰な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廃棄します。

II. 設定手順

AP view での AP アップリンクブロードキャストおよびマルチキャストパケットのレート制限の設定方法を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. AP を作成し、その view に移行する	**wlan ap** *ap-name*	―
3. AP のアップリンクブロードキャストおよびマルチキャストパケットのレート制限を設定する	**rrop anti-bmc** { **broadcast | multicast** } **upstream client-rate-limit enable**	デフォルト：AP group viewの設定を使用します。AP group viewに設定がない場合、System viewの設定を使用します。
4. AP が各クライアントから受信するブロードキャストもしくはマルチキャストパケットのレートを設定します。	**rrop anti-bmc** { **broadcast | multicast** } **upstream client-rate-limit pps** *max-pps*	デフォルト：AP group viewの設定を使用します。AP group viewに設定がない場合、System viewの設定を使用します。

AP group view での AP アップリンクブロードキャストおよびマルチキャストパケットのレート制限の設定方法を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―

操作	コマンド	補足
2. APグループを作成し、その view に移行する	**wlan ap-group** *group-name*	ー
3. APのアップリンクブロードキャストおよびマルチキャストパケットのレート制限を設定する	**rrop anti-bmc** { **broadcast** | **multicast** } **upstream client-rate-limit enable**	デフォルト： System viewの設定を使用します。
4. APが各クライアントから受信するブロードキャストもしくはマルチキャストパケットのレートを設定します。	**rrop anti-bmc** { **broadcast** | **multicast** } **upstream client-rate-limit pps** *max-pps*	デフォルト： System viewの設定を使用します。

System view での AP アップリンクブロードキャストおよびマルチキャストパケットのレート制限の設定方法を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. APのアップリンクブロードキャストおよびマルチキャストパケットのレート制限を設定する	**rrop anti-bmc** { **broadcast** | **multicast** } **upstream client-rate-limit enable**	デフォルト：無効
3. APが各クライアントから受信するブロードキャストもしくはマルチキャストパケットのレートを設定します。	**rrop anti-bmc** { **broadcast** | **multicast** } **upstream client-rate-limit pps** *max-pps*	デフォルト： APが各クライアントから受信したブロードキャストもしくはマルチキャストパケットのレートは制限されません。

1.9 クライアント高速キープアライブの設定

I. クライアント高速キープアライブの設定について

この機能により、AP は、クライアントに送信されたユニキャストパケットの確認応答状態に基づいて、クライアントがまだオンラインであるかどうかを確認することができます。AP はユーザーデータを 3 つのグループに分けて個別にカウントします。キープアライブの間隔 (interval-value パラメータで設定) 中に、3 グループのユニキャストパケットの確認応答が受信されなかった場合、AP はクライアントがオフラインであると判断し、クライアントへの接続を終了します。これにより、無線リソースの使用率が向上します。グループ内のユニキャストパケットの数は、count-value パラメータで設定します。

この機能は、クライアントの移動性が高いシナリオに適用することができます。ネットワーク品質が悪い場合は、キープアライブカウントを減らすか、キープアライブ間隔を短くする必要があります。

II. 設定手順

AP の radio view でのクライアント高速キープアライブの設定方法を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． AP グループを作成し、その view に移行する	**wlan ap** *ap-name*	―
3． radio view に移行する	**radio** *radio-id*	―
4． クライアント高速キープアライブを設定する	**rrop client fast-keep-alive** { **disable** | **enable** [**count** *count-value*] [**interval** *interval-value*]	デフォルト : AP group radio view の設定を使用します。

AP group radio view でのクライアント高速キープアライブの設定方法を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． AP グループを作成し、その view に移行する	**wlan ap-group** *group-name*	―
3． AP model view に移行する	**ap-model** *ap-model*	―
4． radio view に移行する	**radio** *radio-id*	―
5． クライアント高速キープアライブを設定する	**rrop client fast-keep-alive** { **disable** | **enable** [**count** *count-value*] [**interval** *interval-value*]	デフォルト：有効 (count 450、interval 10)

目次

このセクションのページは **12-x-x** です。

2 章 WLAN メッシュの設定 2-1
2.1 概要 2-1
2.1.1 WLAN メッシュネットワーク 2-1
2.1.2 メッシュプロファイル 2-2
2.1.3 ネイバ検出とメッシュリンク確立 2-2
2.1.4 無線配置システム 2-3
2.1.5 メッシュピアブラックリスト、ホワイトリスト 2-5
2.1.6 プロトコルと標準 2-5
2.2 WLAN メッシュ設定の制限とガイドライン 2-6
2.3 WLAN メッシュ設定作業リスト 2-6
2.4 メッシュプロファイルの設定 2-6
2.5 無線へのメッシュプロファイルのバインド 2-7
2.6 メッシュポリシーの設定 2-8
2.7 無線へのメッシュポリシーのバインド 2-8
2.8 MPP のプローブ要求送信無効化 2-9
2.9 同一 AC に関連付く MPP がメッシュピアになることの有効化 2-10
2.10 メッシュピアブラックリスト・ホワイトリストの設定 2-11
2.11 メッシュインタフェースの設定 2-11
2.11.1 メッシュインタフェースの作成 2-11
2.11.2 メッシュインタフェースへのアクセスポート属性の設定 2-12
2.11.3 メッシュインタフェースへのトランクポート属性の設定 2-13
2.11.4 メッシュインタフェースへのハイブリッドポート属性の設定 2-14
2.11.5 無線へのメッシュインタフェースのバインド 2-15
2.12 WLAN メッシュのための表示と保守コマンド 2-16
2.13 WLAN メッシュ設定例 2-16
2.13.1 WLAN メッシュの設定例 2-16
2.13.2 LAN メッシュネットワークの VLAN 設定の設定例 2-19

2章 WLAN メッシュの設定

2.1 概要

WLAN メッシュにより、AP 同士が無線で接続できます。WLAN メッシュネットワーク上の AP が直接、あるいは複数の AP を介して接続できます。1 台の AP で障害が発生したとき、残りの AP が互いに通信を継続します。

2.1.1 WLAN メッシュネットワーク

1 章 に WLAN メッシュネットワークを示します。

WLAN メッシュネットワークの AP はメッシュポイント（MP）です。MP は以下の役割を担います。

- シングルパーパス MP－メッシュサービスのみ提供します。
- メッシュアクセスポイント（MAP）－メッシュサービスとアクセスサービスを提供します。
- メッシュポータルポイント（MPP）－有線ネットワークに有線接続を提供します。

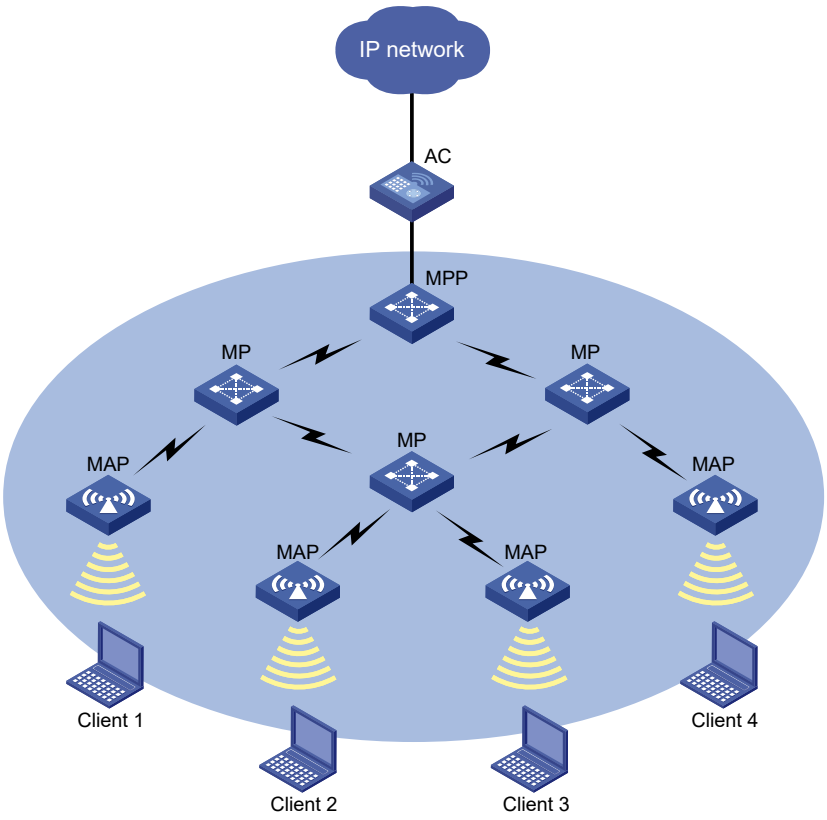


図2-1 WLAN メッシュネットワーク図

2.1.2 メッシュプロファイル

メッシュプロファイルは、メッシュネットワークを運用するためのメッシュプロトコルの集まりです。メッシュプロファイルには以下の属性が含まれます。

- メッシュ ID－メッシュネットワークを識別します。
- メッシュセキュリティー認証、鍵管理モード、事前共有鍵などネイバ認証のための設定を含みます。
- Keepalive 間隔－メッシュリンク内に Keepalive パケットを送信する間隔を指定します。MAC アドレスの大きい MP は Keepalive 間隔で Keepalive パケットを終端まで送信します。Keepalive パケットを送信した MP は、3 回連続の Keepalive 間隔以内に応答を受信しない場合、メッシュリンクを切断します。Keepalive パケットを受信する MP が 3 回連続の Keepalive 間隔以内に 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。リンク状態を正確に検出するために、送信端の Keepalive 間隔は受信端の Keepalive 間隔の 3 倍以下に設定してください。

メッシュネットワークを形成するために、AP は同じメッシュ ID とメッシュセキュリティ設定にする必要があります。

2.1.3 ネイバ検出とメッシュリンク確立

MP は、互いに検出できるように同じラジオとチャネルで動作する必要があります。MP は、互いに検出した後メッシュリンクを確立できます。

利用可能な検出方法は以下の通りです。

- **アクティブスキャニング**－MP はネイバを検出し、メッシュリンクを確立するためにプローブ要求フレームを送信します。
- **パッシブスキャニング**－MP は他の MP の情報を収集するためビーコンフレームを受信します。ネイバが存在する場合、AP はメッシュリンクを確立するためプローブ要求フレームを送信します。

この章では、アクティブスキャニングでのネイバ検出およびメッシュリンク確立のプロセスを説明します。

図 2-2 に示すように、MP はプローブ要求フレームとプローブ応答フレーム内のメッシュプロファイルを交換することでメッシュリンクを確立します。

以下の条件が満たされると、MP は別の MP をメッシュピアとして追加します。

- MP のメッシュプロファイルが一致する。
- 受信した要求もしくは応答内にピアリンクを承認するビットが設定されている。

MP 同士は互いにリンクオープン要求を送信することでメッシュリンクを確立します。メッシュリンクは、MP 同士が互いのリンクオープン要求を認識したあとに確立されます。

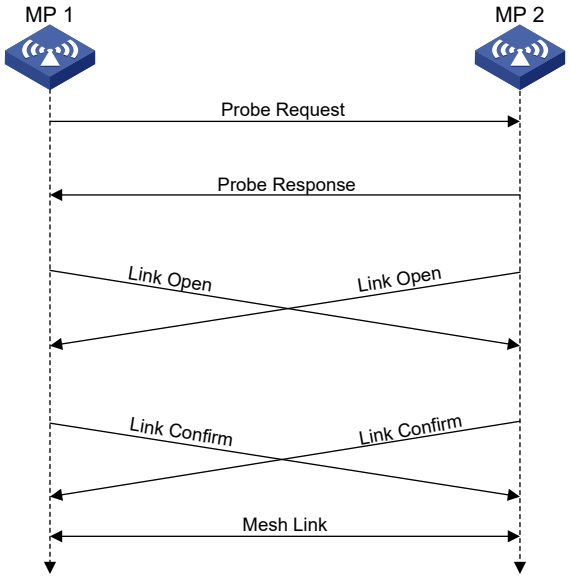


図2-2 ネイバ検出と WLAN メッシュネットワークでのメッシュリンク確立

AP は、メッシュリンクを確立するために AC からメッシュプロファイルを取得する必要があります。AP はメッシュリンク確立前に以下のタスクを実行します。

1) AC を発見するため、最初に検出した WLAN メッシュネットワークと一時的なメッシュリンク（テンポラリリンク）を確立します。テンポラリリンクではコンフィグレーションデータのみ転送できます。
2) メッシュプロファイルを含むコンフィグレーションを取得するため、AC との CAPWAP トンネル確立を試行します。
3) コンフィグレーションを取得後、テンポラリリンクを切断します。（テンポラリリンクは 2 分程度で切断されます。）

上記タスク実行後、AP はネイバ検出を実行し、WLAN メッシュネットワークに参加するためメッシュリンクを確立します。

AP が AC との CAPWAP トンネル確立に失敗した場合、AP は検出した他のメッシュネットワーク 1 つ 1 つに対してメッシュリンクの確立を試行します。

2.1.4 無線配置システム

無線配置システム（WDS）は WLAN メッシュのアプリケーションです。WDS は、各所に配置された LAN を接続するために AP 間のメッシュリンクを使用します。AP は、LAN からきた 802.3 フレームを、802.11s フレームとしてメッシュリンクに転送します。

管理上選択した AP 間でメッシュリンクを確立させることで、point-to-point トポロジもしくはスタートポロジでの WDS を作成できます。もしくは、自動ネイバ検出により、AP が自動的に作成したトポロジを使用できます。メッシュピアホワイトリストを設定しないことで、自動ネイバ検出が可能です。

I. Point-to-point トポロジ

図 2-3 に示すように、2 つの LAN を接続するために 2 台の AP 間でメッシュリンクを設定できます。



図2-3 WDS point-to-point トポロジ

II. スタートポロジ

図 2-4 に示すように、1 台の中心となる AP と複数の AP 間でメッシュリンクを設定し、複数の LAN を接続できます。

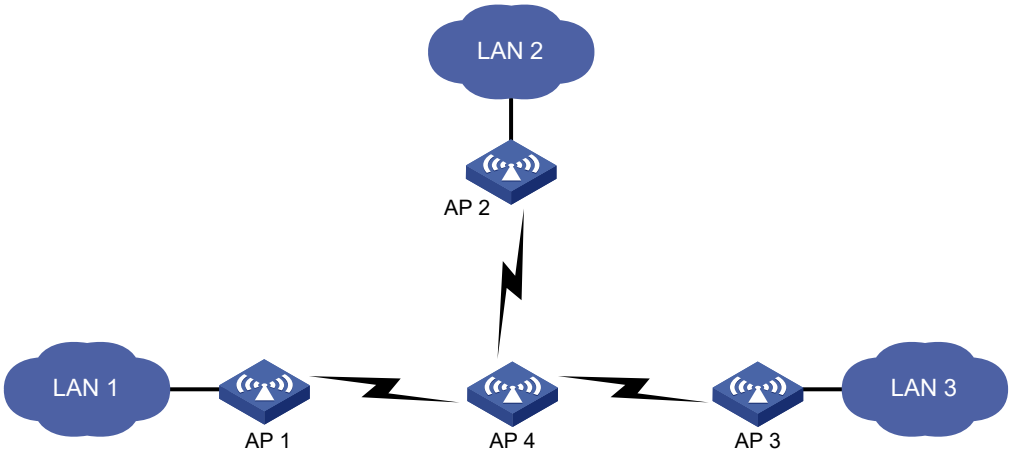


図2-4 スタートポロジ

III. 管理なしで作成されたトポロジ

接続する AP を指定しない場合、WDS トポロジは AP 間の自動ネイバ検出とメッシュリンク確立に依存します。

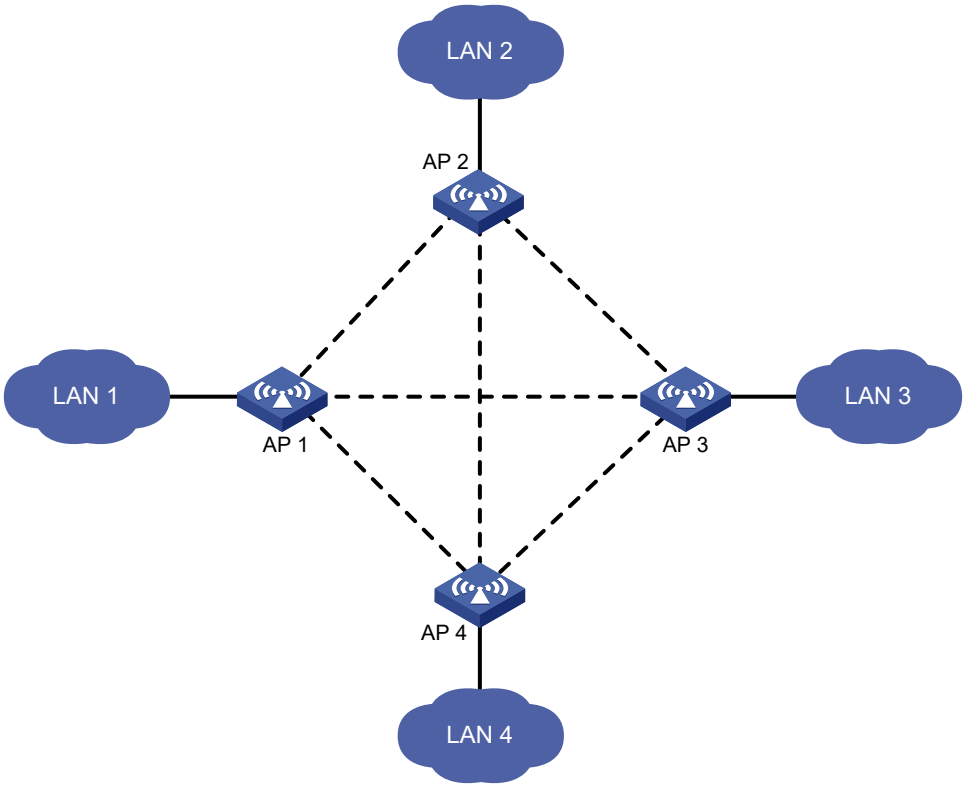


図2-5 自動トポロジ設定

2.1.5 メッシュピアブラックリスト、ホワイトリスト

ネイバ MP がローカル MP とメッシュリンクを確立できるかどうかをコントロールするため、ブラックリストもしくはホワイトリストを設定できます。

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。つまり、ホワイトリスト内のネイバ MP のみローカル MP とメッシュリンクを確立できます。また、ブラックリストのみ設定した場合、ブラックリスト内のネイバ MP はローカル MP とメッシュリンクを確立できません。

2.1.6 プロトコルと標準

- Draft P802.11s_D1.06
- ANSI/IEEE Std 802.11, 1999 Edition
- IEEE Std 802.11a
- IEEE Std 802.11b
- IEEE Std 802.11g
- IEEE Std 802.11i
- IEEE Std 802.11s
- IEEE Std 802.11-2004
- draft-ohara-capwap-lwapp-03

2.2 WLANメッシュ設定の制限とガイドライン

以下の方法により AP を設定できます。

- AP view で 1 台ずつ AP を設定します。
- AP group view に AP を割り当て、AP group view にて設定します。
- global configuration view ですべての AP を設定します。

AP view、AP group view、global configuration view に同様の設定をした場合、AP view、AP group view、global configuration view の順に設定が適用されます。

🕮 **メモ：**

レーダ検出時のチャネル移動において、メッシュ AP 間でチャネルを同じにする機能はありません。メッシュ接続にはレーダ検出が必要なチャネルの使用は推奨しません。

2.3 WLAN メッシュ設定作業リスト

作業リスト	補足
（必須設定項目）メッシュプロファイルの設定	ー
（必須設定項目）ラジオへのメッシュプロファイルのバインド	ー
（オプション設定項目）メッシュポリシーの設定	メッシュリンクの設定調整や保守のためにこの作業を実施します。
（オプション設定項目）ラジオへのメッシュポリシーのバインド	ー
（オプション設定項目）MPPのプローブ要求送信無効化	ー
（オプション設定項目）メッシュピアになるために同一ACに関連付くMPPの有効化	ー
（オプション設定項目）メッシュピアブラックリスト/ホワイトリストの設定	MPが適切なネイバMPとメッシュリンクを確立することを保証するためにこの作業を実施します。
（オプション設定項目）メッシュインタフェースの設定	ー

2.4 メッシュプロファイルの設定

I. 制限とガイドライン

同一メッシュネットワーク内の MP は、メッシュ ID とメッシュセキュリティ設定を同一にする必要があります。

リンク状態を正確に検出するために、送信端の keepalive 間隔は受信端の keepalive 間隔の 3 倍以下に設定して下さい。

II. 設定手順

操作	コマンド	補足
1． system view に移行する	**system-view**	—

操作	コマンド	補足
2． メッシュプロファイルを作成し、view に移行する	**wlan mesh-profile** *mesh-profile-number*	デフォルト：設定なし
3． メッシュ ID を指定する	**mesh-id** *mesh-id*	デフォルト：設定なし
4． （オプション設定項目）メッシュセキュリティを設定する	**a.** SAE認証と鍵管理モードを有効にする **akm mode sae** b. 事前共有鍵を設定する **preshared-key** { **pass-phrase** | **raw-key** } { **cipher** | **simple** } *string*	デフォルト：設定なし
5． （オプション設定項目）メッシュリンク keepalive 間隔を設定する	**link-keepalive** *keepalive-interval*	デフォルト：2秒
6． メッシュプロファイルを有効にする	**mesh-profile enable**	デフォルト：無効

2.5 無線へのメッシュプロファイルのバインド

I. メッシュプロファイルバインディング

AP がメッシュネットワークに参加するためには、AP の無線にメッシュプロファイルをバインドする必要があります。AP が異なるメッシュネットワークに参加できるように、無線インタフェースに異なるメッシュプロファイルをバインドできます。

II. 設定手順

AP view での設定方法は以下の通りです。

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP view に移行する	**wlan ap** *ap-name*	—
3． radio view に移行する	**radio** *radio-id*	—
4． 無線インタフェースにメッシュプロファイルをバインドする	**mesh-profile** *mesh-profile-number*	デフォルト：AP group radio viewの設定を使用します。

AP group view での設定方法は以下の通りです。

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP group view に移行する	**wlan ap-group** *group-name*	—
3． AP model view に移行する	**ap-model** *ap-model*	—
4． radio view に移行する	**radio** *radio-id*	—

操作	コマンド	補足
5. 無線インタフェースにメッシュプロファイルをバインドする	**mesh-profile** *mesh-profile-number*	デフォルト：バインドされていません。

2.6 メッシュポリシーの設定

I. メッシュポリシー

メッシュポリシーはメッシュリンクの設定と保守の役割を含みます。

🕮 **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。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. メッシュポリシーを作成し、view に移行する	**wlan mesh-policy** *policy-name*	デフォルト：システム定義のメッシュポリシーが存在します。そのポリシー名は **default_mesh_policy**です。
3. （オプション設定項目）リンク開始を有効にする	**link-initiation enable**	デフォルト：有効
4. （オプション設定項目）メッシュリンクの最大数を設定する	**link-maximum-number** *max-link-number*	デフォルト：2
5. （オプション設定項目）プローブ要求間隔を設定する	**probe-request-interval** *interval-value*	デフォルト：1000ms
6. （オプション設定項目）メッシュリンクホールド RSSI（メッシュリンクを保持する最小信号強度）を設定する	**link-hold-rssi** *value*	デフォルト：15dBm

2.7 無線へのメッシュポリシーのバインド

I. メッシュポリシーバインディング

デフォルトでは、システム定義のメッシュポリシーが各無線にバインドされています。このシステム定義のメッシュポリシーは削除または修正できません。無線のリンク設定と保

守設定を変更するには、ユーザ定義のメッシュポリシーを無線インタフェースにバインドし、システム定義のメッシュポリシーと置き換える必要があります。

II. 設定手順

AP view での設定方法は以下の通りです。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP view に移行する	**wlan ap** *ap-name*	—
3. radio view に移行する	**radio** *radio-id*	—
4. 無線インタフェースにメッシュポリシーをバインドする	**mesh-policy name** *policy-name*	デフォルト：AP groupのRadio viewの設定を使用します。

AP group view での設定方法は以下の通りです。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP group view に移行する	**wlan ap-group** *group-name*	—
3. AP model view に移行する	**ap-model** *ap-model*	—
4. radio view に移行する	**radio** *radio-id*	—
5. 無線インタフェースにメッシュポリシーをバインドする	**mesh-policy name** *policy-name*	デフォルト：APグループのRadio viewにはシステム定義のメッシュポリシー **default_mesh_policy**がバインドされています。

2.8 MPPのプローブ要求送信無効化

I. プローブ要求送信無効化について

WLAN メッシュネットワークを有線ネットワークに接続する際、MPP は多くのメッシュリンクを確立しなければならない可能性があります。MPP のパフォーマンスを維持するため、MPP がネイバ検出のためにプローブ要求を送信するのを無効にすることができます。MPP は他の MP からのプローブ要求にのみ応答します。

II. 設定手順

AP view での設定方法は以下の通りです。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP view に移行する	**wlan ap** *ap-name*	—

操作	コマンド	補足
3. MPP のプローブ要求送信を無効にする	**portal-service enable**	デフォルト：AP group viewの設定を使用します。AP group viewに設定がない場合、global configuration viewの設定を使用します。

AP group view での設定方法は以下の通りです。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP group view に移行する	**wlan ap-group** *group-name*	—
3. MPP のプローブ要求送信を無効にする	**portal-service enable**	デフォルト： global configuration viewの設定を使用します。

global configuration view での設定方法は以下の通りです。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. global configuration view に移行する	**wlan global configuration**	—
3. MPP のプローブ要求送信を無効にする	**portal-service enable**	デフォルト： MPPはプローブ要求を送信できます。

2.9 同一ACに関連付くMPPがメッシュピアになることの有効化

I. 同一 AC に関連付くメッシュピアについて

ループを避けるため、同一 AC に関連付く MPP 同士はデフォルトではメッシュピアになることはできません。同一 AC に関連付いた MPP 同士がメッシュピアになるためには、本機を有効にしてください。同一 AC に関連付いた MPP が VLAN1 に属さないことを確認してください。また、ループを防ぐため、すべての装置に STP を設定してください。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. global configuration view に移行する	**wlan global configuration**	—
3. 同一 AC の MPP がメッシュピアになることを有効にする	**mesh-peer intra-ac-mpp enable**	デフォルト： ループを防ぐため、同一ACに関連付いたMPPはメッシュピアになれません。

2.10 メッシュピアブラックリスト・ホワイトリストの設定

AP view での設定方法は以下の通りです。

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP view に移行する	**wlan ap** *ap-name*	—
3． radio view に移行する	**radio** *radio-id*	—
4． MP の MAC アドレスを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追加する	**mesh peer-mac-address** [**blacklist**] *mac-address*	デフォルト：AP group viewの設定を使用します。

AP group view での設定方法は以下の通りです。

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP group view に移行する	**wlan ap-group** *group-name*	—
3． AP model view に移行する	**ap-model** *ap-model*	—
4． radio view に移行する	**radio** *radio-id*	—
5． MP の MAC アドレスを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追加する	**mesh peer-mac-address** [**blacklist**] *mac-address*	デフォルト：設定なし ブラックリスト（ホワイトリスト）にMAのMACアドレスを追加するにはこの操作を繰り返します。 同一のMACアドレスを追加しようとした場合、最後の設定が適用されます。

2.11 メッシュインタフェースの設定

2.11.1 メッシュインタフェースの作成

I. メッシュインタフェースの作成について

MP がメッシュネットワークの同一 VLAN で互いに通信できるようにメッシュインタフェースを作成します。

II. 設定手順

AP view での設定方法は以下の通りです。

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP view に移行する	**wlan ap** *ap-name*	—

操作	コマンド	補足
3. メッシュインタフェースを作成し、その view に移行する	**interface wlan-mesh** *interface-number*	デフォルト：設定なし

AP group view での設定方法は以下の通りです。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP group view に移行する	**wlan ap-group** *group-name*	—
3. メッシュインタフェースを作成し、その view に移行する	**interface wlan-mesh** *interface-number*	デフォルト：設定なし

2.11.2 メッシュインタフェースへのアクセスポート属性の設定

I. アクセスポートについて

アクセスポートでは 1 つの VLAN のみ許可します。

II. 制限とガイドライン

メッシュインタフェースにアクセスポートを設定する前に VLAN が存在することを確認してください。

III. 設定手順

AP view での設定方法は以下の通りです。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP view に移行する	**wlan ap** *ap-name*	—
3. メッシュインタフェースを作成し、その view に移行する	**interface wlan-mesh** *interface-number*	デフォルト：設定なし
4. メッシュインタフェースのリンクタイプをアクセスに設定する	**mesh-port link-type access**	デフォルト：アクセスポート
5. アクセスタイプのメッシュインタフェースに VLAN を割り当てる	**mesh-port access vlan** *vlan-id*	デフォルト：VLAN 1

AP group view での設定方法は以下の通りです。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP group view に移行する	**wlan ap-group** *group-name*	—

操作	コマンド	補足
3. メッシュインタフェースを作成し、その view に移行する	**interface wlan-mesh** *interface-number*	デフォルト：設定なし
4. メッシュインタフェースのリンクタイプをアクセスに設定する	**mesh-port link-type access**	デフォルト：アクセスポート
5. アクセスタイプのメッシュインタフェースに VLAN を割り当てる	**mesh-port access vlan** *vlan-id*	デフォルト：VLAN 1

2.11.3 メッシュインタフェースへのトランクポート属性の設定

I. トランクポートについて

トランクポートでは複数の VLAN を許可します。

II. 制限とガイドライン

ポートのリンクタイプをトランクとハイブリッド間で変更する場合、一度リンクタイプをアクセスに設定してください。

存在しない VLAN をトランクポートのポート VLAN として指定できます。

トランクポートがポート VLAN からパケットを転送できるようにするには、ポート VLAN にトランクポートを割り当てる必要があります。

III. 設定手順

AP view での設定方法は以下の通りです。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP view に移行する	**wlan ap** *ap-name*	—
3. メッシュインタフェースを作成し、その view に移行する	**interface wlan-mesh** *interface-number*	デフォルト：設定なし
4. メッシュインタフェースのリンクタイプをトランクに設定する	**mesh-port link-type trunk**	デフォルト：アクセスポート
5. トランクポートに PVID を設定する	**mesh-port trunk pvid vlan** *vlan-id*	デフォルト：VLAN 1
6. トランクタイプのメッシュインタフェースに VLAN を割り当てる	**mesh-port trunk permit vlan** { *vlan-id-list* | **all** }	デフォルト：VLAN1のみ

AP group view での設定方法は以下の通りです。

操作	コマンド	補足
1. system view に移行する	**system-view**	—

操作	コマンド	補足
2． AP group view に移行する	**wlan ap-group** *group-name*	—
3． メッシュインタフェースを作成し、その view に移行する	**interface wlan-mesh** *interface-number*	デフォルト：設定なし
4． メッシュインタフェースのリンクタイプをトランクに設定する	**mesh-port link-type trunk**	デフォルト：アクセスポート
5． トランクポートに PVID を設定する	**mesh-port trunk pvid vlan** *vlan-id*	デフォルト：VLAN 1
6． トランクタイプのメッシュインタフェースに VLAN を割り当てる	**mesh-port trunk permit vlan** { *vlan-id-list* | **all** }	デフォルト：VLAN1のみ

2.11.4 メッシュインタフェースへのハイブリッドポート属性の設定

I. ハイブリッドポートについて

ハイブリッドポートでは複数の VLAN を許可します。

II. 制限とガイドライン

ポートのリンクタイプをトランクとハイブリッド間で変更する場合、一度リンクタイプをアクセスに設定してください。

存在しない VLAN をハイブリッドポートのポート VLAN として指定できます。

すでに存在している VLLAN にハイブリッドポートを割り当てていることを確認してください。

ハイブリッドポートがポート VLAN からパケットを転送できるようにするには、ポート VLAN にハイブリッドポートを割り当てる必要があります。

III. 設定手順

AP view での設定方法は以下の通りです。

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP view に移行する	**wlan ap** *ap-name*	—
3． メッシュインタフェースを作成し、その view に移行する	**interface wlan-mesh** *interface-number*	デフォルト：設定なし
4． メッシュインタフェースのリンクタイプをハイブリッドに設定する	**mesh-port link-type hybrid**	デフォルト：アクセスポート
5． ハイブリッドポートに PVID を設定する	**mesh-port hybrid pvid vlan** *vlan-id*	デフォルト：ハイブリッドポートのPVIDは、リンクタイプがアクセスであるときにポートが所属しているVLANのIDです。

操作	コマンド	補足
6. ハイブリッドタイプのメッシュインタフェースに VLAN を指定する	**mesh-port hybrid permit vlan** *vlan-id-list* { **tagged** | **untagged** }	デフォルト：ハイブリッドポートは、リンクタイプがアクセスであるときにポートが所属しているVLANのタグなしメンバです。

AP group view での設定方法は以下の通りです。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP group view に移行する	**wlan ap-group** *group-name*	—
3. メッシュインタフェースを作成し、その view に移行する	**interface wlan-mesh** *interface-number*	デフォルト：設定なし
4. メッシュインタフェースのリンクタイプをハイブリッドに設定する	**mesh-port link-type hybrid**	デフォルト：アクセスポート
5. ハイブリッドポートに PVID を設定する	**mesh-port hybrid pvid vlan** *vlan-id*	デフォルト：ハイブリッドポートのPVIDは、リンクタイプがアクセスであるときにポートが所属しているVLANのIDです。
6. ハイブリッドタイプのメッシュインタフェースに VLAN を指定する	**mesh-port hybrid permit vlan** *vlan-id-list* { **tagged** | **untagged** }	デフォルト：ハイブリッドポートは、リンクタイプがアクセスであるときにポートが所属しているVLANのタグなしメンバです。

2.11.5 無線へのメッシュインタフェースのバインド

I. 制限とガイドライン

AP view で作成されたメッシュインタフェースは、radio view 内のラジオにのみバインドできます。AP group view で作成されたメッシュインタフェースは radio view と AP group radio view のどちらのラジオにもバインドできます。

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。

II. 設定手順

AP view での設定方法は以下の通りです。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP view に移行する	**wlan ap** *ap-name*	—
3. radio view に移行する	**radio** *radio-id*	—
4. 無線インタフェースにメッシュインタフェースをバインドする	**mesh-interface** *interface-number*	デフォルト：AP group radio viewの設定を使用します。

AP group view での設定方法は以下の通りです。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP group view に移行する	**wlan ap-group** *group-name*	—
3. AP model view に移行する	**ap-model** *ap-model*	—
4. radio view に移行する	**radio** *radio-id*	—
5. ラジオにメッシュインタフェースをバインドする	**mesh-interface** *interface-number*	デフォルト：設定なし

2.12 WLANメッシュのための表示と保守コマンド

display コマンドはすべての view で実行できます。

操作	コマンド
メッシュリンク情報を表示する	**display wlan mesh-link ap** [**name** *ap-name*] [**verbose**]
メッシュポリシー情報を表示する	**display wlan mesh-policy** [*mesh-policy-name*]
メッシュプロファイル情報を表示する	**display wlan mesh-profile** [*mesh-profile-number*]

2.13 WLANメッシュ設定例

2.13.1 WLAN メッシュの設定例

I. ネットワーク設定

図 2-6 に示すように、クライアントにネットワークアクセスを提供するために 802.11n 5GHz WLAN メッシュネットワークを確立します。チャネル 36 でメッシュリンクを確立するために、MPP と MAP1 と MAP2 を設定します。

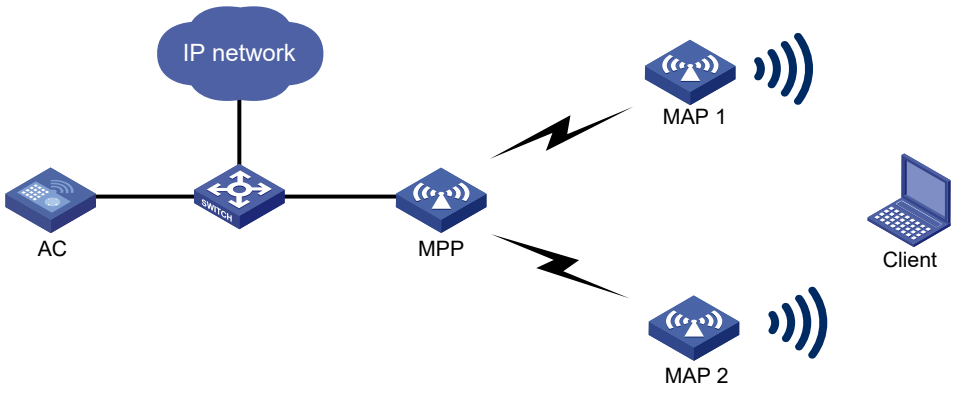


図2-6 ネットワーク図

II. 設定手順

1)　MPP を設定します。

メッシュプロファイルを設定します。

```
<AC> system-view
[AC] wlan mesh-profile 1
```

メッシュ ID を 1 に設定します。

```
[AC-wlan-mesh-profile-1] mesh-id 1
```

認証と鍵管理に対して SAE を有効にします。

```
[AC-wlan-mesh-profile-1] akm mode sae
```

事前共有鍵を設定します。

```
[AC-wlan-mesh-profile-1] preshared-key pass-phrase simple 12345678
```

メッシュプロファイルを有効にします。

```
[AC-wlan-mesh-profile-1] mesh-profile enable
[AC-wlan-mesh-profile-1] quit
```

2)　サービステンプレートを設定します。

```
[AC] wlan service-template service1
[AC-wlan-st-service1] ssid mesh-network
[AC-wlan-st-service1] service-template enable
[AC-wlan-st-service1] quit
```

3)　MPP の設定を行います。

MPP に対して AP view を作成します。適切な AP モデル、シリアル ID を選択、指定していることを確認してください。

```
[AC] wlan ap mpp1 model QX-W1030
[AC-wlan-ap-mpp1] serial-id 219801A1K0917BG0000S
```

メッシュプロファイルを MPP のラジオ 1 にバインドします。

```
[AC-wlan-ap-mpp] radio 1
[AC-wlan-ap-mpp-radio-1] mesh-profile 1
```

MPP のラジオ 1 の無線タイプを 802.11n(5GHz)に設定します。

```
[AC-wlan-ap-mpp-radio-1] type dot11an
```

無線の作動チャネルを 36 に設定します。

```
[AC-wlan-ap-mpp-radio-1] channel 36
```

ラジオを有効にします。

```
AC-wlan-ap-mpp-radio-1] radio enable
```

```
[AC-wlan-ap-mpp-radio-1] quit
```

4)　MAP を設定します。

MAP1 の AP view を作成します。適切な AP モデル、シリアル ID を選択、指定していることを確認してください。

```
[AC] wlan ap map1 model QX-W1030
[AC-wlan-ap-map1] serial-id 219801A1K0917BG0000B
```

MAP のラジオ 1 にメッシュプロファイルをバインドします。

```
[AC-wlan-ap-map1] radio 1
[AC-wlan-ap-map1-radio-1] mesh-profile 1
```

MAP のラジオ 1 にサービステンプレートをバインドします。

```
[AC-wlan-ap-map1-radio-1] service-template service1
```

MAP のラジオ 1 の無線タイプを 802.11n(5GHz)に設定します。

```
[AC-wlan-ap-map1-radio-1] type dot11an
```

無線の作動チャネルを 36 に設定します。

```
[AC-wlan-ap-map1-radio-1] channel 36
```

ループを防ぐために MPP の MAC アドレスをメッシュピアホワイトリストに追加します。MAP1 は MPP とのみメッシュリンクを確立できます。

```
[AC-wlan-ap-map1-radio-1] mesh peer-mac-address 77a2-c25d-e316
```

ラジオを有効にします。

```
[AC-wlan-ap-map1-radio-1] radio enable
[AC-wlan-ap-map1-radio-1] quit
[AC-wlan-ap-map1] quit
```

MAP2 に対して MAP1 と同様に設定します。

```
[AC] wlan ap map2 model QX-W1030
[AC-wlan-ap-map2] serial-id 210235A29G007C000090
[AC-wlan-ap-map2] radio 1
[AC-wlan-ap-map2-radio-1] mesh-profile 1
[AC-wlan-ap-map2-radio-1] service-template service1
[AC-wlan-ap-map2-radio-1] type dot11an
[AC-wlan-ap-map2-radio-1] channel 36
[AC-wlan-ap-map2-radio-1] mesh peer-mac-address 77a2-c25d-e316
[AC-wlan-ap-map2-radio-1] radio enable
[AC-wlan-ap-map2-radio-1] quit
[AC-wlan-ap-map2] quit
```

```
[AC] quit
```

III. 設定の確認

MPP が MAP とメッシュリンクを確立することを確認します。

```
<AC> display wlan mesh-link ap
 AP Name: mpp
 Peer           Local          Status     RSSI Packets(Rx/Tx)
 4a9b-c5bb-e43f 77a2-c25d-e316 Forwarding 22   6058/1900
 a6b5-1c5a-22ff 77a2-c25d-e316 Forwarding 35   5354/1900

AP Name: map1
 Peer           Local          Status     RSSI Packets(Rx/Tx)
 77a2-c25d-e316 4a9b-c5bb-e43f Forwarding 22   1900/6058

AP Name: map2
 Peer           Local          Status     RSSI Packets(Rx/Tx)
 77a2-c25d-e316 a6b5-1c5a-22ff Forwarding 35   1900/5354
```

クライアントが AP と関連付いたことを確認します。

```
<AC> display wlan client
 Total number of clients: 1

MAC address     Username              AP name                 R IP address
VLAN
000f-e265-6400 N/A                map1                1 1.1.1.1        300
```

2.13.2 LAN メッシュネットワークの VLAN 設定の設定例

I. ネットワーク設定

図 2-7 に示すように、LAN1 と LAN2 は VLAN2 に属しています。チャネル 36 でメッシュリンクを確立し、VLAN2 からのトラフィックを許可するように MPP1 と MPP2 を設定します。

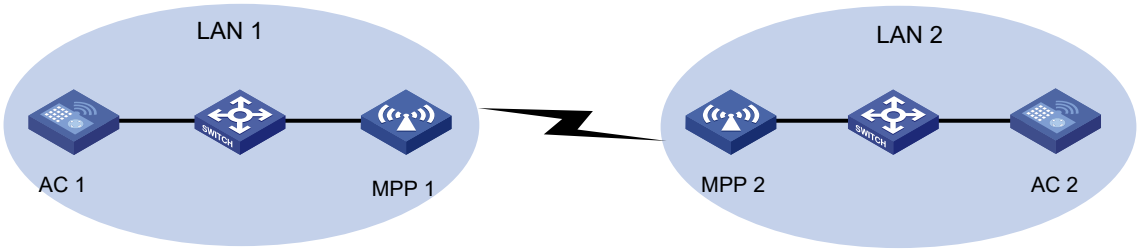


図2-7 ネットワーク図

II. 設定手順

1)　AP1 を設定します。

メッシュプロファイルを作成します。

```
<AC1> system-view
```

```
[AC1] wlan mesh-profile 1
```

メッシュ ID を 1 に設定します。

```
[AC1-wlan-mesh-profile-1] mesh-id 1
```

認証と鍵管理に対して SAE を有効にします。

```
[AC1-wlan-mesh-profile-1] akm mode sae
```

事前共有鍵を設定します。

```
[AC1-wlan-mesh-profile-1] preshared-key pass-phrase simple 12345678
```

メッシュプロファイルを有効にする。

```
AC1-wlan-mesh-profile-1] mesh-profile enable
[AC1-wlan-mesh-profile-1] quit
```

2)　サービステンプレートを設定します。

```
[AC] wlan service-template service1
[AC-wlan-st-service1] ssid mesh-network
[AC-wlan-st-service1] service-template enable
[AC-wlan-st-service1] quit
```

3)　MPP を設定します。

MPP の AP view を作成します。適切な AP モデル、シリアル ID を選択、指定していることを確認してください。

```
[AC] wlan ap map1 model QX-W1030
[AC-wlan-ap-map1] serial-id 219801A1K0917BG0000B
```

MAP のラジオ 1 にメッシュプロファイルをバインドします。

```
[AC-wlan-ap-map1] radio 1
[AC-wlan-ap-map1-radio-1] mesh-profile 1
```

MPP のラジオ 1 の無線タイプを 802.11n(5GHz)に設定します。

```
AC-wlan-ap-mpp-radio-1] type dot11an
```

無線の作動チャネルを 36 に設定します。

```
[AC-wlan-ap-mpp-radio-1] channel 36
```

ラジオを有効にします。

```
[AC-wlan-ap-mpp-radio-1] radio enable
[AC-wlan-ap-mpp-radio-1] quit
```

4)　メッシュインタフェースを設定します。

メッシュインタフェースを作成します。

```
[AC1-wlan-ap-mpp1] interface wlan-mesh 1
[AC1-wlan-ap-mpp1-wlan-mesh-1] quit
```

MPP のラジオ 1 にメッシュインタフェースをバインドします。

```
[AC1-wlan-ap-mpp1] radio 1
[AC1-wlan-ap-mpp1-radio-1] mesh-interface 1
[AC1-wlan-ap-mpp1-radio-1] quit
```

リンクタイプをトランクに設定します。

```
[AC1-wlan-ap-mpp1] interface wlan-mesh 1
[AC1-wlan-ap-mpp1-wlan-mesh-1] mesh-port link-type trunk
```

トランクポートを VLAN2 に割り当てます。

```
[AC1-wlan-ap-mpp1-wlan-mesh-1] mesh-port trunk permit vlan 2
[AC1-wlan-ap-mpp1-wlan-mesh-1] quit
```

remote-configuration を有効にします。

```
[AC1-wlan-ap-mpp1] remote-configuration enable
```

5)　AC1 と同様に AC2 を設定します。（詳細は省略します。）

III. 設定の確認

VLAN インタフェース 2 を設定し、AC1 と AC2 が互いに ping 通信できることを確認してください。

目次

このセクションのページは **12-x-x** です。

3 章 IoT 機能の設定 3-1
3.1 概要 3-1
3.1.1 AeroScout ロケーション 3-1
3.1.2 ワイヤレスロケーションの概要 3-1
3.1.3 ワイヤレスロケーションシステム 3-1
3.1.4 ワイヤレスロケーションのメカニズム 3-2
3.2 設定作業リスト 3-2
3.3 AeroScout ロケーションの設定 3-2
3.3.1 AeroScout ロケーションの有効化 3-2
3.3.2 無線ベースのロケーションの有効化 3-3
3.3.3 AeroScout ロケーションモードの指定 3-4
3.3.4 ロケーションサーバの IP アドレスとポート番号の指定 3-5
3.3.5 ロケーションサーバからのメッセージを受信するポートの指定 3-6
3.3.6 タグのマルチキャスト MAC アドレスの指定 3-7
3.3.7 検出するデバイスのタイプの指定 3-8
3.3.8 タイムスタンプのタイプの指定 3-9
3.3.9 MU ロケーションパケット集約の有効化 3-10
3.3.10 AeroScout ロケーションパケットのレポートモードの指定 3-11
3.3.11 ワイヤレスロケーションの表示および管理 3-12
3.4 BLE 機能の設定 3-12
3.4.1 手動モジュールの設定 3-12
3.4.2 自動モジュールおよび自動モジュール変換の設定 3-13
3.4.3 モジュールの説明の設定 3-14
3.4.4 サポート対象モジュールタイプの指定 3-14
3.4.5 モジュールの有効化 3-15
3.4.6 モジュールの送信電力の設定 3-15
3.4.7 BLE デバイスのエージングタイムの設定 3-16
3.4.8 BLE モジュールの iBeacon 送信設定 3-17
3.4.9 モジュールの再起動 3-18
3.4.10 モジュールの自動ファームウェアアップグレードの設定 3-19
3.4.11 IoT AP の表示および管理 3-19
3.5 サーバへの IoT データのレポート設定 3-20
3.5.1 IoT トランスポートプロファイルの作成 3-20
3.5.2 IoT データレポート用のサーバアドレスの設定 3-20
3.5.3 Microsoft Azure IoT Hub DPS の設定 3-20
3.5.4 サーバに送信するキープアライブパケットの送信間隔の設定 3-21
3.5.5 IoT データをサーバにレポートする間隔の設定 3-21
3.5.6 IoT トランスポートプロファイルの有効化 3-21
3.5.7 IoT トランスポートプロファイルのバインド 3-22
3.5.8 IoT トランスポートプロファイルの表示および管理 3-22
3.6 AeroScout ロケーションの設定例 3-23
3.7 BLE 機能の設定例 3-25
3.7.1 iBeacon を送信する 3-25
3.7.2 AP が収集した周辺装置のレポートを Azure IoT Hub DPS へ送信する 3-26

3章 IoT 機能の設定

3.1 概要

3.1.1 AeroScout ロケーション

AeroScout ロケーションは、信号強度の三角測量を使用してタグと MU を特定するために使用されます。信号強度三角測量は、WLAN 内の少なくとも 3 つの AP によって検出された相対的な信号強度を三角測量することによって、クライアントの位置を決定します。

3.1.2 ワイヤレスロケーションの概要

802.11 ワイヤレスロケーショントラックまたは Bluetooth Low Energy (BLE) デバイスにより、医療監視、資産管理、物流管理が可能です。

3.1.3 ワイヤレスロケーションシステム

図 3-1 に示すように、ワイヤレスロケーションシステムには、802.11 または BLE デバイス、情報レシーバ (802.11 または BLE AP) 、およびロケーションサーバが含まれています。802.11 のデバイスには、タグ (定期的に 802.11 パケットのみを送信できる小型のワイヤレスデバイス) と MU(タグを除くすべての 802.11 デバイス) が含まれます。

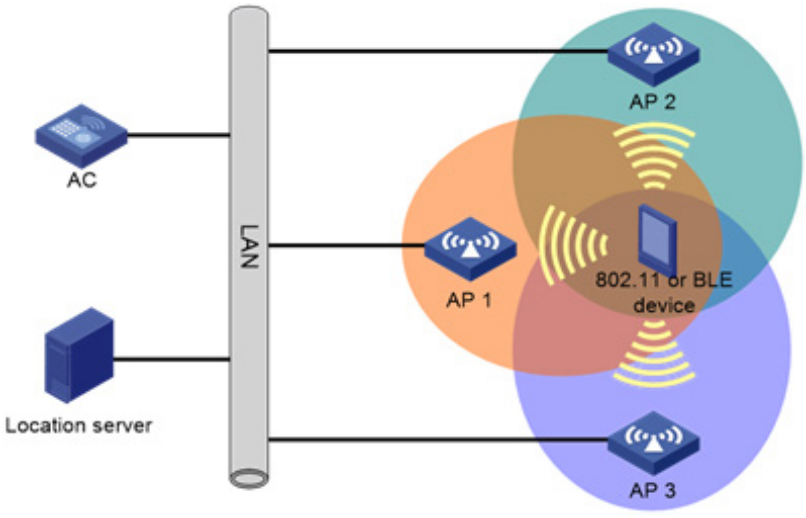


図3-1 ネットワーク図

3.1.4 ワイヤレスロケーションのメカニズム

ワイヤレスロケーションは次のように動作します。

1) 802.11 または BLE デバイスがワイヤレスパケットを送信します。
2) ワイヤレスパケットを受信すると、AP は収集したロケーション情報 (RSSI およびタイムスタンプを含む) をロケーションパケットにカプセル化し、そのパケットをロケーションサーバに送信します。

ロケーションサーバは、802.11 または BLE デバイスのロケーションを計算します。ロケーションサーバは、802.11 または BLE デバイスを見つけるために、少なくとも 3 つの AP からのロケーション情報を必要とします

3.2 設定作業リスト

作業リスト
AeroScout ロケーションの設定
(必須設定項目) AeroScoutロケーションの有効化
無線ベースのロケーションの有効化
AeroScoutロケーションモードの指定
ロケーションサーバのIPアドレスとポート番号の指定
ロケーションサーバからのメッセージを受信するポートの指定
タグのマルチキャストMACアドレスの指定
検出するデバイスのタイプの指定
(オプション設定項目) タイムスタンプのタイプ指定
(オプション設定項目) MUロケーションパケット集約の有効化
(オプション設定項目) AeroScoutロケーションパケットのレポートモードの指定

3.3 AeroScoutロケーションの設定

🕮 **メモ：**

現在のバージョンでは、AeroScout ロケーション機能は QX-W1240 ではサポートしていません。

3.3.1 AeroScout ロケーションの有効化

この機能により、AP はサポートされているすべてのチャネルをスキャンします。すべてのチャネルにデバイスを配置しない場合は、チャネルスキャンホワイトリストまたはブラックリストを設定します。チャネルスキャンのホワイトリストおよびブラックリストの詳細については、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*9 無線管理*”の”*7 章 チャネルスキャンの設定*”を参照してください。

I. 制限とガイドライン

AP がロケーションパケットをロケーションサーバに送信するには、AeroScout ロケーションと無線ベースロケーションの両方を有効にする必要があります。

II. 設定手順

1)　AP View での AeroScout ロケーションの有効化

操作	コマンド	補足
1.　system view に移行する	**system-view**	—
2.　AP view に移行する	**wlan ap** *ap-name* [**model** *model-name*]	—
3.　AeroScout ロケーションを有効にする	**rfid-tracking aeroscout enable**	デフォルト：AP group Viewの設定を使用します。

2)　AP group View での AeroScout ロケーションの有効化

操作	コマンド	補足
1.　system view に移行する	**system-view**	—
2.　AP group view に移行する	**wlan ap-group** *group-name*	デフォルト：デフォルトAPグループ（default-group）が存在し、デフォルトAPグループは削除することができません。
3.　AeroScout ロケーションを有効にする	**rfid-tracking aeroscout enable**	デフォルト：Global configuration Viewの設定を使用します。

3)　Global configuration View での AeroScout ロケーションの有効化

操作	コマンド	補足
1.　system view に移行する	**system-view**	—
2.　Global configuration view に移行する	**wlan global-configuration**	—
3.　AeroScout ロケーションを有効にする	**rfid-tracking aeroscout enable**	デフォルト：無効

3.3.2 無線ベースのロケーションの有効化

I. 制限とガイドライン

AP がロケーションパケットをロケーションサーバに送信するには、AeroScout ロケーションと無線ベースのロケーションを両方有効にする必要があります。

II. 設定手順

1)　AP View での無線ベースのロケーションの有効化

操作	コマンド	補足
1.　system view に移行する	**system-view**	—

操作	コマンド	補足
2． AP view に移行する	**wlan ap** *ap-name* [**model** *model-name*]	—
3． radio view へ移行する	**radio** *radio-id*	—
4． 無線ベースのロケーションを有効にする	**rfid-tracking radio enable**	デフォルト：AP group Viewの設定を使用します。

2)　AP group View での無線ベースのロケーションの有効化

操作	コマンド	補足
5． system view に移行する	**system-view**	—
6． AP group view に移行する	**wlan ap-group** *group-name*	デフォルト：デフォルトAPグループ（default-group）が存在し、デフォルトAPグループは削除することができません。
7． AP model view に移行する	**ap-model** *ap-model*	—
8． radio view へ移行する	**radio** *radio-id*	—
9． 無線ベースのロケーションを有効にする	**rfid-tracking radio enable**	デフォルト：無効

3.3.3 AeroScout ロケーションモードの指定

AeroScout ロケーションには、次のロケーションモードがあります。

- ダイナミックロケーション：AP はロケーションサーバとネゴシエーションを行い、タグのマルチキャスト MAC アドレス、パケット希釈属性、およびロケーションサーバの IP アドレスとポート番号を取得します。ロケーションサーバは、AP の AeroScout バージョン、MAC アドレス、無線モード、およびチャネル情報を取得します。次に、ロケーションサーバは AP にロケーションパケットを送信するように通知します。
- スタティックロケーション：AP は AC から定義済みのロケーション属性を取得し、ロケーションサーバへのロケーションパケットの送信を開始します。ロケーションサーバが AP によるダイナミックネゴシエーションをサポートしていない場合は、スタティック AeroScout ロケーションを使用します。

ダイナミック AeroScout ロケーションでは、AP はロケーションサーバの IP アドレスとポート番号をフラッシュメモリに保存します。この情報を使用して、IP 変更イベントまたはリブートイベントをレポートし、サーバが時間内に応答できるようにします。AP は次のような情報を保持します。

1)　AP は、サーバ情報を含む configuration メッセージを受信すると、10 分のタイマを開始します。10 分以内に別の set configuration メッセージを受信すると、AP はキャッシュ内の設定情報だけを更新します。タイマが期限切れになると、AP はフラッシュメモリに情報を保存します。
2)　AP が最初の configuration メッセージを受信してから 10 分以内に IP 変更イベントまたはリブートイベントが発生した場合、サーバ情報はフラッシュメモリに保存されません。AP は、IP 変更またはリブートメッセージをロケーションサーバに送信しません。

I. 設定手順

1)　AP View での AeroScout ロケーションモードの指定

操作	コマンド	補足
1.　system view に移行する	**system-view**	—
2.　AP view に移行する	**wlan ap** *ap-name* [**model** *model-name*]	—
3.　AeroScout ロケーションモードを指定する	**rfid-tracking aeroscout engine-detection { dynamic | static }**	デフォルト：AP group Viewの設定を使用します。

2)　AP group View での AeroScout ロケーションモードの指定

操作	コマンド	補足
1.　system view に移行する	**system-view**	—
2.　AP group view に移行する	**wlan ap-group** *group-name*	デフォルト：デフォルトAPグループ（default-group）が存在し、デフォルトAPグループは削除することができません。
3.　AeroScout ロケーションモードを指定する	**rfid-tracking aeroscout engine-detection { dynamic | static }**	デフォルト：Global configuration Viewの設定を使用します。

3)　Global configuration View での AeroScout ロケーションモードの指定

操作	コマンド	補足
1.　system view に移行する	**system-view**	—
2.　Global configuration view に移行する	**wlan global-configuration**	—
3.　AeroScout ロケーションモードを指定する	**rfid-tracking aeroscout engine-detection { dynamic | static }**	デフォルト：ダイナミックAeroScoutロケーションを使用します。

3.3.4 ロケーションサーバの IP アドレスとポート番号の指定

AP がロケーションサーバと通信するために、ロケーションサーバの IPv4 アドレスとポート番号を指定します。ダイナミック AeroScout ロケーションが使用されている場合、この機能は有効になりません。

I. 設定手順

1)　AP View でのロケーションサーバの IP アドレスとポート番号の指定

操作	コマンド	補足
1.　system view に移行する	**system-view**	—
2.　AP view に移行する	**wlan ap** *ap-name* [**model** *model-name*]	—
3.　ロケーションサーバの IP アドレスとポート番号を指定する	**rfid-tracking aeroscout engine-address** *engine-address* **engine-port** *engine-port*	デフォルト：AP group Viewの設定を使用します。

2) AP group View でのロケーションサーバの IP アドレスとポート番号の指定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP group view に移行する	**wlan ap-group** *group-name*	デフォルト：デフォルトAPグループ（default-group）が存在し、デフォルトAPグループは削除することができません。
3. ロケーションサーバの IP アドレスとポート番号を指定する	**rfid-tracking aeroscout engine-address** *engine-address* **engine-port** *engine-port*	デフォルト：Global configuration Viewの設定を使用します。

3) Global configuration View でのロケーションサーバの IP アドレスとポート番号の指定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. Global configuration view に移行する	**wlan global-configuration**	—
3. ロケーションサーバの IP アドレスとポート番号を指定する	**rfid-tracking aeroscout engine-address** *engine-address* **engine-port** *engine-port*	デフォルト：設定なし

3.3.5 ロケーションサーバからのメッセージを受信するポートの指定

AP がロケーションサーバからのメッセージを受信するポートを指定するには、次の作業を実行します。スタティック AeroScout ロケーションが設定されている場合、AP は指定されたポートから受信したパケットに応答しません。

I. 設定手順

1) AP View でのロケーションサーバからのメッセージを受信するポートの指定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP view に移行する	**wlan ap** *ap-name* [**model** *model-name*]	—
3. ロケーションサーバからのメッセージを受信するポートを指定する	**rfid-tracking aeroscout vendor-port** *vendor-port-number*	デフォルト：AP group Viewの設定を使用します。

2) AP group View でのロケーションサーバからのメッセージを受信するポートの指定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP group view に移行する	**wlan ap-group** *group-name*	デフォルト：デフォルトAPグループ（default-group）が存在し、デフォルトAPグループは削除することができません。

操作	コマンド	補足
3． ロケーションサーバからのメッセージを受信するポートを指定する	**rfid-tracking aeroscout vendor-port** *vendor-port-number*	デフォルト：Global configuration Viewの設定を使用します。

3) Global configuration View でのロケーションサーバからのメッセージを受信するポートの指定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． Global configuration view に移行する	**wlan global-configuration**	—
3． ロケーションサーバからのメッセージを受信するポートを指定する	**rfid-tracking aeroscout vendor-port** *vendor-port-number*	デフォルト：1144

3.3.6 タグのマルチキャスト MAC アドレスの指定

タグによって送信されるパケットの宛先 MAC アドレスは、製造元によって定義されたマルチキャスト MAC アドレスです。AP がタグを識別するためのマルチキャスト MAC アドレスを指定するには、次の作業を実行します。

I. 制限とガイドライン

スタティック AeroScout ロケーションが使用されている場合、タグのマルチキャスト MAC アドレスの指定が必要です。ダイナミック AeroScout ロケーションが使用されている場合、この機能は有効になりません。

タグのマルチキャスト MAC アドレスを指定しない場合、AP は受信した 802.11 パケットすべてが MU からのものであると判断します。

II. 設定手順

1) AP View でのタグのマルチキャスト MAC アドレスの指定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP view に移行する	**wlan ap** *ap-name* [**model** *model-name*]	—
3． タグのマルチキャスト MAC アドレスを指定する	**rfid-tracking aeroscout tag-multicast-address** mac-address	デフォルト：AP group Viewの設定を使用します。

2) AP group View でのタグのマルチキャスト MAC アドレスの指定

操作	コマンド	補足
1． system view に移行する	**system-view**	—

操作	コマンド	補足
2. AP group view に移行する	**wlan ap-group** *group-name*	デフォルト：デフォルトAPグループ（default-group）が存在し、デフォルトAPグループは削除することができません。
3. タグのマルチキャストMAC アドレスを指定する	**rfid-tracking aeroscout tag-multicast-address** *mac-address*	デフォルト：Global configuration Viewの設定を使用します。

3) Global configuration View でのタグのマルチキャスト MAC アドレスの指定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. Global configuration view に移行する	**wlan global-configuration**	—
3. タグのマルチキャストMAC アドレスを指定する	**rfid-tracking aeroscout tag-multicast-address** *mac-address*	デフォルト：設定なし

3.3.7 検出するデバイスのタイプの指定

🕮 **メモ：**

検出するデバイスのタイプとして、**tag** を指定する場合は、タグからの信号のロスを軽減するために”**scan scan-time**”と”**scan channel whitelist**”を設定することを推奨します。

この機能を使用すると、AP は指定されたタイプのデバイスに関するロケーション情報だけをロケーションサーバに送信します。

I. 設定手順

1) AP View での検出するデバイスのタイプの指定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP view に移行する	**wlan ap** *ap-name* [**model** *model-name*]	—
3. radio view へ移行する	**radio** *radio-id*	—
4. 検出するデバイスのタイプを指定する	**rfid-tracking mode { mu | tag }**	デフォルト：AP group Viewの設定を使用します。
5. (推奨設定) スキャン期間を設定する。	**scan scan-time** *scan-time*	デフォルト：AP group radio viewの設定を使用します。スキャン期間として300ミリ秒を設定することを推奨します。
6. (推奨設定) チャネルスキャンホワイトリストを設定する。	**scan channel whitelist** *channel-list*	デフォルト：AP group radio viewの設定を使用します。タグが利用するチャネルをホワイトリストに設定することを推奨します。

2)　AP group View での検出するデバイスのタイプの指定

操作	コマンド	補足
1．　system view に移行する	**system-view**	—
2．　AP group view に移行する	**wlan ap-group** *group-name*	デフォルト：デフォルトAPグループ（default-group）が存在し、デフォルトAPグループは削除することができません。
3．　AP model view に移行する	**ap-model** *ap-model*	—
4．　radio view へ移行する	**radio** *radio-id*	—
5．　検出するデバイスのタイプを指定する	**rfid-tracking mode { mu | tag }**	デフォルト：設定なし。 このコマンドを複数回実行するとmuとtagの両方を検出するようにAPを設定できます。muとtagの一方は必ず設定します。
6．　(推奨設定) スキャン期間を設定する。	**scan scan-time** *scan-time*	デフォルト：100ミリ秒。 スキャン期間として300ミリ秒を設定することを推奨します。
7．　(推奨設定) チャネルスキャンホワイトリストを設定する。	**scan channel whitelist** *channel-list*	デフォルト：設定なし。 タグが利用するチャネルをホワイトリストに設定することを推奨します。

3.3.8 タイムスタンプのタイプの指定

AP はワイヤレスロケーションパケットを受信すると、ロケーションパケットに絶対タイムスタンプまたは相対タイムスタンプを追加します。絶対タイムスタンプは、1970 年からの経過時間を表します。相対タイムスタンプは、AP が起動してからの経過時間を表します。

タグパケットは、相対タイムスタンプだけでカプセル化できます。MU パケットが相対タイムスタンプと絶対タイムスタンプのどちらでカプセル化されるかは、ロケーションサーバの設定によって異なります。一部のベンダのロケーションサーバは、絶対タイムスタンプでカプセル化された MU パケットだけをサポートしています。

I. 設定手順

1)　AP View でのタイムスタンプのタイプの指定

操作	コマンド	補足
1．　system view に移行する	**system-view**	—
2．　AP view に移行する	**wlan ap** *ap-name* [**model** *model-name*]	—
3．　タイムスタンプのタイプを指定する	**rfid-tracking aeroscout timestamp { absolute | relative }**	デフォルト：AP group Viewの設定を使用します。

2)　AP group View でのタイムスタンプのタイプの指定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP group view に移行する	**wlan ap-group** *group-name*	デフォルト：デフォルトAPグループ（default-group）が存在し、デフォルトAPグループは削除することができません。
3． タイムスタンプのタイプを指定する	**rfid-tracking aeroscout timestamp { absolute | relative }**	デフォルト：Global configuration Viewの設定を使用します。

3) Global configuration View でのタイムスタンプのタイプの指定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． Global configuration view に移行する	**wlan global-configuration**	—
3． タイムスタンプのタイプを指定する	**rfid-tracking aeroscout timestamp { absolute | relative }**	デフォルト：相対タイムスタンプ

3.3.9 MU ロケーションパケット集約の有効化

デフォルトでは、AP は MU ロケーションパケットを受信するとすぐに、そのパケットをロケーションサーバに報告します。これは多くのネットワークリソースを消費します。

この機能を使用すると、AP は受信した MU ロケーションパケットを 1 つのロケーションパケットに集約し、集約したパケットを指定した間隔でロケーションサーバに報告します。集約パケットのサイズが 1400 バイトに達すると、AP はロケーションパケットを直ちにロケーションサーバに報告します。

I. 制限とガイドライン

この機能は、AeroScout ロケーションモードがスタティックモードの場合にだけ有効です。

II. 設定手順

1) AP View での MU ロケーションパケット集約の有効化

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP view に移行する	**wlan ap** *ap-name* [**model** *model-name*]	—
3． MU ロケーションパケット集約を有効にする	**rfid-tracking aeroscout aggregate-report interval** *interval*	デフォルト：AP group Viewの設定を使用します。

2) AP group View での MU ロケーションパケット集約の有効化

操作	コマンド	補足
1． system view に移行する	**system-view**	—

操作	コマンド	補足
2． AP group view に移行する	**wlan ap-group** *group-name*	デフォルト：デフォルトAPグループ（default-group）が存在し、デフォルトAPグループは削除することができません。
3． MU ロケーションパケット集約を有効にする	**rfid-tracking aeroscout aggregate-report interval** *interval*	デフォルト：Global configuration Viewの設定を使用します。

3) Global configuration View での MU ロケーションパケット集約の有効化

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． Global configuration view に移行する	**wlan global-configuration**	—
3． MU ロケーションパケット集約を有効にする	**rfid-tracking aeroscout aggregate-report interval** *interval*	デフォルト：無効

3.3.10 AeroScout ロケーションパケットのレポートモードの指定

ロケーションサーバにロケーションパケットをレポートするモードには、AC (集中レポート) と AP (ローカルレポート) があります。集中レポートモードでは、AP は最初にロケーションパケットを AC に送信する必要があります。

I. 設定手順

1) AP View での AeroScout ロケーションパケットのレポートモードの指定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP view に移行する	**wlan ap** *ap-name* [**model** *model-name*]	—
3． AeroScout ロケーションパケットのレポートモードを指定する	**rfid-tracking aeroscout report-mode { central | local }**	デフォルト：AP group Viewの設定を使用します。

2) AP group View での AeroScout ロケーションパケットのレポートモードの指定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP group view に移行する	**wlan ap-group** *group-name*	デフォルト：デフォルトAPグループ（default-group）が存在し、デフォルトAPグループは削除することができません。
3． AeroScout ロケーションパケットのレポートモードを指定する	**rfid-tracking aeroscout report-mode { central | local }**	デフォルト：Global configuration Viewの設定を使用します。

3) Global configuration View での AeroScout ロケーションパケットのレポートモードの指定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. Global configuration view に移行する	**wlan global-configuration**	—
3. AeroScout ロケーションパケットのレポートモードを指定する	**rfid-tracking aeroscout report-mode { central | local }**	デフォルト：ローカルレポートモード

3.3.11 ワイヤレスロケーションの表示および管理

すべての view で display コマンドを実行できます。

操作	コマンド
ワイヤレスロケーションの無線情報を表示する	**display wlan rfid-tracking radio** [**ap** *apname*]

3.4 BLE機能の設定

⚠ **注意：**

2.4GHz 無線インタフェースでのデータ通信は、BLE モジュールでの通信にパケットロス等の影響を与える為、同一 AP で 2.4GHz 無線インタフェースと BLE 機能は併用しないことを推奨します。

🕮 **メモ：**

- BLE 機能の設定は、ソフトウェアバージョン 9.6.08c を含む以降のソフトウェアからサポートしています。
- BLE 機能は、QX-W1110 と QX-W1200 シリーズの AP でサポートしています。

3.4.1 手動モジュールの設定

AP でモジュールを設定および管理するには、AP のモジュール view に移行する必要があります。

以下に、手動モジュールの設定を示します。

I. AP View での手動モジュールの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP view に移行する	**wlan ap** *ap-name* [**model** *model-name*]	—
3. 手動モジュールを設定する	**module** *module-id*	デフォルト：設定なし

II. AP group View での手動モジュールの設定

操作	コマンド	補足
4. system view に移行する	**system-view**	—
5. AP group view に移行する	**wlan ap-group** *group-name*	—
6. AP model view に移行する	**ap-model** *ap-model*	—
7. 手動モジュールを設定する	**module** *module-id*	デフォルト：設定なし

3.4.2 自動モジュールおよび自動モジュール変換の設定

自動モジュールを設定するには、自動モジュールを手動モジュールに変換するか、AP グループを介して設定する必要があります。

自動モジュール変換機能を有効にすると、モジュールがオンラインになった後、自動的に自動モジュールを手動モジュールに変換します。手動モジュールに自動的に変換されるのは、自動モジュール変換機能を有効にした後でオンラインになったモジュールのみです。オンライン状態の自動モジュールを手動モジュールに変換する場合は、iot auto-module persistent all コマンドを使用します。

以下に、自動モジュールおよび自動モジュール変換の設定を示します。

I. AP View での自動モジュールおよび自動モジュール変換の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP view に移行する	**wlan ap** *ap-name* [**model** *model-name*]	—
3. 自動モジュールを有効にする	**iot auto-module { disable | enable }**	デフォルト：AP group viewの設定を使用します
4. (任意) 自動モジュール変換を有効にする	**iot auto-module persistent { disable | enable }**	デフォルト：AP group viewの設定を使用します
5. (任意) すべてのオンライン自動モジュールを手動モジュールに変換する	**iot auto-module persistent all**	—

II. AP group View での自動モジュールおよび自動モジュール変換の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP group view に移行する	**wlan ap-group** *group-name*	—
3. 自動モジュールを有効にする	**iot auto-module { disable | enable }**	デフォルト：無効
4. (任意) 自動モジュール変換を有効にする	**iot auto-module persistent { disable | enable }**	デフォルト：無効

操作	コマンド	補足
5. (任意) すべてのオンライン自動モジュールを手動モジュールに変換する	**iot auto-module persistent all**	—

3.4.3 モジュールの説明の設定

IoT AP にインストールまたは接続されているモジュールを効率的に管理するには、モデル、場所、および機能に基づいたモジュールの説明を設定します。

以下に、モジュールの説明を設定する手順を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP view に移行する	**wlan ap** *ap-name* [**model** *model-name*]	—
3. モジュール view に移行する	**module** *module-id*	—
4. モジュールの説明を設定する	**description** *text*	デフォルト：設定なし

3.4.4 サポート対象モジュールタイプの指定

AP 上のモジュールを正しく動作させるには、サポート対象モジュールタイプが物理モジュールタイプと一致している必要があります。

以下に、サポートされるモジュールタイプの指定の設定を示します。

I. AP View でのサポート対象モジュールタイプの指定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP view に移行する	**wlan ap** *ap-name* [**model** *model-name*]	—
3. モジュール view に移行する	**module** *module-id*	—
4. サポート対象モジュールタイプを設定する	**type BLE**	デフォルト：AP group viewの設定を使用します

II. AP group View でのサポート対象モジュールタイプの指定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP group view に移行する	**wlan ap-group** *group-name*	—
3. AP model view に移行する	**ap-model** *ap-model*	—

操作	コマンド	補足
4. モジュール view に移行する	**module** *module-id*	—
5. サポート対象モジュールタイプを設定する	**type BLE**	デフォルト：設定なし

3.4.5 モジュールの有効化

以下に、モジュールの有効化の設定を示します。

I. AP View でのモジュールの有効化

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP view に移行する	**wlan ap** *ap-name* [**model** *model-name*]	—
3. モジュール view に移行する	**module** *module-id*	—
4. モジュールを有効化する	**module enable**	デフォルト：AP group viewの設定を使用します

II. AP group View でのモジュールの有効化

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP group view に移行する	**wlan ap-group** *group-name*	—
3. AP model view に移行する	**ap-model** *ap-model*	—
4. モジュール view に移行する	**module** *module-id*	—
5. モジュールを有効化する	**module enable**	デフォルト：無効

3.4.6 モジュールの送信電力の設定

モジュールの送信電力は、送信電力レベルまたは送信電力値で指定することができます。

送信できる送信電力レベル、送信電力値を以下に示します。

- レベル 1 (4dBm)
- レベル 2 (-1dBm)
- レベル 3 (-5dBm)
- レベル 4 (-9dBm)

以下に、モジュールの送信電力の設定を示します。

I. AP View でのモジュールの送信電力の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP view に移行する	**wlan ap** *ap-name* [**model** *model-name*]	—
3. モジュール view に移行する	**module** *module-id*	—
4. モジュールの送信電力を設定する	**tx-power {** *power-level* **| value** *power-value* **}**	デフォルト：AP group viewの設定を使用します

II. AP group View でのモジュールの送信電力の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP group view に移行する	**wlan ap-group** *group-name*	—
3. AP model view に移行する	**ap-model** *ap-model*	—
4. モジュール view に移行する	**module** *module-id*	—
5. モジュールの送信電力を設定する	**tx-power {** *power-level* **| value** *power-value* **}**	デフォルト：レベル1

3.4.7 BLE デバイスのエージングタイムの設定

以下に、BLE デバイスのエージングタイムの設定を示します

I. AP view での BLE デバイスのエージングタイムの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP view に移行する	**wlan ap** *ap-name* [**model** *model-name*]	—
3. モジュール view に移行する	**module** *module-id*	—
4. BLE デバイスのエージングタイムを設定する	**rfid-tracking ble aging-time** *aging-time*	デフォルト：AP group viewの設定を使用します

II. AP group view での BLE デバイスのエージングタイムの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP group view に移行する	**wlan ap-group** *group-name*	—
3. AP model view に移行する	**ap-model** *ap-model*	—
4. モジュール view に移行する	**module** *module-id*	—

操作	コマンド	補足
5. BLE デバイスのエージングタイムを設定する	**rfid-tracking ble aging-time** *aging-time*	デフォルト：global configuration viewの設定を使用します

III. global configuration view での BLE デバイスのエージングタイムの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. global configuration view に移行する	**wlan ap** *ap-name* [**model** *model-name*]	—
3. BLE デバイスのエージングタイムを設定する	**rfid-tracking ble aging-time** *aging-time*	デフォルト：180秒

3.4.8 BLE モジュールの iBeacon 送信設定

この機能により、BLE モジュールは iBeacon アドバタイズメントを定期的にブロードキャストできます。iBeacon アドバタイズメントには、UUID、Major-ID、Minor-ID、および測定電力が含まれます。iBeacon アドバタイズメントを受信したアプリケーションソフトウェアは、アドバタイズメント情報に応じた具体的なアクションを行い、ソフトウェア機能を実現します。

BLE モジュールの iBeacon 送信設定の手順を以下に示します。

I. AP view での BLE モジュールの iBeacon 送信の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP view に移行する	**wlan ap** *ap-name* [**model** *model-name*]	—
3. モジュール view に移行する	**module** *module-id*	—
4. サポートされるモジュールタイプを設定する	**type BLE**	デフォルト：AP group viewの設定を使用します
5. BLE モジュールの iBeacon 送信を設定する	**rfid-tracking ble advertisement { disable | enable }**	デフォルト：AP group viewの設定を使用します
6. アドバタイズメント情報を設定する	**rfid-tracking ble advertisement [** *ad-number* **] { major-id** *major-id* **| measured-power** *measured-power* **| minor-id** *minor-id* **| uuid** *uuid* **}**	デフォルト：AP group viewの設定を使用します
7. iBeacon アドバタイズメントの送信間隔を設定する	**rfid-tracking ble advertisement [** *ad-number* **] interval** *interval*	デフォルト：AP group viewの設定を使用します
8. BLE アドバタイズメントモードを設定する	**rfid-tracking ble advertisement mode { continuous** *ad-number* **| periodic {** *ad-number period* *}&<2>* **}**	デフォルト：AP group viewの設定を使用します

操作	コマンド	補足
9. iBeacon の送信パラメータを設定する	**rfid-tracking ble advertisement** [*ad-number*] { **major-id** *major-id* | **measured-power** *measured-power* | **minor-id** *minor-id* | **uuid** *uuid* }	デフォルト：AP group viewの設定を使用します

II. AP group view での BLE モジュールの iBeacon 送信の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP group view に移行する	**wlan ap-group** *group-name*	—
3. AP model view に移行する	**ap-model** *ap-model*	—
4. モジュール view に移行する	**module** *module-id*	—
5. サポートされるモジュールタイプを設定する	**type BLE**	デフォルト：設定なし
6. BLE モジュールの iBeacon 送信を設定する	**rfid-tracking ble advertisement { disable | enable }**	デフォルト：ad1およびad2アドバタイズメントのiBeacon送信は無効
7. アドバタイズメント情報を設定する	**rfid-tracking ble advertisement** [*ad-number*] { **major-id** *major-id* | **measured-power** *measured-power* | **minor-id** *minor-id* | **uuid** *uuid* }	デフォルト：UUIDはE1CC5B618C06428E8720FE619DB80193、major-IDは1、minor-IDは1、測定電力はad 1またはad 2 iBeaconアドバタイズメントで-58 dBmです
8. iBeacon アドバタイズメントをブロードキャストする間隔を設定する	**rfid-tracking ble advertisement** [*ad-number*] **interval** *interval*	デフォルト：100センチ秒
9. BLE アドバタイズメントモードを設定する	**rfid-tracking ble advertisement mode { continuous** *ad-number* | **periodic {** *ad-number period* }&<2> }	デフォルト：ad 1アドバタイズメントを連続モードで送信します
10. iBeacon のアドバタイズメント情報を設定する	**rfid-tracking ble advertisement** [*ad-number*] { **major-id** *major-id* | **measured-power** *measured-power* | **minor-id** *minor-id* | **uuid** *uuid* }	デフォルト：ad1とad2のアドバタイズメント情報は以下のとおりです。 Major-idは1 Minor-idは1 measured-powerは-58dBm uuidはE1CC5B618C06428E8720FE619DB80193です

3.4.9 モジュールの再起動

system view で以下の操作を実行します

操作	コマンド
1. system view に移行する	**system-view**
2. モジュールを再起動する	**wlan execute module reset ap** *ap-name* **module** *module-id*

3.4.10 モジュールの自動ファームウェアアップグレードの設定

この機能を有効にすると、モジュールのファームウェアバージョンが AP のイメージファイルに保存されているバージョンと異なる場合、モジュールはすぐにファームウェアをアップグレードします。この機能を有効にすると、モジュールがインストールされている IoT AP が再起動するたびにこの機能が有効になります。

以下に、モジュールの自動ファームウェアアップグレードの設定を示します。

I. AP view でのモジュールの自動ファームウェアアップグレードの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP view に移行する	**wlan ap** *ap-name* [**model** *model-name*]	—
3. モジュール view に移行する	**module** *module-id*	—
4. モジュールの自動ファームウェアアップグレードを設定する	**module firmware-upgrade { disable | enable }**	デフォルト：AP group viewの設定を使用します

II. AP group view でのモジュールの自動ファームウェアアップグレードの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP group view に移行する	**wlan ap-group** *group-name*	—
3. AP model view に移行する	**ap-model** *ap-model*	—
4. モジュール view に移行する	**module** *module-id*	—
5. モジュールの自動ファームウェアアップグレードを設定する	**module firmware-upgrade { disable | enable }**	デフォルト：有効

3.4.11 IoT AP の表示および管理

すべての view で display コマンドを実行できます。

操作	コマンド
APのモジュール情報を表示する	**display wlan module-information { all | ap** *ap-name* **module { all |** *module-id* **} } [online]**
APの検出した周辺装置情報を表示する	**display iot ble neighbor-information ap** *ap-name* **{ module all | module** *module-id* **| mac** *mac-addr* **}**

3.5 サーバへのIoTデータのレポート設定

🕮 **メモ：**

サーバへの IoT データのレポート設定は、ソフトウェアバージョン 9.6.08c を含む以降のソフトウェアからサポートしています。

3.5.1 IoT トランスポートプロファイルの作成

IoT トランスポートプロファイルには、IoT データレポート用のサーバアドレスやレポート間隔などを設定します。最大 8 つの IoT トランスポートプロファイルを作成できます。

IoT トランスポートプロファイルを削除する際は、事前に IoT トランスポートプロファイルのバインドを解除する必要があります。

以下に、IoT トランスポートプロファイルの作成手順を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. IoT トランスポートプロファイルを作成し、その view に移行する	**iot transport-profile** *transport-profile-name*	デフォルト：設定なし

3.5.2 IoT データレポート用のサーバアドレスの設定

IoT トランスポートプロファイルを有効にするには、IoT データレポート用のサーバアドレスを設定する必要があります。サーバアドレスを編集するには、最初に IoT トランスポートプロファイルを無効にします。

以下に、IoT データレポート用のサーバアドレスの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. IoT トランスポートプロファイルを作成し、その view に移行する	**iot transport-profile** *transport-profile-name*	デフォルト：設定なし
3. IoT データレポート用のサーバアドレスを設定する	**server-url** *server-url-string*	デフォルト：設定なし

3.5.3 Microsoft Azure IoT Hub DPS の設定

IoT データレポート用のサーバが Microsoft Azure IoT hub DPS の場合、IoT トランスポートプロファイルを有効にする前に、Microsoft Azure IoT Hub DPS の設定が必要です。Microsoft Azure IoT Hub DPS の設定を編集するには、IoT トランスポートプロファイルを無効にする必要があります。

以下に、Microsoft Azure IoT Hub DPS の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. IoT トランスポートプロファイルを作成し、その view に移行する	**iot transport-profile** *transport-profile-name*	デフォルト：設定なし
3. Microsoft Azure IoT Hub DPS のグループ対称キーを設定する	**azure-dps group-symmetric-key { cipher | simple }** *string*	デフォルト：設定なし
4. Microsoft Azure IoT Hub DPS の ID スコープを設定する	**azure-dps id-scope** *id-scope*	デフォルト：設定なし

3.5.4 サーバに送信するキープアライブパケットの送信間隔の設定

以下に、サーバに送信するキープアライブパケットの送信間隔の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. IoT トランスポートプロファイルを作成し、その view に移行する	**iot transport-profile** *transport-profile-name*	デフォルト：設定なし
3. サーバに送信するキープアライブパケットの送信間隔を設定する	**keepalive interval** *interval*	デフォルト：60秒

3.5.5 IoT データをサーバにレポートする間隔の設定

レポートする間隔が長すぎるとサービスに影響しますが、間隔を短くすると AC の負荷が増加するため、適切な値を設定する必要があります。

以下に、IoT データをサーバに報告する間隔の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. IoT トランスポートプロファイルを作成し、その view に移行する	**iot transport-profile** *transport-profile-name*	デフォルト：設定なし
3. IoT データをサーバにレポートする間隔を設定する	**report interval** *interval*	デフォルト：60秒

3.5.6 IoT トランスポートプロファイルの有効化

以下に、IoT トランスポートプロファイルの有効化の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—

操作	コマンド	補足
2. IoT トランスポートプロファイルを作成し、その view に移行する	**iot transport-profile** *transport-profile-name*	デフォルト：設定なし
3. IoT トランスポートプロファイルを有効にする	**transport-profile enable**	デフォルト：無効

3.5.7 IoT トランスポートプロファイルのバインド

オンライン AP は、グローバルコンフィグレーション view で IoT トランスポートプロファイルをバインドした後にのみ、IoT データをサーバにレポートします。

既存の IoT トランスポートプロファイル名のみを指定できます。

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。

以下に、IoT トランスポートプロファイルのバインド設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. グローバルコンフィグレーション view に移行する	**wlan global-configuration**	—
3. IoT トランスポートプロファイルをバインドする	**iot-transport-profile** *transport-profile-name*	デフォルト：設定なし

3.5.8 IoT トランスポートプロファイルの表示および管理

すべての view で display コマンドを実行できます。

操作	コマンド
IoTトランスポートプロファイルに関する情報を表示する	**display iot transport-profile**
使用中のIoTトランスポートプロファイル情報を表示する	**display iot transport-profile in-use**

3.6 AeroScoutロケーションの設定例

I. ネットワーク要件

図 3-2 に示すように、AP 1、AP 2、AP 3 のワイヤレスロケーションを設定して、MU と Tag の位置を確認します。Tag はチャネル 6 を利用するものとします。

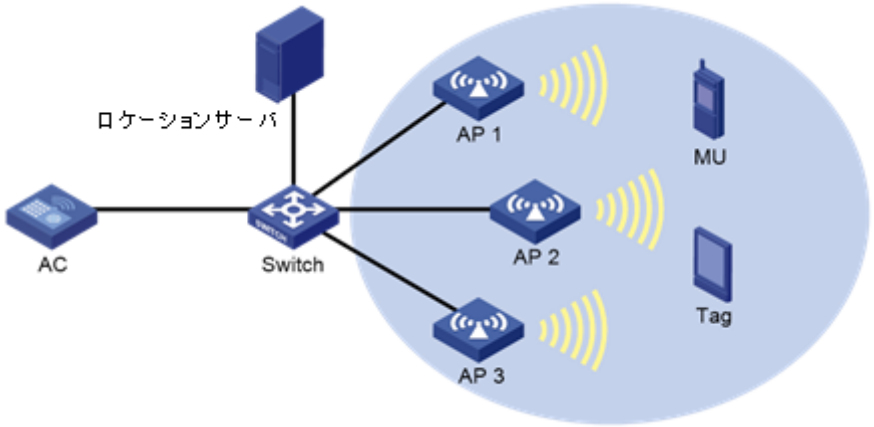


図3-2 ネットワーク図

II. 設定手順

1)　ロケーションサーバを設定します。

#ロケーションサーバで 3 つの AP の IP アドレスを設定するか、ブロードキャストによって AP を検出するようにロケーションサーバを設定します。（詳細は省略します。）

#ロケーションサーバでワイヤレスロケーションを設定します。（詳細は省略します。）

2)　AP1 の AeroScout ロケーションを設定します

AP 名 ap1 の AP を作成し、モデル名、シリアル番号を指定します。

```
[AC] wlan ap ap1 model QX-W1130
[AC-wlan-ap-ap1] serial-id 219801A0CNC148165154
```

#AeroScout ロケーションを有効にします。

```
[AC-wlan-ap-ap1] rfid-tracking aeroscout enable
```

#無線ベースのロケーションを有効にします。

```
[AC-wlan-ap-ap1] radio 3
[AC-wlan-ap-ap1-radio-3] rfid-tracking radio enable
```

#検索するデバイスタイプとしてタグと MU を設定します。

```
[AC-wlan-ap-ap1-radio-3] rfid-tracking mode tag
[AC-wlan-ap-ap1-radio-3] rfid-tracking mode mu
```

#スキャンの期間を 300 ミリ秒、チャネル 6 をホワイトリストに設定します。

```
[AC-wlan-ap-ap1-radio-3] scan scan-time 300
[AC-wlan-ap-ap1-radio-3] scan channel whitelist 6
```

#AP1 の radio 3 を有効にします。

```
[AC-wlan-ap-ap1-radio-3] radio enable
[AC-wlan-ap-ap1-radio-3] quit
[AC-wlan-ap-ap1] quit
```

3)　AP2 の AeroScout ロケーションを設定します

AP 名 ap2 の AP を作成し、モデル名、シリアル番号を指定します。

```
[AC] wlan ap ap2 model QX-W1130
[AC-wlan-ap-ap2] serial-id 219801A0CNC148165155
```

#AeroScout ロケーションを有効にします。

```
[AC-wlan-ap-ap2] rfid-tracking aeroscout enable
```

#無線ベースのロケーションを有効にします。

```
[AC-wlan-ap-ap2] radio 3
[AC-wlan-ap-ap2-radio-3] rfid-tracking radio enable
```

#検索するデバイスタイプとしてタグと MU を設定します。

```
[AC-wlan-ap-ap2-radio-3] rfid-tracking mode tag
[AC-wlan-ap-ap2-radio-3] rfid-tracking mode mu
```

#スキャンの期間を 300 ミリ秒、チャネル 6 をホワイトリストに設定します。

```
[AC-wlan-ap-ap2-radio-3] scan scan-time 300
[AC-wlan-ap-ap2-radio-3] scan channel whitelist 6
```

#AP2 の radio 3 を有効にします。

```
[AC-wlan-ap-ap2-radio-3] radio enable
[AC-wlan-ap-ap2-radio-3] quit
[AC-wlan-ap-ap2] quit
```

4)　AP3 の AeroScout ロケーションを設定します

AP 名 ap3 の AP を作成し、モデル名、シリアル番号を指定します。

```
[AC] wlan ap ap3 model QX-W1130
[AC-wlan-ap-ap3] serial-id 219801A0CNC148165156
```

#AeroScout ロケーションを有効にします。

```
[AC-wlan-ap-ap3] rfid-tracking aeroscout enable
```

#無線ベースのロケーションを有効にします。

```
[AC-wlan-ap-ap3] radio 3
[AC-wlan-ap-ap3-radio-3] rfid-tracking radio enable
```

#検索するデバイスタイプとしてタグと MU を設定します。

```
[AC-wlan-ap-ap3-radio-3] rfid-tracking mode tag
[AC-wlan-ap-ap3-radio-3] rfid-tracking mode mu
```

#スキャンの期間を 300 ミリ秒、チャネル 6 をホワイトリストに設定します。

```
[AC-wlan-ap-ap3-radio-3] scan scan-time 300
[AC-wlan-ap-ap3-radio-3] scan channel whitelist 6
```

#AP3 の radio 3 を有効にします。

```
[AC-wlan-ap-ap3-radio-3] radio enable
[AC-wlan-ap-ap3-radio-3] quit
[AC-wlan-ap-ap3] quit
```

III. 設定確認

#ワイヤレスロケーションが有効になっていること、および各 AP の検索するデバイスのタイプを確認するため、**display wlan rfid-tracking radio** コマンドを使用します。

```
<AC> display wlan rfid-tracking radio
                                  Wireless Locating
--------------------------------------------------------------------------------
 AP                                   Radio   Type
--------------------------------------------------------------------------------
 ap1                                  3       MU/Tag
 ap2                                  3       MU/Tag
 ap3                                  3       MU/Tag
--------------------------------------------------------------------------------
```

#グラフィックスソフトウェアによって提供されるマップ、フォーム、またはレポートによって、MU およびタグの位置情報を表示できることを確認します。

（詳細は省略します。）

3.7 BLE機能の設定例

3.7.1 iBeacon を送信する

I. ネットワーク要件

図 3-3 に示すように、AP から iBeacon を送信するようにします。

iBeacon のアドバタイズメント情報は、major-id を 1234、minor-id を 5678、uuid を 11223344556677881122334455667788 で送信するものとします。

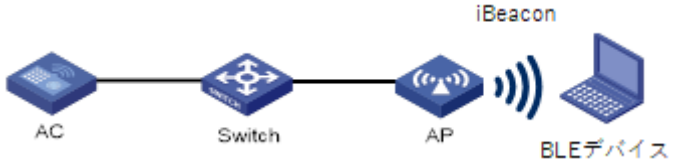


図3-3 ネットワーク図

II. 設定手順

1)　AP の BLE モジュールを設定します。

#AP 名 ap1 の AP を作成し、モデル名、シリアル番号を指定します。

```
[AC] wlan ap ap1 model QX-W1110
[AC-wlan-ap-ap1] serial-id 219801A0CNC148165154
```

#モジュール 1 を作成し、モジュールタイプ BLE を設定します。

```
[AC-wlan-ap-ap1] module 1
[AC-wlan-ap-ap1-module-1] type BLE
[AC-wlan-ap-ap1-module-1] module enable
```

2)　iBeacon の送信設定をします。

#iBeacon の送信を有効化します。

```
[AC-wlan-ap-ap1-module-1] rfid-tracking ble advertisement enable
```

#iBeacon のアドバタイズメント情報(major-id、minor-id、uuid)を設定します。

```
[AC-wlan-ap-ap1-module-1] rfid-tracking ble advertisement major-id 1234
[AC-wlan-ap-ap1-module-1] rfid-tracking ble advertisement minor-id 5678
[AC-wlan-ap-ap1-module-1] rfid-tracking ble advertisement uuid
11223344556677881122334455667788
```

III. 設定確認

BLE デバイスで、AP が送信した iBeacon を受信できるか確認します。

（詳細は省略します。）

3.7.2 AP が収集した周辺装置のレポートを Azure IoT Hub DPS へ送信する

I. ネットワーク要件

図 3-4 に示すように、AP が収集した周辺装置のレポートを、Microsoft Azure IoT Hub DPS へ送信するようにします。

- 事前に外部ネットワークへの接続設定が完了しているものとします。
- 事前に、Azure Cloud サービスにログインし、IoT Hub と DPS サービスの設定が完了しているものとします。

- IoT データレポート用のサーバアドレスは” global.azure-devices-provisioning.net”を設定するものとします。
- Microsoft Azure IoT Hub DPS の ID スコープは”12345678”を設定するものとします。
- Microsoft Azure IoT Hub DPS 登録グループのは”abcdefgh”を設定するものとします。

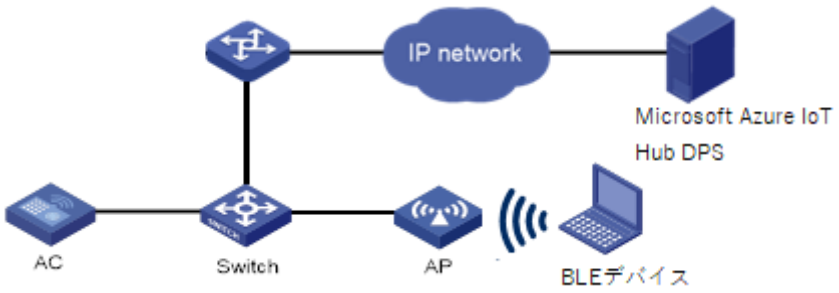


図3-4 ネットワーク図

II. 設定手順

1)　Microsoft Azure Hub DPS にレポートを送信する設定をします。

IoT トランスポートプロファイル “azure-profile”を作成します。

```
<AC> System-View
[AC] iot transport-profile azure-profile
```

#IoT データレポート用のサーバアドレスを設定します。

```
[AC-iot-transport-profile-azure-profile] server-url global.azure-devices-provisioning.net
```

Microsoft Azure IoT Hub DPS の ID スコープを設定します。

```
[AC-iot-transport-profile-azure-profile] azure-dps id-scope 12345678
```

Microsoft Azure IoT Hub DPS 登録グループの対称キーを設定します。

```
[AC-iot-transport-profile-azure-profile] azure-dps group-symmetric-key simple abcdefgh
```

#IoT トランスポートプロファイルを有効化します。

```
[AC-iot-transport-profile-azure-profile] transport-profile enable
[AC-iot-transport-profile-azure-profile] quit
```

#グローバルコンフィグレーション view で IoT トランスポートプロファイルをバインドします。

```
[AC] wlan global-configuration
[AC-wlan-global-configuration] iot-transport-profile azure-profile
[AC-wlan-global-configuration] quit
```

2)　AP の IoT モジュールを設定します。

#AP 名 ap1 の AP を作成し、モデル名、シリアル番号を指定します。

```
[AC] wlan ap ap1 model QX-W1110
[AC-wlan-ap-ap1] serial-id 219801A0CNC148165154
```

#モジュール 1 を作成し、モジュールタイプ BLE を設定します。

```
[AC-wlan-ap-ap1] module 1
[AC-wlan-ap-ap1-module-1] type BLE
[AC-wlan-ap-ap1-module-1] module enable
```

3)　設定の確認

Microsoft Azure IoT Hub DPS との接続を確認する為、**display iot transport-profile in-use** コマンドを使用します。

```
<AC> display iot transport-profile in-use
Connect status: connected
Connected for: 0d 0h 0m 12s
Profile name: azure-profile
Server URL: global.azure-devices-provisioning.net
Server type: azure iot
Azure DPS information
  ID scope: 12345678
  Key type: symmetric
  Group key(cipher): /5LdDRZLigriZAsBwv…….
  Register ID: sn-210235A3KXA8765408
Report interval: 60 seconds
Keepalive interval: 60 seconds
Total sent messages: 0
Sent BLE data messages: 0
Sent keepalive messages: 0
Total received messages: 0
```

#AP が収集した周辺の BLE デバイス情報を確認する為、**display iot ble neighbor-information ap ap1 module 1** コマンドを使用します。

```
<AC> display iot ble neighbor-information ap ap1 module 1
ModuleID  MAC address      Address type          RSSI   Last update time
 ------------------------------------------------------------------------
------
 1         c61b-fa2f-d008   Static                -82    Mon May 16
15:17:03 2022
 1         5d86-6f24-c949   Static                -83    Mon May 16
15:16:38 2022
 1         63b9-fead-f9c0   Static                -80    Mon May 16
15:17:12 2022
 1         ff8b-4380-0a5d   Static                -84    Mon May 16
15:17:07 2022
 1         47d5-895d-1553   Static                -77    Mon May 16
15:16:54 2022
 1         5714-552b-06cb   Static                -82    Mon May 16
15:16:17 2022
 1         7e89-b341-2d98   Static                -83    Mon May 16
15:17:14 2022
 1         4d37-de1a-b0ae   Static                -73    Mon May 16
15:17:12 2022
 1         d005-e316-7e99   Public                -81    Mon May 16
15:16:53 2022
 1         1c52-14c0-da52   Public                -83    Mon May 16
15:17:15 2022
 1         0758-9970-5e38   Static                -79    Mon May 16
15:17:11 2022
 1         2b6f-b895-029b   Static                -76    Mon May 16
15:17:15 2022
```

#Azure IoT Hub のページで、AP 周辺の BLE デバイス情報が登録されていることを確認します。

（詳細は省略します。）

目次

このセクションのページは **12-x-x** です。

4 章 Hotspot 2.0 の設定 4-1
4.1 概要 4-1
4.1.1 Hotspot 2.0 の動作メカニズム 4-1
4.1.2 プロトコルと標準 4-4
4.2 Hotspot 2.0 のタスクの概要 (バージョン 1 の場合) 4-4
4.3 Hotspot 2.0 のタスクの概要 (バージョン 2 の場合) 4-5
4.4 Hotspot 2.0 ポリシーの設定 4-5
4.4.1 Hotspot 2.0 ポリシーを設定するための前提条件 4-5
4.4.2 Hotspot 2.0 ポリシーの作成 4-6
4.4.3 サービスプロバイダ情報の設定 4-6
4.4.4 Hotspot 2.0 ネットワークパラメータ設定 4-7
4.4.5 Hotspot 2.0 ネットワーク最適化の設定 4-8
4.4.6 サービステンプレートへの Hotspot 2.0 ポリシーのバインド 4-9
4.5 オンラインサインアップサービスの設定 4-9
4.5.1 OSU サーバの設定 4-9
4.5.2 オンラインサインアップサービスの SSID の設定 4-10
4.5.3 OSU サーバアイコンの管理 4-10
4.5.4 OSU サーバの Hotspot 2.0 ポリシーへのバインド 4-11
4.6 AP 場所情報の設定 4-11
4.6.1 場所 URL でのエスケープから特定の特殊文字を除外する 4-12
4.7 Hotspot 2.0 の表示および管理 4-12
4.8 Hotspot 2.0 設定の例 4-13
4.8.1 例:Hotspot 2.0 Samsung アプリケーションの設定 4-26
4.8.2 例:Hotspot 2.0 の設定 (バージョン 2 の場合) 4-35

4章 Hotspot 2.0 の設定

🕮 **メモ：**

Hotspot 2.0 の設定は、ソフトウェアバージョン 9.6.05c を含む以降のソフトウェアからサポートしています。

4.1 概要

Wi-Fi Alliance によって開発された Hotspot 2.0 は、ワイヤレスクライアントに自動ネットワーク検出、自動認証、およびシームレスなローミングを提供します。

Hotspot 2.0 には 2 つのバージョンがあります。バージョン 2 はバージョン 1 と完全に互換性があります。

4.1.1 Hotspot 2.0 の動作メカニズム

Hotspot 2.0 は次のように動作します。

1) クライアントは、Hotspot 2.0 ネットワークを検出するワイヤレススキャンを実行します。
2) クライアントは、AP と Generic Advertisment Service (GAS) フレームを交換して Hotspot 2.0 の情報を取得し、最適な BSS を選択します。
3) クライアントはオンラインのサインアップを実行します。このステップは Hotspot 2.0 のバージョン 2 でのみ要求されます。

I. スキャン

次のスキャンタイプを使用できます。

- **アクティブスキャン**

図 4-1 に示すように、ワイヤレスクライアントは、プローブ要求を送信して周囲のワイヤレスネットワークを定期的にスキャンし、受信したプローブ応答からネットワーク情報を取得します。

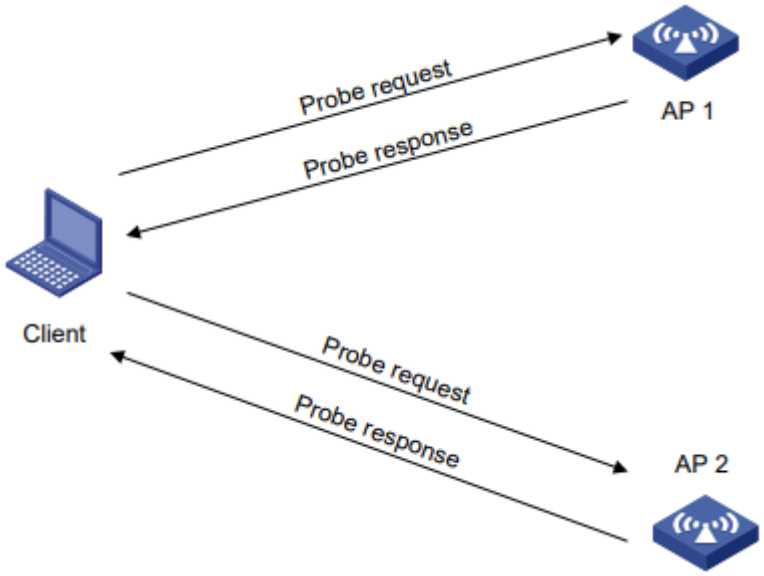


図 4-1 アクティブスキャン図

- **パッシブスキャン**

ワイヤレスクライアントは、サポートされているチャネルで AP から送信されたビーコンフレームを定期的にリッスンし、図 4-2 に示すように周辺のワイヤレスネットワークに関する情報を取得します。

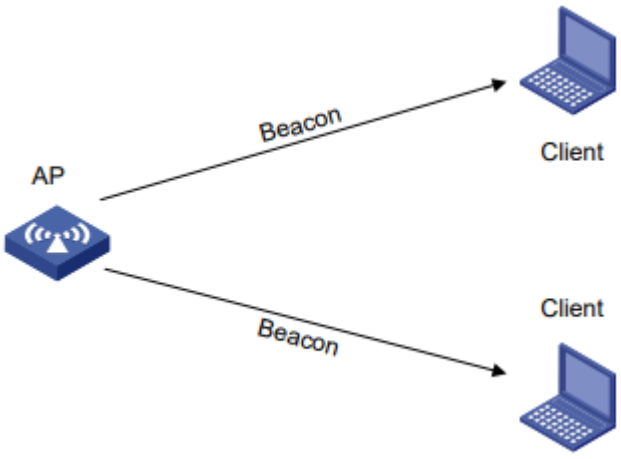


図 4-2 パッシブスキャン図

II. GAS フレーム交換

アクティブまたはパッシブスキャンによって Hotspot 2.0 ネットワークを検出した後、クライアントは、AP の Hotspot 2.0 情報を取得するために、AP と GAS フレームを交換します。取得した Hotspot 2.0 情報とローカル設定に基づいて、クライアントは最適な BSS を選択します。

図 4-3 に示すように、クライアントは、次のプロセスを使用して、AP と GAS フレームを交換します。

1) クライアントは、GAS 初期要求を送信します。
2) 要求を受信すると、AP は GAS 初期応答に Hotspot 2.0 情報をカプセル化し、応答の長さを調べます。
   - 長さが制限を超えない場合、AP は GAS 初期応答をクライアントに送信します。GAS フレーム交換が完了し、クライアントは認証要求を送信できます。
   - 長さが制限を超えると、AP は応答をフラグメント化し、GAS 初期応答の最初のフラグメントをクライアントに送信します。応答は、カムバック遅延後に Hotspot 2.0 情報を要求するようにクライアントに通知します。
3) クライアントは、カムバック遅延後に GAS カムバック要求を AP に送信します。
4) AP は、2 番目のフラグメントをクライアントに通信する GAS カムバック応答を送信します。
5) 応答の長さが制限を超える場合、クライアントと AP はステップ 3 と 4 を繰り返し、すべてのフラグメントがクライアントに送信されるまで処理を続けます。

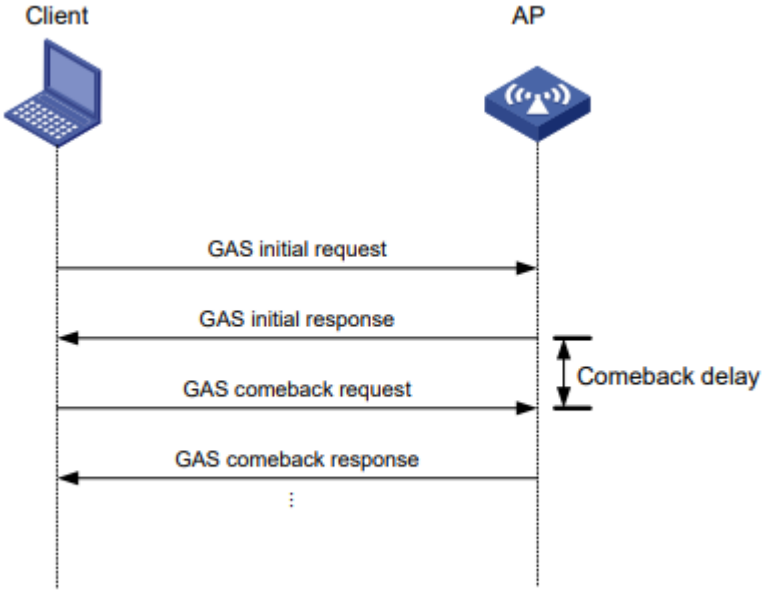


図 4-3 GAS フレーム交換図

III. オンラインサインアップ (バージョン 2 の場合)

GAS フレーム交換の後、クライアントは OSU AP を介して Online Sign Up (OSU) サーバに接続し、オンラインでサインアップします。サインアップしたクライアントはクレデンシャルを取得し、再認証されることなく自動的に Hotspot 2.0 ネットワークにアクセスできます。クライアントは、次の方法を使用して OSU AP に関連付けることができます。

- **Open OSU** – 認証なし
- **OSEN OSU** – Layer2 認証

図 4-4 に示すように、オンラインサインアップは次のように動作します。

1) クライアントは、AP と GAS フレームを交換することによって AP から OSU サーバリストを取得し、OSU サーバを選択します。
2) クライアントは、オープン OSU または OSEN OSU を介して OSU AP と関連付けられます。
3) OSU サーバは、資格情報と認証情報をクライアントに送信するか、クライアントの期限切れの資格情報を更新します。
4) 新しくプロビジョニングされた資格情報を使用して、クライアントは OSU AP との関連付けを解除し、Hotspot 2.0 サービスを提供する AP に関連付けます。

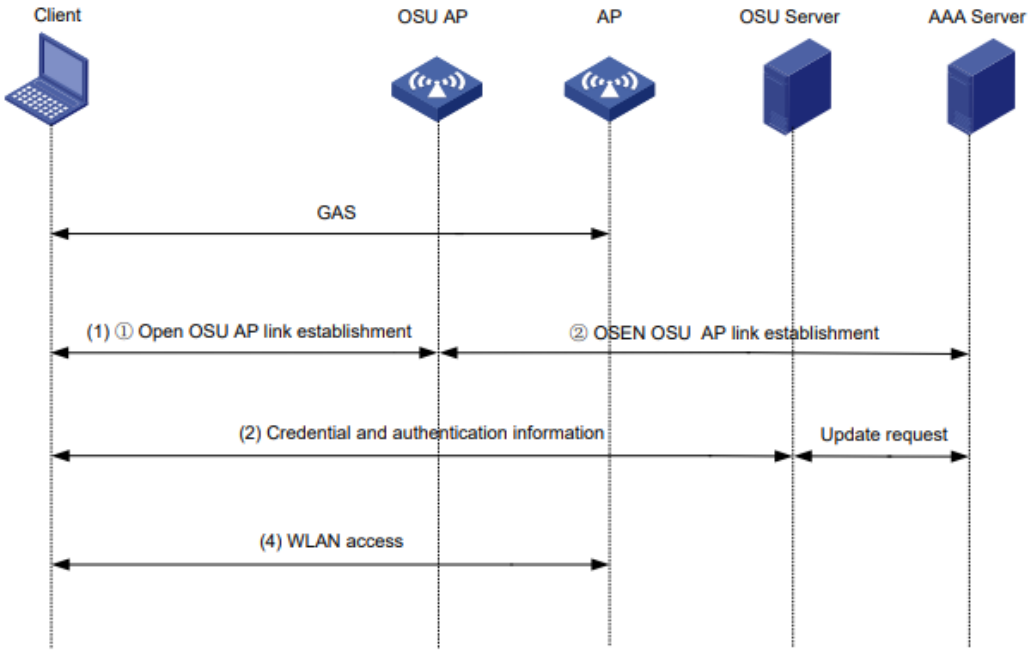


図 4-4 オンラインサインアップ図

4.1.2 プロトコルと標準

- IEEE Standard for Information technology—Telecommunications and information exchange between systems— Local and metropolitan area networks— Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 9: Interworking with External Networks
- Wi-Fi Alliance Technical Committee Hotspot 2.0 Technical Task Group Hotspot 2.0 (Release 2)Technical Specification Version 3.04

4.2 Hotspot 2.0のタスクの概要 (バージョン1の場合)

Hotspot 2.0 (バージョン 1) を設定するには、次のタスクを実行します。

I. Hotspot 2.0 ポリシーの設定

a) (必須項目)Hotspot 2.0ポリシーの作成

b) (必須項目)サービスプロバイダ情報の設定

c) (必須項目)Hotspot 2.0ネットワークパラメータの設定

d) (オプション設定項目) Hotspot 2.0ネットワーク最適化の設定

e) (必須項目)Hotspot 2.0ポリシーのサービステンプレートへのバインド

II. (オプション設定項目) オンラインサインアップサービスの設定

4.3 Hotspot 2.0のタスクの概要 (バージョン2の場合)

Hotspot 2.0 (バージョン 2) を設定するには、次のタスクを実行します。

I. Hotspot 2.0 ポリシーの設定

a) (必須項目)Hotspot 2.0ポリシーの作成

b) (必須項目)サービスプロバイダ情報の設定

c) (オプション設定項目) Hotspot 2.0ネットワークパラメータの設定

d) (オプション設定項目) Hotspot 2.0ネットワーク最適化の設定

e) (必須項目)Hotspot 2.0ポリシーをサービステンプレートにバインドする

II. オンラインサインアップサービスの設定

a) (必須項目)OSUサーバの設定

b) (必須項目)オンラインサインアップサービスのSSIDの設定

c) (必須項目)OSUサーバのアイコンの管理

d) (必須項目)OSUサーバのHotspot 2.0ポリシーへのバインド

III. (オプション設定項目) AP の場所情報の設定

4.4 Hotspot 2.0ポリシーの設定

4.4.1 Hotspot 2.0 ポリシーを設定するための前提条件

Hotspot 2.0 には、802.1X AKM モード、RSN IE、および AES-CCMP cipher スイートが必要です。

バージョン 1 のみをサポートしているクライアントが Hotspot 2.0 ネットワークにアクセスするには、まずクライアントで OI、NAI、ドメインなどのネットワーク情報を設定します。次に、これらの設定をクライアントの設定ファイルに保存します。

4.4.2 Hotspot 2.0 ポリシーの作成

I. このタスクについて

Hotspot 2.0 ポリシーは、Hotspot 2.0 パラメータのセットを定義します。

II. 設定手順

Hotspot 2.0 ポリシーの作成は以下の通りです。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. Hotspot 2.0 ポリシーを作成し、その view を開始する	**wlan hotspot-policy** *policy-number*	—
3. (オプション設定項目) Hotspot 2.0 ポリシーの名前を指定する	**policy-name** *name*	デフォルトでは、Hotspot 2.0 ポリシーに名前は指定されません。

4.4.3 サービスプロバイダ情報の設定

I. このタスクについて

- NAI realm and authentication type — アクセスネットワークの NAI レルムおよび NAI レルムの認証タイプ。
- [Organization identifier] (OI;組織 ID) — ローミングコンソーシアム ID。クライアントがローミングコンソーシアムに対する証明書を持っている場合、クライアントはローミングコンソーシアムが提供するすべての無線サービスにローミングできます。
- 3rd Generation Partnership Project] (3GPP) 情報 — 国コードとネットワークコードが含まれます。国コードは国を識別し、ネットワークコードは国内のサービスプロバイダを識別します。
- ISP domain — クライアントの ISP ドメイン。
- Service provider name — サービスプロバイダ名と言語コード。

II. 設定手順

サービスプロバイダ情報の設定は以下の通りです。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. Hotspot 2.0 ポリシーview に移行します。	**wlan hotspot-policy** *policy-number*	—
3. NAI レルムを作成し、NAI レルムの認証タイプを指定します。	**nai-realm name** *realm-name* **eap-method** *eap-method-id* **auth-method** *auth-method-id* **authentication** *authentication*	デフォルトでは、NAIレルムは存在しません。
4. OI を指定します。	**roam-oi** *oi* [**in-beacon**]	デフォルトでは、OIは指定されません。 この手順は、Hotspot 2.0のバージョン2にのみ必須設定項目です。

操作	コマンド	補足
5. (オプション設定項目) 3GPP 情報設定。	**3gpp-info country-code** *mobile-country-code* **network-code** *mobile-network-code*	デフォルトでは、国コードおよびネットワークコードは設定されていません。
6. ドメイン名を設定します。	**domain-name** *domain-name*	デフォルトでは、ドメイン名は設定されていません。この手順は、Hotspot 2.0のバージョン1にのみ必須設定項目です。
7. (オプション設定項目) サービスプロバイダ名を指定します。	**operator-name** *operator-name* **lang-code** *lang-code*	デフォルトでは、サービスプロバイダ名は指定されません。

4.4.4 Hotspot 2.0 ネットワークパラメータ設定

I. 概要

Hotspot 2.0 ネットワークパラメータには、次のものがあります。

- アクセスネットワークタイプ — 詳細については、コマンドマニュアルのセクション 12 WLAN アドバンスド機能 "*Hotspot 2.0 の設定*"を参照してください。
- 同種 ESS 識別子 (HESSID) — HESSID は同種 ESS を一意に識別します。
- ネットワーク認証タイプ — 詳細については、コマンドマニュアルのセクション 12 WLAN アドバンスド機能 "*Hotspot 2.0 の設定*"を参照してください。
- IP アドレスの可用性 — 関連付けられたクライアントに割り当てられている IP アドレスのバージョンとタイプ。
- WAN リンクステータスパラメータ — 速度とリンクステータス情報が含まれます。Hotspot 2.0 がアップリンクとダウンリンクの速度とリンクステータス (WAN のクローズ、テスト中、有効など) を配信できるようにパラメータを設定できます。
- IP プロトコルのポートステータス — closed、open、および unknown が含まれます。

II. 設定手順

Hotspot 2.0 ネットワークパラメータ設定は以下の通りです。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. Hotspot 2.0 ポリシーview に移行する。	**wlan hotspot-policy** *policy-number*	—
3. アクセスネットワークの種別を設定する。	**network-type** *network-type* [**access-internet**]	デフォルトでは、アクセスネットワークの種別は設定されていない。
4. HESSID を設定する。	**hessid** *hessid*	デフォルトでは、HESSIDは設定されていません。この手順は、Hotspot 2.0のバージョン1にのみ必要です。
5. (オプション設定項目) ネットワーク認証の種類を指定します。	**authentication-type** { **0** [**redirect-url** *url*] | **1** | **2 redirect-url** *url* | **3** }	デフォルトでは、ネットワーク認証の種類は指定されていません。
6. IP アドレスの可用性設定。	**ip-type ipv4** *ipv4-type* **ipv6** *ipv6-type*	デフォルトでは、IPv4アドレスの可用性は1、IPv6アドレスの可用性は2です。

操作	コマンド	補足
7. IP プロトコルのポートステータスを設定します。	**ip-protocol** { **esp** | **icmp** | **tcp** | **udp** } **port-number** *port-number* { **closed** | **open** | **unknown** }	デフォルトでは、IPプロトコルのポートステータスは設定されていません。
8. WAN リンクステータスパラメータを設定します。	**wan-metrics** { **link-down** | **link-test** | **link-up** } [**asymmetric downlink-speed** *downlink-speed* **uplink-speed** *uplink-speed* | **symmetric link-speed** *link-speed*]	デフォルトでは、WANリンクステータスパラメータは設定されていません。

4.4.5 Hotspot 2.0 ネットワーク最適化の設定

I. 概要

Hotspot 2.0 ネットワークでは、次のネットワーク最適化機能を使用できます。

- Downstream Group-Addressed Forwarding (DGAF) — AP がすべてのダウンストリームワイヤレスブロードキャスト ARP パケットおよびワイヤレスマルチキャストパケットを転送できるようにします。ダウンストリームマルチキャストを使用したスプーフィング攻撃を防止するには、AP の DGAF 機能をディセーブルにします。
- Comeback delay — クライアントが GAS カムバック要求を頻繁に送信しないようにします。
- GAS initial request limit — AC の負荷を軽減するために、クライアントが指定された間隔内に送信できる GAS 初期要求の最大数を制限します。

II. 設定手順

Hotspot 2.0 ネットワーク最適化の設定は以下の通りです。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. Hotspot 2.0 ポリシーを作成し、その view を開始する	**wlan hotspot-policy** *policy-number*	—
3. DGAF 機能を無効にします。	**undo dgaf enable**	デフォルトでは、DGAF機能は有効になっています。
4. カムバック遅延を設定します。	**comeback-delay** *value*	デフォルトでは、カムバック遅延は1 TU (1024ミリ秒) です。
5. 指定した間隔内にクライアントが送信できる GAS 初期要求の最大数を設定します。	**gas-limit number** *number* **interval** *interval*	デフォルトでは、クライアントが送信できるGAS初期要求の数は制限されません。

4.4.6 サービステンプレートへの Hotspot 2.0 ポリシーのバインド

I. 概要

Hotspot 2.0 ネットワークを構築するには、サービステンプレートを使用して、Hotspot 2.0 ポリシーを AP のサービステンプレートにバインドする必要があります。

II. 設定手順

サービステンプレートへの Hotspot 2.0 ポリシーのバインド設定は以下の通りです。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. サービステンプレート View に移行します。	**wlan service-template** *service-template-name*	—
3. Hotspot 2.0 ポリシーをサービステンプレートにバインドします。	**hotspot-policy** *policy-number*	デフォルトでは、Hotspot 2.0 ポリシーはサービステンプレートにバインドされていません。

4.5 オンラインサインアップサービスの設定

4.5.1 OSU サーバの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. OSU サーバを作成してその view に移行するか、既存の OSU サーバの view に移行する	**wlan osu-provider** *osu-provider-number*	—
3. OSU サーバの名前を設定する	**friendly-name** *friendly-name* **lang-code** *lang-code*	デフォルト：設定なし
4. OSU サーバの URI を指定する	**uri** *uri*	デフォルト：指定なし
5. クライアントが OSU サーバと通信するためのプロトコルを指定する	**method** *method-id*	デフォルト：指定なし
6. OSU サーバのアイコンを指定する	**icon-file** *filename* **lang-code** *lang-code* **icon-type** *icon-type*	デフォルト：指定なし OSUサーバのアイコンを指定する前に、バージョンファイルが保存されているルートディレクトリでmkdirコマンドを使用してディレクトリアイコンが作成されていることを確認してください。次に、FTPまたはTFTPを使用して、アイコンファイルをディレクトリにダウンロードしてください。

操作	コマンド	補足
7. (オプション設定項目) OSU サーバの説明を設定する	**description** *description* **lang-code** *lang-code*	デフォルト：設定なし
8. (オプション設定項目) OSU サーバのネットワークアクセス識別子（NAI）を設定する	**nai** *nai*	デフォルト：設定なし

4.5.2 オンラインサインアップサービスの SSID の設定

I. 設定の制限とガイドライン

オンラインサインアップサービス用に設定された SSID が、オンラインサインアップサービステンプレートの SSID と同じであることを確認します。

II. 設定手順

オンラインサインアップサービスの SSID の設定は以下の通りです。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. Hotspot 2.0 ポリシーview に移行します。	**wlan hotspot-policy** *policy-number*	—
3. オンラインサインアップサービスの SSID を設定します。	**osu-ssid** *ssid-name*	デフォルトでは、オンラインサインアップサービスに SSIDは設定されていません。

4.5.3 OSU サーバアイコンの管理

I. 概要

このタスクでは、OSU サーバに指定されたすべてのアイコンファイルをロードして、アイコンファイルの変更が発生したときに変更を検証したり、アイコンファイルを無効にしたりできます。

II. 設定手順

OSU サーバアイコンの管理は以下の通りです。

操作	コマンド	補足
1. system view に移行する	**system-view**	—

操作	コマンド	補足
2． OSU サーバのアイコンファイルを管理します。 OSU サーバのアイコンファイルを読み込みます。	**wlan hotspot osu-icon upload**	—
OSU サーバのアイコンファイルを管理します。 OSU サーバのアイコンファイルをアンロードします。	**wlan hotspot osu-icon unload**	—

4.5.4 OSU サーバの Hotspot 2.0 ポリシーへのバインド

I. 設定の制限とガイドライン

Hotspot 2.0 ポリシーは、最大 32 台の OSU サーバにバインドできます。

OSU サーバを Hotspot 2.0 ポリシーにバインドする前に、OSU サーバに必要なすべての設定が完了していることを確認してください。

II. 設定手順

OSU サーバの Hotspot 2.0 ポリシーへのバインド設定は以下の通りです。

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． Hotspot 2.0 ポリシーview に移行する。	**wlan hotspot-policy** *policy-number*	—
3． OSU サーバを Hotspot 2.0 ポリシーにバインドします。	**osu-provider** *osu-provider-number*	デフォルトでは、OSUサーバはHotspot 2.0ポリシーにバインドされていません。

4.6 AP場所情報の設定

I. 概要

AP 場所情報は AP の場所を示し、クライアントが最適な AP に接続するのに役立ちます。

II. 設定手順

AP 場所情報の設定は以下の通りです。

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． APview を入力します。	**wlan ap** *ap-name*	—

操作	コマンド	補足
3. AP の場所グループと場所タイプを指定します。	**venue group** *venue-group-number* **type** *venue-type-number*	デフォルトでは、APの場所グループと場所タイプは指定されていません。 この手順は、Hotspot 2.0のバージョン1の場合にのみ必要です。
4. AP の場所名を設定します。	**venue name** *venue-name* ***lang-code*** *lang-code* [**url** *url*]	デフォルトでは、APに場所名は設定されていません。 この手順は、Hotspot 2.0バージョン1の場合だけ必要です。

4.6.1 場所 URL でのエスケープから特定の特殊文字を除外する

I. 概要

クライアントが特殊文字を構文またはコマンドとして解釈し、意図した意味を変更しないようにするには、これらの文字を安全な形式 (エスケープ文字) に変換する必要があります。

実際には、サーバによっては、URL 内の特定の特殊文字のエスケープ文字が認識されず、エラーが発生することがあります。このような場合は、このタスクを実行して、特定の特殊文字をエスケープから除外できます。

場所 URL では、大文字と小文字および数字以外の文字はエスケープする必要がなく、このコマンドを使用して残りの特殊文字を構成できます。

デフォルトでは、装置は composition1 の特殊文字をエスケープしません。

サーバによっては、URL 内の特定の特殊文字のエスケープ文字が認識されず、例外が発生する場合があります。これに対処するには、これらの特定の文字がエスケープされないように機能を構成します。

II. 設定手順

場所 URL でのエスケープから特定の特殊文字を除外する設定は以下の通りです。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. 場所 URL のエスケープから特定の特殊文字を除外します。	**wlan venue url-unescape-chars** { **composition1** | **composition2** | **custom** *character-string* }	デフォルトでは、Venue URL はcomposition1方式を採用し、composition1に含まれる特殊文字はエスケープされません。

4.7 Hotspot 2.0の表示および管理

任意の view で表示コマンドを実行します。(バージョン 1 の場合)

操作	コマンド
サービステンプレートの情報を表示する。	**display wlan service-template** [*service-template-name*] [**verbose**]

任意の view で表示コマンドを実行する。(バージョン 2 の場合)

操作	コマンド
ロードされているすべての OSU サーバのアイコンファイルを表示します。	**display wlan hotspot uploaded-osu-icon**
サービステンプレートの情報を表示します。	**display wlan service-template** [*service-template-name*] [**verbose**]

4.8 Hotspot 2.0 設定の例

I. ネットワーク要件

図 4-5 に示すように、Hotspot 2.0 を構成して、携帯電話ネットワークからワイヤレスネットワークに電話を切り替えることができるようにします。

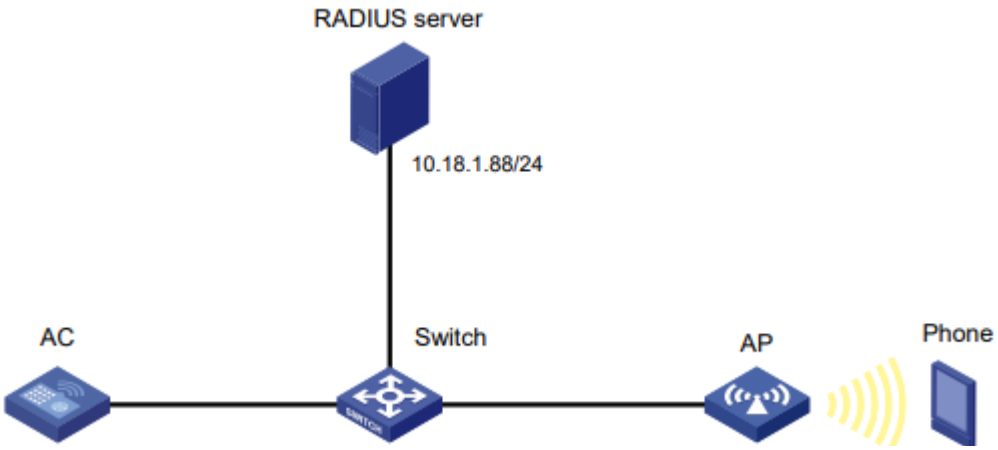


図 4-5 ネットワーク図

II. 前提条件

クライアント認証、許可、アカウンティングを正しく動作させるには、RADIUS サーバに証明書をインストールし、ユーザアカウントを作成する必要があります。AAA の詳細は、オペレーションマニュアルのセクション 13 ユーザアクセスと認証 "*AAA*"の"*一般的に使用される標準 RADIUS 属性の説明*"を参照してください。

III. AC の設定

1)　Hotspot 2.0 ポリシー設定:

Hotspot 2.0 ポリシーを作成します。

```
<AC> system-view
[AC] wlan hotspot-policy 1
```

EAP-TLS 認証設定します。

```
[AC-wlan-hs-1] nai-realm name abc.com eap-method 6 auth-method 2 authentication 4
```

ドメイン名を abc.com に設定。

```
[AC-wlan-hs-1] domain-name abc.com
```

HESSID を 1232 ff23-0123 に設定します。

```
[AC-wlan-hs-1] hessid 1232-ff23-0123
[AC-wlan-hs-1] quit
```

2)　802.1X 認証および RADIUS スキーム設定:

802.1X 認証方式を EAP として設定します。

```
[AC] dot1x authentication-method eap
```

RADIUS スキーム imcc を作成します。

```
[AC] radius scheme imcc
```

プライマリー・認証・サーバの IP アドレスとポート番号をそれぞれ 10.18.1.88 と 1812 に設定します。

```
[AC-radius-imcc] primary authentication 10.18.1.88 1812
```

プライマリー・アカウンティング・サーバーの IP アドレスとポート番号をそれぞれ 10.18.1.88 と 1813 に設定します。

```
[AC-radius-imcc] primary accounting 10.18.1.88 1813
```

認証サーバおよびアカウンティングサーバとパケットを交換する AC の共有鍵を 12345678 に設定します。

AC を設定して、RADIUS サーバに送信されたユーザ名のドメイン名を削除します。

```
[AC-radius-imcc] user-name-format without-domain
[AC-radius-imcc] quit
```

3)　ドメイン imc を作成し、認証、許可、およびアカウンティングに RADIUS スキーム imcc を使用するようにドメインを設定します。

```
[AC] domain imc
[AC-isp-imc] authentication lan-access radius-scheme imcc
[AC-isp-imc] authorization lan-access radius-scheme imcc
[AC-isp-imc] accounting lan-access radius-scheme imcc
[AC-isp-imc] quit
```

IV. AP の設定

サービステンプレート service1 の作成。

```
<AC> system-view
[AC] wlan service-template service1
```

SSID を service に設定します。

```
[AC-wlan-st-service1] ssid service
```

Hotspot 2.0 ポリシー1 をサービステンプレートにバインドします。

```
[AC-wlan-st-service1] hotspot-policy 1
```

ビーコンおよびプローブ応答で RSN IE を有効にします。

```
[AC-wlan-st-service1] security-ie rsn
```

AES-CCMP cipher スイートをイネーブルにします。

```
[AC-wlan-st-service1] cipher-suite ccmp
```

認証および鍵管理モードを 802.1X に設定します。

```
[AC-wlan-st-service1] akm mode dot1x
```

WLAN クライアントの認証モードを 802.1X に設定します。

```
[AC-wlan-st-service1] client-security authentication-mode dot1x
```

認証ドメインとしてドメイン imc を指定します。

```
[AC-wlan-st-service1] dot1x domain imc
```

サービステンプレートを有効にします。

```
[AC-wlan-st-service1] service-template enable
[AC-wlan-st-service1] quit
```

AP ap1 を作成し、AP モデルとシリアル ID を指定します。

```
[AC] wlan ap ap1 model W1120
[AC-wlan-ap-ap1] serial-id 219801A28N819CE0002T
```

#AP の無線 2 にサービステンプレートサービスをバインドします。

```
[AC-wlan-ap-ap1] radio 2
[AC-wlan-ap-ap1-radio-2] radio enable
[AC-wlan-ap-ap1-radio-2] service-template service1
[AC-wlan-ap-ap1-radio-2] quit
[AC-wlan-ap-ap1] quit
```

V. RADIUS サーバの設定 (IMCv7)

この例は、IMC PLAT 7.1 および IMC UAM 7.1 で作成されました。

IMC サーバを設定するには、次の手順を実行します。

1) IMC プラットフォームにログインします。
2) [User] タブをクリックします。
3) アクセス装置を追加します。

a) ナビゲーションツリーから、[User Access Policy] > [Access Device Management] >

[Access Device] を選択します。

b)　アクセス装置の設定ページで、[Add] をクリックします。

c)　[Add Access Device] ページで、次のパラメータを設定します。

- 共有鍵を 12345678 に設定します。
- IP アドレス 10.18.1.1 (AC の IP アドレス) の装置を選択または手動で追加します。
- その他のパラメータはデフォルト設定を使用します。

d)　[OK]をクリックします。

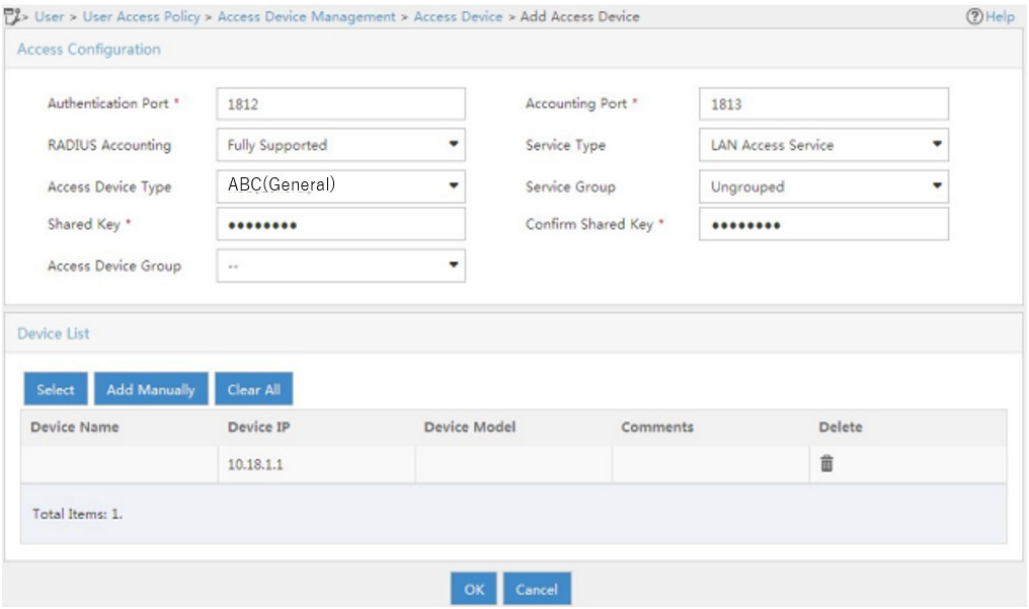


図 4-6 アクセス装置の追加図

4)　アクセスポリシーを追加します。

a)　ナビゲーションツリーから、[User Access Policy] > [Access Policy] を選択します。

b)　アクセス装置の設定ページで、[Add] をクリックします。

c)　[Add Access Policy] ページで、次のパラメータを設定します。

- アクセスポリシー名を 802.1X_policy に設定します。
- [Certificate Type] リストから [EAP-PEAP Authentication] を選択し、[Certificate Sub-Type] リストから、クライアントの認証方式と同じ証明書サブタイプを選択します。
- その他のパラメータにはデフォルト設定を使用します。

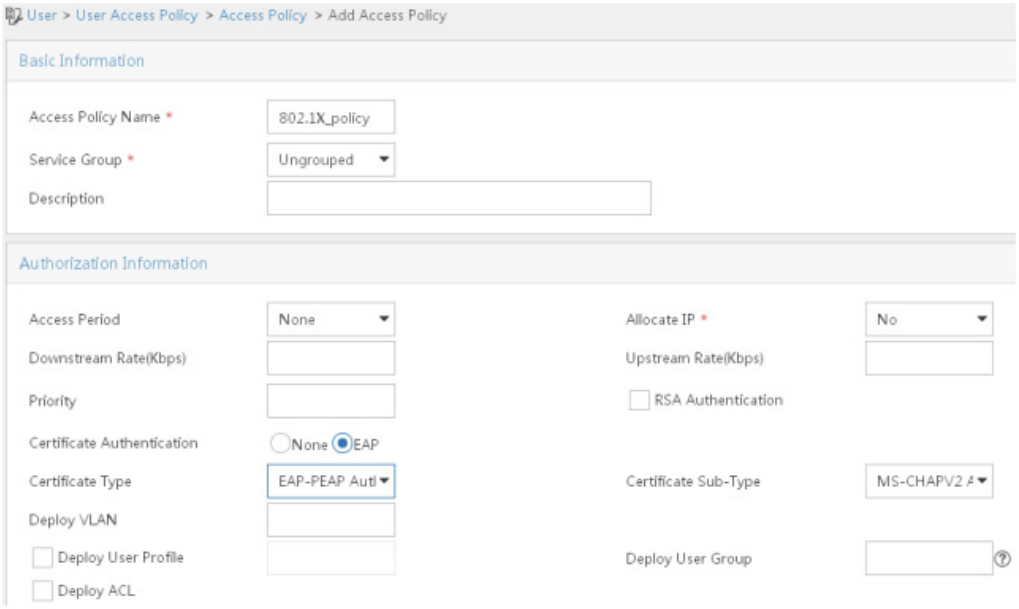


図 4-7 アクセスポリシーの追加図

5)　アクセスサービスを追加します。

a)　ナビゲーションツリーから、[User Access Policy] > [Access Service] を選択します。

b)　アクセスサービス設定ページで、[Add] をクリックします。

c)　[Add Access Service] ページで、サービス名を802.1X_serとして設定し、作成した802.1Xポリシーをデフォルトのアクセスポリシーとして使用します。

d)　その他のパラメータにはデフォルト設定を使用します。

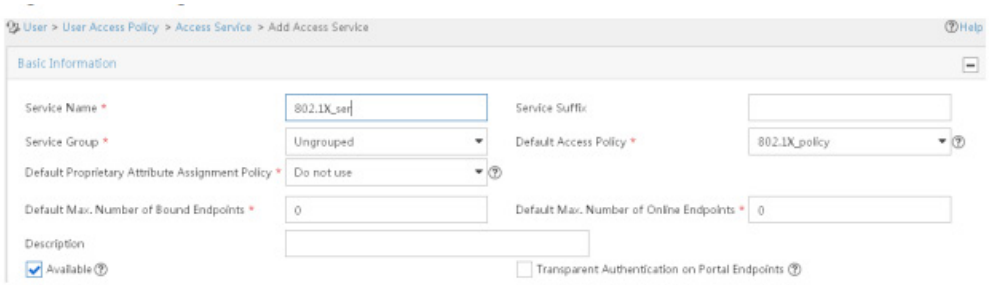


図 4-8 アクセスサービスの追加図

6)　アクセスユーザを追加します。

a)　ナビゲーションツリーから、[Access User] > [All Access Users] を選択します。

b)　アクセスユーザ 設定ページで、[Add] をクリックします。

c)　[Add Access User] ページで、[Add User] をクリックします。

d)　[Add User] ウィンドウで、次のパラメータを設定します。

- ユーザ名を admin に設定します。
- アカウント名を admin に設定します。
- [Access Service] 領域で設定した 802.1X ユーザを選択します。

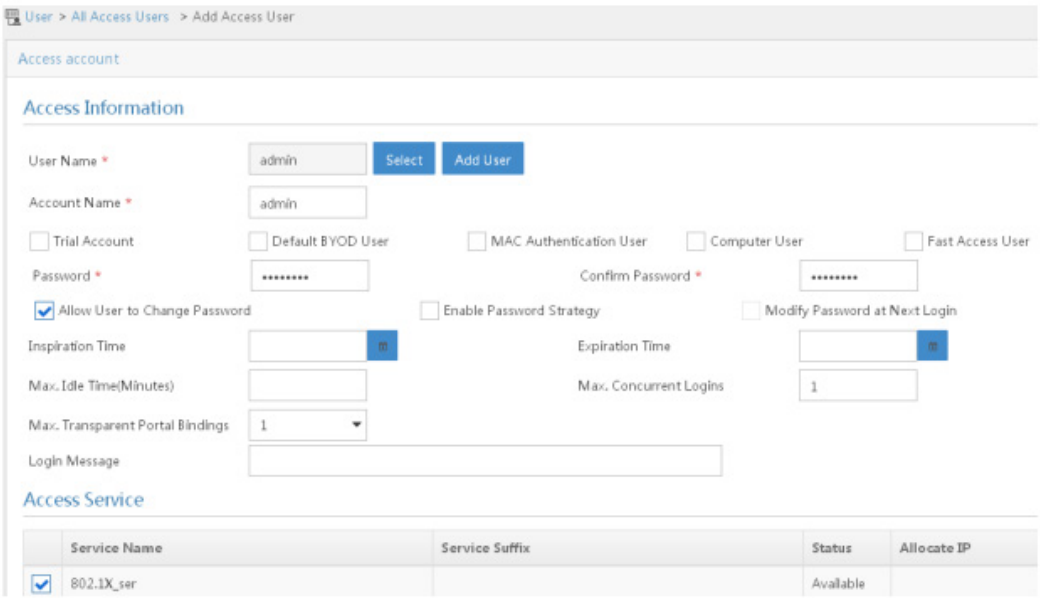


図 4-9 アクセスユーザの追加図

VI. 電話機の設定

この例は、iPhone 5S を使用して作成しました。

電話機を設定するには、次の手順を実行します。

1)　MacBook Air に Apple 設定 App をインストールし、iPhone 5S をラップトップに接続します。



図 4-10 設定アプリの適用図

2)　Apple Configurator アプリを開き、上部のメニューから [Supervise] を選択します。次に、リストの下にある [+] をクリックし、[Create New Profile] を選択します。

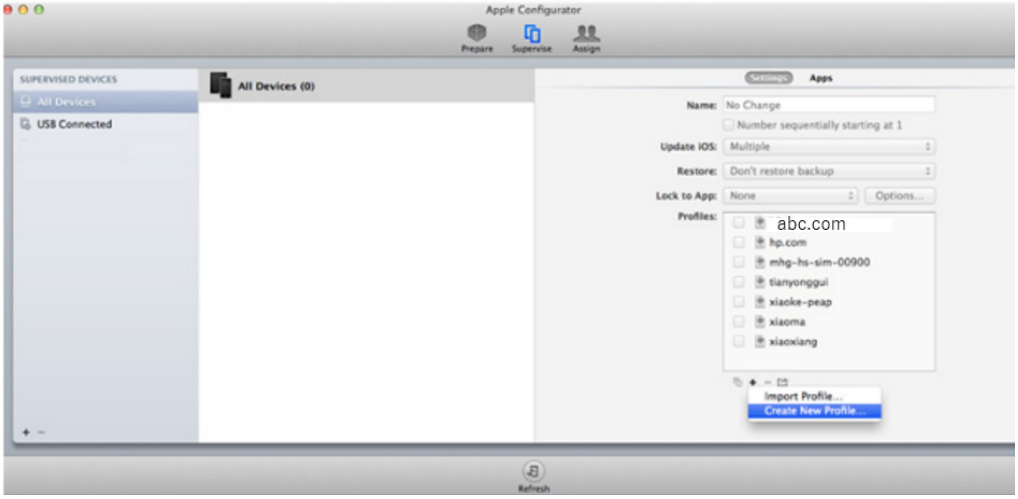


図 4-11 新しいプロファイルの作成図

3)　左側のナビゲーションツリーで [General] をクリックし、[Name] フィールドに「abc.com」と入力します。その他のパラメータは省略可能です。



図 4-12 General 設定図

4)　左側のナビゲーションツリーで [Wi-Fi] をクリックし、メニューから [Configure] をクリックします。次に、[Network Type] リストから [Passpoint] を選択します。



図 4-13 パスポイントの有効化図

5)　表示されるページで、次のタスクを実行します。

- [Accepted EAP Types] 領域で、[PEAP] を選択します。
- [Username] 領域と [Password] 領域にそれぞれ admin と 12345678 を入力します。
- [Identity Certificate] リストから [None] を選択します。
- [Outer Identity] 領域に admin と入力します。

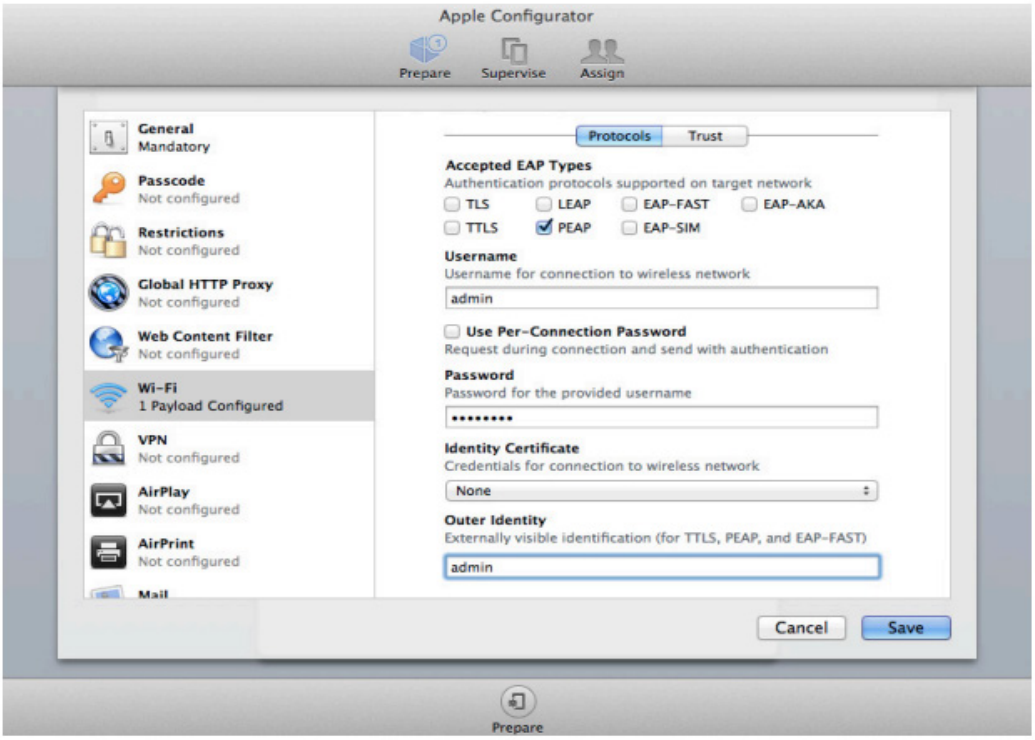


図 4-14 EAP-PEAP 認証の設定図

□ [Provider Display Name] フィールドに「abc.com」と入力し、AC の Hotspot ポリシーで設定したドメイン名を入力します。

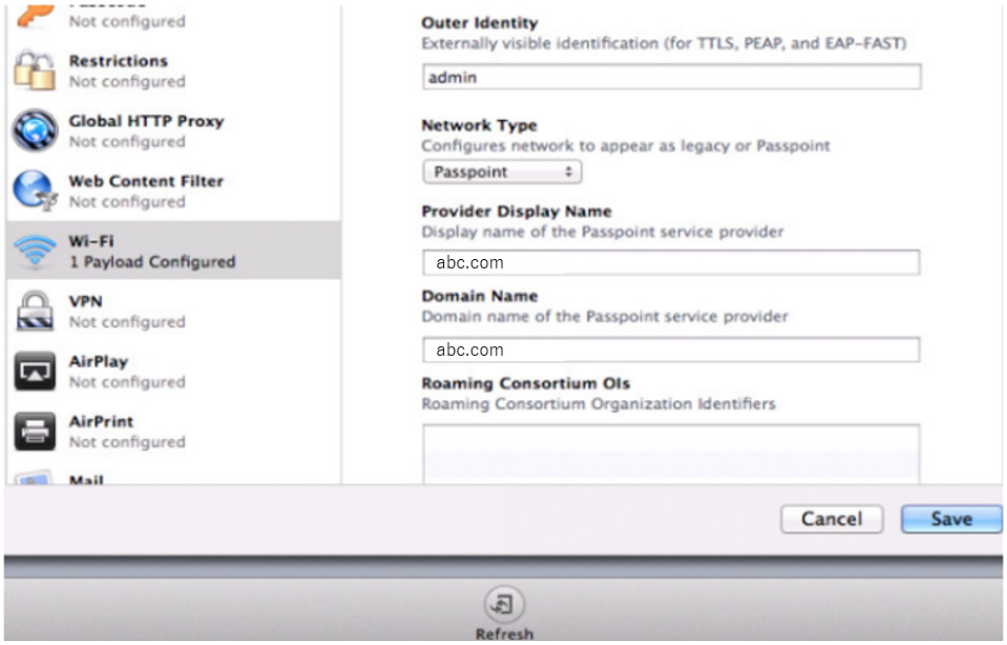


図 4-15 ドメイン名の設定図

□ Roaming Consortium OIs (ローミングコンソーシアム)、NAI Real Names、および MCC/MNC を空白のままにするか、AC の Hotspot ポリシーで設定した値を入力します。次に、[Save] をクリックします。

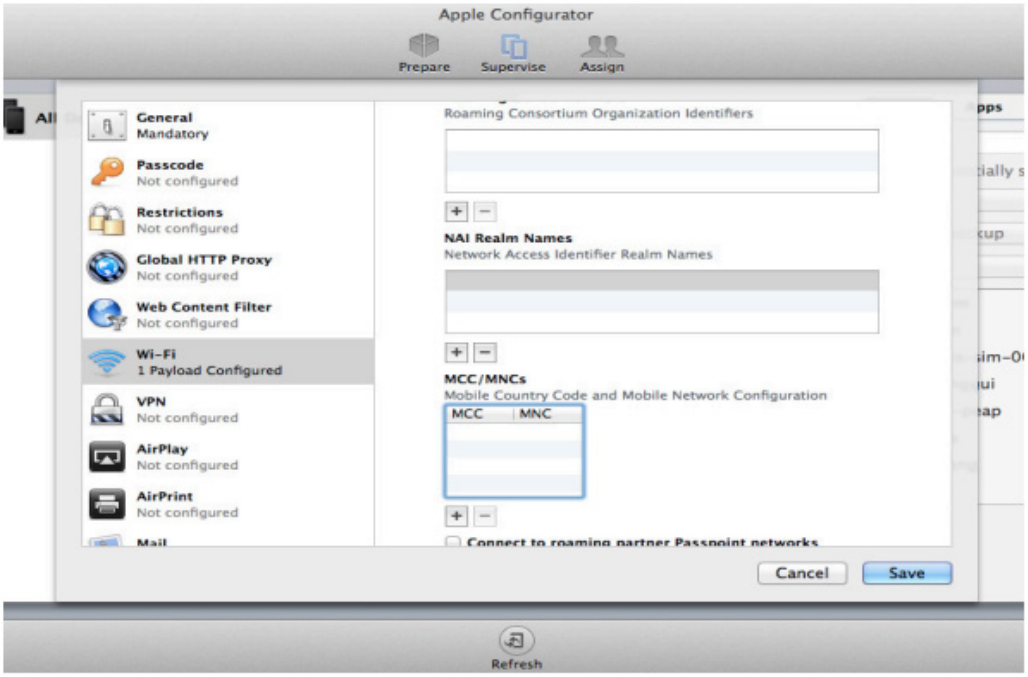


図 4-16 その他のオプションの設定図

6)　[Prepare] をクリックし、[Setting] タブの [Install Profiles…] をクリックします。



図 4-17 プロファイルのインストール図

7)　[Next] をクリックします。



図 4-18 プロファイルのインストール図

8)　プロファイル abc.com を選択し、[Next] をクリックします。

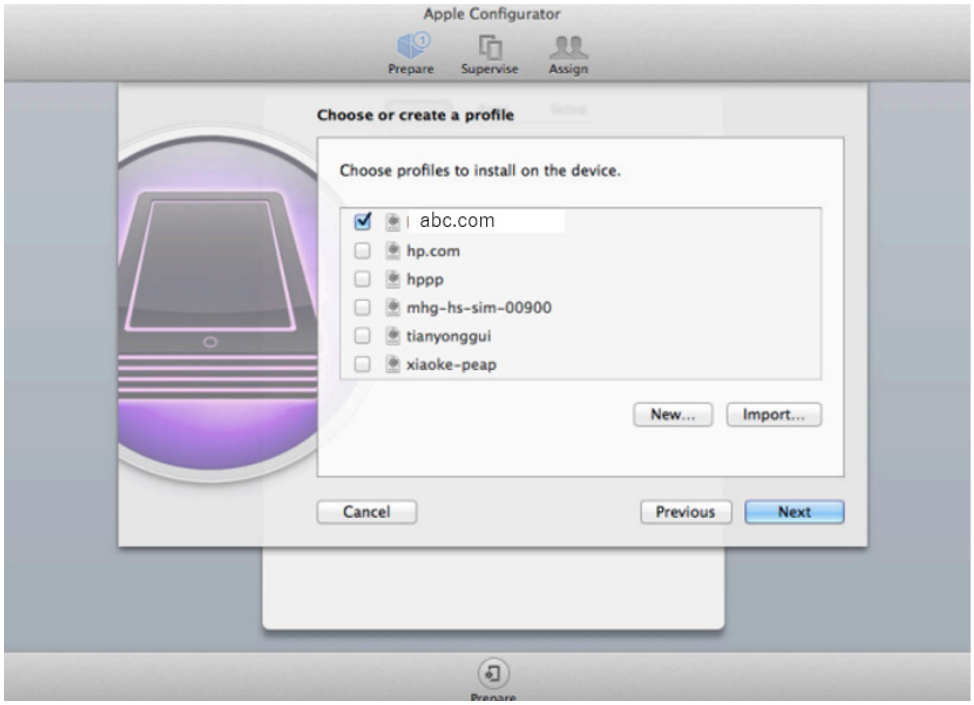


図 4-19 作成したプロファイルの選択

9)　[Install] をクリックします。

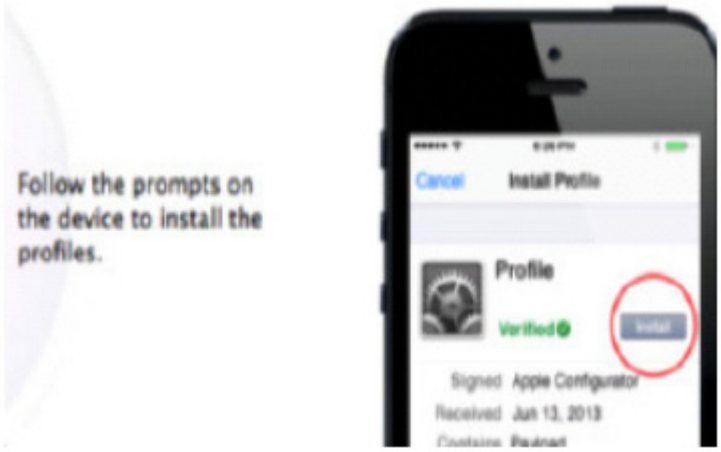


図 4-20 プロファイルのインストール図

インストールが完了すると、[Apple Configurator] ページに [Install Succeeded] と表示され、すべての設定が iPhone 5S に導入されます。電話機は必要なサービスを見つけると、自動的に WLAN に接続します。

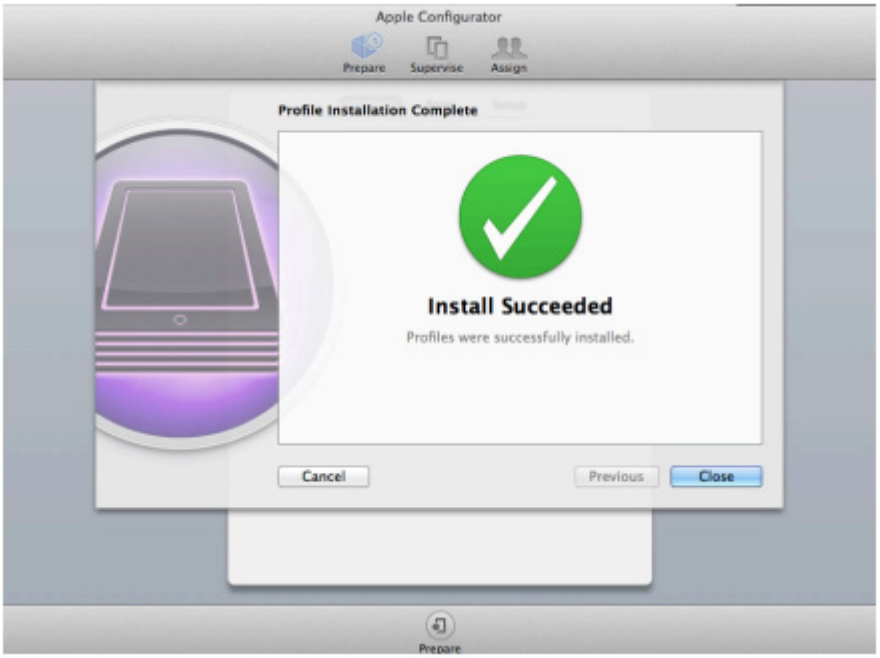


図 4-21 インストール完了図

VII. 設定の確認

#電話機が WLAN サービスに自動的に接続できることを確認します。

[AC] display wlan client verbose	
Total number of clients: 1	
MAC address	: 6021-c05d-19e0
IPv4 address	:105.0.0.5
IPv6 address	: N/A
Username	: admin
AID	: 1
AP ID	: 2
AP name	: ap1
Radio ID	: 2
Channel	: 36
SSID	: service
BSSID	: 70f9-6dd7-cfd0
VLAN ID	: 1
Sleep count	: 0
Wireless mode	: 802.11gn
Channel bandwidth	: 20MHz
SM power save	: Enabled
SM power save mode	: Static
Short GI for 20MHz	: Supported
Short GI for 40MHz	: Not supported
STBC RX capability	: Not supported
STBC TX capability	: Not supported
LDPC RX capability	: Not supported
Block Ack	: TID 0 In
Support HT-MCS set	: 0, 1, 2, 3, 4, 5, 6, 7
Supported rates	: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps
QoS mode	: WMM
Listen interval	: 10
RSSI	: 49
Rx/Tx rate	: 1/72.2 Mbps
Authentication method	: Open system
Security mode	: RSN
AKM mode	: 802.1X
Cipher suite	: CCMP

User authentication mode	: 802.1X
WPA3 status	: N/A
Authorization ACL ID	: N/A
Authorization user profile	: N/A
Authorization CAR	: N/A
Roam status	: N/A
Key derivation	: SHA1
PMF status	: N/A
Forwarding policy name	: N/A
Online time	: 0days 0hours 0minutes 36seconds
FT status	: Inactive

4.8.1 例:Hotspot 2.0 Samsung アプリケーションの設定

I. ネットワーク要件

図 4-22 に示すように、Hotspot 2.0 を設定して、電話機が携帯電話ネットワークからワイヤレスネットワークに切り替えられるようにします。

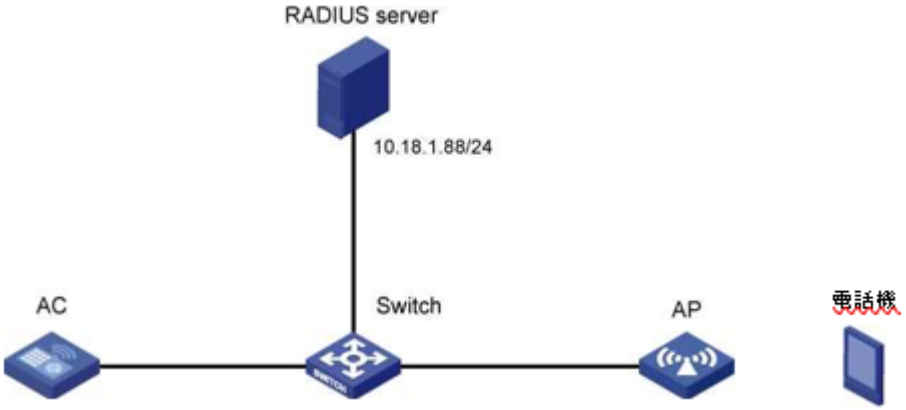


図 4-22 ネットワーク図

II. 前提条件

Hotspot 2.0 を設定する前に、次の作業を完了します。

- クライアントの認証、許可、アカウンティングを正しく動作させるには、RADIUS サーバに証明書をインストールし、ユーザアカウントを作成する必要があります。AAA の詳細は、オペレーションマニュアルのセクション 13 ユーザアクセスと認証 "*AAA*" の"*一般的に使用される標準 RADIUS 属性の説明*"を参照してください。
- 802.1X にアクセスし、電話機に証明書をインストールします。

III. AC の設定

1)　Hotspot 2.0 ポリシーを設定します。

#Hotspot 2.0 ポリシーを作成します。

```
<AC>system-view
[AC] wlan hotspot-policy 1
```

#NAI レルム abc.com の認証タイプを設定する。

```
[AC-wlan-hs-1] nai-realm name abc.com eap-method 6 auth-method 2 authentication 4
```

ドメイン名を domain.abc.com に設定する。

```
[AC-wlan-hs-1] domain-name domain.abc.com
```

#HESSID を AP の MAC アドレスである 1232 ff23-0123 に設定します。

```
[AC-wlan-hs-1] hessid 1232-ff23-0123
[AC-wlan-hs-1] quit
```

2)　802.1X 認証および RADIUS スキーム:

#802.1X 認証方式を EAP として使用します。

```
[AC] dot1x authentication-method eap
```

#RADIUS スキーム imcc を作成します。

```
[AC] radius scheme imcc
```

プライマリー認証サーバの IP アドレスとポート番号それぞれを 10.18.1.88、1812 に設定します。

```
[AC-radius-imcc] primary authentication 10.18.1.88 1812
```

プライマリー・アカウンティング・サーバーの IP アドレスとポート番号をそれぞれ 10.18.1.88 と 1813 に設定します。

```
[AC-radius-imcc] primary accounting 10.18.1.88 1813
```

#認証サーバおよびアカウンティングサーバとパケットを交換する AC の共有鍵を 12345678 に設定します。

```
[AC-radius-imcc] key authentication simple 12345678
[AC-radius-imcc] key accounting simple 12345678
```

#AC を設定して、RADIUS サーバに送信されたユーザ名のドメイン名を削除します。

```
[AC-radius-imcc] user-name-format without-domain
[AC-radius-imcc] quit
```

3)　ドメイン imc を作成し、認証、許可、およびアカウンティングに RADIUS スキーム imcc を使用するようにドメインを設定します。

```
[AC] domain imc
[AC-isp-imc] authentication lan-access radius-scheme imcc
[AC-isp-imc] authorization lan-access radius-scheme imcc
[AC-isp-imc] accounting lan-access radius-scheme imcc
[AC-isp-imc] quit
```

IV. AP の設定

#サービステンプレートサービスの作成。

```
<AC> system-view
[AC] wlan service-template service1
```

#SSID を service に設定する。

```
[AC-wlan-st-service1] ssid service
```

#Hotspot 2.0 ポリシー1 をサービステンプレートにバインドする。

```
[AC-wlan-st-service1] hotspot-policy 1
```

ビーコンおよびプローブ応答で RSN IE を有効にする。

```
[AC-wlan-st-stname] security-ie rsn
```

#AES-CCMP cipher スイートをイネーブルにします。

```
[AC-wlan-st-service1] cipher-suite ccmp
```

認証および鍵管理モードを 802.1X に設定します。

```
[AC-wlan-st-service1] akm mode dot1x
```

#WLAN クライアントの認証モードを 802.1X に設定します。

```
[AC-wlan-st-service1] client-security authentication-mode dot1x
```

認証ドメインとしてドメイン imc を指定します。

```
[AC-wlan-st-service1] dot1x domain imc
```

#サービステンプレートを有効にする。

```
[AC-wlan-st-service1] service-template enable
[AC-wlan-st-service1] quit
```

#AP ap1 を作成し、AP モデルとシリアル ID を指定する。

```
[AC] wlan ap1 model W1120
[AC-wlan-ap-ap1] serial-id 219801A28N819CE0002T
```

#サービステンプレート service1 を AR の無線 2 にバインドする。

```
[AC-wlan-ap-ap1] radio 2
[AC-wlan-ap 1-radio-2] radio enable
[AC-wlan-ap-ap1-radio-2] service-template service1
[AC-wlan-ap-ap1-radio-2] quit
[AC-wlan-ap-ap1] quit
```

