NEC

GVT-256678-001-00 1.5

QX-W1200 シリーズ アクセスポイント

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	2025/03	初版発行
1.1	2025/12	・「セクション 1 はじめに」の「14 章 装置管理」の「AP の給電モードの設定」に W1210/W1230 の AP での機能利用サポートに関する記載を追加しました。 ・「セクション 2 WLAN」の「1 章 無線管理」の「無線モードの指定」と「6GHz 帯の無線モードの設定」にデフォルト値を追記しました。 ・「セクション 2 WLAN」の「1 章 無線管理」の「基本的な無線機能の設定」に「レーダチャネルスイッチバックの設定」を追加しました。 ・「セクション 2 WLAN」の「1 章 無線管理」の 6GHz 帯の無線で下記設定のサービステンプレートの使用についての説明を追加、設定例を更新しました。 **・wpa3 enterprise-only-mode** **・wpa3 enterprise-transition-mode** **・wpa3 parsonal optional** ・「セクション 2 WLAN」の「3 章 WLAN セキュリティ」の「WPA3」の説明に **enterprise-trantision-mode**、**enterprise-only-mode** のパラメータ、メモ書きを更新しました。 ・「セクション 2 WLAN」の「14 章 WLAN 最適化」の「AP のトラフィックスケジューリングモードの設定」をサポートしました。 ・「セクション 2 WLAN」の「14 章 WLAN 最適化」の「クライアント高速キープアライブの設定」をサポートしました。 ・「セクション 10 システム管理」の「7 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。 ・「セクション 10 システム管理」の「8 章 NetMeister」の「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。 ・誤記訂正
1.2	2026/02	・「セクション 2 WLAN」の「1 章 無線管理の設定」の「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」の設定手順を更新しました。 ・「セクション 7-IP マルチキャスト」の「2 章 IGMP スヌーピング」の「マルチキャストグループポリシーが動作しない」の解決策を更新しました。 ・「セクション 9-セキュリティ」の「1 章 AAA」の「RADIUS のトラブルシューティング」の解決策を更新しました。
1.3	2026/04	・「セクション 10-システム管理」の「7 章 Information Center」に「キープアライブログ送信の設定の有効化」のデフォルト値を変更しました。

版数	日付	改版内容
1.4	2026/07	・「セクション 02-WLAN」の「1 章 無線管理の設定」に、**wpa3-enterprise-transition-mode** を 6G に設定した場合の説明を追加しました。 ・「セクション 02-WLAN」の「2 章 WLAN アクセスの設定」の SSID ステルスに 6GHz 無線に関する注記を追加しました。 ・「セクション 02-WLAN」の「7 章 WIPS の設定」に、無線通信と WIPS センサの併用に関するメモを追加しました。 ・「セクション 02-WLAN」の「9 章 WLAN ローミングの設定」に、「FT を有効にする」に補足を追加しました。 ・「セクション 02-WLAN」の「9 章 WLAN ローミングの設定」に、「802.11k の設定」を追加しました。 ・「セクション 02-WLAN」の「14 章 WLAN 最適化」の「クライアント高速キープアライブの設定」の記述を修正しました。 ・「セクション 02-WLAN」の「17 章 WLAN メッシュの設定」に、同シリーズ、同バージョンの組み合わせのみをサポートするメモを追加しました。 ・「セクション 02-WLAN」の「17 章 WLAN メッシュの設定」に、メッシュを使う Radio では WIPS を使わないことを推奨するメモを追加しました。 ・「セクション 09-セキュリティ」の「1 章 AAA」に、Radius サーバ機能に関する記載を追加しました。 ・「セクション 10-システム管理」の「1 章 システムの保守とデバッグ」に、「iPerf」を追加しました。 ・「セクション 11-謝辞」の「1 章 謝辞」を更新しました。 誤記訂正
1.5	2026/11	・「セクション 01-はじめに」の「1 章 CLI の概要」に「コマンド履歴バッファの管理と使用」を追加しました。 ・「セクション 01-はじめに」の「3 章 ログイン」の「Web コンソールによるログイン」に、W1200 でのデフォルト有効化の説明を記載しました。 ・「セクション 01-はじめに」の「6 章 Web コンソールによるログイン」の「HTTP ログインの手順」と「HTTPS ログインの手順」に Web コンソールによるログインのデフォルト有効化に対応したバージョンを記載しました。 ・「セクション 01-はじめに」の「14 章 装置管理」に「トランシーバのパラメータ表示」を追加しました。 ・「セクション 01-はじめに」の「14 章 装置管理」の「AP の給電モードの仕様」に、QX-W1220、QX-W1210-E の仕様を追加しました。 ・「セクション 02-WLAN」の「1 章 無線管理の設定」に、QX-W1220、QX-W1210-E の説明を追加しました。 ・「セクション 02-WLAN」の「1 章 無線管理の設定」に、「アンテナタイプの設定」、「屋外用 AP の屋内利用モードの設定」を追加しました。 ・「セクション 02-WLAN」の「1 章 無線管理の設定」に、「R/F ドラ

版数	日付	改版内容
		イバのリセット」を追加しました。 ・「セクション 02-WLAN」の「2 章 WLAN アクセスの設定」の下記コマンドに、デフォルト値のバージョン差分を記載しました。 **・wlan client idle-timeout** ・「セクション 02-WLAN」の「2 章 WLAN アクセスの設定」の「WLAN アクセスの表示と維持」に下記コマンドを追加しました。 **・display wlan client cache** ・「セクション 02-WLAN」の「3 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** ・「セクション 02-WLAN」の「7 章 WIPS の設定」の「分類ポリシーの設定」にメモを追加しました。 ・「セクション 04-アクセス」の「4 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** ・「セクション 09-セキュリティ」の「1 章 AAA の設定」に、EAP-TLS サポートについての説明と設定例を追加しました。 ・「セクション 09-セキュリティ」の「1 章 AAA の設定」の「EAP プロファイルの設定」と「RADIUS サーバ設定の有効化」に、CRL の設定手順と説明を追加しました。 ・「セクション 09-セキュリティ」の「1 章 AAA の設定」に、「RADIUS サーバの認証ログ出力の設定」を追加しました。 ・「セクション 10-システム管理」の「7 章 Information center」の「ログファイルへのログの保存」と「ログの最小記録期間の設定」の説明を修正しました。 ・「セクション 10-システム管理」の「8 章 NetMeister」に、下記コマンドを追加しました。 **・netmeister ngn enable** ・「セクション 10-システム管理」に「9 章 パケットキャプチャの設定」を追加しました。

Copyright © NEC Corporation 2023-2026

All Rights Reserved

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

商標

本マニュアルに記載されているその他の商標は、各社が保有します。

注意

- 本装置は *QX-W1200 シリーズ アクセスポイント コマンドマニュアル*に記載されているコマンドのみ使用することができます。*QX-W1200 シリーズ アクセスポイント コマンドマニュアル*に記載されていないコマンドを使用した場合の動作については保証しません。
- 本マニュアルの内容は、予告なく変更されることがあります。本マニュアルのすべての記述、情報、および推奨事項は、明示的か暗黙的かにかかわらず、いかなる種類の保証の対象になりません。

本マニュアルについて

バージョン

本マニュアルに対応する製品バージョンは Version 7.5.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-W1200 シリーズ アクセスポイントに関する詳細な説明があります。

マニュアル	内容
QX-W1200 シリーズ アクセスポイント インスタレーションマニュアル	システムのインストールについて説明しています。
QX-W1200 シリーズ アクセスポイント オペレーションマニュアル	機能の設定について説明しています。
QX-W1200 シリーズ アクセスポイント コマンドマニュアル	機能に関するコマンドについて説明しています。
QX-W1200 シリーズ アクセスポイント Anchor-AC オペレーションマニュアル	Anchor-AC として動作させる場合の機能設定について説明しています。
QX-W1200 シリーズ アクセスポイント Anchor-AC コマンドマニュアル	Anchor-AC として動作させる場合の機能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

このオペレーションマニュアルは以下のセクションで構成されます。

- **はじめに**

  AP 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、管理の設定について説明します。

- **WLAN**

  WLAN の設定について説明します。

- **インタフェース**

  Ethernet ポートの設定について説明します。

- **アクセス**

  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。

- **IP サービス**

  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。

- **ルーティングプロトコル**

  各種ルーティングプロトコル（IPv4）の設定について説明します。

- **IP マルチキャスト**

  IGMP スヌーピングの設定について説明します。

- **ACL and QoS**

  QoS、ACL の設定について説明します。

- **セキュリティ**

  AAA、RADIUS、802.1X、MAC アドレス認証、SSH 等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、AP 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。

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

IV. マウス操作

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

V. 記号

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

VI. ネットワークアイコン

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

VII. 設定例

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

VIII. セキュリティ強化

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

本マニュアルは以下に示すセクションで構成されています。

01 - はじめに

02 - WLAN

03 - インタフェース

04 - アクセス

05 - IP サービス

06 - ルーティングプロトコル

07 - IP マルチキャスト

08 - ACL and QoS

09 - セキュリティ

10 - システム管理

11 - 謝辞

QX-W1200 シリーズ アクセスポイント

オペレーションマニュアル

1. はじめに

本マニュアルは以下に示す章で構成されています。

01-CLI の概要

02-RBAC

03-ログイン

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-SNMP によるログイン

08-ログインユーザの制御

09-FTP

10-TFTP

11-ファイルシステム管理

12-コンフィグレーションファイル管理

13-ソフトウェアのアップグレード

14-装置管理

15-Auto Config

16-Tcl の使用

目次

このセクションのページは **1-x-x** です。

1 章 CLI の概要 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 1-3
1.4.1 コマンドラインの編集 1-3
1.4.2 引数の文字列あるいはテキストタイプ値の入力 1-4
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 1-5
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 1-7
1.4.7 情報の同期出力 1-8
1.5 コマンドラインのエラーメッセージ 1-8
1.6 履歴コマンドの保存 1-9
1.7 コマンド履歴バッファの管理と使用 1-10
1.7.1 コマンド履歴バッファ内のコマンドの表示 1-10
1.7.2 コマンド履歴バッファ内のコマンドの呼び出し 1-10
1.7.3 コマンド履歴バッファでコマンドの繰り返し 1-10
1.8 CLI 表示の管理 1-11
1.8.1 出力のスクリーンの休止 1-11
1.8.2 表示コマンドの各出力ラインの番号表示 1-11
1.8.3 出力のフィルタリング 1-12
1.8.4 display コマンドのファイルへの保存 1-14
1.8.5 display コマンドからの出力の有効的な表示、管理 1-15
1.9 稼働中の設定の保存 1-16

1章 CLI の概要

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 1-1 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[AP-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。

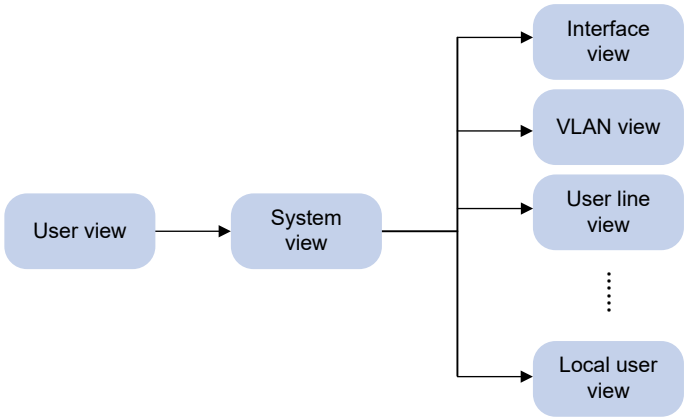


図 1-1 CLI views

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**

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。

```
<AP> ?
User view commands:
  archive           Archive configuration
  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。

```
<AP> 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。

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

```
<AP> b?
  backup       Backup operation
  boot-loader  Software image file management
  bootrom      Update/read/backup/restore bootrom
<AP> 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 7.1.064, ESS 5103 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
CMTunnel	CMTunnel
Dialer	Dia
GigabitEthernet	GE
LoopBack	Loop
NULL	NULL
Tunnel	Tun
Virtual-Template	VT
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

エイリアス	コマンド
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

CLI を補助するため、表 1-4 にホットキーを定義します。またデフォルトで指定済みのホットキーを示します。ホットキーを押すことでコマンドを入力することと同じことを行うことができます。これらのホットキーは装置が定義しています。

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** { **ctrl_g** | **ctrl_l** | **ctrl_o** | **ctrl_t** | **ctrl_u** } *command*	デフォルト： ● **Ctrl+G**は**display current-configuration**コマンドを表示します。 ● **Ctrl+L**は**display ip routing-table**コマンドを表示します。 ● **Ctrl+O**は **undo debugging all**コマンドを表示します。 ● **Ctrl+T**コマンドと**Ctrl+U**コマンドは未割り当てです。
3． （オプション設定項目）ホットキーを表示する	**display hotkey**	すべてのviewで実行可能です。

表 1-4 システムで予約済みのホットキー

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+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+N	履歴バッファの次のコマンドを表示します。
Ctrl+P	履歴バッファの前のコマンドを表示します。
Ctrl+R	現在の行のコマンドを再表示します。
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。
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 詳細はコマンドマニュアルのセクション10 *システム管理 "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。	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、コマンドマニュアルのセクション 1 *はじめに “ログイン”* 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。

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

1.8.3 出力のフィルタリング

display コマンドに、**|** { **begin** | **exclude** | **include** } *regular-expression* 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。

- **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。
|	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。

文字	意味	例
( )	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。

```
<AP> display current-configuration | begin line
#
line con 0
 user-role network-admin
#
line vty 0 4
 authentication-mode scheme
 user-role network-operator
#
 ssh server enable
#
return
```

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。

```
<AP> 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。

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

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。

<AP> 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。

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

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

```
<AP> 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。

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

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

1.8.5 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*] [**>** *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。

```
<AP> 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。

```
<AP> 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。

```
<AP> 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。

詳細はコマンドマニュアルのセクション 1 *はじめに “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 **1-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 2-5
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 2-6
2.6 リソースアクセスポリシーの設定 2-7
2.6.1 ユーザロールのインタフェースポリシーの設定 2-7
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 2-8
2.7.1 デフォルトユーザロール機能の有効化 2-8
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 2-9
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 2-10
2.8 一時的なユーザロールの許可設定 2-11
2.8.1 設定ガイドライン 2-11
2.8.2 ユーザロールの認証の設定 2-12
2.8.3 一時的なユーザロールの許可の取得 2-13
2.9 RBAC 設定の表示と維持 2-13
2.10 RBAC の設定例 2-14
2.10.1 ローカル AAA 認証ユーザの RBAC の設定例 2-14
2.10.2 RADIUS 認証ユーザの RBAC の設定例 2-16
2.10.3 RBAC の一時的なユーザロールの許可の設定例 2-19
2.11 RBAC のトラブルシューティング 2-22
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 2-22
2.11.2 RADIUS ユーザによるログインが常に失敗する 2-22

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。(オペレーションマニュアルのセクション 1 *はじめに “RBAC”の “ユーザロールのルール”*を参照してください。)
- 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。(オペレーションマニュアルのセクション 1 *はじめに “RBAC”の “リソースアクセスポリシー”*を参照してください)

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 **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。ユーザロールのルールの優先順位はオペレーションマニュアルのセクション 1 *はじめに "RBAC"の "ユーザロールのルールの設定"*を参照してください。

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。**display security-logfile summary**コマンド、**info-center security-logfile directory**コマンド、 **security-logfile save**コマンドを除きます。
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、SSH 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”*、*“SSH”* を参照してください。ユーザラインの詳細は、オペレーションマニュアルのセクション 1 *はじめに “ログイン”*、および *“CLI によるログイン”* 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

ユーザロールはアクセス管理を行うために、作成することができます。あらかじめ定義されたユーザロールに加えて、64 個まで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に対して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	• コマンドのルール： **rule** *number* { **deny** | **permit** } **command** *command-string* • 機能のルール： **rule** *number* { **deny** | **permit** } { **execute** | **read** | **write** } * **feature** [*feature-name*] • 機能グループのルール： **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**	ー
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**	―
2． user role view に移行する	**role name** *role-name*	―
3． ユーザロールの interface policy view へ移行する	**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**	―
2． user role view に移行する	**role name** *role-name*	―
3． ユーザロールの VLAN policy view へ移行する	**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(オペレーションマニュアルのセクション 1 *はじめに　“RBAC”の“ユーザロールの割り当て”*を参照してください)で割り当てる手順が異なります。AAA 認証の詳細は、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。

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、RADIUS サーバのマニュアル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オペレーションマニュアルのセクション 1 *はじめに　"ログイン"*、および *"CLI によるログイン"* を参照してください。SSH 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"* 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**	―
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*] | { **console** | **vty** } *first-num2* [*last-num2*] } ● user line class viewに移行する： **line class** { **console** | **vty** }	user line viewとuser line class viewの優先順位と設定方法については、オペレーションマニュアルのセクション1 *はじめに　"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：console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。

キーワード	認証モード	記述
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。 ● 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VTYユーザ用にリモートAAA認証を実行します。 ● AUXユーザは文字列を入力するか、何も入力しないでEnterキーを押すことで一時的なユーザロールを取得することができます。
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) 一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 一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一時的な許可を取得する	**super** [*rolename*]	[*rolename*]を指定しない場合、一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*]
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。

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

Telnet サーバを有効にします。

```
[AP] 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。

```
[AP] line vty 0 4
[AP-line-vty0-4] authentication-mode scheme
[AP-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。

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

ユーザロール **role1** を作成します。

```
[AP] 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。

```
[AP-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。

```
[AP-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。

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

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

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

```
[AP-luser-manage-user1] password simple aabbcc
```

サービスタイプを Telnet に設定します。

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

ユーザにユーザロール **role1** を割り当てます。

```
[AP-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。

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

III. 設定の確認

AP に Telnet を行い、AP 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。

```
<AP> system-view
[AP] vlan 10
[AP-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。

```
[AP] 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。

```
[AP] display clock
09:31:56 UTC Sat 01/01/2011
[AP] 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。

```
<AP> debugging role all
Permission denied.
<AP> 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。

AP 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。

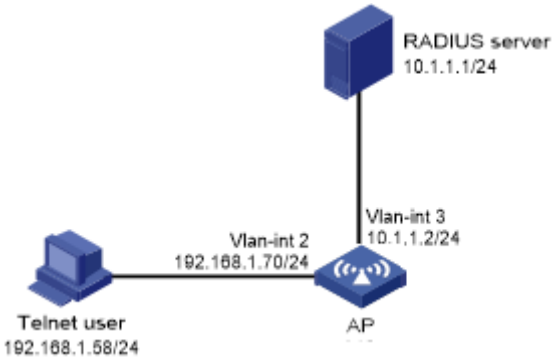


図 2-2 ネットワーク図

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)　AP 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。

```
<AP> system-view
[AP] interface vlan-interface 2
```

```
[AP-Vlan-interface2] ip address 192.168.1.70 255.255.255.0
[AP-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。

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

Telnet サーバを有効にします。

```
[AP] 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。

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

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

```
[AP] 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。

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

AP 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。

```
[AP-radius-rad] key authentication simple expert
[AP-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。

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

機能グループ **fgroup1** を作成します。

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

機能グループに機能 **arp**、**radius** を追加します。

```
[AP-featuregrp-fgroup1] feature arp
[AP-featuregrp-fgroup1] feature radius
```

```
[AP-featuregrp-fgroup1] quit
```

ユーザロール **role2** を作成します。

```
[AP] 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。

```
[AP-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。

```
[AP-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。

```
[AP-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。

```
[AP-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。

```
[AP-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。

```
[AP-role-role2] vlan policy deny
[AP-role-role2-vlanpolicy] permit vlan 1 to 20
[AP-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)

AP 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

AP に Telnet し、AP 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。

```
<AP> system-view
[AP] domain abc
[AP-isp-abc] authentication login radius-scheme abc
[AP-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。

```
[AP] radius scheme rad
[AP-radius-rad] primary authentication 2.2.2.2
[AP-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。

```
[AP] vlan 10
[AP-vlan10] quit
[AP] 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。

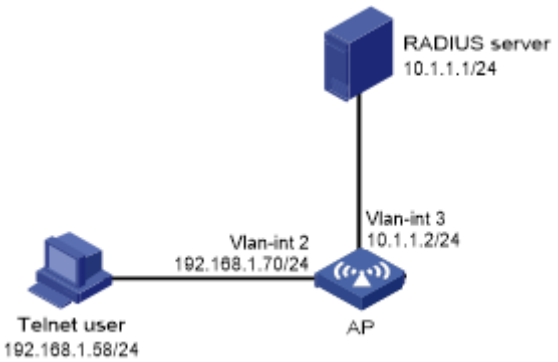


図 2-3 ネットワーク図

II. 設定手順

1)　AP 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。

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

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

Telnet サーバを有効にします。

```
[AP] 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。

```
[AP] line vty 0 15
[AP-line-vty0-15] authentication-mode scheme
[AP-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。

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

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

```
[AP] 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。

```
[AP-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。

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

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

```
[AP] 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。

```
[AP-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。

```
[AP-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。

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

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

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

ユーザのサービスタイプを Telnet に設定します。

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

ユーザのパスワードを **aabbcc** に設定します。

```
[AP-luser-manage-test] password simple aabbcc
```

level-0 をユーザに割り当てます。

```
[AP-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。

```
[AP-luser-manage-test] undo authorization-attribute user-role network-operator
[AP-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 abcdef654321 に設定します。

```
[AP] super password role network-admin simple abcdef654321
[AP] 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)　AP に Telnet 接続を行い、ユーザ名 test@bbb、パスワード aabbcc 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。

```
<AP> 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:
<AP>?
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

<AP>
```

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。

```
<AP> 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 abcdef654321 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 **1-x-x** です。

3 章 ログイン..... 3-1

3章 ログイン

初回の装置へのログインは、コンソールポート、Telnet 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やコンソール、Telnet、SSH、Web コンソール、SNMP、のログイン方法に変更することができます。

本マニュアルに登場する「FIT」という用語は、特に断りがない場合、Anchor-FIT モードで動作する AP のことを含みます。

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、デフォルトのパスワードはqx_admin、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有効、デフォルトのパスワードはqx_admin、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。
	SSH接続によるログイン（FITは未サポート）	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コンソールによるログイン（FITは未サポート）		QX-W1240のソフトウェアバージョン7.5.129を含む以降のソフトウェアおよび、QX-W1200のソフトウェアバージョン7.5.143bを含む以降のソフトウェアでは、デフォルトでWebコンソールへアクセス可能です。 🕮 メモ 詳細はQX-W1200シリーズインスタレーションマニュアルのセクション４起動と設定“装置の操作”の“Webコンソールによる接続”を参照してください。
SNMPからのアクセス（FITは未サポート）		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 **1-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装置にログインするには、コンソール端末（例 PC）と端末エミュレーションプログラム（例 Windows の HyperTerminal）などのユーザ端末の関連設定をコンソールポートと同じにしなければなりません。Windows Server 2003 では手動で HyperTerminal を追加する必要があります。Windows Server2008、Windows7、Windows Vista、またはほかのオペレーティングシステムではサードパーティの端末エミュレーションプログラムを取得し、インストールする必要があります。ほかのターミナル端末エミュレーションプログラムの使い方については、プログラムのユーザズガイドあるいはオンラインヘルプを見てください。

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。

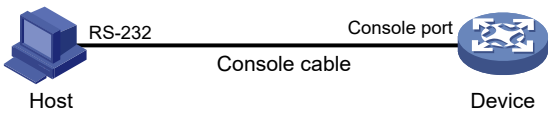


図 4-1 コンソールポートとの接続

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（Windows のハイパーターミナルなど）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

図 4-2 から図 4-4 は Windows のハイパーターミナルでの設定を示します。Windows サーバ 2003 ではハイパーターミナルを最初に追加し、装置にログインする手順に従ってください。Windows 2008 サーバ、Windows 7 などその他の Windows OS や、ほかの OS ではサードパーティの端末エミュレータを起動してください。

a) スタートボタンをクリックします。
b) メニューからすべてのプログラム ＞ アクセサリ ＞ 通信 ＞ハイパーターミナルを選

択します。

装置にシリアルポートが接続されていることを確認します。

a)　デスクトップにあるマイコンピュータアイコンを右クリックします。

b)　コンピュータ管理ウィンドウ画面で管理を選択します。

c)　ナビゲーションツリーからシステムツール＞デバイスマネージャーを選択します。

d)　ポート（COM＆LPT）を選択します。

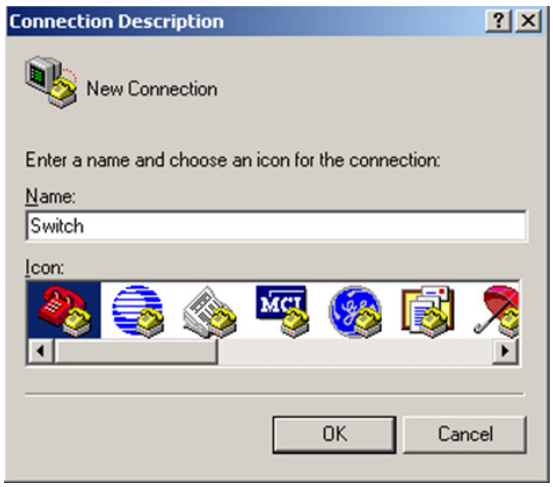


図 4-2 接続の作成



図 4-3 シリアルポートの設定

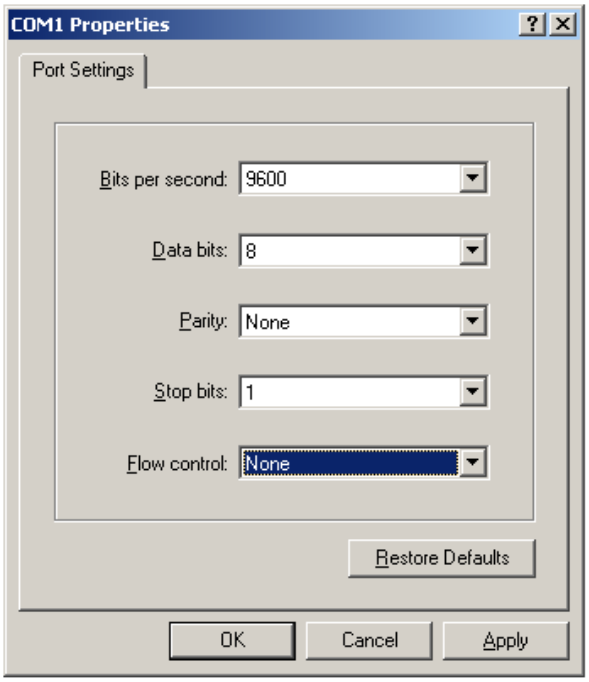


図 4-4 シリアルポートのプロパティの設定

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 **1-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 None 認証の設定 5-3
5.2.2 Password 認証の設定 5-4
5.2.3 Scheme 認証の設定 5-4
5.2.4 console ユーザラインの共通設定 5-5
5.3 Telnet からのログイン 5-7
5.3.1 装置の Telnet ログインの設定 5-7
5.3.2 装置から Telnet サーバへの Telnet 接続 5-13
5.4 SSH からのログイン 5-13
5.4.1 SSH ログインの設定 5-13
5.4.2 装置から SSH サーバへの SSH 接続 5-15
5.5 CLI ログインの表示と維持 5-15

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、オペレーションマニュアルのセクション 1 *はじめに “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
コンソールユーザライン	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、コンソールと 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、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。

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オペレーションマニュアルのセクション 1 *はじめに* *“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。

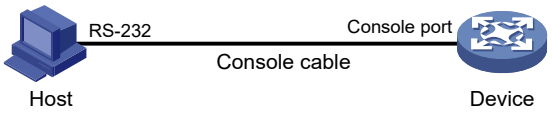


図 5-1 コンソールポートによるログイン

デフォルトでコンソールポートは有効です。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用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）コンソール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 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. 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。 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

操作	コマンド	備考
		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**
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。

5.2.2 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． 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。 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． Password 認証モードを有効にする	**authentication-mode password**	デフォルト：**password**
4． password を設定する	**set authentication password** { **hash** | **simple** } *password*	デフォルト：**qx_admin**
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。

5.2.3 Scheme 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． 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。 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：**password**

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。

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。

5.2.4 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． 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。 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。

操作	コマンド	備考
		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。
6． データビットを設定する	**databits** { **5** | **6** | **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	**auto-execute command**	デフォルト：無効

操作	コマンド	備考
user line 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	*command*	ユーザが現在のuser line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console line viewあるいはconsole line class viewでサポートしていません。
13．端末サービスを有効にする	**shell**	デフォルト：有効 console line viewあるいはconsole line class viewでコマンドは**undo shell**サポートしていません。

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。

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	―
（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）現在のTelnetユーザの最大数の設定	―
（オプション設定項目）出力telnetパケットのDSCP値の設定	―
（オプション設定項目）VTYユーザラインの共通設定	―

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． Telnet サーバを有効化する	**telnet server enable**	デフォルト：有効

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
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** 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： VTY line viewは**network-operator**。 VTY line class viewは**network-admin**です。

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。

```
<AP>
```

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

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、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** 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：**qx_admin**
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： VTY line view：**network-operator** VTY line class view：**network-admin**

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:
<AP>
```

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**	—

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、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． Scheme 認証を有効にする	**authentication-mode scheme**	デフォルト：**password** 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。

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:
<AP>
```

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． Telnet サービスのポート番号を指定する	● IPv4ネットワーク： **telnet server port** *port-number*	デフォルト：23
3． 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、ToS、IPのトラフィックフィールド、IPパケットで運ばれます。
4． 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。

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。

操作	コマンド	備考
		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。
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：** user lineにこのコマンドを実行すると、user lineによるCLIアクセスができなくなる可能性があります。このコマンドを設定する前に、異なるuser lineあるいはconsole 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”* 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、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”、“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** | **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． （オプション設定項目）SSH ユーザを生成し、認証モードを指定する	**ssh user** *username* **service-type stelnet authentication-type** { **password | { any | password-publickey | publickey** } **assign publickey** *keyname* }	デフォルト：設定なし
5． 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。
6． scheme 認証を有効にする	**authentication-mode scheme**	デフォルト：**password** 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。
7． （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、

操作	コマンド	備考
		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。
8． system view から戻る	**quit**	—
9． （オプション設定項目）VTY ユーザラインの共通設定	オペレーションマニュアルのセクション1 *はじめに* *“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。	—
10． （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。

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については、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”* 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* | { **console** | **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**	―
特定のユーザラインを解放する	**free line** { *num1* | { **console** | **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* | { **console** | **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 **1-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 6-3
6.3 Web ログインの表示と維持 6-5
6.4 Web ログインの設定例 6-6
6.4.1 HTTP ログインの設定例 6-6

6章 Web コンソールによるログイン

🕮 **メモ：**

Web コンソールによるログインは、ソフトウェアバージョン 7.5.114 を含む以降のソフトウェアからサポートしています。

装置は HTTP（1.0、1.1）と HTTPS を使用して Web コンソール機能（Web サーバ機能）をサポートしています。端末の Web ブラウザを使用して、装置の Web コンソールにアクセスしてログインし、装置を管理できます。

HTTPS はクライアントとサーバ間で交換するデータの完全性とセキュリティを保証するため SSL を使用しています。HTTP よりも安全です。正当なクライアントのみが Web インタフェースにアクセスできるように証明書ベースのアクセス管理ポリシーを定義することができます。

⚠ **重要：**

- QX-W1240 のソフトウェアバージョン 7.5.129 以降および、QX-W1200 のソフトウェアバージョン 7.5.143b 以降では FAT モードおよび Anchor-AC モードにおいて、Web コンソール機能がデフォルトで有効になっています。上記条件に該当しない場合（QX-W1240 のソフトウェアバージョンが 7.5.114 を含む以前のソフトウェア、QX-W1200 のソフトウェアバージョンが 7.5.142a を含む以前のソフトウェア）は、装置で Web コンソール接続用の設定を行う必要があります。
- QX-W1240 のソフトウェアバージョン 7.5.129 を含む以降のソフトウェアおよび、QX-W1200 のソフトウェアバージョン 7.5.143b を含む以降のソフトウェアをご利用の場合は QX-W1200 シリーズアクセスポイントインスタレーションマニュアルのセクション４起動と設定“装置の操作”の“ Web コンソールによる接続”を参照し、装置へログインしてください。

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**	ー
2． HTTP サービスを有効にする	**ip http enable**	デフォルト：無効 🕮メモ： QX-W1240のソフトウェアバージョン7.5.129を含む以降のソフトウェアおよび、QX-W1200のソフトウェアバージョン7.5.143bを含む以降のソフトウェアでは、デフォルトで有効です。
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

操作	コマンド	補足
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。
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 🕮メモ： QX-W1240のソフトウェアバージョン7.5.129を含む以降のソフトウェアおよび、QX-W1200のソフトウェアバージョン7.5.143bを含む以降のソフトウェアでは、デフォルトで“admin”ユーザが作成されています。
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。 🕮メモ： QX-W1240のソフトウェアバージョン7.5.129を含む以降のソフトウェアおよび、QX-W1200のソフトウェアバージョン7.5.143bを含む以降のソフトウェアでは、デフォルトで“necqx_admin”が設定されています。
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

操作	コマンド	補足
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 📖メモ： QX-W1240のソフトウェアバージョン7.5.129を含む以降のソフトウェアおよび、QX-W1200のソフトウェアバージョン7.5.143bを含む以降のソフトウェアでは、デフォルトで有効です。

6.2 HTTPSログインの設定

装置は HTTPS ログインモードをサポートします。

- **Simplified モード**—装置は自己署名の証明書（装置自身によって作成し署名された証明書）、およびデフォルトの SSL の設定を使用します。装置は装置で HTTPS サービスを有効にしたのち Simplified モードで動作します。
- **Secure モード**—装置は CA、およびセキュリティを保証するためユーザ定義のセキュリティ保護の設定によって署名された証明書を使用します。Secure モードで動作させるため以下の処理を行う必要があります。
  - □ 装置で HTTPS サービスを有効にします。
  - □ サービスの SSL サーバポリシーを指定します。
  - □ PKI ドメインのパラメータを設定します。

Simplified モードは設定が容易ですが Secure モードに比べてセキュリティが高くありません。Secure モードは設定が複雑ですが、Secure モードより高いセキュリティを提供します。

SSL、PKI 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 "SSL"、"PKI"* 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．　HTTPS サービスを有効にする	**ip https enable**	デフォルト：無効 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が開始します。 ● 装置でローカル認証がある場合、SSLハンドシェイクは成功し、HTTPSサービスが開始します。 ● 装置でローカル証明書がない場合、証明書アプリケーション処理が開始します。証明書アプリケーション処理は時間がかかるため、SSLハンドシェイクのネゴシエーションが失敗し、HTTPSサービスが開始しない可能性があります。この問題に対応するためHTTPSサービスが有効になるまで再度コマンドを実行してください。 ● 🕮メモ：QX-W1240のソフトウェアバージョン7.5.129を含む以降のソフトウェアおよび、QX-W1200のソフトウェアバージョン7.5.143bを含む以降のソフトウェアでは、デフォルトで有効です。
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。

操作	コマンド	補足
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 🕮メモ： QX-W1240のソフトウェアバージョン7.5.129を含む以降のソフトウェアおよび、QX-W1200のソフトウェアバージョン7.5.143bを含む以降のソフトウェアでは、デフォルトで“admin”ユーザが作成されています。
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。 🕮メモ： QX-W1240のソフトウェアバージョン7.5.129を含む以降のソフトウェアおよび、QX-W1200のソフトウェアバージョン7.5.143bを含む以降のソフトウェアでは、デフォルトで“necqx_admin”が設定されています。
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 🕮メモ： QX-W1240のソフトウェアバージョン7.5.129を含む以降のソフトウェアおよび、QX-W1200のソフトウェアバージョン7.5.143bを含む以降のソフトウェアでは、デフォルトで有効です。

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**

操作	コマンド
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。

```
<AP> system-view
[AP] vlan 100
[AP-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。

```
[AP] interface vlan-interface 100
[AP-Vlan-interface100] ip address 192.168.100.99 24
[AP-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。

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

HTTP を有効にします。

```
[AP] 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 **1-x-x** です。

7 章 SNMP によるログイン..... 7-1

7章 SNMP によるログイン

NMS で SNMP を実行することで、装置の MIB の GET、SET を行い、装置の管理/設定を行うことができます。

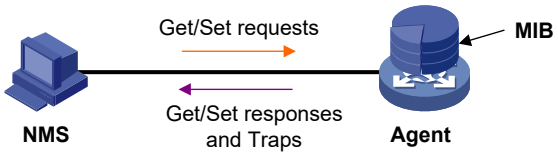


図 7-1 SNMP アクセス

装置は SNMPv1、SNMPv2c、SNMPv3 をサポートし、さまざまなネットワーク管理製品で動作します。NMS は同じ SNMP のバージョンを使用する必要があります。

SNMP に関する詳細はオペレーションマニュアルのセクション 10 *システム管理 “SNMP”* を参照してください。

デフォルトで SNMP によるログインはできません。他の方法で装置にログインして、SNMP によるアクセスを可能にする為の設定を行う必要があります。

目次

このセクションのページは **1-x-x** です。

8 章 ログインユーザの制御 8-1
8.1 Telnet/SSH ログインの制御 8-1
8.1.1 設定手順 8-1
8.1.2 設定例 8-2
8.2 SNMP ログインの制御 8-3
8.2.1 設定手順 8-3
8.2.2 設定例 8-4

8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 の詳細はオペレーションマニュアルのセクション 8 *ACL and QoS　"ACL"* を参照してください。

8.1 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。

8.1.1 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** *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** *acl-number*	デフォルト：ACLはなし 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 "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。

8.1.2 設定例

I. ネットワーク要件

図 8-1 に示すように装置が 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。

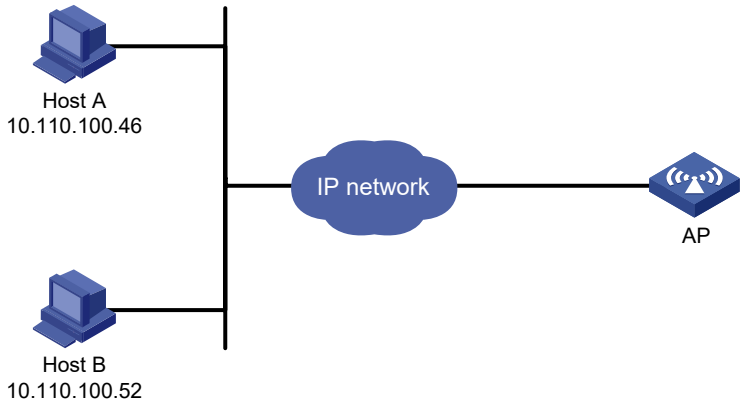


図 8-1 ネットワーク図

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。

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

```
[AP] telnet server acl 2000
```

8.2 SNMPログインの制御

送信元 IP アドレスによって SNMP アクセスを制御する標準 ACL（2000～2999）を使用します。要求された MIB view にアクセスするため、NMS は ACL によって許可された送信元 IP アドレスを使用する必要があります。

8.2.1 設定手順

以下に SNMPv1/v2c アクセス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． SNMP v1/v2 コミュニティ、グループ、ユーザに ACL を適用する	● SNMPコミュニティを作成し、ACLを適用する：**snmp-agent community** { **read** | **write** } [**simple** | **cipher**] *community-name* [**mib-view** *view-name*] [**acl** *acl-number*] * ● SNMPv1/v2cグループを作成し、グループにユーザを追加し、その後ACLを適用する： 1． **snmp-agent group** { **v1** | **v2c** } *group-name* [**read-view** *view-name*] [**write-view** *view-name*] [**notify-view** *view-name*] [**acl** *acl-number*] * 2． SNMPv1/v2c ユーザ：**snmp-agent usm-user** { **v1** | **v2c** } *user-name group-name* [**acl** *acl-number*] *	SNMPに関する詳細はオペレーションマニュアルのセクション10 *システム管理* *"SNMP"* を参照してください。

以下に SNMPv3 アクセス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． SNMPv3 グループに ACL を適用する	**snmp-agent group v3** *group-name* [**authentication** | **privacy**] [**read-view** *view-name*] [**write-view** *view-name*] [**notify-view** *view-name*] [**acl** *acl-number*] *	―
3． SNMPv3 ユーザに ACL を適用する	**snmp-agent usm-user v3** *user-name group-name* [{ **cipher** | **simple** } **authentication-mode** { **md5** | **sha** } *auth-password* [**privacy-mode** { **aes128** | **3des** | **des56** } *priv-password*]] [**acl** *acl-number*] *	SNMPに関する詳細はオペレーションマニュアルのセクション10 *システム管理* *"SNMP"* 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。

8.2.2 設定例

I. ネットワーク要件

図 8-2 に示すように AP が Host A と Host B からの SNMP のアクセスを許可するように設定します。

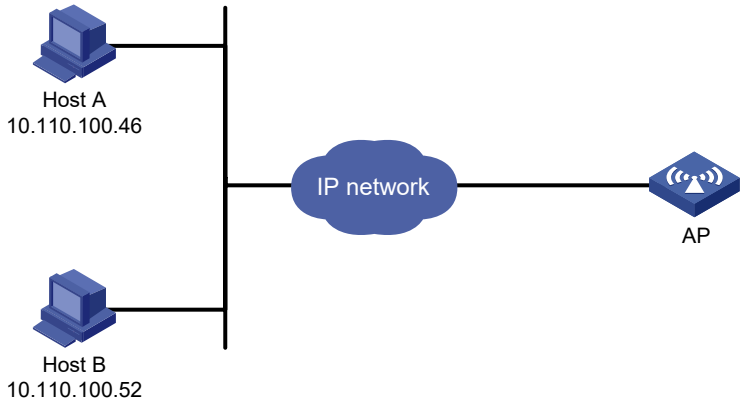


図 8-2 ネットワーク図

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。

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

HTTP に ACL を適用し、Host B の Web ユーザだけが AP にアクセスできるようにします。

```
[AP] ip http acl 2030
```

目次

このセクションのページは **1-x-x** です。

9 章 FTP 9-1
9.1 FTP クライアントの使用 9-1
9.1.1 FTP 接続の確立 9-1
9.1.2 FTP サーバのディレクトリの管理 9-2
9.1.3 FTP サーバの動作 9-2
9.1.4 別のユーザアカウントへの変更 9-3
9.1.5 FTP 接続の維持とトラブルシューティング 9-3
9.1.6 FTP 接続の終了 9-4
9.1.7 表示コマンドとヘルプ情報 9-4
9.1.8 FTP クライアントの表示と維持 9-4
9.1.9 FTP クライアント設定例 9-4

9章 FTP

FTP（File Transfer Protocol）は、図 9-1 に示すように、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、ファイルのアップロ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。AP は FTP クライアントとして動作することができます。



図 9-1 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。

9.1 FTPクライアントの使用

9.1.1 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**	—

操作	コマンド	補足
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* }]] * • （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。

9.1.2 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*

9.1.3 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*	—
FTP転送モードを設定する	• ASCII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*	—

9.1.4 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*]

9.1.5 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**	—

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

9.1.6 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**
FTPサーバとの接続を切断し、user viewに戻る	• **bye** • **quit**

9.1.7 表示コマンドとヘルプ情報

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*]

9.1.8 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**

9.1.9 FTP クライアント設定例

I. ネットワーク要件

図 9-2 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 **123456** 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 AP 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。

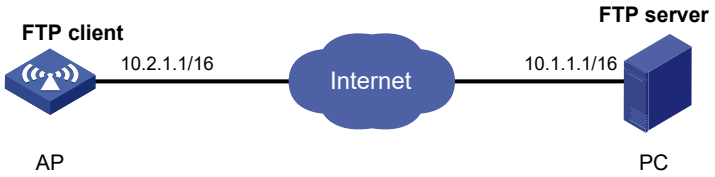


図 9-2 ネットワーク図

II. 設定手順

#図 9-2 に示すように IP アドレスを設定し、AP 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。）

AP 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 **123456** を使用して、FTP サーバ 10.1.1.1 にログインします。

```
<AP> 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 AP 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、AP 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.
<AP>
```

目次

このセクションのページは **1-x-x** です。

10 章 TFTP 10-1
10.1 TFTP クライアントの設定 10-1

10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 10-1 TFTP アプリケーションシナリオ

10.1 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* }] *	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 **1-x-x** です。

11 章 ファイルシステム管理 11-1
11.1 概要 11-1
11.1.1 ファイルシステム 11-1
11.1.2 ディレクトリ 11-1
11.1.3 ファイル 11-2
11.1.4 ディレクトリ、ファイル名の指定 11-3
11.2 ファイルシステムの管理の制限とガイドライン 11-3
11.3 ファイルシステムの管理 11-4
11.3.1 記憶媒体のフォーマット 11-4
11.3.2 記憶媒体の回復 11-4
11.4 ディレクトリの管理 11-4
11.4.1 ディレクトリ情報の表示 11-4
11.4.2 カレント作業ディレクトリの表示 11-5
11.4.3 カレント作業ディレクトリの変更 11-5
11.4.4 ディレクトリの作成 11-5
11.4.5 ディレクトリ名の変更 11-5
11.4.6 ディレクトリのアーカイブ（圧縮）/解凍 11-5
11.4.7 ディレクトリの削除 11-6
11.4.8 ディレクトリの動作モードの設定 11-6
11.5 ファイルの管理 11-6
11.5.1 ファイル情報の表示 11-6
11.5.2 テキストファイルの内容表示 11-6
11.5.3 ファイル名の変更 11-7
11.5.4 ファイルのコピー 11-7
11.5.5 ファイルの移動 11-7
11.5.6 ファイルの圧縮/解凍 11-7
11.5.7 ファイルのアーカイブ（圧縮）/解凍 11-7
11.5.8 ファイルの削除/回復 11-8
11.5.9 ごみ箱のファイルを削除する 11-8
11.5.10 ファイルの動作モードの設定 11-8

11章 ファイルシステム管理

11.1 概要

11.1.1 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。

11.1.2 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。
- **logfile**—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。

11.1.3 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

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。

11.1.4 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 11-1 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 11-1 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 11-1 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

11.2 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。

11.3 ファイルシステムの管理

11.3.1 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** *filesystem*

11.3.2 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*

11.4 ディレクトリの管理

11.4.1 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**]

11.4.2 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**

11.4.3 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* | **..** | */* }

11.4.4 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*

11.4.5 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*

11.4.6 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*

11.4.7 ディレクトリの削除

ディレクトリを削除する場合、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削除する必要があります。ファイルを削除する場合、**delete** コマンドを使用します。サブディレクトリを削除する場合、 **rmdir** コマンド使用します。

ディレクトリを完全に削除すると、ごみ箱のディレクトリ内のすべてのファイルは自動的に完全に削除されます。

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*

11.4.8 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。

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。

11.5 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オペレーションマニュアルのセクション 1 *はじめに “FTP”、“TFTP”* を参照してください。**save** コマンドについてはコマンドマニュアルのセクション 1 *はじめに “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。

11.5.1 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**]

11.5.2 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*

11.5.3 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*

11.5.4 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* } [**source interface** *interface-type interface-number*]

11.5.5 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* }

11.5.6 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*

11.5.7 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*

11.5.8 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*
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。

11.5.9 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。

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**]

11.5.10 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**	―

操作	コマンド	補足
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 **1-x-x** です。

12 章 コンフィグレーションファイル管理 12-1
12.1 概要 12-1
12.1.1 コンフィグレーションタイプ 12-1
12.1.2 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 . 12-2
12.1.3 コンフィグレーションファイルのフォーマット形式 12-2
12.1.4 スタートアップコンフィグレーションファイルの選択..... 12-2
12.1.5 コンフィグレーションファイルの内容とフォーマット..... 12-3
12.2 2 つのコンフィグレーション設定の差分表示..... 12-3
12.3 カレントコンフィグレーションの保存..... 12-4
12.4 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 12-5
12.5 TFTP サーバへスタートアップコンフィグレーションファイルのバックアップ 12-5
12.6 TFTP サーバからスタートアップコンフィグレーションファイルの復元 12-6
12.7 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 12-7
12.8 コンフィグレーションファイルの表示と維持..... 12-7

12章 コンフィグレーションファイル管理

12.1 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、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。

12.1.1 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。

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。（詳細はオペレーションマニュアルのセクション 1 *はじめに “コンフィグレーションファイル管理”* の *“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”* 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。

12.1.2 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。

12.1.3 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。

12.1.4 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。

12.1.5 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。

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。

12.2 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*

操作	コマンド
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**

12.3 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。（オペレーションマニュアルのセクション 1 *はじめに“コンフィグレーションファイル管理”の“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”*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。

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。

12.4 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。

12.5 TFTPサーバへスタートアップコンフィグレーションファイルのバックアップ

バックアップを行う前に、以下の要件が完了していることを確認してください。

- 装置と TFTP サーバ間が通信可能であることを確認してください。
- TFTP サービスが有効にされていることを確認してください。
- 読み書き許可があることを確認してください。

以下に、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を TFTP サーバにバックアップする設定を示します。

操作	コマンド	補足
1.　（オプション設定項目）user view で指定されたスタートアップコンフィグレーションファイルを確認する	**display startup**	スタートアップコンフィグレーションファイルが指定されていない場合、バックアップは失敗します。
2.　user view で TFTP サーバにスタートアップコンフィグレーションファイルをバックアップする	**backup startup-configuration to** *ipv4-server* [*dest-filename*]	–

12.6 TFTPサーバからスタートアップコンフィグレーションファイルの復元

TFTP サーバから装置の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を復元します。

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を復元する前に、以下の要件が完了していることを確認してください。

- サーバが到達可能であることを確認してください。
- TFTP サービスが有効にされていることを確認してください。
- 読み書き許可があることを確認してください。

以下に TFTP サーバからスタートアップアップコンフィグレーションファイルを復元する操作を示します。

操作	コマンド	補足
1.　user view で TFTP サーバからスタートアップコンフィグレーションファイルを復元する	**restore startup-configuration from** *ipv4-server src-filename*	–
2.　（オプション設定項目）メインの次回の起動で使用するように指定されたコンフィグレーションファイルが設定されていることを確認する	**display startup** **display saved-configuration**	–

12.7 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。

12.8 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*]]]]
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**

操作	コマンド
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 **1-x-x** です。

13 章 ソフトウェアのアップグレード 13-1
13.1 概要 13-1
13.1.1 ソフトウェアタイプ 13-1
13.1.2 ソフトウェアファイル名の規則 13-1
13.1.3 Comware イメージの読み込み手順 13-1
13.1.4 システム起動プロセス 13-2
13.2 アップグレード方法 13-3
13.3 アップグレードの準備 13-3
13.4 アップグレード設定作業リスト 13-4
13.5 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 13-4
13.6 ソフトウェア設定の表示と維持 13-5
13.7 CLI によるソフトウェアアップグレード例 13-5

13章 ソフトウェアのアップグレード

13.1 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。

13.1.1 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。

13.1.2 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。

13.1.3 Comware イメージの読み込み手順

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。 Boot イメージとシステム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。

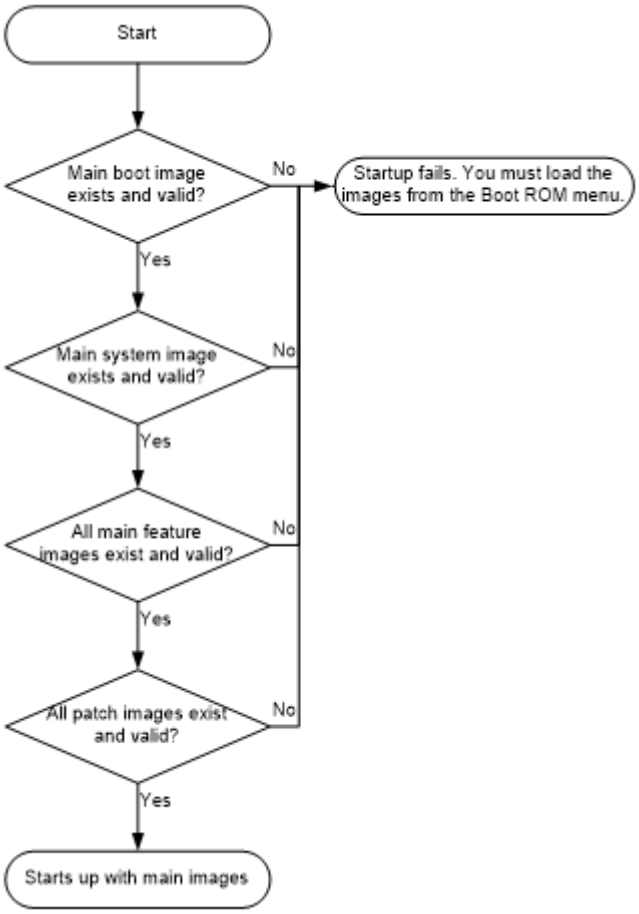


図 13-1 Comware イメージの読み込み手順の全体

13.1.4 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。

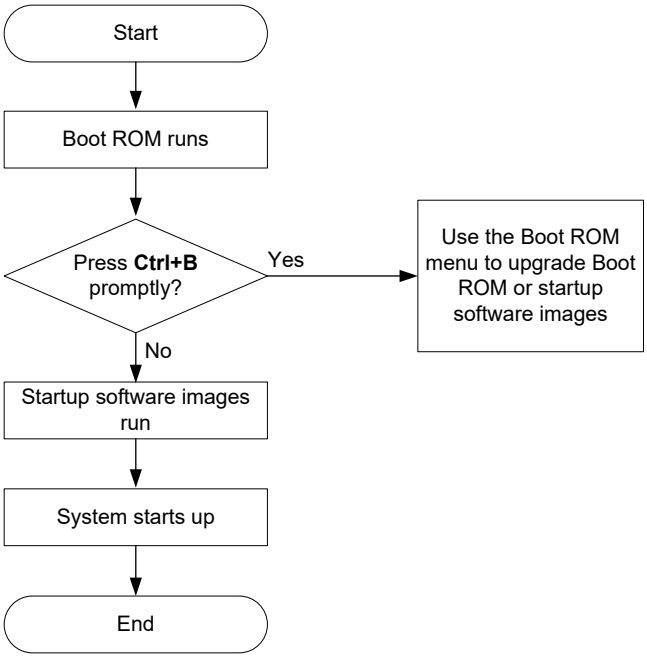


図 13-2 システム起動プロセス

13.2 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*インスタレーションマニュアル*を参照してください。

13.3 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、オペレーションマニュアルのセクション 1 *はじめに “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、オペレーションマニュアルのセクション 1 *はじめに “FTP”*、*“TFTP”* を参照してください。

13.4 アップグレード設定作業リスト

作業リスト	補足
（オプション設定項目）Boot ROMのBoot ROMイメージへの読み込み	ソフトウェアアップグレードを行う際、Boot ROMイメージのアップグレードが必要な場合、Comwareイメージをアップグレードする前に、このコマンドを使用してBoot ROMに新しいBoot ROMイメージをアップグレードします。このコマンドは、予期しない電気的な故障によってアップグレードの失敗が発生するリスクを減少させ、アップグレードを行う時間を削減することができます。 この作業を省略した場合、スタートアップソフトウェアイメージをアップグレードする際に装置は自動的にBoot ROMをアップグレードします。 Boot ROMイメージは装置を再起動したのち適用します。
（必須設定項目）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	―

13.5 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スタートアップファイルとしてアップグレードファイルを指定する	• アプローチ1：**boot-loader file** *ipe-filename* **main** • アプローチ2：**boot-loader file boot** *boot-package* **system** *system-package* **main**	アップグレードするファイルは装置の記憶媒体のルートディレクトリに保存する必要があります。 ファイル名が正しいことを確認してください。 アプローチ1が使用される場合、ファイル名は *storage-medium*:/*base-filename*.**ipe** を使用します。 例 flash:/startup.**ipe** アプローチ2が使用される場合、ファイル名は *storage-medium*:/*base-filename*.**bin** を使用します。 例 flash:/startup-boot.**bin**
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**	スタートアップ後、各装置はダウンロードされたBoot ROMイメージをRAMに読み込ませ、ファイルのスタートアップソフトウェアを読み込みます。
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。