V. RADIUS サーバの設定 (IMCv7)

この例は、IMC PLAT 7.1 および IMC UAM 7.1 で作成されています。

IMC サーバを設定するには、次の手順を実行します。

1) IMC プラットフォームにログインします。
2) [User] タブをクリックします。
3) アクセス装置を追加します。

a) ナビゲーションツリーから、[User Access Policy] > [Access Device Management] > [Access Device] を選択します。

b) アクセス装置の設定ページで、[Add] をクリックします。

c) [Add Access Device] ページで、次のパラメータを設定します。

- 共有鍵を 12345678 に設定します。
- IP アドレス 10.18.1.1 (AC の IP アドレス) の装置を選択または手動で追加します。
- その他のパラメータにはデフォルト設定を使用します。

d) [OK] をクリックします。 [Accepted EAP Types] 領域で、[PEAP] を選択します。

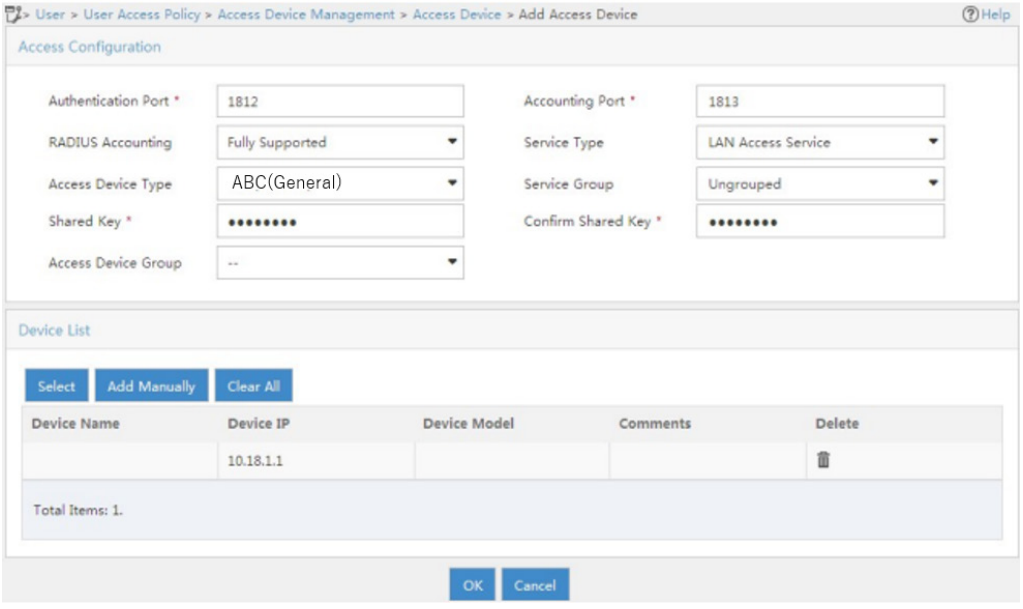


図 4-23 アクセス装置の追跡図

4) アクセスポリシーを追加します。

a) ナビゲーションツリーから、User Access Policy] > [Access Policy] を選択します。

b) アクセスポリシーの設定ページで、[Add] をクリックします。

c) [Add Access Policy] ページで、次のパラメータを設定します。

- アクセスポリシー名を 802.1X_policy に設定します。
- [Certificate Type] リストから [EAP-PEAP Authentication] を選択し、[Certificate Sub-Type] リストから、クライアントの認証方式と同じ証明書サブタイプを選択します。
- その他のパラメータにはデフォルト設定を使用します。

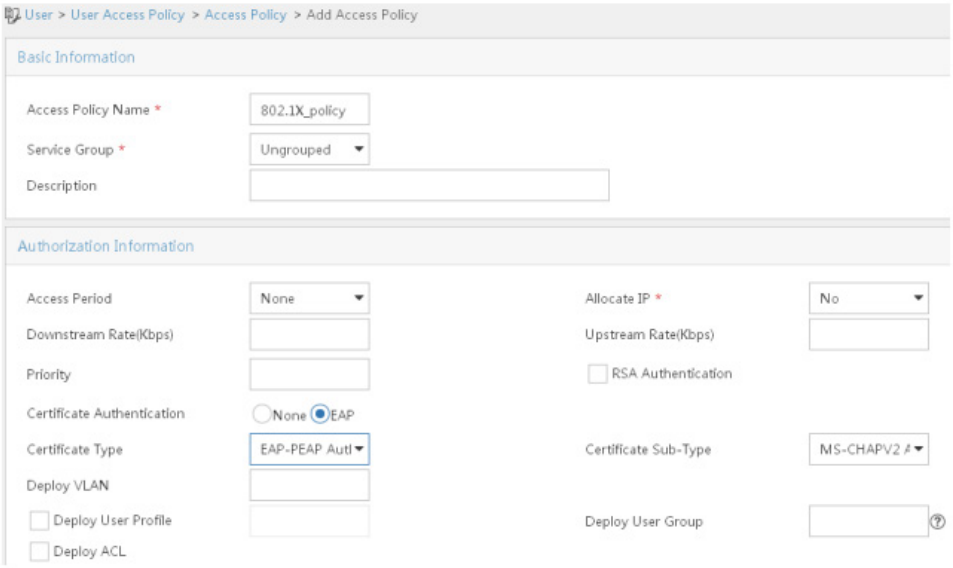


図 4-24 アクセスポリシーの追加図

5) アクセスサービスを追加します。

a) ナビゲーションツリーから、[User Access Policy] > [Access Service] を選択します。

b) アクセスサービス設定ページで、[Add] をクリックします。

c) [Add Access Service] ページで、サービス名を802.1X_serとして設定し、作成した802.1Xポリシーをデフォルトのアクセスポリシーとして使用します。

d) その他のパラメータにはデフォルト設定を使用します。

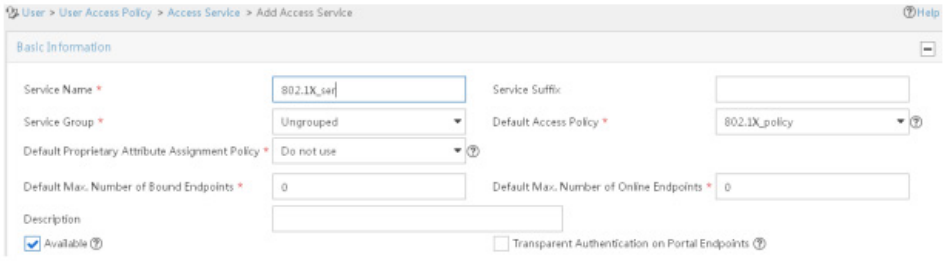


図 4-25 アクセスサービスの追加図

6)　アクセスユーザを追加します。

a)　ナビゲーションツリーから、[Access User] > [All Access Users] を選択します。

b)　アクセスユーザ 設定ページで、[Add] をクリックします。

c)　[Add Access User] ページで、[Add User] をクリックします。

d)　[ユーザの追加] 画面で、次のパラメータを設定します。

- ユーザ名を admin に設定します。
- アカウント名を admin に設定します。
- エリアで設定した 802.1X ユーザを選択します。

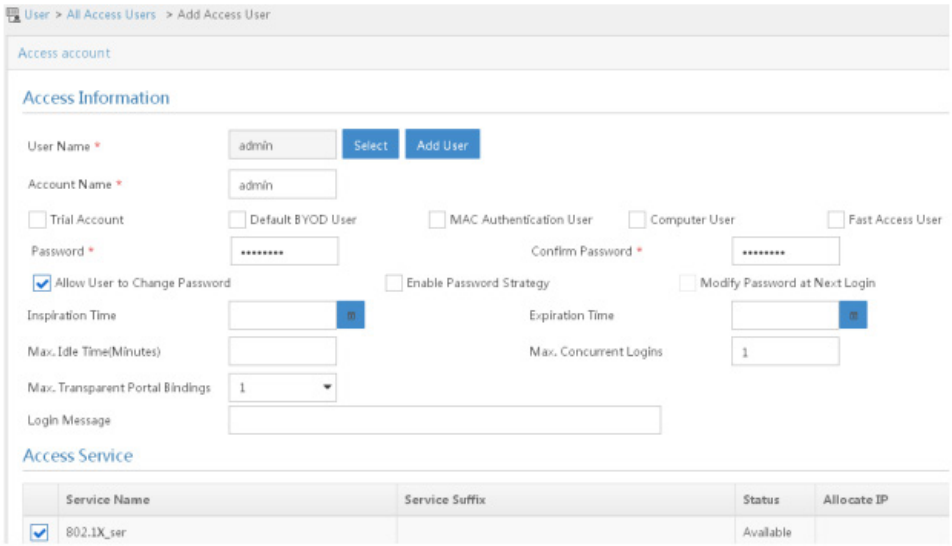


図 4-26 アクセスユーザの追加図

VI. 電話機の設定

重要：

- 電話機と AC の Hotspot 2.0 ポリシーの両方に同じレルム名とドメインを設定します。
- 設定電話機と RADIUS サーバの両方に同じユーザ名とパスワードを設定します。
- 設定では、電話機、AC の Hotspot 2.0 ポリシー、および RADIUS サーバに同じ認証タイプを使用します。

この例では、Samsung S4 電話機を使用します。

電話機を設定:

1)　テキストエディタを使用して Hotspot 2.0 設定ファイルを編集し、cred.conf という名前で PC または電話機に保存します。

```
cred={
realm="abc.com"
username="admin"
password="12345678"
```

domain="domain.abc.com"

eap=PEAP

phase2="auth=MSCHAPV2"}

2) 設定ファイルを電話機のルートディレクトリに保存します。

- PC で設定ファイルを編集する場合は、次のどちらかの方法で設定ファイルを電話機にインポートし、ルートディレクトリに保存します。
  - □ USB ケーブルを使用して電話機を PC に接続し、cred.conf を PC から電話機にコピーします。
  - □ cred.conf を添付した電子メールを電話機に送信し、ファイルを電話機に保存します。
- テキストエディタを使用して電話機でファイルを編集する場合は、電話機のルートディレクトリに保存します。

3) 電話機で WLAN をオンにします。



図 4-27 WLAN オン図

4) [Advanced] をクリックします。

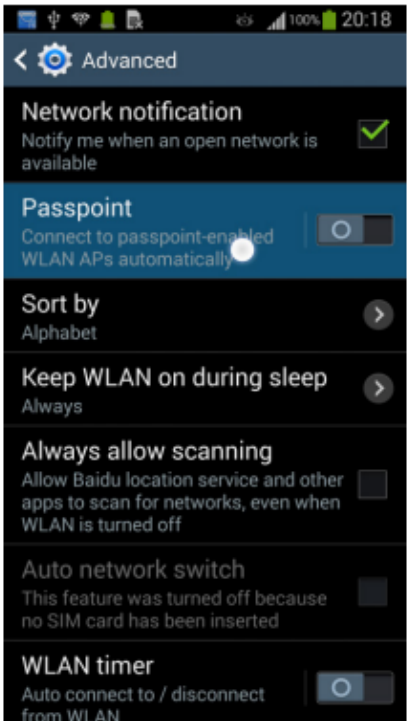


図 4-28 WLAN の詳細設定の構成図

5)　[Advanced] ページで、Passpoint を有効にします。



図 4-29 パスポイントの有効化図

VII. 設定の確認

#電話機が WLAN サービスに自動的に接続できることを確認します。

```
[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                       : admin
AID                            : 1
AP ID                          : 2
AP name                        : ap1
Radio ID                       : 2
Channel                        : 36
SSID                           : service
BSSID                          : 0026-3e08-1150
VLAN ID                        : 1
Sleep count                    : 0
Wireless mode                  : 802.11gn
Channel bandwidth              : 20MHz
SM power save                  : Enabled
SM power save mode             : Static
Short GI for 20MHz             : Supported
Short GI for 40MHz             : Not supported
STBC RX capability             : Not supported
STBC TX capability             : Not supported
LDPC RX capability             : Not supported
Block Ack                      : TID 0 In
Support HT-MCS set             : 0, 1, 2, 3, 4, 5, 6, 7
Supported rates                : 1, 2, 5.5, 6, 9, 11,
                                 12, 18, 24, 36, 48, 54 Mbps
QoS mode                       : WMM
Listen interval                : 10
RSSI                           : 49
Rx/Tx rate                     : 130/11 Mbps
Authentication method          : Open system
Security mode                  : RSN
AKM mode                       : 802.1X
```

Cipher suite	: CCMP
User authentication mode	: 802.1X
WPA3 status	: 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	: N/A
Online time	: 0days 0hours 0minutes 36seconds
FT status	: Inactive

4.8.2 例:Hotspot 2.0 の設定 (バージョン 2 の場合)

I. ネットワーク要件

図 4-30 に示すように、Hotspot 2.0 を設定して、電話機がセルラーネットワークからワイヤレスネットワークに切り替えられるようにします。

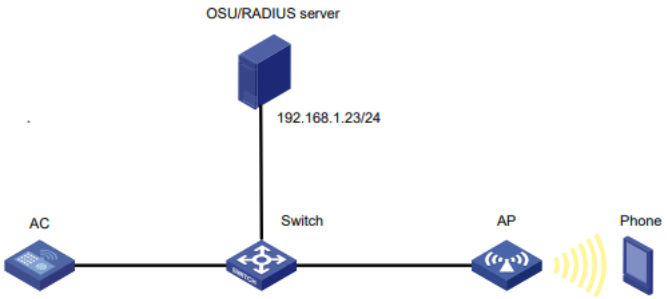


図 4-30 ネットワーク図

II. 設定の制限とガイドライン

Hotspot 2.0 を設定する場合は、次の設定の制限とガイドラインに従ってください。

1) AAA の詳細は、オペレーションマニュアルのセクション 13 ユーザアクセスと認証 "*AAA*"の"*一般的に使用される標準 RADIUS 属性の説明*"を参照してください。
2) OSU サーバのアイコンをアップロードする前に、バージョンファイルが保存されているルートディレクトリにアイコンファイルがあることを確認します。FTP または TFTP を使用してアイコンファイルを送信できます。

III. 設定手順

1)　OSU サーバ設定:

#OSU サーバ 1 を作成します。

```
<AC>system-view
[AC] wlan osu-provider 1
```

#OSU サーバの名前を osu_test に設定します。

```
[AC-wlan-osu-1] friendly-name osu_test lang-code eng
```

#OSU サーバの URI を指定します。

```
[AC-wlan-osu-1] uri https://192.168.1.23:8088/service
```

#クライアントが OSU サーバと通信する際のプロトコルを SOAP-XML SPP に設定します。

```
[AC-wlan-osu-1] method 1
```

#OSU サーバのアイコンを指定します。

```
[AC-wlan-osu-1] icon-file test.png lang-code eng icon-type png
```

#設定 OSU サーバの説明。

```
[AC-wlan-osu-1] description "The OSU provider." lang-code eng
```

#NAI を設定します。

```
[AC-wlan-osu-1] nai example.com
[AC-wlan-osu-1] quit
```

2)　Hotspot 2.0 ポリシー設定:

#Hotspot の作成 2.0 ポリシー1。

```
[AC] wlan hotspot-policy 1
```

#NAI レルム example.com の認証タイプを指定します。

```
[AC-wlan-hs-1] nai-realm name example.com eap-method 5 auth-method 2 authentication 4
```

#アクセスネットワークタイプを「ワイルドカード」に設定します。

```
[AC-wlan-hs-1] network-type 15
```

#OI を 80F62E に設定し、ビーコンに OI を追加します。

```
[AC-wlan-hs-1] roam-oi 80F62E in-beacon
```

ドメイン名を domain.com に設定します。

```
[AC-wlan-hs-1] domain-name domain.com
```

#IPv4 アドレスおよび IPv6 アドレスの可用性を 1 に設定します。

```
[AC-wlan-hs-1] ip-type ipv4 1 ipv6 1
```

#オンラインサインアップサービスの SSID を osu-ssid に設定します。

```
[AC-wlan-hs-1] osu-ssid osu-ssid
```

#OSU サーバ 1 を Hotspot 2.0 ポリシー1 にバインドします。

```
[AC-wlan-hs-1] osu-provider 1
[AC-wlan-hs-1] quit
```

#指定したアイコンファイルが変更された場合、指定した OSU サーバのアイコンをアップロードする。

```
[AC] wlan hotspot osu-icon upload
```

3)　オンラインサインアップサービス用のサービステンプレート設定

#サービステンプレート osu を作成する。

```
[AC] wlan service-template osu
```

#SSID を osu-ssid に設定する。

```
[AC-wlan-st-osu] ssid osu-ssid
```

#サービステンプレートを有効にする。

```
[AC-wlan-st-osu] service-template enable
[AC-wlan-st-osu] quit
```

4)　802.1X 認証と RADIUS サーバ設定:

#設定 802.1X 認証方式を EAP として使用。

```
[AC] dot1x authentication-method eap
```

#RADIUS スキーム imcc を作成。

```
[AC] radius scheme imcc
```

プライマリー認証サーバの IP アドレスを「192.168.1.23」、ポート番号を「1813」に設定する。

```
[AC-radius-imcc] primary authentication 192.168.1.23 1812
```

プライマリーアカウンティングサーバの IP アドレスを「192.168.1.23」、ポート番号を「1813」に設定する。

```
[AC-radius-imcc] primary accounting 192.168.1.23 1813
```

#認証およびアカウンティングサーバとパケット交換する AC の共有鍵を「12345678」に設定する。

```
[AC-radius-imcc] key authentication simple 12345678
[AC-radius-imcc] key accounting simple 12345678
```

#AC を設定して、RADIUS サーバに送信されたユーザ名のドメイン名を削除します。

```
[AC-radius-imcc] user-name-format without-domain
[AC-radius-imcc] quit
```

5)　ISP ドメイン設定:

ドメイン imc を作成し、認証、許可、アカウンティングに RADIUS スキーム imcc を使用するようにドメインを設定します。

```
[AC] domain imc
[AC-isp-imc] authentication lan-access radius-scheme imcc
[AC-isp-imc] authorization lan-access radius-scheme imcc
[AC-isp-imc] accounting lan-access radius-scheme imcc
[AC-isp-imc] quit
```

6)　無線サービス用の設定サービステンプレート設定:

#サービステンプレート stname の作成。

```
[AC] wlan service-template stname
```

#SSID を service に設定する。

```
[AC-wlan-st-stname] ssid service
```

#Hotspot 2.0 ポリシー1 をサービステンプレートにバインドします。

```
[AC-wlan-st-stname] hotspot-policy 1
```

7)　AP 設定:

#AP ap1 を作成し、AP モデルとシリアル ID を指定します。

```
[AC] wlan ap1 model W1120
[AC-wlan-ap-ap1] serial-id 219801A28N819CE0002T
```

#AP の場所名を設定します。

```
[AC-wlan-ap-ap1] venue name "ABC lab" lang-code eng url
```

#サービステンプレート stname を AP の無線 2 にバインドする。

```
[AC-wlan-ap-ap1] radio 2
[AC-wlan-ap-ap1-radio-2] radio enable
[AC-wlan-ap-ap1-radio-2] service-template stname
[AC-wlan-ap-ap1-radio-2] service-template osu
[AC-wlan-ap-ap1-radio-2] quit
[AC-wlan-ap-ap1] quit
```

IV. 設定の確認

#OSU サーバアイコンがロードされていることを確認します。

```
[AC] display wlan hotspot uploaded-osu-icon
Total number of icons: 1
Icon name Icon type
test.png    png
```

#電話機が WLAN サービスに自動的に接続できることを確認します。

```
[AC] display wlan client verbose
Total number of clients: 1

MAC address                    : d022-bee8-a267
IPv4 address                   : 192.168.1.52
IPv6 address                   : N/A
Username                       : abcd
AID                            : 2
AP ID                          : 1
AP name                        : ap1
Radio ID                       : 2
Channel                        : 36
SSID                           : service
BSSID                          : 5866-ba74-e790
VLAN ID                        : 1
Sleep count                    : 37
Wireless mode                  : 802.11gn
Channel bandwidth              : 20MHz
SM power save                  : Disabled
Short GI for 20MHz             : Supported
Short GI for 40MHz             : Not supported
STBC RX capability             : Supported
STBC TX capability             : Not supported
LDPC RX capability             : Not supported
Block Ack                      : TID 0 Both
                                 TID 2 Out
Supported HT MCS set           : 0, 1, 2, 3, 4, 5, 6, 7
Supported rates                : 1, 2, 5.5, 6, 9, 11,
                                 12, 18, 24, 36, 48, 54 Mbps
QoS mode                       : WMM
Listen interval                : 10
RSSI                           : 45
Rx/Tx rate                     : 72.2/72.2 Mbps
Authentication method          : Open system
Security mode                  : RSN
AKM mode                       : 802.1X
```

Cipher suite	: CCMP
User authentication mode	: 802.1X
WPA3 status	: N/A
Authorization ACL ID	: N/A
Authorization user profile	: N/A
Authorization CAR	: N/A
Roam status	: N/A
Key derivation	: SHA1
PMF status	: N/A
Forwarding policy name	: N/A
Online time	: 0days 0hours 1minutes 29seconds
FT status	: Inactive

QX-W2300AC シリーズ アクセスコントローラ

オペレーションマニュアル

13. 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 アクセス認証

02-WLAN IP スヌーピング

03-AAA

目次

このセクションのページは **13-x-x** です。

1章 WLANアクセス認証 1-1
1.1 概要 1-1
1.2 認証モード 1-1
1.3 802.1X認証 1-1
1.4 MAC認証 1-6
1.5 WLAN VLANの操作 1-6
1.6 WLANアクセス認証の前提条件 1-9
1.7 グローバルWLANアクセス認証パラメータの設定 1-9
1.7.1 802.1X認証のためのEAPリレーまたはEAP終了の有効化 1-10
1.7.2 802.1X認証要求の最大試行回数の設定 1-10
1.7.3 802.1X認証タイマの設定 1-10
1.7.4 MAC認証ユーザアカウント形式の設定 1-11
1.7.5 グローバルMAC認証ドメインの指定 1-12
1.7.6 MAC認証タイマの設定 1-12
1.8 サービス特有のWLAN認証パラメータの設定 1-13
1.8.1 認証モードの設定 1-13
1.8.2 WLANクライアントのオーセンティケータの指定 1-13
1.8.3 オンラインユーザハンドシェーク機能の設定 1-13
1.8.4 オンラインユーザハンドシェークセキュリティ機能の設定 1-14
1.8.5 802.1X認証ドメインの指定 1-15
1.8.6 同時802.1Xクライアントの最大数の設定 1-15
1.8.7 定期的なオンラインユーザ再認証機能の有効化 1-15
1.8.8 同時MAC認証クライアントの最大数の設定 1-16
1.8.9 サービス固有のMAC認証ドメインの指定 1-16
1.8.10 802.1XまたはMAC認証の失敗を無視する 1-17
1.8.11 WLAN Auth-Fail VLANの設定 1-18
1.8.12 サーバからの認可情報の無視 1-18
1.8.13 認可フェールオフライン機能の有効化 1-18
1.8.14 アカウンティング開始トリガー機能の設定 1-19
1.8.15 accounting-updateトリガー機能の設定 1-20
1.8.16 accounting-restartトリガー機能の設定 1-20
1.8.17 IPプロトコルバージョンによる802.1Xデュアルスタッククライアントのトラフィックアカウンティングの有効化 1-21
1.9 失敗許可機能の設定 1-22
1.9.1 失敗許可について 1-22
1.9.2 失敗許可機能の設定 1-23
1.9.3 RADIUSサーバ検出の設定 1-23
1.9.4 レーダーによる通信停止回避用サービステンプレート設定 1-23
1.10 WLANアクセス認証の設定例 1-24
1.10.1 802.1 X EAP-PEAP RADIUS認証の設定 1-24
1.10.2 RADIUSサーバとして機能するACでのローカル802.1 X EAP-PEAP認証の設定 1-28
1.10.3 RADIUSベースのMAC認証の設定 1-32
1.10.4 802.1X CHAPローカル認証の設定例 1-36
1.10.5 レーダーによる通信停止回避用サービステンプレートの設定例 1-38

1.10.6 PSK認証、認証バイパス時の失敗許可機能設定例 1-40
1.10.7 プライベートPSK認証、MACアドレス認証時の失敗許可機能設定例 1-41
1.10.8 802.1X認証時の失敗許可機能設定例 1-44
1.10.9 認証装置をAPに指定時の802.1X認証設定例 1-47

1章 WLAN アクセス認証

1.1 概要

WLAN アクセス認証は、MAC ベースのネットワークアクセス制御を提供して、WLAN アクセスセキュリティを確保します。この機能には、次の認証方法が含まれます。

- **802.1X 認証:**拡張認証プロトコル (EAP) を使用して、クライアント、オーセンティケータ、および認証サーバの認証情報を転送します。
- **MAC 認証:**送信元 MAC アドレスを認証してネットワークアクセスを制御します。この機能には、クライアントソフトウェアは必要ありません。クライアントは、ネットワークアクセスのためにユーザ名やパスワードを入力する必要はありません。オーセンティケータは、unknown MAC アドレスを検出すると、MAC 認証プロセスを開始します。MAC アドレスが認証されると、クライアントは許可されたネットワークリソースにアクセスできます。認証されない場合、オーセンティケータはクライアントのアクセスを拒否します。

1.2 認証モード

認証モード	動作メカニズム	侵入防御
bypass（デフォルト）	認証を行いません。	不可
dot1x	802.1X認証のみを実行します。	可
mac	MACアドレス認証のみを実行します。	可
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。	可

1.3 802.1X認証

I. 認証方式

デバイスは、RADIUS サーバを介したリモート 802.1X 認証と、CHAP 方式を使用するローカル 802.1X 認証をサポートします。RADIUS 認証とローカル認証の詳細については、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*13 ユーザアクセスと認証*“の”*3 章 AAA*“を参照してください。

II. オーセンティケータ

オーセンティケータは、クライアントを認証して WLAN へのアクセスを制御します。

AC+fit AP ネットワークでは、client-security authentication-location コマンドを使用して、クライアントのオーセンティケータを AC またはその接続された AP に指定できます。

III. EAP パケットカプセル化

802.1X では、クライアントとオーセンティケータ間で EAP パケットを WLAN 経由で渡すための EAPOL(EAP over LAN) を定義しています。オーセンティケータと認証サーバ間で、802.1X は次のいずれかの方法を使用して認証情報を配信します。

- 「EAPリレー」 で説明されているように、EAPOR(EAP over RADIUS) を使用して、RADIUS で EAP パケットをカプセル化します。
- 「EAPの終了」 で説明されているように、EAP パケットから認証情報を抽出し、標準の RADIUS パケットに情報をカプセル化します。

IV. EAP リレー

このモードでは、オーセンティケータは EAPOR パケットを使用して認証情報を RADIUS サーバに送信します。RADIUS サーバは EAP-Message 属性と Message-Authenticator 属性をサポートする必要があります。

図 1-1に、EAP リレーモードでの基本的な 802.1X 認証プロセスを示します。この例では、EAP-MD5 が使用されます。

🕮 **メモ：**

- AP が接続されたクライアントの認証者として機能する場合、AP が EAP および RADIUS パケットを処理することを除いて、図 1-1の認証プロセスを使用します。

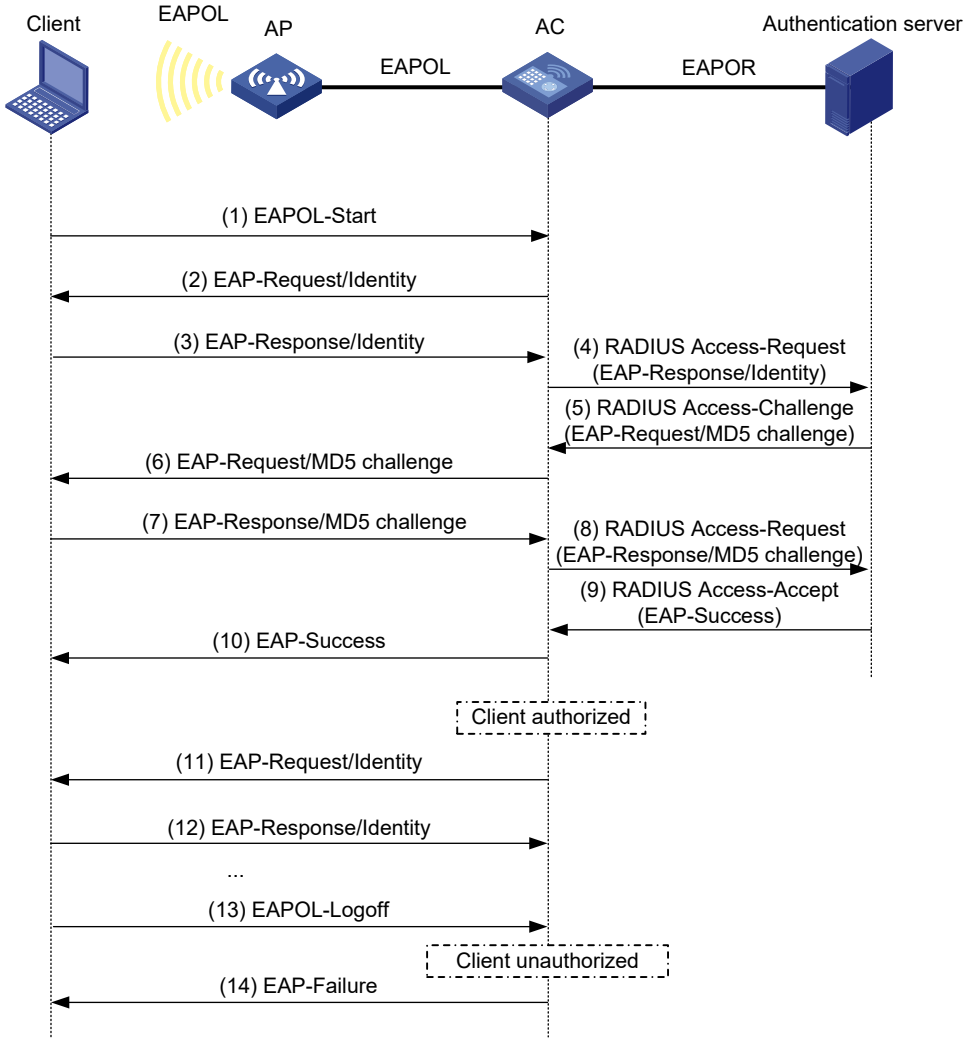


図 1-1 EAP リレーモードでの 802.1X 認証プロセス

次の手順では、802.1X 認証プロセスについて説明します。

1. ユーザが 802.1X クライアントを起動し、登録されたユーザ名とパスワードを入力すると、802.1X クライアントは EAPOL-Start パケットをオーセンティケータに送信します。

   クライアントと AP のアソシエーションメカニズムの詳細については、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*8 WLAN セキュリティ*”の”*1 章 WLAN セキュリティ*”を参照してください。
2. オーセンティケータは、EAP-Request/Identity パケットで応答し、ユーザ名を要求します。
3. クライアントは、EAP-Response/Identity パケット内のユーザ名をオーセンティケータに送信します。
4. オーセンティケータは、RADIUS Access-Request パケット内の EAP-Response/Identity パケットを認証サーバに中継します。
5. 認証サーバは、RADIUS Access-Request 内のユーザ名を使用して、ユーザデータベースを検索します。一致するエントリが見つかった場合、サーバはランダムに生成されたチャレンジ (EAP-Request/MD5-challenge) を使用して、エントリ内のパスワードを暗

号化します。その後、サーバは RADIUS Access-Challenge パケットでチャレンジをオーセンティケータに送信します。

6. オーセンティケータは、EAP-Request/MD5-Challenge パケットをクライアントに送信します。
7. クライアントは、受信したチャレンジを使用してパスワードを暗号化し、暗号化されたパスワードを EAP-Response/MD5-Challenge パケットでオーセンティケータに送信します。
8. オーセンティケータは、RADIUS Access-Request パケット内の EAP-Response/MD5-Challenge パケットを認証サーバに中継します。
9. 認証サーバは、受信した暗号化パスワードと、ステップ 5 で生成した暗号化パスワードを比較します。2 つのパスワードが同一の場合、サーバはクライアントを有効と見なし、認証者に RADIUS Access-Accept パケットを送信します。
10. 認証者は、RADIUS Access-Accept パケットを受信すると、クライアントがネットワークにアクセスできるようにします。
11. クライアントがオンラインになった後、オーセンティケータは定期的にハンドシェーク要求を送信し、クライアントがまだオンラインかどうかを調べます。
12. ハンドシェーク要求を受信すると、クライアントは応答を返します。何回も連続してハンドシェークを試行した後 (デフォルトでは 2 回) 、クライアントが応答を返さなかった場合、オーセンティケータはクライアントをログオフします。このハンドシェークメカニズムにより、異常にオフラインになった 802.1X クライアントが使用するネットワークリソースを適時に解放できます。
13. クライアントは EAPOL-Logoff パケットを送信して、オーセンティケータからのログオフを要求します。
14. オーセンティケータは EAPOL-Logoff パケットに応答して、EAP-Failure パケットをクライアントに送信します。

V. EAP の終了

このモードでは、オーセンティケータは次の操作を実行します。

1. クライアントから受信した EAP パケットを終了します。
2. クライアント認証情報を標準の RADIUS パケットにカプセル化します。
3. PAP または CHAP を使用して RADIUS サーバと通信します。

図 1-2に、EAP 終了モードでの基本的な 802.1X 認証プロセスを示します。この例では、CHAP 認証が使用されます。

🕮 **メモ：**

- AP が接続されたクライアントの認証者として機能する場合、AP が EAP および RADIUS パケットを処理することを除いて、図 1-2の認証プロセスが使用されます。

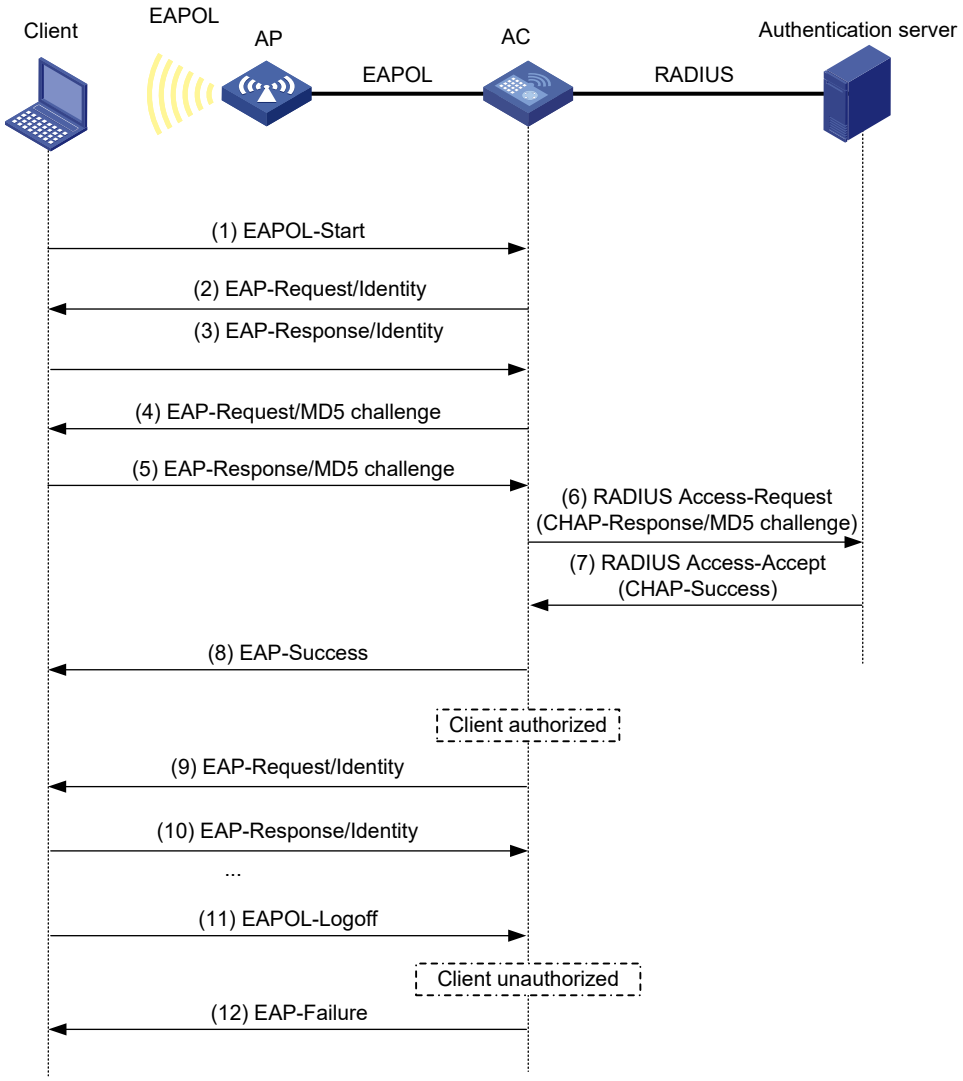


図 1-2 EAP 終了モードでの 802.1X 認証プロセス

EAP 終了モードでは、認証サーバではなくオーセンティケータがパスワード暗号化の MD5 チャレンジを生成します。その後、オーセンティケータは MD5 チャレンジをユーザ名と暗号化されたパスワードとともに標準の RADIUS パケットで RADIUS サーバに送信します。

VI. 802.1X 認証の開始

802.1X 認証は、オーセンティケータに関連付けられた直後にクライアントに対して開始されます。クライアントまたはオーセンティケータのいずれかが 802.1X 認証を開始できます。

- **クライアントの開始:**クライアントはオーセンティケータに EAPOL-Start パケットを送信し、オーセンティケータに関連付けられた後で 802.1X 認証を開始します。
- **オーセンティケータの開始:**オーセンティケータは EAP-Request/Identity パケットを送信し、クライアントがオーセンティケータに関連付けられた後で 802.1X 認証を開始します。クライアントのタイムアウトタイマ内に応答が受信されなかった場合、オーセンティケータはパケットを再送信します。

1.4 MAC認証

I. 認証方式

認証サーバ (ローカル認証) または RADIUS サーバを介して MAC 認証を実行できます。RADIUS 認証およびローカル認証の詳細については、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*13 ユーザアクセスと認証*“の”*3 章 AAA*“を参照してください。

II. オーセンティケータ

オーセンティケータは、クライアントを認証して WLAN へのアクセスを制御します。

AC+fit AP ネットワークでは、client-security authentication-location コマンドを使用して、AC または AP をオーセンティケータとして指定できます。

III. ユーザアカウントポリシー

クライアントを識別するには、ユーザアカウントが必要です。MAC 認証では、次のユーザアカウントポリシーがサポートされます。

- クライアントごとに 1 つの MAC ベースのユーザアカウント。オーセンティケータは、MAC 認証のクライアントのユーザ名およびパスワードとして、パケット内の送信元 MAC アドレスを使用します。
- すべてのクライアントに対して 1 つの共有ユーザアカウント。オーセンティケータ上のすべての MAC 認証クライアントに対して、1 つのユーザ名とパスワードを指定します。ユーザ名は大文字と小文字を区別する 1～55 文字の文字列で、アットマーク (@) を含めることはできません。パスワードには、1～63 文字のプレーンテキスト文字列または、1～117 文字の暗号テキスト文字列を使用できます。

IV. MAC 認証手順

RADIUS 認証:

- **MAC ベースのアカウント**:オーセンティケータは、パケットの送信元 MAC アドレスをユーザ名およびパスワードとして認証のために RADIUS サーバに送信します。
- 共有アカウント:オーセンティケータは、認証のために共有アカウントのユーザ名およびパスワードを RADIUS サーバに送信します。
- ローカル認証:
- MAC ベースのアカウント:オーセンティケータは、パケットの送信元 MAC アドレスをユーザ名とパスワードとして使用して、一致するローカルアカウントデータベースを検索します。
- 共有アカウント:オーセンティケータは、共有アカウントのユーザ名とパスワードを使用して、一致するローカルアカウントデータベースを検索します。

1.5 WLAN VLANの操作

I. VLAN の許可

WLAN クライアントの認可 VLAN を指定して、クライアントのネットワークリソースへのアクセスを制御できます。クライアントが 802.1X または MAC 認証に合格すると、認

証サーバはオーセンティケータに認可 VLAN 情報を割り当てます。デバイスがオーセンティケータとして動作すると、次の形式のサーバ割り当て VLAN を解決できます。

- Vlan ID
- VLAN 名:VLAN 名は、アクセスデバイス上の VLAN の説明を表します。
- VLAN グループ名:VLAN グループの詳細については、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“5 ネットワーク接続”の”3 章 VLAN”を参照してください。
- VLAN ID+VLAN 名:文字列では、一部の VLAN は ID で表され、一部の VLAN は名前で表されます。

サーバが VLAN のグループを割り当てると、アクセスデバイスは VLAN ID の形式に従って VLAN を選択して割り当てます。

認可 VLAN のタイプ	VLAN の選択および割り当てルール
・VLAN ID ・VLAN 名 ・VLAN ID＋VLAN 名	装置は、VLANのグループから最も小さいIDのVLANを選択します。
VLAN グループ名	1.装置は、オンラインユーザ数が最も少ないVLANを選択します。 2.複数のVLANのオンライン802.1Xユーザの数が同じ場合、デバイスはIDが最も小さいVLANを選択します。

🕮 **メモ：**

- デバイスは、クライアントに VLAN を割り当てる前に、VLAN 名と VLAN グループ名を VLAN ID に変換します。

デバイスは、次の状況でクライアントの VLAN 許可に失敗します。

- デバイスは、許可 VLAN 情報の解決に失敗します。
- サーバはデバイスに VLAN 名を割り当てますが、デバイスにはその名前を使用する VLAN がありません。
- サーバはデバイスに VLAN グループ名を割り当てますが、VLAN グループが存在しないか、VLAN グループに VLAN が割り当てられていません。

階層型 AC ネットワークでは、オーセンティケータとデータ転送用のデバイスは異なるデバイスにすることができます。たとえば、中央 AC は認証を実行し、ローカル AC または AP はデータ トラフィックを転送します。

認可 VLAN 情報はデータ転送の制御に使用されるため、データ トラフィックを転送するデバイスによって割り当てられる必要があります。VLAN 割り当ては、オーセンティケータと転送デバイスが同じデバイスであるかどうかに応じて、ローカル VLAN 割り当てまたはリモート VLAN 割り当てにできます。

- ローカル VLAN 割り当て:オーセンティケータと転送デバイスは同じデバイスです。オーセンティケータは、認可 VLAN 情報を取得した後、情報を解決して VLAN を割り当てます。
- リモート VLAN 割り当て:オーセンティケータと転送デバイスは異なるデバイスです。オーセンティケータは、認可 VLAN 情報を取得した後、その情報をリモート転送デバイスに送信します。その後、転送デバイスは情報を解決し、VLAN を割り当てます。

II. 認証失敗 VLAN

WLAN 認証失敗 VLAN は、組織のセキュリティ戦略に準拠していないために、WLAN アクセス認証に失敗したクライアントに対応します。たとえば、VLAN は間違ったパスワードまたはユーザ名を入力したクライアントに対応します。認証失敗 VLAN は、認証タイム

アウトまたはネットワーク接続の問題で認証に失敗した WLAN クライアントには対応しません。

認証失敗 VLAN 内のクライアントは、限られたネットワークリソースのセットにアクセスできます。

RSNA を使用するクライアントは、802.1X 認証に失敗した後、認証失敗 VLAN に割り当てることはできません。オーセンティケータは、クライアントを直接ログオフします。

認証失敗 VLAN 機能は、侵入防御よりも優先されます。クライアントが認証に失敗すると、認証失敗 VLAN 設定が最初に適用されます。認証失敗 VLAN が設定されていない場合は、侵入保護機能が有効になります。どちらの機能も設定されていない場合、オーセンティケータはクライアントから直接ログオフします。

III. クリティカル VLAN

WLAN クリティカル VLAN は、ISP ドメイン内のすべての RADIUS サーバに到達できないため、WLAN アクセス認証に失敗したクライアントに対応します。クリティカル VLAN 内のクライアントは、設定に応じて制限されたネットワークリソースセットにアクセスできます。

オーセンティケータは、30 秒間隔でクリティカル VLAN 内のクライアントを再認証します。

- クライアントが再認証に合格すると、オーセンティケータはクライアントを認可 VLAN に割り当てます。認可 VLAN が設定されていない場合、クライアントは初期 VLAN に割り当てられます。
- すべての RADIUS サーバが到達不能であるためにクライアントが再認証に失敗した場合、クライアントはまだクリティカル VLAN にあります。
- クライアントが到達不能なサーバ以外の理由で再認証に失敗した場合、デバイスはクライアントを Auth-Fail VLAN に割り当てます。Auth-Fail VLAN が設定されていない場合、デバイスは侵入保護設定に応じてクライアントを処理します。侵入保護機能が設定されていない場合、デバイスはクライアントからログオフします。

重要な VLAN 機能は、RSNA を使用する 802.1X クライアントでは有効になりません。これらのクライアントがすべての RADIUS サーバに到達できないために認証に失敗した場合、オーセンティケータは直接クライアントをログオフします。

IV. ACL の割り当て

802.1X または MAC 認証クライアントの ACL を指定して、ネットワークリソースへのクライアントのアクセスを制御できます。クライアントが認証に成功すると、認証サーバはこのクライアントのトラフィックをフィルタリングするために ACL をクライアントに割り当てます。認証サーバは、オーセンティケータとして機能するローカルデバイスまたは RADIUS サーバ上に配置できます。いずれの場合も、オーセンティケータで ACL のルールを設定する必要があります。AP がオーセンティケータとして動作する場合は、AC で ACL ルールを設定する必要があります。

クライアントのアクセス制御基準を変更するには、次のいずれかの方法を使用できます。

- オーセンティケータの ACL ルールを変更します。
- クライアントに別の ACL を指定します。

V. ユーザプロファイルの割り当て

WLAN クライアントのユーザプロファイルを指定して、クライアントのネットワークリソースへのアクセスを制御できます。クライアントが 802.1X または MAC 認証に合格すると、認証サーバはトラフィックをフィルタリングするためにユーザプロファイルをクライアントに割り当てます。認証サーバは、オーセンティケータとして機能するローカルデバイス上に置くことも、RADIUS サーバ上に置くこともできます。いずれの場合も、オーセンティケータでユーザプロファイルを設定する必要があります。AP がオーセンティケータとして動作する場合は、AC でユーザプロファイルを設定する必要があります。

クライアントのアクセス権限を変更するには、次のいずれかの方法を使用できます。

- オーセンティケータのユーザプロファイル設定を変更します。
- クライアントに別のユーザプロファイルを指定します。

VI. CAR 属性の割り当て

デバイスは、RADIUS 拡張属性によって割り当てられた CAR 属性を使用して、認証されたオンライン 802.1X または MAC 認証ユーザのアクセスレートを制御できます。RADIUS 拡張属性の詳細については、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*13 ユーザアクセスと認証*“の”*3 章 AAA*“を参照してください。

次の CAR 属性を使用できます。

- Input-Average-Rate:着信トラフィックの平均レート (bps 単位)
- Output-Average-Rate:発信トラフィックの平均レート (bps 単位)

1.6 WLANアクセス認証の前提条件

I. 802.1X の前提条件

802.1X 認証を設定する前に、次のタスクを完了します。

- ISP ドメインを設定し、ドメイン内の 802.1X ユーザの AAA 方式を指定します。
- RADIUS 認証を使用する場合は、RADIUS サーバでユーザアカウントを作成します。
- ローカル認証を使用する場合は、アクセスデバイスでローカルユーザアカウントを作成し、サービスタイプを lan-access に設定します。

II. MAC 認証の前提条件

MAC 認証を設定する前に、ISP ドメインを設定し、ドメイン内の AAA 方式を指定します。詳細については、「AAA の設定」 を参照してください。

- ローカル認証の場合、ローカルユーザアカウント (ユーザ名とパスワードを含む) を作成し、ローカルユーザの LAN アクセスサービスを指定する必要もあります。
- RADIUS 認証の場合、デバイスと RADIUS サーバが相互に到達できることを確認し、RADIUS サーバにユーザアカウントを作成します。デバイスと RADIUS サーバで、MAC 認証に一貫したユーザアカウントポリシーが使用されていることを確認します。

1.7 グローバルWLANアクセス認証パラメータの設定

1.7.1 802.1X 認証のための EAP リレーまたは EAP 終了の有効化

I. 制約事項とガイドライン

EAP リレーモードを使用する場合は、次の制約事項とガイドラインが適用されます。

- RADIUS スキームビューの user-name-format コマンドは有効になりません。デバイスは、認証データを変更せずにクライアントからサーバに送信します。user-name-format コマンドの詳細については、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“13 ユーザアクセスと認証“の” 3 章 AAA “を参照してください。
- RADIUS サーバでクライアントと同じ認証方式が使用されていることを確認します。オーセンティケータの場合、dot 1 x authentication-method eap コマンドを使用するだけで EAP リレーが有効になります。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. EAP リレーまたは EAP 終端を有効にする	**dot1x authentication-method** { **chap** | **eap** | **pap** }	デフォルト： EAP終端 有効 認証方式 CHAP

1.7.2 802.1X 認証要求の最大試行回数の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. 802.1X 認証要求の送信の最大試行回数を設定する	**dot1x retry** *retries*	デフォルト： 10

1.7.3 802.1X 認証タイマの設定

802.1X では、次のタイマを使用してクライアントおよび RADIUS サーバとの通信を制御します。

802.1X 認証プロセスは、次のタイマによって制御されます。

- ハンドシェークタイマ(handshake-period):このタイマはユーザ認証が成功した後に起動し、デバイス側はこの間隔を周期としてハンドシェーク要求メッセージを送信し、定期的にユーザのオンライン状況を検出する。送信回数を N に設定すると、デバイス側でクライアントからの応答メッセージが N 回連続して受信されない場合、ユーザはオフラインになったと見なされます。
- 周期的再認証タイマ(reauth-period):ポートで周期的再認証機能(コマンド dot1x re-authenticate)が有効になると、デバイス側はこの間隔を周期としてポート上のオンラインユーザに対して再認証を開始する。すでにオンラインになっている 802.1X ユーザの場合は、現在の再認証サイクルが終了し、認証が完了するまで、新しい設定サイクルに従って再認証が行われません。
- 認証サーバタイムアウトタイマ(server-timeout):アクセスデバイスが RADIUS Access-Request パケットを認証サーバに送信したときに開始します。このタイマが期限切れになっても応答がない場合、802.1X 認証は失敗します。サーバタイムアウ

トタイマが期限切れになる前に強制ログオフされないようにするには、サーバタイムアウトタイマを次の値の積以下の値に設定します。

- RADIUS scheme view で **retry** コマンドを使用して設定された RADIUS パケット送信の最大試行回数。
- RADIUS scheme view で **timer response-timeout** コマンドを使用して設定された RADIUS サーバ応答タイムアウトタイマ。RADIUS メッセージ送信の最大試行回数、RADIUS サーバ応答タイムアウト時間の詳細については、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*13 ユーザアクセスと認証*“の”*3 章 AAA*“を参照してください。

- クライアント認証タイムアウトタイマ(supp-timeout):設備側はクライアントに EAP-Request/MD5 Challenge 要求メッセージを送信した後、設備側はこのタイマを起動し、もしこのタイマが設定した時間内に、設備側はクライアントの応答を受信しなければ、設備側はこのメッセージを再送する。

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。

I. 制限事項とガイドライン

ほとんどの場合、デフォルトの設定で十分です。ネットワークの状態に応じて、タイマを編集できます。次に 2 つの例を示します。

- 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やします。
- 異なるパフォーマンス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調整します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. クライアントのタイムアウトタイマを設定する	**dot1x timer supp-timeout** *supp-timeout-value*	デフォルト： 2秒
3. サーバのタイムアウトタイマを設定する	**dot1x timer server-timeout** *server-timeout-value*	デフォルト：100秒
4. ハンドシェークタイマを設定する	**dot1x timer handshake-period** *handshake-period-value*	デフォルト：15秒
5. 定期的な再認証タイマを設定する	**dot1x timer reauth-period** *reauth-period-value*	デフォルト：3600秒
6. ユーザ名要求タイムアウトタイマを設定する	**dot1x timer tx-period** *tx-period-value*	デフォルト：2秒

1.7.4 MAC 認証ユーザアカウント形式の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—

操作	コマンド	補足
2. MAC 認証ユーザアカウント形式を設定する	・クライアント毎に1つのMACをユーザアカウントとして使用 **mac-authentication user-name-format mac-address** [{ **with-hyphen** [**six-section** | **three-section**] | **without-hyphen** } [**lowercase** | **uppercase**]] ・全てのクライアント毎に1つの共有アカウントを使用 **mac-authentication user-name-format fixed** [**account** *name*] [**password** { **cipher** | **simple** } *password*]	デフォルト： ユーザ名とパスワードにMACアドレスを使用する。MACアドレスは、ハイフンなしの16進数表記で、小文字です。

1.7.5 グローバル MAC 認証ドメインの指定

MAC 認証は、WLAN クライアントの ISP ドメインを以下の順序で選択します：

1. サービステンプレート view で **mac-authentication domain** コマンドを使用して指定されたドメイン。
2. システム view で **mac-authentication domain** コマンドを使用して指定されたグローバル MAC 認証ドメイン。
3. **domain default enable** コマンドを使用して指定されたデフォルトドメイン。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. MAC 認証クライアントの ISP ドメインを指定する	**mac-authentication domain** *domain-name*	デフォルト： なし

1.7.6 MAC 認証タイマの設定

MAC 認証では、次のタイマを使用します。

- オフライン検出タイマ:ユーザがアイドル状態であるとデバイスが判断する前に、デバイスがユーザからのトラフィックを待機する間隔を設定します。タイマが切れる前にデバイスがユーザからのトラフィックを受信していない場合、デバイスはそのユーザをログオフし、ユーザのアカウンティングを停止するようにアカウンティングサーバに要求します。
- Quiet タイマ:MAC 認証に失敗したユーザに対してデバイスが MAC 認証を実行できるようになるまでの待機時間を設定します。MAC アドレスからのすべてのパケットは、待機時間中にドロップされます。この待機メカニズムにより、認証の繰り返しがシステムパフォーマンスに影響を与えることを防ぎます。
- サーバタイムアウトタイマ:RADIUS サーバが使用できないとデバイスが判断する前に、デバイスが RADIUS サーバからの応答を待機する間隔を設定します。MAC 認証中にタイマが期限切れになると、ユーザはネットワークにアクセスできなくなります。

操作	コマンド	補足
1. system view に移行する	**system-view**	—

操作	コマンド	補足
2. MAC 認証タイマを設定する	**mac-authentication timer** { **offline-detect** *offline-detect-value* | **quiet** *quiet-value* | **server-timeout** *server-timeout-value* }	デフォルト： オフライン検出タイマ:300秒、 Quietタイマ:60秒、 サーバタイムアウトタイマ:100秒

1.8 サービス特有のWLAN認証パラメータの設定

1.8.1 認証モードの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
1. サービステンプレート view に移行する	**wlan service-template** *service-template-name*	—
2. WLAN クライアントの認証モードを設定する	client-security authentication-mode { dot1x | mac | mac-and-dot1x }	デフォルト：bypassモード 装置は認証を行いません。

1.8.2 WLAN クライアントのオーセンティケータの指定

クライアントのオーセンティケータを、AC またはその接続された AP に指定できます。

I. 制約事項とガイドライン

AC がクライアントデータトラフィックを転送するように設定されている場合は、認証を成功させるために、AC をオーセンティケータとして指定する必要もあります。クライアントデータトラフィックを転送するデバイスを指定する方法については、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*6 WLAN アクセス*”の”*1 章 WLAN アクセス*”を参照してください。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. サービステンプレート view に移行する	**wlan service-template** *service-template-name*	—
3. WLAN クライアントのオーセンティケータを指定する	**client-security authentication-location** { **ac** | **ap** }	デフォルト：ac

1.8.3 オンラインユーザハンドシェーク機能の設定

オンラインユーザハンドシェーク機能は、オンライン 802.1X クライアントの接続ステータスを調べます。デバイスは、dot 1 x timer handshake-period コマンドを使用して指定された間隔で、ユニキャスト EAP-Request/Identity ハンドシェークメッセージをオンラインクライアントに送信します。デバイスがハンドシェークの最大試行回数を超えてもクライ

アントから応答を受信しない場合、デバイスはクライアントをオフライン状態に設定します。

I. 制限事項とガイドライン

デバイスは、クライアントからのハンドシェーク応答に応答しません。一部のクライアントは、ハンドシェーク応答に対するデバイスの応答を受信しない場合、再認証を開始したり、オフラインになったりすることがあります。ネットワークにそのようなクライアントがある場合は、オンラインユーザハンドシェーク機能を無効にします。

オンラインユーザハンドシェーク機能によって、一部のワイヤレスクライアントがオフラインになることがあります。このようなワイヤレスクライアントが存在する場合は、ベストプラクティスとしてこの機能を無効にしてください。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
1. サービステンプレート view に移行する	**wlan service-template** *service-template-name*	—
2. オンラインユーザハンドシェーク機能を有効にする	**dot1x handshake enable**	デフォルト：無効

1.8.4 オンラインユーザハンドシェークセキュリティ機能の設定

オンラインユーザハンドシェークセキュリティ機能は、ハンドシェークメッセージに認証情報を追加します。この機能により、不正なクライアントがデバイスとハンドシェークメッセージを交換するのを防ぐことができます。この機能により、デバイスはクライアントからのハンドシェーク応答メッセージ内の認証情報と、認証サーバによって割り当てられた認証情報を比較します。一致が見つからない場合、デバイスはクライアントからログオフします。

I. 制約事項とガイドライン

オンラインユーザハンドシェークセキュリティ機能を使用するには、オンラインユーザハンドシェーク機能が有効になっていることを確認します。

オンラインユーザハンドシェークセキュリティ機能は、オンライン認証された 802.1X クライアントのみを保護します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. サービステンプレート view に移行する	**wlan service-template** *service-template-name*	—
3. オンラインユーザハンドシェーク機能を有効にする	**dot1x handshake enable**	デフォルト：無効
4. オンラインユーザハンドシェークセキュリティ機能を有効にする	**dot1x handshake secure enable**	デフォルト：無効

1.8.5 802.1X 認証ドメインの指定

802.1X 認証では、次の順序で WLAN クライアントの ISP ドメインが選択されます。

1. サービステンプレートビューで dot 1 x domain コマンドを使用して指定されたドメイン。
2. ユーザ名に含まれるドメイン。
3. デフォルトドメイン。domain default enable コマンドを使用して設定できます。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. サービステンプレート view に移行する	**wlan service-template** *service-template-name*	—
3. サービステンプレートの 802.1X 認証ドメインを指定する	**dot1x domain** *domain-name*	デフォルト：指定なし

1.8.6 同時 802.1X クライアントの最大数の設定

サービステンプレートが無線で許可する同時 802.1X クライアントの数を制限するには、このタスクを実行します。

この設定は無線ごとに有効になります。サービステンプレートの 802.1X クライアントの数が無線の制限に達すると、その無線のサービステンプレートを介して追加の 802.1X クライアントがネットワークにアクセスできなくなります。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. サービステンプレート view に移行する	**wlan service-template** *service-template-name*	—
3. サービステンプレートが無線でサポートする同時 802.1X クライアントの最大数を設定する	**dot1x max-user** *count*	デフォルト：512

1.8.7 定期的なオンラインユーザ再認証機能の有効化

定期的なオンラインユーザ再認証は、オンラインクライアントの接続状態を追跡し、サーバによって割り当てられた認可属性を更新します。属性には、ACL、VLAN、およびユーザプロファイルベースの QoS が含まれます。再認証間隔はユーザが設定できます。

サーバがセッションタイムアウトタイマ (Session-Timeout 属性) と終了アクション (Termination-Action 属性) の設定をクライアントに割り当てると、サーバが割り当てた設定がクライアントに有効になる場合があります。サーバが割り当てた Session-Timeout 属性と Termination-Action 属性の設定を識別するには、display dot1x connection コマンドを実行します。

- 終了アクションが Default (ログオフ) の場合、デバイスでの定期的なオンラインユーザ再認証は、定期的な再認証タイマがサーバが割り当てたセッションタイムアウトタイマより短い場合にのみ有効になります。

- 終了アクションが Radius-request の場合、デバイスでの定期的なオンラインユーザ再認証設定は有効になりません。サーバが割り当てたセッションタイムアウトタイマが期限切れになると、デバイスはオンライン 802.1X クライアントを再認証します。

サーバによってセッションタイムアウトタイマが割り当てられていない場合、デバイスが定期的な 802.1X 再認証を実行するかどうかは、デバイスの定期的な再認証設定によって決まります。

Session-Timeout および Termination-Action 属性の割り当てのサポートは、サーバモデルによって異なります。

I. 制約事項とガイドライン

この機能により、一部の無線クライアントがオフラインになることがあります。このようなワイヤレスクライアントが存在する場合は、ベストプラクティスとしてこの機能を無効にしてください。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. サービステンプレート view に移行する	**wlan service-template** *service-template-name*	—
3. 定期的なオンラインユーザ再認証を有効にする	**dot1x re-authenticate enable**	デフォルト：無効

1.8.8 同時 MAC 認証クライアントの最大数の設定

サービステンプレートが無線でサポートする同時 MAC 認証クライアントの数を制限するには、次のタスクを実行します。

この設定は無線ごとに有効になります。サービステンプレートの MAC 認証クライアントの数が無線の制限に達した場合、その無線のサービステンプレートを介して追加の MAC 認証クライアントがネットワークにアクセスすることはできません。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. サービステンプレート view に移行する	**wlan service-template** *service-template-name*	—
3. サービステンプレートが無線でサポートする同時 MAC 認証クライアントの最大数を設定する	**mac-authentication max-user** *count*	デフォルト：4096

1.8.9 サービス固有の MAC 認証ドメインの指定

MAC 認証では、次の順序で WLAN クライアントの ISP ドメインが選択されます。

- サービステンプレートビューで mac-authentication domain コマンドを使用して指定されたドメイン。

- システムビューで mac-authentication domain コマンドを使用して指定されたグローバル MAC 認証ドメイン。
- domain default enable コマンドを使用して設定可能なデフォルトドメイン。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. サービステンプレート view に移行する	**wlan service-template** *service-template-name*	—
3. MAC 認証クライアントの ISP ドメインを指定する	**mac-authentication domain** *domain-name*	デフォルト：設定なし

1.8.10 802.1X または MAC 認証の失敗を無視する

この機能により、クライアントは、802.1X または MAC 認証に失敗しても、オンラインになるか、認証プロセスを続行できます。

この機能は、次のクライアントに適用されます。

- 802.1X 認証を使用するクライアント。
- この機能により、デバイスは 802.1X 認証の失敗を無視し、802.1X 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、WLAN 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、ポータル認証を実行するときにユーザ名とパスワードを提供します。

この機能により、クライアントの認証プロセスが次のように簡略化されます。

- 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。デバイスを使用すると、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。デバイスは 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。クライアントはポータル認証に合格すると、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。

I. 制限事項とガイドライン

RSN を使用して新しい AP にローミングする 802.1X クライアントの場合は、この機能を設定しないでください。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. サービステンプレート view に移行する	**wlan service-template** *service-template-name*	—
3. 802.1X または MAC 認証の失敗を無視するようにデバイスを設定する	**client-security ignore-authentication**	デフォルト：無効

1.8.11 WLAN Auth-Fail VLAN の設定

オーセンティケータは、Auth-Fail VLAN 内のクライアントを 30 秒間隔で再認証します。

- クライアントが再認証に合格すると、オーセンティケータはクライアントを認可 VLAN に割り当てます。認可 VLAN が設定されていない場合、クライアントは初期 VLAN に割り当てられます。
- クライアントが再認証に失敗した場合、クライアントは Auth-Fail VLAN にとどまります。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. サービステンプレート view に移行する	**wlan service-template** *service-template-name*	—
3. WLAN Auth-Fail VLAN を設定する	**client-security authentication fail-vlan** *vlan-id*	デフォルト：設定なし

1.8.12 サーバからの認可情報の無視

クライアントが 802.1X または MAC 認証に合格した後に、サーバ (ローカルまたはリモート) から受信した許可情報を無視するようにデバイスを設定できます。許可情報には、VLAN、ACL、およびユーザプロファイル情報が含まれます。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. サービステンプレート view に移行する	**wlan service-template** *service-template-name*	—
3. 認証サーバから受け取った認可情報を無視する	**client-security ignore-authorization**	デフォルト : 認証サーバから受け取った認可情報が使用

1.8.13 認可フェールオフライン機能の有効化

許可-フェール-オフライン機能は、ACL また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す。

クライアントは、次の状況で ACL またはユーザプロファイルの許可に失敗します。

- デバイスまたはサーバは、指定された ACL またはユーザプロファイルをクライアントに割り当てることができません。
- 割り当てられた ACL またはユーザプロファイルが存在しません。

I. 制限事項とガイドライン

この機能は、VLAN 認証に失敗したクライアントには適用されません。デバイスは常にこれらのクライアントをログオフします。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. サービステンプレート view に移行する	**wlan service-template** *service-template-name*	—

操作	コマンド	補足
3. 認証フェールオフライン機能を有効する	**client-security authorization-fail offline**	デフォルト：無効

1.8.14 アカウンティング開始トリガー機能の設定

accounting-start trigger は、クライアントが 802.1X または MAC 認証に合格した後にデバイスが start-accounting 要求を送信するための条件を指定します。

accounting-start trigger は、IP ベースまたは非 IP ベースにすることができます。

- IP ベースの accounting-start trigger:デバイスは、802.1X または MAC 認証クライアントの IP アドレスを学習し、その IP アドレスが指定されたタイプであることを確認すると、start-accounting 要求を送信します。
- 非 IP ベースのアカウンティング開始トリガー:デバイスは、クライアントの IP アドレスを調べずに、クライアントが認証に合格した直後にアカウンティング開始要求を送信します。

IP ベースのアカウンティング開始トリガーと組み合わせて、アカウンティング遅延タイマを設定できます。アカウンティング遅延タイマは、指定されたアクションを実行する前に、デバイスが 802.1X または MAC 認証クライアントの IP アドレスを学習する最大間隔を指定します。

遅延タイマは、クライアントが 802.1X または MAC 認証に合格すると開始されます。アカウンティング遅延タイマが期限切れになる前に、デバイスが IP ベースのアカウンティング開始トリガーと一致する IP アドレスの学習に失敗した場合、デバイスは次のいずれかのアクションを実行します。

- no-ip-logoff アクションが指定されていない場合は、すぐに start-accounting 要求を送信します。
- no-ip-logoff アクションが指定されている場合は、クライアントをログオフします。

遅延タイマが設定されていない場合、デバイスはクライアントの IP アドレスを学習したときにのみ、クライアントの開始アカウンティング要求を送信します。アカウンティングの詳細については、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*13 ユーザアクセスと認証*“の”*3 章 AAA*“を参照してください。

I. 制約事項とガイドライン

トリガーが IP アドレスタイプベースの場合は、そのタイプの IP アドレスの学習を有効にする必要があります。無線クライアントの IP アドレス学習については、 QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*13 ユーザアクセスと認証*“の”*2 章 WLAN IP スヌーピング*“を参照してください。

トリガーは、トリガーが設定された後にオンラインになったクライアントに対してのみ有効です。

デバイスがクライアントの IP アドレスを学習するための一般的な時間に応じて、アカウンティング遅延タイマを設定します。ベストプラクティスとして、パフォーマンスの低いネットワークで遅延タイマを増やします。

操作	コマンド	補足
1. system view に移行する	**system-view**	—

操作	コマンド	補足
2． サービステンプレート view に移行する	**wlan service-template** *service-template-name*	—
3． クライアントの accounting-start トリガーを設定する	**client-security accounting-start trigger** { **IPv4** | **none** }	デフォルト：無効
4． (オプション設定項目) アカウンティング遅延タイマを設定する	**client-security accounting-delay time** *time* [**no-ip-logoff**]	デフォルト: クライアントのIPアドレスを学習した場合にのみ、クライアントのstart-accounting要求を送信する

1.8.15 accounting-update トリガー機能の設定

この機能を使用して、イベントベースのアカウンティング更新トリガーを指定します。この機能を使用すると、オンライン 802.1X または MAC 認証クライアントの IP アドレスが変更されたときに、デバイスから更新アカウンティング要求を送信できます。

I. 制限事項とガイドライン

accounting-start トリガーと組み合わせて accounting-update トリガーを使用します。accounting-update トリガーは、client-security accounting-start trigger コマンドを使用して accounting-start トリガーを設定した場合にのみ有効になります。

イベントベースの accounting-update トリガーに加えて、timer realtime-accounting コマンドを使用して、定期的な accounting-update 間隔を設定できます。

accounting-update トリガーは、トリガーが設定された後にオンラインになったクライアントに対してのみ有効です。

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． サービステンプレート view に移行する	**wlan service-template** *service-template-name*	—
3． accounting-update トリガーを設定する	**client-security accounting-update trigger IPv4**	デフォルト：設定なし

1.8.16 accounting-restart トリガー機能の設定

IPv4 アドレスベースのアカウンティング再起動トリガーは、802.1X および MAC 認証クライアントに適用されます。

このトリガーは、クライアントの IPv4 アドレスが変更されたときに、stop-accounting 要求を送信してから start-accounting 要求をアカウンティングサーバに送信することで、クライアントのアカウンティングを再起動します。

stop-accounting 要求と start-accounting 要求の間の遅延は設定可能です。

I. 制限事項とガイドライン

IPv4 アドレスベースの accounting-restart トリガーは、client-security accounting-update trigger コマンドを使用して IPv4 用に設定された accounting-update トリガーよりも優先順位が高くなります。

II. 前提条件

サービステンプレートでこの機能を設定する前に、そのサービステンプレートを無効にする必要があります。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. サービステンプレート view に移行する	**wlan service-template** *service-template-name*	—
3. IPv4 アドレスベースの accounting-restart トリガーを有効にする	**client-security accounting-restart trigger ipv4** [**delay** *interval*]	デフォルト：無効

1.8.17 IP プロトコルバージョンによる 802.1X デュアルスタッククライアントのトラフィックアカウンティングの有効化

802.1X デュアルスタッククライアントの IPv4 トラフィックを個別に測定するには、この機能を使用します。この機能を使用すると、802.1X デュアルスタッククライアントについて AAA アカウンティングサーバに送信されるトラフィックデータは、IP プロトコルバージョンによって分離されます。

I. 制約事項とガイドライン

この機能は、無線ターミネータソリューションには適用されません。

II. 前提条件

サービステンプレートでこの機能を設定する前に、そのサービステンプレートを無効にする必要があります。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. サービステンプレート view に移行する	**wlan service-template** *service-template-name*	—
3. IP プロトコルバージョン別に 802.1X デュアルスタッククライアントのトラフィックアカウンティングを有効にする	**client-security accounting dual-stack separate enable**	デフォルト：無効

1.9 失敗許可機能の設定

1.9.1 失敗許可について

🕮 **メモ：**

- 失敗許可機能は、AP が AC と通信不能になってから数分後に動作します。 動作を開始するまでは新規クライアントは接続できません。
- 1 つの無線に対して設定できるバックアップ用のサービステンプレート(SSID)は 1 つのみです。
- リモート AP が設定されている場合、AP が AC と通信不能になってもこの機能は使用できません。

失敗許可機能(**fail-permit enable**)をサービステンプレートで有効にすることで、AP が AC もしくは RADIUS サーバと通信不能になった場合にも、新規クライアントが SSID に接続できます。また、AP は AC と通信不能になった場合でも、10 分ごとに再起動しません。

失敗許可機能は、RADIUS サーバもしくは AC と AP 間の通信が切断された後も、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。

認証失敗許可イベントがクライアントに与える影響は、クライアントの認証方法と、バックアップ用のサービステンプレート(**fail-permit template**)があるかによって異なります。

- PSK 認証クライアント:
  - バックアップ用のサービステンプレートがない場合、接続済みのクライアントは AC と AP が切断後も接続を維持します。
  - バックアップ用のサービステンプレートがある場合、接続済みのクライアントは切断されます。バックアップ用のサービステンプレートには手動で再接続する必要があります。
- MAC 認証クライアント:
  - バックアップ用のサービステンプレートがない場合、AP が AC と通信不能になった後、クライアントは一時的に切断されますが、再接続で引き続きネットワークにアクセスできます。同一サービステンプレートに PSK 認証も設定しておくことで、AC もしくは RADIUS サーバと AP の切断前は、クライアントは MAC 認証及び PSK 認証で認証され、切断後は PSK 認証で認証されます。
  - バックアップ用のサービステンプレートがある場合、接続済みのクライアントは切断されます。バックアップ用のサービステンプレートには手動で再接続する必要があります。
- 802.1 X 認証クライアント
  - 2 つのサービステンプレートを設定する必要があります。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、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 AC もしくは 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 AC と通信不能になった後、もしくは RADIUS サーバと通信不能になった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。AC もしくは 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、切断後はバックアップ用の PSK 認証で認証されます。

1.9.2 失敗許可機能の設定

認証クライアントのサービステンプレートで失敗許可機能を有効にするには、次のタスクを実行します。

I. 制約事項とガイドライン

この機能は、サービステンプレートが無効になっている場合に設定でき、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。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. サービステンプレート view に移行する	**wlan service-template** *service-template-name*	—
3. fail-permit を有効にする	**fail-permit enable** [**keep-online**]	デフォルト：無効

1.9.3 RADIUS サーバ検出の設定

失敗許可機能を利用するサービステンプレートが RADIUS サーバによる認証を行っている場合、失敗許可を有効にするには、次の手順を実行します。

I. 前提条件

1. **radius-server test-profile** コマンドを実行して、RADIUS サーバの到達可能性をテストするための RADIUS テストプロファイルを設定します。

   プロファイルで、必要に応じて検出パケットの送信間隔を設定します。間隔が短いほど、変更に対する応答が早くなります。
2. 認証 ISP ドメインの RADIUS スキームの RADIUS サーバにプロファイルを適用します。

   RADIUS サーバとの通信が到達不能と判断されたときに失敗許可機能が動作します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. RADIUS サーバ検出を設定する	**radius-server test-profile** *profile-number* **username** *name* [**interval** *interval*]	デフォルト：設定なし

1.9.4 レーダーによる通信停止回避用サービステンプレート設定

レーダー検出時に有効になるサービステンプレート（バックアップ用サービステンプレート）を別の無線に設定することにより、レーダー検出時の通信停止時間を回避します。レーダー検出時、サービステンプレートの切り替えを自動的に行い、SSID を送信するチャネルを切り替えます。SSID に接続中のクライアントを別のチャネルに移動できます。

レーダー検出した無線が別チャネルで通信を開始すると、バックアップ用のサービステンプレートは無効となり、元の無線のサービステンプレートが有効になります。

I. 制限事項とガイドライン

同じサービステンプレート内で fail-permit enable コマンドと fail-permit template コマンドは排他設定です。

この機能は、サービステンプレートが無効になっている場合に設定でき、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。

- バックアップ用サービステンプレートには、fail-permit 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。

バックアップ用テンプレートを正常に動作させるために以下の設定を推奨します。

- バックアップ用テンプレートを設定する場合、失敗許可機能を有効にするサービステンプレートでは、AKM モードを PSK に設定するか、AKM モードを指定しないでください。
- client forwarding-location を AP にし、AP がクライアントデータトラフィックを転送できるようにしてください。

１つの AP には１つのバックアップ用テンプレートのみを設定してください。複数のバックアップ用サービステンプレートを設定した場合、AP の無線に最初にバインドされたものだけが有効になります。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. サービステンプレート view に移行する	**wlan service-template** *service-template-name*	—
3. サービステンプレートをバックアップ用テンプレートとして指定する	**fail-permit template**	デフォルト：設定なし

1.10 WLANアクセス認証の設定例

1.10.1 802.1 X EAP-PEAP RADIUS 認証の設定

I. ネットワーク要件

図 1-3に示すように、EAP-PEAP を使用してクライアントの 802.1 X RADIUS 認証を実行するように AC を設定します。

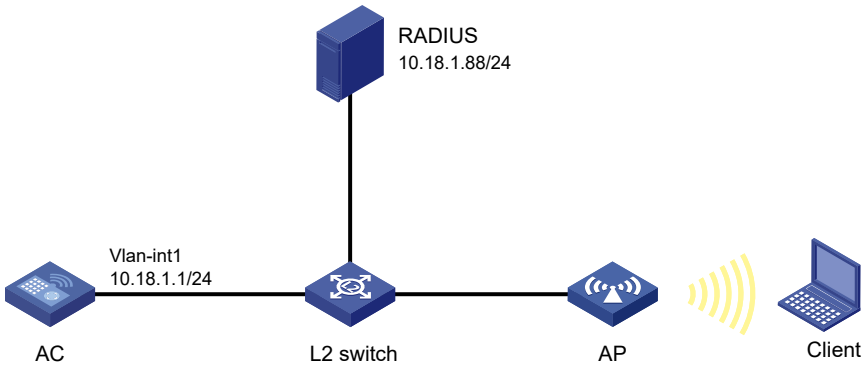


図 1-3 ネットワーク図

II. 設定手順

この例では、RADIUS を含む基本的な AAA 設定のみを提供します。AAA コマンドの詳細については、QX-W2300AC シリーズアクセスコントローラコマンドマニュアルの“*13 ユーザアクセスと認証*“の”*3 章 AAA*“を参照してください。

III. AC の設定

1)　802.1 X と RADIUS スキームを設定します。

#EAP リレーを使用して 802.1 X クライアントを認証するように AC を設定します。

```
<AC> system-view
[AC] dot1x authentication-method eap
```

#RADIUS スキームを作成する。

```
[AC] radius schem RADIUS
```

#プライマリ authentication サーバとプライマリ accounting サーバを指定する。

```
[AC-radius-RADIUS] primary authentication 10.18.1.88 1812
[AC-radius RADIUS] primary accounting 10.18.1.88 1813
```

#サーバとのセキュア通信のための共有キーをプレーンテキストで 12345678 に設定する。

```
[AC-radius- RADIUS] key authentication simple 12345678
[AC-radius- RADIUS] key accounting simple 12345678
```

#RADIUS サーバに送信されるユーザ名からドメイン名を除外する。

```
[AC-radius RADIUS] user-name-format without-domain
[AC-radius- RADIUS] quit
```

2)　ISP ドメインの AAA 方式を設定します。

#DOMAIN という名前の ISP ドメインを作成します。

```
[AC] domain DOMAIN
```

#LAN クライアントの認証、許可、およびアカウンティングに RADIUS スキーム imcc を使用するように ISP ドメインを設定します。

```
[AC-isp-DOMAIN] authentication lan-access radius-scheme RADIUS
[AC-isp-DOMAIN] authorization lan-access radius-scheme RADIUS
[AC-isp-DOMAIN] accounting lan-access radius-scheme RADIUS
[AC-isp-DOMAIN] quit
```

3) サービステンプレートの設定:

#wlas_eap_peap という名前のサービステンプレートを作成する。

```
[AC] wlan service-template wlas_eap_peap
```

#認証モードを 802.1 X に設定する。

```
[AC-wlan-st-wlan_eap_peap]
```

#サービステンプレートの ISP ドメイン imc を指定する。

```
[AC-wlan-st-wlan_eap_peap] dot1x domain DOMAIN
```

#SSID を wlas_eap_peap に設定する。

```
[AC-wlan-st-wlan_eap_peap] ssid wlan_eap_peap
```

#AKM モードを 802.1 X に設定する。

```
[AC-wlan-st-wlan_eap_peap] akm mode dot1x
```

#CCMP 暗号スイートを設定する。

```
[AC-wlan-st-wlan_eap_peap] cipher-suite ccmp
```

#ビーコンおよびプローブ応答で RSN-IE を有効にする。

```
[AC-wlan-st-wlan_eap_peap] security-ie rsn
```

#サービステンプレートを有効にする。

```
[AC-wlan-st-wlan_eap_peap] service-template enable
[AC-wlan-st-wlan_eap_peap] quit
```

4) 手動 AP ap 1 を設定し、サービステンプレートを AP 無線にバインドします。

#ap 1 を作成し、AP モデルとシリアル ID を指定します。

```
[AC] ap ap1 model WA1020
[AC-wlan-ap1] serial-id 219801A28N819CE0002T
```

#チャネル 149 を AP の radio1 の動作チャネルとして設定し、有効にします。

```
[AC-wlan-ap-ap1] radio 1
[AC-wlan-ap-ap1-radio-1] channel 149
[AC-wlan-ap-ap1-radio-1] radio enable
```

#サービステンプレート wlas_eap_peap を radio 1 にバインドする。

```
[AC-wlan-ap-ap1-radio-1] service-template wlas_imc_peap
[AC-wlan-ap-ap1-radio-1] quit
[AC-wlan-ap-ap1] quit
```

IV. RADIUS サーバの設定:

RADIUS サーバの設定を行います。(詳細は省略します)

V. 設定の確認

1. クライアントで、ユーザ名 user とパスワード dot1x を使用してネットワークにアクセスできることを確認します。(詳細は省略します)
2. AC で、下記のコマンドを実行し、ユーザが認証オンラインになったことを確認します。

#オンライン 802.1 X クライアント情報を表示します。

```
[AC] display dot1x connection
           User MAC address           : 0023-8933-2090
           AP name                    : ap1
           Radio ID                   : 1
           SSID                       : wlas_eap_peap
           BSSID                      : 000f-e201-0003
           User name                  : user
           Authentication domain      : DOMAIN
           Authentication method      : EAP
           Initial VLAN               : 1
           Authorization VLAN         : N/A
           Authorization ACL number   : N/A
           Authorization user profile : N/A
           Authorization CAR          : N/A
           Termination action         : Default
           Session timeout period     : 6001 s
           Online from                : 2014/04/18 09:25:18
Online duration            : 0h 1m 1s

Total number of connected APs: 1
Total number of connected manual APs: 1
Total number of connected auto APs: 0
Total number of connected common APs: 1
Total number of connected WTUs: 0
Total number of inside APs: 0
Maximum supported APs: 6144
Remaining APs: 6144
Total AP licenses: 128
local AP licenses: 0
Server AP licenses: 0
Remaining local AP licenses: 127
```

```
Sync AP licenses: 0


Total connections: 1.
```

#WLAN クライアント情報を表示する。

```
[AC] display wlan client
Total number of clients           : 1

MAC address    Username             AP name              R IP address      VLAN
           0023-8933-2090 user              ap1                 1 10.18.1.100
           1


Total connections: 1.
```

1.10.2 RADIUS サーバとして機能する AC でのローカル 802.1 X EAP-PEAP 認証の設定

I. ネットワーク要件

図 1-4に示すように、

- AC と AP は L2 switch を介して接続されます。
- AC は EAP-PEAP 方式を使用して、無線クライアントの 802.1 X 認証を実行します。

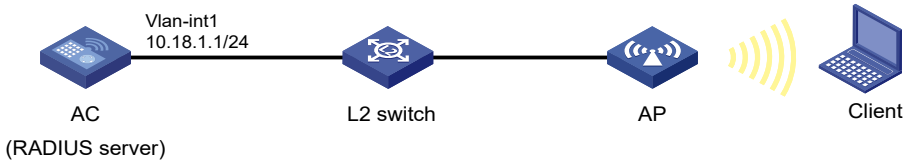


図 1-4 ネットワーク図

II. 前提条件

CA 証明書ファイルとローカル証明書ファイルが AC に保存されている。

クライアントには、ネットワークアクセス認証に必要な証明書がインストールされている。

III. AC の設定

この例では、RADIUS コマンドなど、一部の AAA コマンドを使用しています。これらの AAA コマンドの詳細については、QX-W2300AC シリーズアクセスコントローラコマンドマニュアルの“*13 ユーザアクセスと認証*“の”*3 章 AAA*“を参照してください。

1) 802.1 X 認証方式を指定し、RADIUS スキームを設定します。

#802.1 X 認証方式を EAP に設定します。

```
<AC> system-view
[AC] dot1x authentication-method eap
```

#freeradius という名前の RADIUS スキームを作成し、そのビューを入力します。

```
[AC] radius scheme freeradius
```

#10.18.1.1 のサーバをプライマリ認証サーバに指定し、認証ポート番号を 1812、共有キーをプレーンテキスト文字列 12345678 に設定する。

```
[AC-radius-freeradius] primary authentication 10.18.1.1 1812
[AC-radius-freeradius] key authentication simple 12345678
```

#RADIUS サーバに送信されるユーザ名にドメイン名を含めないようにデバイスを設定する。

```
[AC-radius-freeradius] user-name-format without-domain
[AC-radius-freeradius] quit
```

2) freeradius という名前の ISP ドメインを作成し、LAN ユーザーの認証と承認に RADIUS スキーム freeradius を使用するように ISP ドメインを設定します。AC が RADIUS サーバとして動作する場合、アカウンティングはサポートされません。

```
[AC] domain freeradius
[AC-isp-freeradius] authentication lan-access radius-scheme freeradius
[AC-isp-freeradius] authorization lan-access radius-scheme freeradius
[AC-isp-freeradius] accounting lan-access none
[AC-isp-freeradius] quit
```

3) サービステンプレートの設定:

#wlas_freeradius_peap という名前のサービステンプレートを作成します。

```
[AC] wlan service-template wlas_freeradius_peap
```

#認証モードを 802.1 X に設定し、802.1 X 認証に ISP ドメイン freeradius を指定する。

```
[AC-wlan-st-wlas_freeradius_peap] client-security authentication-mode dot1x
[AC-wlan-st-wlas_freeradius_peap] dot1x domain freeradius
```

#SSID を wlas_freeradius_peap に設定し、AKM モードを 802.1 X に設定し、暗号スイートを CCMP に設定し、ビーコン応答とプローブ応答で RSN IE を有効にします。

```
[AC-wlan-st-wlas_freeradius_peap] ssid wlas_freeradius_peap
[AC-wlan-st-wlas_freeradius_peap] akm mode dot1x
[AC-wlan-st-wlas_freeradius_peap] cipher-suite ccmp
[AC-wlan-st-wlas_freeradius_peap] security-ie rsn
```

#サービステンプレートを有効にする。

```
[AC-wlan-st-wlas_freeradius_peap] service-template enable
[AC-wlan-st-wlas_freeradius_peap] quit
```

4) 手動 AP を設定し、サービステンプレートを AP の無線にバインドします。

#ap 1 という名前の AP を作成し、AP モデルとシリアル番号を指定します。

```
[AC] wlan ap ap1 model WA1020
[AC-wlan-ap-ap1] serial-id 219801A28N819CE0002T
```

#無線 1 にチャネル 149 を指定し、無線を有効にする。

```
[AC-wlan-ap-ap1] radio 1
```

```
[AC-wlan-ap-ap1-radio-1] channel 149
[AC-wlan-ap-ap1-radio-1] radio enable
```

#サービステンプレート wlas_freeradius_peap を radio 1 にバインドする。

```
[AC-wlan-ap-ap1-radio-1] service-template wlas_freeradius_peap
[AC-wlan-ap-ap1-radio-1] quit
[AC-wlan-ap-ap1] quit
```

5) ローカル RADIUS サーバをインストールします。

#freeradius.bin ファイルが AC にインストールされているかどうかを確認します。

```
[AC] display install active
```

#AC にファイルがインストールされていない場合は、ファイル freeradius.bin をインストールします。AC にファイルがインストールされている場合は、再インストールする必要はありません。

```
[[AC] quit
<AC> install activate feature flash:/freeradius.bin
Verifying the file flash:/freeradius.bin on the device...Done.
Identifying the upgrade methods...Done.
Upgrade summary according to following table:

flash:/freeradius.bin
            Running Version             New Version
            None                        Release 5433

Upgrade Way: Service Upgrade
Upgrading software images to compatible versions. Continue? [Y/N]: y
This operation might take several minutes, please wait....Done.
<AC> install commit
This operation will take several minutes, please wait.....................Done.
```

#ファイルが AC に正常にインストールされたことを確認します。

```
[AC] display install active
```

6) 802.1 X 認証用のローカルユーザを設定します。

#dot 1 x という名前のローカルユーザを作成し、パスワードをプレーンテキストの 123456 に設定します。

```
[AC] local-user dot1x class network
[AC-luser-network-dot1x] password simple 123456
```

#ローカルユーザに LAN アクセスサービスの利用を許可する。

```
[AC-luser-network-dot1x] service-type lan-access
```

#ローカルユーザにユーザロール network-operator を割り当てる。

```
[AC-luser-network-dot1x] authorization-attribute user-role network-operator
[AC-luser-network-dot1x] quit
```

7) ローカル RADIUS サーバで EAP 認証を設定します。

#dot1x という名前の EAP プロファイルを作成し、そのビューを入力します。

```
[AC] eap-profile dot1x
```

#EAP 認証方式を PEAP-MSCHAPv 2 に設定する。

```
[AC-eap-profile-dot1x] method peap-mschapv2
```

#EAP 認証用の CA 証明書ファイルを指定する。

```
[AC-eap-profile-dot1x] ca-file ca.pem
```

#EAP 認証用のローカル証明書ファイルを指定する。

```
[AC-eap-profile-dot1x] certificate-file server.pem
```

#ローカル証明書の秘密鍵ファイルを指定する。

```
[AC-eap-profile-dot1x] private-key-file server.pem
```

#ローカル証明書の秘密鍵パスワードを指定する。

```
[AC-eap-profile-dot1x] private-key-password simple whatever
[AC-eap-profile-dot1x] quit
```

#EAP プロファイル dot 1 x を AC 上の RADIUS サーバに適用する。

```
[AC] radius-server eap-profile dot1x
```

#RADIUS クライアント (NAS) を 10.18.1.1 で指定し、共有キーをプレーンテキストの 12345678 に設定する。

```
[AC] radius-server client ip 10.18.1.1 key simple 12345678
```

#RADIUS サーバの設定を有効にする。802.1 X ローカルユーザの設定が変更された場合、変更を有効にするには、RADIUS サーバの設定を再度有効にする必要があります。

```
[AC] radius-server activate
```

🕮 **メモ：**

- ローカル RADIUS サーバでの EAP 認証設定の詳細については、 QX-W2300AC シリーズアクセスコントローラコマンドマニュアルの“*13 ユーザアクセスと認証*“の”*3 章 AAA* “を参照してください

IV. クライアントの設定

「802.1 X EAP-PEAP RADIUS認証の設定」 と同様にクライアントを設定します。(詳細は省略します)

V. 設定の確認

#AC で、アクティブな RADIUS クライアントを表示して、RADIUS クライアントの設定を確認します。

```
[AC] display radius-server active-client
Total 1 RADIUS clients.
Client IP: 10.18.1.1
```

#クライアントで、802.1 X 接続を介してサービステンプレート wlas_freeradius_peap に接続します。ユーザ名 dot 1 x とパスワード 123456 を入力します。

フェーズ 2 の ID 認証に MSCHAPV 2 を使用する場合、Android エンドポイントでは CA 証明書の検証はオプションです。CA 証明書の検証を選択した場合は、一致する CA 証明書をエンドポイントにインストールする必要があります。(詳細は表示されない。)

#AC で、オンライン 802.1 X ユーザ情報を表示して、表示されたユーザ名がクライアントで入力したユーザ名と同じであることを確認します。

```
[AC] display dot1x connection
Total connections: 1
User MAC address             : e0cc-f881-3f42
AP name                       : ap1
Radio ID                      : 1
SSID                          : wlas_freeradius_peap
BSSID                         : 000f-e201-0003
User name                     : dot1x
Authentication domain       : freeradius
IPv4 address                  : 10.18.1.10
Authentication method       : EAP
Initial VLAN                  : 1
Authorization VLAN          : 1
Authorization ACL number    : N/A
Authorization user profile : N/A
Authorization CAR           : N/A
Termination action          : Default
Session timeout last from   : 2021/03/01 15:41:33
Session timeout period      : 86400 s
Online from                   : 2021/03/01 15:41:33
Online duration               : 0h 0m 5s
```

#AC で、802.1 X ユーザがオンラインになったことを確認するために、オンライン WLAN クライアント情報を表示します。

```
[AC] display wlan client
Total number of clients: 1

MAC address    Username             AP name              R IP address      VLAN
e0cc-f881-3f42 dot1x                ap1                    1 10.18.1.10       1
```

1.10.3 RADIUS ベースの MAC 認証の設定

I. ネットワーク要件

図 1-5に示すように、RADIUS サーバを使用してクライアントの MAC 認証を実行するように AC を設定します。

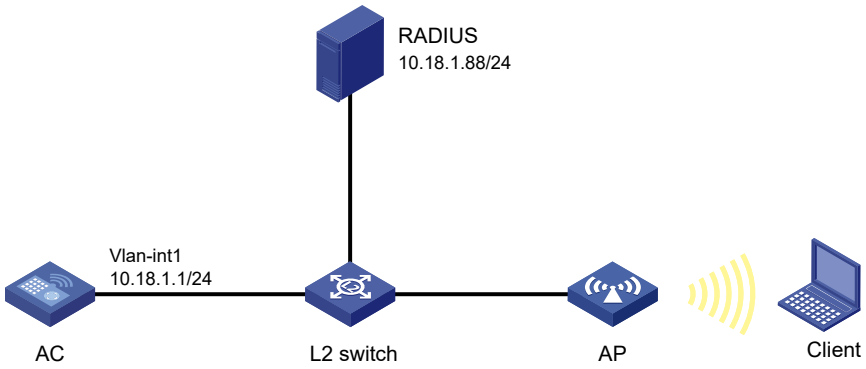


図 1-5 ネットワーク図

II. 設定手順

#RADIUS サーバ、AC、AP、およびクライアントが相互に到達できることを確認します。(詳細は省略します)

III. AC の設定

1)　RADIUS スキームを設定します。

#RADIUS スキームを作成します。

```
<AC> system-view
[AC] radius scheme RADIUS
```

#プライマリ認証サーバとプライマリ会計サーバを指定する。

```
[AC-radius-RADIUS] primary authentication 10.18.1.88 1812
[AC-radius-RADIUS] primary accounting 10.18.1.88 1813
```

#サーバとのセキュア通信のための共有キーをプレーンテキストで 12345678 に設定する。

```
[AC-radius-RADIUS key authentication simple 12345678
[AC-radius-RADIUS] key accounting simple 12345678
```

#RADIUS サーバに送信されるユーザ名からドメイン名を除外する。

```
[AC-radius-RADIUS] user-name-format without-domain
[AC-radius-RADIUS] quit
```

2)　ISP ドメインの AAA 方式を設定します。

#imc という名前の ISP ドメインを作成する。

```
[AC] domain DOMAIN
```

#LAN クライアントの認証、許可、およびアカウンティングに RADIUS スキーム imcc を使用するように ISP ドメインを設定します。

```
[AC-isp-DOMAIN] authentication lan-access radius-scheme RADIUS
[AC-isp-DOMAIN] authorization lan-access radius-scheme RADIUS
[AC-isp-DOMAIN] accounting lan-access radius-scheme RADIUS
```

```
[AC-isp-DOMAIN] quit
```

3) MAC 認証クライアントと共有するアカウントのユーザ名 123 とパスワード aaa_maca をプレーンテキストで指定します。

重要：

MAC ベースのアカウントを使用する場合は、RADIUS サーバ上の各アカウントのユーザ名とパスワードが、各 MAC 認証ユーザの MAC アドレスと同じであることを確認してください。
共有アカウントを使用する場合は、MAC 認証クライアントのユーザ名とパスワードが、デバイスと RADIUS サーバで同じになるように設定してください。

```
[AC] mac-authentication user-name-format fixed account 123 password simple aaa_maca
```

4) サービステンプレートを設定します。

#maca_radius という名前のサービステンプレートを作成する。

```
[AC] wlan service-template maca_radius
```

#SSID を maca_imc に設定する。

```
[AC-wlan-st-maca_imc] ssid maca_radius
```

#認証モードを MAC 認証にする。

```
[AC-wlan-st-maca_radius] client-security authentication-mode mac
```

#サービステンプレートの ISP ドメイン imc を指定する。

```
[AC-wlan-st-maca_radius] mac-authentication domain DOMAIN
```

#サービステンプレートを有効にする。

```
[AC-wlan-st-maca_radius] service-template enable
[AC-wlan-st-maca_radius] quit
```

5) 手動 AP ap 1 を設定し、サービステンプレートを AP 無線にバインドします。

#ap 1 という名前の手動 AP を作成し、AP モデルとシリアル ID を指定します。

```
[AC] wlan ap ap1 model WA1020
[AC-wlan-ap-ap1] serial-id 219801A28N819CE0002T
```

#チャネル 149 を AP の無線 1 の動作チャネルとして設定し、無線 1 を有効にします。

```
[AC-wlan-ap-ap1] radio 1
[AC-wlan-ap-ap1-radio-1] channel 149
[AC-wlan-ap-ap1-radio-1] radio enable
```

#サービステンプレート maca_imc を radio 1 にバインドする。

```
[AC-wlan-ap-ap1-radio-1] service-template maca_radius
[AC-wlan-ap-ap1-radio-1] quit
[AC-wlan-ap-ap1] quit
```

IV. RADIUS サーバを設定します。

RADIUS サーバの設定を行います。(詳細は省略します)

V. 設定の確認

1) クライアントで、ユーザ名 123 とパスワード aaa_maca を使用してネットワークにアクセスできることを確認します。
2) AC で、次のタスクを実行して、ユーザが認証に合格してオンラインになったことを確認します。

#オンライン MAC 認証クライアント情報を表示します。

```
[AC] display mac-authentication connection
User MAC address                : 0023-8933-2098
AP name                         : ap1
Radio ID                        : 1
SSID                            : maca_imc
BSSID                           : 000f-e201-0001
User name                       : 123
Authentication domain           : imc
Initial VLAN                    : 1
Authorization VLAN              : N/A
Authorization ACL number        : N/A
Authorization user profile      : N/A
Authorization CAR               :N/A
Authorization URL               :
Termination action              : Default
Session timeout period          : 6001 s
Online from                     : 2014/04/17 17:21:12
Online duration                 : 0h 0m 30s

Total connections: 1.
```

#WLAN クライアント情報を表示する。

```
[AC] display wlan client
Total number of clients           : 1

MAC address    Username            AP name              R IP address      VLAN
0023-8933-2098 123                   ap1                   1 10.18.1.100     1
```

1.10.4 802.1X CHAP ローカル認証の設定例

I. ネットワーク要件

図 1-6に示すようにクライアントの 802.1X ローカル認証を行うために AC で CHAP を使用します。



図 1-6 ネットワーク図

II. 設定手順

1)　802.1X、ローカルクライアントを設定します。

EAP 終端を実行し、CHAP を使用するように AC を設定します。

```
<AC> system-view
[AC] dot1x authentication-method chap
```

ユーザ名 chap1、プレーンテキストでパスワード 123456 のローカルネットワークアクセスユーザを追加します。

```
[AC] local-user chap1 class network
[AC-luser-network-chap1] password simple 123456
```

サービスタイプを lan-access に設定します。

```
[AC-luser-network-chap1] service-type lan-access
[AC-luser-network-chap1] quit
```

2)　ISP ドメインの AAA 方式を設定します。

ISP ドメイン local を作成します。

```
[AC] domain local
```

LAN クライアントでローカル認証、ローカル許可、ローカルアカウンティングを使用する ISP ドメインを設定します。

```
[AC-isp-local] authentication lan-access local
[AC-isp-local] authorization lan-access local
[AC-isp-local] accounting lan-access local
[AC-isp-local] quit
```

3)　サービステンプレートを設定します。

サービステンプレート wlas_local_chap を作成します。

```
[AC] wlan service-template wlas_local_chap
```

認証モードを 802.1X に設定します。

```
[AC-wlan-st-wlas_local_chap] client-security authentication-mode dot1x
```

サービステンプレートの ISP ドメインを local に設定します。

```
[AC-wlan-st-wlas_local_chap] dot1x domain local
```

wlas_local_chap に SSID を設定します。

```
[AC-wlan-st-wlas_local_chap] ssid wlas_local_chap
```

サービステンプレートを有効にします。

```
[AC-wlan-st-wlas_local_chap] service-template enable
[AC-wlan-st-wlas_local_chap] quit
```

4) AP 名が ap1 のマニュアル AP を設定し、サービステンプレートを AP に関連づけます。

AP ap1 を作成し、AP モデル、シリアル ID を設定します。

```
[AC] wlan ap ap1 model QX-W1020
[AC-wlan-ap-ap1] serial-id 210235A1BSC123000050
[AC-wlan-ap-ap1] quit
```

AP の radio 1 の動作チャネルとしてチャネル 64 を設定し、radio 1 を有効にします。

```
[AC] wlan ap ap1
[AC-wlan-ap-ap1] radio 1
[AC-wlan-ap-ap1-radio-1] channel 64
[AC-wlan-ap-ap1-radio-1] radio enable
```

サービステンプレート wlas_local_chap を radio 1 に関連づけます。

```
[AC-wlan-ap-ap1-radio-1] service-template wlas_local_chap
[AC-wlan-ap-ap1-radio-1] quit
[AC-wlan-ap-ap1] quit
```

III. 設定の確認

802.1X の設定を確認します。

```
[AC] display wlan service-template
[AC] display dot1x
```

802.1X クライアントが認証にパスしたのち、クライアント設定の情報を表示します。

```
[AC] display dot1x connection
```

1.10.5 レーダーによる通信停止回避用サービステンプレートの設定例

I. ネットワーク要件

図 1-62 に示すように レーダーによる通信停止回避用サービステンプレートを使用します。

オリジナルのサービステンプレートを 2 つ、バックアップ用のサービステンプレートを 2 つ使用します。

通常時はそれぞれの無線に分かれて通信を行いますが、レーダー検出時にはレーダー未検出の無線のみで通信を継続します。



図 1-7 ネットワーク図

II. 設定手順

1)　サービステンプレート service1 を作成します。

SSID service1 を指定します。

AKM モードとして PSK を設定し、プレーンテキストで共有鍵 12345678 を指定します。

cipher スイートとして CCMP を設定し、セキュリティ IE として RSN を設定します。

```
[AC-wlan-st-service1] ssid service1
[AC-wlan-st-service1] akm mode psk
[AC-wlan-st-service1] preshared-key pass-phrase simple 12345678
[AC-wlan-st-service1] cipher-suite ccmp
[AC-wlan-st-service1] security-ie rsn
[AC-wlan-st-service1] service-template enable
[AC-wlan-st-service1] quit
```

2)　バックアップ用のサービステンプレート service1_BU を作成します。

fail-permit template 以外は 1)と同じ指定にします。

```
[AC-wlan-st-service1_BU] ssid service1
[AC-wlan-st-service1_BU] fail-permit template
[AC-wlan-st-service1_BU] akm mode psk
[AC-wlan-st-service1_BU] preshared-key pass-phrase simple 12345678
```

```
[AC-wlan-st-service1_BU] cipher-suite ccmp
[AC-wlan-st-service1_BU] security-ie rsn
[AC-wlan-st-service1_BU] service-template enable
[AC-wlan-st-service1_BU] quit
```

3) オリジナルのサービステンプレート service2 を作成します。

SSID service2 を指定します。

AKM モードとして PSK を設定し、プレーンテキストで共有鍵 12345678 を指定します。

cipher スイートとして CCMP を設定し、セキュリティ IE として RSN を設定します。

```
[AC-wlan-st-service2] ssid service2
[AC-wlan-st-service2] akm mode psk
[AC-wlan-st-service2] preshared-key pass-phrase simple 12345678
[AC-wlan-st-service2] cipher-suite ccmp
[AC-wlan-st-service2] security-ie rsn
[AC-wlan-st-service2] service-template enable
[AC-wlan-st-service2] quit
```

4) バックアップ用のサービステンプレート service2_BU を作成します。

fail-permit template 以外は 3)と同じ指定にします。

```
[AC-wlan-st-service2_BU] ssid service2
[AC-wlan-st-service2_BU] fail-permit template
[AC-wlan-st-service2_BU] akm mode psk
[AC-wlan-st-service2_BU] preshared-key pass-phrase simple 12345678
[AC-wlan-st-service2_BU] cipher-suite ccmp
[AC-wlan-st-service2_BU] security-ie rsn
[AC-wlan-st-service2_BU] service-template enable
[AC-wlan-st-service2_BU] quit
```

5) AP 名 ap1 の AP を作成し、モデル名、シリアル番号を指定します。

```
[AC] wlan ap ap1 model QX-W1020
[AC-wlan-ap-ap1] serial-id 219801A0CNC138011454
```

6) オリジナルとバックアップ用のサービステンプレートが別 radio に割り当てます。

```
[AC-wlan-ap-ap1] radio 1
[AC-wlan-ap-ap1-radio-1] service-template service1
[AC-wlan-ap-ap1-radio-1] service-template service2_BU
[AC-wlan-ap-ap1-radio-1] radio enable
[AC-wlan-ap-ap1-radio-1] quit
```

```
[AC-wlan-ap-ap1] radio 2
[AC-wlan-ap-ap1-radio-2] service-template service2
[AC-wlan-ap-ap1-radio-2] service-template service1_BU
[AC-wlan-ap-ap1-radio-2] radio enable
[AC-wlan-ap-ap1-radio-2] quit
```

1.10.6 PSK 認証、認証バイパス時の失敗許可機能設定例

I. ネットワーク要件

図 1-8に示すように Switch は AP とクライアントに IP アドレスを割り当てるため、DHCP サーバとして動作します。

- オープンシステム認証と認証バイパスを設定します。
- ネットワークにアクセスするため、クライアントは共有鍵 12345678 を使用します。

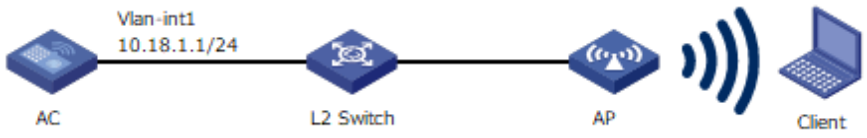


図 1-8 ネットワーク図

II. 設定手順

1) サービステンプレート service1 を作成します。

```
<AC> system-view
[AC] wlan service-template service1
```

#サービステンプレートの SSID サービスを指定します。

```
[AC-wlan-st-service1] ssid service
```

AKM モードとして PSK を設定し、プレーンテキストで共有鍵 12345678 を指定します。

```
[AC-wlan-st-service1] akm mode psk
[AC-wlan-st-service1] preshared-key pass-phrase simple 12345678
```

cipher スイートとして CCMP を設定し、セキュリティ IE として RSN を設定します。

```
[AC-wlan-st-service1] cipher-suite ccmp
[AC-wlan-st-service1] security-ie rsn
```

#失敗許可機能を有効にします。

```
[AC-wlan-st-service1] fail-permit enable
```

#サービステンプレートを有効にします。

```
[AC-wlan-st-service1] service-template enable
[AC-wlan-st-service1] quit
```

2) AP 名 ap1 の AP を作成し、モデル名、シリアル番号を指定します。

```
[AC] wlan ap ap1 model QX-W1020
[AC-wlan-ap-ap1] serial-id 219801A0CNC138011454
```

3) サービステンプレート service1 を AP の radio 1 に割り当て、radio 1 を有効にします。

```
[AC-wlan-ap-ap1] radio 1
[AC-wlan-ap-ap1-radio-1] service-template service1
[AC-wlan-ap-ap1-radio-1] radio enable
[AC-wlan-ap-ap1-radio-1] return
```

III. 設定確認

正しいパスワードでクライアントが SSID に接続できることを確認します。（詳細は省略します。）

AP が AC と切断されてから数分後、失敗許可機能が動作開始し、新規クライアントが SSID に接続できることを確認します。（詳細は省略します。）

1.10.7 プライベート PSK 認証、MAC アドレス認証時の失敗許可機能設定例

I. ネットワーク要件

図 1-9に示すように、Switch は AP とクライアントに IP アドレスを割り当てるため、DHCP サーバとして動作します。

- ログイン名、パスワードとして MAC アドレスを使用して、クライアントがネットワークにアクセスできるように MAC アドレス認証を設定します。
- クライアントが PSK として MAC アドレスを使用できるようにプライベート PSK AKM モードを設定します。

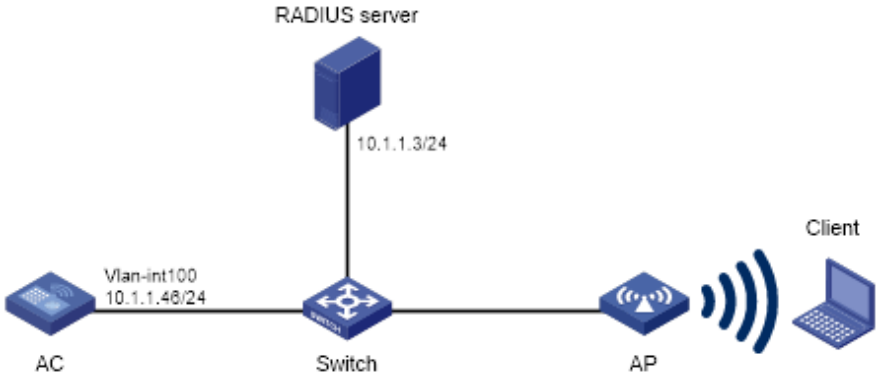


図 1-9 ネットワーク図

II. 設定手順

1) RADIUS サーバでユーザ名 00-23-12-45-67-7a、パスワード 00-23-12-45-67-7a を設定し、RADIUS サーバと AC が互いに通信可能なことを確認します。（詳細は省略します。）
2) WLAN サービステンプレート service1 を作成します。

#サービステンプレートの SSID サービスを指定します。

```
<AC> system-view
[AC] wlan service-template service1
[AC-wlan-st-service1] ssid service
```

#AKM モードとして PSK を設定し、プレーンテキストで鍵 12345678 を指定します。

```
[AC-wlan-st-service1] akm mode psk
[AC-wlan-st-service1] preshared-key pass-phrase simple 12345678
```

cipher スイートとして CCMP を設定し、セキュリティ IE として RSN を設定します。

```
[AC-wlan-st-service1] cipher-suite ccmp
[AC-wlan-st-service1] security-ie rsn
```

MAC アドレス認証を設定します。

```
[AC-wlan-st-service1] client-security authentication-mode mac
```

失敗許可機能を有効にします。

```
[AC-wlan-st-service1] fail-permit enable
```

#サービステンプレートを有効にします。

```
[AC-wlan-st-service1] service-template enable
[AC-wlan-st-service1] quit
```

3) RADIUS サーバ検出を設定します。

```
[AC] radius-server test-profile 1 username nectest interval 1
```

4) RADIUS スキームを設定します。

RADIUS スキーム radius1 を作成し、RADIUS scheme view に移行します。

```
[AC] radius scheme radius1
```

プライマリ認証サーバ、アカウンティングサーバを指定します。

```
[AC-radius-radius1] primary authentication 10.1.1.3 1812 test-profile 1
[AC-radius-radius1] primary accounting 10.1.1.3 1813
```

プレーンテキストで認証サーバ、アカウンティングサーバの共有鍵 12345 を設定します。

```
[AC-radius-radius1] key authentication simple 12345678
[AC-radius-radius1] key accounting simple 12345678
```

RADIUS サーバの設定にもとづいて、RADIUS サーバにユーザ名を送信するように設定します。RADIUS サーバに送信するユーザ名からドメイン名を除外します。

```
[Device-radius-rs1] user-name-format without-domain
[Device-radius-rs1] quit
```

#RADIUS サーバに送信するユーザ名にドメイン名を含めます。

```
[Device-radius-rs1] user-name-format with-domain
[Device-radius-rs1] quit
```

5) ISP ドメイン dom1 を作成し、ISP ドメインの RADIUS スキームを設定します。

```
[AC] domain dom1
[AC-isp-dom1] authentication lan-access radius-scheme radius1
[AC-isp-dom1] authorization lan-access radius-scheme radius1
[AC-isp-dom1] accounting lan-access radius-scheme radius1
[AC-isp-dom1] quit
```

6) ISP ドメイン dom1 のユーザ名、パスワードとして MAC アドレスを設定します。

```
[AC] mac-authentication domain dom1
[AC] mac-authentication user-name-format mac-address with-hyphen lowercase
```

7) AP 名 ap1 の AP を作成し、モデル名、シリアル番号を指定します。

```
[AC] wlan ap ap1 model QX-W1020
[AC-wlan-ap-ap1] serial-id 219801A0CNC138011454
```

8) サービステンプレート service1 を AP の radio 1 に割り当て、radio 1 を有効にします。

```
[AC-wlan-ap-ap1] radio 1
[AC-wlan-ap-ap1-radio-1] service-template service1
[AC-wlan-ap-ap1-radio-1] radio enable
[AC-wlan-ap-ap1-radio-1] return
```

🕮 **メモ：**

AAA、RADIUS コマンドの詳細はコマンドマニュアルのセクション 9 *セキュリティ “AAA”* を参照してください。

III. 設定の確認

MAC アドレスを登録済みのクライアントが SSID に接続できることを確認します。（詳細は省略します。）

AP が AC と切断されてから数分後、もしくは RADIUS サーバと切断されてから数分後、失敗許可機能が動作開始し、新規クライアントが PSK 認証で SSID に接続できることを確認します。（詳細は省略します。）

1.10.8 802.1X 認証時の失敗許可機能設定例

I. ネットワーク要件

図 1-10に示すように、Switch は AP とクライアントに IP アドレスを割り当てるため、DHCP サーバとして動作します。

- ログイン名 abcdef、パスワード 123456 を使用して、クライアントがネットワークにアクセスできるようにオープンシステム認証と 802.1X 認証を設定します。
- AKM モードとして 802.1X を設定します。

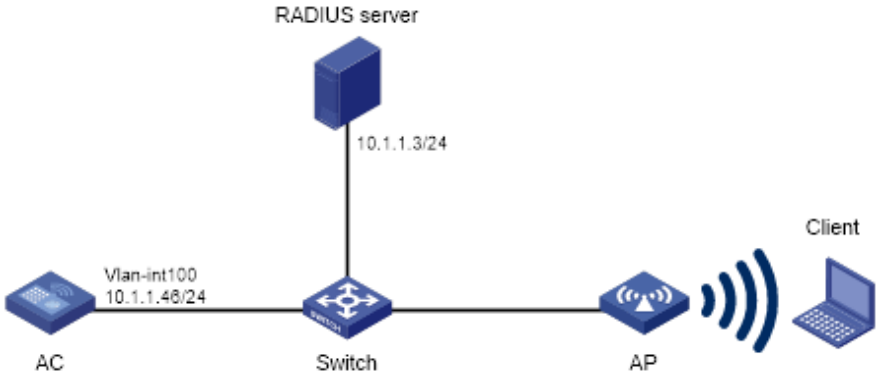


図 1-10 ネットワーク図

II. 設定手順

1) RADIUS サーバでユーザ名 abcdef、パスワード 123456 を設定し、RADIUS サーバと AC が互いに通信可能なことを確認します。（詳細は省略します。）
2) 802.1X クライアントを設定します。（詳細は省略します。）
3) 802.1X 認証用の WLAN サービステンプレート service1 を作成します。

```
<AC> system-view
[AC] wlan service-template service1
```

#サービステンプレートの SSID サービスを指定します。

```
[AC-wlan-st-service1] ssid service_dot1x
```

AKM モードとして 802.1X を設定します。

```
[AC-wlan-st-service1] akm mode dot1x
```

cipher スイートとして CCMP を設定し、セキュリティ IE として RSN を設定します。

```
[AC-wlan-st-service1] cipher-suite ccmp
[AC-wlan-st-service1] security-ie rsn
```

802.1X 認証モードを設定します。

```
[AC-wlan-st-service1] client-security authentication-mode dot1x
```

802.1X 認証ドメインとして dom1 を設定します。

```
[AC-wlan-st-service1] dot1x domain dom1
```

#失敗許可機能を有効にします。

```
[AC-wlan-st-service1] fail-permit enable
```

#サービステンプレートを有効にします。

```
[AC-wlan-st-service1] service-template enable
[AC-wlan-st-service1] quit
```

4) バックアップの PSK 認証用のサービステンプレートを作成します。

```
<AC> system-view
[AC] wlan service-template service1_bu
```

#サービステンプレートの SSID サービスを指定します。

```
[AC-wlan-st-service1_bu] ssid service_psk
```

AKM モードとして PSK を設定し、プレーンテキストで共有鍵 12345678 を指定します。

```
[AC-wlan-st-service1_bu] akm mode psk
[AC-wlan-st-service1_bu] preshared-key pass-phrase simple 12345678
```

cipher スイートとして CCMP を設定し、セキュリティ IE として RSN を設定します。

```
[AC-wlan-st-service1_bu] cipher-suite ccmp
[AC-wlan-st-service1_bu] security-ie rsn
```

バックアップ用に fail-permit template を設定します。

```
[AC-wlan-st-service1_bu] fail-permit template
```

サービステンプレートを有効にします。

```
[AC-wlan-st-service1_bu] service-template enable
[AC-wlan-st-service1_bu] quit
```

5) RADIUS サーバ検出を設定します。

```
[AC] radius-server test-profile 1 username nectest interval 1
```

6) RADIUS スキームを設定します。

RADIUS スキーム radius1 を作成し、RADIUS scheme view に移行します。

```
[AC] radius scheme radius1
```

プライマリ認証サーバ、アカウンティングサーバを指定します。

```
[AC-radius-radius1] primary authentication 10.1.1.3 1812 test-profile 1
[AC-radius-radius1] primary accounting 10.1.1.3 1813
```

プレーンテキストで認証サーバ、アカウンティングサーバの共有鍵 12345 を設定します。

```
[AC-radius-radius1] key authentication simple 12345
[AC-radius-radius1] key accounting simple 12345
```

RADIUS サーバの設定にもとづいて、RADIUS サーバにユーザ名を送信するように設定します。RADIUS サーバに送信するユーザ名からドメイン名を除外します。

```
[Device-radius-rs1] user-name-format without-domain
[Device-radius-rs1] quit
```

RADIUS サーバに送信するユーザ名にドメイン名を含めます。

```
[Device-radius-rs1] user-name-format with-domain
[Device-radius-rs1] quit
```

7) ISP ドメイン dom1 を作成し、ISP ドメインの RADIUS スキームを設定します。

```
[AC] domain dom1
[AC-isp-dom1] authentication lan-access radius-scheme radius1
[AC-isp-dom1] authorization lan-access radius-scheme radius1
[AC-isp-dom1] accounting lan-access radius-scheme radius1
[AC-isp-dom1] quit
```

8) AP 名 ap1 の AP を作成し、モデル名、シリアル番号を指定します。

```
[AC] wlan ap ap1 model QX-W1020
[AC-wlan-ap-ap1] serial-id 219801A0CNC138011454
```

9) サービステンプレート service1 と service1_bu を AP の radio 1 に割り当て、radio 1 を有効にします。

```
[AC-wlan-ap-ap1] radio 1
[AC-wlan-ap-ap1-radio-1] service-template service1
[AC-wlan-ap-ap1-radio-1] service-template service1_bu
[AC-wlan-ap-ap1-radio-1] radio enable
[AC-wlan-ap-ap1-radio-1] return
```

メモ：

AAA、RADIUS コマンドの詳細は、コマンドマニュアルのセクション 9 *セキュリティ "AAA"* を参照してください。

III. 設定の確認

クライアントが SSID に接続できることを確認します。（詳細は省略します。）

AP が AC と切断されてから、もしくは RADIUS サーバと切断されてから数分後、失敗許可機能が動作開始し、新規クライアントが PSK 認証で SSID に接続できることを確認します。（詳細は省略します。）

1.10.9 認証装置を AP に指定時の 802.1X 認証設定例

AC－AP 間で CAPWAP トンネルが確立されている際は、AC が認証装置として動作し、AC－AP 間の CAPWAP トンネルが切断された際は AP が認証装置として動作するための設定例を示します。AP が認証装置として動作することで、AC との CAPWAP トンネルが切断されている間も新規クライアントの接続が可能となります。

I. ネットワーク要件

図 1-11に示すように、Switch は AP とクライアントに IP アドレスを割り当てるため、DHCP サーバとして動作します。

- ログイン名 abcdef、パスワード 123456 を使用して、クライアントがネットワークにアクセスできるようにオープンシステム認証と 802.1X 認証を設定します。
- AKM モードとして 802.1X を設定します。

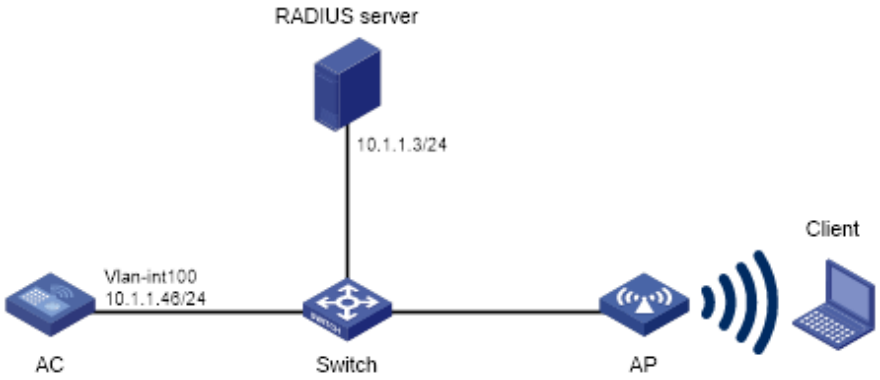


図 1-11 ネットワーク図

II. 設定手順

1) RADIUS サーバでユーザ名 abcdef、パスワード 123456 を設定し、RADIUS サーバと AC が互いに通信可能なことを確認します。（詳細は省略します。）
2) 802.1X クライアントを設定します。（詳細は省略します。）

3) 802.1X 認証用の WLAN サービステンプレート service1 を作成します。

```
<AC> system-view
[AC] wlan service-template service1
```

サービステンプレートの SSID サービスを指定します。

```
[AC-wlan-st-service1] ssid service_dot1x
```

AKM モードとして 802.1X を設定します。

```
[AC-wlan-st-service1] akm mode dot1x
```

cipher スイートとして CCMP を設定し、セキュリティ IE として RSN を設定します。

```
[AC-wlan-st-service1] cipher-suite ccmp
[AC-wlan-st-service1] security-ie rsn
```

802.1X 認証モードを設定します。

```
[AC-wlan-st-service1] client-security authentication-mode dot1x
```

802.1X 認証ドメインとして dom1 を設定します。

```
[AC-wlan-st-service1] dot1x domain dom1
```

失敗許可機能を有効にします。

```
[AC-wlan-st-service1] fail-permit enable
```

サービステンプレート service1 を有効にします。

```
[AC-wlan-st-service1] service-template enable
[AC-wlan-st-service1] quit
```

4) バックアップの 802.1X 認証用サービステンプレートを作成します。

```
<AC> system-view
[AC] wlan service-template service1_bu
```

サービステンプレートの SSID サービスを指定します。

```
[AC-wlan-st-service1_bu] ssid service_dot1x
```

AKM モードとして 802.1X を設定します。

```
[AC-wlan-st-service1_bu] akm mode dot1x
```

cipher スイートとして CCMP を設定し、セキュリティ IE として RSN を設定します。

```
[AC-wlan-st-service1_bu] cipher-suite ccmp
[AC-wlan-st-service1_bu] security-ie rsn
```

802.1X 認証モードを設定します。

```
[AC-wlan-st-service1_bu] client-security authentication-mode dot1x
```

802.1X 認証ドメインとして dom1 を設定します。

```
[AC-wlan-st-service1_bu] dot1x domain dom1
```

クライアント関連付けを AP に設定します。

```
[AC-wlan-st-service1_bu] client association-location ap
```

認証装置を AP に指定します。

```
[AC-wlan-st-service1_bu] client-security authentication-location ap
```

バックアップ用に fail-permit template を設定します。

```
[AC-wlan-st-service1_bu] fail-permit template
```

サービステンプレートを有効にします。

```
[AC-wlan-st-service1_bu] service-template enable
[AC-wlan-st-service1_bu] quit
```

5) RADIUS スキームを設定します。

RADIUS スキーム radius1 を作成し、RADIUS scheme view に移行します。

```
[AC] radius scheme radius1
```

プライマリ認証サーバ、アカウンティングサーバを指定します。

```
[AC-radius-radius1] primary authentication 10.1.1.3 1812
[AC-radius-radius1] primary accounting 10.1.1.3 1813
```

プレーンテキストで認証サーバ、アカウンティングサーバの共有鍵 12345 を設定します。

```
[AC-radius-radius1] key authentication simple 12345
[AC-radius-radius1] key accounting simple 12345
```

RADIUS サーバの設定にもとづいて、RADIUS サーバにユーザ名を送信するように設定します。RADIUS サーバに送信するユーザ名からドメイン名を除外します。

```
[Device-radius-rs1] user-name-format without-domain
[Device-radius-rs1] quit
```

RADIUS サーバに送信するユーザ名にドメイン名を含めます。

```
[Device-radius-rs1] user-name-format with-domain
[Device-radius-rs1] quit
```

6) ISP ドメイン dom1 を作成し、ISP ドメインの RADIUS スキームを設定します。

```
[AC] domain dom1
[AC-isp-dom1] authentication lan-access radius-scheme radius1
[AC-isp-dom1] authorization lan-access radius-scheme radius1
[AC-isp-dom1] accounting lan-access radius-scheme radius1
[AC-isp-dom1] quit
```

7) AP 名 ap1 の AP を作成し、モデル名、シリアル番号を指定します。

```
[AC] wlan ap ap1 model QX-W1020
[AC-wlan-ap-ap1] serial-id 219801A0CNC138011454
```

8) サービステンプレート service1 と service1_bu を AP の radio 1 に割り当て、radio 1 を有効にします。

```
[AC-wlan-ap-ap1] radio 1
[AC-wlan-ap-ap1-radio-1] service-template service1
[AC-wlan-ap-ap1-radio-1] service-template service1_bu
[AC-wlan-ap-ap1-radio-1] radio enable
[AC-wlan-ap-ap1-radio-1] return
```

9) 以下の設定を記述した“.mpcfg”形式のファイル“AP_RADIUS.mpcfg”を作成し、AC に格納する。

```
#
 dot1x authentication-method eap
#
radius scheme radius1
 primary authentication 10.1.1.3 1812
 primary accounting 10.1.1.3 1813
 key authentication simple 12345
 key accounting  simple 12345
#
domain dom1
 authentication default radius-scheme radius1
 authorization default radius-scheme radius1
 accounting default radius-scheme radius1
#
```

10) AP に“AP_RADIUS.mpcfg”を適用する。

```
[AC-wlan-ap-ap1] map-configuration cfa0:/AP_RADIUS.mpcfg
```

メモ：

AAA、RADIUS コマンドの詳細は、コマンドマニュアルのセクション 9 *セキュリティ“AAA”*を参照してください。

III. 設定の確認

クライアントが SSID に接続できることを確認します。（詳細は省略します。）

AP が AC と切断されてから、もしくは RADIUS サーバと切断されてから数分後、失敗許可機能が動作開始し、新規クライアントが 802.1X 認証で SSID に接続できることを確認します。（詳細は省略します。）

目次

このセクションのページは **13-x-x** です。

2章 WLAN IP スヌーピング 2-1
2.1 概要 2-1
2.1.1 クライアントIPv4アドレスの学習 2-1
2.2 ARPパケットスヌーピングの無効化 2-1
2.3 DHCPv4パケットのスヌーピングの設定 2-2

2章 WLAN IP スヌーピング

2.1 概要

WLAN IP snooping は AP が ARP snooping、DHCP snooping を使用してクライアントの IP アドレス、MAC アドレスを学習することを有効にします。IP アドレス、MAC アドレス、学習方式を記録した snooping エントリを生成します。エントリは、クライアントパケットを転送するかどうかを決定するために、AAA によって 802.1 X および MAC 認証クライアントのアカウンティングに使用されます。

2.1.1 クライアント IPv4 アドレスの学習

AP は以下の方法を使用してクライアントの IPv4 アドレスを学習することができます。

- クライアントとサーバ間で交換される DHCPv4 パケットを確認します。
- クライアントによって送信される ARP パケットを確認します。

IP アドレスを学習する優先度は DHCPv4 パケット、ARP パケットのスヌーピングの順番で行われます。各機能の詳細は、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*5 ネットワーク接続*”の”*8 章 ARP*”、“*5 ネットワーク接続*”の”*DHCP*”を参照してください（DHCP 関連は 12 章から 17 章に記載しています）。

2.2 ARPパケットスヌーピングの無効化

AP はデフォルトで ARP パケットと DHCPv4 パケットによってクライアントの IPv4 アドレスを学習します。

この設定を行うことによって ARP パケットからクライアントの IPv4 のアドレスの学習を無効にします。

I. 設定手順

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． サービステンプレートを作成し、その view に移行する	**wlan service-template** *service-template-name*	―
3． ARP パケットの snooping を無効にする	**undo client ipv4-snooping arp-learning enable**	デフォルト：有効

2.3 DHCPv4パケットのスヌーピングの設定

デフォルトでは、AP は ARP および DHCPv4 パケットをスヌーピングすることによってクライアント IPv4 アドレスを学習します。このタスクを実行して、DHCPv4 パケットからのクライアント IPv4 アドレス学習を無効にし、DHCP を介した IPv4 アドレス学習のタイムアウトを設定できます。

タイムアウトを設定すると、システムは、指定された期間内に DHCP を介して IPv4 アドレスを取得できなかったクライアントをログオフします。

I. 制約事項とガイドライン

タイムアウトは、AC から後でオンラインになるクライアントに対してのみ有効です。

II. 設定手順

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． サービステンプレートを作成し、その view に移行する	**wlan service-template** *service-template-name*	―
3． DHCPv4 パケットのスヌーピングを無効にする	undo client ipv4-snooping dhcp-learning enable	デフォルト：有効
4． (オプション設定項目) DHCP による IPv4 アドレスの取得に失敗したクライアントの強制ログオフを有効にする	**client ipv4-snooping dhcp-learning timeout** *value*	デフォルト：無効

目次

このセクションのページは **13-x-x** です。

3章 AAA 3-1
3.1 概要 3-1
3.1.1 RADIUS 3-2
3.1.2 装置のAAA実装 3-7
3.1.3 プロトコルと標準 3-10
3.1.4 RADIUS属性 3-10
3.2 AAAタスクの概要 3-13
3.2.1 ローカルユーザの設定 3-14
3.2.2 ローカルユーザ設定タスクの概要 3-15
3.2.3 デバイス管理ユーザの属性の設定 3-15
3.2.4 ネットワークアクセスユーザの属性の設定 3-16
3.2.5 インタラクティブモードでのデバイス管理ユーザのパスワードの変更 3-18
3.2.6 ユーザグループ属性の設定 3-18
3.2.7 ローカルユーザの確認とメンテナンス 3-19
3.3 RADIUSクライアント機能の設定 3-20
3.3.1 RADIUSクライアント機能のタスク一覧 3-20
3.3.2 RADIUSスキームの作成 3-20
3.3.3 RADIUS認証サーバの指定 3-20
3.3.4 RADIUSアカウンティングサーバの指定 3-21
3.3.5 セキュアなRADIUS通信のための共有キーの指定 3-22
3.3.6 RADIUSサーバのステータスの設定 3-23
3.3.7 RADIUSタイマの設定 3-25
3.3.8 ユーザ名形式とトラフィック統計情報単位の設定 3-26
3.3.9 RADIUS要求送信の最大試行回数の設定 3-26
3.3.10 リアルタイムアカウンティングの最大試行回数の設定 3-27
3.3.11 RADIUSパケットのDSCP優先度の設定 3-27
3.3.12 RADIUSパケットのNAS IPアドレスの指定 3-27
3.3.13 属性Acct-Session-Idの形式の指定 3-28
3.3.14 すべてのRADIUSサーバがブロックされた場合にAAA要求に対して実行するアクションの指定 3-29
3.3.15 RADIUSストップアカウンティングパケットバッファリングの設定 3-29
3.3.16 再認証のためのRADIUSサーバ選択モードの指定 3-30
3.3.17 RADIUSアカウンティング機能の設定 3-30
3.3.18 RADIUSのSNMP通知の有効化 3-31
3.3.19 RADIUSの確認とメンテナンス 3-31
3.4 ISPドメインの作成 3-32
3.4.1 ISPドメインについて 3-32
3.4.2 ISPドメイン設定の制約事項とガイドライン 3-33
3.4.3 ISPドメインの作成 3-33
3.4.4 デフォルトのISPドメインの指定 3-33
3.5 ISPドメイン属性の設定 3-34
3.5.1 ISPドメインステータスの設定 3-34
3.6 ISPドメインのAAA方式の設定 3-34
3.6.1 ISPドメインの認証方式の設定 3-34

3.6.2 ISPドメインの認可方式の設定 3-36
3.6.3 ISPドメインのアカウンティング方式の設定 3-37
3.6.4 ISPドメインの検証とメンテナンス 3-39
3.7 同時ログインユーザの最大数の設定 3-39
3.8 NAS-IDの設定 3-40
3.8.1 NAS-IDについて 3-40
3.8.2 ISPドメインでのNAS-IDの設定 3-40
3.9 パスワード変更プロンプトのログ記録の有効化 3-40
3.10 EAPプロファイルの設定 3-41
3.10.1 EAPプロファイルの概要 3-41
3.10.2 EAPプロファイルの制約事項とガイドライン 3-41
3.10.3 EAPプロファイルの前提条件 3-42
3.10.4 EAPプロファイルの設定 3-42
3.11 RADIUSサーバ機能の設定 3-42
3.11.1 RADIUSサーバ機能のタスク一覧 3-42
3.11.2 RADIUSユーザの設定 3-43
3.11.3 RADIUSクライアントの指定 3-43
3.11.4 EAP認証の設定 3-44
3.11.5 RADIUSサーバ設定の有効化 3-44
3.11.6 RADIUSサーバ設定の無効化 3-45
3.11.7 RADIUSサーバ機能の確認とメンテナンス 3-45
3.12 AAAの設定例 3-45
3.12.1 802.1X EAP-PEAP認証をRADIUSサーバとして機能するACで構成する 3-45
3.13 AAAのトラブルシューティング 3-49
3.13.1 RADIUS認証の失敗 3-49
3.13.2 RADIUSパケット配信障害 3-50
3.13.3 RADIUSアカウンティングエラー 3-50
3.14 付録 3-51
3.14.1 付録A一般的に使用されるRADIUS属性 3-51
3.14.2 付録B一般的に使用される標準RADIUS属性の説明 3-52

3章 AAA

3.1 概要

AAA は認証（Authentication）、許可（Authorization）、アカウンティング（Accounting）の 3 つのセキュリティ機能の総称です。実用的なネットワークアクセス管理を行うためのフレームワークを提供します。それぞれの以下のセキュリティ機能を提供します。

- **認証** － リモートユーザを特定し、有効なユーザか否かを判断します。
- **許可（認可）** － 認証に成功したユーザに対して提供する権限を制限します。
- **アカウンティング（課金）** － サービスタイプ、開始/終了の時間、トラフィックを含む認証に成功したユーザのネットワークサービスの使用情報を登録します。これにより、アカウンティング機能は、時間ベースおよびトラフィックベースで、ネットワークセキュリティの監視にも使用することができます。

通常、AAA ではクライアント/サーバモデルを使用します。クライアントは NAS（Network Access Server）上で動作し、サーバで集中的にユーザ情報を管理します。AAA ネットワークにおいて、図 3-1に示すように、NAS はユーザのためのサーバですが、AAA サーバのためのクライアントでもあります。

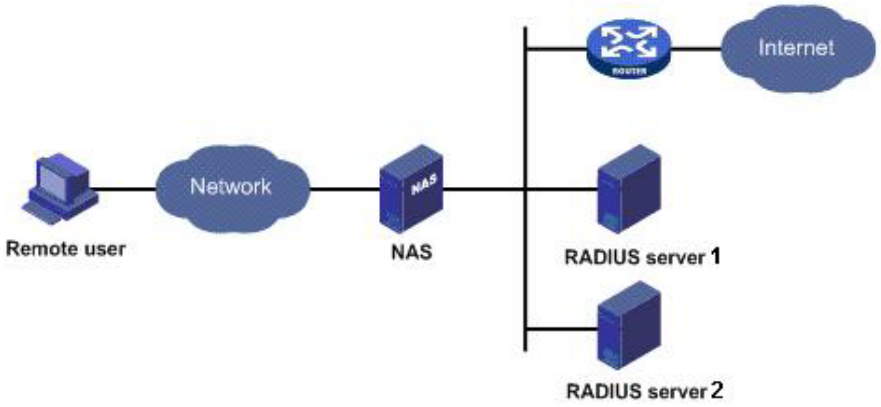


図 3-1 AAA のネットワーク構成

ユーザが NAS への接続を確立し、ほかのネットワーク、またはいくつかのネットワークリソースにアクセスするための権利を取得しようとする場合、NAS は、ユーザ、または対応する接続を認証します。NAS はユーザの AAA 情報をサーバ（RADIUS サーバ）に透過的に通すことができます。その結果 NAS はアクセス要求を許可/禁止するか決定します。

AAA を実現する方法として、最も使用されるものとして RADIUS があります。

図 3-1に示すように、RADIUS サーバ 1 と RADIUS サーバ 2 があります。この場合、必要に応じて、認証、許可、アカウンティングの役割を決めることができます。たとえば、RADIUS サーバ 2 を認証と許可に使用し、RADIUS サーバ 1 をアカウンティングサーバにすることができます。

必要に応じて、AAA を使用してセキュリティ機能を選択することができます。たとえば、会社の従業員が指定のリソースにアクセスする前に、認証を行いたい場合、認証サーバの

みを設定することで実行可能です。ネットワークの使用情報を登録したい場合、アカウンティングサーバも設定することで実行可能になります。

装置は、ダイナミックにパスワードの認証を行うことができます。

3.1.1 RADIUS

RADIUS（Remote Authentication Dial-In User Service）は、クライアント/サーバモデルにおける分散情報交換プロトコルの 1 つです。RADIUS は非許可ユーザのアクセスからネットワークを保護することから、高いセキュリティとリモートユーザアクセスの両方が必要な環境でよく使用されます。

RADIUS 許可は、RADIUS 認証と組み合わせて使用されます。ユーザ許可情報は、認証のレスポンスによって運ばれます。RADIUS はトランスポートプロトコルとして UDP を使用します。RADIUS は認証に UDP ポート 1812 を、アカウンティングに UDP ポート 1813 を使用します。

RADIUS は、元々ダイヤルインユーザアクセスのために定義されました。RADIUS は、イーサネットアクセス、ADSL アクセスのようなより多くのアクセス方式をサポートするために拡張されました。

I. クライアント/サーバモデル

RADIUS クライアントは、ネットワーク中に配置された NAS（Network Attached Storage）上で動作します。NAS は指定されたサーバにユーザ情報を転送し、そのレスポンス（たとえば、ユーザのアクセスリクエストを許可/拒否する）によって動作します。

RADIUS サーバは、ネットワークセンターのコンピュータ、またはワークステーションで動作し、ユーザ認証とネットワークアクセスサービスに関連した情報を管理します。

RADIUS サーバは以下のプロセスを実行します。

1) RADIUS クライアントから認証要求、許可要求、アカウンティング要求を受信します。
2) ユーザ認証、許可、アカウンティングを実行します。
3) ユーザアクセスコントロール情報（たとえば、ユーザのアクセスリクエストを許可/拒否する）をクライアントに送信します。

加えて RADIUS サーバは、認証プロキシのサービスを提供する別の RADIUS サーバのクライアントによって実行することができます。

通常、RADIUS サーバは、Users、Clients、Dictionary の 3 つのデータベースを管理します。

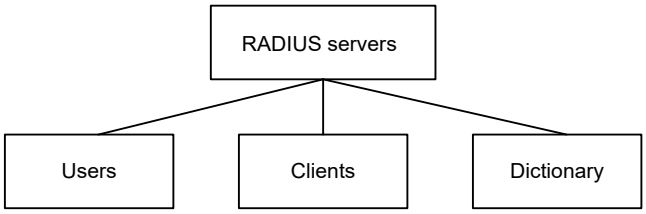


図 3-2 RADIUS サーバデータベース

- **Users** － ユーザ名、パスワード、適用プロトコル、IP アドレスのようなユーザ情報を収容します。
- **Clients** － 共有鍵や IP アドレスのような RADIUS クライアントについての情報を収容します。
- **Dictionary** － RADIUS のプロトコル属性とその値を把握するための情報を収容します。

II. 情報交換セキュリティメカニズム

RADIUS クライアントとサーバは、あらかじめ設定された共有鍵を用いて、情報の交換を行います。RADIUS パケットは Authenticator と呼ばれる 16 バイトフィールドがあります。このフィールドは、MD5 アルゴリズム、共有鍵、ほかのいくつかの情報を使用して作成されたシグネチャを送信します。パケットの受信者はシグネチャを確認し、シグネチャが正しいときのみパケットを受信します。このメカニズムは RADIUS クライアントとサーバ間の情報交換のセキュリティを保証することができます。

共有鍵は RADIUS パケットにあるユーザのパスワードを暗号化するのに使われます。

III. ユーザ認証メカニズム

RADIUS サーバは、PAP、CHAP、EAP のような複数のユーザ認証方式をサポートします。

IV. RADIUS の標準的なパケット交換プロセス

図 3-3にユーザホスト、RADIUS クライアント、RADIUS サーバ間の情報交換について示します。

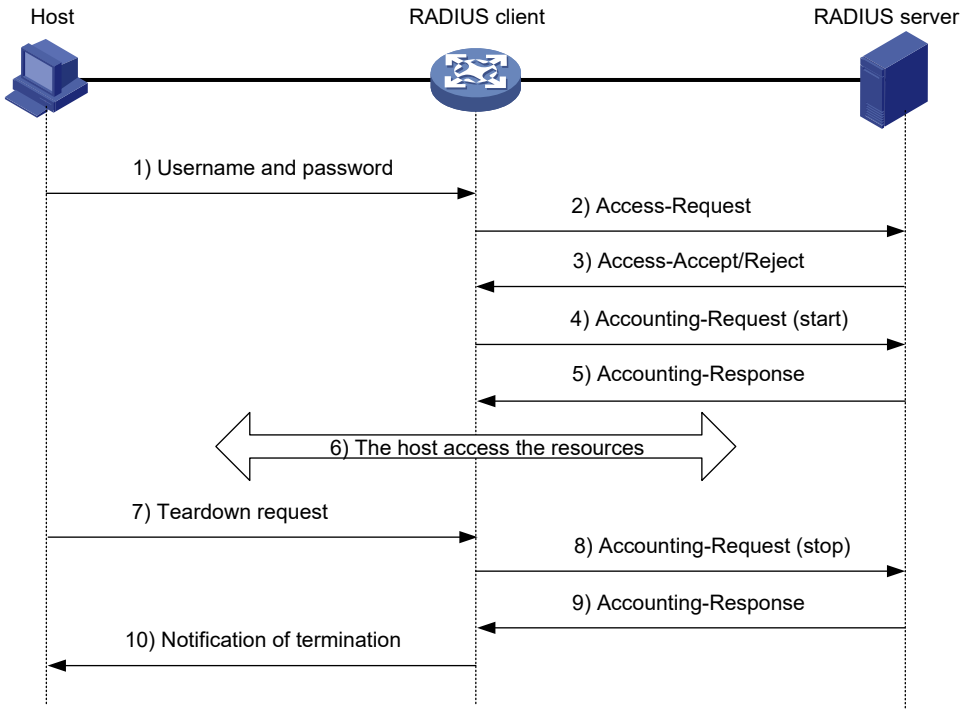


図 3-3 RADIUS の標準的なパケット交換プロセス

RADIUS は以下のように動作します。

1) ホストは、RADIUS クライアントにユーザ名とパスワードを転送し、接続リクエストを送信し始めます。
2) ユーザ名とパスワードを受信した後、RADIUS クライアントは MD5（Message-Digest5）アルゴリズムを使用して暗号化されたユーザパスワードと共有鍵を持つ認証要求（Access-Request）パケットを RADIUS サーバに送信します。
3) RADIUS サーバはユーザ名とパスワードを認証します。認証が成功した場合、ユーザの許可情報を含む Access-Accept message パケットを送り返します。認証に失敗した場合、Access-Reject message パケットを送り返します。
4) RADIUS クライアントは、返された認証結果に従ってユーザを許可、または拒否します。ユーザを許可した場合、クライアントは RADIUS サーバにアカウンティング開始要求（Accounting-Request）パケットを送信します。
5) RADIUS サーバはアカウンティング開始応答（Accounting-Response）パケットを返し、アカウンティングし始めます。
6) ユーザはネットワークリソースにアクセスすることができるようになります。
7) ホストが RADIUS クライアントに接続切断要求を行います。
8) RADIUS クライアントは RADIUS サーバにアカウンティング停止要求（Accounting-Request）パケットを送信します
9) RADIUS サーバは、ユーザのアカウンティングを停止するためにアカウンティング停止応答（Accounting-Response）パケットをクライアントに送り返します。
10) ユーザのネットワークリソースへのアクセスが停止します。

V. RADIUS パケットフォーマット

RADIUS は転送メッセージに UDP を使用します。転送メッセージは、時間管理メカニズム、再送メカニズム、バックアップサーバメカニズムを含む一連のメカニズムによって RADIUS サーバとクライアント間でのスムーズなメッセージ交換を確実にします。図 3-4 に RADIUS パケットのフォーマットを示します。

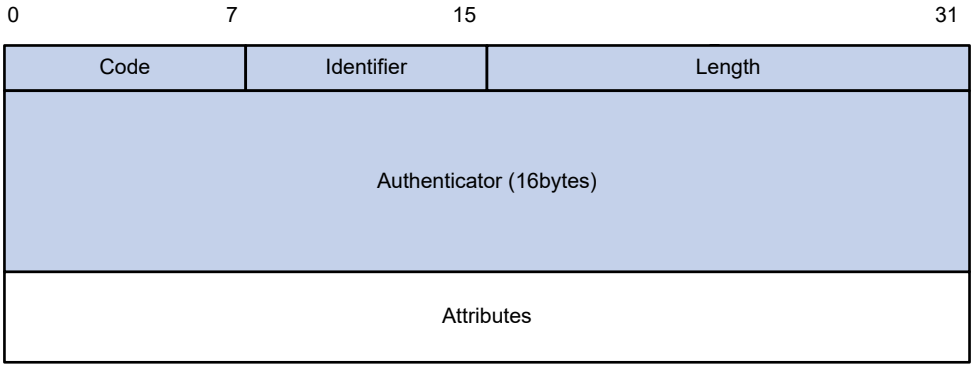


図 3-4 RADIUS パケットフォーマット

以下にフィールドの説明について記載します。

- Code フィールド（1 バイト長）は RADIUS パケットのタイプを表します。表 3-1にコードフィールドと主な値について説明します。

表 3-1 コードフィールドの主な値

Code	パケットタイプ	説明
1	Access-Request	クライアントからサーバに送信されるパケットです。このタイプのパケットは、ユーザを認証するためにサーバにユーザ情報を運ぶために使用されます。このパケットはユーザ名属性を含む必要があり、オプションとしてNAS-IPアドレス、ユーザパスワード、NAS-ポートの属性を含むことができます。
2	Access-Accept	サーバからクライアントに送信されるパケットです。Access-Requestで運ばれるすべての属性値を許可できる場合、つまり、認証が成功する場合、サーバはAccess-Accept応答パケットを送信します。
3	Access-Reject	サーバからクライアントに送信されるパケットです。Access-Requestで運ばれる情報を許可できない場合、サーバはユーザを拒否し、Access-Reject応答パケットを送信します。
4	Accounting-Request	クライアントからサーバに送信されるパケットです。このタイプのパケットはユーザのアカウンティングを開始/停止するためにサーバにユーザ情報を運ぶために使用されます。このパケットは、サーバがアカウンティングの開始/停止するための応答を示すAcct-Status-Type属性を含みます。
5	Accounting-Response	サーバからクライアントに送信されるパケットです。サーバからクライアントに送信するこのタイプのパケットは、Accounting-Requestを受信し、正確にアカウンティング情報を記録し始めたことを通知します。

- Identifier フィールド（1 バイト長）は、要求パケットと応答パケットをマッチングして、再送済みの要求パケットを検出するために使用されます。（認証あるいはアカウンティングのような）同じタイプの要求/応答パケットは同じ identifier を持ちます。
- Length フィールド（2 バイト長）は、Code、Identifier、Length、Authenticator、Attribute フィールドを含む全パケット長を示します。このフィールドの値の範囲は 20～4096 です。この範囲よりも大きい値は、不要なものとみなされ、パケットを受信されても無視します。受信パケットの長さが Length フィールドの範囲よりも小さな値の場合、そのパケットは破棄されます。
- Authenticator フィールド（16 バイト長）は、RADIUS サーバからの応答パケットを認証するために使用され、アルゴリズムを隠すパスワードにも使用されます。要求 Authenticator と応答 Authenticator の 2 種類の Authenticator があります。
- Attribute フィールド（可変長）は、要求、または応答の詳細設定を定義するために指定の認証、許可、アカウンティング情報を運びます。このフィールドは Type、Length、Value の 3 つのサブフィールドが含まれます。
  - **Type** － 属性のタイプを示します。
  - **Length** － Type、Length、Value フィールドを含む属性の長さを示します。
  - **Value** － 属性の値を示します。フォーマットと内容はサブフィールドに依存します。

一般的に使用される RADIUS 属性は、RFC2865、RFC2866、RFC2867、RFC2868 で定義されています。詳細は、本章の *“一般的に使われる標準 RADIUS 属性”* を参照してください。

表 3-2 一般的に使用される RADIUS 属性

No.	属性	No.	属性
1	User-Name	45	Acct-Authentic
2	User-Password	46	Acct-Session-Time
3	CHAP-Password	47	Acct-Input-Packets
4	NAS-IP-Address	48	Acct-Output-Packets
5	NAS-Port	49	Acct-Terminate-Cause
6	Service-Type	50	Acct-Multi-Session-Id
7	Framed-Protocol	51	Acct-Link-Count
8	Framed-IP-Address	52	Acct-Input-Gigawords
9	Framed-IP-Netmask	53	Acct-Output-Gigawords
10	Framed-Routing	54	(unassigned)
11	Filter-ID	55	Event-Timestamp
12	Framed-MTU	56-59	(unassigned)
13	Framed-Compression	60	CHAP-Challenge
14	Login-IP-Host	61	NAS-Port-Type
15	Login-Service	62	Port-Limit
16	Login-TCP-Port	63	Login-LAT-Port
17	(unassigned)	64	Tunnel-Type
18	Reply-Message	65	Tunnel-Medium-Type
19	Callback-Number	66	Tunnel-Client-Endpoint
20	Callback-ID	67	Tunnel-Server-Endpoint
21	(unassigned)	68	Acct-Tunnel-Connection
22	Framed-Route	69	Tunnel-Password
23	Framed-IPX-Network	70	ARAP-Password
24	State	71	ARAP-Features
25	Class	72	ARAP-Zone-Access
26	Vendor-Specific	73	ARAP-Security
27	Session-Timeout	74	ARAP-Security-Data
28	Idle-Timeout	75	Password-Retry
29	Termination-Action	76	Prompt
30	Called-Station-Id	77	Connect-Info
31	Calling-Station-Id	78	Configuration-Token
32	NAS-Identifier	79	EAP-Message

No.	属性	No.	属性
33	Proxy-State	80	Message-Authenticator
34	Login-LAT-Service	81	Tunnel-Private-Group-id
35	Login-LAT-Node	82	Tunnel-Assignment-id
36	Login-LAT-Group	83	Tunnel-Preference
37	Framed-AppleTalk-Link	84	ARAP-Challenge-Response
38	Framed-AppleTalk-Network	85	Acct-Interim-Interval
39	Framed-AppleTalk-Zone	86	Acct-Tunnel-Packets-Lost
40	Acct-Status-Type	87	NAS-Port-Id
41	Acct-Delay-Time	88	Framed-Pool
42	Acct-Input-Octets	89	(unassigned)
43	Acct-Output-Octets	90	Tunnel-Client-Auth-id
44	Acct-Session-Id	91	Tunnel-Server-Auth-id

VI. 拡張 RADIUS 属性

RADIUS プロトコルは優れた拡張性を持ちます。RFC 2865 で定義されている属性番号 26（Vender-Specific）は、標準 RADIUS プロトコルが提供しない機能をベンダが実装するために拡張属性を定義することができます。

ベンダはアプリケーションを拡張するために、RADIUS パケットの複数の TLV（type-length-value）のサブ属性をカプセル化することができます。図 3-5に示すように、属性番号 26 でカプセル化されるサブ属性は、以下の 4 つで構成されます。

- **Vendor-ID** – ベンダ ID を示します。最上位のバイト値は 0 で、ほかの 3 つのバイト値には RFC1700 に準拠したコードが入ります。RADIUS サブ属性は 25506 のベンダ ID をサポートします。
- **Vendor-Type** – サブ属性のタイプを示します。
- **Vendor-Length** – サブ属性の長さを示します。
- **Vendor-Data** – サブ属性の内容を示します。

拡張 RADIUS 属性の詳細については、本章の *"QX シリーズ用 RADIUS 属性"* を参照してください。

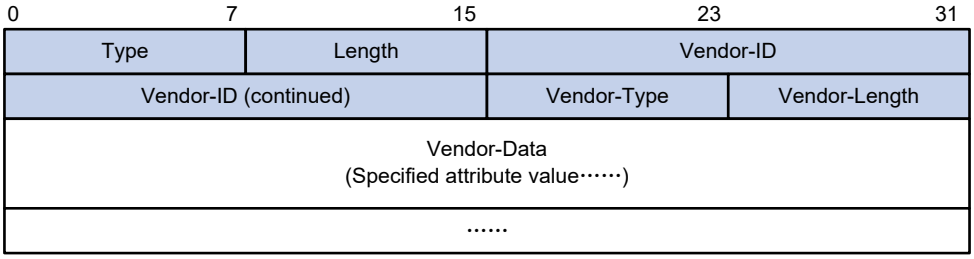


図 3-5 属性番号 26 の拡張 RADIUS 属性フォーマット

3.1.2 装置の AAA 実装

この章は AAA のユーザ管理と方法について記載します。

I. ISP ドメインにもとづくユーザ管理とユーザクセスタイプ

AAA は ISP ドメインとアクセスタイプもとづいてユーザを管理します。

NAS で各ユーザは 1 つの ISP ドメインに属しています。通常、NAS は、ユーザがログインするために使用するユーザ名によって、ISP ドメインを決定します。

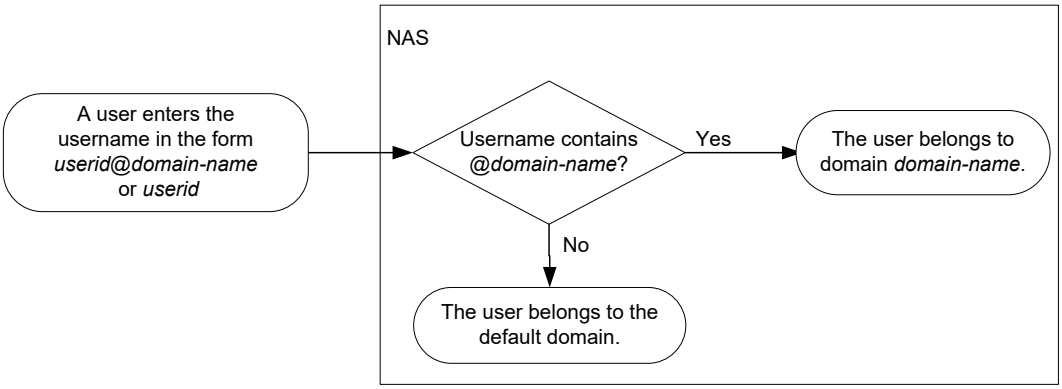


図 3-6 ユーザ名を用いた ISP ドメインの決定

AAA はアクセスタイプにもとづいて、同じ ISP ドメインのユーザを管理します。装置はログインユーザのみサポートします。ログインユーザは以下のタイプのユーザアクセスをサポートします。

- **LAN**－802.1X 認証あるいは MAC アドレス認証にパスした LAN ユーザを含みます。
- **Login**－SSH、Telnet、FTP、装置にログインしている端末のユーザを含みます。端末のユーザはコンソールポートを通してアクセスすることができます。
- **ポータル**－ポータルユーザは、ネットワークアクセスのためにポータル認証を通過する必要があります。

🕮 **メモ：**

ユーザ認証の管理ポリシに対応するため、装置は 802.1X のような認証モジュールを提供します。認証モジュールを設定した場合、アクセスタイプのユーザの ISP ドメインは認証モジュールの設定に依存します。

II. AAA 認証方式

AAA は ISP ドメインの異なるタイプのユーザのため、異なる認証、許可、アカウンティング方式を設定することができます。NAS はユーザの ISP ドメインとアクセスタイプを決定し、ユーザのアクセスを管理するため、設定された認証方式を使用します。

AAA は ISP ドメインのデフォルト方式の設定をサポートします。デフォルト方式は、特定の AAA 方式が設定されていないユーザに使われます。

装置は、以下の認証方式をサポートします。

- **認証なし** － すべてのユーザが信頼され、認証が実施されません。通常、この方式はセキュリティ目的で使われません。
- **ローカル認証** － 認証は、ユーザ名、パスワード、属性を含むユーザ情報の設定された NAS によって実行されます。ローカル認証は、高速かつ低コストですが、収容できる情報量は、記憶容量に依存します。
- **リモート認証** － アクセス装置は、ユーザを認証するために RADIUS サーバを利用します。RADIUS に関して、装置はユーザ認証を実行するために、標準的な RADIUS プロトコルを使用することができます。リモート認証の特徴は、集中した情報管理、高い能力、高い信頼性、複数の装置のための集中した認証が挙げられます。また、リモート認証サーバが有効でないときのバックアップ方式としてローカル認証を設定することができます。

装置は、以下の許可方式をサポートします。

- **許可なし** － NAS は許可を実行しません。認証にパスするとネットワークに以下のデフォルト許可情報を適用します。
  - □ ログインユーザはネットワークにアクセスできません。
  - □ ログインユーザはレベル 0 ユーザロールを獲得します。
  - □ FTP、SFTP ユーザが認証にパスしたとき、作業ディレクトリが NAS のルートディレクトリになりますが、アクセスすることはできません。
- **ローカル許可** － ユーザは、ユーザのために設定された属性に従って、NAS によって許可されます。
- **リモート許可** － NAS はユーザを許可するため、RADIUS サーバと協力します。RADIUS 許可は RADIUS 認証と結び付けられます。RADIUS 許可は、RADIUS 認証が成功した後のみ動作し、許可情報は Access-Accept で運ばれます。リモートサーバが有効でない場合は、バックアップ方式としてローカル許可、または許可なしを設定することができます。

装置は、以下のアカウンティング方式をサポートします。

- **アカウンティングなし** － NAS はユーザのアカウンティングを実行しません。
- **ローカルアカウンティング** － ローカルアカウンティング方式は NAS 上で実行されます。ユーザ数の統計情報を収集し、ローカルユーザ接続の数を制御します。ローカルアカウンティング方式は、ユーザ管理のための統計情報を提供しません。
- **リモートアカウンティング** － NAS は、ユーザアカウンティングのために、RADIUS サーバと連携します。リモートサーバが利用できない場合に備えて、バックアップ方法としてローカルアカウンティング方式を設定することができます。

加えて、装置は、セキュリティを向上させるために、以下のサービスを提供します。

- **ユーザロール切り替え認証** － ログアウトや切断を行うことなしで、一時的なユーザロールを使用してユーザを認証します。

III. AAA 拡張機能

デバイスは、デバイスセキュリティを強化するために次のログインサービスを提供します。

- コマンド認可:ログインユーザが入力したコマンドが許可されるかどうかを NAS が認可サーバに判断できるようにします。ログインユーザは、認可サーバによって許可されたコマンドだけを実行できます。コマンド認可の詳細については、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*2 基本機能*”の”*7 章 ログインユーザの制御*”を参照してください。
- コマンドアカウンティング:コマンド認可が無効になっている場合、コマンドアカウンティングを使用すると、デバイスで実行されたすべての有効なコマンドをアカウンティングサーバに記録できます。コマンド認可が有効になっている場合、コマンドアカウンティングを使用すると、認証されたすべてのコマンドをアカウンティングサーバに記録できます。

- ユーザロール認証:ログアウトまたは切断せずに、別のユーザロールを取得する各ユーザを認証します。

3.1.3 プロトコルと標準

以下に AAA、RADIUS に関連したプロトコルと標準を示します。

- RFC 2865, Remote Authentication Dial In User Service (RADIUS)
- RFC 2866, RADIUS Accounting
- RFC 2867, RADIUS Accounting Modifications for Tunnel Protocol Support
- RFC 2868, RADIUS Attributes for Tunnel Protocol Support
- RFC 2869, RADIUS Extensions
- RFC 5176, Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)
- RFC 1777, Lightweight Directory Access Protocol
- RFC 2251, Lightweight Directory Access Protocol (v3)

3.1.4 RADIUS 属性

I. 一般的に使われる標準 RADIUS 属性

番号	属性	説明
1	User-Name	認証されるユーザ名です。
2	User-Password	PAP認証のユーザパスワードです。PAP認証モードでAccess-Requestパケットでのみ存在します。
3	CHAP-Password	CHAP認証のユーザパスワードです。CHAP認証モードでAccess-Requestパケットでのみ存在します。
4	NAS-IP-Address	サーバがクライアントを認識するIPアドレスです。通常、クライアントはNASのアクセスインタフェースで識別され、NASのIPアドレスと呼ばれます。Access-Requestパケットでのみ存在します。
5	NAS-Port	ユーザがアクセスするNASの物理ポートです。
6	Service-Type	ユーザが要求したあるいは提供されたType of serviceです。
7	Framed-Protocol	フレーム化されるカプセル化プロトコルです。
8	Framed-IP-Address	ユーザに割り当てられるIPアドレスです。
11	Filter-ID	フィルタリスト名です。 • 名前が全て数字の場合、ACL番号を表します。 • 名前が"user-group=name1;name2;..;namex"のような形式の文字列の場合、ユーザグループ名のリストを表します。このタイプのフィルタリストはSSL VPNユーザにのみ適用可能です。 名前が全て数字の形式でない場合、あるいは等号記号（=）を含まない場合、ユーザプロファイル名を示します。
12	Framed-MTU	ユーザとNAS間のデータリンクの最大転送ユニット（MTU）です。たとえば802.1X EAP認証です。NASはこの属性を使用してEAPパケットのMTUサイズが超過しないようにサーバに知らせます。
14	Login-IP-Host	ユーザクセスを行うNASインタフェースのIPアドレスです。

番号	属性	説明
15	Login-Service	ユーザがログインするためのサービスタイプです。
18	Reply-Message	ユーザに表示されるテキストです。認証失敗などでサーバがユーザに通知するために使われます。
26	Vendor-Specific	ベンダ仕様属性です。パケットはベンダ属性のような1つ以上の属性を含めることができます。それは1つ以上のサブ属性を含みます。
27	Session-Timeout	セッションが終了する前に提供されるサービスの最大継続時間です。
28	Idle-Timeout	セッションが終了する前に許可される最大Idle時間です。
31	Calling-Station-Id	NASがサーバに送信したユーザ識別子です。QXシリーズのデバイスによって提供されるLANアクセスサービスとして、この属性は、ユーザのHHHH-HHHH-HHHH形式のMACアドレスを保持します。
32	NAS-Identifier	NASがRADIUSサーバを識別するために使用する識別子です。
40	Acct-Status-Type	Accounting-Requestパケットタイプです。 ● **1** – Start ● **2** – Stop ● **3** – Interim-Update ● **4** – Reset-Charge ● **7** – Accounting-On （第3世代（3G）移動体通信システムの標準化プロジェクト）で定義。） ● **8** – Accounting-Off （第3世代（3G）移動体通信システムの標準化プロジェクト）で定義。） ● **9 ～ 14**– トンネルアカウンティング用に予約 ● **15** – 故障用に予約
45	Acct-Authentic	ユーザによって使われる認証方式です。 ● **1** – RADIUS ● **2** – Local ● **3** – Remote
60	CHAP-Challenge	NASは、CHAP認証の間、MD5を計算するためにCHAPチャレンジを作成します。
61	NAS-Port-Type	ユーザによって、認証されているNASの物理ポートタイプです。 ● **15** – Ethernet ● **16** – ADSLのすべてのタイプ ● **17** – ケーブル （ケーブルTV用） ● **19** – WLAN-IEEE 802.11 ● **201** – VLAN ● **202** – ATM もしポートがATMやEthernetで、VLANがそのポートに実装された場合、この属性の値は201です。
79	EAP-Message	NASが、EAPを経由して、カプセル化しているEAPパケットを許可するために使われます。
80	Message-Authenticator	偽のAccess-Requestを防ぐため、認証し、認証パケットをチェックするのに使われます。この属性は、RADIUSがEAP認証をサポートするときに使われます。
87	NAS-Port-Id	ユーザを認証しているNASのポートです。

II. QX シリーズ用 RADIUS 属性

番号	属性	説明
1	Input-Peak-Rate	ユーザからNASへの最大レート（bps）です。
2	Input-Average-Rate	ユーザからNASへの平均レート（bps）です。
3	Input-Basic-Rate	ユーザからNASへの基本レート（bps）です。
4	Output-Peak-Rate	NASからユーザへの最大レート（bps）です。
5	Output-Average-Rate	NASからユーザへの平均レート（bps）です。
6	Output-Basic-Rate	NASからユーザへの基本レート（bps）です。
15	Remanent_Volume	異なるサーバタイプのため、異なるユニットの存在している有効な接続のトータルトラフィックです。
20	Command	セッション管理で使われるセッション処理です。 ● **1**– Trigger-Request ● **2**– Terminate-Request ● **3**– SetPolicy ● **4**– Result ● **5**– PortalClear
24	Control_Identifier	再送パケット用の識別子です。同一セッションの再送されたパケット用の属性は同じ値を使用する必要があります。異なるセッションの再送されたパケット用の属性は同じ値としてもいいです。再送パケットのクライアントの応答は、この属性を持ち、属性の値は同一にしなくてはいけません。 start、stop、interim updateタイプのAccounting-Requestパケットのための Control-Identifier属性がある場合、値は意味をなしません。
25	Result_Code	Trigger-RequestあるいはSetPolicy動作の戻り値です。値が0の場合、動作が成功し、他の値の場合、動作は失敗しています。
26	Connect_ID	ユーザ接続のインデックスです。
28	Ftp_Directory	FTPユーザの作業ディレクトリです。FTPユーザのため、RADIUSクライアントがFTPサーバとして動作するとき、この属性はRADIUSクライアントのFTPディレクトリを設定するのに使われます。
29	Exec_Privilege	実行ユーザの優先度です。
59	NAS_Startup_Timestamp	NASの開始時間です。1970 年1月1日0時0分0秒（UTC時間）からの経過時間を示しています。
60	Ip_Host_Addr	認証とアカウンティング要求で使われるユーザのIPアドレス、MACアドレスです。IPアドレスA.B.C.DとMACアドレスhh:hh:hh:hh:hh:hhの間には空白が必要です。
61	User_Notify	サーバからクライアントに透過的に送信する必要がある情報です。
62	User_HeartBeat	802.1Xユーザが認証をパスした後、32バイト長で割り当てられるハッシュ値です。この属性は、デバイスのユーザリストに記録され、802.1Xユーザからハンドシェイクメッセージをチェックするために使われます。この属性はAccess-Acceptパケットと Accounting-Requestパケットでのみ存在します。
111	Longitude-Latitude	NASの緯度、経度の情報です。

番号	属性	説明
140	User_Group	SSL VPNユーザが認証をパスした後、割り当てられるユーザグループです。ユーザは複数のユーザグループに属することができます。ユーザグループは、セミコロンで区切られます。この属性はSSL VPNデバイスと共有するために使われます。
141	Security_Level	SSL VPNユーザがセキュリティ認証をパスした後、割り当てられるセキュリティレベルです。
201	Input-Interval-Octets	実時間のアカウンティング間隔に入力したバイト数です。
202	Output-Interval-Octets	実時間のアカウンティング間隔に出力したバイト数です。
203	Input-Interval-Packets	デバイスでのユニットセットにおけるアカウンティング間隔に入力したパケット数です。
204	Output-Interval-Packets	デバイスでのユニットセットにおけるアカウンティング間隔に出力したパケット数です。
205	Input-Interval-Gigawords	4Gバイトで分割されたアカウンティング間隔に入力したバイト数の結果です。
206	Output-Interval-Gigawords	4Gバイトで分割されたアカウンティング間隔に出力したバイト数の結果です。
207	Backup-NAS-IP	RADIUSパケットを送信するためのバックアップの送信元IPアドレスです。
255	Product_ID	装置名です。

3.2 AAAタスクの概要

AAA を設定するには、次のタスクを実行します。

1) AAA スキームの設定

ローカル認証を使用する場合は、ローカルユーザと関連属性を設定します。リモート認証を使用する場合は、必要な RADIUS スキームを設定し、サーバに従ってユーザ属性を設定します。

操作	補足
ローカルユーザの設定	
RADIUSクライアント機能の設定	

2) ISP ドメインの設定

操作	補足
ISPドメインの作成	
ISPドメイン属性の設定	

3) ISPドメインのAAA方式の設定

必要に応じて、ISP ドメインの認証、認可、およびアカウンティング方式を設定します。これらの方式は、既存の AAA 方式を使用します。

操作	補足
ISPドメインの認証方式の設定	
ISPドメインの認可方式の設定	
ISPドメインのアカウンティング方式の設定	

4) (オプション設定項目) 高度な AAA 機能の設定

操作	補足
同時ログインユーザの最大数の設定	
NAS-IDの設定	
パスワード変更プロンプトのログ記録の有効化	

3.2.1 ローカルユーザの設定

ローカル認証、許可、およびアカウンティングを実装するには、ローカルユーザを作成し、デバイスでユーザ属性を設定します。ローカルユーザと属性は、デバイス上のローカルユーザデータベースに格納されます。ローカルユーザは、ユーザ名とユーザタイプの組み合わせによって一意に識別されます。

ローカルユーザは、次のタイプに分類されます。

- デバイス管理ユーザ:デバイス管理のためにデバイスにログインするユーザ。
- ネットワークアクセスユーザ:デバイスを介してネットワークリソースにアクセスするユーザ。

ネットワークアクセスユーザには、一時的にネットワークにアクセスするゲストも含まれます。ゲストはポータルサービスのみを使用できます。

設定可能なローカルユーザ属性を次に示します。

- 説明:ユーザの説明情報。
- サービスタイプ:ユーザが使用できるサービス。ローカル認証では、ローカルユーザのサービスタイプがチェックされます。使用可能なサービスタイプがない場合、ユーザは認証に合格できません。
- ユーザの状態:ローカルユーザがネットワークサービスを要求できるかどうか。アクティブとブロックの 2 つのユーザ状態があります。アクティブ状態のユーザはネットワークサービスを要求できますが、ブロック状態のユーザは要求できません。
- 同じユーザ名を使用した同時ログインの上限:同じユーザ名を使用してデバイスに同時にアクセスできるユーザの最大数。この数が上限に達すると、ユーザ名を使用してデバイスにアクセスできるローカルユーザはなくなります。
- ユーザグループ:各ローカルユーザはローカルユーザグループに属し、グループのすべての属性を持ちます。属性には、パスワード制御属性と認可属性が含まれます。ローカルユーザグループの詳細については、本章の“*ユーザグループ属性の設定*“ を参照してください。
- バインディング属性:バインディング属性はユーザのスコープを制御し、ユーザのローカル認証中にチェックされます。ユーザの属性がローカルユーザアカウントに設定されたバインディング属性と一致しない場合、ユーザは認証を渡すことができません。
- 認可属性:認可属性は、ローカル認証に合格した後のユーザの権限を示します。

ローカルユーザのサービスタイプに基づいて認可属性を設定します。

認可属性は、ユーザグループ view またはローカルユーザ view で設定できます。ローカルユーザ view での認可属性の設定は、ユーザグループ view での属性設定よりも優先されます。

ユーザグループ view で設定された属性は、ユーザグループ内のすべてのローカルユーザに対して有効になります。

ローカルユーザ view で設定された属性は、ローカルユーザに対してのみ有効になります。

- パスワード制御属性:パスワード制御属性は、ローカルユーザのパスワードセキュリティの制御に役立ちます。パスワード制御属性には、パスワードのエージングタイム、パスワードの最小長、パスワード構成チェック、パスワード複雑性チェック、およびログイン試行制限が含まれます。

パスワード制御属性は、システム view、ユーザグループ view、またはローカルユーザ view で設定できます。有効範囲が小さいパスワード制御属性の方が優先度が高くなります。パスワード管理およびグローバルパスワード設定の詳細については、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*15 セキュリティ*”の”*3 章 パスワード管理*”を参照してください。

- 有効期間:ネットワークアクセスユーザが認証に有効と見なされる期間。

3.2.2 ローカルユーザ設定タスクの概要

ローカルユーザを設定するには、次のタスクを実行します。

操作	補足
ローカルユーザ属性の設定 デバイス管理ユーザの属性の設定 ネットワークアクセスユーザの属性の設定	
(オプション設定項目)インタラクティブモードでのデバイス管理ユーザのパスワードの変更	
(オプション設定項目)ユーザグループ属性の設定	

3.2.3 デバイス管理ユーザの属性の設定

I. 制限事項とガイドライン

password-control enable コマンドを使用してパスワード制御をグローバルに有効にすると、デバイスはローカルユーザパスワードを表示せず、実行コンフィギュレーションにも保持しません。パスワード制御をグローバルに無効にすると、ローカルユーザパスワードは自動的に実行コンフィギュレーションに復元されます。実行コンフィギュレーションを表示するには、**display current-configuration** コマンドを使用します。

認可属性とパスワード制御属性は、ローカルユーザ view またはユーザグループ view で設定できます。ローカルユーザ view の設定は、ユーザグループ view の設定よりも優先されます。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. デバイス管理ユーザ view に移行する	**local-user** *user-name* [**class manage**]	—
3. デバイス管理ユーザのパスワードを設定する	**password** [{ **hash** | **simple** } **string**]	—
4. デバイス管理ユーザにサービスを設定する	**service-type** { **ftp** | { **http** | **https** | **ssh** | **telnet** | **terminal** } * }	デフォルト：設定なし

操作	コマンド	補足
5. (オプション設定項目) デバイス管理ユーザのステータスを設定する	**state** { **active** | **block** }	デフォルト：active
6. (オプション設定項目) デバイス管理ユーザ名を使用して同時ログインの上限を設定する	**access-limit** *max-user-number*	デフォルト：制限なし
7. (オプション設定項目) デバイス管理ユーザの認可属性を設定	**authorization-attribute** { **idle-cut** *minutes* | **user-role** *role-name* | **work-directory** *directory-name* } *	デフォルト：FTP、SFTP、SCPのユーザ作業ディレクトリは、NASのルートディレクトリですが、ユーザにはアクセス権限がありません。ネットワークオペレーターのユーザロールは、ネットワーク管理者またはレベル15のユーザによって作成されたローカルユーザが割り当てられます。
8. (オプション設定項目) デバイス管理ユーザのパスワード制御属性を設定する	・パスワードのエージングタイムを設定します。 **password-control aging** *aging-time* ・パスワードの最小長を設定します。 **password-control length** *length* ・パスワード構成ポリシを設定します。 **password-control composition type-number** *type-number* [**type-length** *type-length*] ・パスワード複雑性チェックポリシを設定します。 **password-control complexity** { **same-character** | **user-name** } **check** ・最大ログイン試行回数と、ログインに失敗した場合に実行するアクションを設定します。 **password-control login-attempt** *login-times* [**exceed** { **lock** | **lock-time** *time* | **unlock** }]	デフォルト：ユーザが属するユーザグループのパスワード制御属性
9. (オプション設定項目) デバイス管理ユーザをユーザグループに割り当てる	**group** *group-name*	デフォルト：設定なし

3.2.4 ネットワークアクセスユーザの属性の設定

I. 制限事項とガイドライン

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の有効ステータスは、デバイス管理ユーザのパスワードをデバイスが保存する方法に影響します。

- ネットワークアクセスユーザに対してパスワード制御をグローバルに有効にすると、デバイスはユーザのパスワードを表示せず、実行コンフィギュレーションのパスワードも保持しません。
- ネットワークアクセスユーザのパスワード制御をグローバルに無効にすると、デバイスは自動的にユーザのパスワードを実行コンフィギュレーションに復元します。

ネットワークアクセスユーザのパスワード制御をグローバルに有効にするには、**password-control enable network-class** コマンドを使用します。実行コンフィギュレーションを表示するには、**display current-configuration** コマンドを使用します。

認可属性とパスワード制御属性は、ローカルユーザ view またはユーザグループ view で設定できます。ローカルユーザ view の設定は、ユーザグループ view の設定よりも優先されます。

ユーザのサービスタイプに基づいてロケーションバインディング属性を設定します。

- ポータルユーザの場合、ユーザがデバイスにアクセスする際に使用するポータル対応インタフェースを指定します。VLAN インタフェースでポータルが有効になっており、**portal roaming enable** コマンドを使用しない場合は、レイヤ 2 イーサネットインタフェースを指定します。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. ネットワークアクセスユーザ view に移行する	**local-user** *user-name* [**class network**]	—
3. ネットワークアクセスユーザのパスワードを設定する	**password** { **cipher** | **simple** } *string*	—
4. (オプション設定項目) ネットワークアクセスユーザの説明を設定	**description** *text*	デフォルト：設定なし
5. ネットワークアクセスユーザにサービスを割り当てる	**service-type** { **ike** | **ipoe** | **portal** | **sslvpn** }	デフォルト：設定なし
6. (オプション設定項目) ネットワークアクセスユーザのステータスを設定する	**state** { **active** | **block** }	デフォルト：active
7. (オプション設定項目) 同時ログインの上限を設定	**access-limit** *max-user-number*	デフォルト：制限なし
8. (オプション設定項目) ネットワークアクセスユーザのバインディング属性を設定する	**bind-attribute** { **ip** *ip-address* | **location interface** *interface-type interface-number* | **mac** *mac-address* | **vlan** *vlan-id* } *	デフォルト：設定なし
9. (オプション設定項目) ネットワークアクセスユーザの認可属性を設定する	**authorization-attribute** { **acl** *acl-number* | **idle-cut** *minutes* | **ip** *ipv4-address* | **ip-pool** *ipv4-pool-name* | { **primary-dns** | **secondary-dns** } { *ip ipv4-address* } | **session-timeout** *minutes* | **user-profile** *profile-name* | **vlan** *vlan-id* } *	デフォルト：設定なし 許可属性なし

操作	コマンド	補足
10. (オプション設定項目) ネットワークアクセスユーザのパスワード制御属性を設定する	・パスワードの最小長を設定します。 **password-control length** *length* ・パスワード構成ポリシを設定します。 **password-control composition type-number** *type-number* [**type-length** *type-length*] ・パスワード複雑性チェックポリシを設定します。 **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制御属性を使用
11. (オプション設定項目) ネットワークアクセスユーザをユーザグループに割り当てる	**group** *group-name*	デフォルト：設定なし

3.2.5 インタラクティブモードでのデバイス管理ユーザのパスワードの変更

既存のデバイス管理ユーザのパスワードをインタラクティブモードで変更するには、ユーザ view で次のコマンドを実行します。

操作	コマンド	補足
1. パスワードを変更する	**password**	—

3.2.6 ユーザグループ属性の設定

ユーザグループは、ローカルユーザの設定と管理を簡素化します。ユーザグループには、ローカルユーザのグループが含まれ、一連のローカルユーザ属性があります。ユーザグループのローカルユーザ属性を設定して、グループ内のローカルユーザの集中ユーザ属性管理を実装できます。管理可能なローカルユーザ属性には、認可属性が含まれます。

無線ユーザをユーザグループ別に分離するには、各ユーザにユーザグループを割り当て、ユーザグループ分離を設定します。

- グループ内分離:グループ内のユーザは、レイヤ 2 またはレイヤ 3 で相互に到達できません。
- グループ間分離:グループ内のユーザは、他のグループのユーザと通信できません。

I. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. ユーザグループ view に移行する	**user-group** *group-name*	—

操作	コマンド	補足
3. ユーザグループの認可属性を設定する	**authorization-attribute** { **acl** *acl-number* | **idle-cut** *minutes* | **ip-pool** *ipv4-pool-name* | { **primary-dns** | **secondary-dns** } { **ip** *ipv4-address* } | **session-group-profile** *session-group-profile-name* | **session-timeout** *minutes* | **subscriber-id** *subscriber-id* | **user-profile** *profile-name* | **vlan** *vlan-id* | **work-directory** *directory-name* } *	デフォルト：設定なし
4. (オプション設定項目) ユーザグループのパスワード制御属性を設定する	・パスワードのエージングタイムを設定します。 **password-control aging** *aging-time* ・パスワードの最小長を設定します。 **password-control length** *length* ・パスワード構成ポリシを設定します。 **password-control composition type-number** *type-number* [**type-length** *type-length*] ・パスワード複雑性チェックポリシを設定します。 **password-control complexity** { **same-character** | **user-name** } **check** ・最大ログイン試行回数とログイン失敗時のアクションを設定します。 **password-control login-attempt** *login-times* [**exceed** { **lock** | **lock-time time** | **unlock** }]	デフォルト : ユーザグループはグローバルパスワード制御設定を使用します。

🕮 **メモ：**

ユーザグループベースのユーザ分離は、ワイヤレス集中転送シナリオのユニキャストパケットに対してのみ有効です。

3.2.7 ローカルユーザの確認とメンテナンス

I. ローカルユーザーとユーザーグループ情報の表示

すべての view で **display** コマンドを実行できます。

操作	コマンド
ローカルユーザの設定とオンラインユーザの統計情報を表示する	**display local-user** [**class** { **manage** | **network** [**guest**] } | **idle-cut** { **disable** | **enable** } | **service-type** { **ftp** | **http** | **https** | **ike** | **ipoe** | **portal** | **ssh** | **sslvpn** | **telnet** | **terminal** } | **state** { **active** | **block** } | **user-name** *user-name* **class** { **manage** | **network** [**guest**] } | **vlan** *vlan-id*]
ユーザグループの設定を表示する	**display user-group** { **all** | **name group-name** } [**identity-member** { **all** | **group** | **user** }]

3.3 RADIUSクライアント機能の設定

3.3.1 RADIUS クライアント機能のタスク一覧

RADIUS クライアントを設定するには、次のタスクを実行します。

操作	補足
RADIUSスキームの作成	
RADIUS認証サーバの指定	
RADIUSアカウンティングサーバの指定	
セキュアなRADIUS通信のための共有キーの指定	
(オプション設定項目)RADIUSサーバのステータスの設定	
(オプション設定項目)RADIUSタイマの設定	
(オプション設定項目)RADIUSパケットのパラメータ設定 ユーザ名形式とトラフィック統計情報単位の設定 RADIUS要求送信の最大試行回数の設定 リアルタイムアカウンティングの最大試行回数の設定 RADIUSパケットのDSCP優先度の設定 RADIUSパケットのNAS IPアドレスの指定	
(オプション設定項目)RADIUS属性パラメータの設定 属性Acct-Session-Idの形式の指定	
(オプション設定項目)拡張RADIUS機能の設定 すべてのRADIUSサーバがブロックされた場合にAAA要求に対して実行するアクションの指定 RADIUSストップアカウンティングパケットバッファリングの設定 再認証のためのRADIUSサーバ選択モードの指定 RADIUSアカウンティング機能の設定 RADIUSのSNMP通知の有効化	

3.3.2 RADIUS スキームの作成

I. 制約事項とガイドライン

最大 16 個の RADIUS スキームを作成できます。RADIUS スキームは、複数の ISP ドメインで使用できます。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. RADIUS スキームを作成し、RADIUS スキーム view に移行する	**radius scheme** *radius-scheme-name*	デフォルト：設定なし

3.3.3 RADIUS 認証サーバの指定

RADIUS 認証サーバは、認証情報が RADIUS クライアントに送信される認証応答にピギーバックされるため、認証と認可を同時に完了します。

RADIUS スキームには、1 つのプライマリ認証サーバと最大 16 のセカンダリ認証サーバを指定できます。セカンダリサーバは、プライマリサーバが到達不能になったときに AAA サービスを提供します。デバイスは、セカンダリサーバが設定されている順序でアクティブサーバを検索します。

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、デバイスはプライマリおよびセカンダリサーバの役割を考慮せずに、すべてのサーバにワークロードを分散します。デバイスは、アクティブなサーバごとに現在サービスを提供しているユーザの重み値と数を確認し、認証要求を受信するパフォーマンス上最も適切なサーバを決定します。

I. 制約事項とガイドライン

冗長性が必要ない場合は、プライマリサーバのみを指定します。

RADIUS 認証サーバは、あるスキームのプライマリ認証サーバと、別のスキームのセカンダリ認証サーバとして同時に機能できます。

スキーム内の 2 つの認証サーバ (プライマリ,セカンダリ) は、ホスト名、IP アドレス、ポート番号の組み合わせを同じにすることはできません。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. RADIUS スキーム view に移行する	**radius scheme** *radius-scheme-name*	—
3. プライマリ RADIUS 認証サーバを指定する	**primary authentication** { *host-name* | *ipv4-address* } [*port-number* | **key** { **cipher** | **simple** } *string* | **test-profile** *profile-name* | **weight** *weight-value*] *	デフォルト：設定なし weightキーワードは、RADIUSスキームでRADIUSサーバのロードシェアリング機能が有効な場合にのみ機能します。
4. (オプション設定項目) セカンダリ RADIUS 認証サーバを指定する	**secondary authentication** { *host-name* | *ipv4-address* } [*port-number* | *key* { **cipher** | **simple** } *string* | **test-profile** *profile-name* | **weight** *weight-value*] *	デフォルト：設定なし weightキーワードは、RADIUSスキームでRADIUSサーバのロードシェアリング機能が有効な場合にのみ機能します。

3.3.4 RADIUS アカウンティングサーバの指定

RADIUS スキームには、1 つのプライマリアカウンティングサーバと最大 16 のセカンダリアカウンティングサーバを指定できます。セカンダリサーバは、プライマリサーバが使用できなくなったときに AAA サービスを提供します。デバイスは、セカンダリサーバが設定されている順序でアクティブサーバを検索します。

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、デバイスはプライマリおよびセカンダリサーバの役割を考慮せずに、すべてのサーバにワークロードを分散します。デバイスは、アクティブなサーバごとに現在サービスを提供しているユーザの重み値と数を確認し、パフォーマンス上最も適切なサーバを判断してアカウンティング要求を受信します。

I. 制約事項とガイドライン

冗長性が必要ない場合は、プライマリサーバのみを指定します。

RADIUS アカウンティングサーバは、1 つのスキームのプライマリアカウンティングサーバとして機能し、同時に別のスキームのセカンダリアカウンティングサーバとして機能できます。

スキーム内の 2 つのアカウンティングサーバ (プライマリまたはセカンダリ) は、ホスト名、IP アドレス、ポート番号の組み合わせを同じにすることはできません。

RADIUS は、FTP、SFTP、および SCP ユーザのアカウンティングをサポートしていません。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. RADIUS スキーム view に移行する	**radius scheme** *radius-scheme-name*	―
3. プライマリアカウンティングサーバを指定する	**primary accounting** { *host-name* | *ipv4-addres* } [*port-number* | **key** { **cipher** | **simple** } *string* | **test-profile** *profile-name* | **weight** *weight-value*] *	デフォルト：設定なし weightキーワードは、RADIUSスキームでRADIUSサーバのロードシェアリング機能が有効な場合にのみ機能します。
4. (オプション設定項目) セカンダリカウンティングサーバを指定する	**secondary accounting** { *host-name* | *ipv4-address* } [*port-number* | **key** { **cipher** | **simple** } *string* | **test-profile** *profile-name* | **weight** *weight-value*] *	デフォルト：設定なし weightキーワードは、RADIUSスキームでRADIUSサーバのロードシェアリング機能が有効な場合にのみ機能します。

3.3.5 セキュアな RADIUS 通信のための共有キーの指定

RADIUS クライアントおよびサーバは、MD 5 アルゴリズムと共有キーを使用して、パケット認証および view ザパスワード暗号化のためのオーセンティケータ値を生成します。クライアントとサーバは、通信の種類ごとに同じキーを使用する必要があります。

このタスクで設定されるキーは、スキーム内の同じ種類 (アカウンティングまたは認証) のすべてのサーバ用です。キーの優先順位は、RADIUS サーバ用に個別に設定されたキーよりも低くなります。

I. 制限事項とガイドライン

デバイスに設定されている共有キーは、RADIUS サーバに設定されている共有キーと同じである必要があります。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―

操作	コマンド	補足
2． RADIUS スキーム view に移行する	**radius scheme** *radius-scheme-name*	—
3． 共有キーを設定する	**key** { **accounting** | **authentication** } { **cipher** | **simple** } *string*	デフォルト：設定なし

3.3.6 RADIUS サーバのステータスの設定

現在のサーバが使用できなくなったときにデバイスが通信する RADIUS サーバを制御するには、RADIUS サーバのステータスをブロックまたはアクティブに設定します。1 つのプライマリ RADIUS サーバと複数のセカンダリ RADIUS サーバを指定できます。セカンダリサーバは、プライマリサーバのバックアップとして機能します。

RADIUS サーバのロードシェアリング機能が有効になっている場合、デバイスは次のルールに基づいてサーバを選択します。

- デバイスは、すべてのアクティブなサーバの重み値と現在のユーザ数を確認し、サーバの重みとユーザ数の情報に基づいてアクティブなサーバを選択します。
- 使用中のサーバを認証または開始アカウンティングプロセス中に変更または削除した後に到達不能になった場合、デバイスは次の操作を実行します。
  a. サーバとの通信がタイムアウトになると、デバイスはすべてのアクティブサーバの重み値と現在のユーザ数をチェックして、別のアクティブサーバを選択します。
  b. デバイスは、選択したサーバとの通信を試みます。
- デバイスがオンラインユーザの開始アカウンティング要求を正常に送信したアカウンティングサーバを削除すると、そのオンラインユーザのリアルタイムアカウンティングは失敗します。その理由は、デバイスがそのオンラインユーザの開始アカウンティング要求を正常に送信したアカウンティングサーバとだけ通信できるためです。

RADIUS サーバのロードシェアリング機能が無効になっている場合、デバイスは次のルールに基づいてサーバを選択します。

- プライマリサーバがアクティブ状態の場合、デバイスは最初にプライマリサーバとの通信を試みます。プライマリサーバに到達できない場合、デバイスはサーバが設定されている順序でアクティブなセカンダリサーバを検索します。
- 1 つ以上のサーバがアクティブ状態の場合、サーバが使用できない場合でも、デバイスはこれらのアクティブなサーバとの通信だけを試みます。
- すべてのサーバがブロック状態の場合、デバイスはプライマリサーバとの通信だけを試みます。
- サーバに到達できない場合、デバイスは次の操作を実行します。
  - □ サーバのステータスをブロックに変更します。
  - □ サーバのクワイエットタイマを開始します。
  - □ 優先順位が最も高いアクティブ状態の次のセカンダリサーバとの通信を試みます。
- サーバのクワイエットタイマの期限が切れるか、サーバを手動でアクティブ状態に設定すると、サーバのステータスはアクティブに戻ります。デバイスは、認証またはアカウンティングプロセス中に再度サーバをチェックしません。
- デバイスが使用可能なセカンダリサーバを見つけるか、アクティブ状態のすべてのセカンダリサーバをチェックするまで、検索プロセスは続行されます。到達可能なサーバがない場合、認証またはアカウンティングは失敗します。
- デバイスは、このセクションのサーバ選択ルールに従って、新しいユーザの認証またはアカウンティングに到達可能なサーバを選択します。ただし、**reauthentication server-select inherit** コマンドを使用して、再認証用の RADIUS サーバ選択モードが

継承するように設定されている場合、これらのルールはオンラインユーザの再認証には適用されません。

- 使用中の 1 つのサーバを削除してそのサーバに到達できなくなった場合、デバイスは元のサーバとの通信がタイムアウトしたときにアクティブ状態の別のサーバを探します。デバイスは最初にプライマリサーバをチェックし、次に設定されている順序でセカンダリサーバをチェックします。
- RADIUS サーバのステータスが自動的に変更されると、デバイスは、このサーバが指定されているすべての RADIUS スキームで、このサーバのステータスをそれに応じて変更します。
- RADIUS サーバが手動でブロックに設定されている場合、サーバにテストプロファイルが指定されているかどうかに関係なく、サーバのサーバ検出は無効になります。RADIUS サーバがアクティブ状態に設定されている場合、既存のテストプロファイルが指定されているサーバのサーバ検出が有効になります。

デフォルトでは、デバイスはすべての RADIUS サーバのステータスをアクティブに設定します。ただし、状況によっては、サーバのステータスを変更する必要があります。たとえば、サーバに障害が発生した場合、サーバへの通信試行を回避するために、サーバのステータスをブロックに変更できます。

I. 制限事項とガイドライン

設定されたサーバステータスはどの設定ファイルにも保存できず、**display radius scheme** コマンドを使用しないと表示できません。

デバイスの再起動後、すべてのサーバがアクティブ状態に復元されます。

II. 設定手順

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． RADIUS スキーム view に移行する	**radius scheme** *radius-scheme-name*	—
3． RADIUS サーバのステータスを設定する	プライマリRADIUS認証サーバのステータスを設定する **state primary authentication** { **active** | **block** }	デフォルト：active
	プライマリRADIUSアカウンティングサーバのステータスを設定する **state primary accounting** { **active** | **block** }	
	セカンダリRADIUS認証サーバのステータスを設定する **state secondary authentication** [{ *host-name* | *ipv4-address* } [*port-number*]] { **active** | **block** }	
	セカンダリRADIUSアカウンティングサーバのステータスを設定する **state secondary accounting** [{ *host-name* | *ipv4-address* } [*port-number*]] { **active** | **block** }	

3.3.7 RADIUS タイマの設定

デバイスは、次のタイプのタイマを使用して RADIUS サーバとの通信を制御します。

- サーバ応答タイムアウトタイマ (応答タイムアウト) :RADIUS 要求の再送信間隔を定義します。このタイマは、RADIUS 要求の送信直後に開始されます。タイマが切れる前にデバイスが RADIUS サーバからの応答を受信しない場合は、要求を再送信します。
- Server quiet timer (quiet) :到達不能なサーバをブロック状態に維持する期間を定義します。あるサーバに到達できない場合、デバイスはサーバのステータスをブロック状態に変更し、サーバのこのタイマを開始して、アクティブ状態の別のサーバとの通信を試みます。サーバのクワイエットタイマの期限が切れると、デバイスはサーバのステータスをアクティブに戻します。
- リアルタイムアカウンティングタイマ (realtime-accounting) :デバイスがオンラインユーザの RADIUS アカウンティングサーバにリアルタイムアカウンティングパケットを送信する間隔を定義します。

I. 制限事項とガイドライン

RADIUS パケット送信の最大試行回数と RADIUS サーバ応答タイムアウトタイマを設定する場合は、セカンダリサーバの数を考慮します。RADIUS スキームに多数のセカンダリサーバが含まれている場合、再送信プロセスが長すぎる可能性があり、Telnet などのアクセスモジュール内のクライアント接続がタイムアウトする可能性があります。

クライアント接続のタイムアウト期間が短い場合、多数のセカンダリサーバによって初期認証またはアカウンティングの試行が失敗する可能性があります。この場合、RADIUS パケット送信試行とサーバ応答タイムアウトタイマを調整するのではなく、クライアントを再接続します。通常、デバイスが到達不能なサーバをブロックし、到達可能なサーバを見つける時間を短縮したため、次の試行は成功します。

サーバのクワイエットタイマが正しく設定されていることを確認します。タイマが短すぎると、認証またはアカウンティングの失敗が頻繁に発生する可能性があります。これは、デバイスがアクティブ状態の到達不能なサーバとの通信を試行し続けるためです。タイマが長すぎると、障害から回復した到達可能なサーバが一時的にブロックされることがあります。これは、タイマの期限が切れるまで、サーバがブロック状態のままになるためです。

リアルタイムの短いアカウンティング間隔は、アカウンティングの精度を向上させるのに役立ちますが、多くのシステムリソースを必要とします。1000 人以上のユーザがいる場合は、間隔を 15 分以上に設定します。

II. 設定手順

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． RADIUS スキーム view に移行する	**radius scheme** *radius-scheme-name*	—
3． 必要に応じて、RADIUS タイマを設定する	RADIUSサーバの応答タイムアウトタイマを設定する **timer response-timeout** *seconds*	デフォルト：3秒
	サーバのサイレントタイマを設定する **timer quiet** *minutes*	デフォルト：5分

操作	コマンド	補足
	リアルタイムアカウンティングタイマを設定する **timer realtime-accounting interval** [*second*]	デフォルト：12分

3.3.8 ユーザ名形式とトラフィック統計情報単位の設定

ユーザ名は userid@isp-name 形式で、isp-name 部分はユーザの ISP ドメイン名を表します。デフォルトでは、ISP ドメイン名はユーザ名に含まれます。ただし、古い RADIUS サーバでは、ISP ドメイン名を含むユーザ名が認識されない場合があります。この場合、送信する各ユーザ名のドメイン名を削除するようにデバイスを設定できます。

デバイスは、オンラインユーザトラフィック統計情報をアカウンティングパケットで報告します。トラフィック測定単位は設定可能です。

I. 制約事項とガイドライン

2 つ以上の ISP ドメインが同じ RADIUS スキームを使用する場合は、ドメイン識別のために ISP ドメイン名をユーザ名に保持するように RADIUS スキームを設定します。

アカウンティングの精度を高めるには、デバイスと RADIUS アカウンティングサーバに設定されているトラフィック統計情報の単位が同じであることを確認します。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. RADIUS スキーム view に移行する	**radius scheme** *radius-scheme-name*	—
3. RADIUS サーバに送信するユーザ名の形式を設定する	**user-name-format** { **keep-original** | **with-domain** | **without-domain** }	デフォルト：with-domain
4. トラフィック統計情報のデータフローおよびパケット測定単位を設定する	**data-flow-format** { **data** { **byte** | **giga-byte** | **kilo-byte** | **mega-byte** } | **packet** { **giga-packet** | **kilo-packet** | **mega-packet** | **one-packet** } }*	デフォルト：byte と packet

3.3.9 RADIUS 要求送信の最大試行回数の設定

RADIUS は UDP パケットを使用してデータを転送します。UDP 通信は信頼できないため、RADIUS は信頼性を向上させるために再送信メカニズムを使用します。NAS が応答タイムアウトタイマ内に要求に対するサーバ応答を受信しない場合、RADIUS 要求は再送信されます。RADIUS サーバの応答タイムアウトタイマの詳細については、本章の“*RADIUS サーバのステータスの設定*“ を参照してください。

NAS が同じサーバに RADIUS 要求を再送信する最大数を設定できます。最大数に達すると、NAS はアクティブ状態の他の RADIUS サーバとの通信を試みます。その時点でアク

ティブ状態の他のサーバがない場合、NAS は認証またはアカウンティングの試行が失敗したと見なします。

I. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. RADIUS スキーム view に移行する	**radius scheme** *radius-scheme-name*	―
3. RADIUS 要求送信の最大試行回数を設定する	**retry** *retries*	デフォルト：3回

3.3.10 リアルタイムアカウンティングの最大試行回数の設定

リアルタイムアカウンティングの最大試行回数を設定すると、デバイスは、許可された試行の範囲内でアカウンティング応答を受信しなかったユーザを切断します。

I. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. RADIUS スキーム view に移行する	**radius scheme** *radius-scheme-name*	―
3. リアルタイムアカウンティングの最大試行回数を設定する	**retry realtime-accounting** *retries*	デフォルト：5回

3.3.11 RADIUS パケットの DSCP 優先度の設定

IPv4 パケットの ToS フィールド優先度によって、RADIUS パケットの送信優先度が決まります。値が大きいほど、優先度が高くなります。

I. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
1. RADIUS パケットの DSCP 優先度を設定する	**radius dscp** *dscp-value*	デフォルト：0

3.3.12 RADIUS パケットの NAS IP アドレスの指定

RADIUS サーバ上のデバイスを一意に識別する NAS IP アドレスを指定するには、次の作業を実行します。デバイスは、発信 RADIUS 要求の NAS-IP-Address に、指定された NAS IP アドレスを設定します。

また、NAS は、指定された NAS IP アドレスを使用して、着信 RADIUS DAE パケット内の NAS IP アドレスと照合し、ユーザ照合を行います。

I. NAS IP アドレス設定の制約事項とガイドライン

NAS IP アドレスは、RADIUS スキーム view とシステム view の両方で指定できます。

- RADIUS スキーム view で **nas-ip** コマンドを使用して指定した NAS IP アドレスは、RADIUS スキームにのみ適用されます。
- システム view で **radius nas-ip** コマンドを使用して指定した NAS IP アドレスは、すべての RADIUS スキームに適用されます。
- RADIUS スキーム view で指定した NAS IP アドレスは、システム view で指定した NAS IP アドレスよりも優先されます。

発信 RADIUS パケットの NAS IP アドレスを直接指定することも、発信 RADIUS パケットの NAS IP アドレスを提供するインタフェースを指定することもできます。インタフェース設定と IP アドレス設定は互いに上書きされます。

II. システム view での RADIUS パケットの NAS IP アドレスの指定

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. RADIUS パケットの NAS IP アドレスを設定する	**radius nas-ip** { **interface** *interface-type interface-number* | { **ipv4-address** } }	デフォルト : 発信するインタフェースのプライマリIPv4アドレス

III. RADIUS スキーム view での RADIUS パケットの NAS IP アドレスの指定

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. RADIUS スキーム view に移行する	**radius scheme** *radius-scheme-name*	ー
3. RADIUS パケットの NAS IP アドレスを設定する	**nas-ip** { *ipv4-address* | *interface* }	デフォルト :

3.3.13 属性 Acct-Session-Id の形式の指定

種類の異なる RADIUS サーバでは、属性 Acct-Session-Id の形式の要件が異なる場合があります。次の種類を使用できます。

- Common—この形式では、Acct-Session-Id 属性は 38 文字以上の文字列です。この文字列には、アクセスタイプを示すプレフィックス、日付と時刻、シーケンス番号、アクセスノードの LIP アドレス、デバイス ID、およびアクセスプロセスのジョブ ID が含まれます。
- Simplified—:この形式では、Acct-Session-Id 属性は 16 文字の文字列です。この文字列には、アクセスノードのプレフィックス (アクセスタイプを示す) 、月、シーケンス番号、デバイス ID、および LIP アドレスが含まれます。

RADIUS サーバの要件を満たすために、属性 Acct-Session-Id の形式を指定します。

I. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. 属性 Acct-Session-Id の形式を指定する	**aaa session-id mode** { **common** | **simplified** }	デフォルト：common

3.3.14 すべての RADIUS サーバがブロックされた場合に AAA 要求に対して実行するアクションの指定

RADIUS スキーム内のすべてのサーバがブロックされている場合、デバイスは、そのスキームを使用するドメインで AAA 要求を受信すると、次のいずれかのアクションを実行します。

- attempt:スキーム内のサーバへの接続を試みます。RADIUS サーバ選択メカニズムの詳細については、 本章の“RADIUSサーバのステータスの設定“を参照してください。
- skip:スキーム内のすべてのサーバをスキップし、バックアップ方式に切り替えます。

試行アクションは、スキーム内で最も優先度の高いサーバが使用可能な場合に備えて、デバイスにスキームを使用する機会を与えます。ただし、使用できないサーバと通信しようとすると、AAA 要求の応答時間が長くなります。ベストプラクティスとして、AAA 要求への迅速な応答が必要なシナリオでは、skip アクションを指定します。

I. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. RADIUS スキーム view に移行する	**radius scheme** *radius-scheme-name*	ー
3. スキーム内のすべてのサーバがブロックされた場合に AAA 要求に対して実行するアクションを指定する	**server-block-action** { **attempt** | **skip** }	デフォルト：attempt

3.3.15 RADIUS ストップアカウンティングパケットバッファリングの設定

デバイスは、ホストからの接続ティアダウン要求または管理者からの接続ティアダウンコマンドを受信すると、RADIUS ストップアカウンティング要求を送信します。ただし、デバイスは 1 回の送信でストップアカウンティング要求に対する応答を受信できない場合があります。デバイスが、アカウンティングサーバから応答を受信していない RADIUS ストップアカウンティング要求をバッファリングできるようにします。デバイスは、応答を受信するまで要求を再送信します。

送信時間を制限するには、個々の RADIUS ストップアカウンティング要求に対して実行できる最大送信試行回数を設定します。要求に対して最大試行が行われると、デバイスはバッファされた要求を破棄します。

I. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. RADIUS スキーム view に移行する	**radius scheme** *radius-scheme-name*	―
3. 応答を受信していない RADIUS stop-accounting 要求のバッファリングを有効にする	**stop-accounting-buffer enable**	デフォルト：有効
4. (オプション設定項目) 個々の RADIUS ストップアカウンティング要求の最大送信試行回数を設定する	**retry stop-accounting** *retries*	デフォルト：500

3.3.16 再認証のための RADIUS サーバ選択モードの指定

この機能を使用して、再認証での RADIUS サーバ選択メカニズムを設定します。次の RADIUS サーバ選択モードを使用できます。

- Inherit:デバイスは、ユーザの認証を実行した RADIUS サーバを使用して、そのユーザを再認証します。このモードでは、再認証に使用される時間が短縮されます。ただし、RADIUS サーバに到達できない場合、再認証は失敗します。
- Reselect:デバイスは、ユーザを再認証するために到達可能な RADIUS サーバを検索します。このモードでは、継承モードよりも時間がかかります。ただし、このモードでは、デバイスは再認証に最適な到達可能な RADIUS サーバを使用します。RADIUS サーバの選択には、次の要因が影響します。
  - 設定順序を含む、RADIUS スキームのサーバ設定
  - RADIUS サーバのロードシェアリング機能のステータス
  - RADIUS スキームの RADIUS サーバのステータス

I. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. RADIUS スキーム view に移行する	**radius scheme** *radius-scheme-name*	―
3. 再認証する RADIUS サーバの選択モードを指定する	**reauthentication server-select** { **inherit** | **reselect** }	デフォルト：inherit

3.3.17 RADIUS アカウンティング機能の設定

accounting-on 機能を有効にすると、デバイス全体の再起動後に、デバイスは自動的に accounting-on パケットを RADIUS サーバに送信します。accounting-on パケットを受信すると、RADIUS サーバはすべてのオンラインユーザをログアウトし、デバイスを介して再度ログインできるようにします。この機能がないと、ユーザは再起動後に再度ログインできません。これは、RADIUS サーバによってオンラインになったと見なされるためです。

デバイスが accounting-on パケットの再送信を待機する間隔と最大再試行回数を設定できます。

I. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. RADIUS スキーム view に移行する	**radius scheme** *radius-scheme-name*	―
3. accounting-on を有効にする	**accounting-on enable** [**interval** *interval* | **send** *send-times*] *	デフォルト：無効

3.3.18 RADIUS の SNMP 通知の有効化

RADIUS に対して SNMP 通知が有効になっている場合、SNMP エージェントは RADIUS によって生成される次の通知をサポートします。

- RADIUS サーバ到達不能通知:RADIUS サーバに到達できません。RADIUS は、指定された RADIUS 要求の送信試行回数以内に、アカウンティング要求または認証要求に対する応答を受信しなかった場合に、この通知を生成します。
- RADIUS サーバ到達可能通知:RADIUS サーバに到達できます。RADIUS は、待機タイマの期限が切れた後、以前にブロックされた RADIUS サーバに対してこの通知を生成します。
- Excessive authentication failures notification:認証試行の合計数と比較した認証失敗の数が、指定されたしきい値を超えています。

RADIUS SNMP 通知を正しく送信するには、デバイスで SNMP を設定する必要があります。SNMP 設定の詳細については、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*17 ネットワーク管理と監視*”の” *4 章 SNMP*”を参照してください。

I. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. RADIUS の SNMP 通知を有効にする	**snmp-agent trap enable radius** [**accounting-server-down** | **accounting-server-up** | **authentication-error-threshold** | **authentication-server-down** | **authentication-server-up**] *	デフォルト：無効

3.3.19 RADIUS の確認とメンテナンス

すべての view で **display** コマンドを実行できます。

I. RADIUS スキーム設定の確認

操作	コマンド
すべてのRADIUSスキームまたは指定したRADIUSスキームの設定を表示する	**display radius scheme** [*radius-scheme-name*]

II. RADIUS 統計情報の表示とクリア

操作	コマンド
RADIUSパケット統計情報を表示する	**display radius statistics**
RADIUS統計情報をクリアする user viewでのみ実行可能	**reset radius statistics**

III. バッファされた RADIUS ストップアカウンティング要求に関する情報の表示とクリア

操作	コマンド
応答を受信していないバッファされたRADIUSストップアカウンティング要求に関する情報を表示する	**display stop-accounting-buffer** { **radius-scheme** *radius-scheme-name* | **session-id** *session-id* | **time-range** *start-time end-time* | **user-name** *user-name* }
応答を受信していないバッファ内のRADIUS stop-accounting要求をクリアする	**reset stop-accounting-buffer** { **radius-scheme** *radius-scheme-name* | **session-id** *session-id* | **time-range** *start-time end-time* | **user-name** *user-name* }

3.4 ISPドメインの作成

3.4.1 ISP ドメインについて

複数の ISP があるネットワークシナリオでは、デバイスは異なる ISP のユーザに接続できます。これらのユーザは、異なるユーザ名とパスワードの構造、異なるサービスタイプ、異なる権限など、異なるユーザ属性を持つことができます。異なる ISP のユーザを管理するには、必要に応じて各 ISP ドメインの認証、認可、およびアカウンティングの方法とドメイン属性を設定します。

デバイスは、システム定義の ISP ドメインシステムを含め、最大 1024 の ISP ドメインをサポートします。ISP ドメインのいずれかをデフォルトドメインとして指定できます。

デバイスでは、各ユーザは ISP ドメインに属しています。ユーザがログイン時に ISP ドメイン名を指定しなかった場合、デバイスはそのユーザがデフォルトの ISP ドメインに属していると見なします。

各 ISP ドメインには、システム定義の AAA 方式のセットがあります。これは、ローカル認証、ローカル認可、およびローカルアカウンティングです。ISP ドメインに AAA 方式

を設定しない場合、デバイスはドメイン内のユーザに対してシステム定義の AAA 方式を使用します。

デバイスは、次の順序で各ユーザの認証ドメインを選択します。

1) アクセスモジュールに指定された認証ドメイン
2) ユーザ名の ISP ドメイン
3) デバイスのデフォルトの ISP ドメイン

選択したドメインがデバイス上に存在しない場合、デバイスは存在しないドメインに割り当てられたユーザに対応する ISP ドメインを検索します。(認証ドメイン設定のサポートは、アクセスモジュールによって異なります)。ISP ドメインが設定されていない場合、ユーザ認証は失敗します。

3.4.2 ISP ドメイン設定の制約事項とガイドライン

ISP ドメインがデフォルトの ISP ドメインの場合は削除できません。**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、ドメインをデフォルト以外の ISP ドメインに変更します。

システム定義の ISP ドメインシステムの設定は変更できますが、ドメインを削除することはできません。

RADIUS の認証、認可、アカウンティングの失敗を回避するには、短いドメイン名を使用して、ドメイン名を含むユーザ名が 253 文字を超えないようにします。

RADIUS のアカウンティングの失敗を回避するには、RADIUS サーバに送信されるユーザ名に含まれるドメイン名が 247 文字を超えないようにします。

3.4.3 ISP ドメインの作成

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. ISP ドメインを作成し、ISP ドメイン view に移行する	**domain name isp-name** *domain isp-name*	デフォルト： ドメイン名 system設定済

3.4.4 デフォルトの ISP ドメインの指定

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. デフォルトの ISP ドメインを指定する	**domain default enable** *isp-name*	デフォルト： ドメイン名 system設定済

3.5 ISPドメイン属性の設定

3.5.1 ISP ドメインステータスの設定

ISP ドメインの状態を設定することで、ドメイン内のユーザからのネットワークサービス要求を許可または拒否できます。

- Active:デバイスはドメイン内のユーザからのネットワークサービス要求を許可します。
- Blocked:デバイスはドメイン内のユーザからのネットワークサービス要求を拒否します。特定の時間帯にユーザのネットワークサービス要求を拒否するには、指定した時間範囲内でドメインをブロック状態にするようにデバイスを設定できます。

I. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. ISP ドメイン view に移行する	**domain name** *isp-name*	—
3. ISP ドメインのステータスを設定する	**state** { **active** | **block** [**time-range**] [**offline**] }	デフォルト：active

3.6 ISPドメインのAAA方式の設定

3.6.1 ISP ドメインの認証方式の設定

I. 制限事項とガイドライン

認証を設定する場合は、次の制限事項とガイドラインに従ってください。

- 高可用性のために、1 つのプライマリ認証方式と複数のバックアップ認証方式を指定できます。プライマリ方式が無効な場合、デバイスはバックアップ方式を順番に使用しようとします。
- たとえば、**radius-scheme** *radius-scheme-name* **local none** パラメータは、プライマリ RADIUS 認証方式と 2 つのバックアップ方式 (ローカル認証と認証なし) を指定します。デバイスはデフォルトで RADIUS 認証を実行し、RADIUS サーバが無効な場合はローカル認証を実行します。デバイスは、前の方法が両方とも無効な場合は認証を実行しません。

リモート認証方法は、次の状況では無効です。

- 指定された認証スキームが存在しない
- 認証パケットの送信に失敗した
- デバイスで認証サーバからの認証応答パケットを受信しない

デバイス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、ローカル認証方式は無効になります。

- 認証方式が RADIUS スキームを使用し、認可方式が RADIUS スキームを使用しない場合、AAA は RADIUS サーバからの認証結果だけを受け入れます。RADIUS サーバ

からの Access-Accept メッセージにも認可情報が含まれますが、デバイスはその情報を無視します。

- RADIUS 方式が指定されている場合、デバイスは RADIUS サーバのユーザ名$enabn$をロール認証に使用します。
  - □ レベル n ユーザロールを取得するには、RADIUS サーバでレベル n ユーザロールのユーザアカウントを$enabn$形式で作成する必要があります。変数 n は、ターゲットユーザロールレベルを表します。
  - □ レベル n 以外のユーザロールを取得するには、次のタスクを実行する必要があります。
  - □ サーバに$enab 0$という名前のユーザアカウントを作成します。
  - □ アカウントの cisco-av-pair 属性を allowed-roles="role"の形式で設定します。変数 role は、ターゲットユーザロールを表します。

ユーザロール認証の詳細については、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*2 基本機能*”の”*2 章 RBAC*”を参照してください。

プライマリ認証方式がローカルの場合、ユーザの認証には次の規則が適用されます。

- デバイスは、次のいずれかの理由でローカル認証が無効な場合にのみ、バックアップ認証方式を順番に使用します。
  - □ ローカル認証プロセスで例外が発生します。
  - □ デバイスにユーザ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認証が無効な場合、デバイスはバックアップ認証方式に切り替えません。ユーザの認証に失敗しました。

II. 前提条件

認証方式を設定する前に、次のタスクを完了します。

1) 設定するアクセスタイプまたはサービスタイプを決定します。AAA では、アクセスタイプとサービスタイプごとに認証方式を設定できます。
2) すべてのアクセスタイプまたはサービスタイプのデフォルト認証方式を設定するかどうかを決定します。デフォルト認証方式は、すべてのアクセスユーザに適用されます。ただし、この方式は、アクセスタイプまたはサービスタイプに指定されている認証方式よりも優先度が低くなります。

III. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. ISP ドメイン view に移行する	**domain name** *isp-name*	—
3. (オプション設定項目) すべてのタイプのユーザのデフォルト認証方式を指定する	**authentication default** { **radius-scheme** *radius-scheme-name* [**local**] [**none**] | [**local**] [**none**] | **local** [**radius-scheme** *radius-scheme-name*] * [**none**] | **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }	デフォルト：**local**

操作	コマンド	補足
4. ユーザタイプまたはサービスの認証方式を指定する	・ネットワークアクセスユーザの認証方式を指定します。 **authentication lan-access** { **radius-scheme** *radius-scheme-name* [**local**] [**none**] | | **local** | **radius-scheme** *radius-scheme-name*] * [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] } ・ログインユーザの認証方式を指定します。 **authentication login** { **radius-scheme** **radius-scheme-name** [**local**] [**none**] | | **local** | **radius-scheme** *radius-scheme-name*] * [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }	デフォルト : デフォルトの認証方式

3.6.2 ISP ドメインの認可方式の設定

I. 制約事項とガイドライン

高可用性のために、1 つのプライマリ認可方式と複数のバックアップ認可方式を指定できます。プライマリ方式が無効な場合、デバイスはバックアップ方式を順番に使用しようとします。たとえば、**radius-scheme** *radius-scheme-name* **local none** パラメータは、プライマリ RADIUS 許可方式と 2 つのバックアップ方式 (ローカル許可と無許可) を指定します。デバイスはデフォルトで RADIUS 許可を実行し、RADIUS サーバが無効な場合はローカル許可を実行します。デバイスは、上記の両方の方法が無効な場合は許可を実行しません。

リモート許可方法は、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。
- 認可パケットの送信に失敗します。
- デバイスは、認可サーバから認可応答パケットを受信しません。

デバイス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、ローカル認可方式は無効になります。

RADIUS スキームを認可方式として使用するには、ISP ドメインの認証方式として設定されている RADIUS スキームの名前を指定します。認可方式として無効な RADIUS スキームを指定した場合、RADIUS の認証および認可は失敗します。

プライマリ認可方式がローカルの場合、ユーザの認可には次の規則が適用されます。

- デバイスは、次のいずれかの理由でローカル認可が無効な場合にのみ、バックアップ認可方式を順番に使用します。
  - □ ローカル認可プロセスで例外が発生します。
  - □ デバイスでユーザ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認証が無効な場合、デバイスはバックアップ認証方式に切り替えません。ユーザの認可が失敗します。

II. 前提条件

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. ISP ドメイン view に移行する	**domain name** *isp-name*	ー
3. (オプション設定項目) すべてのタイプのユーザのデフォルト認可方式を指定する	**authorization default** { **radius-scheme** *radius-scheme-name* [**local**] [**none**] | | **local** [**radius-scheme** *radius-scheme-name*] * [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }	デフォルト：local
4. ユーザタイプまたはサービスの認可方式を指定する	・ネットワークアクセスユーザの認可方式を指定します。 **authorization lan-access** { **radius-scheme** *radius-scheme-name* [**local**] [**none**] | | **local** | **radius-scheme** *radius-scheme-name*] * [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] } ・ログインユーザの認可方式を指定します。 **authorization login** { **radius-scheme** *radius-scheme-name* [**local**] [**none**] | | **local** | **radius-scheme** *radius-scheme-name*] * [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }	デフォルト : デフォルトの認証方式

3.6.3 ISP ドメインのアカウンティング方式の設定

I. 制限事項とガイドライン

高可用性のために、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アカウンティング方式を指定できます。プライマリ方式が無効な場合、デバイスはバックアップ方式を順番に使用しようとします。たとえば、**radius-scheme** *radius-scheme-name* **local none** パラメータは、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とノーアカウンティング) を指定します。デバイスはデフォルトで RADIUS アカウンティングを実行し、RADIUS サーバが無効な場合はローカルアカウンティングを実行します。デバイスは、前述の両方の方法が無効な場合はアカウンティングを実行しません。

リモートアカウンティングの方法は、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す。
- デバイスは、アカウンティングサーバからのアカウンティング応答パケットを受信しません。

デバイス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。

FTP、SFTP、および SCP ユーザは、アカウンティングをサポートしていません。

ローカルアカウンティングでは、課金の統計情報は提供されません。同じローカルユーザアカウントを使用する同時ユーザの数をカウントおよび制御するだけです。しきい値は、**access-limit** コマンドを使用して設定します。

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。

- デバイスは、次のいずれかの理由でローカルアカウンティングが無効な場合にのみ、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す。
  - □ デバイスでユーザ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。

II. 前提条件

アカウンティング方式を設定する前に、次のタスクを完了します。

1) 設定するアクセスタイプまたはサービスタイプを決定します。AAA では、アクセスタイプとサービスタイプごとにアカウンティング方式を設定できます。
2) すべてのアクセスタイプまたはサービスタイプに対してデフォルトのアカウンティング方式を設定するかどうかを決定します。デフォルトのアカウンティング方式は、すべてのアクセスユーザに適用されます。ただし、この方式は、アクセスタイプまたはサービスタイプに指定されているアカウンティング方式よりも優先度が低くなります。

III. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. ISP ドメイン view に移行する	**domain name** *isp-name*	―
3. (オプション設定項目) すべてのタイプのユーザのデフォルトのアカウンティング方式を指定する	**accounting default** { **radius-scheme** *radius-scheme-name* [**local**] [**none**] | **local** [**radius-scheme** *radius-scheme-name*] * [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }	デフォルト：local

操作	コマンド	補足
4. ユーザタイプのアカウンティング方式を指定する	・ネットワークアクセスユーザのアカウンティング方式を指定します。 **accounting lan-access** { **radius-scheme** *radius-scheme-name* [**local**] [**none**] | | **local** | **radius-scheme** *radius-scheme-name*] * [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] } ・ログインユーザのアカウンティング方式を指定する **accounting login** { **radius-scheme** *radius-scheme-name* [**local**] [**none**] | **local** [**radius-scheme** *radius-scheme-name*] * [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }	デフォルト : デフォルトのアカウンティング方式

3.6.4 ISP ドメインの検証とメンテナンス

すべての view で **display** コマンドを実行できます。

操作	コマンド
ISPドメインまたはすべてのISPドメインに関する設定情報を表示する	**display domain [** *isp-name* **]**

3.7 同時ログインユーザの最大数の設定

認証方法に関係なく、特定のプロトコルを使用してデバイスにログオンできる同時ユーザの最大数を設定するには、次の作業を実行します。認証方法には、認証なし、ローカル認証、リモート認証があります。

I. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
1. 同時ログインユーザの最大数を設定する	**aaa session-limit** { **ftp** | **http** | **https** | **ssh** | **telnet** } *max-sessions*	デフォルト：32

3.8 NAS-IDの設定

3.8.1 NAS-ID について

RADIUS 認証中、デバイスは NAS-ID を使用して RADIUS パケットの NAS-Identifier 属性を設定し、RADIUS サーバがユーザのアクセス場所を識別できるようにします。

NAS-ID は複数の view で設定できます。デバイスは、次の順序で NAS-Identifier 属性の NAS-ID を選択します。

1) NAS-ID プロファイル view で VLAN にバインドされた NAS-ID
2) ISP ドメイン view での NAS-ID

NAS-ID が設定されていない場合、デバイスはデバイス名 (**sysname** コマンドを使用して設定) を NAS-ID として使用します。

3.8.2 ISP ドメインでの NAS-ID の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. ISP ドメイン view に移行する	**domain name** *isp-name*	―
3. ISP ドメインの NAS-ID を設定する	**aaa nas-id** *nas-identifier*	デフォルト：設定なし

3.9 パスワード変更プロンプトのログ記録の有効化

この機能を使用して、Telnet、SSH、HTTP、HTTPS、NETCONF over SSH、および NETCONF over SOAP ユーザのパスワードの保護を強化し、システムセキュリティを向上させます。

この機能を使用すると、デバイスでログを生成して、ユーザのログイン時に 24 時間間隔で弱いパスワードを変更するようにユーザに促すことができます。

パスワードは、次の要件を満たさない場合に弱いパスワードとなります。

- **password-control composition** コマンドを使用して設定されたパスワード構成制限。
- **password-control length** コマンドを使用して設定されたパスワードの最小長制限。
- **password-control complexity** コマンドを使用して設定されたパスワード複雑性チェックポリシ。

NETCONF over SSH または NETCONF over SOAP ユーザの場合、次のいずれかの条件が存在すると、デバイスはパスワード変更のプロンプトログも生成します。

- ユーザの現在のパスワードがデフォルトのパスワードであるか、有効期限が切れています。
- ユーザは、初めてデバイスにログインするか、グローバルパスワード制御が有効になった後に新しいパスワードを使用してログインします。

次のいずれかの条件が存在する場合、デバイスはユーザのパスワード変更プロンプトログを生成しなくなります。

- パスワード変更プロンプトログ機能は無効になっています。
- ユーザがパスワードを変更し、新しいパスワードがパスワード制御要件を満たしている。
- 関連するパスワード制御機能の有効化ステータスが変更され、ユーザの現在のパスワードがパスワード制御要件を満たしている。
- パスワード構成ポリシまたはパスワードの最小長が変更されました。

I. 制限事項とガイドライン

パスワード制御の設定を表示するには、**display password-control** コマンドを使用します。パスワード制御コマンドの詳細については、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*15 セキュリティ*”の”*3 章 パスワード管理*”を参照してください。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. パスワード変更プロンプトのログを有効にする	**local-server log change-password-prompt**	デフォルト：有効

3.10 EAPプロファイルの設定

🕮 **メモ：**

この機能は、ソフトウェアバージョン 9.6.08c を含む以降のソフトウェアからサポートしています。

3.10.1 EAP プロファイルの概要

EAP プロファイルは、EAP 認証方式や一部の EAP 認証方式で使用する CA 証明書ファイルなど、EAP 認証設定をまとめたものです。

3.10.2 EAP プロファイルの制約事項とガイドライン

RADIUS サーバステータス検出のために、複数のテストプロファイルで EAP プロファイルを指定できます。

システムは最大 16 個の EAP プロファイルをサポートします。

本装置は複数の EAP 認証方式をサポートしています。装置がピアに認証要求を開始する際、EAP プロファイル内のデフォルトの EAP 認証方式を優先的に使用します。ピアが異なる EAP 認証方式を使用する場合は、サポートされている EAP 認証方式を装置に通知します。装置はローカルとピアの両方でサポートされている方式を選択し、認証要求を再度開始します。

3.10.3 EAP プロファイルの前提条件

ローカル証明書、秘密鍵、または CA 証明書を指定する前に、FTP または TFTP を使用して対応するファイルをデバイスのデフォルトストレージメディアのルートディレクトリに転送してください。クラウドクラスターの場合、ファイルを指定する前に、各メンバーデバイスのデフォルトストレージメディアのルートディレクトリにファイルが存在することを確認してください。

3.10.4 EAP プロファイルの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. EAP プロファイルを作成し、EAP プロファイル view に移行する	**eap-profile** *eap-profile-name*	ー
3. デフォルトの EAP 認証方式を設定する	**method** { **md5** | **peap-mschapv2** | **ttls-mschapv2** }	デフォルト：md5
4. EAP 認証用のローカル証明書ファイルを設定する	**certificate-file** *file-name*	デフォルト：設定なし
5. 秘密鍵ファイルを設定する	**private-key-file** *file-name*	デフォルト：設定なし
6. ローカル証明書の秘密鍵パスワードを設定する	**private-key-password** { **cipher** | **simple** } *string*	デフォルト：設定なし
7. EAP 認証用の CA 証明書ファイルを設定する	**ca-file** *file-name*	デフォルト：設定なし

3.11 RADIUSサーバ機能の設定

🕮 **メモ：**
この機能は、ソフトウェアバージョン 9.6.08c を含む以降のソフトウェアからサポートしています。

3.11.1 RADIUS サーバ機能のタスク一覧

RADIUS サーバを設定するには、次のタスクを実行します。

操作	補足
RADIUSユーザの設定	
RADIUSクライアントの指定	
EAP認証の設定	
RADIUSサーバ設定の有効化	
(オプション設定項目) RADIUSサーバ設定の無効化	

3.11.2 RADIUS ユーザの設定

RADIUS サーバ機能が動作開始すると、デバイスはネットワークアクセスユーザ情報に基づいて RADIUS ユーザを作成します。ネットワークアクセスユーザが削除されると、対応する RADIUS ユーザは最新の RADIUS サーバ設定が反映された後で削除されます。

RADIUS ユーザを設定するには、RADIUS ユーザデータの基礎となるネットワークアクセスユーザを設定する必要があります。RADIUS ユーザには、ユーザ名、パスワード、認可 ACL、認可 VLAN、有効期限という属性があります。

🕮 **メモ：**

認可 ACL、有効期限の設定はサポートしていません。

I. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. ネットワークアクセスユーザ view に移行する	**local-user** *user-name* [**class network**]	—
3. ネットワークアクセスユーザのパスワードを設定する	**password** { **cipher** | **simple** } *string*	—
4. (オプション設定項目) ネットワークアクセスユーザの説明を設定	**description** *text*	デフォルト：設定なし
5. (オプション設定項目) ネットワークアクセスユーザの認可属性を設定する	**authorization-attribute** { **acl** *acl-number* | **session-timeout** *minutes* | **vlan** *vlan-id* } *	デフォルト：設定なし 認可属性なし

3.11.3 RADIUS クライアントの指定

集中管理のために RADIUS クライアントと共有キーを指定してください。RADIUS サーバ機能は、システムによって管理されていない RADIUS クライアントからのリクエストを受け付けません。

I. 制約事項とガイドライン

RADIUS クライアントの IP アドレスは、RADIUS クライアントで指定された送信元 RADIUS パケットの IP アドレスと同じでなければなりません。

詳細は、「3.3.12 RADIUSパケットのNAS IPアドレスの指定」を参照してください。

RADIUS サーバで指定された RADIUS クライアントの共有キーは、RADIUS クライアント側の設定と同じでなければなりません。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—

操作	コマンド	補足
2. Radius クライアントを指定する	**radius-server client ip** *ipv4-address* **key** { **cipher** | **simple** } *string*	デフォルト：設定なし

3.11.4 EAP 認証の設定

EAP 認証に使用する EAP プロファイルを指定します。起動後、RADIUS サーバは指定された EAP プロファイルを使用して RADIUS クライアントとやり取りします。

I. 制約事項とガイドライン

RADIUS サーバは、以下の EAP 認証方式をサポートしています。

- MD5-Challenge
- PEAP-MSCHAPv2
- TTLS-MSCHAPv2

最大 16 個の EAP プロファイルを作成できます。

🕮 **メモ：**

PEAP-GTC、TTLS-GTC、EAP-TLS での EAP 認証方式はサポートしていません。

II. 前提条件

RADIUS サーバで EAP プロファイルを指定する前に、EAP プロファイルの設定を完了してください。詳細については「EAP プロファイルの設定」を参照してください。

III. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. RADIUS サーバに対して EAP プロファイルを指定する	**radius-server eap-profile** *eap-profile-name*	デフォルト：設定なし

3.11.5 RADIUS サーバ設定の有効化

RADIUS サーバ機能は、デバイス起動時に RADIUS クライアント、RADIUS ユーザ、EAP プロファイルを含む RADIUS サーバ設定を反映した状態で自動的に有効となります。

次のいずれかの操作を行った場合は、最新の RADIUS サーバ設定を反映するため、RADIUS サーバ設定の有効化を実行してください。

- RADIUS クライアントまたは RADIUS ユーザの追加、変更、削除を行う。
- RADIUS サーバに指定された EAP プロファイルを変更する。

最新の RADIUS サーバ設定を有効化するまでは、変更した内容が反映されません。

I. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. RADIUS サーバの設定を有効化する	**radius-server activate**	—

3.11.6 RADIUS サーバ設定の無効化

本操作によってすべての RADIUS サーバ設定と、RADIUS サーバ機能が無効化されます。RADIUS サーバ機能を無効にすると、デバイスは RADIUS サーバとして RADIUS ユーザへの認証サービスを提供できなくなります。

I. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. RADIUS サーバ設定を無効化し、RADIUS サーバ機能を無効にする	**radius-server deactivate**	—

3.11.7 RADIUS サーバ機能の確認とメンテナンス

すべての view で **display** コマンドを実行できます。

操作	コマンド
アクティブなRADIUSクライアントに関する情報を表示します。	**display radius-server active-client**
アクティブなEAPプロファイルに関する情報を表示します。	**display radius-server active-eap-profile**
アクティブなRADIUSユーザに関する情報を表示します。	**display radius-server active-user** [*user-name*]

3.12 AAAの設定例

3.12.1 802.1X EAP-PEAP 認証を RADIUS サーバとして機能する AC で構成する

I. ネットワーク要件

図 3-7に示すように AC と AP は L2 スイッチを介して接続されています。

AC は Radius サーバ機能と Radius クライアント機能の両方を提供し、EAP-PEAP 方式を使用して、ワイヤレスクライアントに対して 802.1X 認証を行います。

管理 AP のサービステンプレートにおける認証装置は AC です。

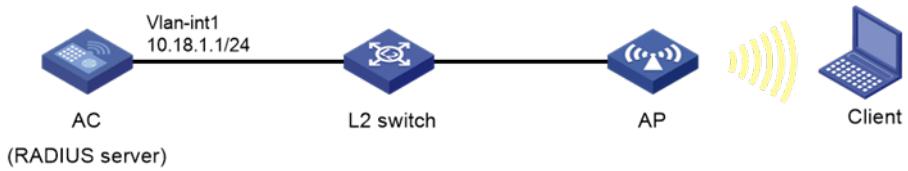


図 3-7 ネットワーク構成

II. 設定手順

CA 証明書ファイルとサーバ証明書ファイル、秘密鍵ファイルは、FTP などを使用してあらかじめ AC に保存しておく必要があります。

本設定例では、AC に CA 証明書ファイル(ca.pem)、サーバ証明書ファイル(server.pem)、秘密鍵ファイル(server-key.pem)、を事前に保存済。秘密鍵のパスワードは(whatever)とします。

端末には、CA 証明書をインストールしておく必要があります。

1. AC に Radius クライアントとしての設定をします。

802.1X 認証方式を EAP に設定します。

```
<AC> system-view
[AC] dot1x
[AC] dot1x authentication-method eap
```

RADIUS スキーム(freeradius)を作成し、Radius サーバとして動作予定の AC 自身の IP アドレス(10.18.1.1)をプライマリ認証サーバとして指定し、認証ポート番号を 1812 に設定し、共有キーを平文の文字列 12345678 に設定します。

```
[AC] radius scheme freeradius
[AC-radius-freeradius] primary authentication 10.18.1.1 1812
[AC-radius-freeradius] key authentication simple 12345678
[AC-radius-freeradius] user-name-format without-domain
[AC-radius-freeradius] quit
```

ISP ドメイン(freeradius)を作成し、LAN ユーザの認証と認可のために RADIUS スキーム freeradius を使用するように ISP ドメインを設定します。AC を RADIUS サーバとして使用する場合、アカウンティングはサポートされません。

```
[AC] domain freeradius
[AC-isp-freeradius] authentication lan-access radius-scheme freeradius
[AC-isp-freeradius] authorization lan-access radius-scheme freeradius
[AC-isp-freeradius] accounting lan-access none
[AC-isp-freeradius] quit
```

2. サービステンプレートを構成します。

サービステンプレート(wlas_freeradius_peap)を作成し、認証モードは 802.1X を設定します。

```
[AC] wlan service-template wlas_freeradius_peap
[AC-wlan-st-wlas_freeradius_peap] client-security authentication-mode dot1x
[AC-wlan-st-wlas_freeradius_peap] dot1x domain freeradius
[AC-wlan-st-wlas_freeradius_peap] ssid wlas_freeradius_peap
[AC-wlan-st-wlas_freeradius_peap] akm mode dot1x
[AC-wlan-st-wlas_freeradius_peap] cipher-suite ccmp
[AC-wlan-st-wlas_freeradius_peap] security-ie rsn
[AC-wlan-st-wlas_freeradius_peap] service-template enable
[AC-wlan-st-wlas_freeradius_peap] quit
```

3. サービステンプレートを AP の Radio にバインドします。

AP にサービステンプレート(wlas_freeradius_peap)をバインドします。

```
[AC] wlan ap ap1 model QX-W1240
[AC-wlan-ap-ap1] serial-id 219801A28N819CE0002T
[AC-wlan-ap-ap1] radio 2
[AC-wlan-ap-ap1-radio-2] radio enable
[AC-wlan-ap-ap1-radio-2] service-template wlas_freeradius_peap
[AC-wlan-ap-ap1-radio-2] quit
[AC-wlan-ap-ap1] quit
```

4. AC に Radius サーバとしての設定をします。

Radius サーバ機能で使用するローカルユーザー(dot1x)を作成し、パスワードを平文で「123456」に設定します。

```
[AC] local-user dot1x class network
[AC-luser-network-dot1x] password simple 123456
[AC-luser-network-dot1x] quit
```

5. RADIUS サーバで EAP 認証を設定します。

EAP プロファイル(dot1x)を作成し、EAP 認証方式を PEAP-MSCHAPv2 に設定します。

```
[AC] eap-profile dot1x
[AC-eap-profile-dot1x] method peap-mschapv2
```

EAP 認証用の CA 証明書ファイル、サーバ証明書ファイル、サーバ証明書の秘密鍵ファイルを指定し、サーバ証明書の秘密鍵パスワードを指定します。

```
[AC-eap-profile-dot1x] ca-file ca.pem
[AC-eap-profile-dot1x] certificate-file server.pem
[AC-eap-profile-dot1x] private-key-file server-key.pem
[AC-eap-profile-dot1x] private-key-password simple whatever
[AC-eap-profile-dot1x] quit
```

AC 上の RADIUS サーバに EAP プロファイル dot1x を適用します。

```
[AC] radius-server eap-profile dot1x
```

Radius クライアントである自身の IP アドレス(10.18.1.1)を指定し、共有キーを平文で 12345678 に設定します。

```
[AC] radius-server client ip 10.18.1.1 key simple 12345678
```

RADIUS サーバ設定を有効化します。Radius サーバ設定や 802.1X 用のローカルユーザの設定を変更した場合、変更を反映させるために RADIUS サーバ設定を再度有効化する必要があります。

```
[AC] radius-server activate
```

III. 設定の確認

AC で、アクティブな RADIUS クライアントを表示して RADIUS クライアントの設定を確認します。

```
[AC] display radius-server active-client
Total 1 RADIUS clients.
Client IP: 10.18.1.1
```

端末側で、サービステンプレート wlas_freeradius_peap に 802.1X 接続を通じて接続します。ユーザ名 dot1x とパスワード 123456 を入力してください。

ID 認証に MSCHAPV2 を使用する場合、Android エンドポイントでは CA 証明書の検証はオプションです。CA 証明書を検証する場合は、エンドポイントに一致する CA 証明書をインストールする必要があります。（詳細は省略。）

AC でオンラインの 802.1X ユーザ情報を表示し、表示されたユーザ名がクライアントで入力したユーザ名と同じであることを確認します。

```
[AC] display dot1x connection
Total connections: 1
User MAC address          : e012-f881-3f42
AP name                   : ap1
Radio ID                  : 1
SSID                      : wlas_freeradius_peap
BSSID                     : 000f-e201-0003
User name                 : dot1x
Authentication domain     : freeradius
IPv4 address              : 10.18.1.10
```

```
Authentication method       : EAP
Initial VLAN                : 1
Authorization VLAN          : 1
Authorization ACL number    : N/A
Authorization user profile : N/A
Authorization CAR           : N/A
Termination action          : Default
Session timeout last from   : 2021/03/01 15:41:33
Session timeout period      : 86400 s
Online from                 : 2021/03/01 15:41:33
Online duration             : 0h 0m 5s
```

AC 上で、オンラインの WLAN クライアント情報を表示し、802.1X ユーザがオンラインになっていることを確認します。

```
[AC] display wlan client
Total number of clients: 1
MAC address     Username          AP name          R IP address      VLAN
e012-f881-3f42 dot1x              ap1              1 10.18.1.10      1
```

3.13 AAAのトラブルシューティング

3.13.1 RADIUS 認証の失敗

I. 症状

ユーザ認証は常に認証に失敗します。

II. 分析

考えられる理由は次のとおりです。

- NAS と RADIUS サーバの間に通信障害が存在する
- ユーザ名にドメイン名が含まれていない、ドメイン名を含むユーザ名の形式が正しくない、または NAS で ISP ドメインが正しく設定されていない
- ユーザが RADIUS サーバで設定されていない
- ユーザが入力したパスワードが間違っている
- RADIUS サーバと NAS で異なる共有キーが設定されている

III. 解決方法

問題を解決するには、次の手順を実行します。

1) 次の項目を確認します。

- □ NAS と RADIUS サーバは、相互に ping を実行する
- □ ユーザ名にはドメイン名が含まれており、ユーザ名の形式は正しく、ISP ドメインは NAS で正しく設定されている
- □ ユーザは RADIUS サーバに設定されている
- □ 正しいパスワードが入力されている
- □ RADIUS サーバと NAS の両方で同じ共有キーが設定されている

2) 問題が解決しない場合は、NEC サポートにお問い合わせください。

3.13.2 RADIUS パケット配信障害

I. 症状

RADIUS パケットが RADIUS サーバに到達できない。

II. 分析

考えられる理由は次のとおりです。

- NAS と RADIUS サーバの間に通信障害が存在する。
- NAS に RADIUS サーバの IP アドレスが設定されていない。
- NAS に設定されている認証およびアカウンティングの UDP ポートが正しくない。
- RADIUS サーバの認証およびアカウンティングのポート番号が他のアプリケーションで使用されている。

III. ソリューション

問題を解決するには、次の手順を実行します。

1) 次の項目を確認します。
   - □ NAS と RADIUS サーバ間のリンクは、物理リンク層とデータリンク層の両方で正常に動作します。
   - □ RADIUS サーバの IP アドレスは、NAS で正しく設定されています。
   - □ NAS に設定されている認証およびアカウンティングの UDP ポート番号は、RADIUS サーバのものと同じです。
   - □ RADIUS サーバの認証およびアカウンティングのポート番号を使用できます。
2) 問題が解決しない場合は、NEC サポートにお問い合わせください。

3.13.3 RADIUS アカウンティングエラー

I. 症状

ユーザは認証および認可されていますが、ユーザのアカウンティングは正常ではありません。

II. 分析

NAS のアカウンティングサーバ設定が正しくありません。次の理由が考えられます。

- NAS に設定されているアカウンティングポート番号が正しくありません。
- NAS に設定されているアカウンティングサーバの IP アドレスが正しくありません。たとえば、NAS は単一のサーバを使用して認証、認可、およびアカウンティングサービスを提供するように設定されていますが、実際にはサービスは異なるサーバによって提供されます。

III. ソリューション

問題を解決するには、次の手順を実行します。

1) 次の項目を確認します。
   - □ アカウンティングポート番号が正しく設定されている。
   - □ アカウンティングサーバの IP アドレスが NAS で正しく設定されている。
2) 問題が解決しない場合は、NEC サポートにお問い合わせください。

3.14 付録

3.14.1 付録 A 一般的に使用される RADIUS 属性

一般的に使用される RADIUS 属性は、RFC 2865、RFC 2866、RFC 2867、および RFC 2868 で定義されています。

表 3-3 一般的に使用される RADIUS 属性

No	属性	No	属性
1	ユーザ名	45	アクト・オーセンティック
2	ユーザパスワード	46	Acct-Session-Time (Acct-Session-Time)
3	CHAP-パスワード (CHAP-Password)	47	Acct-Input-Packets (Acct入力パケット)
4	NAS-IP-Address (NAS-IP-Address)	48	Acct-Output-Packets (Acct-Output-Packets)
5	NAS-ポート	49	Acct-Terminate-Cause (アカウント終了原因)
6	サービスタイプ	50	Acct-Multi-Session-ID
7	Framed-Protocol (フレームプロトコル)	51	Acct-Link-Count (アカウントリンクカウント)
8	Framed-IP-Address (フレームIPアドレス)	52	Acct-Input-Gigawords (Acct-Input-Gigawords)
9	Framed-IP-Netmask (フレームIPネットマスク)	53	Acct-Output-Gigawords (Acct-Output-Gigawords)
10	フレームルーティング	54	(割り当てなし)
11	フィルタID	55	イベントタイムスタンプ
12	フレームMTU	56-59	(割り当てなし)
13	フレーム圧縮	60	CHAP-チャレンジ
14	ログインIPホスト	61	NAS-ポート型
15	ログインサービス	62	ポート制限
16	ログインTCPポート	63	ログインLATポート
17	(未割り当て)	64	トンネル型
18	返信メッセージ	65	トンネル中タイプ
19	コールバック番号	66	トンネルクライアントエンドポイント
20	コールバックID	67	トンネルサーバエンドポイント
21	(未割り当て)	68	Acct-Tunnel-Connection (アクトトンネル接続)
22	フレームルート	69	トンネルパスワード
23	Framed-IPX-Network (フレームIPXネットワーク)	70	ARAP-パスワード
24	状態	71	ARAPの特徴
25	クラス	72	ARAP-Zone-Access
26	ベンダ固有	73	ARAP-セキュリティ
27	セッションタイムアウト	74	ARAP-セキュリティデータ
28	アイドルタイムアウト	75	パスワードの再試行
29	終了アクション	76	プロンプト
30	着信ステーションID	77	接続情報

No	属性	No	属性
31	Calling-Station-Id (発信ステーションID)	78	設定トークン
32	NAS-識別子	79	EAP-メッセージ
33	プロキシ状態	80	メッセージ認証子
34	ログインLATサービス	81	トンネルプライベートグループID
35	ログイン-LAT-ノード	82	トンネル割り当てID
36	ログイン-LAT-グループ	83	トンネル優先
37	フレーム付きAppleTalk-Link	84	ARAP-チャレンジ-レスポンス
38	フレーム化されたAppleTalk-Network	85	Acct-Interim-Intervalの場合
39	Framed-AppleTalk-Zoneの場合	86	Acct-Tunnel-Packets-Lostの場合
40	Acct-Status-Typeの場合	87	NAS-Port-Idの場合
41	Acct-Delay-Time (Acct-Delay-Time)	88	フレームプール (Framed-Pool)
42	Acct-Input-Octets (Acct-Input-Octets)	89	(未割り当て)
43	Acct-Output-Octets (Acct-Output-Octets)	90	Tunnel-Client-Auth-id (トンネルクライアント認証ID)
44	Acct-Session-Id (アカウントセッションID)	91	Tunnel-Server-Auth-id (トンネルサーバ認証ID)

3.14.2 付録 B 一般的に使用される標準 RADIUS 属性の説明

No	属性	説明
1	ユーザ名	認証されるユーザの名前。
2	ユーザパスワード	PAP認証用のユーザパスワードで、PAP認証を使用する場合にAccess-Requestパケットにのみ存在します。
3	CHAPパスワード	CHAP認証用のユーザパスワードのダイジェストで、CHAP認証を使用する場合にアクセス要求パケットにのみ存在します。
4	NAS-IP-Address	クライアントの識別に使用するサーバのIPアドレス。通常、クライアントはアクセスインタフェースのIPアドレスによって識別されます。この属性は、Access-Requestパケットにのみ存在します。
5	NAS-ポート	ユーザがアクセスするNASの物理ポート。
6	サービスタイプ	ユーザが要求したサービスのタイプまたは提供されるサービスのタイプ。
7	フレームプロトコル	フレームアクセスのカプセル化プロトコル。
8	Framed-IP-Address (フレームIPアドレス)	ユーザに割り当てられたIPアドレス。
11	フィルタID	フィルタリストの名前。この属性は次のように解析されます。 属性値は、すべての桁の文字列である場合、ACL番号を表します。 属性値は、user-group=name 1の形式の文字列の場合、ユーザグループ名のリストです。name 2;..。名前空間。このタイプのフィルタリストは、SSL VPNユーザにのみ適用されます。
12	フレームMTU	ユーザとNAS間のデータリンクのMTU。たとえば、この属性を使用して、802.1 X EAP認証で処理できるEAPパケットの最大サイズを定義できます。
14	ログインIPホスト	ユーザがアクセスするNASインタフェースのIPアドレス。
15	ログインサービス	ユーザがログインに使用するサービスのタイプ。
18	返信メッセージ	認証失敗の原因など、サーバが情報を伝達するために使用できる、ユーザに表示されるテキスト。
26	ベンダ固有	ベンダ固有の独自属性。パケットには1つ以上の独自属性を含めることができ、それぞれに1つ以上のサブ属性を含めることができます。

No	属性	説明
27	セッションタイムアウト	セッション終了前のユーザの最大サービス期間。 値0は、ユーザがログアウトされることを示します。値4294967295は、ユーザのオンライン期間に制限がないことを示します。
28	アイドルタイムアウト	セッションの終了前にユーザに許可される最大アイドル時間。
31	Calling-Station-Id (発信ステーションID)	NASがサーバに送信するユーザID。
32	NAS-Identifier (NAS-識別子)	NASがRADIUSサーバに対して自身を識別するために使用する識別情報。
40	Acct-Status-Type (Acct-Status-Type)	Accounting-Requestパケットのタイプ。可能な値は次のとおり。 1:開始。 2:停止。 3:中間更新。 4:リセット-充電。 7:アカウンティング-オン。(3 rd Generation Partnership Projectで定義。) 8:アカウンティング-オフ。(3 rd Generation Partnership Projectで定義。) 9から14:トンネルアカウンティング用に予約済み。 15:失敗用に予約済み。
45	アクト・オーセンティック	ユーザが使用する認証方式。有効な値は次のとおり。 1:RADIUS。 2:ローカル。 3:リモート。
60	CHAPチャレンジ	CHAP認証中にMD 5計算のためにNASによって生成されるCHAPチャレンジ。
61	NAS-ポート型	ユーザを認証しているNASの物理ポートのタイプ。可能な値は次のとおり。 15:イーサネット。 16:オプション設定項目のタイプのADSL。 17:ケーブル。(ケーブルテレビ用ケーブル付き。) 19:wlan-ieee 802.11。 201:VLAN。 202:ATM。 ポートがATMまたはイーサネットポートで、VLANが実装されている場合、この属性の値は201になります。
64	トンネルタイプ	使用されるトンネリングプロトコル。 値13はVLANを表します。値が13の場合、デバイスはTunnel-Type、Tunnel-Medium-Type、およびTunnel-Private-Group-ID属性を属性として解釈し、VLANを割り当てます。
65	Tunnel-Medium-Typeの場合	トンネルの作成に使用するトランスポートメディアタイプ。 VLAN割り当ての場合、802メディアとイーサネットを示す値は6である必要があります。
79	EAP-メッセージ	RADIUSがEAP認証をサポートできるようにEAPパケットをカプセル化するために使用されます。
80	メッセージ認証サーバ	アクセス要求のスプーフィングを防止するための認証パケットの認証と検証に使用されます。この属性は、EAP認証を使用する場合に存在します。
81	トンネルプライベートグループID	トンネルセッションのグループID。VLANを割り当てるために、NASはこの属性を使用してVLAN IDを伝達します。
87	NAS-ポートID	ユーザを認証しているNASのポートを説明する文字列。
185	WLAN-理由コード	WLANエンドポイント認証失敗の理由コード。 長さは32ビットです。最初の16ビットは予約され、残りの16ビットは理由コードを表します。
186	WLAN-Pairwise-Cipher	WLANユニキャストフレーム用の暗号スイート。 長さは32ビットです。最初の24ビットはOUIを表し、残りの8ビットはスイートの種類を表します。

No	属性	説明
187	WLAN-Group-Cipherr	WLANマルチキャストフレームの暗号スイート。 長さは32ビットです。最初の24ビットはOUIを表し、残りの8ビットはスイートの種類を表します。
188	WLAN-AKM-スイート	認証およびキー管理 (AKM) モード。 長さは32ビットです。最初の24ビットはOUIを表し、残りの8ビットはスイートの種類を表します。
189	WLAN-Group-Mgmt-Cipher	WLANマルチキャスト管理フレームの暗号スイート。 長さは32ビットです。最初の24ビットはOUIを表し、残りの8ビットはスイートの種類を表します。

QX-W2300AC シリーズ アクセスコントローラ

オペレーションマニュアル

14. 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-WLAN 高可用性

02-Track

03-クラウドクラスタ

目次

このセクションのページは **14-x-x** です。

1章 WLAN 高可用性 1-1
1.1 デュアルリンクバックアップ 1-1
1.1.1 概要 1-1
1.1.2 制限とガイドライン 1-2
1.1.3 デュアルリンクバックアップ設定作業リスト 1-2
1.1.4 AP接続優先順位の設定とバックアップACの指定 1-2
1.1.5 マスタCAPWAP トンネル プリエンプションの設定 1-3
1.1.6 デュアルリンクバックアップの設定例 1-3
1.2 APホットバックアップ 1-5
1.2.1 概要 1-5
1.2.2 前提条件 1-6
1.2.3 APホットバックアップの有効化 1-6
1.3 クライアントホットバックアップ 1-7
1.3.1 概要 1-7
1.3.2 制限とガイドライン 1-7
1.3.3 前提条件 1-7
1.3.4 クライアントホットバックアップの有効化 1-7
1.3.5 クライアントホットバックアップの遅延時間の設定 1-7
1.3.6 クライアントホットバックアップの検証と維持 1-8

1章 WLAN 高可用性

1.1 デュアルリンクバックアップ

> **注意：**
> クラウドクラスタとデュアルリンクバックアップ機能は併用できません。

1.1.1 概要

デュアルリンクバックアップでは、2 つの AC を相互にバックアップして、シングル AC の障害によるサービス中断のリスクを軽減できます。

デュアルリンクバックアップを有効にすると、AP はマスタ CAPWAP トンネルとバックアップ CAPWAP トンネルをそれぞれマスタ AC とバックアップ AC で確立します。マスタ AC とバックアップ AC は、互いのリンク状態をリアルタイムで検出できません。マスタ AC の障害時にバックアップ AC がトラフィック転送を引き継ぐと、一時的な通信中断が発生します。障害が発生したマスタ AC が回復すると、マスタ CAPWAP トンネルのプリエンプション機能によって、AP 接続の優先順位に基づいてマスタ CAPWAP トンネルが決定されます。

デュアルリンクバックアップは、サービス継続性を考慮しないネットワークに適用できます。

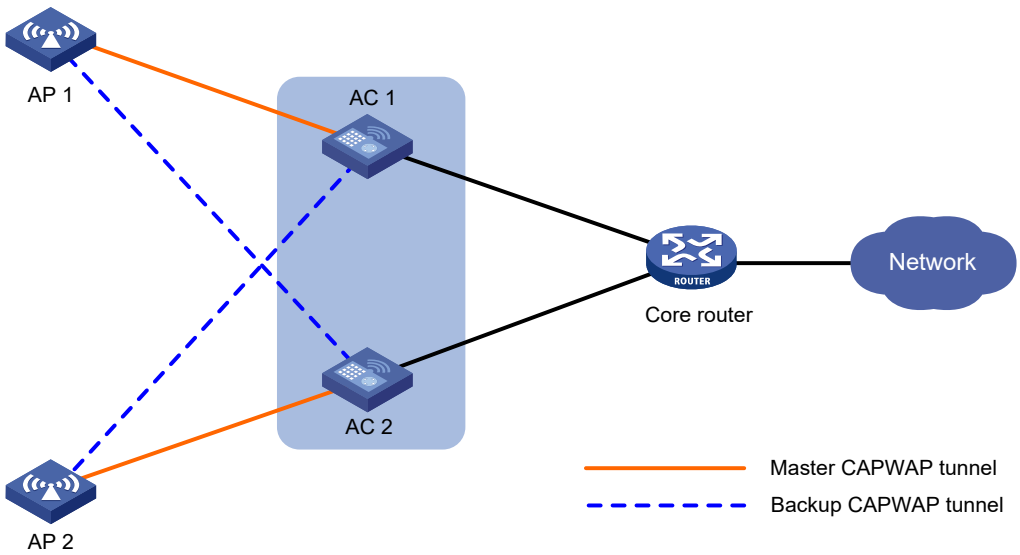


図 1-1 デュアルリンクバックアップのネットワーク図

1.1.2 制限とガイドライン

デュアルリンクバックアップ機能を正しく機能させるには、2 つの AC に自動 AP または手動 AP を設定します。手動 AP 設定は、両方の AC で同一である必要があります。詳細は、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“7 AP 管理”の”1 章 AP 管理”を参照してください。

以下の方法で AP を設定できます。

- AP view で AP を 1 つずつ設定します。
- AP を AP グループに割り当て、AP group view で AP グループを設定します。
- グローバル設定 view ですべての AP を設定します。

AP の場合、これらの view で同じパラメータに対して行った設定は、AP view、AP group view、グローバル設定 view の降順で有効になります。

クラウドクラスタ構成装置を含むデュアルリンクバックアップ構成では AP ライセンス同期機能は使用できません。

1.1.3 デュアルリンクバックアップ設定作業リスト

作業リスト
（必須設定項目） AP接続優先順位の設定とバックアップACの指定
（オプション設定項目）マスタCAPWAP トンネル プリエンプションの設定

1.1.4 AP 接続優先順位の設定とバックアップ AC の指定

AP が最初にマスタ AC とアソシエートできるように、マスタ AC の AP 接続優先順位を高く設定します。

AP がマスタ AC との CAPWAP トンネルを確立した後、AP は指定されたバックアップ AC とのバックアップ CAPWAP トンネルを確立します。

以下に AP 接続優先順位の設定とバックアップ AC の指定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP view または AP group view に移行する	• AP view に移行する **wlan ap** *ap-name* • AP group viewに移行する **wlan ap-group** *group-name*	—
3. AP 接続の優先順位を設定する	**priority** *priority*	デフォルト： AP viewでは、APはAP group viewの設定を使用します。 AP group viewでは、AP接続の優先順位は4です。
4. バックアップ AC を指定する	**backup-ac ip** *ipv4-address*	デフォルト： AP viewでは、APはAP group viewの設定を使用します。 AP group viewでは、バックアップACは指定されません。

1.1.5 マスタ CAPWAP トンネル プリエンプションの設定

バックアップ AC の AP 接続優先度がマスタ AC よりも高い場合、バックアップ CAPWAP トンネルは 10 分後にマスタトンネルになることができます。

以下にマスタ CAPWAP トンネル プリエンプションの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. AP view、AP group view またはグローバル設定 view に移行する	• AP view に移行する **wlan ap** *ap-name* • AP group view に移行する **wlan ap-group** *group-name* • グローバル設定view に移行する **wlan global-configuration**	ー
3. マスタ CAPWAP トンネルプリエンプションを設定する	**wlan tunnel-preempt** { **disable** | **enable** }	デフォルト： AP viewでは、APはAP group viewの設定を使用します。AP group viewに設定が存在しない場合、APはグローバル設定viewの設定を使用します。 AP group viewでは、APはグローバル設定viewの設定を使用します。 グローバル設定viewでは、マスタCAPWAPトンネルプリエンプションは無効になっています。

1.1.6 デュアルリンクバックアップの設定例

I. ネットワーク要件

図 1-2に示すように、AC1 がマスタ AC として機能し、AC2 がバックアップ AC として機能するように設定します。AC1 で障害が発生し、AC2 が引き継いだ場合、AP は AC2 を介して通信できます。AC1 が回復したときに AP が AC1 に再接続するように、2 つの AC でマスタ CAPWAP トンネルプリエンプション機能を設定します。

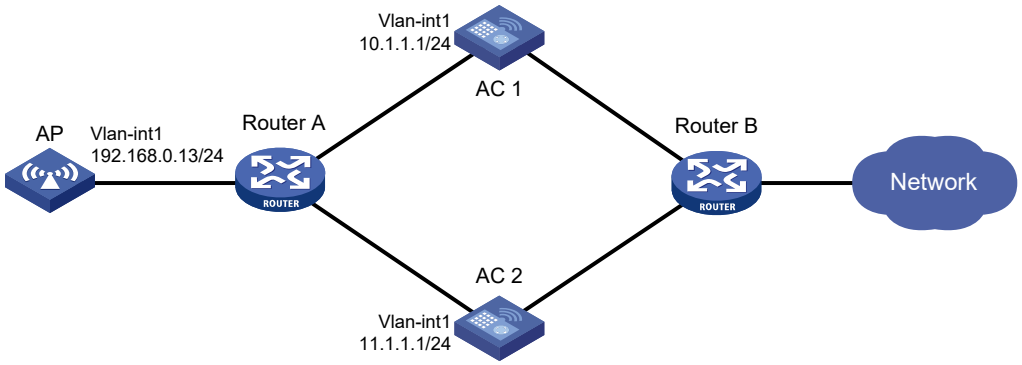


図 1-2 ネットワーク図

II. 設定手順

1)　AC1 を設定します。

VLAN-interface1 を作成し、IP アドレスを割り当てます。

```
<AC1> system-view
[AC1] interface vlan-interface 1
[AC1-Vlan-interface1] ip address 10.1.1.1 24
[AC1-Vlan-interface1] quit
```

AP **ap1** を作成し、AP モデルとシリアル ID を指定します。AP の接続優先度を **7** に設定します。

```
[AC1] wlan ap ap1 model QX-W1110
[AC1-wlan-ap-ap1] serial-id 219801A28N819CE0002T
[AC1-wlan-ap-ap1] priority 7
```

バックアップ AC を指定します。

```
[AC1-wlan-ap-ap1] backup-ac ip 11.1.1.1
```

マスタ CAPWAP トンネルプリエンプションを有効にします。

```
[AC1-wlan-ap-ap1] wlan tunnel-preempt enable
[AC1-wlan-ap-ap1] quit
```

ip route-static コマンドでバックアップ AC への next-hop を指定します(設定は省略)。

2)　AC2 を設定します。

VLAN-interface1 を作成し、IP アドレスを割り当てます。

```
<AC2> system-view
[AC2] interface Vlan-interface 1
[AC2-Vlan-interface1] ip address 11.1.1.1 24
[AC2-Vlan-interface1] quit
```

AP **ap1** を作成し、AP モデルとシリアル ID を指定します。AP の接続優先度を **5** に設定します。

```
[AC2] wlan ap ap1 model QX-W1110
[AC2-wlan-ap-ap1] serial-id 219801A28N819CE0002T
[AC2-wlan-ap-ap1] priority 5
```

バックアップ AC を指定します。

```
[AC2-wlan-ap-ap1] backup-ac ip 10.1.1.1
```

マスタ CAPWAP トンネルプリエンプションを有効にします。

```
[AC2-wlan-ap-ap1] wlan tunnel-preempt enable
[AC2-wlan-ap-ap1] quit
```

ip route-static コマンドでバックアップ AC への next-hop を指定します(設定は省略)。

III. 設定の確認

AC1 で AP をオンラインにします。（詳細は省略します。）

AC1 で VLAN-interface1 をシャットダウンし、3 分以内に待機してその間にサービス中断が発生します。（詳細は省略します。）

AC2 で AP がオンラインになり、AC2 で AP の状態が R/M であることを確認します。（詳細は省略します。）

AC1 で VLAN-interface1 を起動します。（詳細は省略します。）

AP が AC1 で再びオンラインになり、AP の状態が AC1 で R/M、AC2 で R/B であることを確認します。（詳細は省略します。）

1.2 APホットバックアップ

1.2.1 概要

大規模なワイヤレスネットワークでは、複数の AC を使用して多数の AP を管理します。これらの AC がそれぞれ独立して動作する場合、それらを管理することは困難となります。また、1 つの AC に障害が発生すると、その AC に接続されている AP でワイヤレスサービスが中断される可能性があります。複数の AC がクラウドクラスタを形成して AP を一元管理し、AC 障害時のワイヤレスサービスの中断を回避できます。

I. AC の役割

クラウドクラスタ内の AC は次の役割に分けることができます。

役割	説明
マスタ AC	クラウドクラスタ内のマスタ。マスタACはクラウドクラスタ全体を管理します。

役割	説明
下位 AC	クラウドクラスタ内の下位。下位ACは、サービスを処理し、パケットを転送し、マスタACのバックアップとして機能します。マスタACに障害が発生すると、システムはクラウドクラスタ内の下位ACから新しいマスタACを自動的に選択します。
アクティブAC	APを使用してCAPWAPトンネルを確立できるAC。マスタACは常にアクティブACです。
非アクティブAC	APでCAPWAPトンネルを確立できないAC。非アクティブなACは下位のACにしかできません。アクティブACに障害が発生すると、非アクティブACがアクティブACとして選択されます。
直接接続AC	APがCAPWAPトンネル確立プロセスを開始したときに、APから最初のパケットを受信するAC。
非直接接続 AC	APがCAPWAPトンネル確立プロセスを開始したときに、APから最初のパケットを受信しないAC。

II. AP のホットバックアップと回復

AP のホットバックアップを使用すると、クラウドクラスタ内のアクティブ AC (マスタ AC) は、接続されている AP に関する情報をすべての非アクティブ AC に同期できます。アクティブ AC に障害が発生すると、非アクティブ AC の 1 つがアクティブになりサービスを提供し、サービスの継続性を確保します。

1.2.2 前提条件

AP ホットバックアップを設定する前に、対象となる AC にクラウドクラスタを設定します。

1.2.3 AP ホットバックアップの有効化

この機能により、アクティブな AC は、接続されている AP に関する情報をすべての非アクティブ AC に同期できます。アクティブ AC に障害が発生すると、非アクティブ AC の 1 つがアクティブになり、サービスを提供します。

I. 制限とガイドライン

AP ホットバックアップが有効になった後にクラウドクラスタに接続された AP に関する情報のみをバックアップします。AP ホットバックアップを無効にすると、すべての AC がバックアップしている AP 情報を削除します。

II. 設定手順

以下に設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. AP ホットバックアップを有効にする	**wlan ap-backup hot-backup enable global**	デフォルト：無効

1.3 クライアントホットバックアップ

1.3.1 概要

クライアントホットバックアップを使用すると、クラウドクラスタメンバの AC が相互にクライアント情報をバックアップして、AC に障害が発生した場合にクライアントをオンラインに維持できます。クライアントホットバックアップは、クライアント情報が変更されるたびに開始されます。

クライアントホットバックアップは、AP ホットバックアップと連携する必要があります。両方の機能を有効にすると、アクティブ AC は接続された AP およびクライアント情報を他のメンバ AC にバックアップします。アクティブ AC に障害が発生すると、マスタ AC はクラウドクラスタ内の別の AC を選択して、障害が発生した AC に接続されている AP およびクライアントの情報を回復します

1.3.2 制限とガイドライン

アクティブ AC は、クライアントホットバックアップが有効になった後にオンラインになったクライアントのクライアント情報だけをバックアップします。クライアントホットバックアップを無効にすると、すべてのメンバ AC からクライアントホットバックアップ情報が削除されます。

1.3.3 前提条件

クライアントホットバックアップを有効にするには、AP ホットバックアップを有効にする必要があります。

1.3.4 クライアントホットバックアップの有効化

I. 設定手順

以下に設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. クライアントホットバックアップを有効する	**wlan client-backup hot-backup enable**	デフォルト：無効

1.3.5 クライアントホットバックアップの遅延時間の設定

I. 制限とガイドライン

以下の制限とガイドラインに従ってください。

- 本機能はクライアントホットバックアップが有効になっている場合のみ有効になります。

- 本機能はクライアントホットバックアップを設定した後にオンラインになったクライアントに対してのみ有効になります。
- クライアントがオンラインになった後、遅延時間中にプライマリ/セカンダリ AC の切り替えが発生した場合、クライアントは新しいプライマリ AC に自動的に切り替えることができず、クライアントは再接続が必要になります。プライマリ/セカンダリ AC の切り替えはアクティブ AC の再起動によって開始されます。

II. 設定手順

以下に設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. クライアントホットバックアップの遅延時間を有効する	**wlan client-backup hot-backup delay** *delay-time*	デフォルト：60秒

1.3.6 クライアントホットバックアップの検証と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
ACの802.1 X認証ユーザに関するバックアップ情報を表示する	**display dot1x connection-backup [ap** *ap-name* **[radio** *radio-id* **]] slot** *slot-number*
ACのMAC認証ユーザに関するバックアップ情報を表示する	**display mac-authentication connection-backup [ap** *ap-name* **[radio** *radio-id* **]] slot** *slot-number*
クラウドクラスタ内の指定されたメンバデバイスのクライアントホットバックアップ情報を表示する	**display wlan client-backup [ap ap-name [radio** *radio-id* **] | mac-address** *mac-address* **] [verbose] [slot** *slot-number* **]**

目次

このセクションのページは **14-x-x** です。

2章 Track..... 2-1
2.1 概要..... 2-1
2.1.1 コラボレーションの基本..... 2-1
2.2 制限とガイドライン: Track設定..... 2-2
2.3 Track設定作業リスト..... 2-2
2.4 Trackモジュールと検出モジュールの関連づけ..... 2-3
2.4.1 TrackとNQAの関連づけ..... 2-3
2.4.2 Trackとインタフェース管理モジュールの関連づけ..... 2-3
2.5 Trackモジュールとアプリケーションモジュールの関連づけ..... 2-4
2.5.1 Trackとスタティックルーティングの関連づけ..... 2-4
2.6 Trackエントリの表示と維持..... 2-5
2.7 Track設定例..... 2-5
2.7.1 スタティックルーティング-Track-NQAコラボレーション設定..... 2-5

2章 Track

この章でのルータという用語は、ルーティング対応装置を指します。

2.1 概要

Track モジュールは、図 2-1に示すようにアプリケーションと検出モジュール間で動作します。アプリケーションモジュールから、さまざまな検出モジュール間の相違点を保護します。

検出モジュールとアプリケーションモジュールの Track モジュールを連携した後、コラボレーションが有効となります。検出モジュールは、インタフェース状態、リンク状態、ネットワークの接続性、ネットワーク性能のような指定したオブジェクトを調査し、検出結果を Track モジュールに通知します。Track モジュールは関連したアプリケーションモジュールに検出結果を送信します。Track オブジェクトの変更を通知したとき、アプリケーションモジュールは通信の中断とネットワーク性能の低下を防ぐため、結果に対して対応することができます。

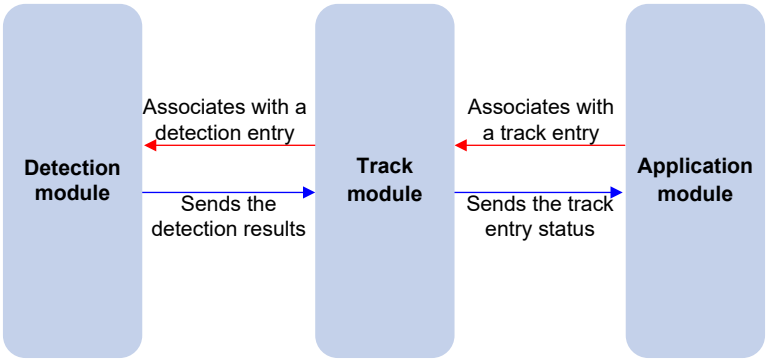


図 2-1 Track モジュールを介したコラボレーション

2.1.1 コラボレーションの基本

Track モジュールは、検出モジュールとアプリケーションモジュール間でコラボレーションします。

I. Track モジュールと検出モジュール間のコラボレーション

検出モジュールは、関連した Track 対象オブジェクトの検出結果を Track 対象モジュールに送信します。結果に依存して、Track モジュールは Track エントリの状態を変更します。

- Track 対象オブジェクト機能が正常の場合、Track エントリの状態は Positive になります。たとえば、以下のいずれかの状況の Track エントリの状態は Positive です。
  - ターゲットインタフェースがアップです。
  - ターゲットネットワークが到達可能です。

- Track 対象オブジェクト機能が正常でない場合、Track エントリの状態は Negative になります。たとえば、以下のいずれかの状況の Track エントリの状態は Negative です。
  - □ ターゲットインタフェースがダウンです。
  - □ ターゲットネットワークが到達不可能です。
- 検出結果が有効でない場合、Track エントリの状態は、NotReady になります。たとえば Track エントリに関連した NQA テストグループが存在しない場合、NotReady になります。

以下の検出モジュールが Track モジュールに関連づけることができます。

- NQA
- インタフェース管理モジュール
- ルート管理モジュール
- LLDP

II. Track モジュールとアプリケーションモジュール間のコラボレーション

Track モジュールは、Track エントリの状態変更をアプリケーションモジュールに報告します。その後、アプリケーションモジュールは、通信の中断やネットワークパフォーマンスの低下を回避するために正しいアクションを実行できます。

2.2 制限とガイドライン: Track設定

アプリケーションモジュールの Track エントリを設定するとき、状態の変化をすぐに通知することを防ぐため、通知遅延を設定できます。

遅延が設定されておらず、ルート収束がリンク状態変更通知よりも遅い場合、通信障害が発生します。たとえば、VRRP グループ内のマスタが Track を介してアップリンクインタフェース障害を検出すると、Track はすぐにマスタにその優先順位を下げるように通知します。その後、優先順位の高いバックアップが新しいマスタとしてプリエンプションされます。障害が発生したアップリンクインタフェースが回復すると、Track モジュールはすぐに元のマスタにその優先順位を復元するように通知します。アップリンクルートが回復していない場合、転送障害が発生します。

2.3 Track設定作業リスト

コラボレーション機能を動作させるため、Track モジュールと検出モジュール、および Track モジュールとアプリケーションモジュールを関連づけます。

以下に Track モジュールの設定作業リストを示します。

作業リスト
（必須設定項目) Trackモジュールと検出モジュールの関連づけ ● TrackとNQAの関連づけ ● Trackとインタフェース管理モジュールの関連づけ
（必須設定項目) Trackモジュールとアプリケーションモジュールの関連づけ: ● Trackとスタティックルーティングの関連づけ

2.4 Trackモジュールと検出モジュールの関連づけ

2.4.1 Track と NQA の関連づけ

NQA は、ネットワークのパフォーマンス、サービス、サービス品質を解析するために複数のテストタイプをサポートしています。たとえば、NQA テストでは、宛先へ到達可能かどうか、あるいは TCP サーバへ TCP 接続がアップであるかどうかを定期的に検出することができます。

NQA テストグループは、Track エントリに関連づけられている場合、以下のように機能します。

- エラーが連続して指定のしきい値に達した場合、NQA モジュールは、Track モジュールに Track 対象オブジェクトの異常を通知します。その後、Track モジュールは、Track エントリの状態を Negative に変更します。
- 指定したしきい値に達していない場合、NQA モジュールは、Track 対象オブジェクトが正常に機能していることを Track モジュールに通知します。Track モジュールは、Track エントリの状態を Positive に変更します。

NQA の詳細は、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*17 ネットワーク管理と監視*”の” *3 章 NQA*”を参照してください。

以下に Track と NQA の関連づけの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. Track エントリを生成し、NQA リアクションエントリと関連づけを行い、track entry view に移行する	**track** *track-entry-number* **nqa entry** *admin-name operation-tag* **reaction** *item-number*	デフォルト：設定なし もし指定したNQAテストグループあるいはTrackエントリのリアクションエントリが存在しない場合、Trackエントリの状態はNotReadyとなります。

2.4.2 Track とインタフェース管理モジュールの関連づけ

インタフェース管理モジュールは、インタフェースのリンク状態やネットワーク層のプロトコルの状態を監視します。インタフェース管理モジュールは、Track エントリに関連づけられている場合、次のように機能します。

- インタフェースのリンクまたはネットワーク層のプロトコル状態がアップになると、インタフェース管理モジュールは、状態の変更を Track モジュールに通知し、Track モジュールは Track エントリの状態を Positive に変更します。
- インタフェースのリンクまたはネットワーク層のプロトコルの状態がダウンになると、インタフェース管理モジュールは、状態の変更を Track モジュールに通知し、Track モジュールは Track エントリの状態を Negative に変更します。

以下に Track とインタフェース管理モジュールの関連づけの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー

操作	コマンド	補足
2． Track をインタフェース管理モジュールと関連づける	• インタフェースのリンク状態に関連付けられたTrackエントリを作成する: **track** *track-entry-number* **interface** *interface-type interface-number* • インタフェースのレイヤ3プロトコル状態に関連付けられたTrack エントリを作成する: **track** *track-entry-number* **interface** *interface-type interface-number* **protocol ipv4**	デフォルト：設定なし

2.5 Trackモジュールとアプリケーションモジュールの関連づけ

2.5.1 Track とスタティックルーティングの関連づけ

スタティックルートは手動でルートを設定します。スタティックルートが設定されたネットワークで、指定された宛先へのパケットは管理者によって指定されたパスを通って転送されます。スタティックルートについての詳細は、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*5 ネットワーク接続*”の”*23 章 スタティックルーティング*”を参照してください。

スタティックルートの欠点は、ネットワークトポロジの変化に適応できないことです。そのため、ネットワークの障害やトポロジの変化が発生すると、ターゲットとの通信ができなくなることがあります。

この問題を回避するために、スタティックルートのバックアップをする別のルートを設定します。スタティックが到達可能であるとき、パケットはスタティックルートを通して転送されます。スタティックルートが到達不可能であるとき、パケットはバックアップルートを通して転送されます。

リアルタイムでスタティックルートの到達可能性をチェックするには、Track とスタティックルート間の関連づけをします。

スタティックルートを設定するときに、出力インタフェースでなくネクストホップを指定すると、スタティックルート、Track モジュール、宛先モジュール間でのコラボレーションを確立することができます。これにより、Track エントリの状態でスタティックルートの到達可能性をチェックすることができます。

- Track エントリの状態が Positive の場合、以下の状況となります。
  - □ スタティックルートのネクストホップが到達可能です。
  - □ 設定されたスタティックルートが有効です。
- Track エントリの状態が Negative の場合、以下の状況となります。
  - □ スタティックルートのネクストホップが到達不可能です。
  - □ 設定されたスタティックルートが無効です。
- Track エントリの状態が NotReady の場合、以下の状況となります。
  - □ スタティックルートのネクストホップの到達可能性が不明です。

□　スタティックルートが有効です。

Track をスタティックルーティングと関連づけるとき、以下の制限とガイドラインに従ってください。

- スタティックルートのルートを復旧させる場合、関連する Track エントリはスタティックルートではなく復旧ルートのネクストホップを監視させる必要があります。そうでなければルートは無効とみなされます。

以下に Track とスタティックルーティングの関連づけの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. ネクストホップの到達可能性をチェックするためにスタティックルーティングと Track エントリを関連づける	**ip route-static** *dest-address* { *mask-length* | *mask* } { *interface-type interface-number* [*next-hop-address*] | *next-hop-address* [**permanent** | **track** *track-entry-number*] [**preference** *preference*] [**tag** *tag-value*] [**description** *text*]	デフォルト：設定なし

2.6 Trackエントリの表示と維持

すべての view で **display** コマンドを表示することができます。

操作	コマンド
Trackエントリの情報を表示する	**display track** { *track-entry-number* | **all** }

2.7 Track設定例

2.7.1 スタティックルーティング-Track-NQA コラボレーション設定

I. ネットワーク要件

図 2-2に示すように設定します。

- AC 1 はサブネット 20.1.1.0/24 内の Host のデフォルトゲートウェイです。
- AC 4 はサブネット 30.1.1.0/24 内の Host のデフォルトゲートウェイです。
- 2 つのサブネット内の Host はスタティックルートを通して互いに通信します。

ネットワークの信頼性を保証するため、ルートのバックアップを設定し、以下のように AC 1 と AC 4 のスタティックルーティング-Track-NQA コラボレーションを設定します。

- AC 1 上で、高い優先度、ネクストホップが AC 2、宛先が 30.1.1.0/24 のスタティックルートを割り当てます。このルートがマスタルートです。ネクストホップが AC 3、宛先が 30.1.1.0/24 へのスタティックルートはバックアップルートとして動作します。AC 1 は、AC 3 を通して 30.1.1.0/24 にパケットを転送します。
- AC 4 上で、高い優先度、ネクストホップが AC 2、宛先が 20.1.1.0/24 のスタティックルートを割り当てます。このルートがマスタルートです。ネクストホップが AC 3、

宛先が 20.1.1.0/24 へのスタティックルートはバックアップルートとして動作します。マスタルートが到達不能であるとき、バックアップルートが適用されます。AC 4 は、

- AC 3 を通して 20.1.1.0/24 にパケットを転送します。

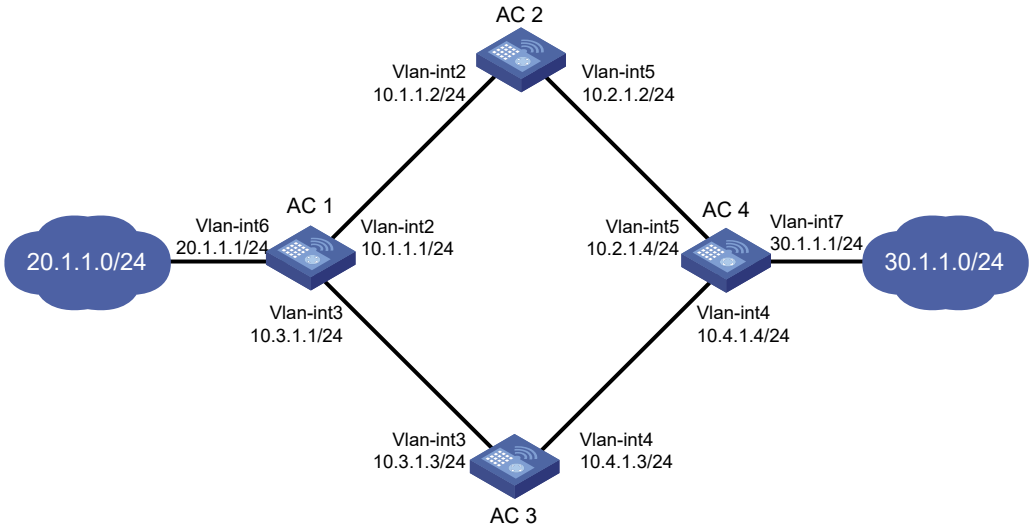


図 2-2 ネットワーク図

II. 設定手順

1) VLAN を作成し、対応するポートを割り当てます。図 2-2に示すように各 VLAN インタフェースの IP アドレスを割り当てます。(詳細は省略します)
2) AC 1 を設定します。

ネクストホップのアドレスを 10.1.1.2、デフォルトの優先度を 60 のスタティックルート 30.1.1.0/24 を設定します。このスタティックルートを Track エントリ 1 に関連づけます。

```
<AC1> system-view
[AC1] ip route-static 30.1.1.0 24 10.1.1.2 track 1
```

ネクストホップのアドレスを 10.3.1.3、優先度を 80 のスタティックルート 30.1.1.0/24 を設定します。

```
[AC1] ip route-static 30.1.1.0 24 10.3.1.3 preference 80
```

ネクストホップのアドレスを 10.1.1.2 のスタティックルート 10.2.1.4 を設定します。

```
[AC1] ip route-static 10.2.1.4 24 10.1.1.2
```

管理者 admin、オペレータタグ test の NQA オペレーションを作成します。

```
[AC1] nqa entry admin test
```

オペレーションタイプを ICMP エコータイプとして設定します。

```
[AC1-nqa-admin-test] type icmp-echo
```

宛先アドレスを 10.2.1.4、ネクストホップのアドレスを 10.1.1.2 に設定します。

```
[AC1-nqa-admin-test-icmp-echo] destination ip 10.2.1.4
[AC1-nqa-admin-test-icmp-echo] next-hop ip 10.1.1.2
```

100 ミリ秒の間隔で繰り返す ICMP エコーオペレーションを設定します。

```
[AC1-nqa-admin-test-icmp-echo] frequency 100
```

リアクションエントリ 1 を設定し、Track モジュールのトリガーを 5 回連続して失敗するように指定します。

```
[AC1-nqa-admin-test-icmp-echo] reaction 1 checked-element probe-fail threshold-type consecutive 5 action-type trigger-only
[AC1-nqa-admin-test-icmp-echo] quit
```

NQA オペレーションを開始します。

```
[AC1] nqa schedule admin test start-time now lifetime forever
```

Track エントリ 1 を設定し、NQA オペレーションのリアクションエントリ 1 に関連づけます。

```
[AC1] track 1 nqa entry admin test reaction 1
```

3)　AC 2 を設定します。

ネクストホップのアドレスが 10.2.1.4、宛先が 30.1.1.0/24 のスタティックルートを設定します。

```
<AC2> system-view
[AC2] ip route-static 30.1.1.0 24 10.2.1.4
```

ネクストホップのアドレスが 10.1.1.1、宛先が 20.1.1.0/24 のスタティックルートを設定します。

```
[AC2] ip route-static 20.1.1.0 24 10.1.1.1
```

4)　AC 3 を設定します。

ネクストホップのアドレスが 10.4.1.4、宛先が 30.1.1.0/24 のスタティックルートを設定します。

```
<AC3> system-view
[AC3] ip route-static 30.1.1.0 24 10.4.1.4
```

ネクストホップのアドレスが 10.3.1.1、宛先が 20.1.1.0/24 のスタティックルートを設定します。

```
[AC3] ip route-static 20.1.1.0 24 10.3.1.1
```

5)　AC 4 を設定します。

ネクストホップのアドレスが 10.2.1.2、宛先が 20.1.1.0/24 のスタティックルートを設定し、デフォルトの優先度を 60 に設定します。このスタティックルートを Track エントリ 1 に割り当てます。

```
<AC4> system-view
[AC4] ip route-static 20.1.1.0 24 10.2.1.2 track 1
```

ネクストホップのアドレスが 10.4.1.3、宛先が 20.1.1.0/24 のスタティックルートを設定し、デフォルトの優先度を 80 に設定します。

```
[AC4] ip route-static 20.1.1.0 24 10.4.1.3 preference 80
```

ネクストホップのアドレスが 10.2.1.2、宛先が 10.1.1.1/24 のスタティックルートを設定します。

```
[AC4] ip route-static 10.1.1.1 24 10.2.1.2
```

管理者 admin、オペレータタグ test の NQA オペレーションを作成します。

```
[AC4] nqa entry admin test
```

テストタイプを ICMP エコータイプとして設定します。

```
[AC4-nqa-admin-test] type icmp-echo
```

オペレーションの宛先 IP アドレスを 10.1.1.1、ネクストホップアドレスを 10.2.1.2 に設定します。

```
[AC4-nqa-admin-test-icmp-echo] destination ip 10.1.1.1
[AC4-nqa-admin-test-icmp-echo] next-hop ip 10.2.1.2
```

ICMP エコーオペレーションのテスト間隔を 100ms に設定します。

```
[AC4-nqa-admin-test-icmp-echo] frequency 100
```

リアクションエントリ 1 を設定し、Track モジュールのトリガーを 5 回連続して失敗するように指定します。

```
[AC4-nqa-admin-test-icmp-echo] reaction 1 checked-element probe-fail threshold-type consecutive 5 action-type trigger-only
[AC4-nqa-admin-test-icmp-echo] quit
```

NQA オペレーションを開始します。

```
[AC4] nqa schedule admin test start-time now lifetime forever
```

Track エントリ 1 を設定し、NQA オペレーションのリアクションエントリ 1 に関連づけます。

```
[AC4] track 1 nqa entry admin test reaction 1
```

III. 設定の確認

AC 1 の Track エントリの情報を表示します。

```
[AC1] display track all
Track ID: 1
  State: Positive
  Duration: 0 days 0 hours 0 minutes 32 seconds
  Notification delay: Positive 0, Negative 0 (in seconds)
  Tracked object:
    NQA entry: admin test
    Reaction: 1
```

出力は、Track エントリの状態が Positive で、NQA オペレーションが成功し、マスタルートが有効であることを示します。

AC 1 のルーティングテーブルを表示します。

```
[AC1] display ip routing-table

Destinations : 10       Routes : 10

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
10.1.1.0/24         Direct 0    0            10.1.1.1        Vlan2
10.1.1.1/32         Direct 0    0            127.0.0.1       InLoop0
10.2.1.0/24         Static 60   0            10.1.1.2        Vlan2
10.3.1.0/24         Direct 0    0            10.3.1.1        Vlan3
10.3.1.1/32         Direct 0    0            127.0.0.1       InLoop0
20.1.1.0/24         Direct 0    0            20.1.1.1        Vlan6
20.1.1.1/32         Direct 0    0            127.0.0.1       InLoop0
30.1.1.0/24         Static 60   0            10.1.1.2        Vlan2
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
```

出力では、AC 1 は AC 2 を通して 30.1.1.0/24 にパケットを転送しています。

AC 2 で VLAN インタフェース 2 の IP アドレスを削除します。

```
<AC2> system-view

[AC2] interface vlan-interface 2

[AC2-Vlan-interface2] undo ip address
```

AC 1 の Track エントリの情報を表示します。

```
[AC1] display track all
Track ID: 1
  State: Negative
  Duration: 0 days 0 hours 0 minutes 32 seconds
  Notification delay: Positive 0, Negative 0 (in seconds)
  Tracked object:
    NQA entry: admin test
    Reaction: 1
```

出力では、Track エントリの状態が Negative で、NQA オペレーションが失敗し、マスタルートが無効であることを示します。

AC 1 のルーティングテーブルを表示します。

```
[AC1] display ip routing-table

Destinations : 10       Routes : 10

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
10.1.1.0/24         Direct 0    0            10.1.1.1        Vlan2
10.1.1.1/32         Direct 0    0            127.0.0.1       InLoop0
10.2.1.0/24         Static 60   0            10.1.1.2        Vlan2
10.3.1.0/24         Direct 0    0            10.3.1.1        Vlan3
10.3.1.1/32         Direct 0    0            127.0.0.1       InLoop0
20.1.1.0/24         Direct 0    0            20.1.1.1        Vlan6
20.1.1.1/32         Direct 0    0            127.0.0.1       InLoop0
30.1.1.0/24         Static 80   0            10.3.1.3        Vlan3
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
```

出力では、AC 1 は AC 3 を通して 30.1.1.0/24 にパケットを転送しています。バックアップルートが適用されています。

マスタが故障したとき、20.1.1.0/24 内の Host が 30.1.1.0/24 内の Host と通信できることを確認してください。

```
[AC1] ping -a 20.1.1.1 30.1.1.1
Ping 30.1.1.1: 56  data bytes, press CTRL_C to break
```

```
Reply from 30.1.1.1: bytes=56 Sequence=1 ttl=254 time=2 ms
Reply from 30.1.1.1: bytes=56 Sequence=2 ttl=254 time=1 ms
Reply from 30.1.1.1: bytes=56 Sequence=3 ttl=254 time=1 ms
Reply from 30.1.1.1: bytes=56 Sequence=4 ttl=254 time=2 ms
Reply from 30.1.1.1: bytes=56 Sequence=5 ttl=254 time=1 ms

--- Ping statistics for 30.1.1.1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.00% packet loss
round-trip min/avg/max/std-dev = 1/1/2/1 ms
```

マスタが故障したとき、30.1.1.0/24 内の Host が 20.1.1.0/24 内の Host と通信できることを確認してください。

[AC2] ping -a 30.1.1.1 20.1.1.1

```
Ping 20.1.1.1: 56  data bytes, press CTRL_C to break
Reply from 20.1.1.1: bytes=56 Sequence=1 ttl=254 time=2 ms
Reply from 20.1.1.1: bytes=56 Sequence=2 ttl=254 time=1 ms
Reply from 20.1.1.1: bytes=56 Sequence=3 ttl=254 time=1 ms
Reply from 20.1.1.1: bytes=56 Sequence=4 ttl=254 time=1 ms
Reply from 20.1.1.1: bytes=56 Sequence=5 ttl=254 time=1 ms

--- Ping statistics for 20.1.1.1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.00% packet loss
round-trip min/avg/max/std-dev = 1/1/2/1 ms
```

目次

このセクションのページは **14-x-x** です。

3 章 クラウドクラスタ 3-1
3.1 クラウドクラスタについて 3-1
3.1.1 概要 3-1
3.1.2 メリット 3-3
3.2 制限とガイドライン 3-4
3.3 クラウドプラットフォームの構成要素 3-4
3.4 物理クラスタの動作メカニズム 3-5
3.4.1 物理クラスタの基本概念 3-5
3.4.2 物理クラスタの接続トポロジ 3-7
3.4.3 物理クラスタの確立と変更 3-8
3.4.4 Leader の役割の選択 3-12
3.4.5 物理クラスタの分割 3-14
3.4.6 物理クラスタの結合 3-15
3.5 コンテナクラスタの動作メカニズム 3-16
3.5.1 コンテナクラスタの基本概念 3-16
3.5.2 コンテナクラスタの接続トポロジ 3-18
3.5.3 コンテナクラスタの確立 3-19
3.5.4 コンテナの監視とインテリジェントな管理 3-20
3.5.5 マスタコンテナの選択 3-20
3.5.6 コンテナクラスタの分割と MAD 3-21
3.5.7 コンテナクラスタの結合 3-26
3.6 クラウドクラスタの設定手順 3-26
3.7 クラウドクラスタの設定 3-26
3.8 物理クラスタの移動 3-27
3.8.1 物理クラスタ A からデバイスを削除 3-28
3.8.2 デバイスを物理クラスタ B に追加 3-28
3.9 物理クラスタの表示と維持 3-29
3.10 MAD の設定 3-29
3.10.1 LACP MAD の設定 3-29
3.10.2 MAD shutdown によるシャットダウンからの除外 3-30
3.10.3 コンテナクラスタの回復 3-31
3.11 コンテナクラスタ設定の最適化 3-31
3.11.1 ソフトウェアイメージ同期のためのソフトウェア自動更新の有効化 3-31
3.11.2 コンテナクラスタのブリッジ MAC アドレスの保持設定 3-32
3.11.3 コンテナクラスタのリンクダウンイベントの通知遅延 3-33
3.11.4 クラウドクラスタの自動結合の有効化 3-34
3.12 WLAN アクセスのためのクラウドクラスタの最適化 3-35
3.12.1 WLAN アクセスのためのクラウドクラスタの最適化の設定 3-35
3.13 コンテナクラスタの表示と維持 3-35
3.14 コンテナクラスタへのアクセス 3-35
3.15 クラウドクラスタの設定例 3-36
3.15.1 クラウドクラスタの設定 3-36
3.15.2 障害のある物理デバイスの交換 3-40
3.15.3 クラスタリンク障害時の割り当てインタフェースの変更 3-43

3.15.4 物理クラスタの別のクラウドクラスタへの移行 3-47

3章 クラウドクラスタ

3.1 クラウドクラスタについて

⚠ **注意：**

クラウドクラスタとデュアルリンクバックアップ機能は併用できません。

🕮 **メモ：**

- QX-W2300AC シリーズは最大 2 台の装置でクラウドクラスタを構築形成することができます。
- QX-W2310AC と QX-W2330AC の組み合わせでのクラウドクラスタ構成は未サポートです。クラウドクラスタを構築する場合、必ず同じ機種同士で設定してください。
- クラウドクラスタは Comware 9 ベースのコンテナクラスタのみをサポートしています。特に明記されていない限り、このドキュメントにおける 「コンテナ」 という用語は、Comware 9 ベースのコンテナを指します。
- AP ホットバックアップ、クライアントホットバックアップの設定については、*1 章 WLAN 高可用性* を参照ください。

クラウドクラスタは、QX 独自のソフトウェア仮想化テクノロジです。アプリケーションと物理デバイスを可能な限り分離するために、Comware 9 コンテナ構成を使用しています。Comware 9 ベースのクラウドクラスタは、次のレイヤに分けられます。

- **物理クラスタ**：物理デバイスレイヤのクラスタを示します。物理クラスタリンクの中心的な考え方は、複数の物理デバイスを接続して 1 つのデバイスに仮想化することです。この仮想化技術を使用すると、複数のデバイスのハードウェアリソースを統合できます。さらに、複数のデバイスのハードウェアリソースの一元的な管理と割り当てが可能になり、リソース使用率が向上し、管理の複雑さが軽減されます。また、ハードウェアレベルのバックアップを実現することにより、システム全体の信頼性が向上します。
- **コンテナクラスタ**：コンテナ（アプリケーションレイヤ）のクラスタを示します。コンテナクラスタ化の中心的な考え方は、物理デバイス上で実行されているコンテナを論理的に接続して 1 つのシステムに仮想化することです。この仮想化技術を使用すると、複数のコンテナのソフトウェア処理機能を統合できます。複数のコンテナの共同運用、統合管理、中断のないメンテナンスを可能にします。

3.1.1 概要

I. 基本的なネットワークアプリケーション

物理デバイスはコンテナと 1 対 1 で対応しており、各物理デバイス上で 1 つのコンテナが実行されます。物理デバイスをクラスタ化してデバイスレベルのバックアップを形成することも、コンテナをクラスタ化してサービスレベルのバックアップを形成することも

できます。物理クラスタ全体がコンテナクラスタに対応することで、簡単なトポロジ、簡単な設定、簡単なメンテナンスが提供されます。

図 3-1 に示すように、2 つのデバイスをクラスタリンクで接続して物理クラスタを形成します。2 つの物理デバイスが 1 つのネットワークデバイス (図 3-1 の Container cluster に対応) に仮想化され、すべてのメンバデバイス上のリソースを所有および管理します。

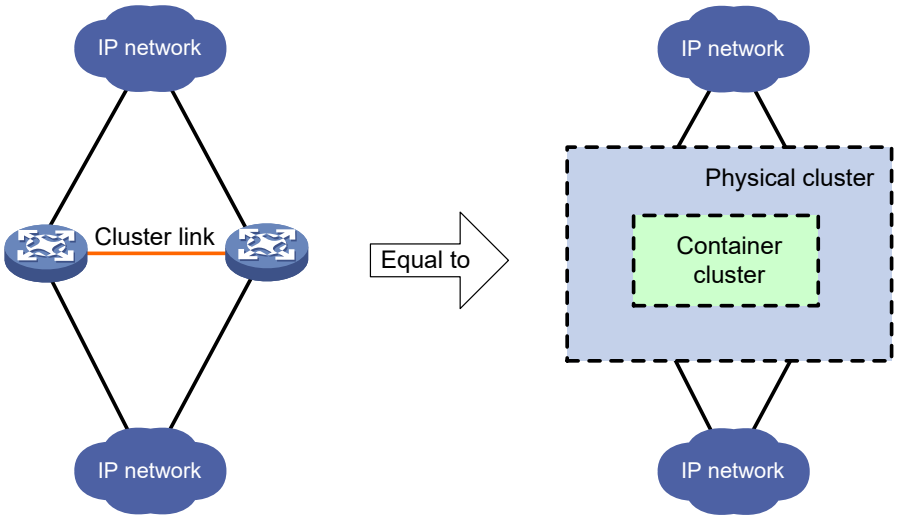


図 3-1 基本的なネットワークアプリケーション

II. クラウドクラスタの構成

図 3-2 に、クラウドクラスタの物理構成を示します。物理クラスタとコンテナクラスタの関係は次のとおりです。

- クラウドプラットフォームモジュール（Cloud platform）は物理デバイス上で動作します。クラウドプラットフォームモジュールは、QX に最適化された Linux システム上で直接動作します。物理デバイス上のクラウドプラットフォームモジュールは、IP チャネルを介して相互に通信し、これらの物理デバイスを物理クラスタに仮想化します。

- コンテナ（Comware container）はクラウドプラットフォームモジュール上で動作し、クラウドプラットフォームモジュールによって管理されます。物理デバイス上のコンテナは、LIPC/MBUS チャネルを通じて相互に通信し、コンテナをコンテナクラスタに仮想化します。コンテナはルーティングやスイッチングなどの基本的な通信機能を提供します。

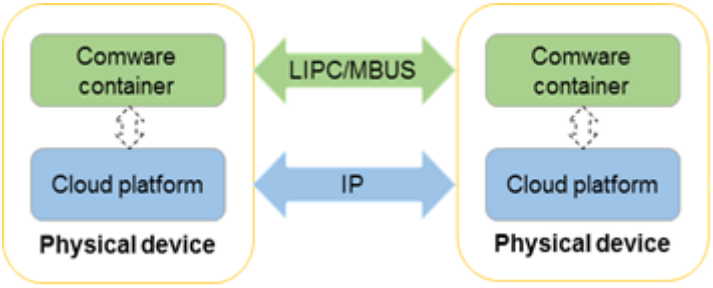


図 3-2 物理構成

図 3-3 に、クラウドクラスタの論理構成を示します。クラウドクラスタは物理デバイスを物理クラスタ（Physical cluster）とコンテナクラスタ（Container cluster）を持つデュアルクラスタ構成です。

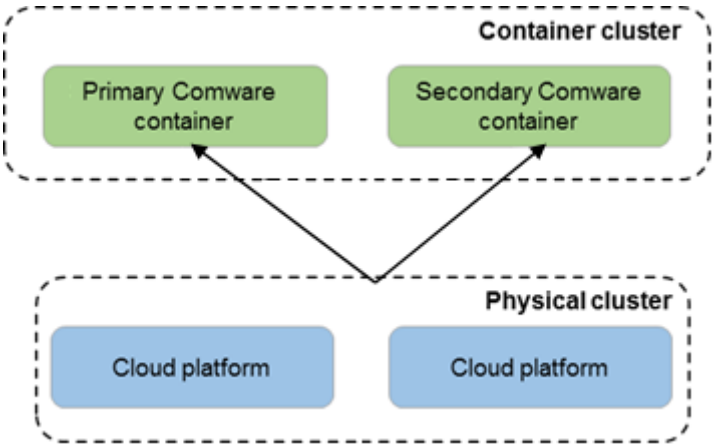


図 3-3 論理構造

3.1.2 メリット

I. クラウドクラスタ全体のメリット

- **Dual-layer virtualization architecture**:クラウドクラスタは、物理クラスタとコンテナクラスタを備えた 2 層の仮想化構成を使用します。これにより、クラウドクラスタシステム全体の柔軟性が次のように向上します。
  - 物理クラスタは、コンテナクラスタのオーケストレーションおよび管理プラットフォームとして機能しながら、物理デバイスの統合管理を実現します。
  - コンテナクラスタは、サービスに対して高い信頼性とインテリジェントなエラスティックスケーリングを提供します。
- **Dual-layer selection of primary containers**:クラウドクラスタは、次のような 2 層プライマリコンテナの選択を採用することで、サービス運用の安定性を向上させます。

- □ 物理クラスタが正常に動作している場合、コンテナクラスタ内のプライマリコンテナは物理クラスタによって選択され、維持されます。
- □ 物理クラスタが正常に動作していない場合、コンテナクラスタのロールはコンテナクラスタ内のロール選択メカニズムによって選択されます。

- **Simplified management**:クラウドクラスタの構築後、ユーザは任意のメンバデバイスの任意のポートを介してクラウドクラスタシステムにログインし、クラウドクラスタ内のすべてのメンバデバイスとコンテナを管理できます。

II. コンテナクラスタレイヤのメリット

- 1:N コンテナバックアップ：コンテナクラスタは複数のコンテナで構成されます。プライマリコンテナはコンテナクラスタの運用、管理、保守を担当し、他のコンテナはバックアップとしてサービスを処理することもできます。プライマリコンテナに障害が発生すると、システムは迅速かつ自動的に新しいプライマリコンテナを選択し、中断のないサービス運用を保証します。これにより、コンテナの 1:N バックアップが実現されます。

- コンテナ間のリンクアグリゲーション: クラウドクラスタを構成する異なるデバイス間でリンクアグリゲーションをサポートします。異なるコンテナ上の異なる物理リンクを論理リンクに集約することができます。物理リンクは相互にバックアップしたり、トラフィック負荷を共有したりすることができます。コンテナがコンテナクラスタを離れる場合でも、他のコンテナ上のリンクはパケットを送受信できるため、集約されたリンクの信頼性が向上します。

- 強力なネットワーク拡張機能 : 物理デバイスを追加することで、コンテナクラスタのインタフェース数と帯域幅を増やすことができます。また、各メンバデバイスには、独自にプロトコルパケットを処理し、パケットを転送するための CPU が搭載されているため、コンテナクラスタは柔軟かつ容易に処理能力を拡張できます。

3.2 制限とガイドライン

クラウドクラスタ構成装置を含むデュアルリンクバックアップ構成では AP ライセンス同期機能は使用できません。

3.3 クラウドプラットフォームの構成要素

デバイス内でクラウドクラスタ機能を実現する構成要素を総称してクラウドプラットフォームと呼びます。クラウドプラットフォームは、次の 4 つで構成されています。

- Cloud platform Manager：物理クラスタの管理に参加する各物理ノードのホストオペレーティングシステムで実行されます。クラウドプラットフォームの高可用性 (HA) 機能、クラスタの確立、およびクラスタメンバの管理を実行します。次の機能がサポートされています。
  - □ 物理クラスタの管理、確立、保守、クラスタメンバの管理、およびクラスタトポロジの生成と更新。

- コンテナクラスタの管理。Manager は、物理クラスタ内のハードウェアリソースの配分に基づいてコンテナをインテリジェントに展開し、コンテナクラスタのプライマリおよびセカンダリコンテナを選択できます。

- Cloud platform Worker : 各物理デバイスのホストオペレーティングシステムで実行されます。物理デバイスとコンテナのライフサイクルを管理します。Worker は、デバイスの物理リソースと状態を定期的に報告し、Manager からのスケジュール指示に応答し、Manager からの指示に基づいてコンテナを作成します。

- Cloud platform Admin：各物理デバイスで実行されます。プライマリコンテナから設定メッセージを受信して処理します。Admin は、デバイスの動作モードとコンテナの説明ファイルを管理し、コンテナの展開を実行するための要求を Manager に送信します。

- Cloud platform Agent：コンテナで実行されます。Agent は、コンテナ内のサービスのヘルスステータスを報告し、サービスモジュールクラスタとコンテナのイベントを通知します。

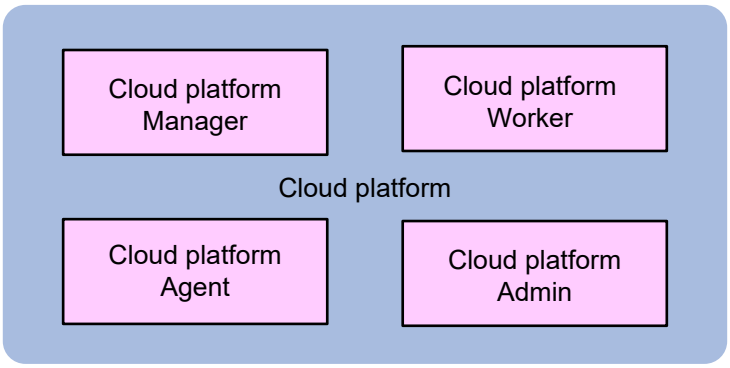


図 3-4 クラウドプラットフォームの構成要素

3.4 物理クラスタの動作メカニズム

3.4.1 物理クラスタの基本概念

I. メンバデバイスの役割

物理クラスタ内のすべてのデバイスをメンバデバイスと呼びます。メンバデバイスは、異なる機能に基づいて 2 つのロールに分けられます。

- Manager:クラウドプラットフォームの高可用性 (HA) 機能を担当し、クラスタメンバを確立および管理します。次の機能が含まれます。
  - 物理クラスタの管理、確立および保守、クラスタメンバの管理、クラスタトポロジの生成および更新。
  - コンテナクラスタの管理、物理クラスタ内のハードウェアリソースの分散に基づいたコンテナのインテリジェントなデプロイ、コンテナクラスタのプライマリおよび下位コンテナの選択。

Manager は、さらに権限に応じて Leader と Follower に分けられます。

- Leader:プライマリマネージャとして、クラウドクラスタ全体の管理と制御を担当し、クラウドクラスタ全体のコントロールセンターとして機能します。
- Follower:バックアップマネージャとして、Leader のバックアップを行います。Leader のバックアップデバイスとして実行され、ビジネスを処理してメッセージを転送します。Leader に障害が発生すると、システムは自動的に Fllower から新しい Leader を選択して、元の Leader の作業を引き継ぎます。

デバイスが Manager として構成されている場合、デバイスは自動的にマネージャーコンポーネントを実行して、関連するマネージャ機能を実行します。

- Worker:ローカルノードの管理、Leader へのノードリソースの報告、および Leader からのコンテナ展開のスケジュールメッセージの受信を担当します。デバイスが Worker として構成されている場合、デバイスはワーカーコンポーネントを自動的に実行して、関連するワーカー機能を実行します。

物理クラスタの初回作成時に、ネットワーク管理者は、Manager が展開されている物理デバイスと、物理デバイスの Leader と Follower の役割を決定します。物理クラスタの操作中に Leader に障害が発生した場合、物理クラスタは自動的に新しい Leader を再選出します。

II. メンバ ID

クラウドクラスタでは、物理デバイスはメンバ ID によって一意に識別され、メンバ ID は物理クラスタとコンテナクラスタの両方のセットアップとメンテナンス時に使用されます。

クラウドクラスタでは、1 つのデバイスだけがデフォルトのメンバ ID を使用でき、他のすべてのデバイスはクラスタに参加する前にメンバ ID を変更する必要があります。メンバ ID を変更する場合は、クラウドクラスタ内で一意であることを確認してください。

- 物理クラスタのセットアップ中に、2 つのデバイスが同じメンバ ID を持つ場合、後で登録するデバイスは物理クラスタに参加できません。
- 物理クラスタの操作中に、新しいデバイスが参加しようとしても、そのメンバ ID が既存のメンバ ID と競合する場合、デバイスは物理クラスタに参加できません。

III. メンバの IP アドレス

メンバの IP アドレスは、物理クラスタ内の内部通信、特に物理クラスタプロトコルメッセージ (レイヤ 3 IP パケット) の交換に使用されます。物理クラスタ内のすべてのメンバデバイスは、メンバ IP アドレスを使用して設定する必要があり、すべてのメンバ IP アドレスは同じネットワークセグメントに属する必要があります。すべてのメンバデバイスがレイヤ 3 で相互に到達できることを確認します。

IV. クラスタ IP アドレス

クラスタ IP アドレス、物理クラスタに参加するようにデバイスを誘導するために、デバイスの管理者が設定する IP アドレスです。物理クラスタ内の既存のメンバデバイスのメンバ IP アドレスをクラスタ IP アドレスにすることができます。ベストプラクティスとして、Leader とするメンバ IP アドレスをクラスタ IP として設定します。

物理クラスタの初期設定時は、Leader のクラスタ IP を設定する必要はありません。クラスタ IP を設定していないデバイスは、自身を Leader と見なします。

V. 物理クラスタの分割

図 3-5 に示すように、物理クラスタの形成後にリンク障害が発生し、物理クラスタ内の隣接する 2 つのメンバデバイスが切断されると、物理クラスタは 2 つの物理クラスタに分割します。このプロセスを物理クラスタの分割と呼びます。

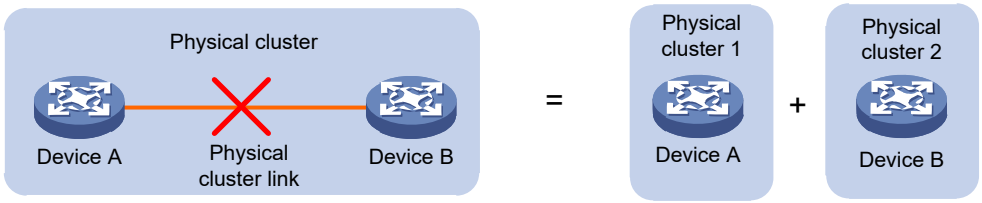


図 3-5 物理クラスタの分割

VI. 物理クラスタの結合

図 3-6 に示すように、リンク障害が修復されると、分割した物理クラスタは自動的に結合します。このプロセスを物理クラスタの結合と呼びます。

分裂した物理クラスタは元のクラスタトポロジを保持し、障害が復旧されると分裂前の物理クラスタ構成でのみ再結合します。異なる物理クラスタが存在していても、結合することはできません。

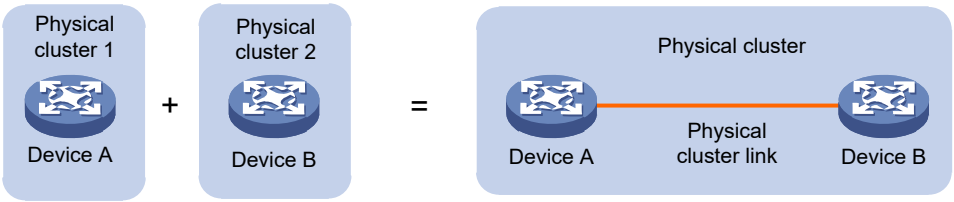
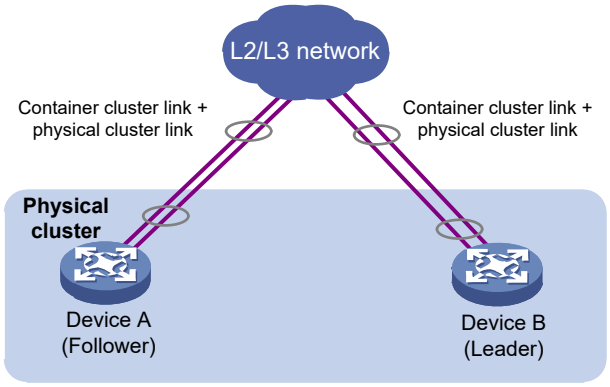


図 3-6 物理クラスタの結合

3.4.2 物理クラスタの接続トポロジ

物理クラスタの制御パケットは、レイヤ 3　IP パケットです。物理クラスタでは、メンバデバイスを同じネットワークセグメントに設定し、このネットワークセグメントを使用して物理クラスタ制御パケットを交換する必要があります。物理クラスタの接続トポロジはスター型の接続です。スター型の接続は、メンバデバイスが物理的に集中しているネットワークに適していますが、図 3-7 に示すように、メンバデバイス間の相互接続を完了するために中間デバイスが必要です。



Star topology

図 3-7 接続トポロジ

メモ:

物理クラスタはコンテナクラスタリンクの制御チャネルを使用して、物理クラスタ制御パケットを送信します。コンテナクラスタネットワークを設定するには、ネットワーク管理者はコマンドを使用して、デバイス上のコンテナクラスタリンクの制御チャネルおよびデータチャネルに物理インタフェースを割り当てる必要があります。制御チャネルは、クラウドクラスタ間で物理クラスタ制御パケットおよびコンテナクラスタ制御パケットを送信するために使用され、データチャネルは、コンテナ間のデータパケットを転送するために使用されます。

3.4.3 物理クラスタの確立と変更

I. 物理クラスタの確立

物理クラスタを確立するためには、最初にデバイス ID を設定する必要があります。物理クラスタを構築するときは、まず物理クラスタの管理に参加するデバイス、リーダデバイス、メンバ ID、およびクラスタ内の内部通信に使用されるネットワークセグメントを含むクラスタの設計について計画します。

Manager のリーダデバイスに次のパラメータを設定します。

- (オプション)メンバ ID。デフォルト値を使用できます。
- (必須) メンバ IP

その後、デバイスを再起動します。デバイスは Leader として機能し、次のように動作します。

1) デバイスは、設定ファイルに従ってクラウドプラットフォームの Admin、Manager、および Worker コンポーネントを起動します。
2) リーダデバイスは、ワーカーデバイスとの内部通信チャネルを確立します。ワーカーデバイスはリーダに登録し、ハードウェアリソース情報を報告します。
3) リーダは、コンテナを起動するようにワーカーに通知します。

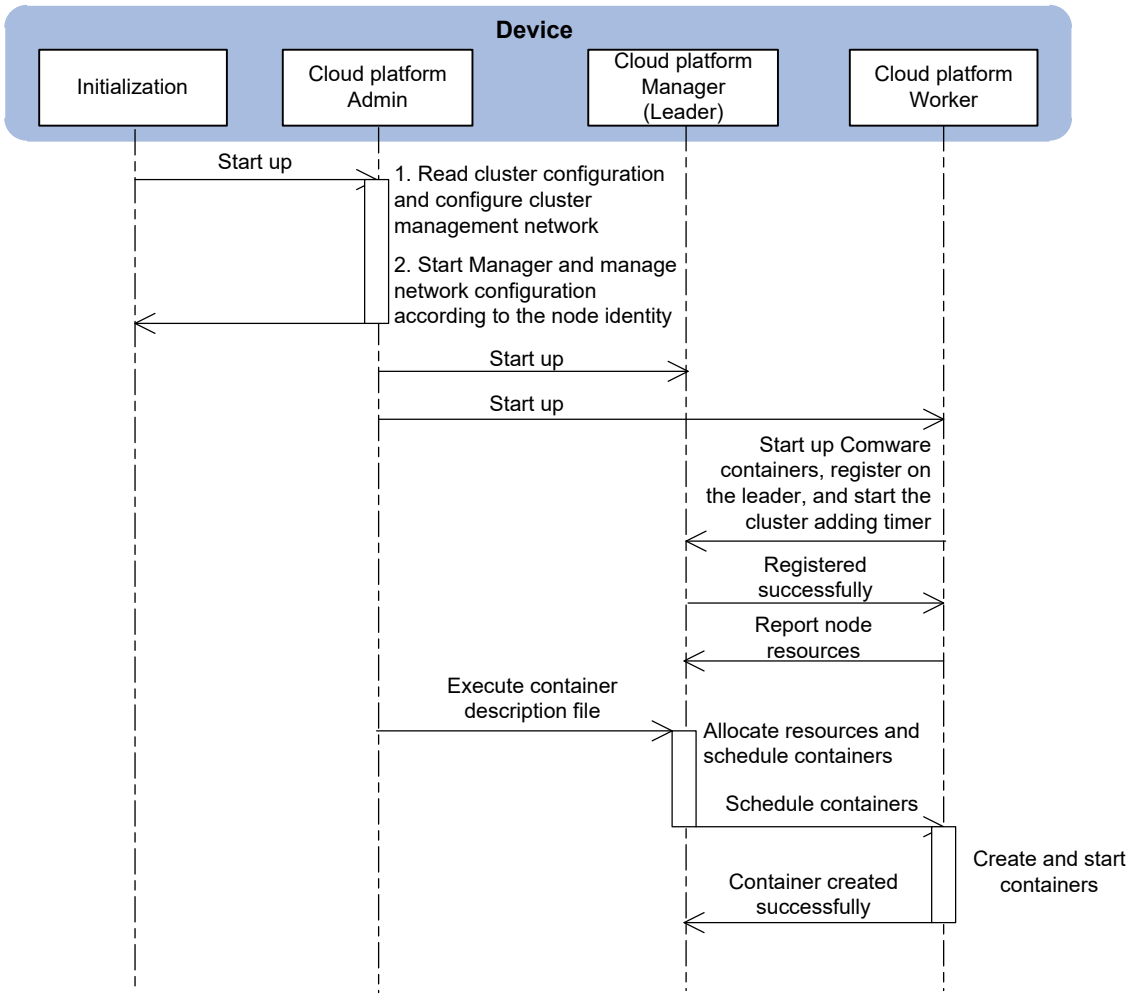


図 3-8 Leader の確立プロセス

II. 物理クラスタへの新しいデバイスの参加

物理クラスタに新しく参加するデバイスも、設定によって ID を決定します。

Manager ロールのフォロワーデバイスの場合は、次のパラメータを設定する必要があります。

- (必須) メンバ ID は、クラスタ内で一意である必要があります。
- (必須) メンバ IP は、リーダデバイスのメンバ IP と同じネットワークセグメント内にあり、互いに通信可能である必要があります。
- (必須) クラスタ IP に参加します。ベストプラクティスとして、リーダデバイスのメンバ IP をクラスタ IP に参加するように指定します。他のメンバデバイスのメンバ IP にすることもできます。

Worker ロールのデバイスの場合、次のパラメータを設定する必要があります。

- (必須) クラスタ内で一意である必要があるメンバ ID
- (必須) リーダデバイスのメンバ IP と同じネットワークセグメント内にあり、互いに通信可能である必要があるメンバ IP

- (必須) クラスタ IP に参加します。ベストプラクティスとして、リーダデバイスのメンバ IP をクラスタ IP に参加するように指定します。他のメンバデバイスのメンバ IP にすることもできます。

次の手順では、フォロワーデバイスがクラスタに参加するプロセスを例として説明します。マネージャーコンポーネントを除くフォロワーデバイスの起動プロセスは、ワーカーデバイスの起動プロセスと同じです。

フォロワーデバイスを構成した後、再起動するとデバイスが設定を読み読み込みます。設定にはクラスタ IP が含まれているため、デバイスはフォロワーデバイスとして起動し、クラスタ参加要求をクラスタ IP に送信します。

- クラスタ IP がリーダデバイスのメンバ IP の場合、リーダデバイスはクラスタ参加要求を受信し、参加の成功を示す応答をユニキャストします。
- クラスタ IP がクラスタ内の別のフォロワーデバイスのメンバ IP の場合、フォロワーデバイスは参加要求をリーダデバイスに転送します。リーダデバイスは、新しいデバイスへの参加が成功したことを示す応答をユニキャストします。

図 3-9 に示すように、物理クラスタに参加している新しいデバイス、デバイス B、デバイス A の起動プロセスは次のとおりです。

1) デバイス B は、設定ファイルに基づいてクラウドプラットフォームの Admin、Manager、および Worker コンポーネントを起動します。
2) ワーカーコンポーネントは自動的に Comware コンテナを起動し、Manager (Follower) と Worker は自動的に Leader に登録してクラスタ参加タイマーを開始します。
3) デバイス A は物理クラスタの Leader であり、Manager (Follower) と Worker に正常な参加メッセージで応答します。
4) Leader は、Hello パケットをメンバに定期的にユニキャストします (正常な Leader として通知します) 。
5) Hello パケットを受信すると、デバイス B は Leader の情報を記録し、ローカルの物理リソース情報を Leader に報告します。
6) ネットワーク管理者がコンテナを作成するコマンドを発行すると、Leader は各メンバデバイスから報告されたリソース情報に基づいて、デバイス B がコンテナを作成して起動するようにスケジュールします。
7) デバイス B のコンテナが正常に起動されると、Worker コンポーネントはコンテナの情報を Leader に報告します。
8) Leader は、Follower が Leader のバックアップとして機能できるように、物理クラスタ情報をデバイス B のマネージャーコンポーネントと同期します。Leader は、現在のクラウドクラスタ内の他のコンテナに関する情報もデバイス B のワーカーコンポーネントと同期します。

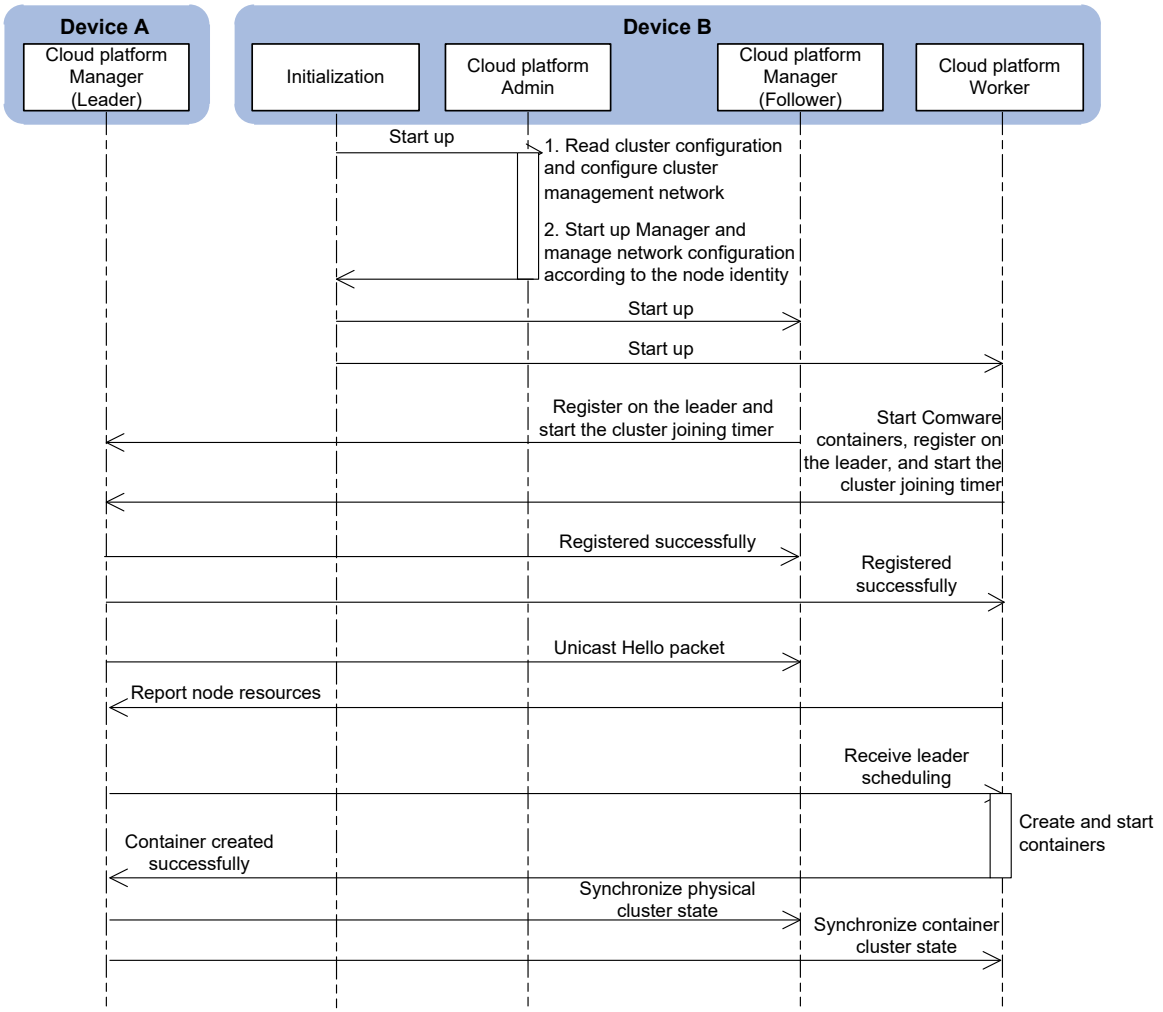


図 3-9 物理クラスタへの新しいデバイスの参加

III. メンバデバイスの物理クラスタからの離脱

物理クラスタが正常に確立されると、Leader はクラスタ内のすべての Manager と Worker の情報を記録し、接続に基づいてクラスタトポロジを構成します。Leader と Follower の関係は、相互作用する Hello パケットによって維持されます。メンバデバイスは、物理クラスタをアクティブに離れることも、強制的に離れることもできます。

- アクティブな離脱
  アクティブな離脱とは、管理者が cloud-cluster member view で undo join-cluster コマンドを実行して、物理クラスタからデバイスを削除するシナリオを指します。デバイスは離脱クラスタメッセージを Leader に送信し、Leader は離脱クラスタ応答メッセージで応答します。次に、Leader は物理クラスタデバイスリストと物理クラスタトポロジからデバイスを削除します。最後に、更新された物理クラスタ情報とクラスタトポロジが他の Follower に同期されます。
- パッシブな離脱
  物理クラスタからのメンバデバイスのパッシブ離脱とは、メンバが Leader のメンバ IP に到達できないシナリオを指します（制御パケットが相手側に到達できません）。メンバデバイスが物理クラスタを受動的に離れるプロセスは、次のとおりです。

a) Leaderは定期的にHelloパケットをユニキャストして、そのステータスをすべてのフ

ォロワーに通知します。Helloパケットの送信期間は1秒で、Helloパケットのタイムアウト時間は10秒に設定されています。これらの設定は変更できません。

b) 各フォロワーは、ローカルに選出タイマを作成します。選出タイマがタイムアウトする前にHelloパケットを受信した場合、Leaderは正常に実行されていると見なされ、FollowerはHello応答パケットで応答します。

c) Leaderが特定のFollowerからHello応答パケットを10秒間受信しない場合、Leaderは Followerが一時的に物理クラスタを離れたと見なし、Followerの状態をオフラインに設定します。Leaderが10秒以内にHello応答パケットを受信した場合、タイマを0秒から再スタートします。

d) 選出タイマがタイムアウトするまでFollowerがLeaderからHelloパケットを受信しない場合、Leaderは失敗したと見なします。Followerはリーダーロールの選択プロセスに入ります。

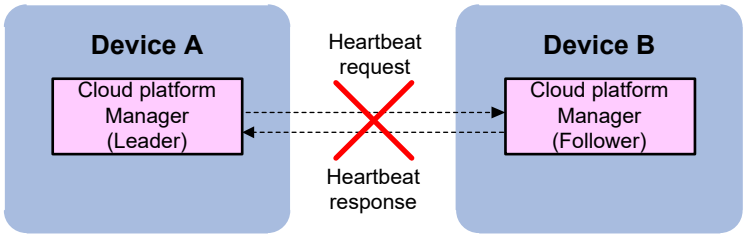


図 3-10 パッシブな離脱

3.4.4 Leader の役割の選択

次のような場合は、すべての Manager が Leader の役割の選択に参加し、Raft アルゴリズムに基づいて Leader を選択します。

· Leader が物理クラスタを離れるか、失敗します。

· 物理クラスタ全体が再起動します。

· 物理クラスタが分割されます。

· 独立して実行されている 2 つの物理クラスタが 1 つの物理クラスタに結合されます。

Raft アルゴリズムの基本原則は、多数派が勝利し、少数派が失敗することです。クラスタの初期設定時に、Leader は設定によって決定されます。メンバデバイスがクラスタに参加または離脱すると、Leader は直ちに、メンバデバイスの数 (n と仮定)、情報、およびクラスタのトポロジをすべての Manager に同期します。したがって、すべてのメンバデバイスは、物理クラスタ内のデバイスの存在を認識します。

物理クラスタがリーダーロールの選択を開始する場合、リーダーロールの選択のルールは次のとおりです。n/2 を超える選出数を持つ Manager が Leader になり、他の Manager がフォロワーになります。選出のラウンドの期間は、選出タイマによって制御されます。選出のラウンドで Leader を選択できなかった場合は、Leader が選択されるまで別のラウンドが開始されます。

図 3-11 に Manager のロール移行プロセスを示します。Leader の選出プロセスは次のとおりです。

1) Manager がフォロワーとして起動し、選出タイマを開始した後、または Follower がプローブメッセージを送信して到達可能なメンバデバイスの数を検出した後:
   - □ 検出された到達可能なメンバの数が、デバイスによって記録されたメンバの総数の半分以下の場合、デバイスはリーダーロールの選出を開始しません。デバイスは引き続き Follower として実行され、到達可能なメンバデバイスの数を定期的にプローブします。
   - □ 検出された到達可能なメンバの数が、デバイスによって記録されたメンバの総数の半分を超える場合、デバイスはリーダーロールの選択をトリガーします。次に、他のメンバに選出要求を送信し、候補者状態に切り替えます。

   選出タイマのメンテナンス中に、選出タイマがタイムアウトしても Leader から Hello メッセージが受信されない場合、デバイスはプローブメッセージを送信して、到達可能なメンバデバイスの数を検出します。
2) 候補者の状態で、デバイスが現在の Leader またはより高い期間の Leader から Hello メッセージを受信すると、選択タイムアウトタイマがリセットされ、Follower にダウングレードされます。
   期間は、物理クラスタでの Leader の選択に使用される重要なパラメータです。値 1 から始まり、デバイスが Leader として選択されるたびに 1 ずつ増加します。
   Leader は、物理クラスタ内のすべての Follower と期間を同期するため、同じ物理クラスタ内のすべての Manager は同じ期間を持ちます。
3) 候補者の状態では、デバイスの選出タイマが期限切れになり、デバイスによって受信された選出数がまだメンバの総数の半分以下である場合)、新しい選出ラウンドが開始されます。デバイスはその期間を 1 つ増やし、候補者の状態のままにします。
4) 候補者の状態では、デバイスの選出タイマが期限切れになり、デバイスが受信した選出数がメンバの総数の半分を超えた場合、デバイスが Leader として選出されます。デバイスは選出タイマを削除し、他のメンバデバイスに Hello メッセージを送信して Leader の役割を通知し、Leader の状態に切り替えます。
5) Leader の状態で、デバイスがより高い期間の Leader から Hello メッセージを受信すると、デバイスは Follower にダウングレードし、選出タイマを作成します。

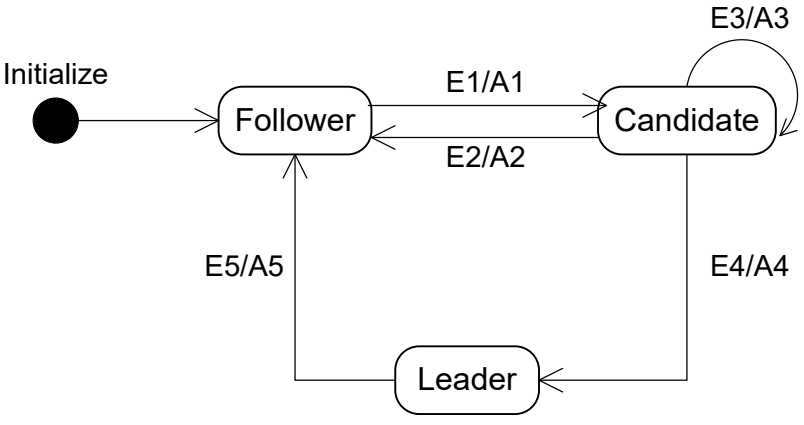


図 3-11 Manager の役割移行

イベントコード	説明
E1	選出タイマが期限切れになりました。

イベントコード	説明
A1	再選出が開始されました。 他のメンバに投票要求を送信します。
E2	現在LeaderまたはよりLeaderからHelloパケットを受信しました。
A2	選出タイマをリセットします。
E3	選出タイムアウトタイマが期限切れになりました。
A3	新しい投票ラウンドが開始されます。期間が1つ増加します。
E4	多数の票を得ました。
A4	選出タイマを削除し、他のメンバに通知を送信しました。
E5	より高い期間のLeaderを検出しました。
A5	選出タイマを作成しました。

3.4.5 物理クラスタの分割

物理クラスタの操作中、クラスタ内の Leader、Follower、および Worker は、クラスタ関係を維持するために、定期的に Hello メッセージを相互に送信します。Hello メッセージがタイムアウトし、一方がもう一方から応答をまだ受信していない場合、それは失敗と見なされ、もう一方のエンドの状態はオフラインに設定されます。

物理クラスタが形成されると、メンバデバイス間のリンクに障害が発生し、Hello メッセージが宛先に到達できない場合、物理クラスタは 2 つの個別の物理クラスタに分割されます。このプロセスはクラスタ分割と呼ばれます。分割後は、両方の物理クラスタが正常に機能しなくなります。

正常に機能するとは、物理クラスタを維持し、物理クラスタに配置されたコンテナを管理できることを意味します。正常に機能しないとは、物理クラスタを維持できても、物理クラスタに配置されたコンテナを管理できないことを意味します。