13.6 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**

13.7 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

AP にファイル **QX-W1240.ipe** を使用してソフトウェアをアップグレードします。

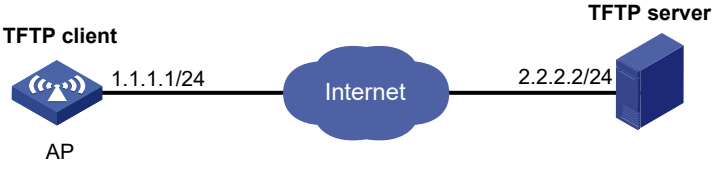


図 13-3 ネットワーク図

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。

```
<Switch> 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-W1240.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。

```
<Switch> tftp 2.2.2.2 get QX-W1240.ipe
```

メインスタートアップソフトウェアとして **QX-W1240.ipe** を指定します。

```
<Switch> boot-loader file flash:/QX-W1240.ipe main
```

スタートアップソフトウェアの設定を確認します。

```
<Switch> 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。

```
<Switch> 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。

```
<Switch> display version
```

目次

このセクションのページは **1-x-x** です。

14 章 装置管理 14-1
14.1 装置管理作業リスト 14-1
14.2 装置名の設定 14-1
14.3 システムクロックの設定 14-1
14.3.1 システムクロックソースの設定 14-1
14.4 AP の給電モードの設定 14-3
14.4.1 AP の給電モードの仕様 14-3
14.4.2 設定手順 14-5
14.5 バナーの設定 14-5
14.5.1 バナーの種類 14-5
14.5.2 バナー入力モード 14-6
14.5.3 設定手順 14-6
14.6 装置の再起動 14-7
14.6.1 CLI による装置の即時再起動 14-8
14.6.2 装置のスケジュール再起動 14-8
14.7 スケジュール自動実行の設定 14-8
14.7.1 設定の制限事項およびガイドライン 14-8
14.7.2 設定手順 14-9
14.7.3 スケジュール自動実行設定例 14-10
14.8 パスワードリカバリ機能の無効化 14-12
14.9 検出間隔の設定 14-12
14.10 CPU 使用率のモニタリングの設定 14-13
14.11 メモリ使用しきい値の設定 14-13
14.12 温度アラームしきい値の設定 14-15
14.13 トランシーバのパラメータ表示 14-15
14.13.1 トランシーバの情報表示 14-15
14.13.2 トランシーバの診断 14-16
14.14 装置管理の表示と維持 14-16

14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。

14.1 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）PoE+受電モードの設定
（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）装置の再起動
（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）パスワードリカバリ機能の無効化
（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）CPU使用率のモニタリングの設定
（必須設定項目）メモリ使用しきい値の設定

14.2 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

14.3 システムクロックの設定

14.3.1 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。装置は、以下のタイミングでシステム時間を FLASH に書き込みます。

- reboot コマンドにより装置を再起動する前
- 装置の稼働時間が 12 時間経過する毎
- AC または Anchor-AC に接続した時 (FIT/Anchor-FIT モードのみ)

- **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、オペレーションマニュアルのセクション 10 *システム管理 “NTP”* を参照してください。

ローカルシステム時刻を使用するように装置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**
3． user view に戻る	**quit**	－
4． ローカルシステムクロックを設定する	**clock datetime time date**	－
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。

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ように装置に NTP 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 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。

操作	コマンド	補足
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。

14.4 APの給電モードの設定

14.4.1 AP の給電モードの仕様

QX-W1240 は 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 以下に制限した PoE+(802.3at)給電での動作が可能です。

- 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。

QX-W1210、QX-W1220、QX-W1230、QX-W1210-E はこのコマンドによる制限をしなくても PoE+(802.3at)給電での動作が可能です。

表 14-1、表 14-2、表 14-3、表 14-4、表 14-5 に QX-W1200 シリーズの AP の給電モード設定時の動作仕様を示します。

表 14-1 QX-W1240 の給電モードの動作仕様

給電モード	必要な給電	10GE interface 最大リンク速度	USB interface 利用制限
High	PoE++	制限なし	制限なし
Middle	PoE+	5Gbps	使用不可
low	PoE+	2.5Gbps	使用不可

表 14-2 QX-W1230 の給電モードの動作仕様

給電モード	必要な給電	10GE interface 最大リンク速度	USB interface 利用制限
High	PoE+	制限なし	未サポート

Middle	PoE+	5Gbps	未サポート
low	PoE+	2.5Gbps	未サポート

表 14-3 QX-W1220 の給電モードの動作仕様

給電モード	必要な給電	10GE interface 最大リンク速度	USB interface 利用制限
High	PoE+	制限なし	未サポート
Middle	PoE+	5Gbps	未サポート
low	PoE+	2.5Gbps	未サポート

表 14-4 QX-W1210 の給電モードの動作仕様

給電モード	必要な給電	10GE interface 最大リンク速度	USB interface 利用制限
High	PoE+	制限なし	制限なし
Middle	PoE+	5Gbps	使用不可
low	PoE+	2.5Gbps	使用不可

表 14-5 QX-W1210-E の給電モードの動作仕様

給電モード	必要な給電	10GE interface 最大リンク速度	USB interface 利用制限
High	PoE+	制限なし	制限なし
Middle	PoE+	5Gbps	使用不可
low	PoE+	2.5Gbps	使用不可

14.4.2 設定手順

🕮 **メモ：**

- QX-W1210、QX-W1230 の AP は、ソフトウェアバージョン 7.5.129 を含む以降のソフトウェアから AP の給電モードの設定をサポートしています。
- QX-W1210-E は 2 個の 10GE ポートを搭載していますが、通信速度の変更対象は 10GE1 のみです。
- 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 enable**" 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。

以下に AP の給電モード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. AP の給電モードを設定する	**wlan power-level default { high | middle | low }**	デフォルト：**high**

14.5 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。

14.5.1 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。
- **Shell** バナー – ログインした後に表示します。

Legal バナー、MOTD バナー、ログインバナー、シェルバナーの順にバナーが表示されます。

14.5.2 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。

```
<AP> system-view
[AP] 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。

```
<AP> system-view
[AP] 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。

```
<AP> system-view
[AP] 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。

```
<AP> system-view
[AP] header shell AHave a nice day.
Please input banner content, and quit with the character 'A'.
A
```

14.5.3 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

操作	コマンド	補足
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* • 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

14.6 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、コマンドマニュアルのセクション 1　*はじめに　“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、コマンドマニュアルのセクション 1 *はじめに “コンフィグレーションファイル管理”*、*“ソフトウェアのアップグレード”*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。

14.6.1 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**]

14.6.2 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

14.7 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。

14.7.1 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、オペレーションマニュアルのセクション 10 *システム管理 “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。

14.7.2 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**	―
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**	―
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。

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**	―
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**	―
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

操作	コマンド	補足
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。

14.7.3 スケジュール自動実行設定例

I. ネットワーク要件

図 14-1 に示すように、AP は GigabitEthernet 1/0/1 を介して PC にアクセスします。

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。

- 毎週月曜日から金曜日の午前 8:00 にインタフェースを有効にします。
- 毎週月曜日から金曜日の 18:00 にインタフェースを無効にします。

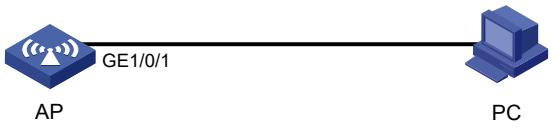


図 14-1 ネットワーク図

II. 設定手順

system view に移行します。

```
<AP> system-view
```

GigabitEthernet 1/0/1 を無効化する job を設定します。

```
[AP] scheduler job shutdown-GigabitEthernet1/0/1
[AP-job-shutdown-GigabitEthernet1/0/1] command 1 system-view
[AP-job-shutdown-GigabitEthernet1/0/1] command 2 interface gigabitethernet 1/0/1
[AP-job-shutdown-GigabitEthernet1/0/1] command 3 shutdown
[AP-job-shutdown-GigabitEthernet1/0/1] quit
```

GigabitEthernet 1/0/1 を有効化する job を設定します。

```
[AP] scheduler job start-GigabitEthernet1/0/1
[AP-job-start-GigabitEthernet1/0/1] command 1 system-view
```

```
[AP-job-start-GigabitEthernet1/0/1] command 2 interface gigabitethernet 1/0/1
[AP-job-start-GigabitEthernet1/0/1] command 3 undo shutdown
[AP-job-start-GigabitEthernet1/0/1] quit
```

毎週月曜日から金曜日の午前 8:00 にインタフェースを有効化する定期スケジュールを設定します。

```
[AP] scheduler schedule START-pc
[AP-schedule-START-pc] job start-GigabitEthernet1/0/1
[AP-schedule-START-pc] time repeating at 8:00 week-day mon tue wed thu fri
[AP-schedule-START-pc] quit
```

毎週月曜日から金曜日の 18:00 にインタフェースを無効化する定期スケジュールを設定します。

```
[AP] scheduler schedule STOP-pc
[AP-schedule-STOP-pc] job shutdown-GigabitEthernet1/0/1
[AP-schedule-STOP-pc] time repeating at 18:00 week-day mon tue wed thu fri
[AP-schedule-STOP-pc] quit
```

III. 設定の確認

全ての job に関する情報を表示します。

```
[AP] display scheduler job
Job name: shutdown-GigabitEthernet1/0/1
 system-view
 interface GigabitEthernet 1/0/1
 shutdown

Job name: start-GigabitEthernet1/0/1
 system-view
 interface GigabitEthernet 1/0/1
 undo shutdown
```

スケジュール情報を表示します。

```
[AP] display scheduler schedule
Schedule name        : START-pc
Schedule type        : Run on every Mon Tue Wed Thu Fri at 08:00:00
Start time           : Wed Feb 28 08:00:00 2017
Last execution time  : Wed Feb 28 08:00:00 2017
Last completion time : Wed Feb 28 08:00:03 2017
Execution counts     : 1
------------------------------------------------------------------------
Job name                                        Last execution status
start-GigabitEthernet1/0/1                              Successful
Schedule name        : STOP-pc
Schedule type        : Run on every Mon Tue Wed Thu Fri at 18:00:00
Start time           : Wed Feb 28 18:00:00 2017
Last execution time  : Wed Feb 28 18:00:00 2017
Last completion time : Wed Feb 28 18:00:01 2017
Execution counts     : 1
------------------------------------------------------------------------
Job name                                        Last execution status
shutdown-GigabitEthernet1/0/1                           Successful
```

スケジュールログ情報を表示します。

```
[AP] display scheduler logfile
```

```
Job name        : start-GigabitEthernet1/0/1
Schedule name   : START-pc
Execution time  : Wed Feb 28 08:00:00 2017
Completion time : Wed Feb 28 08:00:02 2017
---------------------------------                  Job                    output
-----------------------------------
```

<AP>system-view

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

[AP]interface gigabitethernet 1/0/1

[AP-GigabitEthernet1/0/1]undo shutdown

```
Job name        : shutdown-GigabitEthernet1/0/1
Schedule name   : STOP-pc
Execution time  : Wed Feb 28 18:00:00 2017
Completion time : Wed Feb 28 18:00:01 2017
---------------------------------                  Job                    output
-----------------------------------
```

<AP>system-view

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

[AP]interface gigabitethernet 1/0/1

[AP-GigabitEthernet1/0/1]shutdown

14.8 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 メニューからデバイス構成と SDRAM へのアクセスを制御できます。

パスワードリカバリ機能が有効の場合、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

14.9 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

14.10 CPU使用率のモニタリングの設定

CPU 使用率を検出するため、装置は以下の処理を行います。

- サンプリング間隔は 1 分間隔です。CPU 使用率のしきい値とサンプリング間隔を比較します。サンプリング間隔が CPU 使用率のしきい値に到達した場合、装置は trap を送信します。
- CPU 使用率の記録が有効である場合、設定した間隔で CPU 使用率を検出し、保存します。**display cpu-usage history** コマンドを使用して、最近の CPU 使用率を表示できます。

以下に CPU 使用率のモニ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． CPU 使用率のしきい値を設定する	**monitor cpu-usage threshold** *cpu-threshold*	デフォルト：99%
3． CPU 使用率トラッキングを有効化する	**monitor cpu-usage enable**	デフォルト：有効
4． display cpu-usage history コマンドの情報取得間 隔を設定する	**monitor cpu-usage interval** *interval*	デフォルト：1分
5． user view に戻る	**quit**	―
6． CPU 使用率の統計情報を表示する	**display cpu-usage**	すべてのviewで実行可能です。
7． 表で CPU 使用率履歴の統計情報を表示する	**display cpu-usage history** [**job** *job-id*]	すべてのviewで実行可能です。

🕮 **メモ：**

monitor cpu-usage interval コマンドは **display cpu-usage history** コマンドの情報を取得する間隔を表しています。**monitor cpu-usage threshold** コマンドの CPU 使用率を取得する間隔ではありません。

14.11 メモリ使用しきい値の設定

メモリ使用率をモニタするため、装置は以下の処理を行います。

- サンプリング間隔は 1 分です。メモリ容量がしきい値に達したとき、装置はトラップを作成し、送信します。
- 適切な動作とメモリ使用率を改善するため、装置はリアルタイムにおける空きメモリ容量をモニタリングします。空きメモリ容量がしきい値に達したとき、装置は alarm 通知あるいは alarm-removed 通知を生成し、関連するサービスモジュールあるいはプロセスに送信します。

表 14-6 と図 14-2 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。

- 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 14-6 Memory alarm 通知と memory alarm-removed 通知

通知	トリガー状況	補足
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
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

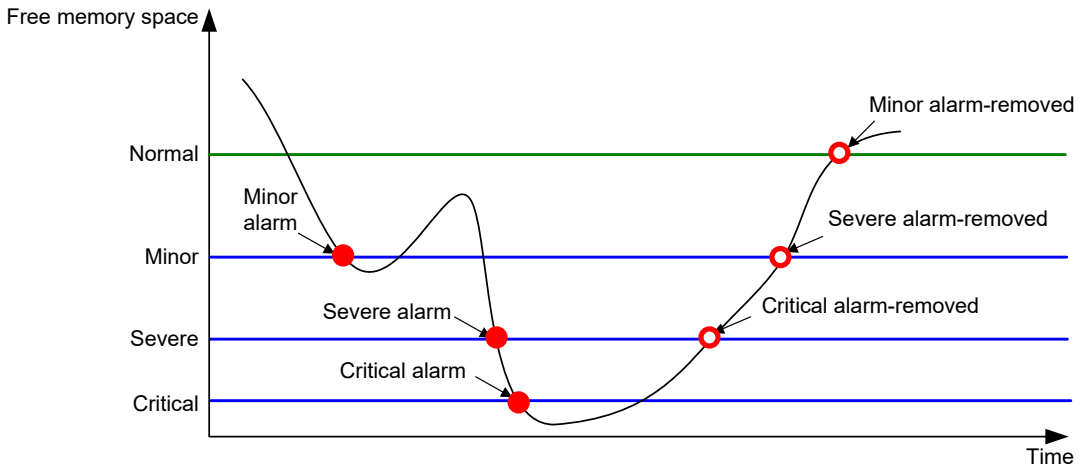


図 14-2 メモリ alarm 通知と alarm-removed 通知

以下にメモリ使用率の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． メモリ使用率しきい値を設定する	**memory-threshold usage** *memory-threshold*	デフォルト：100%

操作	コマンド	補足
3． 空きメモリしきい値を設定する	**memory-threshold minor** *minor-value* **severe** *severe-value* **critical** *critical-value* **normal** *normal-value*	デフォルト： ● **Minor alarmしきい値**–8 MB ● **Severe alarmしきい値**–4 MB ● **Critical alarmしきい値**–2 MB ● **Normal stateしきい値**–10 MB

14.12 温度アラームしきい値の設定

装置は次のしきい値に基づいて温度を監視します。

- 下限温度しきい値
- ワーニングしきい値
- アラームしきい値

装置の温度が下限温度しきい値を下回るか、ワーニング、またはアラームしきい値に達すると、装置はログメッセージとトラップを送信します。

以下に温度アラームしきい値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． 温度アラームしきい値を設定する	**temperature-limit inflow** sensor-number lowlimit warninglimit [*alarmlimit*]	デフォルト： lowlimitは-25、 warninglimitは85、 alarmlimitは90。 ワーニングしきい値は下限温度しきい値よりも高い温度を設定してください。 アラームしきい値はワーニングしきい値よりも高い温度を設定してください。

14.13 トランシーバのパラメータ表示

14.13.1 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*]	―

14.13.2 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*]	―
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値を表示する	**display transceiver diagnosis interface** [*interface-type interface-number*]	―

14.14 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
システムバージョンを表示する	**display version**
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**
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**
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**]
装置の温度情報を表示する	**display environment**
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**
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*]

操作	コマンド
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 **1-x-x** です。

15 章 Auto Config..... 15-1
15.1 概要..... 15-1
15.2 Auto Config 作業リスト..... 15-1
15.3 ファイルサーバの設定..... 15-2
15.4 Auto Config に必要なファイルの準備..... 15-2
15.4.1 ホスト名ファイル..... 15-2
15.4.2 コンフィグレーションファイル..... 15-2
15.4.3 スクリプトファイル..... 15-3
15.5 DHCP サーバの設定..... 15-3
15.5.1 コンフィグレーションガイドライン..... 15-3
15.5.2 HTTP ファイルサーバ使用時の DHCP サーバの設定..... 15-4
15.5.3 TFTP ファイルサーバ使用時の DHCP サーバの設定..... 15-5
15.6 DNS サーバの設定..... 15-5
15.7 ゲートウェイの設定..... 15-6
15.8 Auto Config で使用するインタフェースの準備..... 15-6
15.9 Auto Config の開始と完了..... 15-6

15章 Auto Config

15.1 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場合、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 15-1 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

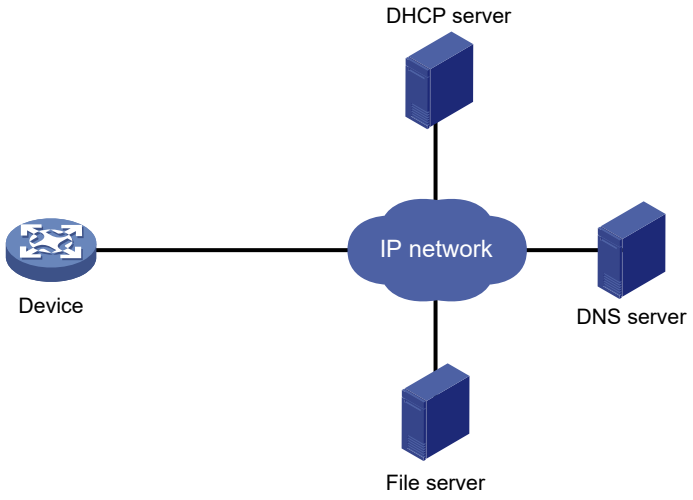


図 15-1 ネットワーク図

15.2 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

15.3 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。

15.4 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、オペレーションマニュアルのセクション 1 *はじめに “Auto Config”の “Auto Config に必要なファイルの準備”* の *“コンフィグレーションファイル”* に記載されているように、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、オペレーションマニュアルのセクション 1 *はじめに*“Auto Config”の *“Auto Config に必要なファイルの準備”* の *“スクリプトファイル”* に記載されているように、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。

15.4.1 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

15.4.2 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。

15.4.3 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 Tcl スクリプト（.tcl files）をサポートします。Tcl スクリプトに関する詳細は、オペレーションマニュアルのセクション 1 *はじめに “Tcl の使用”* 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。

15.5 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

15.5.1 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しようできないため、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順部された各装置は、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。

15.5.2 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

15.5.3 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

15.6 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。

15.7 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。

15.8 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。

15.9 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、コマンドマニュアルのセクション 1 *はじめに “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 **1-x-x** です。

16章 Tclの使用 16-1
16.1 Tclを使用した装置設定 16-1
16.2 Tcl configuration view上でのComwareコマンド実行 16-2

16章 Tcl の使用

Comware V7 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。

16.1 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、接続を解除することでプロセスを終了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。

16.2 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。詳細はオペレーションマニュアルのセクション 1 *はじめに “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 wlan ap ap1 model QX-W1240 ; radio 1
  - **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 " wlan ap ap1 model QX-W1240 ; radio 1"
  - **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 wlan ap ap1 model QX-W1240 ; cli radio 1

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*	

QX-W1200 シリーズ アクセスポイント

オペレーションマニュアル

2.WLAN

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 アクセスの設定

03- WLAN セキュリティ

04- WLAN 認証の概要

05- WLAN 認証の設定

06- WIPS の概要

07- WIPS の設定

08- WLAN QoS の設定

09- WLAN ローミングの設定

10- WLAN 無線リソースの計測の設定

11- チャネルスキャンの設定

12- バンドナビゲーションの設定

13- スペクトル管理の設定

14- WLAN 最適化

15- WLAN IP スヌーピング

16- Web リダイレクトの設定

17-WLAN メッシュの設定

18-WLAN 無線ロードバランス

目次

このセクションのページは **2-x-x** です。

1 章 無線管理の設定（FIT は未サポート） 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 1-2
1.1.3 伝送電力 1-2
1.1.4 伝送速度 1-2
1.1.5 MPDU アグリゲーション 1-3
1.1.6 MSDU アグリゲーション 1-3
1.1.7 MCS 1-4
1.1.8 VHT-MCS 1-6
1.1.9 HE-MCS 1-11
1.1.10 EHT-MCS 1-16
1.1.11 OFDMA 1-22
1.1.12 MU-MIMO 1-22
1.1.13 Spatial reuse 1-23
1.2 設定作業リスト 1-24
1.3 無線の有効化・無効化 1-25
1.4 無線モードの指定 1-26
1.5 屋外用 AP の屋内利用モードの設定 1-26
1.6 基本的な無線機能の設定 1-27
1.6.1 作動チャネルの指定 1-27
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 1-27
1.6.3 アンテナタイプの設定 1-28
1.6.4 最大伝送電力の設定 1-28
1.6.5 伝送速度の設定 1-29
1.6.6 最大伝送距離の設定 1-30
1.6.7 ビーコン間隔の設定 1-30
1.6.8 DTIM 間隔の設定 1-31
1.6.9 AP に関連づけるクライアントの最大数の設定 1-31
1.6.10 802.11b クライアント拒否の設定 1-31
1.6.11 衝突回避モードの指定 1-32
1.6.12 RTS しきい値の設定 1-32
1.6.13 802.11g 保護の設定 1-33
1.6.14 フラグメンテーションしきい値の設定 1-33
1.6.15 レーダチャネルスイッチバックの設定 1-34
1.6.16 R/F ドライバのリセット 1-35
1.7 802.11n 機能の設定 1-35
1.7.1 A-MPDU アグリゲーション方式の指定 1-36
1.7.2 A-MSDU アグリゲーション方式の指定 1-36
1.7.3 LDPC の設定 1-36
1.7.4 STBC の設定 1-36
1.7.5 MCS インデックスの設定 1-37
1.7.6 802.11n/ac/ax クライアント限定アクセスの設定 1-38
1.7.7 802.11n 帯域幅モードの設定 1-38
1.7.8 エネルギ節約機能の設定 1-39

1.7.9 802.11n 保護の設定 ... 1-39
1.8 802.11ac/ax 機能の設定 ... 1-40
1.8.1 NSS の設定 ... 1-40
1.8.2 802.11ac/ax クライアント限定アクセスの設定 ... 1-41
1.8.3 802.11ac/ax 帯域幅モードの設定 ... 1-42
1.8.4 TxBF の設定 ... 1-43
1.8.5 MU-MIMO の設定 ... 1-43
1.8.6 OFDMA の設定 ... 1-44
1.8.7 BSS カラーリングの設定 ... 1-45
1.8.8 TWT ネゴシエーションの設定 ... 1-46
1.9 802.11be 機能の設定 ... 1-47
1.9.1 NSS の設定 ... 1-47
1.9.2 802.11be 帯域幅モードの設定 ... 1-48
1.9.3 MRU の設定 ... 1-49
1.9.4 preamble puncturing 機能の設定 ... 1-50
1.10 6GHz 帯の無線の設定 ... 1-52
1.10.1 6GHz 帯の無線モードの指定 ... 1-52
1.10.2 6GHz 帯無線サービス検出の設定 ... 1-52
1.10.3 サービステンプレートの設定 ... 1-53
1.10.4 サービステンプレートの有効化 ... 1-56
1.10.5 無線に対するサービステンプレートの設定 ... 1-56
1.11 LED 点灯モードの設定 ... 1-57
1.12 無線管理の表示および管理 ... 1-58
1.13 無線管理の設定例 ... 1-58
1.13.1 基本無線機能の設定例 ... 1-58
1.13.2 802.11ac 設定例 ... 1-59
1.13.3 6GHz 帯の無線(Enhanced Open)の設定例 ... 1-60
1.13.4 6GHz 帯の無線(WPA3 パーソナル)の設定例 ... 1-61
1.13.5 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 ... 1-64
1.13.6 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 ... 1-66

1章 無線管理の設定（FIT は未サポート）

本マニュアルに登場する「FIT」という用語は、特に断りがない場合、Anchor-FIT モードで動作する AP のことを含みます。

1.1 概要

無線周波数(Radio Frequency:RF)は、長距離伝送や宇宙空間での放射が可能な電磁周波数を表す、高周波交流電磁波です。WLAN は、データ転送のための伝送媒体として、RF を利用する無線通信技術のひとつです。無線周波数は 300kHz～300GHz の範囲内です。WLAN では、2.4GHz 帯 (2.4GHz～2.4835GHz) 、5 GHz 帯 (5.150GHz～5.350GHz、および 5.470～5.730GHz) 、および 6GHz 帯 (5.925GHz～7.125GHz) の範囲の RF 周波数を使用します。

“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、無線モードとして 802.11a、802.11b、802.11g、802.11n、802.11ac、802.11ax、802.11be を定義しています。

802.11abe は 5GHz 周波数帯域に 802.11be を適用し、802.11gbe は 2.4GHz 周波数帯域に 802.11be を適用します。

802.11eax は 6GHz 周波数帯域に 802.11ax を適用し、802.1gax は 2.4GHz 周波数帯域に 802.11ax を適用します。

表 1-1 は無線モードの対応表を示します。

表 1-1 IEEE 802.11 の対応表

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
802.11eax	6GHz	9600Mbps
802.11be	6GHz	46100Mbps
802.11abe	5GHz	46100Mbps
802.11gbe	2.4GHz	19200Mbps

🕮**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 802.11eax と 802.11gax が含まれます。
- 特に指定が無い場合、文中に登場する“802.11be”には 802.11abe と 802.11gbe 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、インタフェースに対してより影響を受ける可能性が低いです。5GHz 帯の中には、指定された 20 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。

6GHz の周波数帯域は合計 1200MHz の帯域幅を持ち、20MHz の帯域幅を持つ 59 チャンネル、40MHz の帯域幅を持つ 29 チャンネル、80MHz の帯域幅を持つ 14 チャンネル、160MHz の帯域幅を持つ 7 チャンネルを提供できます。つまり、以前の 2.4GHz+5GHz 帯域の合計帯域幅の 2 倍になります。したがって、Wi-Fi アプリケーションで使用可能な周波数帯域幅が 3 倍になり、現在の Wi-Fi スペクトルリソース不足の緩和が期待されます。

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影響をもたらします。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。異なる無線モードごとの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動します。
- **802.11ac**－802.11ac 無線に対する速度は、チャネル帯域幅と NSS によって変動します。

- **802.11gac**－2.4GHz 帯で作動し、802.11ac と互換性があります。速度はチャネル帯域幅と NSS によって変動します。
- **802.11ax**－802.11ax に対する速度は、チャネル帯域幅と NSS によって変動します。
- **802.11gax**－2.4GHz 帯で作動し、802.11ax と互換性があります。速度はチャネル帯域幅と NSS によって変動します。
- **802.11eax**－6GHz 帯で作動し、802.11ax と互換性があります。速度はチャネル帯域幅と NSS によって変動します。
- **802.11be**－802.11be に対する速度は、チャネル帯域幅と NSS によって変動します。
- **802.11abe**－5GHz 帯で作動し、802.11be と互換性があります。速度はチャネル帯域幅と NSS によって変動します。
- **802.11gbe**－2.4GHz 帯で作動し、802.11be と互換性があります。速度はチャネル帯域幅と NSS によって変動します。