図 3-12 に示すように、メンバの合計数は 2 です。分割後は、物理クラスタ 1 と物理クラスタ 2 の両方のメンバが 1 つだけになります。すべてのメンバデバイスは多数決投票をできず、Follower としてのみ機能できます。両方の物理クラスタが正常に機能しません。

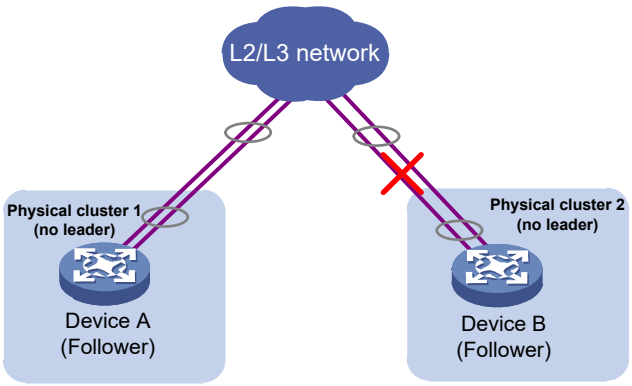


図 3-12 分割によりどちらのメンバにも Leader が存在しない状態

3.4.6 物理クラスタの結合

2 つの物理クラスタは安定しており、独立して動作しています。これらの物理クラスタが相互接続されて 1 つの物理クラスタを形成する場合、このプロセスは物理クラスタの結合と呼ばれます。

1 つの物理クラスタに結合できるのは、同じサブネット内のメンバ IP を持つ物理クラスタだけです。異なるサブネット内のメンバ IP を持つ物理クラスタは、レイヤ 3 ルーティングが到達可能であっても、1 つの物理クラスタに結合できません。

Raft アルゴリズムによって、新しい Leader がフォロワーの間で選出されます。図 3-13 に示すように、デバイス A とデバイス B が最初に物理クラスタを形成し、デバイス B が Leader であるとします。デバイス A とデバイス B の間のクラスタリンクが失敗すると、クラスタは 2 つのクラスタに分割されます。ただし、両方のクラスタのメンバデバイスの数が 2/2 を超えないため、どちらのクラスタでも Leader を選択できません。デバイス A とデバイス B の間のクラスタリンクが復元されると、デバイス A とデバイス B は互いに投票要求メッセージを受信できます。最初に投票応答を受信した人が Leader になり、他のメンバは Follower として機能します。図では、デバイス A が最初に投票応答を受信し、Leader として選出されたとします。

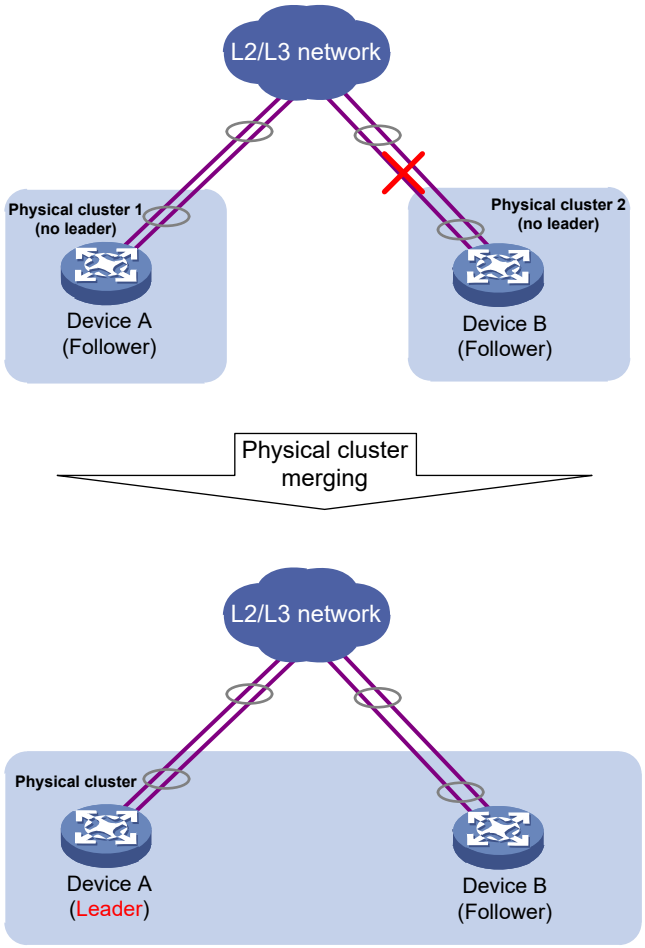


図 3-13 Leader を含まない 2 つのクラスタの結合

3.5 コンテナクラスタの動作メカニズム

3.5.1 コンテナクラスタの基本概念

I. 操作モード

Comware 9 コンテナは出荷時のデフォルト設定でクラスタモードを使用し、他の Comware 9 コンテナとのコンテナクラスタの形成をサポートします。単独で実行されている単一の Comware 9 コンテナもコンテナクラスタと見なされますが、メンバは 1 つです。

II. メンバコンテナの役割

コンテナクラスタ内の各コンテナは、メンバコンテナと呼ばれます。メンバコンテナは、それぞれの機能に応じて次の役割に分けられます。

- マスタコンテナ：コンテナクラスタ全体の管理と制御を担当します。
- スタンバイコンテナ：タスクの処理とパケットの転送中に、マスタコンテナのバックアップコンテナとして実行されます。マスタコンテナに障害が発生すると、システムはスタンバイコンテナから新しいマスタコンテナを自動的に選択します。

物理クラスタが正常に動作している場合、マスタコンテナとスタンバイコンテナの役割は、物理クラスタの Leader によって決定されます。物理クラスタに障害が発生すると、マスタデバイスとスタンバイデバイスの両方が選択されます。

一度に 1 つのマスタコンテナだけがコンテナクラスタに存在し、他のすべてのメンバコンテナはスタンバイコンテナです。

III. コンテナ ID

コンテナクラスタには、コンテナ ID によって一意に識別される複数のコンテナが含まれる場合があります。メンバコンテナ ID は、物理クラスタの Leader によって一様に割り当てられます。

クラウドクラスタでは、メンバ ID を使用して物理デバイスを一意に識別します。メンバコンテナは物理デバイスで実行されるため、メンバコンテナは物理デバイスのメンバ ID を使用してコンテナを一意に識別します。

クラウドクラスタでは、既定のメンバ ID を使用できるデバイスは 1 つだけであり、クラウドクラスタに追加する前に、他のデバイスのメンバ ID を変更する必要があります。メンバ ID を変更する場合は、ID がクラウドクラスタ内で一意であることを確認してください。

- 物理クラスタを設定するときに、同じメンバ ID のデバイスがある場合、後から参加したデバイスは物理クラスタに参加できません。
- 物理クラスタの運用中に、新しいデバイスが物理クラスタに参加しても、その ID が既存のメンバデバイスの ID と競合する場合、そのデバイスは物理クラスタに参加できません。

IV. コンテナクラスタ ドメイン

ドメインは論理的な概念であり、コンテナクラスタはコンテナクラスタ ドメインに対応します。

さまざまなネットワークアプリケーションに対応するために、複数のコンテナクラスタを同じネットワークに配置でき、コンテナクラスタはドメイン ID によって区別されます。図 3-14 に示すように、デバイス A とデバイス B はコンテナクラスタ 1 を形成し、デバイス C とデバイス D はコンテナクラスタ 2 を形成します。異なるコンテナクラスタをドメイン ID で分割することにより、2 つのコンテナクラスタの実行とビジネス操作を分離して維持し、相互に影響を与えることができます。

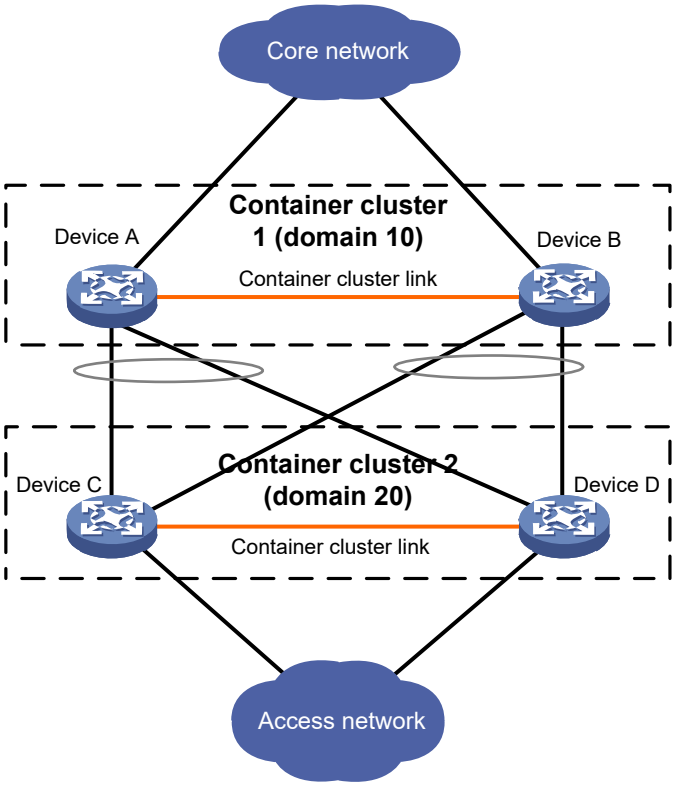


図 3-14 マルチコンテナクラスタ

V. コンテナクラスタの分割

図 3-15 に示すように、コンテナクラスタが形成されると、コンテナクラスタ間の接続に失敗して隣接する 2 つのデバイスが切断されると、コンテナクラスタは 2 つのコンテナクラスタに分割されます。このプロセスは、コンテナクラスタの分割と呼ばれます。

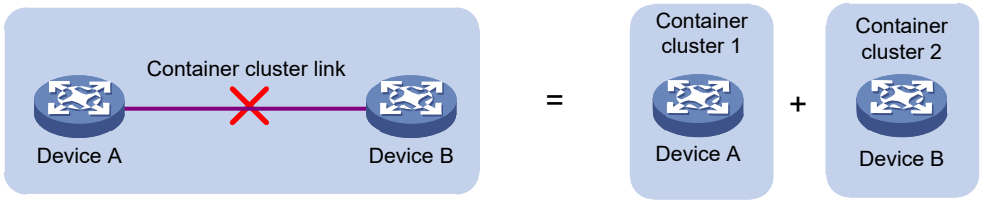


図 3-15 コンテナクラスタの分割

VI. コンテナクラスタの結合

図 3-16 に示すように、2 つのコンテナクラスタが独立して動作していて安定している場合は、物理的な接続と必要な構成を介して 1 つのコンテナクラスタに結合できます。このプロセスは、コンテナクラスタの結合と呼ばれます。

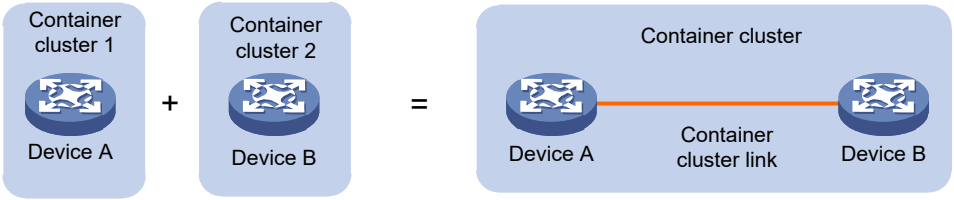
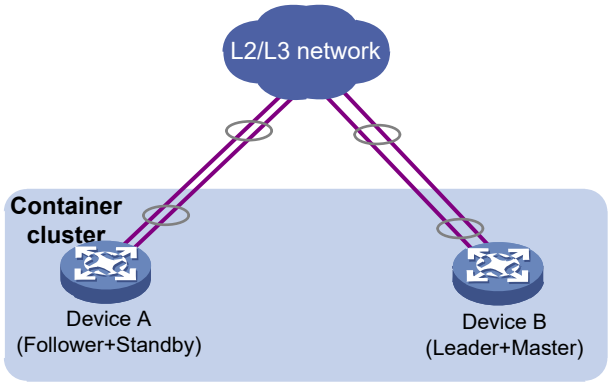


図 3-16 コンテナクラスタの結合

3.5.2 コンテナクラスタの接続トポロジ

物理クラスタはコンテナクラスタリンクの制御チャネルを共有して、物理クラスタ制御メッセージを送信します。コンテナクラスタネットワークを構築するには、ネットワーク管理者はコマンドを使用して、デバイス上のコンテナクラスタリンクの制御チャネルおよびデータチャネルに物理インタフェースを割り当てる必要があります。制御チャネルは、クラウドクラスタ間で物理クラスタ制御メッセージおよびコンテナクラスタ制御メッセージを送信するために使用され、データチャネルはコンテナ間転送データメッセージを送信するために使用されます。

図 3-17 に示すように、物理クラスタの接続トポロジにスタートポロジを使用する場合、中間デバイスはメンバデバイス間の相互接続できるように構築します。



Star topology

図 3-17 コンテナクラスタの接続トポロジ

3.5.3 コンテナクラスタの確立

クラウドプラットフォームの Worker コンポーネントは、コンテナの作成と削除を担当します。

Comware 9 コンテナは、ルーティングと転送機能を実装するために使用される、デバイスの基本的なコンテナです。したがって、デバイスは既定で Comware 9 コンテナをサポートします。物理クラスタは Comware 9 コンテナとの統合のみをサポートし、Comware 9 コンテナによる プライマリコンテナとバックアップコンテナの決定などを管理します。物理クラスタは、Docker テクノロジに基づいて他のコンテナをホストできますが、コンテナクラスタを管理することはできません。

コンテナクラスタを確立するプロセスは次のとおりです。

1) デバイスの電源を入れて起動すると、デバイスは自動的に Comware 9 コンテナの起動を試みます。コンテナ内のクラウドプラットフォームエージェントは、コンテナの作成イベントと削除イベントについて、クラウドプラットフォームの Worker コンポーネントに通知します。
2) Worker コンポーネントは、コンテナの作成イベントと削除イベントを物理クラスタ内の Leader に転送します。
3) Leader は、ノードの物理リソースの状況に基づいて、コンテナの作成または削除を許可するかどうかを決定します。許可されている場合は、コンテナの役割を決定します。最初に作成されたコンテナはマスタコンテナであり、後で作成されたコンテナはすべてスタンバイコンテナです。
4) Leader は、コンテナを作成または削除するようにワーカーに通知します。
5) Worker がコンテナを正常に作成または削除すると、作成または削除の結果が Leader に通知されます。
6) Leader は、コンテナ情報テーブル (LIP とコンテナ MAC を含む) と、保持しているコンテナトポロジ(コンテナ ID、メンバ ID、およびコンテナ MAC を含みます)を更新します。次に、更新されたコンテナ情報テーブルとコンテナトポロジをクラウドクラスタ内のすべてのコンテナに同期します。

3.5.4 コンテナの監視とインテリジェントな管理

クラウドプラットフォームリーダーは、コンテナサービスのメトリックを監視し、その値に基づいてコンテナをインテリジェントに管理します。

コンテナサービスのメトリックは、現在のコンテナの正常性状態など、コンテナで重視する必要がある重要なサービス関連の指標を参照します。コンテナサービスのメトリックは、コンテナのマスタースタンバイ選択の重要な基礎です。コンテナサービスのメトリックが異常な場合、コンテナの基本的な転送機能に影響します。

クラウドプラットフォームの物理クラスタ内の Worker コンポーネントは、コンテナサービスのメトリックの値を定期的に取得します。特定のサービスメトリックの現在の値が以前の値と異なる場合、Worker はコンテナ ID、サービスメトリック名、サービスメトリック値、およびその他の情報を物理クラスタの Leader に報告します。Leader は、それに従って情報を処理します。

コンテナの正常性は、デバイスの実際の正常性状態を反映します。正常性値が高いコンテナは、マスタコンテナとして選択される優先順位が高くなります。

3.5.5 マスタコンテナの選択

マスタコンテナの選択は、次の状況で行われます。

- コンテナクラスタが確立されます。
- マスタコンテナが脱退または失敗します。
- コンテナクラスタが分割されます。
- 独立して実行されている 2 つのコンテナクラスタが 1 つのコンテナクラスタに結合されます。

I. コンテナクラスタ確立時の選択

コンテナクラスタが初めて確立されるか、コンテナクラスタ全体が再起動されると、最初に起動されたコンテナがマスタコンテナになります。他のコンテナはスタンバイコンテナになります。したがって、コンテナクラスタ全体が再起動した後、別のコンテナがマスタコンテナとして選択される可能性があります。

II. マスタコンテナの脱退、障害、またはクラスターの分割時の選択

マスタコンテナの脱退、障害、またはコンテナクラスタの分割時に、マスタコンテナロールの選択プロセスが次のように開始されます。

1) 現在のマスタコンテナには優先順位が付けられます。つまり、優先順位の高い新しいメンバコンテナが参加しても、コンテナクラスタは新しいマスタコンテナを選択しません。このルールは、コンテナクラスタが形成されるときには適用されません。これは、参加しているすべてのデバイスが自分自身をマスタデバイスと見なすためです。
2) ヘルス値が高いコンテナは、マスタコンテナとして優先的に選択されます。
3) 実行時間が長いコンテナが優先されます。コンテナクラスタでは、実行時間の測定精度は 10 秒です。デバイスの起動時間間隔が 10 秒以下の場合、デバイスの実行時間は等しいと見なされます。
4) CPU MAC アドレスが小さいコンテナが優先されます。

上記のルールに基づいて選択された最適なメンバコンテナがマスタコンテナになります。マスタコンテナが決定されると、すぐに Hello メッセージがブロードキャストされ、マスタコンテナの ID と正常性情報がアナウンスされます。このメッセージを受信すると、他のコンテナは役割選択プロセスを停止し、スタンバイコンテナとして機能します。スタン

バイコンテナは、Hello メッセージをマスタコンテナにユニキャストし、独自のロールと正常性情報を伝送します。マスタコンテナは、Hello メッセージを通じてすべてのスタンバイコンテナの情報とトポロジを収集し、この情報を Leader に報告します。コンテナクラスタ情報が更新されると、コンテナクラスタの関係を維持するために、マスタコンテナとスタンバイコンテナの間で Hello メッセージが定期的に送信されます。

クラウドクラスタでは、マスタコンテナの 2 層選択メカニズムがサポートされており、コンテナクラスタの信頼性と堅牢性が向上します。

1) 物理クラスタが正常に実行されている場合、物理クラスタの Leader は、マスタコンテナロールの選択ルールに基づいてマスタコンテナを選択します。
2) 物理クラスタが正常に実行できない (Leader がない) 場合、コンテナクラスタ自体が、マスタコンテナロールの選択ルールに基づいてマスタコンテナを選択します。

III. コンテナクラスタのマージ時の選択

本章の“*コンテナクラスタの結合*”を参照してください。

3.5.6 コンテナクラスタの分割と MAD

I. MAD について

コンテナクラスタでリンク障害が発生すると、複数の新しいコンテナクラスタに分割される可能性があります。これらのコンテナクラスタは同じ IP アドレスと他のレイヤ 3 設定を持つため、アドレスの競合が発生し、ネットワーク障害が拡大します。システムの可用性を向上させるためには、ネットワーク内の複数のコンテナクラスタの存在を検出し、それらを適切に処理し、コンテナクラスタの分割が業務に与える影響を最小限に抑えるメカニズムが必要です。マルチアクティブ検出 (MAD) は、分割検出、競合解決、および障害復旧機能を提供するメカニズムです。

クラウドクラスタは、次の種類の MAD をサポートします。クラウドプラットフォーム MAD とコンテナ内の LACP MAD。クラウドクラスタはクラウドプラットフォーム MAD の使用が優先され、クラウドプラットフォーム MAD が使用できない場合は LACP MAD が使用されます。

タイプ	メリット	制限事項	シナリオ
クラウドプラットフォーム MAD	・物理クラスタの付属機能 ・追加設定が不要	共有コンテナクラスタと物理クラスタリンク、および専用の物理クラスタリンクをサポートする製品の場合、クラウドプラットフォームの MADは、物理クラスタリンクがアップしている限り有効になります (物理クラスタは分割されません) 。	すべてのクラウドクラスタネットワーク
LACP MAD	・高速検出 ・クラウドプラットフォームMADの補助機能	LACP MAD検出メッセージを送信するには、QX シリーズ(拡張LACPプロトコルパケットをサポート) をLACPの対向装置として使用し、各メンバコンテナを接続する必要があります。	LACPリンクを使用してアップストリームまたはダウンストリームデバイスと接続するコンテナクラスタ

II. 分割検出

コンテナクラスタの動作中、マスタコンテナとスタンバイコンテナは、クラスタ関係を維持するために定期的に Hello メッセージを相互に送信します。指定されたタイムアウト期間内にスタンバイコンテナがマスタコンテナから Hello メッセージを受信しない場合、マスタコンテナが失敗したと見なされます。

コンテナは Hello メッセージを送信し、コンテナクラスタメンバ情報とトポロジのローカルレコードに基づいて、接続されているメンバコンテナの数を検出します。この検出された情報は、Leader に報告されます。

- 現在の物理クラスタに Leader が存在する場合、クラウドプラットフォーム MAD が開始されます。クラウドプラットフォーム MAD は、コンテナクラスタが分割されたと判断した場合、既存の競合を解決します。
  図 3-18 に示すように、物理デバイスのデバイス A とデバイス B は物理クラスタを形成し、各デバイスで Comware コンテナが実行されてコンテナクラスタを形成します。リンク障害が発生し、スタンバイコンテナでマスタコンテナから Hello メッセージを受信する障害が発生すると、コンテナクラスタはコンテナクラスタ 1 とコンテナクラスタ 2 に分割されます。ただし、物理クラスタリンクは通常そのままであるため、物理クラスタは引き続き正常に機能します。この時点では、クラウドプラットフォーム MAD を使用してコンテナクラスタの分割を処理します。

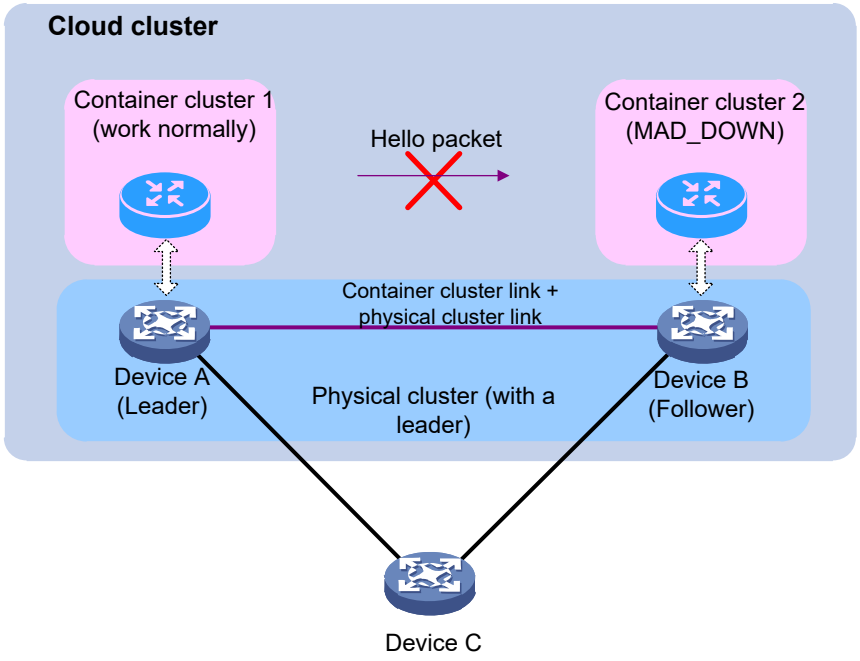


図 3-18 クラウドプラットフォーム MAD

- 現在の物理クラスタに Leader が存在しない場合、マスタコンテナを含まないコンテナクラスタは、選択ルールに基づいて新しいマスタコンテナを選択します。
  LACP MAD は、LACP を介して同じコンテナクラスタドメインに 2 つのマスタコンテナが存在することを検出し、コンテナクラスタが分割されたと見なします。
  図 3-19 に示すように、物理デバイス A とデバイス B は物理クラスタを形成し、Comware コンテナは各デバイスで実行され、コンテナクラスタを形成します。コンテナクラスタ内でリンク障害が発生すると、コンテナクラスタはコンテナクラスタ 1 とコンテナクラスタ 2 に分割されます。物理クラスタリンクはコンテナクラスタリンクと共有されるため、物理クラスタも分割されます。MAD イベントを処理する

Leader が物理クラスタに存在しない場合、LACP MAD はコンテナクラスタの分割を処理します。

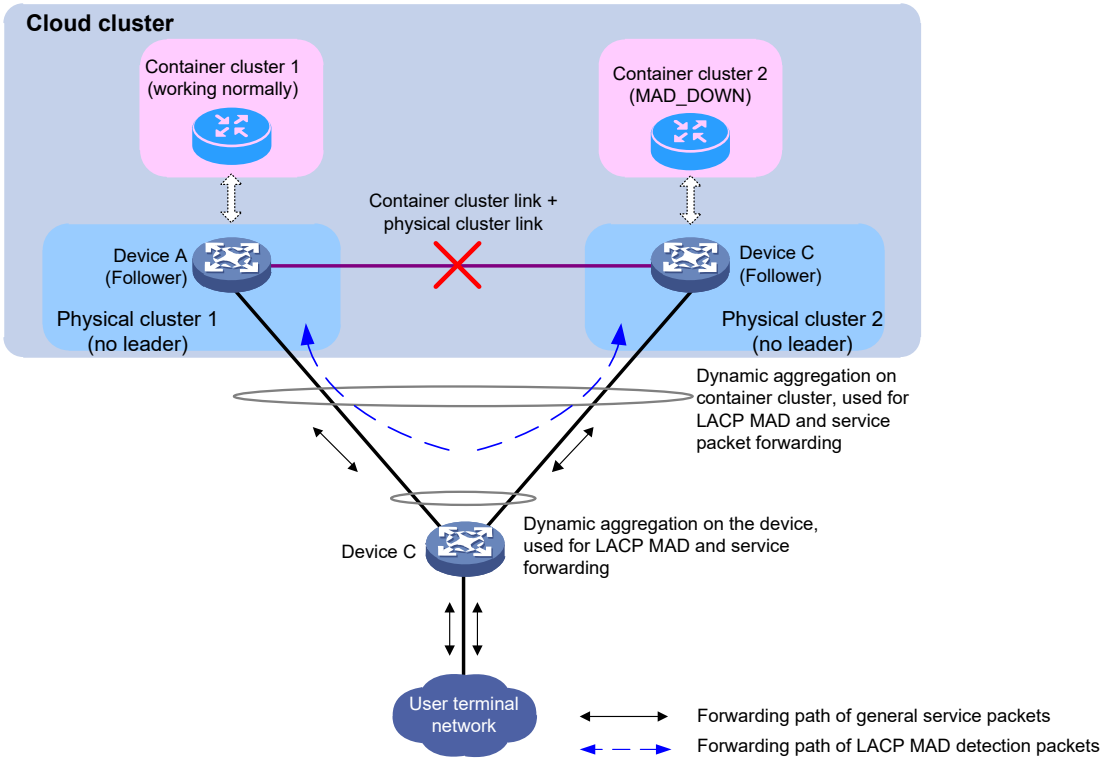


図 3-19 LACP MAD

III. 競合解決

クラウドプラットフォーム MAD と LACP MAD の競合処理メカニズムは若干異なります。

- クラウドプラットフォーム MAD の競合処理メカニズム:

クラウドプラットフォーム MAD は、コンテナクラスタの分割を検出すると、次の競合処理手順を実行します。

a) より多くのメンバを持つコンテナクラスタが優先されます。

b) より多くのメンバコンテナを持つコンテナクラスタは引き続き機能します。より少ないメンバコンテナを持つコンテナクラスタは、回復状態 (無効状態) に移行されます。

c) 一方、分割前のコンテナクラスタのマスタコンテナは引き続きマスタコンテナとして実行され、選択ルールに従って他のコンテナクラスタに対して新しいマスタコンテナが選択されます。このように、両方のコンテナクラスタにはそれぞれのマスタコンテナがあります。

d) ヘルスステータスが高いコンテナクラスタが優先されます。

e) 両方のコンテナクラスタのプライマリデバイスのヘルスステータスが比較されます。ヘルスステータスが高いコンテナクラスタは引き続き動作します。もう一方の

コンテナクラスタは回復状態 (無効状態) に移行されます。

f) マスタとしての実行時間が長いコンテナが優先されます。

g) マスタとしてのCPU MACアドレスが小さいコンテナが優先されます。

コンテナクラスタが回復状態に移行されると、そのクラスタ内のメンバコンテナ上のすべてのサービスポート (予約済みポートを除く) が閉じられ、クラスタがサービスパケットを転送できなくなります。mad exclude interface コマンドを使用して、予約済みポートを設定できます。

- LACP MAD の競合処理メカニズム:

LACP MAD は、コンテナクラスタ内の分割を検出すると、次の競合処理メカニズムを実行します。

a) 両方のクラスタ内のマスタコンテナのヘルスステータスが比較され、ヘルスステータスが高いコンテナクラスタが動作を続け、もう一方のコンテナクラスタが回復状態 (無効状態) に移行されます。

b) ヘルスステータスが等しい場合は、両方のコンテナクラスタ内のメンバコンテナの数が比較されます。他のコンテナクラスタが回復状態 (無効状態) に移行されている間、より多くのメンバコンテナを持つコンテナクラスタは引き続き動作します。

c) メンバコンテナの数も等しい場合、他のコンテナクラスタが回復状態に移行されている間、より小さいマスタメンバIDを持つコンテナクラスタは引き続き動作します。

コンテナクラスタが回復状態に移行されると、そのクラスタ内のコンテナ上のすべてのサービスポート (予約済みポートを除く) が閉じられ、クラスタがサービスパケットを転送できなくなります。mad exclude interface コマンドを使用して、予約済みポートを設定できます。

IV. MAD 障害復旧

MAD 障害復旧方法は、クラウドプラットフォーム MAD と LACP MAD で同じです。

1) 障害のあるリンクを修復して、分割されたコンテナクラスタを自動的に結合します。
2) リンクがまだ修復されていないが、稼働しているコンテナクラスタにも障害が発生している場合は、回復状態のコンテナクラスタを緊急バックアップとして有効にできます。

コンテナクラスタのリンクに障害が発生すると、コンテナクラスタが分割され、複数のアクティブな競合が発生します。そのため、障害のあるコンテナクラスタのリンクを修復し、競合するコンテナクラスタを 1 つに結合し直すと、コンテナクラスタの障害を復元できます。

コンテナクラスタリンクが修復されると、システムは自動的に回復状態のコンテナクラスタを再起動します。再起動後、回復状態だったコンテナクラスタ内のすべてのメンバコンテナが、通常の作業コンテナクラスタにコンテナメンバとして参加します。回復状態だったコンテナクラスタで強制的に閉じられたインタフェースは、実際の物理状態に自動的に回復します。図 3-20 に示すように、コンテナクラスタシステム全体が復元されます。

注意：

手順に従って、回復状態のコンテナクラスタを再起動します。通常の動作状態で誤ってコンテナクラスタを再起動した場合、結合されたコンテナクラスタは回復状態のままになり、すべてのメンバデバイスのインタフェースが閉じられます。このような場合は、**mad restore** コマンドを実行して、コンテナクラスタシステム全体を復元してください。

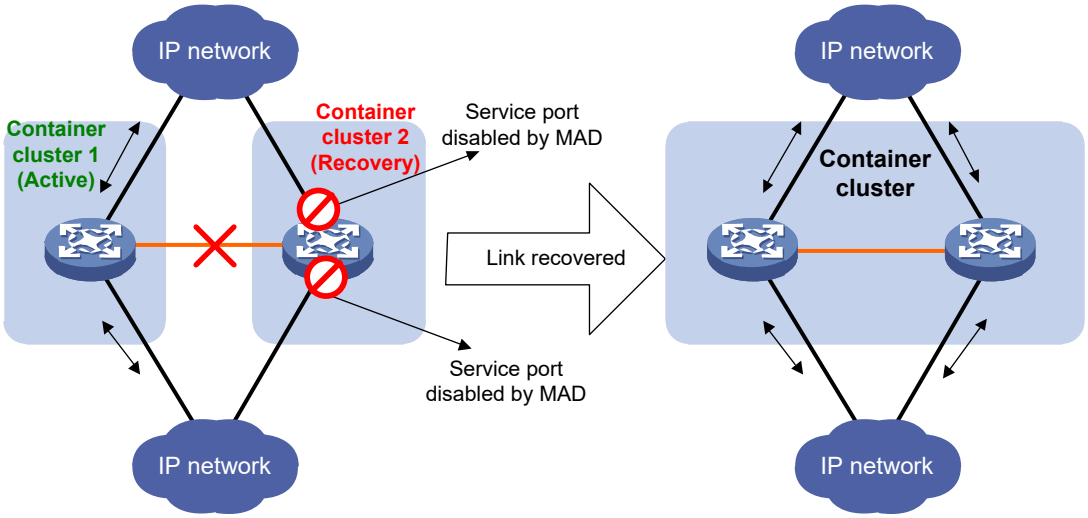


図 3-20 MAD 障害復旧 (コンテナクラスタのリンク障害)

稼働状態のコンテナクラスタがデバイス障害やアップリンク/ダウンリンク回線障害などの理由で障害が発生した場合、回復状態のクラスタに対して **mad restore** コマンドを実行できます。この操作によって回復状態のクラスタが正常な状態に復元され、障害が発生した稼働状態のコンテナクラスタが置き換えられます。次に、障害が発生したコンテナクラスタとリンクを修復します。

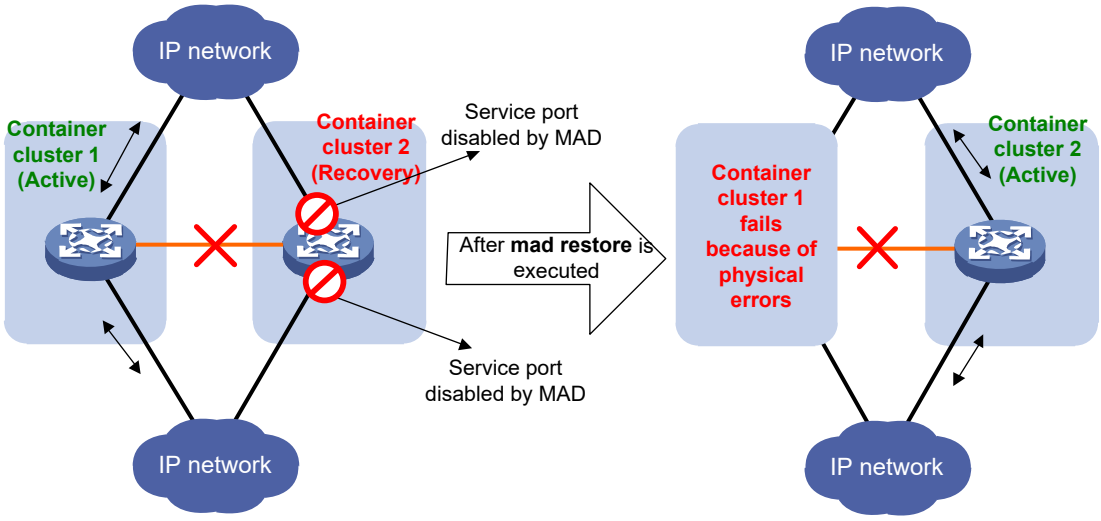


図 3-21 MAD 障害復旧 (障害復旧前に正常に動作するクラスタ障害)

3.5.7 コンテナクラスタの結合

コンテナクラスタの結合は、 MAD 機能が有効かどうかによって、次の 2 つの場合に分けられます。

- 物理クラスタが正常に動作するか、 LACP MAD が設定されている場合、コンテナクラスタのリンクに障害が発生してコンテナクラスタが分割されると、クラウドクラスタは 1 つのコンテナクラスタを正常に動作させます。もう 1 つのコンテナクラスタは無効になります (回復状態) 。2 つの分割コンテナクラスタ間の障害リンクが復元されると、2 つのコンテナクラスタは自動的に結合されます。回復状態のコンテナクラスタは自動的に再起動され、現在正常に実行されているコンテナクラスタにスタンバイコンテナとして参加します。
- 物理クラスタが正常に動作せず、LACP MAD が設定されていない場合、コンテナクラスタリンクが失敗してコンテナクラスタが分割されると、両方のコンテナクラスタが正常に動作します (デュアルマスター現象) 。この場合、2 つのコンテナクラスタ間の障害リンクが復元されると、2 つのコンテナクラスタは自動的にマージされ、マスタコンテナの選択が実行されます。選択ルールは次のとおりです。

a) より多くのメンバコンテナを持つマスタコンテナが優先されます。

b) ヘルス値が高いマスタコンテナが優先されます。

c) 実行時間が長いマスタコンテナが優先されます。

d) CPU MACアドレスが小さいマスタコンテナが優先されます。

マスタコンテナとして選出されたコンテナクラスタは引き続き動作しますが、選出されなかったクラスタは自動的に再起動し、動作中のコンテナクラスタにスタンバイコンテナとして参加します。

3.6 クラウドクラスタの設定手順

Comware コンテナは物理デバイス上で動作し、物理クラスタはコンテナクラスタの制御リンクを共有します。ネットワーク設計を行うときは、次の手順で行います。

1) クラウドクラスタ内のメンバデバイスの数を確認します。
2) デバイスのハードウェア互換性と制限事項を確認します。
3) メンバ ID（slot ID）、メンバ IP、メンバロール、クラスタ IP、クラスタインタフェースなど、クラウドクラスタの設定を実施します。
4) クラスタインタフェースに物理ケーブルを接続します。
5) デバイスのクラスタ設定をアクティブにして、クラスタを形成します。

3.7 クラウドクラスタの設定

以下に設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． cloud cluster member view に移行する	**cloud-cluster member** *member-id*	デフォルト：1
3． メンバ IP を設定する	**member-ip** *ipv4-addr mask-length*	デフォルト：設定なし

操作	コマンド	補足
4. Follower デバイスでクラスタ IP アドレスを指定する	**join-cluster ip** *ipv4-address*	デフォルト：設定なし 物理クラスタを設定するには、ManagerのFollowerデバイスでこのコマンドを設定する必要があります。このコマンドはLeaderデバイスでは必要ありません。 このコマンドが設定されていないManagerデバイスは、自動的に自己生成してLeaderデバイスとしてクラスタに参加します。
5. 物理インタフェースをクラスタリンクに割り当てる	**cluster-link [control | data] bind interface** *interface-type interface-number*	デフォルト：設定なし
6. system view に戻る	**quit**	―
7. (オプション)メンバ ID を変更する	**cloud-cluster member** *member-id* **renumber** *new-member-id*	デフォルト：1 クラウドクラスタ内の1つのデバイスのみがデフォルトのメンバIDを使用でき、他のデバイスはメンバIDを変更してクラウドクラスタに参加する必要があります。 メンバIDを変更する場合は、IDがクラスタ内で一意であることを確認してください。
8. 物理クラスタ設定を有効化する	**cloud-cluster configuration active**	コマンド実行後、対話モードによる設定にて、設定の保存とデバイスの再起動を選択する必要があります。 メンバIDを変更する場合は、このコマンドを実行するとデバイスが再起動されます。デバイスが再起動すると、新しいメンバIDが有効になります。

3.8 物理クラスタの移動

物理クラスタ A から物理クラスタ B にデバイスを移動する場合、最初に物理クラスタ A からデバイスを削除します。削除している間は、物理クラスタ A の設定、データ、およびトポロジはデバイスから削除され、コンテナ関連の設定は保持されます。

その後、デバイスはクラスタを構築する Leader として機能し、物理デバイス上のコンテナは Master として動作します。さらに設定を続けることで、デバイスを物理クラスタ B に追加できます。物理クラスタ A のデータがデバイスに残っている場合、デバイスを物理クラスタ B に追加することはできません。

3.8.1 物理クラスタ A からデバイスを削除

以下に設定を示します。

操作	コマンド	補足
1. クラスタリンクを切断し、物理クラスタ A からデバイスを削除する	―	―
2. デバイスにログインする	―	―
3. system view に移行する	**system-view**	―
4. cloud cluster member view に移行する	**cloud-cluster member** *member-id*	デフォルト：1
5. クラスタからデバイスを削除する	**undo join-cluster**	―
6. system view に戻る	**quit**	―
7. 物理クラスタ設定を有効化する	**cloud-cluster configuration active**	このコマンドの実行後にデバイスが自動的に再起動するかどうかは、デバイスのプロンプト情報を参照してください。

3.8.2 デバイスを物理クラスタ B に追加

以下に設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. cloud cluster member view に移行する	**cloud-cluster member** *member-id*	デフォルト：1
3. デバイスのメンバ IP アドレスを設定する	**member-ip** *ipv4-addr mask-length*	クラスタBの他のメンバIPアドレスが同じサブネット内にあることを確認してください。
4. クラスタ IP アドレスとして、クラスタ B の Leader デバイスの IP アドレスを指定する	**join-cluster ip** *ipv4-address*	―
5. system view に戻る	**quit**	―
6. (オプション)メンバ ID を変更する	**cloud-cluster member** *member-id* **renumber** *new-member-id*	デバイスの現在のメンバIDがクラスタBで使用されていない場合は、この手順を省略できます。
7. クラスタリンクを接続し、デバイスを物理クラスタ B に追加する	―	―
8. 物理クラスタ設定を有効化する	**cloud-cluster configuration active**	このコマンドの実行後にデバイスが自動的に再起動するかどうかは、デバイスのプロンプト情報を参照してください。

3.9 物理クラスタの表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
物理クラスタに関する情報を表示する	**display cloud-cluster [member** *member-id* **] [verbose]**
クラウドクラスタの設定情報を表示する	**display cloud-cluster configuration [member** *member-id* **]**

3.10 MADの設定

3.10.1 LACP MAD の設定

コンテナクラスタの MAD ドメイン ID は、MAD にのみ使用されます。コンテナは、MAD パケットを受信すると、パケット内の MAD ドメイン ID をローカルの MAD ドメイン ID と比較します。両者が同じ場合は、パケットを処理します。クラウドクラスタ内のすべてのコンテナに同じ MAD ドメイン ID を割り当てる必要があります。分割検出を正常に行うには、異なるクラウドクラスタ内のコンテナに異なる MAD ドメイン ID を割り当てます。

コンテナクラスタには、MAD ドメイン ID が 1 つだけあります。MAD ドメイン ID は、**cloud-cluster service-cluster mad domain** または **mad enable** のいずれかのコマンドを使用して変更できます。これらのコマンドを使用して設定された MAD ドメイン ID は、相互に上書きされます。ネットワーク計画に従ってコンテナクラスタの MAD ドメイン ID を変更し、無計画な変更を行わないようにします。

I. 制限とガイドライン

a)　コンテナクラスタへのMADドメインIDの割り当て

各コンテナクラスタには一意のコンテナクラスタドメイン ID を割り当てます。

b)　MAD shutdownされたインタフェースの操作

マルチアクティブコリジョンによってネットワークの問題が発生しないようにするには、回復状態コンテナクラスタで MAD メカニズムによってシャットダウンされたインタフェースを起動するために **undo shutdown** コマンドを使用しないでください。

🕮 **メモ：**

同一ネットワーク上に、クラウドクラスタ構成が複数存在する場合、クラウドクラスタ構成ごとに MAD ドメイン ID が重複しないように設定する必要があります。

II. 設定手順

以下に設定を示します。

操作	コマンド	補足
1.　system view に移行する	**system-view**	ー

操作	コマンド	補足
2. コンテナクラスタにドメイン ID を割り当てる	**cloud-cluster service-cluster domain** *domain-id*	デフォルト：0
3. リンクアグリゲーションインタフェースを作成し、view に移行する	**interface bridge-aggregation** *interface-number*	この手順は、中間デバイスでも実行する必要があります。
4. LACP モードで動作するようにリンクアグリゲーションインタフェースを設定する	**link-aggregation mode dynamic**	デフォルト：静的モード この手順は、中間デバイスでも実行する必要があります。
5. LACP MAD を有効にする	**mad enable**	デフォルト：無効
6. system view に戻る	**quit**	ー
7. Ethernet interface view に移行する	**interface** *interface-type interface-number*	ー
8. 指定したリンクアグリゲーションインタフェースにイーサネットインタフェースを割り当てる	**port link-aggregation group** *group-id*	この手順は、中間デバイスでも実行する必要があります。

3.10.2 MAD shutdown によるシャットダウンからの除外

コンテナクラスタが分離して Recovery 状態に移行すると、システムは自動的に次に示すネットワークインタフェースをシャットダウンから除外します。

- クラスタリンクの物理インタフェース
- リンクアグリゲーションインタフェースのメンバインタフェース (リンクアグリゲーションインタフェースがシャットダウンから除外されている場合)

管理またはその他の特別な目的のために、指定したインタフェースをシャットダウンアクションから除外できます。例えば、以下のような場合です。

- デバイスを管理するインタフェースに Telnet 接続できるように、シャットダウンアクションから除外します。
- VLAN インタフェースとその VLAN に属する物理インタフェースをシャットダウンアクションから除外し、VLAN インタフェースを介してログインできるようにします。

I. 制限とガイドライン

VLAN インタフェースの VLAN に属する物理インタフェースが物理クラスタの複数のメンバデバイスに分散されている場合、除外操作によって IP コリジョンが発生する可能性があります。アクティブなコンテナクラスタと非アクティブなコンテナクラスタの両方で、同一 IP アドレスを持つインタフェースがリンクアップしないよう除外設定をする場合は注意してください。

II. 設定手順

以下に設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． コンテナが Recovery 状態に移行したときにインタフェースをシャットダウンしないように設定する	**mad exclude interface** *interface-type interface-number*	システムによって自動的に除外されたネットワークインタフェースを除き、回復状態のコンテナ上のすべてのネットワークインタフェースがシャットダウンされます。

3.10.3 コンテナクラスタの回復

クラスタリンクが回復する前にアクティブなコンテナクラスタで障害が発生した場合は、非アクティブなコンテナクラスタで **mad restore** コマンドを実行して、トラフィック転送用に非アクティブなコンテナクラスタを回復します。本コマンドを使用すると、非アクティブなコンテナクラスタで MAD によってシャットダウンされたすべてのインタフェースがリンクアップします。

クラスタリンクが分離したまま本コマンドによりマルチアクティブ状態に戻すと、ネットワーク障害が発生する可能性があるため、使用する際は注意してください。

I. 設定手順

以下に設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． 非アクティブなコンテナクラスタを回復する	**mad restore**	―

3.11 コンテナクラスタ設定の最適化

3.11.1 ソフトウェアイメージ同期のためのソフトウェア自動更新の有効化

ソフトウェア自動更新機能は、クラウドクラスタに参加しようとしているデバイスに Master の現在のソフトウェアイメージを自動的に同期します。

ソフトウェア自動更新が無効になっていて、クラスタに参加しようとしている新しいデバイスのソフトウェアイメージが Master と異なる場合は、ソフトウェアの不整合によって新しいデバイスはクラスタに参加できません。ベストプラクティスとして、ソフトウェアの自動更新を有効にします。

I. 前提条件

クラスタに追加するデバイスの Flash メモリに、新しいソフトウェアイメージのための空き容量があることを確認します。

十分な容量がない場合、デバイスは現在のソフトウェアイメージを自動的に削除します。削除しても領域が不足している場合には、デバイスは自動更新を完了できません。ファイルを削除するには、デバイスを再起動し、Boot メニューにアクセスする必要があります。

II. 設定手順

以下に設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． ソフトウェア自動更新を有効にする	**cloud-cluster auto-update enable**	デフォルト：有効

3.11.2 コンテナクラスタのブリッジ MAC アドレスの保持設定

システムのブリッジ MAC アドレスは、LAN 上で一意である必要があります。コンテナクラスタの MAC アドレスは、LAN 上のレイヤ 2 プロトコル(たとえば、LACP)によってコンテナクラスタを識別します。

コンテナクラスタは通常、プライマリコンテナのブリッジ MAC アドレスをブリッジ MAC アドレスとして使用します。この場合、プライマリコンテナはコンテナクラスタのブリッジ MAC アドレスのアドレス所有者と呼ばれます。プライマリコンテナが出た後、コンテナクラスタのブリッジ MAC アドレスは、コンテナクラスタのブリッジ MAC の保持設定に応じて、一定期間または永続的に保持されます。

コンテナクラスタが構築されると、ブリッジの MAC アドレスは次のように処理されます。

1) 2 つのメンバデバイスのブリッジ MAC アドレスが同じ場合、コンテナクラスタの構築は失敗します。コンテナクラスタのブリッジ MAC アドレスは、コンテナクラスタの構築には影響しません。
2) コンテナクラスタが構築された後、新しいコンテナクラスタは、プライマリコンテナのブリッジ MAC アドレスをコンテナクラスタのブリッジ MAC アドレスとして使用します。

II. 制限とガイドライン

⚠ **注意：**

ブリッジ MAC アドレスの競合やブリッジ MAC アドレスの変更により、通信障害や一時的なトラフィックの中断が発生する可能性があります。

コンテナクラスタの異なるメンバデバイスをメンバインタフェースとするリンクアグリゲーションインタフェースがある場合は、**undo cloud-cluster service-cluster mac-address persistent** コマンドを使用しないでください。このコマンドを使用すると、トラフィックが中断される可能性があります。

III. 設定手順

以下に設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． コンテナクラスタのブリッジ MAC の保持設定をする。次のいずれかのタスクを実行する。	アドレス所有者がコンテナクラスタを離れた場合でも、コンテナクラスタのブリッジMACアドレスを保持する **cloud-cluster service-cluster mac-address persistent always**	デフォルト：Timer(6分)
	アドレス所有者がコンテナクラスタを離れた後、6分間コンテナクラスタのブリッジMACアドレスを保持する **cloud-cluster service-cluster mac-address persistent timer**	

3.11.3 コンテナクラスタのリンクダウンイベントの通知遅延

I. アプリケーションのシナリオ

リンクフラッピングによる頻繁なコンテナクラスタの分離と構築を防ぐには、リンクダウンイベントのシステムへの通知を遅延するように設定します。

II. 動作メカニズム

コンテナクラスタリンクには、アップとダウンの 2 つのリンク状態があります。コンテナクラスタの物理インタフェースは、リンクアップイベントを遅延しません。コンテナクラスタリンクがアップした直後にリンクアップイベントを通知します。

コンテナクラスタリンクダウンレポートの遅延時間を設定すると、コンテナクラスタの物理インタフェースは、リンクがダウンした直後にリンクダウンイベントをコンテナクラスタに通知しません。遅延時間に達してもコンテナクラスタリンクがダウンしている場合、インタフェースはリンクダウンイベントをコンテナクラスタに通知します。

III. 制限とガイドライン

コンテナクラスタで一部の機能が使用されている場合は、不要な状態変更を避けるために、遅延時間をそれらの機能のタイムアウトタイマよりも短く設定します。

ベストプラクティスとして、次の条件では遅延時間を 0 に設定します。

- プライマリ/セカンダリデバイスの高速経路切り替えのため、コンテナクラスタリンクの切り替えを必要としている。
- コンテナクラスタで RRPP を使用している。
- コンテナクラスタリンクの物理インタフェースをシャットダウンするか、メンバコンテナを再起動する前に、遅延時間を 0 に設定します。操作が完了したら、遅延時間を変更前の値に戻します。

IV. 設定手順

以下に設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． リンクダウンイベントを通知するコンテナクラスタインタフェースの遅延時間を設定する	**cloud-cluster link-delay** *interval*	デフォルト：遅延なし

3.11.4 クラウドクラスタの自動結合の有効化

I. アプリケーションのシナリオ

クラウドクラスタの自動結合は、次のイベントによって発生する結合に対して有効になります。

- クラウドクラスタリンクは、リンク障害から回復します。
- 結合するクラウドクラスタに既にクラウドクラスタポートの割り当てがあり、クラウドクラスタポートに割り当てられたインタフェースが既に接続されている場合は、クラウドクラスタポート割り当てをアクティブにします。

II. 動作メカニズム

クラウドクラスタの自動結合機能が無効になっている場合は、システムの指示に従って、Master の選択に失敗したクラウドクラスタ内のメンバデバイスを手動で再起動する必要があります。

クラウドクラスタの自動結合機能が有効になっている場合は、Master の選択に失敗したクラウドクラスタ内のメンバデバイスが自動的に再起動して、クラウドクラスタの結合が完了します。

結合を成功させるには、結合するクラウドクラスタでクラウドクラスタの自動結合が有効になっていることを確認します。

III. 設定手順

以下に設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． クラウドクラスタの自動結合を有効にする	**cloud-cluster auto-merge enable**	デフォルト：有効

3.12 WLANアクセスのためのクラウドクラスタの最適化

3.12.1 WLAN アクセスのためのクラウドクラスタの最適化の設定

🕮 **メモ：**

WLAN アクセスのためのクラウドクラスタの最適化の設定はソフトウェアバージョン 9.4.09 を含む以降のソフトウェアからサポートしています。

この機能により、信頼性の高い AP およびクライアントアクセスを保証します。この機能は、クラウドクラスタマスタの選択、新しいメンバの参加、クラウドクラスタメンバロールの変更を加速し、クラウドクラスタイベントによって AP およびクライアントのアクセスが不安定になることを防ぎます。

以下に設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. WLAN アクセスのクラウドクラスタ最適化を有効にする	**cloudcluster-optimize wlan reliable-access**	デフォルト：有効

3.13 コンテナクラスタの表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
コンテナクラスタのコンテナ情報を表示する	**display cloud-cluster service-cluster container [** *container-id* **] [verbose]**

3.14 コンテナクラスタへのアクセス

Comware 9 ベースのコンテナは、コマンドライン、SNMP、NETCONF、Web コンソールなど、ログインのためのユーザインタフェースを提供します。Comware 9 ベースのコンテナクラスタにログインすると、次のタスクを実行できます。

- コンテナクラスタと物理クラスタにアクセスします。
- クラウドクラスタのすべての設定とクラウドクラスタに関する情報 (コンテナクラスタと物理クラスタを含む) を表示します。

次のいずれかの方法を使用して、コンテナクラスタのコマンドラインインタフェース (CLI) にログインします。

- ローカルログイン: 任意のメンバコンテナのコンソールインタフェースからログインします。
- リモートログイン: 任意のメンバコンテナのレイヤ 3 インタフェースで、Telnet、Web コンソール、および SNMP などの方法を使用してログインします。

コンテナクラスタにログインすると、プライマリコンテナの CLI に接続されます。プライマリコンテナは、すべてのユーザ設定をセカンダリコンテナに同期します。

プライマリコンテナは、クラウドプラットフォームの Agent 構成要素を介して、ネットワーク管理者が Leader に対して行った物理クラスタ設定を同期します。その後、Leader はすべての Manager と Worker に対して設定を同期します。これにより、クラウドクラスタ全体の管理を実現できます。

3.15 クラウドクラスタの設定例

3.15.1 クラウドクラスタの設定

I. ネットワーク要件

図 3-22 に示すように設定します。

- AC 1 と AC 2 を含むクラウドクラスタを設定します。
- LACP マルチアクティブ検出 (MAD) とサービスパケット転送に使用される、クラウドクラスタとスイッチ Core 1 および Core 2 間の LACP を設定します。

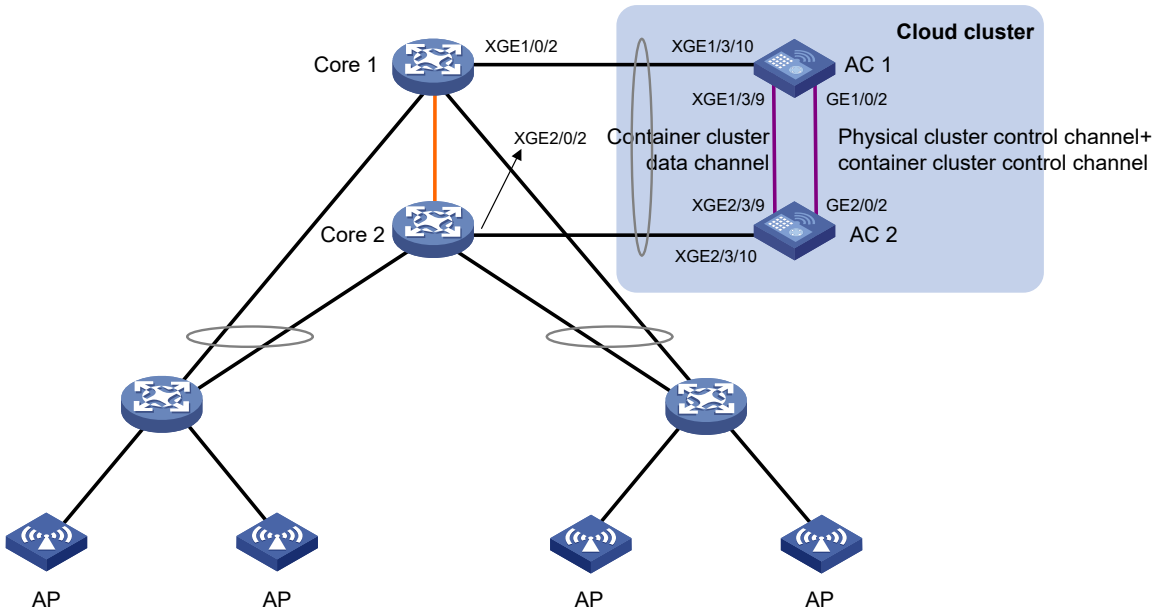


図 3-22 ネットワーク図

II. 設定手順

1)　Core1 と Core2 の設定

スイッチをクラウドクラスタ構成にして AC と接続するインタフェースに LACP を設定します。

設定内容は省略します。

2)　AC1 の設定

#クラウドクラスタ内の AC 1 は、デフォルトのメンバ ID (1) を使用します。編集する必要はありません。

#AC 1 のメンバ IP アドレスを指定します。

クラウドクラスタ内のメンバデバイスのメンバ IP アドレスが同じネットワークセグメントに存在することを確認します。事前にネットワークセグメントを計画します。

このドキュメントでは、例として 192.168.10.0/24 を使用します。

```
<AC1> system-view
[AC1] cloud-cluster member 1
[AC1-ccluster-member-1] member-ip 192.168.10.10 24
```

#クラスタ IP を 192.168.10.10 に指定します。(デバイスが Leader の場合は、この手順を省略できます。)

```
[AC1-ccluster-member-1] join-cluster ip 192.168.10.10
```

#GigabitEthernet 1/0/2 を制御リンクに、Ten-GigabitEthernet 1/3/9 をデータリンクに割り当てます。

```
[AC1-ccluster-member-1] cluster-link control bind interface gigabitethernet 1/0/2
The system will shut down and then bring up the interface after activation
the cloud cluster configuration. Continue? [Y/N]： y
[AC1-ccluster-member-1] cluster-link data bind interface ten-gigabitethernet 1/3/9
The system will shut down and then bring up the interface after activation
the cloud cluster configuration. Continue? [Y/N]： y
[AC1-ccluster-member-1] quit
```

#クラウドクラスタ設定を有効にします。

```
[AC1] cloud-cluster configuration active
New cluster configuration：
  cloud-cluster service-cluster domain 0
  cloud-cluster hello cloud-timeout 7 service-timeout 10
  cloud-cluster member 1
    member-ip 192.168.10.10/24
    join-cluster ip 192.168.10.10
    role manager-worker
    cluster-link control bind interface GigabitEthernet 1/0/2
    cluster-link data bind interface Ten-GigabitEthernet 1/3/9
The system will activate and save the configuration, and it might do a
restart. Continue? [Y/N]：y
```

```
The current configuration will be written to the device. Are you sure? [Y/N]:
y
Please input the file name(*.cfg)[flash:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):test.cfg
Validating file. Please wait...
Saved the current configuration to mainboard device successfully
```

クラウドクラスタの設定は再起動後に有効になります。

3)　AC2 の設定

#AC 2 のメンバ IP アドレスとして 192.168.10.11/24 を指定します。AC 1 と AC 2 のメンバ IP アドレスが同じネットワークセグメントに存在することを確認します。

```
<AC2> system-view
[AC2] cloud-cluster member 1
[AC2-ccluster-member-1] member-ip 192.168.10.11 24
```

#クラスタ IP を 192.168.10.10 に指定します。

```
[AC2-ccluster-member-1] join-cluster ip 192.168.10.10
```

#GigabitEthernet 1/0/2 を制御リンクに、Ten-GigabitEthernet 1/3/9 をデータリンクに割り当てます。

```
[AC2-ccluster-member-1] cluster-link control bind interface GigabitEthernet 1/0/2
The system will shut down and then bring up the interface after activation
the cloud cluster configuration. Continue? [Y/N]: y
[AC2-ccluster-member-1] cluster-link data bind interface Ten-GigabitEthernet 1/3/9
The system will shut down and then bring up the interface after activation
the cloud cluster configuration. Continue? [Y/N]: y
[AC2-ccluster-member-1] quit
```

#AC2 のメンバ ID を 2 に変更します。(クラウドクラスタ内の各メンバデバイスのメンバ ID は一意である必要があります。)

```
[AC2] cloud-cluster member 1 renumber 2
This command will take effect after the cloud cluster configuration is
activated. The command might result in configuration change or loss when it
takes effect. Continue? [Y/N]: y
```

#クラウドクラスタ設定を有効にします。

```
[AC2]cloud-cluster configuration active
New cluster configuration:
  cloud-cluster service-cluster domain 0
  cloud-cluster hello cloud-timeout 7 service-timeout 10
  cloud-cluster member 2
    member-ip 192.168.10.11/24
    join-cluster ip 192.168.10.10
    role manager-worker
    cluster-link control bind interface GigabitEthernet 2/0/2
    cluster-link data bind interface Ten-GigabitEthernet 2/3/9
```

```
The system will activate and save the configuration, and it might do a
restart. Continue? [Y/N]：y
The current configuration will be written to the device. Are you sure? [Y/N]：
y
Please input the file name(*.cfg)[flash：/startup.cfg]
(To leave the existing filename unchanged, press the enter key)：test.cfg
Validating file. Please wait...
Saved the current configuration to mainboard device successfully
```

クラウドクラスタの設定は再起動後に有効になります。AC2 は、物理クラスタに Follower として追加されます。コンテナクラスタでは、AC1 のコンテナがプライマリで、AC2 のコンテナがセカンダリです。

4)　クラウドクラスタが正常にセットアップされたことを確認

#物理クラスタに関する情報を表示します。

```
<AC1> display cloud-cluster
Manager list：
Member ID    Role         Member IP           State       Heartbeat(ms)
1            Leader       192.168.10.10       online      100
2            Follower     192.168.10.11       online      0
Worker list：
Member ID    State        Heartbeat(ms)       Joined at
1            online       100                 2023-02-12 06：13：28
2            online       200                 2023-02-12 06：13：28
```

出力は、物理クラスタに 2 つのメンバデバイスがあることを示しています。AC1 は Leader、AC 2 は Follower です。

#コンテナクラスタに関する情報を表示します。

```
<AC1> display cloud-cluster service-cluster container
Container ID     Slot ID       Member ID      Role         Status
1                1             1              Master       Online
2                2             2              Standby      Online
```

出力は、AC1 のコンテナがプライマで、AC 2 のコンテナがセカンダリであることを示しています。**display cloud-cluster service-cluster container** コマンドでは、それぞれ Master、Standby と表示されます。

5)　LACP MAD の設定

#リンクアグリゲーションインタフェース Bridge-Aggregation 1 を作成し、リンクアグリゲーションモードを dynamic に設定します（LACP に設定します）。

```
<AC1> system-view
[AC1] interface bridge-aggregation 1
[AC1-Bridge-Aggregation1] link-aggregation mode dynamic
```

#LACP MAD を有効にします。

```
[AC1-Bridge-Aggregation1] mad enable
You need to assign a domain ID (range： 0-4294967295)
[Current domain ID is： 0]： 1
The assigned domain ID is： 1
```

```
[AC1-Bridge-Aggregation1] quit
```

Bridge-Aggregation 1 に Ten-GigabitEthernet 1/3/10 を割り当てます。

```
[AC1] interface ten-gigabitethernet 1/3/10
[AC1-Ten-GigabitEthernet1/3/10] port link-aggregation group 1
[AC1-Ten-GigabitEthernet1/3/10] quit
```

Bridge-Aggregation 1 に Ten-GigabitEthernet 2/3/10 を割り当てます。

```
[AC1] interface ten-gigabitethernet 2/3/10
[AC1-Ten-GigabitEthernet2/3/10] port link-aggregation group 1
[AC1-Ten-GigabitEthernet2/3/10] quit
```

3.15.2 障害のある物理デバイスの交換

I. ネットワーク要件

図 3-23 に示すように、クラウドクラスタの AC1(セカンダリ装置)に障害が発生しました。同じモデルの新しいデバイスと交換します。

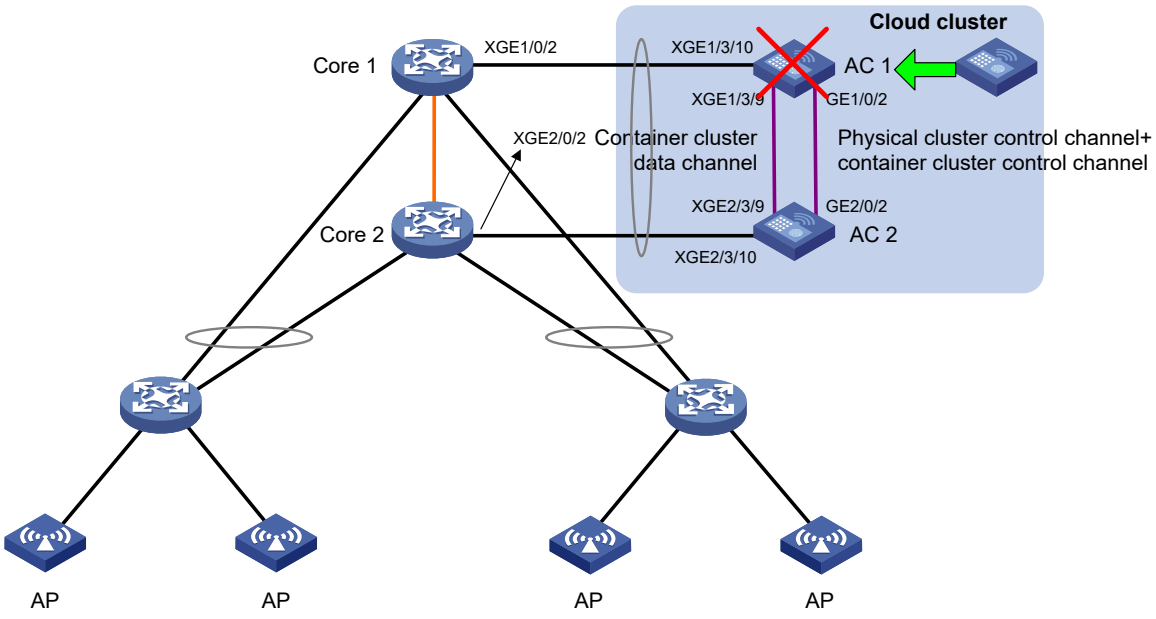


図 3-23 ネットワーク図

II. 解析

1)　AC2 をクラウドクラスタから分離して、AC2 の物理クラスタ設定を有効化します。

AC2 から障害が発生した AC1 に関する情報を削除するため、次の手順を実行します。この手順を実行しない場合、AC1 と同じメンバ ID を持つ新しいデバイスを追加したときに、物理クラスタはメンバ ID の競合が発生したと判断します。その結果、新しいデバイスの物理クラスタへの追加に失敗します。

2)　新しいデバイスにログインします。

AC2 のメンバ IP アドレスとしてクラスタ IP を設定します。

3)　ネットワークから AC1 を削除します。
4)　AC1 の設定を新しいデバイスにコピーするか、新しいデバイスで AC1 の設定を再度実行します。
5)　新しいデバイスをネットワークに接続します。

III. 設定手順

1)　AC2 の設定

#クラウドクラスタから AC2 を分離します。

```
<AC2> system-view
[AC2] cloud-cluster member 2
[AC2-ccluster-member-2] undo join-cluster
[AC2-ccluster-member-2] quit
[AC2] cloud-cluster configuration active
New cluster configuration:
  cloud-cluster service-cluster domain 0
  cloud-cluster hello cloud-timeout 7 service-timeout 10
  cloud-cluster member 2
    member-ip 192.168.10.11/16
    role manager-worker
    cluster-link bind interface GigabitEthernet 2/0/1
The system will activate and save the configuration, and it might do a
restart. Continue? [Y/N]:Y
The current configuration will be written to the device. Are you sure? [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...
```

#AC2 の物理クラスタに関する情報を表示します。

```
[AC2] display cloud-cluster
Manager list:
Member ID    Role         Member IP           State       Heartbeat(ms)
2            Leader       192.168.10.11       online      0
Worker list:
Member ID    State        Heartbeat(ms)       Joined at
2            online       0                   2023-02-25 22:49:52
```

出力は、AC1 に関する情報がクリアされたことを示しています。

2)　新しいデバイスを設定します。

#AC1 の設定ファイルを新しいデバイスにアップロードします。新しいデバイスで **cloud-cluster configuration active** コマンドを実行して、クラウドクラスタ設定を有効化します。新しいデバイスに設定ファイルをアップロードできない場合は、AC1 の設定に従って新しいデバイスを設定します。(AC 2 のメンバ IP アドレスをクラスタ IP として設定します。)

#新しいデバイスのメンバ IP アドレスを指定します。

クラウドクラスタ内のメンバデバイスのメンバ IP アドレスは、同じネットワークセグメントに存在する必要があります。ここでは、例として 192.168.10.10/24 を使用します。

```
<NewAC> system-view
[NewAC] cloud-cluster member 1
[NewAC-ccluster-member-1]
[NewAC-ccluster-member-1] member-ip 192.168.10.10 24
```

#クラスタ IP アドレスとして AC2 の IP アドレスを設定します。

```
[NewAC-ccluster-member-1] join-cluster ip 192.168.10.11
```

#Gigabitethernet 1/0/2 を制御リンクに、Ten-GigabitEthernet 1/3/9 をデータリンクに割り当てます。

```
[NewAC-ccluster-member-1] cluster-link control bind interface gigabitethernet 1/0/2
The system will shut down and then bring up the interface after activation
the cloud cluster configuration. Continue? [Y/N]： y
[NewAC-ccluster-member-1] cluster-link data bind interface ten-gigabitethernet 1/3/9
The system will shut down and then bring up the interface after activation
the cloud cluster configuration. Continue? [Y/N]： y
[NewAC-ccluster-member-1] quit
```

3)　障害が発生した AC1 の接続と同じように、新しいデバイスを接続してクラウドクラスタを有効にします。

#クラウドクラスタ設定を有効にすると、装置を再起動して AC2 が存在するクラウドクラスタに自動的に追加されます。

```
[NewAC] cloud-cluster configuration active
New cluster configuration：
  cloud-cluster service-cluster domain 0
  cloud-cluster hello cloud-timeout 3 service-timeout 5
  cloud-cluster member 1
    member-ip 192.168.10.10/24
    join-cluster ip 192.168.10.11
    role manager-worker
    cluster-link control bind interface GigabitEthernet 1/0/2
    cluster-link data bind interface Ten-GigabitEthernet 1/3/9
The system will activate and save the configuration, and it might do a
restart. Continue? [Y/N]：y
The current configuration will be written to the device. Are you sure? [Y/N]：
y
Please input the file name(*.cfg)[flash：/startup.cfg]
```

```
(To leave the existing filename unchanged, press the enter key)：test.cfg
Rebooting....
```

IV. 設定の確認

#物理クラスタに関する情報を表示します。

```
<AC2> display cloud-cluster
Manager list：
Member ID    Role        Member IP           State       Heartbeat(ms)
1            Follower    192.168.10.10       online      0
2            Leader      192.168.10.11       online      100
Worker list：
Member ID    State       Heartbeat(ms)       Joined at
1            online      100                 2023-02-12 06：13：28
2            online      200                 2023-02-12 06：13：28
```

出力は、物理クラスタに 2 つのメンバデバイスがあることを示しています。AC2 は Leader で、新しいデバイスは Follower です。

#コンテナクラスタに関する情報を表示します。

```
<AC2> display cloud-cluster service-cluster container
Container ID     Slot ID       Member ID      Role        Status
1                1             1              Standby     Online
2                2             2              Master      Online
```

出力は、AC2 のコンテナがプライマリで、新しいデバイスのコンテナがセカンダリであることを示しています。**display cloud-cluster service-cluster container** コマンドでは、それぞれ Master、Standby と表示されます。

🕮 メモ:

Standby 装置を有効にして再起動する場合、装置起動時にクラスタリンクで Master 装置と接続されていないと同期処理がタイムアウトするまでの時間がかかり、起動時間が長くなります。この時間を回避する場合は、クラスタリンクを接続してから設定を有効にしてください。この際、ネットワークループ等の障害を回避するため、クラスタリンク以外のケーブルは接続しないでください。

3.15.3 クラスタリンク障害時の割り当てインタフェースの変更

I. ネットワーク要件

図 3-24 に示すように、GigabitEthernet 1/0/1 と GigabitEthernet 2/0/1 が制御リンクとデータリンクに割り当てられています。GigabitEthernet 1/0/1 で障害が発生したため、クラスタリンクの設定を変更する必要があります。

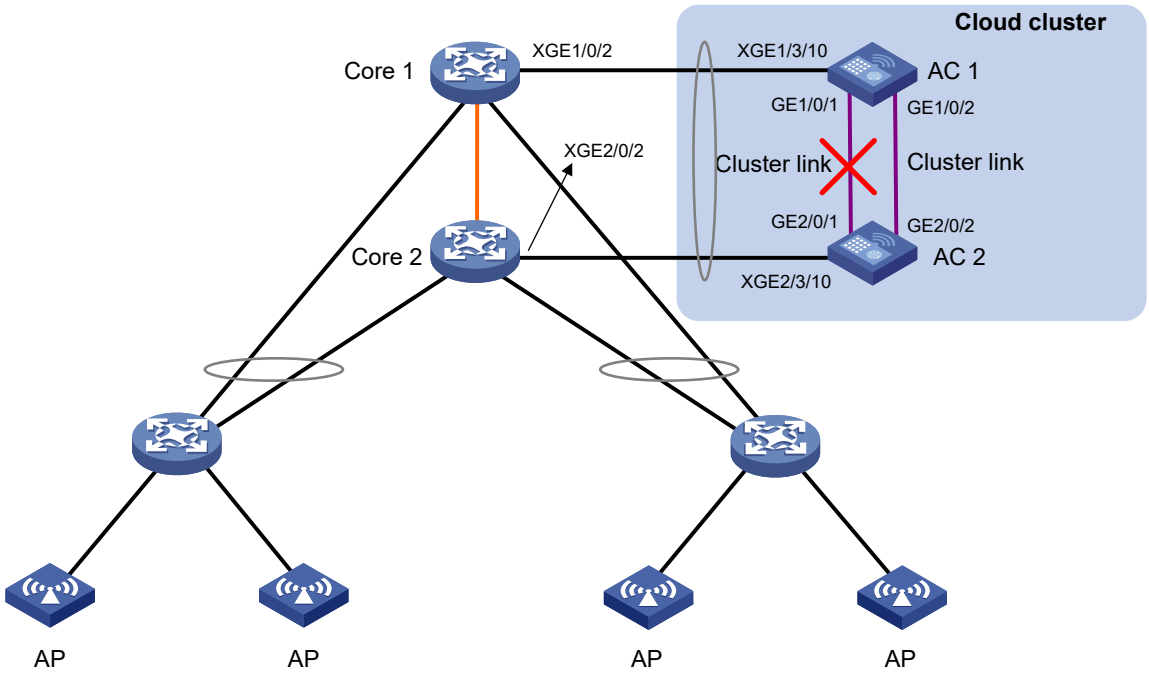


図 3-24 ネットワーク図

II. 設定手順

1)　AC1 の設定

#物理クラスタに関する情報を表示します。

```
<AC1> display cloud-cluster
Manager list:
Member ID    Role         Member IP           State       Heartbeat(ms)
1            Follower     1.1.2.11            offline     --
2            Follower     1.1.2.12            offline     --
Worker list:
Member ID    State        Heartbeat(ms)       Joined at
1            offline      --                  --
2            offline      --                  --
```

出力は、AC1 と AC2 の両方が Follower であることを示しています。

#コンテナクラスタ内のすべてのコンテナに関する詳細情報を表示します。

```
<Sysname> display cloud-cluster service-cluster container verbose
Service-cluster name: System
  Domain ID          : 1
  Cluster Bridge MAC: 00e0-fc00-1001
  Container ID    : 1
    Member ID     : 1
    Slot ID       : 1
    Health        : Healthy(0)
    Bridge MAC    : 00e0-fc00-1001
    CPU MAC       : 00f0-fc00-1001
    Control links: GigabitEthernet1/0/1(DOWN)
    Data links    : GigabitEthernet1/0/1(DOWN)
```

```
    Cluster connection  :  Unreachable
    Status        :  Offline
    Self hello timeout (ms)   :  4000
    Master hello timeout (ms) :  4000
  Container ID    :  2
    Member ID     :  2
    Slot ID       :  2
    Health        :  Normal(0)
    Bridge MAC    :  00e0-fc00-1002
    CPU MAC       :  00f0-fc00-1002
    Ctrl port     :  GigabitEthernet2/0/1(DOWN)
    Data port     :  GigabitEthernet2/0/1(DOWN)
    Cluster connection  :  Unreachable
    Status        :  Offline
    Self hello timeout (ms)   :  4000
    Master hello timeout (ms) :  4000
```

#制御リンクとデータリンクの両方に GigabitEthernet 1/0/2 を割り当てます。

```
<AC1> system-view
[AC1] cloud-cluster member 1
[AC1-ccluster-member-1] cluster-link bind interface gigabitethernet 1/0/2
The system will shut down and then bring up the interface after activation
the cloud cluster configuration. Continue? [Y/N]:  y
[AC1-ccluster-member-1] quit
```

#クラウドクラスタ設定を有効にします。

```
[AC1] cloud-cluster configuration active
New cluster configuration:
  cloud-cluster service-cluster domain 0
  cloud-cluster hello cloud-timeout 7 service-timeout 10
  cloud-cluster member 1
    member-ip 192.168.10.10/24
    join-cluster ip 192.168.10.10
    role manager-worker
    cluster-link bind interface GigabitEthernet 1/0/2
The system will activate and save the configuration, and it might do a
restart.Continue? [Y/N]:y
The current configuration will be written to the device. Are you sure? [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...
Saved the current configuration to mainboard device successfully.
```

2)　AC2 の設定

#AC1 の GigabitEthernet 1/0/2 を AC 2 の GigabitEthernet 2/0/2 に接続します。

#制御リンクとデータリンクの両方に GigabitEthernet 2/0/2 を割り当てます。

```
<AC2> system-view
[AC2] cloud-cluster member 2
```

```
[AC2-ccluster-member-2] cluster-link bind interface GigabitEthernet 2/0/2
The system will shut down and then bring up the interface after activation
the cloud cluster configuration. Continue? [Y/N]： y
[AC2-ccluster-member-1] quit
```

#クラウドクラスタ設定を有効にします。

```
[AC2] cloud-cluster configuration active
New cluster configuration：
  cloud-cluster service-cluster domain 0
  cloud-cluster hello cloud-timeout 7 service-timeout 10
  cloud-cluster member 2
    member-ip 192.168.10.11/24
    join-cluster ip 192.168.10.10
    role manager-worker
    cluster-link bind interface GigabitEthernet 2/0/2
The system will activate and save the configuration, and it might do a
restart. Continue? [Y/N]：y
The current configuration will be written to the device. Are you sure? [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...
Saved the current configuration to mainboard device successfully.
```

AC2 の再起動後にクラスタが回復します。

III. 設定の確認

#物理クラスタに関する情報を表示します。

```
<AC1> display cloud-cluster
Manager list：
Member ID    Role         Member IP           State       Heartbeat(ms)
1            Leader       192.168.10.10       online      100
2            Follower     192.168.10.11       online      0
Worker list：
Member ID    State        Heartbeat(ms)       Joined at
1            online       100                 2023-02-12 06：13：28
2            online       200                 2023-02-12 06：13：28
```

出力は、物理クラスタに 2 つのメンバデバイスがあることを示しています。AC1 は Leader、AC 2 は Follower です。

#コンテナクラスタに関する情報を表示します。

```
<AC1> display cloud-cluster service-cluster container
Container ID      Slot ID       Member ID      Role         Status
1                 1             1              Master       Online
2                 2             2              Standby      Online
```

出力は、AC1 のコンテナがプライマリで、AC2 のコンテナがセカンダリであることを示しています。**display cloud-cluster service-cluster container** コマンドでは、それぞれ Master、Standby と表示されます。

3.15.4 物理クラスタの別のクラウドクラスタへの移行

I. ネットワーク要件

図 3-25 に示すように、デバイス B をクラウドクラスタ A からクラウドクラスタ B に移行します。

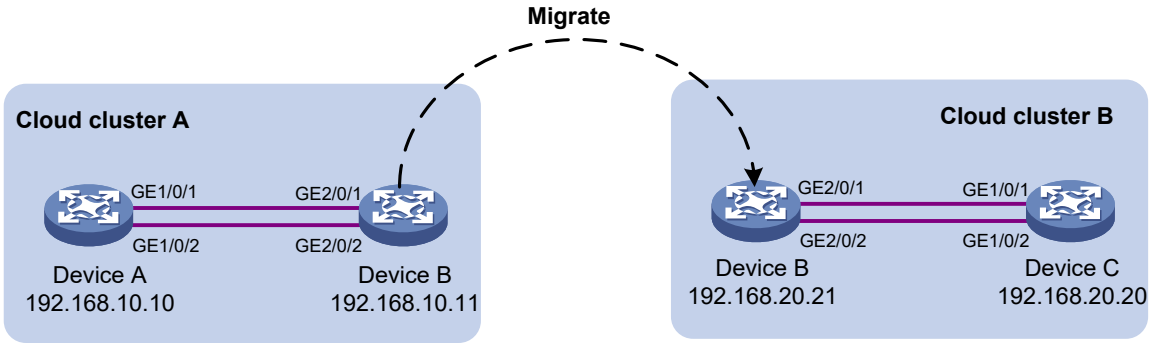


図 3-25 ネットワーク図

II. 設定手順

1)　デバイス B の設定

#クラウドクラスタ A にログインして、デバイス B をクラウドクラスタ A から分離します。

```
<Sysname> system-view
[Sysname] cloud-cluster member 2
[Sysname-ccluster-member-2] undo join-cluster
[Sysname-ccluster-member-2] quit
[Sysname] cloud-cluster configuration active
New cluster configuration:
  cloud-cluster service-cluster domain 0
  cloud-cluster hello cloud-timeout 7 service-timeout 10
  cloud-cluster member 2
    member-ip 192.168.10.11/24
    join-cluster ip 192.168.10.10
    role manager-worker
  cloud-cluster member 2
    role manager-worker
    cluster-link control bind interface GigabitEthernet 2/0/1
    cluster-link data bind interface Ten-GigabitEthernet 2/0/2
The system will activate and save the configuration, and it might do a
restart. Continue? [Y/N]:y
The current configuration will be written to the device. Are you sure? [Y/N]:
y
Please input the file name(*.cfg)[flash:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):test.cfg
Validating file. Please wait...
Saved the current configuration to mainboard device successfully.
```

再起動後、デバイス B はシングルデバイスとして動作します。

#デバイス B の Gigabitethernet 2/0/1 をデバイス C の Gigabitethernet 1/0/1 に接続し、デバイス B の Gigabitethernet 2/0/2 をデバイス C の Gigabitethernet 1/0/2 に接続して、デバイス B をクラウドクラスタ B に移行します。

#デバイス B にクラウドクラスタ B でのメンバ IP アドレスを指定します。デバイス B とデバイス C のメンバ IP アドレスが同じネットワークセグメントに存在することを確認します。

```
<Sysname> system-view
[Sysname] cloud-cluster member 2
[Sysname-ccluster-member-2] member-ip 192.168.20.21 24
```

#クラスタに追加するデバイス B にクラスタ IP アドレスとして、デバイス C のメンバ IP アドレスを設定します。

```
[Sysname-ccluster-member-1] join-cluster ip 192.168.20.20
```

#GigabitEthernet 2/0/1 を制御リンクに、Gigabitethernet 2/0/2 をデータリンクに割り当てます。

```
[Sysname-ccluster-member-1] cluster-link control bind interface gigabitethernet 2/0/1
The system will shut down and then bring up the interface after activation
the cloud cluster configuration. Continue? [Y/N]： y
[Sysname-ccluster-member-1] cluster-link data bind interface ten-gigabitethernet 2/0/2
The system will shut down and then bring up the interface after activation
the cloud cluster configuration. Continue? [Y/N]： y
[Sysname-ccluster-member-1] quit
```

#クラウドクラスタ設定を有効にします。

```
[Sysname] cloud-cluster configuration active
New cluster configuration：
  cloud-cluster service-cluster domain 0
  cloud-cluster hello cloud-timeout 7 service-timeout 10
  cloud-cluster member 2
    member-ip 192.168.20.21/24
    join-cluster ip 192.168.20.20
    role manager-worker
    cluster-link control bind interface GigabitEthernet 2/0/1
    cluster-link data bind interface GigabitEthernet 2/0/2
The system will activate and save the configuration, and it might do a
restart. Continue? [Y/N]：y
The current configuration will be written to the device. Are you sure? [Y/N]：
y
Please input the file name(*.cfg)[flash：/startup.cfg]
(To leave the existing filename unchanged, press the enter key)：test.cfg
Validating file. Please wait...
Saved the current configuration to mainboard device successfully.
```

クラウドクラスタ設定は再起動後に有効になります。デバイス B は自動的にクラウドクラスタ B に追加されます。

III. 設定の確認

#物理クラスタに関する情報を表示します。

```
<Sysname> display cloud-cluster
Manager list:
Member ID    Role        Member IP           State       Heartbeat(ms)
1            Leader      192.168.20.20       online      100
2            Follower    192.168.20.21       online      0
Worker list:
Member ID    State       Heartbeat(ms)       Joined at
1            online      100                 2023-02-12 06:13:28
2            online      200                 2023-02-12 06:13:28
```

出力は、物理クラスタに 2 つのメンバデバイスがあることを示しています。メンバ ID が 1 のデバイス C は Leader、メンバ ID が 2 のデバイス B は Follower です。

#コンテナクラスタに関する情報を表示します。

```
<Sysname> display cloud-cluster service-cluster container
Container ID     Slot ID       Member ID      Role        Status
1                1             1              Master      Online
2                2             2              Standby     Online
```

出力は、メンバ ID が 1 のデバイス C のコンテナがプライマリで、メンバ ID が 2 のデバイス B のコンテナがセカンダリであることを示しています。**display cloud-cluster service-cluster container** コマンドでは、それぞれ Master、Standby と表示されます。

QX-W2300AC シリーズ アクセスコントローラ

オペレーションマニュアル

15. 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-パスワード管理
04-公開鍵
05- SSH
06- SSL
07-接続制限
08-TCP フラグメントアタックプロテクション
09-IP ソースガード
10-ARP アタックプロテクション

目次

このセクションのページは **15-x-x** です。

1章 ACL 1-1
1.1 概要 1-1
1.1.1 ACLの番号づけと命名 1-1
1.1.2 ACLタイプ 1-1
1.1.3 走査順 1-2
1.1.4 ルールナンバリング 1-3
1.1.5 ACLでのフラグメントフィルタリング 1-4
1.2 設定の制限とガイドライン 1-4
1.3 設定作業リスト 1-5
1.4 標準ACLの設定 1-5
1.4.1 IPv4基本ACLの設定 1-5
1.5 拡張ACLの設定 1-6
1.5.1 IPv4拡張ACLの設定 1-6
1.6 L2 ACLの設定 1-7
1.7 ACLのコピー 1-7
1.8 ACLの表示と維持 1-8

1章 ACL

1.1 概要

ACL（Access Control List）は、送信元 IP アドレス、宛先 IP アドレス、ポート番号などにマッチするルールの設定です。

ACL は QoS、セキュリティ、ルーティング、その他の機能でトラフィックの設定に使用できモジュールにおけるパケットの廃棄、転送を決定します。

ACL は主にパケットフィルタリングに使用されます。また、QoS、セキュリティ、ルーティングなどのモジュールで ACL を使用してトラフィックを識別することもできます。パケットのドロップまたは転送の決定は、ACL を使用するモジュールによって異なります。

注意：

ACL の処理には、設定されている view について「interface > vlan > global」の優先順位があります。ACL は、高優先の処理を実行すると低優先の処理を実行しません。つまり、interface に設定された ACL の処理が実行された場合、vlan や global に設定された ACL の処理は実行されません。

1.1.1 ACL の番号づけと命名

各 ACL のタイプには、ACL 番号の固有な範囲があります。ACL を作成するとき、固有の ACL 番号あるいは名前を付ける必要があります。識別を簡略化するために ACL の名前を割り当てることができます。ACL を作成した後、設定した名前を変更、削除することもできません。

同じ番号の基本 ACL または高度な ACL の場合は、ipv 6 キーワードを使用して区別する必要があります。同じ名前の ACL の場合は、ipv 6 キーワードと mac キーワードを使用して区別する必要があります。

1.1.2 ACL タイプ

タイプ	ACL 番号	IP バージョン	マッチング基準
標準ACL	2000～2999	IPv4	送信元IPv4アドレス
		IPv6	送信元IPv6アドレス

タイプ	ACL 番号	IP バージョン	マッチング基準
拡張ACL	3000～3999	IPv4	送信元IPv4アドレス、宛先IPv4アドレス、パケットプライオリティ、プロトコル番号、その他のレイヤ3、またはレイヤ4のプロトコルヘッダ情報
		IPv6	送信元IPv6アドレス、宛先IPv6アドレス、パケットプライオリティ、プロトコル番号、その他のレイヤ3、またはレイヤ4のプロトコルヘッダ情報
L2 ACL	4000～4999	IPv4 IPv6	送信元MACアドレス、宛先MACアドレス、802.1pプライオリティ、リンクレイヤプロトコルタイプなどの、レイヤ2プロトコルヘッダフィールド

🕮 **メモ：**

- ハードウェアベースの ACL（Packet-filter など）は暗黙の permit となります。
- ソフトウェアベースの ACL（telnet, ssh, snmp など）は暗黙の deny になります。

1.1.3 走査順

ACL のルールは指定された順序で探索されます。パケットが、あるルールにマッチした時点で探索動作を終了します。ACL が重複や矛盾したルールを含んでいる場合、探索結果や動作は探索順序に依存します。

ACL の走査順には、以下の 2 つ方法があります。

- **config**：ルール ID を昇順で探索します。大きいルール ID よりも先に小さいルール ID にマッチします。この方法を使用する場合、ルールの内容と順序に注意してください。

🕮 **メモ：**

WLAN client ACL と WLAN AP ACL の走査順は config のみ設定可能です。

- **auto**：depth-first により ACL の探索を行います。depth-first ルールでの走査順は、ACL のタイプによって表 1-1の定義に従って決定されます。

表 1-1 ACL の depth-first 走査順

ACL 種別	走査順
標準IPv4 ACL	1. 送信元 IPv4 アドレスのワイルドカードの 0 が多い順（0 が多いと IPv4 アドレスのワイルドカードの範囲が狭いことを示します。） 2. ルールが作成された順
拡張IPv4 ACL	1. 特定のプロトコル番号 2. 送信元 IP アドレスのワイルドカードマスクの 0 が多い順 3. 宛先 IP アドレスのワイルドカードマスクの 0 が多い順 4. TCP/UDP のポート番号の範囲が小さい順

ACL 種別	走査順
	5. ルールが作成された順
標準IPv6 ACL	1. 送信元 IPv6 アドレスのプレフィックス長（長いプレフィックスは、より狭い IPv6 アドレス範囲を示します。） 2. ルールが作成された順
拡張IPv6 ACL	1. 特定のプロトコル番号 2. 送信元 IPv6 アドレスの長いプレフィックス 3. 宛先 IPv6 アドレスの長いプレフィックス 4. より狭い TCP/UDP サービスポート番号範囲。 5. ルールが作成された順
L2 ACL	1. 送信元 MAC アドレスのマスクの 1 が多い順（1 が多いと MAC アドレスが小さいことを示します。） 2. 宛先 MAC アドレスのマスクの 1 が多い順 3. ルールが作成された順

インバースマスク（inverse mask）と呼ばれるワイルドカードマスクは、10 進数表示のドット表示で表される 32 ビットバイナリです。ネットマスクの 0 は“一致する（do care）”ビットと表現され、1 は“無視する（don’t care）”ビットと表現されます。サブネットマスクの 0 と 1 を反転したものとは異なります。IP アドレスが“do care”ビットである場合、一致させ、“無視する（don’t care）”ビットである場合、無視されます。ワイルドマスクが 0.255.255.255、ネットマスクが 192.168.1.1 の場合、最初の 0 は”一致する（do care）"ビットで、２番目以降が“無視する（don’t care）”ビットであるため、192.0.0.0 のネットワークに一致する ACL となります。ワイルドカードマスクの 0 と 1 は非連続にすることができます。たとえば 0.255.0.255 は有効なワイルドマスクです。

1.1.4 ルールナンバリング

ACL ルールは手動ナンバリングあるいは自動ナンバリングを選択できます。本セクションでは自動ナンバリングの動作を説明します。

I. ルールナンバリングのステップ

作成したルールに ID を割り当てない場合、システムは ACL ルールにルール ID を自動的に割り当てます。ステップのナンバリングルールは、システムが自動的にルールの番号づけを行う増加分を設定します。たとえば、デフォルトの ACL ルールのナンバリングステップは 5 です。ルールに ID を割り当てない場合、ルールには 0、5、10、15･･･の順で自動的に番号が振られます。広いナンバリングのステップの場合、2 つのルールの間に、さらにルールを挿入することができます。

隣接したナンバリングルールより、ルールの間に隙間を導入することによって、新規にルールを挿入するように、ACL に柔軟性を持たせることができます。この機能は config-order ACL にとって重要です。config-order ACL の ACL ルールはルール ID の昇順でマッチされています。

II. 自動ルールナンバリングと再ナンバリング

システムは、現在の最大のステップ番号よりも大きなステップの最小倍数を新しく定義されたルールに割り当てます。これは 0 から始まります。

たとえば、ナンバリングのステップを 5 に設定し、ACL ルールに 0、5、9、10、12 を設定した場合、新しく定義されたルールには 15 が割り当てられます。ACL にルールが 1 つも定義されていない場合、最初に定義されるルールの番号は 0 です。

ルールのステップを変更したとき、ルールは再ナンバリングされ、0 から始まります。たとえば、ルールの番号 5、10、13、15 があるとします。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 となります。

1.1.5 ACL でのフラグメントフィルタリング

通常のパケットフィルタリングはパケットの最初のフラグメントのみマッチし、後続のフラグメントはパスします。攻撃者はネットワークを攻撃するため、最初でないフラグメントを偽造することができます。

このリスクを防ぐため、以下の ACL を使用します。

- デフォルトで、最初のフラグメント以外のパケットを含むすべてのフラグメントをフィルタします。
- マッチ条件の変更を行います。たとえば、最初のフラグメント以外のパケットのみをフィルタします。

1.2 設定の制限とガイドライン

ACL ルールに一致条件が含まれている場合、あるいは以下の一致条件と機能が有効である場合、パケットはソフトウェアベースで転送します。

- 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
- トランスポートレイヤプロトコル
- ICMP メッセージタイプ、メッセージコード、メッセージ名
- VPN インスタンス
- 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を行う場合、パケットはエントリの計算を行う際にコントロールプレーンに送信されます。装置の処理にかかる負荷が大きくなるとパケット転送に影響を与えます。

1.3 設定作業リスト

作業リスト
（必須設定項目） 少なくとも1つの作業を行ってください。 ● 標準ACLの設定 ● 拡張ACLの設定 ● L2 ACLの設定 ● WLAN client ACLの設定 ● WLAN AP ACLの設定
（オプション設定項目） ACLのコピー
（オプション設定項目） ACLへのパケットフィルタの設定

1.4 標準ACLの設定

1.4.1 IPv4 基本 ACL の設定

標準 IPv4 ACL は送信元 IPv4 アドレスにもとづいたパケットにのみマッチします。

以下に標準 IPv4 ACL の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． 標準 IP4 ACL を作成し、その view に移行する	**acl basic** { *acl-number* | **name** *acl-name* } [**match-order** { **auto** | **config** }]	デフォルト：設定なし 設定範囲は2000～2999です。 IPv4 ACLの番号を指定する場合、**acl basic** *acl-number*コマンドを使用した後でviewに移行することができます。 IPv4 ACLの名前を指定する場合、**acl basic name** *acl-name* コマンドを使用した後でviewに移行することができます。
3． （オプション設定項目）標準 IPv4 ACL の説明を設定する	**description** *text*	デフォルト：設定なし
4． （オプション設定項目）ルールの番号づけステップを設定する	**step** *step-value*	デフォルト：5
5． ルールを作成/修正する	**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 **logging**キーワードはモジュール（パケットフィルタリングなど）がサポートしている場合のみ機能します。
6． （オプション設定項目）ルールの説明を設定する	**rule** *rule-id* **comment** *text*	デフォルト：設定なし
7． （オプション設定項目）ルールの注釈を追加	**rule** [*rule-id*] **remark** *text*	デフォルト：設定なし

1.5 拡張ACLの設定

拡張 ACL では、以下の情報にもとづいてマッチングを行うことができます。

- 送信元 IP アドレス
- 送信先 IP アドレス
- パケットのプライオリティ
- プロトコル番号
- TCP/UDP の送信元/送信先ポート番号、TCP フラグ、ICMP メッセージタイプ、ICMP メッセージコードなどの他のプロトコルヘッダ情報

標準 ACL と比較すると、拡張 ACL では柔軟で正確なフィルタリングを行うことができます。

1.5.1 IPv4 拡張 ACL の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． 拡張 IPv4 ACL を作成し、その view に移行する	**acl advanced** { *acl-number* | **name** *acl-name* } [**match-order** { **auto** | **config** }]	デフォルト：設定なし 設定範囲は3000～3999です。 IPv4 ACLの番号を指定する場合、**acl advanced** *acl-number*コマンドを使用した後でviewに移行することができます。 IPv4 ACLの名前を指定する場合、**acl advanced name** *acl-name*コマンドを使用した後でviewに移行することができます。
3． （オプション設定項目）拡張 IPv4 ACL の説明を設定する	**description** *text*	デフォルト：設定なし
4． （オプション設定項目）ルールの番号付けステップを設定する	**step** *step-value*	デフォルト：5
5． ルールを作成/修正する	**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 **logging**キーワードはモジュール（たとえばパケットフィルタリング）がサポートしている場合のみ機能します。
6． （オプション設定項目）ルールの説明を設定する	**rule** *rule-id* **comment** *text*	デフォルト：設定なし
7． （オプション設定項目）ルールの注釈を追加	**rule** [*rule-id*] **remark** *text*	デフォルト：設定なし

1.6 L2 ACLの設定

イーサネットフレームのヘッダを使用した ACL は“L2 ACL”と呼ばれます。L2 ACL では以下のレイヤ 2 のプロトコルヘッダにもとづいてマッチングを行います。

- 送信元 MAC アドレス
- 送信先 MAC アドレス
- 802.1p 優先順位（VLAN プライオリティ）
- リンクレイヤのプロトコルタイプ

以下に L2 ACL の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. L2 ACL を作成し、その view に移行する	**acl mac** { *acl-number* | **name** *acl-name* } [**match-order** { **auto** | **config** }]	デフォルト：設定なし 設定範囲は4000～4999です。 L2 ACLの番号を指定する場合、**acl mac** *acl-number*コマンドを使用した後でviewに移行することができます。 L2 ACLの名前を指定する場合、**acl mac name** *acl-name* コマンドを使用した後でviewに移行することができます。
3. （オプション設定項目）L2 ACL の説明を設定する	**description** *text*	デフォルト：設定なし
4. （オプション設定項目）ルールの番号付けステップを設定する	**step** *step-value*	デフォルト：5
5. ルールを作成/修正する	**rule** [*rule-id*] { **deny** | **permit** } [**cos** *vlan-pri* | **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
6. （オプション設定項目）ルールの説明を設定する	**rule** *rule-id* **comment** *text*	デフォルト：設定なし
7. （オプション設定項目）ルールの注釈を追加	**rule** [*rule-id*] **remark** *text*	デフォルト：設定なし

1.7 ACLのコピー

既存の ACL（送信元 ACL）をコピーして、ACL（宛先 ACL）を新しく作成することができます。新しい ACL（宛先 ACL）は送信元 ACL と同じタイプ、内容を持ちます。ただし同じ ACL 番号、ACL 名ではありません。

ACL のコピーを行うため、以下のことを確認してください。

- 送信元の ACL と宛先 ACL は同じタイプである必要があります。
- コピーを実行する前に、送信元の ACL が存在し、宛先 ACL は存在しないことを確認してください。

以下に ACL のコピーの設定を示します。

操作	コマンド
1. system view に移行する	**system-view**
2. 既存の ACL をコピーし、新しく ACL を作成する	**acl** [**ipv6** | **mac**] **copy** { *source-acl-number* | **name** *source-acl-name* } **to** { *dest-acl-number* | **name** *dest-acl-name* }

1.8 ACLの表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
ACLの設定とマッチした統計情報を表示する	**display acl** [**ipv6** | **mac**] { *acl-number* | **all** | **name** *acl-name* }

user view でのみ **reset** コマンドを実行できます。

操作	コマンド
ACL統計情報をクリアする	**reset acl** [**ipv6** | **mac**] **counter** { *acl-number* | **all** | **name** *acl-name*

目次

このセクションのページは **15-x-x** です。

2章 タイムレンジ 2-1
2.1 設定手順 2-1
2.2 タイムレンジの表示と維持 2-1
2.3 タイムレンジの設定例 2-2
2.3.1 ネットワーク要件 2-2
2.3.2 設定手順 2-2
2.3.3 設定の確認 2-3

2章 タイムレンジ

タイムレンジを適用することで、日時をもとにしたサービスを提供することができます。このタイムレンジは指定した期間のみ適用されます。たとえばタイムレンジを設定し、日時を指定した ACL を設定することができます。もしタイムレンジが存在しない場合、サービスは適用されません。

タイムレンジは以下のタイプがあります。

- **周期的タイムレンジ** － 一週間のある曜日、または複数の曜日で周期的に繰り返します。
- **絶対的タイムレンジ** － 一定期間内のみ有効になり、繰り返しません。

タイムレンジはタイムレンジ名によって一意に決められます。最大 1024 のタイムレンジを設定することができますが、各タイムレンジは、32 の周期的な記述と 12 の絶対的な記述まで設定することができます。

1) すべての周期的タイムレンジを組み合わせます。
2) すべての絶対的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。

2.1 設定手順

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． タイムレンジを作成あるいは修正する	**time-range** *time-range-name* { *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

2.2 タイムレンジの表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
タイムレンジの設定と状態を表示する	**display time-range** { *time-range-name* | **all** }

2.3 タイムレンジの設定例

2.3.1 ネットワーク要件

図 2-1に示すように、Client が Server に 2015 年 6 月 1 日から 2015 年 12 月 31 日の、営業時間 8:00 から 18:00 のみアクセスできるように、AC に ACL を設定します。

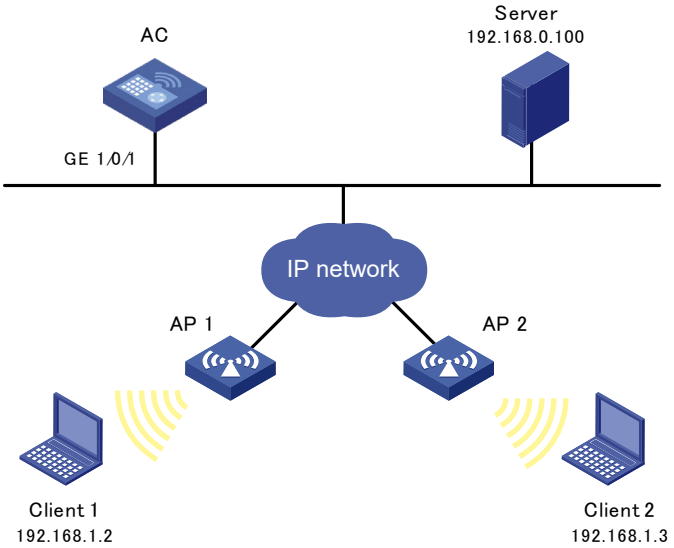


図 2-1 ネットワーク図

2.3.2 設定手順

2015 年 6 月 1 日から 2015 年 12 月 31 日の、営業時間 8:00 から 18:00 の周期的タイムレンジを作成します。

```
<AC> system-view
[AC] time-range work 8:0 to 18:0 working-day from 0:0 6/1/2015 to 24:0 12/31/2015
```

IPv4 標準 ACL 2001 を作成し、タイムレンジ **work** の間、192.168.1.2/32 からのパケットのみ許可するようにルールを設定します。

```
[AC] acl basic 2001
[AC-acl-ipv4-basic-2001] rule permit source 192.168.1.2 0 time-range work
[AC-acl-ipv4-basic-2001] rule deny source any time-range work
[AC-acl-ipv4-basic-2001] quit
```

GigabitEthernet 1/0/1 の出力パケットをフィルタするため、IPv4 標準 ACL 2001 を適用します。

```
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] packet-filter 2001 outbound
```

```
[AC-GigabitEthernet1/0/1] quit
```

2.3.3 設定の確認

#AC でタイムレンジの設定と状態を表示します。

```
[AC] display time-range all
Current time is 09:40:55 5/26/2015 Tuesday

Time-range : work ( Active )
 08:00 to 18:00 working-day
 from 00:00 6/1/2011 to 00:00 1/1/2012
```

出力は、タイムレンジの **work** がアクティブであることを示します。

目次

このセクションのページは **15-x-x** です。

3章 パスワード管理 3-1
3.1 概要 3-1
3.1.1 パスワードの設定 3-1
3.1.2 パスワードのアップデートと有効期限の終了 3-3
3.1.3 ユーザログイン管理 3-4
3.1.4 すべての形式でのパスワードの非表示 3-5
3.1.5 ロギング 3-6
3.2 制限とガイドライン 3-6
3.3 パスワード管理設定作業リスト 3-6
3.4 パスワード管理の有効化 3-7
3.5 グローバルパスワード管理パラメータの設定 3-7
3.6 ユーザグループパスワード管理パラメータの設定 3-9
3.7 ローカルユーザパスワード管理パラメータの設定 3-9
3.8 superパスワード管理パラメータの設定 3-10
3.9 パスワード管理の表示と維持 3-10
3.10 パスワード管理の設定例 3-11
3.10.1 パスワード管理の設定例 3-11

3章 パスワード管理

3.1 概要

パスワード管理は、以下の機能ができます。

- 装置管理ユーザのログインと super パスワードのセットアップ、終了、アップデートを管理します。
- あらかじめ定義されたポリシーにもとづいたユーザログインステータスを制御します。

装置管理ユーザは、ローカルユーザの一種です。ローカルユーザについての詳細は、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*13 ユーザアクセスと認証*“の”*3 章 AAA*“を参照してください。super パスワードについては、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*2 基本機能*”の”*2 章 RBAC*”を参照してください。

🕮 **メモ：**

パスワード管理機能はデフォルトで無効（**undo password-control enable**）に設定されていますが、以下に示すコマンドはパスワード管理機能が無効の場合でも動作します（以下はデフォルトの設定状態を示します）。以下に示すコマンド以外は、パスワード管理機能を有効にすると動作します。

- password-control length enable：文字列の最小値制限有効
- password-control length 10：10 文字以上の文字列（ローカルユーザ）
- password-control composition enable：文字タイプ数の最小値制限有効
- password-control composition type-number 2：最低 2 種類の文字タイプ数（ローカルユーザ）
- password-control complexity user-name check：パスワードにユーザ名と同じ文字列使用不可
- password-control super length 10：10 文字以上の文字列（super ユーザ）
- password-control super composition type-number 2：最低 2 種類の文字タイプ数（super ユーザ）

3.1.1 パスワードの設定

I. 最小パスワード長

ユーザパスワードの最小の長さを設定することができます。ユーザが最小パスワード長よりも短いパスワードを入力した場合、システムはパスワードを拒否します。

II. パスワード設定のポリシー

パスワードは以下のタイプの組み合わせで設定されます。

- A～Z の大文字の英字
- a～z の小文字の英字
- 0～9 の数字
- 特殊文字

表 3-1 特殊文字

文字名	記号	文字名	記号
アンパサンド	&	アポストロフィー	'
アスタリスク	*	アットマーク	@
逆クォート	`	バックスラッシュ	\
半角スペース	ー	キャロット	^
コロン	:	コンマ	,
ダラーマーク	$	ドット	.
イコール	=	感嘆符	!
左アングルブラケット	<	左波括弧	{
左角括弧	[	左丸括弧	(
ハイフン	-	パーセント	%
プラス	+	シャープ	#
ダブルクォーテーション	"	右アングルブラケット	>
右波括弧	}	右角括弧	]
右丸括弧	)	セミコロン	;
スラッシュ	/	チルダ	~
アンダーライン	_	垂直バー	|

システムのセキュリティ要件に応じて、パスワードに含めなくてはいけない文字タイプの最小数と、各種類の文字の最小数を設定することができます。表 3-2にパスワード設定のポリシーを示します。

表 3-2 パスワード設定のポリシー

パスワード組み合わせレベル	文字タイプの最小数	各タイプの最小文字数
Level 1	1	1
Level 2	2	1
Level 3	3	1
Level 4	4	1

すべての組み合わせレベルをパスワードとして使用できます。

ユーザがパスワードを設定あるいは変更するとき、システムはパスワードが要件の組み合わせを満たしているか確認します。満たしていない場合、パスワードの設定あるいは変更操作は失敗します。

III. パスワードの複雑性のポリシー

ユーザ名や連続した文字などのような文字が含まれる複雑でないパスワードは、不正に解読されやすくなります。より高いセキュリティを持たせるため、すべてのユーザのパスワードが相対的に複雑となっているかを確認するようにポリシーを設定することができます。ポリシーが設定され、ユーザがパスワードを設定したとき、パスワードの複雑性を確認します。パスワードがポリシーに適合しない場合、ユーザのパスワード設定は失敗します。

パスワードの複雑性の要件を以下に示します。

- パスワードはユーザ名あるいはユーザ名の逆の順番を含むことができません。たとえば、ユーザ名が **abc** であるとき、**abc982** や **2cba** のようなパスワードはポリシーに適合しません。
- 文字あるいは数字が 3 回以上連続して続くことはできません。たとえば、**a111** のパスワードはポリシーに適合しません。

3.1.2 パスワードのアップデートと有効期限の終了

I. パスワードのアップデート

この機能は、ユーザがパスワードを変更する最小間隔を設定します。ユーザがパスワードを変更するためにログインした際、最後にパスワードを変更してからの間隔が短い場合、システムはパスワードの変更を拒否します。たとえばパスワードを変更する最小間隔を 48 時間に設定した場合、ユーザが 48 時間以内に 2 回パスワードを変更することはできません。

この最小間隔は、以下の場合影響がありません。

- ユーザが最初にログインした後にパスワードを変更します。
- パスワードの有効期限が終了した後にパスワードを変更します。

II. パスワードの終了

パスワードの有効期限の終了は、ユーザのパスワードのライフサイクルを変更させるようにします。パスワードの有効期限が終了した後、ユーザはパスワードの変更が必要となります。

ユーザが期限の切れたパスワードでログインした場合、システムはエラーメッセージを表示します。新しいパスワードを入力するように表示し、新しいパスワードを確認するため、再度新しいパスワードを入力するように表示します。新しいパスワードは正式なもので、ユーザが再入力したとき、最初に入力したパスワードと同一のパスワードを正確に入力する必要があります。

Web ユーザ、Telnet ユーザ、SSH ユーザ、コンソールユーザは、自身のパスワードを変更することができます。管理者は FTP ユーザ用にパスワードを変更する必要があります。

III. パスワード有効期限の終了までの早期通知

ユーザがログインするとき、システムは、パスワードの有効期限が少しで終了となるかどうかを確認します。有効期限が終了する場合、パスワードの変更を行うように通知します。

- ユーザがポリシーに適した新しいパスワードを適用した場合、新しいパスワードと時間を記録します。
- ユーザがパスワードを変更しない、あるいは変更に失敗した場合、システムは現在のパスワードを使用したユーザのログインを許可します。

Web ユーザ、Telnet ユーザ、SSH ユーザ、コンソールユーザは、自身のパスワードを変更することができます。管理者はFTPユーザ用にパスワードを変更する必要があります。

IV. 有効期限が終了したパスワードを使用したログイン

パスワードの有効期限が終了した後、ユーザが、指定した期間内に設定した回数のログインができるように設定することができます。たとえば、パスワードの有効期限が終了した後、最大 3 回、15 日間内にログインできるように設定した場合、ユーザは、パスワードの有効期限が終了した後、15 日以内に 3 回までログインすることができます。

V. パスワード履歴

この機能を有効にすると、システムはユーザが使用したパスワードを記録します。ユーザがパスワードを変更するとき、システムは現在のパスワードと、パスワード履歴にある記録されたパスワードを確認します。新しいパスワードは現在のパスワードとパスワード履歴に記録されたパスワードと、少なくとも 4 文字以上変更する必要があり、4 文字は互いに異なる必要があります。そうでなければ、エラーメッセージを表示し、パスワードは変更されません。

各ユーザ用でパスワード履歴に保持するパスワードの最大数を設定することができます。パスワード履歴の最大数を超えるとき、新しいパスワードが最初のパスワードに上書きされます。

装置管理ユーザの現在のログインパスワードはパスワード履歴に記録されません。これは装置管理ユーザのパスワードは暗号化テキストで保存され、プレーン（平文）テキストに回復することができないためです。

3.1.3 ユーザログイン管理

I. 初回ログイン

グローバルでパスワード管理機能が有効であるとき、ユーザはシステムにアクセスする前に初回ログイン時にパスワードを変更する必要があります。この状況では、パスワードの変更は最小変更間隔の設定に関係なく設定します。

II. ログイン試行制限

連続してログインの試行の失敗を制限することで、パスワードを類推することを効果的に防ぐことができます。

ログイン試行制限は FTP、Web および VTY ユーザに適用します。以下のタイプのユーザには適用しません。

- 存在しないユーザ（装置で設定されていないユーザ）
- コンソールポートを通して装置にログインするユーザ

ユーザがログインに失敗した場合、ユーザのアカウントとユーザの IP アドレスをパスワード管理のブラックリストに追加します。ユーザが最大連続試行回数を超えてログインに

失敗した場合、ログイン試行回数の制限によりユーザとユーザアカウントを以下の方法で制限します。

- パスワード管理ブラックリストから手動でユーザを削除するまでユーザアカウントを無効にします。
- ユーザがユーザアカウントの継続使用を許可します。ユーザがこのアカウントを使用して装置に正常にログインしたとき、ユーザの IP アドレスとユーザアカウントはパスワード管理のブラックリストから削除されます。
- 一定の時間、ユーザアカウントを無効にします。

ユーザは以下の状況のどちらかの状態の時、ログインを行うアカウントを使用することができます。

- □ ログインの試行を無効にする時間が終了したとき、アカウントを使用することができます。
- □ ログインの試行を無効にする時間が終了する前に、パスワード管理のブラックリストから手動でアカウントが削除されたとき、アカウントを使用することができます。

🕮 **メモ：**

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。ブラックリストに追加された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。

III. 最大アカウントアイドルタイム

ユーザアカウントの最大アカウントアイドルタイムを設定することができます。期間内にログインしないアカウントは、無効なアカウントで無効となります。

IV. 弱いパスワードによるログイン制御

システムは、Telnet、SSH、HTTP、HTTPS デバイス管理ユーザの弱いパスワードをチェックします。次の要件を満たしていない場合、パスワードは弱いものとなります。

- パスワード構成の制限。
- パスワード長の最小制限。
- パスワード複雑性チェックポリシー。

デフォルトでは、システムは弱いパスワードに関するメッセージを表示しますが、ユーザにパスワードの変更を強制しません。デバイスのセキュリティを向上させるために、特定された弱いパスワードの変更をユーザに強制する、強制的な弱いパスワード変更機能を有効にできます。ユーザは、パスワードがパスワード要件を満たした後にのみデバイスにログインできます。

3.1.4 すべての形式でのパスワードの非表示

セキュリティ目的のため、ユーザがパスワードを入力したとき、表示されません。

3.1.5 ロギング

システムは、すべての正常なパスワードの変更イベントと、ユーザがパスワード管理ブラックリストへ追加するイベントをロギングします。

3.2 制限とガイドライン

重要 ：
グローバルでパスワード管理機能を正常に有効にするため、装置に装置管理ユーザがログインすることを許可し、装置に十分な記憶容量があることを確認してください。

パスワード管理機能は、いくつかの異なる view で設定することができます。異なる view は異なる機能をサポートします。異なる view の設定、異なる目的のために、以下に示すような設定範囲を持ちます。

- super パスワードの設定は、super パスワードのみ適用されます。
- local user view での設定は、ローカルユーザのパスワードのみに適用します。
- local user view でユーザのパスワード管理ポリシーが設定されていない場合、user group view での設定はユーザグループのローカルユーザのパスワードに適用します。
- local user view と user group view の両方でユーザのパスワード管理ポリシーが設定されていない場合、system view でのグローバルの設定はすべてのユーザグループのローカルユーザのパスワードに適用します。

ローカルユーザパスワードでは、より小さい設定範囲の設定が高い優先度を持ちます。

グローバルパスワード管理が有効の場合、ローカルユーザ用に設定されたパスワードは表示されず、パスワードは現在の設定に保存されません。グローバルパスワード管理が無効の場合、ローカルユーザ用に設定されたパスワードは現在の設定で回復されます。現在の設定を表示するには、**display current-configuration** コマンドを使用します。

3.3 パスワード管理設定作業リスト

以下にパスワード管理を設定するための作業リストを示します。

作業リスト
(必須設定項目) パスワード管理の有効化
(オプション設定項目) グローバルパスワード管理パラメータの設定
(オプション設定項目) ユーザグループパスワード管理パラメータの設定
(オプション設定項目) ローカルユーザパスワード管理パラメータの設定
(オプション設定項目) superパスワード管理パラメータの設定

3.4 パスワード管理の有効化

I. 概要

グローバルでパスワード管理機能を有効にすると、すべてのパスワード管理の設定が適用されます。指定したパスワード管理機能を有効にするには、独自のパスワード制御機能を有効にします。

II. 制限とガイドライン

グローバルパスワード管理をイ有効にした後は、次の制約事項および注意事項に従ってください。

- 対応する **display** コマンドを使用して装置管理者用のパスワードと super パスワードを表示することはできません。ただし、ネットワークアクセス用設定のユーザパスワードは表示できます。
- 装置管理ユーザ用に設定する最初のパスワードには、4 文字以上の異なる文字を含める必要があります。

III. 設定手順

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． グローバルパスワード制御機能を有効にする	**password-control enable** [**network-class**]	デフォルト：無効
3． (オプション設定項目) 指定したパスワード機能を有効にする	**password-control** { **aging** | **composition** | **history** | **length** } **enable**	デフォルト：4つのすべてのパスワード管理機能は有効です。

3.5 グローバルパスワード管理パラメータの設定

I. 制限とガイドライン

グローバルパスワード管理パラメータを system view で設定すると、すべての装置管理ローカルユーザに適用されます。

パスワードエージングタイマ、最小パスワード長、およびパスワード設定ポリシーは、system view、user group view、および local user view で設定できます。アプリケーションスコープが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。ローカルユーザの場合は、local user view で設定されたパスワード設定が最も優先され、system view のグローバル設定が最も優先度が低くなります。

password-control login-attempt コマンドは、即座に適用され、パスワード管理ブラックリストにあるユーザに適用させることができます。他のパスワード管理設定は、既にログインしているユーザ、あるいは設定したパスワードに適用されません。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. 最小パスワード長を設定する	**password-control length** *length*	デフォルト：10文字
3. パスワード設定ポリシーを設定する	**password-control composition type-number** *type-number* [**type-length** *type-length*]	デフォルト：パスワードは少なくとも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。
4. パスワードの複雑性のポリシーを設定する	**password-control complexity** { **same-character** | **user-name** } **check**	デフォルト： **same-character** は無効、**user-name**は有効
5. 各ユーザのパスワード履歴の最大数を設定する	**password-control history** *max-record-number*	デフォルト：4
6. パスワードアップデートの最小間隔を設定する	**password-control update-interval** *interval*	デフォルト：24時間
7. パスワードの有効期限を設定する	**password-control aging** *aging-time*	デフォルト：90日
8. ユーザに通知されるパスワードの有効期限までの日数を設定する	**password-control alert-before-expire** *alert-time*	デフォルト：7日
9. 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する	**password-control expired-user-login delay** *delay* **times** *times*	デフォルト： 最大日時：30日 最大回数：3回
10. パスワード制御ブラックリスト機能を有効にする	**password-control blacklist all-line**	デフォルト：無効
11. 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とログイン最大試行回数を設定する	**password-control login-attempt** *login-times* [**exceed** { **lock** | **lock-time** *time* | **unlock** }]	デフォルト： 最大試行回数：3 アクション：ユーザが試行回数後にログインに失敗したとき、1分間ログインの試行をブロックします。
12. 最大アカウントアイドルタイムを設定する	**password-control login idle-time** *idle-time*	デフォルト：90日 ユーザアカウントがこの期間アイドル状態になると、アカウントは無効になり、装置へのログインに使用できなくなります。アカウントのアイドルタイムの制限を無効にするには、アイドルタイムの値を0に設定します。
13. ユーザ認証タイムアウト時間を設定する	**password-control authentication-timeout** *timeout*	デフォルト：600秒 Telnet、ターミナルユーザに対してのみ有効
14. 初回ログイン時のパスワード変更機能を無効にする	**undo password-control change-password first-login enable**	デフォルト：有効

3.6 ユーザグループパスワード管理パラメータの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. ユーザグループを作成し、user group view に移行する	**user-group** *group-name*	デフォルト : ユーザグループは存在しません。ユーザグループを設定する方法については、QX-W2300ACシリーズアクセスコントローラオペレーションマニュアルの“*13 ユーザアクセスと認証*“の”*3章 AAA*“を参照してください。
3. パスワードの有効期限を設定する	**password-control aging** *aging-time*	デフォルト : グローバルパスワードの有効期限と同一です。
4. 最小パスワード長を設定する	**password-control length** *length*	デフォルト : グローバル最小パスワード長と同一です。
5. パスワード設定ポリシーを設定する	**password-control composition type-number** *type-number* [**type-length** *type-length*]	デフォルト : グローバルパスワード設定ポリシーと同一です。
6. パスワードの複雑性のポリシーを設定する	**password-control complexity** { **same-character** | **user-name** } **check**	デフォルト : グローバルパスワードの複雑性のポリシーと同一です。
7. 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とログイン最大試行回数を設定する	**password-control login-attempt** *login-times* [**exceed** { **lock** | **lock-time** *time* | **unlock** }]	デフォルト : グローバルパスワードのログイン試行ポリシーと同一です。

3.7 ローカルユーザパスワード管理パラメータの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. ローカルユーザを作成し、local user view に移行する	・装置管理ユーザ **local-user** *user-name* **class manage** ・アクセスユーザ **local-user** *user-name* **class network**	デフォルト : 設定なし
3. パスワードの有効期限を設定する	**password-control aging** *aging-time*	デフォルト : ローカルユーザが属しているユーザグループの有効期限と同一です。ユーザグループの有効期限が設定されていない場合、グローバルの設定が適用されます。

操作	コマンド	補足
4. 最小パスワード長を設定する	**password-control length** *length*	デフォルト : ローカルユーザが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。ユーザグループの最小パスワード長が設定されていない場合、グローバルの設定が適用されます。
5. パスワード設定ポリシーを設定する	**password-control composition type-number** *type-number* [**type-length** *type-length*]	デフォルト : ローカルユーザが属しているユーザグループのパスワード設定ポリシーと同一です。ユーザグループのパスワード設定ポリシーが設定されていない場合、グローバルの設定が適用されます。
6. パスワードの複雑性のポリシーを設定する	**password-control complexity** { **same-character** | **user-name** } **check**	デフォルト : ローカルユーザが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。ユーザグループの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、グローバルの設定が適用されます。
7. 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とログイン最大試行回数を設定する	**password-control login-attempt** *login-times* [**exceed** { **lock** | **lock-time** *time* | **unlock** }]	ローカルユーザが所属するユーザグループの設定と同一です。ユーザグループでログイン試行ポリシーが設定されていない場合、グローバルの設定が適用されます。

3.8 superパスワード管理パラメータの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. パスワードの有効期限を設定する	**password-control super aging** *aging-time*	デフォルト：90日
3. 最小パスワード長を設定する	**password-control super length** *length*	デフォルト：10文字
4. パスワード設定ポリシーを設定する	**password-control super composition type-number** *type-number* [**type-length** *type-length*]	デフォルト : superパスワードは少なくとも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。

3.9 パスワード管理の表示と維持

すべての view で **display** コマンドを実行でき、user view で **reset** コマンドを実行できます。

操作	コマンド
パスワード管理の設定を表示する	**display password-control** [**super**]
パスワード管理ブラックリストのユーザ情報を表示する	**display password-control blacklist** [**user-name** *name* | **ip** *ipv4-address*]
パスワード管理ブラックリストからユーザを削除する	**reset password-control blacklist** [**user-name** *name*]
パスワード履歴を削除する	**reset password-control history-record** [**super** [**role** *role-name*] | **network-class** [**user-name** *user-name*] | **user-name** *user-name*]

🕮 **メモ:**

reset password-control history-record コマンドは、パスワード履歴機能が無効になったとき、1 つあるいはすべてのユーザのパスワード履歴を削除することができます。

3.10 パスワード管理の設定例

3.10.1 パスワード管理の設定例

I. ネットワーク要件

グローバルパスワード管理ポリシーを以下のように設定します。

- パスワードは少なくとも 16 文字が必要です。
- パスワードは少なくとも 4 種類以上の文字タイプが必要で各文字タイプに 4 文字以上が必要です。
- FTP あるいは VTY ユーザが 2 回連続してパスワードの試行に失敗すると、ログインの試行を恒久的に禁止します。
- ユーザはパスワードの有効期限後に、60 日内で 5 回ログインすることができます。
- パスワードの有効期限を 30 日に設定します。
- 最小パスワードアップデート間隔を 36 時間に設定します。
- 最大アカウントアイドルタイムを 30 日に設定します。
- パスワードはユーザ名、ユーザ名の逆の順番を含むことができません。
- パスワードに 3 回以上連続した文字を禁止します。

ユーザロール **network-operator** の super パスワード管理ポリシーを以下のように設定します。

- super パスワードは少なくとも 24 文字が必要です。
- super パスワードは少なくとも 4 種類以上の文字タイプが必要で各文字タイプに 5 文字以上が必要です。

ローカル Telnet ユーザ **test** のパスワード管理ポリシーを以下のように設定します。

- パスワードは少なくとも 24 文字が必要です。
- パスワードは少なくとも 4 種類以上の文字タイプが必要で各文字タイプに 5 文字以上が必要です。
- パスワードの有効期限を 20 日に設定します。

II. 設定手順

グローバルにパスワード管理機能を有効にします。

```
<AC> system-view
[AC] password-control enable
```

ユーザが 2 回連続してパスワードの試行に失敗すると、ログインの試行を恒久的に禁止します。

```
[AC] password-control login-attempt 2 exceed lock
```

パスワードの有効期限を 30 日に設定します。

```
[AC] password-control aging 30
```

グローバルの最小パスワード長を 16 に設定します。

```
[AC] password-control length 16
```

最小パスワードアップデート間隔を 36 時間に設定します。

```
[AC] password-control update-interval 36
```

パスワードの有効期限が終了した後、ユーザが 60 日内で 5 回ログインできるように設定します。

```
[AC] password-control expired-user-login delay 60 times 5
```

最大アカウントアイドルタイムを 30 日に設定します。

```
[AC] password-control login idle-time 30
```

ユーザ名、ユーザ名の逆の順番を含むパスワードを拒否するように設定します。

```
[AC] password-control complexity user-name check
```

パスワードに 3 回以上連続した文字を禁止するように指定します。

```
[AC] password-control complexity same-character check
```

グローバルのパスワードを、少なくとも 4 種類以上の文字タイプで、各文字タイプに 4 文字以上が含まれるように指定します。

```
[AC] password-control composition type-number 4 type-length 4
```

super パスワードの最小パスワード長を 24 に設定します。

```
[AC] password-control super length 24
```

super パスワードを、少なくとも 4 種類以上の文字タイプで、各文字タイプに 5 文字以上が含まれるように指定します。

```
[AC] password-control super composition type-number 4 type-length 5
```

ユーザロール **network-operator** に切り替える super パスワードをプレーンテキストで **123456789ABGFTweuix@#$%!**に設定します。

```
[AC] super password role network-operator simple 123456789ABGFTweuix@#$%!
```

装置管理ユーザ **test** を作成します。

```
[AC] local-user test class manage
```

ユーザのサービスタイプを **Telnet** に設定します。

```
[AC-luser-manage-test] service-type telnet
```

ローカルユーザの最小パスワード長を 24 に設定します。

```
[AC-luser-manage-test] password-control length 24
```

ローカルユーザのパスワードを、少なくとも 4 種類以上の文字タイプで各文字タイプに 5 文字以上が含まれるように指定します。

```
[AC-luser-manage-test] password-control composition type-number 4 type-length 5
```

ローカルユーザのパスワードの有効期限を 20 日に設定します。

```
[AC-luser-manage-test] password-control aging 20
```

ローカルユーザのパスワードをインタラクティブモードで設定します。

```
[AC-luser-manage-test] password
Password:
Confirm :
Updating user information. Please wait ... ...
[AC-luser-manage-test] quit
```

III. 設定の確認

グローバルパスワード管理の設定を表示します。

```
<AC> display password-control
Global password control configurations:
 Password control:                       Enabled
 Password aging:                         Enabled (30 days)
 Password length:                        Enabled (16 characters)
 Password composition:                  Enabled (4 types, 4 characters per type)
 Password history:                       Enabled (max history record:4)
 Early notice on password expiration:  7 days
 Maximum login attempts:                 2
 Action for exceeding login attempts:  Lock
 Minimum interval between two updates: 36 hours
 User account idle time:                 30 days
 Logins with aged password:              5 times in 60 days
 Password complexity:                    Enabled (username checking)
                                         Enabled (repeated characters checking)
```

super パスワードのパスワード管理の設定を表示します。

```
<AC> display password-control super
 Super password control configurations:
 Password aging:                         Enabled (90 days)
 Password length:                        Enabled (24 characters)
 Password composition:                  Enabled (4 types, 5 characters per type)
```

ローカルユーザ **test** のパスワード管理設定を表示します。

```
<AC> display local-user user-name test class manage
Total 1 local users matched.

Device management user test:
  State:                     Active
  Service type:              Telnet
  User group:                system
```

```
  Bind attributes:
  Authorization attributes:
    Work directory:          flash:
    User role list:          network-operator
  Password control configurations:
    Password aging:          Enable (20 days)
    Password length:         Enable (24 characters)
    Password composition:    Enable (4 types, 5 characters per type)
```

目次

このセクションのページは **15-x-x** です。

4章 公開鍵 4-1
4.1 概要 4-1
4.2 ローカル鍵ペアの作成 4-2
4.2.1 設定ガイドライン 4-2
4.2.2 設定手順 4-2
4.3 ローカルキーペアのインポート 4-3
4.3.1 制限事項とガイドライン 4-3
4.3.2 前提条件 4-3
4.3.3 設定手順 4-3
4.4 ローカルホスト公開鍵の配布 4-4
4.4.1 指定したフォーマットのホスト公開鍵のファイルへのエクスポート 4-4
4.4.2 ホスト公開鍵の表示 4-4
4.5 ピアホスト公開キーの設定 4-5
4.5.1 ピアホスト公開キーの設定について 4-5
4.5.2 ピアホスト公開キー設定の制約事項とガイドライン 4-5
4.6 ピア公開鍵の設定 4-5
4.6.1 公開鍵ファイルからピアへのホスト公開鍵のインポート 4-5
4.6.2 ピアの公開鍵の入力 4-6
4.7 ローカル鍵ペアの削除 4-6
4.8 公開鍵の表示と維持 4-7
4.9 公開鍵の設定例 4-7
4.9.1 ピアのホスト公開鍵の入力例 4-7
4.9.2 公開鍵ファイルからの公開鍵のインポート例 4-9

4章 公開鍵

4.1 概要

この章では、以下の非対称鍵アルゴリズムの公開鍵の管理について記載します。

- RSA（Revest-Shamir-Adleman）
- DSA（Digital Signature Algorithm）
- ECDSA（Elliptic Curve Digital Signature Algorithm）
- SM2 algorithm

SSH、SSL を含む多くのセキュリティアプリケーションは、図 4-1に示すように 2 つの群の間でセキュリティの通信を行うため、非対称鍵アルゴリズムを使用します。暗号化と複号化を行うため、非対象鍵アルゴリズムは、2 つの分離した鍵（公開鍵と秘密鍵）を使用します。対称鍵は 1 つの鍵のみを使用します。

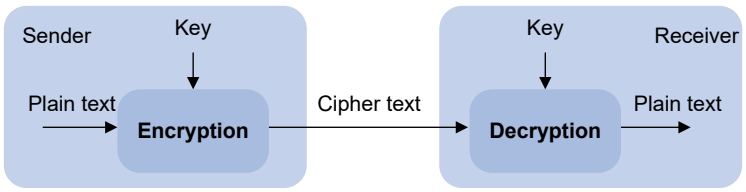


図 4-1 暗号化と複号化

鍵の所有者はプレーンテキスト（平文）で公開鍵を配布することができますが、秘密鍵を保持する必要があります。たとえ攻撃者がアルゴリズムと公開鍵を知っていたとしても秘密鍵を計算することは、数学上、実現不可能です。

セキュリティアプリケーションは以下の目的で非対象鍵アルゴリズムを使用します。

- **暗号化と複号化** – 公開鍵の受信者が情報を暗号化するために公開鍵を使用し、秘密鍵の所有者のみが情報を複号化できます。
- **デジタル署名** – 鍵の所有者は送信する”署名”情報に秘密鍵を使用します。受信者は情報が信頼できるか確認するため、送信者の公開鍵で情報を複号化します。

RSA、DSA はすべてのデジタル署名を実行できますが、RSA のみが暗号化と複号化を行うことができます。

非対称鍵アルゴリズムは、安全でないネットワークでセキュアな鍵の配布を行うことができます。

4.2 ローカル鍵ペアの作成

4.2.1 設定ガイドライン

ローカル鍵ペアを作成するとき、以下のガイドラインに従います。

- 鍵アルゴリズムはセキュリティアルゴリズム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。
  RSA または DSA 鍵ペアを作成する際に、鍵の長さは適切に設定してください。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。
  ECDSA キーペアを作成する場合は、適切な楕円曲線を選択します。楕円曲線によって ECDSA キーの長さが決まります。キーの長さが長いほどセキュリティが高くなり、キーの生成時間が長くなります。
  キーのモジュラス長とキーの長さの詳細については、表 4-1を参照してください。
- 鍵ペアの名前を割り当てない場合、システムは鍵ペアに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。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 4-1 非対称鍵ペアの異なるタイプの比較

タイプ	鍵ペアの数	鍵の長さ	推奨値
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ます。鍵ペアの名前はデフォルト名です。	範囲 : 512～2048ビット デフォルト：1024ビット	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。	範囲 : 512～2048ビット デフォルト：1024ビット	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。	範囲 : 192,256,384,521 ビット	少なくとも256ビットにしてください。

4.2.2 設定手順

以下にローカル鍵ペアを作成する設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. ローカル鍵ペアを作成する	**public-key local create** { **dsa** | **ecdsa** [**secp192r1** | **secp256r1** | **secp384r1** | **secp521r1**] | **rsa** } [**name** *key-name*]	デフォルト：作成なし

4.3 ローカルキーペアのインポート

このタスクは、キーペアファイルからデバイスにキーペアをインポートします。インポートされたキーペアは自動的に保存され、システムの再起動後も使用できます。

このタスクは、インポートするキーペアが証明書とは別のファイルに保存されている場合に実行します。キーペアと証明書が同じファイルに保存されている場合、デバイスは証明書をインポートすることでキーペアを取得できます。

4.3.1 制限事項とガイドライン

デバイスは RSA ホストキーペアのインポートをサポートしていますが、RSA サーバキーペアはサポートしていません。

キーペアに名前を割り当てない場合、システムはキーペアにデフォルト名を割り当て、キーペアをデフォルトとしてマークします。別のキーペアにデフォルト名を割り当てることもできますが、システムはキーペアをデフォルトとしてマークしません。キーペアの名前は、同じキーアルゴリズムを使用するすべての手動で命名されたキーペアの中で一意である必要があります。名前の競合が発生した場合は、既存のキーペアを上書きするかどうかを確認するメッセージが表示されます。

提供された復号パスワードを使用して、暗号化されたキーペアをデバイスに正常にインポートできます。

サポートされているキーのモジュラス長とキーの長さについては、表 4-2を参照してください。

表 4-2 鍵ペアの長さ

タイプ	鍵の長さ
RSA	512～2048ビット
ECDSA	192,256,384,521ビット

4.3.2 前提条件

このタスクを実行する前に、キーペアファイルを FTP またはその他の方法でデバイスのローカルストレージディレクトリに保存します。

4.3.3 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. ローカル鍵ペアをインポートする	**public-key local import** { **ecdsa** | **rsa** } [*key-name*] **filename** *filename*	デフォルト：作成なし

4.4 ローカルホスト公開鍵の配布

ピアの装置が以下のことを行えるようにピアの装置にローカルホスト公開鍵を配布する必要があります。

- 公開鍵を使用して、ローカル装置に送信された情報を暗号化します。
- ローカル装置によって署名されたデジタル署名を認証します。

ローカルホスト公開鍵を配布するには最初に鍵をエクスポートあるいは表示します。

- ホスト公開鍵をエクスポートします。
  - □ ホスト公開鍵をファイルにエクスポートします。
  - □ ホスト公開鍵をモニタ画面に表示し、表示したデータをファイルに保存します。

  ホスト公開鍵をファイルにエクスポートした後、ピアの装置にファイルを転送します。ピアの装置ではファイルからホスト公開鍵をインポートします。
- ホスト公開鍵を表示します。

  ホスト公開鍵を表示した後、鍵を記録します。たとえば、フォーマットされていないファイルにコピーします。ピアの装置で鍵を正確に入力する必要があります。

4.4.1 指定したフォーマットのホスト公開鍵のファイルへのエクスポート

操作	コマンド
1. system view に移行する	**system-view**
2. 指定したフォーマットのローカルホスト公開鍵をファイルへエクスポートする	• RSAホスト公開鍵をエクスポートする： **public-key local export rsa** [**name** *key-name*] { **openssh** | **ssh1** | **ssh2** } [*filename*] • ECDSAホスト公開鍵をエクスポートする： **public-key local export ecdsa** [**name** *key-name*] { **openssh** | **ssh2** } [*filename*] • DSAホスト公開鍵をエクスポートする： **public-key local export dsa** [**name** *key-name*] { **openssh** | **ssh2** } [*filename*]

4.4.2 ホスト公開鍵の表示

すべての view で **display** コマンドを実行することができます。

操作	コマンド
ローカルRSA公開鍵を表示する	**display public-key local rsa public** [**name** *key-name*]
ローカルECDSA公開鍵を表示する	**display public-key local ecdsa public** [**name** *key-name*]
ローカルDSA公開鍵を表示する	**display public-key local dsa public** [**name** *key-name*]

🕮 **メモ：**
ピアの装置に RSA サーバの公開鍵の serverkey（デフォルト）を配布しないでください。

4.5 ピアホスト公開キーの設定

4.5.1 ピアホスト公開キーの設定について

ピアデバイスに送信される情報を暗号化したり、ピアデバイスのデジタル署名を認証したりするには、ローカルデバイスでピアデバイスの公開キーを設定する必要があります。

ピアホストの公開キーを設定するには、次の方法を使用します。

- 公開キーファイルからピアホストの公開キーをインポートします (推奨) 。
- ピアホストの公開キーを手動で入力 (入力またはコピー) します。

4.5.2 ピアホスト公開キー設定の制約事項とガイドライン

ピアホスト公開キーを設定する場合は、次の制約事項とガイドラインに従ってください。

- ピアホスト公開キーを手動で入力する場合は、入力したキーが正しい形式であることを確認します。ピアホスト公開キーを正しい形式で取得するには、display public-key local public コマンドを使用して、ピアデバイス上の公開キーを表示し、キーを記録します。その他の方法で表示される公開キーの形式が正しくない可能性があります。キーが正しい形式でない場合、システムはキーを破棄し、エラーメッセージを表示します。
- デバイスが記録されたピアホスト公開キーの形式をサポートしているかどうかがわからない場合は、ピアホスト公開キーを入力するのではなく、常にインポートします。

4.6 ピア公開鍵の設定

以下の方法を用いてピアのホスト公開鍵を設定することができます。

- 公開鍵ファイルから公開鍵をインポートします。（推奨）
- 公開鍵を手動で設定します。（鍵データを入力またはコピー）

4.6.1 公開鍵ファイルからピアへのホスト公開鍵のインポート

ホスト公開鍵をインポートする前に、ピアの装置にホスト公開鍵がエクスポートされており、ピアの装置からファイルを取得していることを確認してください。ホスト公開鍵のエクスポートについては、本章の *“ローカルホスト公開鍵の配布”* を参照してください。

鍵をインポートしたのち、システムは自動的に公開鍵を PKCS（Public Key Cryptography Standards）フォーマットの文字列へ変換します。

以下に公開鍵ファイルからピアへのホスト公開鍵のインポート手順を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. 公開鍵ファイルからピアのホスト公開鍵をインポートする	**public-key peer** *keyname* **import sshkey** *filename*	デフォルト : ピアのホスト公開鍵は存在しません。

4.6.2 ピアの公開鍵の入力

ホスト公開鍵をインポートする前に、ピアの装置にホスト公開鍵が表示されており、ホスト公開鍵が記録されていることを確認してください。

display public-key local public コマンドを使用して、公開鍵を表示してください。他の方法で表示された公開鍵のフォーマットは、正確ではない場合があります。ホスト公開鍵が正しいフォーマットでない場合、システムはホスト公開鍵を廃棄し、エラーメッセージを表示します。ホスト公開鍵が正しいフォーマットである場合、システムはホスト公開鍵を保存します。

記録されたピアのホスト公開鍵のフォーマットをサポートしているか不明な場合、ピアのホスト公開鍵を入力する方法ではなく、ホスト公開鍵ファイルからインポートする方法を行ってください。

以下にピアの公開鍵の入力手順を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. ピアの公開鍵の名前を指定し、public key view に移行する	**public-key peer** *keyname*	デフォルト : ピアのホスト公開鍵は存在しません。
3. 鍵を入力あるいはコピーする	―	空白と改行は使用できますが保存しません。
4. system view に戻る	**peer-public-key end**	public key viewから戻ると、自動的に公開鍵を保存します。

4.7 ローカル鍵ペアの削除

以下の状況が発生した後、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
- ローカル証明書の有効期限が切れた場合

以下にローカル鍵ペアを削除する設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. ローカル鍵ペアを削除する	**public-key local destroy**{ **dsa** | **ecdsa** | **rsa** } [**name** *key-name*]	―

4.8 公開鍵の表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
ローカル公開鍵を表示する	**display public-key local** { **dsa** | **ecdsa** | **rsa** } **public** [**name** *key-name*]
ピアのホスト公開鍵を表示する	**display public-key peer** [**brief** | **name** *publickey-name*]

4.9 公開鍵の設定例

4.9.1 ピアのホスト公開鍵の入力例

I. ネットワーク要件

図 4-2に示すように、不正なアクセスを防止するため、AC はデジタル署名によって Device を認証します。AC 上で認証パラメータを設定する前に、AC 上で Device の公開鍵を設定します。

- Device の認証に RSA の非対称鍵アルゴリズムを使用するために AC を設定します。
- AC 上で、Device の公開鍵ペアのホスト公開鍵を手動で指定します。

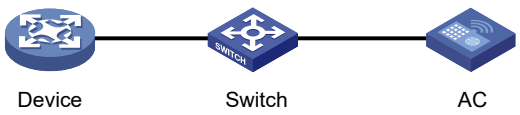


図 4-2 ネットワーク図

II. 設定手順

1)　Device を設定します。

Device にデフォルト名のローカル RSA 鍵ペアを作成し、鍵の長さをデフォルトの 1024 ビットに設定します。

```
<Device> system-view
[Device] 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.
```

すべての RSA 鍵ペアの公開鍵を表示します。

```
[Device] display public-key local rsa public
=============================================
Key name: hostkey (default)
Key type: RSA
Time when key pair created: 16:48:31 2015/05/12
Key code:
   30819F300D06092A864886F70D010101050003818D0030818902818100DA3B90F59237347B
   8D41B58F8143512880139EC9111BFD31EB84B6B7C7A1470027AC8F04A827B30C2CAF79242E
   45FDFF51A9C7E917DB818D54CB7AEF538AB261557524A7441D288EC54A5D31EFAE4F681257
   6D7796490AF87A8C78F4A7E31F0793D8BA06FB95D54EBB9F94EB1F2D561BF66EA27DFD4788
   CB47440AF6BB25ACA50203010001
=============================================
Key name: serverkey (default)
Key type: RSA
Time when key pair created: 16:48:31 2015/05/12
Key code:
   307C300D06092A864886F70D0101010500036B003068026100C9451A80F7F0A9BA1A90C7BC
   1C02522D194A2B19F19A75D9EF02219068BD7FD90FCC2AF3634EEB9FA060478DD0A1A49ACE
   E1362A4371549ECD85BA04DEE4D6BB8BE53B6AED7F1401EE88733CA3C4CED391BAE633028A
   AC41C80A15953FB22AA30203010001
```

2)　AC を設定します。

public key view で Device のホスト公開鍵を入力します。鍵は Device での表示と同一になるように、正確に入力してください。

```
<AC> system-view
[AC] public-key peer device
Enter public key view. Return to system view with "peer-public-key end" command.
[AC-pkey-public-key-device]30819F300D06092A864886F70D010101050003818D00308
18902818100DA3B90F59237347B
[AC-pkey-public-key-device]8D41B58F8143512880139EC9111BFD31EB84B6B7C7A147
0027AC8F04A827B30C2CAF79242E
[AC-pkey-public-key-device]45FDFF51A9C7E917DB818D54CB7AEF538AB261557524A
7441D288EC54A5D31EFAE4F681257
[AC-pkey-public-key-device]6D7796490AF87A8C78F4A7E31F0793D8BA06FB95D54EB
B9F94EB1F2D561BF66EA27DFD4788
[AC-pkey-public-key-device]CB47440AF6BB25ACA50203010001
```

system view に戻り、公開鍵を保存します。

```
[AC-pkey-public-key-device] peer-public-key end
```

III. 設定の確認

Device と同一の鍵であることを確認してください。

```
[AC] display public-key peer name device
=============================================
Key name: device
Key type: RSA
Key modulus: 1024
Key code:
```

```
    30819F300D06092A864886F70D010101050003818D0030818902818100DA3B90F59237347B
    8D41B58F8143512880139EC9111BFD31EB84B6B7C7A1470027AC8F04A827B30C2CAF79242E
    45FDFF51A9C7E917DB818D54CB7AEF538AB261557524A7441D288EC54A5D31EFAE4F681257
    6D7796490AF87A8C78F4A7E31F0793D8BA06FB95D54EBB9F94EB1F2D561BF66EA27DFD4788
    CB47440AF6BB25ACA50203010001
```

4.9.2 公開鍵ファイルからの公開鍵のインポート例

I. ネットワーク要件

図 4-3に示すように、AC は Device をデジタル署名によって認証します。AC 上で認証パラメータを設定する前に、AC 上で Device の公開鍵を設定します。

- Device の認証に RSA の非対称鍵アルゴリズムを使用するために AC を設定します。
- 公開鍵ファイルから AC へ、Device のホスト公開鍵をインポートします。

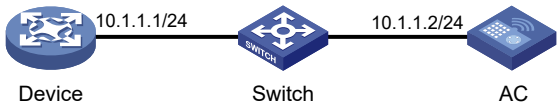


図 4-3 ネットワーク図

II. 設定手順

1)　Device を設定します。

Device にデフォルト名のローカル RSA 鍵ペアを作成し、鍵の長さをデフォルトの 1024 ビットに設定します。

```
<Device> system-view

[Device] 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.
```

すべてのローカル RSA 鍵ペアの公開鍵を表示します。

```
[Device] display public-key local rsa public
=============================================
Key name: hostkey (default)
Key type: RSA
Time when key pair created: 16:48:31 2015/05/12
Key code:
    30819F300D06092A864886F70D010101050003818D0030818902818100DA3B90F59237347B
    8D41B58F8143512880139EC9111BFD31EB84B6B7C7A1470027AC8F04A827B30C2CAF79242E
    45FDFF51A9C7E917DB818D54CB7AEF538AB261557524A7441D288EC54A5D31EFAE4F681257
    6D7796490AF87A8C78F4A7E31F0793D8BA06FB95D54EBB9F94EB1F2D561BF66EA27DFD4788
    CB47440AF6BB25ACA50203010001
=============================================
Key name: serverkey (default)
```

```
Key type: RSA
Time when key pair created: 16:48:31 2015/05/12
Key code:
   307C300D06092A864886F70D0101010500036B003068026100C9451A80F7F0A9BA1A90C7BC
   1C02522D194A2B19F19A75D9EF02219068BD7FD90FCC2AF3634EEB9FA060478DD0A1A49ACE
   E1362A4371549ECD85BA04DEE4D6BB8BE53B6AED7F1401EE88733CA3C4CED391BAE633028A
   AC41C80A15953FB22AA30203010001
```

RSA ホスト公開鍵をファイル **devicea.pub** にエクスポートします。

```
[Device] public-key local export rsa ssh2 device.pub
[Device] quit
```

FTP サーバ機能を有効にし、FTP ユーザをユーザ名 **ftp**、パスワード **123**、FTP のユーザロールを **network-admin** で作成します。

```
[Device] ftp server enable
[Device] local-user ftp
[Device-luser-manage-ftp] password simple 123
[Device-luser-manage-ftp] service-type ftp
[Device-luser-manage-ftp] authorization-attribute user-role network-admin
[Device-luser-manage-ftp] quit
```

2) AC を設定します。

Device から、公開鍵ファイル **devicea.pub** を FTP のバイナリモードで取得します。

```
<AC> ftp 10.1.1.1
Connected to 10.1.1.1 (10.1.1.1).
220 FTP service ready.
User(10.1.1.1:(none)):ftp
331 Password required for ftp.
Password:
230 User logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> binary
200 TYPE is now 8-bit binary
ftp> get device.pub
227 Entering Passive Mode (10,1,1,1,118,252)
150 Accepted data connection
226 File successfully transferred
301 bytes received in 0.003 seconds (98.0 kbyte/s)
ftp> quit
221-Goodbye. You uploaded 0 and downloaded 1 kbytes.
221 Logout.
```

鍵ファイル **devicea.pub** からホスト公開鍵をインポートします。

```
<AC> system-view
[AC] public-key peer device import sshkey device.pub
```

III. 設定の確認

ホスト公開鍵が Device の公開鍵と同一であることを確認します。

[AC] display public-key peer name device

```
==========================================
Key name: device
Key type: RSA
Key modulus: 1024
Key code:
   30819F300D06092A864886F70D010101050003818D0030818902818100DA3B90F59237347B
   8D41B58F8143512880139EC9111BFD31EB84B6B7C7A1470027AC8F04A827B30C2CAF79242E
   45FDFF51A9C7E917DB818D54CB7AEF538AB261557524A7441D288EC54A5D31EFAE4F681257
   6D7796490AF87A8C78F4A7E31F0793D8BA06FB95D54EBB9F94EB1F2D561BF66EA27DFD4788
   CB47440AF6BB25ACA50203010001
```

目次

このセクションのページは **15-x-x** です。

5章 SSH 5-1
5.1 概要 5-1
5.1.1 SSHの動作 5-1
5.1.2 SSH認証方式 5-2
5.2 SSHサーバの設定 5-4
5.2.1 ローカル鍵ペアの作成 5-4
5.2.2 Stelnetサーバ機能の有効化 5-5
5.2.3 SFTPサーバ機能の有効化 5-5
5.2.4 SCPサーバ機能の有効化 5-6
5.2.5 SSHログインのユーザラインの設定 5-6
5.2.6 クライアントのホスト公開鍵の設定 5-6
5.2.7 SSHユーザの設定 5-8
5.2.8 SSH管理パラメータの設定 5-9
5.2.9 SSHセッションの切断 5-10
5.3 Stelnetクライアントの設定 5-10
5.3.1 Stelnetクライアントの作業設定リスト 5-10
5.3.2 ローカル鍵ペアの作成 5-11
5.3.3 SSHパケットの送信元IPアドレスの指定 5-11
5.3.4 Stelnetサーバとの接続の確立 5-12
5.3.5 Stelnetクライアント上のサーバ公開鍵の削除 5-12
5.3.6 Suite BのStelnetサーバとの接続の確立 5-12
5.4 SFTPクライアントの設定 5-13
5.4.1 SFTPクライアントの設定作業リスト 5-13
5.4.2 ローカル鍵ペアの作成 5-13
5.4.3 SFTPパケットの送信元IPアドレスの指定 5-14
5.4.4 SFTPサーバとの接続の確立 5-14
5.4.5 SFTPクライアント上のサーバ公開鍵の削除 5-15
5.4.6 Suite BのSFTPサーバとの接続の確立 5-15
5.4.7 SFTPディレクトリの操作 5-16
5.4.8 SFTPファイルの操作 5-16
5.4.9 ヘルプ情報の表示 5-16
5.4.10 SFTPサーバの接続の切断 5-17
5.5 SCPクライアントの設定 5-17
5.5.1 SCPクライアントの設定作業リスト 5-17
5.5.2 ローカル鍵ペアの作成 5-17
5.5.3 SCPパケットの送信元IPアドレスの指定 5-18
5.5.4 SCPサーバとの接続の確立 5-18
5.5.5 SCPクライアント上のサーバ公開鍵の削除 5-19
5.5.6 Suite BのSCPサーバとの接続の確立 5-19
5.6 SSH2のアルゴリズム設定 5-20
5.6.1 SSH2のアルゴリズムについて 5-20
5.6.2 鍵交換アルゴリズムの指定 5-20
5.6.3 公開鍵アルゴリズムの指定 5-20
5.6.4 暗号化アルゴリズムの指定 5-21

5.6.5 MACアルゴリズムの指定 5-21
5.7 SSHの表示と維持 5-21
5.7.1 公開鍵情報の表示 5-22
5.7.2 SSHサーバの実行ステータスの確認 5-22
5.7.3 SSHクライアント設定の確認 5-22
5.7.4 SSH2アルゴリズムの表示 5-22
5.8 Stelnet設定例 5-23
5.8.1 パスワード認証を有効にしたStelnetサーバ設定例 5-23
5.8.2 公開鍵認証を有効にしたStelnetサーバの設定例 5-25
5.8.3 パスワード認証を有効にしたStelnetクライアント設定例 5-32
5.8.4 公開鍵認証を有効にしたStelnetクライアント設定例 5-36
5.9 SFTP設定例 5-38
5.9.1 パスワード認証を有効にしたSFTPサーバの設定例 5-38
5.9.2 公開鍵認証を有効にしたSFTPクライアント設定例 5-41
5.10 SCP設定例 5-44
5.10.1 パスワード認証を有効によるSCPの設定例 5-44

5章 SSH

5.1 概要

SSH（Secure Shell）はネットワークセキュリティプロトコルです。暗号化と認証を使用して、安全にリモートアクセスを行い、ファイルを転送することができます。

一般的なクライアント／サーバモデルを適用して、SSH は TCP をもとにしてデータの転送を保護するチャネルを確立させます。

SSH は SSH1.x と SSH2.0 の 2 つのバージョンをサポートしています。（以降、SSH1 と SSH2 と記載します。）SSH1 と SSH2 では互換性がありません。SSH2 は SSH1 よりも性能とセキュリティを向上しています。

装置は SSH サーバあるいは SSH クライアントとして動作することができます。

- SSH サーバとして動作する場合、装置は SSH クライアントのサービスを提供し、以下のバージョンを SSH サポートします。
  - Stelnet（Secure Telnet）、SFTP（Secure File Transfer Protocol）で装置は SSH2、SSH1 の SSH バージョンをサポートします。
- SSH クライアントとして動作する場合、装置は SSH2 のみサポートします。ユーザが SSH サーバと SSH 接続を確立するために使用します。

装置は以下の SSH アプリケーションをサポートします。

- **Stelnet（Secure Telnet）** – Stelnet は安全で信頼性のあるネットワーク端末アクセスサービスを提供します。Stelnet を使用して、ユーザはリモートサーバに安全にログインすることができます。Stelnet は、IP スプーフィングやプレーンテキストのパスワードの傍受のような装置への攻撃を保護することができます。装置は Stelnet サーバあるいは Stelnet クライアントとして動作することができます。
- **SFTP（Secure File Transfer Protocol）** – SSH2 をもとにして SSH を使用した SFTP は安全なファイル転送を提供します。装置は SFTP サーバとして動作し、リモートユーザが安全なファイル管理と転送を行うため、SFTP サーバにログインできます。また装置は SFTP クライアントとして動作します。ユーザが装置からリモート装置にログインし、安全なファイル転送を行うことができます。
- **SCP（Secure Copy）** – SSH 2 に基づいて、ファイルをコピーする安全な方法を提供します。装置は SCP サーバとして機能し、ユーザは装置にログインしてファイルのアップロードとダウンロードを行うことができます。装置は SCP クライアントとしても機能し、ユーザは装置からリモート装置にログインして安全なファイル転送を行うことができます。

5.1.1 SSH の動作

この章では、SSH セッションの確立に関連するステージの例を、SSH2 を使用して示します。ステージの詳細は SSH の技術書を参照してください。

表 5-1 SSH セッションを確立するステージ

ステージ	説明
接続の確立	SSHサーバはポート番号22で接続リクエストを受け入れます。クライントが接続要求を初期化した後、サーバとクライントはTCP接続を確立します。
バージョンのネゴシエーション	2つの群（サーバとクライアント）間で使用するバージョンを決めます。
アルゴリズムのネゴシエーション	SSHは複数のアルゴリズムをサポートします。ローカルアルゴリズムにもとづいて、2つの群（サーバとクライアント）は、以下のアルゴリズムを決定します。 • セッション鍵を作成するアルゴリズムの鍵交換アルゴリズム • 暗号データ用の暗号アルゴリズム • デジタル署名と認証のための公開鍵アルゴリズム • データの完全性を保護するためのHMACアルゴリズム
鍵交換	2つの群（サーバとクライアント）は、セッション鍵とセッションIDを動的に作成するため、DH交換アルゴリズムを使用します。 • セッション鍵はデータの転送を保護するために使用します。 • セッションIDはSSH接続を認識するために使用します。 このステージでは、クライアントはサーバと同様に認証します。
認証	SSHサーバはクライアントからの認証要求に応答し、認証を実行します。
セッション要求	認証にパスした後、クライアントがセッション要求（あるいはStelnet、SFTPサービスのリクエスト）をサーバに送信します。
データ交換	サーバが要求に承諾した後、クライアントとサーバはセッションで互いに通信を行います。 このステージでは、テキストフォーマットでコマンドを貼り付け、CLIで実行することができます。一度に貼り付けることができるテキストは、2000バイトよりも少ない値としてください。コマンドを正常に実行するため同じviewで使用することを推奨します。 2000バイト以上のコマンドを実行する場合、設定ファイルにコマンドを保存し、SFTPを通してサーバにアップロードし、サーバを再起動してください。

5.1.2 SSH 認証方式

この章では装置を SSH サーバとして動作させるとき、サポートする認証方式について記載します。

I. パスワード認証

SSH サーバは、AAA を使用してクライアントを認証します。パスワード認証は以下のように処理します。

1) SSH クライアントは暗号化されたユーザ名とパスワードが含まれる認証要求をサーバに送信します。
2) SSH サーバは以下の処理を行います。

a) プレーンテキストのユーザ名とパスワードを取得するため要求を復号化します。

b) ローカル、あるいはリモートAAA認証によってユーザ名とパスワードが正しいか確認します。

c)　認証結果をクライアントに通知します。

セカンダリ認証のため AAA サーバがユーザのパスワードを必要とする場合、ユーザはプロンプトが運ばれる認証応答を SSH サーバに送ります。プロンプトは透過的にクライアントに送信され、ユーザに指定のパスワードを入力するように通知します。ユーザが正しいパスワードを入力したとき、AAA サーバ上でパスワードの妥当性をチェックします。パスワードが有効である場合、SSH サーバはクライアントに認証成功メッセージを返します。

AAA 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 9 *セキュリティ "AAA"* を参照してください。

🕮 **メモ：**

SSH1 は AAA サーバによって開始されるセカンダリパスワード認証をサポートしていません。

II. 公開鍵認証

サーバは、クライアントのデジタル署名を使用してクライアントを認証します。公開鍵認証は以下のように処理します。

1) SSH クライアントはユーザ名、公開鍵、公開鍵アルゴリズム名が含まれる認証要求をサーバに送信します。

   クライアントのデジタル署名が認証で要求される場合、クライアントは認証要求のデジタル署名をカプセル化します。デジタル署名にはクライアントの公開鍵情報が含まれます。

2) サーバは公開鍵が有効かどうかを確認します。

- 公開鍵が無効である場合、認証が失敗します。サーバは認証が失敗したことをクライアントに通知します。
- 公開鍵が有効である場合、サーバはクライアントのデジタル署名を要求します。デジタル署名を受信したのち、サーバはデジタル署名を確認するために公開鍵を使用します。最後に認証結果をクライアントに送信します。

SSH サーバとして動作するとき、装置はデジタル署名を確認するため、公開鍵アルゴリズム RSA と DSA を使用します。

SSH クライアントとして動作するとき、装置はデジタル署名を作成するため、公開鍵アルゴリズム RSA と DSA を使用します。

公開鍵の設定についての詳細は、オペレーションマニュアルのセクション 9 *セキュリティ "公開鍵"* を参照してください。

III. パスワード-公開鍵認証

サーバは SSH2 クライアントに、パスワード認証と公開鍵認証の両方にパスするように要求します。SSH1 クライアントは、サーバの要求に関係なく、どちらか 1 つの認証のみ必要です。

IV. いずれかの認証

サーバはパスワード認証あるいは公開鍵認証のいずれかにパスするようにクライアントに要求します。

5.2 SSHサーバの設定

作業リスト	補足
（オプション設定項目） ローカル鍵ペアの作成	ー
（必須設定項目） Stelnetサーバ機能の有効化	Stelnetでのみ必須設定項目です。
（必須設定項目） SFTPサーバ機能の有効化	SFTPサーバでのみ必須設定項目です。
（必須設定項目）SSHログインのユーザラインの設定	Stelnetでのみ必須設定項目です。
（必須設定項目） クライアントのホスト公開鍵の設定	認証方法が公開鍵、パスワード-公開鍵認証あるいはいずれかの方法を使用する場合、必須設定項目です。
（必須設定項目/オプション設定項目） SSHユーザの設定	認証方法が公開鍵、パスワード-公開鍵認証あるいはいずれかの方法を使用する場合、必須設定項目です。 パスワード認証のみ使用するユーザでは、オプション設定項目です。
（オプション設定項目）SSH管理パラメータの設定	ー

5.2.1 ローカル鍵ペアの作成

DSA、ECDSA、RSA 鍵ペアは、鍵交換ステージのセッション鍵とセッション ID を作成するために必要です。DSA または RSA 鍵ペアは、クライアントがサーバを認証するために、クライアントによって使用されます。クライアントがサーバを認証するとき、サーバから受信した公開鍵を、ローカルに保存したサーバ公開鍵と比較します。鍵が一致している場合、クライアントはサーバから受信したデジタル署名を復号化するため、クライアントがローカルに保存したサーバの公開鍵を使用します。デジタル署名の復号化に成功した場合、認証は成功します。

SSH アプリケーションを実行させるため、装置で SSH コマンドを実行するとき、SSH サーバは自動で 1 つの RSA サーバ鍵ペアと 1 つの DSA サーバ鍵ペアの鍵ペアを作成します。2 つの鍵ペアはデフォルトの名前を使用します。

異なるタイプのキーペアを使用する SSH クライアントをサポートするには、SSH サーバで DSA、ECDSA、RSA キーペアを生成します。

- RSA キーペアーSSH サーバは、RSA 用のサーバキーペアとホストキーペアを生成します。RSA サーバキーペアは、セッションキーの安全な送信のためにセッションキーを暗号化するために SSH 1 でのみ使用されます。SSH 2 ではセッションキーの送信が必要ないため、SSH 2 では使用されません。
- DSA キーペアーSSH サーバは 1 つの DSA ホストキーペアだけを生成します。SSH 1 は DSA アルゴリズムをサポートしません。
- ECDSA キーペアーSSH サーバは ECDSA ホストキーペアを 1 つだけ生成します。

装置の DSA/ECDSA/RSA 鍵ペアを作成するため **public-key local create** コマンドを使用します。

I. 設定ガイドライン

ローカル鍵ペアを作成するとき、以下の制限とガイドラインに従ってください。

- SSH は、デフォルト名でローカルに作成された DSA,ECDSA,RSA の鍵ペアのみをサポートします。
- 鍵ペアの異なるタイプを使用する SSH クライアントをサポートするため、SSH サーバで DSA。ECDSA、RSA 鍵ペアの両方を作成します。
- **public-key local create rsa** コマンドは RSA のサーバ鍵ペアとホスト鍵ペアのみを作成します。SSH1 ではサーバ鍵ペアの公開鍵はセッション鍵の安全な転送を行うため暗号化するのに使用されます。SSH2 は、SSH サーバとクライアントの各セッション鍵を作成する DH アルゴリズムを使用するため、セッション鍵の転送は必要ありません。サーバ鍵ペアは SSH2 で使われません。
- **public-key local create dsa** コマンドは DSA ホスト鍵ペアのみを作成します。SSH1 は DSA アルゴリズムをサポートしません。SSH サーバで **public-key local create dsa** コマンドを使用するとき、鍵の長さは 2048 ビットよりも短くしてください。
- **public-key local create ecdsa** コマンドで、ECDSA ホストキーペアを作成します。鍵の長さは、secp 256 r 1 または secp 384 r 1 のどちらかのみ生成できます。