1.1.5 MPDU アグリゲーション

MPDU（MAC Protocol Data Unit）とは、802.11 フォーマット内のデータフレームです。MPDU アグリゲーションにより、多重の MPDU が 1 つの A-MPDU（Aggregate MPDU）に集約します。これにより、追加情報、ACK（Acknowledgement）フレーム、PLCP（Physical Layer Convergence Procedure）ヘッダオーバーヘッドが削減され、ネットワーク処理能力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（Quality of Service）優先度、送信元アドレス、宛先アドレスをもたなければなりません。

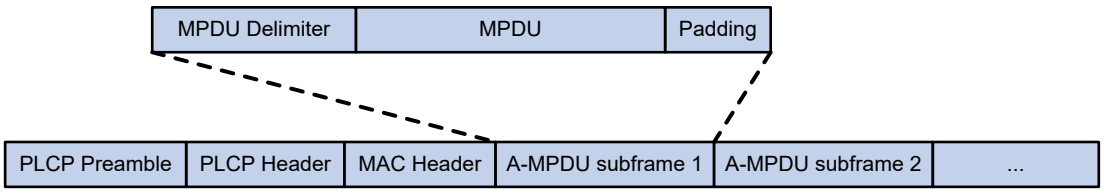


図 1-1 A-MPDU フォーマット

1.1.6 MSDU アグリゲーション

AP もしくはクライアントは、イーサネットヘッダを有する MSDU （MAC Service Data Unit）をカプセル化し、転送するために、フレームを 802.11 フォーマットに変換します。

MSDU アグリゲーションにより、多重の MSDU が 1 つの A-MSDU（Aggregate MSDU）に集約します。これにより、PLCP 序文、PLCP ヘッダ、MAC ヘッダオーバーヘッドが削減され、ネットワーク処理能力と転送効率が向上します。

A-MSDU 内のすべての MSDU は、同じ QoS 優先度、送信元アドレス、宛先アドレスをもたなければなりません。装置が A-MSDU を受信すると、処理のために A-MSDU を多重 MSDU に記憶します。

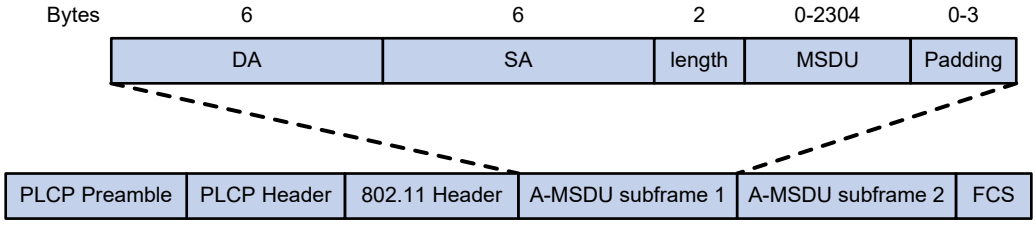


図 1-2 A-MSDU フォーマット

1.1.7 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。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 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

MCS インデックスは以下のタイプに分類されます。

- **必須 MCS インデックス**—AP に対して必須の MCS インデックスです。クライアントは、必須 MCS インデックスを AP に対してサポートするときのみ、802.11n AP に関連づけることができます。
- **サポート MCS インデックス**—AP によりサポートされた MCS インデックスです（必須 MCS インデックスは除きます）。サポート MCS インデックスにより、必須 MCS インデックスとサポート MCS インデックスの両方をサポートするクライアントは、AP と接続するためにより高い速度を使用できます。
- **マルチキャスト MCS インデックス**—AP がマルチキャストフレームを転送する速度と一致する MCS インデックスです。

🕮 **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。

1.1.8 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。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
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

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	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
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

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	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

802.11ac の NSS は、以下のタイプに分類されます。

- **必須 NSS**－AP に対して必須の NSS です。クライアントは、AP に対する必須 NSS をサポートするときのみ 802.11ac AP と関連づけることができます。
- **サポート NSS**－AP にサポートされた NSS です（必須 NSS は除きます）。クライアントが必須 NSS とサポート NSS の両方をサポートする場合、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を使用することができます。
- **マルチキャスト NSS**－AP は、マルチキャストフレームを転送するために、VHT-MCS データ速度表内の速度を使用します。

🕮 **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。

1.1.9 HE-MCS

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

802.11ax の HE-MCS は、以下のタイプに分類されます。

- **必須 HE-MCS**－AP に対して必須の HE-MCS です。802.11ax AP に関連づけるには、クライアントは AP に対する必須 HE-MCS をサポートする必要があります。
- **サポート HE-MCS**－必須 HE-MCS に加えて、AP によってサポートされる HE-MCS です。クライアントが必須とサポートされている 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速度を使用して AP と通信できます。
- **マルチキャスト HE-MCS**－AP がマルチキャストフレームを送信する速度の HE-MCS です。

🕮 **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。

1.1.10 EHT-MCS

IEEE 802.11be で定義されている非常に高いスループットと符号化方式 (EHT-MCS) の拡張により、無線データレートが決まります。

802.11be EHT-MCS は次のタイプに分類されます。

- Mandatory EHT-MCS：必須 EHT-MCS です。802.11be AP に関連付けるには、クライアントは AP の必須 EHT-MCS をサポートする必要があります。
- Supported EHT-MCS:必須 EHT-MCS 以外に AP でサポートされる EHT-MCS です。クライアントが必須とサポートされる EHT-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 EHT-MCS:AP がマルチキャストフレームを送信するレートの EHT-MCS。

EHT-MCS は、0～13 の整数で表される EHT-MCS インデックスによって識別されます。EHT-MCS パラメータは、EHT-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。

802.11be は、20 MHz、40 MHz、80 MHz、160 MHz、および 320 帯域幅モードをサポートし、最大 16 の空間ストリームをサポートします。802.11gbe は、20 MHz および 40 MHz 帯域幅モードをサポートします。

表 1-34～表 1-48 に、AP でサポートされている EHT-MCS のパラメータを示します。

表 1-34 EHT-MCS パラメータ（20 MHz, NSS =1）

EHT-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	8.6
1	1	QPSK	16	17.2
2	1	QPSK	24	25.8
3	1	16-QAM	33	34.4
4	1	16-QAM	49	51.6
5	1	64-QAM	65	68.8
6	1	64-QAM	73	77.4
7	1	64-QAM	81	86
8	1	256-QAM	98	103.2
9	1	256-QAM	108	114.7
10	1	1024-QAM	122	129
11	1	1024-QAM	135	143.4
12	1	4096-QAM	146.3	154.9
13	1	4096-QAM	162.5	172.1

表 1-35 EHT-MCS パラメータ（20 MHz, NSS =2）

EHT-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	17.2
1	2	QPSK	32	34.4
2	2	QPSK	48	51.6
3	2	16-QAM	66	68.8
4	2	16-QAM	98	103.2
5	2	64-QAM	130	137.6
6	2	64-QAM	146	154.8
7	2	64-QAM	162	172
8	2	256-QAM	196	206.4
9	2	256-QAM	216	229.4
10	2	1024-QAM	244	258
11	2	1024-QAM	270	286.8
12	2	4096-QAM	292.6	309.7
13	2	4096-QAM	325	344.1

表 1-36 EHT-MCS パラメータ（20 MHz, NSS =3）

EHT-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	25.8
1	3	QPSK	48	51.6
2	3	QPSK	72	77.4
3	3	16-QAM	99	103.2
4	3	16-QAM	147	154.8
5	3	64-QAM	195	206.4
6	3	64-QAM	219	232.2
7	3	64-QAM	243	258
8	3	256-QAM	294	309.6
9	3	256-QAM	324	344.1
10	3	1024-QAM	366	387
11	3	1024-QAM	405	430.2
12	3	4096-QAM	438.8	464.6
13	3	4096-QAM	487.5	516.2

表 1-37 EHT-MCS パラメータ（40 MHz, NSS =1）

EHT-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	17.2
1	1	QPSK	33	34.4
2	1	QPSK	49	51.6
3	1	16-QAM	65	68.8
4	1	16-QAM	98	103.2
5	1	64-QAM	130	137.6
6	1	64-QAM	146	154.9
7	1	64-QAM	163	172.1
8	1	256-QAM	195	206.5
9	1	256-QAM	217	229.4
10	1	1024-QAM	244	258.1
11	1	1024-QAM	271	286.8
12	1	4096-QAM	292.5	309.7
13	1	4096-QAM	325	344.1

表 1-38 EHT-MCS パラメータ（40 MHz, NSS =2）

EHT-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	34.4
1	2	QPSK	66	68.8
2	2	QPSK	98	103.2
3	2	16-QAM	130	137.6
4	2	16-QAM	196	206.4
5	2	64-QAM	260	275.2
6	2	64-QAM	292	309.8
7	2	64-QAM	326	344.2
8	2	256-QAM	390	413
9	2	256-QAM	434	458.8
10	2	1024-QAM	488	516.2
11	2	1024-QAM	542	573.6
12	2	4096-QAM	585	619.3
13	2	4096-QAM	650	688.2

表 1-39 EHT-MCS パラメータ（40 MHz, NSS =3）

EHT-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	51.6
1	3	QPSK	99	103.2
2	3	QPSK	147	154.8
3	3	16-QAM	195	206.4
4	3	16-QAM	294	309.6
5	3	64-QAM	390	412.8
6	3	64-QAM	438	464.7
7	3	64-QAM	489	516.3
8	3	256-QAM	585	619.5
9	3	256-QAM	651	688.2
10	3	1024-QAM	732	774.3
11	3	1024-QAM	813	860.4
12	3	4096-QAM	877.5	929.1
13	3	4096-QAM	975	1032.4

表 1-40 EHT-MCS パラメータ（40 MHz, NSS =4）

EHT-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	68.8
1	4	QPSK	132	137.6
2	4	QPSK	196	206.4
3	4	16-QAM	260	275.2
4	4	16-QAM	392	412.8
5	4	64-QAM	520	550.4
6	4	64-QAM	584	619.6
7	4	64-QAM	652	688.4
8	4	256-QAM	780	826
9	4	256-QAM	868	917.6
10	4	1024-QAM	976	1032.4
11	4	1024-QAM	1084	1147.2
12	4	4096-QAM	1170	1238.8
13	4	4096-QAM	1300	1376.5

表 1-41 EHT-MCS パラメータ（80 MHz, NSS =1）

EHT-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	36
1	1	QPSK	68	72.1
2	1	QPSK	102	108.1
3	1	16-QAM	136	144.1
4	1	16-QAM	204	216.2
5	1	64-QAM	272	288.2
6	1	64-QAM	306	324.4
7	1	64-QAM	340	360.3
8	1	256-QAM	408	432.4
9	1	256-QAM	453	480.4
10	1	1024-QAM	510	540.4
11	1	1024-QAM	567	600.5
12	1	4096-QAM	612.5	648.5
13	1	4096-QAM	680.6	720.6

表 1-42 EHT-MCS パラメータ（80 MHz, NSS =2）

EHT-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	72
1	2	QPSK	136	144.2
2	2	QPSK	204	216.2
3	2	16-QAM	272	288.2
4	2	16-QAM	408	432.4
5	2	64-QAM	544	576.4
6	2	64-QAM	612	648.8
7	2	64-QAM	680	720.6
8	2	256-QAM	816	864.8
9	2	256-QAM	906	960.8
10	2	1024-QAM	1020	1080.8
11	2	1024-QAM	1134	1201
12	2	4096-QAM	1225	1297.1
13	2	4096-QAM	1361.1	1441.2

表 1-43 EHT-MCS パラメータ（80 MHz, NSS =3）

EHT-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	108
1	3	QPSK	204	216.3
2	3	QPSK	306	324.3
3	3	16-QAM	408	432.3
4	3	16-QAM	612	648.6
5	3	64-QAM	816	864.6
6	3	64-QAM	918	973.2
7	3	64-QAM	1020	1080.9
8	3	256-QAM	1224	1297.2
9	3	256-QAM	1359	1441.2
10	3	1024-QAM	1530	1621.2
11	3	1024-QAM	1701	1801.5
12	3	4096-QAM	1837.5	1945.6
13	3	4096-QAM	2041.7	2161.8

表 1-44 EHT-MCS パラメータ（80 MHz, NSS =4）

EHT-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	144
1	4	QPSK	272	288.4
2	4	QPSK	408	432.4
3	4	16-QAM	544	576.4
4	4	16-QAM	816	864.8
5	4	64-QAM	1088	1152.8
6	4	64-QAM	1224	1297.6
7	4	64-QAM	1360	1441.2
8	4	256-QAM	1632	1729.6
9	4	256-QAM	1812	1921.6
10	4	1024-QAM	2040	2161.6
11	4	1024-QAM	2268	2402
12	4	4096-QAM	2450	2594.1
13	4	4096-QAM	2722.2	2882.4

表 1-45 EHT-MCS パラメータ（160 MHz, NSS =1）

EHT-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	68	72.1
1	1	QPSK	136	144.1
2	1	QPSK	204	216.2
3	1	16-QAM	272	288.2
4	1	16-QAM	408	432.4
5	1	64-QAM	544	576.5
6	1	64-QAM	612	648.5
7	1	64-QAM	681	720.6
8	1	256-QAM	817	864.7
9	1	256-QAM	907	960.7
10	1	1024-QAM	1021	1080.9
11	1	1024-QAM	1134	1201
12	1	4096-QAM	1225	1297.1
13	1	4096-QAM	1361.1	1441.2

表 1-46 EHT-MCS パラメータ（160 MHz, NSS =2）

EHT-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	136	144.1
1	2	QPSK	272	288.2
2	2	QPSK	408	432.4
3	2	16-QAM	544	576.5
4	2	16-QAM	817	864.7
5	2	64-QAM	1089	1152.9
6	2	64-QAM	1225	1297.1
7	2	64-QAM	1361	1441.2
8	2	256-QAM	1633	1729.4
9	2	256-QAM	1815	1921.5
10	2	1024-QAM	2042	2161.8
11	2	1024-QAM	2269	2401.9
12	2	4096-QAM	2450	2594.1
13	2	4096-QAM	2722.2	2882.4

表 1-47 EHT-MCS パラメータ（160 MHz, NSS =3）

EHT-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	204	216.2
1	3	QPSK	408	432.4
2	3	QPSK	613	648.5
3	3	16-QAM	817	864.7
4	3	16-QAM	1225	1297.1
5	3	64-QAM	1633	1729.4
6	3	64-QAM	1838	1945.6
7	3	64-QAM	2042	2161.8
8	3	256-QAM	2450	2594.1
9	3	256-QAM	2722	2882.4
10	3	1024-QAM	3062	3242.6
11	3	1024-QAM	3403	3602.9
12	3	4096-QAM	3675	3891.2
13	3	4096-QAM	4083	4323.5

表 1-48 EHT-MCS パラメータ（160 MHz, NSS =4）

EHT-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	272	288.2
1	4	QPSK	544	576.5
2	4	QPSK	817	864.7
3	4	16-QAM	1089	1152.9
4	4	16-QAM	1633	1729.4
5	4	64-QAM	2178	2305.9
6	4	64-QAM	2450	2594.1
7	4	64-QAM	2722	2882.4
8	4	256-QAM	3267	3458.8
9	4	256-QAM	3630	3843.1
10	4	1024-QAM	4083	4323.5
11	4	1024-QAM	4537	4803.9
12	4	4096-QAM	4900	5188.2
13	4	4096-QAM	5444.4	5764.7

🕮 **メモ：**

すべての EHT-MCS データ速度については、IEEE802.11be を参照してください。

1.1.11 OFDMA

802.11 a、802.11 g、802.11 n、および 802.11 ac では、データ伝送に直交周波数分割多重方式 (OFDM) を使用して、1 人のユーザが特定の時間帯にすべてのサブキャリアでデータを伝送できるようにします。OFDM に基づき、直交周波数分割多元接続 (OFDMA) は、特定のサブキャリア (トーン) を持つ Resource Unit (RU) として知られるサブチャネルにチャネルを分割し、同時伝送のために異なる RU を異なるユーザに割り当てます。これにより、データレートが増加し、伝送遅延が減少します。

802.11 ax は OFDMA を使用し、いくつかのヌルサブキャリアを予約して、RU でのサブキャリア間干渉を低減します。

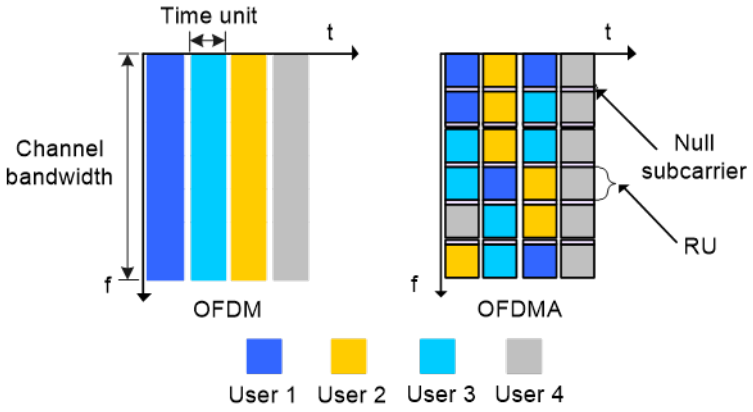


図 1-3 OFDM および OFDMA の動作モード

1.1.12 MU-MIMO

マルチユーザ Multiple-Input Multiple-Output (MU-MIMO) は、帯域幅を個々のストリームに分割して、複数のユーザが同時にデータを送受信できるようにします。

- ダウンリンク MU-MIMO では、AP はビームフォーミングを使用して、異なる場所にある無線クライアントにパケットを送信します。複数の無線クライアントは AP から同時にデータを受信できるようになります。

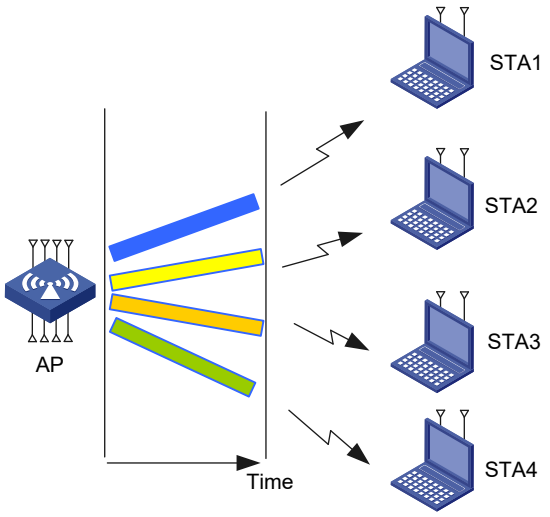


図 1-4 ダウンリンク MU-MIMO

- アップリンク MU-MIMO では、異なる場所にある無線クライアントから AP にパケット同時に送信することを可能にします。

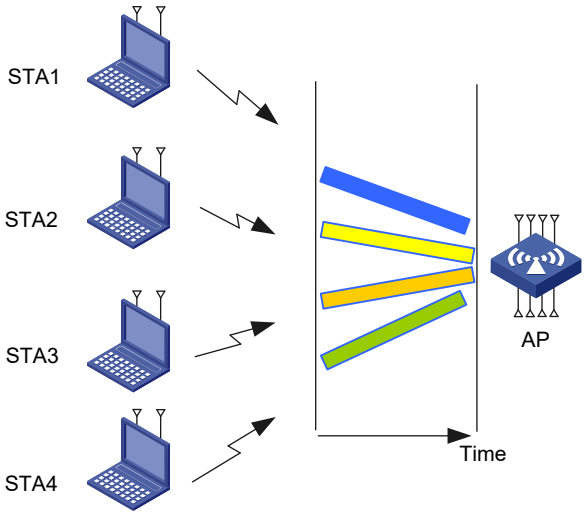


図 1-5 アップリンク MU-MIMO

1.1.13 Spatial reuse

Spatial reuse は、無線クライアントが重複する基本サービスセット (OBSS) からの信号を識別し、無線の衝突を回避し、干渉を管理するために特定の情報を使用するのに役立ちます。高密度環境におけるシステム性能とスペクトル資源利用を効果的に改善できます。

802.11 ax は、BSS ごとに BSS カラーと呼ばれる一意でない ID (1 から 63 の範囲)を割り当てて、パケットがクライアントと同じ BSS からのものかどうかを識別できるようにします。

クライアントは 802.11 ax パケットを受信すると、まずパケットヘッダの色を調べます。カラーが関連する AP の BSS のカラーと同じである場合、クライアントはそのパケットが Intra-BSS パケットであると判断します。色が関連する AP の BSS の色と異なる場合、

クライアントはそのパケットが BSS 間パケットであると判断します。クライアントは内部 BSS パケットだけを処理し、内部 BSS パケットは無視します。

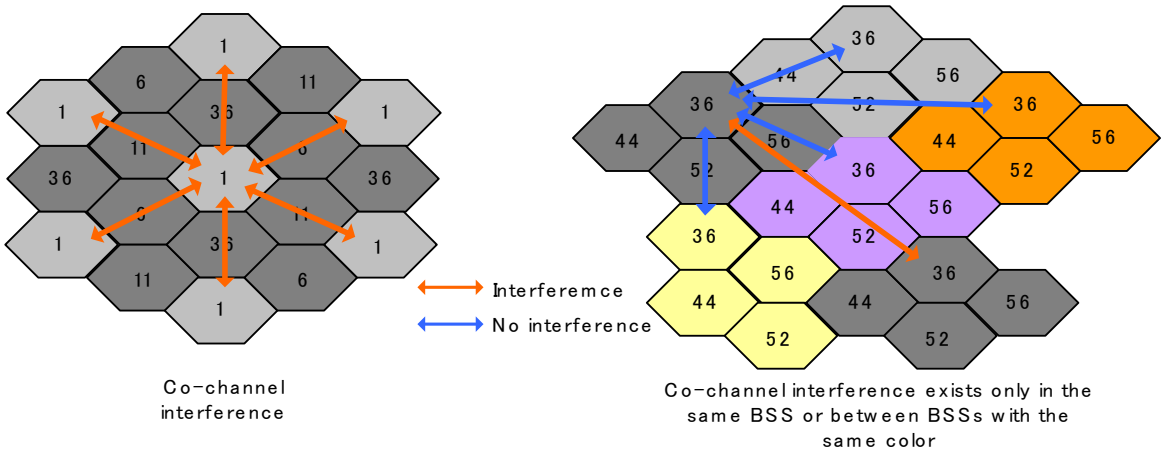


図 1-6 BSS カラーリング

1.2 設定作業リスト

操作	補足
（必須設定項目） 無線の有効化・無効化	—
（必須設定項目） 無線モードの指定	—
（オプション設定項目） 屋外用APの屋内利用モードの設定	—
（オプション設定項目） 基本的な無線機能の設定 • 作動チャネルの指定 • アンテナタイプの設定 • アンテナゲインの設定 • 最大伝送電力の設定 • 伝送速度の設定 • プリアンプルタイプの設定 • 最大伝送距離の設定 • ビーコン間隔の設定 • DTIM間隔の設定 • APに関連づけるクライアントの最大数の設定 • 802.11bクライアントアクセスの設定 • 衝突回避モードの指定 • RTSしきい値の設定 • 802.11g保護の設定 • フラグメンテーションしきい値の設定 • サービステンプレートの無線モードの設定	基本的な無線機能はすべての無線に適用されます。

操作	補足
（オプション設定項目） 802.11n機能の設定 ● A-MPDUアグリゲーション方式の指定 ● A-MSDUアグリゲーション方式の指定 ● LDPCの設定 ● STBCの設定 ● MCSインデックスの設定 ● 802.11nと802.11ac/axクライアント限定アクセスの設定 ● 802.11n帯域幅モードの設定 ● エネルギ節約機能の設定 ● 802.11n保護の設定	80211n機能は802.11anと802.11gn、802.11ac、802.11gac、802.11ax、802.11gax無線にのみ適用されます。
（オプション設定項目） 802.11ac/ax機能の設定 ● NSSの設定 ● 802.11ac/axクライアント限定アクセスの設定 ● 802.11ac/ax帯域幅モードの設定 ● TxBFの設定	802.11ac/ax機能は802.11ac、802.11gac、802.11ax、802.11gax無線にのみ適用されます。
（オプション設定項目） 802.11be機能の設定 ● NSSの設定 ● 802.11be帯域幅モードの設定 ● MRUの設定 ● preamble puncturing	—
(オプション設定項目) 6GHz帯の無線の設定 ● 6GHz帯の無線モードの指定 ● 6GHz帯無線サービス検出の設定 ● サービステンプレートの設定 ● サービステンプレートの有効化 ● 無線に対するサービステンプレートの設定	—

1.3 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． radio interface view へ移行する	**interface wlan-radio** *interface-number*	—
3． 無線を有効/無効にする	● radio interface を有効にします。 **undo shutdown** ● radio interface を無効にします。 **shutdown**	デフォルト：radio interfaceは有効です。

1.4 無線モードの指定

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。

無線モードを指定する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． radio interface view へ移行する	**interface wlan-radio** *interface-number*	—
3． 無線モードを指定する	**type** { **dot11a** | **dot11abe** | **dot11ac** | **dot11an** | **dot11ax** | **dot11b** | **dot11be** | **dot11g** | **dot11gac** | **dot11gax** | **dot11gbe** | **dot11gn** }	デフォルト： W1240 ● Radio1：802.11be (6GHz) ● Radio2：802.11abe (5GHz) ● Radio3：802.11gbe (2.4GHz) W1230 ● Radio1：802.11be (6GHz) ● Radio2：802.11abe (5GHz) ● Radio3：802.11gbe (2.4GHz) W1220 ● Radio1：802.11be (6GHz) ● Radio2：802.11abe (5GHz) ● Radio3：802.11gbe (2.4GHz) W1210 ● Radio1：802.11abe (5GHz) ● Radio2：802.11gbe (2.4GHz) W1210-E ● Radio1：802.11abe (5GHz) ● Radio2：802.11gbe (2.4GHz)

⚠ **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。

1.5 屋外用APの屋内利用モードの設定

🕮 **メモ**：

屋外用 AP の屋内利用モードの設定はソフトウェアバージョン 7.5.143b を含む以降のソフトウェアからサポートしています。

日本国内では、電波法により屋外での 5.2GHz(36ch～48ch)、5.3GHz(52ch～64ch)の電波の使用を禁じられています。QX-W1210-E はデフォルトで 5.2GHz(36ch～48ch)、5.3GHz(52ch～64ch)の使用を制限しています。

QX-W1210-E を屋内に設置して使用する場合は、屋内利用モードを有効にすることで、5.2GHz(36ch～48ch)と、5.3GHz(52ch～64ch)を使用できます。

⚠ **注意**：
屋外に設置した AP ではこの機能を有効化しないでください。

屋外用 AP の屋内利用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． global configuration view へ移行する	**wlan global-configuration**	—
3． 屋内利用モードを有効にする	**indoor-use enable**	デフォルト：無効（屋外モード）

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。

無線の作動チャネル上でレーダ信号が検出されると、チャネルが手動で指定されているか自動的に割り当てられているかにかかわらず、無線は使用中のチャネルを変更します。30 分後、変更前に使用していたチャネルに戻り、静止タイマを起動します。静止時間内にレーダ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信号が検出されると、無線はチャネルを変更します。

作動チャネル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． radio view へ移行する	**interface wlan-radio** *interface-number*	—
3． 作動チャネルを指定する	**channel** { *channel-number* | **auto** }	デフォルト：システムは無線の作動チャネルを自動で選択します。

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

ブラックリストにより、使用しないチャネルを複数選択できます。装置はブラックリストに含まれないチャネルを選択します。ホワイトリストにより、使用したいチャネルを複数

選択することができます。装置はホワイトリストに含まれるチャネルを選択します。ブラックリストとホワイトリストの両方を同じ無線インタフェースに設定することはできません。

ブラックリスト、ホワイトリストのチャネル選択は以下の通りです。

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． radio interface view へ移行する	**interface wlan-radio** *interface-number*	—
3． 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：**

アンテナタイプの設定はソフトウェアバージョン 7.5.143b を含む以降のソフトウェアからサポートしています。

QX-W1210-E では、標準添付の無指向性アンテナ（ANT-256-477V）もしくはオプション品の指向性アンテナ（ANT-256-08P-M4）を使用できます。