II. 設定手順

以下に SSH サーバでローカル DSA、ECDSA、RSA 鍵ペアを生成する設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. ローカル DSA,ECDSA,RSA 鍵ペアを作成する	**public-key local create { dsa | ecdsa { secp 256 r 1 | secp 384 r 1 } | rsa }**	デフォルト : 鍵ペアは存在しません。

5.2.2 Stelnet サーバ機能の有効化

装置で Stelnet サーバ機能を有効にしたのち、クライアントは Stelnet を通して装置にログインすることができます。

以下に Stelnet サーバ機能の有効化の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. Stelnet サーバ機能を有効にする	**ssh server enable**	デフォルト：無効

5.2.3 SFTP サーバ機能の有効化

装置で SFTP サーバ機能を有効にしたのち、クライアントは SFTP を通して装置にログインすることができます。

SFTP サーバとして動作する装置は SSH1 クライアントから開始された SFTP 接続をサポートしません。

以下に SFTP サーバ機能の有効化の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． SFTP サーバ機能を有効にする	**sftp server enable**	デフォルト：無効

5.2.4 SCP サーバ機能の有効化

装置で SCP サーバ機能を有効にしたのち、クライアントは SCP を通して装置にログインすることができます。

SCP サーバとして動作する装置は SSH1 クライアントから開始された SCP 接続をサポートしません。

以下に SCP サーバ機能の有効化の設定を示します。

操作	コマンド	補足
3． system view に移行する	**system-view**	―
4． SCP サーバ機能を有効にする	**scp server enable**	デフォルト：無効

5.2.5 SSH ログインのユーザラインの設定

SSH アプリケーションに依存して、SSH クライアントは Stelnet クライアント、あるいは SFTP クライアントとなります。

Stelnet 接続を確立するため、Stelnet クライアントは VTY ユーザラインを通して装置にアクセスする必要があります。SSH クライアントが SSH ログインできるようにユーザラインを設定する必要があります。この設定は次回ログインしたときにのみ適用します。

SFTP クライアントは VTY ユーザラインを使用しないで装置にアクセスします。

以下に Stelnet クライアントのユーザラインの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． VTY line view に移行する	**line vty** *first-number2* [*last-number2*]	―
3． ログイン認証モードをスキームに設定する	**authentication-mode scheme**	デフォルト：**password** コマンドの詳細は、コマンドマニュアルのセクション2 *基本機能“ログイン”*を参照してください。

5.2.6 クライアントのホスト公開鍵の設定

サーバがクライアントを認証するために公開鍵を使用する場合、サーバは SSH ユーザ名とクライアントから受信したホスト公開鍵をローカルに保存されている内容と比較しま

す。内容が一致した場合、クライアントが送信したデジタル署名を確認します。クライアントはホスト公開鍵に関連する秘密鍵にもとづいてデジタル署名を作成します。

公開鍵認証、パスワード-公開鍵認証、あるいはあらゆる認証を使用する SSH サーバのために、以下の処理を行う必要があります。

1) サーバ上でクライアントの DSA あるいは RSA ホスト公開鍵を設定します。

   SSH サーバの SSH クライアントホスト公開鍵は 20 以下に設定することを推奨します。

2) デジタル署名を作成するため関連するクライアントのホスト秘密鍵を指定します。もし装置が SSH クライアントとして動作する場合、クライアントの公開鍵アルゴリズムを指定します。アルゴリズムは、デジタル署名を作成するため、関連する秘密鍵を決定します。

クライアントのホスト公開鍵の内容を入力する、あるいは公開鍵ファイルからクライアントのホスト公開鍵をインポートすることができます。クライアントのホスト公開鍵をインポートすることを推奨します。

I. クライアントのホスト公開鍵の入力

クライアントのホスト公開鍵を入力する前に、クライアントのホスト公開鍵を取得するため、クライアントで **display public-key local public** コマンドを使用してください。他の方法で取得したホスト公開鍵は正式な形式でない可能性があるため、サーバに保存することができません。

以下にクライアントのホスト公開鍵を入力する方法を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. public key view に移行する	**public-key peer** *keyname*	ー
3. クライアントのホスト公開鍵を設定する	ホスト公開鍵の内容を入力する	ホスト公開鍵は変換されないDER復号形式である必要があります。 ホスト公開鍵の内容を入力する場合、空白と改行を使用することができます。 ホスト公開鍵を保存するとき、空白と改行は自動で削除されます。 詳細は、オペレーションマニュアルのセクション15 *セキュリティ“公開鍵”*を参照してください。
4. system view に戻る	**peer-public-key end**	ー

II. 公開鍵ファイルからのクライアントのホスト公開鍵のインポート

ホスト公開鍵をインポートする前に、クライアントの公開鍵ファイル（バイナリ形式）を FTP あるいは TFTP を使用してサーバにアップロードします。インポートを行う間、サーバは自動的に公開鍵ファイルのホスト公開鍵を、PKCS 形式に変換します。

以下に公開鍵ファイルからクライアントのホスト公開鍵をインポートする設定を示します。

操作	コマンド
1. system view に移行する	**system-view**
2. 公開鍵ファイルからクライアントの公開鍵をインポートする	**public-key peer** *keyname* **import sshkey** *filename*

5.2.7 SSH ユーザの設定

認証方式に依存して SSH ユーザとローカルユーザを設定します。

- 認証方式が公開鍵である場合、サーバに 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 ユーザに正しい作業ディレクトリとユーザロールを割り当てることができるように、2 つのユーザは同一のユーザ名にする必要があります。
- 認証方式がパスワード認証である場合、以下の処理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アカウントを設定します。
  - 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で SSH ユーザを設定します。

  ssh user コマンドを使用して SSH ユーザあるいはローカルユーザを作成する必要はありません。しかし集中管理を行うため、パスワード認証のみの SSH ユーザを含むすべての SSH ユーザを表示する場合、SSH ユーザあるいはローカルユーザを作成するコマンドを使用することができます。そのような SSH ユーザが作成される場合、サービスタイプと認証方式が正しく指定されていることを確認してください。
- 認証方式がパスワード-公開鍵認証あるいはそれ以外の認証方式である場合、SSH ユーザを作成し、以下の処理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アカウントを設定します。
  - 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で SSH ユーザを設定します。

  どちらの場合においても、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にする必要があります。

I. 設定ガイドライン

SSH ユーザを設定するとき、以下の制限とガイドラインに従ってください。

- SSH サーバは 1024 の SSH ユーザをサポートします。
- SFTP ユーザの作業ディレクトリは認証方式に依存します。
  - パスワード認証が使用される場合、作業ディレクトリは AAA によって許可されます。
  - 認証方式が公開鍵あるいはパスワード-公開鍵認証である場合、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。
- SSH ユーザでは、ユーザロールは認証方式に依存します。
  - パスワード認証が使用される場合、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。

- 認証方式が公開鍵あるいはパスワード-公開鍵認証である場合、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。

- すでにログインしている SSH ユーザの認証方式あるいは公開鍵を変更する場合、変更内容は次回ユーザがログインしたときに適用されます。
- パスワード認証を除いて、他の認証方式は、指定されたクライアントのホスト公開鍵が必要です。
  - クライアントが直接サーバにユーザの公開鍵の情報を送信する場合、サーバのクライアントの公開鍵を指定する必要があります。指定される公開鍵はすでに存在している必要があります。公開鍵の詳細は、オペレーションマニュアルのセクション 9 *セキュリティ “SSH”の “クライアントのホスト公開鍵の設定”* を参照してください。

II. 設定手順

以下に SSH ユーザを設定し、サービスタイプと認証方式を指定する手順を示します。

操作	コマンド
1. system view に移行する	**system-view**
2. SSH ユーザを作成し、サービスタイプと認証方式を指定する	**ssh user** *username* **service-type** { **all** | **scp** | **sftp** | **stelnet** } **authentication-type** { **password** | { **any** | **password-publickey** | **publickey** } [**assign** { **pki-domain** *domain-name* | **publickey** *keyname*&<1-6> }] }

5.2.8 SSH 管理パラメータの設定

以下に SSH 管理パラメータの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. SSH1 クライアントのサポートを有効にする	**ssh server compatible-ssh1x enable**	デフォルト：無効
3. SSH アルゴリズムの再ネゴシエーションとキー再交換を有効にする	**ssh server key-re-exchange enable** [**interval** *interval*]	デフォルト：無効 コマンドの設定後に確立された新しいSSH接続に対してのみ有効です。
4. RSA サーバのキーペアを更新する最小間隔を設定する	**ssh server rekey-interval** *interval*	デフォルト：RSAサーバ鍵ペアのアップデートを行いません。 この設定は、SSH 1クライアントでのみ有効です。
5. SSH ユーザ認証タイムアウトタイマを設定する	**ssh server authentication-timeout** *time-out-value*	デフォルト：60秒 タイムアウトタイマが終了したとき、接続用の認証が終了していない場合、接続を確立することができません。
6. SSH 認証の最大試行回数を設定する	**ssh server authentication-retries** *times*	デフォルト：3

操作	コマンド	補足
7. SSH ユーザの接続を管理する ACL を設定する	• SSHユーザのIPv4 ACLを設定する： **ssh server acl** { *basic-acl-number* | *advanced-acl-number* | **mac** *mac-acl-number* }	デフォルト：設定なし
8. SSH サーバが SSH クライアントに送信するパケットの DSCP を設定する	• IPv4パケットのDSCPを設定する： **ssh server dscp** *dscp-value*	デフォルト：48 DSCPはパケットのプライオリティを決定し、パケットを転送する優先度を決定します。DSCPの値が大きいほど優先度は高くなります。
9. SFTP 接続アイドルタイムアウトタイマを設定する	**sftp server idle-timeout** *time-out-value*	デフォルト：10分 アイドルタイマが指定したしきい値を超えたとき、システムは自動的に接続を切断します。
10. オンライン SSH ユーザの最大同時接続数を指定する	**aaa session-limit ssh** *max-sessions*	デフォルト：32 オンラインSSHユーザが上限に到達したとき、システムは新しいSSH接続要求を拒否します。オンラインSSHユーザには影響しません。

5.2.9 SSH セッションの切断

デバイスは同時に複数のログインセッションをサポートしています。SSH ログインユーザが設定に干渉するのを避けるために、SSH ログインユーザを切断することができます。

操作	コマンド
SSH セッションを切断する	**free ssh** { **user-ip** *ip-address* [**port** *port-number*] | **user-pid** *pid-number* | **username** *username* }

5.3 Stelnetクライアントの設定

5.3.1 Stelnet クライアントの作業設定リスト

設定リスト	補足
（必須設定項目）ローカル鍵ペアの作成	Stelnetサーバが**publickey**、**password-publickey,any**の認証方式を使用する際は必須です。
（オプション設定項目）SSHパケットの送信元IPアドレスの指定	―
（必須設定項目）Stelnetサーバとの接続の確立	―

設定リスト	補足
（オプション設定項目）Stelnetクライアント上のサーバ公開鍵の削除	
（オプション設定項目）Suite BのStelnetサーバとの接続の確立	

5.3.2 ローカル鍵ペアの作成

Stelnet サーバが **publickey**、**password-publickey**、あるいは **any** の認証方式を使用する際は、Stelnet クライアントでローカル鍵ペアを作成してください。

I. 設定ガイドライン

Stelnet クライアントでローカル鍵ペアを設定する際には、以下のガイドラインに従ってください。

- SSH のローカル DSA、ECDSA 及び RSA 鍵ペアはデフォルト名を使用します。鍵ペアに名前を割り当てることはできません。
- DSA 鍵ペアを作成するとき、鍵の長さは 2048 ビットよりも短くしてください。

II. 設定手順

以下に Stelnet クライアントでローカル鍵ペアを生成する設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． ローカル鍵ペアを作成する	**public-key local create** { **dsa** | **ecdsa** { **secp256r1** | **secp384r1** } | **rsa** }	デフォルト : 鍵ペアは存在しません。

5.3.3 SSH パケットの送信元 IP アドレスの指定

以下のため、SSH パケットの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の IP アドレスを指定することを推奨します。

- Stelnet クライアントと Stelnet サーバが互いに通信できることを保証します。
- 認証サービスの Stelnet クライアントの管理を向上します。

以下に SSH パケットの送信元 IP アドレスの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． SSH パケットの送信元 IP アドレスを設定する	• SSHパケットの送信元IPv4アドレスを指定する: **ssh client source** { **interface** *interface-type interface-number* | **ip** *ip-address* }	デフォルト：設定なし IPv4 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。

5.3.4 Stelnet サーバとの接続の確立

Stelnet サーバにアクセスするとき、装置はサーバを認証するためサーバのホスト公開鍵を使用します。装置でサーバのホスト公開鍵が設定されていない場合、装置はアクセスを継続するかどうかを確認するメッセージを表示します。

- アクセスを継続する場合、装置はサーバにアクセスし、サーバのホスト公開鍵をダウンロードします。
- アクセスを継続しない場合、接続は確立することができません。

安全でないネットワークでは装置でサーバのホスト公開鍵を設定することを推奨します。

以下に Stelnet サーバの接続を確立する設定を示します。

操作	コマンド	補足
Stelnetサーバの接続を確立する	• IPv4 Stelnetサーバの接続を確立する：**ssh2** *server* [*port-number*] [**identity-key** { **dsa** | **rsa** } | **prefer-compress zlib** | **prefer-ctos-cipher** { **3des-cbc** | **aes128-cbc** | **des-cbc** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** } | **prefer-kex** { **dh-group-exchange-sha1** | **dh-group1-sha1** | **dh-group14-sha1** } | **prefer-stoc-cipher** { **3des-cbc** | **aes128-cbc** | **des-cbc** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** }] * [**dscp** *dscp-value* | **escape** *character* | **public-key** *keyname* | **source** { **interface** *interface-type interface-number* | **ip** *ip-address* }] *	user viewで実行できます。

5.3.5 Stelnet クライアント上のサーバ公開鍵の削除

ローカルに保存されたサーバ公開キーがデバイス要件を満たしていない場合、クライアントはサーバに接続できません。サーバに接続するには、クライアントに保存されているサーバ公開キーを削除し、サーバに正しい公開キーが生成されていることを確認します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. 保存されているサーバ公開鍵を削除する	**delete ssh client server-public-key** [**server-ip** *ip-address*]	—

5.3.6 Suite B の Stelnet サーバとの接続の確立

ユーザ view で次のコマンドを実行して、Suite B に基づいた Stelnet サーバへの接続を確立します。

操作	コマンド	補足
Suite B のStelnetサーバに接続する	• IPv4 Stelnetサーバの接続を確立する： **ssh2** *server* [*port-number*] **suite-b** [**128-bit** | **192-bit**] **pki-domain** *domain-name* [**server-pki-domain** *domain-name*] [**prefer-compress zlib**] [**dscp** *dscp-value* | **escape** *character* | **source** { **interface** *interface-type interface-number* | **ip** *ip-address* }] *	user viewで実行できます。

5.4 SFTPクライアントの設定

5.4.1 SFTP クライアントの設定作業リスト

作業リスト	補足
（必須設定項目） ローカル鍵ペアの作成	Stelnetサーバが**publickey**、**password-publickey,any**の認証方式を使用する際は必須です。
（オプション設定項目）SFTPパケットの送信元IPアドレスの指定	—
（必須設定項目）SFTPサーバとの接続の確立	—
（オプション設定項目）保存されているサーバ公開鍵を削除する	—
（オプション設定項目）Suite BのSFTPサーバとの接続の確立	—
（オプション設定項目）SFTPディレクトリの操作	—
（オプション設定項目）SFTPファイルの操作	—
（オプション設定項目）ヘルプ情報の表示	—
（オプション設定項目）SFTPサーバの接続の切断	—

5.4.2 ローカル鍵ペアの作成

SFTP サーバが **publickey**、**password-publickey**、あるいは **any** の認証方式を使用する際は、SFTP クライアントでローカル鍵ペアを作成してください。

I. 設定ガイドライン

SFTP クライアントでローカル鍵ペアを設定する際には、以下のガイドラインに従ってください。

- SSH のローカル DSA、ECDSA 及び RSA 鍵ペアはデフォルト名を使用します。鍵ペアに名前を割り当てることはできません。
- DSA 鍵ペアを作成するとき、鍵の長さは 2048 ビットよりも短くしてください。
- ECDSA キーペアを生成する場合、secp256 r 1 または secp384 r 1 ECDSA キーペアのみを生成できます。

II. 設定手順

以下に SFTP クライアントでローカル鍵ペアを生成する設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． ローカル鍵ペアを作成する	**public-key local create** { **dsa** | **ecdsa** { **secp256r1** | **secp384r1** } | **rsa** }	デフォルト：鍵ペアは存在しません。

5.4.3 SFTP パケットの送信元 IP アドレスの指定

以下のため、SFTP パケットの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の IP アドレスを指定することを推奨します。

- SFTP クライアントと SFTP サーバが互いに通信できることを保証します。
- 認証サービスの SFTP クライアントの管理を向上します。

以下に SFTP パケットの送信元 IP アドレスの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． SFTP パケットの送信元 IP アドレスを指定する	• IPv4： **sftp client source** { **ip** *ip-address* | **interface** *interface-type interface-number* }	デフォルト：設定なし IPv4 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IPv4アドレスを使用します。

5.4.4 SFTP サーバとの接続の確立

SFTP サーバにアクセスするとき、装置はサーバを認証するためサーバのホスト公開鍵を使用します。装置でサーバのホスト公開鍵が設定されていない場合、装置はアクセスを継続するかどうかを確認するメッセージを表示します。

- アクセスを継続する場合、装置はサーバにアクセスし、サーバのホスト公開鍵をダウンロードします。
- アクセスを継続しない場合、接続は確立することができません。

安全でないネットワークでは装置でサーバのホスト公開鍵を設定することを推奨します。

接続が完了したのち、ディレクトリあるいはファイルのような操作を行うため、サーバの SFTP client view に直接移行することができます。

操作	コマンド	補足
SFTPサーバの接続を確立する	• IPv4： **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* }] *	user viewで実行できます。

5.4.5 SFTP クライアント上のサーバ公開鍵の削除

ローカルに保存されたサーバ公開キーがデバイス要件を満たしていない場合、クライアントはサーバに接続できません。サーバに接続するには、クライアントに保存されているサーバ公開キーを削除し、サーバに正しい公開キーが生成されていることを確認します。

操作	コマンド	補足
3． system view に移行する	**system-view**	—
4． 保存されているサーバ公開鍵を削除する	**delete ssh client server-public-key** [**server-ip** *ip-address*]	—

5.4.6 Suite B の SFTP サーバとの接続の確立

ユーザ view で次のコマンドを実行して、Suite B に基づいた SFTP サーバへの接続を確立します。

操作	コマンド	補足
Suite B のSFTPサーバに接続する	• IPv4： **sftp** *server* [*port-number*] **suite-b** [**128-bit** | **192-bit**] **pki-domain** *domain-name* [**server-pki-domain** *domain-name*] [**prefer-compress zlib**] [**dscp** *dscp-value* | **source** { **interface** *interface-type interface-number* | **ip** *ip-address* }] *	user viewで実行できます。

5.4.7 SFTP ディレクトリの操作

操作	コマンド	補足
SFTPサーバの作業ディレクトリを変更する	**cd** [*remote-path*]	SFTP client viewで有効です。
上位のディレクトリに戻る	**cdup**	SFTP client viewで有効です。
SFTPサーバの現在の作業ディレクトリを表示する	**pwd**	SFTP client viewで有効です。
指定したディレクトリにあるファイルを表示する	• **dir** [**-a** | **-l**] [*remote-path*] • **ls** [**-a** | **-l**] [*remote-path*]	SFTP client viewで有効です。 **dir**コマンドは**ls**コマンドと同一です。
SFTPサーバの指定したディレクトリ名を変更する	**rename** *oldname newname*	SFTP client viewで有効です。
SFTPサーバで新しいディレクトリを作成する	**mkdir** *remote-path*	SFTP client viewで有効です。
SFTPサーバから1つ以上のディレクトリを削除する	**rmdir** *remote-path*	SFTP client viewで有効です。

5.4.8 SFTP ファイルの操作

操作	コマンド	補足
SFTPサーバの指定したディレクトリ名を変更する	**rename** *old-name new-name*	SFTP client viewで有効です。
SFTPサーバからファイルをダウンロードし、ローカルに保存する	**get** *remote-file* [*local-file*]	SFTP client viewで有効です。
SFTPサーバにローカルファイルをアップロードする	**put** *local-file* [*remote-file*]	SFTP client viewで有効です。
指定したディレクトリにあるファイルを表示する	• **dir** [**-a** | **-l**] [*remote-path*] • **ls** [**-a** | **-l**] [*remote-path*]	SFTP client viewで有効です。 **dir**コマンドは**ls**コマンドと同一です。
SFTPサーバから1つ以上のディレクトリを削除する	• **delete** *remote-file* • **remove** *remote-file*	SFTP client viewで有効です。 **delete**コマンドは**remove**コマンドと同一です。

5.4.9 ヘルプ情報の表示

コマンドのフォーマットやパラメータのような SFTP クライアントコマンドのヘルプ情報を表示することができます。

以下にヘルプ情報の表示を示します。

操作	コマンド	補足
SFTPクライアントコマンドのヘルプ情報を表示する	• **help** • **?**	どちらか一方のコマンドを使用します。 SFTP client viewで有効です。 2つのコマンドは同一機能です。

5.4.10 SFTP サーバの接続の切断

操作	コマンド	補足
SFTPサーバの接続を切断し、user viewに戻る	• **bye** • **exit** • **quit**	いずれか1つのコマンドを使用します。 SFTP client viewで有効です。 3つのコマンドは同一機能です。

5.5 SCPクライアントの設定

5.5.1 SCP クライアントの設定作業リスト

作業リスト	補足
（必須設定項目）ローカル鍵ペアの作成	Stelnetサーバが**publickey**、**password-publickey**,**any**の認証方式を使用する際は必須です。
（オプション設定項目）SCPパケットの送信元IPアドレスの指定	―
（必須設定項目）SCPサーバとの接続の確立	―
（オプション設定項目）SCPクライアント上のサーバ公開鍵の削除	―
（オプション設定項目）Suite BのSCPサーバとの接続の確立	―

5.5.2 ローカル鍵ペアの作成

SCP サーバが **publickey**、**password-publickey**、あるいは **any** の認証方式を使用する際は、SCP クライアントでローカル鍵ペアを作成してください。

I. 設定ガイドライン

SFTP クライアントでローカル鍵ペアを設定する際には、以下のガイドラインに従ってください。

- SSH のローカル DSA、ECDSA 及び RSA 鍵ペアはデフォルト名を使用します。鍵ペアに名前を割り当てることはできません。
- DSA 鍵ペアを作成するとき、鍵の長さは 2048 ビットよりも短くしてください。
- ECDSA キーペアを生成する場合、secp256 r 1 または secp384 r 1 ECDSA キーペアのみを生成できます。

II. 設定手順

以下に SFTP クライアントでローカル鍵ペアを生成する設定を示します。

操作	コマンド	補足
5． system view に移行する	**system-view**	ー
6． ローカル鍵ペアを作成する	**public-key local create** { **dsa** | **ecdsa** { **secp256r1** | **secp384r1** } | **rsa** }	デフォルト : 鍵ペアは存在しません。

5.5.3 SCP パケットの送信元 IP アドレスの指定

以下のため、SCP パケットの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の IP アドレスを指定することを推奨します。

- SCP クライアントと SCP サーバが互いに通信できることを保証します。
- 認証サービスの SCP クライアントの管理を向上します。

以下に SFTP パケットの送信元 IP アドレスの設定を示します。

操作	コマンド	補足
7． system view に移行する	**system-view**	ー
8． SCP パケットの送信元 IP アドレスを指定する	• IPv4 : **scp client source** { **interface** *interface-type interface-number* | **ip** *ip-address* }	デフォルト : 設定なし IPv4 SCP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IPv4アドレスを使用します。

5.5.4 SCP サーバとの接続の確立

SCP サーバにアクセスするとき、装置はサーバを認証するためサーバのホスト公開鍵を使用します。装置でサーバのホスト公開鍵が設定されていない場合、装置はアクセスを継続するかどうかを確認するメッセージを表示します。

- アクセスを継続する場合、装置はサーバにアクセスし、サーバのホスト公開鍵をダウンロードします。
- アクセスを継続しない場合、接続は確立することができません。

安全でないネットワークでは装置でサーバのホスト公開鍵を設定することを推奨します。

接続が完了したのち、ディレクトリあるいはファイルのような操作を行うため、サーバの SCP client view に直接移行することができます。

操作	コマンド	補足
SCPサーバの接続を確立する	• IPv4： **scp** *server* [*port-number*] { **put** | **get** } *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* }] * [**user** *username* [**password** *password*]]	user viewで実行できます。

5.5.5 SCP クライアント上のサーバ公開鍵の削除

ローカルに保存されたサーバ公開キーがデバイス要件を満たしていない場合、クライアントはサーバに接続できません。サーバに接続するには、クライアントに保存されているサーバ公開キーを削除し、サーバに正しい公開キーが生成されていることを確認します。

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． 保存されているサーバ公開鍵を削除する	**delete ssh client server-public-key** [**server-ip** *ip-address*]	—

5.5.6 Suite B の SCP サーバとの接続の確立

ユーザ view で次のコマンドを実行して、Suite B に基づいた SCP サーバへの接続を確立します。

操作	コマンド	補足
Suite B のSCPサーバに接続する	• IPv4： **scp** *server* [*port-number*] { **put** | **get** } *source-file-name* [*destination-file-name*] **suite-b** [**128-bit** | **192-bit**] **pki-domain** *domain-name* [**server-pki-domain** *domain-name*] [**prefer-compress zlib**] [**source** { **interface** *interface-type interface-number* | **ip** *ip-address* }] * [**user** *username* [**password** *password* [**no-more-input**]]]	user viewで実行できます。

5.6 SSH2のアルゴリズム設定

5.6.1 SSH2 のアルゴリズムについて

SSH 2 クライアントおよびサーバは、Stelnet、SFTP、SCP セッションの確立中に、次のタイプのアルゴリズムをネゴシエーションに使用します。

- 鍵交換アルゴリズム
- 公開鍵アルゴリズム
- 暗号化アルゴリズム
- MAC アルゴリズム

アルゴリズムを指定すると、SSH2 は指定されたアルゴリズムのみをネゴシエーションに使用します。クライアントは指定されたアルゴリズムを使用してネゴシエーションを開始し、サーバは一致するアルゴリズムを使用してクライアントとネゴシエートします。同じ種類のアルゴリズムを複数指定した場合は、先に指定したアルゴリズムを優先度します。

5.6.2 鍵交換アルゴリズムの指定

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． 鍵交換アルゴリズムを指定する	**ssh2 algorithm key-exchange** { **dh-group-exchange-sha1** | **dh-group1-sha1** | **dh-group14-sha1** | **ecdh-sha2-nistp256** | **ecdh-sha2-nistp384** } *	デフォルト：優先順位の高い順に、ecdh-sha 2-nistp 256、ecdh-sha 2-nistp 384、dh-group-exchange-sha 1、dh-group 14-sha 1、dh-group 1-sha 1の各キー交換アルゴリズムを使用します。

5.6.3 公開鍵アルゴリズムの指定

操作	コマンド	補足
1． system view に移行する	**system-view**	ー

操作	コマンド	補足
2. 鍵交換アルゴリズムを指定する	**ssh2 algorithm public-key** { **dsa** | **ecdsa-sha2-nistp256** | **ecdsa-sha2-nistp384** | **rsa** } *	デフォルト : 優先度が高い順に、ecdsa-sha 2-nistp 256、ecdsa-sha 2-nistp 384、rsa、およびdsa公開鍵アルゴリズムを使用します。

5.6.4 暗号化アルゴリズムの指定

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. 暗号化アルゴリズムを指定する	**ssh2 algorithm cipher** { **3des-cbc** | **aes128-cbc** | **aes128-ctr** | **aes128-gcm** | **aes192-ctr** | **aes256-cbc** | **aes256-ctr** | **aes256-gcm** | **des-cbc** } *	デフォルト : 優先順位の高い順にaes 128-ctr、aes 192-ctr、aes 256-ctr、aes 128-gcm、aes 256-gcm、aes 128-cbc、3 des-cbc、aes 256-cbc、およびdes-cbc暗号化アルゴリズムを使用します。

5.6.5 MAC アルゴリズムの指定

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. MAC アルゴリズムを指定する	**ssh2 algorithm mac** { **md5** | **md5-96** | **sha1** | **sha1-96** | **sha2-256** | **sha2-512** } *	デフォルト : 優先度の高い順にsha 2-256、sha 2-512、sha 1、md 5、sha 1-96、md 5-96のMACアルゴリズムを使用します。

5.7 SSHの表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
SFTPクライアントの送信元IPアドレスを表示する	**display sftp client source**
Stelnetクライアントの送信元IPアドレスを表示する	**display ssh client source**
SSHサーバのステータス情報あるいはセッション情報を表示する	**display ssh server** { **session** | **status** }
SSHサーバのSSHユーザ情報を表示する	**display ssh user-information** [*username*]
ローカル鍵ペアの公開鍵を表示する	**display public-key local** { **dsa** | **rsa** } **public** [**name** *publickey-name*]

操作	コマンド
SSHピアの公開鍵を表示する	**display public-key peer** [**brief** | **name** *publickey-name*]

5.7.1 公開鍵情報の表示

すべての view で **display** コマンドを実行できます。

操作	コマンド
ローカル鍵ペアの公開鍵を表示する	**display public-key local** { **dsa** | **ecdsa** | **rsa** } **public** [**name** *publickey-name*]
SSHピアの公開鍵を表示する	**display public-key peer** [**brief** | **name** *publickey-name*]
SSHクライアントのサーバ公開キーの情報を表示する	**display ssh client server-public-key** [**server-ip** *ip-address*]

5.7.2 SSH サーバの実行ステータスの確認

すべての view で **display** コマンドを実行できます。

操作	コマンド
SSHサーバのステータス情報あるいはセッション情報を表示する	**display ssh server** { **session** | **status** }
SSHサーバのSSHユーザ情報を表示する	**display ssh user-information** [*username*]

5.7.3 SSH クライアント設定の確認

すべての view で **display** コマンドを実行できます。

操作	コマンド
SFTPクライアントの送信元IPアドレスを表示する	**display sftp client source**
Stelnetクライアントの送信元IPアドレスを表示する	**display ssh client source**
SCPクライアントの送信元IPアドレスを表示する	**display scp client source**

5.7.4 SSH2 アルゴリズムの表示

すべての view で **display** コマンドを実行できます。

操作	コマンド
SSH 2アルゴリズムを表示する	**display ssh2 algorithm**

5.8 Stelnet設定例

5.8.1 パスワード認証を有効にした Stelnet サーバ設定例

I. ネットワーク要件

図 5-1に示すように設定します。

- 無線クライアントと AC 間のルートは到達可能です。
- AC は Stelnet サーバとして動作し、パスワード認証を使用します。
- Stelnet クライアントのユーザ名とパスワードは AC に保存されます。

クライアントと AC 間の接続を確立しログインすることで設定を管理することができます。

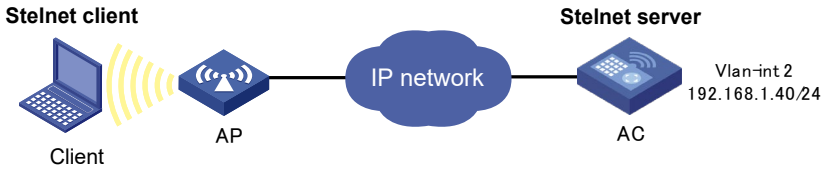


図 5-1 ネットワーク図

II. 設定手順

1)　Stelnet サーバを設定します。

RSA 鍵ペアを作成します。

```
<AC> system-view
[AC] public-key local create rsa
The range of public key size 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.
```

DSA 鍵ペアを作成します。

```
[AC] public-key local create dsa
The range of public key size 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.
```

SSH サーバ機能を有効にします。

```
[AC] ssh server enable
```

VLAN インタフェース 2 に IP アドレスを割り当てます。SSH 接続の宛先アドレスとして Stelnet クライアントは VLAN インタフェース 2 の IP アドレスを使用します。

```
[AC] interface vlan-interface 2
[AC-Vlan-interface2] ip address 192.168.1.40 255.255.255.0
[AC-Vlan-interface2] quit
```

ユーザラインの認証モードを AAA に設定します。

```
[AC] line vty 0 15
[AC-line-vty0-15] authentication-mode scheme
[AC-line-vty0-15] quit
```

ローカル装置管理ユーザ **client001** を作成します。

```
[AC] local-user client001 class manage
```

ユーザのプレーンテキストのパスワードを **aabbcc**、サービスタイプを **ssh** に設定します。

```
[AC-luser-manage-client001] password simple aabbcc
[AC-luser-manage-client001] service-type ssh
```

ユーザにユーザロールを **network-admin** に割り当てます。

```
[AC-luser-manage-client001] authorization-attribute user-role network-admin
[AC-luser-manage-client001] quit
```

SSH ユーザ **client001** を作成します。ユーザのサービスタイプを **stelnet**、認証方式を **password** に設定します。SSH ユーザが作成されていない場合、デフォルトでパスワード認証が使用されます。

```
[AC] ssh user client001 service-type stelnet authentication-type password
```

2)　Stelnet サーバとの接続を確立します。

Stelnet クライアントのソフトウェアは、PuTTY、OpenSSH など異なるタイプがあります。この例では PuTTY バージョン 0.58 を Stelnet クライアントとして使用します。

Stelnet サーバとの接続を確立します。

a)　図 5-2に示すようにPuTTY.exeを起動させ、インタフェースを入力します。

b)　**Host Name**フィールド（あるいは**IP address**）で、StelnetサーバのIPアドレス192.168.1.40を入力します。

c)　**Open**をクリックします。

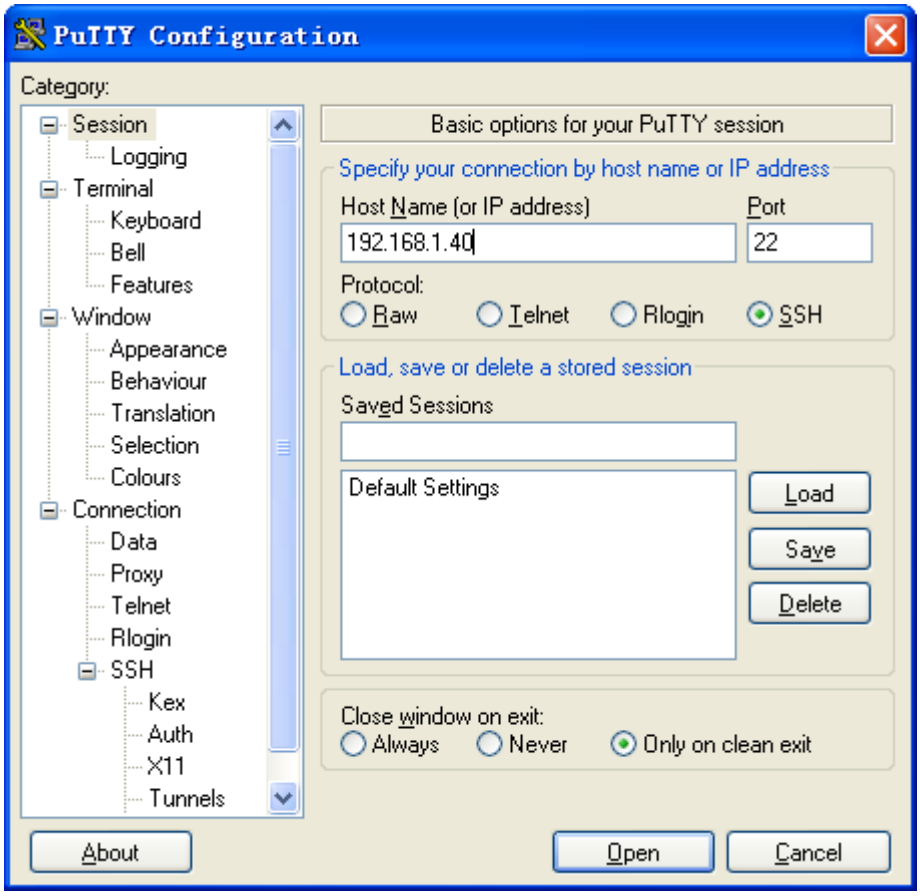


図 5-2 ホスト名（あるいは IP アドレス）の指定

接続が正常に確立されると、ユーザ名とパスワードを入力するようにシステムから通知されます。ユーザ名（この例では **client001**）とパスワード（この例では **aabbcc**）を入力してサーバにログインします。

5.8.2 公開鍵認証を有効にした Stelnet サーバの設定例

I. ネットワーク要件

図 5-3に示すように設定します。

- ワイヤレスクライアントと AC 間のルートは到達可能です。
- AC は Stelnet サーバとして動作し、パスワード認証と RSA 公開鍵アルゴリズムを使用します。

クライアントと AC 間の接続を確立しログインすることで設定を管理することができます。

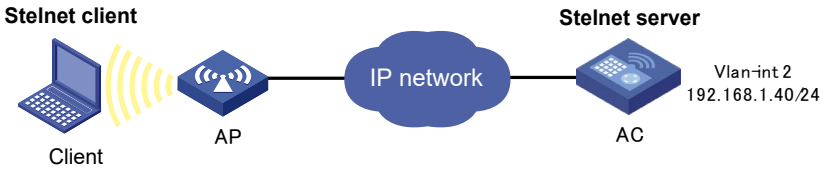


図 5-3 ネットワーク図

II. 設定手順

サーバの設定では、クライアントのホスト公開鍵が必要となります。Stelnet サーバを設定する前に、クライアントで RSA 鍵ペアを作成するため、クライアントソフトウェアを使用します。

Stelnet クライアントのソフトウェアは、PuTTY、OpenSSH など異なるタイプがあります。この例では PuTTY バージョン 0.58 を Stelnet クライアントとして使用します。

設定手順を以下に示します。

1) Stelnet クライアントで RSA 鍵ペアを作成します。

a) クライアントでPuTTY.exeを起動させ、SSH-2 RSAを選択し、Generateをクリックします。



図 5-4 クライアントの鍵ペアの作成

b) 鍵ペアを作成しているとき、マウスを継続して動かしてください。図 5-5に示すように、緑の進捗バーの上にマウスを置かないでください。そうしなければ、進捗バーが動作をストップしてしまい、鍵ペアの作成をとめてしまいます。

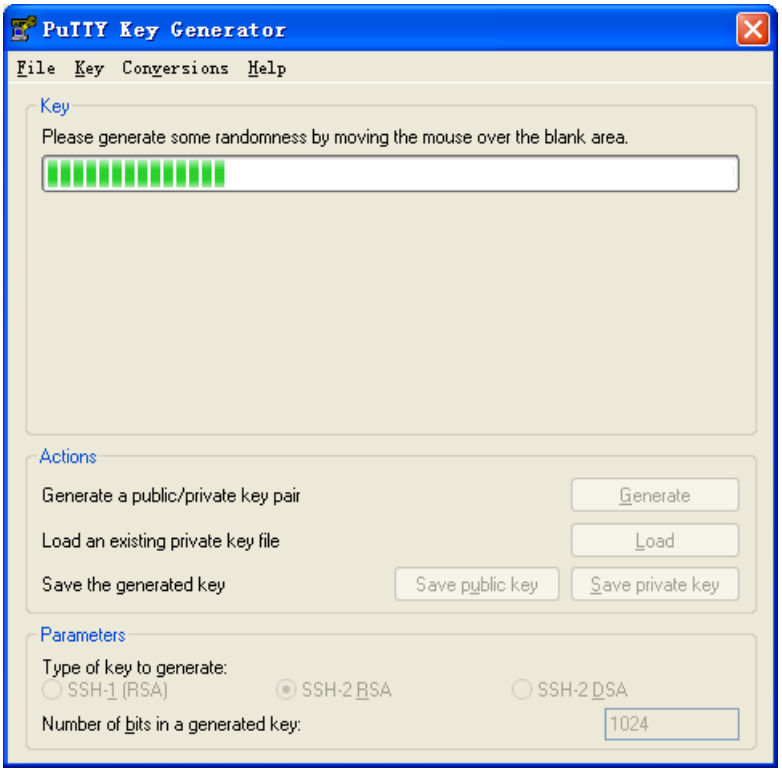


図 5-5 プロセスの作成

c)　鍵ペアが作成された後、**Save public key**をクリックし、ファイル名**key.pub**を入力し、**Save**をクリックします。ファイルの保存ウィンドウ画面が表示されます。

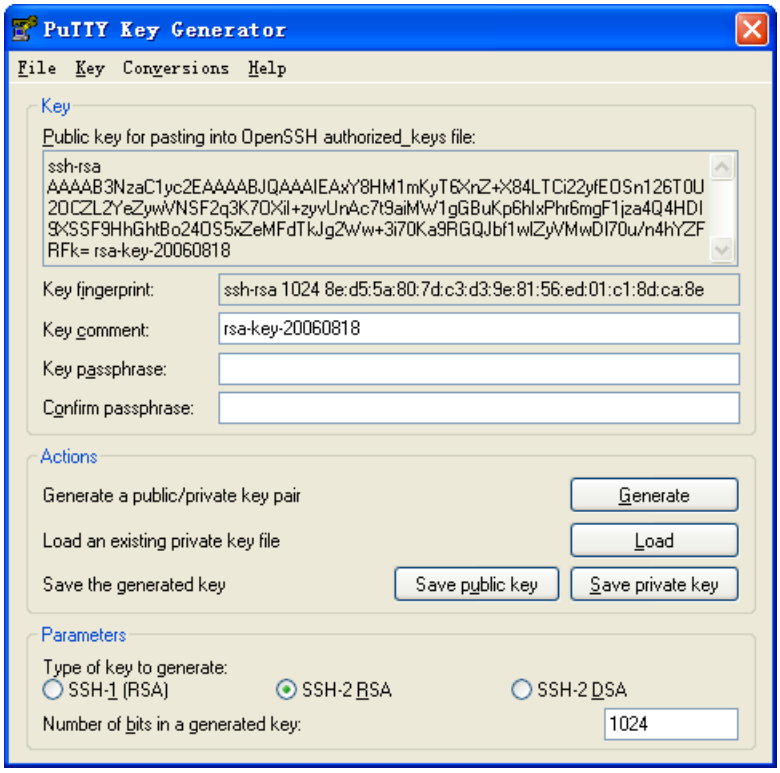


図 5-6 クライアントの鍵ペアの保存

d)　ファイル名（この例では**key.pub**）を入力し、**Save**をクリックします。

e)　図 5-6に示すページで、秘密鍵を保存するため、**Save private key**をクリックします。確認ダイアログボックスが表示されます。

f)　**Yes**をクリックします。ファイルの保存ウィンドウが表示されます。

g)　ファイル名（この例では**private.ppk**）を入力し、**Save**をクリックします。

h)　FTPあるいはTFTPを使用してサーバに公開鍵ファイルを転送します。（詳細は省略します）

2)　Stelnet サーバを設定します。

RSA 鍵ペアを作成します。

<AC> system-view

[AC] public-key local create rsa

```
The range of public key size 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.
```

DSA 鍵ペアを作成します。

```
[AC] public-key local create dsa
The range of public key size 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.
```

SSH サーバ機能を有効にします。

```
[AC] ssh server enable
```

VLAN インタフェース 2 に IP アドレスを割り当てます。SSH 接続の宛先アドレスとして Stelnet クライアントは VLAN インタフェース 2 の IP アドレスを使用します。

```
[AC] interface vlan-interface 2
[AC-Vlan-interface2] ip address 192.168.1.40 255.255.255.0
[AC-Vlan-interface2] quit
```

ユーザラインの認証モードを AAA に設定します。

```
[AC] line vty 0 15
[AC-line-vty0-15] authentication-mode scheme
[AC-line-vty0-15] quit
```

ファイル **key.pub** からクライアントの公開鍵をインポートし、名前を **ackey** とします。

```
[AC] public-key peer ackey import sshkey key.pub
```

SSH ユーザ **client002** を作成します。ユーザの認証方式を公開鍵に指定します。公開鍵 **ackey** をユーザに割り当てます。

```
[AC] ssh user client002 service-type stelnet authentication-type publickey assign publickey ackey
```

ローカル装置管理ユーザ **client002** を作成します。ユーザのサービスタイプを **ssh**、ユーザロールを **network-admin** に設定します。

```
[AC] local-user client002 class manage
[AC-luser-manage-client002] service-type ssh
[AC-luser-manage-client002] authorization-attribute user-role network-admin
[AC-luser-manage-client002] quit
```

3) 秘密鍵ファイルを指定し、Stelnet サーバとの接続を確立します。

a) 図 5-7に示すようにStelnetクライアントでPuTTY.exeを起動させ、インタフェースに移行します。

b) **Host Name**フィールド（あるいは**IP address**）で、StelnetサーバのIPアドレス192.168.1.40を入力します。

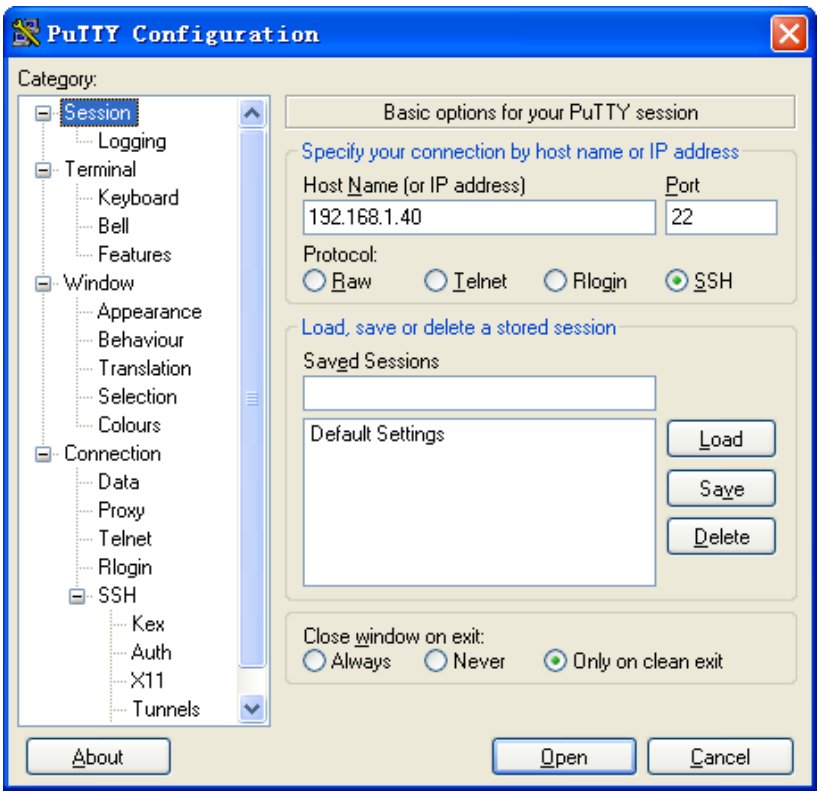


図 5-7 ホスト名（あるいは IP アドレス）の指定

c)　ナビゲーションツリーから**Connection**を選択し、**SSH**を選択します。図 5-8に示すようにウィンドウ画面が表示されます。

d)　**Protocol options**の**Preferred SSH protocol version**で**2**を選択します。

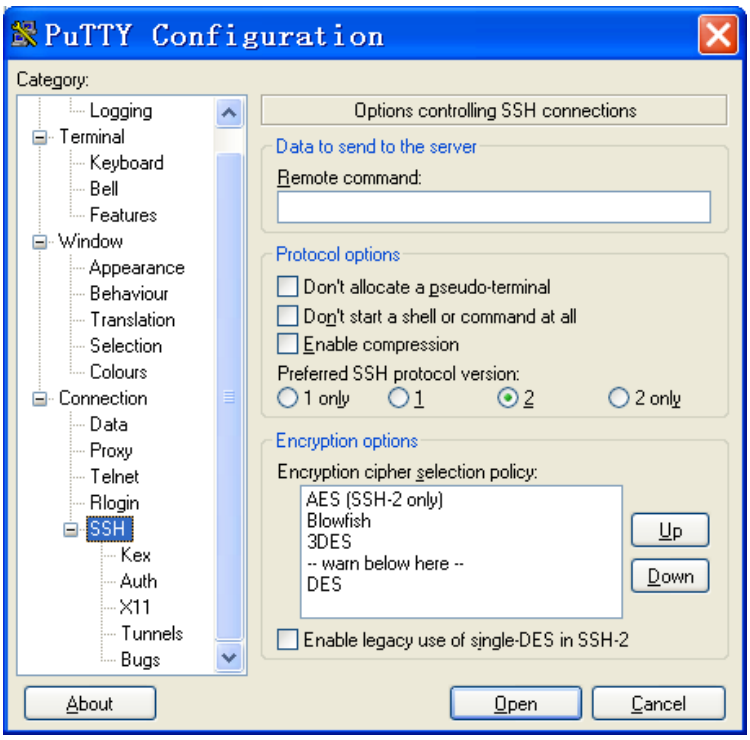


図 5-8 SSH バージョンの指定

e)　ナビゲーションツリーから**Connection**を選択し、**SSH**を選択し、**Auth**を選択します。図 5-9に示すようにウィンドウ画面が表示されます。

f)　ファイル選択画面から**Browse**をクリックし、秘密鍵ファイル（この例では**private.ppk**）を選択し、**OK**をクリックします。

g)　**Open**をクリックします。

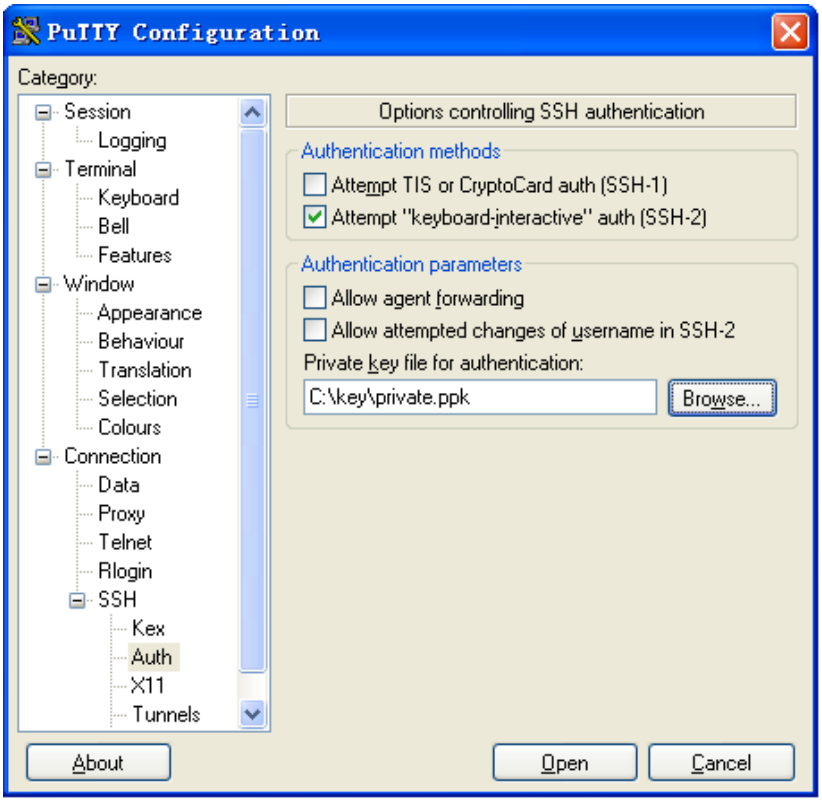


図 5-9 秘密鍵ファイルの指定

接続が正常に確立されると、ユーザ名を入力するようにシステムから通知されます。ユーザ名（**client002**）を入力し、Stelnet サーバにログインします。

5.8.3 パスワード認証を有効にした Stelnet クライアント設定例

I. ネットワーク要件

図 5-10に示すように設定します。

- スイッチは Stelnet サーバとして動作し、Stelnet クライアントを認証するためにパスワード認証を使用します。クライアントのユーザ名とパスワードはスイッチ B に保存されます。

AC とスイッチ間の接続を確立しスイッチにログインすることで設定を管理できます。

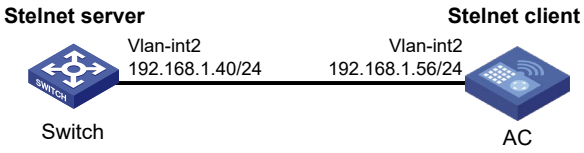


図 5-10 ネットワーク図

II. 設定手順

1)　Stelnet サーバを設定します。

RSA 鍵ペアを作成します。

```
<Switch> system-view
[Switch] public-key local create rsa
The range of public key size 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.
```

DSA 鍵ペアを作成します。

```
[Switch] public-key local create dsa
The range of public key size 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.
```

SSH サーバ機能を有効にします。

```
[Switch] ssh server enable
```

VLAN インタフェース 2 に IP アドレスを割り当てます。SSH 接続の宛先アドレスとして Stelnet クライアントは VLAN インタフェース 2 の IP アドレスを使用します。

```
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ip address 192.168.1.40 255.255.255.0
[Switch-Vlan-interface2] quit
```

ユーザラインの認証モードを AAA に設定します。

```
[Switch] line vty 0 15
[Switch-line-vty0-15] authentication-mode scheme
[Switch-line-vty0-15] quit
```

ローカル装置管理ユーザ **client001** を作成します。

```
[Switch] local-user client001 class manage
```

ユーザのプレーンテキストのパスワードを **aabbcc**、サービスタイプを **ssh** に指定します。

```
[Switch-luser-manage-client001] password simple aabbcc
[Switch-luser-manage-client001] service-type ssh
```

ユーザのユーザロールを **network-admin** と設定します。

```
[Switch-luser-manage-client001] authorization-attribute user-role network-admin
[Switch-luser-manage-client001] quit
```

SSH ユーザ **client001** を作成します。ユーザのサービスタイプを **stelnet**、認証方式を **password** に設定します。SSH ユーザが作成されていない場合、デフォルトでパスワード認証が使用されます。

```
[Switch] ssh user client001 service-type stelnet authentication-type password
```

2)　Stelnet サーバ 192.168.1.40 との接続を確立します。

VLAN インタフェース 2 に IP アドレスを割り当てます。

```
<AC> system-view
[AC] interface vlan-interface 2
[AC-Vlan-interface2] ip address 192.168.1.56 255.255.255.0
[AC-Vlan-interface2] quit
[AC] quit
```

サーバとの接続を確立する前に、クライアントでサーバのホスト公開鍵を設定するかどうかを決定することができます。

- クライアントでサーバのホスト公開鍵を設定する場合、以下の作業を行います。

サーバのホスト公開鍵を表示するため、サーバで **display public-key local dsa public** コマンドを使用します。（詳細は省略します。）

クライアントの public key view に移行し、サーバのホスト公開鍵をクライアントにコピーします。

```
[AC] public-key peer key1
```

public key view に移行します。**peer-public-key end** コマンドで system view に戻ります。

```
[AC-pkey-public-key-key1]308201B73082012C06072A8648CE3804013082011F0281810
0D757262C4584C44C211F18BD96E5F0
[AC-pkey-public-key-key1]61C4F0A423F7FE6B6B85B34CEF72CE14A0D3A5222FE08C
ECE65BE6C265854889DC1EDBD13EC8B274
[AC-pkey-public-key-key1]DA9F75BA26CCB987723602787E922BA84421F22C3C89CB
9B06FD60FE01941DDD77FE6B12893DA76E
[AC-pkey-public-key-key1]EBC1D128D97F0678D7722B5341C8506F358214B16A2FAC4
B368950387811C7DA33021500C773218C
```

```
[AC-pkey-public-key-key1]737EC8EE993B4F2DED30F48EDACE915F02818100822690
09E14EC474BAF2932E69D3B1F18517AD95
[AC-pkey-public-key-key1]94184CCDFCEAE96EC4D5EF93133E84B47093C52B20CD3
5D02492B3959EC6499625BC4FA5082E22C5
[AC-pkey-public-key-key1]B374E16DD00132CE71B020217091AC717B612391C76C1FB
2E88317C1BD8171D41ECB83E210C03CC9
[AC-pkey-public-key-key1]B32E810561C21621C73D6DAAC028F4B1585DA7F42519718
CC9B09EEF0381840002818000AF995917
[AC-pkey-public-key-key1]E1E570A3F6B1C2411948B3B4FFA256699B3BF871221CC9C
5DF257523777D033BEE77FC378145F2AD
[AC-pkey-public-key-key1]D716D7DB9FCABB4ADBF6FB4FDB0CA25C761B308EF5300
9F7101F7C62621216D5A572C379A32AC290
[AC-pkey-public-key-key1]E55B394A217DA38B65B77F0185C8DB8095522D1EF044B46
5E8716261214A5A3B493E866991113B2D
[AC-pkey-public-key-key1]485348
[AC-pkey-public-key-key1] peer-public-key end
[AC] quit
```

サーバへの SSH 接続を確立し、サーバのホスト公開鍵を指定します。

```
<AC> ssh2 192.168.1.40 public-key key1
Username: client001
Press CTRL+C to abort.
Connecting to 192.168.1.40 port 22.
client001@192.168.1.40's password:
Enter a character ~ and a dot to abort.

*******************************************************************************
*                                                                             *
*                              BOOTROM, Version 101                           *
*                                                                             *
*******************************************************************************


<Switch>
```

正しいパスワードを入力した後、スイッチにログインすることができます。

- クライアントにサーバのホスト公開鍵がない場合、システムはサーバにアクセスするとき、アクセスを継続するかどうか確認する画面を表示します。サーバにアクセスするため、**Yes** を選択し、サーバのホスト公開鍵をダウンロードします。

```
<AC> ssh2 192.168.1.40
Username: client001
Press CTRL+C to abort.
Connecting to 192.168.1.40 port 22.
The server is not authenticated. Continue? [Y/N]:y
Do you want to save the server public key? [Y/N]:y
client001@192.168.1.40's password:
Enter a character ~ and a dot to abort.
```

```
********************************************************************************
*                                                                              *
*                           BOOTROM, Version 101                               *
*                                                                              *
********************************************************************************


<Switch>
```

正しいパスワードを入力した後、スイッチにログインすることができます。サーバのホスト公開鍵はクライアントに保存されます。次回接続を行うとき、システムはサーバに認証するかどうか確認する画面を表示しません。

5.8.4 公開鍵認証を有効にした Stelnet クライアント設定例

I. ネットワーク要件

図 5-11に示すように設定します。

- スイッチは Stelnet サーバとして動作し、公開鍵認証と DSA 公開鍵アルゴリズムを使用します。

AC とスイッチ間に Stelnet 接続が確立しスイッチにログインすることで設定を管理できます。

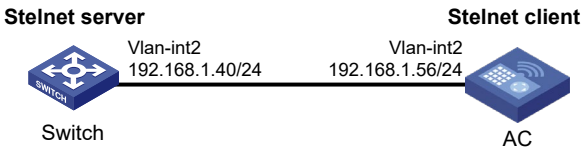


図 5-11 ネットワーク図

II. 設定手順

サーバの設定ではクライアント公開鍵が必要となります。Stelnet サーバを設定する前に、クライアントで DSA 鍵ペアを作成するためにクライアントソフトウェアを使用します。

1)　Stelnet クライアントを設定します。

VLAN インタフェース 2 に IP アドレスを割り当てます。

```
<AC> system-view
[AC] interface vlan-interface 2
[AC-Vlan-interface2] ip address 192.168.1.56 255.255.255.0
[AC-Vlan-interface2] quit
```

DSA 鍵ペアを作成します。

```
[AC] public-key local create dsa
The range of public key size 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.
```

DSA ホスト公開鍵をファイル **key.pub** にエクスポートします。

```
[AC] public-key local export dsa ssh2 key.pub
[AC] quit
```

FTP あるいは TFTP を使用して、サーバに公開鍵ファイル **key.pub** を転送します。（詳細は省略します）

2) Stelnet サーバを設定します。

RSA 鍵ペアを作成します。

```
<Switch> system-view
[Switch] public-key local create rsa
The range of public key size 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.
```

DSA 鍵ペアを作成します。

```
[Switch] public-key local create dsa
The range of public key size 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.
```

SSH サーバ機能を有効にします。

```
[Switch] ssh server enable
```

VLAN インタフェース 2 に IP アドレスを割り当てます。SSH 接続の宛先アドレスとして Stelnet クライアントは VLAN インタフェース 2 の IP アドレスを使用します。

```
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ip address 192.168.1.40 255.255.255.0
[Switch-Vlan-interface2] quit
```

ユーザラインの認証モードを AAA に設定します。

```
[Switch] line vty 0 15
[Switch-line-vty0-15] authentication-mode scheme
```

```
[Switch-line-vty0-15] quit
```

ファイル **key.pub** からピアの公開鍵をインポートし、名前を **ackey** とします。

```
[Switch] public-key peer ackey import sshkey key.pub
```

ローカル装置管理ユーザ **client002** を作成します。ユーザの認証方式を公開鍵に指定します。ユーザに公開鍵 **ackey** を割り当てます。

```
[Switch] ssh user client002 service-type stelnet authentication-type publickey assign publickey ackey
```

ローカル装置管理ユーザ **client002** を作成します。ユーザのサービスタイプを SSH に指定します。ユーザにユーザロール **network-admin** を割り当てます。

```
[Switch] local-user client002 class manage
[Switch-luser-manage-client002] service-type ssh
[Switch-luser-manage-client002] authorization-attribute user-role network-admin
[Switch-luser-manage-client002] quit
```

3) Stelnet サーバ 192.168.1.40 に SSH 接続を確立します。

```
<AC> ssh2 192.168.1.40
Username: client002
Press CTRL+C to abort.
Connecting to 192.168.1.40 port 22.
The server is not authenticated. Continue? [Y/N]:y
Do you want to save the server public key? [Y/N]:n
Enter a character ~ and a dot to abort.

******************************************************************************
*                                                                            *
*                          BOOTROM, Version 101                              *
*                                                                            *
******************************************************************************


<Switch>
```

サーバにアクセスするため **Yes** を選択し、サーバのホスト公開鍵をダウンロードします。次回接続を行うとき、クライアントはクライアントで保存されたサーバのホスト公開鍵を使用してサーバを認証します。

5.9 SFTP設定例

5.9.1 パスワード認証を有効にした SFTP サーバの設定例

I. ネットワーク要件

図 5-12に示すように設定します。

- SFTP サーバとして AC 2 が動作し、SFTP クライアントを認証するためにパスワード認証を使用します。クライアントのユーザ名とパスワードは AC 2 に保存されます。

AC 1 と AC 2 間に SFTP 接続を確立し AC 2 にログインすることでファイルの管理および転送をすることができます。

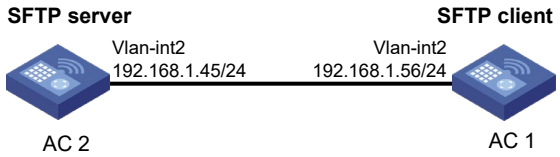


図 5-12 ネットワーク図

II. 設定手順

1)　SFTP サーバを設定します。

RSA 鍵ペアを作成します。

```
<AC2> system-view
[AC2] public-key local create rsa
The range of public key size 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.
```

DSA 鍵ペアを作成します。

```
[AC2] public-key local create dsa
The range of public key size 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.
```

SFTP サーバ機能を有効にします。

```
[AC2] sftp server enable
```

VLAN インタフェース 2 に IP アドレスを割り当てます。SFTP クライアントは SSH 接続用の宛先アドレスとして VLAN インタフェース 2 の IP アドレスを使用します。

```
[AC2] interface vlan-interface 2
[AC2-Vlan-interface2] ip address 192.168.1.45 255.255.255.0
[AC2-Vlan-interface2] quit
```

ローカル装置管理ユーザ **client002** を作成します。プレーンテキストのパスワードを **aabbcc** とし、サービスタイプを **ssh** とします。ユーザにユーザロール **network-admin** を割り当て、作業ディレクトリを **flash:/**に設定します。

```
[AC2] local-user client002 class manage
[AC2-luser-manage-client002] password simple aabbcc
```

```
[AC2-luser-manage-client002] service-type ssh
[AC2-luser-manage-client002] authorization-attribute user-role network-admin work-directory flash:/
[AC2-luser-manage-client002] quit
```

ローカル装置管理ユーザ **client002** を作成します。ユーザの認証モードを **password**、サービスタイプを **sftp** に設定します。SSH ユーザが作成されていない場合、デフォルトでパスワード認証が使用されます。

```
[AC2] ssh user client002 service-type sftp authentication-type password
```

2)　SFTP クライアントとサーバ間の接続を確立します。

装置は SFTP クライアントソフトウェアの異なるタイプをサポートします。この例では PuTTY バージョン 0.58 の PSFTP を動作させる SFTP クライアントを使用します。

メモ：

PSFTP はパスワード認証のみサポートしています。

SFTP サーバへの接続を確立するために、以下を行います。

a)　図 5-13に示すようにクライアントインタフェースを起動させるため、**psftp.exe**を動作させ、以下のコマンドを入力します。

```
open 192.168.1.45
```

b)　SFTPサーバにログインするため、ユーザ名**client002**、パスワード**aabbcc**を入力します。

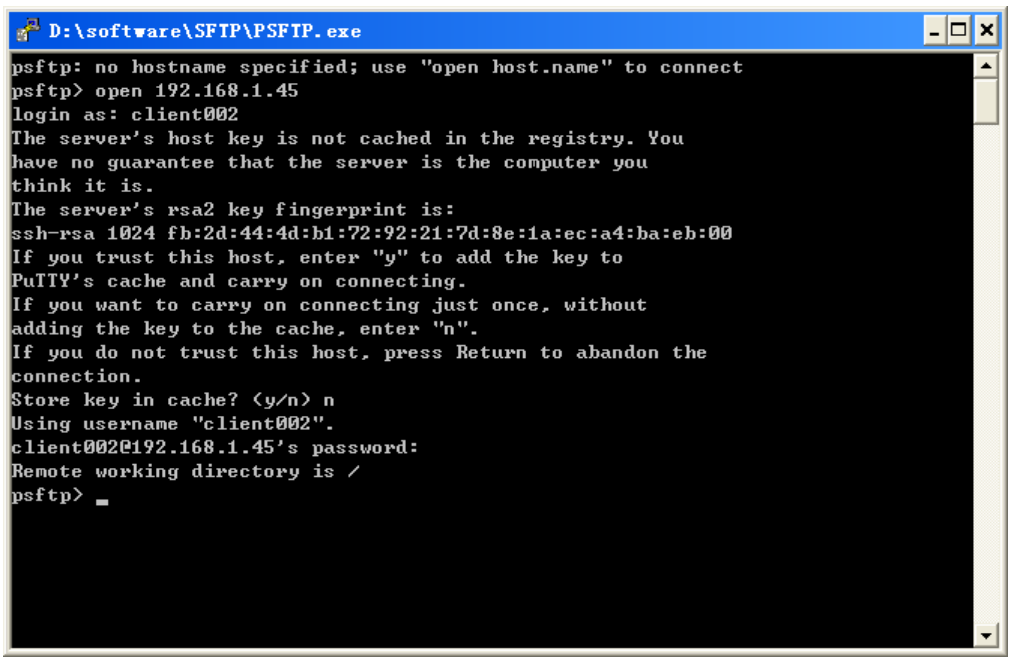


図 5-13 SFTP クライアントインタフェース

5.9.2 公開鍵認証を有効にした SFTP クライアント設定例

I. ネットワーク要件

図 5-14に示すように設定します。

- SFTP サーバとして AC 2 が動作し、公開鍵認証と RSA 公開鍵アルゴリズムを使用します。

AC 1 と AC 2 間に SFTP 接続を確立し AC 2 にログインすることでファイルの管理および転送することができます。

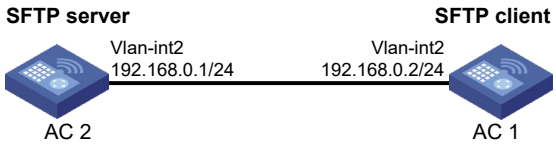


図 5-14 ネットワーク図

II. 設定手順

サーバの設定では、クライアントのホスト公開鍵が必要です。SFTP サーバを設定する前に、クライアントの RSA 鍵ペアを作成するため、クライアントソフトウェアを使用します。

1)　SFTP クライアントを設定します。

VLAN インタフェース 2 に IP アドレスを設定します。

```
<AC1> system-view
[AC1] interface vlan-interface 2
[AC1-Vlan-interface2] ip address 192.168.0.2 255.255.255.0
[AC1-Vlan-interface2] quit
```

RSA 鍵ペアを作成します。

```
[AC1] public-key local create rsa
The range of public key size 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.
```

ホスト公開鍵をファイル **pubkey** にエクスポートします。

```
[AC1] public-key local export rsa ssh2 pubkey
[AC1] quit
```

公開鍵ファイル **pubkey** を FTP あるいは TFTP を使用してサーバに転送します。（詳細は省略します）

2)　SFTP サーバを設定します。

RSA 鍵ペアを作成します。

```
<AC2> system-view
[AC2] public-key local create rsa
The range of public key size 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.
```

DSA 鍵ペアを作成します。

```
[AC2] public-key local create dsa
The range of public key size 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.
```

SFTP サーバ機能を有効にします。

```
[AC2] sftp server enable
```

VLAN インタフェース 2 に IP アドレスを割り当てます。SFTP クライアントは SSH 接続用の宛先アドレスとして VLAN インタフェース 2 の IP アドレスを使用します。

```
[AC2] interface vlan-interface 2
[AC2-Vlan-interface2] ip address 192.168.0.1 255.255.255.0
[AC2-Vlan-interface2] quit
```

ファイルからピアの公開鍵 **pubkey** をインポートし、名前を **ackey** とします。

```
[AC2] public-key peer ackey import sshkey pubkey
```

SSH ユーザ **client001** を作成し、サービスタイプを **sftp** とし、認証方式を **publickey** とし、公開鍵を **ackey** と設定します。

```
[AC2] ssh user client001 service-type sftp authentication-type publickey assign publickey ackey
```

ローカル装置管理ユーザ **client001** を作成します。

```
[AC2] local-user client001 class manage
```

ユーザのサービスタイプを **ssh** に指定します。

```
[AC2-luser-manage-client001] service-type ssh
```

ユーザにユーザロール **network-admin** を割り当て、作業ディレクトリを **flash:/**に設定します。

```
[AC2-luser-manage-client001] authorization-attribute user-role network-admin work-directory flash:/

[AC2-luser-manage-client001] quit
```

3) SFTP クライアントとの接続を確立します。

SFTP サーバと接続を確立し、SFTP client view に移行します。

```
<AC1> sftp 192.168.0.1 identity-key rsa
Username: client001
Press CTRL+C to abort.
Connecting to 192.168.0.1 port 22.
The server is not authenticated. Continue? [Y/N]:y
Do you want to save the server public key? [Y/N]:n
sftp>
```

サーバで現在の作業ディレクトリのファイルを表示し、ファイル名 **z** を削除し、正常に削除されているか確認します。

```
sftp> dir -l
-rwxrwxrwx   1 noone    nogroup      1759 Aug 23 06:52 config.cfg
-rwxrwxrwx   1 noone    nogroup       225 Aug 24 08:01 pubkey2
-rwxrwxrwx   1 noone    nogroup       283 Aug 24 07:39 pubkey
drwxrwxrwx   1 noone    nogroup         0 Sep 01 06:22 new
-rwxrwxrwx   1 noone    nogroup       225 Sep 01 06:55 pub
-rwxrwxrwx   1 noone    nogroup         0 Sep 01 08:00 z
sftp> delete z
Removing /z
sftp> dir -l
-rwxrwxrwx   1 noone    nogroup      1759 Aug 23 06:52 config.cfg
-rwxrwxrwx   1 noone    nogroup       225 Aug 24 08:01 pubkey2
-rwxrwxrwx   1 noone    nogroup       283 Aug 24 07:39 pubkey
drwxrwxrwx   1 noone    nogroup         0 Sep 01 06:22 new
-rwxrwxrwx   1 noone    nogroup       225 Sep 01 06:55 pub
```

ディレクトリ名 **new1** を追加し、正常に作成されているか確認します。

```
sftp> mkdir new1

sftp> dir -l
-rwxrwxrwx   1 noone    nogroup      1759 Aug 23 06:52 config.cfg
-rwxrwxrwx   1 noone    nogroup       225 Aug 24 08:01 pubkey2
-rwxrwxrwx   1 noone    nogroup       283 Aug 24 07:39 pubkey
drwxrwxrwx   1 noone    nogroup         0 Sep 01 06:22 new
-rwxrwxrwx   1 noone    nogroup       225 Sep 01 06:55 pub
drwxrwxrwx   1 noone    nogroup         0 Sep 02 06:30 new1
```

ディレクトリ **new1** を **new2** に名前を変換し､正常に変更されていることを確認します。

```
sftp> rename new1 new2

sftp> dir -l
-rwxrwxrwx   1 noone    nogroup      1759 Aug 23 06:52 config.cfg
-rwxrwxrwx   1 noone    nogroup       225 Aug 24 08:01 pubkey2
-rwxrwxrwx   1 noone    nogroup       283 Aug 24 07:39 pubkey
drwxrwxrwx   1 noone    nogroup         0 Sep 01 06:22 new
-rwxrwxrwx   1 noone    nogroup       225 Sep 01 06:55 pub
drwxrwxrwx   1 noone    nogroup         0 Sep 02 06:33 new2
```

サーバからファイル **pubkey2** をダウンロードし、ローカルファイル **public** として保存します。

```
sftp> get pubkey2 public
Fetching / pubkey2 to public
```

```
/pubkey2                                  100% 225     1.4KB/s   00:00
```

ローカルファイル **pu** をサーバにアップロードし、**puk** として保存し、正常にアップロードされていることを確認します。

```
sftp> put pu puk
Uploading pu to / puk
sftp> dir -l
-rwxrwxrwx   1 noone    nogroup      1759 Aug 23 06:52 config.cfg
-rwxrwxrwx   1 noone    nogroup       225 Aug 24 08:01 pubkey2
-rwxrwxrwx   1 noone    nogroup       283 Aug 24 07:39 pubkey
drwxrwxrwx   1 noone    nogroup         0 Sep 01 06:22 new
drwxrwxrwx   1 noone    nogroup         0 Sep 02 06:33 new2
-rwxrwxrwx   1 noone    nogroup       283 Sep 02 06:35 pub
-rwxrwxrwx   1 noone    nogroup       283 Sep 02 06:36 puk
sftp>
```

SFTP client view から戻ります。

```
sftp> quit
<AC1>
```

5.10 SCP設定例

5.10.1 パスワード認証を有効による SCP の設定例

I. ネットワーク要件

図 5-15に示すように設定します。

- AC2 は SCP サーバとして機能し、パスワード認証を使用して SCP クライアントを認証します。クライアントのユーザ名とパスワードは AC 2 に保存されます。
- AC1 は SCP クライアントとして動作します。AC1 のユーザが SCP を介して AC2 にログインすると、ユーザはネットワーク管理者として AC 間でファイルを転送できます。

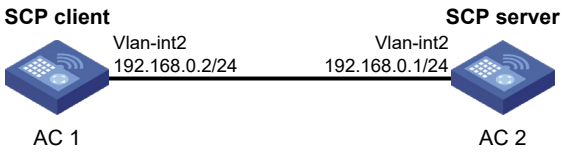


図 5-15 ネットワーク図

II. 設定手順

1)　SCP サーバを設定します。
#RSA キーペアを生成します。

```
<AC2> system-view
[AC2] 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.
```

#DSA キーペアを生成します。

```
[AC2] public-key local create dsa
The range of public key size 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.
```

#ECDSA キーペアを生成します。

```
[AC2] public-key local create ecdsa secp256r1
Generating Keys...
.
Create the key pair successfully.
```

SCP サーバ機能を有効にします。

```
[AC2] scp server enable
```

#VLAN-interface 2 の IP アドレスを設定します。クライアントはこのアドレスを SCP 接続の宛先として使用します。

```
[AC2] interface vlan-interface 2
[AC2-Vlan-interface2] ip address 192.168.0.1 255.255.255.0
[AC2-Vlan-interface2] quit
```

ローカル装置管理ユーザ **client001** を作成します。

```
[AC2] local-user client001 class manage
```

#パスワードをプレーンテキストで”123456TESTplat&!”に設定します。

```
[AC2-luser-manage-client001] password simple 123456TESTplat&!
```

ユーザのサービスタイプを **ssh** に指定します。

```
[AC2-luser-manage-client001] service-type ssh
```

ユーザにユーザロール **network-admin** を割り当て、作業ディレクトリを **flash:/**に設定します。

```
[AC2-luser-manage-client001] authorization-attribute user-role network-admin
[AC2-luser-manage-client001] quit
```

SSH ユーザ **client001** を作成し、サービスタイプを **scp** とし、認証方式を **password** とします。

```
[AC2] ssh user client001 service-type scp authentication-type password
```

2)　SCP クライアントを設定します。

#VLAN-interface 2 の IP アドレスを設定します。

```
<AC1> system-view
[AC1] interface vlan-interface 2
[AC1-Vlan-interface2] ip address 192.168.0.2 255.255.255.0
[AC1-Vlan-interface2] quit
[AC1] quit
```

3)　SCP サーバに接続し、サーバから remote.bin ファイルをダウンロードし、local.bin という名前でローカルに保存します。

```
<AC1> scp 192.168.0.1 get remote.bin local.bin
Username: client001
Press CTRL+C to abort.
Connecting to 192.168.0.1 port 22.
The server is not authenticated. Continue? [Y/N]:y
Do you want to save the server public key? [Y/N]:n
client001@192.168.0.1's password:
remote.bin                                    100% 2875     2.8KB/s   00:00
```

目次

このセクションのページは **15-x-x** です。

6章 SSL 6-1
6.1 SSL概要 6-1
6.1.1 SSLセキュリティメカニズム 6-1
6.1.2 SSLプロトコルスタック 6-2
6.1.3 SSLプロトコルバージョン 6-2
6.2 制限事項とガイドライン 6-2
6.3 SSL設定作業リスト 6-2
6.4 SSLサーバポリシーの設定 6-3
6.4.1 設定必要条件 6-3
6.4.2 設定手順 6-3
6.5 SSLサーバのSSLプロトコルバージョンの無効化 6-4
6.6 SSLネゴシエーション実行中におけるSSLサーバの完全な証明書チェーンのクライアントへの送信 6-4
6.7 SSLクライアントポリシーの設定 6-5
6.7.1 設定必要条件 6-5
6.7.2 設定手順 6-5
6.8 SSLの表示 6-5

6章 SSL

6.1 SSL概要

Secure Sockets Layer (SSL) は、HTTP のような TCP ベースのアプリケーションレイヤプロトコルのセキュアなコネクションサービスを提供するセキュリティプロトコルです。

SSL は、e ビジネスやインタネットでセキュアなデータ通信を保証する必要があるオンライン銀行などに広く使われます。

6.1.1 SSL セキュリティメカニズム

SSL によって提供されるセキュアな通信は以下の特徴があります。

- **機密性**－SSL はデータを暗号化する対称暗号アルゴリズムを使用しています。そして対称暗号アルゴリズムによって作成された鍵を暗号化するために、Rivest, Shamir, and Adelman (RSA)の非対称の鍵アルゴリズムを使用します。
- **認証**－SSL は証明書を基にした、デジタル署名に使われるサーバとクライアントの同一性を示す認証をサポートしています。SSL サーバとクライアントは、公開鍵基盤を用いて、認証局(CA)から証明書を取得します。
- **信頼性**－SSL は、メッセージの完全性をチェックするため、鍵を基にしたメッセージ認証コード(MAC)を使用します。MAC アルゴリズムは、可変長のメッセージを固定長に変更します。図 6-1にメッセージの完全性をチェックする MAC アルゴリズムを使用する SSL について示します。送信元は、鍵のために、メッセージの MAC の値を計算する MAC アルゴリズムを使用します。次に送信元は、MAC の値をメッセージに添付し、結果を宛先に送信します。宛先は同じ鍵を用い、受信したメッセージの MAC の値を計算する MAC アルゴリズムを使用し、受信された MAC の値とローカルに計算された値と比較します。それぞれの MAC の値が同じならば、宛先はメッセージが損なわれていないと判断します。MAC の値が異なる場合、転送中にメッセージが変更されたと認識し、メッセージを廃棄します。

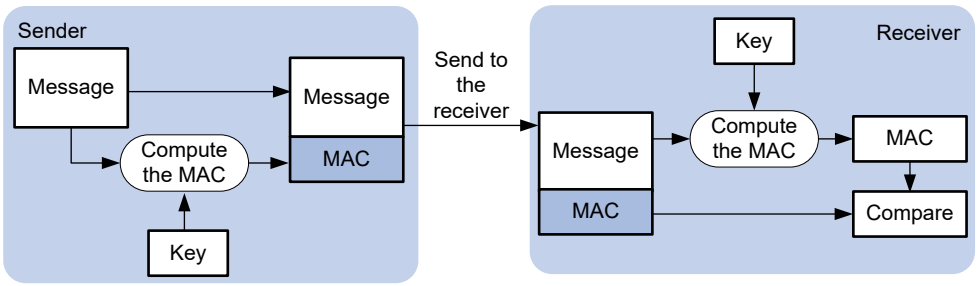


図 6-1 MAC アルゴリズムによるメッセージの完全性の検証

6.1.2 SSL プロトコルスタック

図 6-2に示すように、SSL は 2 つのレイヤのプロトコルから構成されます。低いレイヤの SSL レコードプロトコルと、上位の SSL ハンドシェイクプロトコル、SSL change cipher spec プロトコル、SSL alert プロトコルがあります。

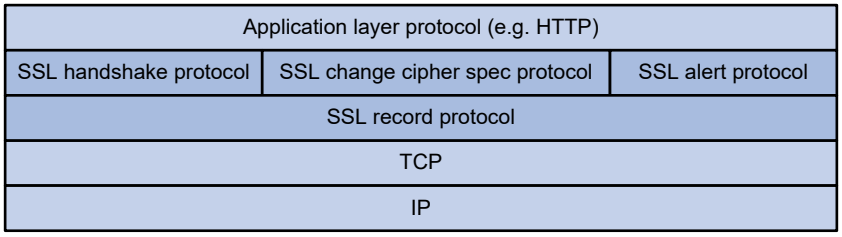


図 6-2 SSL プロトコルスタック

- **SSL レコードプロトコル**－転送されたデータをフラグメントし、データに MAC を追加し、計算します。対向先に転送する前にデータを暗号化します。
- **SSL ハンドシェイクプロトコル**－SSL プロトコルスタックの重要な部分です。信頼できるセキュアな通信に使われる暗号方式を決めます（非対称暗号アルゴリズム、鍵交換アルゴリズム、MAC アルゴリズムを含みます）。また、サーバとクライアント間の鍵交換をセキュアに行い、サーバとクライアントが、なりすましなどが行われていないことを示す同一性の認証を提供します。SSL ハンドシェイクプロトコルを通して、セッションがサーバとクライアント間で取得されます。セッションは、セッション ID、ピア証明書、暗号文、master secret を含んだパラメータから構成されます。
- **SSL 変更暗号文スペックプロトコル(SSL change cipher spec protocol)**－連続パケットを保護し、新規にネゴシエートされた暗号方式と鍵を基にして転送するためにクライアントとサーバ間でやりとりされるプロトコルです。
- **SSL 警告プロトコル(SSL alert protocol)**－SSL クライアントとサーバにお互いに警告メッセージを送信するプロトコルです。警告メッセージは、警告シビアリティレベルと説明文を含みます。

6.1.3 SSL プロトコルバージョン

SSL プロトコルのバージョンには、SSL 2.0、SSL 3.0、TLS 1.0 (または SSL 3.1)、TLS 1.1、TLS 1.2、および TLS 1.3 が含まれます。SSL 3.0 は安全でないことがわかっているため、SSL サーバーの SSL 3.0 を無効にしてセキュリティを確保できます。

6.2 制限事項とガイドライン

デフォルトでは、SSL サーバはすべての SSL プロトコルバージョンを実行しているクライアントと通信できます。サーバはクライアントから SSL 2.0 Client Hello メッセージを受信すると、通信に新しいバージョンを使用するようにクライアントに通知します。

6.3 SSL設定作業リスト

SSL サーバの設定作業リストを以下に示します。

作業	補足
SSLサーバポリシーの設定	必須設定項目
SSLサーバポリシー用のPKIドメイン指定	必須設定項目
SSLサーバのSSLプロトコルバージョンの無効化	オプション設定項目
SSLネゴシエーション実行中におけるSSLサーバの完全な証明書チェーンのクライアントへの送信	オプション設定項目

SSL クライアントの設定作業リストを以下に示します。

作業	補足
SSLサーバポリシーの設定	必須設定項目
SSLクライアントポリシー用のPKIドメイン指定	必須設定項目
SSLクライアントポリシーのSSLプロトコルバージョンを指定	オプション設定項目
デジタル証明書を使用したサーバの認証を設定する	オプション設定項目

6.4 SSLサーバポリシーの設定

SSL サーバポリシーは、サーバが立ち上がったときに使われる SSL パラメータです。SSL サーバポリシーは HTTP プロトコルのようなアプリケーションレイヤのプロトコルに関連している場合のみ効果があります。

6.4.1 設定必要条件

SSL サーバポリシーの PKI ドメインを設定します。PKI ドメインは、サーバ側の証明書を取得するのに使われます。

6.4.2 設定手順

以下に SSL サーバポリシーを設定する手順を示します。

操作	コマンド	補足
1. system view へ移行する	**system-view**	―
2. SSL サーバポリシーを作成し、その view へ移行する	**ssl server-policy** *policy-name*	―
3. SSL サーバポリシー用の PKI ドメインを指定する	**pki-domain** *domain-name*&<*1-2*>	デフォルト：なし

🕮 **メモ：**

クライアント認証を有効にした場合、クライアント用にローカル証明書を要求する必要があります。

6.5 SSLサーバのSSLプロトコルバージョンの無効化

セキュリティを強化するために、SSL サーバがセッションネゴシエーションに特定の SSL プロトコルバージョンを使用しないようにすることができます。

SSL サーバは、SSL サーバポリシーの SSL プロトコルバージョンが有効になっているバージョンでのみ

以下に装置で SSL サーバの SSL プロトコルバージョンを無効にする手順を示します。

操作	コマンド	補足
1. system view へ移行する	**system-view**	ー
2. SSL サーバの SSL プロトコルバージョンを無効にする	**ssl version** { **ssl3.0** | **tls1.0** | **tls1.1** | **tls1.2** | **tls1.3** } **disable**	デフォルト：SSL3.0、TLS1.0、TLS1.1、TLS1.2が有効

6.6 SSLネゴシエーション実行中におけるSSLサーバの完全な証明書チェーンのクライアントへの送信

クライアントがサーバ証明書を確認するための完全な証明書チェーンを持っていない場合、SSL セッションが正常に確立されるようにするためにこの機能を設定します。

以下に SSL ネゴシエーションの実行中に SSL サーバが完全な証明書チェーンをクライアントに送信することを有効にする手順を示します。

操作	コマンド	補足
1. system view へ移行する	**system-view**	ー
2. SSL サーバポリシーの作成とその view へ移行する	**ssl server-policy** *policy-name*	ー
3. SSL ネゴシエーションの実行中に SSL サーバが完全な証明書チェーンをクライアントに送信することを有効にする	**certificate-chain-sending enable**	デフォルト：SSLネゴシエーションの実行中、SSLサーバは、完全な証明書チェーンではなくサーバ証明書をクライアントに送信します

6.7 SSLクライアントポリシーの設定

SSL クライアントポリシーは、装置が SSL クライアントとして動作するときに使用される SSL パラメータセットです。SSL クライアントは、SSL クライアントポリシーの設定を使用してサーバへの接続を確立します。

SSL クライアントポリシーに設定する SSL パラメータには、PKI ドメイン、優先暗号スイートが含まれます。

6.7.1 設定必要条件

SSL クライアントポリシーの PKI ドメインを設定します。PKI ドメインは、クライアント側の証明書を取得するのに使われます。

6.7.2 設定手順

以下に SSL クライアントポリシーを設定する手順を示します。

操作	コマンド	補足
1. system view へ移行する	**system-view**	―
2. SSL クライアントポリシーを作成し、その view へ移行する	**ssl client-policy** *policy-name*	―
3. SSL クライアントポリシー用の PKI ドメインを指定する	**pki-domain** *domain-name*	デフォルト：なし
4. SSL クライアントポリシーの SSL プロトコルバージョンを指定する	**version** { **ssl3.0** | **tls1.0** | **tls1.1** | **tls1.2** | **tls1.3** }	デフォルト：TLS1.0
5. デジタル証明書を使用したサーバの認証を設定する	**server-verify enable**	デフォルト：有効

6.8 SSLの表示

操作	コマンド	補足
SSLクライアントポリシー情報を表示する	**display ssl client-policy** [*policy-name*]	すべてのviewでコマンドを実行できます。
SSLサーバポリシー情報を表示する	**display ssl server-policy** [*policy-name*]	すべてのviewでコマンドを実行できます。

目次

このセクションのページは **15-x-x** です。

7章 接続制限 7-1
7.1 概要 7-1
7.2 接続制限設定の設定作業リスト 7-1
7.3 接続制限ポリシーの作成 7-1
7.4 接続制限ポリシーの設定 7-2
7.4.1 IPv4接続制限ポリシーの設定 7-2
7.5 接続制限ポリシーの適用 7-3
7.6 ログ出力抑制の設定 7-3
7.7 接続制限の表示および管理 7-3
7.7.1 接続制限設定の確認 7-3
7.7.2 接続制限統計の表示とクリア 7-4
7.8 接続制限のトラブルシューティング 7-4
7.8.1 セグメントが重複している接続制限ルール内のACL 7-4

7章 接続制限

7.1 概要

接続制限機能により、デバイスは確立された接続数を監視し制限することができます。

図 7-1に示すように、次の問題が存在する可能性があります。

- ホスト B が短時間に大量の接続を開始すると、システムリソースが使い尽くされ、ホスト A がインターネットにアクセスできなくなる可能性があります。
- 内部サーバが短時間に大量の接続要求を受信すると、サーバは他の要求を処理できません。

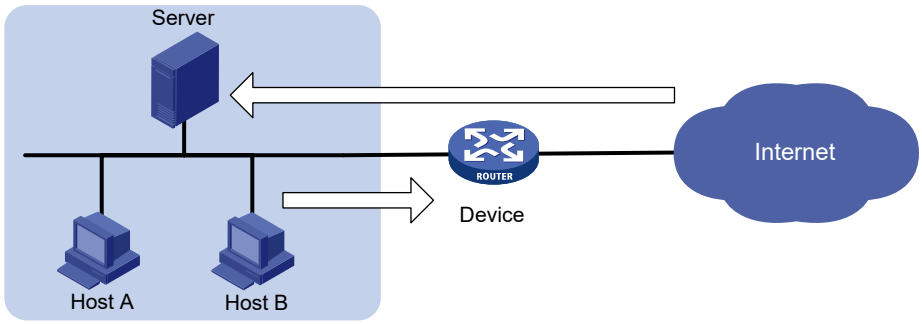


図 7-1 ネットワーク図

これらの問題を解決するには、作成した接続制限ポリシーをグローバルまたはインタフェースに適用し、すべてのインタフェースまたは単一インタフェースで接続制限を設定します。

7.2 接続制限設定の設定作業リスト

操作
接続制限ポリシーの作成
接続制限ポリシーの設定 IPv4接続制限ポリシーの設定
接続制限ポリシーを適用する
ログ出力抑制の設定

7.3 接続制限ポリシーの作成

接続制限ポリシーには、一連の接続制限ルールが含まれており、それぞれの接続制限ルールは、接続の範囲と接続制限基準を定義します。

接続制限ポリシーを作成するためには、次の作業を実行します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. 接続制限ポリシーを作成し、その view に移行する	**connection-limit policy** *policy-id*	デフォルト：設定なし

7.4 接続制限ポリシーの設定

接続制限ポリシーを使用するには、ポリシーに接続制限ルールを追加する必要があります。接続制限ルールには、接続の範囲と接続制限基準を定義します。接続制限基準に基づいて範囲内の接続は制限されます。接続制限基準に一致する接続数が上限に達すると、接続数が下限値を下回るまで、デバイスは新しい接続を受け入れません。接続制限基準に一致しない接続は制限されません。

各接続制限ルールでは、ACL を使用して接続の範囲を定義します。さらに、この接続制限ルールでは、次のフィルタリング方法を使用して接続を制限することができます。

- **宛先毎**－宛先 IP アドレスによるユーザー接続を制限します。
- **サービス毎**－ユーザー接続をサービス（トランスポート層プロトコルとサービスポート）別に制限します。
- **送信元毎**－送信元 IP アドレスによるユーザー接続を制限します。

複数のフィルタリング方法を選択でき、選択した方法が同時に有効になります。たとえば、宛先毎とサービス毎の両方を指定した場合、同じサービスを使用し、同じ IP アドレス宛のユーザー接続が制限の対象となります。接続制限ルールでフィルタリング方法を指定しない場合、その範囲内のすべてのユーザー接続が制限の対象となります。

接続制限ポリシーが適用されると、デバイス上の接続は、ルール ID の昇順でポリシー内のすべての接続制限ルールとの照合を行います。ID の小さいルールほど接続の範囲は小さくし多くのフィルタリング方法を指定することを推奨します。

7.4.1 IPv4 接続制限ポリシーの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. connection limit policy に移行する	**connection-limit policy** *policy-id*	—
3. 接続制限ルールを設定する	**limit** *limit-id* **acl** { *acl-number* | **name** *acl-name* } [**per-destination** | **per-service** | **per-source**] * **amount** *max-amount min-amount* | **rate** *rate* } * [**description** *text*]	デフォルト：設定なし
4. (オプション設定項目) 接続制限ルールの説明を設定する	**description** *text*	デフォルト：設定なし

7.5 接続制限ポリシーの適用

接続制限ポリシーを有効にするには、グローバルまたはインタフェースにポリシーを適用する必要があります。インタフェースに適用される接続制限ポリシーは、インタフェース上の指定された接続に対してのみ有効です。グローバルに適用される接続制限ポリシーは、デバイス上の指定されたすべての接続に適用されます。

異なる接続制限ポリシーを、デバイス上のグローバルと個々のインタフェースのそれぞれに適用することもできます。この場合、デバイスは、受信インタフェースのポリシー、グローバルのポリシー、送信インタフェースのポリシーの順序で、接続を照合します。接続の数が定義されたポリシーのうち最も低い接続上限値に達している限り、新しい接続を受け入れることはできなくなります。

接続制限ポリシーを適用するためには、次の手順を実行します。

操作	コマンド	補足
1. system view に移行する	system-view	—
2. 接続制限ポリシーを適用する	• グローバルへの接続制限ポリシーの適用 **connection-limit apply global policy** *policy-id* • インタフェースへの接続制限ポリシーの適用 1. **interface** *interface-type interface-number* 2. **connection-limit apply policy** *policy-id*	デフォルト : 接続制限ポリシーは適用されていません。 接続制限ポリシーは1つずつのみグローバルまたはインタフェースに適用できます。新しいIPv4接続制限ポリシーを設定した場合、古いポリシーを上書きします。

7.6 ログ出力抑制の設定

デフォルトでは、装置は接続制限ルールが一致するたびにログメッセージを記録します。短期間に頻繁に一致した場合、大量のログメッセージを記録します。

この機能は、指定された期間内に同じログメッセージの生成を抑制します。

操作	コマンド	補足
3. system view に移行する	system-view	—
4. ログ出力の抑制間隔を設定する	**connection-limit log-suppress interval** *time-value*	デフォルト：抑制しない

7.7 接続制限の表示および管理

7.7.1 接続制限設定の確認

display コマンドはすべてのビューで実行できます。

操作	コマンド
グローバルまたはインタフェースで IPv4 接続制限ルールに一致する接続に関する統計情報を表示する	**display connection-limit stat-nodes** { **global** | **interface** *interface-type interface-number* } [**destination** *destination-ip* | **service-port** *port-number* | **source** *source-ip*] * [**count**]

7.7.2 接続制限統計の表示とクリア

display コマンドはすべてのビューで実行し、**reset** コマンドは user view で実行できます。

操作	コマンド
接続制限統計を表示する	**display connection-limit statistics** { **global** | **interface** *interface-type interface-number* }
接続制限統計をクリアする	**reset connection-limit statistics** { **global** | **interface** *interface-type interface-number* }

7.8 接続制限のトラブルシューティング

7.8.1 セグメントが重複している接続制限ルール内の ACL

I. 症状

対象の接続制限ポリシーには 2 つのルールがあります。ルール 1 は、セグメント 192.168.0.0/24 の各ホストからの接続の上限を 10 に設定します。ルール 2 は、192.168.0.100/24 からの接続の上限を 100 に設定します。

```
<AC> system-view
[AC] acl basic 2001
[AC-acl-ipv4-basic-2001] rule permit source 192.168.0.0 0.0.0.255
[AC-acl-ipv4-basic-2001] quit
[AC] acl basic 2002
[AC-acl-ipv4-basic-2002] rule permit source 192.168.0.100 0
[AC-acl-ipv4-basic-2002] quit
[AC] connection-limit policy 1
[AC-connection-limit-policy-1] limit 1 acl 2001 per-destination amount 10 5
[AC-connection-limit-policy-1] limit 2 acl 2002 per-destination amount 100 10
```

その結果、192.168.0.100 のホストは、外部ネットワークに対して最大 10 の接続しか開始できません。

II. 解決策

この問題を解決するには、

1) ルール ID を交換して、2 つの接続制限ルールを再調整します。
2) 問題が解決しない場合は、サポートに問い合わせてください。

目次

このセクションのページは **15-x-x** です。

8 章 TCP フラグメントアタックプロテクション 8-1
8.1 概要 8-1
8.2 TCP フラグメント攻撃防止の設定 8-1

8章 TCP フラグメントアタックプロテクション

8.1 概要

攻撃者は、RFC1858 で定義されている攻撃用 TCP フラグメントを送信して、TCP フラグメント攻撃を開始します。

- TCP ヘッダーが 20 バイトより小さい最初のフラグメント
- フラグメントオフセットが 8 バイト (FO=1) の最初以外のフラグメント

通常、パケットフィルタは、TCP パケットの最初のフラグメントの送信元と宛先の IP アドレス、送信元と宛先のポート、およびトランスポート層プロトコルを検出します。最初のフラグメントが検出に合格すると、TCP パケットの後続のすべてのフラグメントが通過できるようになります。

攻撃 TCP パケットの最初のフラグメントはパケットフィルタ内で一致しないため、後続のフラグメントはすべて通過できます。受信ホストがフラグメントを再構成すると、TCP フラグメント攻撃が発生します。

TCP フラグメント攻撃を防ぐには、TCP フラグメント攻撃防止を有効にして、攻撃 TCP フラグメントを破棄します。

8.2 TCPフラグメント攻撃防止の設定

TCP フラグメント攻撃防止機能は、受信した TCP フラグメントの長さとフラグメントオフセットを検出し、攻撃 TCP フラグメントをドロップします。

I. 制限事項とガイドライン

TCP フラグメント攻撃防止は、シングルパケット攻撃防止よりも優先されます。両方を使用する場合、着信 TCP パケットは最初に TCP フラグメント攻撃防止によって処理された後、シングルパケット攻撃防御ポリシーによって処理されます。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. TCP フラグメント攻撃防止を有効にする	**attack-defense tcp fragment enable**	デフォルト：有効

目次

このセクションのページは **15-x-x** です。

9章 IPソースガード 9-1
9.1 概要 9-1
9.2 設定手順 9-1
9.3 IPSGの設定例 9-2
9.3.1 ネットワーク要件 9-2
9.3.2 設定手順 9-3
9.3.3 設定の確認 9-4

9章 IP ソースガード

9.1 概要

IP ソースガード（IPSG）は、AP で受信するパケットをフィルタするための WLAN スヌーピングエントリを使用して、なりすまし攻撃を防止します。

WLAN スヌーピングは AP ではデフォルトで有効になっています。WLAN スヌーピングエントリは IP-MAC バインディングです。

- IPv4 ネットワークでは、WLAN スヌーピングはクライアントの IP-MAC バインディングを、AP を通過する ARP メッセージまたは DHCP パケットから読み取ります。IPSG は DHCP パケットから取得した WLAN スヌーピングエントリのみを使用します。

QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*5 ネットワーク接続*”の”*12 章 DHCP の概要*”を参照してください。

図 9-1に示すように、AP は DHCP サーバから IP アドレスを取得したクライアントについて、WLAN スヌーピングエントリを持っています。IPSG は、正当なクライアントからのパケットのみを転送します。

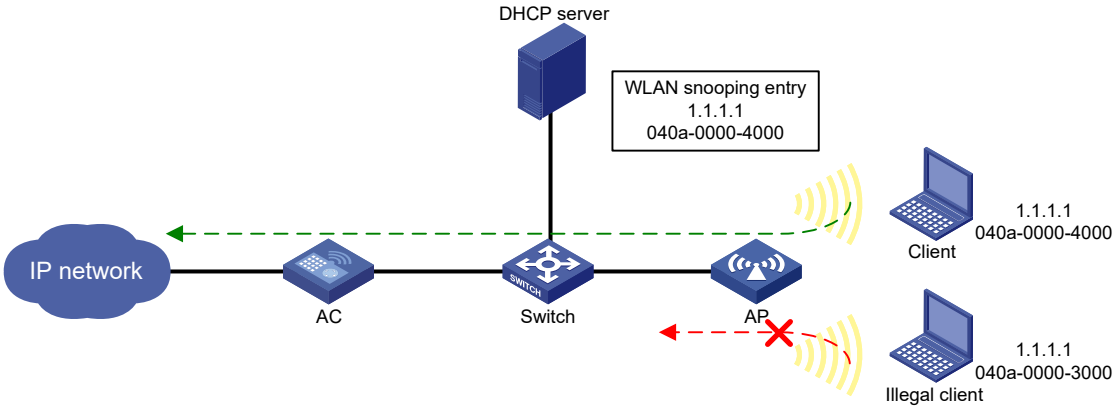


図 9-1 IPSG の適用

9.2 設定手順

サービサービステンプレートのために有効化された IPSG は、サービステンプレートに基づいて作成された BSS におけるクライアントからのパケットのみをフィルタします。他の BSS のクライアントには影響しません。

以下に IPSG 機能を有効にする設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—

操作	コマンド	補足
2． service template view に移行する	**wlan service-template** *service-template-number*	―
3． IPv4 の IPSG 機能を有効化する	**ip verify source**	デフォルト：無効

9.3 IPSGの設定例

9.3.1 ネットワーク要件

図 9-2に示すように、クライアントは SSID サービス越しに WLAN にアクセスします。クライアント 1 とクライアント 2 は DHCP サーバ(スイッチ)越しに IP アドレスを取得します。

AP に到達するパケットをフィルタリングさせるために､AC 上でサービステンプレートの IPSG を有効化します。AP はクライアント 1 およびクライアント 2 からのパケットのみを転送します。

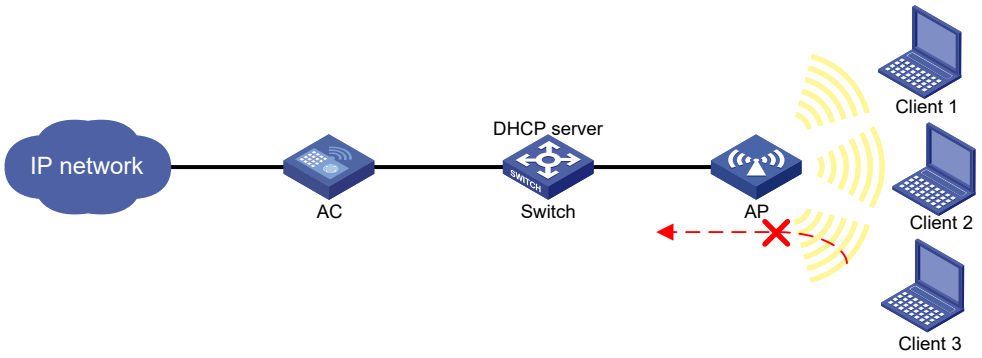


図 9-2 ネットワーク図

9.3.2 設定手順

サービステンプレート 1 を作成します。

```
<AC> system-view
[AC] wlan service-template 1
```

サービステンプレートのための SSID を設定し、サービステンプレートを有効化します。

```
[AC-wlan-st-1] ssid service
[AC-wlan-st-1] service-template enable
```

IPv4 の IPSG 機能を有効化します。

```
[AC-wlan-st-1] ip verify source
[AC-wlan-st-1] quit
```

アクセスポイント ap1 を QX-W1020 モードで作成し、シリアル ID を 210235A29G007C000020 に設定します。

```
[AC] wlan ap ap1 model QX-W1020
[AC-wlan-ap-ap1] serial-id 210235A29G007C000020
```

radio 2 の radio view に移行し、サービステンプレート 1 と radio 2 を関連付けます。

```
[AC-wlan-ap-ap1] radio 2
[AC-wlan-ap-ap1-radio-2] service-template 1
[AC-wlan-ap-ap1-radio-2] quit
[AC-wlan-ap-ap1] quit
```

9.3.3 設定の確認

クライアント 1 とクライアント 2 が DHCP で IP アドレスを取得し、クライアント 3 には手動でクライアント 1 の IP アドレスをアサインします（詳細は示しません）。

クライアント 1 とクライアント 2 からのパケットが通過を許可されることを確認します（詳細は示しません）。

クライアント 3 からのパケットが廃棄されることを確認します（詳細は示しません）。

目次

このセクションのページは **15-x-x** です。

10 章 ARP アタックプロテクション 10-1
10.1 概要 10-1
10.2 ARP アタックプロテクション設定作業リスト 10-1
10.3 解決不能 IP 攻撃保護の設定 10-2
10.3.1 解決不能 IP 攻撃保護ついて 10-2
10.3.2 ARP 送信元抑制の設定 10-2
10.3.3 ARP ブラックホールルーティングの設定 10-2
10.3.4 解決できない IP 攻撃保護の表示と維持 10-3
10.4 ARP パケットレート制限 10-3
10.5 送信元ベースの ARP アタック detection の設定 10-4
10.5.1 設定手順 10-4
10.5.2 送信元 MAC アドレスにもとづく ARP アタック detection の表示と維持 10-5
10.5.3 設定例 10-5
10.6 ARP パケット送信元 MAC アドレス正当性チェックの設定 10-7
10.6.1 ARP パケット送信元 MAC アドレス正当性チェックの表示と維持 10-7
10.7 ARP 確認応答の設定 10-7
10.8 authorized ARP の設定 10-8
10.8.1 設定例 10-8
10.9 ARP アタック detection の設定 10-11
10.9.1 制約事項とガイドライン 10-11
10.9.2 ユーザの正当性の確認の設定 10-12
10.9.3 設定ガイドライン 10-12
10.9.4 設定手順 10-12
10.9.5 ARP パケット正当性の確認の設定 10-13
10.9.6 ARP 制限転送の設定 10-14
10.9.7 ユーザ妥当性チェック中に ARP パケットの入力ポートを無視する 10-14
10.9.8 ARP アタック detection ログの有効化 10-15
10.9.9 ARP アタック detection の表示と維持 10-15
10.9.10 ユーザの正当性の確認の設定例 10-15
10.10 ARP スキャンと固定 ARP の設定 10-18
10.10.1 ARP スキャンの開始 10-19
10.10.2 自動 ARP スキャンの設定 10-19
10.10.3 固定 ARP の設定 10-19
10.11 ARP 送信者 IP アドレスチェックの設定 10-20
10.11.1 設定ガイドライン 10-20
10.11.2 設定手順 10-20

10章 ARP アタックプロテクション

10.1 概要

ARP アタックとウイルスは LAN のセキュリティを脅かしています。この章では、そのような ARP アタックを発見、防御するための機能について記載します。

ARP は実装が容易ですが、セキュリティメカニズムを持っていないため、ネットワーク攻撃に対して脆弱です。攻撃者は ARP の脆弱性を悪用し、以下の方法でネットワーク装置を攻撃する可能性があります。

- 信頼されたユーザあるいは、ゲートウェイによるものとして見せかけた ARP パケットを送信し、装置は不正な ARP をエントリに追加します。
- 大量の宛先 MAC アドレス到達不能の IP パケットによって、受信装置の CPU が過負荷になるまで IP アドレスの解決処理を行います。ARP は到達不能の IP パケットに対応する MAC アドレスを検出することができません。
- 大量の ARP パケットによって、受信装置の CPU が過負荷になります。

10.2 ARPアタックプロテクション設定作業リスト

作業リスト
フラッド防御の設定： • 解決不能IP攻撃保護の設定 • ARPパケットレート制限 • 送信元ベースのARPアタックdetectionの設定
ユーザとゲートウェイのなりすましの防御： • ARPパケット送信元MACアドレス正当性チェックの設定 • ARP確認応答の設定 • authorized ARPの設定 • ARP アタックdetectionの設定 • ARP制限転送の設定 • ユーザ妥当性チェック中にARPパケットの入力ポートを無視する • ARPアタック detectionログの有効化 • ARPスキャンと固定ARPの設定 • ARP送信者IPアドレスチェックの設定

10.3 解決不能IP攻撃保護の設定

10.3.1 解決不能 IP 攻撃保護ついて

装置がホストから大量の解決不能 IP パケットを受信した場合、次のような状況が発生する可能性があります。

- 大量の ARP 要求を送信し、ターゲットサブネットに過負荷をかけます。
- 宛先 IP アドレスを解決しようとし続け、CPU に過負荷をかけます。

このような IP 攻撃からデバイスを保護するために、次の機能を設定できます。

- ARP 送信元抑制－特定の IP アドレスから受信する解決できない IP パケットの数が 5 秒以内に一定以上受信した場合、その IP アドレスからのパケットの解決を停止します。インターバル時間が経過すると、デバイスは ARP 解決を続行します。この機能は、攻撃パケットの送信元 IP アドレスが同じ場合に適用されます。
- ARP ブラックホールルーティング－未解決の IP アドレスを宛先とするブラックホールルートを作成します。装置は、ブラックホールルートが削除されるまで、一致するすべてのパケットをドロップします。ブラックホールルートは、エージングタイマに到達するか、ルートが到達可能になると削除されます。

未解決の IP アドレスに対してブラックホールルートが作成されると、装置は ARP 要求を送信することで、最初の ARP ブラックホールルートプローブをすぐに開始します。解決に失敗した場合、装置はプローブ設定に従ってプローブを続行します。プローブで IP アドレス解決が成功した場合、装置はブラックホールルートを通常のルートに変換します。装置がすべてのプローブを完了する前に ARP ブラックホールルートが期限切れになると、装置はブラックホールルートを削除し、残りのプローブを実行しません。

この機能は、攻撃パケットの送信元アドレスが同じかどうかに関係なく適用できます。

10.3.2 ARP 送信元抑制の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. ARP 送信元抑制を有効にする	**arp source-suppression enable**	デフォルト：無効
3. 送信元 IP アドレスごとに 5 秒以内に処理できる解決できないパケットの最大数を設定する	**arp source-suppression limit** *limit-value*	デフォルト：10

10.3.3 ARP ブラックホールルーティングの設定

I. 制限とガイドライン

ARP ブラックホール ルートのプローブ カウントを大きな値 (25 など) に設定します。デバイスが一時的に宛先 IP アドレスに到達できず、プローブ カウントが小さすぎる場合、問題が解決する前にすべてのプローブが終了する可能性があります。その結果、非攻撃パケットはドロップされます。 この設定により、このような状況を回避できます。

II. 設定手順

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． ARP ブラックホールルーティングを有効にする	**arp resolving-route enable**	デフォルト：無効
3． (オプション設定項目) 未解決の IP アドレスごとに ARP ブラックホールルートプローブの数を設定する	**arp resolving-route probe-count** *count*	デフォルト：3
4． (オプション設定項目) ARP ブラックホールルートのプローブ間隔を設定する	**arp resolving-route probe-interval** *interval*	デフォルト：1秒

10.3.4 解決できない IP 攻撃保護の表示と維持

すべての view で display コマンドを実行することができます。

操作	コマンド
ARP送信元抑制設定情報を表示する	**display arp source-suppression**

10.4 ARPパケットレート制限

ARP パケットレート制限機能を使用すると、CPU に配信される ARP パケットのレートを制限できます。ARP 攻撃検出対応デバイスは、受信したすべての ARP パケットを検査のために CPU に送信します。過剰な ARP パケットを処理すると、デバイスが誤動作したり、クラッシュしたりします。この問題を解決するには、ARP パケットレート制限を設定します。インタフェース上の ARP パケットの受信レートがレート制限を超えると、それらのパケットは破棄されます。

SNMP モジュールへの通知の送信を有効にしたり、ARP パケットレート制限のロギングを有効にしたりできます。

- 通知の送信が有効になっている場合、デバイスは通知の送信間隔内で最も高いしきい値超過 ARP パケットレートを SNMP モジュールに送信します。
- ARP パケットレート制限のログが有効になっている場合、デバイスはログメッセージで送信間隔内の最大しきい値超過 ARP パケットレートをインフォメーションセンターに送信します。ログ出力ルールを設定するようにインフォメーションセンターモジュールを設定できます。

I. 制限とガイドライン

ベストプラクティスとして、ARP 攻撃検出、ARP スヌーピング、または ARP fast-reply が有効な場合、または ARP フラッド攻撃が検出された場合に、この機能を設定します。

ARPパケットレート制限に対して過剰な通知およびログメッセージが送信される場合は、通知およびログメッセージの送信間隔を長くすることができます。

LAG インタフェースで ARP パケットレート制限の通知送信およびログ記録を有効にすると、機能はすべての LAG メンバーポートに適用されます。

II. 設定手順

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． (オプション設定項目) ARP パケットレート制限の SNMP 通知を有効にする	**snmp-agent trap enable arp** [**rate-limit**]	デフォルト：無効
3． (オプション設定項目) ARP パケットレート制限のロギングを有効にする	**arp rate-limit log enable**	デフォルト：無効
4． (オプション設定項目) 通知およびログメッセージの送信間隔を設定する	**arp rate-limit log interval** *interval*	デフォルト：60秒
5． インタフェース view に移行する	**interface** *interface-type interface-number*	―
6． ARP パケットレート制限を有効にする	**arp rate-limit** [*pps*]	デフォルト：有効

10.5 送信元ベースのARPアタックdetectionの設定

この機能は CPU に送られる ARP パケットの数を確認します。5 秒間に同じ送信元からの ARP パケットの受信した数がしきい値を超えた場合、装置は、この MAC アドレスを ARP アタックエントリテーブルに追加します。エントリのエージングタイマが終了する前に、装置は以下の方法で攻撃に対応します。

- **モニタモード** ― ログメッセージを作成します。
- **フィルタモード** ― ログメッセージを作成し、攻撃する MAC アドレスからの後続の ARP パケットをフィルタします。

この機能ではゲートウェイやサーバの MAC アドレスを除外するように設定することができます。ゲートウェイやサーバの MAC アドレスを除外した場合、たとえ攻撃者からの ARP パケットだとしても、除外された ARP パケットの確認を行いません。

10.5.1 設定手順

以下に送信元 MAC アドレスにもとづく ARP アタック detection の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―

操作	コマンド	補足
2． 送信元 MAC アドレスにもとづく ARP アタック detection を有効にし、モードを指定する	**arp source-mac** { **filter** | **monitor** }	デフォルト：無効
3． しきい値を設定する	**arp source-mac threshold** *threshold-value*	デフォルト：30
4． ARP アタックエントリのエージングタイマを設定する	**arp source-mac aging-time** *time*	デフォルト：300秒
5． （オプション設定項目） ARP アタック detection 機能から除外する MAC アドレスを設定する	**arp source-mac exclude-mac** *mac-address*&<1-n>	デフォルト：設定なし

🕮 **メモ：**

ARP アタックエントリのエージングタイマが終了したとき、エントリの MAC アドレスからの ARP パケットは正常に処理することができます。

10.5.2 送信元 MAC アドレスにもとづく ARP アタック detection の表示と維持

すべての view で **display** コマンドを実行することができ、user view で **reset** コマンドを実行することができます。

操作	コマンド
送信元MACアドレスにもとづくARPアタックdetectionで検出されたARPアタックエントリを表示する	**display arp source-mac interface** *interface-type interface-number*
送信元MACベースのARP攻撃検出によってドロップされたパケットの統計情報を表示する	**display arp source-mac statistics**
送信元MACベースのARP攻撃検出によってドロップされたパケットの統計情報をクリア	**reset arp source-mac statistics**

10.5.3 設定例

I. ネットワーク要件

図 10-1 に示すように、Host はゲートウェイ（AC）を介してインターネットにアクセスします。悪意のあるユーザがゲートウェイに大量の ARP 要求を送信した場合、ゲートウェイがクラッシュする可能性があり、クライアントからの要求を処理できません。この問題

を解決するために、ゲートウェイ上で送信元 MAC アドレスにもとづく ARP アタック detection を設定します。

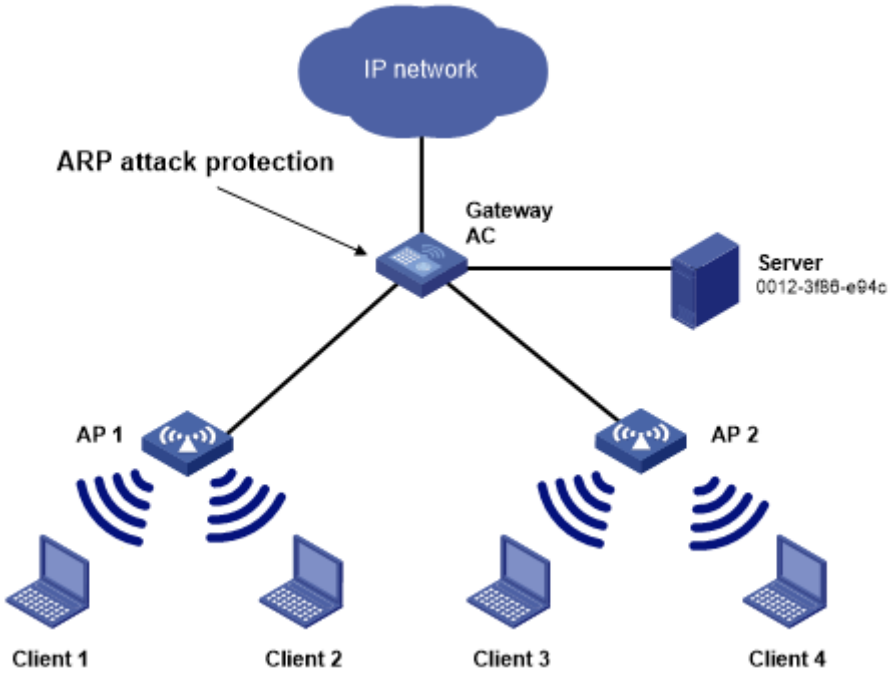


図 10-1 ネットワーク図

II. 設定要件

攻撃者は、有効な Host の MAC アドレスを送信元 MAC アドレスとして使用し、ARP パケットを大量に偽造することがあります。このような攻撃を防ぐために、次の手順でゲートウェイを設定します。

1) 送信元 MAC アドレスにもとづく ARP アタック detection を有効にし、フィルタモードを指定します。
2) しきい値を設定します。
3) ARP アタックエントリのエージングタイマを設定します。
4) この機能からサーバの MAC アドレスを除外します。

III. 設定手順

送信元 MAC アドレスにもとづく ARP アタック detection を有効にし、フィルタモードを指定します。

```
<AC> system-view
[AC] arp source-mac filter
```

しきい値を 30 に設定します。

```
[AC] arp source-mac threshold 30
```

ARP アタックエントリのエージングタイマを 60 秒に設定します。

```
[AC] arp source-mac aging-time 60
```

MAC アドレス 0012-3f86-e94c を除外します。

```
[AC] arp source-mac exclude-mac 0012-3f86-e94c
```

10.6 ARPパケット送信元MACアドレス正当性チェックの設定

この機能を有効にすることで、ゲートウェイはイーサネットヘッダの送信元 MAC アドレスが ARP メッセージのメッセージ部分にある送信元 MAC アドレスと異なる場合、ARP パケットをフィルタします。これによりゲートウェイは正しい ARP エントリを学習します。

以下に ARP パケット送信元 MAC アドレス正当性チェックの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． ARP パケット送信元 MAC アドレス正当性チェックを設定する	**arp valid-check enable**	デフォルト：無効

10.6.1 ARP パケット送信元 MAC アドレス正当性チェックの表示と維持

すべての view で **display** コマンドを実行することができ、user view で **reset** コマンドを実行することができます。

操作	コマンド
ARPパケット送信元MACアドレス整合性チェックによってドロップされたパケットの統計情報を表示する	**display arp valid-check statistics**
ARPパケット送信元MAC整合性チェックでドロップされたパケットの統計情報をクリアする	**reset arp valid-check statistics**

10.7 ARP確認応答の設定

ユーザのなりすましを防御するため、ARP 確認応答機能をゲートウェイで設定します。

ARP 確認応答機能は、ゲートウェイが不正な ARP エントリを作成することを防御します。

以下に ARP 確認応答機能の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー

操作	コマンド	補足
2． ARP 確認応答機能を有効にする	**arp active-ack** [**strict**] **enable**	デフォルト：無効 strictを設定する場合は、ARP ブラックホールルーティングを有効にしてください。

10.8 authorized ARPの設定

authorized ARP エントリは、DHCP サーバ上の DHCP クライアントのアドレスリースまたは DHCP リレーエージェント上のダイナミッククライアントエントリに基づいて生成されます。

この機能を使用して、ユーザスプーフィングを防止し、許可されたクライアントだけがネットワークリソースにアクセスできるようにします。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． インタフェース view に移行する	**interface** *interface-type interface-number*	下記インタフェースタイプをサポートします。 レイヤ3イーサネットインタフェース レイヤ3イーサネットサブインタフェース VLANインタフェース
3． authorized ARP を有効にする	**arp authorized enable**	デフォルト：無効

10.8.1 設定例

I. DHCP サーバでの authorized ARP の設定

1)　ネットワーク要件

図 10-2 に示すように、Client は DHCP を介して IPv4 アドレスを取得します。AC (DHCP サーバ) の VLAN インタフェース 10 に authorized ARP を設定して、ユーザの有効性を確保します。

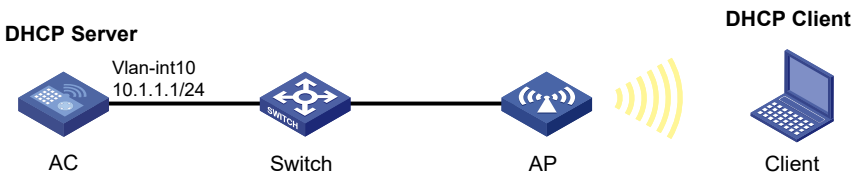


図 10-2 ネットワーク図

2)　設定手順

DHCP を設定する。

```
[AC] dhcp enable
[AC] dhcp server ip-pool 1
[AC-dhcp-pool-1] network 10.1.1.0 mask 255.255.255.0
[AC-dhcp-pool-1] quit
```

VLAN-interface 10 の IP アドレスを指定します。

```
[AC] vlan 10
[AC-vlan10] quit
[AC] interface vlan-interface 10
[AC-Vlan-interface10] ip address 10.1.1.1 24
```

VLAN インタフェース 10 で authorized ARP を有効にする。

```
[AC-Vlan-interface10] arp authorized enable
[AC-Vlan-interface10] quit
```

3)　設定の確認

#AC で authorized ARP エントリ情報を表示する。

```
[AC] display arp
  Type: S-Static   D-Dynamic   O-Openflow   R-Rule   I-Invalid
IP address      MAC address    VLAN/VSI name Interface/Link ID        Aging
Type
10.1.1.2        0012-3f86-e94c --            GE1/0/1                   20    D
```

IP アドレス 10.1.1.2 がクライアントに割り当てられていることを示しています。

クライアントは、AC と通信するために、authorized ARP エントリの IP アドレスと MAC アドレスを使用する必要があります。それ以外の場合、通信は失敗します。これにより、ユーザの妥当性が確保されます。

II. DHCP リレーエージェントでの authorized ARP の設定

1)　ネットワーク要件

図 10-3 に示すように、スイッチは DHCP サーバとして機能し、サブネット 10.10.1.0/24 の IP アドレスを DHCP クライアントに割り当てます。AC は DHCP リレーエージェントとして動作します。AC の VLAN インタフェース 20 で authorized ARP を設定し、ユーザの有効性を確保します。

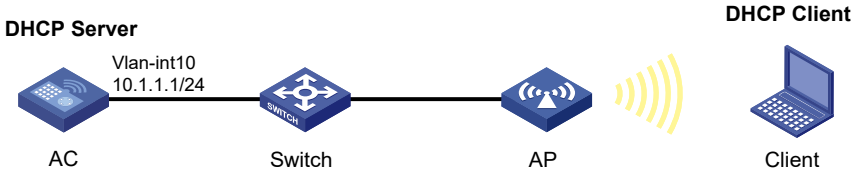


図 10-3 ネットワーク図

2)　設定手順

a)　スイッチを設定します。

VLAN-interface 10 の IP アドレスを指定します。

```
<Switch> system-view
[Switch] interface vlan-interface 10
[Switch-Vlan-interface10] ip address 10.1.1.1 24
[Switch-Vlan-interface10] quit
```

DHCP を設定をします。

```
[Switch] dhcp enable
[Switch] dhcp server ip-pool 1
[Switch-dhcp-pool-1] network 10.10.1.0 mask 255.255.255.0
[Switch-dhcp-pool-1] gateway-list 10.10.1.1
[Switch-dhcp-pool-1] quit
[Switch] ip route-static 10.10.1.0 24 10.1.1.2
```

b)　ACを設定します。

DHCP を有効にします。

```
<AC> system-view
[AC] dhcp enable
```

VLAN-interface 10 および VLAN-interface 20 の IP アドレスを指定する。

```
[AC] interface vlan-interface 10
[AC-Vlan-interface10] ip address 10.1.1.2 24
[AC-Vlan-interface10] quit
[AC] interface vlan-interface 20
[AC-Vlan-interface20] ip address 10.10.1.1 24
```

VLAN-interface 20 で DHCP リレーエージェントを有効にする。

```
[AC-Vlan-interface20] dhcp select relay
```

DHCP リレーエージェントに DHCP サーバアドレス 10.1.1.1 を指定する。

```
[AC-Vlan-interface20] dhcp relay server-address 10.1.1.1
```

VLAN インタフェース 20 で authorized ARP を有効にする。

```
[AC-Vlan-interface20] arp authorized enable
[AC-Vlan-interface20] quit
```

DHCP リレーエージェントへのリレーエントリの記録を有効にする。

```
[AC] dhcp relay client-information record
```

3)　設定の確認

#AC で authorized ARP エントリ情報を表示する。

```
[AC] display arp
  Type: S-Static   D-Dynamic   O-Openflow   R-Rule  I-Invalid
IP address      MAC address    VLAN/VSI name Interface/Link ID        Aging
Type
10.10.1.2       0012-3f86-e94c --           GE1/0/2                  20    D
```

IP アドレス 10.10.1.2 がクライアントに割り当てられていることを示しています。

クライアントは、AC と通信するために、authorized ARP エントリの IP アドレスと MAC アドレスを使用する必要があります。それ以外の場合、通信は失敗します。これにより、ユーザの妥当性が確保されます。

10.9 ARP アタックdetectionの設定

ARP アタック detection 機能は、ユーザやゲートウェイのなりすまし攻撃を防ぐため、許可されていないクライアントの ARP パケットをブロックするようにアクセス装置で有効にします。ARP detection 機能は ARP トラステッドポートから受信した ARP パケットを確認しません。

ARP アタック detection 機能は、以下の特徴があります。

- ユーザの正当性確認
- ARP パケットの正当性の確認
- ARP 制限転送
- ユーザ有効性チェック中に無視される ARP パケット入力ポート
- ARP 攻撃検出のログ

ARP パケットの正当性とユーザの正当性の両方が有効である場合、最初に ARP パケットの正当性の確認を行い、次にユーザの正当性の確認を行います。

ARP snooping と ARP アタック detection を同時に設定しないでください。同時に設定した場合、ARP snooping エントリを生成できません。

10.9.1 制約事項とガイドライン

レイヤ 2 イーサネットインタフェースは、インタフェースまたはインタフェースが属する VLAN で ARP アタック detection を有効にした後、ARP アタック detection が有効になります。

レイヤ 2 イーサネットインタフェースは、インタフェースとそのインタフェースが属する VLAN の両方で ARP アタック detection を無効にした場合にのみ、ARP アタック detection で無効になります。

レイヤ 2 イーサネットインタフェースの両方で ARP アタック detection が有効になっていて、ARP 信頼ポートとして設定されている場合、ARP 信頼ポートの設定が有効になります。デバイスイーサネットインタフェースパケットに対して ARP アタック detection を実行しません。

10.9.2 ユーザの正当性の確認の設定

以下の順に受信 ARP パケットの送信元 IP アドレスと送信元 MAC アドレスを比較します。

- ユーザの正当性確認のルール
  - □ 一致した場合、装置はルールに従って ARP パケットを処理します。
  - □ 一致するアドレスがない場合や、ユーザの正当性確認が設定されていない場合、以下の処理をします。
- DHCP スヌーピングエントリ
  - □ 一致が見つかった場合、デバイスは ARP パケットが有効であると判断します。次に、デバイスはターゲット IP アドレスを含むエントリを検索することでパケットを転送します。
    - ➢ 一致が見つかり、受信インタフェースが、一致する送信者 IP アドレスを持つエントリ内のインタフェースと異なる場合、デバイスはレイヤ 3 転送を実行します。
    - ➢ 一致が見つかったが、受信インタフェースが、一致する送信者 IP アドレスを持つエントリ内のインタフェースと同じである場合、デバイスはレイヤ 2 転送を実行します。
    - ➢ 一致するものが見つからない場合、デバイスはレイヤ 2 転送を実行します。
  - □ 一致するアドレスがなかった場合、装置は ARP パケットを廃棄します。

DHCP スヌーピングエントリは、DHCP スヌーピングによって自動的に生成されます。

10.9.3 設定ガイドライン

以下の 1 つ以上のアイテムが設定されていることを確認してください。

- ユーザの正当性確認ルール
- DHCP スヌーピング

どのアイテムも設定されていない場合、ARP untrusted インタフェース上のすべての受信 ARP パケットを転送します。

IP ソース ガード バインディングに対して ARP アタック detection が有効になっている IP アドレス、MAC アドレス、および VLAN を指定します。 そうしないと、IP ソース ガード バインディングに一致する ARP パケットはありません。

10.9.4 設定手順

I. ユーザ有効性チェックルールの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. ユーザ妥当性チェックルールを設定する	**arp detection rule** *rule-id* { **deny** | **permit** } **ip** { *ip-address* [*mask*] | **any** } **mac** { *mac-address* [*mask*] | **any** } [**vlan** *vlan-id*]	デフォルト：設定なし

II. VLAN での ARP アタック detection の有効化

操作	コマンド	補足
3． system view に移行する	**system-view**	―
4． VLAN view に移行する	**vlan** *vlan-id*	―
5． ARP detection を有効にする	**arp detection enable**	デフォルト：無効
6． system view に戻る	**quit**	―
7． Ethernet interface view あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	―
8． （オプション設定項目） ARP 検出を除外するトラステッドインタフェースとして設定する	**arp detection trust**	デフォルト：非トラステッドインタフェース

10.9.5 ARP パケット正当性の確認の設定

非トラステッドポートで受信された ARP パケットが正当かどうか確認を行い、以下のオブジェクトについて指定します。

- **src-mac**–ARP パケットのメッセージ部分にある送信元 MAC アドレスが、イーサネットヘッダの送信元 MAC アドレスと一致するかどうか確認します。一致する場合には通過、そうでなければパケットは廃棄されます。
- **dst-mac**–ARP 応答の宛先 MAC アドレスを確認します。宛先 MAC アドレスがすべて 0、すべて 1、あるいはイーサネットヘッダの宛先 MAC アドレスと矛盾する場合、パケットは無効と判断され廃棄されます。
- **ip**–ARP 応答の送信元 IP アドレスと宛先 IP アドレスを確認します。すべて 0、すべて 1、あるいはマルチキャスト IP アドレスである場合、パケットは無効と判断して廃棄されます。

以下に ARP パケット正当性の確認の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． VLAN view に移行する	**vlan** *vlan-id*	―
3． ARP detection を有効にする	**arp detection enable**	デフォルト：無効
4． system view に戻る	**quit**	―
5． ARP パケット正当性の確認を有効にし、オブジェクトを指定する	**arp detection validate** { **dst-mac** | **ip** | **src-mac** } *	デフォルト：無効
6． Ethernet interface view あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	―
7． （オプション設定項目） ARP 検出を除外するトラステッドインタフェースとして設定する	**arp detection trust**	デフォルト：非トラステッドインタフェース

10.9.6 ARP 制限転送の設定

🕮 **メモ：**

ARP 制限転送は宛先 MAC アドレスのようなマルチポート MAC アドレスの ARP パケットには適用されません。

ARP 制限転送は、非トラステッドインタフェースで受信され、ユーザの正当性の確認をパスした ARP パケットの転送を以下のように制御します。

- パケットが ARP 要求である場合、トラステッドインタフェースを通して転送されます。
- パケットが ARP 応答である場合、宛先 MAC アドレスに従って転送されます。MAC アドレステーブル内に一致するアドレスがない場合、トラステッドインタフェースを通して転送されます。

ARP 制限転送の設定をする前に、ユーザの正当性の確認の設定を行ってください。

以下に ARP 制限転送の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． VLAN view に移行する	**vlan** *vlan-id*	―
3． ARP 制限転送を有効にする	**arp restricted-forwarding enable**	デフォルト：無効

10.9.7 ユーザ妥当性チェック中に ARP パケットの入力ポートを無視する

ARP アタック detection は、ARP の信頼できないインタフェースからの ARP パケットに対してユーザ妥当性チェックを実行します。受信した ARP パケットの送信者 IP と送信者 MAC は、ユーザ妥当性チェックに使用されるエントリと比較されます。さらに、ユーザ妥当性チェックでは、ARP パケットの入力ポートとエントリのポートが比較されます。一致するポートが見つからない場合、ARP パケットは廃棄されます。ユーザ有効性チェックの詳細については、 本章の“*ユーザの正当性の確認の設定*” を参照してください。

ユーザ有効性チェック中に ARP パケットの入力ポートを無視するようにデバイスを設定できます。ARP パケットがユーザ有効性チェックに合格すると、デバイスはパケットのレイヤ 2 転送を直接実行します。ARP パケットのターゲット IP アドレスによって、一致するスタティック IPSG バインディング、802.1 X セキュリティエントリ、DHCP スヌーピングエントリを検索しなくなりました。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． ユーザ妥当性チェック中に ARP パケットの入力ポートを無視する	**arp detection port-match-ignore**	デフォルト：無視しません

10.9.8 ARP アタック detection ログの有効化

ARP アタック detection ログ機能を使用すると、デバイスは不正な ARP パケットが検出されたときに ARP アタック detection ログメッセージを生成できます。ARP アタック detection ログメッセージには、次の情報が含まれます。

- ARP パケットの受信インタフェース
- 送信元 IP アドレス
- ドロップされた ARP パケットの総数

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. ARP アタック detection ログを有効にする	**arp detection log enable** [**interval** *interval* | **number** *number* | **threshold** *threshold-value*]*	デフォルト：無効

10.9.9 ARP アタック detection の表示と維持

すべての view で **display** コマンドを実行することができ、user view で **reset** コマンドを実行することができます。

操作	コマンド
ARP detectionが有効なVLANを表示する	**display arp detection**
ARP攻撃元の統計情報を表示する	**display arp detection statistics attack-source**
ARP攻撃元の統計情報を表示する	**display arp detection statistics attack-source chassis** *chassis-number* **slot** *slot-number*
ARP攻撃元の統計情報をクリアする	**reset arp detection statistics attack-source**

10.9.10 ユーザの正当性の確認の設定例

I. ネットワーク要件

図 10-4 に示すように、Client に対する 802.1X セキュリティエントリに基づき、ARP パケット正当性チェックとユーザ正当性チェックを実行するように AC を設定します。

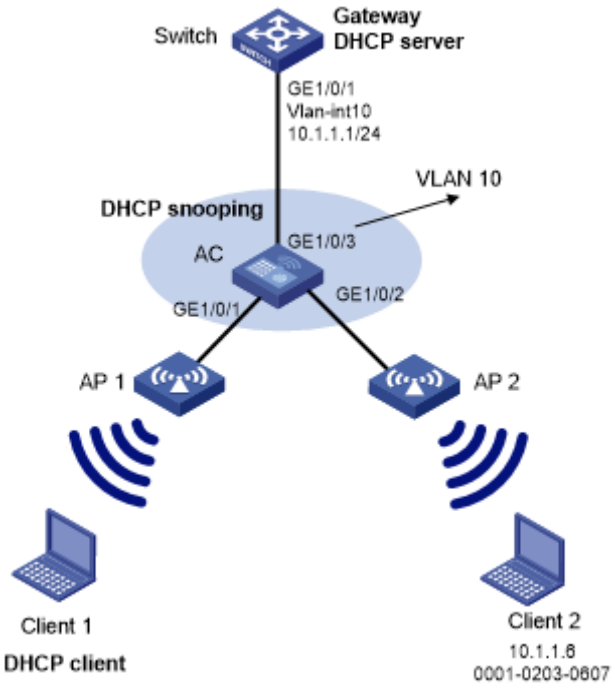


図 10-4 ネットワーク図

II. 設定手順

1) AC のすべてのインタフェースに VLAN10 を追加し、Switch の VLAN インタフェース 10 の IP アドレスを設定します。（詳細は省略します。）
2) Switch の DHCP サーバを設定し、DHCP アドレスプール 0 を設定します。

```
<Switch> system-view
[Switch] dhcp enable
[Switch] dhcp server ip-pool 0
[Switch-dhcp-pool-0] network 10.1.1.0 mask 255.255.255.0
```

3) Client 1 と Client 2 を 802.1X クライアントに設定し、ARP アタック detection の IP アドレスをアップロードするよう設定します。（詳細は省略します。）
4) AC を設定します。

802.1X を有効にします。

```
<AC> system-view
[AC] dot1x authentication-method chap
```

ISP ドメイン local を作成し、ISP domain view に移行します。

```
[AC] domain local
```

#LAN クライアント用にローカル認証、許可、アカウンティングを ISP ドメインに設定します。

```
[AC-isp-local] authentication lan-access local
[AC-isp-local] authorization lan-access local
```

```
[AC-isp-local] accounting lan-access local
[AC-isp-local] quit
```

サービステンプレート wlas_local_chap を作成し、その view に移行します。

```
[AC] wlan service-template wlas_local_chap
```

認証モードを 802.1X に設定します。

```
[AC-wlan-st-wlas_local_chap] client-security authentication-mode dot1x
```

サービステンプレート local を設定します。

```
[AC-wlan-st-wlas_local_chap] dot1x domain local
```

wlas_local_chap に SSID を設定します。

```
[AC-wlan-st-wlas_local_chap] ssid wlas_local_chap
```

サービステンプレートを有効にします。

```
[AC-wlan-st-wlas_local_chap] service-template enable
[AC-wlan-st-wlas_local_chap] quit
```

ap1 を作成し、AP モデル、シリアル ID を設定します。

```
[AC] wlan ap ap1 model QX-W1020
[AC-wlan-ap-ap 1] serial-id 210235A1BSC123000050
[AC-wlan-ap-ap 1] quit
```

AP の radio1 の動作チャネル 64 を設定し、radio 1 を有効にします。

```
[AC] wlan ap ap1
[AC-wlan-ap-ap1] radio 1
[AC-wlan-ap-ap1-radio-1] channel 64
[AC-wlan-ap-ap1-radio-1] radio enable
```

サービステンプレート wlas_local_chap を radio 1 に関連づけます。

```
[AC-wlan-ap-ap1-radio-1] service-template wlas_local_chap
[AC-wlan-ap-ap1-radio-1] quit
[AC-wlan-ap-ap1] quit
```

ネットワークアクセスユーザ test を追加します。

```
[AC] local-user test class network
[AC-luser-network-test] service-type lan-access
[AC-luser-network-test] password simple test
[AC-luser-network-test] quit
```

VLAN 10 の ARP アタック detection を有効にし、802.1X エントリをもとにしたユーザの正当性の確認を行います。

```
[AC] vlan 10
[AC-vlan10] arp detection enable
```

#ARP トラステッドインタフェースとして上流のインタフェースを設定します。デフォルトでインタフェースは非トラステッドインタフェースです。

```
[AC-vlan10] interface gigabitethernet 1/0/3
[AC-GigabitEthernet1/0/3] arp detection trust
[AC-GigabitEthernet1/0/3] quit
```

設定を行った後、GigabitEthernet 1/0/1 と、GigabitEthernet 1/0/2 で受信した ARP パケットが 802.1X エントリに対して確認を行います。

10.10 ARPスキャンと固定ARPの設定

ARP スキャンは通常、小規模で安定したネットワークで固定 ARP 機能とともに使用されます。

ARP スキャンは、アドレス範囲内のデバイスの ARP エントリを自動的に作成します。デバイスは、次の手順で ARP スキャンを実行します。

1. アドレス範囲内の各 IP アドレスに対して ARP 要求を送信します。
2. 受信した ARP 応答を通じて MAC アドレスを取得します。
3. ダイナミック ARP エントリを作成します。

自動 ARP スキャンを有効にすると、デバイスは arp scan auto send-rate コマンドを使用して設定されたレートで、指定されたスキャン範囲内のすべての IP アドレスに定期的に ARP 要求を送信します。

スキャン範囲に多数の IP アドレスがある場合は、ARP パケット送信レートを制限できます。これにより、ARP トラフィックのバーストによる CPU 使用率とネットワーク負荷の高騰を回避できます。

ARP 要求の送信にスキャン範囲と送信元アドレスを指定すると、インタフェースはスキャン範囲内のすべての IP アドレスをスキャンします。スキャン範囲のみを指定した場合、インタフェースはスキャン範囲とインタフェースのサブネットアドレスの両方に属する IP アドレスをスキャンします。

固定 ARP は、既存のダイナミック ARP エントリ (ARP スキャンによって生成されたものを含む) をスタティック ARP エントリに変換します。これらのスタティック ARP エントリは、手動で設定された ARP エントリと同じ属性です。この機能により、ARP エントリが攻撃者によって変更されることを防ぎます。

I. 制限とガイドライン

既存の ARP エントリの IP アドレスはスキャンされません。

ARP スキャンをトリガーし、自動 ARP スキャンを有効にすると、両方が有効になります。ベストプラクティスとして、自動 ARP スキャンは、ユーザがオンラインになり、頻繁にオフラインになるネットワークでのみ使用します。

スタティック ARP エントリの合計数の制限により、一部のダイナミック ARP エントリが変換に失敗する可能性があります。

arp fixup コマンドは 1 回限りの操作です。このコマンドを再度使用して、後で学習したダイナミック ARP エントリをスタティックに変換できます。

ダイナミック ARP エントリから変換されたスタティック ARP エントリを削除するには、undo arp ip-address コマンドを使用します。また、reset arp all コマンドを使用してすべての ARP エントリを削除したり、reset arp static コマンドを使用してすべてのスタティック ARP エントリを削除したりすることもできます。

10.10.1 ARP スキャンの開始

操作	コマンド
1． system view に移行する	**system-view**
2． インタフェース view に移行する	**interface** *interface-type interface-number*
3． ARP スキャンを開始する	**arp scan** [*start-ip-address* **to** *end-ip-address*]

注意：

ARP スキャンには時間がかかります。進行中のスキャンを停止するには、Ctrl+C を押します。スキャンが終了する前に受信した ARP 応答に基づいてダイナミック ARP エントリが作成されます。

10.10.2 自動 ARP スキャンの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． 自動 ARP スキャンの ARP パケット送信レートを設定する	**arp scan auto send-rate** { **ppm** *ppm* | *pps* }	デフォルト：48pps
3． interface view に移行する	**interface** *interface-type interface-number*	―
4． 自動 ARP スキャンを有効にする	**arp scan auto enable** [*start-ip-address* **to** *end-ip-address* [**source-addr** *source-ip-address*]]	デフォルト：無効

10.10.3 固定 ARP の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． 既存のダイナミック ARP エントリをスタティック ARP エントリに変換する	**arp fixup**	ARP 変換は 1 回限りの操作です

🕮 **メモ：**

arp fixup コマンドを使用して、学習したダイナミック ARP エントリをスタティックに変換できます。
ダイナミック ARP エントリから変換されたスタティック ARP エントリには、手動で設定されたスタティック ARP エントリと同じ属性です。 スタティック ARP エントリの総数に対するデバイスの制限により、一部のダイナミック ARP エントリは変換に失敗する場合があります。
変換後のスタティック ARP エントリには、次のエントリを含めることができます。

- 変換前の既存のダイナミックおよびスタティック ARP エントリ
- 変換中に学習した新しいダイナミック ARP エントリ
- 変換中に期限切れになったダイナミック ARP エントリは、スタティック ARP エントリに変換されません。

ダイナミック ARP エントリから変更されたスタティック ARP エントリを削除するには、**undo arp ip-address** コマンドを使用します。 このようなスタティック ARP エントリをすべて削除するには、**reset arp all** または **reset arp static** コマンドを使用します。

10.11 ARP送信者IPアドレスチェックの設定

この機能により、ゲートウェイは ARP 学習の前に VLAN 内の ARP パケットの送信者 IP アドレスを確認できます。送信者 IP アドレスが許可された IP アドレス範囲内にある場合、ゲートウェイは ARP 学習を続行します。送信者 IP アドレスが範囲外の場合、ゲートウェイは ARP パケットを攻撃パケットと判断して廃棄します。

10.11.1 設定ガイドライン

VLAN がサブ VLAN であり、スーパーVLAN に関連付けられている場合、このチェック機能はサブ VLAN でのみ設定します。

プライマリ VLAN に関連付けられたセカンダリ VLAN 間でレイヤ 3 通信が設定されている場合、この機能はプライマリ VLAN で設定します。プライマリ VLAN に関連付けられたセカンダリ VLAN 間でレイヤ 3 通信が設定されていない場合、目的の VLAN でこの機能を設定します。

10.11.2 設定手順

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． vlan view に移行する	**vlan** *vlan-id*	―
3． ARP 送信者 IP アドレスチェック機能を有効にし、IP アドレス範囲を指定する	**arp sender-ip-range** *start-ip-address end-ip-address*	デフォルト：無効

QX-W2300AC シリーズ アクセスコントローラ

オペレーションマニュアル

16. 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 の概要
02- QoS ポリシー
03-プライオリティマッピング
04-トラフィックポリシング
05-トラフィックフィルタリング
06-プライオリティマーキング
07-付録
08-WLAN QoS

目次

このセクションのページは **16-x-x** です。

1章 QoSの概要 1-1
1.1 QoSサービスモデル 1-1
1.1.1 ベストエフォートサービスモデル 1-1
1.1.2 IntServモデル 1-1
1.1.3 DiffServモデル 1-2
1.2 QoS技術の概要 1-2
1.2.1 ネットワークのQoS技術の展開 1-2
1.2.2 装置のQoS処理フロー 1-3
1.2.3 QoS設定のアプローチ 1-3

1章 QoS の概要

QoS（Quality of Service）は、ネットワークトラフィックのフォワーディングプロセスで帯域幅、遅延、パケットロスに関与します。帯域の保証や、遅延、ジッタ、パケットロス率等の低減を行うことによって、QoS の向上ができます。

QoS でトラフィックの優先度付けを行い、各トラフィックに対するネットワークリソースの割り当てを考慮する必要があります。

本章では、QoS サービスモデルと広く使用される QoS の技術を紹介します。

1.1 QoSサービスモデル

この章では一般的な QoS サービスモデルについて説明します。

1.1.1 ベストエフォートサービスモデル

ベストエフォートモデルは、単独のサービスモデルです。最も簡単なサービスモデルです。ベストエフォートサービスモデルは、他のモデルに比べて信頼性は低くなり、遅延や信頼性などの保証はしません。

ベストエフォートサービスモデルは、インターネットでのデフォルトのモデルです。ほとんどのネットワークアプリケーションに適用され、FIFO（First In First Out）キューイングとして実装されます。

1.1.2 IntServ モデル

IntServ（integrated service）は、複数の多様な QoS 要件に適用できる多重サービスモデルです。このモデルは、各データフローに QoS を保証、識別することができ、きめ細かく差別化された QoS を提供します。

IntServ モデルでは、データを送信する前にアプリケーション上で、特定の種類のサービスを使用できるようにネットワークへ要求する必要があります。IntServ の要求は、RSVP シグナリングによって行われます。RSVP は、送信元から宛先までの装置で動作し、データフローがあらかじめ要求/予約したリソースより多くのリソースを使わないよう、各アプリケーションフローをモニタします。

IntServ は装置の高い処理能力が必要となります。IntServ モデルはネットワークへの大量のデータトラフィックが、ストレージデバイスの処理能力に非常に大きな負担がかかります。したがって多くのデータフローが流れるコアインターネット網や何百万のフローが流れるネットワークなどの大規模のネットワークでは利用されず、IntServ モデルは中小規模のネットワークで利用されます。

1.1.3 DiffServ モデル

DiffServ（differentiated service）は、多様な QoS 要件を満たせる多重サービスモデルです。IntServ とは異なり、DiffServ はデータを送信する前に、アプリケーションからネットワークに信号に出す必要がありません。DiffServ は、実行や拡張が容易に行えます。

1.2 QoS技術の概要

QoS 技術には以下の機能があります。

- トラフィックの分類
- トラフィックポリシング
- トラフィックシェーピング
- レート制限
- 輻輳管理
- 輻輳回避

このマニュアルに記載するすべての QoS 技術は、DiffServ モデルにもとづいています。

1.2.1 ネットワークの QoS 技術の展開

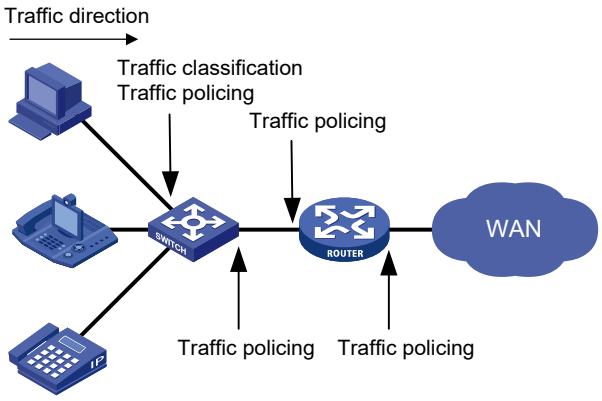


図 1-1 ネットワークの QoS 技術の位置

図 1-1に示すように、以下にトラフィックの分類、トラフィックポリシーの主要な機能を実装します。

- **トラフィックの分類**－異なった特性、異なったクラスのパケットを組織化するために、ある評価基準を使用します。トラフィックの分類にもとづいて、差別化されたサービスを提供することができます。
- **トラフィックポリシング**－トラフィックが設定したしきい値を超えたとき、ネットワークリソースの過剰使用を防ぐため、フローの制限等の対策を施行できます。トラフィックポリシーは、ポートの入力トラフィック、出力トラフィックの双方向に適用できます。

- **トラフィックシェーピング**－トラフィックの出力レートをダウンストリームデバイスで使用可能なネットワークリソースに適応させ、パケットドロップを排除します。トラフィックシェーピングは通常、ポートの発信トラフィックに適用されます。
- **輻輳管理**－輻輳発生時にパケット転送シーケンスを決定するリソーススケジューリングポリシーを提供します。通常、輻輳管理はポートの発信トラフィックに適用されます。
- **輻輳回避**－ネットワークリソースの使用状況を監視します。通常、ポートの発信トラフィックに適用されます。輻輳が悪化すると、輻輳回避はパケットをドロップすることによってキューの長さを短縮します。

1.2.2 装置の QoS 処理フロー

図 1-2に示すように QoS モジュールはトラフィックの処理を行います。

1) トラフィックの分類処理は、後続の QoS アクションを行うため、トラフィックを識別し、分類します。
2) QoS モジュールはトラフィック処理プロセスフェーズとネットワークの状態に従い、分類されたトラフィックでさまざまな QoS アクションを行います。たとえば、入力トラフィックのトラフィックポリシーを実行するように QoS モジュールを設定できます。

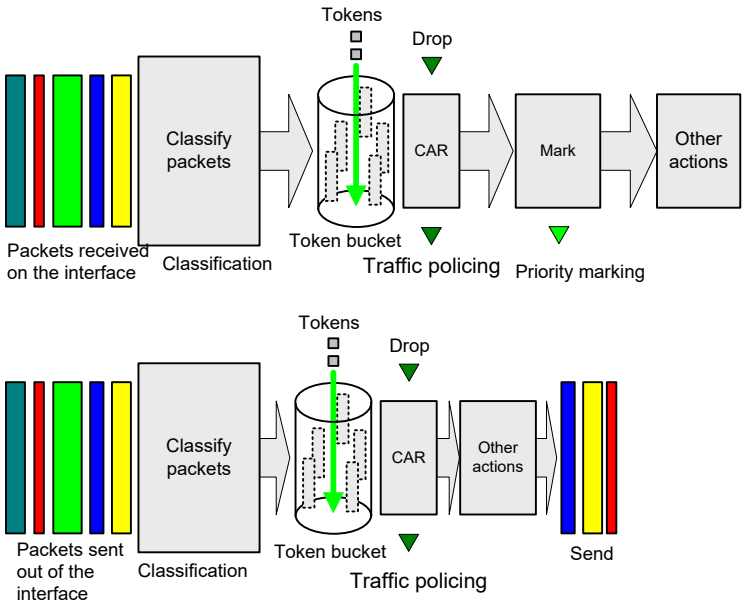


図 1-2 QoS 処理フロー

1.2.3 QoS 設定のアプローチ

MQC(modular QoS configuration)アプローチまたは非 MQC アプローチを使用して QoS を設定できます。

MQC アプローチでは、QoS ポリシーを使用して QoS サービスパラメータを設定します。QoS ポリシーは、さまざまなクラスのトラフィックに対して実行する QoS アクションを定義し、トラフィックを制御するオブジェクト (インターフェイスなど) に適用できます。

非 MQC アプローチでは、QoS ポリシーを使用せずに QoS サービスパラメータを設定します。たとえば、レート制限機能を使用して、QoS ポリシーを使用せずにインターフェイスにレート制限を設定できます。

両方のアプローチをサポートする機能もありますが、一方だけをサポートする機能もあります。

目次

このセクションのページは **16-x-x** です。

2 章 QoS ポリシー 2-1
2.1 QoS ポリシーのタスク 2-1
2.2 トラフィッククラスの定義 2-1
2.3 トラフィック動作の定義 2-1
2.4 QoS ポリシーの定義 2-2
2.5 QoS ポリシーの適用 2-2
2.5.1 インタフェースへの QoS ポリシーの適用 2-3
2.5.2 ユーザプロファイルへの QoS ポリシーの適用 2-3
2.6 インタフェースの QoS ポリシーのトラフィックレート統計情報収集期間の設定 2-3
2.7 QoS ポリシーの情報表示と維持 2-4

2章 QoS ポリシー

QoS ポリシーには、次のコンポーネントがあります。

- **トラフィッククラス**－パケットを照合する基準を定義します。
- **トラフィック動作**－一致するパケットに対して実行する QoS アクションを定義します。

トラフィッククラスをトラフィック動作に関連付けることで、QoS ポリシーは一致するパケットに対して QoS アクションを実行できます。

QoS ポリシーは、複数のクラス動作アソシエーションを持つことができます。

2.1 QoSポリシーのタスク

作業リスト
トラフィッククラスの定義
トラフィック動作の定義
QoSポリシーの定義
QoSポリシーの適用 インタフェースへのQoSポリシーの適用 ユーザプロファイルへのQoSポリシーの適用
(オプション設定項目)インタフェースのQoSポリシーのトラフィックレート統計情報収集期間の設定

2.2 トラフィッククラスの定義

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. トラフィッククラスを作成し、演算子を定義して class view に移行する	**traffic classifier** *classifier-name* [**operator** { **and** | **or** }]	デフォルト：設定なし
3. (オプション設定項目) トラフィッククラスの説明を設定する	**description** *text*	デフォルト：設定なし
4. 一致条件を設定する	**if-match** *match-criteria*	デフォルト：設定なし

2.3 トラフィック動作の定義

トラフィック動作でトラフィックフィルタリング、トラフィックポリシー、プライオリティマーキング等の QoS の動作を定義します。

以下にトラフィック動作の設定手順を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． トラフィック動作を作成し traffic behavior view に移行する	**traffic behavior** *behavior-name*	デフォルト：設定なし
3． QoS の動作を定義する	トラフィックポリシー、トラフィックフィルタリング、プライオリティマーキングなどのトラフィック動作の目的に応じて、QX-W2300ACシリーズアクセスコントローラオペレーションマニュアルの“*16 QoS*”を参照してください。	デフォルト：設定なし

2.4 QoSポリシーの定義

トラフィック動作を QoS ポリシーのトラフィッククラスに関連づけます。トラフィック動作は、クラスの一致条件にマッチしたパケットに実行されます。

トラフィッククラス定義のために QoS ポリシーによって ACL が参照された場合は、ACL のアクション（許可あるいは拒否）に従って処理されます。アクションはトラフィック動作に関連づけられたものが使われます。

クラスとトラフィック動作の関連づけ手順を以下に示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． QoS ポリシーを作成し、qos policy view に移行する	**qos policy** *policy-name*	デフォルト：設定なし
3． トラフィッククラスとトラフィック動作を関連づける	**classifier** *classifier-name* **behavior** *behavior-name* [**insert-before** *before-classifier-name*]	デフォルト：設定なし 複数、作成する場合、コマンドを繰り返してください。

2.5 QoSポリシーの適用

QoS ポリシーは以下の種類に適用できます。

- **インタフェース**－QoS ポリシーはインタフェースで送受信したトラフィックに適用します。
- **ユーザプロファイル**－QoS ポリシーはユーザプロファイルのオンラインユーザが送受信するトラフィックに適用できます。

QoS ポリシーを適用している場合、QoS ポリシーを適用した後でも QoS ポリシーのトラフィッククラス、トラフィック動作、トラフィッククラスとトラフィッククラスの関連づけの設定を修正できます。トラフィッククラスがトラフィックの分類の ACL を参照する場合、ACL を削除あるいは修正できます。（たとえば、ACL のルールへの追加、削除、修正です）

2.5.1 インタフェースへの QoS ポリシーの適用

1 つの QoS ポリシーを複数のインタフェースに適用できますが、インタフェースの 1 つの方向（インバウンド/アウトバウンド）に適用できる QoS ポリシーは 1 つのみです。

インタフェースの出力トラフィックに適用された QoS ポリシーはローカルパケットに適用されません。ローカルパケットは、装置の正常動作を維持するためのパケットです。一般的なローカルパケットはリンクのメンテナンスパケットやルーティング、SSH パケットがあります。

以下にインタフェースへの QoS ポリシーの適用手順を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． interface view に移行する	**interface** *interface-type interface-number*	―
3． QoS ポリシーを適用する	**qos apply policy** *policy-name* { **inbound** | **outbound** }	デフォルト：設定なし

2.5.2 ユーザプロファイルへの QoS ポリシーの適用

ユーザプロファイルを設定すると、ユーザに基づいてトラフィックポリシングを実行できます。ユーザが認証に合格すると、認証サーバはユーザに関連付けられたユーザプロファイルの名前をデバイスに送信します。ユーザプロファイルビューで設定された QoS ポリシーは、ユーザがオンラインになったときにのみ有効になります。

I. 制限とガイドライン

QoS ポリシーは、複数のユーザプロファイルに適用できます。各ユーザプロファイルの一方向では、1 つのポリシーのみを適用できます。方向にすでに適用されている QoS ポリシーを変更するには、まず適用されている QoS ポリシーを削除します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． ユーザプロファイル view に移行する	**user-profile** *profile-name*	―
3． QoS ポリシーを適用する	**qos apply policy** *policy-name* { **inbound** | **outbound** }	デフォルト：設定なし

2.6 インタフェースのQoSポリシーのトラフィックレート統計情報収集期間の設定

平均転送レートやドロップレートなど、一定期間のクラスごとのトラフィック統計情報の収集を有効にできます。たとえば、統計情報収集期間を n 分に設定すると、システムは次の操作を実行します。

- 最新の n 分のトラフィック統計情報を収集します。

- n/5 分ごとに統計情報を更新します。

display qos policy interface コマンドで、収集したトラフィックレート統計情報を確認できます。

I. 制限とガイドライン

サブインターフェイスは、メインインターフェイスで設定された統計情報収集期間を使用します。

操作	コマンド	補足
4． system view に移行する	**system-view**	—
5． インタフェース view に移行する	**interface** *interface-type interface-number*	—
6． インタフェースのトラフィックレート統計情報収集期間を設定する	**qos flow-interval** *interval*	デフォルト：5分

2.7 QoSポリシーの情報表示と維持

すべての view で **display** コマンドを実行でき、user view で **reset** コマンドを実行できます。

操作	コマンド
トラフィッククラスの設定情報を表示する	**display traffic classifier user-defined** [*classifier-name*]
トラフィック動作についての情報を表示する	**display traffic behavior user-defined** [*behavior-name*]
QoSポリシーの設定を表示する	**display qos policy user-defined** [*policy-name* [**classifier** *classifier-name*]]
指定したinterface、あるいはすべてのinterfaceのQoSポリシーの設定を表示する	**display qos policy interface** [*interface-type interface-number*] [**inbound** | **outbound**]

目次

このセクションのページは **16-x-x** です。

3章 プライオリティマッピング 3-1
3.1 概要 3-1
3.1.1 プライオリティの導入 3-1
3.1.2 プライオリティマッピング 3-1
3.2 プライオリティマッピングの設定作業リスト 3-2
3.3 プライオリティマッピングの設定 3-2
3.4 プライオリティマッピングのパケットプライオリティを信用するインタフェースの設定3-3
3.5 インタフェースのポートプライオリティの変更 3-3
3.6 プライオリティマッピングの表示と維持 3-4

3章 プライオリティマッピング

3.1 概要

パケットを受信すると、装置は以下のいずれかのプライオリティにもとづいて QoS プライオリティのパラメータを転送するパケットに上書きします。

- パケットに含まれているプライオリティのフィールドの値
- 入力ポートのポートプライオリティ

このプロセスはプライオリティマッピングと呼ばれます。このプロセスの間、装置はプライオリティマッピングのルールに従ってパケットのプライオリティを修正することができます。QoS プライオリティのパラメータはパケットのスケジュールプライオリティとフォワーディングプライオリティを決めます。

プライオリティマッピングはプライオリティマッピングテーブルに実装され、以下のプライオリティを決定します。

- 802.11e プライオリティ
- 802.1p プライオリティ
- DSCP
- IP プレシーデンス
- ローカルプレシーデンス
- ドロップ優先順位

3.1.1 プライオリティの導入

プライオリティは、ローカルプライオリティとパケットに含まれているプライオリティと、スケジューリング用にローカルに割り当てられるプライオリティがあります。

パケットに含まれているプライオリティは、802.1p プライオリティ、DSCP プレシーデンス、IP プレシーデンスがあります。パケットに含まれるプライオリティは、他の装置でも使用されるため、ネットワークに影響します。プライオリティの詳細は、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*16 QoS*”の“*7 章 付録*”を参照してください。

ローカルプライオリティは装置内でのみ使用されるため、ネットワークに影響しません。ローカルプライオリティは、ローカルプレシーデンスと呼ばれ、キューのスケジューリング用に使用されます。ローカルプレシーデンスの値は出力キューに対応します。ローカルプレシーデンスの値が高いパケットが高い出力キューに割り当てられます。

3.1.2 プライオリティマッピング

装置はさまざまなプライオリティマッピングのタイプを提供します。プライオリティマッピングは、プライオリティマッピングテーブルを参照し、その後のパケットを処理するため、パケットに割り当てるプライオリティを決定します。

デフォルトのプライオリティマップはプライオリティマッピングに利用できます。デフォルトのマップは、ほとんどの場合において通常に使用することができます。デフォルトのプライオリティマップでは要件を満たすことができない場合、必要に応じてプライオリティのマッピングを変更することができます。デフォルトのプライオリティは、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*16 QoS*”の“*7 章 付録*”を参照してください。

3.2 プライオリティマッピングの設定作業リスト

以下の方法を使用してプライオリティマッピングを設定することができます。

プライオリティマッピングテーブル、ポートのプライオリティのトラステッドモード、ポートプライオリティを変更することによって、プライオリティマッピングを変更することができます。

- **プライオリティのトラステッドモードの設定**－プライオリティマッピングで運ばれた受信パケットのトラステッドプライオリティタイプ（たとえば、802.1p）を検索するために使用するプライオリティを設定することができます。システムはターゲットのプライオリティのタイプと値にトラステッドプライオリティの値をマッピングします。
- **ポートプライオリティの変更**－パケットのプライオリティを信用しない場合、受信パケットのポートプライオリティが使用されます。ポートのポートプライオリティを変更することによって、ポートで受信するパケットのプライオリティを変更します。

プライオリティマッピングを設定するには、以下の手順を実施してください。

作業リスト
（オプション設定項目）プライオリティマッピングの設定
（必須設定項目）いずれか1つを設定してください。 • プライオリティマッピングのパケットプライオリティを信用するインタフェースの設定 • インタフェースのポートプライオリティの変更

3.3 プライオリティマッピングの設定

装置は以下のタイプのプライオリティマッピングを提供します。

プライオリティマッピング	説明
dot11e-lp	802.11e-ローカルプライオリティマッピングテーブルです。
dot1p-lp	802.1p-ローカルプライオリティマッピングテーブルです。
dscp-lp	DSCP-ローカルプライオリティマッピングテーブルです。
lp-dot11e	ローカル-802.11eプライオリティマッピングテーブルです。
lp-dot1p	ローカル-802.1pプライオリティマッピングテーブルです。
lp-dscp	ローカル-DSCPプライオリティマッピングテーブルです。