使用するアンテナと同じアンテナタイプを設定する必要があります。

アンテナタイプ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． radio interface view へ移行する	**interface wlan-radio** *interface-number*	—
3． アンテナタイプを設定する	**ntenna type** *antenna-type*	デフォルト：APモデルによって異なります。 QX-W1210-E : ANT-256-477V(無指向性アンテナ) 他のAPモデル：internal(内蔵アンテナ)

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、無線モード、アンテナタイプ、帯域幅モードにより変わります。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。

最大伝送電力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. radio interface view へ移行する	**interface wlan-radio** *interface-number*	—
3. 最大伝送電力を設定する	**max-power** *radio-power*	デフォルト：radio interfaceはサポートされた最大伝送電力を使用します。

1.6.5 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 で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 と関連づけられたあと、クライアントは AP と通信するために、サポートされた速度の中からより高い速度を選択することができます。インタフェース信号、再伝送パケット、あるいは廃棄パケットの増減に伴い、AP は自動的に伝送速度を増減します。
- **マルチキャスト速度**—AP 伝送マルチキャストもしくは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。

伝送速度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. radio interface view へ移行する	**interface wlan-radio** *interface-number*	—

3. 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

操作	コマンド	補足
		• 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

1.6.6 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、周辺の環境に依存します。

- 障害物が何もないエリア：約 300m
- 障害物のあるエリア：約 35m～50m

最大伝送距離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. radio interface view へ移行する	**interface wlan-radio** *interface-number*	—
3. 最大伝送距離を設定する	**distance** *distance*	デフォルト：1km

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。ビーコン間隔を短くすると、クライアントは AP を容易に検出することができますが、システムリソースの消費量が増加します。

ビーコン間隔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. radio interface view へ移行する	**interface wlan-radio** *interface-number*	—
3. ビーコン間隔を設定する	**beacon-interval** *interval*	デフォルト：100 TU

1.6.8 DTIM 間隔の設定

AP は、DTIM（Delivery Traffic Indication Map）に従ったビーコンを周期的にブロードキャストします。ビーコンをブロードキャストしたのち、AP は DTIM 間隔の値にもとづいてバッファされたブロードキャストとマルチキャストフレームを送信します。たとえば、DTIM 間隔を 5 に設定した場合、AP はバッファされたブロードキャストとマルチキャストフレームを 5 ビーコンフレームごとに送信します。

DTIM 間隔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． radio interface view へ移行する	**interface wlan-radio** *interface-number*	—
3． DTIM 間隔を設定する	**dtim** counter	デフォルト：1

1.6.9 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。

AP に関連づけるクライアントの最大数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． radio interface view へ移行する	**interface wlan-radio** *interface-number*	—
3． 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

1.6.10 802.11b クライアント拒否の設定

低速度の 802.11b クライアントによる、無線データ伝送のパフォーマンスの低下を防ぐために、802.11g、802.11gn、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。

802.11b クライアント拒否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． radio interface view へ移行する	**interface wlan-radio** *interface-number*	—
3． 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

1.6.11 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、無線装置はデータを転送する前に RTS（Request to Send）パケットもしくは CTS（Clear to Send）パケットを送信し、衝突を回避します。

AP に対して以下の衝突回避モードのいずれかを指定することができます。

- **RTS/CTS**－AP は、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。
- **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、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 *“802.11g 保護の設定”* を参照してください。

衝突回避モード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． radio interface view へ移行する	**interface wlan-radio** *interface-number*	—
3． 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

1.6.12 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。

RTS しきい値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. radio interface view へ移行する	**interface wlan-radio** *interface-number*	—
3. RTS しきい値を設定する	**protection-threshold** *size*	デフォルト：2346 バイト

1.6.13 802.11g 保護の設定

重要：

この機能は、802.11g 無線、802.11n（2.4GHz）無線、802.11gac 無線、802.11gax 無線にのみ適用されます。

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、802.11ac、802.11ax 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、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 *“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 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 AP に関連づけされたとき、自動的に適用されます。

802.11g 保護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. radio interface view へ移行する	**interface wlan-radio** *interface-number*	—
3. 802.11g 保護を設定する	**dot11g protection** { **disable** | **enable** }	デフォルト：無効

1.6.14 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。

フラグメント 1 つを受信しないとき、すべてのフレームではなく受信しなかったフラグメントのみ再転送します。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。

フラグメンテーションしきい値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. radio interface view へ移行する	**interface wlan-radio** *interface-number*	—
3. 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

1.6.15 レーダチャネルスイッチバックの設定

🕮 **メモ：**

- QX-W1210、QX-W1230 は、ソフトウェアバージョン 7.5.118 を含む以降のソフトウェアからレーダチャネルスイッチバックの設定をサポートしています。
- QX-W1240 は、ソフトウェアバージョン 7.5.129 を含む以降のソフトウェアからレーダチャネルスイッチバックの設定をサポートしています。

無線の作動チャネル上でレーダ信号が検出されると、チャネルが手動で指定されているか自動的に割り当てられているかにかかわらず、無線は使用中のチャネルを変更します。

レーダチャネルスイッチバックを無効にすると、レーダ信号の検出によるチャネル変更をしてから 30 分経過しても、AP が元のチャネルに切り替えないようにすることができます。この場合、AP は新しいチャネルを使用し続けます。

以下にレーダチャネルスイッチバック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. global configuration view へ移行する	**wlan global-configuration**	—
3. レーダチャネルスイッチバックを設定する	**radar-channel-switchback disable**	デフォルト：有効

1.6.16 R/F ドライバのリセット

🕮 **メモ：**

この機能はソフトウェアバージョン 7.5.143b を含む以降のソフトウェアからサポートしています。

I. R/F ドライバのリセット機能の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. radio interface view へ移行する	**interface wlan-radio** *interface-number*	—
3. R/F ドライバのリセット機能を設定する	**option smart-chip-protection** { **disable** | **enable** } **interval** *interval*	デフォルト：無効

II. オンデマンドでの R/F ドライバのリセット

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. R/F ドライバをリセットする	**wlan option smart-chip-protection pronto radio** *radio-id*	—

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。

⚠ **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

A-MPDU アグリゲーション方式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． radio interface view へ移行する	**interface wlan-radio** *interface-number*	—
3． 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

A-MSDU アグリゲーション方式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． radio interface view へ移行する	**interface wlan-radio** *interface-number*	—
3． 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 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。

LDPC 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． radio interface view へ移行する	**interface wlan-radio** *interface-number*	—
3． LDPC を設定する	**ldpc** { **disable** | **enable** }	デフォルト：無効

1.7.4 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。

STBC 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． radio interface view へ移行する	**interface wlan-radio** *interface-number*	—
3． STBC を設定する	**stbc** { **disable** | **enable** }	デフォルト：有効

1.7.5 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。

MCS インデックス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． radio interface view へ移行する	**interface wlan-radio** *interface-number*	—
3． 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
4． 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。
5． 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。

1.7.6 802.11n/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、AP が 802.11n/ac/ax クライアントのみ許可するようします。

802.11n/ac/ax クライアント限定アクセス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． radio interface view へ移行する	**interface wlan-radio** *interface-number*	—
3． 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

1.7.7 802.11n 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。

現在の無線のチャネルが指定の帯域幅モードをサポートしていない場合、無線はチャネルの設定を消去し、別のチャネルを選択します。

帯域幅モードが 40MHz に設定されるとき、隣接するチャネルが 1 つにまとめることができる場合、無線は 40MHz 帯域幅を使用します。1 つにまとめる隣接したチャネルが無い場合、20MHz 帯域幅を使用します。

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。

802.11n 帯域幅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． radio interface view へ移行する	**interface wlan-radio** *interface-number*	—
3． 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。

1.7.8 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。

エネルギ節約機能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. radio interface view へ移行する	**interface wlan-radio** *interface-number*	—
3. 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

1.7.9 802.11n 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、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“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 装置とは、802.11n 装置と 802.11ac/ax 装置を指します。

802.11n 保護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. radio interface view へ移行する	**interface wlan-radio** *interface-number*	—
3. 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

802.11n に基づき、802.11ac/ax はさらにデータ転送速度が高速になります。より高い帯域幅、より広い空間ストリーム、より先進の変調方式によりネットワークパフォーマンスが向上します。

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。

NSS 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. radio interface view へ移行する	**interface wlan-radio** *interface-number*	—
3. 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

操作	コマンド	補足
4. 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
5. 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。

802.11ac/ax クライアント限定アクセス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. radio interface view へ移行する	**interface wlan-radio** *interface-number*	—
3. 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。
- QX-W1240 で 160MHz をサポートしているのは Radio1 と Radio2 のみです。Radio3 では未サポートです。

802.11ac/ax 帯域幅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． radio interface view へ移行する	**interface wlan-radio** *interface-number*	—
3． 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：**

マルチユーザ TxBF を使用する場合は、シングルユーザ TxBF も有効にする必要があります。

TxBF（Transmit beamforming）により、意図したクライアントに RF 信号の焦点を当てるために、AP はチャネル情報に基づく転送パラメータを調整可能になります。この機能を使用することで RF 信号の品質が向上します。TxBF にはシングルユーザ TxBF とマルチユーザ TxBF があります。

- **シングルユーザ TxBF**－シングルユーザ TxBF により、AP は 1 つのクライアントに対する信号を向上させることができます。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**－マルチユーザ TxBF は、802.11ac Wave2 の一部です。マルチユーザ TxBF により、AP は接続されたクライアントに異なる RF 信号を送信することができ、干渉と伝送遅延が低減します。これにより、トラフィックスループットと帯域幅使用率が向上します。マルチユーザ TxBF は、クライアントが多数存在し、高帯域幅使用率と低伝送遅延が要求される WLAN に適用できます。

TxBF 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. radio interface view へ移行する	**interface wlan-radio** *interface-number*	—
3. シングルユーザ TxBF を設定する	**su-txbf** { **disable** | **enable** }	デフォルト：無効
4. マルチユーザ TxBF を設定する	**mu-txbf** { **disable** | **enable** }	デフォルト：無効 マルチユーザTxBFを有効にすることで、ダウンリンクMU-MIMOも有効になります。

1.8.5 MU-MIMO の設定

マルチユーザ Multiple-Input Multiple-Output (MU-MIMO) は、帯域幅を個々のストリームに分割して、複数のユーザが同時にデータを送受信できるようにします。

- ダウンリンク MU-MIMO では、AP はビームフォーミングを使用して、異なる場所にある無線クライアントにパケットを送信します。複数の無線クライアントは AP から同時にデータを受信できるようになります。
- アップリンク MU-MIMO では、異なる場所にある無線クライアントから AP にパケット同時に送信することを可能にします。

MU-MIMO 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. radio interface view へ移行する	**interface wlan-radio** *interface-number*	—
3. シングルユーザ TxBF を設定する	**su-txbf** { **disable** | **enable** }	デフォルト：無効
4. ダウンリンク MU-MIMO を設定する	**mu-txbf** { **disable** | **enable** }	デフォルト：無効 マルチユーザTxBFを有効にすることで、ダウンリンクMU-MIMOも有効になります。
5. アップリンク MU-MIMO を設定する	**ul-mu-mimo { disable | enable }**	デフォルト：無効

1.8.6 OFDMA の設定

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

OFDMA 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. radio interface view へ移行する	**interface wlan-radio** *interface-number*	—
3. ダウンリンク OFDMA を設定する	**dl-ofdma** { **disable** | **enable** }	デフォルト：有効
4. アップリンク OFDMA を設定する	**ul-ofdma** { **disable** | **enable** }	デフォルト：有効

1.8.7 BSS カラーリングの設定

I. BSS カラーリングについて

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。

II. 制限とガイドライン

本機能は 802.11ax 無線でのみ設定可能です。

BSS カラーリング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. radio interface view へ移行する	**interface wlan-radio** *interface-number*	—
3. BSS カラーリングを設定する	**bss-color** { **disable** | **enable** }	デフォルト：有効

1.8.8 TWT ネゴシエーションの設定

I. TWT ネゴシエーションについて

Trget Wake Time (TWT) 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。

II. 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 および 802.11gax でのみ有効です。無線タイプを 802.11ax または 802.11gax 以外に変更すると、設定が削除されます。

TWT ネゴシエーション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. radio interface view へ移行する	**interface wlan-radio** *interface-number*	—
3. TWT ネゴシエーションを設定する	**twt negotiate** { **disable** | **enable** }	デフォルト：有効

1.9 802.11be機能の設定

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。

NSS 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. radio interface view へ移行する	**interface wlan-radio** *interface-number*	—
3. 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
4. 最大サポート NSS を設定する	**dot11be support maximum-nss** *nss-number*	デフォルト： 8
5. 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。

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。

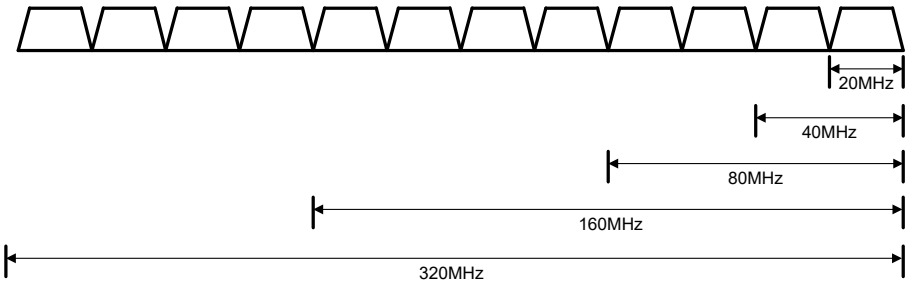


図 1-7 802.11be 帯域幅モード

802.11be 帯域幅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. radio interface view へ移行する	**interface wlan-radio** *interface-number*	—
3. 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** [**secondary-channel** *channel-number*] }	デフォルト： 160MHz
4. 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

操作	コマンド	補足
5. 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。

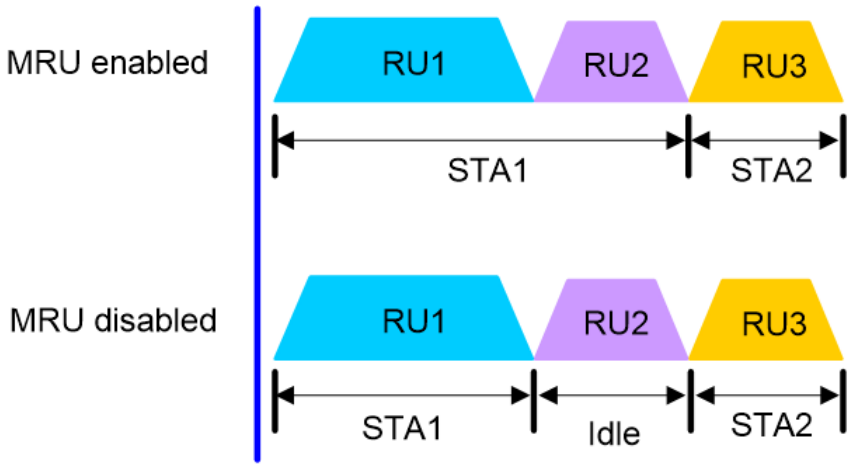


図 1-8 MRU

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。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. radio interface view へ移行する	**interface wlan-radio** *interface-number*	—
3. 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。
- puncturing の設定は最低 1 個のサービステンプレートをバインドしていないと失敗します。

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 1-9 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 1-10 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。

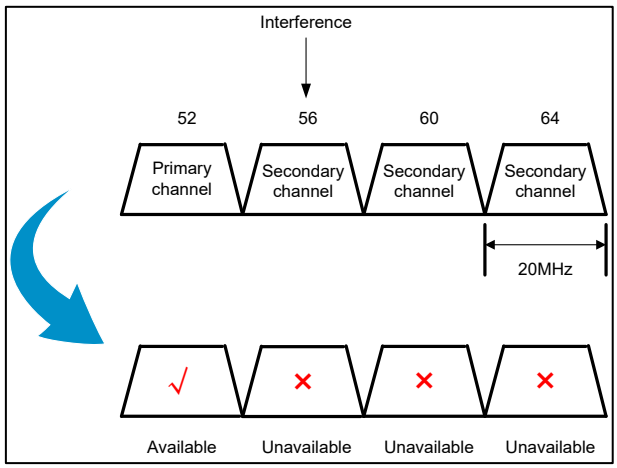


図 1-9 preamble puncturing がサポートされていない場合

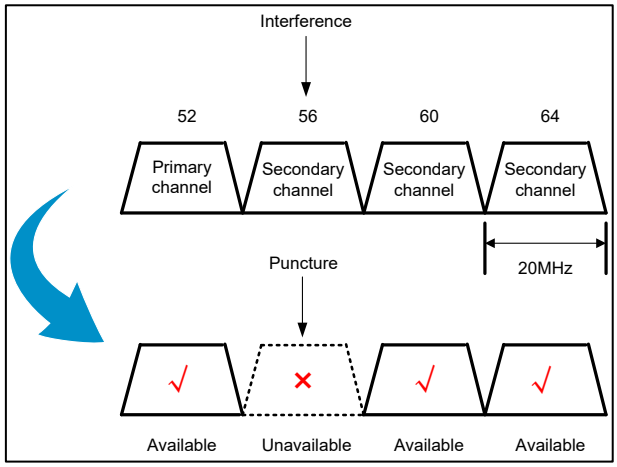


図 1-10 preamble puncturing がサポートされている場合

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 機能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. radio interface view へ移行する	**interface wlan-radio** *interface-number*	—
3. 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

1.10.1 6GHz 帯の無線モードの指定

6GHz 帯の無線モードを指定する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. radio interface view へ移行する	**interface wlan-radio** *interface-number*	—
3. 無線モードを指定する	**type { dot11be** | **dot11eax** }	W1240 デフォルト：dot11be W1230 デフォルト：dot11be W1220 デフォルト：dot11be W1210 デフォルト：—（W1210のRadio1のデフォルトは5GHz）

1.10.2 6GHz 帯無線サービス検出の設定

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。AP の 2.4GHz または 5GHz 無線は、デフォルトでは有効です。

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
4. system view に移行する	**system-view**	—
5. global configuration view へ移行する	**wlan global-configuration**	—
6. 6GHz 帯無線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： ソフトウェアバージョン 7.5.101のソフトウェア：無効 ソフトウェアバージョン 7.5.105を含む以降のソフトウェア：有効

1.10.3 サービステンプレートの設定

🕮 **メモ：**

- 6GHz 帯の無線での WPA3 エンタープライズの 192bit セキュリティなしモード(**enterprise-only-mode**)の利用は、ソフトウェアバージョン 7.5.129 を含む以降のソフトウェアからサポートしています。
- 6GHz 帯の無線での WPA3 エンタープライズ 192bit セキュリティなしモード(**wpa3 enterprise-transition-mode**)の利用は、ソフトウェアバージョン 7.5.129 を含む以降のソフトウェアからサポートしています。
- 6GHz 帯の無線での WPA3 パーソナル(**wpa3 personal optional**)の利用は、ソフトウェアバージョン 7.5.129 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 7.2.89 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。
- WPA3 エンタープライズの 192bit セキュリティなし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

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

🕮 **メモ：**

6GHz 帯の無線での WPA3 パーソナル(**wpa3 personal optional**)の利用は、ソフトウェアバージョン 7.5.129 を含む以降のソフトウェアからサポートしています。

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 または Enhanced Open システム認証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

操作	コマンド	補足
4. WPA3-SAE の SAE 交換時の PWE 生成方式として H2E 方式を設定する	**akm sae pwe h2e**	🕮 メモ：ソフトウェアバージョン7.5.129を含む以降のソフトウェアでは、**akm sae pwe h2e**コマンド設定は不要です。
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. WPA3 エンタープライズ 192bit セキュリティなしモードの設定

🕮 **メモ：**

- 6GHz 帯の無線での WPA3 エンタープライズの 192bit セキュリティなしモード(**enterprise-only-mode**)の利用は、ソフトウェアバージョン 7.5.129 を含む以降のソフトウェアからサポートしています。
- WPA3 エンタープライズ 192bit セキュリティなしモード(**wpa3 enterprise-transition-mode**)の利用は、ソフトウェアバージョン 7.5.129 を含む以降のソフトウェアからサポートしています。

WPA3 エンタープライズの 192bit セキュリティなしモードは、**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。

WPA3 エンタープライズ 192bit セキュリティなし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 192bit セキュリティなしモードを設定する	**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 GCMP を設定する	**cipher-suite ccmp**	デフォルト：設定なし

1.10.4 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

1.10.5 無線に対するサービステンプレートの設定

無線に対する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. wlan radio interface view へ移行する	**interface wlan-radio** *interface*	—

操作	コマンド	補足
3． 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 LED点灯モードの設定

AP 上で以下のモードで LED を点灯させるように設定できます。

- **quiet**－すべての LED をオフにします。
- **awake**－すべての LED を 1 分毎に点灯させます。
- **always-on**－すべての LED を常に点灯にします。
- **normal**－ノーマルモードでは AP の作動状況を識別します。

LED 点灯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． LED 点灯モードを設定する	**wlan led-mode** { **always-on** | **awake** | **normal** | **quiet** }	デフォルト：normal

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
クライアント情報の表示	**display wlan client** [**interface** *interface-type interface-number* | **mac-address** *mac-address* | **service-template** *service-template-name*] [**verbose**]

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 1-11 のように構成し、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 802.11b、channel 6、19 dBm を設定します。

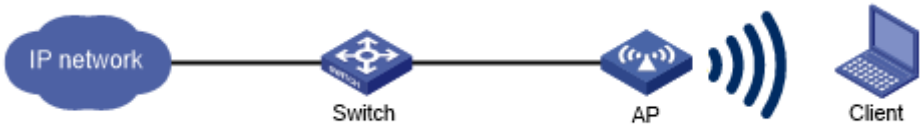


図 1-11 ネットワーク図

II. 設定手順

radio interface view に移行します。

```
<AP> system-view
[AP] interface wlan-radio 1/0/3
```

無線モードを dot11b に設定します。

```
[AP-WLAN-Radio1/0/3] type dot11b
```

作動チャネルを channel 6 に設定します。

```
[AP-WLAN-Radio1/0/3] channel 6
```

最大伝送電力を 19 dBm に設定します。

```
[AP-WLAN-Radio1/0/3] max-power 19
```

III. 設定の確認

オンラインのクライアントが 802.11b クライアントであることを確認します。

```
[AP-WLAN-Radio1/0/3] display wlan client verbose
Total number of clients: 1

MAC address                          : 000f-e265-6400
IPv4 address                         : 10.1.1.114
IPv6 address                         : 2001::1234:5678:0102:0304
Username                             : N/A
AID                                  : 1
AP ID                                : 1
AP name                              : ap1
Radio ID                             : 3
SSID                                 : office
BSSID                                : 0026-3e08-1150
VLAN ID                              : 1
Power save mode                      : Active
Wireless mode                        : 802.11b
Supported rates                      : 1, 2 Mbps
QoS mode                             : WMM
Listen interval                      : 10
RSSI                                 : 62
Rx/Tx rate                           : 130/11
Authentication method                : Open system
Security mode                        : PRE-RSNA
AKM mode                             : N/A
Cipher suite                         : N/A
User authentication mode             : Bypass
Authorization ACL ID                 : 3001(Not effective)
Authorization user profile           : N/A
Roam status                          : N/A
Key derivation                       : SHA1
PMF status                           : Enabled
Forward policy                       : N/A
Online time                          : 0hr 1min 13sec
FT status                            : Inactive
```

1.13.2 802.11ac 設定例

I. ネットワーク要件

図 1-12 のように構成し、無線を 802.11ac 無線として指定します。無線上で A-MSDU アグリゲーションと A-MPDU アグリゲーション方式、TxBF を有効にします。

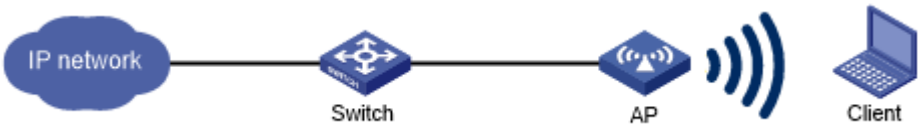


図 1-12 ネットワーク図

II. 設定手順

radio interface view に移行します。

```
<AP> system-view
[AP] interface wlan-radio 1/0/1
```

dot.11ac 無線を指定します。

```
[AP-WLAN-Radio1/0/1] type dot11ac
```

A-MPDU、A-MSDU アグリゲーション方式を有効にします。

```
[AP-WLAN-Radio1/0/1] a-mpdu enable
[AP-WLAN-Radio1/0/1] a-msdu enable
```

無線を有効にします。

```
[AP-WLAN-Radio1/0/1] undo shutdown
```

1.13.3 6GHz 帯の無線(Enhanced Open)の設定例

I. ネットワーク要件

図 1-13 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 1-13 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。

```
<AP> system-view
[AP] wlan global-configuration
[AP-wlan-global-configuration] wlan out-band 6g-discovery enable
[AP-wlan-global-configuration] quit
```

#サービステンプレート service を作成します。

```
[AP] wlan service-template service
```

#サービステンプレートの SSID を指定します。

```
[AP-wlan-st-service] ssid service
```

#enhanced open システム認証を有効にします。

```
[AP-wlan-st-service] enhanced-open enable
```

#サービステンプレート service を有効にします。

```
[AP-wlan-st-service] service-template enable
[AP-wlan-st-service] quit
```

#サービステンプレート radio2 を作成します。

```
[AP] wlan service-template radio2
```

#サービステンプレートの SSID を指定します。

```
[AP-wlan-st-radio2] ssid radio2
```

#サービステンプレート radio2 を有効にします。

```
[AP-wlan-st-radio2] service-template enable
[AP-wlan-st-radio2] quit
```

#サービステンプレート service を AP の radio 1 に割り当て、radio 1 を有効にします。

```
[AP] interface WLAN-Radio 1/0/1
[AP-WLAN-Radio1/0/1] undo shutdown
[AP-WLAN-Radio1/0/1] service-template service
[AP-WLAN-Radio1/0/1] quit
```

#サービステンプレート radio2 を AP の radio 2 に割り当て、radio 2 を有効にします。

```
[AP] interface WLAN-Radio 1/0/2
[AP-WLAN-Radio1/0/2] undo shutdown
[AP-WLAN-Radio1/0/2] service-template radio2
[AP-WLAN-Radio1/0/2] quit
```

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 パーソナル)の設定例

I. ネットワーク要件

図 1-14 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 1-14 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。

```
<AP> system-view
[AP] wlan global-configuration
[AP-wlan-global-configuration] wlan out-band 6g-discovery enable
[AP-wlan-global-configuration] quit
```

#サービステンプレート service を作成します。

```
[AP] wlan service-template service
```

#サービステンプレートの SSID を指定します。

```
[AP-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。

```
[AP-wlan-st-service1] akm mode psk
[AP-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。

```
[AP-wlan-st-service] cipher-suite ccmp
[AP-wlan-st-service] 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 7.5.129 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。

```
[AP-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 7.5.129 を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。

```
[AP-wlan-st-service1] akm sae pwe h2e
```

#サービステンプレート service を有効にします。

```
[AP-wlan-st-service] service-template enable
[AP-wlan-st-service] quit
```

#サービステンプレート radio2 を作成します。

```
[AP] wlan service-template radio2
```

#サービステンプレートの SSID を指定します。

```
[AP-wlan-st-radio2] ssid radio2
```

#サービステンプレート radio2 を有効にします。

```
[AP-wlan-st-radio2] service-template enable
[AP-wlan-st-radio2] quit
```

#サービステンプレート service を AP の radio 1 に割り当て、radio 1 を有効にします。

```
[AP] interface WLAN-Radio 1/0/1
[AP-WLAN-Radio1/0/1] undo shutdown
[AP-WLAN-Radio1/0/1] service-template service
[AP-WLAN-Radio1/0/1] quit
```

#サービステンプレート radio2 を AP の radio 2 に割り当て、radio 2 を有効にします。

```
[AP] interface WLAN-Radio 1/0/2
[AP-WLAN-Radio1/0/2] undo shutdown
[AP-WLAN-Radio1/0/2] service-template radio2
[AP-WLAN-Radio1/0/2] quit
```

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 セキュリティあり)の設定例

I. ネットワーク要件

図 1-15 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。

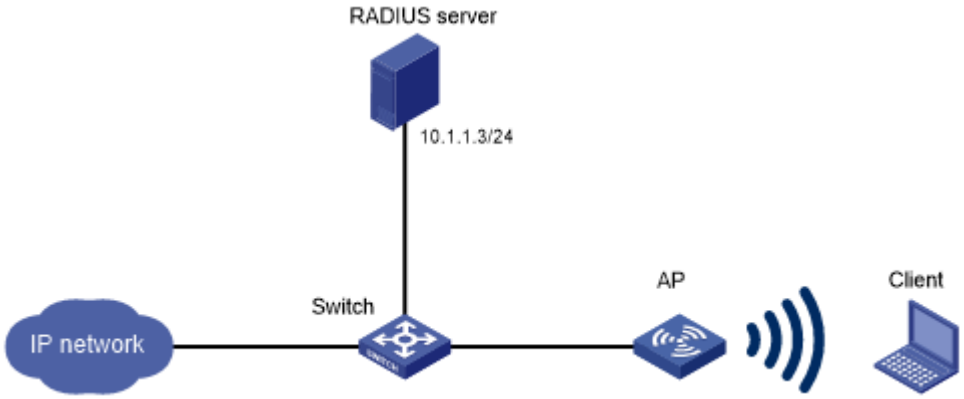


図 1-15 ネットワーク図

II. 設定手順

#6GHz 帯無線サービスの検出を有効にします。

```
<AP> system-view
[AP] wlan global-configuration
[AP-wlan-global-configuration] wlan out-band 6g-discovery enable
[AP-wlan-global-configuration] quit
```

#サービステンプレート service を作成します。

```
[AP] wlan service-template service
```

#サービステンプレートの SSID を指定します。

```
[AP-wlan-st-service] ssid service
```

AKM モードとして 802.1X を設定します。

```
[AP-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。

```
[AP-wlan-st-service1] cipher-suite gcmp
[AP-wlan-st-service1] security-ie rsn
```

WPA3 の設定を enterprise に設定します。

```
[AP-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。

```
[AP-wlan-st-service1] pmf mandatory
```

KDF を sha1-and-sha256 に設定します。

```
[AP-wlan-st-service1] key-derivation sha1-and-sha256
```

802.1X 認証モードを設定します。

```
[AP-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。

```
[AP-wlan-st-service1] dot1x domain dom1
```

#サービステンプレート service を有効にします。

```
[AP-wlan-st-service] service-template enable
[AP-wlan-st-service] quit
```

#サービステンプレート radio2 を作成します。

```
[AP] wlan service-template radio2
```

#サービステンプレートの SSID を指定します。

```
[AP-wlan-st-radio2] ssid radio2
```

#サービステンプレート radio2 を有効にします。

```
[AP-wlan-st-radio2] service-template enable
[AP-wlan-st-radio2] quit
```

RADIUS スキーム radius1 を作成し、RADIUS scheme view に移行します。

```
[AP] 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。

```
[AP-radius-radius1] primary authentication 10.1.1.3 1812
[AP-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。

```
[AP-radius-radius1] key authentication simple 12345
[AP-radius-radius1] key accounting simple 12345
```

#dot1x を設定します。

```
[AP] dot1x
[AP] 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。

```
[AP] domain dom1
```

```
[AP-isp-dom1] authentication lan-access radius-scheme radius1
[AP-isp-dom1] authorization lan-access radius-scheme radius1
[AP-isp-dom1] accounting lan-access radius-scheme radius1
[AP-isp-dom1] quit
```

#サービステンプレート service を AP の radio 1 に割り当て、radio 1 を有効にします。

```
[AP] interface WLAN-Radio 1/0/1
[AP-WLAN-Radio1/0/1] undo shutdown
[AP-WLAN-Radio1/0/1] service-template service
[AP-WLAN-Radio1/0/1] quit
```

#サービステンプレート radio2 を AP の radio 2 に割り当て、radio 2 を有効にします。

```
[AP] interface WLAN-Radio 1/0/2
[AP-WLAN-Radio1/0/2] undo shutdown
[AP-WLAN-Radio1/0/2] service-template radio2
[AP-WLAN-Radio1/0/2] quit
```

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。）

1.13.6 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帯の無線でのWPA3エンタープライズの192bitセキュリティなしモード(**enterprise-only-mode、enterprise-only-mode**)の利用は、ソフトウェアバージョン 7.5.129 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 1-16 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。

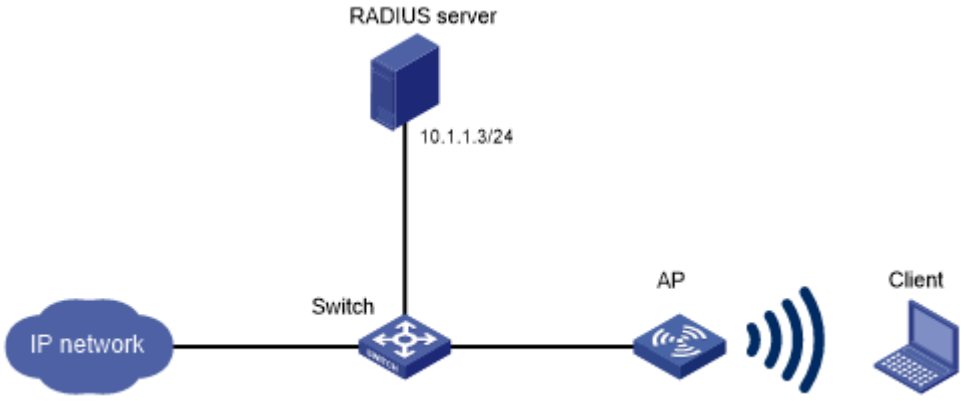


図 1-16 ネットワーク図

II. 設定手順

#6GHz 帯無線サービスの検出を有効にします。

```
<AP> system-view
[AP] wlan global-configuration
[AP-wlan-global-configuration] wlan out-band 6g-discovery enable
[AP-wlan-global-configuration] quit
```

#サービステンプレート service を作成します。

```
[AP] wlan service-template service
```

#サービステンプレートの SSID を指定します。

```
[AP-wlan-st-service] ssid service
```

AKM モードとして 802.1X を設定します。

```
[AP-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。

```
[AP-wlan-st-service] cipher-suite ccmp
[AP-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。

```
[AP-wlan-st-service] wpa3 enterprise-only-mode
```

- wpa3 enterprise-transition-mode を設定します。

```
[AP-wlan-st-service] wpa3 enterprise-transition-mode
```

802.1X 認証モードを設定します。

```
[AP-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。

```
[AP-wlan-st-service] dot1x domain dom1
```

#サービステンプレート service を有効にします。

```
[AP-wlan-st-service] service-template enable
[AP-wlan-st-service] quit
```

#サービステンプレート radio2 を作成します。

```
[AP] wlan service-template radio2
```

#サービステンプレートの SSID を指定します。

```
[AP-wlan-st-radio2] ssid radio2
```

#サービステンプレート radio2 を有効にします。

```
[AP-wlan-st-radio2] service-template enable
[AP-wlan-st-radio2] quit
```

RADIUS スキーム radius1 を作成し、RADIUS scheme view に移行します。

```
[AP] 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。

```
[AP-radius-radius1] primary authentication 10.1.1.3 1812
[AP-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。

```
[AP-radius-radius1] key authentication simple 12345
[AP-radius-radius1] key accounting simple 12345
```

#dot1x を設定します。

```
[AP] dot1x
[AP] 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。

```
[AP] domain dom1
[AP-isp-dom1] authentication lan-access radius-scheme radius1
[AP-isp-dom1] authorization lan-access radius-scheme radius1
[AP-isp-dom1] accounting lan-access radius-scheme radius1
[AP-isp-dom1] quit
```

#サービステンプレート service を AP の radio 1 に割り当て、radio 1 を有効にします。

```
[AP] interface WLAN-Radio 1/0/1
[AP-WLAN-Radio1/0/1] undo shutdown
[AP-WLAN-Radio1/0/1] service-template service
```

```
[AP-WLAN-Radio1/0/1] quit
```

#サービステンプレート radio2 を AP の radio 2 に割り当て、radio 2 を有効にします。

```
[AP] interface WLAN-Radio 1/0/2
[AP-WLAN-Radio1/0/2] undo shutdown
[AP-WLAN-Radio1/0/2] service-template radio2
[AP-WLAN-Radio1/0/2] quit
```

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**2-x-x** です。

2章 WLANアクセスの設定（FITは未サポート） 2-1
2.1 WLANアクセスの概要 2-1
2.1.1 スキャニング 2-1
2.1.2 関連づけ 2-3
2.2 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 2-3
2.3 ACLにもとづくアクセス制御 2-4
2.4 設定作業リスト 2-4
2.5 サービステンプレートの設定 2-5
2.6 SSIDの設定 2-5
2.7 サービステンプレートに紐付くクライアントの最大数の設定 2-6
2.8 サービステンプレートに対する記述の設定 2-6
2.9 クイックアソシエーションの有効化 2-6
2.10 サービステンプレートの有効化 2-7
2.11 無線インタフェースに対するサービステンプレートの設定 2-7
2.12 領域コードの指定 2-7
2.13 APのブロードキャストプローブ要求への応答の無効化 2-8
2.14 クライアントアイドルタイムアウトタイマの設定 2-8
2.15 クライアントkeepaliveの設定 2-9
2.16 NAS IDの設定 2-9
2.17 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 2-9
2.18 ホワイトリストへのクライアントの追加 2-10
2.19 スタティックブラックリストへのクライアントの追加 2-10
2.20 ACLにもとづくアクセス制御の設定 2-10
2.21 ダイナミックブラックリストエントリに対するエージングタイマの設定 2-11
2.22 クライアント再認証を行う前のアイドル時間の設定 2-11
2.23 WLANアクセスのSNMP notificationの有効化 2-11
2.24 WLANアクセスの表示と維持 2-12
2.25 WLANアクセスの設定例 2-13
2.25.1 WLANアクセスの設定例 2-13
2.25.2 ホワイトリストの設定例 2-14
2.25.3 スタティックブラックリストの設定例 2-15
2.25.4 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例 2-16

2章 WLAN アクセスの設定（FIT は未サポート）

本章では、WLAN に関する無線設定コマンドについて説明します。本章のコマンドは、QX-W1200 シリーズの Anchor-AC と FAT モードで実行することができます。

2.1 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、オペレーションマニュアルのセクション 2 *WLAN "WLAN セキュリティ"* を参照してください。

WLAN 認証に関する詳細は、オペレーションマニュアルのセクション 2 *WLAN "WLAN 認証の設定"* を参照してください。

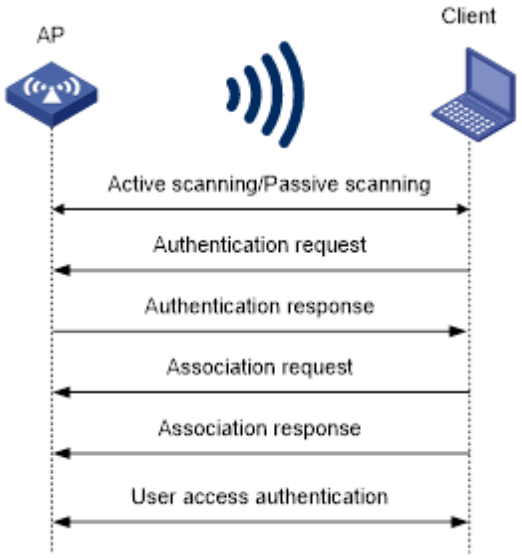


図 2-1 WLAN アクセスプロセス

2.1.1 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 2-2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。

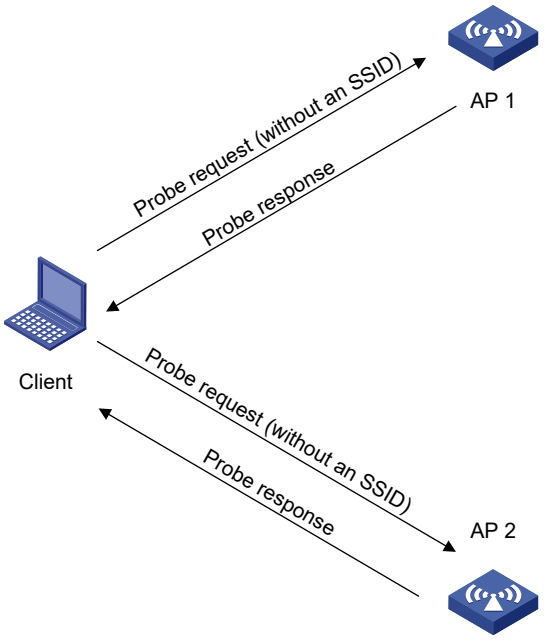


図 2-2 すべての無線ネットワークのスキャニング

- 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 2-3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。

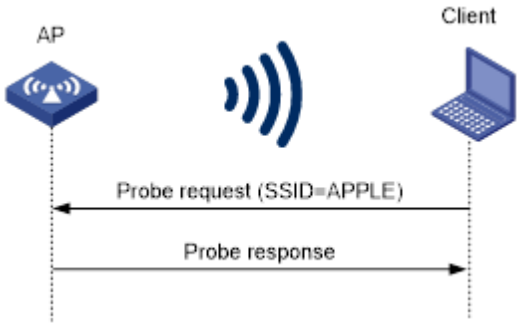


図 2-3 特定の無線ネットワークのスキャニング

II. パッシブスキャニング

図 2-4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。

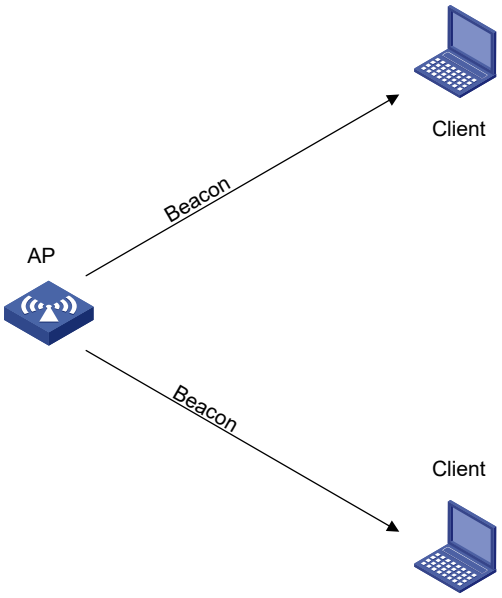


図 2-4 パッシブスキャニング

2.1.2 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。

2.2 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**－指定されたエージングタイマ内に、特定の AP を通って 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 に不正クライアントと判断された場合、クライアントはダイナミックにリストへ追加されます。無線攻撃に関する詳細は、オペレーションマニュアルのセクション 2 *WLAN “WIPS の設定”* を参照してください。

AP が関連づけ要求を受信すると、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。

2.3 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。

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。

2.4 設定作業リスト

作業リスト
（必須設定項目）サービステンプレートの設定
（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に紐付くクライアントの最大数の設定
（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
（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
（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）無線インタフェース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）領域コードの指定
（オプション設定項目）APのブロードキャストプローブ要求への応答の無効化
（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タイマの設定
（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）NAS ID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）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）ACLにもとづくアクセス制御の設定
（オプション設定項目）ダイナミックブラックリストエントリに対するエージングタイマの設定
（オプション設定項目）WLANアクセスのSNMP notificationの有効化

2.5 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。

サービステンプレート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. 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

2.6 SSIDの設定

AP は、ビーコンフレーム内で SSID を配信します。BSS 内のクライアント数が制限を越える、もしくは BSS が入手不可能な場合、クライアントが BSS を発見することを防ぐために SSID ステルスを有効にすることができます。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。

SSID 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. 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 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。

2.7 サービステンプレートに紐付くクライアントの最大数の設定

紐付けるクライアント数を制限することで過負荷を防ぎます。この機能を設定すると、最大数に達した場合、新たなクライアントは WLAN に紐付くことができなくなります。

サービステンプレートに紐付くクライアントの最大数を設定する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 に移行する	**wlan service-template** *service-template-name*	—
3. サービステンプレートに紐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

2.8 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

2.9 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。

クイックアソシエーションを有効にする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. 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

2.10 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

2.11 無線インタフェース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。

無線インタフェースへのサービステンプレート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. WLAN-Radio interface view に移行する	**interface wlan-radio** *interface-number*	—
3. 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 無線インタフェースに対して最大16のサービステンプレートを設定することができます。

2.12 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。

領域コード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. global configuration 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

2.13 APのブロードキャストプローブ要求への応答の無効化

ブロードキャストプローブ要求は、SSID が空欄の ANY 接続です。

この機能によってブロードキャストプローブ要求への応答を無効(SSID が空欄の ANY 接続拒否)ができます。

AP のブロードキャストプローブ要求への応答の無効化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. 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	**undo wlan broadcast-probe reply**	デフォルト：ブロードキャストプローブ要求に応答します。

メモ：

SSID が"ANY"の文字列である ANY 接続は、本機能に限らず"ANY"の文字列を持つサービステンプレートを作成しなければ接続されません。

2.14 クライアントアイドルタイムアウトタイマの設定

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。

AP でのクライアントアイドルタイムアウトタイマ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. クライアントアイドルタイムアウトタイマを設定する	**wlan client idle-timeout** *timeout*	デフォルト： ソフトウェアバージョン 7.5.105を含む以前のソフトウェアは3600秒 ソフトウェアバージョン 7.5.114を含む以降のソフトウェアは300秒

2.15 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。

AP でのクライアント keepalive 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. クライアント keepalive を有効にし、クライアント keepalive 間隔を設定する	**wlan client keep-alive** *interval*	デフォルト：無効

2.16 NAS IDの設定

NAS ID（Network Access Server 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 NAS の ID で区別します。

無線にサービステンプレートが設定された状態で NAS ID 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 を使用します。

NAS ID 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. global configuration view に移行する	**wlan global-configuration**	—
3. 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

2.17 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。

2.18 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。

ホワイトリストへのクライアントの追加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. 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

2.19 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。

ホワイトリストとブラックリストが設定されている場合、ホワイトリストのみが適用されます。

スタティックブラックリストへのクライアントの追加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. 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

2.20 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。

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。

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. 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*	デフォルト：設定なし

2.21 ダイナミックブラックリストエントリに対するエージングタイマの設定

設定されたエージングタイマは、ダイナミックブラックリストに追加したあとのエントリに対してのみ適用されます。

ホワイトリストとブラックリストが設定されている場合、ホワイトリストのみが適用されます。

ダイナミックブラックリストエントリに対するエージングタイマ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. ダイナミックブラックリストエントリのエージングタイマを設定する	**wlan dynamic-blacklist lifetime** *lifetime*	デフォルト：300秒 ダイナミックブラックリストエントリのエージングタイマは、不正クライアントエントリに対してのみ適用されます。

2.22 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

2.23 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 の詳細はオペレーションマニュアルのセクション 10 *システム管理 "SNMP"* を参照してください。

WLAN アクセスの SNMP notification を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 アクセスの SNMP notification を有効にする	**snmp-agent trap enable wlan client**	デフォルト：無効
3. クライアント監査の SNMP notification を有効にする	**snmp-agent trap enable wlan client-audit**	デフォルト：無効

2.24 WLANアクセスの表示と維持

すべての view で **display** コマンドと **wlan link-test** 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
BSS（Basic Service Set）の情報を表示する	**display wlan bss** { **all** | **bssid** *bssid* } [**verbose**]
ブラックリストエントリを表示する	**display wlan blacklist** { **dynamic** | **static** }
指定されたまたはすべての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**]
クライアントのキャッシュ情報を表示する	**display wlan client cache** [**mac-address** *mac-address*] 🕮 メモ：このコマンドはソフトウェアバージョン7.5.143bを含む以降のソフトウェアからサポートしています。
クライアントのデバイス情報を表示する	**display wlan client device-information [mac-address** *mac-address* **]**
クライアント情報を表示する	**display wlan client** [**interface wlan-radio** *interface-number* | **mac-address** *mac-address* | **service-template** *service-template-name*] [**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**]
ホワイトリストエントリを表示する	**display wlan whitelist**
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除去する	**reset wlan dynamic-blacklist** [**mac-address** *mac-address*]
クライアントへの無線リンクの品質をテストする	**wlan link-test** *mac-address*
クライアントの統計情報を表示する	**reset wlan statistics client** { **all** | **mac-address** *mac-address* }

2.25 WLANアクセスの設定例

2.25.1 WLAN アクセスの設定例

I. ネットワーク要件

図 2-5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。

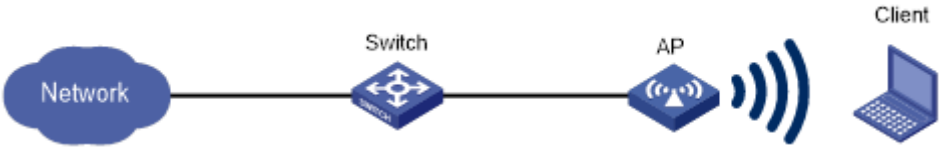


図 2-5 ネットワーク図

II. 設定手順

サービステンプレート service1 を作成します。SSID に trade-off を設定し、サービステンプレートを有効にします。

```
<AP> system-view
[AP] wlan service-template service1
[AP-wlan-st-service1] ssid trade-off
[AP-wlan-st-service1] service-template enable
[AP-wlan-st-service1] quit
```

WLAN-Radio 1/0/1 に対してサービステンプレート service1 を設定します。

```
[AP] interface wlan-radio 1/0/1
[AP-WLAN-Radio1/0/1] undo shutdown
[AP-WLAN-Radio1/0/1] service-template service1
[AP-WLAN-Radio1/0/1] quit
```

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。

```
[AP] 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        : Not configured
```

```
VLAN ID                          : 3
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                     : Not configured
Critical VLAN ID                 : Not configured
802.1X handshake                 : Disabled
802.1X handshake secure          : Disabled
802.1X domain                    : my-domain
MAC-auth domain                  : Not configured
Max 802.1X users per BSS         : 4096
Max MAC-auth users per BSS       : 4096
802.1X re-authenticate           : 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
```

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。

```
[AP] display wlan client service-template service1
```

```
[AP] display wlan client service-template service1
Total number of clients: 1

MAC address     Username    AP name   RID   IP address      IPv6 address   VLAN
0023-8933-223b  user        fatap     1     3.0.0.3
```

2.25.2 ホワイトリストの設定例

I. ネットワーク要件

図 2-6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 2-6 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。

```
<AP> system-view
[AP] 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。

```
<AP> display wlan whitelist
Total number of clients: 1
 MAC addresses:
  0000-000f-1211
```

2.25.3 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 2-7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。

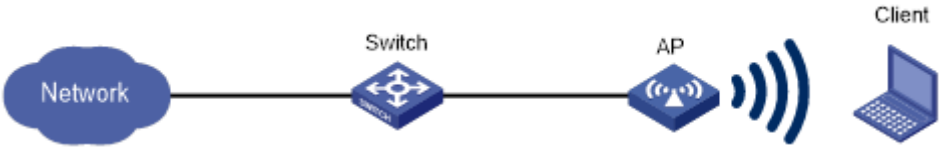


図 2-7 ネットワーク図

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。

```
<AP> system-view
[AP] 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。

```
<AP> display wlan blacklist static
Total number of clients: 1
 MAC addresses:
  0000-000f-1211
```

2.25.4 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例

I. ネットワーク要件

図 2-8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、サービステンプレートに ACL を設定します。

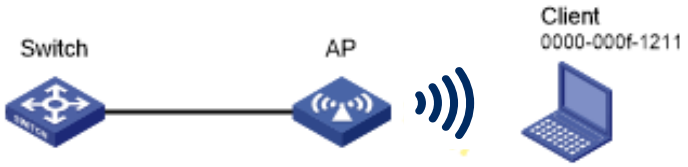


図 2-8 ネットワーク図

II. 設定手順

ACL 4000 に、送信元 MAC アドレス 0000-000f-1211 を許可する設定を追加します。

```
<AP> system-view
[AP] acl number 4000
[AP -acl-mac-4000] rule 1 permit source-mac 0000-000f-1211 ffff-ffff-ffff
[AP -acl-mac-4000] quit
```

#サービステンプレート service1 に ACL4000 を設定します。

```
 [AP] wlan service-template service1
[AP -wlan-st-service1] access-control acl 4000
```

III. 設定の確認

MAC アドレス 0000-000f-1211 のクライアントが AP 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**2-x-x** です。

3 章 WLAN セキュリティ（FIT は未サポート） 3-1
3.1 WLAN セキュリティ概要 3-1
3.2 IEEE802.11i (RSNA) 3-1
3.2.1 認証 3-1
3.2.2 鍵管理 3-2
3.2.3 暗号化方式 3-7
3.3 管理フレームの保護 3-7
3.3.1 アクティブ SA クエリ 3-8
3.3.2 パッシブ SA クエリ 3-8
3.4 プロトコルと標準 3-9
3.5 WLAN セキュリティ設定作業リスト 3-10
3.5.1 AKM モードの設定 3-10
3.5.2 暗号化規格の設定 3-11
3.5.3 暗号化方式の設定 3-11
3.5.4 PSK の設定 3-12
3.5.5 KDF の設定 3-12
3.5.6 GTK アップデートの設定 3-13
3.5.7 PTK ライフタイムの設定 3-14
3.5.8 TKIP MIC failure ホールドタイムの設定 3-14
3.5.9 管理フレーム保護の設定 3-15
3.5.10 WPA3 の設定 3-16
3.5.11 WPA3-SAE の SAE 交換時の PWE 生成方式の設定 3-16
3.5.12 Enhanced Open システム認証の設定 3-18
3.5.13 移行モードでの推奨サービステンプレートの指定 3-19
3.5.14 WLAN セキュリティの SNMP notification の有効化 3-19
3.6 WLAN セキュリティの表示と維持 3-20
3.7 WLAN セキュリティの設定例 3-21
3.7.1 WPA-PSK(TKIP)設定例 3-21
3.7.2 WPA2-PSK(AES)＋MAC アドレス認証設定例 3-22
3.7.3 802.1X AKM 設定例 3-25
3.7.4 管理フレーム保護設定例 3-28
3.7.5 WPA3 エンタープライズ(192bit セキュリティなし)設定例 3-30
3.7.6 WPA3 パーソナル設定例 3-33

3章 WLAN セキュリティ（FIT は未サポート）

本章では、WLAN セキュリティに関するコマンドについて説明します。本章のコマンドは、QX-W1200 シリーズの Anchor-AC と FAT モードで実行することができます

3.1 WLANセキュリティ概要

IEEE802.11 は Pre Robust Security Network Association (Pre-RSNA) を使用します。Pre-RSNA 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)が導入されました。WLAN のセキュリティを向上させるため、RSNA を選択してください。

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。

3.2 IEEE802.11i (RSNA)

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 には 2 つのセキュリティモードがあります。Wi-Fi Protected Access (WPA) と Robust Security Network (RSN) です。各モードの説明は以下のとおりです。

- 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。

3.2.1 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。802.1X 認証の詳細はオペレーションマニュアルのセクション 2 *WLAN "WLAN 認証の概要"*、および *"WLAN 認証の設定"* を参照してください。

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。

3.2.2 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



図 3-1 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 3-2 EAPOL-Key の構造

表 3-1 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

フィールド	説明
Key information	鍵情報は表 3-2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。
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。

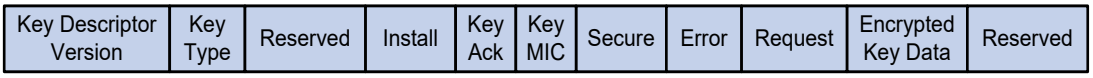


図 3-3 Key information の構造

表 3-2 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。

フィールド	説明
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。
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。