以下にプライオリティマッピングの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	－

操作	コマンド	補足
2． priority map view に移行する	**qos map-table** { **dot11e-lp** | **dot1p-lp** | **dscp-lp** | **lp-dot11e** | **lp-dot1p** | **lp-dscp** }	―
3． プライオリティマッピングを設定する	**import** *import-value-list* **export** *export-value*	デフォルト：デフォルトのプライオリティマップ 詳細は、QX-W2300ACシリーズアクセスコントローラオペレーションマニュアルの“*16 QoS*”の“*7章 付録*”を参照してください。 新規の設定は、既存に上書きします。

3.4 プライオリティマッピングのパケットプライオリティを信用するインタフェースの設定

インタフェースのプライオリティマッピングのパケットで運ばれた特定のプライオリティフィールドを信用するように装置を設定できます。

インタフェース上で信用できるパケットのプライオリティタイプを設定する場合は、以下の内で使用可能なキーワードを使用します。

- **dot1p**：マッピングのため受信したパケットの802.1pプライオリティを使用します。
- **dscp**：マッピングのため受信したIPパケットのDSCPプレシーデンスを使用します。

プライオリティトラステッドモードの設定手順を以下に示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． interface view に移行する	**interface** *interface-type interface-number*	―
3． パケットプライオリティタイプの信用を設定する	**qos trust** { **dot1p** | **dscp** }	デフォルト：ポートプライオリティを信用する

3.5 インタフェースのポートプライオリティの変更

インタフェースがパケットのプライオリティを信用しない設定の場合、装置は受信したパケットのプライオリティパラメータセットを探すために、自身のポートプライオリティを使用します。ポートプライオリティを変更することで、異なるインタフェースで受信されたトラフィックに優先順位を付けることができます。

ポートプライオリティの変更手順を以下に示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． interface view に移行する	**interface** *interface-type interface-number*	―
3． ポートプライオリティを設定する	**qos priority** *priority-value*	デフォルト：0

3.6 プライオリティマッピングの表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
プライオリティマッピングの設定を表示する	**display qos map-table** [**dot11e-lp** | **dot1p-lp** | **dscp-lp** | **lp-dot11e** | **lp-dot1p** | **lp-dscp**]
ポートに設定されているトラステッドプレシーデンスを表示する	**display qos trust interface** [*interface-type interface-number*]

目次

このセクションのページは **16-x-x** です。

4章 トラフィックポリシング 4-1
4.1 概要 4-1
4.1.1 トラフィックレートの検証とトークンバケット 4-1
4.1.2 トラフィックポリシング 4-2
4.2 トラフィックポリシングの設定 4-3
4.2.1 QoSポリシーを使用したトラフィックポリシングの設定 4-3
4.3 トラフィックポリシングの表示と維持 4-3

4章 トラフィックポリシング

4.1 概要

トラフィックポリシングはネットワークリソース（帯域幅を含みます）の割り当てを手助けし、ネットワーク性能を向上させます。たとえば、パケット転送に使用する帯域幅を制限し保証することで、バーストトラフィックに起因するネットワークの輻輳を回避したりすることができます。

トラフィックポリシングは、特定のトラフィックが割り当てた帯域幅を上回る場合、リソースの使用量を制限します。 トラフィックを検証するには、トークンバケットを使用します。

4.1.1 トラフィックレートの検証とトークンバケット

I. トークンバケットの機能

トークンバケットは、トークンを保持するための一定の容量を持つ容器と見なすことができます。システムは、設定されたレートでトークンをバケットに入れます。トークンバケットが一杯になると、トークンがバケットからあふれます。

II. トークンバケットを使用したトラフィックレートの検証

トラフィックは、バケット内のトークンの数を見て検証します。バケット転送に対して、バケット内のトークンの数に余裕がある場合、以下のように対応します。

- トラフィックは仕様に対応します。（適合トラフィックと呼ばれます）
- 対応するトークンがバケットから取り外されます。

そうでない場合、トラフィックは仕様に対応しません。（余剰トラフィックと呼ばれます）

トークンバケットは以下の設定可能なパラメータがあります。

- **CIR（Committed Information Rate）**－トークンが許可されたトラフィック平均レートによってバケットに入るレートです。
- **CBS（Committed Burst Size）**－バーストサイズあるいはトークンバケットの容量です。各バーストで許可された最大トラフィックサイズです。設定されたバーストサイズは最大パケットサイズよりも大きくする必要があります。

各パケットが到着するたびに検証されます。

III. 複雑な検証

トークンバケットには、以下の設定可能なパラメータがあります。

より複雑な環境でトラフィックを評価し、より多くのポリシーの柔軟性を行うようにトークンバケット（バケット C）を設定することができます。

- **1 レート 2 色**—1 つのトークンバケットと以下のパラメータを使用します。
  - **CIR**（Committed Information Rate）：バケット C に入るトークンのレートです。バケット C によって許可された平均転送レートを設定します。
  - **CBS**（Committed Burst Size）：バケット C のサイズです。バケット C が転送できるトラフィックの転送バーストを設定します。

  パケットが到達するとき、以下のルールに従います。
  - バケット C にパケットを転送するために十分なトークンがある場合、パケットは green に色分けされます。
  - そうでない場合、パケットは red に色分けされます。

4.1.2 トラフィックポリシング

トラフィックポリシングは、入出力トラフィックのポリシーをサポートすることができます。

一般的なトラフィックポリシングのアプリケーションは、ネットワークの特定のトラフィックを監視し、トラフィックを妥当な範囲内で制限します。別のアプリケーションは、ネットワークリソースが積極的に使用しないようにするため、余剰トラフィックの調整を行います。たとえば、HTTP パケットの帯域幅を全体の 50%未満に制限することができます。セッションのトラフィックが制限を超過すると、トラフィックポリシングはパケットの廃棄やパケットの IP プレシーデンスをリセットすることができます。図 4-1にインタフェースの出力トラフィックのポリシングの例を示します。

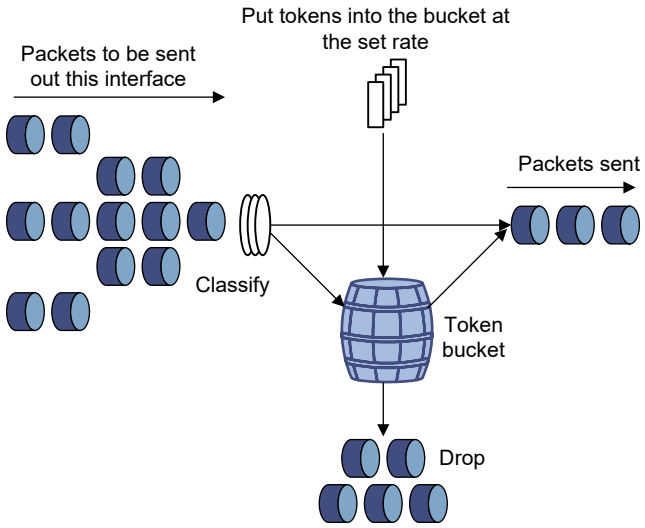


図 4-1 トラフィックポリシング

トラフィックポリシングは、ISP（Internet Service Provider）のネットワークのトラフィックの制限などに広く使用されます。トラフィックポリシングはトラフィックを分類し、検証結果にもとづいて、トラフィックを事前に定義されたトラフィック動作で処理します。トラフィック動作には以下があります。

- 適合トラフィックを転送します。

- 余剰トラフィックを破棄します。

4.2 トラフィックポリシングの設定

インタフェースまたはコントロールプレーンのトラフィックポリシングは、QoS ポリシーを使用することによってのみ設定できます。

4.2.1 QoS ポリシーを使用したトラフィックポリシングの設定

以下に QoS ポリシー（MQC アプローチ）を使用したトラフィックポリシングの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. トラフィッククラスを作成し traffic class view に移行する	**traffic classifier** *classifier-name* [**operator** { **and** | **or** }]	デフォルト：設定なし
3. 一致条件を設定する	**if-match** *match-criteria*	デフォルト：設定なし **if-match**コマンドの詳細は、QX-W2300ACシリーズアクセスコントローラコマンドマニュアルの“*16 QoS*”の“*1章QoSポリシー*”を参照してください。
4. system view に戻る	**quit**	ー
5. トラフィック動作を作成し traffic behavior view に移行する	**traffic behavior** *behavior-name*	デフォルト：設定なし
6. トラフィックポリシングアクションを設定する	**car cir** *committed-information-rate* [**cbs** *committed-burst-size*] [**green** *action* | **red** *action* | **yellow** *action*] *	どちらか一方の設定を行います。 デフォルト：設定なし
7. system view に戻る	**quit**	ー
8. QoS ポリシーを作成し QoS policy view に移行する	**qos policy** *policy-name*	デフォルト：設定なし
9. トラフィック行動とトラフィッククラスを関連づける	**classifier** *classifier-name* **behavior** *behavior-name*	デフォルト：設定なし
10. system view に戻る	**quit**	ー
11. QoS ポリシーを適用する	• インタフェースへ適用	デフォルト：設定なし

4.3 トラフィックポリシングの表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
トラフィック動作の設定を表示する	**display traffic behavior user-defined** [*behavior-name*]

目次

このセクションのページは **16-x-x** です。

5章 トラフィックフィルタリング 5-1
5.1 設定手順 5-1
5.2 設定例 5-2
5.2.1 ネットワーク要件 5-2
5.2.2 設定手順 5-2

5章 トラフィックフィルタリング

トラフィックフィルタリングは、設定したアクションとクラスを組み合わせることにより受信/送信トラフィックをフィルタします。たとえば、ネットワークの状態にしたがって指定した送信元 IP アドレスのパケットをフィルタすることができます。

5.1 設定手順

以下にトラフィックフィルタリングの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． トラフィッククラスを作成し、traffic class view に移行する	**traffic classifier** *classifier-name* [**operator** { **and** | **or** }]	デフォルト：設定なし
3． マッチ条件を設定する	**if-match** *match-criteria*	デフォルト：設定なし
4． system view に戻る	**quit**	―
5． トラフィック動作を作成し、traffic behavior view に移行する	**traffic behavior** *behavior-name*	デフォルト：設定なし
6． トラフィックフィルタリングアクションを設定する	**filter** { **deny** | **permit** }	デフォルト：設定なし
7． system view に戻る	**quit**	―
8． QoS ポリシーを作成し、QoS policy view に移行する	**qos policy** *policy-name*	デフォルト：設定なし
9． トラフィッククラスと QoS ポリシーのトラフィック動作を関連づける	**classifier** *classifier-name* **behavior** *behavior-name*	デフォルト：設定なし
10．system view に戻る	**quit**	―
11．QoS ポリシーを適用する	● VLANにQoSポリシーを適用する	デフォルト：設定なし
12．（オプション設定項目）トラフィックフィルタリングの設定を表示する	**display traffic behavior user-defined** [*behavior-name*]	すべてのviewで実行できます。

5.2 設定例

5.2.1 ネットワーク要件

図 5-1に示すように、GigabitEthernet 1/0/1 で受信し、送信元ポート番号が 21 ではないパケットをフィルタするためにトラフィックフィルタリングを設定します。

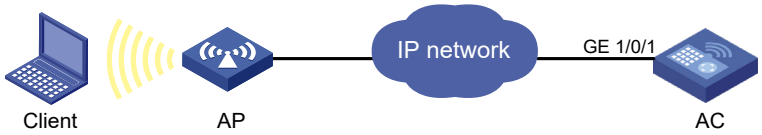


図 5-1 ネットワーク図

5.2.2 設定手順

拡張 ACL 3000 を作成し、送信元ポートが 21 ではないパケットにマッチするルールを設定します。

```
<AC> system-view
[AC] acl advanced 3000
[AC-acl-ipv4-adv-3000] rule 0 permit tcp source-port neq 21
[AC-acl-ipv4-adv-3000] quit
```

トラフィッククラス **classifier_1** を作成し、トラフィッククラスにマッチする条件として ACL 3000 を参照するように設定します。

```
[AC] traffic classifier classifier_1
[AC-classifier-classifier_1] if-match acl 3000
[AC-classifier-classifier_1] quit
```

#トラフィック動作 **behavior_1** を作成し、パケットを廃棄するトラフィックフィルタリングのアクションを設定します。

```
[AC] traffic behavior behavior_1
[AC-behavior-behavior_1] filter deny
[AC-behavior-behavior_1] quit
```

QoS ポリシー**policy** を作成し、トラフィッククラス **classifier_1** とトラフィック動作 **behavior_1** を関連づけます。

```
[AC] qos policy policy
[AC-qospolicy-policy] classifier classifier_1 behavior behavior_1
[AC-qospolicy-policy] quit
```

GigabitEthernet 1/0/1 の入力トラフィックに QoS ポリシー **policy** を適用します。

```
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] qos apply policy policy inbound
```

目次

このセクションのページは **16-x-x** です。

6章 プライオリティマーキング 6-1
6.1 概要 6-1
6.2 設定手順 6-1
6.3 プライオリティマーキングの設定例 6-2
6.3.1 ネットワーク要件 6-2
6.3.2 設定手順 6-3

6章 プライオリティマーキング

6.1 概要

プライオリティマーキングは、トラフィックのプライオリティを変更するためにパケットのプライオリティフィールドまたはフラグビットを設定します。たとえば、パケットを転送するプライオリティを変更する場合、トラフィッククラスの IP プレシーデンスまたは DSCP を設定するプライオリティマーキングを用います。

プライオリティマーキングを設定するために、パケットクラスのプライオリティフィールドあるいはフラグビットを以下のように設定します。

1) トラフィック動作をプライオリティマーキングアクションに設定します。
2) トラフィッククラスをトラフィック動作に関連づけます。

プライオリティマーキングの設定は、プライオリティマッピングと同時に設定することができます。詳細は、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*16 QoS*”の“*3 章 プライオリティマッピング*”を参照してください。

6.2 設定手順

以下にプライオリティマーキングの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. トラフィッククラスを作成し、traffic class view に移行する	**traffic classifier** *classifier-name* [**operator** { **and** | **or** }]	デフォルト：設定なし
3. マッチ条件を設定する	**if-match** *match-criteria*	デフォルト：設定なし **if-match**コマンドの詳細は QX-W2300ACシリーズアクセスコントローラコマンドマニュアルの“*16 QoS*”の“*1 章QoSポリシー*”を参照してください。
4. system view に戻る	**quit**	ー
5. トラフィック動作を作成し、traffic behavior view に移行する	**traffic behavior** *behavior-name*	デフォルト：設定なし

操作	コマンド	補足
6. プライオリティマーキングアクションを設定する	● DSCP値を設定する： **remark dscp** *dscp-value* ● ローカルプレシーデンスを設定する： **remark local-precedence** *local-precedence-value*	1つ以上のいずれかのコマンドを設定します。 デフォルト：設定なし
7. system view に戻る	**quit**	ー
8. QoS ポリシーを作成し、QoS policy view に移行する	**qos policy** *policy-name*	デフォルト：設定なし
9. トラフィッククラスにQoS ポリシーのトラフィック動作を関連付け得る	**classifier** *classifier-name* **behavior** *behavior-name*	デフォルト：設定なし
10. system view に戻る.	**quit**	ー
11. QoS ポリシーを適用する	● インタフェースにQoSポリシーを適用する	デフォルト：設定なし
12. （オプション設定項目）プライオリティマーキングの設定を表示する	**display traffic behavior user-defined** [*behavior-name*]	すべてのviewで実行できます。

6.3 プライオリティマーキングの設定例

6.3.1 ネットワーク要件

図 6-1に示すように、以下の要件を満足するようにプライオリティマーキングを設定します。

トラフィック送信元	宛先	プライオリティ
Client A, B	Data server	High
Client A, B	Mail server	Medium
Client A, B	File server	Low

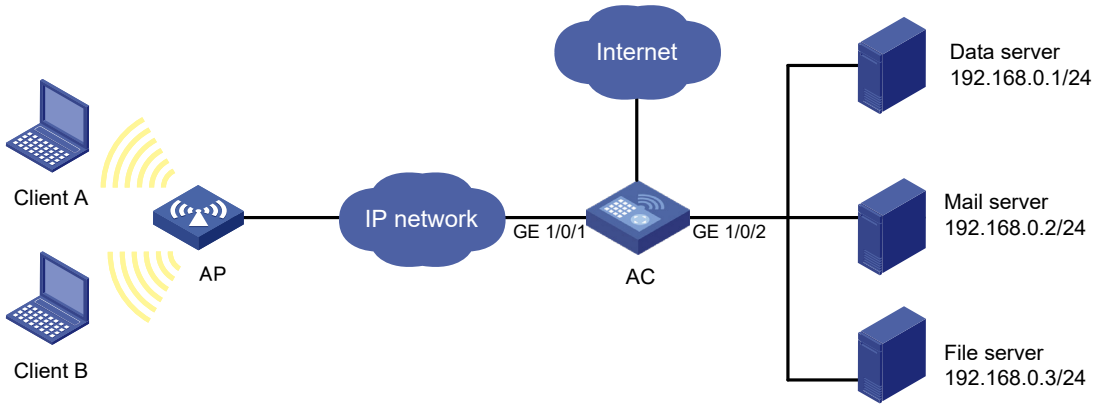


図 6-1 ネットワーク図

6.3.2 設定手順

拡張 ACL 3000 を作成し、宛先 IP アドレス 192.168.0.1 にパケットがマッチするルールを設定します。

```
<AC> system-view
[AC] acl advanced 3000
[AC-acl-ipv4-adv-3000] rule permit ip destination 192.168.0.1 0
[AC-acl-ipv4-adv-3000] quit
```

拡張 ACL 3001 を作成し、宛先 IP アドレス 192.168.0.2 にパケットがマッチするルールを設定します。

```
[AC] acl advanced 3001
[AC-acl-ipv4-adv-3001] rule permit ip destination 192.168.0.2 0
[AC-acl-ipv4-adv-3001] quit
```

拡張 ACL 3002 を作成し、宛先 IP アドレス 192.168.0.3 にパケットがマッチするルールを設定します。

```
[AC] acl advanced 3002
[AC-acl-ipv4-adv-3002] rule permit ip destination 192.168.0.3 0
[AC-acl-ipv4-adv-3002] quit
```

トラフィッククラス **classifier_dbserver** を作成し、トラフィッククラスのマッチ条件に ACL 3000 を適用します。

```
[AC] traffic classifier classifier_dbserver
[AC-classifier-classifier_dbserver] if-match acl 3000
[AC-classifier-classifier_dbserver] quit
```

トラフィッククラス **classifier_mserver** を作成し、トラフィッククラスのマッチ条件に ACL 3001 を適用します。

```
[AC] traffic classifier classifier_mserver
[AC-classifier-classifier_mserver] if-match acl 3001
[AC-classifier-classifier_mserver] quit
```

トラフィッククラス **classifier_fserver** を作成し、トラフィッククラスのマッチ条件に ACL 3002 を適用します。

```
[AC] traffic classifier classifier_fserver
[AC-classifier-classifier_fserver] if-match acl 3002
[AC-classifier-classifier_fserver] quit
```

トラフィック動作 **behavior_dbserver** を作成し、ローカルプレシーデンスの値を 4 としたアクションを設定します。

```
[AC] traffic behavior behavior_dbserver
[AC-behavior-behavior_dbserver] remark local-precedence 4
[AC-behavior-behavior_dbserver] quit
```

トラフィック動作 **behavior_mserver** を作成し、ローカルプレシーデンスの値を 3 としたアクションを設定します。

```
[AC] traffic behavior behavior_mserver
[AC-behavior-behavior_mserver] remark local-precedence 3
[AC-behavior-behavior_mserver] quit
```

トラフィック動作 **behavior_fserver** を作成し、ローカルプレシーデンスの値を 2 としたアクションを設定します。

```
[AC] traffic behavior behavior_fserver
[AC-behavior-behavior_fserver] remark local-precedence 2
[AC-behavior-behavior_fserver] quit
```

QoS ポリシー**policy_server** を作成し、トラフィッククラスを QoS ポリシーのトラフィック動作に関連づけます。

```
[AC] qos policy policy_server
[AC-qospolicy-policy_server] classifier classifier_dbserver behavior behavior_dbserver
[AC-qospolicy-policy_server] classifier classifier_mserver behavior behavior_mserver
[AC-qospolicy-policy_server] classifier classifier_fserver behavior behavior_fserver
[AC-qospolicy-policy_server] quit
```

GigabitEthernet 1/0/1 の入力トラフィックに QoS ポリシー**policy_server** を適用します。

```
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] qos apply policy policy_server inbound
[AC-GigabitEthernet1/0/1] quit
```

目次

このセクションのページは **16-x-x** です。

7章 付録 7-1
7.1 付録A 頭字語 7-1
7.2 付録B デフォルトプライオリティマップ 7-1
7.3 付録C パケットプレシーデンスの概要 7-3
7.3.1 IPプレシーデンスとDSCPフィールドの値 7-3
7.3.2 802.1pプライオリティ 7-4
7.3.3 802.11eプライオリティ 7-5

7章 付録

7.1 付録A 頭字語

頭字語	フルスペル
AF	Assured Forwarding
BE	Best Effort
BQ	Bandwidth Queuing
CAR	Committed Access Rate
CBS	Committed Burst Size
CE	Congestion Experienced
CIR	Committed Information Rate
CQ	Custom Queuing
DCBX	Data Center Bridging Exchange Protocol
DiffServ	Differentiated Service
DSCP	Differentiated Services Code Point
EBS	Excess Burst Size
ECN	Explicit Congestion Notification
EF	Expedited Forwarding
FIFO	First in First out
FQ	Fair Queuing
GMB	Guaranteed Minimum Bandwidth
GTS	Generic Traffic Shaping
IntServ	Integrated Service
ISP	Internet Service Provider
LLQ	Low Latency Queuing
LSP	Label Switched Path
MPLS	Multiprotocol Label Switching
PE	Provider Edge
PIR	Peak Information Rate
PQ	Priority Queuing
PW	Pseudowire
QoS	Quality of Service
QPPB	QoS Policy Propagation Through the Border Gateway Protocol
RED	Random Early Detection
RSVP	Resource Reservation Protocol
RTP	Real-Time Transport Protocol
SP	Strict Priority
ToS	Type of Service
VoIP	Voice over IP
VPN	Weighted Fair Queuing
WFQ	Weighted Fair Queuing
WRED	Weighted Random Early Detection
WRR	Weighted Round Robin

7.2 付録B デフォルトプライオリティマップ

デフォルトの dscp-dscp プライオリティマップでは、入力した値と出力の値が同一となります。

表 7-1 デフォルトの dot1p-lp プライオリティマップ

プライオリティの入力値	dot1p-lp マッピング
dot1p	lp
0	2
1	0
2	1
3	3
4	4
5	5
6	6
7	7

表 7-2 デフォルトの dot11e-lp プライオリティマップ

プライオリティの入力値	dot1p-lp マッピング
dot11e	lp
0	2
1	0
2	1
3	3
4	4
5	5
6	6
7	7

表 7-3 デフォルトの dscp-lp プライオリティマップ

プライオリティの入力値	dscp-dot1p マッピング
dscp	dot1p
0 ～ 7	0
8 ～ 15	1
16 ～ 23	2
24 ～ 31	3
32 ～ 39	4
40 ～ 47	5
48 ～ 55	6
56 ～ 63	7

表 7-4 デフォルトの lp-dot1p、lp-dot11e、lp-dscp プライオリティマップ

プライオリティの入力値	lp-dot1p マッピング	lp-dot11e マッピング	lp-dscp マッピング
lp	dot1p	dot11e	DSCP
0	1	1	0
1	2	2	8
2	0	0	16
3	3	3	24
4	4	4	32
5	5	5	40
6	6	6	48
7	7	7	56

表 7-5 デフォルトのポートプライオリティマップ

ポートプライオリティ	ローカルプレシーデンス
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7

7.3 付録C パケットプレシーデンスの概要

7.3.1 IP プレシーデンスと DSCP フィールドの値

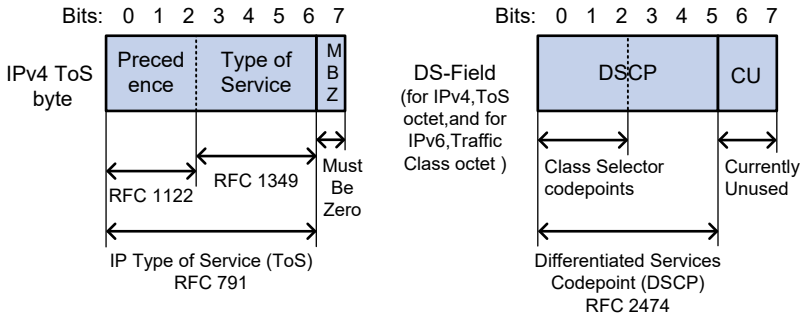


図 7-1 ToS、DS フィールド

図 7-1に示すように、IP ヘッダの ToS フィールドは 8 ビットが含まれます。最初の 3 ビット(0～2)は、0～7 までの IP プレシーデンスを示します。RFC2474 に従い、ToS フィールドは、右側の DS(Differentiated Services)フィールドとして再定義されます。ここで最初の 6 ビット(0～5)は DSCP を表し、0～63 までの値となります。残りの 2 ビット(6、7)は予約された値として使われません。

表 7-6 IP プレシーデンス

IP プレシーデンス(10 進表示)	IP プレシーデンス(2 進表示)	説明
0	000	Routine
1	001	priority
2	010	immediate
3	011	flash
4	100	flash-override
5	101	critical
6	110	internet
7	111	network

表 7-7 DSCP 値

DSCP 値(10 進表示)	DSCP 値(2 進表示)	説明
46	101110	ef
10	001010	af11
12	001100	af12
14	001110	af13
18	010010	af21
20	010100	af22
22	010110	af23
26	011010	af31
28	011100	af32
30	011110	af33
34	100010	af41
36	100100	af42
38	100110	af43
8	001000	cs1
16	010000	cs2
24	011000	cs3
32	100000	cs4
40	101000	cs5
48	110000	cs6
56	111000	cs7
0	000000	be (default)

7.3.2 802.1p プライオリティ

802.1p プライオリティは、レイヤ 2 ヘッダにありレイヤ 3 ヘッダを解析する必要がなく、QoS がレイヤ 2 で必要となるところで使用されます。

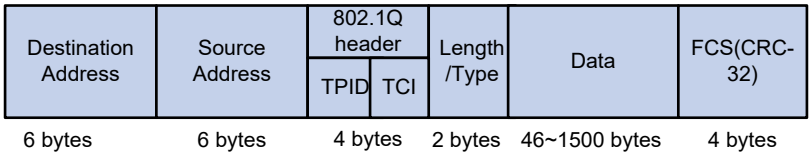


図 7-2 802.1Q タグヘッダの Ethernet フレーム

図 7-2に示すように、4 バイトの 802.1Q タグヘッダはタグプロトコル識別子(TPID、2 バイト長)とタグ管理情報(TCI、2 バイト長)から構成されます。TPID の値は 0x8100 です。図 7-3は、802.1Q ヘッダのフォーマットを示します。802.1Q タグヘッダのプライオリティフィールドは、IEEE802.1p で定義され、802.1p プライオリティと呼ばれます。表 7-8 に 802.1p プライオリティの値を示します。

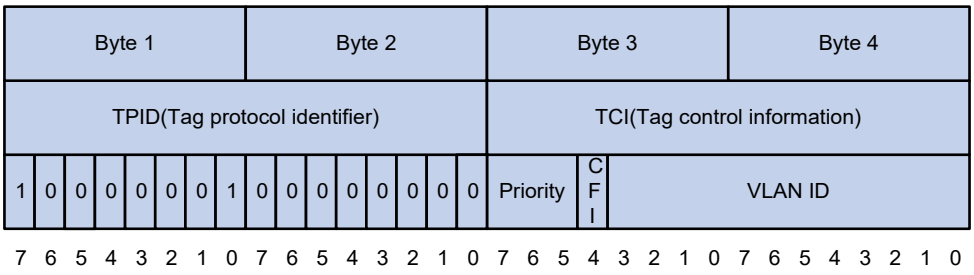


図 7-3 802.1Q タグヘッダ

表 7-8 802.1p プライオリティの説明

802.1p プライオリティ(10 進表示)	802.1p プライオリティ(2 進表示)	説明
0	000	best-effort
1	001	background
2	010	spare
3	011	excellent-effort
4	100	controlled-load
5	101	video
6	110	voice
7	111	network-management

7.3.3 802.11e プライオリティ

WLAN 上で QoS サービスを提供するために、802.11e 標準が開発されました。IEEE802.11e は、IEEE802.11 の MAC レイヤ拡張です。IEEE802.11e は、2 バイトの QoS 制御フィールドを 802.11e MAC フレームヘッダに追加します。3 ビットの QoS 制御フィールドは、0 から 7 の範囲の 802.11e 優先度を表します。

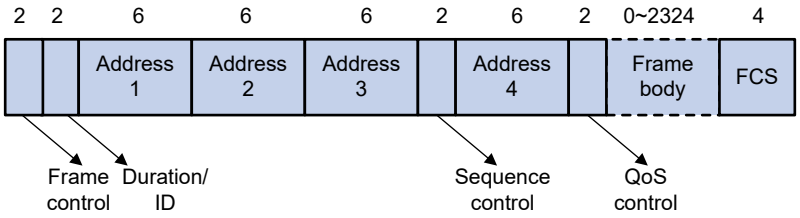


図 7-4 802.11e フレームの構造

目次

このセクションのページは **16-x-x** です。

8章 WLAN QoS 8-1
8.1 WLAN QoSについて 8-1
8.1.1 WMMプロトコル 8-1
8.1.2 SVP 8-3
8.1.3 クライアント制限 8-3
8.1.4 プロトコルと標準 8-4
8.2 制約事項とガイドライン 8-4
8.3 WMMの設定 8-4
8.3.1 WMMのタスク 8-4
8.3.2 WMMの有効化 8-4
8.3.3 EDCAパラメータの設定 8-5
8.3.4 クライアントのAC-BEまたはAC-BKキューのEDCAパラメータ設定 8-5
8.3.5 クライアントのAC-VIまたはAC-VOキューのEDCAパラメータ設定 8-6
8.3.6 優先順位マッピングのパケット優先順位を信頼するポートの設定 8-7
8.4 SVPマッピングの設定 8-7
8.5 クライアントレート制限の設定 8-8
8.5.1 クライアントのレート制限について 8-8
8.5.2 制限事項とガイドライン 8-8
8.5.3 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の設定 8-8
8.5.4 無線ベースのクライアントレート制限の設定 8-8
8.5.5 クライアントタイプベースのクライアントレート制限の設定 8-9
8.6 WMMの検証とメンテナンス 8-9
8.7 WLAN QoSの設定例 8-10
8.7.1 基本WMMの設定 8-10
8.7.2 CACの設定 8-11
8.7.3 SVPマッピングの設定 8-12
8.7.4 トラフィック差別化の設定 8-13
8.7.5 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の設定 8-15

8章 WLAN QoS

8.1 WLAN QoSについて

802.11 ネットワークは、競合ベースの無線アクセスを提供します。アプリケーションにQoS サービスを提供するために、IEEE は 802.11 ベースの WLAN 用の 802.11e を開発しました。

WLAN QoS の機能には、WMM、SVP、帯域幅保証、クライアントのレート制限などがあります。

8.1.1 WMM プロトコル

I. WMM について

Wi-Fi Alliance は、異なるベンダーの QoS 提供デバイスが相互運用できるように、WMM(Wi-Fi Multimedia) 標準を定義しました。WMM を使用すると、WLAN が QoS サービスを提供できるため、オーディオおよびビデオアプリケーションの WLAN でのパフォーマンスが向上します。

802.11 の DCF(Distributed Coordination Function) は、AP とクライアントが CSMA/CA(carrier sense multiple access with collision avoidance) アクセスメカニズムを使用する必要があります。AP またはクライアントは、データ伝送のためにチャネルを保持する前にチャネルをリッスンします。チャネルの指定されたアイドル時間がタイムアウトすると、AP またはクライアントはコンテンションウィンドウ内のバックオフスロットをランダムに選択してバックオフを実行します。最初にバックオフを完了したデバイスがチャネルを取得します。802.11 では、すべてのデバイスのアイドル時間と競合ウィンドウが同じです。そのため、チャネルの競合時には等しくなります。

QoS サービスを提供するために、WMM はデータトラフィックを異なる優先順位を持つ 4 つの AC に分割します。優先順位の高い AC のトラフィックは、チャネルを使用する可能性が高くなります。

II. 用語

- EDCA(**Enhanced distributed channel access**)
  優先度の高いパケットを優先的に送信し、そのようなパケットにより多くの帯域幅を割り当てるために WMM によって定義されたチャネル競合メカニズムです。
- AC(**Access category**)
  音声トラフィック用の AC-VO、ビデオトラフィック用の AC-VI、ベストエフォートトラフィック用の AC-BE、バックグラウンドトラフィック用の AC-BK の各 AC を定義します。4 つの AC の優先順位は降順です。
- CAC(**Connect Admission Control**)
  高優先度 AC (AC-VO および AC-VI) を使用してこれらのクライアントに十分な帯域幅を保証できるクライアントの数を制限します。
- U-APSD(**Unscheduled automatic power save delivery**)
  クライアントの電力を節約するために WMM によって定義された省電力方法です。

III. EDCA パラメータ

- **アービトレーションフレーム間間隔番号**
  802.11 ベースの WLAN では、各クライアントのアイドル時間 (DIFS) は同じですが、WMM は各 AC のアイドル時間を定義します。アイドル時間は、AIFSN が増加するにつれて長くなります。
- **指数形式の CWmin/指数形式の CWmax**
  ECWmin/ECWmax はバックオフスロットを決定し、2 つの値が増加するにつれて増加します。
- **伝送機会制限**
  TXOP 制限は、競合が成功した後にクライアントがチャネルを保持できる最大時間を指定します。値が大きいほど、時間が長くなります。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 つのパケットだけを送信できます。

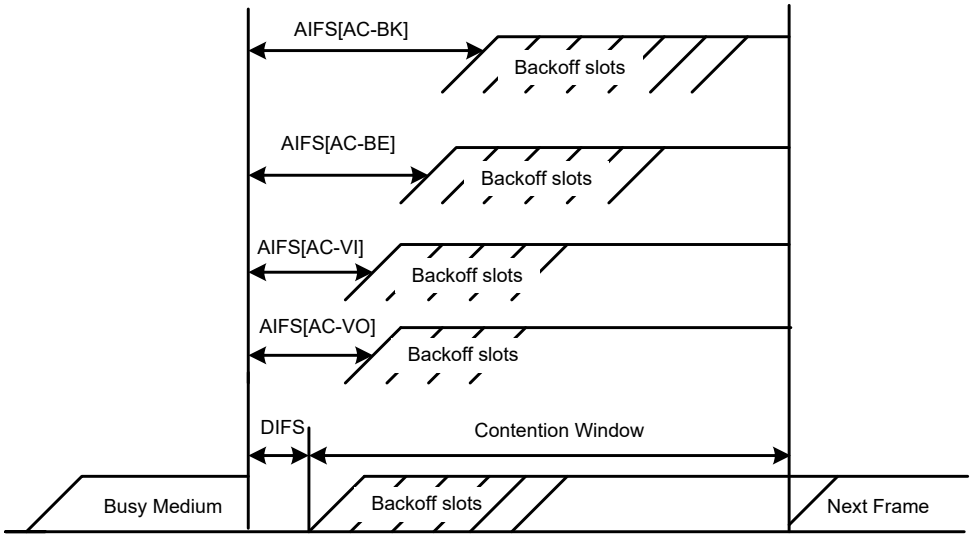


図 8-1 EDCA パラメータ

IV. CAC アドミッションポリシー

CAC では、クライアントが送信に優先度の高い AC を使用する前に、AP から許可を得る必要があります。これにより、アクセス権を得たクライアントの帯域幅が保証されます。CAC はリアルタイムトラフィック (AC-VO および AC-VI トラフィック) を制御しますが、一般的なデータ トラフィック (AC-BE および AC-BK トラフィック) は制御しません。

クライアントが優先度の高い AC (AC-VO または AC-VI) を使用する場合は、AP に要求を送信する必要があります。AP は、次のいずれかのアドミッションコントロールポリシーに基づいて肯定応答または否定応答を返します。

- **チャネル使用量ベースのアドミッションポリシー**
  AP は、既存の高優先度 AC キューと要求された AC キューのチャネル占有時間を、それぞれある期間内で計算します。2 つの値の合計がチャネルの最大保持時間以下の場合、クライアントは要求された AC キューを使用できます。そうでない場合、要求は拒否されます。
- **クライアントベースのアドミッションポリシー**
  高優先度 AC キューを使用するクライアントの数が高優先度 AC クライアントの最大数よりも少ない場合、要求は受け入れられます。そうでない場合、要求は拒否されます。計算中、AC-VO キューと AC-VI キューの両方を使用している場合、クライアントは 1 つのクライアントとしてカウントされます。

メディアリソースが不足しているために要求が拒否された場合、AP はクライアントに AC-BE を割り当てます。すでに優先度の高い AC キューを使用しているクライアントは影響を受けません。

メディアリソースを計算する場合、AP は CAC が有効になる前に要求を受け入れます。優先度の高い AC キューに対する後続の要求が受け入れられるかどうかは、リソースの使用状況によって大きく制限されます。

V. U-APSD 省電力メカニズム

U-APSD を使用すると、スリープモードのクライアントは、トリガーパケットを受信した後にのみ、指定された数のパケットをウェイクアップして受信できます。U-APSD は、802.11 APSD の省電力メカニズムを改善します。

WMM を有効にすると、U-APSD が自動的に有効になります。

VI. ACK ポリシー

WMM では、次の ACK ポリシーが定義されています。

- **通常の ACK**
  受信者は受信した各ユニキャストパケットを確認応答します。
- **No ACK**
  受信者は、無線パケット交換中に受信したパケットを確認応答しません。このポリシーにより、通信品質が強く干渉が弱い環境での伝送効率が向上します。通信品質が低下すると、このポリシーによりパケット損失率が高くなる可能性があります。802.11 n クライアントによって送信される A-MPDU パケットの場合、No ACK ポリシーは有効になりません。

8.1.2 SVP

SVP(SpectraLink Voice Priority) は、音声トラフィックに QoS サービスを提供するために SpectraLink によって開発されたものです。

8.1.3 クライアント制限

この機能は、1 つのクライアントによる積極的な帯域幅の使用を防ぎ、同じ AP に関連付けられたクライアント間での帯域幅の公平な使用を保証します。

クライアントのレート制限には、次のいずれかのモードを設定できます。

- **ダイナミックモード**
  すべてのクライアントが共有する合計帯域幅を設定します。各クライアントのレート制限は、合計レートをオンラインクライアントの数で割った値です。たとえば、合計レートが 10Mbps で、5 つのクライアントがオンラインの場合、各クライアントのレート制限は 2Mbps です。
- **静的モード**
  各クライアントが使用できる帯域幅を設定します。レート制限に関連付けられたクライアントの数を掛けた値が AP によって提供される使用可能な帯域幅を超えた場合、クライアントは設定された帯域幅を取得できないことがあります。

8.1.4 プロトコルと標準

- *802.11e-2005, Amendment 8: Medium Access Control (MAC) Quality of Service Enhancements, IEEE Computer Society, 2005*

Wi-Fi, WMM Specification version 1.1, Wi-Fi Alliance, 2005

8.2 制約事項とガイドライン

次の方法を使用して AP を設定できます。

- AP view で AP を 1 つずつ設定します。
- AP を AP グループに割り当て、AP グループ view で AP グループを設定します。
- グローバル設定 view ですべての AP を設定します。

AP の場合、これらのビューで同じパラメータに対して行った設定は、AP ビュー、AP グループビュー、グローバル設定ビューの降順で有効になります。

8.3 WMMの設定

8.3.1 WMM のタスク

作業リスト
WMMの有効化
(オプション設定項目)EDCAパラメータの設定
(オプション設定項目)クライアントのAC-BEまたはAC-BKキューのEDCAパラメータ設定
(オプション設定項目)クライアントのAC-VIまたはAC-VOキューのEDCAパラメータ設定
(オプション設定項目)優先順位マッピングのパケット優先順位を信頼するポートの設定

8.3.2 WMM の有効化

すべての 802.11n、802.11ac、および 802.11ax クライアントは WMM をサポートする必要があります。802.11n、802.11ac、または 802.11ax クライアントが関連付けられた AP と通信するには、無線が 802.11an、802.11gn、802.11ac、または 802.11ax モードで動作するときに WMM を有効にします。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． AP view または AP グループの AP モデル view に移行する	AP viewに移行する **wlan ap** *ap-name* APグループのAPモデルviewに移行する **wlan ap-group** *group-name* **ap-model** *ap-model*	―
3． 無線 view に移行する	**radio** *radio-id*	―

操作	コマンド	補足
4． WMM を有効にする	**wmm enable**	無線viewでは、無線はAPグループの無線viewの設定を使用します。 APグループの無線viewでは、WMMが有効になっています。

8.3.3 EDCA パラメータの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． AP view または AP グループの AP モデル view に移行する	AP viewに移行する **wlan ap** *ap-name* APグループのAPモデルviewに移行する **wlan ap-group** *group-name* **ap-model** *ap-model*	―
3． 無線 view に移行する	**radio** *radio-id*	―
4． EDCA パラメータを設定する	**edca radio** { **ac-be** | **ac-bk** | **ac-vi** | **ac-vo** } { **ack-policy** { **noack** | **normalack** } | **aifsn** *aifsn-value* | **ecw ecwmin** *ecwmin-value* **ecwmax** *ecwmax-value* | **txoplimit** *txoplimit-value* } *	無線viewでは、無線はAPグループの無線viewの設定を使用します。 APグループの無線viewでは、EDCAパラメータを表 8-1に示します。

表 8-1 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

8.3.4 クライアントの AC-BE または AC-BK キューの EDCA パラメータ設定

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． AP view または AP グループの AP モデル view に移行する	AP viewに移行する **wlan ap** *ap-name* APグループのAPモデルviewに移行する **wlan ap-group** *group-name* **ap-model** *ap-model*	―
3． 無線 view に移行する	**radio** *radio-id*	―

操作	コマンド	補足
4. EDCA パラメータを設定する	**edca client** { **ac-be** | **ac-bk** } { **aifsn** *aifsn-value* | **ecw ecwmin** *ecwmin-value* **ecwmax** *ecwmax-value* | **txoplimit** *txoplimit-value* } *	無線viewでは、無線はAPグループの無線viewの設定を使用します。 APグループの無線viewでは、EDCAパラメータを表 8-2に示します。

表 8-2 クライアントの AC-BE または 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

8.3.5 クライアントの AC-VI または AC-VO キューの EDCA パラメータ設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. AP view または AP グループの AP モデル view に移行する	AP viewに移行する **wlan ap** *ap-name* APグループのAPモデルviewに移行する **wlan ap-group** *group-name* **ap-model** *ap-model*	―
3. 無線 view に移行する	**radio** *radio-id*	―
4. EDCA パラメータを設定する	**edca client** { **ac-vi** | **ac-vo** } { **aifsn** *aifsn-value* | **cac** { **disable** | **enable** } | **ecw ecwmin** *ecwmin-value* **ecwmax** *ecwmax-value* | **txoplimit** *txoplimit-value* } *	無線viewでは、無線はAPグループの無線viewの設定を使用します。 APグループの無線viewでは、EDCAパラメータを表 8-3に示します。
5. (オプション設定項目) CAC ポリシーを設定する	**cac policy** { **channelutilization** [*channelutilization-value*] | **client** [*client-number*] }	無線viewでは、無線はAPグループの無線viewの設定を使用します。 APグループの無線ビューでは、許可されるクライアントの最大数は20です

表 8-3 クライアントの AC-VI または AC-VO 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

8.3.6 優先順位マッピングのパケット優先順位を信頼するポートの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. サービステンプレート view に移行する	**wlan service-template** *service-template-name*	―
3. 信頼できるパケット優先度タイプを設定する	**qos trust** { **dot11e** | **dscp** }	デフォルト：
4. ポートプライオリティを設定する	**qos priority** *priority*	デフォルト：0

8.4 SVPマッピングの設定

この機能は、IP ヘッダーにプロトコル ID 119 を持つパケットを AC-VI または AC-VO キューに割り当て、指定された優先度の SVP パケットを提供します。SVP では、SVP パケットのランダムバックオフは必要ありません。したがって、AC-VI または AC-VO キューに SVP パケットしかない場合は、ECWmin と ECWmax の両方を 0 に設定できます。

SVP マッピングが無効の場合、SVP パケットは AC-BE キューに割り当てられます。

I. 制限とガイドライン

SVP マッピングは、非 WMM クライアントでのみ有効です。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. AP view または AP グループの AP モデル view に移行する	AP viewに移行する **wlan ap** *ap-name* APグループのAPモデルviewに移行する **wlan ap-group** *group-name* **ap-model** *ap-model*	―
3. 無線 view に移行する	**radio** *radio-id*	―
4. SVP マッピングを有効にする	**svp map-ac** { **ac-vi** | **ac-vo** }	無線viewでは、無線はAPグループの無線viewの設定を使用します。 APグループの無線viewでは、無効です。

8.5 クライアントレート制限の設定

8.5.1 クライアントのレート制限について

レート制限方法によって、サービステンプレートベース、無線ベース、またはクライアントタイプベースのクライアントのレート制限を設定できます。レート制限モードによって、クライアントのレート制限に動的モードまたは静的モードを設定できます。

複数のメソッドとモードが設定されている場合は、すべての設定が有効になります。クライアントのレートは、すべてのクライアントレート制限設定の中で最小値に制限されます。

8.5.2 制限事項とガイドライン

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は、同じサービステンプレートに関連付けられているすべてのクライアントで有効になります。

無線ベースのクライアントレート制限は、同じ無線に関連付けられているすべてのクライアントで有効になります。

クライアントタイプベースのクライアントレート制限は、指定されたプロトコルのすべてのクライアントで有効になります。

8.5.3 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の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． サービステンプレート view に移行する	**wlan service-template** *service-template-name*	―
3． 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する	**client-rate-limit** { **inbound** | **outbound** } **mode** { **dynamic cir** *cir* [**min** *min-cir*] [**max** *max-cir*] | **static cir** *cir* } [**cbs** *cbs*]	デフォルト：設定なし

8.5.4 無線ベースのクライアントレート制限の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． AP view または AP グループの AP モデル view に移行する	AP viewに移行する **wlan ap** *ap-name* APグループのAPモデルviewに移行する **wlan ap-group** *group-name* **ap-model** *ap-model*	―
3． 無線 view に移行する	**radio** *radio-id*	―

操作	コマンド	補足
4. 無線ベースのクライアントレート制限を有効にする	**client-rate-limit** { **disable** | **enable** }	デフォルト: 無線viewでは、無線はAPグループの無線viewの設定を使用します。APグループの無線viewでは、disableです。
5. 無線ベースのクライアントレート制限を設定する	**client-rate-limit** { **inbound** | **outbound** } **mode** { **dynamic cir** *cir* [**min** *min-cir*] [**max** *max-cir*] | **static cir** *cir* }	デフォルト: 無線viewでは、無線はAPグループの無線viewの設定を使用します。APグループの無線viewでは、設定なしです。

8.5.5 クライアントタイプベースのクライアントレート制限の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. 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する	**wlan client-rate-limit** { **dot11a** | **dot11ac** | **dot11an** | **dot11b** | **dot11g** | **dot11gac** | **dot11gn** } { **inbound** | **outbound** } **cir** *cir* [**cbs** *cbs*]	デフォルト:設定なし

8.6 WMMの検証とメンテナンス

すべての view で **display** コマンドを実行できます。

操作	コマンド
クライアントのWMM統計情報を表示する	**display wlan wmm client** [**ap** *ap-name* | **mac-address** *mac-address*]
無線のWMM統計情報を表示表示する	**display wlan wmm radio** [**ap** *ap-name*]

user view で **reset** コマンドを実行できます。

操作	コマンド
クライアントのWMM統計情報をクリアする	**reset wlan wmm client** [**ap** *ap-name* | **mac-address** *mac-address*]
無線のWMM統計情報をクリアする	**reset wlan wmm radio** [**ap** *ap-name*]

8.7 WLAN QoSの設定例

8.7.1 基本 WMM の設定

I. ネットワーク構成

図 8-2に示すように、AP とクライアントがトラフィックに優先順位を付けることができるように、AC で WMM を有効にします。

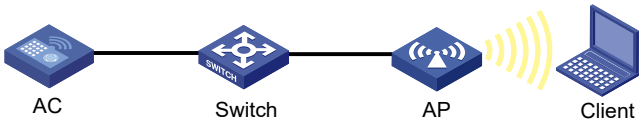


図 8-2 ネットワーク図

II. 設定手順

#market という名前のサービステンプレートを作成し、SSID を market に設定し、サービステンプレートを有効にする。

```
<AC> system-view
[AC] wlan service-template market
[AC-wlan-st-market] ssid market
[AC-wlan-st-market] service-template enable
[AC-wlan-st-market] quit
```

#ap 1 という名前の手動 AP を作成し、AP モデルとシリアル ID を指定します。

```
[AC] wlan ap ap1 model WA1020
[AC-wlan-ap-ap1] serial-id 219801A28N819CE0002T
```

#WMM を有効にし、サービステンプレート market を radio 1 にバインドし、radio 1 を有効にする。

```
[AC-wlan-ap-ap1] radio 1
[AC-wlan-ap-ap1-radio-1] service-template market
[AC-wlan-ap-ap1-radio-1] wmm enable
[AC-wlan-ap-ap1-radio-1] radio enable
```

III. 設定確認

#無線の WMM 統計情報を表示する。

```
[AC] display wlan wmm radio
          AP ID : 1    AP Name : ap1

           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
 CAC information
 Clients accepted                        : 0
  Voice                                  : 0
  Video                                  : 0
 Total request medium time(µs)           : 0
  Voice(µs)                              : 0
  Video(µs)                              : 0
Calls rejected due to insufficient resources    : 0
Calls rejected due to invalid parameters        : 0
Calls rejected due to invalid medium time       : 0
Calls rejected due to invalid delay bound       : 0
Radio : 2
 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
 CAC information
 Clients accepted                : 0
  Voice                          : 0
  Video                          : 0
 Total request medium time(µs)    : 0
  Voice(µs)                      : 0
  Video(µs)                      : 0
 Calls rejected due to insufficient resources  : 0
 Calls rejected due to invalid parameters      : 0
 Calls rejected due to invalid medium time     : 0
 Calls rejected due to invalid delay bound     : 0
```

8.7.2 CAC の設定

I. ネットワーク構成

図 8-3に示すように、最大 10 クライアントが AC-VO および AC-VI キューを使用できるように CAC を構成します。

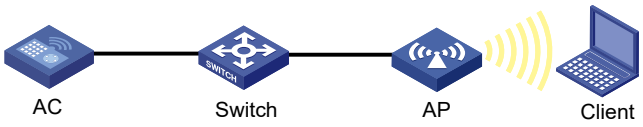


図 8-3 ネットワーク図

II. 設定手順

1. market という名前のサービステンプレートを作成し、SSID を market に設定して、サービステンプレートを有効にします。

```
<AC> system-view
[AC] wlan service-template market
[AC-wlan-st-market] ssid market
[AC-wlan-st-market] service-template enable
```

```
[AC-wlan-st-market] quit
```

2. ap 1 という名前の手動 AP を作成し、AP モデルとシリアル ID を指定します。

```
[AC] wlan ap ap1 model WA1020
[AC-wlan-ap-ap1] serial-id 219801A28N819CE0002T
```

3. WMM の設定

サービステンプレートマーケットをラジオ 1 にバインドする。

```
[AC-wlan-ap-ap1] radio 1
[AC-wlan-ap-ap1-radio-1] service-template market
```

AC-VO および AC-VI キューに対して WMM を有効にし、クライアント数を 10 に制限するように CAC ポリシーを設定する。

```
[AC-wlan-ap-ap1-radio-1] wmm enable
[AC-wlan-ap-ap1-radio-1] edca client ac-vo cac enable
[AC-wlan-ap-ap1-radio-1] edca client ac-vi cac enable
[AC-wlan-ap-ap1-radio-1] cac policy client 10
```

#無線 1 を有効にする。

```
[AC-wlan-ap-ap1-radio-1] radio enable
```

I. 設定確認

クライアントが優先度の高い AC キュー (AC-VO または AC-VI) の使用を要求したとします。次の情報を確認します。

- 高優先度 AC キューを使用するクライアントの数が、高優先度 AC クライアントの最大数 (この例では 10) よりも少ない場合、要求は受け入れられます。
- 高優先度 AC キューを使用するクライアントの数が、高優先度 AC クライアントの最大数 (この例では 10) と等しい場合、要求は拒否されます。AP はクライアントからのパケットの優先順位を下げます。

8.7.3 SVP マッピングの設定

I. ネットワーク構成

図 8-4に示すように、AC で SVP マッピングを設定して、SVP パケットを AC-VO キューに割り当てます。AP の AC-VO キューの ECWmin と ECWmax を 0 に設定します。

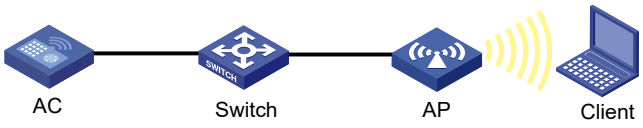


図 8-4 ネットワーク図

II. 設定手順

1. market という名前のサービステンプレートを作成し、SSID を market に設定して、サービステンプレートを有効にします。

```
<AC> system-view
[AC] wlan service-template market
[AC-wlan-st-market] ssid market
[AC-wlan-st-market] service-template enable
[AC-wlan-st-market] quit
```

2. ap 1 という名前の手動 AP を作成し、AP モデルとシリアル ID を指定します。

```
[AC] wlan ap ap1 model WA1020
[AC-wlan-ap-ap1] serial-id 219801A28N819CE0002T
```

3. SVP マッピングの設定

WMM を有効にする。

```
[AC-wlan-ap-ap1] radio 1
[AC-wlan-ap-ap1-radio-1] wmm enable
```

#SVP パケットを AC-VO キューに割り当て、クライアントの AC-VO キューの EDCA パラメータを設定する。

```
[AC-wlan-ap-ap1-radio-1] svp map-ac ac-vo
[AC-wlan-ap-ap1-radio-1] edca client ac-vo ecw ecwmin 0 ecwmax 0
```

#サービステンプレート market を radio 1 にバインドし、radio を有効にする。

```
[AC-wlan-ap-ap1-radio-1] service-template market
[AC-wlan-ap-ap1-radio-1] radio enable
```

III. 設定確認

非 WMM クライアントがオンラインになり、SVP パケットを AC に送信する場合、AC が SVP パケットを AC-VO キューに割り当てることを確認します。

8.7.4 トラフィック差別化の設定

I. ネットワーク構成

図 8-5に示すように、クライアントからの 802.11 パケットを AC-VO キューに追加するように、AC でプライオリティマッピングを設定します。

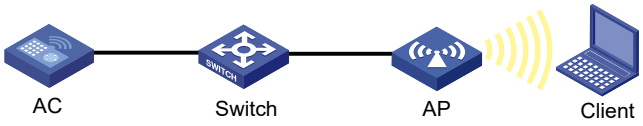


図 8-5 ネットワーク図

II. 設定手順

#market という名前のサービステンプレートを作成し、SSID を market に設定する。

```
<AC> system-view
[AC] wlan service-template market
[AC-wlan-st-market] ssid market
[AC-wlan-st-market] service-template enable
[AC-wlan-st-market] quit
```

#優先度マッピングを設定し、サービステンプレートを有効にする。

```
[AC-wlan-st-market] qos priority 7
[AC-wlan-st-market] service-template enable
[AC-wlan-st-market] quit
```

#ap 1 という名前の手動 AP を作成し、AP モデルとシリアル ID を指定します。

```
[AC] wlan ap ap1 model WA1020
[AC-wlan-ap-ap1] serial-id 219801A28N819CE0002T
```

WMM を有効にする。

```
[AC-wlan-ap-ap1] radio 1
[AC-wlan-ap-ap1-radio-1] wmm enable
```

#サービステンプレート market を radio 1 にバインドし、radio 1 を有効にする。

```
[AC-wlan-ap-ap1-radio-1] service-template market
[AC-wlan-ap-ap1-radio-1] radio enable
[AC-wlan-ap-ap1-radio-1] quit
[AC-wlan-ap-ap1] quit
```

I. 設定確認

AC で次の作業を行う。

- terminal monitor コマンドを実行して、現在の端末でログの監視を有効にする。
- terminal debugging コマンドを実行して、現在の端末でデバッグ情報の表示を有効にする。
- debugging wlan wmm all コマンドを実行して、すべての WMM デバッグ機能を有効にする。

#クライアントと AP 上のスイッチに ping を実行して、ネットワーク接続が正しいことを確認する。

#クライアントから AP へのパケットの優先順位が 7 に変更され、AP からクライアントへのパケットの優先順位が変更されていないことを確認します。

8.7.5 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の設定

I. ネットワーク構成

図 8-6に示すように、AC は AP と同じネットワーク内にあります。AC で次のタスクを実行します。

- 着信クライアントトラフィックのレートを制限する静的モードクライアントレート制限を設定します。
- 発信クライアントトラフィックのレートを制限する動的モードクライアントレート制限を設定します。

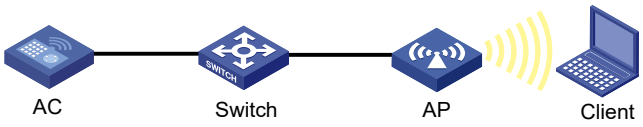


図 8-6 ネットワーク図

II. 設定手順

service という名前のサービステンプレートを作成し、その SSID を service に設定する。

```
<AC> system-view
[AC] wlan service-template service
[AC-wlan-st-service] ssid service
```

#スタティックモードでは着信トラフィックのレートを 8000 Kbps に制限し、ダイナミックモードでは発信トラフィックのレートを 8000 Kbps に制限します。

```
[AC-wlan-st-service] client-rate-limit inbound mode static cir 8000
[AC-wlan-st-service] client-rate-limit outbound mode dynamic cir 8000
[AC-wlan-st-service] service-template enable
[AC-wlan-st-service] quit
```

#ap 1 という名前の手動 AP を作成し、AP モデルとシリアル ID を指定する。

```
[AC] wlan ap ap1 model WA6320
[AC-wlan-ap-ap1] serial-id 219801A28N819CE0002T
```

#サービステンプレートサービスを無線 1 にバインドし、無線 1 を有効にする。

```
[AC-wlan-ap-ap1] radio 1
[AC-wlan-ap-ap1-radio-1] service-template service
[AC-wlan-ap-ap1-radio-1] radio enable
[AC-wlan-ap-ap1-radio-1] return
```

QX-W2300AC シリーズ アクセスコントローラ

オペレーションマニュアル

17. ネットワーク管理と監視

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

02- システムのデバッグ

03-NQA

04-SNMP

05-RMON

06-NETCONF

07-プロセスモニタリングとメンテナンス

08-ポートミラーリング

09-パケットキャプチャ

10-NetMeister

目次

このセクションのページは **17-x-x** です。

1 章 システムの保守 1-1
1.1 Ping 1-1
1.1.1 ping コマンドを使用したネットワークの接続試験 1-1
1.1.2 Ping 設定例 1-1
1.2 Tracert 1-3
1.2.1 設定要件 1-4
1.2.2 tracert コマンドを使用した故障の検出、ルートにあるすべてのノードの確認 1-4
1.2.3 Tracert 設定例 1-4

1章 システムの保守

1.1 Ping

ping コマンドで、指定したアドレスに到達可能かどうかを確認したり、ネットワーク接続を試験したりすることができます。

ping は ICMP エコーリクエスト（ECHO-REQUEST）を宛先装置に送信します。リクエストを受信した、宛先リクエストは ICMP のリクエストに応答して送信元装置に ICMP エコーリプライ（ECHO-REPLY）を送信します。送信元装置は、パケット送信数、受信したパケットリプライ数、ラウンドトリップタイムの ping の統計情報を表示します。これらの統計情報を解析することによってネットワークの性能を測定することができます。

1.1.1 ping コマンドを使用したネットワークの接続試験

すべての view で **ping** コマンドを実行できます。

操作	コマンド	補足
指定したアドレスに到達可能かどうかを確認する	• IPv4ネットワーク： **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*	-

🕮 **メモ**：

パ低速度ネットワークで ping コマンドを設定する場合、タイムアウトタイマには大きな値を設定してください。
タイムアウトタイマは、**-t** キーワードで変更ができます。

1.1.2 Ping 設定例

I. ネットワーク要件

図 1-1 に示すように、AC と Device B 間で通信可能かどうか確認します。互いに通信可能である場合、AC から Device B のルートについての詳細な情報を取得します。

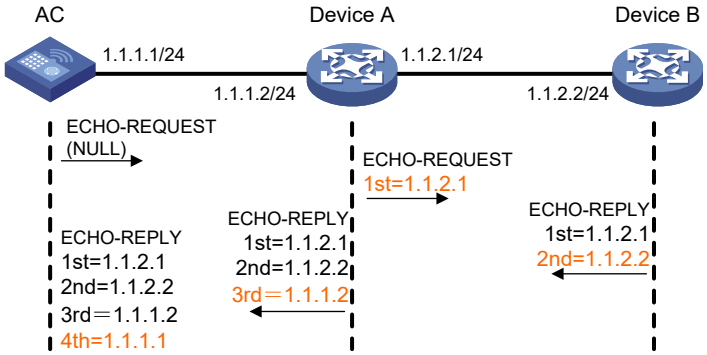


図 1-1 ネットワーク図

II. 設定手順

AC で **ping** コマンドを使用し、Device B と通信可能かどうか確認します。

```
<AC> 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=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
```

出力は、以下の状態を示します。

- AC が Device B に 5 つの ICMP パケットを送信、AC は ICMP パケットを受信します。
- パケットの送信失敗がありません。
- ルートが到達可能です。

AC から Device B の詳細なルート情報を取得します。

```
<AC> 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
```

図 1-1 に示すように **ping -r** のテスト手順は以下となります。

1)　送信元（AC）は RR オプションを空で ICMP エコーリクエストを宛先（Device B）に対して送信します。

2) 中間デバイス（Device A）は ICMP エコーリクエストの RR オプションに出力インタフェースの IP アドレス（1.1.2.1）を追加し、転送します。
3) リクエストを受信した宛先デバイスはリクエストの RR オプションをコピーし、RR オプションに出力インタフェースの IP アドレス（1.1.2.2）を追加します。ICMP エコーリプライを送信します。
4) 中間デバイスは ICMP エコーリプライの RR オプションに出力インタフェースの IP アドレス（1.1.1.2）を追加し、リプライを転送します。
5) リプライを受信した送信元デバイスは RR オプションにインタフェースの IP アドレス（1.1.1.1）を追加します。最後に、1.1.1.1 <-> {1.1.1.2; 1.1.2.1} <-> 1.1.2.2 という AC～Device B 間の詳細な情報を取得します。

1.2 Tracert

Tracert（traceroute と呼ばれます）は、ネットワークが有効かどうか確認するために、送信元から宛先にパケットを伝送するレイヤ 3 デバイスの IP アドレスの追跡を行います。ネットワークに不具合があった場合に、tracert コマンドを使用して機能しなくなったノードを特定するのに有用です。

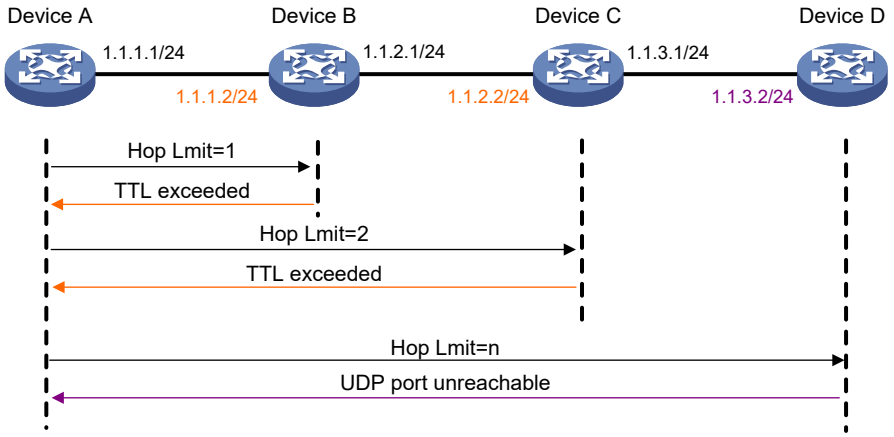


図 1-2 Tracert の動作

Tracert はデバイスの IP アドレスを取得するため、受信した ICMP エラーメッセージを使用します。図 1-2 に示すように、tracert が動作します。

1) 送信元デバイス（Device A）が宛先デバイス（Device D）に TTL 値が 1 のパケットを送信します。パケットの UDP 番号は宛先のアプリケーションで使用されないポート番号です。
2) 最初のホップ（Device B）（パケットを最初に受信するレイヤ 3 デバイス）は、1.1.1.2 の IP アドレスがカプセル化された TTL-expired ICMP エラーメッセージを送信元に返します。このように、送信元デバイスは最初のレイヤ 3 デバイスのアドレス（1.1.1.2）を受信します。
3) 送信元デバイスが宛先のデバイスに TTL 値が 2 のパケットを送信します。
4) 2 番目のホップ（Device C）が TTL-expired ICMP エラーメッセージで応答し、これで送信元デバイスは 2 番目のレイヤ 3 デバイスのアドレス（1.1.2.2）を取得します。
5) このプロセスは、最終宛先のデバイスに到達するまで続きます。宛先のアプリケーションは UDP ポートを使用していません。宛先は IP アドレス 1.1.3.2 の到達不能 ICMP エラーメッセージのリプライをします。

6)　送信元デバイスは以下のことを認識します。
- 到達不能 ICMP エラーメッセージを受信したとき、宛先に届いたことを認識します。
- 宛先デバイスまでのパスは 1.1.1.2 から、1.1.2.2 から、1.1.3.2 であると認識します。

1.2.1 設定要件

tracert コマンドを使用する前に、以下の作業を行ってください。

IPv4 ネットワーク：

- 中間デバイス（送信元デバイスと宛先デバイスの間のデバイス）で ICMP タイムアウトパケットの送信を有効にします。もし中間デバイスが QX シリーズの場合、デバイスで **ip ttl-expires enable** コマンドを実行してください。
- 中間デバイス（送信元デバイスと宛先デバイスの間のデバイス）で ICMP 宛先到達不能パケットの送信を有効にします。もし中間デバイスが QX シリーズの場合、デバイスで **ip unreachables enable** コマンドを実行してください。

1.2.2 tracert コマンドを使用した故障の検出、ルートにあるすべてのノードの確認

すべての view で **tracert** コマンドを実行できます。

操作	コマンド
送信元から宛先のルートを表示する	• IPv4ネットワーク： **tracert** [**-a** *source-ip* | **-f** *first-ttl* | **-m** *max-ttl* | **-p** *port* | **-q** *packet-number* | **-t** *tos* | **-w** *timeout*] * *host*

1.2.3 Tracert 設定例

I. ネットワーク要件

図 1-3 に示すように、AC は Device B への Telnet が失敗しています。

AC と Device B 間でネットワークの接続性を確認します。互いに通信できない場合、ネットワークの故障したノードを特定できます。



図 1-3 ネットワーク図

II. 設定手順

1)　図 1-3 に示すように Device に IP アドレスを設定します。
2)　AC でスタティックルートを設定します。

```
<AC> system-view
[AC] ip route-static 0.0.0.0 0.0.0.0 1.1.1.2
[AC] quit
```

3) **ping** コマンドを使用して AC と Device B 間の接続性を確認します。

```
<AC> ping 1.1.2.2
Ping 1.1.2.2(1.1.2.2): 56 -data bytes, press CTRL_C to break
Request time out
Request time out
Request time out
Request time out
Request time out

--- Ping statistics for 1.1.2.2 ---
5 packet(s) transmitted,0 packet(s) received,100.0% packet loss
```

出力は、AC と Device B が通信不可能であることを示します。

4) **tracert** コマンドを使用して、故障したノードを特定します。

Device A で ICMP タイムアウトパケットの送信を有効にします。

```
<DeviceA> system-view
[DeviceA] ip ttl-expires enable
```

Device B で ICMP 到達不可能パケットの送信を有効にします。

```
<DeviceB> system-view
[DeviceB] ip unreachables enable
```

AC で **tracert** コマンドを実行します。

```
<AC> 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) 1 ms 2 ms 1 ms
 2  * * *
 3  * * *
 4  * * *
 5
<AC>
```

出力は、AC と Device A は互いに通信できますが、AC と Device B は通信できないことを示します。Device A と Device B 間の通信でエラーが発生していることを示します。

5) 問題を確認するため AC と Device B で以下のコマンドを実行します。

- **debugging ip icmp** コマンドを使用して AC と Device B で ICMP パケットの送受信ができるか確認を行います。
- **display ip routing-table** コマンドを使用して AC と Device B のルートがあるか確認します。

目次

このセクションのページは **17-x-x** です。

2 章 システムのデバッグ 2-1
2.1 システムのデバッグ 2-1
2.1.1 スイッチのデバッグ情報の制御 2-1
2.1.2 システムデバッグの設定 2-2

2章 システムのデバッグ

2.1 システムのデバッグ

装置は、さまざまなデバッグ機能があります。サポートしているプロトコルおよび機能の大半に対し、システムはユーザのエラー診断に役立つデバッグ情報を提供しています。

2.1.1 スイッチのデバッグ情報の制御

次の 2 つのスイッチがデバッグ情報の表示を制御します。

- **モジュールデバッグスイッチ** － モジュール特有のデバッグ情報を制御します。
- **画面出力スイッチ** － 所定の画面にデバッグ情報を表示するかを制御します。出力する画面上で **terminal monitor** コマンド、**terminal logging level** コマンドを使用します。

図 2-1 に示すように、モジュールデバッグスイッチと画面出力スイッチの関係を示したものです。デバイスは、デバッグ情報をモジュール 1、2、3 に出力できると仮定します。両方に電源が入っているときのみ情報は端末に出力されます。

デバッグ情報は通常、コンソールに表示されます。他の宛先にデバッグ情報を送信することができます。

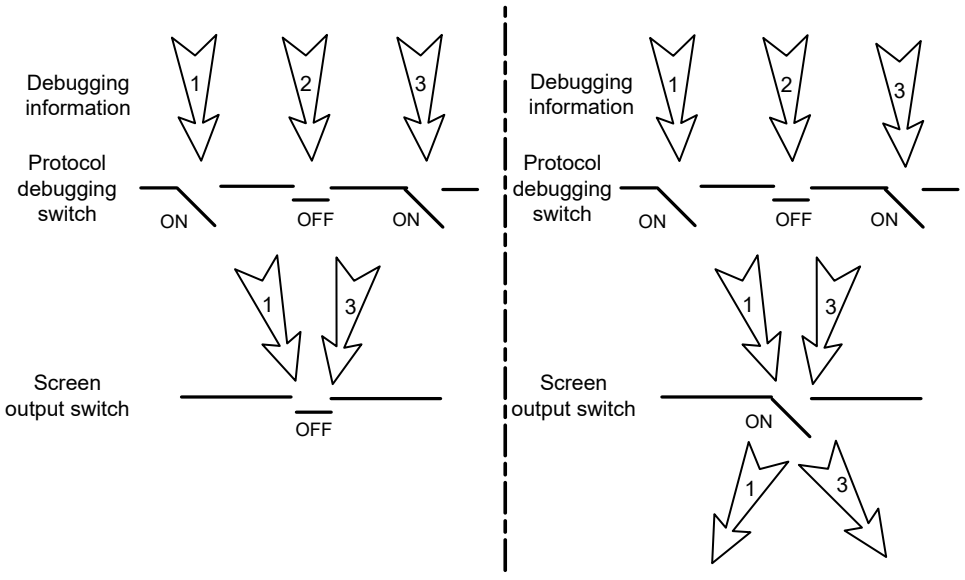


図 2-1 モジュールデバッグスイッチと画面出力スイッチの関係

2.1.2 システムデバッグの設定

デバッグコマンドの出力は、メモリ容量に影響します。システム性能を保証するため、異常な状況にあるプロトコルに関連したデバッグのみ有効にしてください。デバッグを行った後、**undo debugging all** コマンドを使用してすべてのデバッグ機能を無効にしてください。

以下にデバッグ機能の設定を示します。

操作	コマンド	補足
1. user view でプロトコルのデバッグを有効にする	**debugging** { **all** [**timeout** *time*] | *module-name* [*option*] }	デフォルト：無効
2. （オプション設定項目） すべての view で有効なデバッグ機能を表示する	**display debugging** [*module-name*]	—

目次

このセクションのページは **17-x-x** です。

3章 NQA 3-1
3.1 概要 3-1
3.1.1 NQAのテストタイプ 3-1
3.1.2 コラボレーション 3-2
3.1.3 しきい値監視機能 3-2
3.2 NQA設定作業リスト 3-3
3.3 NQAサーバの設定 3-3
3.4 NQAクライアントの有効化 3-4
3.5 NQAクライアントのNQAテストの設定 3-4
3.5.1 NQAテストの設定作業リスト 3-4
3.5.2 ICMPエコーテストの設定 3-4
3.5.3 ICMPジッタテストの設定 3-5
3.5.4 DHCPテストの設定 3-6
3.5.5 DNSテストの設定 3-7
3.5.6 FTPテストの設定 3-8
3.5.7 HTTPテストの設定 3-9
3.5.8 UDPジッタテストの設定 3-10
3.5.9 SNMPテストの設定 3-11
3.5.10 TCPテストの設定 3-12
3.5.11 UDPエコーテストの設定 3-13
3.5.12 UDP tracertの設定 3-14
3.5.13 音声テストの設定 3-15
3.5.14 DLSwテストの設定 3-17
3.5.15 パスジッタの設定 3-18
3.5.16 NQAテストのオプションパラメータの設定 3-19
3.5.17 しきい値監視機能の設定 3-20
3.5.18 NQA統計情報収集機能の設定 3-22
3.5.19 NQA履歴記録保存の設定 3-23
3.5.20 NQAクライアントにおけるNQAテストのスケジューリング 3-23
3.6 NQAクライアントでのNQAテンプレートの設定 3-24
3.6.1 NQAの表示と維持 3-25
3.7 NQA設定例 3-25
3.7.1 ICMPエコーテスト設定例 3-25
3.7.2 FTPテスト設定例 3-27
3.7.3 UDPジッタテスト設定例 3-28
3.7.4 SNMPテスト設定例 3-31
3.7.5 HTTPテスト設定例 3-32
3.7.6 TCPテスト設定例 3-33
3.7.7 UDPエコーテスト設定例 3-35
3.7.8 NQAコラボレーショテスト設定例 3-36

3章 NQA

3.1 概要

NQA（Network quality analyzer）は、ネットワークの性能、IP サービスのサービスレベルとアプリケーションを確認し、ネットワークの問題を診断することができます。以下のタイプのテストをサポートしています。

- ICMP エコーテスト
- DHCP
- DLSw
- DNS
- FTP
- HTTP
- SNMP
- TCP
- UDP エコーテスト
- UDP ジッタ
- 音声

図 3-1に示すように、NQA 送信元装置（NQA クライアント）は、ネットワークパフォーマンスを測定するため、NQA 宛先装置に IP サービスとアプリケーションのシミュレーションを行うデータを送信します。取得した性能の測定基準は、1 方向の遅延、ジッタ、音声品質、アプリケーション性能、サーバ応答時間が含まれます。

NQA のすべてのタイプは NQA クライアントが必要ですが、TCP、UDP エコー、UDP ジッタ、音声は NQA サーバのみ必要です。FTP のように、すでに宛先装置でサービスが提供されている場合、NQA サーバは必要ではありません。

さまざまなテストのニーズを満たすため、特定の IP アドレスとポートをリスニングし、応答する NQA サーバを設定することができます。

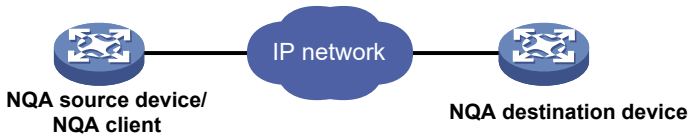


図 3-1 ネットワーク図

3.1.1 NQA のテストタイプ

以下に異なる NQA テストタイプを示します。

- TCP あるいは DLSw テストは接続をセットアップします。
- UDP ジッタや音声テストは指定した数のプローブパケットを送信します。プローブパケット数は **probe packet-number** コマンドで設定可能です。
- FTP テストはファイルのアップロードあるいはダウンロードを行います。
- HTTP テストは Web ページを取得します。
- DHCP テストは DHCP を通して IP アドレスを取得します。

- DNS テストは IP アドレスにドメイン名を変換します。
- ICMP エコーテストは ICMP エコーリクエストを送信します。
- UDP エコーテストは UDP ペットを送信します。
- SNMP テストは SNMPv1 パケット、SNMPv2c パケット、SNMPv3 パケットを送信します。

3.1.2 コラボレーション

NQA は、アプリケーションモジュールがあらかじめ定義されたアクションを行うことができるようにするため、アプリケーションモジュールの状態あるいはパフォーマンスの変更を通知するようにトラックモジュールとコラボレーションすることができます。

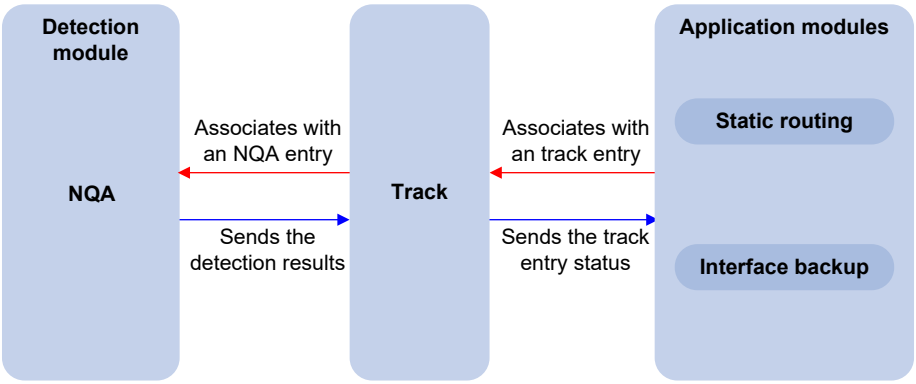


図 3-2 コラボレーション

以下に、コラボレーションを使用して、192.168.0.88 のスタティックルートの動作をモニタする方法を示します。

1) NQA は 192.168.0.88 の到達可能性をモニタします。
2) 192.168.0.88 が到達不可能となったとき、NQA はその変化をトラックモジュールに通知します。
3) トラックモジュールは、スタティックルーティングモジュールに状態の変化を通知します。
4) スタティックルーティングモジュールはスタティックルートを無効にします。

コラボレーションについての詳細は、QX-W2300AC シリーズ アクセスコントローラ オペレーションマニュアルの”*14 高可用性*”の”*2 章 Track*”を参照してください。

3.1.3 しきい値監視機能

しきい値監視機能は、NQA が指定したしきい値を越えたとき、指定されたアクションを実行します。

表 3-1に監視対象とサポートするテストタイプの関係について示します。

表 3-1 監視対象とサポートするテストタイプの関係

監視対象	サポートするテストタイプ
プローブ期間	UDPジッタ、音声を除くすべてのNQAテスト

監視対象	サポートするテストタイプ
検査失敗回数	UDPジッタ、音声を除くすべてのNQAテスト
廃棄パケット数	UDPジッタ、音声テスト
1方向のジッタ（送信元から宛先、宛先から送信元）	UDPジッタ、音声テスト
1方向の遅延（送信元から宛先、宛先から送信元）	UDPジッタ、音声テスト
ICPIF（Calculated Planning Impairment Factor）	音声テスト
MOS（Mean Opinion Scores）	音声テスト

3.2 NQA設定作業リスト

作業リスト	補足
NQAサーバの設定	TCP、UDP、UDPジッタ、音声テストでは必須設定項目
（必須設定項目）NQAクライアントの有効化	ー
（必須設定項目）NQAクライアントのNQAテストの設定	ー

3.3 NQAサーバの設定

TCP、UDP エコー、UDP ジッタ、音声テストを実行するため、宛先装置で NQA サーバを有効にする必要があります。NQA サーバは。指定されたアドレスとポート番号で NQA クライアントからの要求に応答します。IP アドレスとポート番号は NQA クライアントが設定したものと一致する必要があります。また現在リスニングしているものとは別にする必要があります。

NQA サーバ上で、各 IP アドレスとポート番号に対応した複数の TCP、UDP リスニングサービスを設定することができます。リスニングサービスは NQA サーバで固有にする必要があります。IP アドレスとポート番号は NQA クライアントで設定された IP アドレスとポート番号と同一にする必要があります。

以下に NQA サーバの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. NQA サーバを有効にする	**nqa server enable**	デフォルト：無効
3. TCP、UDP リスニングサービスを設定する	● TCPリスニングサービスを設定する： **nqa server tcp-connect** *ip-address port-number* [**tos** *tos*] ● UDPリスニングサービスを設定する： **nqa server udp-echo** *ip-address port-number* [**tos** *tos*]	NQAサーバによって送信された応答パケットのIPパケットヘッダのToS値を指定することができます。 デフォルトのToS値：0

3.4 NQAクライアントの有効化

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． NQA クライアントを有効にする	**nqa agent enable**	デフォルト：有効 NQAクライアントを有効にしたのちNQAの設定が適用されます。

3.5 NQAクライアントのNQAテストの設定

3.5.1 NQA テストの設定作業リスト

作業リスト
（必須設定項目） 少なくとも1つを設定してください。 ● ICMPエコーテストの設定 ● ICMPジッタテストの設定 ● DHCPテストの設定 ● DNSテストの設定 ● FTPテストの設定 ● HTTPテストの設定 ● UDPジッタテストの設定 ● SNMPテストの設定 ● TCPテストの設定 ● UDPエコーテストの設定 ● UDP tracertの設定 ● DLSwテストの設定 ● パスジッタの設定
（オプション設定項目）NQAテストのオプションパラメータの設定
（オプション設定項目） しきい値監視機能の設定
（オプション設定項目） NQA統計情報収集機能の設定
（オプション設定項目） NQA履歴記録保存の設定
（必須設定項目）NQAクライアントにおけるNQAテストのスケジューリング

3.5.2 ICMP エコーテストの設定

ICMP エコーテストは宛先装置の到達可能性をテストします。ICMP エコーテストは **ping** コマンドと同等の機能ですが、さらに詳細な情報が得られます。送信元と宛先間で複数のパスがある場合、ICMP エコーテストでネクストホップを指定できます。

以下に ICMP エコーテストの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー

操作	コマンド	補足
2. NQA テストを作成し、NQA operation view に移行する	**nqa entry** *admin-name operation-tag*	デフォルト：設定なし
3. ICMP エコータイプを指定し、その view に移行する	**type icmp-echo**	―
4. ICMP エコーリクエストの宛先アドレスを指定する	● IPv4ネットワーク： **destination ip** *ip-address*	デフォルト：設定なし
5. （オプション設定項目）各 ICMP エコーリクエストのペイロードサイズを指定する	**data-size** *size*	デフォルト：100バイト
6. （オプション設定項目）各 ICMP エコーリクエストのペイロードに入る文字列を指定する	**data-fill** *string*	デフォルト：0001020304050607080 9（16進数表示）
7. （オプション設定項目）ICMP エコーリクエストの送信元アドレスを指定する	● 送信元インタフェースを指定する： **source interface** *interface-type interface-number* ● 送信元IPv4アドレスを指定する： **source ip** *ip-address*	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。 指定されていない場合、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アドレスが適用されます。 **source ip**コマンドと**source interface**コマンドの両方が設定された場合、最後に設定したコマンドが適用されます。 指定した送信元インタフェースはアップ状態でなくてはいけません。 送信元IPv4アドレスはローカルインタフェースのアドレスで、アップ状態でなくてはいけません。そうでなければICMPエコーテストに失敗します。
8. （オプション設定項目）ICMP エコーリクエストのネクストホップを指定する	ネクストホップIPv4アドレスを指定する： **next-hop ip** *ip-address*	デフォルト：設定なし

3.5.3 ICMP ジッタテストの設定

ICMP ジッタテストは、単方向および双方向のジッタを測定します。動作結果は、ネットワークがリアルタイムの音声サービスやビデオサービスなどのジッタに敏感なサービスを伝送できるかどうかを判断するのに役立ちます。

1. NQA クライアントは、宛先デバイスに ICMP パケットを送信します。

2. 宛先デバイスは、受信した各パケットにタイムスタンプを付け、パケットを NQA クライアントに返送します。

3. 応答を受信すると、NQA クライアントはタイムスタンプに従ってジッタを計算します。

ICMP ジッタテストは、プローブごとに宛先デバイスに多数の ICMP パケットを送信します。送信するパケット数は、probe packet-number コマンドを使用して決定されます。

以下に ICMP エコーテストの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. NQA テストを作成し、NQA operation view に移行する	**nqa entry** *admin-name operation-tag*	デフォルト：設定なし
3. ICMP ジッタタイプを指定し、その view に移行する	**type icmp-jitter**	ー
4. ICMP パケットの宛先 IP アドレスを指定する	**destination ip** *ip-address*	デフォルト：設定なし
5. プローブごとに送信される ICMP パケットの数を設定する	**probe packet-number** *number*	デフォルト：10
6. ICMP パケットの送信間隔を設定する	**probe packet-interval** *interval*	デフォルト：20ミリ秒
7. NQA クライアントが応答タイムアウトと見なすまでに、サーバからの応答を待機する時間を指定する	**probe packet-timeout** *timeout*	デフォルト：3000ミリ秒
8. ICMP パケットの送信元 IP アドレスを指定する	**source ip** *ip-address*	デフォルト：出力インタフェースのプライマリIPアドレス

3.5.4 DHCP テストの設定

DHCP テストは、DHCP サーバが DHCP クライアントリクエストに応答できるかどうかをテストします。また DHCP サーバから IP アドレスを取得する時間を計測することができます。

NQA クライアントは、DHCP サーバから IP アドレスを取得するために DHCP リクエストを転送する DHCP リレーエージェントをテストします。DHCP テストを実行するインタフェースはインタフェースの IP アドレスを変更しません。DHCP テストを完了したとき、取得した IP アドレスを解放するため、NQA クライアントはパケットを送信します。

以下に DHCP テストの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. NQA テストを作成し、NQA operation view に移行する	**nqa entry** *admin-name operation-tag*	デフォルト：設定なし

操作	コマンド	補足
3. DHCP タイプを指定し、その view に移行する	**type dhcp**	―
4. DHCP パケットの宛先 IP アドレスとしてDHCPサーバの IP アドレスを指定する	**destination ip** *ip-address*	デフォルト：設定なし
5. （オプション設定項目）DHCP リクエストパケットの送信元 IP アドレスを指定する	**source ip** *ip-address*	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。 指定する送信元IPアドレスはローカルインタフェースのIPアドレスにする必要があります。またローカルインタフェースはアップ状態にする必要があります。そうでない場合、プローブパケットを送信できません。 NQAクライアントはDHCPサーバに送信するDHCP要求の**giaddr**フィールドに送信元IPアドレスを追加します。

3.5.5 DNS テストの設定

DNS テストは DNS クライアントが DNS サーバを通してドメイン名を IP アドレスに変換する時間を測定します。

DNS テストは DNS 解決をテストします。取得した DNS エントリは保存しません。

以下に DNS テストの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. NQA テストを作成し、NQA operation view に移行する	**nqa entry** *admin-name operation-tag*	デフォルト：設定なし
3. DNS タイプを指定し、その view に移行する	**type dns**	―
4. DNS パケットの宛先アドレスとして DNS サーバの IP アドレスを指定する	**destination ip** *ip-address*	デフォルト：設定なし
5. 変換に必要なドメイン名を指定する	**resolve-target** *domain-name*	デフォルト：設定なし

3.5.6 FTP テストの設定

FTP テストはNQA クライアントがFTP サーバからファイルを転送するかダウンロードする時間をテストします。

FTP テストを設定するとき、以下の制限とガイドラインに従ってください。

- **filename** コマンドが設定され、**put** オペレーションが行われるとき、NQA クライアントにファイルが存在す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ために **get** オペレーションを行う場合、FTP サーバの指定した URL にファイルが存在す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 テストを行う場合、小さいサイズの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。

以下に FTP テストの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. NQA テストを作成し、NQA operation view に移行する	**nqa entry** *admin-name operation-tag*	デフォルト：設定なし
3. FTP タイプを指定し、その view に移行する	**type ftp**	―
4. 宛先のFTPサーバのURLを指定する	**url** *url*	デフォルト：指定なし 以下のどちらかのフォーマットでURLを入力します。 ● ftp://*host*/*filename* ● ftp://*host*:*port*/*filename* **get**オペレーションを行うとき、ファイル名が必要です。
5. （オプション設定項目）FTP リクエストパケットの送信元 IP アドレスを指定する	**source ip** *ip-address*	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。 送信元IPアドレスはローカルインタフェースのIPアドレスにする必要があります。またローカルインタフェースはアップ状態にする必要があります。そうでない場合、FTPは送信できません。
6. FTP のオペレーションタイプを指定する	**operation** { **get** | **put** }	デフォルト：**get** FTPサーバからファイルを取得します。
7. FTP ログインユーザ名を指定する	**username** *username*	デフォルト：設定なし
8. FTP ログインパスワードを指定する	**password** { **cipher** | **simple** } *string*	デフォルト：設定なし
9. （オプション設定項目）転送されるファイル名を指定する	**filename** *file-name*	デフォルト：設定なし この操作は**put**オペレーションが行われるときに必要です。

3.5.7 HTTP テストの設定

HTTP テストは NQA クライアントが HTTP サーバからデータを取得する時間をテストします。

以下に HTTP テストの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. NQA テストを作成し、NQA operation view に移行する	**nqa entry** *admin-name operation-tag*	デフォルト：設定なし
3. HTTP タイプを指定し、その view に移行する	**type http**	―
4. 宛先の HTTP サーバの URL を指定する	**url** *url*	デフォルト：指定なし 以下のどちらかのフォーマットでURLを入力します。 ● http://*host*/*resource* ● http://*host*:*port*/*resource*
5. HTTP ログインユーザ名を指定する	**username** *username*	デフォルト：設定なし
6. HTTP ログインパスワードを指定する	**password** { **cipher** | **simple** } *password*	デフォルト：設定なし
7. （オプション設定項目）リクエストパケットの送信元 IP アドレスを指定する	**source ip** *ip-address*	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。 送信元IPアドレスはローカルインタフェースのIPアドレスにする必要があります。またローカルインタフェースはアップ状態にする必要があります。そうでない場合、リクエストは送信できません。
8. （オプション設定項目）HTTP オペレーションタイプを指定する	**operation** { **get** | **post** }	デフォルト：**get** HTTPサーバからファイルを取得します。
9. （オプション設定項目）HTTP バージョンを指定する	**version** { **v1.0** | **v1.1** }	デフォルト：HTTP 1.0

3.5.8 UDP ジッタテストの設定

注意：

UDP ジッタテストをポート番号 1～1023 で行わないでください。1～1023 を使用した場合 NQA テストは失敗するか、このポートに該当するサービスが動作しなくなります。

ジッタは相互のパケット遅延の変動値を意味します。UDP ジッタテストはネットワークで音声サービスやビデオサービスなどのジッタに敏感なリアルタイムサービスを行えるかどうか確認するため、片方向、双方向のジッタをテストします。

UDP ジッタテストは以下のように動作します。

1) NQA クライアントは通常の間隔で宛先ポートに UDP パケットを送信します。
2) 宛先装置は、受信した各パケットにタイムスタンプを追加し、NQA クライアントにパケットを送り返します。
3) 応答を受信すると、NQA クライアントは、タイムスタンプに従ってジッタを計算します。

UDP ジッタテストは、NQA サーバと NQA クライアントの両方が必要です。UDP ジッタテストを実行する前に、NQA サーバで UDP リスニングサービスの設定を行う必要があります。UDP リスニングサービスの詳細は、本章の *"NQA サーバの設定"* を参照してください。

以下に UDP ジッタテストの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. NQA テストを作成し、NQA operation view に移行する	**nqa entry** *admin-name operation-tag*	デフォルト：設定なし
3. UDP ジッタタイプを指定し、その view に移行する	**type udp-jitter**	―
4. UDP パケットの宛先アドレスを指定する	**destination ip** *ip-address*	デフォルト：設定なし 宛先アドレスはNQAサーバでリスニングサービスを行っているIPアドレスと同一です。
5. UDP パケットの宛先ポートを指定する	**destination port** *port-number*	デフォルト：設定なし 宛先ポートはNQAサーバでリスニングサービスを行っているポートと同一です。

操作	コマンド	補足
6. （オプション設定項目）UDP パケットの送信元 IP アドレスを指定する	● IPv4ネットワーク **source ip** *ip-address*	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。 送信元IPアドレスはローカルインタフェースのIPアドレスにする必要があります。またローカルインタフェースはアップ状態にする必要があります。そうでない場合、UDPパケットは送信できません。
7. （オプション設定項目）UDP パケットの送信元アドレスを指定する	● IPv4ネットワーク **destination ip** *ip-address*	デフォルト：設定なし
8. （オプション設定項目）UDP パケットの送信元アドレスを指定する	**source port** *port-number*	デフォルト：設定なし
9. （オプション設定項目）各 UDP パケットのペイロードサイズを指定する	**data-size** *size*	デフォルト：100バイト
10. （オプション設定項目）各 UDP パケットのペイロードで使われる文字列を指定する	**data-fill** *string*	デフォルト：00010203040506070809（16進数表示）
11. （オプション設定項目）UDP ジッタテストで送信する UDP パケット数を指定する	**probe packet-number** *packet-number*	デフォルト：10
12. （オプション設定項目）UDP パケットを送信する間隔を設定する	**probe packet-interval** *interval*	デフォルト：20ミリ秒
13. （オプション設定項目）NQA クライアントの UDP パケットの受信待ち時間を指定する	**probe packet-timeout** *timeout*	デフォルト：3000ミリ秒

🕮 **メモ：**

display nqa result コマンドあるいは **display nqa statistics** コマンドを使用して UDP ジッタテストを確認してください。**display nqa history** コマンドは、UDP ジッタテストの結果や統計情報を表示しません。

3.5.9 SNMP テストの設定

SNMP テストは NQA クライアントが SNMP パケットを SNMP エージェントに送信し、SNMP エージェントから応答パケットを受信する時間を測定します。

以下に SNMP テストの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. NQA テストを作成し、NQA operation view に移行する	**nqa entry** *admin-name operation-tag*	デフォルト：設定なし
3. SNMP タイプを指定し、その view に移行する	**type snmp**	ー
4. SNMP パケットの宛先アドレスを指定する	**destination ip** *ip-address*	デフォルト：設定なし
5. （オプション設定項目）SNMP パケットの送信元ポート番号を指定する	**source port** *port-number*	デフォルト：設定なし
6. （オプション設定項目）SNMP パケットの送信元 IP アドレスを指定する	**source ip** *ip-address*	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。 送信元IPアドレスはローカルインタフェースのIPアドレスにする必要があります。またローカルインタフェースはアップ状態にする必要があります。そうでない場合、SNMPパケットは送信できません。
7. SNMP パケットの宛先ポート番号を指定する	**destination port** *port-number*	デフォルト：161

3.5.10 TCP テストの設定

TCP テストは、NQA クライアントと NQA サーバ上のポート間で TCP 接続が確立される時間を測定するために使われます。これにより指定したサーバのポートの有効性と能力を判断します。

TCP テストは NQA サーバと NQA クライアントの両方が必要です。TCP テストを実行する前に、NQA サーバで TCP リスニングサービスの設定を行う必要があります。TCP リスニングサービスの詳細は、本章の *“NQA サーバの設定”* を参照してください。

以下に TCP テストの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. NQA テストを作成し、NQA operation view に移行する	**nqa entry** *admin-name operation-tag*	デフォルト：設定なし
3. TCP タイプを指定し、その view に移行する	**type tcp**	ー
4. TCP パケットの宛先アドレスを指定する	● IPv4ネットワーク **destination ip** *ip-address*	デフォルト：設定なし 宛先アドレスはNQAサーバでリスニングサービスを行っているIPアドレスです。

操作	コマンド	補足
5. TCP パケットの宛先ポート番号を指定する	**destination port** *port-number*	デフォルト：設定なし 宛先ポート番号はNQAサーバでリスニングサービスを行っているポート番号です。
6. （オプション設定項目）TCP パケットの送信元 IP アドレスを指定する	● IPv4ネットワーク **source ip** *ip-address*	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。 送信元IPアドレスはローカルインタフェースのIPアドレスにする必要があります。またローカルインタフェースはアップ状態にする必要があります。そうでない場合、TCPパケットは送信できません。

3.5.11 UDP エコーテストの設定

UDP エコーテストはクライアントと NQA サーバの UDP ポート間のラウンドトリップ時間をテストします。

UDP エコーテストは、NQA サーバと NQA クライアントの両方が必要です。UDP エコーテストを行う前に、NQA サーバで UDP をリスニングするサービスを設定してください。

以下に UDP エコーテストの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. NQA テストを作成し、NQA operation view に移行する	**nqa entry** *admin-name operation-tag*	デフォルト：設定なし
3. UDP エコータイプを指定し、その view に移行する	**type udp-echo**	ー
4. UDP パケットの宛先アドレスを指定する	● IPv4ネットワーク **destination ip** *ip-address*	デフォルト：設定なし 宛先アドレスは、NQAサーバでリスニングサービスが設定されたIPアドレスと同一でなくてはいけません。
5. UDP パケットの宛先ポートを指定する	**destination port** *port-number*	デフォルト：設定なし 宛先ポート番号は、NQAサーバでリスニングサービスが設定されたポート番号と同一でなくてはいけません。
6. （オプション設定項目）各 UDP パケットのペイロードサイズを指定する	**data-size** *size*	デフォルト：100バイト

操作	コマンド	補足
7. （オプション設定項目）各 UDP パケットのペイロードに入る文字列を指定する	**data-fill** *string*	デフォルト：00010203040506070809（16進数表示
8. （オプション設定項目）UDP パケットの送信元ポートを指定する	**source port** *port-number*	デフォルト：設定なし
9. （オプション設定項目）UDP パケットの送信元 IP アドレスを指定する	● IPv4 ネットワーク **source ip** *ip-address*	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。 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、アップ状態でなくてはいけません。 そうでなければUDPパケットが送信できません。

3.5.12 UDP tracert の設定

UDP tracert は、送信元デバイスから宛先デバイスへのルーティングパスを決定します。

UDP tracert は、プローブごとのパスに沿ってホップに UDP パケットを送信します。

I. 前提条件

UDP tracert を設定する前に、次のタスクを実行する必要があります。

- 送信元デバイスと宛先デバイス間の中間デバイスで、ICMP 時間超過メッセージの送信を有効にします。中間デバイスが QX シリーズの場合は、ip ttl-expires enable コマンドを使用します。
- 宛先デバイスで ICMP 宛先到達不能メッセージの送信を有効にします。宛先デバイスが QX シリーズの場合は、ip unreachables enable コマンドを使用します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. NQA テストを作成し、NQA operation view に移行する	**nqa entry** *admin-name operation-tag*	デフォルト：設定なし
3. UDP tracert タイプを指定し、その view に移行する	**type udp-echo**	ー
4. 操作対象の機器を指定する	**destination ip** *ip-address*	デフォルト：設定なし
5. UDP パケットの宛先ポート番号を指定する	**destination port** *port-number*	デフォルト：33434
6. UDP パケットの出力インタフェースを指定する	**out interface** *interface-type interface-number*	デフォルト：

操作	コマンド	補足
7. UDP パケットの送信元 IP アドレスを指定する	インタフェースを指定する **source interface** *interface-type interface-number* IPアドレスを指定する **source ip** *ip-address*	デフォルト：
8. UDP パケットの送信元ポート番号を指定する	**source port** *port-number*	デフォルト : 未使用ポートをランダムに選択する
9. (オプション設定項目) 各 UDP パケットのペイロードサイズを設定する	**data-size** *size*	デフォルト：100byte
10. (オプション設定項目) フラグメンテーションなし機能を有効にする	**no-fragment enable**	デフォルト：無効

3.5.13 音声テストの設定

⚠ **注意**：
音声テストでポート 1～1023 を使用しないでください。1～1023 を使用した場合、このポートに関連したサービスが使えなくなります。

音声テストは VoIP ネットワーク性能を測定します。

音声テストは以下のように動作します。

1) NQA クライアントは指定した間隔で音声パケットを宛先装置（NQA サーバ）に送信します。

   音声パケットは以下のコーデックタイプがあります。

   - G.711 A-law
   - G.711 μ-law
   - G.729 A-law

2) 宛先装置は、受信した各音声パケットにタイムスタンプを追加し、NQA クライアントにパケットを送り返します。
3) 応答を受信すると、NQA クライアントは、タイムスタンプに従ってジッタと 1 方向遅延を計算します。

VoIP ネットワーク性能に反映される以下のパラメータは、音声テストによって収集されたメトリックを使用して計算することができます。

- **ICPIF（Calculated Planning Impairment Factor）**－パケットのロスや遅延による VoIP ネットワークの音声データの減衰を測定します。高い値は低いサービス品質を表します。
- **MOS（Mean Opinion Scores）**－ICPIF を使用して得られた 1～5 の MOS の値です。高い値は高いサービス品質を表します。

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。

音声テストは、NQA サーバと NQA クライアントの両方が必要です。音声テストを実行する前に、NQA サーバで UDP リスニングサービスの設定を行う必要があります。UDP リスニングサービスの詳細は、本章の *"NQA サーバの設定"* を参照してください。

1 回の音声テストで 1 回のテストが行われます。

以下に音声テストの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. NQA テストを作成し、NQA operation view に移行する	**nqa entry** *admin-name operation-tag*	デフォルト：設定なし
3. 音声タイプを指定し、その view に移行する	**type voice**	ー
4. 音声パケットの宛先アドレスを指定する	**destination ip** *ip-address*	デフォルト：設定なし 宛先アドレスは、NQAサーバでリスニングサービスが設定されたIPアドレスと同一でなくてはいけません。
5. 音声パケットの宛先ポートを指定する	**destination port** *port-number*	デフォルト：設定なし 宛先ポートはNQAサーバでリスニングサービスを行っているポートです。
6. （オプション設定項目）コーデックタイプを指定する	**codec-type** { **g711a** | **g711u** | **g729a** }	デフォルト：G.711 A-law
7. （オプション設定項目）計算される MOS と ICPIF 値のアドバンテージファクタを設定する	**advantage-factor** *factor*	デフォルト：0
8. （オプション設定項目）音声パケットの送信元 IP アドレスを指定する	**source ip** *ip-address*	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。 送信元IPアドレスはローカルインタフェースのIPアドレスにする必要があります。またローカルインタフェースはアップ状態にする必要があります。そうでない場合、音声パケットは送信できません。
9. （オプション設定項目）音声パケットの送信元ポート番号を指定する	**source port** *port-number*	デフォルト：設定なし
10. （オプション設定項目）音声パケットのペイロードサイズを指定する	**data-size** *size*	デフォルト: コーデックタイプによって異なります。 G.711A-law、G.711 μ-lawは172バイト、G.729 A-lawは32バイトです。
11. （オプション設定項目）各 UDP パケットのペイロードで使われる文字列を指定する	**data-fill** *string*	デフォルト： 00010203040506070809（16進数表示）

操作	コマンド	補足
12.（オプション設定項目）音声テストで送信する UDP パケット数を指定する	**probe packet-number** *packet-number*	デフォルト：1000
13.（オプション設定項目）音声パケットを送信する間隔を設定する	**probe packet-interval** *interval*	デフォルト：20ミリ秒
14.（オプション設定項目）NQA クライアントの音声パケットの受信待ち時間を指定する	**probe packet-timeout** *timeout*	デフォルト：5000ミリ秒

🕮 **メモ：**

display nqa result コマンドあるいは **display nqa statistics** コマンドを使用して音声テストを確認してください。**display nqa history** コマンドは、音声テストの結果や統計情報を表示しません。

3.5.14 DLSw テストの設定

DLSw テストは DLSw 装置の応答時間を測定します。

以下に DLSw テストの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. NQA テストを作成し、NQA operation view に移行する	**nqa entry** *admin-name operation-tag*	デフォルト：設定なし
3. DLSw タイプを指定し、その view に移行する	**type dlsw**	―
4. プローブパケットの宛先 IP アドレスを指定する	**destination ip** *ip-address*	デフォルト：設定なし
5.（オプション設定項目）プローブパケットの送信元 IP アドレスを指定する	**source ip** *ip-address*	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。 送信元IPアドレスはローカルインタフェースのIPアドレスにする必要があります。またローカルインタフェースはアップ状態にする必要があります。そうでない場合、プローブパケットは送信できません。

3.5.15 パスジッタの設定

パスジッタ動作は、NQA クライアントから宛先へのパス上の各ホップへのジッタ、負のジッタ、および正のジッタを測定します。

パスジッタ動作は、プローブごとに次の手順を実行します。

1. NQA クライアントから tracert を介して宛先へのパスを取得します。最大 64 ホップを検出できます。
2. パス上の各ホップに多数の ICMP エコー要求を送信します。送信する ICMP エコー要求の数は、probe packet-number コマンドを使用して設定します。

I. 前提条件

UDP tracert を設定する前に、次のタスクを実行する必要があります。

- 送信元デバイスと宛先デバイス間の中間デバイスで、ICMP 時間超過メッセージの送信を有効にします。中間デバイスが QX シリーズの場合は、ip ttl-expires enable コマンドを使用します。
- 宛先デバイスで ICMP 宛先到達不能メッセージの送信を有効にします。宛先デバイスが QX シリーズの場合は、ip unreachables enable コマンドを使用します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. NQA テストを作成し、NQA operation view に移行する	**nqa entry** *admin-name operation-tag*	デフォルト：設定なし
3. パスジッタの種類を指定し、その view に移行する	**type path-jitter**	―
4. ICMP エコー要求の宛先 IP アドレスを指定する	**destination ip** *ip-address*	デフォルト：設定なし
5. ICMP エコー要求の送信元 IP アドレスを指定する	**source ip** *ip-address*	デフォルト：33434
6. パスジッタ動作のプローブパラメータを設定する	プローブごとに送信する ICMPエコー要求の数を設定する **probe packet-number** *number*	デフォルト：10
	ICMPエコー要求の送信間隔を設定する **probe packet-interval** *interval*	デフォルト：20ミリ秒
	NQAクライアントが応答タイムアウトと見なすまでに、サーバからの応答を待機する時間を指定する **probe packet-timeout** *timeout*	デフォルト：3000ミリ秒
7. （オプション設定項目）各 ICMP エコー要求のペイロードサイズを設定する	**data-size** *size*	デフォルト：100byte

操作	コマンド	補足
8. （オプション設定項目）ICMP エコー要求のペイロード充填文字列を指定する	**data-fill** *string*	デフォルト：16進数の 00010203040506070809

3.5.16 NQA テストのオプションパラメータの設定

テストグループを指定しない場合、パラメータはすべてのテストタイプに適用されます。

NQA テストのオプションパラメータは 1 回のテストのみ有効です。

以下に NQA テストのオプションパラメータの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. NQA テストを作成し、NQA operation view に移行する	**nqa entry** *admin-name operation-tag*	デフォルト：設定なし
3. NQA テストタイプを指定し、その view に移行する	**type** { **dhcp** | **dlsw** | **dns** | **ftp** | **http** | **icmp-echo** | **snmp** | **tcp** | **udp-echo** | **udp-jitter** | **voice** }	ー
4. 説明を設定する	**description** *text*	デフォルト：設定なし
5. NQA テストを連続して行う間隔を指定する	**frequency** *interval*	デフォルト： 音声テストは6000ミリ秒、他のテストは0msです。 1回のテストで1回のテストが実行されます。 間隔が終了したとき、テストが完了していない場合、次のテストは開始しません。
6. 1 回の NQA テストの検査回数を指定する	**probe count** *times*	デフォルト：1回 音声テストでは無効です。1回のテストで1回のテストが実行されます。
7. NQA テストのタイムアウト時間を指定する	**probe timeout** *timeout*	デフォルト：3000ms UDPジッタテストと音声テストでは無効です。
8. テストパケットの TTL を指定する	**ttl** *value*	デフォルト：20 DHCPテストでは無効です。
9. NQA テストパケットの IP パケットヘッダの ToS 値を設定する	**tos** *value*	デフォルト：0
10. ルーティングテーブルバイパス機能を有効にする	**route-option bypass-route**	デフォルト：無効 DHCPテストでは無効です。

3.5.17 しきい値監視機能の設定

I. しきい値タイプ

NQA テストは以下のしきい値タイプをサポートします。

- **平均** – モニタリングされた性能の平均値が、上限あるいは下限を超えた場合、しきい値違反が発生します。
- **合計** – テストのモニタデータがしきい値を違反した回数の合計を監視します。回数の合計数が特定の値に達するか超えた場合、しきい値違反が発生します。
- **連続** – テストグループを開始してからのモニタデータのしきい値違反の連続回数を監視します。モニタデータのしきい値違反の連続回数が特定の回数になった場合、しきい値違反が発生します。

平均、合計のしきい値タイプは NQA テストごとにカウントされますが、連続タイプはテストグループが開始されてからの時間となります。

II. トリガー動作

以下のアクションがトリガー動作となります。

- **none** – NQA は端末画面にのみ結果を表示します。NMS にトラップを送信しません。
- **trap-only** – NQA は端末画面に結果を表示します。NMS にトラップを送信します。
- **trigger-only** – NQA は端末画面に結果を表示します。コラボレーションに関連づけられたほかのモジュールにトラップを送信します。

QX シリーズはトリガー動作 **trigger-only** をサポートしていません。

DNS テストは、トラップメッセージの送信動作をサポートしません。

III. リアクションエントリ

リアクションエントリでは、しきい値監視を行うため、監視対象、しきい値タイプ、トリガー動作を実装します。

リアクションエントリの状態には、無効、しきい値超過、しきい値未満があります。

- NQA のテストグループが開始する前は、リアクションエントリは無効の状態です。
- しきい値が違反している場合、エントリの状態はしきい値超過に設定されます。それ以外の場合、エントリの状態はしきい値未満に設定されています。

リアクションエントリの動作が trap-only の場合、トラップメッセージはエントリの状態が変化したときに NMS に送信されます。

IV. 設定手順

しきい値監視の設定を行う前に、**snmp-agent target-host** コマンドを使用してトラップメッセージの宛先アドレスを設定してください。このコマンドの詳細は、QX-W2300AC シリーズアクセスコントローラコマンドマニュアルの“*17 ネットワーク管理と監視*”の”*4 章 SNMP*”を参照してください。

以下にしきい値監視機能の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. NQA テストを作成し、NQA operation view に移行する	**nqa entry** *admin-name operation-tag*	デフォルト：設定なし
3. 指定状況下になったときネットワーク管理サーバにトラップを送信する	**reaction trap** { **path-change** | **probe-failure** *consecutive-probe-failures* | **test-complete** | **test-failure** [*accumulate-probe-failures*] }	デフォルト：設定なし UDPジッタテストと音声テストは**test-complete**キーワードのみサポートしています。
4. しきい値監視機能を設定する	• 動作時間を監視する **reaction** *item-number* **checked-element probe-duration threshold-type** { **accumulate** *accumulate-occurrences* | **average** | **consecutive** *consecutive-occurrences* } **threshold-value** *upper-threshold lower-threshold* [**action-type** { **none** | **trap-only** }]	ICMPジッタ、UDPジッタ、UDP tracert、音声操作では未サポートです。
	• 障害時間を監視する **reaction** *item-number* **checked-element probe-fail threshold-type** { **accumulate** *accumulate-occurrences* | **consecutive** *consecutive-occurrences* } [**action-type** { **none** | **trap-only** }]	ICMPジッタ、UDPジッタ、UDP tracert、音声操作では未サポートです。
	• ラウンドトリップ時間を監視する **reaction** *item-number* **checked-element rtt threshold-type** { **accumulate** *accumulate-occurrences* | **average** } **threshold-value** *upper-threshold lower-threshold* [**action-type** { **none** | **trap-only** }]	ICMPジッタ、UDPジッタ、音声操作のみサポート
	• パケット損失を監視する **reaction** *item-number* **checked-element packet-loss threshold-type accumulate** *accumulate-occurrences* [**action-type** { **none** | **trap-only** }]	ICMPジッタ、UDPジッタ、音声操作のみサポート
	• 一方向ジッタを監視する **reaction** *item-number* **checked-element** { **jitter-ds** | **jitter-sd** } **threshold-type** { **accumulate** *accumulate-occurrences* | **average** } **threshold-value** *upper-threshold*	ICMPジッタ、UDPジッタ、音声操作のみサポート

操作	コマンド	補足
	lower-threshold [**action-type** { **none** | **trap-only** }]	
	● 一方向遅延を監視する **reaction** *item-number* **checked-element** { **owd-ds** | **owd-sd** } **threshold-value** *upper-threshold lower-threshold*	ICMPジッタ、UDPジッタ、音声操作のみサポート
	● ICPIF値を監視する **reaction** *item-number* **checked-element icpif threshold-value** *upper-threshold lower-threshold* [**action-type** { **none** | **trap-only** }]	音声操作のみサポート
	● MOS値を監視する **reaction** *item-number* **checked-element mos threshold-value** *upper-threshold lower-threshold* [**action-type** { **none** | **trap-only** }]	音声操作のみサポート

3.5.18 NQA 統計情報収集機能の設定

NQA は統計情報グループとして同一の収集間隔で統計情報を収集します。統計情報グループについて情報を表示するには、**display nqa statistics** コマンドを使用します。

NQA は、1 回のみの NQA テストの統計情報グループを作成しません。**frequency** コマンドを使用し、テスト間隔を 0 に設定した場合、NQA は統計情報グループを作成しません。

以下に NQA 統計情報収集機能の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． NQA テストを作成し、NQA operation view に移行する	**nqa entry** *admin-name operation-tag*	デフォルト：設定なし
3． NQA テストタイプを指定し、その view に移行する	**type** { **dhcp** | **dlsw** | **dns** | **ftp** | **http** | **icmp-echo** | **snmp** | **tcp** | **udp-echo** | **udp-jitter** | **voice** }	―
4． （オプション設定項目）統計情報を収集する間隔を指定する	**statistics interval** *interval*	デフォルト：60分
5． （オプション設定項目）保持する統計情報グループ数の最大値を設定する	**statistics max-group** *number*	デフォルト：2グループ 最大値を0に設定すると統計情報を収集しません。 統計グループが最大数となったとき、新しい統計情報グループを保存するため、一番古い統計情報グループが削除されます。

3.5.19 NQA 履歴記録保存の設定

NQA 履歴記録保存機能は、UDP ジッタテストおよび音声テストでは利用できません。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. NQA テストを作成し、NQA operation view に移行する	**nqa entry** *admin-name operation-tag*	デフォルト：設定なし
3. NQA テストの履歴記録の保存を有効にする	**history-record enable**	デフォルト：無効
4. （オプション設定項目）履歴記録の保存期間を設定する	**history-record keep-time** *keep-time*	デフォルト：120分 保存期間が満了したとき記録が削除されます。
5. （オプション設定項目）履歴記録を保存できる最大数を指定する	**history-record number** *number*	デフォルト：50 もし最大数を超過した場合、一番古い履歴が削除されます。

3.5.20 NQA クライアントにおける NQA テストのスケジューリング

指定した開始時間と終了時間（開始時間＋テスト間隔）を設定することにより、NQA テストグループをスケジューリングできます。指定した開始時間がシステム時間を過ぎていた場合、NQA テストは即座に開始します。開始時間と終了時間が共にシステム時間を過ぎていた場合、NQA テストは行われません。**display clock** コマンドにより現在のシステム時間を確認することができます。

以下に NQA テストのスケジューリングを設定するときの制限とガイドラインを示します。

- NQA operation view あるいはスケジュールされた NQA テストの view に移行することはできません。
- システム時間を調整しても、開始されたあるいは終了した NQA テストには影響しません。開始する前の NQA テストはシステム時間の調整のみが適用されます。

以下に NQA クライアントにおける NQA テストをスケジューリングする設定を示します。

操作	コマンド
1. system view に移行する	**system-view**
2. NQA テストのスケジューリングのパラメータを指定する	**nqa schedule** *admin-name operation-tag* **start-time** { *hh:mm:ss* [*yyyy/mm/dd* | *mm/dd/yyyy*] | **now** } **lifetime** { *lifetime* | **forever** } [**recurring**]

3.6 NQAクライアントでのNQAテンプレートの設定

I. 制約事項とガイドライン

NQA テンプレートの一部の操作パラメータは、テンプレート設定またはテンプレートを使用する機能によって指定できます。両方を指定すると、テンプレート設定のパラメータが有効になります。

3.6.1 NQA の表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
NQAテストの履歴記録を表示する	**display nqa history** [*admin-name operation-tag*]
NQAテストの最新の結果を表示する	**display nqa result** [*admin-name operation-tag*]
NQAテストの統計情報を表示する	**display nqa statistics** [*admin-name operation-tag*]
NQAサーバ状態を表示する	**display nqa server**

3.7 NQA設定例

3.7.1 ICMP エコーテスト設定例

I. ネットワーク要件

図 3-3に示すように、ラウンドトリップ時間をテストするため、AC の NQA クライアントから Device A への ICMP エコーテストを設定します。AC のネクストホップは Device B です。

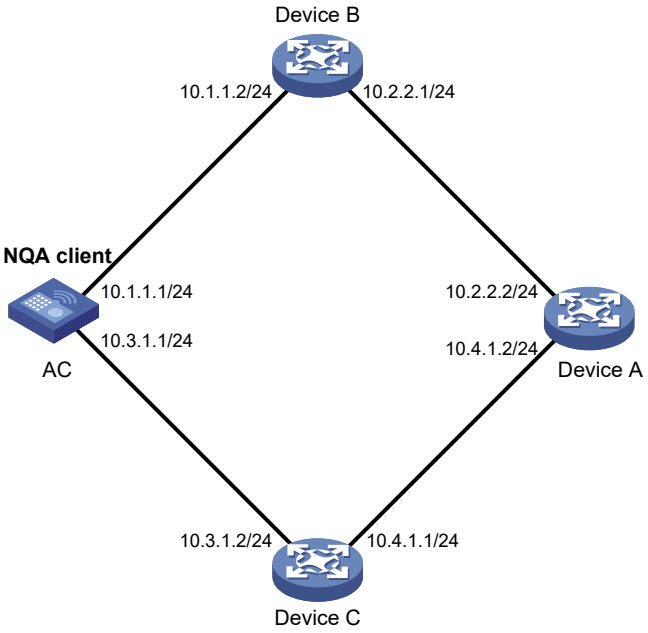


図 3-3 ネットワーク図

II. 設定手順

各インタフェースに IP アドレスを割り当てます（詳細は省略します）。

装置が互いに通信できるようにスタティックルートまたはルーティングプロトコルを設定します（詳細は省略します）。

ICMP エコーテストを作成します。

```
<AC> system-view
[AC] nqa entry admin test1
[AC-nqa-admin-test1] type icmp-echo
```

ICMP エコーリクエストの宛先 IP アドレスとして 10.2.2.2 を指定します。

```
[AC-nqa-admin-test1-icmp-echo] destination ip 10.2.2.2
```

ネクストホップとして 10.1.1.2 を設定します。ICMP エコーリクエストは Device B から Device A に送信されます。

```
[AC-nqa-admin-test1-icmp-echo] next-hop ip 10.1.1.2
```

ICMP エコーテスト検査を 10 回実行します。

```
[AC-nqa-admin-test1-icmp-echo] probe count 10
```

ICMP エコーテストのタイムアウト時間を 500ms に指定します。

```
[AC-nqa-admin-test1-icmp-echo] probe timeout 500
```

NQA テストを連続して行う間隔を 5000ms に設定します。

```
[AC-nqa-admin-test1-icmp-echo] frequency 5000
```

NQA 履歴記録の保存を有効にします。

```
[AC-nqa-admin-test1-icmp-echo] history-record enable
```

NQA 履歴記録の保存できる最大数を 10 に設定します。

```
[AC-nqa-admin-test1-icmp-echo] history-record number 10
[AC-nqa-admin-test1-icmp-echo] quit
```

ICMP エコーテストを開始します。

```
[AC] nqa schedule admin test1 start-time now lifetime forever
```

ICMP エコーテスト開始から一定の時間が経過した後、テストを停止します。

```
[AC] undo nqa schedule admin test1
```

ICMP エコーテストの最新の結果を表示します。

```
[AC] display nqa result admin test1
NQA entry (admin admin, tag test1) test results:
    Send operation times: 10              Receive response times: 10
    Min/Max/Average round trip time: 2/5/3
    Square-Sum of round trip time: 96
    Last succeeded probe time: 2011-08-23 15:00:01.2
  Extended results:
    Packet loss ratio: 0%
    Failures due to timeout: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
```

ICMP エコーテストの履歴記録を表示します。

```
[AC] display nqa history admin test1
NQA entry (admin admin, tag test) history records:
  Index      Response     Status           Time
  370        3            Succeeded        2007-08-23 15:00:01.2
  369        3            Succeeded        2007-08-23 15:00:01.2
  368        3            Succeeded        2007-08-23 15:00:01.2
  367        5            Succeeded        2007-08-23 15:00:01.2
  366        3            Succeeded        2007-08-23 15:00:01.2
  365        3            Succeeded        2007-08-23 15:00:01.2
  364        3            Succeeded        2007-08-23 15:00:01.1
  363        2            Succeeded        2007-08-23 15:00:01.1
  362        3            Succeeded        2007-08-23 15:00:01.1
  361        2            Succeeded        2007-08-23 15:00:01.1
```

出力は、AC からのパケットが Device B を通して Device A に送信できたことを示しています。NQA テスト中のパケットロスはありません。最小、最大、平均ラウンドトリップ時間はそれぞれ、2、5、3ms です。

3.7.2 FTP テスト設定例

I. ネットワーク要件

図 3-4に示すように、AC が FTP サーバにファイルをアップロードする時間を測定するために FTP テストを設定します。ログインユーザ名は admin、ログインパスワードは systemtest、FTP サーバに転送されるファイルは config.txt とします。



図 3-4 ネットワーク図

II. 設定手順

各インタフェースに IP アドレスを割り当てます（詳細は省略します）。

装置が互いに通信できるようにスタティックルートまたはルーティングプロトコルを設定します（詳細は省略します）。

FTP テストを作成します。

```
<AC> system-view
[AC] nqa entry admin test1
[AC-nqa-admin-test1] type ftp
```

FTP サーバの URL を指定します。

```
[AC-nqa-admin-test-ftp] url ftp://10.2.2.2
```

送信元 IP アドレス 10.1.1.1 を指定します。

```
[AC-nqa-admin-test1-ftp] source ip 10.1.1.1
```

Device が FTP サーバにファイル config.txt をアップロードするように設定します。

```
[AC-nqa-admin-test1-ftp] operation put
[AC-nqa-admin-test1-ftp] filename config.txt
```

FTP テストのユーザ名 admin を指定します。

```
[AC-nqa-admin-test1-ftp] username admin
```

FTP テストのパスワード systemtest を指定します。

```
[AC-nqa-admin-test1-ftp] password simple systemtest
```

履歴記録を保存するように設定します。

```
[AC-nqa-admin-test1-ftp] history-record enable
[AC-nqa-admin-test1-ftp] quit
```

FTP テストを開始します。

```
[AC] nqa schedule admin test1 start-time now lifetime forever
```

FTP テストを一定期間実行したのち、テストを停止します。

```
[AC] undo nqa schedule admin test1
```

FTP テストの最新の結果を表示します。

```
[AC] display nqa result admin test1
NQA entry (admin admin, tag test1) test results:
    Send operation times: 1              Receive response times: 1
    Min/Max/Average round trip time: 173/173/173
    Square-Sum of round trip time: 29929
    Last succeeded probe time: 2011-11-22 10:07:28.6
  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
```

FTP テストの履歴記録を表示します。

```
[AC] display nqa history admin test1
NQA entry (admin admin, tag test1) history records:
  Index      Response     Status           Time
  1          173          Succeeded        2011-11-22 10:07:28.6
```

出力は、AC が FTP サーバへのファイルアップロードに 173 ミリ秒かかったことを示しています。

3.7.3 UDP ジッタテスト設定例

I. ネットワーク要件

図 3-5に示すように、AC と Device 間のジッタ、遅延、ラウンドトリップ時間を測定するため、UDP ジッタテストを設定します。



図 3-5 ネットワーク図

II. 設定手順

1) 各インタフェースに IP アドレスを割り当てます（詳細は省略します）。
2) 装置が互いに通信できるようにスタティックルートまたはルーティングプロトコルを設定します（詳細は省略します）。
3) 各装置間で時刻が同期するように NTP を設定します（詳細は省略します）。
4) Device を設定します。

NQA サーバを有効にします。

```
<Device> system-view
[Device] nqa server enable
```

IP アドレス 10.2.2.2、UDP ポート 9000 でリスニングサービスを設定します。

```
[Device] nqa server udp-echo 10.2.2.2 9000
```

5) AC を設定します。

UDP ジッタテストを作成します。

```
<AC> system-view
[AC] nqa entry admin test1
[AC-nqa-admin-test1] type udp-jitter
```

UDP ジッタテストの宛先 IP アドレス 10.2.2.2 を設定します。

```
[AC-nqa-admin-test1-udp-jitter] destination ip 10.2.2.2
```

宛先ポート 9000 を設定します。

```
[AC-nqa-admin-test1-udp-jitter] destination port 9000
```

1000 ミリ秒の間隔で UDP ジッタテストを繰り返すように設定します。

```
[AC-nqa-admin-test1-udp-jitter] frequency 1000
[AC-nqa-admin-test1-udp-jitter] quit
```

UDP ジッタテストを開始します。

```
[AC] nqa schedule admin test1 start-time now lifetime forever
```

UDP ジッタテストを一定期間実行したのち、テストを停止します。

```
[AC] undo nqa schedule admin test1
```

UDP ジッタテストの最新の結果を表示します。

```
[AC] display nqa result admin test1
NQA entry (admin admin, tag test1) test results:
```

```
    Send operation times: 10            Receive response times: 10
    Min/Max/Average round trip time: 15/32/17
    Square-Sum of round trip time: 3235
    Last packet received time: 2011-05-29 13:56:17.6
  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: 4                  Min positive DS: 1
    Max positive SD: 21                 Max positive DS: 28
    Positive SD number: 5               Positive DS number: 4
    Positive SD sum: 52                 Positive DS sum: 38
    Positive SD average: 10             Positive DS average: 10
    Positive SD square-sum: 754         Positive DS square-sum: 460
    Min negative SD: 1                  Min negative DS: 6
    Max negative SD: 13                 Max negative DS: 22
    Negative SD number: 4               Negative DS number: 5
    Negative SD sum: 38                 Negative DS sum: 52
    Negative SD average: 10             Negative DS average: 10
    Negative SD square-sum: 460         Negative DS square-sum: 754
  One way results:
    Max SD delay: 15                    Max DS delay: 16
    Min SD delay: 7                     Min DS delay: 7
    Number of SD delay: 10              Number of DS delay: 10
    Sum of SD delay: 78                 Sum of DS delay: 85
    Square-Sum of SD delay: 666         Square-Sum of DS delay: 787
    SD lost packets: 0                 DS lost packets: 0
    Lost packets for unknown reason: 0
```

UDP ジッタテストの履歴記録を表示します。

```
[AC] display nqa statistics admin test1
NQA entry (admin admin, tag test1) test statistics:
  NO. : 1
    Start time: 2011-05-29 13:56:14.0
    Life time: 47 seconds
    Send operation times: 410           Receive response times: 410
    Min/Max/Average round trip time: 1/93/19
    Square-Sum of round trip time: 206176
  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: 410
    Min positive SD: 3                  Min positive DS: 1
    Max positive SD: 30                 Max positive DS: 79
    Positive SD number: 186             Positive DS number: 158
    Positive SD sum: 2602               Positive DS sum: 1928
    Positive SD average: 13             Positive DS average: 12
    Positive SD square-sum: 45304       Positive DS square-sum: 31682
    Min negative SD: 1                  Min negative DS: 1
    Max negative SD: 30                 Max negative DS: 78
    Negative SD number: 181             Negative DS number: 209
    Negative SD sum: 181                Negative DS sum: 209
    Negative SD average: 13             Negative DS average: 14
    Negative SD square-sum: 46994       Negative DS square-sum: 3030
  One way results:
    Max SD delay: 46                    Max DS delay: 46
    Min SD delay: 7                     Min DS delay: 7
    Number of SD delay: 410             Number of DS delay: 410
    Sum of SD delay: 3705               Sum of DS delay: 3891
```

```
    Square-Sum of SD delay: 45987          Square-Sum of DS delay: 49393
    SD lost packets: 0                   DS lost packets: 0
    Lost packets for unknown reason: 0
```

3.7.4 SNMP テスト設定例

I. ネットワーク要件

図 3-6に示すように、NQA クライアントが SNMP エージェントから応答を取得する時間を測定するため、SNMP テストを設定します。



図 3-6 ネットワーク図

II. 設定手順

1) 各インタフェースに IP アドレスを割り当てます（詳細は省略します）。
2) 装置が互いに通信できるようにスタティックルートまたはルーティングプロトコルを設定します（詳細は省略します）。
3) SNMP エージェントを設定します。

SNMP のバージョンを all に設定します。

```
<Device> system-view
[Device] snmp-agent sys-info version all
```

write コミュニティを private に設定します。

```
[Device] snmp-agent community write private
```

4) AC を設定します。

SNMP テストを作成します。

```
<AC> system-view
[AC] nqa entry admin test1
[AC-nqa-admin-test1] type snmp
```

SNMP テストの宛先 IP アドレスを 10.2.2.2 に設定します。

```
[AC-nqa-admin-test1-snmp] destination ip 10.2.2.2
```

履歴記録を保存するように設定します。

```
[AC-nqa-admin-test1-snmp] history-record enable
[AC-nqa-admin-test1-snmp] quit
```

SNMP テストを開始します。

```
[AC] nqa schedule admin test1 start-time now lifetime forever
```

SNMP テストを一定期間実行したのち、テストを停止します。

```
[AC] undo nqa schedule admin test1
```

SNMP テストの最新の結果を表示します。

```
[AC] display nqa result admin test1
NQA entry (admin admin, tag test1) test results:
    Send operation times: 1              Receive response times: 1
    Min/Max/Average round trip time: 50/50/50
    Square-Sum of round trip time: 2500
    Last succeeded probe time: 2011-11-22 10:24:41.1
  Extended results:
    Packet loss ratio: 0%
    Failures due to timeout: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
```

SNMP テストの履歴記録を表示します。

```
[AC] display nqa history admin test1
NQA entry (admin admin, tag test1) history records:
  Index      Response     Status           Time
  1          50           Succeeded        2011-11-22 10:24:41.1
```

出力は、AC が SNMP エージェントから応答を受信するのに 50 ミリ秒かかったことを示します。

3.7.5 HTTP テスト設定例

I. ネットワーク要件

図 3-7に示すように、HTTP サーバからデータを取得する時間をテストするため、NQA クライアントに HTTP テストを設定します。



図 3-7 ネットワーク図

II. 設定手順

各インタフェースに IP アドレスを割り当てます（詳細は省略します）。

装置が互いに通信できるようにスタティックルートまたはルーティングプロトコルを設定します（詳細は省略します）。

HTTP テストを作成します。

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

```
[AC] nqa entry admin test1
[AC-nqa-admin-test1] type http
```

HTTP サーバの URL を指定します。

```
[AC-nqa-admin-test-http] url http://10.2.2.2/index.htm
```

HTTP サーバからデータを取得するように HTTP テストを設定します。

```
[AC-nqa-admin-test1-http] operation get
```

HTTP version 1.0 を使用するように設定します。

```
[AC-nqa-admin-test1-http] version v1.0
```

履歴記録を保存するように設定します。

```
[AC-nqa-admin-test1-http] history-record enable
[AC-nqa-admin-test1-http] quit
```

HTTP テストを開始します。

```
[AC] nqa schedule admin test1 start-time now lifetime forever
```

HTTP テストを一定期間実行したのち、テストを停止します。

```
[AC] undo nqa schedule admin test1
```

HTTP テストの最新の結果を表示します。

```
[AC] display nqa result admin test1
NQA entry (admin admin, tag test1) test results:
    Send operation times: 1              Receive response times: 1
    Min/Max/Average round trip time: 64/64/64
    Square-Sum of round trip time: 4096
    Last succeeded probe time: 2011-11-22 10:12:47.9
  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
```

HTTP テストの履歴記録を表示します。

```
[AC] display nqa history admin test1
NQA entry (admin admin, tag test1) history records:
  Index      Response     Status           Time
  1          64           Succeeded        2011-11-22 10:12:47.9
```

出力は、AP が HTTP サーバからのデータを取得に 64 ミリ秒かかったことを示します。

3.7.6 TCP テスト設定例

I. ネットワーク要件

図 3-8に示すように、AC と Device が TCP 接続を確立するまでの時間を測定するために TCP テストを設定します。



図 3-8 ネットワーク図

II. 設定手順

1) 各インタフェースに IP アドレスを割り当てます（詳細は省略します）。
2) 装置が互いに通信できるようにスタティックルートまたはルーティングプロトコルを設定します（詳細は省略します）。
3) Device を設定します。

NQA サーバを有効にします。

```
<Device> system-view
[Device] nqa server enable
```

IP アドレス 10.2.2.2、TCP ポート 9000 でリスニングサービスを設定します。

```
[Device] nqa server tcp-connect 10.2.2.2 9000
```

4) AC を設定します。

TCP テストを作成します。

```
<AC> system-view
[AC] nqa entry admin test1
[AC-nqa-admin-test1] type tcp
```

宛先 IP アドレスを 10.2.2.2 に設定します。

```
[AC-nqa-admin-test1-tcp] destination ip 10.2.2.2
```

宛先ポート番号を 9000 に設定します。

```
[AC-nqa-admin-test1-tcp] destination port 9000
```

履歴記録を保存するように設定します。

```
[AC-nqa-admin-test1-tcp] history-record enable
[AC-nqa-admin-test1-tcp] quit
```

TCP テストを開始します。

```
[AC] nqa schedule admin test1 start-time now lifetime forever
```

TCP テストを一定期間実行したのち、テストを停止します。

```
[AC] undo nqa schedule admin test1
```

TCP テストの最新の結果を表示します。

```
[AC] display nqa result admin test1
NQA entry (admin admin, tag test1) test results:
    Send operation times: 1              Receive response times: 1
    Min/Max/Average round trip time: 13/13/13
    Square-Sum of round trip time: 169
```

```
    Last succeeded probe time: 2011-11-22 10:27:25.1
  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
```

TCP テストの履歴記録を表示します。

```
[AC] display nqa history admin test1
NQA entry (admin admin, tag test1) history records:
  Index      Response     Status           Time
  1          13           Succeeded        2011-11-22 10:27:25.1
```

出力は、AC の NQA サーバのポート 9000 との TCP 接続確立に 13 ミリ秒かかったことを示します。

3.7.7 UDP エコーテスト設定例

I. ネットワーク要件

図 3-9に示すように、AC と Device のラウンドトリップ時間をテストするために UDP エコーテストを設定します。宛先ポート番号は 8000 番です。



図 3-9 ネットワーク図

II. 設定手順

1) 各インタフェースに IP アドレスを割り当てます（詳細は省略します）。
2) 装置が互いに通信できるようにスタティックルートまたはルーティングプロトコルを設定します（詳細は省略します）。
3) Device を設定します。

NQA サーバを有効にします。

```
<Device> system-view
[Device] nqa server enable
```

IP アドレス 10.2.2.2、UDP ポート 8000 でリスニングサービスを設定します。

```
[Device] nqa server udp-echo 10.2.2.2 8000
```

4) AC を設定します。

UDP エコーテストを作成します。

```
<AC> system-view
[AC] nqa entry admin test1
[AC-nqa-admin-test1] type udp-echo
```

宛先 IP アドレスを 10.2.2.2 に設定します。

```
[AC-nqa-admin-test1-udp-echo] destination ip 10.2.2.2
```

宛先ポート番号を 8000 に設定します。

```
[AC-nqa-admin-test1-udp-echo] destination port 8000
```

履歴記録を保存するように設定します。

```
[AC-nqa-admin-test1-udp-echo] history-record enable
[AC-nqa-admin-test1-udp-echo] quit
```

UDP エコーテストを開始します。

```
[AC] nqa schedule admin test1 start-time now lifetime forever
```

UDP エコーテストを一定期間実行したのち、テストを停止します。

```
[AC] undo nqa schedule admin test1
```

UDP エコーテストの最新の結果を表示します。

```
[AC] display nqa result admin test1
NQA entry (admin admin, tag test1) test results:
    Send operation times: 1              Receive response times: 1
    Min/Max/Average round trip time: 25/25/25
    Square-Sum of round trip time: 625
    Last succeeded probe time: 2011-11-22 10:36:17.9
  Extended results:
    Packet loss ratio: 0%
    Failures due to timeout: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
```

UDP エコーテストの履歴記録を表示します。

```
[AC] display nqa history admin test1
NQA entry (admin admin, tag test1) history records:
  Index      Response     Status           Time
  1          25           Succeeded        2011-11-22 10:36:17.9
```

出力は、AC と Device のポート 8000 番との間でのラウンドトリップ時間が 25ms であったことを示します。

3.7.8 NQA コラボレーショテスト設定例

I. ネットワーク要件

図 3-10に示すように、AC のネクストホップとして Switch A と Switch B へのスタティックルートを設定します。スタティックルートの状態を監視するために、スタティックルート、トラックエントリ、ICMP エコーテストを関連付けます。

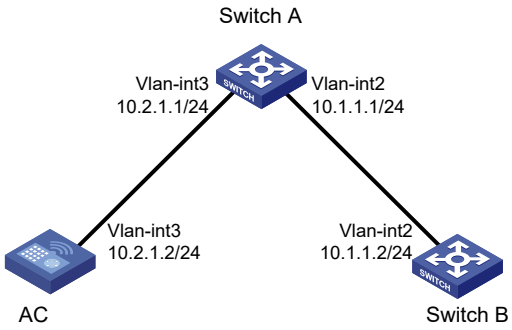


図 3-10 ネットワーク図

II. 設定手順

1)　各インタフェースに IP アドレスを割り当てます（詳細は省略します）。
2)　AC でスタティックルートを設定し、トラックエントリ 1 と関連付けます。

```
<AC> system-view
[AC] ip route-static 10.1.1.2 24 10.2.1.1 track 1
```

3)　ICMP エコーテストを設定します。

管理者名 admin とオペレーションタグ test1 で NQA オペレーションを作成します。

```
[AC] nqa entry admin test1
```

NQA オペレーションのタイプを ICMP エコーに設定します。

```
[AC-nqa-admin-test1] type icmp-echo
```

宛先 IP アドレスを 10.2.1.1 に設定します。

```
[AC-nqa-admin-test1-icmp-echo] destination ip 10.2.1.1
```

テスト間隔を 100 ミリ秒に設定します。

```
[AC-nqa-admin-test1-icmp-echo] frequency 100
```

リアクションエントリ 1 を作成します。連続して 5 回失敗するとコラボレーションが起動します。

```
[AC-nqa-admin-test1-icmp-echo] reaction 1 checked-element probe-fail
threshold-type consecutive 5 action-type trigger-only
[AC-nqa-admin-test1-icmp-echo] quit
```

ICMP テストを開始します。

```
[AC] nqa schedule admin test1 start-time now lifetime forever
```

4)　トラックエントリ 1 を作成し、NQA オペレーションのリアクションエントリ 1 と関連付けます。

```
[AC] track 1 nqa entry admin test1 reaction 1
```

III. 設定の確認

AC 上のすべてのトラックエントリについて情報を表示します。

```
[AC] display track all
Track ID: 1
  State: Positive
  Duration: 0 days 0 hours 0 minutes 0 seconds
  Notification delay: Positive 0, Negative 0 (in seconds)
  Tracked object:
    NQA entry: admin test1
    Reaction: 1
```

AC のルーティングテーブルのうち、すべてのアクティブなルートについて情報を表示します。

```
[AC] display ip routing-table

Destinations : 13        Routes : 13

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
0.0.0.0/32          Direct 0    0            127.0.0.1       InLoop0
10.1.1.0/24         Static 60   0            10.2.1.1        Vlan3
10.2.1.0/24         Direct 0    0            10.2.1.2        Vlan3
10.2.1.0/32         Direct 0    0            10.2.1.2        Vlan3
10.2.1.2/32         Direct 0    0            127.0.0.1       InLoop0
10.2.1.255/32       Direct 0    0            10.2.1.2        Vlan3
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
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
```

出力は、ネクストホップ 10.2.1.1 のスタティックルートがアクティブで、トラックエントリの状態が有効であることを示しています。

スイッチ A の VLAN インタフェース 3 の IP アドレスを削除します。

```
<SwitchA> system-view
[SwitchA] interface vlan-interface 3
[SwitchA-Vlan-interface3] undo ip address
```

AC 上のすべてのトラックエントリについて情報を表示します。

```
[AC] display track all
Track ID: 1
  State: Negative
  Duration: 0 days 0 hours 0 minutes 0 seconds
  Notification delay: Positive 0, Negative 0 (in seconds)
  Tracked object:
    NQA entry: admin test1
    Reaction: 1
```

AC のルーティングテーブルのうち、アクティブなルートについての要約情報を表示します。

```
[AC] 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
```

```
10.2.1.0/24          Direct 0    0           10.2.1.2        Vlan3
10.2.1.0/32          Direct 0    0           10.2.1.2        Vlan3
10.2.1.2/32          Direct 0    0           127.0.0.1       InLoop0
10.2.1.255/32        Direct 0    0           10.2.1.2        Vlan3
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
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
```

出力は、スタティックルートが存在せず、トラックエントリの状態が無効であることを示しています。

目次

このセクションのページは **17-x-x** です。

4章 SNMP 4-1
4.1 概要 4-1
4.1.1 SNMPの構造 4-1
4.1.2 MIBとviewベースのMIBアクセス管理 4-1
4.1.3 SNMPの動作 4-2
4.1.4 プロトコルバージョン 4-2
4.1.5 アクセスコントロールモード 4-3
4.2 SNMP基本パラメータの設定 4-3
4.2.1 SNMPv1あるいはSNMPv2c基本パラメータの設定 4-3
4.2.2 SNMPv3基本パラメータの設定 4-5
4.3 SNMPロギングの設定 4-6
4.4 SNMP通知の設定 4-7
4.4.1 SNMP notificationの有効化 4-7
4.4.2 ホストへnotificationを送信するSNMPエージェントの設定 4-8
4.5 SNMP通知の送信シミュレーション 4-9
4.6 SNMPの表示と維持 4-10
4.7 設定例 4-11
4.7.1 SNMPv1/SNMPv2cの設定例 4-11
4.7.2 SNMPv3の設定例 4-13

4章 SNMP

4.1 概要

SNMP（Simple Network Management Protocol）はネットワークで装置にアクセスし、操作させるための管理システムとして、ベンダ、物理的な特徴、相互接続技術に関係なく、広く使われているインタネット標準プロトコルです。

SNMP を使用することで、装置の状態のモニタリング、トラブルシューティング、コリジョンの統計情報やほかの情報の管理を行うため、ネットワーク管理者が、装置の情報を確認し、設定することができます。

4.1.1 SNMP の構造

SNMP は以下の機能で構成されています。

- **SNMP マネジャー** － NMS（network management system）上で動作し、ネットワーク内の SNMP-capable デバイスをモニタし管理します。
- **SNMP エージェント** － 管理対象デバイス上で動作し、NMS からのリクエストを受信し操作します。インタフェースの状態の変化などのイベント発生時に NMS に Trap を送信します。
- **MIB（Management Information Base）** － SNMP **マネジャー**が読み取り、設定するために、SNMP エージェントによって保持されているインタフェース状態や CPU 使用率などの変数を指定します。

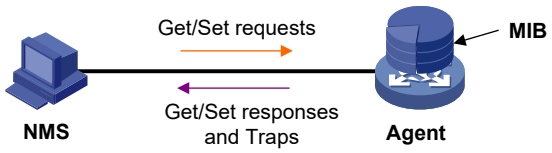


図 4-1 NMS、エージェント、MIB の関係

4.1.2 MIB と view ベースの MIB アクセス管理

MIB はツリー構造の「ノード」「オブジェクト」と呼ばれる変数を保存し、各ノードを固有の OID で区別します。OID はルートノードからリーフノードへのパスを示す番号列です。図 4-2では、オブジェクト B は OID {1.2.1.1}で区別されます。

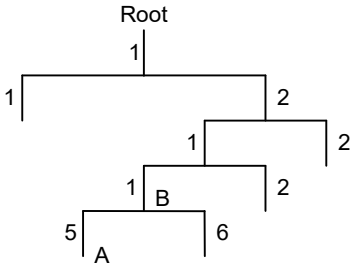


図 4-2 MIB ツリー

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）を表し、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。

MIB view は複数の view を持つことができます。複数の view は、*view-name oid-tree* の組み合わせで識別されます。

SNMP グループあるいはコミュニティに MIB view を割り当てることによって、MIB のアクセスを管理することができます。

4.1.3 SNMP の動作

SNMP は以下の基本的な動作を提供します。

- **Get** – エージェント MIB の SNMP オブジェクトノードを取得します。
- **Set** – エージェント MIB のオブジェクトノードの値を変更します。
- **Notification** – SNMP エージェントが NMS にイベントを通知するため、trap あるいは inform があります。Notification の 2 つのタイプの違いは、inform では ack（確認応答）が必要ですが、trap では必要ありません。trap は SNMPv1、SNMPv2c、SNMPv3 で有効ですが、inform は SNMPv2c、SNMPv3 でのみ有効です。

4.1.4 プロトコルバージョン

NMS と SNMP エージェントは相互に通信するため、同じ SNMP バージョンを使用する必要があります。

- **SNMPv1** – 認コミュニティ名で認証を行います。SNMP エージェントにアクセスするために、NMS は SNMP エージェントでセットしたものと同じコミュニティ名を使わなければなりません。NMS が使用するコミュニティ名がエージェントでセットしたものと違う場合、NMS はエージェントにアクセスするための SNMP セッションを構築することができない、もしくはエージェントからの Trap と Notification を受信することができません。
- **SNMPv2c** – コミュニティ名で認証を行います。SNMPv1 と互換を取り、より多くの動作モード、データ タイプ、エラーコードをサポートします。

- **SNMPv3** – USM （User-Based Security Model） を使ってセキュアな SNMP 通信を実現します。整合性、信頼性、および機密保持のために SNMP パケットを認証し暗号化する、認証とプライバシーのメカニズムを設定できます。

4.1.5 アクセスコントロールモード

SNMP は MIB オブジェクトにアクセスするため、以下のモードを使用します。

- VACM（View-based Access Control Model）モデルーVACM モードは MIB view を SNMP コミュニティやユーザ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。

もし同じ SNMP コミュニティやユーザに複数回割り当てた場合、最後に作成した設定が適用されます。

VACM モードは NMS から MIB オブジェクトにアクセスする権限のみ必要です。

4.2 SNMP基本パラメータの設定

SNMPv3 は SNMPv1、SNMPv2c と多くの点で異なります。章を分けて設定方法について説明します。

4.2.1 SNMPv1 あるいは SNMPv2c 基本パラメータの設定

以下に SNMPv1 あるいは SNMPv2c 基本パラメータの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. （オプション設定項目） SNMP エージェントを有効にする	**snmp-agent**	デフォルト：無効 **snmp-agent calculate-password** コマンドを除いた**snmp-agent** で始まるいずれかのコマンドで SNMP エージェントを有効にできます。 IPアドレスを設定するまで SNMPポートは開きません。
3. （オプション設定項目） システム連絡先を設定する	**snmp-agent sys-info contact** *sys-contact*	デフォルト：設定なし
4. （オプション設定項目） システム所在地を設定する	**snmp-agent sys-info location** *sys-location*	デフォルト：設定なし
5. SNMPv1 あるいは SNMPv2c を有効にする	**snmp-agent sys-info version** { **all** | { **v1** | **v2c** } * }	デフォルト：SNMPv3が有効

操作	コマンド	補足
6. （オプション設定項目） ローカルエンジン ID を変更する	**snmp-agent local-engineid** *engineid*	デフォルト：ローカルエンジン ID はCompany ID＋ device ID
7. （オプション設定項目） MIB view を作成または更新する	**snmp-agent mib-view** { **excluded** | **included** } *view-name oid-tree* [**mask** *mask-value*]	デフォルト：**ViewDefault** このviewは**iso**サブツリーのすべてのオブジェクトが対象ですが、**snmpUsmMIB**と**snmpVacmMIB**と**snmpModules.18**はアクセス可能です。 *view-name*、*old-tree*のペアはそれぞれviewのレコードを表します。別のMIBサブツリーマスクに同じレコード名を複数回指定した場合、最後の設定が有効です。デフォルトMIBビューの4つのサブツリーを除いて、最大16の一意のMIBビューレコードを作成できます。

8. SNMP アクセス権を設定する	• （アプローチ1） SNMPコミュニティを作成する：**snmp-agent community** { **read** | **write** } [**simple** | **cipher**] *community-name* [**mib-view** *view-name*] [**acl** { *acl-number* | **name** *acl-name* }] *
	• （アプローチ2） SNMPv1/SNMPv2cグループを作成し、グループにユーザを追加する：
	  • **snmp-agent group** { **v1** | **v2c** } *group-name* [**read-view** *view-name*] [**write-view** *view-name*] [**notify-view** *view-name*] [**acl** { *acl-number* | **name** *acl-name* }] *
	  • **snmp-agent usm-user** { **v1** | **v2c** } *user-name group-name* [**acl** { *acl-number* | **name** *acl-name* }] *
		どちらか一方のアプローチを使用します。
		デフォルト：SNMPグループあるいはSNMPコミュニティは設定なし
		アプローチ2の*user-name*はアプローチ1のコミュニティ名と同じで、NMBで設定されるコミュニティ名と同じでなければなりません。

9. （オプション設定項目） SNMP エージェントが送受信できる SNMP パケットの最大バイトサイズ（バイト）を設定する	**snmp-agent packet max-size** *byte-count*	デフォルト：1500バイト

4.2.2 SNMPv3 基本パラメータの設定

SNMPv3 ユーザはグループで管理されます。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、プライバシーキー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設定し、SNMP 間の通信が失敗しないようにするため、グループのセキュリティモデルの設定とセキュリティキーは、表 4-1に従い、NMS の設定に合わせる必要があります。

表 4-1 異なるセキュリティモデルの基本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キーワード	ユーザのセキュリティキー設定	補足
プライバシーあり、認証あり	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キーが設定されていない場合、SNMP 間の通信は失敗します。
プライバシーなし、認証あり	authentication	認証キー	認証キーが設定されていない場合、SNMP間の通信は失敗します。ユーザのプライバシーキー（ある場合）は影響しません。
認証なし、プライバシーなし	authentication あるいはprivacyのいずれもありません。	なし	認証キー、プライバシーキーが設定されても適用されません。

以下に SNMPv3 基本パラメータの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. （オプション設定項目） SNMP エージェントを有効にする	**snmp-agent**	デフォルト：無効 **snmp-agent calculate-password** コマンドを除いた**snmp-agent** で始まるいずれかのコマンドで SNMP エージェントを有効にできます。
3. （オプション設定項目） システム連絡先を設定する	**snmp-agent sys-info contact** *sys-contact*	デフォルト：設定なし
4. （オプション設定項目） システム所在地を設定する	**snmp-agent sys-info location** *sys-location*	デフォルト：設定なし
5. SNMPv3 を有効にする	**snmp-agent sys-info version v3**	デフォルト：有効

操作	コマンド	補足
6. （オプション設定項目） ローカルエンジン ID を設定する	**snmp-agent local-engineid** *engineid*	デフォルト：ローカルエンジン ID はCompany ID＋ device ID です。 ⚠ **重要：** ローカルエンジンIDの変更後、既存のSNMPv3ユーザと暗号キーは無効になります。SNMPv3ユーザと暗号キーを再設定してください。
7. （オプション設定項目） MIB view を作成または更新する	**snmp-agent mib-view** { **excluded** | **included** } *view-name oid-tree* [**mask** *mask-value*]	デフォルト：**ViewDefault** このview は**iso**サブツリーのすべてのオブジェクトが対象ですが、**snmpUsmMIB**と**snmpVacmMIB**と**snmpModules.18**はアクセス可能です。 *view-name*、*old-tree*のペアはそれぞれviewのレコードを表します。別のMIBサブツリーマスクに同じレコード名を複数回指定した場合、最後の設定が有効です。デフォルトMIBビューの4つのサブツリーを除いて、最大16の一意のMIBビューレコードを作成できます。
8. （オプション設定項目）SNMPv3 グループを作成する	**snmp-agent group v3** *group-name* [**authentication** | **privacy**] [**read-view** *view-name*] [**write-view** *view-name*] [**notify-view** *view-name*] [**acl** { *acl-number* | **name** *acl-name* }] *	デフォルト：設定なし
9. （オプション設定項目） 平文テキストキーを暗号キーに変換する	**snmp-agent calculate-password** *plain-password* **mode** { **3desmd5** | **3dessha** | **md5** | **sha** } { **local-engineid** | **specified-engineid** *engineid* }	―
10. SNMPv3 ユーザを作成する	**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** { *acl-number* | **name** *acl-name* }] *	**cipher**キーワードが指定されると、*auth-password*と*priv-password*は暗号キーとして使用されます。
11. （オプション設定項目） SNMP エージェントが送受信できる SNMP パケットの最大バイトサイズ（バイト）を設定する	**snmp-agent packet max-size** *byte-count*	デフォルト：1500バイト

4.3 SNMPロギングの設定

必要なときのみ SNMP ロギングを設定してください。SNMP ロギングを設定するとメモリに負担をかけ、装置の性能に影響を与える可能性があります。

SNMP エージェントは、GET リクエスト、SET リクエスト、SET 応答、SNMP 通知、SNMP 認証失敗をロギングしますが、GET 応答はロギングしません。

- **GET オペレーション** － エージェントは NMS の IP アドレス、アクセスノード名、ノード OID をロギングします。
- **SET オペレーション** － エージェントは NMS の IP アドレス、アクセスノード名、ノード OID、変数値、エラーコード、エラーインデックスをロギングします
- **通知トラッキング** － NMS に SNMP 通知を送信したのち、エージェントをロギングします。
- **SNMP 認証失敗** ー エージェントは SNMP 認証の失敗をロギングします。

SNMP モジュールは Information Center にログを送信します。

コンソールやログバッファなどの特定の宛先にメッセージを出力するため、Information Center を設定することができます。各ログエントリのノードフィールド（MIB ノード名）と値フィールド（MIB ノードの値）の合計最大サイズは 1024 バイトです。最大サイズを超過した場合、Information Center はフィールドのデータを切り捨てます。Information Center の詳細は、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“3 *システム管理*”の”*5 章 Information Center*”を参照してください。

以下に SNMP ロギングの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． （オプション設定項目）SNMP ロギングを有効にする	**snmp-agent log** { **all** | **authfail** | **get-operation** | **set-operation** }	デフォルト：無効
3． （オプション設定項目）SNMP 通知ロギングを有効にする	**snmp-agent trap log**	デフォルト：無効

4.4 SNMP通知の設定

SNMP エージェントはリンク状態の変更やユーザログイン、ログアウトなどの重要なイベントの notification （trap、inform）を NMS に通知します。特に説明がない限り、コマンドラインの **trap** キーワードは trap と inform を含みます。

4.4.1 SNMP notification の有効化

必要なときのみ SNMP notification を有効にしてください。SNMP notification はメモリに負担をかけ、装置の性能に影響を与える可能性があります。

インタフェースのリンク状態が変更したとき、以下を行ってください。

- **snmp-agent trap enable standard** [**linkdown** | **linkup**] *コマンドを設定し、グローバルで linkUp あるいは linkDown notification を有効にしてください。
- インタフェースで **enable snmp trap updown** コマンドを設定し、インタフェースで linkUp あるいは linkDown notification を有効にしてください。

モジュールで notification を有効にした後、notification がモジュールの設定に依存して作成されます。詳細は、各モジュールの設定ガイドを参照してください。

以下に SNMP notification を有効にする設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. notification を有効にする	**snmp-agent trap enable** [**configuration** | *protocol* | **standard** [**authentication** | **coldstart** | **linkdown** | **linkup** | **warmstart**] * | **system**]	デフォルト：**configuration**、**standard**、**system**が有効です。ほかのSNMP notificationはモジュールによって変わります。
3. interface view に移行する	**interface** *interface-type interface-number*	ー
4. リンク状態の notification を有効にする	**enable snmp trap updown**	デフォルト：有効

4.4.2 ホストへ notification を送信する SNMP エージェントの設定

ホストに trap あるいは inform する notification を送信する SNMP エージェントを設定することができます。一般的にホストは NMS で、解析や管理に使われます。trap を受信したとき、NMS は trap を受信するとき確認応答を送信しないため、trap は inform よりも少ないリソースで使用することができます。

I. 設定ガイドライン

ネットワークの輻輳が発生する、あるいは宛先に到達できないとき、SNMP エージェントはキューに notification をバッファします。キューのサイズと notification の保持時間（キューに保持できる最大時間）を設定することができます。notification は保持時間が満了したとき削除されます。notification のキューが一杯になったとき、もっとも古い notification が自動的に削除されます。

インタフェースの説明やインタフェースタイプを追加させるため、標準 linkUp/linkDown notification を拡張することができますが、NMS が拡張 SNMP メッセージをサポートしていることを確認する必要があります。

inform を送信するために、以下を確認してください。

- SNMP エージェントと NMS は SNMPv2c あるいは SNMPv3 を使用します。
- SNMPv3 が使用される場合、SNMPv3 基本設定を行う際に NMS の SNMP エンジン ID を設定してください。また SNMPv3 ユーザを作成するとき、SNMP エンジンの IP アドレスを指定してください。

II. 設定要件

- NMS として基本 SNMP の設定と同じように SNMP エージェントを設定してください。SNMPv1 あるいは SNMPv2c を使用する場合、コミュニティ名を設定してください。SNMPv3 を使用する場合、notification の SNMPv3 ユーザ、MIB view を設定してください。
- SNMP エージェントと NMS が互いに到達可能であるようにしてください。

III. 設定手順

以下にホストに notification を送信する SNMP エージェントの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. 宛先ホストを設定する	• （アプローチ1）宛先ホストにtrapを送信する： **snmp-agent target-host trap address udp-domain** { *address* } [**udp-port** *port-number*] **params securityname** *security-string* [**v1** | **v2c** | **v3** [**authentication** | **privacy**]] • （アプローチ2）宛先ホストにinformを送信する： **snmp-agent target-host inform address udp-domain** { *address* } [**udp-port** *port-number*] **params securityname** *security-string* { **v2c** | **v3** [**authentication** | **privacy**] }	どちらか一方を使用します。 デフォルト：設定なし
3. （オプション設定項目） notification の送信元アドレスを設定する	**snmp-agent** { **inform** | **trap** } **source** *interface-type* { *interface-number* }	デフォルト: SNMPは送信元IPアドレスとして出力インタフェースのIPアドレスを使用します。
4. （オプション設定項目） 拡張 linkUp/linkDown notification を有効にする	**snmp-agent trap if-mib link extended**	デフォルト：標準 linkUp/linkDown notificationを使用します
5. （オプション設定項目） notification キューサイズを設定する	**snmp-agent trap queue-size** *size*	デフォルト：100
6. （オプション設定項目） notification ライフタイムを設定する	**snmp-agent trap life** *seconds*	デフォルト：120秒

4.5 SNMP通知の送信シミュレーション

🕮 **メモ：**

simulate snmp-trap コマンドはソフトウェアバージョン 9.4.09 を含む以降のソフトウェアからサポートしています。

I. SNMP 通知の送信シミュレーションについて

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。

II. 前提条件

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。

III. 設定方法

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. SNMP 通知の送信シミュレートする	● すべてのSNMP通知をシミュレートする： **simulate snmp-trap all** [**ifindex** *ifindex*] ● 特定のSNMP通知をシミュレートする： **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>]	変数は通知ノードにより異なります。*n* の値は通知ノードの仕様に依存します。

4.6 SNMPの表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
連絡先、所在地、SNMP のバージョンを含むSNMPエージェントのシステム情報を表示する	**display snmp-agent sys-info** [**contact** | **location** | **version**] *

操作	コマンド
SNMPエージェント統計情報を表示する	**display snmp-agent statistics**
ローカルエンジンIDを表示する	**display snmp-agent local-engineid**
SNMPグループ情報を表示する	**display snmp-agent group** [*group-name*]
notificationキューの基本情報を表示する	**display snmp-agent trap queue**
notificationを送信できるモジュールおよびnotificationの状態（有効あるいは無効）を表示する	**display snmp-agent trap-list**
SNMPv3ユーザ情報を表示する	**display snmp-agent usm-user** [**engineid** *engineid* | **group** *group-name* | **username** *user-name*] *
SNMP v1またはSNMP v2c のコミュニティ情報を表示する	**display snmp-agent community** [**read** | **write**]
MIB view情報を表示する	**display snmp-agent mib-view** [**exclude** | **include** | **viewname** *view-name*]

4.7 設定例

4.7.1 SNMPv1/SNMPv2c の設定例

SNMPv1 の設定手順は SNMPv2c 設定手順と同一です。この設定例は SNMPv1 を使用します。

I. ネットワーク要件

図 4-3に示すように、NMS（1.1.1.2/24）は SNMPv1 で SNMP エージェント（1.1.1.1/24）を管理します。エージェントはイベントを報告する notification を NMS に自動的に送信します。

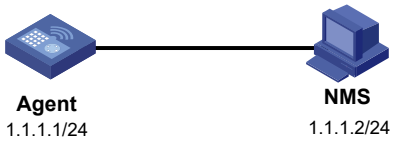


図 4-3 ネットワーク図

II. 設定手順

1) SNMP エージェントを設定します。

エージェントの IP アドレスを設定し、NMS と通信可能であることを確認します。（詳細は省略します。）

SNMPv1 を指定し、読み込みのみのコミュニティ **public** と読み書き可能なコミュニティ **private** を生成します。

```
<AC> system-view
[AC] snmp-agent sys-info version v1
[AC] snmp-agent community read public
[AC] snmp-agent community write private
```

エージェントの連絡先と所在地情報を設定します。

```
[AC] snmp-agent sys-info contact NEC
[AC] snmp-agent sys-info location Tokyo
```

SNMP notification を有効にし、SNMP trap の宛先として IP アドレスが 1.1.1.2 の NMS を設定し、コミュニティ名として **public** を使用します。（NMS が trap を受信できること確認するため、**snmp-agent target-host** コマンドで設定されている SNMP のバージョンを NMS と同一に指定します。）

```
[AC] snmp-agent trap enable
[AC] snmp-agent target-host trap address udp-domain 1.1.1.2 params securityname public v1
```

2) SNMP NMS を設定します。
   - SNMPv1 を指定します。
   - 読み込みのみのコミュニティ **public** と読み書き可能なコミュニティ **private** を作成します。
   - 必要に応じて、タイムアウト時間と再トライを行う最大数を設定します。

NMS の設定についての詳細は、NMS のマニュアルを参照してください。

メモ：

エージェントと NMS の SNMP 設定は同一にする必要があります。

III. 設定の確認

エージェントから Null0 インタフェースの MTU 値を取得します。取得に成功します。

```
Send request to 1.1.1.1/161 ...
Protocol version: SNMPv1
Operation: Get
Request binding:
1: 1.3.6.1.2.1.2.2.1.4.135471
Response binding:
1: Oid=ifMtu.135471 Syntax=INT Value=1500
Get finished
```

エージェントの MIB ノードの値を取得するため、wrong コミュニティ名を使用します。NMS で trap の認証に失敗していることがわかります。

```
1.1.1.1/2934 V1 Trap = authenticationFailure
SNMP Version = V1
Community = public
Command = Trap
Enterprise = 1.3.6.1.4.1.43.1.16.4.3.50
GenericID = 4
```

```
SpecificID = 0
Time Stamp = 8:35:25.68
```

4.7.2 SNMPv3 の設定例

I. ネットワーク要件

図 4-4に示すように、NMS（1.1.1.2/24）は SNMPv3 でエージェント（1.1.1.1/24）のインタフェース状態をモニタし管理します。エージェントはイベントを通知する notification を NMS に自動的に送信します。

NMS とエージェントは SNMP セッションを構成するときに認証を行います。認証アルゴリズムは SHA-1 で、認証キーは **123456TESTauth&!**です。NMS とエージェント間のパケットは、AES アルゴリズム、プライバシーキー**123456TESTencr&!**で暗号化されます。

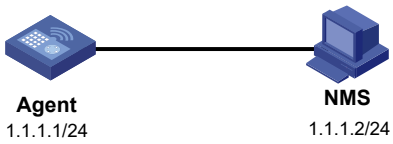


図 4-4 ネットワーク図

II. 設定手順

1) SNMP エージェントを設定します。

エージェントの IP アドレス 1.1.1.1/24 を設定し、NMS と通信可能であることを確認します。（詳細は省略します。）

SNMPv3 グループ **managev3group** を作成します。test view の SNMPv3 グループ **managev3group** に、アクセス権限を設定します。snmpMIB ノード（OID：1.3.6.1.2.1.11）下のオブジェクトを読み込みおよび書き込みができるように設定し、ほかの MIB オブジェクトはアクセスできないようにします。

```
AC> system-view
[AC] undo snmp-agent mib-view ViewDefault
[AC] snmp-agent mib-view included test snmp
[AC] snmp-agent group v3 managev3group privacy read-view test write-view test
```

SNMPv3 グループ **managev3group** にアクセス権限を設定します。test view のシステムノード（OID：1.3.6.1.2.1.1）とインタフェースノード（OID：1.3.6.1.2.1.2）下のオブジェクトを読み込みのみができるように設定します。

```
[AC] snmp-agent mib-view included test 1.3.6.1.2.1.1
[AC] snmp-agent mib-view included test 1.3.6.1.2.1.1
[AC] snmp-agent group v3 managev3group privacy read-view test
```