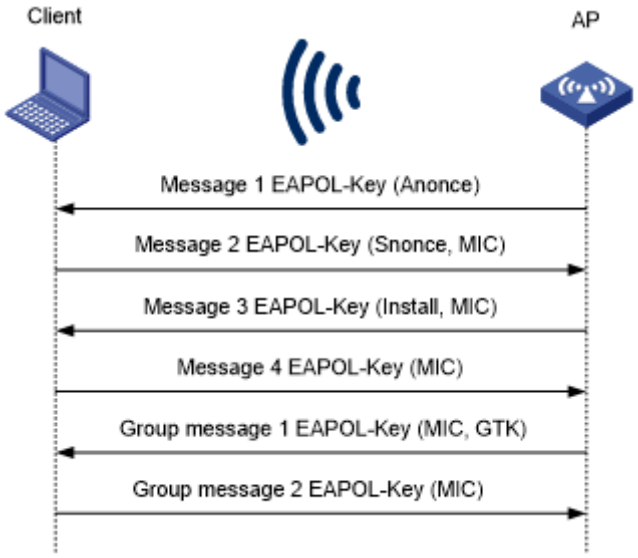


図 3-4 WPA 鍵交換プロセス

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。

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。

MIC を作成するため PTK の KCK を使用します。

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。

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。

MIC を作成するため PTK の KCK を使用します。

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。

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。

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。

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。

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。

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。

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。

2 つの MIC が同一である場合、GTK をインストールします。

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。

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。

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。

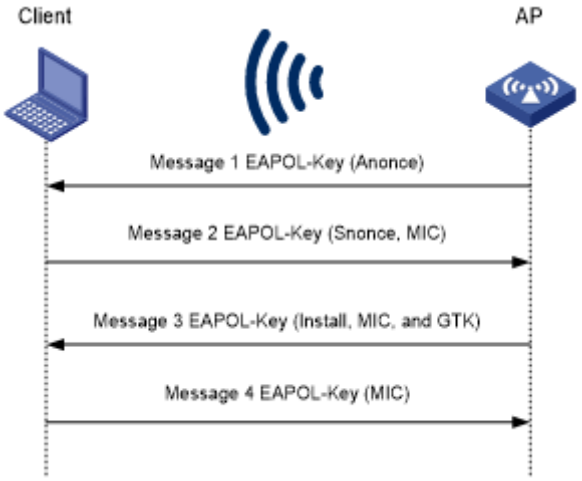


図 3-5 RSN 鍵交換のプロセス

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。

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。

MIC を作成するため PTK の KCK を使用します。

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。

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。

MIC を作成するため PTK の KCK を使用します。

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。

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。

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。

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。

2 つの MIC が同一である場合、PTK、GTK をインストールします。

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。

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。

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。

3.2.3 暗号化方式

I. TKIP

TKIP は RC4 アルゴリズムを使用します。TKIP には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。TKIP は 128 ビットの RC4 暗号アルゴリズムを使用しています。IV の長さは 48 ビットです。
- 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。

3.3 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。

3.3.1 アクティブ SA クエリ

図 3-6 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復帰時間が含まれます。

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。アソシエーション復帰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。

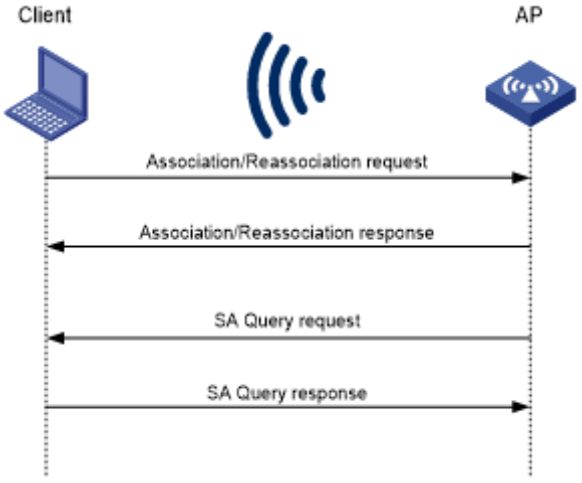


図 3-6 アクティブ SA クエリのプロセス

3.3.2 パッシブ SA クエリ

図 3-7 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。

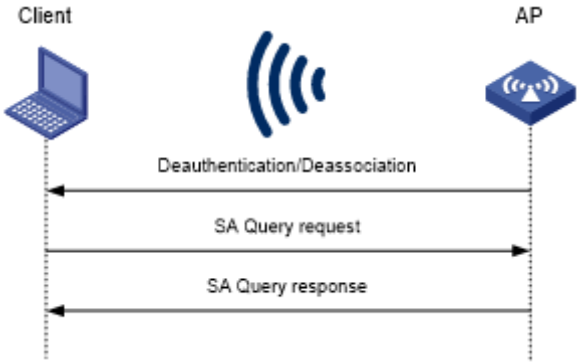


図 3-7 パッシブ SA クエリのプロセス

3.4 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*

3.5 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。
- 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してください。
- 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。

RSNA 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）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ライフタイムの設定
（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）管理フレーム保護の設定
（オプション設定項目）SNMP notificationの有効化

3.5.1 AKM モードの設定

以下の各 AKM モードは特定の認証モードを使用します。

- **802.1X AKM**–802.1X 認証モード
- **PSK AKM**–MAC アドレスあるいは認証バイパスモード
- **WiFi alliance anonymous 802.1X AKM**–802.1X 認証モード

以下に AKM 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． WLAN service template view に移行する	**wlan service-template** *service-template-name*	―
3． AKM モードを設定する	**akm mode** { **dot1x** | **psk** | **anonymous-dot1x** }	デフォルト：設定なし

3.5.2 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** { **osen** | **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。

3.5.3 暗号化方式の設定

暗号化方式には以下があります。

- TKIP
- CCMP
- GCMP

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**	―
2. WLAN service template view に移行する	**wlan service-template** *service-template-name*	―
3. 暗号化方式を設定する	**cipher-suite** { **ccmp** | **gcmp** | **tkip** }	デフォルト：設定なし

⚠ **重要：**

- QX-W1200 シリーズでは WEP は未サポートです。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ります。よりセキュリティ強度の高い AES を利用してください。
- AES を使用する場合は CCMP を設定してください。

3.5.4 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。AKM モードが 802.1X で、PSK を設定した場合、WLAN サービステンプレートを有効にすることができますが PSK の設定は適用されません。

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**	―
2． WLAN service template view に移行する	**wlan service-template** *service-template-name*	―
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

3.5.5 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**	―
2． WLAN service template view に移行する	**wlan service-template** *service-template-name*	―
3． KDF を設定する	**key-derivation** { **sha1** | **sha256** | **sha1-and-sha256** }	デフォルト：HMAC-SHA1

3.5.6 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

3.5.7 PTK ライフタイムの設定

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。

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 rekey 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

3.5.8 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。

3.5.9 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

3.5.10 WPA3 の設定

🕮 **メモ：**

- QX-W1200 シリーズの 6GHz 帯の Radio は、WPA3 パーソナル(**mandatory**)と WPA3 エンタープライズ 192bit セキュリティモードが使用できます。ソフトウェアバージョン 7.5.129 を含む以降のソフトウェアから、WPA3 パーソナル(**optional**)、WPA3 エンタープライズ 192bit セキュリティなしモード(**wpa3 enterprise-only-mode** 、 **wpa3 enterprise-transition-mode**)が使用できます。
- 192bit セキュリティなしの WPA3 エンタープライズについては、管理フレーム保護で実現します。**pmf** を参照して下さい。
- **wpa3 enterprise-only-mode** と **wpa3 enterprise-transition-mode** を設定する場合、事前に **pmf** コマンドと **key-derivation** コマンドがサービステンプレートに設定されていないことを確認してください。

- WPA3 エンタープライズの 192bit セキュリティモードー**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 エンタープライズの 192bit セキュリティなしモードー **wpa3 enterprise-only-mode**、**wpa3 enterprise-transition-mode**、または **pmf** 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。管理フレーム保護の設定を参照して下さい。
- WPA3 パーソナルー**wpa3 personal** 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。
- **mandatory:** WPA3 パーソナルで、WPA3 セキュリティモードを必須モードに指定します。WPA3 セキュリティモードをサポートしていないクライアントはアクセスできません。
- **optional:** WPA3 パーソナルで、WPA3 セキュリティモードをオプションモードに指定します。WPA3 セキュリティモードをサポートしているクライアントとサポートしていないクライアントのどちらもアクセスできます。

以下に WPA3 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. WLAN service template view に移行する	**wlan service-template** *service-template-name*	ー
3. WPA3 を有効にする	**wpa3** { **enterprise** | **enterprise-only-mode** | **enterprise-transition-mode** | **personal** { **mandatory** | **optional** } }	デフォルト：無効

3.5.11 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。

🕮 **メモ：**

- QX-W1200 シリーズの Radio1 で WPA3 パーソナルを使用する場合は、" **akm sae pwe h2e**" を設定してください。
- **both-h2e-hnp** を指定すると **hnp** のみをサポートしたクライアントでローミングに失敗する場合があります。クライアントの問題ですが、ローミング失敗を避けるために" **akm sae pwe hnp**" を設定してください。

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

3.5.12 Enhanced Open システム認証の設定

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、WPA 3 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。
- HMAC-SHA 1 および HMAC-SHA 256 アルゴリズムを KDF として指定します。

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

3.5.13 移行モードでの推奨サービステンプレートの指定

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 Enhanced Open 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。

3.5.14 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、オペレーションマニュアルのセクション 10 *システム管理 “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

3.6 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** [**interface** *interface-type interface-number* | **mac-address** *mac-address* | **service-template** *service-template-name*] [**verbose**]

詳細はコマンドマニュアルのセクション 2 WLAN *“WLAN アクセスの設定”*を参照してください。

3.7 WLANセキュリティの設定例

3.7.1 WPA-PSK(TKIP)設定例

I. ネットワーク要件

図 3-8 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。

- 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。

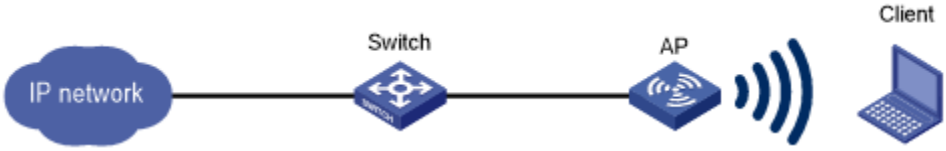


図 3-8 ネットワーク図

II. 設定手順

1)　サービステンプレート service1 を作成します。

```
<AP> system-view
[AP] 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。

```
[AP-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。

```
[AP-wlan-st-service1] akm mode psk
[AP-wlan-st-service1] preshared-key pass-phrase simple 12345678
```

WPA(TKIP)のために、暗号化規格に WPA、暗号化方式に TKIP を指定します。

```
[AP-wlan-st-service1] cipher-suite tkip
[AP-wlan-st-service1] security-ie wpa
```

4)　サービステンプレート service1 を有効にします。

```
[AP-wlan-st-service1] service-template enable
[AP-wlan-st-service1] quit
```

5)　サービステンプレート service1 を AP の WLAN-Radio 1/0/2 に割り当てます。

```
[AP] interface WLAN-Radio 1/0/1
[AP-WLAN-Radio1/0/2] undo shutdown
[AP-WLAN-Radio1/0/2] service-template service1
[AP-WLAN-Radio1/0/2] quit
```

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。

```
[AP] 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
VLAN ID                        : 1
AKM mode                       : PSK
Security IE                    : WPA
Cipher suite                   : TKIP
TKIP countermeasure time       : 0
PTK lifetime                   : 43200 sec
GTK rekey                      : Enabled
GTK rekey method               : Time-based
GTK rekey time                 : 86400 sec
GTK rekey client-offline       : Enabled
User authentication mode           : Bypass
Intrusion protection           : Disabled
Intrusion protection mode      : Temporary-block
Temporary block time           : 180 sec
Temporary service stop time    : 20 sec
Fail VLAN ID                   : 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
Forward policy                 : Not configured
Forwarder                      : AP
FT status                      : Disabled
QoS trust                      : Port
QoS priority                   : 0
```

3.7.2 WPA2-PSK(AES)＋MAC アドレス認証設定例

I. ネットワーク要件

図 3-9 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 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。

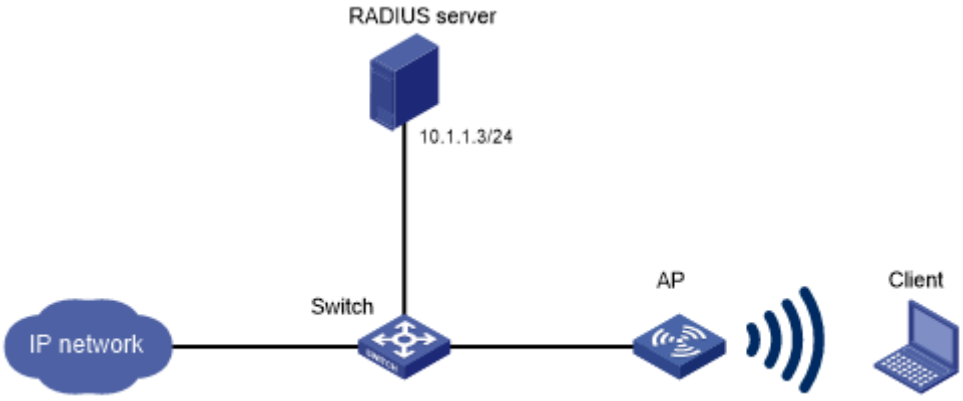


図 3-9 ネットワーク図

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 AP が互いに通信可能なことを確認します。
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 として service を指定します。

```
<AP> system-view
[AP] wlan service-template service1
[AP-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。

```
[AP-wlan-st-service1] akm mode psk
[AP-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 を指定します。

```
[AP-wlan-st-service1] cipher-suite ccmp
[AP-wlan-st-service1] security-ie rsn
```

MAC アドレス認証を設定します。

```
[AP-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。

```
[AP-wlan-st-service1] service-template enable
[AP-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。

```
[AP] 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。

```
[AP-radius-radius1] primary authentication 10.1.1.3 1812
[AP-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。

```
[AP-radius-radius1] key authentication simple 12345678
[AP-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。

```
[AP-radius-radius1] user-name-format without-domain
[AP-radius-radius1] 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。

```
[AP-radius-radius1] user-name-format with-domain
[AP-radius-radius1] 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。

```
[AP] domain dom1
[AP-isp-dom1] authentication lan-access radius-scheme radius1
[AP-isp-dom1] authorization lan-access radius-scheme radius1
[AP-isp-dom1] accounting lan-access radius-scheme radius1
[AP-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。

```
[AP] mac-authentication domain dom1
[AP] mac-authentication user-name-format fixed account abc password simple 123
```

8)　サービステンプレート service1 を AP の WLAN-Radio 1/0/2 に割り当てます。

```
[AP] interface WLAN-Radio 1/0/2
[AP-WLAN-Radio1/0/2] undo shutdown
[AP-WLAN-Radio1/0/2] service-template service1
[AP-WLAN-Radio1/0/2] quit
```

🕮 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

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。

```
[AP] 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
VLAN ID                        : 1
AKM mode                       : PSK
Security IE                    : RSN
Cipher suite                   : CCMP
TKIP countermeasure time       : 0
```

```
PTK lifetime                  : 43200 sec
GTK rekey                     : Enabled
GTK rekey method              : Time-based
GTK rekey time                : 86400 sec
GTK rekey client-offline      : Enabled
User authentication mode          : 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
Forward policy                : Not configured
Forwarder                     : AP
FT status                     : Disabled
QoS trust                     : Port
QoS priority                  : 0
```

3.7.3 802.1X AKM 設定例

I. ネットワーク要件

図 3-10 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 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。

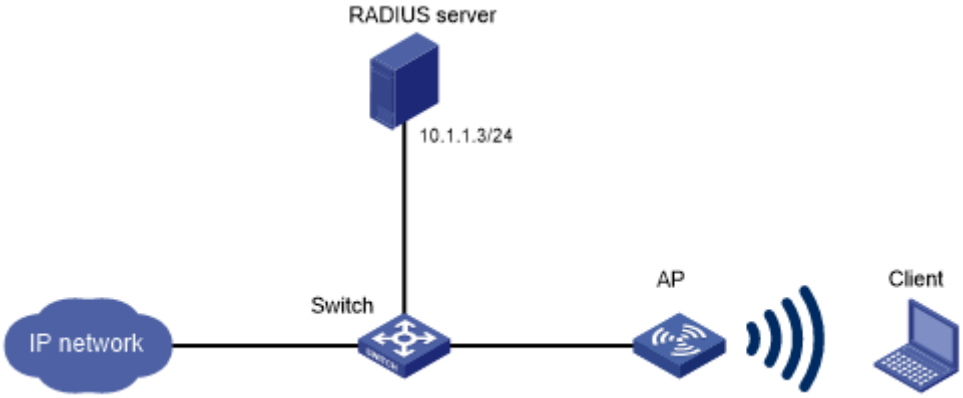


図 3-10 ネットワーク図

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 AP が互いに通信可能なことを確認します。
2) 802.1X クライアントを設定します。
3) WLAN サービステンプレート service1 を作成します。

```
<AP> system-view
[AP] wlan service-template service1
```

4) サービステンプレートの SSID として service を指定します。

```
[AP-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。

```
[AP-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。

```
[AP-wlan-st-service1] cipher-suite ccmp
[AP-wlan-st-service1] security-ie wpa
```

802.1X 認証モードを設定します。

```
[AP-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。

```
[AP-wlan-st-service1] dot1x domain dom1
```

6) サービステンプレート service1 を有効にします。

```
[AP-wlan-st-service1] service-template enable
[AP-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。

```
[AP] 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。

```
[AP-radius-radius1] primary authentication 10.1.1.3 1812
[AP-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。

```
[AP-radius-radius1] key authentication simple 12345
[AP-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。

```
[AP-radius-radius1] user-name-format without-domain
[AP-radius-radius1] 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。

```
[AP-radius-radius1] user-name-format with-domain
[AP-radius-radius1] 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。

```
[AP] domain dom1
[AP-isp-dom1] authentication lan-access radius-scheme radius1
[AP-isp-dom1] authorization lan-access radius-scheme radius1
[AP-isp-dom1] accounting lan-access radius-scheme radius1
[AP-isp-dom1] quit
```

9) サービステンプレート service1 を AP の WLAN-Radio 1/0/2 割り当て、radio 2 を有効にします。

```
[AP] interface WLAN-Radio 1/0/2
[AP-WLAN-Radio1/0/2] undo shutdown
[AP-WLAN-Radio1/0/2] service-template service1
[AP-WLAN-Radio1/0/2] quit
```

🕮 **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

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。

```
[AP] 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        : Not configured
VLAN ID                        : 1
AKM mode                       : 802.1X
Security IE                    : WPA
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
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       : 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                     : AP
FT status                     : Disabled
QoS trust                     : Port
QoS priority                  : 0
```

3.7.4 管理フレーム保護設定例

I. ネットワーク要件

図 3-11 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。

- 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。

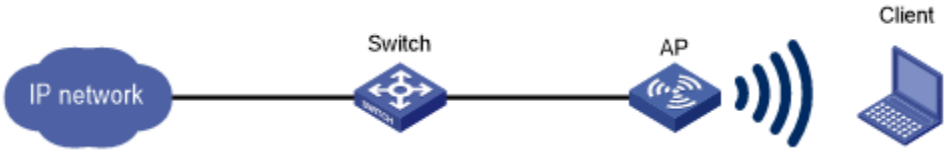


図 3-11 ネットワーク図

II. 設定手順

1)　WLAN サービステンプレート service1 を作成します。

```
<AP> system-view
[AP] wlan service-template service1
```

2)　サービステンプレートの SSID として service を指定します。

```
[AP-wlan-st-service1] ssid service
```

3)　管理フレーム保護を optional モードで有効にします。

```
[AP-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。

```
[AP-wlan-st-service1] akm mode psk
[AP-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。

```
[AP-wlan-st-service1] cipher-suite ccmp
[AP-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。

```
[AP-wlan-st-service1] service-template enable
```

```
[AP-wlan-st-service1] quit
```

6)　サービステンプレート service1 を AP の WLAN-Radio 1/0/2 に割り当てます。

```
[AP] interface WLAN-Radio 1/0/2
[AP-WLAN-Radio1/0/2] undo shutdown
[AP-WLAN-Radio1/0/2] service-template service1
[AP-WLAN-Radio1/0/2] quit
```

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。

```
[AP] 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        : Not configured
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       : 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 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-AND-SHA256
PMF status                     : Optional
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
```

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。

```
[AP] display wlan client verbose
Total number of clients: 1
```

```
MAC address                    : 5250-0012-0411
Username                       : 11w
Radio ID                       : 2
SSID                           : service
BSSID                          : 1111-2222-3333
VLAN ID                        : 1
Power save mode                : Active
Wireless mode                  : 802.11a
QoS mode                       : None
Listen interval                : 100
RSSI                           : 0
Rx/Tx rate                     : 0/0
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                    : Normal
Key derivation                 : SHA256
PMF status                     : Enabled
Online time                    : 0hr 0min 10sec
```

3.7.5 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 3-12 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。

- WPA3 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。

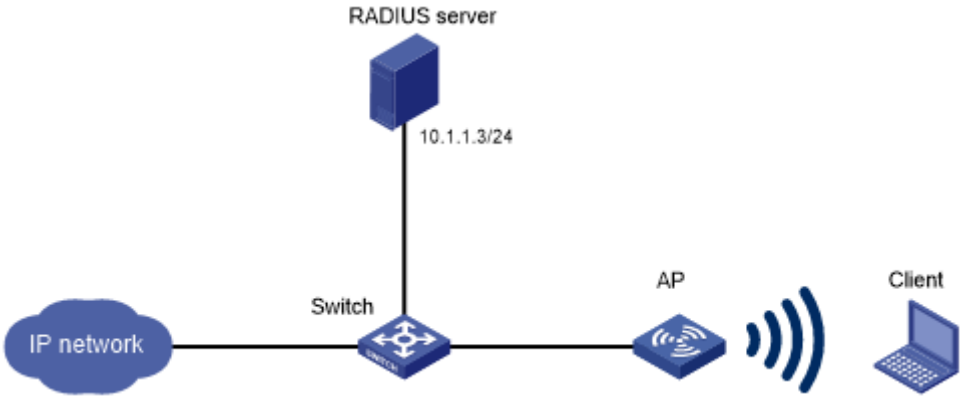


図 3-12 ネットワーク図

II. 設定手順

1)　サービステンプレート service1 を作成します。

```
<AP> system-view
[AP] 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。

```
[AP-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。

```
[AP-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。

```
[AP-wlan-st-service1] cipher-suite ccmp
[AP-wlan-st-service1] security-ie rsn
```

802.1X 認証モードを設定します。

```
[AP-wlan-st-service1] client-security authentication-mode dot1x
```

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。

```
[AP-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)　802.1X 認証ドメインとして dom1 を設定します。

```
[AP-wlan-st-service1] dot1x domain dom1
```

6)　サービステンプレート service1 を有効にします。

```
[AP-wlan-st-service1] service-template enable
[AP-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。

```
[AP] 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。

```
[AP-radius-radius1] primary authentication 10.1.1.3 1812
[AP-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。

```
[AP-radius-radius1] key authentication simple 12345
[AP-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。

```
[AP-radius-rs1] user-name-format without-domain
[AP-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。

```
[AP-radius-rs1] user-name-format with-domain
[AP-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。

```
[AP] domain dom1
[AP-isp-dom1] authentication lan-access radius-scheme radius1
[AP-isp-dom1] authorization lan-access radius-scheme radius1
[AP-isp-dom1] accounting lan-access radius-scheme radius1
```

```
[AP-isp-dom1] quit
```

9)　サービステンプレート service1 を AP の WLAN-Radio 1/0/2 に割り当てます。

```
[AP] interface WLAN-Radio 1/0/2
[AP-WLAN-Radio1/0/2] undo shutdown
[AP-WLAN-Radio1/0/2] service-template service1
[AP-WLAN-Radio1/0/2] quit
```

III. 設定の確認

 # display wlan service-template verbose コマンドを使用します。

```
<AP>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
```

3.7.6 WPA3 パーソナル設定例

I. ネットワーク要件

図 3-13 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。

- WPA3 パーソナルを設定します。
- 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。

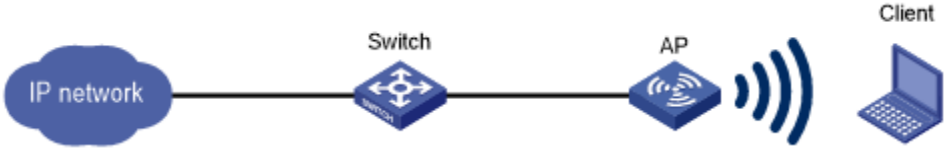


図 3-13 ネットワーク図

II. 設定手順

1)　サービステンプレート service1 を作成します。

```
<AP> system-view
[AP] 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。

```
[AP-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。

```
[AP-wlan-st-service1] akm mode psk
[AP-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。

```
[AP-wlan-st-service1] cipher-suite ccmp
[AP-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。

```
[AP-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。

```
[AP-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。

```
[AP-wlan-st-service1] service-template enable
[AP-wlan-st-service1] quit
```

7)　サービステンプレート service1 を AP の WLAN-Radio 1/0/2 に割り当てます。

```
[AP] interface WLAN-Radio 1/0/2
[AP-WLAN-Radio1/0/2] undo shutdown
```

```
[AP-WLAN-Radio1/0/2] service-template service1
[AP-WLAN-Radio1/0/2] quit
```