ユーザ **managev3user** を、SNMPv3 グループ **managev3group** に追加し、認証アルゴリズム **sha**、認証キー**123456TESTauth&!**、暗号化アルゴリズム **aes128**、プライバシーキー**123456TESTencr&!**を設定します。

```
[AC] snmp-agent usm-user v3 managev3user managev3group simple authentication-mode sha 123456TESTauth&! privacy-mode aes128 123456TESTencr&!
```

エージェントの連絡先と所在地情報を設定します。

```
[AC] snmp-agent sys-info contact NEC

[AC] snmp-agent sys-info location Tokyo
```

エージェントで notifications を有効にします。Trap の宛先として 1.1.1.2 の NMS を指定し、Trap のユーザ名を VACMtest に設定します。

```
[AC] snmp-agent trap enable

[AC] snmp-agent target-host trap address udp-domain 1.1.1.2 params securityname VACMtest v3 privacy
```

2) SNMP NMS を設定します。
   - □ SNMPv3 を指定します。
   - □ SNMPv3 ユーザ **VACMtest** を作成します。
   - □ 認証機能とプライバシー機能の両方を有効にしてください。
   - □ 認証に **SHA-1** を使用し、暗号化に **AES** を設定してください。
   - □ 認証キー**123456TESTauth&!**とプライバシーキー**123456TESTencr&!**を設定してください。
   - □ 必要に応じて、タイムアウト時間と再トライを行う最大数を設定します。

NMS の設定についての詳細は、NMS のマニュアルを参照してください。

🕮 **メモ：**

エージェントと NMS の SNMP 設定は同一にする必要があります。

III. 設定の確認

エージェントから sysName を取得します。取得に成功します。値 Agent が戻ります。

Sysname に sysName ノードの値を設定します。取得に成功します。

エージェントでインタフェースをシャットダウンあるいはアップにします。NMS は linkUP （OID：1.3.6.1.6.3.1.1.5.4） あるいは linkDown （OID：1.3.6.1.6.3.1.1.5.3）の notification を受信します。

目次

このセクションのページは **17-x-x** です。

5章 RMON 5-1
5.1 概要 5-1
5.1.1 RMONグループ 5-1
5.1.2 アラームグループとプライベートアラームグループのサンプルタイプ 5-3
5.1.3 プロトコルと標準 5-4
5.2 RMON統計機能の設定 5-4
5.2.1 RMONイーサネット統計機能エントリの作成 5-4
5.2.2 RMON履歴管理エントリの作成 5-4
5.2.3 RMONアラーム機能の設定 5-5
5.3 RMONの表示と維持 5-6
5.4 RMON設定例 5-7
5.4.1 イーサネット統計情報グループの設定例 5-7
5.4.2 履歴グループの設定例 5-8
5.4.3 アラーム機能の設定例 5-9

5章 RMON

5.1 概要

RMON（Remote Monitoring）は、SNMP を拡張した機能です。リモートモニタリングとネットワーク装置とサブネットの管理を行います。RMON モニタ（ネットワーク装置に組み込まれた RMON エージェント）は定期的に、または継続的に、ポートに接続されたネットワークのトラフィック統計情報を収集します。統計情報がアラームのしきい値を超えたとき、管理対象装置は、自動的にトラップを送信することができます。NMS は、常に MIB 変数をポーリングし結果を比較する必要はありません。

RMON は、例外条件の NMS を通知するために SNMP トラップを使用しています。RMON SNMP トラップは、ブロードキャストトラフィックのしきい値を超過したトラフィックイベントなど、様々なイベントを報告します。対照的に、SNMP 標準トラップは、リンクアップ、リンクダウン、モジュールの障害などの装置の動作状態の変化を報告します。

SNMP の詳細は、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*17 ネットワーク管理と監視*”の” *4 章 SNMP*”を参照してください。

NEC は、RMON モニタとして、組み込み RMON エージェントの機能を提供しています。NMS は RMON MIB にアクセスすることで基本的な SNMP の動作を行うことができます。

5.1.1 RMON グループ

標準 RMON グループのうち、NEC では、統計情報グループ、履歴グループ、イベントグループ、アラームグループ、プローブ設定グループ、およびユーザ履歴グループをサポートします。プローブ設定グループとユーザ履歴グループは CLI から設定できません。設定を行うために MIB にアクセスする必要があります。

I. 統計情報グループ

統計情報グループは、モニタされたイーサネットインタフェースのトラフィック情報の統計情報を取得し、イーサネット統計情報テーブル（ethernetStatsTable）の統計情報を記録します。統計情報は以下があります。

- ネットワークの衝突数
- CRC アライメントエラー
- アンダーサイズ/オーバーサイズパケット
- ブロードキャスト数
- マルチキャスト数
- 受信バイト数
- 受信パケット数

イーサネット統計情報テーブルの統計情報は統計情報の総数です。

II. 履歴グループ

履歴グループは、定期的にインタフェース上のトラフィック情報の統計情報を収集し、履歴レコードテーブル（ethernetHistoryTable）の統計情報を記録します。統計情報は以下があります。

- 帯域幅使用率
- エラーパケット数
- パケットの合計数

履歴レコードテーブルは各サンプリング間隔でインタフェースに受信されたトラフィックの統計情報を記録します。

III. イベントグループ

イベントグループは、アラームグループとプライベートアラームグループで定義されているアラームによって発生したイベントの作成と通知を制御します。RMON アラームイベントは以下の方法で処理されます。

- **Log**－イベントログテーブル内のイベント情報（発生したイベント時間、イベントの内容を含みます。）をロギングします。管理デバイスは、SNMP Get 操作によってログを収集することができます。
- **Trap**－イベントが発生したとき、NMS に SNMP 通知を送信します。
- **Log-Trap**－イベントログテーブルのイベント情報をロギングし、イベントが発生したときに、SNMP 通知を送信します。
- **None**－処理を行いません。

IV. アラームグループ

RMON アラームグループは、インタフェース上の受信パケット（etherStatsPkts）のカウントなどのアラーム変数をモニタします。アラームエントリを作成したのち、RMON エージェントは指定した間隔でモニタアラーム変数の値を取得します。モニタ対象の変数の値が増加方向のしきい値を超えると、増加方向のイベントが発生します。変数の値が減少方向のしきい値を下回ると、減少方向のイベントが発生します。その後イベントは、イベントグループで定義したように処理されます。

アラームエントリがしきい値を連続して複数回交差する場合、RMON エージェントは、最初のしきい値が交差したときにアラームイベントを発生します。サンプリングされた値が増加方向あるいは減少方向のしきい値を超えた時点で 1 つのイベントが発生します。反対方向のしきい値を超えるまで次のイベントは発生しません。たとえば、図 5-1に示すように、増加方向のしきい値を超えると 1 つのイベントが発生し、減少方向のしきい値を超えるまで次のイベントは発生しません。

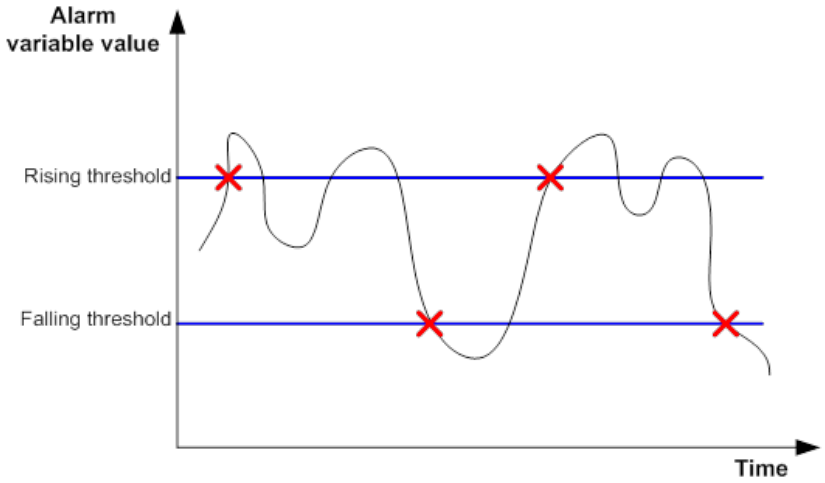


図 5-1 増加方向と減少方向のアラームイベント

V. プライベートアラームグループ

プライベートアラームグループは複数のアラーム変数の値を計算し、計算結果を定義済みの増加方向と減少方向のしきい値と比較します。

RMON エージェントは変数をサンプリングし、プライベートアラームにもとづいたアラームアクションを以下のように行います。

1) ユーザ定義した形式のプライベートアラーム変数をサンプリングします。
2) 定義した形式にもとづいてサンプリングした値を計算します。
3) 定義されたしきい値と計算した値を比較し、以下のいずれかのアクションを行います。
   - 比較結果が増加方向のしきい値以上である場合、増加方向のアラームイベントに関するイベントをトリガします。
   - 比較結果が減少方向のしきい値以下である場合、減少方向のアラームイベントに関するイベントをトリガします。

アラームエントリがしきい値を連続して複数回交差する場合、RMON エージェントは、最初のしきい値が交差したときにアラームイベントを発生します。サンプリングされた値が増加方向あるいは減少方向のしきい値を超えた時点で 1 つのイベントが発生します。反対方向のしきい値を超えるまで次のイベントは発生しません。たとえば、増加方向のしきい値を超えると 1 つのイベントが発生し、減少方向のしきい値を超えるまで次のイベントは発生しません。

5.1.2 アラームグループとプライベートアラームグループのサンプルタイプ

RMON エージェントは以下のサンプルタイプをサポートします。

- **absolute**– RMON は、サンプル値をしきい値と直接比較します。増加方向のしきい値と減少方向のしきい値の変数を、サンプリングした後に比較します。
- **delta**– RMON は現在のサンプル値を最後に取得したサンプル値から引き、その差を増加方向のしきい値と減少方向のしきい値と比較します。

5.1.3 プロトコルと標準

- RFC 4502, *Remote Network Monitoring Management Information Base Version 2*
- RFC 2819, *Remote Network Monitoring Management Information Base Status of this Memo*

5.2 RMON統計機能の設定

RMON 統計機能はイーサネット統計グループと履歴グループによって実装されます。統計機能は、レイヤ 2 およびレイヤ 3 イーサネットインタフェースでのみ使用できます。

イーサネット統計グループはイーサネット統計情報テーブルで定義された変数であり、記録されたコンテンツは、統計エントリが現在時刻に作成された時点からの変数の合計です。設定の詳細は、本章の *"RMON イーサネット統計機能エントリの作成"* を参照してください。

ヒストリグループは、各サンプリング間隔の変数で収集された統計情報を提供します。ヒストリグループは収集を管理するため、履歴管理テーブルを使用し、履歴テーブルに収集された統計情報を記録します。設定の詳細は、本章の *"*RMON履歴管理エントリの作成*"* を参照してください。

5.2.1 RMON イーサネット統計機能エントリの作成

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. interface view に移行する	**interface** *interface-type interface-number*	ー
3. RMON 統計情報テーブルにインタフェースのエントリを作成する	**rmon statistics** *entry-number* [**owner** *text*]	デフォルト：設定なし 1つのイーサネットインタフェースに1つの統計エントリを作成でき、デバイス上に最大で100の統計エントリを作成できます。エントリ制限に達すると、新しいエントリを作成することができなくなります。

5.2.2 RMON 履歴管理エントリの作成

1 つのインタフェースに複数の履歴管理エントリを設定することができますが、エントリ数とサンプリング間隔は同一にしてはいけません。

指定したバケットサイズが有効な履歴テーブルサイズを超過しても、履歴管理エントリを作成することができます。RMON はバケットサイズを可能な限り予期したサイズに設定します。

以下に RMON 履歴管理エントリの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． interface view に移行する	**interface** *interface-type interface-number*	―
3． RMON 履歴管理テーブルにインタフェースのエントリを作成する	**rmon history** *entry-number* **buckets** *number* **interval** *sampling-interval* [**owner** *text*]	デフォルト：設定なし 最大で100の履歴管理エントリを作成できます。

5.2.3 RMON アラーム機能の設定

RMON アラーム機能を設定するときに、以下のガイドラインに従ってください。

- RMON アラーム機能の設定を行う前、アラームが発生したとき NMS に通知するため、SNMP エージェントを設定してください。SNMP エージェントについては QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*17 ネットワーク管理と監視*”の”*4 章 SNMP*”を参照してください。
- 新しいイベント、アラーム、プライベートアラームを作成するために以下の条件が必要です。
  - □ 新しいエントリのパラメータは、すでに存在するエントリと同じにすることはできません。
  - □ エントリ数が最大になっていないこと。

表 5-1に比較されるパラメータとエントリの制限を示します。

表 5-1 RMON の設定制限

エントリ	比較パラメータ	エントリの最大数
イベント	● イベント記述（**description** *string*） ● イベントタイプ（**log**、**trap**、**logtrap**、**none**） ● コミュニティ名（*security-string*）	60
アラーム	● アラーム変数（*alarm-variable*） ● サンプリング間隔（*sampling-interval*） ● サンプルタイプ（**absolute**、**delta**） ● 増加方向のしきい値（*threshold-value1*） ● 減少方向のしきい値 （*threshold-value2*）	60
プライベートアラーム	● アラーム変数式（*prialarm-formula*） ● サンプリング間隔（*sampling-interval*） ● サンプルタイプ（**absolute**、**delta**） ● 増加方向のしきい値（*threshold-value1*） ● 減少方向のしきい値 （*threshold-value2*）	50

以下に RMON アラーム機能の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―

操作	コマンド	補足
2.　（オプション設定項目）イベントテーブルにイベントエントリを作成する	**rmon event** *entry-number* [**description** *string*] { **log** | **log-trap** *security-string* | **none** | **trap** *security-string* } [**owner** *text*]	デフォルト：設定なし
3.　アラームテーブルあるいはプライベートアラームテーブルにエントリを作成する	• アラームテーブルにエントリを作成する： **rmon alarm** *entry-number alarm-variable sampling-interval* { **absolute** | **delta** } [**startup-alarm** { **falling** | **rising** | **rising-falling** }] **rising-threshold** *threshold-value1 event-entry1* **falling-threshold** *threshold-value2 event-entry2* [**owner** *text*] • プライベートアラームテーブルにエントリを作成する： **rmon prialarm** *entry-number prialarm-formula prialarm-des sampling-interval* { **absolute** | **delta** } [**startup-alarm** { **falling** | **rising** | **rising-falling** }] **rising-threshold** *threshold-value1 event-entry1* **falling-threshold** *threshold-value2 event-entry2* **entrytype** { **forever** | **cycle** *cycle-period* } [**owner** *text*]	デフォルト：設定なし アラームを作成されていないイベントと関連付けることができますが、イベントを設定したのち、アラームが動作します。

5.3 RMONの表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
RMON統計情報を表示する	**display rmon statistics** [*interface-type interface-number*]
RMON履歴管理エントリと履歴サンプルを表示する	**display rmon history** [*interface-type interface-number*]
RMONアラームエントリを表示する	**display rmon alarm** [*entry-number*]
RMONプライベートアラームエントリを表示する	**display rmon prialarm** [*entry-number*]
RMONイベントエントリを表示する	**display rmon event** [*entry-number*]
イベントエントリのログ情報を表示する	**display rmon eventlog** [*entry-number*]

5.4 RMON設定例

5.4.1 イーサネット統計情報グループの設定例

I. ネットワーク要件

図 5-2に示すように、GigabitEthernet 1/0/1 のトラフィックの統計情報の合計を収集するため、AC 上で RMON イーサネット統計情報グループエントリを作成します。

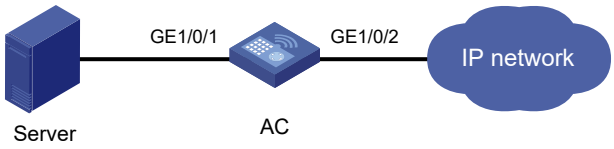


図 5-2 ネットワーク図

II. 設定手順

GigabitEthernet 1/0/1 の RMON イーサネット統計情報エントリを作成します。

```
<AC> system-view
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] rmon statistics 1 owner user1
```

GigabitEthernet 1/0/1 の RMON エージェントで収集された統計情報を表示します。

```
<AC> display rmon statistics gigabitethernet 1/0/1
EtherStatsEntry 1 owned by user1 is VALID.
  Interface : GigabitEthernet1/0/1<ifIndex.3>
  etherStatsOctets          : 21657     , etherStatsPkts           : 307
  etherStatsBroadcastPkts   : 56        , etherStatsMulticastPkts  : 34
  etherStatsUndersizePkts   : 0         , etherStatsOversizePkts   : 0
  etherStatsFragments       : 0         , etherStatsJabbers        : 0
  etherStatsCRCAlignErrors  : 0         , etherStatsCollisions     : 0
  etherStatsDropEvents (insufficient resources): 0
  Incoming packets by size:
  64      : 235       ,  65-127   : 67        ,  128-255   : 4
  256-511: 1          ,  512-1023: 0          ,  1024-1518: 0
```

NMS から SNMP Get 操作を行いトラフィックの統計情報を取得します。（詳細は省略します。）

5.4.2 履歴グループの設定例

I. ネットワーク要件

図 5-3に示すように、1 分ごとの GigabitEthernet 1/0/1 のトラフィックの統計情報をサンプリングするため、AC 上で RMON 履歴管理エントリを作成します。

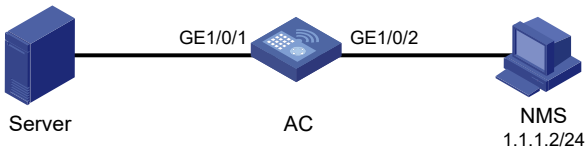


図 5-3 ネットワーク図

II. 設定手順

1 分ごとの GigabitEthernet 1/0/1 のトラフィックの統計情報をサンプリングするため、RMON 履歴管理エントリを作成します。履歴統計テーブルに最大 8 つのインタフェース用のサンプルを記録します。

```
<AC> system-view
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] rmon history 1 buckets 8 interval 60 owner user1
```

GigabitEthernet 1/0/1 で収集された履歴統計情報を表示します。

```
[AC-GigabitEthernet1/0/1] display rmon history
HistoryControlEntry 1 owned by user1 is VALID
  Sampled interface     : GigabitEthernet1/0/1<ifIndex.3>
  Sampling interval     : 60(sec) with 8 buckets max
  Sampling record 1 :
    dropevents        : 0         , octets               : 834
    packets           : 8         , broadcast packets    : 1
    multicast packets : 6         , CRC alignment errors : 0
    undersize packets : 0         , oversize packets     : 0
    fragments         : 0         , jabbers              : 0
    collisions        : 0         , utilization          : 0
  Sampling record 2 :
    dropevents        : 0         , octets               : 962
    packets           : 10        , broadcast packets    : 3
    multicast packets : 6         , CRC alignment errors : 0
    undersize packets : 0         , oversize packets     : 0
    fragments         : 0         , jabbers              : 0
    collisions        : 0         , utilization          : 0
  Sampling record 3 :
    dropevents        : 0         , octets               : 830
    packets           : 8         , broadcast packets    : 0
    multicast packets : 6         , CRC alignment errors : 0
    undersize packets : 0         , oversize packets     : 0
    fragments         : 0         , jabbers              : 0
    collisions        : 0         , utilization          : 0
  Sampling record 4 :
    dropevents        : 0         , octets               : 933
    packets           : 8         , broadcast packets    : 0
    multicast packets : 7         , CRC alignment errors : 0
```

```
    undersize packets : 0          , oversize packets     : 0
    fragments         : 0          , jabbers              : 0
    collisions        : 0          , utilization          : 0
  Sampling record 5 :
    dropevents        : 0          , octets               : 898
    packets           : 9          , broadcast packets    : 2
    multicast packets : 6          , CRC alignment errors : 0
    undersize packets : 0          , oversize packets     : 0
    fragments         : 0          , jabbers              : 0
    collisions        : 0          , utilization          : 0
  Sampling record 6 :
    dropevents        : 0          , octets               : 898
    packets           : 9          , broadcast packets    : 2
    multicast packets : 6          , CRC alignment errors : 0
    undersize packets : 0          , oversize packets     : 0
    fragments         : 0          , jabbers              : 0
    collisions        : 0          , utilization          : 0
  Sampling record 7 :
    dropevents        : 0          , octets               : 766
    packets           : 7          , broadcast packets    : 0
    multicast packets : 6          , CRC alignment errors : 0
    undersize packets : 0          , oversize packets     : 0
    fragments         : 0          , jabbers              : 0
    collisions        : 0          , utilization          : 0
  Sampling record 8 :
    dropevents        : 0          , octets               : 1154
    packets           : 13         , broadcast packets    : 1
    multicast packets : 6          , CRC alignment errors : 0
    undersize packets : 0          , oversize packets     : 0
    fragments         : 0          , jabbers              : 0
    collisions        : 0          , utilization          : 0
```

NMS から SNMP Get 操作を行いトラフィックの統計情報を取得します。（詳細は省略します。）

5.4.3 アラーム機能の設定例

I. ネットワーク要件

図 5-4に示すように、GigabitEthernet 1/0/1 の入力トラフィックの入力トラフィックの統計情報をモニタし、以下のイベントが発生するとき、SNMP でアラームを送信します。

- サンプリング間隔の値が 5 秒で、増加方向のしきい値（100）を超えます。
- サンプリング間隔の値が 5 秒で、減少方向のしきい値（50）を下回ります。

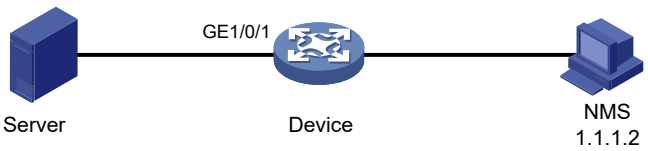


図 5-4 ネットワーク図

II. 設定手順

1.1.1.2 の NMS の SNMP 設定と同様に、SNMP エージェント（AC）の設定を行います。この例では SNMPv1、public コミュニティの読み込み、プライベートコミュニティの書き込みの設定を使用します。

```
<AC> system-view
[AC] snmp-agent
[AC] snmp-agent community read public
[AC] snmp-agent community write private
[AC] snmp-agent sys-info version v1
[AC] snmp-agent trap enable
[AC] snmp-agent trap log
[AC] snmp-agent target-host trap address udp-domain 1.1.1.2 params securityname public
```

GigabitEthernet 1/0/1 の RMON イーサネット統計情報エントリを作成します。

```
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] rmon statistics 1 owner user1
[AC-GigabitEthernet1/0/1] quit
```

ノード 1.3.6.1.2.1.16.1.1.1.4.1 の delta サンプル値が 100 を超えた場合、あるいは 50 を下回った場合、SNMP 通知を送信するために RMON イベントエントリ、RMON アラームエントリを作成します。

```
[AC] rmon event 1 trap public owner user1
[AC] rmon alarm 1 1.3.6.1.2.1.16.1.1.1.4.1 5 delta rising-threshold 100 1 falling-threshold 50 1 owner user1
```

🕮 **メモ：**

1.3.6.1.2.1.16.1.1.1.4.1 は GigabitEthernet 1/0/1 のオブジェクトインスタンスです。ここで 1.3.6.1.2.1.16.1.1.1.4 は入力トラフィックの合計オブジェクトを示し、1 は GigabitEthernet 1/0/1 の RMON イーサネット統計情報エントリインデックスです。

RMON アラームエントリを表示します。

```
<AC> display rmon alarm 1
AlarmEntry 1 owned by user1 is VALID.
  Sample type          : delta
  Sampled variable     : 1.3.6.1.2.1.16.1.1.1.4.1<etherStatsOctets.1>
  Sampling interval (in seconds)    : 5
  Rising threshold      : 100(associated with event 1)
  Falling threshold     : 50(associated with event 1)
  Alarm sent upon entry startup  : risingOrFallingAlarm
  Latest value          : 0
```

GigabitEthernet 1/0/1 の統計情報を表示します。

```
<AC> display rmon statistics gigabitethernet 1/0/1
EtherStatsEntry 1 owned by user1 is VALID.
  Interface : GigabitEthernet1/0/1<ifIndex.3>
  etherStatsOctets         : 57329     , etherStatsPkts          : 455
  etherStatsBroadcastPkts  : 53        , etherStatsMulticastPkts : 353
  etherStatsUndersizePkts  : 0         , etherStatsOversizePkts  : 0
  etherStatsFragments      : 0         , etherStatsJabbers       : 0
  etherStatsCRCAlignErrors : 0         , etherStatsCollisions    : 0
  etherStatsDropEvents (insufficient resources): 0
  Incoming packets by size :
  64     : 7         ,  65-127  : 413       ,  128-255  : 35
  256-511: 0         ,  512-1023: 0         ,  1024-1518: 0
```

NMS でアラームイベントを照会します。（詳細は省略します。）

AC では、イベントが発生するとアラームイベントメッセージが表示されます。 以下に、アラームイベントメッセージの例を示します。

```
[AC] % Apr  6 09:23:53:357 2013 sysname SNMP/6/SNMP_NOTIFY: Notification fallingA
larm(1.3.6.1.2.1.16.0.2) with alarmIndex(1.3.6.1.2.1.16.3.1.1.1.1)=1;alarmVariab
le(1.3.6.1.2.1.16.3.1.1.3.1)=1.3.6.1.2.1.16.1.1.1.4.1;alarmSampleType(1.3.6.1.2.
1.16.3.1.1.4.1)=2;alarmValue(1.3.6.1.2.1.16.3.1.1.5.1)=0;alarmFallingThreshold(1
.3.6.1.2.1.16.3.1.1.8.1)=50.
```

目次

このセクションのページは **17-x-x** です。

6章 NETCONF 6-1
6.1 概要 6-1
6.1.1 NETCONFの構成 6-1
6.1.2 NETCONFメッセージフォーマット 6-2
6.1.3 NETCONFの使用方法 6-3
6.1.4 プロトコルと標準 6-4
6.2 NETCONFの設定作業リスト 6-4
6.3 NETCONF over SOAP の有効化 6-4
6.4 NETCONFロギング の有効化 6-5
6.5 NETCONFセッションの確立 6-5
6.5.1 NETCONFセッションアイドルタイムアウト時間の設定 6-5
6.5.2 xml viewへの移行 6-6
6.5.3 capabilityの交換 6-6
6.6 イベント通知の設定 6-7
6.6.1 登録手順 6-7
6.6.2 イベント通知の登録例 6-8
6.7 設定のロック/ロック解除 6-9
6.7.1 コンフィグレーションのロック 6-9
6.7.2 コンフィグレーションのロック解除 6-10
6.7.3 コンフィグレーションのロック例 6-10
6.8 サービスオペレーションの実行 6-11
6.8.1 get/get-bulkの実行 6-11
6.8.2 get-config/get-bulk-configの実行 6-13
6.8.3 edit-configオペレーションの実行 6-13
6.8.4 全てのモジュールのコンフィグレーション取得例 6-14
6.8.5 シスログのコンフィグレーション取得例 6-15
6.8.6 インタフェーステーブルのデータ取得例 6-16
6.8.7 パラメータ値の変更例 6-17
6.9 コンフィグレーションの保存、ロールバックと読み込み 6-18
6.9.1 コンフィグレーションの保存 6-18
6.9.2 コンフィグレーションファイルからのロールバック 6-19
6.9.3 ロールバックポイントからのロールバック 6-19
6.9.4 コンフィグレーションの読み込み 6-23
6.9.5 コンフィグレーションの保存例 6-24
6.10 データのフィルタリング 6-25
6.10.1 テーブルベースフィルタリング 6-25
6.10.2 コラムベースフィルタリング 6-25
6.10.3 正規表現によるデータのフィルタリング例 6-27
6.10.4 条件一致によるデータのフィルタリング例 6-29
6.11 NETCONF経由のCLI実行 6-30
6.11.1 実行手順 6-30
6.11.2 CLI実行例 6-30
6.12 NETCONFセッション情報の取得 6-31
6.13 他のNETCONFセッション排除 6-32

6.13.1 実行例 6-33
6.14 CLIへの復帰 6-33
6.15 付録 6-35
6.15.1 NETCONFサポートオペレーション 6-35

6章 NETCONF

6.1 概要

NETCONF (Network Configuration Protocol)は、XML ベースの、フィルタリング機能を持ったネットワーク管理プロトコルです。NETCONF は、ネットワークデバイスを管理、運用する為の、プログラマブルなメカニズムを提供します。NETCONF を使用して、デバイスのパラメータ設定、パラメータ値や統計情報を取得できます。

NETCONF メッセージでは、それぞれのデータは固定の要素として包含されています。これにより、同じベンダの異なるデバイスにおいて、同一のアクセス方法と結果出力を提供することが可能になります。異なるベンダのデバイスにおいても、NETCONF メッセージの XML マッピングにより、同一の効果を得ることも可能になります。異なるベンダの異なるデバイスにより構築されるネットワーク環境において、デバイスの設定と管理をシンプルで能率的に行う為の、NETCONF をベースにした NMS システムを開発することができます。

6.1.1 NETCONF の構成

NETCONF は 4 つのレイヤ(content レイヤ、operations レイヤ、RPC レイヤと transport protocol レイヤ)から構成されます。

表 6-1 NETCONF レイヤと XML レイヤ

NETCONF レイヤ	XML レイヤ	説明
Content	コンフィグレーションデータ、状態と統計情報	Contentレイヤは、コンフィグレーションデータ、状態と統計情報からなる管理オブジェクトを含んでいます。
Operations	<get>,<get-config>,<edit-config>…	Operationsレイヤは、XMLでエンコードされたパラメータにより記述されたRPC処理として実行される、基本的なオペレーションセットを定義します。NETCONFの基本動作には、データ取得、コンフィグレーション、ロックとセッション処理があります。デバイスがサポートするオペレーションについては、表6-4を参照してください。
RPC	<rpc>,<rpc-reply>	RPCレイヤは、シンプルでトランスポート層に依存しない、RPCエンコードのフレーミングメカニズムを提供します。<rpc>要素と<rpc-rely>要素は、NETCONFの要求と応答のデータ(operationsレイヤとcontentレイヤ)を囲む為に使用されます。

NETCONF レイヤ	XML レイヤ	説明
Transport Protocol	Console/Telnet/SSH/HTTP/HTTPS/TLS	transport protocolレイヤは、信頼ある、コネクション型のシリアルデータリンクを提供します。TELNET、SSHやコンソールポートからCLIにログインし、NETCONFを操作できます。また、HTTPやHTTPSでログインし、NETCONF や NETCONF over SOAPを操作できます。

6.1.2 NETCONF メッセージフォーマット

I. NETCONF

注意:

XML view で NETCONF を操作する際、XML メッセージの最後に終端文字列”]]>]]”を追加する必要があります。終端文字列を追加しないと、デバイスはメッセージを認識できません。本章での例では、終端文字が省略されています。実際の操作には終端文字を追加してください。

全ての NETCONF メッセージは XML ベースであり、RFC4741 に準拠しています。デバイスが受信する全ての NETCONF メッセージは、実際に処理される前に XML スキーマのチェックをパスしなければなりません。もし XML スキーマチェックに失敗すると、デバイスはクライアントにエラーメッセージを送信します。

NETCONF メッセージに半角カナが含まれていると、XML 変換が失敗し、文字が疑問符（？）に置き換えられた応答が返されます。

以下の例は、デバイスの全インタフェースの全パラメータを取得する NETCONF メッセージです。

```
<?xml version="1.0" encoding="utf-8"?>
<rpc message-id ="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <get-bulk>
    <filter type="subtree">
      <top xmlns="http://www.nec.com/netconf/data:1.0">
        <Ifmgr>
          <Interfaces>
                 <Interface/>
          </Interfaces>
        </Ifmgr>
      </top>
    </filter>
  </get-bulk>
</rpc>
```

II. NETCONF over SOAP

全ての NETCONF-over-SOAP メッセージは XML ベースで、RFC4741 準拠です。NETCONF メッセージは SOAP メッセージ中の<BODY>要素で包含されます。また、NETCONF over SOAP メッセージは、以下のルールに従います。

- SOAP メッセージは、SOAP エンベロープの名前空間を使用しなければなりません。

- SOAP メッセージは、SOAP エンコーディングの名前空間を使用しなければなりません。
- SOAP メッセージは、以下の情報を含むことができません。
  - DTD 参照
  - XML 処理命令

以下の例は、デバイスの全インタフェースの全てのパラメータを取得するNETCONF-over-SOAP メッセージです。

```
<env:Envelope xmlns:env="http://www.w3.org/2003/05/soap-envelope">
  <env:Header>
    <auth:Authentication env:mustUnderstand="1"
xmlns:auth="http://www.nec.com/netconf/base:1.0">
      <auth:AuthInfo>800207F0120020C</auth:AuthInfo>
    </auth:Authentication>
  </env:Header>
  <env:Body>
    <rpc message-id ="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
      <get-bulk>
        <filter type="subtree">
          <top xmlns="http://www.nec.com/netconf/data:1.0">
            <Ifmgr>
              <Interfaces>
                     <Interface/>
              </Interfaces>
            </Ifmgr>
          </top>
        </filter>
      </get-bulk>
    </rpc>
  </env:Body>
</env:Envelope>
```

6.1.3 NETCONF の使用方法

NETCONF の表 6-2に示した方法で、デバイスの運用と設定が可能です。

表 6-2 NETCONF のデバイス設定方法

設定ツール	ログイン方法	補足
CLI	• Consoleポート • SSH • Telnet	NETCONFを実行するには、適切なNETCONFメッセージをCLIのXML viewにコピーします。この方法は、開発とテスト目的です。
デバイスの標準Webインタフェース	• HTTP • HTTPS	システムは自動的にWebインタフェースの設定操作をNETCONFメッセージに変換し、NETCONF操作を実装するためにデバイスに送信します。 この方法は、最も一般的に使用される方法です。
専用設定ツール	–	この方法を使用するには、NETCONF over SOAPを有効にする必要があります。 初期値では、デバイスは専用設定ツールのURLを解釈できません。デバイスにこれらのURLを解釈させる為には、専用設定ツールから送信するSOAP （Simple Object Access Protocol）のNETCONFメッセージをエンコードする必要があります。

6.1.4 プロトコルと標準

- RFC 3339, *Date and Time on the Internet: Timestamps*
- RFC 4741, *NETCONF Configuration Protocol*
- RFC 4742, *Using the NETCONF Configuration Protocol over Secure SHell (SSH)*
- RFC 4743, *Using NETCONF over the Simple Object Access Protocol (SOAP)*
- RFC 5277, *NETCONF Event Notifications*
- RFC 5381, *Experience of Implementing NETCONF over SOAP*
- RFC 5539, *NETCONF over Transport Layer Security (TLS)*
- RFC 6241, *Network Configuration Protocol*

6.2 NETCONFの設定作業リスト

作業リスト
(オプション設定項目) NETCONF over SOAP の有効化
(オプション設定項目) NETCONFロギング の有効化
(必須設定項目) NETCONFセッションの確立
(オプション設定項目) イベント通知の設定
(オプション設定項目) 設定のロック/ロック解除
(オプション設定項目) get/get-bulkの実行
(オプション設定項目) gget-config/get-bulk-configの実行
(オプション設定項目) edit-configオペレーションの実行
(オプション設定項目) コンフィグレーションの保存、ロールバックと読み込み
(オプション設定項目) データのフィルタリング
(オプション設定項目) NETCONF経由のCLI実行
(オプション設定項目) NETCONFセッション情報の取得
(オプション設定項目) 他のNETCONFセッション排除
(オプション設定項目) CLIへの復帰

6.3 NETCONF over SOAP の有効化

NETCONF メッセージは SOAP メッセージでカプセル化され、HTTP または HTTPS 上で転送されます。NETCONF over SOAP の有効後、NETCONF を操作する為の設定インタフェースを開発できます。

以下の方法で、NETCONF over SOAP を有効化します。

手順	コマンド	補足
1. system view に移行する	**system-view**	ー
2. NETCONF over SOAP を有効化する	• NETCONF over SOAP over HTTP を有効化する： **netconf soap http enable** • NETCONF over SOAP over HTTPS を有効化する： **netconf soap https enable**	デフォルトは、NETCONF over SOAPが無効です。

6.4 NETCONFロギング の有効化

本機能は、異なる NETCONF オペレーション元と NETCONF オペレーションによる NETCONF ログ出力を有効化します。

手順	コマンド	補足
1. system view に移行する	**system-view**	ー
2. NETCONF ロギングを有効化する	**netconf log source** { { **soap** | **web** } * } { { **protocol-operation** { **all** | { **action** | **config** | **get** | **set** | **session** | **syntax** | **others** } * } } | **verbose** }	デフォルトは、NETCONF ロギングが無効です。

6.5 NETCONFセッションの確立

クライアントは、デバイスに要求を処理させる前に hello メッセージを送信し、capability 交換を完了させる必要があります。

aaa session-limit コマンドを使用して、デバイスがサポートできる NETCONF セッションの最大数を設定できます。もし上限に達すると、新しいユーザはデバイスにアクセスできません。このコマンドの詳細については、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*13 ユーザアクセスと認証*“の”*3 章 AAA*“を参照してください。

NETCONF 操作を実行する前に、他のユーザが装置を設定または管理していないことを確認してください。複数のユーザが同時に装置を設定または管理する場合、期待と異なる結果になる可能性があります。

6.5.1 NETCONF セッションアイドルタイムアウト時間の設定

NETCONF パケットが、NETCONF セッションアイドルタイムアウト時間内に NETCONF セッションに変換されない場合、装置はセッションを終了します。

NETCONF セッションアイドルタイムアウト時間の設定方法は以下の通りです。

手順	コマンド	補足
1. system view に移行する	**system-view**	ー
2. NETCONF セッションアイドルタイムアウト時間を設定する	**netconf** { **soap** | **agent** } **idle-timeout** *minute*	デフォルト：NETCONFセッションアイドルタイムアウト時間は以下の通りです。 ● NETCONFのSOAP over HTTPセッションとNETCONF over HTTPSセッションは10分です。 ● NETCONF over SSHセッション、NETCONF over Telnetセッショ

手順	コマンド	補足
		ン、NETCONF overコンソールセッションはタイムアウトしません。

6.5.2 xml view への移行

操作	コマンド	補足
XML viewに移行する	**xml**	user viewで使用可能です。

6.5.3 capability の交換

XML view に移行し、クライアントとデバイスがそれぞれの capability を交換すると、その後の NETCONF オペレーションが実行できるようになります。デバイスが hello メッセージの中で通知する capability は、以下のとおりです。

```
<?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:netc
onf:capability:validate:1.1</capability><capability>urn:ietf:params:netco
nf:capability:interleave:1.0</capability><capability>urn:nec:params:netco
nf:capability:nec-netconf-ext:1.0</capability></capabilities><session-id>
1</session-id></hello>]]>]]>
```

- <capabilities>パラメータは、デバイスがサポートする capability を表します。
- <session-id>パラメータは、現在のセッションに割り当てられたユニークな ID を表します。

デバイスから hello メッセージを受信後、以下のメッセージをコピーして、クライアントがサポートする capability(ユーザ変更可能)をデバイスに通知します。

```
<hello xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <capabilities>
    <capability>
     capability-set
    </capability>
  </capabilities>
</hello>
```

capability-set はクライアントがサポートする capability を表します。

<capability>と</capability>タグで囲む必要があります。

6.6 イベント通知の設定

注意：
イベント通知は、NETCONF over CLI でのみサポートします。NETCONF over SOAP ではサポートしていません。

イベント通知を登録後、設定されたイベントがデバイスで発生すると、デバイスは NETCONF クライアントにイベント通知を送信します。通知には、code、group、severity、start time とイベントの説明が含まれます。デバイスはログサブスクリプションのみをサポートします。

イベント登録は、現在のセッションにのみ有効です。セッション終了後は、イベント登録は自動的に解除されます。

複数のイベント通知登録メッセージを送信し、複数のイベント通知を設定することも可能です。

6.6.1 登録手順

クライアントからイベント通知を登録するには、以下のメッセージをコピーします。

<?xml version="1.0" encoding="UTF-8"?>

```
<rpc message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
    <create-subscription
xmlns="urn:ietf:params:xml:ns:netconf:notification:1.0">
         <stream>NETCONF</stream>
         <filter>
             <event xmlns="http://www.nec.com/netconf/event:1.0">
                 <Code>code</Code>
                 <Group>group</Group>
                 <Severity>severity</Severity>
             </event>
         </filter>
         <startTime>start-time</startTime>
         <stopTime>stop-time</stopTime>
    </create-subscription>
</rpc>
```

- <stream>パラメータは、デバイスがサポートするストリームタイプを表します。NETCONF のみサポートです。
- <event>パラメータは、設定するイベントを表します。
- <code>パラメータは、ニーモニックシンボルを表します。
- <group>パラメータは、モジュール名を表します。
- <severity>パラメータは、イベントレベルの重要度を表します。
- <start-time>パラメータは、通知の開始時刻を表します。
- <stop-time>パラメータは、通知の終了時刻を表します。

クライアントから登録要求を受信後、登録成功すれば、デバイスは以下のフォーマットで応答を返信します。

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply message-id="101"
xmlns:netconf="urn:ietf:params:xml:ns:netconf:base:1.0">
    <ok/>
</rpc-reply>
```

登録が失敗すると、デバイスは以下のフォーマットでエラーメッセージを返信します。

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply message-id="101"
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
<rpc-error>
   <error-type>error-type</error-type>
   <error-tag>error-tag</error-tag>
   <error-severity>error-severity</error-severity>
   <error-message xml:lang="en">error-message</error-message>
</rpc-error>
</rpc-reply>
```

エラーメッセージについての詳細は、RFC4741 を参照してください。

6.6.2 イベント通知の登録例

I. ネットワーク要件

時刻の制限無しで、全てのイベントを登録します。登録成功後、デバイスとクライアント間のセッションが切断されない限り、デバイスでの全てのイベントがクライアントに送信されます。

II. 実行手順

XML view に移行します。

```
<AC> xml
```

capability を交換します。

```
<hello xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
    <capabilities>
        <capability>
            urn:ietf:params:netconf:base:1.0
        </capability>
    </capabilities>
</hello>
```

時刻の制限無しで、全てのイベントを設定します。

```
<rpc message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
    <create-subscription xmlns
="urn:ietf:params:xml:ns:netconf:notification:1.0">
        <stream>NETCONF</stream>
    </create-subscription>
</rpc>
```

III. 結果確認

クライアントが以下の応答を受信すれば、設定は成功です。

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"
message-id="101">
    <ok/>
</rpc-reply>
```

もしデバイスの fan 1 で異常発生すると、全てのイベントが設定されているので、デバイスは以下のテキストをクライアントに送信します。

```
<?xml version="1.0" encoding="UTF-8"?>
<notification xmlns="urn:ietf:params:xml:ns:netconf:notification:1.0">
    <eventTime>2011-01-04T12:30:46</eventTime>
    <event xmlns="http://www.nec.com/netconf/event:1.0">
        <Group>DEV</Group>
```

```
        <Code>FAN_DIRECTION_NOT_PREFERRED</Code>
        <Slot>6</Slot>
        <Severity>Alert</Severity>
        <context>Fan 1 airflow direction is not preferred on slot 6, please
check it.</context>
    </event>
</notification>
```

他のクライアント(192.168.100.130)がデバイスにログインすると、全てのイベントが設定されているので、デバイスはクライアントに通知します。

```
<?xml version="1.0" encoding="UTF-8"?>
<notification xmlns="urn:ietf:params:xml:ns:netconf:notification:1.0">
    <eventTime>2011-01-04T12:30:52</eventTime>
    <event xmlns="http://www.nec.com/netconf/event:1.0">
        <Group>SHELL</Group>
        <Code>SHELL_LOGIN</Code>
        <Slot>6</Slot>
        <Severity>Notification</Severity>
        <context>VTY logged in from 192.168.100.130.</context>
    </event>
</notification>
```

6.7 設定のロック/ロック解除

デバイスは、最大 32 個の NETCONF セッションをサポートします。最大 32 のユーザは同時に、NETCONF を使用してデバイスの運用や監視を行うことができます。デバイスの設定や保守中、あるはネットワーク障害対応中、ユーザはコンフィグをロックして、他のユーザから変更されないようにすることもできます。コンフィグロック後は、ロックを保持しているユーザだけが、設定を変更可能です。他のユーザはコンフィグ取得のみ可能です。

さらに、ロックを保持しているユーザだけが、ロックを解除できます。ロック解除後は、他のユーザも現在のコンフィグを変更、または、コンフィグのロックが可能です。ロックを保持しているユーザのセッションが終了すると、システムは自動的にロックを解放します。

6.7.1 コンフィグレーションのロック

クライアントからコンフィグレーションをロックするには、以下のテキストをコピーします。

```
<?xml version="1.0" encoding="UTF-8"?>
  <rpc message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
    <lock>
      <target>
        <running/>
      </target>
    </lock>
  </rpc>
```

ロックリクエスト受信後、ロックが成功すると、デバイスは以下のフォーマットで応答を返信します。

```
<?xml version="1.0" encoding="UTF-8"?>
  <rpc-reply message-id="101"
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
     <ok/>
  </rpc-reply>
```

6.7.2 コンフィグレーションのロック解除

クライアントからコンフィグレーションのロックを解除するには、以下のテキストをコピーします。

```
<?xml version="1.0" encoding="UTF-8"?>
  <rpc message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
    <unlock>
      <target>
        <running/>
      </target>
    </unlock>
  </rpc>
```

ロック解除リクエストを受信後、ロック解除が成功すると、デバイスは以下のフォーマットで応答を返信します。

```
<?xml version="1.0" encoding="UTF-8"?>
    <rpc-reply message-id="101"
    xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
      <ok/>
    </rpc-reply>
```

6.7.3 コンフィグレーションのロック例

I. ネットワーク要件

デバイスのコンフィグレーションをロックし、他のユーザが変更できないようにします。

II. 実行手順

XML view に移行します。

```
<AC> xml
```

capability を交換します。

```
<hello xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
    <capabilities>
        <capability>
            urn:ietf:params:netconf:base:1.0
        </capability>
    </capabilities>
</hello>
```

コンフィグレーションをロックします。

```
<?xml version="1.0" encoding="UTF-8"?>
  <rpc message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
    <lock>
      <target>
        <running/>
      </target>
    </lock>
  </rpc>
```

III. 結果確認

クライアントが以下の応答を受信すれば、ロック設定は成功です。

```
<?xml version="1.0" encoding="UTF-8"?>
    <rpc-reply message-id="101"
    xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
```

```
      <ok/>
    </rpc-reply>
```

もし他のクライアントがロックを要求すると、デバイスは以下の応答を返信します。

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply message-id="101"
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <rpc-error>
    <error-type>protocol</error-type>
    <error-tag>lock-denied</error-tag>
    <error-severity>error</error-severity>
    <error-message xml:lang="en">Lock failed because the NETCONF lock is held
by another session.</error-message>
    <error-info>
      <session-id>1</session-id>
    </error-info>
  </rpc-error>
</rpc-reply>
```

応答出力では、セッション ID 1 のクライアントがロックを保持していることが示され、ロックを保持しているクライアントのみロック解除することができます。

6.8 サービスオペレーションの実行

NETCONF を使用してデバイスのサービスオペレーションを実行し、特定の情報を変更したり取得したりできます。基本的なオペレーションには、get、get-bulk、get-config、get-bulk-config と edit-config があり、全てのデータ取得、コンフィグレーション取得や特定のモジュールのデータ変更を行う際に使用されます。

🕮 **メモ：**

get、get-bulk、get-config、get-bulk-config の操作中、NETCONF は取得したデータの識別不可能な文字を疑問符（？）で置き換えてから、クライアントにデータを送信します。

6.8.1 get/get-bulk の実行

get オペレーションは、条件に一致するデバイスのコンフィグレーションや状態の情報を取得する際に使用されます。いくつかのケースでは、このオペレーションの効率は良くありません。

get-bulk オペレーションは、最初のデータから、指定したインデックスまでのエントリを取得する際に使用されます。データは、デバイスのコンフィグレーションや状態といった情報のエントリです。取得するデータの数は count 属性で指定し、インデックスは index 属性で指定します。返信される出力には、インデックス情報は含まれません。index 属性を指定しないと、デフォルトの 1 が使用されます。

以下どちらかの条件が揃った場合、get-bulk オペレーションは最初のデータから指定したインデックスまで全てのデータを取得します。

- count 属性を指定しない場合。
- 一致したデータエントリの数が、count 属性で指定した値より小さい場合。

クライアントから get オペレーションを実行するには、以下のテキストをコピーします。

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <getoperation>
    <filter>
      <top xmlns=" http://www.nec.com/netconf/data:1.0">
          Specify the module, submodule, table name, and column name
      </top>
    </filter>
  </getoperation>
</rpc>
```

<getoperation>は<get>、または<get-bulk>です。<filter>要素はデータのフィルタリングに使用され、モジュール名、サブモジュール名、テーブル名やコラム名が使用されます。

- モジュール名やサブモジュール名が指定されないと、オペレーションは全てのモジュールとサブモジュールを取得します。モジュール名またはサブモジュール名が指定されると、オペレーションは指定されたモジュールまたはサブモジュールについて取得します。
- テーブル名が指定されないと、オペレーションは全てのテーブルについて取得します。テーブル名が指定されると、オペレーションは指定されたテーブルの全てについて取得します。
- インデックスのコラムが指定されないと、オペレーションは全てのコラムのデータを取得します。コラムと他のコラムが指定されると、オペレーションはインデックスのコラムと指定されたコラムのデータを取得します。

<get>と<get-bulk>メッセージは似ています。<get-bulk>メッセージは count 属性と index 属性を伝達します。以下は、<get-bulk>メッセージの例です。

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc message-id ="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"
xmlns:xc="http://www.nec.com/netconf/base:1.0">
  <get-bulk>
    <filter type="subtree">
      <top xmlns=http://www.nec.com/netconf/data:1.0
mlns:base="http://www.nec.com/netconf/base:1.0">
        <Syslog>
            <Logs xc:count="5">
                   <Log>
                      <Index>10</Index>
                   </Log>
            </Logs>
        </Syslog>
      </top>
    </filter>
  </get-bulk>
</rpc>
```

count 属性は、以下のルールに従います。

- count 属性は、モジュールノードとテーブルノードで指定できます。他のノードでは解釈されません。
- count 属性がモジュールノードで指定されると、子ノードに count 属性が含まれない場合は、count 属性は引き継がれます。

I. 結果確認

get-bulk 要求を受信後、デバイスはオペレーションに成功すると、以下のフォーマットで応答を返信します。

```
<?xml version="1.0"?>
<rpc-reply message-id="100"
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <data>
     Device state and configuration data
```

```
  </data>
</rpc-reply>
```

6.8.2 get-config/get-bulk-config の実行

get-config と get-bulk-config オペレーションは、CLI、MIB、Web で設定された、デフォルトではないコンフィグレーションの取得に使用されます。<get-config> と <get-bulk-config>メッセージは、データのフィルタリング用に<filter>要素が使用できます。

<get-config>と<get-bulk-config>メッセージは似ています。以下は、<get-config>メッセージの例です。

```
<?xml version="1.0"?>
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <get-config>
    <source>
      <running/>
    </source>
    <filter>
      <top xmlns="http://www.nec.com/netconf/config:1.0">
          Specify the module name, submodule name, table name, and column name
      </top>
    </filter>
  </get-config>
</rpc>
```

I. 結果確認

get-config 要求を受信後、デバイスはオペレーションに成功すると、以下のフォーマットで応答を返信します。

```
<?xml version="1.0"?>
<rpc-reply message-id="100"
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <data>
    All data matching the specified filter
  </data>
</rpc-reply>
```

6.8.3 edit-config オペレーションの実行

edit-config オペレーションは、merge、create、replace、remove、delete、default-operation、error-option と test-option 属性をサポートします。属性についての詳細は、本章の *“付録”* の *“NETCONF サポートオペレーション”* を参照してください。

<edit-config>オペレーションを実行するには、以下のテキストをコピーします。

```
<?xml version="1.0"?>
<rpc message-id="100"  xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <edit-config>
    <target><running></running></target>
<error-option>
   Default operation when an error occurs
</error-option>
    <config>
      <top xmlns="http://www.nec.com/netconf/config:1.0">
        Specify the module name, submodule name, table name, and column name
      </top>
```

```
    </config>
  </edit-config>
</rpc>
```

error-option は、操作中に発生したエラーに応答して実行されるアクションを示します。値については以下の通りです。

- stop-on-error—操作を停止します。
- continue-on-error—操作を続行します。
- rollback-on-error—edit-config 操作が実行される前に、設定をロールバックします。デフォルトでは、装置が設定をロールバックしている間は、edit-config 操作を実行することはできません。ロールバック時間がクライアントの待機できる最大時間を超えた場合、クライアントは edit-config 操作が失敗したと判断し、操作を再度実行します。以前のロールバックは完了していないため、操作によって別のロールバックがトリガーされます。このプロセスが繰り返されると、CPU とメモリのリソースがなくなり、装置が再起動します。装置が設定をロールバックしているときに edit-config 操作を実行できるようにするには、action 操作を実行して DisableEditConfigWhenRollback 属性の値を false に変更します。

edit-config 要求を受信後、デバイスはオペレーションに成功すると、以下のフォーマットで応答を返信します。

```
<?xml version="1.0">
<rpc-reply message-id="100"
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <ok/>
</rpc-reply>
```

get オペレーションを実行し、現在のパラメータ値と、edit-config オペレーションで指定したパラメータが同じ事を確認します(詳細は省略します)。

6.8.4 全てのモジュールのコンフィグレーション取得例

I. ネットワーク要件

全てのモジュールのコンフィグレーションを取得します。

II. 実行手順

XML view に移行します。

```
<AC> xml
```

capability を交換します。

```
<hello xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
    <capabilities>
        <capability>
            urn:ietf:params:netconf:base:1.0
        </capability>
    </capabilities>
</hello>
```

全てのモジュールのコンフィグレーションを取得します。

```
<rpc message-id="100"
     xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <get-config>
    <source>
      <running/>
    </source>
  </get-config>
```

```
</rpc>
```

III. 結果確認

クライアントが以下のテキストを受信すれば、get-config オペレーションは成功です。

```
<rpc-reply xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"
xmlns:web="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="101">
    <data>
        <top xmlns="http://www.nec.com/netconf/config:1.0">
            <Ifmgr>
                <Interfaces>
                    <Interface>
                        <IfIndex>1307</IfIndex>
                        <Shutdown>1</Shutdown>
                    </Interface>
                    <Interface>
                        <IfIndex>1308</IfIndex>
                        <Shutdown>1</Shutdown>
                    </Interface>
                    <Interface>
                        <IfIndex>1309</IfIndex>
                        <Shutdown>1</Shutdown>
                    </Interface>
                    <Interface>
                        <IfIndex>1311</IfIndex>
                            <VlanType>2</VlanType>
                    </Interface>
                    <Interface>
                        <IfIndex>1313</IfIndex>
                            <VlanType>2</VlanType>
                    </Interface>
                </Interfaces>
            </Ifmgr>
            <Syslog>
                <LogBuffer>
                    <BufferSize>120</BufferSize>
                </LogBuffer>
            </Syslog>
            <System>
                <Device>
                    <SysName>NEC</SysName>
                    <TimeZone>
                        <Zone>+11:44</Zone>
                        <ZoneName>beijing</ZoneName>
                    </TimeZone>
                </Device>
            </System>
        </top>
    </data>
</rpc-reply>
```

6.8.5 シスログのコンフィグレーション取得例

I. ネットワーク要件

シスログモジュールのコンフィグレーションを取得します。

II. 実行手順

XML view に移行します。

```
<AC> xml
```

capability を交換します。

```
<hello xmlns="urn:ietf:params:xml:ns:netconf:bat7uuse:1.0">
    <capabilities>
        <capability>
            urn:ietf:params:netconf:base:1.0
        </capability>
    </capabilities>
</hello>
```

シスログモジュールのコンフィグレーションを取得します。

```
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <get-config>
    <source>
      <running/>
    </source>
    <filter type="subtree">
      <top xmlns="http://www.nec.com/netconf/config:1.0">
        <Syslog/>
      </top>
    </filter>
  </get-config>
</rpc>
```

III. 結果確認

クライアントが以下のテキストを受信すれば、get-config オペレーションは成功です。

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"
message-id="101">
    <data>
        <top xmlns="http://www.nec.com/netconf/config:1.0">
            <Syslog>
                    <LogBuffer>
                        <BufferSize>120</BufferSize>
                    </LogBuffer>
            </Syslog>
        </top>
    </data>
</rpc-reply>
```

6.8.6 インタフェーステーブルのデータ取得例

I. ネットワーク要件

インタフェーステーブルのデータを取得します。

II. 実行手順

XML view に移行します。

```
<AC> xml
```

capability を交換します。

```
<hello xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
    <capabilities>
        <capability>urn:ietf:params:netconf:base:1.0</capability>
    </capabilities>
</hello>
```

インタフェーステーブルのデータを取得します。

```
<rpc message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"
xmlns:web="urn:ietf:params:xml:ns:netconf:base:1.0">
    <get-bulk>
        <filter type="subtree">
            <top xmlns="http://www.nec.com/netconf/data:1.0"
xmlns:web="http://www.nec.com/netconf/base:1.0">
                <Ifmgr>
                    <Interfaces web:count="1">
                    </Interfaces>
                </Ifmgr>
            </top>
        </filter>
    </get-bulk>
</rpc>
```

III. 結果確認

クライアントが以下のテキストを受信すれば、get-bulk オペレーションは成功です。

```
<rpc-reply xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"
xmlns:web="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="101">
  <data>
    <top xmlns="http://www.nec.com/netconf/data:1.0">
      <Ifmgr>
        <Interfaces>
          <Interface>
            <IfIndex>3</IfIndex>
            <Name>FortyGigE1/0/2</Name>
            <AbbreviatedName>FGE1/0/2</AbbreviatedName>
            <PortIndex>3</PortIndex>
            <ifTypeExt>22</ifTypeExt>
            <ifType>6</ifType>
            <Description>FortyGigE1/0/2 Interface</Description>
            <AdminStatus>2</AdminStatus>
            <OperStatus>2</OperStatus>
            <ConfigSpeed>0</ConfigSpeed>
            <ActualSpeed>100000</ActualSpeed>
            <ConfigDuplex>3</ConfigDuplex>
            <ActualDuplex>1</ActualDuplex>
          </Interface>
        </Interfaces>
      </Ifmgr>
    </top>
  </data>
</rpc-reply>
```

6.8.7 パラメータ値の変更例

I. ネットワーク要件

シスログモジュールのログバッファサイズを 512 に変更します。

II. 実行手順

XML view に移行します。

```
<AC> xml
```

capability を交換します。

```
<hello xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
```

```
    <capabilities>
        <capability>urn:ietf:params:netconf:base:1.0</capability>
    </capabilities>
</hello>
```

シスログモジュールのログバッファサイズを 512 に変更します。

```
<rpc message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"
xmlns:web="urn:ietf:params:xml:ns:netconf:base:1.0">
<edit-config>
    <target>
        <running/>
    </target>
    <config>
        <top xmlns="http://www.nec.com/netconf/config:1.0"
web:operation="merge">
            <Syslog>
                <LogBuffer>
                    <BufferSize>512</BufferSize>
                </LogBuffer>
            </Syslog>
        </top>
    </config>
</edit-config>
</rpc>
```

III. 結果確認

クライアントが以下のテキストを受信すれば、edit-config オペレーションは成功です。

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply message-id="100"
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <ok/>
</rpc-reply>
```

6.9 コンフィグレーションの保存、ロールバックと読み込み

NETCONF でコンフィグレーションの保存、ロールバックと読み込みを行います。

save、rollback、load 操作を実行すると、多くのシステムリソースが消費されます。システムリソースが大量に占有されている場合は、これらの操作を実行しないでください。

デフォルトでは、装置が設定をロールバックしているときに edit-config 操作を実行することはできません。装置が設定をロールバックしているときに edit-config 操作を実行するには、action 操作を実行して DisableEditConfigWhenRollback 属性の値を false に変更します。

6.9.1 コンフィグレーションの保存

クライアントから指定ファイルにコンフィグレーションを保存するには、以下のテキストをコピーします。

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <save OverWrite="false">
    <file>Specify the configuration file name</file>
  </save>
</rpc>
```

指定するコンフィグレーションファイル名は、ストレージのメディア名で始まり、拡張子”.cfg”で終わる必要があります。保存するパス名とファイル名の合計は、191 文字を超えてはいけません。テキストに file コラムを含める場合はファイル名を指定する必要があり、指定したファイルは next-startup コンフィグレーションファイルとなります。もし file コラムを含めない場合、コンフィグレーションは自動的にデフォルトのメイン next-startup コンフィグレーションファイルに保存されます。

OverWrite 属性は、指定されたコンフィグレーションファイルがすでに存在する場合にのみ有効です。 属性でデフォルト値の true を使用すると、現在の設定が保存され、元のファイルが上書きされます。 属性値が false に設定されている場合、現在の構成を保存することができず、システムはエラーメッセージを表示します。

save 要求の受信後、デバイスはオペレーションに成功すると、以下のフォーマットで応答を返信します。

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply message-id="101"
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <ok/>
</rpc-reply>
```

6.9.2 コンフィグレーションファイルからのロールバック

クライアントからコンフィグレーションをロールバックするには、以下のテキストをコピーします。

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <rollback>
    <file>Specify the configuration file name</file>
  </rollback>
</rpc>
```

指定するコンフィグレーションファイル名は、ストレージのメディア名で始まり、拡張子”.cfg”で終わる必要があります。保存するパス名とファイル名の合計は、191 文字を超えてはいけません。

rollback 要求の受信後、デバイスはオペレーション成功すると以下のフォーマットを返信します。

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply message-id="101"
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
      <ok/>
</rpc-reply>
```

6.9.3 ロールバックポイントからのロールバック

本機能は、下記条件何れかが発生した際、デバイスのカレントコンフィグレーションをロールバックポイントにロールバックします。

- NETCONF クライアントがロールバック要求を送信。
- NETCONF セッションのアイドルタイムがロールバックアイドルタイムアウト時間より長い。
- NETCONF クライアントが意図せずデバイスから切断された。

ロールバックポイントのコンフィグレーションにロールバックするには、以下のタスクを行います。

1) システムのロック

複数のユーザが同時に NETCONF を使用して、デバイス設定を行っているかもしれません。他のユーザからのカレントコンフィグ変更を防ぐ為、コンフィグレーションをロールバックする前にシステムをロックする事を推奨します。

2) ロールバックオペレーションの開始をマークします。本章の *"save-point/begin オペレーションの実行"* を参照してください。
3) デバイスのコンフィグレーション編集。本章の *"edit-config オペレーションの実行"* を参照してください。
4) ロールバックポイントの設定。本章の *"save-point/commit オペレーションの実行"* を参照してください。
5) ロールバックポイントからのコンフィグレーションロールバック。本章の *"save-point/rollback オペレーションの実行"* を参照してください。
6) コンフィグレーションのロールバック終了。本章の *"save-point/end オペレーションの実行"* を参照してください。
7) ロックを解放します。

I. save-point/begin オペレーションの実行

#クライアントからロールバックポイントからのロールバク開始をマークするには、以下のテキストをコピーします。

```
<rpc message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
      <save-point>
        <begin>
          <confirm-timeout>100</confirm-timeout>
        </begin>
      </save-point>
</rpc>
```

<confirm-timeout>で、ロールバックのアイドルタイムアウト値を 1 から 65535 秒(デフォルト 600 秒)の範囲で指定します。

save-point/begin リクエスト受信後、デバイスはオペレーションに成功すると、以下のフォーマットで応答を返信します。

```
<rpc-reply message-id="101"
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <data>
    <save-point>
       <commit>
          <commit-id>1</commit-id>
       </commit>
    </save-point>
  </data>
</rpc-reply>
```

II. save-point/commit オペレーションの実行

システムは最大 50 のロールバックポイントをサポートします。上限に達した場合、force 属性を指定して、最も古いロールバックポイントを上書きする必要があります。

#クライアントからロールバックポイントを設定するには、以下のテキストをコピーします。

```
<rpc message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <save-point>
    <commit>
      <label>SUPPORT VLAN<label>
      <comment>vlan 1 to 100 and interfaces. Each vlan used for different
custom as follows: ……</comment>
    </commit>
  </save-point>
</rpc>
```

<label>と<comment>パラメータはオプションです。

save-point/commit リクエスト受信後、デバイスはオペレーションに成功すると、以下のフォーマットで応答を返信します。

```
<rpc-reply message-id="101"
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <data>
    <save-point>
       <commit>
          <commit-id>2</commit-id>
       </commit>
    </save-point>
  </data>
</rpc-reply>
```

III. save-point/rollback オペレーションの実行

#クライアントからコンフィグレーションをロールバックするには、以下のテキストをコピーします。

```
<rpc message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <save-point>
    <rollback>
      <commit-id/>
      <commit-index/>
      <commit-label/>
    </rollback>
  </save-point>
</rpc>
```

- <commit-id>パラメータは、ロールバックポイントの一意の識別子です。
- <commit-index>パラメータで、最大 50 のロールバックポイントを指定します。0 は直近の編集ポイント、49 は最古の編集ポイントを示します。
- <commit-label>パラメータで、ロールバックポイントへ排他的につけられるラベルを指定します。ラベルはロールバックポイントに必須ではありません。

save-point/rollback リクエスト受信後、デバイスはロールバックオペレーションに成功すると、以下のフォーマットで応答を返信します。

```
<rpc-reply message-id="101"
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <ok></ok>
</rpc-reply>
```

IV. save-point/end オペレーションの実行

#クライアントからロールバックを終了するには、以下のテキストをコピーします。

```
<rpc message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
```

```
  <save-point>
    <end/>
  </save-point>
</rpc>
```

save-point/end リクエスト受信後、デバイスは end オペレーションに成功すると、以下のフォーマットで応答を返信します。

```
<rpc-reply message-id="100"
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
   <ok/>
</rpc-reply>
```

V. save-point/get-commits オペレーションの実行

#クライアントからロールバックポイントのコンフィグレーション情報を取得するには、以下のテキストをコピーします。

```
<rpc message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <save-point>
    <get-commits>
      <commit-id/>
      <commit-index/>
      <commit-label/>
    </get-commits>
  </save-point>
</rpc>
```

ロールバックポイントのコンフィグレーションを取得するには、<commit-id>、<commit-index>か<commit-label>パラメータ何れか一つを指定します。何れのパラメータも指定されない場合、全てのロールバックポイントのコンフィグレーションとして動作します。以下は<save-point>/<get-commit>リクエストの例です。

```
<rpc message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <save-point>
    <get-commits>
      <commit-label>SUPPORT VLAN</commit-label>
    </get-commits>
  </save-point>
</rpc>
```

save-point/get-commits リクエスト受信後、デバイスは get-commits オペレーションに成功すると、以下のフォーマットで応答を返信します。

```
<rpc-reply message-id="101"
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <data>
    <save-point>
         <commit-information>
           <CommitID>2</CommitID>
           <TimeStamp>Thu Oct 30 11:30:28 1980</TimeStamp>
           <UserName>test</UserName>
           <Label>SUPPORT VLAN</Label>
         </commit-information>
    </save-point>
  </data>
</rpc-reply>
```

VI. save-point/get-commit-information オペレーションの実行

#クライアントからロールバックポイントに対応するコンフィグレーションを取得するには、以下のテキストをコピーします。

```
<rpc message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <save-point>
```

```
    <get-commit-information>
      <commit-information>
         <commit-id/>
         <commit-index/>
         <commit-label/>
      </commit-information>
      <compare-information>
         <commit-id/>
         <commit-index/>
         <commit-label/>
      </compare-information
    </get-commit-information>
  </save-point>
</rpc>
```

指定するロールバックポイントのコンフィグレーションを取得するには、<commit-id>、<commit-index> か <commit-label> パラメータの何れか 1 つを指定します。<compare-information>パラメータはオプションです。何れのパラメータも指定されない場合、直近で設定されたロールバックポイントを取得します。以下は、<save-point>/<get-commit-information>リクエストの例です。

```
<rpc message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <save-point>
    <get-commit-information>
              <commit-information>
                 <commit-label>SUPPORT VLAN</commit-label>
              </commit-information>
    </get-commit-information>
  </save-point>
</rpc>
```

save-point/get-commit-information リクエスト受信後、デバイスは get-commit-information オペレーションに成功すると、以下のフォーマットで応答を返信します。

```
<rpc-reply message-id="101"
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
   <data>
     <save-point>
        <commit-information>
           <content>
              …
              interface vlan 1
              …
           </content>
        </commit-information>
     </save-point>
   </data>
</rpc-reply>
```

6.9.4 コンフィグレーションの読み込み

load オペレーションの実行以後、読み込まれたコンフィグレーションは現在のコンフィグレーションにマージされます。

- 新しいコンフィグレーションは、そのまま読み込まれます。
- コンフィグレーションが既に存在する場合、読み込まれたコンフィグレーションで上書きします。

コンフィグレーションファイルの一部の設定は、既存の設定と競合する可能性があります。ファイル内の設定を有効にするには、既存の競合する設定を削除して、コンフィグレーションファイルを読み込みます。

#クライアントからコンフィグレーションを読み込むには、以下のテキストをコピーします。

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <load>
     <file>Specify the configuration file name</file>
  </load>
</rpc>
```

指定するコンフィグレーションファイル名は、ストレージのメディア名で始まり、拡張子”.cfg”で終わる必要があります。保存するパスとファイル名の合計は、191 文字を超えてはいけません。

load 要求の受信後、デバイスはオペレーションに成功すると、以下のフォーマットで応答を返信します。

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply message-id="101"
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
      <ok/>
</rpc-reply>
```

6.9.5 コンフィグレーションの保存例

I. ネットワーク要件

現在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 my_config.cfg に保存します。

II. 実行手順

XML view に移行します。

```
<AC> xml
```

capability を交換します。

```
<hello xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
    <capabilities>
        <capability>
            urn:ietf:params:netconf:base:1.0
        </capability>
    </capabilities>
</hello>
```

現在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 my_config.cfg に保存します。

```
<?xml version="1.0" encoding="UTF-8"?>
  <rpc message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
    <save>
      <file>my_config.cfg</file>
    </save>
  </rpc>
```

III. 結果確認

クライアントが以下の応答を受信すれば、save オペレーションは成功です。

```
<?xml version="1.0" encoding="UTF-8"?>
  <rpc-reply message-id="101"
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
      <ok/>
  </rpc-reply>
```

6.10 データのフィルタリング

get、get-bulk、get-config や get-bulk-config オペレーション実行時、情報をフィルタするために filter を定義できます。データフィルタリングには以下があります。

- テーブルベースフィルタリング—テーブル情報のフィルタリング
- コラムベースフィルタリング—単一コラムのフィルタリング

テーブルベースフィルタリングは、コラムベースフィルタリングを設定した後に有効です。

6.10.1 テーブルベースフィルタリング

filter 属性にマッチ条件を指定する事で、テーブルベースのフィルタリングを実行可能です。例えば IP アドレスのフィルタリングを行う事ができます。ネームスペースは http://www.nec.com/netconf/base:1.0 です。

＃クライアントから IPv4 ルーティングテーブルで IP アドレス 1.1.1.0、マスク長 24 に最も合致するデータを取得するには、以下のテキストをコピーします。

```
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"
xmlns:nec="http://www.nec.com/netconf/base:1.0">
  <get>
    <filter type="subtree">
      <top xmlns="http://www.nec.com/netconf/data:1.0">
        <Route>
          <Ipv4Routes>
            <RouteEntry nec:filter=”IP 1.1.1.0 MaskLen 24 longer”/>
          </Ipv4Routes>
        </Route>
      </top>
    </filter>
  </get>
</rpc>
```

6.10.2 コラムベースフィルタリング

コラムベースのフィルタリングには、全一致、正規表現や条件指定があります。全一致フィルタリングは最高優先で、条件指定は最低優先です。複数のフィルタ条件が指定された場合、最も優先度の高いものが有効です。

- 全一致

  XML メッセージの要素指定で全一致が使用できます。複数の要素が指定されると、システムは指定された要素の全てに一致するデータを応答します。

  # クライアントから、UP している全てのインタフェースのコンフィグレーションを取得するには、以下のテキストをコピーします。

```
<rpc message-id ="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <get>
    <filter type="subtree">
      <top xmlns="http://www.nec.com/netconf/data:1.0">
        <Ifmgr>
```

```
          <Interfaces>
            <Interface>
              <AdminStatus>2</AdminStatus>
            </Interface>
          </Interfaces>
        </Ifmgr>
      </top>
    </filter>
  </get>
</rpc>
```

現在のテーブルのコラム名と同じ属性名を同じ行に指定して、全一致が行えます。システムは、属性名に一致するコンフィグレーションデータのみを応答します。上記の要素指定と同等の、全一致による XML メッセージは以下のとおりです。

```
<rpc message-id ="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <get>
    <filter type="subtree">
      <top xmlns="http://www.nec.com/netconf/data:1.0"xmlns:data="
http://www.nec.com/netconf/data:1.0">
        <Ifmgr>
          <Interfaces>
            <Interface data:AdminStatus="2"/>
          </Interfaces>
        </Ifmgr>
      </top>
    </filter>
  </get>
</rpc>
```

要素指定と属性指定による全一致の例で、両方とも等しく UP 状態の全インタフェースのコンフィグレーションを取得できることが示されています。

- 正規表現

  文字列による複雑な正規表現を行うには、要素に regExp 属性を指定します。

  サポートされるデータ型には、整数、日付と時刻、文字列、IPv4 アドレス、IPv4 マスク、MAC アドレス、OID、タイムゾーンが含まれます。

  # クライアントから、全て A から Z の大文字のインタフェースディスクリプションを取得するには、以下のテキストをコピーします。

```
<rpc message-id="1-0" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"
xmlns:nec="http://www.nec.com/netconf/base:1.0">
  <get-config>
    <source>
      <running/>
    </source>
    <filter type="subtree">
      <top xmlns="http://www.nec.com/netconf/config:1.0">
        <Ifmgr>
          <Interfaces>
            <Interface>
              <Description nec:regExp="^[A-Z]*$"/>
            </Interface>
          </Interfaces>
        </Ifmgr>
      </top>
    </filter>
  </get-config>
</rpc>
```

- 条件一致

  数字や文字列で複雑なデータフィルタリングを行うには、要素に match 属性を追加します。表 6-3は条件一致のオペレーション一覧です。

表 6-3 条件一致の演算子

オペレーション	演算子	補足
More than	match="more:value"	指定値より大きいです。サポートするデータのタイプは、日付、数字と文字列です。
Less than	match="less:value"	指定値より小さいです。サポートするデータのタイプは、日付、数字と文字列です。
Not less than	match="notLess:value"	指定値より小さくないです。サポートするデータのタイプは、日付、数字と文字列です。
Not more than	match="notMore:value"	指定値より大きくないです。サポートするデータのタイプは、日付、数字と文字列です。
Equal	match="equal:value"	指定値と等しいです。サポートするデータのタイプは、日付、数字、文字列、OIDとBOOLです。
Not equal	match="notEqual:value"	指定値と等しくありません。サポートするデータのタイプは、日付、数字、文字列、OIDとBOOLです。
Include	match="include:string"	指定文字列を含みます。サポートするデータのタイプは文字列のみです。
Not include	match="exclude:string"	指定文字列を含みません。サポートするデータのタイプは文字列のみです。
Start with	match="startWith:string"	指定文字で始まります。サポートするデータのタイプは文字列とOIDです。
End with	match="endWith:string"	指定文字で終わります。サポートするデータのタイプは文字列のみです。

クライアントから CPU 使用率が 50%より大きい拡張情報のエンティティを取得するには、以下のテキストをコピーします。

```
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"
xmlns:nec="http://www.nec.com/netconf/base:1.0">
  <get>
    <filter type="subtree">
      <top xmlns="http://www.nec.com/netconf/data:1.0">
        <Device>
          <ExtPhysicalEntities>
            <Entity>
                <CpuUsage nec:match="more:50"></CpuUsage>
            </Entity>
          </ExtPhysicalEntities>
        </Device>
      </top>
    </filter>
  </get>
</rpc>
```

6.10.3 正規表現によるデータのフィルタリング例

I. ネットワーク要件

Ifmgr モジュール配下のインタフェーステーブルで、ディスクリプションにコロンを含むデータを取得します。

II. 実行手順

XML view に移行します。

```
<AC> xml
```

capability を交換します。

```
<hello xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
    <capabilities>
        <capability>
            urn:ietf:params:netconf:base:1.0
        </capability>
    </capabilities>
</hello>
```

Ifmgr モジュール配下のインタフェーステーブルで、ディスクリプションにコロンを含むデータを取得します。

```
<?xml version="1.0"?>
<rpc message-id="100"
     xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"
xmlns:reg="http://www.nec.com/netconf/base:1.0">
  <get>
    <filter type="subtree">
      <top xmlns="http://www.nec.com/netconf/data:1.0">
        <Ifmgr>
          <Interfaces>
            <Interface>
                <Description  reg:regExp=":"/>
            </Interface>
          </Interfaces>
        </Ifmgr>
      </top>
    </filter>
  </get>
</rpc>
```

III. 結果確認

クライアントが以下のテキストを受信すれば、オペレーションは成功です。

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"
xmlns:reg="http://www.nec.com/netconf/base:1.0" message-id="100">
    <data>
        <top xmlns="http://www.nec.com/netconf/data:1.0">
            <Ifmgr>
                <Interfaces>
                    <Interface>
                        <IfIndex>2681</IfIndex>
                        <Description>FortyGigE1/0/1
Interface</Description>
                    </Interface>
                    <Interface>
                        <IfIndex>2682</IfIndex>
                        <Description>FortyGigE1/0/2
Interface</Description>
                    </Interface>
                    <Interface>
                        <IfIndex>2683</IfIndex>
                        <Description>FortyGigE1/0/3
Interface</Description>
                    </Interface>
                    <Interface>
                        <IfIndex>2684</IfIndex>
                        <Description>FortyGigE1/0/4
Interface</Description>
```

```
                    </Interface>
                  <Interface>
            </Ifmgr>
        </top>
    </data>
</rpc-reply>
```

6.10.4 条件一致によるデータのフィルタリング例

I. ネットワーク要件

Ifmgr モジュール配下のインタフェーステーブルにおいて、ifindex 値が 5,000 より小さくないコラムを取得します。

II. 実行手順

XML view に移行します。

```
<AC> xml
```

capability を交換します。

```
<hello xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
    <capabilities>
        <capability>
            urn:ietf:params:netconf:base:1.0
        </capability>
    </capabilities>
</hello>
```

Ifmgr モジュール配下のインタフェーステーブルにおいて、ifindex 値が 5,000 より小さくないコラムを取得します。

```
<rpc message-id="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"
xmlns:nc="http://www.nec.com/netconf/base:1.0">
  <get>
    <filter type="subtree">
      <top xmlns="http://www.nec.com/netconf/data:1.0">
        <Ifmgr>
          <Interfaces>
            <Interface>
                <IfIndex nc:match="more:5000"/>
                <Name/>
            </Interface>
          </Interfaces>
        </Ifmgr>
      </top>
    </filter>
  </get>
</rpc>
```

III. 結果確認

クライアントが以下のテキストを受信すれば、オペレーションは成功です。

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"
xmlns:nc="http://www.nec.com/netconf/base:1.0" message-id="100">
    <data>
        <top xmlns="http://www.nec.com/netconf/data:1.0">
            <Ifmgr>
                <Interfaces>
                    <Interface>
```

```
                        <IfIndex>7241</IfIndex>
                        <Name>NULL0</Name>
                    </Interface>
                    <Interface>
                        <IfIndex>7243</IfIndex>
                        <Name>Register-Tunnel0</Name>
                    </Interface>
                </Interfaces>
            </Ifmgr>
        </top>
    </data>
</rpc-reply>
```

6.11 NETCONF経由のCLI実行

XML メッセージにコマンドラインを内包し、デバイスのコンフィグレーションが行えます。

6.11.1 実行手順

クライアントからコマンドを実行するには、以下のテキストをコピーします。

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
      <CLI>
        <Execution>
          Commands
        </Execution>
      </CLI>
</rpc>
```

<Execution>で一行一コマンドを指定することにより、複数のコマンドを実行できます。

CLI オペレーション要求の受信後、デバイスはオペレーションに成功すると、以下のフォーマットで応答を返信します。

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply message-id="101"
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <CLI>
    <Execution>
      <![CDATA[Responses to the commands]]>
    </Execution>
  </CLI>
</rpc-reply>
```

6.11.2 CLI 実行例

I. 設定要件

デバイスに、**display current-configuration** コマンドを送信します。

II. 実行手順

XML view に移行します。

```
<AC> xml
```

capability を交換します。

```
<hello xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
    <capabilities>
        <capability>
            urn:ietf:params:netconf:base:1.0
        </capability>
    </capabilities>
</hello>
```

クライアントから以下のテキストをコピーして、**display current-configuration** コマンドを実行します。

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
      <CLI>
        <Execution>
          display current-configuration
        </Execution>
      </CLI>
</rpc>
```

III. 結果確認

クライアントが以下のテキストを受信すると、オペレーションは成功です。

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply message-id="101"
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <CLI>
    <Execution><![CDATA[
<AC>display current-configuration
#
 version 7.1.045, ESS 2305
#
 sysname AC
#
(省略)
return
   ]]>
   </Execution>
  </CLI>
</rpc-reply>
```

6.12 NETCONFセッション情報の取得

get-sessions オペレーションで、デバイスの NETCONF セッション情報を取得できます。

クライアントでデバイスのセッション情報を取得するには、以下のメッセージをコピーします。

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
    <get-sessions/>
</rpc>
```

get-sessions 要求の受信後、デバイスはオペレーションに成功すると、以下のフォーマットで応答を返信します。

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply message-id="101"
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <get-sessions>
```

```
    <Session>
      <SessionID>Configuration session ID </SessionID>
      <Line>line information</Line>
      <UserName>Name of the user creating the session</UserName>
      <Since>Time when the session was created</Since>
      <LockHeld>Whether the session holds a lock</LockHeld>
    </Session>
  </get-sessions>
</rpc-reply>
```

以下は、NETCONF セッション情報の取得例です。

XML view に移行します。

```
<AC> xml
```

capability を交換します。

```
<hello xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
    <capabilities>
        <capability>
            urn:ietf:params:netconf:base:1.0
        </capability>
    </capabilities>
</hello>
```

クライアントで以下のメッセージをコピーし、デバイスの現在の NETCONF セッション情報を取得します。

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
    <get-sessions/>
</rpc>
```

クライアントが以下のメッセージを受信すれば、オペレーションは成功です。

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"
message-id="101">
    <get-sessions>
        <Session>
            <SessionID>1</SessionID>
            <Line>vty0</Line>
            <UserName></UserName>
            <Since>2013-01-05T00:24:57</Since>
            <LockHeld>false</LockHeld>
        </Session>
    </get-sessions>
</rpc-reply>
```

出力結果は、ID が 1 の NETCONF セッションが存在することを示しています。ログインユーザのタイプは vty0、ログイン時刻は 2013/1/05 00:24:57 で、コンフィグレーションのロックはしていません。

6.13 他のNETCONFセッション排除

NETCONF は他のクライアントのセッションを排除することができます。排除されたクライアントは、user view に戻されます。

クライアントから指定 NETCONF セッションを排除するには、以下のメッセージをコピーします。

```
<rpc message-id="101"    xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
     <kill-session>
       <session-id>
         Specified session-ID
       </session-id>
```

```
     </kill-session>
</rpc>
```

kill-session 要求の受信後、デバイスはオペレーションに成功すると、以下のフォーマットで応答を返信します。

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply message-id="101"
    xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
      <ok/>
</rpc-reply>
```

6.13.1 実行例

I. 設定要件

セッション ID1 のユーザが、セッション ID2 のユーザを排除します。

II. 実行手順

XML view に移行します。

```
<AC> xml
```

capability を交換します。

```
<hello xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
    <capabilities>
        <capability>
            urn:ietf:params:netconf:base:1.0
        </capability>
    </capabilities>
</hello>
```

セッション ID2 のセッションを排除します。

```
<rpc message-id="101"    xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
     <kill-session>
       <session-id>2</session-id>
     </kill-session>
</rpc>
```

III. 結果確認

クライアントが以下のテキストを受信すると、NETCONF セッション ID2 のセッションは排除され、セッション ID2 のクライアントは XML view から user view に戻されます。

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply message-id="101"
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
    <ok/>
</rpc-reply>
```

6.14 CLIへの復帰

XML view から CLI に戻るには、以下の close-session 要求を送信します。

```
<?xml version="1.0"?>
<rpc message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
        <close-session/>
```

```
</rpc>
```

デバイスは close-session 要求を受信すると、以下の応答を送信して CLI の user view に復帰します。

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply message-id="101"
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
   <ok/>
</rpc-reply>
```

6.15 付録

6.15.1 NETCONF サポートオペレーション

表 6-4は、NETCONF で使用可能なオペレーションの一覧です。

表 6-4 NETCONF のデバイスコンフィグレーションメソッド

オペレーション	説明	XML 例
get	デバイスのコンフィグレーションと状態を取得します。	シスログのコンフィグレーションと状態を取得します。 <rpc message-id ="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" xmlns:xc="http://www.nec.com/netconf/base:1.0"> <get> <filter type="subtree"> <top xmlns="http://www.nec.com/netconf/data:1.0"> <Syslog> </Syslog> </top> </filter> </get> </rpc>
get-config	デフォルトではないコンフィグレーションを取得します。存在しない場合、デバイスは空の応答を返信します。	インタフェーステーブルのデフォルトではないコンフィグレーションを取得します。 <rpc message-id ="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" xmlns:xc="http://www.nec.com/netconf/base:1.0"> <get-config> <source> <running/> </source> <filter type="subtree"> <top xmlns="http://www.nec.com/netconf/config:1.0"> <Ifmgr> <Interfaces> <Interface/> </Interfaces> </Ifmgr> </top> </filter> </get-config> </rpc>
get-bulk	最初のデータから、指定したインデックスまでのエントリ(デバイスのコンフィグレーションや状態を含む)を取得します。	全てのインタフェースのコンフィグレーションと状態を取得します。 <rpc message-id ="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"> <get-bulk> <filter type="subtree"> <top

オペレーション	説明	XML 例
		xmlns="http://www.nec.com/netconf/data:1.0"> <lfmgr> <Interfaces xc:count="" xmlns:xc=" http://www.nec.com/netconf/base:1.0"> <Interface/> </Interfaces> </lfmgr> </top> </filter> </get-bulk> </rpc>
get-bulk-config	最初のデータから、指定したインデックスまでのデフォルトではないエントリを取得します。	全てのインタフェースについて、デフォルトではないコンフィグレーションを取得します。 <rpc message-id ="100" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"> <get-bulk-config> <source> <running/> </source> <filter type="subtree"> <top xmlns="http://www.nec.com/netconf/config:1.0"> <lfmgr> </lfmgr> </top> </filter> </get-bulk-config> </rpc>
edit-config: incremental	元データに影響無く、コラムにコンフィグレーションデータを追加します。 Incremental属性は、vlan許可リストといったコラムリストに追加します。 Incremental属性は、replace以外のedit-configオペレーションに使用できます。	<rpc message-id ="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" xmlns:nec="http://www.nec.com/netconf/base:1.0"> <edit-config> <target> <running/> </target> <config xmlns:xc="urn:ietf:params:xml:ns:netconf:base:1.0"> <top xmlns="http://www.nec.com/netconf/config:1.0"> <VLAN xc:operation="merge"> <HybridInterfaces> <Interface> <IfIndex>10</IfIndex> <UntaggedVlanList nec:incremental="true">1-10</UntaggedVlanList> </Interface> </HybridInterfaces> </VLAN> </top> </config> </edit-config> </rpc>
edit-config: merge	running-configurationを変更します。merge属性を	バッファサイズを120に変更します。 <rpc message-id ="101"

オペレーション	説明	XML 例
	使用する場合は、指定レベルでオペレーションのターゲットを指定する必要があります。 ● 指定ターゲットが既に存在する場合、ターゲットを直接変更します。 ● 指定ターゲットが存在しない場合、ターゲットを作成して設定します。 ● 指定ターゲットが存在せず、新規作成できない場合、エラーメッセージが返信されます。	xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" xmlns:xc="urn:ietf:params:xml:ns:netconf:base:1.0"> <edit-config> <target> <running/> </target> <config> <top xmlns="http://www.nec.com/netconf/config:1.0"><Syslog xmlns="http://www.nec.com/netconf/config:1.0" xc:operation="merge"> <LogBuffer> <BufferSize>120</BufferSize> </LogBuffer> </Syslog> </top> </config> </edit-config> </rpc>
edit-config: create	指定ターゲットを新規に作成します。create属性をedit-configオペレーションで使用するには、ターゲットを指定する必要があります。 ● テーブルがターゲットの新規作成が可能で、指定ターゲットが存在しない場合、オペレーションは新規作成した後ターゲットを設定します。 ● 指定ターゲットが存在する場合、data-existエラーメッセージが返信されます。	XMLデータフォーマットは、merge属性のedit-configメッセージと同じです。属性を**merge**から**create**に変更してください。
edit-config: replace	指定ターゲットを置換します。 ● 指定ターゲットが存在する場合、メッセージで伝達されたコンフィグレーションで置換します。 ● 指定ターゲットが存在せず、新規作成が可能な場合、ターゲットを作成してコンフィグレーションを適用します。 ● ターゲットが存在せず、新規作成が不	シンタックスは、merge属性のedit-configメッセージと同じです。属性を**merge**から**replace**に変更してください。

オペレーション	説明	XML 例
	可の場合、オペレーションは完了せず、エラーメッセージinvalid-valueが返信されます。	
edit-config: remove	指定コンフィグレーションを削除します。 ● 指定ターゲットがテーブルインデックスのみの場合、オペレーションは指定ターゲットの全てのコンフィグレーションとターゲット自体も削除します。 ● 指定ターゲットがテーブルインデックスとコンフィグレーションデータを持つ場合、オペレーションは該当ターゲットの指定コンフィグレーションを削除します。 ● 指定ターゲットが存在しない、またはXMLメッセージでターゲットを指定しない場合、成功メッセージが返信されます。	シンタックスはmerge属性のedit-configメッセージと同じです。属性を**merge**から**remove**に変更してください。
edit-config: delete	指定コンフィグレーションを消去します。 ● 指定ターゲットがテーブルインデックスのみの場合、オペレーションは該当ターゲットの全てのコンフィグレーションとターゲット自体も削除します。 ● 指定ターゲットがテーブルインデックスとコンフィグレーションデータを持つ場合、オペレーションは該当ターゲットの指定コンフィグレーションを削除します。 ● 指定ターゲットが	シンタックスはmerge属性のedit-configメッセージと同じです。属性を**merge**から**delete**に変更してください。

オペレーション	説明	XML 例
	存在しない場合、ターゲットが存在しないことを表すエラーメッセージを返信します。	
edit-config: default-operation	現在のコンフィグレーションを、デフォルトオペレーションを使用して変更します。edit-configメッセージで属性を指定しない場合、NETCONFはmerge、create、deleteとreplaceの一つをデフォルトオペレーションとして使用します。指定した<default-operation>は一回限り有効です。<edit-config>メッセージの属性とデフォルトオペレーションを指定しない場合、常に**merge**が適用されます。 ● **merge**—<default-operation>のデフォルト値です。 ● **replace—**オペレーション属性が指定せず、デフォルトオペレーションをreplaceとする場合に使用されます。 ● **none**—オペレーション属性を指定せず、デフォルトオペレーションをnoneとする場合に使用されます。この値が指定された場合、edit-configオペレーションはコンフィグレーションの適用ではなく、スキーマの検証としてのみ使用されます。スキーマが正しければ、成功メッセージが返信されます。正しくなければ、エラーメッセージが返信されます。	スキーマの確認用に、空のオペレーションを実行します。 <rpc message-id ="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"> <edit-config> <target> <running/> </target> <default-operation>none</default-operation> <config xmlns:xc="urn:ietf:params:xml:ns:netconf:base:1.0"> <top xmlns="http://www.nec.com/netconf/config:1.0"> <lfmgr> <Interfaces> <Interface> <Index>262</Index> <Description>222222</Description> </Interface> </Interfaces> </lfmgr> </top> </config> </edit-config> </rpc>
edit-config: error-option	コンフィグレーションエラーが発生した場合	error-optionをcontinue-on-errorとして、二つのインタフェースのコンフィグレーションを行います。 <rpc message-id ="101"

オペレーション	説明	XML 例
	の動作を定義します。error-option要素は、以下から一つの値をとります。 ● **stop-on-error**—エラー発生時にオペレーションを停止し、エラーメッセージを返信します。error-optionのデフォルト値です。 ● **continue-on-error**—エラー発生時でもオペレーションを継続し、エラーメッセージを返信します。 ● **rollback-on-error**—コンフィグレーションをロールバックします。現在のバージョンでは未サポートで、将来拡張用です。	xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"> <edit-config> <target> <running/> </target> <error-option>continue-on-error</error-option> <config xmlns:xc="urn:ietf:params:xml:ns:netconf:base:1.0"> <top xmlns="http://www.nec.com/netconf/config:1.0"> <lfmgr xc:operation="merge"> <Interfaces> <Interface> <Index>262</Index> <Description>222</Description> <ConfigSpeed>1000000</ConfigSpeed> <ConfigDuplex>1</ConfigDuplex> </Interface> <Interface> <Index>263</Index> <Description>333</Description> <ConfigSpeed>1000000</ConfigSpeed> <ConfigDuplex>1</ConfigDuplex> </Interface> </Interfaces> </lfmgr> </top> </config> </edit-config> </rpc>
edit-config: test-option	edit-configオペレーションで、コンフィグレーションを適用するかどうか定義します。test-option要素は、以下から一つの値をとります。 ● **test-then-set**—設定前に検証を行います。問題あれば、edit-configオペレーションは実行されません。これはtest-optionのデフォルト値です。 ● **set**—検証を行わず、直接設定を行います。 ● **test-only**—設定を行わず、検証のみ行います。問題なければ、成功メッセージが返信されます。問題あれば、エラーメッセージが返信さ	インタフェース設定のコンフィグレーションを検証します。 <rpc message-id ="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"> <edit-config> <target> <running/> </target> <test-option>test-only</test-option> <config xmlns:xc="urn:ietf:params:xml:ns:netconf:base:1.0"> <top xmlns="http://www.nec.com/netconf/config:1.0"> <lfmgr xc:operation="merge"> <Interfaces> <Interface> <Index>262</Index> <Description>222</Description> <ConfigSpeed>100</ConfigSpeed> <ConfigDuplex>1</ConfigDuplex> </Interface> </Interfaces> </lfmgr> </top> </config> </edit-config> </rpc>

オペレーション	説明	XML 例
	れます。	
action	コンフィグレーションデータではなく、リセットのようなアクションを実行します。	全てのインタフェースの統計情報をクリアします。 <rpc message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"> <action> <top xmlns="http://www.nec.com/netconf/action:1.0"> <lfmgr> <ClearAllIfStatistics> <Clear> </Clear> </ClearAllIfStatistics> </lfmgr> </top> </action> </rpc>
lock	edit-configで変更可能なコンフィグレーションデータをロックします。その他のコンフィグレーションはロックオペレーションで制限されません。ロックオペレーションはNETCONFセッションのみに対してであり、SNMPのような他のプロトコルに対してではありません。	コンフィグレーションをロックします。 <rpc message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"> <lock> <target> <running/> </target> </lock> </rpc>
unlock	コンフィグレーションのロックを解除し、NETCONFセッションでデバイスのコンフィグレーションを変更可能にします。NETCONFセッションが終了すると、ロックしたコンフィグレーションも解除されます。	コンフィグレーションのロックを解除します。 <rpc message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"> <unlock> <target> <running/> </target> </unlock> </rpc>
get-sessions	システムのNETCONFセッション情報を取得します。	システムの全てのNETCONFセッション情報を取得します。 <rpc message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"> <get-sessions/> </rpc>
close-session	現在のNETCONFセッションを終了し、コンフィグレーションのロックを解除し、メモリなどのリソースを解放します。現在のユーザは、XML viewからログオフ	現在のユーザのNETCONFセッションを終了します。 <rpc message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"> <close-session /> </rpc>

オペレーション	説明	XML 例
	します。	
kill-session	他のユーザのNETCONFセッションを排除させます。現在のユーザのNETCONFセッションは終了できません。	セッションID1のNETCONFセッションを排除させます。 <rpc message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"> <kill-session> <session-id>1</session-id> </kill-session> </rpc>
CLI	CLIを実行します。要求メッセージは<CLI>要素で囲まれたコマンドを内包し、コマンド実行結果のメッセージは<CLI>で囲まれます。NETCONFは以下のviewをサポートします。 ● **Execution—**User viewをサポートします。 ● **Configuration—**System viewをサポートします。 他のviewのコマンドを実行するには、該当viewに移行するコマンドを指定した後、実行するコマンドを記述してください。	system viewで**display this**コマンドを実行します。 <rpc message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"> <CLI> <Configuration>display this</Configuration> </CLI> </rpc>
save	running configurationを保存します。<file>要素で保存ファイルを指定できます。fileコラムが指定されないと、running configurationは自動的にメインnext-startupコンフィグレーションとして保存されます。OverWrite属性は、指定されたファイルがすでに存在する場合に、現在のコンフィグレーションが元のコンフィグレーションファイルを上書きするかどうかを決定します。	running configurationを**test.cfg**ファイルに保存します。 <rpc message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"> <save OverWrite="false"> <file>test.cfg</file> </save> </rpc>
load	コンフィグレーションを読み込みます。デバイスがloadオペレーションを完了すると、指定ファイルのコンフィグレーションが、現在のコンフィグレーションにマージされます。	a1.cfgファイルのコンフィグレーションを、現在のコンフィグレーションにマージします。 <rpc message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"> <load> <file>a1.cfg</file> </load> </rpc>

オペレーション	説明	XML 例
rollback	コンフィグレーションをロールバックします。<file>要素でコンフィグレーションファイルを指定する必要があります。デバイスがロールバックオペレーションを完了すると、現在のコンフィグレーションは全て、指定されたファイルのコンフィグレーションに置き換わります。	現在のコンフィグレーションを、1A.cfgファイルのコンフィグレーションにロールバックします。 <rpc message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"> <rollback> <file>1A.cfg</file> </rollback> </rpc>

目次

このセクションのページは **17-x-x** です。

7 章 プロセスモニタリングとメンテナンス 7-1
7.1 ユーザプロセスの表示と維持 7-1

7章 プロセスモニタリングとメンテナンス

装置のシステムソフトウェアは、フル機能でモジュラー型の Linux カーネルをベースにした拡張可能なネットワークオペレーティングシステムです。システム（Comware）ソフトウェアは、独立した以下のプロセスがあります。

- **ユーザプロセス**－ユーザ空間で動作します。ユーザプロセスでたいていのシステムソフトウェア機能が動作します。各プロセスは、独立して動作します。あるプロセスが故障しても、その他のプロセスに影響しません。システムは自動的にユーザプロセスをモニタリングします。システムソフトウェアは preemptive マルチスレッティングをサポートしています。プロセスは複数のアクティビティをサポートするために、複数のスレッドを動作することができます。マルチスレッティングの実装は、ソフトウェアのバージョンに依存します。

7.1 ユーザプロセスの表示と維持

すべての view で **display** コマンドを実行でき、user view でその他のコマンドを実行できます。

操作	コマンド
プロセス例外に関する情報を表示する	**display exception context** [**count** *value*]
コアファイルディレクトリを表示する	**display exception filepath**
カーネルスレッドのデッドループ情報を表示する	**display kernel deadloop** *show-number* [*offset*] [**verbose**]
カーネルスレッドの例外情報を表示する	**display kernel exception** *show-number* [*offset*] [**verbose**]
カーネルスレッドの再起動情報を表示する	**display kernel reboot** *show-number* [*offset*] [**verbose**]
カーネルスレッド不足情報を表示する	**display kernel starvation** *show-number* [*offset*] [**verbose**]
例外でコアファイルを作成するための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(デフォルトは1）を設定する	**process core** { **maxcore** *value* | **off** } { **job** *job-id* | **name** *process-name* }
コアファイルを保存するディレクトリ（デフォルトはマスタ装置のflash:/）を指定する	**exception filepath** *directory*
プロセス例外に関する情報をクリアする	**reset exception context**
カーネルスレッドのデッドループ情報をクリアする	**reset kernel deadloop**
カーネルスレッド例外情報をクリアする	**reset kernel exception**
カーネルスレッドの再起動情報をクリアする	**reset kernel reboot**

操作	コマンド
カーネルスレッド不足情報をクリアする	**reset kernel starvation**

目次

このセクションのページは **17-x-x** です。

8 章 ポートミラーリング 8-1
8.1 概要 8-1
8.1.1 用語 8-1
8.1.2 ローカルポートミラーリングの実行 8-2
8.2 ローカルポートミラーリング設定作業リスト 8-3
8.3 ローカルミラーリンググループの作成 8-3
8.4 ローカルミラーリンググループのソースポートの作成 8-3
8.4.1 設定の制限とガイドライン 8-3
8.4.2 system view でのソースポートの設定 8-3
8.4.3 interface view でのソースポートの設定 8-4
8.5 ローカルミラーリンググループのモニタポートの作成 8-4
8.5.1 設定の制限とガイドライン 8-4
8.5.2 system view でのモニタポートの設定 8-4
8.5.3 interface view でのモニタポートの設定 8-4
8.6 ポートミラーリングの表示と維持 8-5
8.7 ポートミラーリングの設定例 8-5

8章 ポートミラーリング

8.1 概要

ポートミラーリングはポートを通過したパケットを分析するために、データ監視端末が接続されているモニタポートへパケットをコピーします。

8.1.1 用語

以下にポートミラーリングの設定で使用する用語を示します。

I. ミラーリングソース

1 つのモニタ対象ポートをミラーリングソースにすることができます。モニタ対象ポートはソースポートと呼ばれます。ミラーリングソースを通過するパケットはパケットを解析するデータをモニタリングするデバイスに接続するポートにコピーされます。コピーはミラーパケットと呼ばれます。

II. ソースデバイス

ミラーリングソースが存在するデバイスは”送信元デバイス”あるいは”ソースデバイス”と呼ばれます。

III. ミラーリング宛先

ミラーリング宛先は、ミラーリングされたパケットの宛先ポート（別名モニタポートとも呼ばれます）であり、データ監視装置に接続します。モニタポートは、接続されている監視装置にミラーリングされたパケットを転送します。

モニタポートは複数のポートをモニタすることができ、場合によっては複数の重複したパケットを受信する可能性があります。たとえば、以下の状況が存在するとき、2 つのパケットのコピーはポート 1 で受信されます。

- ポート 1 は同一デバイス上のポート 2 とポート 3 の送受信トラフィックをモニタします。
- パケットがポート 2 からポート 3 へ転送されます。

IV. 宛先デバイス

モニタポートが存在するデバイスは"宛先デバイス"あるいは”ディスティネーションデバイス”と呼ばれます。

V. ミラーリング方向

ミラーリング方向は、受信トラフィック、送信トラフィック、送受信トラフィックがあり、モニタリングソースでコピーされます。

- **受信** – ミラーリングソースで受信したパケットをコピーします。
- **送信** – ミラーリングソースに送信したパケットをコピーします。
- **送受信** – ミラーリングソースで送受信したパケットをコピーします。

VI. ミラーリンググループ

ポートミラーリングはポートミラーリンググループによって実行されます。ミラーリンググループには 3 つのタイプ（ローカル、リモートソース、リモート宛先ミラーリング）があります。

8.1.2 ローカルポートミラーリングの実行

ローカルポートミラーリングでは、以下の状況となります。

- ソースデバイスは、データをモニタリングするデバイスに直接接続されています。
- ソースデバイスは、データをモニタリングするデバイスにミラーリングしたパケットを転送する宛先デバイスとして動作できます。

ローカルミラーリンググループは、同一装置上のミラーリングソースとミラーリング宛先を含むミラーリンググループです。

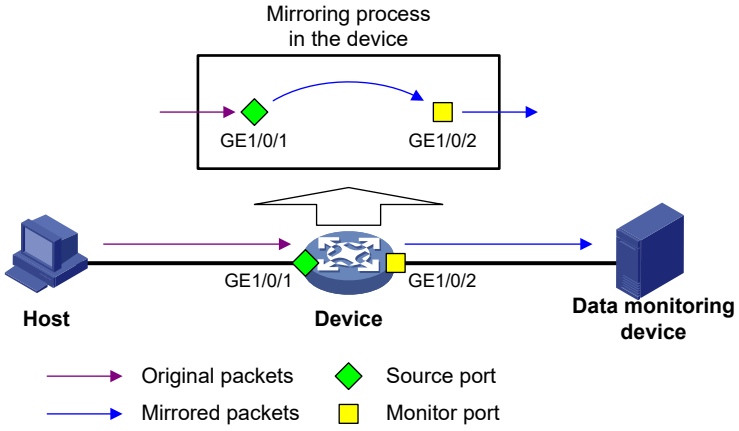


図 8-1 ローカルポートミラーリングの実行

図 8-1 に示すように、ソースポート GigabitEthernet 1/0/1 とモニタポート GigabitEthernet 1/0/2 は同じデバイス上にあります。GigabitEthernet 1/0/1 のパケットは GigabitEthernet 1/0/2 にコピーされ、解析を行うためデータ監視装置に転送されます。

8.2 ローカルポートミラーリング設定作業リスト

作業リスト
1.　（必須設定項目） ローカルミラーリンググループの作成
2.　（必須設定項目） ローカルミラーリンググループのソースポートの作成
3.　（必須設定項目） ローカルミラーリンググループのモニタポートの作成

8.3 ローカルミラーリンググループの作成

操作	コマンド	補足
1.　system view に移行する	**system-view**	―
2.　ローカルミラーリンググループを作成する	**mirroring-group** *group-id* **local**	デフォルト：設定なし

8.4 ローカルミラーリンググループのソースポートの作成

ローカルミラーリンググループのソースポートは、以下のいずれかの方法で設定することができます。

- system view でミラーリンググループにソースポートを割り当てます。
- interface view でソースポートとしてミラーリンググループにポートを割り当てます。

  interface view でミラーリンググループに複数のポートを割り当てる場合、上記の方法を繰り返してください。

8.4.1 設定の制限とガイドライン

ローカルミラーリンググループにソースポートを設定するとき、以下の設定の制限とガイドラインに従ってください。

- レイヤ 2 アグリゲートインタフェースはソースポートとして設定することができません。
- ミラーリンググループは複数のソースポートを持つことができます。
- ポートはソースポートとして、1 つのミラーリンググループに対してのみ動作します。
- ソースポートをモニタポートとして設定できません。

8.4.2 system view でのソースポートの設定

操作	コマンド	補足
1.　system view に移行する	**system-view**	―
2.　指定したローカルミラーリンググループにモニタポートを設定する	**mirroring-group** *group-id* **mirroring-port** *interface-list* { **both** | **inbound** | **outbound** }	デフォルト：設定なし

8.4.3 interface view でのソースポートの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. interface view に移行する	**interface** *interface-type interface-number*	―
3. 指定したミラーリンググループにモニタポートを設定する	**mirroring-group** *group-id* **mirroring-port** { **both** | **inbound** | **outbound** }	デフォルト：設定なし

8.5 ローカルミラーリンググループのモニタポートの作成

ミラーリンググループのモニタポートを設定する場合、以下のいずれかの方法で設定することができます。

- system view でミラーリンググループのモニタポートを設定します。
- interface view でポートをモニタポートとしてミラーリンググループに割り当てることができます。

8.5.1 設定の制限とガイドライン

ローカルミラーリンググループにモニタポートを設定するとき、以下の設定の制限とガイドラインに従ってください。

- モニタポートでスパニングツリー機能を有効にしないでください。
- レイヤ 2 アグリゲートインタフェースはモニタポートとして設定することができません。
- モニタポートは、ポートミラーリングのために使用してください。データをモニタリングするデバイスがミラーされたトラフィックのみを受信するように、ポートミラーリングのモニタポートを使用してください。

8.5.2 system view でのモニタポートの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. 指定したローカルミラーリンググループにモニタポートを設定する	**mirroring-group** *group-id* **monitor-port** *interface-list*	デフォルト：設定なし

8.5.3 interface view でのモニタポートの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. interface view に移行する	**interface** *interface-type interface-number*	―

操作	コマンド	補足
3. 指定したミラーリンググループにモニタポートを設定する	**mirroring-group** *group-id* **monitor-port**	デフォルト：設定なし

8.6 ポートミラーリングの表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
ミラーリンググループの情報を表示する	**display mirroring-group** { *group-id* | **all** | **local** }

8.7 ポートミラーリングの設定例

I. ネットワーク要件

図 8-2 に示すように、サーバが IP ネットワークの双方向のトラフィックを監視できるように、AC でローカルポートミラーリングを設定します。

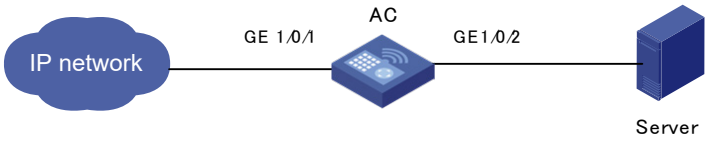


図 8-2 ネットワーク図

II. 設定手順

ローカルミラーリンググループ 1 を作成します。

```
<AC> system-view
[AC] mirroring-group 1 local
```

GigabitEthernet 1/0/1 の双方向のトラフィックを監視するようにローカルミラーリンググループ 1 を設定します。

```
[AC] mirroring-group 1 mirroring-port gigabitethernet 1/0/1 both
```

ローカルミラーリンググループ 1 のモニタポートとして GigabitEthernet 1/0/2 を設定します。

```
[AC] mirroring-group 1 monitor-port gigabitethernet 1/0/2
```

III. 設定の確認

ミラーリンググループの設定を確認します。

```
[AC] display mirroring-group 1
Mirroring group 1:
    Type: Local
    Status: Active
    Mirroring port:
        GigabitEthernet1/0/1  both
    Monitor port: GigabitEthernet1/0/2
```

目次

このセクションのページは **17-x-x** です。

9章 パケットキャプチャの設定 9-1
9.1 概要 9-1
9.1.1 パケットキャプチャモード 9-1
9.1.2 フィルタ要素 9-1
9.2 キャプチャフィルタルール 9-2
9.2.1 キャプチャフィルタキーワード 9-2
9.2.2 キャプチャフィルタ演算子 9-4
9.2.3 キャプチャフィルタルール式 9-5
9.3 ディスプレイフィルタルール 9-7
9.3.1 ディスプレイフィルタキーワード 9-7
9.3.2 ディスプレイフィルタ演算子 9-8
9.3.3 ディスプレイフィルタルール式 9-9
9.4 制限とガイドライン 9-10
9.5 ローカルパケットキャプチャの設定 9-10
9.6 パケットキャプチャの停止 9-11
9.6.1 制限とガイドライン 9-11
9.7 パケットキャプチャの表示と管理 9-11
9.8 パケットキャプチャ設定例 9-11
9.8.1 ローカルパケットキャプチャ設定例 9-11

9章 パケットキャプチャの設定

9.1 概要

パケットキャプチャ機能は、CPU に転送される受信パケットをキャプチャします。この機能により、キャプチャされたパケットがリアルタイムに表示され、キャプチャされたパケットを分析のために“.pcap”ファイルに保存することができます。

9.1.1 パケットキャプチャモード

ローカルパケットキャプチャは、キャプチャされたパケットを FTP サーバ上のリモートファイルまたはローカルファイルに保存します。

リモートパケットキャプチャは未サポートです。

9.1.2 フィルタ要素

パケットキャプチャは、キャプチャフィルタとディスプレイフィルタをサポートします。条件式を使用して、キャプチャまたは表示するパケットを照合することができます。

キャプチャフィルタまたはディスプレイフィルタには、キーワード文字列または演算子によって接続された複数のキーワード文字列が含まれます。

キーワードには、次のタイプがあります。

- **Qualifiers**—固定されたキーワード文字列です。たとえば、IPv4 プロトコルを指定するためには **ip** 修飾子を使用する必要があります。
- **Variables**—ユーザが必要な形式で指定した値です。たとえば、IP アドレスを 2.2.2.2 と指定を行うことや、その他の有効な値を設定できます。

変数は、1 つまたは複数の修飾子で設定する必要があります。たとえば、2.2.2.2 でホストから送信されたパケットをキャプチャするには、フィルタ **src host 2.2.2.2** を使用します。

演算子には次のタイプがあります。

- **Logical operators**—AND 演算などの論理演算を実行します。
- **Arthmentic operators**—ADD 演算などの算術演算を実行します。
- **Relationnal operators**—キーワード文字列間の関係を示します。たとえば、=演算子は等価を示します。

このドキュメントは、これらの要素に関する基本的な情報を提供します。キャプチャおよび表示フィルタの詳細については、次の Web サイトを参照してください。

- https://wiki.wireshark.org/CaptureFilters
- https://wiki.wireshark.org/DisplayFilters

9.2 キャプチャフィルタルール

9.2.1 キャプチャフィルタキーワード

I. 修飾子

表 9-1 キャプチャフィルタの修飾子

カテゴリー	説明	例
Protocol	プロトコルに基づいてパケットを照合します。 プロトコル修飾子を指定しない場合、フィルタはサポートされているプロトコルと一致します。	• **arp**—ARPと一致します。 • **icmp**—ICMPと一致します。 • **ip**—IPv4と一致します。 • **tcp**—TCPと一致します。 • **udp**—UDPと一致します。
Direction	送信元または宛先の場所（IPアドレスまたはポート番号）に基づいてパケットを照合します。 direction修飾子を指定しない場合は、**src or dst**修飾子が適用されます。	• **src**—送信元IPアドレスと照合します。 • **dst**—宛先IPアドレスと照合します。 • **src or dst**—送信元または宛先IPアドレスと照合します。 ⚠ **メモ：** direction修飾子を指定しない場合は、**src or dst**修飾子が適用されます。たとえば、**port 23**は**src or dst port 23**と同等です。
Type	方向の種類を指定します。	• **host**—ホストのIPアドレスと照合します。 • **net**—IPサブネットと照合します。 • **port**—サービスポート番号と照合します。 • **portrange**—サービスポート範囲と照合します。 ⚠ **メモ：** Type修飾子を指定しないと、**host**修飾子が適用されます。たとえば、**src 2.2.2.2**は**src host 2.2.2.2**と同等です。

カテゴリー	説明	例
Others	前述の修飾子以外の修飾子です。	• **broadcast**—ブロードキャストパケットと照合します。 • **multicast**—マルチキャストパケット及びブロードキャストパケットと照合します。 • **less**—特定のサイズ以下のパケットと照合します。 • **greater**—特定のサイズ以上のパケットと照合します。 • **len**—パケットレングスで照合します。 • **vlan**—VLANで照合します。

II. 変数

キャプチャフィルタの変数は、1 つ以上の修飾子で変更する必要があります。

ブロードキャスト、マルチキャスト、およびすべてのプロトコル修飾子では、変数を変更できません。その他の修飾子の後には、変数を指定する必要があります。

表 9-2 キャプチャフィルタの変数タイプ

変数タイプ	説明	例
Integer	バイナリ、8進、10進、16進表記示します。	**port 23**条件式は、ポート番号23との間で送受信されるトラフィックと一致します。
Integer range	ハイフンで繋いだ整数で示します。	**portrange 100-200**の条件式は、100～200の範囲の任意のポートに送受信されるトラフィックと一致します。
IPv4 address	ドット付き10進表記で示します。	**src 1.1.1.1**条件式は、1.1.1.1のIPv4ホストから送信されたトラフィックと一致します。
IPv4 subnet	IPv4ネットワークIDまたはマスク付きIPv4アドレスで示します。	次のそれぞれの式は、IPv4サブネット1.1.1.0/24との間で送受信されるトラフィックと一致します。 • **src 1.1.1** • **src net 1.1.1.0/24**

9.2.2 キャプチャフィルタ演算子

I. 論理演算子

論理演算子は左結合です。それらは左から右にグループ化します。**not** 演算子が最も高い優先度を持ちます。**and** と **or** 演算子は同じ優先順位を持ちます。

表 9-3 キャプチャフィルタの論理演算子

英数字以外の記号	英数字記号	説明
!	not	条件の結果を元に戻します。この演算子を使用して、条件の反対の値に一致するトラフィックを取得します。 たとえば、HTTP以外のトラフィックをキャプチャするには、**not port 80**と指定してください。
&&	and	2つが条件に加わります。それぞれの条件に一致するトラフィックを取得するには、この演算子を使用します。 たとえば、**1.1.1.1**との間で送受信されるHTTP以外のトラフィックをキャプチャするには、**host 1.1.1.1 and not port 80**と指定してください。
||	or	2つが条件に加わります。いずれかの条件に一致するトラフィックをキャプチャするには、この演算子を使用します。 たとえば、**1.1.1.1**または**2.2.2.2**との間で送受信されるトラフィックをキャプチャするには、**host 1.1.1.1 or host 2.2.2.2**と指定してください。

II. 算術演算子

表 9-4 キャプチャフィルタの算術演算子

英数字以外の記号	説明
+	2つの値を加算します。
-	ある値を別の値から引きます。
*	ある値を別の値に乗算します。
/	ある値を別の値で割ります。
&	バイナリ形式の2つの整数値に対するビット単位のAND演算の結果を返します。
|	バイナリ形式の2つの整数値に対するビット単位のOR演算の結果を返します。

英数字以外の記号	説明
<<	演算子の左側のオペランドに対してビット単位の左シフト演算を実行します。右側のオペランドは、シフトするビット数を指定します。
>>	演算子の左側のオペランドに対してビット単位の右シフト演算を実行します。右側のオペランドは、シフトするビット数を指定します。
[ ]	プロトコルレイヤに対するバイトオフセットを指定します。このオフセットは、照合を始めるバイトを示します。 オフセット値を角カッコで囲み、プロトコル修飾子を指定する必要があります。たとえば、**ip [6]**はIPv4パケット（IPv4ペイロードの先頭から6バイト離れたバイト）のペイロードの7番目のバイトと照合します。

III. 関係演算子

表 9-5 キャプチャフィルタの関係演算子

英数字以外の記号	説明
=	イコール たとえば、ip[6]=0x1cは、ペイロードの第7バイトが0x1cに等しい場合、IPv4パケットに一致します。
!=	ノットイコール たとえば、長さが60バイトでない場合、**len!= 60**はパケットと一致します。
>	～より大きい たとえば、長さが100バイトを超える場合、**len>100**はパケットに一致します。
<	～未満 たとえば、長さが100バイト未満の場合、**len <100**はパケットと一致します。
>=	～以上またはイコール たとえば、長さが100バイト以上または等しい場合、**len>=100**はパケットに一致します。
<=	～より小さいまたはイコール たとえば、長さが100バイト以下または等しい場合、**len<=100**はパケットに一致します。

9.2.3 キャプチャフィルタルール式

I. 論理式

論理演算の結果と一致するパケットをキャプチャするには、このタイプの式を使用します。

論理式には、キーワードと論理演算子が含まれます。次に例を示します。

- **not port 23 and not port 22**:ポート番号が 23 でも 22 でもないパケットをキャプチャします。
- **port 23 or icmp**:ポート番号が 23 のパケットまたは ICMP パケットをキャプチャします。

論理式では、修飾子は、最も近い論理演算子で接続された複数の変数を変更できます。たとえば、IPv4 アドレス 192.168.56.1 または IPv4 ネットワーク 192.168.27 から送信されたパケットをキャプチャするには、次の式のいずれかを使用します。

- **src 192.168.56.1 or 192.168.27**
- **src 192.168.56.1 or src 192.168.27**

II. expr relop expr 式

このタイプの式を使用して、算術演算の結果と一致するパケットをキャプチャします。

この式には、キーワード、算術演算子 (expr) 、および関係演算子 (relop) が含まれます。たとえば、**len+100>=200** は 100 バイト以上のパケットをキャプチャします。

III. proto [expr:size] 式

このタイプの式を使用して、プロトコル層を基準としたバイト数の算術演算の結果と一致するパケットをキャプチャします。

このタイプの式には、次の要素が含まれます。

- *proto*:プロトコル層を指定します。
- []:プロトコル層を基準としたバイト数の算術演算を実行します。
- *expr*:算術式を指定します。
- *size*:バイトオフセットを指定します。このオフセットは、プロトコル層を基準としたバイト数を示します。演算は、指定されたバイトに対して実行されます。オフセットを指定しない場合、オフセットは 1 バイトに設定されます。

たとえば、**ip [0] &0xf!=5** は、最初のバイトを 0x0f と AND 演算した結果が 5 でない場合に IP パケットをキャプチャします。

フィールドを照合するには、expr:size にフィールド名を指定します。たとえば、**icmp [icmptype] =0x08** は、Type フィールドに 0x08 の値を含む ICMP パケットをキャプチャします。

IV. vlan vlan_id 式

802.1Q タグ付き VLAN トラフィックをキャプチャするには、このタイプの式を使用します。

このタイプの式には、vlan vlan_id キーワードと論理演算子が含まれます。vlan_id 変数は、VLAN ID を指定する整数です。たとえば、**vlan 1 and ip** は VLAN 1 の IPv4 パケットをキャプチャします。

VLAN からパケットをキャプチャするには、キャプチャフィルタを次のように設定します。

- インターフェイスで許可されているタグ付きパケットをキャプチャするには、他の式の前に vlan vlan_id 式を使用する必要があります。たとえば、192.168.1.10 から 192.168.1.1 に送信される VLAN 3 のパケットをキャプチャするには、**vlan 3 and src 192.168.1.10 and dst 192.168.1.1** を使用します。
- インターフェイスで受信されるタグなしパケットをキャプチャするには、次のルールに従ってください。
  - デバイスがパケットヘッダーに VLAN タグを追加する場合は、キャプチャフィルタ式に 「vlan xx」 を追加します。レイヤ 3 パケットの場合、xx は発信インターフェイスのデフォルト VLAN ID を表します。レイヤ 2 パケットの場合、xx は着信インターフェイスのデフォルト VLAN ID を表します。

□ デバイスがパケットヘッダーに VLAN タグを追加しない場合は、キャプチャフィルタ式に 「vlan xx」 を追加しないでください。

9.3 ディスプレイフィルタルール

ディスプレイフィルタルールは、表示するパケットのみを識別します。ファイルに保存するパケットには影響しません。

9.3.1 ディスプレイフィルタキーワード

I. 修飾子

表 9-6 ディスプレイフィルタの修飾子

カテゴリー	説明	例
Protocol	プロトコルと照合します。	• **eth**—イーサネットに一致します。 • **ftp**—FTPに一致します。 • **http**－HTTPに一致します。 • **icmp**—ICMPに一致します。 • **ip**—IPv4に一致します。 • **tcp**—TCPに一致します。 • **telnet**—Telnetに一致します。 • **udp**—UDPに一致します。
Packet field	*protocol.field[.level1-subfield]…[.leveln-subfield]*形式の点線の文字列を使用して、パケット内のフィールドを照合します。	• **tcp.flags.syn**—TCPのflagsフィールドのSYNビットと一致します。 • **tcp.port**—送信元または宛先ポートのフィールドと一致します。

II. 変数

パケットフィールド修飾子には変数が必要です。

表 9-7 ディスプレイフィルタの変数タイプ

変数タイプ	説明
Integer	バイナリ、8進、10進、16進表記で示します。 たとえば、1500バイト以下のIPパケットを表示するには、次のいずれかの式を使用します。 • **ip.len le 1500** • **ip.len le 02734** • **ip.len le 0x436**

変数タイプ	説明
Boolean	この変数型には、trueまたはfalseの2つの値があります。 この変数タイプは、パケット内のフィールドの存在を識別するためにパケットフィールド文字列を単独で使用する場合に適用されます。 ● フィールドが存在する場合、一致結果はtrueです。フィルタにパケットが表示されます。 ● フィールドが存在しない場合、一致結果はfalseです。フィルタはパケットを表示しません。 たとえば、SYNフィールドを含むTCPパケットを表示するには、**tcp.flags.syn**を使用します。
MAC address(6バイト)	コロン（:）、ドット（.）、またはハイフン（-）を使用して、MACアドレスを2つまたは4つのセグメントに分割します。 たとえば、宛先MACアドレスがffff.ffff.ffffのパケットを表示するには、次のいずれかの式を使用します。 ● **eth.dst==ff:ff:ff:ff:ff:ff** ● **eth.dst==ff-ff-ff-ff-ff-ff** ● **eth.dst==ffff.ffff.ffff**
IPv4 address	ドット付き10進表記で表されます。 例： ● 192.168.0.1との間で送受信されるIPv4パケットを表示するには、**ip.addr==192.168.0.1**を使用します。 ● 129.111.0.0/16に送信されたIPv4パケットを表示するには、**ip.addr==129.111.0.0/16**を使用します。
String	文字列 たとえば、リクエストバージョンフィールドの文字列HTTP/1.1を含むHTTPパケットを表示するには、**http.request version=="HTTP/1.1"**を使用します。

9.3.2 ディスプレイフィルタ演算子

論理演算子は左結合です。左から右にグループ化されます。[]演算子の優先順位は最も高くなります。**not** 演算子の優先順位は最も高くなります。**and** 演算子と **or** 演算子の優先順位は同じです。

I. 論理演算子

表 9-8 ディスプレイフィルタの論理演算子

英数字以外の記号	英数字記号	説明
[ ]	英数字の記号は使用できません。	プロトコル修飾子と共に使用します。詳細は、本章の“*ディスプレイフィルタルール式*”の“*proto [...] 式*”を参照してください。
!	not	この演算子に接続されている条件と一致しないパケットを表示します。

英数字以外の記号	英数字記号	説明
&&	and	2つが条件に加わります。 それぞれの条件に一致するトラフィックを表示するには、この演算子を使用します。
||	or	2つが条件に加わります。 いずれかの条件に一致するトラフィックを表示するには、この演算子を使用します。

II. 関係演算子

表 9-9 ディスプレイフィルタの関係演算子

英数字以外の記号	英数字記号	説明
==	eq	イコール たとえば、**ip.src==10.0.0.5**は、送信元IPアドレスが10.0.0.5のパケットを表示します。
!=	ne	ノットイコール たとえば、**ip.src!=10.0.0.5**は、送信元IPアドレスが10.0.0.5ではないパケットを表示します。
>	gt	～より大きい たとえば、**frame.len>100**は、100バイトを超える長さのフレームを表示します。
<	lt	～未満 たとえば、**frame.len<100**は、100バイト未満の長さのフレームを表示します。
>=	ge	～以上またはイコール たとえば、**frame.len ge 0x100**は、256バイト以上の長さのフレームを表示します。
<=	le	～より小さいかイコール たとえば、**frame.len le 0x100**は、256バイト以下の長さのフレームを表示します。

9.3.3 ディスプレイフィルタルール式

I. 論理式

論理演算の結果と一致するパケットを表示する場合に使用します。

論理式には、キーワードと論理演算子が含まれます。たとえば、**ftp or icmp** は、すべての FTP パケットと ICMP パケットを表示します。

II. 関係式

比較演算の結果と一致するパケットを表示する場合に使用します。

関係式には、キーワードと関係演算子が含まれます。たとえば、**ip.len<=28** と指定すると、長さフィールドに 28 バイト以下の値を含む IP パケットが表示されます。

III. パケットフィールド式

特定のフィールドを含むパケットを表示するには、このタイプの式を使用します。

パケットフィールド式には、パケットフィールド文字列のみが含まれます。たとえば、**tcp.flags.syn** は SYN ビットフィールドを含むすべての TCP パケットを表示します。

IV. proto [...] 式

特定のフィールド値を含むパケットを表示するには、このタイプの式を使用します。

このタイプの式には、次の要素が含まれます。

- *proto*:プロトコル層またはパケットフィールドを指定します。
- [...] :プロトコル層またはパケットフィールドに対して相対的なバイト数と一致します。一致するバイトの値は、16 進整数文字列である必要があります。角カッコ内の式には、次の形式を使用できます。
  - [*n:m*] :指定したプロトコル層またはフィールドの先頭から n バイトのオフセット以降の合計 m バイトと一致します。1 バイトだけと一致させるには、[n] と [n:1] の両方の形式を使用できます。たとえば、**eth.src [0:3] ==00:00:83** は、送信元 MAC アドレスの最初の 3 バイトが 0x00、0x00、および 0x83 であるイーサネットフレームと一致します。**eth.src [2] ==83** 式は、送信元 MAC アドレスの 3 バイト目が 0x83 であるイーサネットフレームと一致します。
  - [*n-m*]:指定されたプロトコル層またはパケットフィールドの先頭からの (n+1) 番目のバイトから始まり、合計 (m-n+1) バイトと一致します。たとえば、**eth.src [1-2] ==00:83** は、送信元 MAC アドレスの 2 番目と 3 番目のバイトがそれぞれ 0x00 と 0x83 であるイーサネットフレームと一致します。

9.4 制限とガイドライン

パケットキャプチャ機能は、9196 バイト以下のフレーム長のパケットだけをキャプチャできます。パケットのフレーム長が 9196 バイトを超える場合、システムはパケットをキャプチャしません。

9.5 ローカルパケットキャプチャの設定

このタスクを実行して、AP 無線で受信パケットをキャプチャし、キャプチャしたパケットを FTP サーバ上のファイルに保存します。キャプチャされたパケットを表示するには、FTP サーバに接続された Wireshark クライアントを使用します。

AP 無線でローカルパケットキャプチャを設定するには、次の手順を実行します。

操作	コマンド	補足
AP無線でローカルパケットキャプチャを設定します。	**packet-capture local ap** *ap-name* **radio** *radio-id* [**capture-filter** *capt-expression* | **limit-frame-size bytes** | **autostop filesize** *kilobytes* | **autostop duration** *seconds*] * **write url** *url* [**username** *username* [**password** { **cipher** | **simple** } *key*]]	このコマンドを実行した後でも、CLIから他のコマンドを設定できます。その操作はパケットキャプチャには影響しません。

9.6 パケットキャプチャの停止

パケットのキャプチャ中にキャプチャを停止するには、**packet-capture stop** コマンドを使用します。

9.6.1 制限とガイドライン

階層型ネットワーク上のローカル AC がオフラインになると、中央 AC はローカル AC に接続されている AP のパケットキャプチャ管理プロセスを停止します。ただし、AP のパケットキャプチャは続行されます。パケットキャプチャを停止するには、AP の中央 AC でパケットキャプチャを再度有効にし、**packet-capture stop** コマンドを実行する必要があります。

9.7 パケットキャプチャの表示と管理

すべてのビューで **display** コマンドを実行できます。

操作	コマンド
パケットキャプチャ状態の表示	**display packet-capture status**

9.8 パケットキャプチャ設定例

9.8.1 ローカルパケットキャプチャ設定例

I. ネットワーク要件

図 9-1に示すように、AP の無線 1 でローカルパケットキャプチャを有効にすると、192.168.20.173 から送信された 1KB の TCP パケットがキャプチャされます。スイッチは、APによって送信されたキャプチャされたパケットを保存するためのFTPサーバとして機能します。

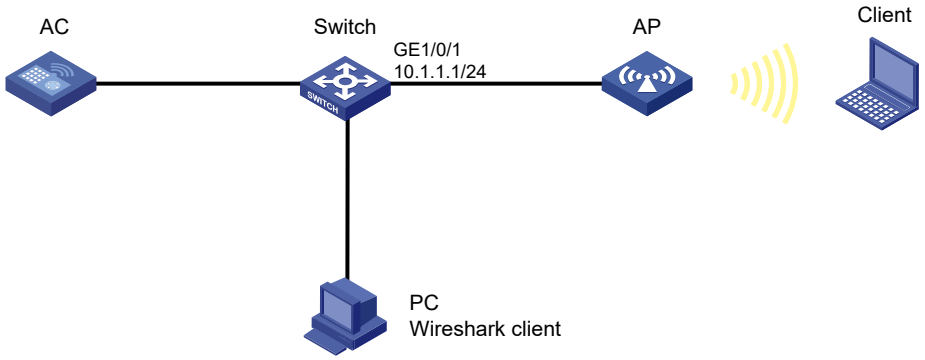


図 9-1 ネットワーク図

II. 設定手順

1)　スイッチの設定

装置管理ユーザを作成します。

```
<Switch> system-view
[Switch] local-user abc class manage
```

ローカルユーザのパスワードを平文で **123456** に設定します。

```
[Switch-luser-abc] password simple 123456
```

ユーザのユーザロールを **network-admin** として指定し、ユーザの作業ディレクトリを指定します。

```
[Switch-luser-abc] authorization-attribute user-role network-admin work-directory flash:/
```

ユーザのサービスタイプを **ftp** として指定します。

```
[Switch-luser-abc] service-type ftp
[Switch-luser-abc] quit
```

スイッチの FTP サーバを有効にします。

```
[Switch] ftp server enable
[Switch] quit
```

2)　AP の無線 1 では、192.168.20.173 からの TCP パケットの 1 KB をキャプチャします。ユーザ名を **abc**、パスワードを **123456** と指定します。取得したパケットを FTP サーバ 10.1.1.1 に **abc.pcap** ファイルで保存します。

```
<AC> packet-capture local ap ap1 radio 1 autostop filesize 1 capture-filter "src 192.168.20.173 and tcp" write url ftp://10.1.1.1/abc.pcap username abc password simple 123456
```

III. 設定の確認

display packet-capture status コマンドを実行してキャプチャ状態を表示します。

Wireshark クライアントを FTP サーバに接続し、キャプチャされたパケットを PC に表示します。（詳細は示しません。）

目次

このセクションのページは **17-x-x** です。

10 章 NetMeister 10-1
10.1 概要 10-1
10.1.1 NetMeister の利用 10-1
10.1.2 設定手段について 10-3
10.2 設定作業リスト 10-4
10.2.1 手動設定による NetMeister の利用 10-5
10.2.2 ゼロタッチプロビジョニング機能による NetMeister の利用 10-8
10.3 NetMeister による管理 10-16
10.3.1 タブ一覧 10-17
10.4 NetMeister の表示と維持 10-18
10.5 NetMeister の設定例 10-18
10.5.1 親機モードでの NetMeister 接続 10-18
10.5.2 子機モードでの NetMeister 接続 10-20
10.6 NetMeister 利用のトラブルシューティング 10-22
10.6.1 NetMeister に QX が登録できない 10-22
10.6.2 NetMeister でグラフが正しく表示されない。 10-23
10.6.3 NetMeister のリモートログインが使えない 10-23
10.6.4 ファームウェア更新が成功しない 10-23
10.6.5 NetMeisterPrime 機能が使用できない 10-24

10章 NetMeister

> 🕮 **メモ:**
> クラウドクラスタで利用する場合、MAC アドレスが Master 選定によって変化しないように **cloud-cluster service-cluster mac-address persistent always** コマンドを設定してください。また、クラウドクラスタ分裂によって同一 MAC の装置が複数登録されないように MAD 機能を利用して下さい。

10.1 概要

NetMeister(ネットマイスター)は、NEC プラットフォームズが提供するクラウド型統合管理サービスです。NetMeister 対応のネットワーク機器をクラウド上で一元的に管理することができます。この章では、本装置を NetMeister に登録するための設定について説明します。

NetMeister の操作/詳細に関しては、NetMeister が提供する操作ガイドをご確認ください。

https://www.necplatforms.co.jp/product/netmeister/

10.1.1 NetMeister の利用

NetMeister を利用する場合、あらかじめ NetMeister のサイトで「アカウント登録」と「グループ登録」が必要です。

QX-W シリーズは、NetMeister における親機モード、および、子機モードをサポートします。

親機モードでは、NetMeister と MQTT によって直接接続状態を確立し、NetMeister によって管理する事ができます。ただし、親機モードには、NetMeister Prime(有償サービス)の利用が必要です。NetMeister Prime については NetMeister が提供する操作ガイドをご確認ください。

子機モードでは、親機モードの装置と連携する事で NetMeister からの応答を受け、NetMeister によって管理する事ができます。図 10-1 に示すように、子機モードだけでは NetMeister を利用できません。

> 🕮 **メモ:**
> QX-W シリーズの親機モードは、子機モードと連携する動作を有しておりません。子機モードで NetMeister を利用する場合、QX-W シリーズ以外の親機モード対応を装置が必要です。親機モード対応装置については NetMeister が提供する操作ガイドをご確認ください。

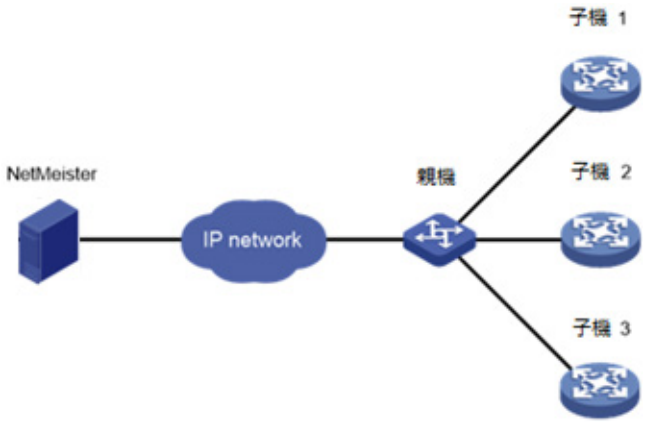


図 10-1 NetMeister との接続イメージ

子機モードを NetMeister によって管理する場合、親機モードの機器と同じのグループに属する必要があります。図 10-2 に示すように、子機モードは、親機モードの機器との通信と NetMeister と直接通信の両方を利用して NetMeister 上で管理され、NetMeister に関する通信は https(ssl)でおこなわれます(デフォルトポート番号: 443)。親機モードは、NetMeister に関する通信は mqtt(デフォルトポート番号:8883)と https(ssl)でおこなわれます。 (デフォルトポート番号:443)

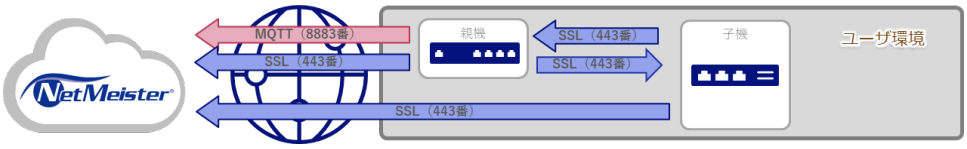


図 10-2 NetMeister への通信イメージ

図 10-3 に示すように、プロキシサーバを用いて外部ネットワークに接続をしている環境でも NetMeister を利用可能です。プロキシサーバのアドレスを設定することで、NetMeister 宛の通信をプロキシサーバ経由でおこなうことが可能です。

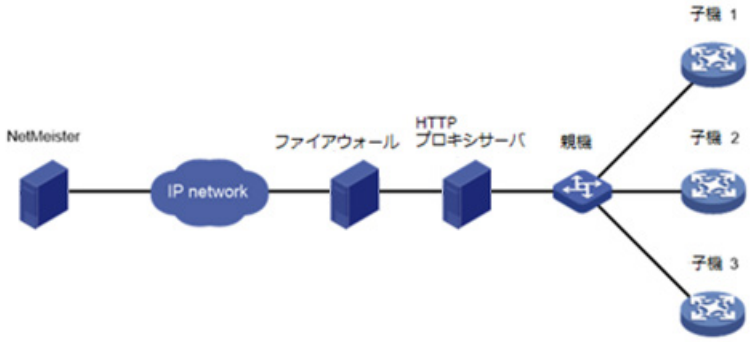


図 10-3 プロキシサーバを用いた NetMeister の利用環境

図 10-4 に示すように、子機で NetMeister への接続に proxy サーバを利用する場合、NetMeister 宛の通信のみ proxy サーバを経由します。親機と子機の間にプロキシサーバ及びファイアウォールがある様な特殊な環境の場合、親機と子機の間の通信を透過させるために、ファイアウォールで親機の LAN 側 IP 宛の通信を許可する必要があります。同様に、

ファイアウォールを跨ぐ位置にある NTP サーバ/DNS サーバ/SSH クライアント等との通信をする場合は、それらの許可も必要です。

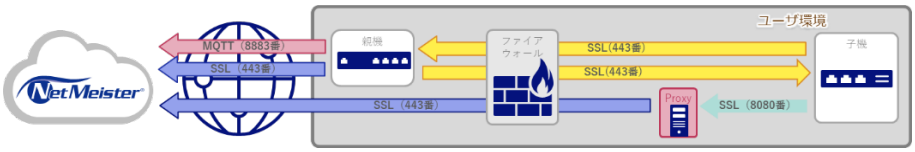


図 10-4 プロキシサーバを用いた NetMeister の通信イメージ

10.1.2 設定手段について

装置を NetMeister で管理をするためには、装置に手動でコンフィグを設定して環境に接続する手段と、ゼロタッチプロビジョニング機能(ZTP 機能)を利用して接続する手段があります。

ゼロタッチプロビジョニング機能は、スタートアップコンフィグレーションファイルを設定されていない状態で装置が起動する場合、NetMeister の親機から受けた DHCP パケットの情報を元に NetMeister から自動でコンフィグレーションファイルを取得し、適用することを可能にします。ゼロタッチプロビジョニング機能は装置に起動コンフィグが設定されていない状態で起動した際に自動で動作します。

図 10-5 に示すように、ゼロタッチプロビジョニング機能を利用する場合、管理者が事前に NetMeister 上に装置情報と利用するコンフィグレーションファイルを登録しておくことで、現場で装置設置をする作業者が、装置の操作をすることなく NetMeister に接続することが可能です。

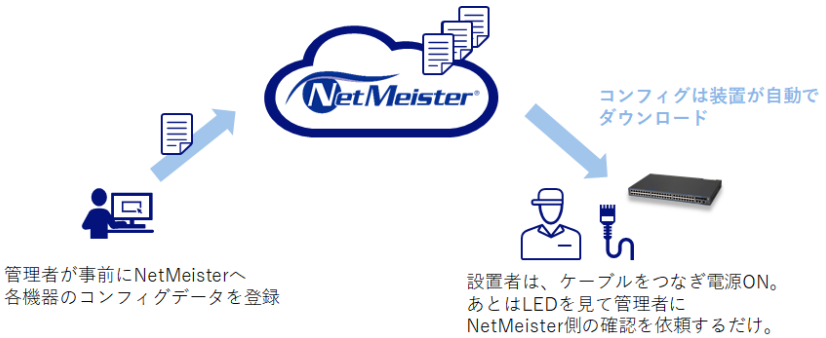


図 10-5 ゼロタッチプロビジョニングのイメージ

ゼロタッチプロビジョニング機能は、Auto Config 機能と交互に実行されます。Auto Config 機能については、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*2 基本機能*”の”*16 章 Auto Config*”を参照してください。

10.2 設定作業リスト

作業リスト
手動設定による NetMeister の利用
外部ネットワークへの接続準備 ● (必須設定項目) 自装置のIPアドレスの設定 ● (必須設定項目) 使用するDNSサーバの設定 ● (必須設定項目) ルーティングの設定
NetMeister機能に関係する追加設定 ● (推奨設定項目) 時刻、及び、タイムゾーン(+9:00)の設定 ● (オプション設定項目) Webコンソールユーザの設定 ● (オプション設定項目) SSHユーザの設定 ● (オプション設定項目) LLDPの設定
NetMeisterを利用するための設定 親機モードの場合 ● (オプション設定項目) NetMeister上に表示するホスト名の設定 ● (必須設定項目) 親機モードの設定 ● (必須設定項目) グループIDとグループパスワードの設定 ● (オプション設定項目) MQTTのポート番号の設定 ● (必須設定項目) 拠点IDの設定 ● (オプション設定項目) プロキシサーバのアドレスの設定 ● (オプション設定項目) イベントログの送信無効の設定 ● (オプション設定項目)注意レベルのNMアラームの送信有効の設定 ● (必須設定項目) NetMeister機能の有効化 ● 子機モードの場合 ● (オプション設定項目) NetMeister上に表示するホスト名の設定 ● (必須設定項目) グループIDとグループパスワードの設定 ● (必須設定項目) 親機のIPアドレスとポート番号の設定 ● (オプション設定項目) プロキシサーバのアドレスの設定 ● (オプション設定項目) イベントログの送信無効の設定 ● (オプション設定項目)注意レベルのNMアラームの送信有効の設定 ● (必須設定項目) NetMeister機能の有効化
ゼロタッチプロビジョニング機能による NetMeister の利用
事前準備作業 ● (必須設定項目)親機の設定 ● (必須設定項目)コンフィグレーションファイルの準備 ● (必須設定項目)装置情報の確認
NetMeisterへの情報登録 ● (必須設定項目)コンフィグレーションファイルの登録 ● (必須設定項目)装置情報の登録 ● (必須設定項目)プロビジョニングの設定
設置作業 ● (必須設定項目)プロビジョニングの有効化

10.2.1 手動設定による NetMeister の利用

I. 外部ネットワークへの接続準備

NetMeister と通信をするために、装置は親機を通して外部ネットワークに接続できる環境に接続されている必要があります。自装置の IP アドレス、使用する DNS サーバ、ルーティングの設定をしてください。DNS サーバは、親機から通知される NetMeister のアドレスを把握するために必要です。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． VLAN インタフェースを作成し、VLAN interface view に移行する	**interface vlan-interface** vlan-interface-id	ー
3． VLAN インタフェースに IP アドレスを割り当てる	・固定アドレスを割り当てる。 **ip address** *ip-address* { *mask* | *mask-length* } **[sub]** ・DHCPでアドレスを取得する **ip address dhcp-alloc**	デフォルト：設定なし
4． VLAN view から戻る	**Quit**	ー
5． DNS サーバの IP アドレスを指定する	**dns server** *ip-address*	デフォルト：設定なし DHCPサーバから情報を取得する場合は設定の必要はありません。
6． ルーティングの設定をする	**ip route-static** *dest-address* { *mask-length* | *mask* } { *interface-type interface-number* [*next-hop-address*] | *next-hop-address* } [**permanent** | **track** *track-entry-number*] [**preference** *preference*] [**tag** *tag-value*] [**description** text]	デフォルト：設定なし DHCPサーバから情報を取得する場合は設定の必要はありません。

II. NetMeister 機能に関係する追加設定

NetMeister で利用する機能によっては従来の装置機能を設定しておく必要があります。

それぞれの機能の設定手順についてはそれぞれの機能の章を参照してください。

各NetMeister機能についての説明はNetMeisterが提供する操作ガイドをご確認ください。

NetMeister 機能	必要設定	補足
CPU/メモリ/温度/ポートトラフィック情報表示	時刻 （手動/NTP）、及び、タイムゾーン（+9:00）	設定をしない場合、正しいグラフ情報になりません。 V9.6.08cを含む以降のソフトウェアではNetMeisterに接続した際に時刻とタイムゾーンが自動で設定されます。
HTTPSでリモートログインする	Webコンソール利用設定	
SSHでリモートログインする	SSH接続利用設定	
デバイスマップを見る（L2モード）	LLDP有効化	親機でも設定が必要です。

🕮 **メモ:**

本追加設定や装置名、管理 AP 名などの基本情報は NetMeister に接続したタイミングと、その後の周期情報更新で Netmeister に通知されます。NetMeister 接続後にこれらの設定を変更し、即時情報を更新したい場合は **netmeister update** コマンドを実行することで可能です。**netmeister update** コマンドは Version 9.4.09 を含む以降のソフトウェアからサポートしています。

III. NetMeister を利用するための設定

1)　親機モードの場合

NetMeister を利用するために、NetMeister のサイトで設定したグループ ID、グループパスワードを設定してください。MQTT のポート番号は 443 に変更が可能です。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. (オプション設定項目) NetMeister 上に表示するホスト名を設定する	**sysname** sysname	デフォルト：装置名
3. 親機モードを有効にする	**netmeister mode parent**	デフォルト：無効
4. グループ ID とグループパスワードを設定する	**netmeister account** *account* **password { cipher** *cipherPassword* **| simple** *plainPassword* **}**	デフォルト：設定なし
5. (オプション設定項目)MQTT のポート番号を設定する	**netmeister parent-mode mqtt port { 8883 | 443]**	デフォルト：8883
6. サイト名を設定する	**netmeister parent-mode sitename** *string*	デフォルト：設定なし
7. (オプション設定項目) プロキシサーバのアドレスを指定する。	**netmeister proxy url** *url* [**username** *username* **password** { **cipher** | **simple** } *string*]	デフォルト：設定なし MQTT通信もproxyサーバを利用します。
8. (オプション設定項目) イベントログの送信を無効にする。	**undo netmeister event log enable**	デフォルト：イベントログを送信します。
9. (オプション設定項目) イベントログ(syslog)の送信を無効にする。	**undo netmeister event syslog enable**	デフォルト：v9.6.08c 以降のソフトウェアから送信
10. (オプション設定項目) 注意レベルの NM アラームの送信を有効にする。	**netmeister alarm enable notice**	デフォルト：無効 Version 9.4.09を含む以降のソフトウェアから有効にできます。
11. NetMeister 機能の有効化	**netmeister enable**	デフォルト：無効

2)　子機モードの場合

NetMeister を利用するために、NetMeister のサイトで設定したグループ ID、グループパスワードと、親機の IP アドレス、ポート番号の設定をしてください。プロキシサーバの

アドレスを設定すると、NetMeister への https 通信のために任意のプロキシサーバを利用します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． (オプション設定項目) NetMeister 上に表示するホスト名を設定する	**sysname** sysname	デフォルト：装置名
3． グループ ID とグループパスワードを設定する	**netmeister account** *account* **password { cipher** *cipherPassword* **| simple** *plainPassword* **}**	デフォルト：設定なし
4． 親機の IP アドレスとポート番号を指定する	**netmeister parent ip** *ip-address* **[port** *port-number* **]**	デフォルト：設定なし 最大2つまで設定が可能です。 ポート番号を指定しない場合、デフォルトで443が使用されます。
5． (オプション設定項目) プロキシサーバのアドレスを指定する。	**netmeister proxy url** *url* [**username** *username* **password** { **cipher** | **simple** } *string*]	デフォルト：設定なし
6． (オプション設定項目) イベントログの送信を無効にする。	**undo netmeister event log enable**	デフォルト：イベントログを送信します。
7． (オプション設定項目) イベントログ(syslog)の送信を無効にする。	**undo netmeister event syslog enable**	デフォルト：v9.6.08c 以降のソフトウェアから送信
8． (オプション設定項目) 注意レベルの NM アラームの送信を有効にする。	**netmeister alarm enable notice**	デフォルト：無効 Version 9.4.09を含む以降のソフトウェアから有効にできます。
9． NetMeister 機能の有効化	**netmeister enable**	デフォルト：無効

IV. NetMeister の表示と維持

すべての view で display コマンドを実行できます。

操作	コマンド
NetMeisterおよび親機との接続状態を表示する	**display netmeister**

10.2.2 ゼロタッチプロビジョニング機能による NetMeister の利用

I. 事前準備作業

🕮 **メモ:**

ゼロタッチプロビジョニング機能の利用可能条件:

親機モードで接続する場合

- DHCP サーバが必要です。
- proxy 経由のゼロタッチプロビジョニングをおこなう場合、同じネットワーク内に proxy 経由で NetMeister に接続している他の親機モードの装置と、Option43 を付与できる DHCP サーバが必要です。
- 装置で利用する正しいコンフィグレーションファイルの事前準備が 1 装置につき 1 つ必要です。
- 利用する装置の MAC アドレス、シリアルナンバー、装置名の情報が必要です。
- コンフィグダウンロード時は、NetMeister 側でダウンロードの有効時間の指定が必要です。

子機モードで接続する場合

- NetMeister に接続している他の親機モードの装置が必要です。
- Option43 を付与できる DHCP サーバが必要です。
- proxy 経由のゼロタッチプロビジョニングをおこなう場合、NetMeister に接続している他の親機モードの装置が proxy 経由で NetMeister に接続している必要があります。
- 装置で利用する正しいコンフィグレーションファイルの事前準備が 1 装置につき 1 つ必要です。
- 利用する装置の MAC アドレス、シリアルナンバー、装置名の情報が必要です。
- コンフィグダウンロード時は、NetMeister 側でダウンロードの有効時間の指定が必要です。

その他の補足

- QX-W シリーズの AP は、動作モードをあらかじめ利用するモードに変更しておく必要があります。

1) DHCP サーバの設定

ゼロタッチプロビジョニング機能を利用する場合、NetMeister にアクセスするための IP アドレス、ゲートウェイアドレス、DNS サーバ情報は DHCP サーバから取得する必要があります。また、子機モードで利用する場合、または proxy 経由でゼロタッチプロビジョニングを行う場合、親機から情報を得るために Option43 によって親機アドレスを通知する必要があります。

Option43 のフォーマット
NEC,zerotouch,<親機IPv4アドレス>,<親機待ち受けポート> 例）**NEC,zerotouch,192.0.2.1,443**

NetMeister 機能のゼロタッチプロビジョニング子機対応機能(QX 未サポート)をサポートする親機を DHCP サーバとする場合、ゼロタッチプロビジョニング用の DHCP リクエストにだけ Option43 の情報を通知することが可能です。NetMeister 機能のゼロタッチプロビジョニング子機対応に関しては NetMeister 操作ガイドを参照してください。

2) コンフィグレーションファイルの準備

ゼロタッチプロビジョニング機能で設定を行う対象装置のために、コンフィグファイルをテキストで作成し、zip 圧縮してください。間違ったコンフィグファイルを使用しないよう、あらかじめ実機で確認をしたコンフィグを使用することを推奨します。

下記にコンフィグレーションファイルのサンプルを示します。

親機モードのコンフィグレーションのサンプル

```
#
 clock timezone JST add 09:00:00
#
 ssh server enable
#
 ip https enable
#
 lldp global enable
#
interface Vlan-interface1
 ip address dhcp-alloc
#
 ntp-service enable
 ntp-service unicast-server ntp.nict.jp
#
line vty 0
 authentication-mode scheme
#
local-user nec class manage
 password simple qx12345678
 service-type ssh https
 authorization-attribute user-role network-admin
#
 netmeister mode parent
 netmeister account test password simple abcdefg
 netmeister parent-mode mqtt port 443
 netmeister parent-mode sitename kyoten1
 netmeister enable
#
```

子機モードのコンフィグレーションのサンプル

```
#
 clock timezone JST add 09:00:00
#
 ssh server enable
#
 ip https enable
#
 lldp global enable
#
interface Vlan-interface1
 ip address dhcp-alloc
#
 ntp-service enable
 ntp-service unicast-server ntp.nict.jp
#
line vty 0
 authentication-mode scheme
#
local-user nec class manage
 password simple qx12345678
 service-type ssh https
 authorization-attribute user-role network-admin
#
 netmeister account test password simple abcdefg
 netmeister parent ip 1.1.1.1 port 443
 netmeister enable
#
```

3) 装置情報の確認

ゼロタッチプロビジョニング機能を利用する装置の MAC アドレス、シリアルナンバー、装置名の情報を確認してください。 MAC アドレス、シリアルナンバー、装置名は、梱包箱または装置の本体ラベルに記載されています。

II. NetMeister への情報登録

NetMeister にログインしてください。(NetMeister を利用するためのアカウントおよびグループの作成についての説明は省略します。NetMeister 操作ガイドを確認してください。)

1) NetMeister でのゼロタッチプロビジョニングは、NetMeister 画面左側メニューの「設定」からおこないます。

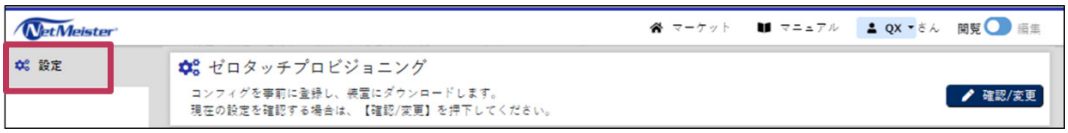


図 10-6 設定メニューの表示

2)　ゼロタッチプロビジョニングの設定のために編集モードにします。



図 10-7 編集モードへの変更

3)　コンフィグレーションファイルを NetMeister 上に登録します。



図 10-8 コンフィグ登録画面

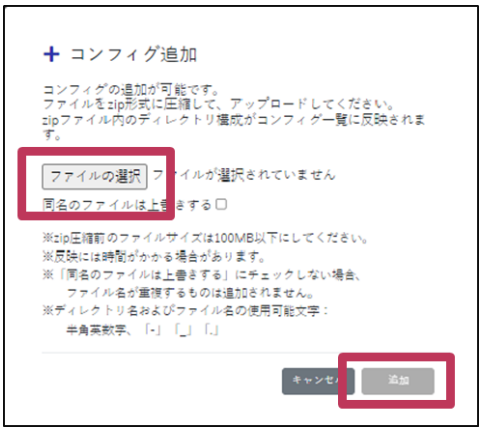


図 10-9 コンフィグの選択

🕮 **メモ:**

NetMeister へのコンフィグレーションファイルの登録は zip 形式でおこないます。複数のコンフィグレーションファイルをフォルダに格納して zip 圧縮しておくことで一度に登録も可能です。

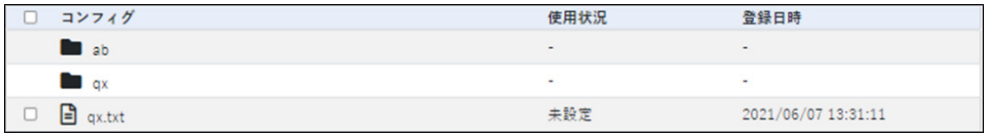


図 10-10 コンフィグ登録後の表示

4)　ゼロタッチプロビジョニングを利用する装置情報を登録します。

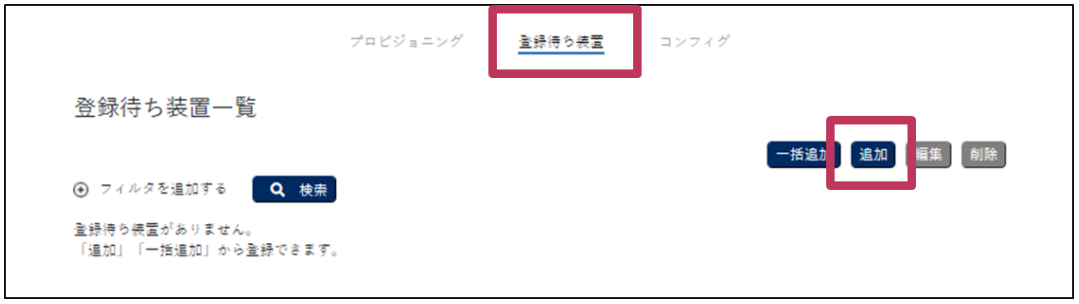


図 10-11 登録待ち装置設定画面



図 10-12 装置情報の登録例

🕮 **メモ:**

装置情報の登録では、シリアル番号の入力は大文字小文字を区別します。
MAC アドレスの入力は大文字小文字を区別しません。
「：」「-」などは含めないでください。
シリーズ名、機種名の選択を間違えないよう注意してください。



図 10-13 登録後の表示

5)　登録したコンフィグレーションファイルと装置情報を紐づけます。



図 10-14 プロビジョニングの設定画面

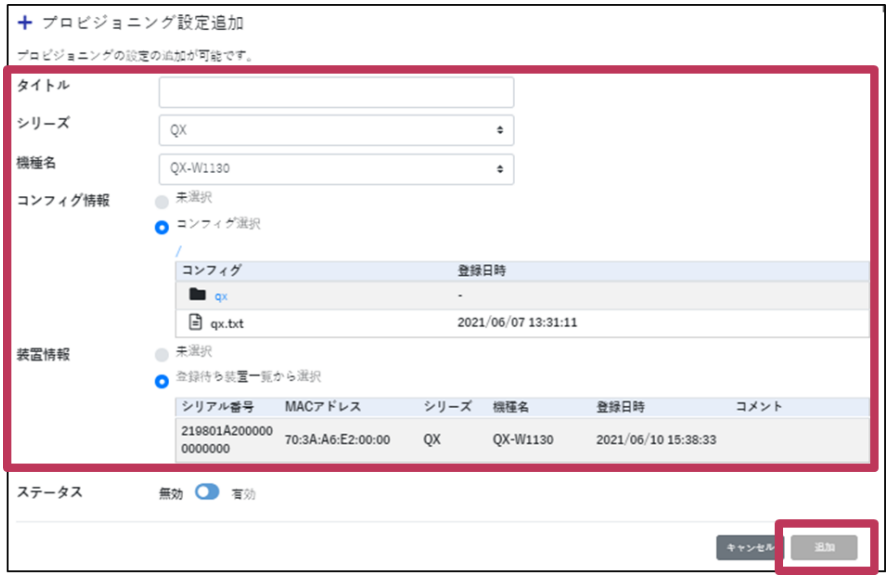


図 10-15 装置とコンフィグの選択

🕮 **メモ:**

タイトルは任意の文字列を入力してください。
シリーズ名と装置名を選択すると、他は選択可能なものだけが表示されますので任意の組み合わせを選択してください。
設置作業者がすぐに作業をしない場合はステータスを[無効]で登録しておきます。

III. 設置作業

1) 設置作業者が作業する時間を考慮し、コンフィグのダウンロード可能時間を設定します。一覧から対象の行を選択すると、現在の設定情報が下に表示されます。



図 10-16 プロビジョニング設定一覧

2)　選択した設定のステータスを[編集]から有効にし、コンフィグダウンロード可能時間を設定します。



図 10-17 ステータスの変更と DL 有効時間の設定

メモ:

有効時にダウンロード後の無効パターンを指定できますが、QX のゼロタッチプロビジョニングは、ダウンロード完了時はコンフィグを次回起動のコンフィグとして保存、再起動しますので、どちらを選んでも 1 度のみの取得動作です。(次回以降の起動時は保存済のコンフィグを使用して起動します。)

3)　設置場所で設置作業者が指定の装置を開梱します。
4)　準備後、管理者に装置設置開始の連絡をします。
5)　管理者は NetMeister 上で対象のゼロタッチプロビジョニングの有効化をします。
6)　設置作業者は指定の環境に装置を接続します。
7)　接続した装置は NetMeister から自動的にコンフィグを取得します。

QX のゼロタッチプロビジョニングでは、取得したコンフィグデータを自動で次回起動のコンフィグとしてセットし、再起動します。

DHCP サーバの設定ミスやインターネット環境に出られない環境など、何らかの理由で失敗している場合はリトライを繰り返し、再起動はしません。環境を見直してください。ゼロタッチプロビジョニングのプロセスを止めるためには、CLI で<Ctrl+C>または<Ctrl+D>を押下してください。

8)　再起動を LED 変化で確認し、管理者に連絡します。

起動時の LED 変化は下記の通りです。

表 10-1 QX-W2300AC シリーズ

状態	SYS LED
Boot 起動中	消灯→オレンジ点灯→緑点灯
System 起動中	緑点滅(0.5s)→点灯
ゼロタッチプロビジョニング中	緑点滅(1s)
ゼロタッチプロビジョニング成功時	(自動再起動)消灯→オレンジ点灯→緑点灯
コンフィグ読み込み中	緑点滅(1s)
起動完了	緑点灯

9)　NetMeister 上で状態を確認します。



図 10-18 動作状態の確認

結果がダウンロード成功の場合、コンフィグ取得を終えています。装置詳細画面に装置が表示されたことをチェックしてください。装置情報の誤入力や、環境の問題で NetMeister にアクセスができていない場合はカウントがされません。



図 10-19 装置一覧の確認

装置が再起動し、起動したにもかかわらず装置一覧に表示されない場合、準備されたコンフィグに NetMeister に接続するための設定の不備がある可能性があります。

装置一覧に装置が表示されれば NetMeister で管理ができています。

IV. 参考

NetMeister であらかじめアカウント管理から通知設定でゼロタッチ通知にチェックをいれておくと、ゼロタッチプロビジョニングによるコンフィグ取得成功時にメールが通知されます。



図 10-20 アカウント管理



図 10-21 通知の設定

10.3 NetMeisterによる管理

Netmeister の操作、及び、対応機能に関しては NetMeister が提供する操作ガイドをご確認ください。

https://www.necplatforms.co.jp/product/netmeister/

10.3.1 タブ一覧

NetMeister 上の装置詳細の画面に表示されるタブは、機器ごとに表示される内容が異なり、NetMeister prime の利用によって表示、利用可能になる機能もあります。また、表示のレイアウトは NetMeister 側の更新によって変わる可能性があります。詳細は NetMeister が提供する操作ガイドをご確認ください。

なお、表示のレイアウトは NetMeister 側の更新によって変わる可能性があります。

本装置は以下のタブに対応しています。

タブ名	説明
装置概要	装置の詳細画面を表示します。 詳細はNetMeisterが提供する操作ガイドをご確認ください。
アラーム	Anchor-AC および FAT は温度異常/FAN 異常/CPU 異常/メモリ異常/異常再起動時にアラームを送信します。温度センサや FAN を持たない装置はそれらのアラームを送信することはありません。温度/FAN/CPU/メモリのしきい値はシステム管理の各種しきい値設定値に依存します。
デバイスリスト	MAC テーブルと ARP テーブルを合わせた情報を表示します。 オプション装置は対象外です。
コンフィグ	NetMeister 上にコンフィグを保存、装置の次回起動コンフィグとの比較、反映が可能です。オプション装置は対象外です。
ログ	NetMeister から定期的に装置情報を取得し、NetMeister に保存できます。装置ごとに、時間帯を指定できます。オプション装置は対象外です。
Ping 監視	V9.4.09 を含む以降のソフトウェアで表示されます。 NetMeister から装置に対して Ping 監視の設定ができます。 オプション装置は対象外です。
管理 AP	display wlan ap all reboot-record コマンド相当の情報を表示します。 取得ボタン操作後に、管理下 AP から収集した情報を表示します。再起動履歴の情報に更新がある場合、取得ボタン操作時に Ancho-AC は情報の更新処理をおこなうため、再起動履歴部分の情報は表示されません。3 分程度待った後、再度取得ボタンを押すことで再起動履歴情報も表示されます。 オプション装置は対象外です。
接続フェーズ	無線端末の接続フェーズ毎の失敗状況と、最終的な接続割合を確認することができます。オプション装置の情報は Anchor-AC の情報に含まれます。
無線 LAN	アクセスポイント一覧はサービステンプレートを適用して有効になっている一覧のみ表示します。無線端末一覧は接続された端末の一覧を表示します。周辺 AP 一覧は wips 設定が有効な場合にのみ、取得している情報が表示されます。オプション装置は対象外です。(Anchor-AC の無線 LAN 情報に含みます。)

タブ名	説明
VLAN	display vlan コマンド、及び、display interface Vlan-interface brief 相当の情報を表示します。 オプション装置は対象外です。
ポート状態	物理インタフェースの情報を表示します。 オプション装置は対象外です。
ファイル管理	V9.6.08c を含む以降のソフトウェアで表示されます。 装置のディレクトリの確認、削除が可能です。一部のファイルについては取得、転送も可能です。 オプション装置は対象外です。

10.4 NetMeisterの表示と維持

操作	コマンド
NetMeister との接続状態を表示する	**display netmeister**

🕮 **メモ:**

display netmeister コマンドで表示する情報は装置から親機、及び、NetMeister への接続に関する状態です。装置からの通信に問題が無く、NetMeister、親機から装置への要求メッセージが届いていない場合などは、NetMeister 上の状態表示と装置側の状態情報は一致しない場合があります。

10.5 NetMeisterの設定例

10.5.1 親機モードでの NetMeister 接続

I. ネットワーク要件

図 10-22 に示すように、Device A に親機モードの設定をします。

- あらかじめ NetMeister のサイトで「アカウント登録」をし、「グループ登録」としてグループ ID(aaa)とグループパスワード(bbb)が設定されていることとします。
- DNS サーバとして 10.0.0.254 が動作していることとします。

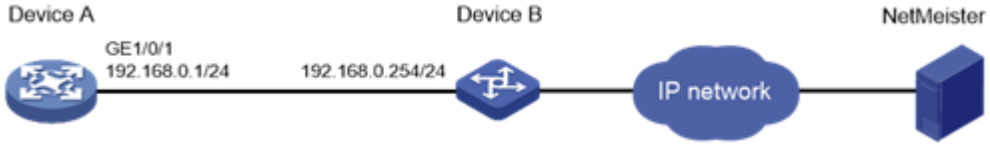


図 10-22 ネットワーク図

II. 設定手順

1. 外部ネットワークへの接続準備をします。

#VLAN インタフェースを作成し、IP アドレスをインタフェースに割り当てます。

```
<DeviceA> system-view
[DeviceA] vlan 1
[DeviceA-vlan1] port gigabitethernet 1/0/1
[DeviceA-vlan1] quit
[DeviceA] interface vlan-interface 1
[DeviceA -Vlan-interface1] ip address 192.168.0.1 24
[DeviceA -Vlan-interface1] quit
```

DNS サーバを指定します。

```
[DeviceA] dns server 10.0.0.254
```

ルーティング設定をします。

```
[DeviceA] ip route-static 0.0.0.0 0 192.168.0.254
```

2. その他の追加機能の設定をします。

時刻とタイムゾーン(+9:00)の設定をします。

```
[DeviceA] clock timezone JST add 09:00:00
[DeviceA] ntp-service enable
[DeviceA] ntp-service unicast-server 192.168.0.254
```

ssh と web コンソールアクセス用の設定をします。

```
[DeviceA]ssh server enable
[DeviceA]ip https enable
[DeviceA]line vty 0
[DeviceA-line-vty0]authentication-mode scheme
[DeviceA-line-vty0]local-user nec class manage
[DeviceA-luser-manage-nec]password simple qx12345678
[DeviceA-luser-manage-nec]service-type ssh https
[DeviceA-luser-manage-nec]authorization-attribute user-role network-admin
[DeviceA-luser-manage-nec]quit
```

lldp の有効化をします。

```
[DeviceA] lldp global enable
```

3. NetMeister を利用するための設定をします。

親機モードを利用するための設定をします。

```
[DeviceA] netmeister mode parent
```

グループ ID(aaa)とグループパスワード(bbb)を設定します。

```
[DeviceA] netmeister account aaa password simple bbb
```

親機モードで NetMeister に接続する際の MQTT のポート番号を 443 に変更します。

```
[DeviceA] netmeister parent-mode mqtt port 443
```

親機モードで利用するための拠点 id(kyoten1)を指定します。

```
[DeviceA] netmeister parent-mode sitename kyoten1
```

NetMeister 機能の有効化をします。

```
[DeviceA] netmeister enable
```

III. 設定の確認

1. 外部ネットワークと疎通ができることを確認するために、いずれかの外部ネットワークと ping の疎通ができることを確認します。

```
<SwitchA>ping 1.1.1.1
Ping 1.1.1.1 (1.1.1.1): 56 data bytes, press CTRL+C to break
56 bytes from 1.1.1.1: icmp_seq=0 ttl=52 time=68.584 ms
56 bytes from 1.1.1.1: icmp_seq=1 ttl=52 time=49.657 ms
56 bytes from 1.1.1.1: icmp_seq=2 ttl=52 time=48.447 ms
56 bytes from 1.1.1.1: icmp_seq=3 ttl=52 time=58.423 ms
56 bytes from 1.1.1.1: icmp_seq=4 ttl=52 time=59.423 ms

--- Ping statistics for 1.1.1.1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 48.447/56.907/68.584/7.336 ms
```

2. NetMeister および親機との接続状態を確認します。

```
<DeviceA> display netmeister
NetMeister state          :  Enabled
Mode                      :  Parent
Connection state with NetMeister:  Connected
Account name              :  aaa
Event log                 :  Enabled
Proxy information:
State                     :  --
Parent information:
Site name                 :  kyoten1
Interval                  :  3600 sec
MQTT interval             :  60 sec
MQTT status               :  Connected
```

🕮 **メモ:**

- NetMeister prime を利用していない場合、親機モードの QX は接続を完了できません。NetMeister の操作ガイドを参照し、ライセンス適用を行ってください。

10.5.2 子機モードでの NetMeister 接続

I. ネットワーク要件

図 10-23 に示すように、Device B を親機とし、子機である Device A の設定をします。

- あらかじめ NetMeister のサイトで「アカウント登録」をし、「グループ登録」としてグループ ID(aaa)とグループパスワード(bbb)が設定されていることとします。
- あらかじめ親機は外部ネットワークに接続するための設定を行い、グループ ID(aaa)に属していることとします。
- DNS サーバとして 10.0.0.254 が動作していることとします。

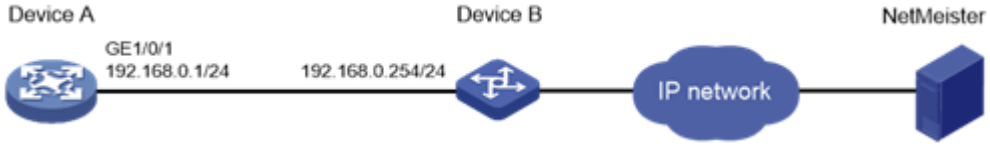


図 10-23 ネットワーク図

II. 設定手順

1. 外部ネットワークへの接続準備をします。

#VLAN インタフェースを作成し、IP アドレスをインタフェースに割り当てます。

```
<DeviceA> system-view
[DeviceA] vlan 1
[DeviceA-vlan1] port gigabitethernet 1/0/1
[DeviceA-vlan1] quit
[DeviceA] interface vlan-interface 1
[DeviceA -Vlan-interface1] ip address 192.168.0.1 24
[DeviceA -Vlan-interface1] quit
```

DNS サーバを指定します。

```
[DeviceA] dns server 10.0.0.254
```

ルーティング設定をします。

```
[DeviceA] ip route-static 0.0.0.0 0 192.168.0.254
```

2. その他の追加機能の設定をします。

時刻とタイムゾーン(+9:00)の設定をします。

```
[DeviceA] clock timezone JST add 09:00:00
[DeviceA] ntp-service enable
[DeviceA] ntp-service unicast-server 192.168.0.254
```

ssh と web コンソールアクセス用の設定をします。

```
[DeviceA]ssh server enable
[DeviceA]ip https enable
[DeviceA]line vty 0
[DeviceA-line-vty0]authentication-mode scheme
[DeviceA-line-vty0]local-user nec class manage
[DeviceA-luser-manage-nec]password simple qx12345678
[DeviceA-luser-manage-nec]service-type ssh https
[DeviceA-luser-manage-nec]authorization-attribute user-role network-admin
[DeviceA-luser-manage-nec]quit
```

lldp の有効化をします。

```
[DeviceA] lldp global enable
```

3. NetMeister を利用するための設定をします。

グループ ID(aaa)とグループパスワード(bbb)を設定します。

```
[DeviceA] netmeister account aaa password simple bbb
```

親機の IP アドレスとポート番号(デフォルト:443)を指定します。

```
[DeviceA] netmeister parent ip 192.168.0.254 port 443
```

NetMeister 機能の有効化をします。

```
[DeviceA] netmeister enable
```

III. 設定の確認

1. 外部ネットワークと疎通ができることを確認するために、いずれかの外部ネットワークと ping の疎通ができることを確認します。

```
<SwitchA>ping 1.1.1.1
Ping 1.1.1.1 (1.1.1.1): 56 data bytes, press CTRL+C to break
56 bytes from 1.1.1.1: icmp_seq=0 ttl=52 time=68.584 ms
56 bytes from 1.1.1.1: icmp_seq=1 ttl=52 time=49.657 ms
56 bytes from 1.1.1.1: icmp_seq=2 ttl=52 time=48.447 ms
56 bytes from 1.1.1.1: icmp_seq=3 ttl=52 time=58.423 ms
56 bytes from 1.1.1.1: icmp_seq=4 ttl=52 time=59.423 ms

--- Ping statistics for 1.1.1.1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 48.447/56.907/68.584/7.336 ms
```

2. NetMeister および親機との接続状態を確認します。

```
<DeviceA> display netmeister
NetMeister state                          :  Enabled
Connection state with NetMeister          :  Connected
Account name                              :  aaa
Parent 1:
 IP address                               :  192.168.0.254
 Port number                              :  443
 Connection state                         :  Connected
```

10.6 NetMeister利用のトラブルシューティング

NetMeister 操作ガイドにも装置毎の機能対応一覧、及び、NetMeister 機能に関する注意事項、FAQ が記載されていますので参照して下さい。

10.6.1 NetMeister に QX が登録できない

I. 症状

QX で NetMeister を利用したいが NetMeister に装置が登録できない。

II. 解決策

子機モードで利用する場合

1) 同一グループに既に親機モードで登録されていないか確認し、登録されている場合は装置削除します。
2) 親機となる装置が NetMeister に接続できているか確認します。
3) 子機で **display netmeister** コマンドによって接続ステータスを確認します。
4) 親機との接続ができていない場合、子機で設定したグループ ID およびパスワードが親機で設定しているものと同じであるか確認します。
5) NetMeister との接続ができていない場合、子機から外部ネットワークに DNS を使用した通信ができることを確認します。
6) 問題が解決しない場合、NetMeister のサイトから問い合わせをしてください。

親機モードで利用する場合

1) NetMeister 上で同一グループに該当装置が既に子機モードで登録されていないか確認し、登録されている場合は装置削除します。
2) NetMeister 上のライセンスの数が十分か確認します。

3) **display netmeister** コマンドによって接続ステータスを確認します。
4) 外部ネットワークに DNS を使用した通信ができることを確認します。
5) 問題が解決しない場合、NetMeister のサイトから問い合わせをしてください。

10.6.2 NetMeister でグラフが正しく表示されない。

I. 症状

QX の装置詳細画面でグラフ情報が正しく表示されない。

II. 解決策

1) 装置にタイムゾーン(+9:00)が設定されていることを確認します。
2) 装置の時刻が正しいことを確認します。
3) NetMeister に装置登録した後に時刻設定を変更した場合は、周期的な装置情報更新のために、1 時間待つか NetMeister 機能を一度無効にし、再度有効にします。
4) 問題が解決しない場合、NetMeister のサイトから問い合わせてください。

🕮 **メモ:**

V9.6.08c を含む以降のソフトウェアでは、装置は NetMeister に接続したタイミングでタイムゾーン(+9:00)と時刻設定を自動でおこないます。

10.6.3 NetMeister のリモートログインが使えない

I. 症状

QX にリモートログインができない。

II. 解決策

1) 装置に ssh または web コンソール接続の設定がされてあることを確認します。
2) リモートログインでのアクセスに利用する PC がプライベートアドレスではないことを確認します。
3) 操作 PC と対象の装置間でファイアウォールやフィルタなど、通信制限がない事を確認します。
4) 環境がプロキシやファイアウォールを利用していないことを確認します。
5) 問題が解決しない場合、NetMeister のサイトから問い合わせてください。

10.6.4 ファームウェア更新が成功しない

I. 症状

NetMeister で管理している装置のファームウェア更新(バージョンアップ)が成功しない。

🕮 **メモ:**

AC の管理下 AP は NetMeister に管理されていませんので NetMeister とは関係なく、AC がバージョンアップされた後に AC と AC 管理下 AP 間の仕組みによって自動バージョンアップ処理が行われます。

II. 解決策

1) タスク一覧からタスクの状態を確認します。
2) タスク結果が失敗と表示され、詳細理由にディレクトリサイズが足りない、または、セットに失敗したと表示されている場合、装置のディレクトリサイズが不足していますので不要なファイルを削除します。

🕮 **メモ:**

ファームウェア更新をするためには、NetMeister から取得する ipe 形式のソフトウェアと、それを bin ファイルに解凍する分のディレクトリの空き容量が必要です。
NetMeister 機能[コマンド実行]によって、NetMeister からディレクトリ確認コマンド(**dir**)及び削除コマンド(**delete /unreserved**)等の実行が可能です。

3) 問題が解決しない場合、NetMeister のサイトから問い合わせてください。

10.6.5 NetMeisterPrime 機能が使用できない

I. 症状

NetMeister に prime ライセンスを適用(またはトライアル)したが機能が使用できない。

II. 解決策

1) NetMeister メニューからライセンスの適用状態を確認し、適用されていない場合は適用操作をします。(NetMeister が提供する NetMeister 操作ガイド参照)
2) 子機モードの場合、手動で有償化操作をする必要があります。
3) prime 機能にはライセンス適用時に即座に利用できるものと、周期的な装置情報更新のタイミングで識別され使用可能になる機能がありますので、1 時間待つか NetMeister 機能を一度無効にし、再度有効にします。
4) 問題が解決しない場合、NetMeister のサイトから問い合わせてください。

QX-W2300AC シリーズ アクセスコントローラ

オペレーションマニュアル

18. 謝辞

本マニュアルは以下に示す章で構成されています。

01- 謝辞

目次

このセクションのページは **18-x-x** です。

1 章 謝辞（Acknowledgments） **1-1**

1章 謝辞（Acknowledgments）

This document provides copyright information regarding the third-party software that are included, either in whole or in part, in this product.

Acknowledgements:
This product includes software developed by the University of California, Berkeley and its contributors.
This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/).
This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).
This product includes software developed by the University of California, Lawrence Berkeley Laboratory and its contributors.

This product contains third parties component softwares and they will be used and distributed under the specific license. If you want to obtain source code of Open Source Software included in this product, please send a request to our support team: https://www.nec.com/, we will provide the source code included in this product in exchange for a fee no higher than the physical cost of providing the source code.

[aws-iot-device-sdk-embedded-C 3.1.1]
[COPYRIGHT]
##
##
[LICENSE]
Apache License
Version 2.0, January 2004

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.
"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.
"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.
"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.
"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.
"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.
"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.
"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).
"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."
"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.
2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.
3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.
4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:
1. You must give any other recipients of the Work or Derivative Works a copy of this License; and
2. You must cause any modified files to carry prominent notices stating that You changed the files; and
3. You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and
4. If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.
You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.
5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.
6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required

for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.
7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.
8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.
9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

##
##

Components are made available under the terms of the Eclipse Public License v1.0
and Eclipse Distribution License v1.0 which accompany this distribution.

The Eclipse Public License is available at
  http://www.eclipse.org/legal/epl-v10.html
and the Eclipse Distribution License is available at
  http://www.eclipse.org/org/documents/edl-v10.php.

##
##

Copyright (C) 2012, iSEC Partners.

Permission is hereby granted, free of charge, to any person obtaining a copy of
this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE

SOFTWARE.

##
##

Project

```
                                  _   _ ____  _
                              ___| | | |  _ \| |
                             / __| | | | |_) | |
                            | (__| |_| |  _ <| |___
                             \___|\___/|_| \_\_____|
```

Copyright (C) 1998 - 2011, Daniel Stenberg, <daniel@haxx.se>, et al.

This software is licensed as described in the file COPYING, which
you should have received as part of this distribution. The terms
are also available at http://curl.haxx.se/docs/copyright.html.

You may opt to use, copy, modify, merge, publish, distribute and/or sell
copies of the Software, and permit persons to whom the Software is
furnished to do so, under the terms of the COPYING file.

This software is distributed on an "AS IS" basis, WITHOUT WARRANTY OF ANY
KIND, either express or implied.

##
##

Copyright (c) 2010 Serge A. Zaitsev

Permission is hereby granted, free of charge, to any person obtaining a copy
of this software and associated documentation files (the "Software"), to deal
in the Software without restriction, including without limitation the rights
to use, copy, modify, merge, publish, distribute, sublicense, and/or sell
copies of the Software, and to permit persons to whom the Software is
furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in
all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE
AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER
LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,
OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN
THE SOFTWARE.

##
##
[NOTICE]
AWS C SDK for Internet of Things Service
Copyright 2010-2015 Amazon.com, Inc. or its affiliates. All Rights Reserved.

This product includes software developed by
Amazon Inc (http://www.amazon.com/).

****
THIRD PARTY COMPONENTS
****
This software includes third party software subject to the following licensing:
- Embedded C MQTT Client - From the Eclipse Paho Project - EPL v1.0
- mbedTLS (external library, included in tarball or downloaded separately) - Apache 2.0
- jsmn (JSON Parsing) - MIT
- cURL (hostname verification) - MIT

The licenses for these third party components are included in LICENSE.txt

---
[boolean.h 1.19]
[COPYRIGHT]
Copyright (C) 2004-2007 Internet Systems Consortium, Inc. ("ISC")
Copyright (C) 1998-2001 Internet Software Consortium.

[LICENSE]
Permission to use, copy, modify, and/or distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ISC DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

[bootstrap 2.3.2]
[COPYRIGHT]
Copyright 2012 Twitter, Inc.

[LICENSE]

Apache License
Version 2.0, January 2004
http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the

editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

   (a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

   (b) You must cause any modified files to carry prominent notices stating that You changed the files; and

   (c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

   (d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed

as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

[bootstrap-datetimepicker 1.2.0]

Apache License

Version 2.0, January 2004
http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

   (a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

   (b) You must cause any modified files to carry prominent notices stating that You changed the files; and

   (c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

   (d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

   You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or
   agreed to in writing, Licensor provides the Work (and each
   Contributor provides its Contributions) on an "AS IS" BASIS,
   WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or
   implied, including, without limitation, any warranties or conditions
   of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A
   PARTICULAR PURPOSE. You are solely responsible for determining the
   appropriateness of using or redistributing the Work and assume any
   risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory,
   whether in tort (including negligence), contract, or otherwise,
   unless required by applicable law (such as deliberate and grossly
   negligent acts) or agreed to in writing, shall any Contributor be
   liable to You for damages, including any direct, indirect, special,
   incidental, or consequential damages of any character arising as a
   result of this License or out of the use or inability to use the
   Work (including but not limited to damages for loss of goodwill,
   work stoppage, computer failure or malfunction, or any and all
   other commercial damages or losses), even if such Contributor
   has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing
   the Work or Derivative Works thereof, You may choose to offer,
   and charge a fee for, acceptance of support, warranty, indemnity,
   or other liability obligations and/or rights consistent with this
   License. However, in accepting such obligations, You may act only
   on Your own behalf and on Your sole responsibility, not on behalf
   of any other Contributor, and only if You agree to indemnify,
   defend, and hold each Contributor harmless for any liability
   incurred by, or claims asserted against, such Contributor by reason
   of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

APPENDIX: How to apply the Apache License to your work.

   To apply the Apache License to your work, attach the following
   boilerplate notice, with the fields enclosed by brackets "[]"
   replaced with your own identifying information. (Don't include
   the brackets!) The text should be enclosed in the appropriate
   comment syntax for the file format. We also recommend that a
   file or class name and description of purpose be included on the
   same "printed page" as the copyright notice for easier
   identification within third-party archives.

Copyright [yyyy] [name of copyright owner]

Licensed under the Apache License, Version 2.0 (the "License");
you may not use this file except in compliance with the License.
You may obtain a copy of the License at

    http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software
distributed under the License is distributed on an "AS IS" BASIS,
WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
See the License for the specific language governing permissions and
limitations under the License.

[bootstrap-dropdown 2.3.2]
[COPYRIGHT]
  Copyright 2013 Twitter, Inc.

[LICENSE]

Apache License
Version 2.0, January 2004

http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of
   this License, each Contributor hereby grants to You a perpetual,
   worldwide, non-exclusive, no-charge, royalty-free, irrevocable
   (except as stated in this section) patent license to make, have made,
   use, offer to sell, sell, import, and otherwise transfer the Work,
   where such license applies only to those patent claims licensable
   by such Contributor that are necessarily infringed by their
   Contribution(s) alone or by combination of their Contribution(s)
   with the Work to which such Contribution(s) was submitted. If You
   institute patent litigation against any entity (including a
   cross-claim or counterclaim in a lawsuit) alleging that the Work
   or a Contribution incorporated within the Work constitutes direct
   or contributory patent infringement, then any patent licenses
   granted to You under this License for that Work shall terminate
   as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the
   Work or Derivative Works thereof in any medium, with or without
   modifications, and in Source or Object form, provided that You
   meet the following conditions:

   (a) You must give any other recipients of the Work or
       Derivative Works a copy of this License; and

   (b) You must cause any modified files to carry prominent notices
       stating that You changed the files; and

   (c) You must retain, in the Source form of any Derivative Works
       that You distribute, all copyright, patent, trademark, and
       attribution notices from the Source form of the Work,
       excluding those notices that do not pertain to any part of
       the Derivative Works; and

   (d) If the Work includes a "NOTICE" text file as part of its
       distribution, then any Derivative Works that You distribute must
       include a readable copy of the attribution notices contained
       within such NOTICE file, excluding those notices that do not
       pertain to any part of the Derivative Works, in at least one
       of the following places: within a NOTICE text file distributed
       as part of the Derivative Works; within the Source form or
       documentation, if provided along with the Derivative Works; or,
       within a display generated by the Derivative Works, if and
       wherever such third-party notices normally appear. The contents
       of the NOTICE file are for informational purposes only and
       do not modify the License. You may add Your own attribution
       notices within Derivative Works that You distribute, alongside
       or as an addendum to the NOTICE text from the Work, provided
       that such additional attribution notices cannot be construed
       as modifying the License.

   You may add Your own copyright statement to Your modifications and
   may provide additional or different license terms and conditions
   for use, reproduction, or distribution of Your modifications, or
   for any such Derivative Works as a whole, provided Your use,
   reproduction, and distribution of the Work otherwise complies with
   the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise,
   any Contribution intentionally submitted for inclusion in the Work
   by You to the Licensor shall be under the terms and conditions of
   this License, without any additional terms or conditions.
   Notwithstanding the above, nothing herein shall supersede or modify
   the terms of any separate license agreement you may have executed
   with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade
   names, trademarks, service marks, or product names of the Licensor,
   except as required for reasonable and customary use in describing the
   origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or
   agreed to in writing, Licensor provides the Work (and each
   Contributor provides its Contributions) on an "AS IS" BASIS,
   WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or
   implied, including, without limitation, any warranties or conditions
   of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A
   PARTICULAR PURPOSE. You are solely responsible for determining the
   appropriateness of using or redistributing the Work and assume any
   risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory,
   whether in tort (including negligence), contract, or otherwise,
   unless required by applicable law (such as deliberate and grossly
   negligent acts) or agreed to in writing, shall any Contributor be
   liable to You for damages, including any direct, indirect, special,
   incidental, or consequential damages of any character arising as a
   result of this License or out of the use or inability to use the
   Work (including but not limited to damages for loss of goodwill,
   work stoppage, computer failure or malfunction, or any and all
   other commercial damages or losses), even if such Contributor
   has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing
   the Work or Derivative Works thereof, You may choose to offer,
   and charge a fee for, acceptance of support, warranty, indemnity,
   or other liability obligations and/or rights consistent with this
   License. However, in accepting such obligations, You may act only
   on Your own behalf and on Your sole responsibility, not on behalf
   of any other Contributor, and only if You agree to indemnify,
   defend, and hold each Contributor harmless for any liability
   incurred by, or claims asserted against, such Contributor by reason
   of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

[bootstrap-modal 2.1]
[COPYRIGHT]
Copyright 2013 Twitter, Inc.

[LICENSE]

Apache License
Version 2.0, January 2004
http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

   "License" shall mean the terms and conditions for use, reproduction,
   and distribution as defined by Sections 1 through 9 of this document.

   "Licensor" shall mean the copyright owner or entity authorized by
   the copyright owner that is granting the License.

   "Legal Entity" shall mean the union of the acting entity and all
   other entities that control, are controlled by, or are under common
   control with that entity. For the purposes of this definition,
   "control" means (i) the power, direct or indirect, to cause the
   direction or management of such entity, whether by contract or
   otherwise, or (ii) ownership of fifty percent (50%) or more of the
   outstanding shares, or (iii) beneficial ownership of such entity.

   "You" (or "Your") shall mean an individual or Legal Entity
   exercising permissions granted by this License.

   "Source" form shall mean the preferred form for making modifications,
   including but not limited to software source code, documentation
   source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

   (a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

   (b) You must cause any modified files to carry prominent notices stating that You changed the files; and

(c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

(d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only

on Your own behalf and on Your sole responsibility, not on behalf
of any other Contributor, and only if You agree to indemnify,
defend, and hold each Contributor harmless for any liability
incurred by, or claims asserted against, such Contributor by reason
of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

[bootstrapSwitch 1.3.0]

Apache License
Version 2.0, January 2004
http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction,
and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by
the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all
other entities that control, are controlled by, or are under common
control with that entity. For the purposes of this definition,
"control" means (i) the power, direct or indirect, to cause the
direction or management of such entity, whether by contract or
otherwise, or (ii) ownership of fifty percent (50%) or more of the
outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity
exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications,
including but not limited to software source code, documentation
source, and configuration files.

"Object" form shall mean any form resulting from mechanical
transformation or translation of a Source form, including but
not limited to compiled object code, generated documentation,
and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or
Object form, made available under the License, as indicated by a
copyright notice that is included in or attached to the work
(an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object
form, that is based on (or derived from) the Work and for which the
editorial revisions, annotations, elaborations, or other modifications
represent, as a whole, an original work of authorship. For the purposes
of this License, Derivative Works shall not include works that remain
separable from, or merely link (or bind by name) to the interfaces of,
the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including
the original version of the Work and any modifications or additions
to that Work or Derivative Works thereof, that is intentionally
submitted to Licensor for inclusion in the Work by the copyright owner
or by an individual or Legal Entity authorized to submit on behalf of
the copyright owner. For the purposes of this definition, "submitted"
means any form of electronic, verbal, or written communication sent
to the Licensor or its representatives, including but not limited to
communication on electronic mailing lists, source code control systems,
and issue tracking systems that are managed by, or on behalf of, the
Licensor for the purpose of discussing and improving the Work, but
excluding communication that is conspicuously marked or otherwise
designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

   (a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

   (b) You must cause any modified files to carry prominent notices stating that You changed the files; and

   (c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

   (d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

   You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise,

any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

[bootstrap-tab 2.3.2]
[COPYRIGHT]
Copyright 2013 Twitter, Inc.

[LICENSE]

Apache License
Version 2.0, January 2004
http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition,

"control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the
   Work or Derivative Works thereof in any medium, with or without
   modifications, and in Source or Object form, provided that You
   meet the following conditions:

   (a) You must give any other recipients of the Work or
       Derivative Works a copy of this License; and

   (b) You must cause any modified files to carry prominent notices
       stating that You changed the files; and

   (c) You must retain, in the Source form of any Derivative Works
       that You distribute, all copyright, patent, trademark, and
       attribution notices from the Source form of the Work,
       excluding those notices that do not pertain to any part of
       the Derivative Works; and

   (d) If the Work includes a "NOTICE" text file as part of its
       distribution, then any Derivative Works that You distribute must
       include a readable copy of the attribution notices contained
       within such NOTICE file, excluding those notices that do not
       pertain to any part of the Derivative Works, in at least one
       of the following places: within a NOTICE text file distributed
       as part of the Derivative Works; within the Source form or
       documentation, if provided along with the Derivative Works; or,
       within a display generated by the Derivative Works, if and
       wherever such third-party notices normally appear. The contents
       of the NOTICE file are for informational purposes only and
       do not modify the License. You may add Your own attribution
       notices within Derivative Works that You distribute, alongside
       or as an addendum to the NOTICE text from the Work, provided
       that such additional attribution notices cannot be construed
       as modifying the License.

   You may add Your own copyright statement to Your modifications and
   may provide additional or different license terms and conditions
   for use, reproduction, or distribution of Your modifications, or
   for any such Derivative Works as a whole, provided Your use,
   reproduction, and distribution of the Work otherwise complies with
   the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise,
   any Contribution intentionally submitted for inclusion in the Work
   by You to the Licensor shall be under the terms and conditions of
   this License, without any additional terms or conditions.
   Notwithstanding the above, nothing herein shall supersede or modify
   the terms of any separate license agreement you may have executed
   with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade
   names, trademarks, service marks, or product names of the Licensor,
   except as required for reasonable and customary use in describing the
   origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or
   agreed to in writing, Licensor provides the Work (and each
   Contributor provides its Contributions) on an "AS IS" BASIS,
   WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or
   implied, including, without limitation, any warranties or conditions
   of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A
   PARTICULAR PURPOSE. You are solely responsible for determining the
   appropriateness of using or redistributing the Work and assume any
   risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory,
   whether in tort (including negligence), contract, or otherwise,
   unless required by applicable law (such as deliberate and grossly
   negligent acts) or agreed to in writing, shall any Contributor be
   liable to You for damages, including any direct, indirect, special,

incidental, or consequential damages of any character arising as a
result of this License or out of the use or inability to use the
Work (including but not limited to damages for loss of goodwill,
work stoppage, computer failure or malfunction, or any and all
other commercial damages or losses), even if such Contributor
has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing
the Work or Derivative Works thereof, You may choose to offer,
and charge a fee for, acceptance of support, warranty, indemnity,
or other liability obligations and/or rights consistent with this
License. However, in accepting such obligations, You may act only
on Your own behalf and on Your sole responsibility, not on behalf
of any other Contributor, and only if You agree to indemnify,
defend, and hold each Contributor harmless for any liability
incurred by, or claims asserted against, such Contributor by reason
of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

[bootstrap-typeahead 2.3.2]

license:

```
/* ============================================================
 * bootstrap-typeahead.js v2.3.2
 * http://getbootstrap.com/2.3.2/javascript.html#typeahead
 * ============================================================
 * Copyright 2013 Twitter, Inc.
 *
 * Licensed under the Apache License, Version 2.0 (the "License");
 * you may not use this file except in compliance with the License.
 * You may obtain a copy of the License at
 *
 * http://www.apache.org/licenses/LICENSE-2.0
 *
 * Unless required by applicable law or agreed to in writing, software
 * distributed under the License is distributed on an "AS IS" BASIS,
 * WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
 * See the License for the specific language governing permissions and
 * limitations under the License.
 * ============================================================ */
```

[containerd 1.4.11]

Apache License
Version 2.0, January 2004
https://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction,
and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by
the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all
other entities that control, are controlled by, or are under common
control with that entity. For the purposes of this definition,
"control" means (i) the power, direct or indirect, to cause the
direction or management of such entity, whether by contract or
otherwise, or (ii) ownership of fifty percent (50%) or more of the
outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity

exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

(a) You must give any other recipients of the Work or
Derivative Works a copy of this License; and

(b) You must cause any modified files to carry prominent notices
stating that You changed the files; and

(c) You must retain, in the Source form of any Derivative Works
that You distribute, all copyright, patent, trademark, and
attribution notices from the Source form of the Work,
excluding those notices that do not pertain to any part of
the Derivative Works; and

(d) If the Work includes a "NOTICE" text file as part of its
distribution, then any Derivative Works that You distribute must
include a readable copy of the attribution notices contained
within such NOTICE file, excluding those notices that do not
pertain to any part of the Derivative Works, in at least one
of the following places: within a NOTICE text file distributed
as part of the Derivative Works; within the Source form or
documentation, if provided along with the Derivative Works; or,
within a display generated by the Derivative Works, if and
wherever such third-party notices normally appear. The contents
of the NOTICE file are for informational purposes only and
do not modify the License. You may add Your own attribution
notices within Derivative Works that You distribute, alongside
or as an addendum to the NOTICE text from the Work, provided
that such additional attribution notices cannot be construed
as modifying the License.

You may add Your own copyright statement to Your modifications and
may provide additional or different license terms and conditions
for use, reproduction, or distribution of Your modifications, or
for any such Derivative Works as a whole, provided Your use,
reproduction, and distribution of the Work otherwise complies with
the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise,
any Contribution intentionally submitted for inclusion in the Work
by You to the Licensor shall be under the terms and conditions of
this License, without any additional terms or conditions.
Notwithstanding the above, nothing herein shall supersede or modify
the terms of any separate license agreement you may have executed
with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade
names, trademarks, service marks, or product names of the Licensor,
except as required for reasonable and customary use in describing the
origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or
agreed to in writing, Licensor provides the Work (and each
Contributor provides its Contributions) on an "AS IS" BASIS,
WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or
implied, including, without limitation, any warranties or conditions
of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A
PARTICULAR PURPOSE. You are solely responsible for determining the
appropriateness of using or redistributing the Work and assume any
risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory,
whether in tort (including negligence), contract, or otherwise,
unless required by applicable law (such as deliberate and grossly
negligent acts) or agreed to in writing, shall any Contributor be
liable to You for damages, including any direct, indirect, special,
incidental, or consequential damages of any character arising as a
result of this License or out of the use or inability to use the
Work (including but not limited to damages for loss of goodwill,
work stoppage, computer failure or malfunction, or any and all
other commercial damages or losses), even if such Contributor
has been advised of the possibility of such damages.

```
   9. Accepting Warranty or Additional Liability. While redistributing
      the Work or Derivative Works thereof, You may choose to offer,
      and charge a fee for, acceptance of support, warranty, indemnity,
      or other liability obligations and/or rights consistent with this
      License. However, in accepting such obligations, You may act only
      on Your own behalf and on Your sole responsibility, not on behalf
      of any other Contributor, and only if You agree to indemnify,
      defend, and hold each Contributor harmless for any liability
      incurred by, or claims asserted against, such Contributor by reason
      of your accepting any such warranty or additional liability.

   END OF TERMS AND CONDITIONS

   Copyright The containerd Authors

   Licensed under the Apache License, Version 2.0 (the "License");
   you may not use this file except in compliance with the License.
   You may obtain a copy of the License at

       https://www.apache.org/licenses/LICENSE-2.0

   Unless required by applicable law or agreed to in writing, software
   distributed under the License is distributed on an "AS IS" BASIS,
   WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
   See the License for the specific language governing permissions and
   limitations under the License.
[NOTICE]
Docker
Copyright 2012-2015 Docker, Inc.

This    product    includes    software    developed    at    Docker,    Inc.
(https://www.docker.com).

The following is courtesy of our legal counsel:


Use and transfer of Docker may be subject to certain restrictions by the
United States and other governments.
It is your responsibility to ensure that your use and/or transfer does not
violate applicable laws.

For more information, please see https://www.bis.doc.gov

See also https://www.apache.org/dev/crypto.html and/or seek legal counsel.
--------------------------------------------------------------------------------
---
[cpio 2.11]
[COPYRIGHT]
  Copyright (C) 1990, 1991, 1992, 2001, 2006, 2007, 2009, 2010 Free
  Software Foundation, Inc.

[LICENSE]
          GNU GENERAL PUBLIC LICENSE
             Version 3, 29 June 2007

 Copyright (C) 2007 Free Software Foundation, Inc. <http://fsf.org/>
 Everyone is permitted to copy and distribute verbatim copies
 of this license document, but changing it is not allowed.

              Preamble

  The GNU General Public License is a free, copyleft license for
software and other kinds of works.

  The licenses for most software and other practical works are designed
to take away your freedom to share and change the works.  By contrast,
the GNU General Public License is intended to guarantee your freedom to
share and change all versions of a program--to make sure it remains free
software for all its users.  We, the Free Software Foundation, use the
```

GNU General Public License for most of our software; it applies also to any other work released this way by its authors. You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for them if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you these rights or asking you to surrender the rights. Therefore, you have certain responsibilities if you distribute copies of the software, or if you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must pass on to the recipients the same freedoms that you received. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

Developers that use the GNU GPL protect your rights with two steps: (1) assert copyright on the software, and (2) offer you this License giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains that there is no warranty for this free software. For both users' and authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

Some devices are designed to deny users access to install or run modified versions of the software inside them, although the manufacturer can do so. This is fundamentally incompatible with the aim of protecting users' freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we stand ready to extend this provision to those domains in future versions of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents. States should not allow patents to restrict development and use of software on general-purpose computers, but in those that do, we wish to avoid the special danger that patents applied to a free program could make it effectively proprietary. To prevent this, the GPL assures that patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS

0. Definitions.

"This License" refers to version 3 of the GNU General Public License.

"Copyright" also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

"The Program" refers to any copyrightable work licensed under this License. Each licensee is addressed as "you". "Licensees" and "recipients" may be individuals or organizations.

To "modify" a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a "modified version" of the earlier work or a work "based on" the earlier work.

A "covered work" means either the unmodified Program or a work based on the Program.

To "propagate" a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To "convey" a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays "Appropriate Legal Notices" to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

1. Source Code.

The "source code" for a work means the preferred form of the work for making modifications to it. "Object code" means any non-source form of a work.

A "Standard Interface" means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The "System Libraries" of an executable work include anything, other than the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A "Major Component", in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The "Corresponding Source" for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

2. Basic Permissions.

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated

conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered by this License only if the output, given its content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed; section 10 makes it unnecessary.

3. Protecting Users' Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of technological measures.

4. Conveying Verbatim Copies.

You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice; keep intact all notices stating that this License and any non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

5. Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

a) The work must carry prominent notices stating that you modified it, and giving a relevant date.

b) The work must carry prominent notices stating that it is released under this License and any conditions added under section 7. This requirement modifies the requirement in section 4 to "keep intact all notices".

c) You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not

invalidate such permission if you have separately received it.

d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an "aggregate" if the compilation and its resulting copyright are not used to limit the access or legal rights of the compilation's users beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.

6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, in one of these ways:

a) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange.

b) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for software interchange, for a price no more than your reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.

c) Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This alternative is allowed only occasionally and noncommercially, and only if you received the object code with such an offer, in accord with subsection 6b.

d) Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in the same way through the same place at no further charge. You need not require recipients to copy the Corresponding Source along with the object code. If the place to copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.

e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.

A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object code work.

A "User Product" is either (1) a "consumer product", which means any

tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, "normally used" refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

"Installation Information" for a User Product means any methods, procedures, authorization keys, or other information required to install and execute modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

7. Additional Terms.

"Additional permissions" are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

a) Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or

b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or

c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or

d) Limiting the use for publicity purposes of names of licensors or authors of the material; or

e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or

f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on those licensors and authors.

All other non-permissive additional terms are considered "further restrictions" within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above requirements apply either way.

8. Termination.

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or

run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10. Automatic Licensing of Downstream Recipients.

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An "entity transaction" is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

11. Patents.

A "contributor" is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's "contributor version".

A contributor's "essential patent claims" are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For purposes of this definition, "control" includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a "patent license" is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To "grant" such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. "Knowingly relying" means you have

actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is "discriminatory" if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.

12. No Surrender of Others' Freedom.

If conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot convey a covered work so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

13. Use with the GNU Affero General Public License.

Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed under version 3 of the GNU Affero General Public License into a single combined work, and to convey the resulting work. The terms of this License will continue to apply to the part which is the covered work, but the special requirements of the GNU Affero General Public License, section 13, concerning interaction through a network will apply to the combination as such.

14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of the GNU General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU General Public License, you may choose any version ever published by the Free Software Foundation.

If the Program specifies that a proxy can decide which future versions of the GNU General Public License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Program.

Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

15. Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

17. Interpretation of Sections 15 and 16.

If the disclaimer of warranty and limitation of liability provided above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates an absolute waiver of all civil liability in connection with the Program, unless a warranty or assumption of liability accompanies a copy of the Program in return for a fee.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively state the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This program is free software: you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation, either version 3 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License

```
    along with this program.  If not, see <http://www.gnu.org/licenses/>.

Also add information on how to contact you by electronic and paper mail.

  If the program does terminal interaction, make it output a short
notice like this when it starts in an interactive mode:

    <program>  Copyright (C) <year>  <name of author>
    This program comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
    This is free software, and you are welcome to redistribute it
    under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate
parts of the General Public License.  Of course, your program's commands
might be different; for a GUI interface, you would use an "about box".

  You should also get your employer (if you work as a programmer) or school,
if any, to sign a "copyright disclaimer" for the program, if necessary.
For more information on this, and how to apply and follow the GNU GPL, see
<http://www.gnu.org/licenses/>.

  The GNU General Public License does not permit incorporating your program
into proprietary programs.  If your program is a subroutine library, you
may consider it more useful to permit linking proprietary applications with
the library.  If this is what you want to do, use the GNU Lesser General
Public License instead of this License.  But first, please read
<http://www.gnu.org/philosophy/why-not-lgpl.html>.

--------------------------------------------------------------------------
---
[crypto-js 3.1.2]
# License
/*
CryptoJS v3.1.2
code.google.com/p/crypto-js
(c) 2009-2013 by Jeff Mott. All rights reserved.
code.google.com/p/crypto-js/wiki/License
*/
(c) 2009-2013 by Jeff Mott. All rights reserved.

Redistribution and use in source and binary forms, with or without modification,
are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this
list of conditions, and the following disclaimer.
Redistributions in binary form must reproduce the above copyright notice, this
list of conditions, and the following disclaimer in the documentation or other
materials provided with the distribution.
Neither the name CryptoJS nor the names of its contributors may be used to
endorse or promote products derived from this software without specific prior
written permission.
THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS,"
AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, ARE
DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE
FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR
SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER
CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY,
OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE
OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
--------------------------------------------------------------------------
---
[curl 7.53.1]
[COPYRIGHT]
  Copyright (c) 1996 - 2010, Daniel Stenberg, <daniel@haxx.se>.
  All rights reserved.

[LICENSE]
 Permission to use, copy, modify, and distribute this software for any purpose
```

with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN
NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder.

[dosfstools 4.1]

GNU GENERAL PUBLIC LICENSE
Version 3, 29 June 2007

Copyright (C) 2007 Free Software Foundation, Inc. <http://fsf.org/>
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The GNU General Public License is a free, copyleft license for software and other kinds of works.

The licenses for most software and other practical works are designed to take away your freedom to share and change the works. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change all versions of a program--to make sure it remains free software for all its users. We, the Free Software Foundation, use the GNU General Public License for most of our software; it applies also to any other work released this way by its authors. You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for them if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you these rights or asking you to surrender the rights. Therefore, you have certain responsibilities if you distribute copies of the software, or if you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must pass on to the recipients the same freedoms that you received. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

Developers that use the GNU GPL protect your rights with two steps: (1) assert copyright on the software, and (2) offer you this License giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains that there is no warranty for this free software. For both users' and authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

Some devices are designed to deny users access to install or run modified versions of the software inside them, although the manufacturer can do so. This is fundamentally incompatible with the aim of

protecting users' freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we stand ready to extend this provision to those domains in future versions of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents. States should not allow patents to restrict development and use of software on general-purpose computers, but in those that do, we wish to avoid the special danger that patents applied to a free program could make it effectively proprietary. To prevent this, the GPL assures that patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS

0. Definitions.

"This License" refers to version 3 of the GNU General Public License.

"Copyright" also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

"The Program" refers to any copyrightable work licensed under this License. Each licensee is addressed as "you". "Licensees" and "recipients" may be individuals or organizations.

To "modify" a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a "modified version" of the earlier work or a work "based on" the earlier work.

A "covered work" means either the unmodified Program or a work based on the Program.

To "propagate" a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To "convey" a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays "Appropriate Legal Notices" to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

1. Source Code.

The "source code" for a work means the preferred form of the work for making modifications to it. "Object code" means any non-source form of a work.

A "Standard Interface" means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The "System Libraries" of an executable work include anything, other than the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A "Major Component", in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The "Corresponding Source" for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

2. Basic Permissions.

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered by this License only if the output, given its content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed; section 10 makes it unnecessary.

3. Protecting Users' Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of

technological measures.

4. Conveying Verbatim Copies.

You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice; keep intact all notices stating that this License and any non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

5. Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

a) The work must carry prominent notices stating that you modified it, and giving a relevant date.

b) The work must carry prominent notices stating that it is released under this License and any conditions added under section 7. This requirement modifies the requirement in section 4 to "keep intact all notices".

c) You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.

d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an "aggregate" if the compilation and its resulting copyright are not used to limit the access or legal rights of the compilation's users beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.

6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, in one of these ways:

a) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange.

b) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the

product that is covered by this License, on a durable physical medium customarily used for software interchange, for a price no more than your reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.

c) Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This alternative is allowed only occasionally and noncommercially, and only if you received the object code with such an offer, in accord with subsection 6b.

d) Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in the same way through the same place at no further charge. You need not require recipients to copy the Corresponding Source along with the object code. If the place to copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.

e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.

A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object code work.

A "User Product" is either (1) a "consumer product", which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, "normally used" refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

"Installation Information" for a User Product means any methods, procedures, authorization keys, or other information required to install and execute modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a

network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

7. Additional Terms.

"Additional permissions" are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

a) Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or

b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or

c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or

d) Limiting the use for publicity purposes of names of licensors or authors of the material; or

e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or

f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on those licensors and authors.

All other non-permissive additional terms are considered "further restrictions" within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above requirements apply either way.

8. Termination.

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10. Automatic Licensing of Downstream Recipients.

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An "entity transaction" is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

11. Patents.

A "contributor" is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's "contributor version".

A contributor's "essential patent claims" are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For purposes of this definition, "control" includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a "patent license" is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To "grant" such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. "Knowingly relying" means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is "discriminatory" if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.

12. No Surrender of Others' Freedom.

If conditions are imposed on you (whether by court order, agreement or

otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot convey a covered work so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

13. Use with the GNU Affero General Public License.

Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed under version 3 of the GNU Affero General Public License into a single combined work, and to convey the resulting work. The terms of this License will continue to apply to the part which is the covered work, but the special requirements of the GNU Affero General Public License, section 13, concerning interaction through a network will apply to the combination as such.

14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of the GNU General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU General Public License, you may choose any version ever published by the Free Software Foundation.

If the Program specifies that a proxy can decide which future versions of the GNU General Public License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Program.

Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

15. Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

17. Interpretation of Sections 15 and 16.

If the disclaimer of warranty and limitation of liability provided above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates an absolute waiver of all civil liability in connection with the Program, unless a warranty or assumption of liability accompanies a copy of the Program in return for a fee.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively state the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

```
<one line to give the program's name and a brief idea of what it does.>
Copyright (C) <year>  <name of author>

This program is free software: you can redistribute it and/or modify
it under the terms of the GNU General Public License as published by
the Free Software Foundation, either version 3 of the License, or
(at your option) any later version.

This program is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
GNU General Public License for more details.

You should have received a copy of the GNU General Public License
along with this program.  If not, see <http://www.gnu.org/licenses/>.
```

Also add information on how to contact you by electronic and paper mail.

If the program does terminal interaction, make it output a short notice like this when it starts in an interactive mode:

```
<program>  Copyright (C) <year>  <name of author>
This program comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
This is free software, and you are welcome to redistribute it
under certain conditions; type `show c' for details.
```

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, your program's commands might be different; for a GUI interface, you would use an "about box".

You should also get your employer (if you work as a programmer) or school, if any, to sign a "copyright disclaimer" for the program, if necessary. For more information on this, and how to apply and follow the GNU GPL, see <http://www.gnu.org/licenses/>.

The GNU General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Lesser General Public License instead of this License. But first, please read <http://www.gnu.org/philosophy/why-not-lgpl.html>.

[echarts 2.2.7]

license:
Copyright (c) 2013, Baidu Inc.
All rights reserved.

Redistribution and use of this software in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of Baidu Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission of Baidu Inc.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

[font-awesome 4.1.0]
[COPYRIGHT]
Font Awesome 4.1.0 by @davegandy - http://fontawesome.io - @fontawesome

[LICENSE]
The Font Awesome font is licensed under the SIL OFL 1.1:
http://scripts.sil.org/OFL
Font Awesome CSS, LESS, and SASS files are licensed under the MIT License:
http://opensource.org/licenses/mit-license.html

This Font Software is licensed under the SIL Open Font License, Version 1.1.
This license is copied below, and is also available with a FAQ at:
https://openfontlicense.org

SIL OPEN FONT LICENSE Version 1.1 - 26 February 2007

PREAMBLE
The goals of the Open Font License (OFL) are to stimulate worldwide development of collaborative font projects, to support the font creation efforts of academic and linguistic communities, and to provide a free and open framework in which fonts may be shared and improved in partnership with others.

The OFL allows the licensed fonts to be used, studied, modified and redistributed freely as long as they are not sold by themselves. The fonts, including any derivative works, can be bundled, embedded, redistributed and/or sold with any software provided that any reserved names are not used by derivative works. The fonts and derivatives, however, cannot be released under any other type of license. The requirement for fonts to remain under this license does not apply to any document created using the fonts or their derivatives.

DEFINITIONS
"Font Software" refers to the set of files released by the Copyright Holder(s) under this license and clearly marked as such. This may include source files, build scripts and documentation.

"Reserved Font Name" refers to any names specified as such after the copyright statement(s).

"Original Version" refers to the collection of Font Software components as distributed by the Copyright Holder(s).

"Modified Version" refers to any derivative made by adding to, deleting, or substituting -- in part or in whole -- any of the components of the Original Version, by changing formats or by porting the Font Software to a new environment.

"Author" refers to any designer, engineer, programmer, technical writer or other person who contributed to the Font Software.

PERMISSION & CONDITIONS
Permission is hereby granted, free of charge, to any person obtaining a copy of the Font Software, to use, study, copy, merge, embed, modify, redistribute, and sell modified and unmodified copies of the Font Software, subject to the following conditions:

1) Neither the Font Software nor any of its individual components, in Original or Modified Versions, may be sold by itself.

2) Original or Modified Versions of the Font Software may be bundled, redistributed and/or sold with any software, provided that each copy contains the above copyright notice and this license. These can be included either as stand-alone text files, human-readable headers or in the appropriate machine-readable metadata fields within text or binary files as long as those fields can be easily viewed by the user.

3) No Modified Version of the Font Software may use the Reserved Font Name(s) unless explicit written permission is granted by the corresponding Copyright Holder. This restriction only applies to the primary font name as presented to the users.

4) The name(s) of the Copyright Holder(s) or the Author(s) of the Font Software shall not be used to promote, endorse or advertise any Modified Version, except to acknowledge the contribution(s) of the Copyright Holder(s) and the Author(s) or with their explicit written permission.

5) The Font Software, modified or unmodified, in part or in whole, must be distributed entirely under this license, and must not be distributed under any other license. The requirement for fonts to remain under this license does not apply to any document created using the Font Software.

TERMINATION
This license becomes null and void if any of the above conditions are not met.

DISCLAIMER
THE FONT SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF COPYRIGHT, PATENT, TRADEMARK, OR OTHER RIGHT. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, INCLUDING ANY GENERAL, SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF THE USE OR INABILITY TO USE THE FONT SOFTWARE OR FROM OTHER DEALINGS IN THE FONT SOFTWARE.

[freeradius-server 3.0.27]
[COPYRIGHT]

dnl Copyright 息 2004 Scott James Remnant <scott@netsplit.com>.
dnl Copyright 息 2012-2015 Dan Nicholson <dbn.lists@gmail.com>
Copyright (C) 2001-2017 Free Software Foundation, Inc.
Copyright (C) 1997-2017 Free Software Foundation, Inc.

Copyright 1992-2021 Free Software Foundation, Inc.

Copyright (C) 1992-1996, 1998-2012 Free Software Foundation, Inc.
Copyright (C) 2012 Free Software Foundation, Inc.
Copyright (c) 2009 Dean Povey <povey@wedgetail.com>

Copyright (C) 1999-2015 The FreeRADIUS Server Project

Copyright (C) 1999, 2000, 2001, 2002, 2003, 2004, 2005, 2006, 2007, 2008, 2009
Alan DeKok
<aland@deployingradius.com>

Copyright (C) 1996, 1997, 1999, 2000, 2002, 2003, 2004, 2005 Free
Software Foundation, Inc.

Copyright (C) 2011-2015 Arran Cudbard-Bell <a.cudbardb@freeradius.org>

Copyright (C) 2003, 2004, 2005 Kostas Kalevras <kkalev@noc.ntua.gr>

Copyright (C) 2004 Cladju Consulting, Inc.

Copyright (C) 2001, 2002, 2003, 2004, 2005 Google, Inc.

Copyright (C) 2003, 2004 Michael Richardson <mcr@sandelman.ottawa.on.ca>

Copyright (C) 2002, 2003, 2004 Novell, Inc.

Copyright (C) 2002 Miguel A.L. Paraz <mparaz@mparaz.com>

Copyright (C) 2002 Simon Ekstrand <simon@routemeister.net>

Copyright (C) 2001 Chad Miller <cmiller@surfsouth.com>

Copyright (C) 2001 hereUare Communications, Inc.

Copyright (C) 2000 Jochen Friedrich <jochen@scram.de>

Copyright (C) 2000, 2002 Miquel van Smoorenburg

Copyright (C) 2000 Jeff Carneal <jeff@apex.net>

Copyright (C) 2000 Alan Curry <pacman@world.std.com>

Copyright (C) 2000 David Kerry <davidk@snti.com>

Copyright (C) 2000 Dmitri Ageev <d_ageev@ortcc.ru>

Copyright (C) 2000 Nathan Neulinger <nneul@umr.edu>

Copyright (C) 2000 Mike Machado <mike@innercite.com>

Copyright (C) 2000, 2001 Chad Miller <cmiller@surfsouth.com>

Copyright (C) 1997, 1998, 1999 Cistron Internet Services B.V.

Copyright (C) 1999 Kunihiro Ishiguro <kunihiro@zebra.org>

[LICENSE]
GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.
51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your

freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate

copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you

received the program in object code or executable form with such
an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that

system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

```
    <one line to give the program's name and a brief idea of what it does.>
    Copyright (C) <year>  <name of author>

    This program is free software; you can redistribute it and/or modify
    it under the terms of the GNU General Public License as published by
    the Free Software Foundation; either version 2 of the License, or
    (at your option) any later version.

    This program is distributed in the hope that it will be useful,
    but WITHOUT ANY WARRANTY; without even the implied warranty of
    MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
    GNU General Public License for more details.

    You should have received a copy of the GNU General Public License
    along with this program; if not, write to the Free Software
    Foundation, Inc., 51 Franklin St, Fifth Floor, Boston, MA  02110-1301  USA


Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this
when it starts in an interactive mode:

    Gnomovision version 69, Copyright (C) year name of author
    Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
    This is free software, and you are welcome to redistribute it
    under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate
parts of the General Public License.  Of course, the commands you use may
be called something other than `show w' and `show c'; they could even be
mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your
school, if any, to sign a "copyright disclaimer" for the program, if
necessary.  Here is a sample; alter the names:

  Yoyodyne, Inc., hereby disclaims all copyright interest in the program
  `Gnomovision' (which makes passes at compilers) written by James Hacker.

  <signature of Ty Coon>, 1 April 1989
  Ty Coon, President of Vice

This General Public License does not permit incorporating your program into
proprietary programs.  If your program is a subroutine library, you may
consider it more useful to permit linking proprietary applications with the
library.  If this is what you want to do, use the GNU Library General
Public License instead of this License.
------------------------------------------------------------------------------
---
[freescale-openflow-controller 1.0]
[COPYRIGHT]
  Copyright (c) 2012, 2013  Freescale.

[LICENSE]
                                 Apache License
                           Version 2.0, January 2004
                        http://www.apache.org/licenses/

   TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

   1. Definitions.

      "License" shall mean the terms and conditions for use, reproduction,
      and distribution as defined by Sections 1 through 9 of this document.

      "Licensor" shall mean the copyright owner or entity authorized by
      the copyright owner that is granting the License.
```

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct

or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

   (a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

   (b) You must cause any modified files to carry prominent notices stating that You changed the files; and

   (c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

   (d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

   You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise,

unless required by applicable law (such as deliberate and grossly
negligent acts) or agreed to in writing, shall any Contributor be
liable to You for damages, including any direct, indirect, special,
incidental, or consequential damages of any character arising as a
result of this License or out of the use or inability to use the
Work (including but not limited to damages for loss of goodwill,
work stoppage, computer failure or malfunction, or any and all
other commercial damages or losses), even if such Contributor
has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing
the Work or Derivative Works thereof, You may choose to offer,
and charge a fee for, acceptance of support, warranty, indemnity,
or other liability obligations and/or rights consistent with this
License. However, in accepting such obligations, You may act only
on Your own behalf and on Your sole responsibility, not on behalf
of any other Contributor, and only if You agree to indemnify,
defend, and hold each Contributor harmless for any liability
incurred by, or claims asserted against, such Contributor by reason
of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

APPENDIX: How to apply the Apache License to your work.

To apply the Apache License to your work, attach the following
boilerplate notice, with the fields enclosed by brackets "[]"
replaced with your own identifying information. (Don't include
the brackets!) The text should be enclosed in the appropriate
comment syntax for the file format. We also recommend that a
file or class name and description of purpose be included on the
same "printed page" as the copyright notice for easier
identification within third-party archives.

Copyright [yyyy] [name of copyright owner]

Licensed under the Apache License, Version 2.0 (the "License");
you may not use this file except in compliance with the License.
You may obtain a copy of the License at

http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software
distributed under the License is distributed on an "AS IS" BASIS,
WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
See the License for the specific language governing permissions and
limitations under the License.

[glibc 2.28]
[LICENSE]

GNU LESSER GENERAL PUBLIC LICENSE
Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.
51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts
as the successor of the GNU Library Public License, version 2, hence
the version number 2.1.]

Preamble

The licenses for most software are designed to take away your
freedom to share and change it. By contrast, the GNU General Public
Licenses are intended to guarantee your freedom to share and change
free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the library's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA

Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the library, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the library `Frob' (a library for tweaking knobs) written by James Random Hacker.

<signature of Ty Coon>, 1 April 1990
Ty Coon, President of Vice

That's all there is to it!

[grpc 1.34.0]

Apache License
Version 2.0, January 2004
http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You

meet the following conditions:

(a) You must give any other recipients of the Work or
Derivative Works a copy of this License; and

(b) You must cause any modified files to carry prominent notices
stating that You changed the files; and

(c) You must retain, in the Source form of any Derivative Works
that You distribute, all copyright, patent, trademark, and
attribution notices from the Source form of the Work,
excluding those notices that do not pertain to any part of
the Derivative Works; and

(d) If the Work includes a "NOTICE" text file as part of its
distribution, then any Derivative Works that You distribute must
include a readable copy of the attribution notices contained
within such NOTICE file, excluding those notices that do not
pertain to any part of the Derivative Works, in at least one
of the following places: within a NOTICE text file distributed
as part of the Derivative Works; within the Source form or
documentation, if provided along with the Derivative Works; or,
within a display generated by the Derivative Works, if and
wherever such third-party notices normally appear. The contents
of the NOTICE file are for informational purposes only and
do not modify the License. You may add Your own attribution
notices within Derivative Works that You distribute, alongside
or as an addendum to the NOTICE text from the Work, provided
that such additional attribution notices cannot be construed
as modifying the License.

You may add Your own copyright statement to Your modifications and
may provide additional or different license terms and conditions
for use, reproduction, or distribution of Your modifications, or
for any such Derivative Works as a whole, provided Your use,
reproduction, and distribution of the Work otherwise complies with
the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise,
any Contribution intentionally submitted for inclusion in the Work
by You to the Licensor shall be under the terms and conditions of
this License, without any additional terms or conditions.
Notwithstanding the above, nothing herein shall supersede or modify
the terms of any separate license agreement you may have executed
with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade
names, trademarks, service marks, or product names of the Licensor,
except as required for reasonable and customary use in describing the
origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or
agreed to in writing, Licensor provides the Work (and each
Contributor provides its Contributions) on an "AS IS" BASIS,
WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or
implied, including, without limitation, any warranties or conditions
of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A
PARTICULAR PURPOSE. You are solely responsible for determining the
appropriateness of using or redistributing the Work and assume any
risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory,
whether in tort (including negligence), contract, or otherwise,
unless required by applicable law (such as deliberate and grossly
negligent acts) or agreed to in writing, shall any Contributor be
liable to You for damages, including any direct, indirect, special,
incidental, or consequential damages of any character arising as a
result of this License or out of the use or inability to use the
Work (including but not limited to damages for loss of goodwill,
work stoppage, computer failure or malfunction, or any and all

other commercial damages or losses), even if such Contributor
has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing
the Work or Derivative Works thereof, You may choose to offer,
and charge a fee for, acceptance of support, warranty, indemnity,
or other liability obligations and/or rights consistent with this
License. However, in accepting such obligations, You may act only
on Your own behalf and on Your sole responsibility, not on behalf
of any other Contributor, and only if You agree to indemnify,
defend, and hold each Contributor harmless for any liability
incurred by, or claims asserted against, such Contributor by reason
of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

APPENDIX: How to apply the Apache License to your work.

To apply the Apache License to your work, attach the following
boilerplate notice, with the fields enclosed by brackets "[]"
replaced with your own identifying information. (Don't include
the brackets!) The text should be enclosed in the appropriate
comment syntax for the file format. We also recommend that a
file or class name and description of purpose be included on the
same "printed page" as the copyright notice for easier
identification within third-party archives.

Copyright [yyyy] [name of copyright owner]

Licensed under the Apache License, Version 2.0 (the "License");
you may not use this file except in compliance with the License.
You may obtain a copy of the License at

http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software
distributed under the License is distributed on an "AS IS" BASIS,
WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
See the License for the specific language governing permissions and
limitations under the License.

[jquery.event.drag 2.2]
[COPYRIGHT]

```
/*!
 * jquery.event.drag - v 2.2
 * Copyright (c) 2010 Three Dub Media - http://threedubmedia.com
 * Open Source MIT License - http://threedubmedia.com/code/license
 */
```

[jquery-ui 1.9.2]
[COPYRIGHT]

Copyright 2012 jQuery Foundation and other contributors,
http://jqueryui.com/

[LICENSE]

This software consists of voluntary contributions made by many
individuals (AUTHORS.txt, http://jqueryui.com/about) For exact
contribution history, see the revision history and logs, available
at http://jquery-ui.googlecode.com/svn/

Permission is hereby granted, free of charge, to any person obtaining
a copy of this software and associated documentation files (the
"Software"), to deal in the Software without restriction, including
without limitation the rights to use, copy, modify, merge, publish,
distribute, sublicense, and/or sell copies of the Software, and to
permit persons to whom the Software is furnished to do so, subject to
the following conditions:

```
The above copyright notice and this permission notice shall be
included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND,
EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF
MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND
NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE
LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION
OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION
WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

--------------------------------------------------------------------------
---
[json c 0.12]
[COPYRIGHT]
  Copyright (c) 2009-2012 Eric Haszlakiewicz

[LICENSE]
Permission is hereby granted, free of charge, to any person obtaining a
copy of this software and associated documentation files (the "Software"),
to deal in the Software without restriction, including without limitation
the rights to use, copy, modify, merge, publish, distribute, sublicense,
and/or sell copies of the Software, and to permit persons to whom the
Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included
in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE
AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER
LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,
OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE
SOFTWARE.

----------------------------------------------------------------
[COPYRIGHT]
Copyright (c) 2004, 2005 Metaparadigm Pte Ltd

[LICENSE]
Permission is hereby granted, free of charge, to any person obtaining a
copy of this software and associated documentation files (the "Software"),
to deal in the Software without restriction, including without limitation
the rights to use, copy, modify, merge, publish, distribute, sublicense,
and/or sell copies of the Software, and to permit persons to whom the
Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included
in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE
AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER
LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,
OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE
SOFTWARE.
--------------------------------------------------------------------------
---
[jstree 3.0.0]
[COPYRIGHT]
  Copyright (c) 2013 Ivan Bozhanov

[LICENSE]
Permission is hereby granted, free of charge, to any person
obtaining a copy of this software and associated documentation
files (the "Software"), to deal in the Software without
restriction, including without limitation the rights to use,
copy, modify, merge, publish, distribute, sublicense, and/or sell
```

```
copies of the Software, and to permit persons to whom the
Software is furnished to do so, subject to the following
conditions:

The above copyright notice and this permission notice shall be
included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND,
EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES
OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND
NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT
HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY,
WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING
FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR
OTHER DEALINGS IN THE SOFTWARE.
-------------------------------------------------------------------------------
---
[libiconv 1.15.0]
[COPYRIGHT]
    Copyright (C) 1991 Free Software Foundation, Inc.
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.
[This is the first released version of the library GPL. It is
numbered 2 because it goes with version 2 of the ordinary GPL.]

[LICENSE]
                    GNU LIBRARY GENERAL PUBLIC LICENSE
                       Version 2, June 1991

                            Preamble

  The licenses for most software are designed to take away your
freedom to share and change it.  By contrast, the GNU General Public
Licenses are intended to guarantee your freedom to share and change
free software--to make sure the software is free for all its users.

  This license, the Library General Public License, applies to some
specially designated Free Software Foundation software, and to any
other libraries whose authors decide to use it.  You can use it for
your libraries, too.

  When we speak of free software, we are referring to freedom, not
price.  Our General Public Licenses are designed to make sure that you
have the freedom to distribute copies of free software (and charge for
this service if you wish), that you receive source code or can get it
if you want it, that you can change the software or use pieces of it
in new free programs; and that you know you can do these things.

  To protect your rights, we need to make restrictions that forbid
anyone to deny you these rights or to ask you to surrender the rights.
These restrictions translate to certain responsibilities for you if
you distribute copies of the library, or if you modify it.

  For example, if you distribute copies of the library, whether gratis
or for a fee, you must give the recipients all the rights that we gave
you.  You must make sure that they, too, receive or can get the source
code.  If you link a program with the library, you must provide
complete object files to the recipients so that they can relink them
with the library, after making changes to the library and recompiling
it.  And you must show them these terms so they know their rights.

  Our method of protecting your rights has two steps: (1) copyright
the library, and (2) offer you this license which gives you legal
permission to copy, distribute and/or modify the library.

  Also, for each distributor's protection, we want to make certain
that everyone understands that there is no warranty for this free
library.  If the library is modified by someone else and passed on, we
want its recipients to know that what they have is not the original
```

version, so that any problems introduced by others will not reflect on the original authors' reputations.

痿・

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that companies distributing free software will individually obtain patent licenses, thus in effect transforming the program into proprietary software. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License, which was designed for utility programs. This license, the GNU Library General Public License, applies to certain designated libraries. This license is quite different from the ordinary one; be sure to read it in full, and don't assume that anything in it is the same as in the ordinary license.

The reason we have a separate public license for some libraries is that they blur the distinction we usually make between modifying or adding to a program and simply using it. Linking a program with a library, without changing the library, is in some sense simply using the library, and is analogous to running a utility program or application program. However, in a textual and legal sense, the linked executable is a combined work, a derivative of the original library, and the ordinary General Public License treats it as such.

Because of this blurred distinction, using the ordinary General Public License for libraries did not effectively promote software sharing, because most developers did not use the libraries. We concluded that weaker conditions might promote sharing better.

However, unrestricted linking of non-free programs would deprive the users of those programs of all benefit from the free status of the libraries themselves. This Library General Public License is intended to permit developers of non-free programs to use free libraries, while preserving your freedom as a user of such programs to change the free libraries that are incorporated in them. (We have not seen how to achieve this as regards changes in header files, but we have achieved it as regards changes in the actual functions of the Library.) The hope is that this will lead to faster development of free libraries.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, while the latter only works together with the library.

Note that it is possible for a library to be covered by the ordinary General Public License rather than by this special one.

痿・

GNU LIBRARY GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Library General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

痿・

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

痿・

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

痿・

6. As an exception to the Sections above, you may also compile or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit

modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

c) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

d) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

痿・

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your

rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

瘘・

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Library General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a

license version number, you may choose any version ever published by the Free Software Foundation.

痿・

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

痿・

Appendix: How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the library's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Library General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Library General Public License for more details.

You should have received a copy of the GNU Library General Public License along with this library; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA

Also add information on how to contact you by electronic and paper mail.

```
You should also get your employer (if you work as a programmer) or your
school, if any, to sign a "copyright disclaimer" for the library, if
necessary.  Here is a sample; alter the names:

  Yoyodyne, Inc., hereby disclaims all copyright interest in the
  library `Frob' (a library for tweaking knobs) written by James Random Hacker.

  <signature of Ty Coon>, 1 April 1990
  Ty Coon, President of Vice

That's all there is to it!
--------------------------------------------------------------------------------
---
[liblmdb 0.9.70]
[COPYRIGHT]
Copyright 2011-2021 Howard Chu, Symas Corp.
All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted only as authorized by the OpenLDAP
Public License.

A copy of this license is available in the file LICENSE in the
top-level directory of the distribution or, alternatively, at
<http://www.OpenLDAP.org/license.html>.

OpenLDAP is a registered trademark of the OpenLDAP Foundation.

Individual files and/or contributed packages may be copyright by
other parties and/or subject to additional restrictions.

This work also contains materials derived from public sources.

Additional information about OpenLDAP can be obtained at
<http://www.openldap.org/>.

[LICENSE]
The OpenLDAP Public License
  Version 2.8, 17 August 2003

Redistribution and use of this software and associated documentation
("Software"), with or without modification, are permitted provided
that the following conditions are met:

1. Redistributions in source form must retain copyright statements
   and notices,

2. Redistributions in binary form must reproduce applicable copyright
   statements and notices, this list of conditions, and the following
   disclaimer in the documentation and/or other materials provided
   with the distribution, and

3. Redistributions must contain a verbatim copy of this document.

The OpenLDAP Foundation may revise this license from time to time.
Each revision is distinguished by a version number.  You may use
this Software under terms of this license revision or under the
terms of any subsequent revision of the license.

THIS SOFTWARE IS PROVIDED BY THE OPENLDAP FOUNDATION AND ITS
CONTRIBUTORS ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES,
INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED.  IN NO EVENT
SHALL THE OPENLDAP FOUNDATION, ITS CONTRIBUTORS, OR THE AUTHOR(S)
OR OWNER(S) OF THE SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT,
INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING,
BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER
CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN
```

```
ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE
POSSIBILITY OF SUCH DAMAGE.

The names of the authors and copyright holders must not be used in
advertising or otherwise to promote the sale, use or other dealing
in this Software without specific, written prior permission.  Title
to copyright in this Software shall at all times remain with copyright
holders.

OpenLDAP is a registered trademark of the OpenLDAP Foundation.

Copyright 1999-2003 The OpenLDAP Foundation, Redwood City,
California, USA.  All Rights Reserved.  Permission to copy and
distribute verbatim copies of this document is granted.----------------------
-----------------------------------------------------------
[libssh2 1.8.0]
[COPYRIGHT]
  Copyright (c) 2004-2007 Sara Golemon <sarag@libssh2.org>
  Copyright (c) 2005,2006 Mikhail Gusarov <dottedmag@dottedmag.net>
  Copyright (c) 2006-2007 The Written Word, Inc.
  Copyright (c) 2007 Eli Fant <elifantu@mail.ru>
  Copyright (c) 2009 Daniel Stenberg
  Copyright (C) 2008, 2009 Simon Josefsson
  Copyright (c) 2000 Markus Friedl
  Copyright (c) 2015 Microsoft Corp.
  All rights reserved.

[LICENSE]
  Redistribution and use in source and binary forms,
  with or without modification, are permitted provided
  that the following conditions are met:

    Redistributions of source code must retain the above
    copyright notice, this list of conditions and the
    following disclaimer.

    Redistributions in binary form must reproduce the above
    copyright notice, this list of conditions and the following
    disclaimer in the documentation and/or other materials
    provided with the distribution.

    Neither the name of the copyright holder nor the names
    of any other contributors may be used to endorse or
    promote products derived from this software without
    specific prior written permission.

  THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND
  CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES,
  INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES
  OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
  ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR
  CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
  SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING,
  BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR
  SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS
  INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY,
  WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING
  NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE
  USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY
  OF SUCH DAMAGE.


------------------------------------------------------------------------
---
[liburcu 0.6.8]
[COPYRIGHT]
  Copyright (c) 2009 Mathieu Desnoyers <mathieu.desnoyers@efficios.com>
  Copyright (c) 2009 Paul E. McKenney, IBM Corporation.

[LICENSE]
```

This library is free software; you can redistribute it and/or
modify it under the terms of the GNU Lesser General Public
License as published by the Free Software Foundation; either
version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU
Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public
License along with this library; if not, write to the Free Software
Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

IBM's contributions to this file may be relicensed under LGPLv2 or later.

[lz4 r120]
LZ4 Library
Copyright (c) 2011-2020, Yann Collet
All rights reserved.

Redistribution and use in source and binary forms, with or without modification,
are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this
list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice,
this
list of conditions and the following disclaimer in the documentation and/or
other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND
ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED
WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE
DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE
FOR
ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES
(INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON
ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT
(INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS
SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

[moby 18.06.0-ce]

Apache License
Version 2.0, January 2004
https://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction,
and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by
the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all
other entities that control, are controlled by, or are under common
control with that entity. For the purposes of this definition,
"control" means (i) the power, direct or indirect, to cause the
direction or management of such entity, whether by contract or
otherwise, or (ii) ownership of fifty percent (50%) or more of the
outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You

meet the following conditions:

(a) You must give any other recipients of the Work or
Derivative Works a copy of this License; and

(b) You must cause any modified files to carry prominent notices
stating that You changed the files; and

(c) You must retain, in the Source form of any Derivative Works
that You distribute, all copyright, patent, trademark, and
attribution notices from the Source form of the Work,
excluding those notices that do not pertain to any part of
the Derivative Works; and

(d) If the Work includes a "NOTICE" text file as part of its
distribution, then any Derivative Works that You distribute must
include a readable copy of the attribution notices contained
within such NOTICE file, excluding those notices that do not
pertain to any part of the Derivative Works, in at least one
of the following places: within a NOTICE text file distributed
as part of the Derivative Works; within the Source form or
documentation, if provided along with the Derivative Works; or,
within a display generated by the Derivative Works, if and
wherever such third-party notices normally appear. The contents
of the NOTICE file are for informational purposes only and
do not modify the License. You may add Your own attribution
notices within Derivative Works that You distribute, alongside
or as an addendum to the NOTICE text from the Work, provided
that such additional attribution notices cannot be construed
as modifying the License.

You may add Your own copyright statement to Your modifications and
may provide additional or different license terms and conditions
for use, reproduction, or distribution of Your modifications, or
for any such Derivative Works as a whole, provided Your use,
reproduction, and distribution of the Work otherwise complies with
the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise,
any Contribution intentionally submitted for inclusion in the Work
by You to the Licensor shall be under the terms and conditions of
this License, without any additional terms or conditions.
Notwithstanding the above, nothing herein shall supersede or modify
the terms of any separate license agreement you may have executed
with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade
names, trademarks, service marks, or product names of the Licensor,
except as required for reasonable and customary use in describing the
origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or
agreed to in writing, Licensor provides the Work (and each
Contributor provides its Contributions) on an "AS IS" BASIS,
WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or
implied, including, without limitation, any warranties or conditions
of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A
PARTICULAR PURPOSE. You are solely responsible for determining the
appropriateness of using or redistributing the Work and assume any
risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory,
whether in tort (including negligence), contract, or otherwise,
unless required by applicable law (such as deliberate and grossly
negligent acts) or agreed to in writing, shall any Contributor be
liable to You for damages, including any direct, indirect, special,
incidental, or consequential damages of any character arising as a
result of this License or out of the use or inability to use the
Work (including but not limited to damages for loss of goodwill,
work stoppage, computer failure or malfunction, or any and all

```
      other commercial damages or losses), even if such Contributor
      has been advised of the possibility of such damages.

   9. Accepting Warranty or Additional Liability. While redistributing
      the Work or Derivative Works thereof, You may choose to offer,
      and charge a fee for, acceptance of support, warranty, indemnity,
      or other liability obligations and/or rights consistent with this
      License. However, in accepting such obligations, You may act only
      on Your own behalf and on Your sole responsibility, not on behalf
      of any other Contributor, and only if You agree to indemnify,
      defend, and hold each Contributor harmless for any liability
      incurred by, or claims asserted against, such Contributor by reason
      of your accepting any such warranty or additional liability.

   END OF TERMS AND CONDITIONS

   Copyright 2013-2018 Docker, Inc.

   Licensed under the Apache License, Version 2.0 (the "License");
   you may not use this file except in compliance with the License.
   You may obtain a copy of the License at

       https://www.apache.org/licenses/LICENSE-2.0

   Unless required by applicable law or agreed to in writing, software
   distributed under the License is distributed on an "AS IS" BASIS,
   WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
   See the License for the specific language governing permissions and
   limitations under the License.

NOTICE

Docker
Copyright 2012-2017 Docker, Inc.

This product includes software developed at Docker, Inc.
(https://www.docker.com).

This product contains software (https://github.com/kr/pty) developed
by Keith Rarick, licensed under the MIT License.

The following is courtesy of our legal counsel:


Use and transfer of Docker may be subject to certain restrictions by the
United States and other governments.
It is your responsibility to ensure that your use and/or transfer does not
violate applicable laws.

For more information, please see https://www.bis.doc.gov

See also https://www.apache.org/dev/crypto.html and/or seek legal counsel.

--------------------------------------------------------------------------
---
[multiselect 0.9.5]
[COPYRIGHT]
  Copyright (c) 2012 Louis Cuny

[LICENSE]
            DO WHAT THE FUCK YOU WANT TO PUBLIC LICENSE
                    Version 2, December 2004

 Copyright (C) 2004 Sam Hocevar <sam@hocevar.net>

 Everyone is permitted to copy and distribute verbatim or modified
 copies of this license document, and changing it is allowed as long
 as the name is changed.

            DO WHAT THE FUCK YOU WANT TO PUBLIC LICENSE
```

```
   TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

  0. You just DO WHAT THE FUCK YOU WANT TO.
------------------------------------------------------------------------
---
[nanomsg 1.0.0]

Permission is hereby granted, free of charge, to any person obtaining a copy
of this software and associated documentation files (the "Software"),
to deal in the Software without restriction, including without limitation
the rights to use, copy, modify, merge, publish, distribute, sublicense,
and/or sell copies of the Software, and to permit persons to whom
the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included
in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL
THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER
LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING
FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS
IN THE SOFTWARE.

"nanomsg" is a trademark of Martin Sustrik
------------------------------------------------------------------------
---
[ncurses 5.7]
[COPYRIGHT]
  Copyright (c) 1998-2004,2006 Free Software Foundation, Inc.

[LICENSE]
--                                                                      -
-
-- Permission is hereby granted, free of charge, to any person obtaining a   -
-
-- copy of this software and associated documentation files (the             -
-
-- "Software"), to deal in the Software without restriction, including       -
-
-- without limitation the rights to use, copy, modify, merge, publish,       -
-
-- distribute, distribute with modifications, sublicense, and/or sell copies -
-
-- of the Software, and to permit persons to whom the Software is furnished  -
-
-- to do so, subject to the following conditions:                            -
-
--                                                                         -
-
-- The above copyright notice and this permission notice shall be included   -
-
-- in all copies or substantial portions of the Software.                    -
-
--                                                                         -
-
-- THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS   -
-
-- OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF                -
-
-- MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN -
-
-- NO EVENT SHALL THE ABOVE COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM,       -
-
-- DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR     -
-
-- OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE -
-
```

```
-- USE OR OTHER DEALINGS IN THE SOFTWARE.                                -
-
--                                                                       -
-
-- Except as contained in this notice, the name(s) of the above copyright    -
-
-- holders shall not be used in advertising or otherwise to promote the      -
-
-- sale, use or other dealings in this Software without prior written        -
-
-- authorization.                                                           -
-
--------------------------------------------------------------------------
---
[net-snmp 5.4.3]
Various copyrights apply to this package, listed in various separate
parts below.  Please make sure that you read all the parts.

---- Part 1: CMU/UCD copyright notice: (BSD like) -----


       Copyright 1989, 1991, 1992 by Carnegie Mellon University

        Derivative Work - 1996, 1998-2000
Copyright 1996, 1998-2000 The Regents of the University of California

           All Rights Reserved

Permission to use, copy, modify and distribute this software and its
documentation for any purpose and without fee is hereby granted,
provided that the above copyright notice appears in all copies and
that both that copyright notice and this permission notice appear in
supporting documentation, and that the name of CMU and The Regents of
the University of California not be used in advertising or publicity
pertaining to distribution of the software without specific written
permission.

CMU AND THE REGENTS OF THE UNIVERSITY OF CALIFORNIA DISCLAIM ALL
WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED
WARRANTIES OF MERCHANTABILITY AND FITNESS.  IN NO EVENT SHALL CMU OR
THE REGENTS OF THE UNIVERSITY OF CALIFORNIA BE LIABLE FOR ANY SPECIAL,
INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING
FROM THE LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF
CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN
CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.


---- Part 2: Networks Associates Technology, Inc copyright notice (BSD) -----

Copyright (c) 2001-2003, Networks Associates Technology, Inc
All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions are met:

*  Redistributions of source code must retain the above copyright notice,
   this list of conditions and the following disclaimer.

*  Redistributions in binary form must reproduce the above copyright
   notice, this list of conditions and the following disclaimer in the
   documentation and/or other materials provided with the distribution.

*  Neither the name of the Networks Associates Technology, Inc nor the
   names of its contributors may be used to endorse or promote
   products derived from this software without specific prior written
   permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS
IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO,
THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
```

PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 3: Cambridge Broadband Ltd. copyright notice (BSD) -----

Portions of this code are copyright (c) 2001-2003, Cambridge Broadband Ltd. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* The name of Cambridge Broadband Ltd. may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 4: Sun Microsystems, Inc. copyright notice (BSD) -----

Copyright (c) 2003 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A. All rights reserved.

Use is subject to license terms below.

This distribution may include materials developed by third parties.

Sun, Sun Microsystems, the Sun logo and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of the Sun Microsystems, Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO,

THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 5: Sparta, Inc copyright notice (BSD) -----

Copyright (c) 2003-2010, Sparta, Inc
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of Sparta, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 6: Cisco/BUPTNIC copyright notice (BSD) -----

Copyright (c) 2004, Cisco, Inc and Information Network
Center of Beijing University of Posts and Telecommunications.
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of Cisco, Inc, Beijing University of Posts and Telecommunications, nor the names of their contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY,

WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 7: Fabasoft R&D Software GmbH & Co KG copyright notice (BSD) -----

Copyright (c) Fabasoft R&D Software GmbH & Co KG, 2003
oss@fabasoft.com
Author: Bernhard Penz <bernhard.penz@fabasoft.com>

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* The name of Fabasoft R&D Software GmbH & Co KG or any of its subsidiaries, brand or product names may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

[net-snmp 5.9.1]
Various copyrights apply to Netsnmp 5.9.1 package, listed in various separate parts below:
---- Part 1: CMU/UCD copyright notice: (BSD like) -----

Copyright 1989, 1991, 1992 by Carnegie Mellon University

Derivative Work - 1996, 1998-2000
Copyright 1996, 1998-2000 The Regents of the University of California

All Rights Reserved

Permission to use, copy, modify and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appears in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of CMU and The Regents of the University of California not be used in advertising or publicity pertaining to distribution of the software without specific written permission.

CMU AND THE REGENTS OF THE UNIVERSITY OF CALIFORNIA DISCLAIM ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL CMU OR THE REGENTS OF THE UNIVERSITY OF CALIFORNIA BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM THE LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

---- Part 2: Networks Associates Technology, Inc copyright notice (BSD) -----

Copyright (c) 2001-2003, Networks Associates Technology, Inc
All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice,
  this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright
  notice, this list of conditions and the following disclaimer in the
  documentation and/or other materials provided with the distribution.

* Neither the name of the Networks Associates Technology, Inc nor the
  names of its contributors may be used to endorse or promote
  products derived from this software without specific prior written
  permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS
IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO,
THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR
CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL,
EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,
PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS;
OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY,
WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR
OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF
ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 3: Cambridge Broadband Ltd. copyright notice (BSD) -----

Portions of this code are copyright (c) 2001-2003, Cambridge Broadband Ltd.
All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice,
  this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright
  notice, this list of conditions and the following disclaimer in the
  documentation and/or other materials provided with the distribution.

* The name of Cambridge Broadband Ltd. may not be used to endorse or
  promote products derived from this software without specific prior
  written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER ``AS IS'' AND ANY
EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE
LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF
SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR
BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY,
WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE
OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN
IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 4: Sun Microsystems, Inc. copyright notice (BSD) -----

Copyright (c) 2003 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara,
California 95054, U.S.A. All rights reserved.

Use is subject to license terms below.

This distribution may include materials developed by third parties.

Sun, Sun Microsystems, the Sun logo and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of the Sun Microsystems, Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 5: Sparta, Inc copyright notice (BSD) -----

Copyright (c) 2003-2013, Sparta, Inc
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of Sparta, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 6: Cisco/BUPTNIC copyright notice (BSD) -----

Copyright (c) 2004, Cisco, Inc and Information Network
Center of Beijing University of Posts and Telecommunications.
All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice,
  this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright
  notice, this list of conditions and the following disclaimer in the
  documentation and/or other materials provided with the distribution.

* Neither the name of Cisco, Inc, Beijing University of Posts and
  Telecommunications, nor the names of their contributors may
  be used to endorse or promote products derived from this software
  without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS
IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO,
THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR
CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL,
EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,
PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS;
OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY,
WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR
OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF
ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 7: Fabasoft R&D Software GmbH & Co KG copyright notice (BSD) -----

Copyright (c) Fabasoft R&D Software GmbH & Co KG, 2003
oss@fabasoft.com
Author: Bernhard Penz <bernhard.penz@fabasoft.com>

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice,
  this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright
  notice, this list of conditions and the following disclaimer in the
  documentation and/or other materials provided with the distribution.

* The name of Fabasoft R&D Software GmbH & Co KG or any of its subsidiaries,
  brand or product names may not be used to endorse or promote products
  derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER ``AS IS'' AND ANY
EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE
LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF
SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR
BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY,
WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE
OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN
IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 8: Apple Inc. copyright notice (BSD) -----

Copyright (c) 2007 Apple Inc. All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:

1. Redistributions of source code must retain the above copyright
notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above

copyright notice, this list of conditions and the following
disclaimer in the documentation and/or other materials provided
with the distribution.
3. Neither the name of Apple Inc. ("Apple") nor the names of its
contributors may be used to endorse or promote products derived
from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY APPLE AND ITS CONTRIBUTORS "AS IS" AND
ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO,
THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A
PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL APPLE OR ITS
CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT
LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF
USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND
ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY,
OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT
OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
SUCH DAMAGE.

---- Part 9: ScienceLogic, LLC copyright notice (BSD) -----

Copyright (c) 2009, ScienceLogic, LLC
All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions are
met:

* Redistributions of source code must retain the above copyright notice,
  this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright
  notice, this list of conditions and the following disclaimer in the
  documentation and/or other materials provided with the distribution.

* Neither the name of ScienceLogic, LLC nor the names of its
  contributors may be used to endorse or promote products derived
  from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS
``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT
LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR
A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT
HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT,
INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING,
BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS
OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND
ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR
TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE
USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH
DAMAGE.

---- Part 10: Lennart Poettering copyright notice (BSD-like) -----

Copyright 2010 Lennart Poettering

Permission is hereby granted, free of charge, to any person
obtaining a copy of this software and associated documentation files
(the "Software"), to deal in the Software without restriction,
including without limitation the rights to use, copy, modify, merge,
publish, distribute, sublicense, and/or sell copies of the Software,
and to permit persons to whom the Software is furnished to do so,
subject to the following conditions:

The above copyright notice and this permission notice shall be
included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND,
EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF

MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND
NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS
BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN
ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN
CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE
SOFTWARE.

---- Part 11: IETF copyright notice (BSD) -----

Copyright (c) 2013 IETF Trust and the persons identified as authors of
the code. All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions are
met:

* Redistributions of source code must retain the above copyright notice,
this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright
notice, this list of conditions and the following disclaimer in the
documentation and/or other materials provided with the distribution.

* Neither the name of Internet Society, IETF or IETF Trust, nor the
names of specific contributors, may be used to endorse or promote
products derived from this software without specific prior written
permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS
IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED
TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A
PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER
OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL,
EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,
PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR
PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF
LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING
NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS
SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 12: Arista Networks copyright notice (BSD) ----

Copyright (c) 2013, Arista Networks, Inc.
All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions are
met:

* Redistributions of source code must retain the above copyright notice,
this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright
notice, this list of conditions and the following disclaimer in the
documentation and/or other materials provided with the distribution.

* Neither the name of Arista Networks, Inc. nor the names of its
contributors may be used to endorse or promote products derived
from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS
``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT
LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR
A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT
HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT,
INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING,
BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS
OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND
ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR
TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE

USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH
DAMAGE.

---- Part 13: VMware, Inc. copyright notice (BSD) -----

Copyright (c) 2016, VMware, Inc.
All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice,
  this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright
  notice, this list of conditions and the following disclaimer in the
  documentation and/or other materials provided with the distribution.

* Neither the name of VMware, Inc. nor the names of its contributors
  may be used to endorse or promote products derived from this software
  without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS
IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO,
THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR
CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL,
EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,
PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS;
OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY,
WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR
OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF
ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 14: USC/Information Sciences Institute copyright notice (BSD) -----

Copyright (c) 2017-2018, Information Sciences Institute
All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice,
  this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright
  notice, this list of conditions and the following disclaimer in the
  documentation and/or other materials provided with the distribution.

* Neither the name of Information Sciences Institue nor the names of its
  contributors may be used to endorse or promote products derived from
  this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS
IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO,
THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR
CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL,
EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,
PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS;
OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY,
WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR
OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF
ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

[ntp 4.2 6p2-RC4]
This file is automatically generated from html/copyright.html

  Copyright Notice

jpg "Clone me," says Dolly sheepishly.

Last update: 11-May-2010 04:41 UTC

The following copyright notice applies to all files collectively called the Network Time Protocol Version 4 Distribution. Unless specifically declared otherwise in an individual file, this notice applies as if the text was explicitly included in the file.

```
*************************************************************************
*                                                                       *
* Copyright (c) University of Delaware 1992-2010                        *
*                                                                       *
* Permission to use, copy, modify, and distribute this software and     *
* its documentation for any purpose with or without fee is hereby       *
* granted, provided that the above copyright notice appears in all      *
* copies and that both the copyright notice and this permission         *
* notice appear in supporting documentation, and that the name          *
* University of Delaware not be used in advertising or publicity        *
* pertaining to distribution of the software without specific,          *
* written prior permission. The University of Delaware makes no         *
* representations about the suitability this software for any           *
* purpose. It is provided "as is" without express or implied            *
* warranty.                                                             *
*                                                                       *
*************************************************************************
```

The following individuals contributed in part to the Network Time Protocol Distribution Version 4 and are acknowledged as authors of this work.

1. [1]Mark Andrews <mark_andrews@isc.org> Leitch atomic clock controller
2. [2]Bernd Altmeier <altmeier@atlsoft.de> hopf Elektronik serial line and PCI-bus devices
3. [3]Viraj Bais <vbais@mailman1.intel.com> and [4]Clayton Kirkwood <kirkwood@striderfm.intel.com> port to WindowsNT 3.5
4. [5]Michael Barone <michael,barone@lmco.com> GPSVME fixes
5. [6]Karl Berry <karl@owl.HQ.ileaf.com> syslog to file option
6. [7]Greg Brackley <greg.brackley@bigfoot.com> Major rework of WINNT port. Clean up recvbuf and iosignal code into separate modules.
7. [8]Marc Brett <Marc.Brett@westgeo.com> Magnavox GPS clock driver
8. [9]Piete Brooks <Piete.Brooks@cl.cam.ac.uk> MSF clock driver, Trimble PARSE support
9. [10]Nelson B Bolyard <nelson@bolyard.me> update and complete broadcast and crypto features in sntp
10. [11]Jean-Francois Boudreault <Jean-Francois.Boudreault@viagenie.qc.ca> IPv6 support
11. [12]Reg Clemens <reg@dwf.com> Oncore driver (Current maintainer)
12. [13]Steve Clift <clift@ml.csiro.au> OMEGA clock driver
13. [14]Casey Crellin <casey@csc.co.za> vxWorks (Tornado) port and help with target configuration
14. [15]Sven Dietrich <sven_dietrich@trimble.com> Palisade reference clock driver, NT adj. residuals, integrated Greg's Winnt port.
15. [16]John A. Dundas III <dundas@salt.jpl.nasa.gov> Apple A/UX port
16. [17]Torsten Duwe <duwe@immd4.informatik.uni-erlangen.de> Linux port
17. [18]Dennis Ferguson <dennis@mrbill.canet.ca> foundation code for NTP Version 2 as specified in RFC-1119
18. [19]John Hay <jhay@icomtek.csir.co.za> IPv6 support and testing
19. [20]Dave Hart <davehart@davehart.com> General maintenance, Windows port interpolation rewrite
20. [21]Claas Hilbrecht <neoclock4x@linum.com> NeoClock4X clock driver
21. [22]Glenn Hollinger <glenn@herald.usask.ca> GOES clock driver
22. [23]Mike Iglesias <iglesias@uci.edu> DEC Alpha port
23. [24]Jim Jagielski <jim@jagubox.gsfc.nasa.gov> A/UX port
24. [25]Jeff Johnson <jbj@chatham.usdesign.com> massive prototyping overhaul
25. [26]Hans Lambermont <Hans.Lambermont@nl.origin-it.com> or [27]<H.Lambermont@chello.nl> ntpsweep

26. [28]Poul-Henning Kamp <phk@FreeBSD.ORG> Oncore driver (Original author)
27. [29]Frank Kardel [30]<kardel (at) ntp (dot) org> PARSE <GENERIC> driver (>14 reference clocks), STREAMS modules for PARSE, support scripts, syslog cleanup, dynamic interface handling
28. [31]William L. Jones <jones@hermes.chpc.utexas.edu> RS/6000 AIX modifications, HPUX modifications
29. [32]Dave Katz <dkatz@cisco.com> RS/6000 AIX port
30. [33]Craig Leres <leres@ee.lbl.gov> 4.4BSD port, ppsclock, Magnavox GPS clock driver
31. [34]George Lindholm <lindholm@ucs.ubc.ca> SunOS 5.1 port
32. [35]Louis A. Mamakos <louie@ni.umd.edu> MD5-based authentication
33. [36]Lars H. Mathiesen <thorinn@diku.dk> adaptation of foundation code for Version 3 as specified in RFC-1305
34. [37]Danny Mayer <mayer@ntp.org>Network I/O, Windows Port, Code Maintenance
35. [38]David L. Mills <mills@udel.edu> Version 4 foundation: clock discipline, authentication, precision kernel; clock drivers: Spectracom, Austron, Arbiter, Heath, ATOM, ACTS, KSI/Odetics; audio clock drivers: CHU, WWV/H, IRIG
36. [39]Wolfgang Moeller <moeller@gwdgv1.dnet.gwdg.de> VMS port
37. [40]Jeffrey Mogul <mogul@pa.dec.com> ntptrace utility
38. [41]Tom Moore <tmoore@fievel.daytonoh.ncr.com> i386 svr4 port
39. [42]Kamal A Mostafa <kamal@whence.com> SCO OpenServer port
40. [43]Derek Mulcahy <derek@toybox.demon.co.uk> and [44]Damon Hart-Davis <d@hd.org> ARCRON MSF clock driver
41. [45]Rob Neal <neal@ntp.org> Bancomm refclock and config/parse code maintenance
42. [46]Rainer Pruy <Rainer.Pruy@informatik.uni-erlangen.de> monitoring/trap scripts, statistics file handling
43. [47]Dirce Richards <dirce@zk3.dec.com> Digital UNIX V4.0 port
44. [48]Wilfredo S nchez <wsanchez@apple.com> added support for NetInfo
45. [49]Nick Sayer <mrapple@quack.kfu.com> SunOS streams modules
46. [50]Jack Sasportas <jack@innovativeinternet.com> Saved a Lot of space on the stuff in the html/pic/ subdirectory
47. [51]Ray Schnitzler <schnitz@unipress.com> Unixware1 port
48. [52]Michael Shields <shields@tembel.org> USNO clock driver
49. [53]Jeff Steinman <jss@pebbles.jpl.nasa.gov> Datum PTS clock driver
50. [54]Harlan Stenn <harlan@pfcs.com> GNU automake/autoconfigure makeover, various other bits (see the ChangeLog)
51. [55]Kenneth Stone <ken@sdd.hp.com> HP-UX port
52. [56]Ajit Thyagarajan <ajit@ee.udel.edu>IP multicast/anycast support
53. [57]Tomoaki TSURUOKA <tsuruoka@nc.fukuoka-u.ac.jp>TRAK clock driver
54. [58]Paul A Vixie <vixie@vix.com> TrueTime GPS driver, generic TrueTime clock driver
55. [59]Ulrich Windl <Ulrich.Windl@rz.uni-regensburg.de> corrected and validated HTML documents according to the HTML DTD

References

1. mailto:%20mark_andrews@isc.org
2. mailto:%20altmeier@atlsoft.de
3. mailto:%20vbais@mailman1.intel.co
4. mailto:%20kirkwood@striderfm.intel.com
5. mailto:%20michael.barone@lmco.com
6. mailto:%20karl@owl.HQ.ileaf.com
7. mailto:%20greg.brackley@bigfoot.com
8. mailto:%20Marc.Brett@westgeo.com
9. mailto:%20Piete.Brooks@cl.cam.ac.uk
10. mailto:%20nelson@bolyard.me
11. mailto:%20Jean-Francois.Boudreault@viagenie.qc.ca
12. mailto:%20reg@dwf.com
13. mailto:%20clift@ml.csiro.au
14. mailto:casey@csc.co.za
15. mailto:%20Sven_Dietrich@trimble.COM

16. mailto:%20dundas@salt.jpl.nasa.gov
17. mailto:%20duwe@immd4.informatik.uni-erlangen.de
18. mailto:%20dennis@mrbill.canet.ca
19. mailto:%20jhay@icomtek.csir.co.za
20. mailto:%20davehart@davehart.com
21. mailto:%20neoclock4x@linum.com
22. mailto:%20glenn@herald.usask.ca
23. mailto:%20iglesias@uci.edu
24. mailto:%20jagubox.gsfc.nasa.gov
25. mailto:%20jbj@chatham.usdesign.com
26. mailto:Hans.Lambermont@nl.origin-it.com
27. mailto:H.Lambermont@chello.nl
28. mailto:%20phk@FreeBSD.ORG
29. http://www4.informatik.uni-erlangen.de/%7ekardel
30. mailto:%20kardel(at)ntp(dot)org
31. mailto:%20jones@hermes.chpc.utexas.edu
32. mailto:%20dkatz@cisco.com
33. mailto:%20leres@ee.lbl.gov
34. mailto:%20lindholm@ucs.ubc.ca
35. mailto:%20louie@ni.umd.edu
36. mailto:%20thorinn@diku.dk
37. mailto:%20mayer@ntp.org
38. mailto:%20mills@udel.edu
39. mailto:%20moeller@gwdgv1.dnet.gwdg.de
40. mailto:%20mogul@pa.dec.com
41. mailto:%20tmoore@fievel.daytonoh.ncr.com
42. mailto:%20kamal@whence.com
43. mailto:%20derek@toybox.demon.co.uk
44. mailto:%20d@hd.org
45. mailto:%20neal@ntp.org
46. mailto:%20Rainer.Pruy@informatik.uni-erlangen.de
47. mailto:%20dirce@zk3.dec.com
48. mailto:%20wsanchez@apple.com
49. mailto:%20mrapple@quack.kfu.com
50. mailto:%20jack@innovativeinternet.com
51. mailto:%20schnitz@unipress.com
52. mailto:%20shields@tembel.org
53. mailto:%20pebbles.jpl.nasa.gov
54. mailto:%20harlan@pfcs.com
55. mailto:%20ken@sdd.hp.com
56. mailto:%20ajit@ee.udel.edu
57. mailto:%20tsuruoka@nc.fukuoka-u.ac.jp
58. mailto:%20vixie@vix.com
59. mailto:%20Ulrich.Windl@rz.uni-regensburg.de

[openldap 2.4.45]
[COPYRIGHT]
Copyright 1998-2017 The OpenLDAP Foundation
All rights reserved.

[NOTE]
Redistribution and use in source and binary forms, with or without
modification, are permitted only as authorized by the OpenLDAP
Public License.

A copy of this license is available in the file LICENSE in the
top-level directory of the distribution or, alternatively, at
<http://www.OpenLDAP.org/license.html>.

OpenLDAP is a registered trademark of the OpenLDAP Foundation.

Individual files and/or contributed packages may be copyright by
other parties and/or subject to additional restrictions.

This work is derived from the University of Michigan LDAP v3.3
distribution. Information concerning this software is available
at <http://www.umich.edu/~dirsvcs/ldap/ldap.html>.

This work also contains materials derived from public sources.

```
Additional information about OpenLDAP can be obtained at
<http://www.openldap.org/>.

---

Portions Copyright 1998-2012 Kurt D. Zeilenga.
Portions Copyright 1998-2006 Net Boolean Incorporated.
Portions Copyright 2001-2006 IBM Corporation.
All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted only as authorized by the OpenLDAP
Public License.

---

Portions Copyright 1999-2008 Howard Y.H. Chu.
Portions Copyright 1999-2008 Symas Corporation.
Portions Copyright 1998-2003 Hallvard B. Furuseth.
Portions Copyright 2007-2011 Gavin Henry.
Portions Copyright 2007-2011 Suretec Systems Ltd.
All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that this notice is preserved.
The names of the copyright holders may not be used to endorse or
promote products derived from this software without their specific
prior written permission.  This software is provided ``as is''
without express or implied warranty.

---

Portions Copyright (c) 1992-1996 Regents of the University of Michigan.
All rights reserved.

Redistribution and use in source and binary forms are permitted
provided that this notice is preserved and that due credit is given
to the University of Michigan at Ann Arbor.  The name of the
University may not be used to endorse or promote products derived
from this software without specific prior written permission.  This
software is provided ``as is'' without express or implied warranty.

[LICENSE]
The OpenLDAP Public License
  Version 2.8, 17 August 2003

Redistribution and use of this software and associated documentation
("Software"), with or without modification, are permitted provided
that the following conditions are met:

1. Redistributions in source form must retain copyright statements
   and notices,

2. Redistributions in binary form must reproduce applicable copyright
   statements and notices, this list of conditions, and the following
   disclaimer in the documentation and/or other materials provided
   with the distribution, and

3. Redistributions must contain a verbatim copy of this document.

The OpenLDAP Foundation may revise this license from time to time.
Each revision is distinguished by a version number.  You may use
this Software under terms of this license revision or under the
terms of any subsequent revision of the license.

THIS SOFTWARE IS PROVIDED BY THE OPENLDAP FOUNDATION AND ITS
CONTRIBUTORS ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES,
INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED.  IN NO EVENT
```

SHALL THE OPENLDAP FOUNDATION, ITS CONTRIBUTORS, OR THE AUTHOR(S)
OR OWNER(S) OF THE SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT,
INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING,
BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER
CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN
ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE
POSSIBILITY OF SUCH DAMAGE.

The names of the authors and copyright holders must not be used in
advertising or otherwise to promote the sale, use or other dealing
in this Software without specific, written prior permission. Title
to copyright in this Software shall at all times remain with copyright
holders.

OpenLDAP is a registered trademark of the OpenLDAP Foundation.

Copyright 1999-2003 The OpenLDAP Foundation, Redwood City,
California, USA. All Rights Reserved. Permission to copy and
distribute verbatim copies of this document is granted.

[opennhrp0.14.1]
Copyright (c) 2007-2012 Timo Ter辰s

Permission is hereby granted, free of charge, to any person obtaining a copy
of this software and associated documentation files (the "Software"), to deal
in the Software without restriction, including without limitation the rights
to use, copy, modify, merge, publish, distribute, sublicense, and/or sell
copies of the Software, and to permit persons to whom the Software is
furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in
all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE
AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER
LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,
OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN
THE SOFTWARE.

[openpam 20071221]
[COPYRIGHT]
Copyright (c) 2002-2003 Networks Associates Technology, Inc.
Copyright (c) 2004-2007 Dag-Erling Sm淡rgrav
All rights reserved.

[LICENSE]
This software was developed for the FreeBSD Project by ThinkSec AS and
Network Associates Laboratories, the Security Research Division of
Network Associates, Inc. under DARPA/SPAWAR contract N66001-01-C-8035
("CBOSS"), as part of the DARPA CHATS research program.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:
1. Redistributions of source code must retain the above copyright
   notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright
   notice, this list of conditions and the following disclaimer in the
   documentation and/or other materials provided with the distribution.
3. The name of the author may not be used to endorse or promote
   products derived from this software without specific prior written
   permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS ``AS IS'' AND

```
ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
ARE DISCLAIMED.  IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
SUCH DAMAGE.

--------------------------------------------------------------------------
---
[openssh 5.3p1]
The licences which components of this software fall under are as
follows.  First, we will summarize and say that all components
are under a BSD licence, or a licence more free than that.

OpenSSH contains no GPL code.

1)
     * Copyright (c) 1995 Tatu Ylonen <ylo@cs.hut.fi>, Espoo, Finland
     *                    All rights reserved
     *
     * As far as I am concerned, the code I have written for this software
     * can be used freely for any purpose.  Any derived versions of this
     * software must be clearly marked as such, and if the derived work is
     * incompatible with the protocol description in the RFC file, it must be
     * called by a name other than "ssh" or "Secure Shell".

    [Tatu continues]
     *  However, I am not implying to give any licenses to any patents or
     * copyrights held by third parties, and the software includes parts that
     * are not under my direct control.  As far as I know, all included
     * source code is used in accordance with the relevant license agreements
     * and can be used freely for any purpose (the GNU license being the most
     * restrictive); see below for details.

    [However, none of that term is relevant at this point in time.  All of
    these restrictively licenced software components which he talks about
    have been removed from OpenSSH, i.e.,

     - RSA is no longer included, found in the OpenSSL library
     - IDEA is no longer included, its use is deprecated
     - DES is now external, in the OpenSSL library
     - GMP is no longer used, and instead we call BN code from OpenSSL
     - Zlib is now external, in a library
     - The make-ssh-known-hosts script is no longer included
     - TSS has been removed
     - MD5 is now external, in the OpenSSL library
     - RC4 support has been replaced with ARC4 support from OpenSSL
     - Blowfish is now external, in the OpenSSL library

    [The licence continues]

    Note that any information and cryptographic algorithms used in this
    software are publicly available on the Internet and at any major
    bookstore, scientific library, and patent office worldwide.  More
    information can be found e.g. at "http://www.cs.hut.fi/crypto".

    The legal status of this program is some combination of all these
    permissions and restrictions.  Use only at your own responsibility.
    You will be responsible for any legal consequences yourself; I am not
    making any claims whether possessing or using this is legal or not in
    your country, and I am not taking any responsibility on your behalf.


              NO WARRANTY

    BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY
```

FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

2)

The 32-bit CRC compensation attack detector in deattack.c was contributed by CORE SDI S.A. under a BSD-style license.

```
 * Cryptographic attack detector for ssh - source code
 *
 * Copyright (c) 1998 CORE SDI S.A., Buenos Aires, Argentina.
 *
 * All rights reserved. Redistribution and use in source and binary
 * forms, with or without modification, are permitted provided that
 * this copyright notice is retained.
 *
 * THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESS OR IMPLIED
 * WARRANTIES ARE DISCLAIMED. IN NO EVENT SHALL CORE SDI S.A. BE
 * LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY OR
 * CONSEQUENTIAL DAMAGES RESULTING FROM THE USE OR MISUSE OF THIS
 * SOFTWARE.
 *
 * Ariel Futoransky <futo@core-sdi.com>
 * <http://www.core-sdi.com>
```

3)

ssh-keyscan was contributed by David Mazieres under a BSD-style license.

```
 * Copyright 1995, 1996 by David Mazieres <dm@lcs.mit.edu>.
 *
 * Modification and redistribution in source and binary forms is
 * permitted provided that due credit is given to the author and the
 * OpenBSD project by leaving this copyright notice intact.
```

4)

The Rijndael implementation by Vincent Rijmen, Antoon Bosselaers and Paulo Barreto is in the public domain and distributed with the following license:

```
 * @version 3.0 (December 2000)
 *
 * Optimised ANSI C code for the Rijndael cipher (now AES)
 *
 * @author Vincent Rijmen <vincent.rijmen@esat.kuleuven.ac.be>
 * @author Antoon Bosselaers <antoon.bosselaers@esat.kuleuven.ac.be>
 * @author Paulo Barreto <paulo.barreto@terra.com.br>
 *
 * This code is hereby placed in the public domain.
 *
 * THIS SOFTWARE IS PROVIDED BY THE AUTHORS ''AS IS'' AND ANY EXPRESS
 * OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED
 * WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
 * ARE DISCLAIMED.  IN NO EVENT SHALL THE AUTHORS OR CONTRIBUTORS BE
 * LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
```

```
     * CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF
     * SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR
     * BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY,
     * WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE
     * OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE,
     * EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
```

5)

One component of the ssh source code is under a 3-clause BSD license, held by the University of California, since we pulled these parts from original Berkeley code.

```
     * Copyright (c) 1983, 1990, 1992, 1993, 1995
     *      The Regents of the University of California.  All rights reserved.
     *
     * Redistribution and use in source and binary forms, with or without
     * modification, are permitted provided that the following conditions
     * are met:
     * 1. Redistributions of source code must retain the above copyright
     *    notice, this list of conditions and the following disclaimer.
     * 2. Redistributions in binary form must reproduce the above copyright
     *    notice, this list of conditions and the following disclaimer in the
     *    documentation and/or other materials provided with the distribution.
     * 3. Neither the name of the University nor the names of its contributors
     *    may be used to endorse or promote products derived from this software
     *    without specific prior written permission.
     *
     * THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND
     * ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
     * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE
     * ARE DISCLAIMED.  IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE
     * FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
CONSEQUENTIAL
     * DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
     * OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
     * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
STRICT
     * LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY
WAY
     * OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
     * SUCH DAMAGE.
```

6)

Remaining components of the software are provided under a standard 2-term BSD licence with the following names as copyright holders:

```
 Markus Friedl
 Theo de Raadt
 Niels Provos
 Dug Song
 Aaron Campbell
 Damien Miller
 Kevin Steves
 Daniel Kouril
 Wesley Griffin
 Per Allansson
 Nils Nordman
 Simon Wilkinson
```

Portable OpenSSH additionally includes code from the following copyright holders, also under the 2-term BSD license:

```
 Ben Lindstrom
 Tim Rice
 Andre Lucas
 Chris Adams
 Corinna Vinschen
 Cray Inc.
 Denis Parker
```

```
Gert Doering
Jakob Schlyter
Jason Downs
Juha Yrj 旦 l 辰
Michael Stone
Networks Associates Technology, Inc.
Solar Designer
Todd C. Miller
Wayne Schroeder
William Jones
Darren Tucker
Sun Microsystems
The SCO Group
Daniel Walsh

    * Redistribution and use in source and binary forms, with or without
    * modification, are permitted provided that the following conditions
    * are met:
    * 1. Redistributions of source code must retain the above copyright
    *    notice, this list of conditions and the following disclaimer.
    * 2. Redistributions in binary form must reproduce the above copyright
    *    notice, this list of conditions and the following disclaimer in the
    *    documentation and/or other materials provided with the distribution.
    *
    * THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS'' AND ANY EXPRESS OR
    * IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES
    * OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED.
    * IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT,
    * INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
    * NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF
USE,
    * DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY
    * THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT
    * (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE
OF
    * THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

8) Portable OpenSSH contains the following additional licenses:

    a) md5crypt.c, md5crypt.h

  * "THE BEER-WARE LICENSE" (Revision 42):
  * <phk@login.dknet.dk> wrote this file.  As long as you retain this
  * notice you can do whatever you want with this stuff. If we meet
  * some day, and you think this stuff is worth it, you can buy me a
  * beer in return.   Poul-Henning Kamp

    b) snprintf replacement

 * Copyright Patrick Powell 1995
 * This code is based on code written by Patrick Powell
 * (papowell@astart.com) It may be used for any purpose as long as this
 * notice remains intact on all source code distributions

    c) Compatibility code (openbsd-compat)

       Apart from the previously mentioned licenses, various pieces of code
       in the openbsd-compat/ subdirectory are licensed as follows:

       Some code is licensed under a 3-term BSD license, to the following
       copyright holders:

 Todd C. Miller
 Theo de Raadt
 Damien Miller
 Eric P. Allman
 The Regents of the University of California
 Constantin S. Svintsoff

 * Redistribution and use in source and binary forms, with or without
```

```
* modification, are permitted provided that the following conditions
* are met:
* 1. Redistributions of source code must retain the above copyright
*    notice, this list of conditions and the following disclaimer.
* 2. Redistributions in binary form must reproduce the above copyright
*    notice, this list of conditions and the following disclaimer in the
*    documentation and/or other materials provided with the distribution.
* 3. Neither the name of the University nor the names of its contributors
*    may be used to endorse or promote products derived from this software
*    without specific prior written permission.
*
* THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND
* ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
* ARE DISCLAIMED.  IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE
* FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
* DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
* OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
* LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
* OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
* SUCH DAMAGE.

     Some code is licensed under an ISC-style license, to the following
     copyright holders:

Internet Software Consortium.
Todd C. Miller
Reyk Floeter
Chad Mynhier

* Permission to use, copy, modify, and distribute this software for any
* purpose with or without fee is hereby granted, provided that the above
* copyright notice and this permission notice appear in all copies.
*
* THE SOFTWARE IS PROVIDED "AS IS" AND TODD C. MILLER DISCLAIMS ALL
* WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES
* OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL TODD C. MILLER BE LIABLE
* FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES
* WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION
* OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN
* CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

     Some code is licensed under a MIT-style license to the following
     copyright holders:

Free Software Foundation, Inc.

* Permission is hereby granted, free of charge, to any person obtaining a  *
* copy of this software and associated documentation files (the             *
* "Software"), to deal in the Software without restriction, including       *
* without limitation the rights to use, copy, modify, merge, publish,       *
* distribute, distribute with modifications, sublicense, and/or sell        *
* copies of the Software, and to permit persons to whom the Software is     *
* furnished to do so, subject to the following conditions:                  *
*                                                                           *
* The above copyright notice and this permission notice shall be included   *
* in all copies or substantial portions of the Software.                    *
*                                                                           *
* THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS   *
* OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF                *
* MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT.    *
* IN NO EVENT SHALL THE ABOVE COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM,    *
* DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR     *
* OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR     *
* THE USE OR OTHER DEALINGS IN THE SOFTWARE.                                *
*                                                                           *
* Except as contained in this notice, the name(s) of the above copyright    *
* holders shall not be used in advertising or otherwise to promote the      *
* sale, use or other dealings in this Software without prior written        *
```

```
 * authorization.                                                           *
 ***************************************************************************
/

--------------------------------------------------------------------------------
---
[openssl1.1.1l]

  LICENSE ISSUES
  ==============

  The OpenSSL toolkit stays under a double license, i.e. both the conditions
of
  the OpenSSL License and the original SSLeay license apply to the toolkit.
  See below for the actual license texts.

  OpenSSL License
  ---------------

/* ====================================================================
 * Copyright (c) 1998-2019 The OpenSSL Project.  All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 *
 * 1. Redistributions of source code must retain the above copyright
 *    notice, this list of conditions and the following disclaimer.
 *
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in
 *    the documentation and/or other materials provided with the
 *    distribution.
 *
 * 3. All advertising materials mentioning features or use of this
 *    software must display the following acknowledgment:
 *    "This product includes software developed by the OpenSSL Project
 *    for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
 *
 * 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
 *    endorse or promote products derived from this software without
 *    prior written permission. For written permission, please contact
 *    openssl-core@openssl.org.
 *
 * 5. Products derived from this software may not be called "OpenSSL"
 *    nor may "OpenSSL" appear in their names without prior written
 *    permission of the OpenSSL Project.
 *
 * 6. Redistributions of any form whatsoever must retain the following
 *    acknowledgment:
 *    "This product includes software developed by the OpenSSL Project
 *    for use in the OpenSSL Toolkit (http://www.openssl.org/)"
 *
 * THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
 * EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
 * PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE OpenSSL PROJECT OR
 * ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
 * SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
 * NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
 * LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
 * STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
 * ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
 * OF THE POSSIBILITY OF SUCH DAMAGE.
 * ====================================================================
 *
 * This product includes cryptographic software written by Eric Young
 * (eay@cryptsoft.com).  This product includes software written by Tim
 * Hudson (tjh@cryptsoft.com).
```

```
 *
 */

 Original SSLeay License
 -----------------------

/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
 * All rights reserved.
 *
 * This package is an SSL implementation written
 * by Eric Young (eay@cryptsoft.com).
 * The implementation was written so as to conform with Netscapes SSL.
 *
 * This library is free for commercial and non-commercial use as long as
 * the following conditions are aheared to.  The following conditions
 * apply to all code found in this distribution, be it the RC4, RSA,
 * lhash, DES, etc., code; not just the SSL code.  The SSL documentation
 * included with this distribution is covered by the same copyright terms
 * except that the holder is Tim Hudson (tjh@cryptsoft.com).
 *
 * Copyright remains Eric Young's, and as such any Copyright notices in
 * the code are not to be removed.
 * If this package is used in a product, Eric Young should be given attribution
 * as the author of the parts of the library used.
 * This can be in the form of a textual message at program startup or
 * in documentation (online or textual) provided with the package.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 * 1. Redistributions of source code must retain the copyright
 *    notice, this list of conditions and the following disclaimer.
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in the
 *    documentation and/or other materials provided with the distribution.
 * 3. All advertising materials mentioning features or use of this software
 *    must display the following acknowledgement:
 *    "This product includes cryptographic software written by
 *     Eric Young (eay@cryptsoft.com)"
 *    The word 'cryptographic' can be left out if the rouines from the library
 *    being used are not cryptographic related :-).
 * 4. If you include any Windows specific code (or a derivative thereof) from
 *   the apps directory (application code) you must include an acknowledgement:
 *   "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"
 *
 * THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND
 * ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
 * ARE DISCLAIMED.  IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
 * FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
 * DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
 * OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
 * LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
 * OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
 * SUCH DAMAGE.
 *
 * The licence and distribution terms for any publically available version or
 * derivative of this code cannot be changed.  i.e. this code cannot simply be
 * copied and put under another distribution licence
 * [including the GNU Public Licence.]
 */

--------------------------------------------------------------------------------
---
[ovsdb 2.1.0 (part of openvswitch 2.1.0)]
[COPYRIGHT]
  Copyright (c) 2009, 2010, 2011, 2012, 2013 Nicira, Inc.

[LICENSE]
```

Apache License
Version 2.0, January 2004
http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the

Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

   (a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

   (b) You must cause any modified files to carry prominent notices stating that You changed the files; and

   (c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

   (d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

   You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the

origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or
agreed to in writing, Licensor provides the Work (and each
Contributor provides its Contributions) on an "AS IS" BASIS,
WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or
implied, including, without limitation, any warranties or conditions
of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A
PARTICULAR PURPOSE. You are solely responsible for determining the
appropriateness of using or redistributing the Work and assume any
risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory,
whether in tort (including negligence), contract, or otherwise,
unless required by applicable law (such as deliberate and grossly
negligent acts) or agreed to in writing, shall any Contributor be
liable to You for damages, including any direct, indirect, special,
incidental, or consequential damages of any character arising as a
result of this License or out of the use or inability to use the
Work (including but not limited to damages for loss of goodwill,
work stoppage, computer failure or malfunction, or any and all
other commercial damages or losses), even if such Contributor
has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing
the Work or Derivative Works thereof, You may choose to offer,
and charge a fee for, acceptance of support, warranty, indemnity,
or other liability obligations and/or rights consistent with this
License. However, in accepting such obligations, You may act only
on Your own behalf and on Your sole responsibility, not on behalf
of any other Contributor, and only if You agree to indemnify,
defend, and hold each Contributor harmless for any liability
incurred by, or claims asserted against, such Contributor by reason
of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

[ovsdb 2.1.0 (part of openvswitch 2.1.0)]
[COPYRIGHT]
Copyright (c) 2009, 2010, 2011, 2012, 2013 Nicira, Inc.

[LICENSE]

Apache License
Version 2.0, January 2004
http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction,
and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by
the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all
other entities that control, are controlled by, or are under common
control with that entity. For the purposes of this definition,
"control" means (i) the power, direct or indirect, to cause the
direction or management of such entity, whether by contract or
otherwise, or (ii) ownership of fifty percent (50%) or more of the
outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity
exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications,
including but not limited to software source code, documentation

source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

   (a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

   (b) You must cause any modified files to carry prominent notices

stating that You changed the files; and

(c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

(d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity,

or other liability obligations and/or rights consistent with this
License. However, in accepting such obligations, You may act only
on Your own behalf and on Your sole responsibility, not on behalf
of any other Contributor, and only if You agree to indemnify,
defend, and hold each Contributor harmless for any liability
incurred by, or claims asserted against, such Contributor by reason
of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

[ping 11.0.0 (part of FreeBSD 11.0.0)]
[COPYRIGHT]
Copyright (c) 1992-2016 The FreeBSD Project. All rights reserved.

[LICENSE]
Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:
1. Redistributions of source code must retain the above copyright
notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright
notice, this list of conditions and the following disclaimer in the
documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS ``AS IS'' AND
ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
SUCH DAMAGE.

The 4.4BSD and 4.4BSD-Lite software is distributed under the following
terms:

All of the documentation and software included in the 4.4BSD and 4.4BSD-Lite
Releases is copyrighted by The Regents of the University of California.

Copyright 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:
1. Redistributions of source code must retain the above copyright
notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright
notice, this list of conditions and the following disclaimer in the
documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software
must display the following acknowledgement:
This product includes software developed by the University of
California, Berkeley and its contributors.
4. Neither the name of the University nor the names of its contributors
may be used to endorse or promote products derived from this software
without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND
ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE
FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT

LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
SUCH DAMAGE.

The Institute of Electrical and Electronics Engineers and the American
National Standards Committee X3, on Information Processing Systems have
given us permission to reprint portions of their documentation.

In the following statement, the phrase ``this text'' refers to portions
of the system documentation.

Portions of this text are reprinted and reproduced in electronic form in
the second BSD Networking Software Release, from IEEE Std 1003.1-1988, IEEE
Standard Portable Operating System Interface for Computer Environments
(POSIX), copyright C 1988 by the Institute of Electrical and Electronics
Engineers, Inc. In the event of any discrepancy between these versions
and the original IEEE Standard, the original IEEE Standard is the referee
document.

In the following statement, the phrase ``This material'' refers to portions
of the system documentation.

This material is reproduced with permission from American National
Standards Committee X3, on Information Processing Systems. Computer and
Business Equipment Manufacturers Association (CBEMA), 311 First St., NW,
Suite 500, Washington, DC 20001-2178. The developmental work of
Programming Language C was completed by the X3J11 Technical Committee.

The views and conclusions contained in the software and documentation are
those of the authors and should not be interpreted as representing official
policies, either expressed or implied, of the Regents of the University
of California.

NOTE: The copyright of UC Berkeley's Berkeley Software Distribution ("BSD")
source has been updated. The copyright addendum may be found at
ftp://ftp.cs.berkeley.edu/pub/4bsd/README.Impt.License.Change and is
included below.

July 22, 1999

To All Licensees, Distributors of Any Version of BSD:

As you know, certain of the Berkeley Software Distribution ("BSD") source
code files require that further distributions of products containing all or
portions of the software, acknowledge within their advertising materials
that such products contain software developed by UC Berkeley and its
contributors.

Specifically, the provision reads:

"   * 3. All advertising materials mentioning features or use of this software
      *   must display the following acknowledgement:
      *   This product includes software developed by the University of
      *   California, Berkeley and its contributors."

Effective immediately, licensees and distributors are no longer required to
include the acknowledgement within advertising materials. Accordingly, the
foregoing paragraph of those BSD Unix files containing it is hereby deleted
in its entirety.

William Hoskins
Director, Office of Technology Licensing
University of California, Berkeley

[ping6 11.0.0 (part of FreeBSD 11.0.0)]
[COPYRIGHT]
  Copyright (c) 1992-2016 The FreeBSD Project. All rights reserved.

[LICENSE]
Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:
1. Redistributions of source code must retain the above copyright
   notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright
   notice, this list of conditions and the following disclaimer in the
   documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS ``AS IS'' AND
ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
SUCH DAMAGE.

The 4.4BSD and 4.4BSD-Lite software is distributed under the following
terms:

All of the documentation and software included in the 4.4BSD and 4.4BSD-Lite
Releases is copyrighted by The Regents of the University of California.

Copyright 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
 The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:
1. Redistributions of source code must retain the above copyright
   notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright
   notice, this list of conditions and the following disclaimer in the
   documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software
   must display the following acknowledgement:
This product includes software developed by the University of
California, Berkeley and its contributors.
4. Neither the name of the University nor the names of its contributors
   may be used to endorse or promote products derived from this software
   without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND
ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE
FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
SUCH DAMAGE.

The Institute of Electrical and Electronics Engineers and the American
National Standards Committee X3, on Information Processing Systems have
given us permission to reprint portions of their documentation.

In the following statement, the phrase ``this text'' refers to portions
of the system documentation.

Portions of this text are reprinted and reproduced in electronic form in
the second BSD Networking Software Release, from IEEE Std 1003.1-1988, IEEE
Standard Portable Operating System Interface for Computer Environments
(POSIX), copyright C 1988 by the Institute of Electrical and Electronics

Engineers, Inc. In the event of any discrepancy between these versions and the original IEEE Standard, the original IEEE Standard is the referee document.

In the following statement, the phrase ``This material'' refers to portions of the system documentation.

This material is reproduced with permission from American National Standards Committee X3, on Information Processing Systems. Computer and Business Equipment Manufacturers Association (CBEMA), 311 First St., NW, Suite 500, Washington, DC 20001-2178. The developmental work of Programming Language C was completed by the X3J11 Technical Committee.

The views and conclusions contained in the software and documentation are those of the authors and should not be interpreted as representing official policies, either expressed or implied, of the Regents of the University of California.

NOTE: The copyright of UC Berkeley's Berkeley Software Distribution ("BSD") source has been updated. The copyright addendum may be found at ftp://ftp.cs.berkeley.edu/pub/4bsd/README.Impt.License.Change and is included below.

July 22, 1999

To All Licensees, Distributors of Any Version of BSD:

As you know, certain of the Berkeley Software Distribution ("BSD") source code files require that further distributions of products containing all or portions of the software, acknowledge within their advertising materials that such products contain software developed by UC Berkeley and its contributors.

Specifically, the provision reads:

```
"     * 3. All advertising materials mentioning features or use of this software
       *    must display the following acknowledgement:
       *    This product includes software developed by the University of
       *    California, Berkeley and its contributors."
```

Effective immediately, licensees and distributors are no longer required to include the acknowledgement within advertising materials. Accordingly, the foregoing paragraph of those BSD Unix files containing it is hereby deleted in its entirety.

William Hoskins
Director, Office of Technology Licensing
University of California, Berkeley

[pure-ftpd 1.0.45]
[COPYRIGHT]
Copyright (c) 2001 - 2017
Frank Denis <j at pureftpd dot org> with help of contributors.

[LICENSE]
Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND THE AUTHOR DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

```
--------------------------------------------------------------------------
---
[python 2.7.18]
[COPYRIGHT]
  Copyright (c) 2001, 2002, 2003, 2004, 2005, 2006, 2007, 2008, 2009, 2010,
2011,
  2012, 2013, 2014, 2015, 2016, 2017, 2018, 2019, 2020 Python Software
Foundation.  All
  rights reserved.

  Copyright (c) 2000 BeOpen.com.
  All rights reserved.

  Copyright (c) 1995-2001 Corporation for National Research Initiatives.
  All rights reserved.

  Copyright (c) 1991-1995 Stichting Mathematisch Centrum.
  All rights reserved.

[LICENSE]
PYTHON SOFTWARE FOUNDATION LICENSE VERSION 2
--------------------------------------------

1. This LICENSE AGREEMENT is between the Python Software Foundation
("PSF"), and the Individual or Organization ("Licensee") accessing and
otherwise using this software ("Python") in source or binary form and
its associated documentation.

2. Subject to the terms and conditions of this License Agreement, PSF hereby
grants Licensee a nonexclusive, royalty-free, world-wide license to reproduce,
analyze, test, perform and/or display publicly, prepare derivative works,
distribute, and otherwise use Python alone or in any derivative version,
provided, however, that PSF's License Agreement and PSF's notice of copyright,
i.e., "Copyright (c) 2001, 2002, 2003, 2004, 2005, 2006, 2007, 2008, 2009, 2010,
2011, 2012, 2013, 2014, 2015, 2016, 2017, 2018, 2019, 2020 Python Software
Foundation;
All Rights Reserved" are retained in Python alone or in any derivative version
prepared by Licensee.

3. In the event Licensee prepares a derivative work that is based on
or incorporates Python or any part thereof, and wants to make
the derivative work available to others as provided herein, then
Licensee hereby agrees to include in any such work a brief summary of
the changes made to Python.

4. PSF is making Python available to Licensee on an "AS IS"
basis.  PSF MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR
IMPLIED.  BY WAY OF EXAMPLE, BUT NOT LIMITATION, PSF MAKES NO AND
DISCLAIMS ANY REPRESENTATION OR WARRANTY OF MERCHANTABILITY OR FITNESS
FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF PYTHON WILL NOT
INFRINGE ANY THIRD PARTY RIGHTS.

5. PSF SHALL NOT BE LIABLE TO LICENSEE OR ANY OTHER USERS OF PYTHON
FOR ANY INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES OR LOSS AS
A RESULT OF MODIFYING, DISTRIBUTING, OR OTHERWISE USING PYTHON,
OR ANY DERIVATIVE THEREOF, EVEN IF ADVISED OF THE POSSIBILITY THEREOF.

6. This License Agreement will automatically terminate upon a material
breach of its terms and conditions.

7. Nothing in this License Agreement shall be deemed to create any
relationship of agency, partnership, or joint venture between PSF and
Licensee.  This License Agreement does not grant permission to use PSF
trademarks or trade name in a trademark sense to endorse or promote
products or services of Licensee, or any third party.

8. By copying, installing or otherwise using Python, Licensee
agrees to be bound by the terms and conditions of this License
Agreement.
```

BEOPEN.COM LICENSE AGREEMENT FOR PYTHON 2.0

BEOPEN PYTHON OPEN SOURCE LICENSE AGREEMENT VERSION 1

1. This LICENSE AGREEMENT is between BeOpen.com ("BeOpen"), having an office at 160 Saratoga Avenue, Santa Clara, CA 95051, and the Individual or Organization ("Licensee") accessing and otherwise using this software in source or binary form and its associated documentation ("the Software").

2. Subject to the terms and conditions of this BeOpen Python License Agreement, BeOpen hereby grants Licensee a non-exclusive, royalty-free, world-wide license to reproduce, analyze, test, perform and/or display publicly, prepare derivative works, distribute, and otherwise use the Software alone or in any derivative version, provided, however, that the BeOpen Python License is retained in the Software, alone or in any derivative version prepared by Licensee.

3. BeOpen is making the Software available to Licensee on an "AS IS" basis. BEOPEN MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED. BY WAY OF EXAMPLE, BUT NOT LIMITATION, BEOPEN MAKES NO AND DISCLAIMS ANY REPRESENTATION OR WARRANTY OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF THE SOFTWARE WILL NOT INFRINGE ANY THIRD PARTY RIGHTS.

4. BEOPEN SHALL NOT BE LIABLE TO LICENSEE OR ANY OTHER USERS OF THE SOFTWARE FOR ANY INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES OR LOSS AS A RESULT OF USING, MODIFYING OR DISTRIBUTING THE SOFTWARE, OR ANY DERIVATIVE THEREOF, EVEN IF ADVISED OF THE POSSIBILITY THEREOF.

5. This License Agreement will automatically terminate upon a material breach of its terms and conditions.

6. This License Agreement shall be governed by and interpreted in all respects by the law of the State of California, excluding conflict of law provisions. Nothing in this License Agreement shall be deemed to create any relationship of agency, partnership, or joint venture between BeOpen and Licensee. This License Agreement does not grant permission to use BeOpen trademarks or trade names in a trademark sense to endorse or promote products or services of Licensee, or any third party. As an exception, the "BeOpen Python" logos available at http://www.pythonlabs.com/logos.html may be used according to the permissions granted on that web page.

7. By copying, installing or otherwise using the software, Licensee agrees to be bound by the terms and conditions of this License Agreement.

CNRI LICENSE AGREEMENT FOR PYTHON 1.6.1
---

1. This LICENSE AGREEMENT is between the Corporation for National Research Initiatives, having an office at 1895 Preston White Drive, Reston, VA 20191 ("CNRI"), and the Individual or Organization ("Licensee") accessing and otherwise using Python 1.6.1 software in source or binary form and its associated documentation.

2. Subject to the terms and conditions of this License Agreement, CNRI hereby grants Licensee a nonexclusive, royalty-free, world-wide license to reproduce, analyze, test, perform and/or display publicly, prepare derivative works, distribute, and otherwise use Python 1.6.1 alone or in any derivative version, provided, however, that CNRI's License Agreement and CNRI's notice of copyright, i.e., "Copyright (c) 1995-2001 Corporation for National Research Initiatives; All Rights Reserved" are retained in Python 1.6.1 alone or in any derivative version prepared by Licensee. Alternately, in lieu of CNRI's License Agreement, Licensee may substitute the following text (omitting the

quotes): "Python 1.6.1 is made available subject to the terms and conditions in CNRI's License Agreement. This Agreement together with Python 1.6.1 may be located on the Internet using the following unique, persistent identifier (known as a handle): 1895.22/1013. This Agreement may also be obtained from a proxy server on the Internet using the following URL: http://hdl.handle.net/1895.22/1013".

3. In the event Licensee prepares a derivative work that is based on or incorporates Python 1.6.1 or any part thereof, and wants to make the derivative work available to others as provided herein, then Licensee hereby agrees to include in any such work a brief summary of the changes made to Python 1.6.1.

4. CNRI is making Python 1.6.1 available to Licensee on an "AS IS" basis. CNRI MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED. BY WAY OF EXAMPLE, BUT NOT LIMITATION, CNRI MAKES NO AND DISCLAIMS ANY REPRESENTATION OR WARRANTY OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF PYTHON 1.6.1 WILL NOT INFRINGE ANY THIRD PARTY RIGHTS.

5. CNRI SHALL NOT BE LIABLE TO LICENSEE OR ANY OTHER USERS OF PYTHON 1.6.1 FOR ANY INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES OR LOSS AS A RESULT OF MODIFYING, DISTRIBUTING, OR OTHERWISE USING PYTHON 1.6.1, OR ANY DERIVATIVE THEREOF, EVEN IF ADVISED OF THE POSSIBILITY THEREOF.

6. This License Agreement will automatically terminate upon a material breach of its terms and conditions.

7. This License Agreement shall be governed by the federal intellectual property law of the United States, including without limitation the federal copyright law, and, to the extent such U.S. federal law does not apply, by the law of the Commonwealth of Virginia, excluding Virginia's conflict of law provisions. Notwithstanding the foregoing, with regard to derivative works based on Python 1.6.1 that incorporate non-separable material that was previously distributed under the GNU General Public License (GPL), the law of the Commonwealth of Virginia shall govern this License Agreement only as to issues arising under or with respect to Paragraphs 4, 5, and 7 of this License Agreement. Nothing in this License Agreement shall be deemed to create any relationship of agency, partnership, or joint venture between CNRI and Licensee. This License Agreement does not grant permission to use CNRI trademarks or trade name in a trademark sense to endorse or promote products or services of Licensee, or any third party.

8. By clicking on the "ACCEPT" button where indicated, or by copying, installing or otherwise using Python 1.6.1, Licensee agrees to be bound by the terms and conditions of this License Agreement.

ACCEPT

CWI LICENSE AGREEMENT FOR PYTHON 0.9.0 THROUGH 1.2

Copyright (c) 1991 - 1995, Stichting Mathematisch Centrum Amsterdam, The Netherlands. All rights reserved.

Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of Stichting Mathematisch Centrum or CWI not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission.

STICHTING MATHEMATISCH CENTRUM DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL STICHTING MATHEMATISCH CENTRUM BE LIABLE

```
FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES
WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN
ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT
OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.
--------------------------------------------------------------------------------
---
[respond 1.3.0]
[COPYRIGHT]
  copyright (c) 2012: Scott Jehl, Paul Irish, Nicholas Zakas.

[LICENSE]
  Dual MIT/BSD license


--------------------------------------------------------------------------------
---
[runc 1.1.9]
[COPYRIGHT]
Copyright 2014 Docker, Inc.

Licensed under the Apache License, Version 2.0 (the "License");
you may not use this file except in compliance with the License.
You may obtain a copy of the License at

http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software
distributed under the License is distributed on an "AS IS" BASIS,
WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
See the License for the specific language governing permissions and
limitations under the License.

Copyright 2012-2015 Docker, Inc.

[LICENSE]


                                 Apache License
                           Version 2.0, January 2004
                        http://www.apache.org/licenses/

   TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

   1. Definitions.

      "License" shall mean the terms and conditions for use, reproduction,
      and distribution as defined by Sections 1 through 9 of this document.

      "Licensor" shall mean the copyright owner or entity authorized by
      the copyright owner that is granting the License.

      "Legal Entity" shall mean the union of the acting entity and all
      other entities that control, are controlled by, or are under common
      control with that entity. For the purposes of this definition,
      "control" means (i) the power, direct or indirect, to cause the
      direction or management of such entity, whether by contract or
      otherwise, or (ii) ownership of fifty percent (50%) or more of the
      outstanding shares, or (iii) beneficial ownership of such entity.

      "You" (or "Your") shall mean an individual or Legal Entity
      exercising permissions granted by this License.

      "Source" form shall mean the preferred form for making modifications,
      including but not limited to software source code, documentation
      source, and configuration files.

      "Object" form shall mean any form resulting from mechanical
      transformation or translation of a Source form, including but
      not limited to compiled object code, generated documentation,
      and conversions to other media types.
```

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

   (a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

   (b) You must cause any modified files to carry prominent notices stating that You changed the files; and

   (c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of

the Derivative Works; and

(d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason

of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

This product includes software developed at Docker, Inc. (http://www.docker.com).

The following is courtesy of our legal counsel:

Use and transfer of Docker may be subject to certain restrictions by the United States and other governments.
It is your responsibility to ensure that your use and/or transfer does not violate applicable laws.

For more information, please see http://www.bis.doc.gov

See also http://www.apache.org/dev/crypto.html and/or seek legal counsel.

[NOTICE]
runc

Copyright 2012-2015 Docker, Inc.

This product includes software developed at Docker, Inc. (http://www.docker.com).

The following is courtesy of our legal counsel:

Use and transfer of Docker may be subject to certain restrictions by the United States and other governments.
It is your responsibility to ensure that your use and/or transfer does not violate applicable laws.

For more information, please see http://www.bis.doc.gov

See also http://www.apache.org/dev/crypto.html and/or seek legal counsel.

[select2 3.4.5]
Copyright 2012 Igor Vaynberg

Version: @@ver@@ Timestamp: @@timestamp@@

This software is licensed under the Apache License, Version 2.0 (the "Apache License") or the GNU
General Public License version 2 (the "GPL License"). You may choose either license to govern your
use of this software only upon the condition that you accept all of the terms of either the Apache
License or the GPL License.

You may obtain a copy of the Apache License and the GPL License at:

http://www.apache.org/licenses/LICENSE-2.0
http://www.gnu.org/licenses/gpl-2.0.html

Unless required by applicable law or agreed to in writing, software distributed under the Apache License
or the GPL Licesnse is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND,
either express or implied. See the Apache License and the GPL License for the specific language governing
permissions and limitations under the Apache License and the GPL License.

```
--------------------------------------------------------------------------------
---
[slickgrid 2.1]
[COPYRIGHT]
  Copyright (c) 2010 Michael Leibman, http://github.com/mleibman/slickgrid

[LICENSE]
Permission is hereby granted, free of charge, to any person obtaining
a copy of this software and associated documentation files (the
"Software"), to deal in the Software without restriction, including
without limitation the rights to use, copy, modify, merge, publish,
distribute, sublicense, and/or sell copies of the Software, and to
permit persons to whom the Software is furnished to do so, subject to
the following conditions:

The above copyright notice and this permission notice shall be
included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND,
EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF
MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND
NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE
LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION
OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION
WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.
--------------------------------------------------------------------------------
---
[sqlite3 3.35.5]
** 2006 June 7
**
** The author disclaims copyright to this source code.  In place of
** a legal notice, here is a blessing:
**
**    May you do good and not evil.
**    May you find forgiveness for yourself and forgive others.
**    May you share freely, never taking more than you give.
**
******************************************************************************

--------------------------------------------------------------------------------
---
[talloc 2.1.3]
[COPYRIGHT]
   Copyright (C) Andrew Tridgell 2004
   Copyright (C) Stefan Metzmacher 2006
[LICENSE]
     ** NOTE! The following LGPL license applies to the talloc
     ** library. This does NOT imply that all of Samba is released
     ** under the LGPL

   This library is free software; you can redistribute it and/or
   modify it under the terms of the GNU Lesser General Public
   License as published by the Free Software Foundation; either
   version 3 of the License, or (at your option) any later version.

   This library is distributed in the hope that it will be useful,
   but WITHOUT ANY WARRANTY; without even the implied warranty of
   MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the GNU
   Lesser General Public License for more details.
--------------------------------------------------------------------------------
---
[tassl 1.1.1b]

  LICENSE ISSUES
  ==============

  The TaSSL toolkit stays under a double license, i.e. both the conditions of
  the TaSSL License and the original OpenSSL license apply to the toolkit.
  See below for the actual license texts.
```

```
/* TaSSL license */

/* ====================================================================
 * Copyright (c) 2016 - 2019 Beijing JN TASS Technology Co., Ltd.  All rights
reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 *
 * 1. Redistributions of source code must retain the above copyright
 *    notice, this list of conditions and the following disclaimer.
 *
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in
 *    the documentation and/or other materials provided with the
 *    distribution.
 *
 * 3. All advertising materials mentioning features or use of this
 *    software must display the following acknowledgment:
 *    "This product includes software developed by ・冷ｹ・・・励C・㊦腱代・纖牙 8 舌
$・・
 *    TaSSL Project.(http://www.tass.com.cn/)"
 *
 * 4. The name "TaSSL Project" must not be used to endorse or promote
 *    products derived from this software without prior written
 *    permission. For written permission, please contact
 *    TaSSL@tass.com.cn.
 *
 * 5. Products derived from this software may not be called "TaSSL"
 *    nor may "TaSSL" appear in their names without prior written
 *    permission of the TaSSL Project.
 *
 * 6. Redistributions of any form whatsoever must retain the following
 *    acknowledgment:
 *    "This product includes software developed by Beijing JN TASS Technology
Co., Ltd.
 *    TaSSL Project.(http://www.tass.com.cn/)"
 *
 * THIS SOFTWARE IS PROVIDED BY THE TASSL PROJECT ``AS IS'' AND ANY
 * EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
 * PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE TASSL PROJECT OR
 * ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
 * SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
 * NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
 * LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
 * STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
 * ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
 * OF THE POSSIBILITY OF SUCH DAMAGE.
 * ====================================================================
 *
 * This product includes software developed by the OpenSSL Project
 * for use in the OpenSSL Toolkit (http://www.openssl.org/).
 *
 */

/* OpenSSL License */
/* ====================================================================
 * Copyright (c) 1998-2019 The OpenSSL Project.  All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 *
 * 1. Redistributions of source code must retain the above copyright
 *    notice, this list of conditions and the following disclaimer.
 *
 * 2. Redistributions in binary form must reproduce the above copyright
```

```
 *    notice, this list of conditions and the following disclaimer in
 *    the documentation and/or other materials provided with the
 *    distribution.
 *
 * 3. All advertising materials mentioning features or use of this
 *    software must display the following acknowledgment:
 *    "This product includes software developed by the OpenSSL Project
 *    for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
 *
 * 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
 *    endorse or promote products derived from this software without
 *    prior written permission. For written permission, please contact
 *    openssl-core@openssl.org.
 *
 * 5. Products derived from this software may not be called "OpenSSL"
 *    nor may "OpenSSL" appear in their names without prior written
 *    permission of the OpenSSL Project.
 *
 * 6. Redistributions of any form whatsoever must retain the following
 *    acknowledgment:
 *    "This product includes software developed by the OpenSSL Project
 *    for use in the OpenSSL Toolkit (http://www.openssl.org/)"
 *
 * THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
 * EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
 * PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE OpenSSL PROJECT OR
 * ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
 * SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
 * NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
 * LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
 * STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
 * ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
 * OF THE POSSIBILITY OF SUCH DAMAGE.
 * ====================================================================
 *
 * This product includes cryptographic software written by Eric Young
 * (eay@cryptsoft.com).  This product includes software written by Tim
 * Hudson (tjh@cryptsoft.com).
 *
 */
--------------------------------------------------------------------------------
---
[tcl-snmptools 1.0]
[COPYRIGHT]
  Copyright (C) 2008  Alexandros Stergiakis

[LICENSE]
                    GNU GENERAL PUBLIC LICENSE
                       Version 3, 29 June 2007

 Copyright (C) 2007 Free Software Foundation, Inc. <http://fsf.org/>
 Everyone is permitted to copy and distribute verbatim copies
 of this license document, but changing it is not allowed.

                            Preamble

  The GNU General Public License is a free, copyleft license for
software and other kinds of works.

  The licenses for most software and other practical works are designed
to take away your freedom to share and change the works.  By contrast,
the GNU General Public License is intended to guarantee your freedom to
share and change all versions of a program--to make sure it remains free
software for all its users.  We, the Free Software Foundation, use the
GNU General Public License for most of our software; it applies also to
any other work released this way by its authors.  You can apply it to
your programs, too.
```

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for them if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you these rights or asking you to surrender the rights. Therefore, you have certain responsibilities if you distribute copies of the software, or if you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must pass on to the recipients the same freedoms that you received. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

Developers that use the GNU GPL protect your rights with two steps: (1) assert copyright on the software, and (2) offer you this License giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains that there is no warranty for this free software. For both users' and authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

Some devices are designed to deny users access to install or run modified versions of the software inside them, although the manufacturer can do so. This is fundamentally incompatible with the aim of protecting users' freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we stand ready to extend this provision to those domains in future versions of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents. States should not allow patents to restrict development and use of software on general-purpose computers, but in those that do, we wish to avoid the special danger that patents applied to a free program could make it effectively proprietary. To prevent this, the GPL assures that patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS

0. Definitions.

"This License" refers to version 3 of the GNU General Public License.

"Copyright" also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

"The Program" refers to any copyrightable work licensed under this License. Each licensee is addressed as "you". "Licensees" and "recipients" may be individuals or organizations.

To "modify" a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a "modified version" of the earlier work or a work "based on" the earlier work.

A "covered work" means either the unmodified Program or a work based on the Program.

To "propagate" a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To "convey" a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays "Appropriate Legal Notices" to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

1. Source Code.

The "source code" for a work means the preferred form of the work for making modifications to it. "Object code" means any non-source form of a work.

A "Standard Interface" means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The "System Libraries" of an executable work include anything, other than the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A "Major Component", in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The "Corresponding Source" for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

2. Basic Permissions.

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered by this License only if the output, given its content, constitutes a covered work. This License acknowledges your

rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed; section 10 makes it unnecessary.

3. Protecting Users' Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of technological measures.

4. Conveying Verbatim Copies.

You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice; keep intact all notices stating that this License and any non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

5. Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

a) The work must carry prominent notices stating that you modified it, and giving a relevant date.

b) The work must carry prominent notices stating that it is released under this License and any conditions added under section 7. This requirement modifies the requirement in section 4 to "keep intact all notices".

c) You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.

d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive

interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an "aggregate" if the compilation and its resulting copyright are not used to limit the access or legal rights of the compilation's users beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.

6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, in one of these ways:

a) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange.

b) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for software interchange, for a price no more than your reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.

c) Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This alternative is allowed only occasionally and noncommercially, and only if you received the object code with such an offer, in accord with subsection 6b.

d) Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in the same way through the same place at no further charge. You need not require recipients to copy the Corresponding Source along with the object code. If the place to copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.

e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.

A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object code work.

A "User Product" is either (1) a "consumer product", which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular

product received by a particular user, "normally used" refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

"Installation Information" for a User Product means any methods, procedures, authorization keys, or other information required to install and execute modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

7. Additional Terms.

"Additional permissions" are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

a) Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or

b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or

c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or

d) Limiting the use for publicity purposes of names of licensors or authors of the material; or

e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or

f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on those licensors and authors.

All other non-permissive additional terms are considered "further restrictions" within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above requirements apply either way.

8. Termination.

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or

modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10. Automatic Licensing of Downstream Recipients.

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An "entity transaction" is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

11. Patents.

A "contributor" is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's "contributor version".

A contributor's "essential patent claims" are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For purposes of this definition, "control" includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a "patent license" is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To "grant" such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. "Knowingly relying" means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is "discriminatory" if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.

12. No Surrender of Others' Freedom.

If conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot convey a covered work so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

13. Use with the GNU Affero General Public License.

Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed under version 3 of the GNU Affero General Public License into a single combined work, and to convey the resulting work. The terms of this License will continue to apply to the part which is the covered work, but the special requirements of the GNU Affero General Public License, section 13, concerning interaction through a network will apply to the combination as such.

14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of the GNU General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU General Public License, you may choose any version ever published by the Free Software Foundation.

If the Program specifies that a proxy can decide which future versions of the GNU General Public License can be used, that proxy's public statement of acceptance of a version permanently authorizes you

to choose that version for the Program.

Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

15. Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

17. Interpretation of Sections 15 and 16.

If the disclaimer of warranty and limitation of liability provided above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates an absolute waiver of all civil liability in connection with the Program, unless a warranty or assumption of liability accompanies a copy of the Program in return for a fee.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively state the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This program is free software: you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation, either version 3 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program. If not, see <http://www.gnu.org/licenses/>.

Also add information on how to contact you by electronic and paper mail.

```
  If the program does terminal interaction, make it output a short
notice like this when it starts in an interactive mode:

    <program>  Copyright (C) <year>  <name of author>
    This program comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
    This is free software, and you are welcome to redistribute it
    under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate
parts of the General Public License.  Of course, your program's commands
might be different; for a GUI interface, you would use an "about box".

  You should also get your employer (if you work as a programmer) or school,
if any, to sign a "copyright disclaimer" for the program, if necessary.
For more information on this, and how to apply and follow the GNU GPL, see
<http://www.gnu.org/licenses/>.

  The GNU General Public License does not permit incorporating your program
into proprietary programs.  If your program is a subroutine library, you
may consider it more useful to permit linking proprietary applications with
the library.  If this is what you want to do, use the GNU Lesser General
Public License instead of this License.  But first, please read
<http://www.gnu.org/philosophy/why-not-lgpl.html>.

--------------------------------------------------------------------------
---
[tcltk 8.5.8]
[COPYRIGHT]
  Copyright (c) 1987-1994 The Regents of the University of California.
  Copyright (c) 1993-1996 Lucent Technologies.
  Copyright (c) 1994-1998 Sun Microsystems, Inc.
  Copyright (c) 1998-2000 by Scriptics Corporation.
  Copyright (c) 2002 by Kevin B. Kenny.  All rights reserved.

[LICENSE]
This software is copyrighted by the Regents of the University of
California, Sun Microsystems, Inc., Scriptics Corporation, ActiveState
Corporation and other parties.  The following terms apply to all files
associated with the software unless explicitly disclaimed in
individual files.

The authors hereby grant permission to use, copy, modify, distribute,
and license this software and its documentation for any purpose, provided
that existing copyright notices are retained in all copies and that this
notice is included verbatim in any distributions. No written agreement,
license, or royalty fee is required for any of the authorized uses.
Modifications to this software may be copyrighted by their authors
and need not follow the licensing terms described here, provided that
the new terms are clearly indicated on the first page of each file where
they apply.

IN NO EVENT SHALL THE AUTHORS OR DISTRIBUTORS BE LIABLE TO ANY PARTY
FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES
ARISING OUT OF THE USE OF THIS SOFTWARE, ITS DOCUMENTATION, OR ANY
DERIVATIVES THEREOF, EVEN IF THE AUTHORS HAVE BEEN ADVISED OF THE
POSSIBILITY OF SUCH DAMAGE.

THE AUTHORS AND DISTRIBUTORS SPECIFICALLY DISCLAIM ANY WARRANTIES,
INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY,
FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT.  THIS SOFTWARE
IS PROVIDED ON AN "AS IS" BASIS, AND THE AUTHORS AND DISTRIBUTORS HAVE
NO OBLIGATION TO PROVIDE MAINTENANCE, SUPPORT, UPDATES, ENHANCEMENTS, OR
MODIFICATIONS.

GOVERNMENT USE: If you are acquiring this software on behalf of the
U.S. government, the Government shall have only "Restricted Rights"
in the software and related documentation as defined in the Federal
Acquisition Regulations (FARs) in Clause 52.227.19 (c) (2).  If you
are acquiring the software on behalf of the Department of Defense, the
software shall be classified as "Commercial Computer Software" and the
```

Government shall have only "Restricted Rights" as defined in Clause
252.227-7013 (c) (1) of DFARs. Notwithstanding the foregoing, the
authors grant the U.S. Government and others acting in its behalf
permission to use and distribute the software in accordance with the
terms specified in this license.

[telnet 11.0.0 (part of FreeBSD 11.0.0)]
[COPYRIGHT]
Copyright (c) 1992-2016 The FreeBSD Project. All rights reserved.

[LICENSE]
Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:
1. Redistributions of source code must retain the above copyright
notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright
notice, this list of conditions and the following disclaimer in the
documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS ``AS IS'' AND
ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
SUCH DAMAGE.

The 4.4BSD and 4.4BSD-Lite software is distributed under the following
terms:

All of the documentation and software included in the 4.4BSD and 4.4BSD-Lite
Releases is copyrighted by The Regents of the University of California.

Copyright 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:
1. Redistributions of source code must retain the above copyright
notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright
notice, this list of conditions and the following disclaimer in the
documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software
must display the following acknowledgement:
This product includes software developed by the University of
California, Berkeley and its contributors.
4. Neither the name of the University nor the names of its contributors
may be used to endorse or promote products derived from this software
without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND
ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE
FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
SUCH DAMAGE.

The Institute of Electrical and Electronics Engineers and the American National Standards Committee X3, on Information Processing Systems have given us permission to reprint portions of their documentation.

In the following statement, the phrase ``this text'' refers to portions of the system documentation.

Portions of this text are reprinted and reproduced in electronic form in the second BSD Networking Software Release, from IEEE Std 1003.1-1988, IEEE Standard Portable Operating System Interface for Computer Environments (POSIX), copyright C 1988 by the Institute of Electrical and Electronics Engineers, Inc. In the event of any discrepancy between these versions and the original IEEE Standard, the original IEEE Standard is the referee document.

In the following statement, the phrase ``This material'' refers to portions of the system documentation.

This material is reproduced with permission from American National Standards Committee X3, on Information Processing Systems. Computer and Business Equipment Manufacturers Association (CBEMA), 311 First St., NW, Suite 500, Washington, DC 20001-2178. The developmental work of Programming Language C was completed by the X3J11 Technical Committee.

The views and conclusions contained in the software and documentation are those of the authors and should not be interpreted as representing official policies, either expressed or implied, of the Regents of the University of California.

NOTE: The copyright of UC Berkeley's Berkeley Software Distribution ("BSD") source has been updated. The copyright addendum may be found at ftp://ftp.cs.berkeley.edu/pub/4bsd/README.Impt.License.Change and is included below.

July 22, 1999

To All Licensees, Distributors of Any Version of BSD:

As you know, certain of the Berkeley Software Distribution ("BSD") source code files require that further distributions of products containing all or portions of the software, acknowledge within their advertising materials that such products contain software developed by UC Berkeley and its contributors.

Specifically, the provision reads:

```
"     * 3. All advertising materials mentioning features or use of this software
       *    must display the following acknowledgement:
       *    This product includes software developed by the University of
       *    California, Berkeley and its contributors."
```

Effective immediately, licensees and distributors are no longer required to include the acknowledgement within advertising materials. Accordingly, the foregoing paragraph of those BSD Unix files containing it is hereby deleted in its entirety.

William Hoskins
Director, Office of Technology Licensing
University of California, Berkeley

[traceroute 11.0.0 (part of FreeBSD 11.0.0)]
[COPYRIGHT]
  Copyright (c) 1992-2016 The FreeBSD Project. All rights reserved.

[LICENSE]
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions

are met:
1. Redistributions of source code must retain the above copyright
   notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright
   notice, this list of conditions and the following disclaimer in the
   documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS ``AS IS'' AND
ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
SUCH DAMAGE.

The 4.4BSD and 4.4BSD-Lite software is distributed under the following
terms:

All of the documentation and software included in the 4.4BSD and 4.4BSD-Lite
Releases is copyrighted by The Regents of the University of California.

Copyright 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
 The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:
1. Redistributions of source code must retain the above copyright
   notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright
   notice, this list of conditions and the following disclaimer in the
   documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software
   must display the following acknowledgement:
This product includes software developed by the University of
California, Berkeley and its contributors.
4. Neither the name of the University nor the names of its contributors
   may be used to endorse or promote products derived from this software
   without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND
ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE
FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
SUCH DAMAGE.

The Institute of Electrical and Electronics Engineers and the American
National Standards Committee X3, on Information Processing Systems have
given us permission to reprint portions of their documentation.

In the following statement, the phrase ``this text'' refers to portions
of the system documentation.

Portions of this text are reprinted and reproduced in electronic form in
the second BSD Networking Software Release, from IEEE Std 1003.1-1988, IEEE
Standard Portable Operating System Interface for Computer Environments
(POSIX), copyright C 1988 by the Institute of Electrical and Electronics
Engineers, Inc. In the event of any discrepancy between these versions
and the original IEEE Standard, the original IEEE Standard is the referee
document.

In the following statement, the phrase ``This material'' refers to portions of the system documentation.

This material is reproduced with permission from American National Standards Committee X3, on Information Processing Systems. Computer and Business Equipment Manufacturers Association (CBEMA), 311 First St., NW, Suite 500, Washington, DC 20001-2178. The developmental work of Programming Language C was completed by the X3J11 Technical Committee.

The views and conclusions contained in the software and documentation are those of the authors and should not be interpreted as representing official policies, either expressed or implied, of the Regents of the University of California.

NOTE: The copyright of UC Berkeley's Berkeley Software Distribution ("BSD") source has been updated. The copyright addendum may be found at ftp://ftp.cs.berkeley.edu/pub/4bsd/README.Impt.License.Change and is included below.

July 22, 1999

To All Licensees, Distributors of Any Version of BSD:

As you know, certain of the Berkeley Software Distribution ("BSD") source code files require that further distributions of products containing all or portions of the software, acknowledge within their advertising materials that such products contain software developed by UC Berkeley and its contributors.

Specifically, the provision reads:

```
"     * 3. All advertising materials mentioning features or use of this software
       *    must display the following acknowledgement:
       *    This product includes software developed by the University of
       *    California, Berkeley and its contributors."
```

Effective immediately, licensees and distributors are no longer required to include the acknowledgement within advertising materials. Accordingly, the foregoing paragraph of those BSD Unix files containing it is hereby deleted in its entirety.

William Hoskins
Director, Office of Technology Licensing
University of California, Berkeley

[traceroute6 11.0.0 (part of FreeBSD 11.0.0)]
[COPYRIGHT]
Copyright (c) 1992-2016 The FreeBSD Project. All rights reserved.

[LICENSE]
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT

LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
SUCH DAMAGE.

The 4.4BSD and 4.4BSD-Lite software is distributed under the following
terms:

All of the documentation and software included in the 4.4BSD and 4.4BSD-Lite
Releases is copyrighted by The Regents of the University of California.

Copyright 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
 The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:
1. Redistributions of source code must retain the above copyright
   notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright
   notice, this list of conditions and the following disclaimer in the
   documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software
   must display the following acknowledgement:
This product includes software developed by the University of
California, Berkeley and its contributors.
4. Neither the name of the University nor the names of its contributors
   may be used to endorse or promote products derived from this software
   without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND
ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE
FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
SUCH DAMAGE.

The Institute of Electrical and Electronics Engineers and the American
National Standards Committee X3, on Information Processing Systems have
given us permission to reprint portions of their documentation.

In the following statement, the phrase ``this text'' refers to portions
of the system documentation.

Portions of this text are reprinted and reproduced in electronic form in
the second BSD Networking Software Release, from IEEE Std 1003.1-1988, IEEE
Standard Portable Operating System Interface for Computer Environments
(POSIX), copyright C 1988 by the Institute of Electrical and Electronics
Engineers, Inc. In the event of any discrepancy between these versions
and the original IEEE Standard, the original IEEE Standard is the referee
document.

In the following statement, the phrase ``This material'' refers to portions
of the system documentation.

This material is reproduced with permission from American National
Standards Committee X3, on Information Processing Systems. Computer and
Business Equipment Manufacturers Association (CBEMA), 311 First St., NW,
Suite 500, Washington, DC 20001-2178. The developmental work of
Programming Language C was completed by the X3J11 Technical Committee.

The views and conclusions contained in the software and documentation are
those of the authors and should not be interpreted as representing official
policies, either expressed or implied, of the Regents of the University
of California.

```
NOTE: The copyright of UC Berkeley's Berkeley Software Distribution ("BSD")
source has been updated.  The copyright addendum may be found at
ftp://ftp.cs.berkeley.edu/pub/4bsd/README.Impt.License.Change and is
included below.

July 22, 1999

To All Licensees, Distributors of Any Version of BSD:

As you know, certain of the Berkeley Software Distribution ("BSD") source
code files require that further distributions of products containing all or
portions of the software, acknowledge within their advertising materials
that such products contain software developed by UC Berkeley and its
contributors.

Specifically, the provision reads:

"    * 3. All advertising materials mentioning features or use of this software
      *    must display the following acknowledgement:
      *    This product includes software developed by the University of
      *    California, Berkeley and its contributors."

Effective immediately, licensees and distributors are no longer required to
include the acknowledgement within advertising materials.  Accordingly, the
foregoing paragraph of those BSD Unix files containing it is hereby deleted
in its entirety.

William Hoskins
Director, Office of Technology Licensing
University of California, Berkeley
------------------------------------------------------------------------------
---
[xzdec 5.2.2(part of xz 5.2.2)]
////////////////////////////////////////////////////////////////////////////
//
//
/// \file       xzdec.c
/// \brief      Simple single-threaded tool to uncompress .xz or .lzma files
//
//  Author:     Lasse Collin
//
//  This file has been put into the public domain.
//  You can do whatever you want with this file.
//
////////////////////////////////////////////////////////////////////////////
//
------------------------------------------------------------------------------
---
[zlib 1.2.11]
[COPYRIGHT]
  Copyright (C) 1995-2017 Jean-loup Gailly and Mark Adler

[LICENSE]
  This software is provided 'as-is', without any express or implied
  warranty.  In no event will the authors be held liable for any damages
  arising from the use of this software.

  Permission is granted to anyone to use this software for any purpose,
  including commercial applications, and to alter it and redistribute it
  freely, subject to the following restrictions:

  1. The origin of this software must not be misrepresented; you must not
     claim that you wrote the original software. If you use this software
     in a product, an acknowledgment in the product documentation would be
     appreciated but is not required.
  2. Altered source versions must be plainly marked as such, and must not be
     misrepresented as being the original software.
  3. This notice may not be removed or altered from any source distribution.
```

Jean-loup Gailly Mark Adler
jloup@gzip.org madler@alumni.caltech.edu

[libpcap 1.2.0]
[LICENSE]
Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:

1. Redistributions of source code must retain the above copyright
   notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright
   notice, this list of conditions and the following disclaimer in
   the documentation and/or other materials provided with the
   distribution.
3. The names of the authors may not be used to endorse or promote
   products derived from this software without specific prior
   written permission.

THIS SOFTWARE IS PROVIDED ``AS IS'' AND WITHOUT ANY EXPRESS OR
IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED
WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

[kubernetes 1.22.3]

Apache License
Version 2.0, January 2004
http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction,
and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by
the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all
other entities that control, are controlled by, or are under common
control with that entity. For the purposes of this definition,
"control" means (i) the power, direct or indirect, to cause the
direction or management of such entity, whether by contract or
otherwise, or (ii) ownership of fifty percent (50%) or more of the
outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity
exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications,
including but not limited to software source code, documentation
source, and configuration files.

"Object" form shall mean any form resulting from mechanical
transformation or translation of a Source form, including but
not limited to compiled object code, generated documentation,
and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or
Object form, made available under the License, as indicated by a
copyright notice that is included in or attached to the work
(an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object
form, that is based on (or derived from) the Work and for which the

editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

   (a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

   (b) You must cause any modified files to carry prominent notices stating that You changed the files; and

   (c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

   (d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed

as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

APPENDIX: How to apply the Apache License to your work.

To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets "[]"

```
      replaced with your own identifying information. (Don't include
      the brackets!)  The text should be enclosed in the appropriate
      comment syntax for the file format. We also recommend that a
      file or class name and description of purpose be included on the
      same "printed page" as the copyright notice for easier
      identification within third-party archives.

   Copyright [yyyy] [name of copyright owner]

   Licensed under the Apache License, Version 2.0 (the "License");
   you may not use this file except in compliance with the License.
   You may obtain a copy of the License at

       http://www.apache.org/licenses/LICENSE-2.0

   Unless required by applicable law or agreed to in writing, software
   distributed under the License is distributed on an "AS IS" BASIS,
   WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
   See the License for the specific language governing permissions and
   limitations under the License.
-------------------------------------------------------------------------------
---
```