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。

```
< AP> 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                             : 2
 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**2-x-x** です。

4 章 WLAN 認証の概要（FIT は未サポート） 4-1
4.1 アプリケーションシナリオ 4-1
4.2 802.1X 認証 4-1
4.2.1 802.1X 認証のイニシエーション 4-1
4.2.2 802.1X 認証プロセス 4-2
4.3 MAC アドレス認証 4-5
4.3.1 ユーザアカウントポリシー 4-6
4.3.2 認証方式 4-6
4.4 OUI 認証 4-6
4.5 認証モード 4-7
4.6 侵入保護 4-7
4.7 WLAN の VLAN 操作 4-8
4.7.1 VLAN 認証 4-8
4.7.2 制限 VLAN 4-8
4.8 ほかの機能を用いた WLAN 認証 4-9
4.8.1 ACL の割り当て 4-9
4.8.2 ユーザプロファイルの割り当て 4-9

4章 WLAN 認証の概要（FIT は未サポート）

本章は WLAN 認証の実装について記載します。WLAN 認証はアクセスセキュリティを保証するため、WLAN クライアントを MAC アドレスベースでネットワークアクセスの制御を行います。

WLAN 認証は、802.1X 認証、MAC アドレス認証、OUI 認証があります。

4.1 アプリケーションシナリオ

図 4-1 に示すように、WLAN 認証は FAT AP ネットワークに適用可能です。FAT AP は認証装置として動作し、WLAN へのアクセスを制御するためにクライアントを認証します。

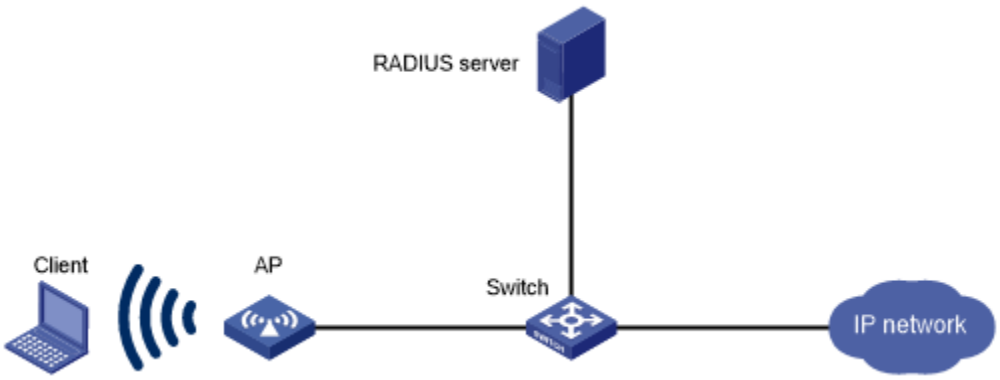


図 4-1 ネットワーク図

4.2 802.1X認証

802.1X はクライアント、認証装置、認証サーバの認証に関する情報を転送するために EAP（Extensible Authentication Protocol）を使用します。

802.1X は WLAN を超えてクライアントと認証装置間で EAP パケットを転送するため、EAPOL（EAP over LAN）を定義しています。認証装置と認証サーバ間で、802.1X は以下の方法の 1 つを使用して認証情報を送信します。

- EAP 中継モードで定義されているように、EAPOR（EAP over RADIUS）を使用して RADIUS の EAP パケットをカプセル化します。
- EAP 終端モードで定義されているように、EAP パケットから認証情報を抽出し、標準 RADIUS パケットの情報をカプセル化します。

EAP パケットのカプセル化の情報について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 “802.1X”* を参照してください。

4.2.1 802.1X 認証のイニシエーション

クライアントと認証装置は 802.1X 認証を開始することができます。

- **クライアントのイニシエーション**－クライアントが認証装置に関連付けられたのち、802.1X 認証を開始するため、クライアントは EAPOL-Start パケットを認証装置に送信します。
- **認証装置のイニシエーション**－クライアントが認証装置に関連付けられたのち、認証装置は認証を開始するため、EAP-Request/Identity パケットをクライアントに送信します。クライアントのタイムアウトタイマ以内に応答がない場合、認証装置はパケットを再送します。

4.2.2 802.1X 認証プロセス

認証装置は RADIUS サーバと通信するため、EAP 中継モードあるいは EAP 終端モードを使用します。

I. EAP 中継モード

このモードでは、認証装置は認証情報を RADIUS サーバに送信するため EAPOR パケットを使用します。RADIUS サーバは EAP-Message、Message-Authenticator 属性をサポートする必要があります。そして RADIUS サーバはクライアントと同一の認証方式を使用する必要があります。EAP 中継モードは、認証装置で **dot1x authentication-method eap** コマンドを設定するだけで有効となります。

図 4-2 に EAP 中継モードの基本的な 802.1X 認証のプロセスを示します。この例では EAP-MD5 が使用されています。

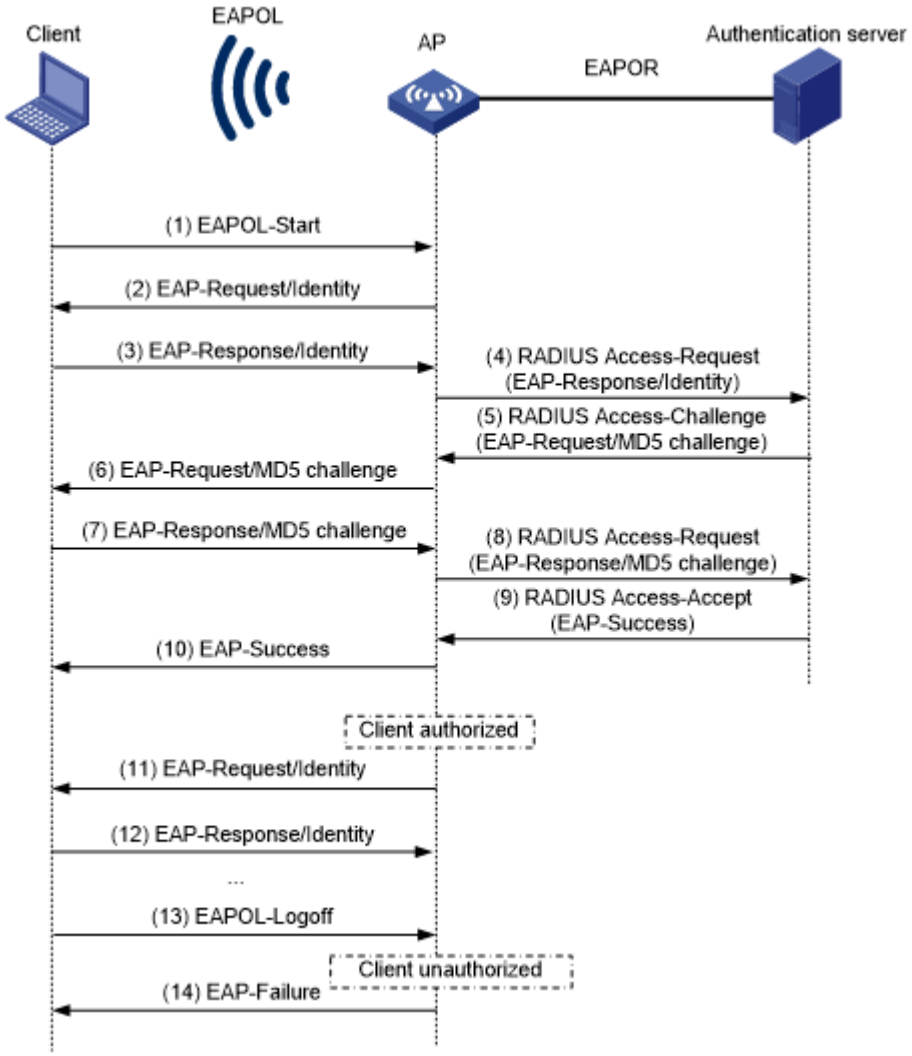


図 4-2 EAP 中継モードの 802.1X 認証プロセス

以下に 802.1X 認証プロセスを示します。

1) ユーザが 802.1X クライアントを実行し、登録されたユーザ名、パスワードを入力したとき、802.1X クライアントは EAPOL-Start パケットを認証装置に送信します。

   クライアントと AP アソシエ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 2 *WLAN “WLAN セキュリティ”* 参照してください。

2) 認証装置はユーザ名を要求するため、EAP-Request/Identity パケットを送信します。
3) クライアントは EAP-Request/Identity パケットのユーザ名を認証装置に送信します。
4) 認証装置は RADIUS Access-Request パケット内の EAP-Response/Identity パケットを、認証サーバに転送します。
5) 認証サーバは認証サーバにあるユーザデータベースを検索するため、RADIUS Access-Request のユーザ名を使用します。一致するエントリが検出された場合、サーバは、エントリのパスワードを暗号化するため、ランダムに作成されたチャレンジ（EAP-Request/MD5-challenge）を使用します。そしてサーバは RADIUS Access-Challenge のチャレンジデータを認証装置に送信します。
6) 認証装置は EAP-Request/MD5-Challenge パケットをクライアントに転送します。

7) クライアントはパスワードを暗号化するため、受信したチャレンジデータを使用します。EAP-Response/MD5-Challenge パケットの暗号化されたパスワードを認証装置に送信します。
8) 認証装置は RADIUS Access-Request パケット内の EAP-Response/MD5-Challenge パケットを認証サーバに転送します。
9) 認証サーバは受信した暗号パスワードと 5）で作成した暗号パスワードを比較します。2 つのパスワードが等しい場合、認証サーバはクライアントが正式であることを認識し、認証装置に RADIUS Access-Accept packet パケットを送信します。
10) RADIUS Access-Accept packet パケットを受信すると、認証装置はクライアントにネットワークへのアクセスを許可します。
11) クライアントがオンラインになったのち、認証装置は定期的にクライアントがオンラインかどうかを確認するため、ハンドシェイクリクエストを送信します。
12) ハンドシェイクリクエストを受信すると、クライアントは応答を返します。ハンドシェイクの連続試行回数（デフォルトで 2 回です）に到達しても、クライアントが応答を返さなかった場合、認証装置はクライアントをログオフします。ハンドシェイクメカニズムはオフラインとなっている 802.1X クライアントを切断することによってネットワークリソースの浪費を防ぐことができます。
13) クライアントはログオフする場合、認証装置に EAPOL-Logoff パケットを送信します。
14) EAPOL-Logoff パケットを受信した場合、認証装置はクライアントに EAP-Failure パケットを送信します。

II. EAP 終端モード

このモードでは認証装置は以下の処理を行います。

1) クライアントから受信した EAP パケットを終端します。
2) 標準 RADIUS パケットのクライアント認証情報をカプセル化します。
3) RADIUS サーバと通信するため PAP あるいは CHAP を使用します。

図 4-3 に EAP 終端モードの基本 802.1X 認証プロセスを示します。この例では CHAP 認証が使用されています。

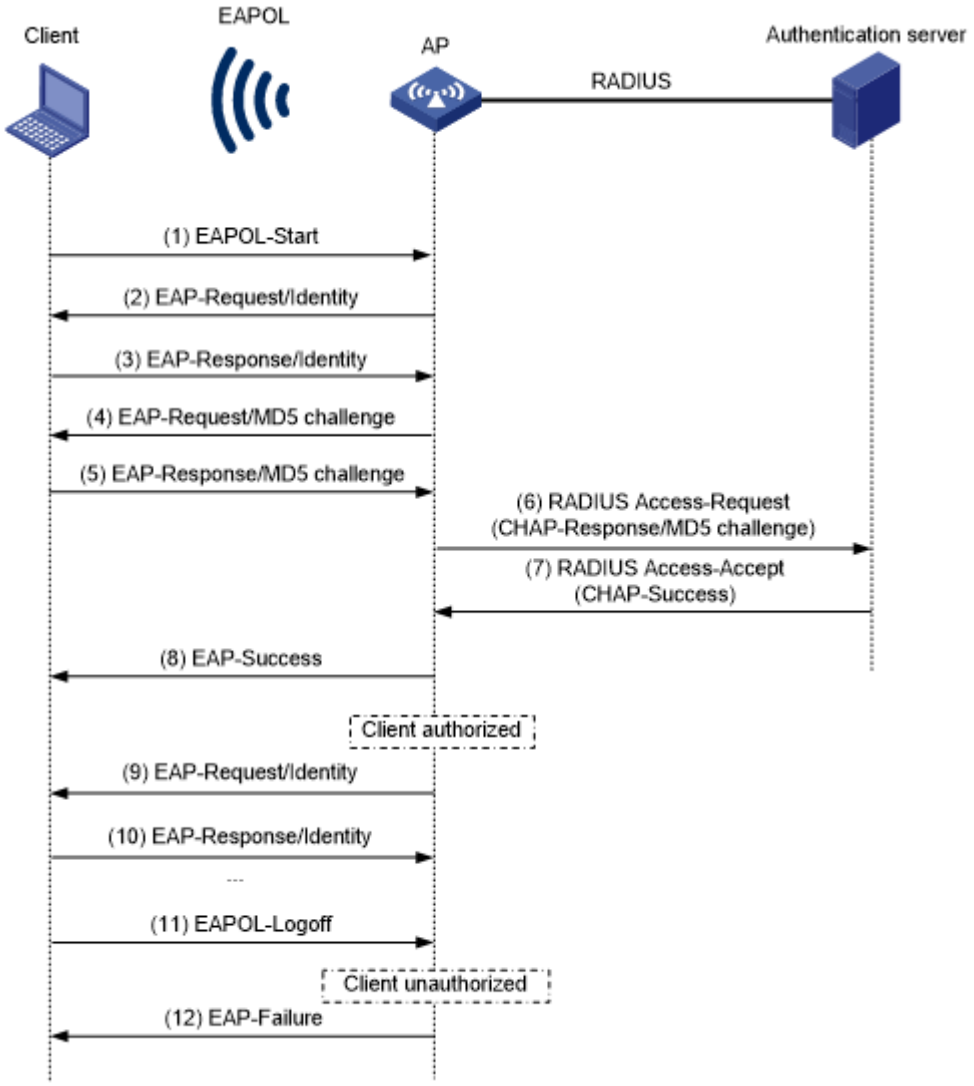


図 4-3 EAP 終端モードの 802.1X 認証プロセス

EAP 終端モードでは、パスワードの暗号化を行うため認証サーバではなく認証装置が MD5 チャレンジを作成します。そして認証装置は MD5 チャレンジに加えて、標準 RADIUS パケットのユーザ名と暗号化されたパスワードを RADIUS サーバに送信します。

4.3 MACアドレス認証

MAC アドレス認証は送信元 MAC アドレスを認証することでネットワークへのアクセスを制御します。この機能はクライアントソフトウェアを必要としません。ユーザは、ネットワークアクセス用のユーザ名とパスワードを入力する必要はありません。

未知の送信元 MAC アドレスが検出された場合、認証装置は、MAC アドレス認証プロセスを開始します。MAC アドレスが認証を通過した場合、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することができます。認証が失敗した場合、認証装置は、サイレント MAC アドレスとして MAC アドレスを記憶し、クライアントのアクセスを拒否します。

4.3.1 ユーザアカウントポリシー

ユーザアカウントはクライアントを識別するために必要です。MAC アドレス認証は、以下のユーザアカウントポリシーをサポートしています。

- **各ユーザのための MAC ベースのユーザアカウント**－認証装置は、MAC アドレス認証を行うため、クライアントのユーザ名、パスワードとしてパケットの未知の送信元 MAC アドレスを使用します。
- **すべてのユーザのための共有のユーザアカウント**－認証装置は、すべての MAC アドレス認証を行うため、クライアントのユーザ名とパスワードを指定します。ユーザ名とパスワードは MAC アドレスでなくても構いません。ユーザ名の設定範囲は 1～55 文字です。大文字、小文字を区別します。@マークを含めることはできません。プレーンテキストのパスワードの設定範囲は 1～63 文字です。暗号テキストのパスワードの設定範囲は 1～117 文字です。

4.3.2 認証方式

認証装置（ローカル認証）あるいは RADIUS サーバを通して MAC アドレス認証を行うことができます。

RADIUS 認証：

- **MAC ベースアカウント**－認証装置は、認証を行うため、ユーザ名、パスワードとしてパケットの送信元 MAC アドレスを RADIUS サーバに送信します。
- **共有アカウント**－認証装置は、認証を行うため共有アカウントのユーザ名とパスワードを RADIUS サーバに送信します。

ローカル認証：

- **MAC ベースアカウント**－認証装置は、ローカルアカウントデータベースに一致するかどうか検索するため、ユーザ名とパスワードとしてパケットの送信元 MAC アドレスを使用します。
- **共有アカウント**－認証装置は、ローカルアカウントデータベースに一致するかどうか検索するため、共有アカウントのユーザ名とパスワードを使用します。

ローカル認証と RADIUS 認証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。

4.4 OUI認証

OUI 認証はクライアントの MAC アドレスの OUI を調査します。認証装置のために設定された OUI の 1 つが、クライアントの OUI に一致している場合、クライアントは OUI 認証にパスします。

🕮 **メモ：**

IEEE によって定義される OUI は、装置ベンダ、メーカー、組織を識別する MAC アドレスの最初の 24 ビットです。MAC アドレスの最初の 3 オクテットは OUI です。

4.5 認証モード

🕮 **メモ：**

mac-and-dot1x パラメータは、ソフトウェアバージョン 7.2.14 を含む以降のソフトウェアからサポートしています。

認証モード	動作メカニズム
bypass（デフォルト）	認証を行いません。
dot1x	802.1X認証のみを実行します。
mac	MACアドレス認証のみを実行します。
mac-or-dot1x	MACアドレス認証を最初に実行し、次に802.1X認証を実行します。クライアントがMACアドレス認証にパスした場合、802.1X認証は実行されません。
dot1x-or-mac	802.1X認証を最初に実行し、次にMACアドレス認証を実行します。クライアントが802.1X認証にパスした場合、MACアドレス認証は実行されません。
oui-or-dot1x	OUI認証を最初に実行し、次に802.1X認証を行います。クライアントがOUI認証にパスした場合、802.1X認証は実行されません。
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。

4.6 侵入保護

認証装置が認証に失敗したクライアントからアソシエーションリクエストを検出した場合、侵入保護が開始されます。

この機能は、リクエストを受信したとき、BSS（basic service set）で以下に示す定義済みのアクションの 1 つが行われます。

- **temporary-block**（デフォルト）ーリクエストの送信元 MAC アドレスをブロック MAC アドレスリストに追加し、リクエストパケットを廃棄します。ブロックされた MAC アドレスのクライアントは一定期間、AP と接続を確立することができません。接続を確立できない期間を設定する場合、**client-security intrusion-protection timer temporary-block** コマンドを使用します。
- **service-stop**—radio インタフェースの BSS が手動で有効にされるまで、リクエストが受信された BSS を停止します。
- **temporary-service-stop**—一定期間リクエストが受信された BSS を停止します。

🕮 **メモ：**

侵入保護はバイパスモードではサポートしません。

4.7 WLANのVLAN操作

4.7.1 VLAN 認証

クライアントがネットワークリソースへのアクセスを制御するため、WLAN クライアント用に許可 VLAN を指定することができます。クライアントが 802.1X あるいは MAC アドレス認証にパスしたとき、認証サーバは許可 VLAN の情報を認証装置に割り当てます。

装置が認証装置として動作するとき、以下の形式でサーバが割り当てた VLAN を解決することができます。

- VLAN ID
- VLAN 名
- VLAN グループ名
- VLAN ID と VLAN 名の組み合わせ

🕮 **メモ：**

装置は VLAN をクライアントに割り当てる前、VLAN 名、VLAN グループ名を VLAN ID に置き換えます。装置がサーバから VLAN グループを受信した場合、許可 VLAN でもっとも小さい VLAN ID をもつ VLAN を選択します。

以下の場合、装置はクライアントの許可 VLAN を拒否します。

- 装置が許可 VLAN の情報を確定することができません。
- サーバは装置に VLAN 名を割り当てますが、VLAN 名を使用している VLAN が存在しません。
- サーバは装置に 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、あるいは VLAN グループに VLAN が割り当てられていません。

許可 VLAN の情報は、データ転送を制御するのに使用します。そのため、許可 VLAN の情報はデータトラフィックを転送する装置に割り当てる必要があります。VLAN 割り当ては、認証装置と転送装置が同一装置であるかによって、ローカル VLAN 割り当て、あるいはリモート VLAN 割り当てにすることができます。

- **ローカル VLAN 割り当て**－認証装置と転送装置は同一装置です。認証装置が許可 VLAN 情報を取得したのち、許可 VLAN 情報を解決し、VLAN を割り当てます。
- **リモート VLAN 割り当て**－認証装置と転送装置は異なる装置です。認証装置が許可 VLAN 情報を取得したのち、リモート転送装置に情報を送信します。転送装置は許可 VLAN 情報を解決し、VLAN を割り当てます。

VLAN の詳細はオペレーションマニュアルのセクション 4 *アクセス “VLAN”* を参照してください。

4.7.2 制限 VLAN

組織のセキュリティ戦略に遵守できずに失敗したことが原因で WLAN 認証に失敗したクライアントに対応するため、クライアントを WLAN の制限 VLAN に収容することができます。たとえば間違ったパスワードやユーザ名を入力したクライアントに制限 VLAN が適応されます。制限 VLAN は認証タイムアウトあるいはネットワークの接続問題のために認証に失敗した WLAN クライアントに適応しません。

制限 VLAN のクライアントは制限されたネットワークリソースにアクセスすることができます。

認証装置は、30 秒間隔で制限 VLAN のクライアントの再認証を行います。

- クライアントが再認証にパスした場合、認証装置はクライアントを許可 VLAN に割り当てます。許可 VLAN が設定されていない場合、クライアントは最初の 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、クライアントは制限 VLAN にとどまります。

RSNA を使用するクライアントは、クライアントが 802.1X 認証に失敗しても、制限 VLAN に割り当てることはできません。認証装置は RSNA を使用するクライアントを直接ログオフします。

制限 VLAN 機能は侵入保護機能よりも優先されます。クライアントが認証に失敗したとき、最初に制限 VLAN の設定を適用します。制限 VLAN が設定されていない場合、侵入保護機能が適用されます。制限 VLAN 機能、侵入保護機能の両方が設定されていない場合、認証装置はクライアントを直接ログオフします。

4.8 ほかの機能を用いたWLAN認証

4.8.1 ACL の割り当て

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するため、802.1X あるいは MAC アドレス認証クライアントに ACL を指定することができます。クライアントが認証にパスしたのち、認証サーバはクライアントのトラフィックをフィルタするため、クライアントに ACL を割り当てます。認証サーバは認証装置として動作するローカル装置、あるいは RADIUS サーバのどちらにすることができます。どちらの場合でも、認証装置で ACL の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の基準を変更する場合、以下の方法の 1 つを使用することができます。

- 認証装置で ACL ルールを変更します。
- 認証サーバでクライアント用に別の ACL を指定します。

ACL の詳細はオペレーションマニュアルのセクション 8 *ACL and QoS “ACL”* を参照してください。

4.8.2 ユーザプロファイルの割り当て

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するため、WLAN クライアントにユーザプロファイルを指定することができます。クライアントが 802.1X あるいは MAC アドレス認証にパスしたのち、認証サーバはトラフィックをフィルタするためクライアントにユーザプロファイルを割り当てます。認証サーバは認証装置として動作するローカル装置、あるいは RADIUS サーバのどちらかにすることができます。どちらの場合でも、認証装置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許可を変更する場合、以下の方法の 1 つを使用することができます。

- 認証装置でユーザプロファイルを変更します。
- 認証サーバでクライアント用に別のユーザプロファイルを指定します。

ユーザプロファイル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“ユーザプロファイル”* 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。

5章 WLAN認証の設定（FITは未サポート） 5-1
5.1 設定要件 5-1
5.2 WLAN認証の設定作業リスト 5-2
5.3 グローバルWLAN認証パラメータの設定 5-3
5.3.1 OUI認証のOUIの設定 5-3
5.3.2 802.1Xでサポートされるドメイン名デリミタの設定 5-3
5.3.3 802.1XのEAP中継モード、EAP終端モードの有効化 5-4
5.3.4 802.1X認証リクエストの最大試行回数の設定 5-4
5.3.5 802.1X認証タイマの設定 5-5
5.3.6 MACアドレス認証の認証方式の設定 5-6
5.3.7 MACアドレス認証のユーザアカウントのフォーマットの設定 5-6
5.3.8 グローバルでのMACアドレス認証ドメインの設定 5-6
5.3.9 MACアドレス認証サーバタイムアウトタイマの設定 5-7
5.4 サービス特有のWLAN認証パラメータの設定 5-7
5.4.1 認証モードの設定 5-7
5.4.2 サーバからの許可情報の無視設定 5-8
5.4.3 WLAN制限VLANの設定 5-8
5.4.4 authorization-fail-offline機能の有効化 5-8
5.4.5 侵入保護の設定 5-9
5.4.6 オンラインユーザハンドシェイク機能の設定 5-9
5.4.7 802.1X認証ドメインの設定 5-10
5.4.8 802.1X認証クライアントの最大同時接続数の設定 5-10
5.4.9 定期的なオンラインユーザ再認証機能の有効化 5-11
5.4.10 MACアドレス認証クライアントの最大同時接続数の設定 5-12
5.4.11 サービス特有のMACアドレス認証のドメインの設定 5-12
5.5 Web認証(ポータル認証)の設定 5-12
5.6 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 5-13
5.6.1 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について 5-13
5.6.2 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作業リスト 5-13
5.6.3 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指定 5-13
5.7 失敗許可機能の有効化 5-14
5.7.1 失敗許可機能について 5-14
5.7.2 失敗許可機能の設定 5-14
5.7.3 RADIUSサーバ検出の設定 5-15
5.8 WLAN認証の表示と維持 5-15
5.9 WLAN認証の設定例 5-16
5.9.1 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 5-16
5.9.2 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 5-17
5.9.3 802.1X認証時の失敗許可機能設定例 5-20

5章 WLAN 認証の設定（FIT は未サポート）

この章は WLAN 認証の設定について記載します。

5.1 設定要件

WLAN 認証を設定する前に、以下の作業を完了してください。

- WLAN クライアントの ISP ドメイン、AAA スキーム（ローカル認証あるいは RADIUS 認証）を設定してください。
- ローカル認証を使用する場合、装置でローカルユーザアカウント（ユーザ名、パスワードを含みます。）を作成してください。サービスタイプを lan-access に設定してください。
- RADIUS 認証を使用する場合、装置と RADIUS サーバが互いに通信可能であることを確認してください。RADIUS サーバでユーザアカウントを作成してください。MAC アドレス認証のクライアント用に MAC ベースのアカウントを使用している場合、各アカウントのユーザ名とパスワードが、各クライアントの MAC アドレスと同一であることを確認してください。

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。

5.2 WLAN認証の設定作業リスト

作業リスト
• （オプション設定項目）グローバルWLAN認証パラメータの設定 　• OUI認証のOUIの設定 　• 802.1Xでサポートされるドメイン名デリミタの設定 　• 802.1XのEAP中継モード、EAP終端モードの有効化 　• 802.1X認証リクエストの最大試行回数の設定 　• 802.1X認証タイマの設定 　• MACアドレス認証の認証方式の設定 　• MACアドレス認証のユーザアカウントのフォーマットの設定 　• グローバルでのMACアドレス認証ドメインの設定 　• MACアドレス認証サーバタイムアウトタイマの設定
• サービス特有のWLAN認証パラメータの設定 　• （必須設定項目）認証モードの設定 　• （オプション設定項目）サーバからの許可情報の無視設定 　• （オプション設定項目）WLAN制限VLANの設定 　• （オプション設定項目）authorization-fail-offline機能の有効化 　• （オプション設定項目）侵入保護の設定 　• （オプション設定項目）オンラインユーザハンドシェイク機能の設定 　• （オプション設定項目）802.1X認証ドメインの設定 　• （オプション設定項目）802.1X認証クライアントの最大同時接続数の設定 　• （オプション設定項目）定期的なオンラインユーザ再認証機能の有効化 　• （オプション設定項目）MACアドレス認証クライアントの最大同時接続数の設定 　• （オプション設定項目）サービス特有のMACアドレス認証のドメインの設定

5.3 グローバルWLAN認証パラメータの設定

5.3.1 OUI 認証の OUI の設定

以下に OUI 認証の OUI 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． OUI 認証の OUI を設定する	**port-security oui index** *index-value* **mac-address** *oui-value*	デフォルト：設定なし このステップはoui-then-dot1xモードでのみ必要です。 OUIを複数設定することができます。装置は最大16 のOUIをサポートします。 コマンドの詳細はコマンドマニュアルのセクション2 *セWLAN “WLAN認証の設定”* を参照してください。

5.3.2 802.1X でサポートされるドメイン名デリミタの設定

以下に 802.1X でサポートされるドメイン名デリミ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． 802.1X クライアントのドメイン名デリミタを設定する	**dot1x domain-delimiter** *string*	デフォルト：（@）デリミタのみサポートします。 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 “802.1X”* を参照してください。

5.3.3 802.1X の EAP 中継モード、EAP 終端モードの有効化

以下に 802.1X EAP 中継モード、EAP 終端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． EAP 中継モード、EAP 終端モードを有効にする	**dot1x authentication-method** { **chap** | **eap** | **pap** }	デフォルト：装置はEAP終端モードを実行し、RADIUSサーバとCHAPを使用して通信します。 EAP中継モードを有効にする場合、**eap**パラメータを指定します。 CHAPあるいはPAPが有効なEAP終端モードを有効にする場合、**chap**パラメータあるいは**pap**パラメータを指定します。 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 "802.1X"* を参照してください。

🕮 **メモ：**

EAP 中継モードが使用された場合、RADIUS scheme view で設定された **user-name-format** コマンドは適用されません。装置はクライアントからサーバに認証データを変更しないで送信します。**user-name-format** コマンドについての詳細は、コマンドマニュアルのセクション 9 *セキュリティ "AAA"* を参照してください。

5.3.4 802.1X 認証リクエストの最大試行回数の設定

以下に 802.1X 認証リクエストの最大試行回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． 802.1X 認証リクエストの最大試行回数を設定する	**dot1x retry** *max-retry-value*	デフォルト：2 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 "802.1X"* を参照してください。

5.3.5 802.1X 認証タイマの設定

802.1X はクライアントと RADIUS サーバ間の相互通信を制御するため、以下のタイマを使用します。

- **クライアントタイムアウトタイマ**－装置がクライアントに EAP-Request/MD5 Challenge パケットを送信するときに起動します。このタイマが時間切れになるまでクライアントから応答がなかった場合、装置は、クライアントにリクエストを再送します。応答を受信することなく最大試行回数に到達した場合、クライアントは認証に失敗します。最大試行回数を設定する場合、**dot1x retry** コマンドを使用します。
- **サーバタイムアウトタイマ**－装置が認証サーバに RADIUS Access-Request パケットを送信するときに起動します。このタイマが時間切れになるまでに応答がなかった場合、装置は、サーバにリクエストを再送します。
- **ハンドシェイクタイマ**－クライアントが認証にパスしたのち、オンラインユーザのハンドシェイクが有効になったときに起動します。装置は各ハンドシェイク間隔でクライアントにハンドシェイクメッセージを送信します。最大ハンドシェイク試行回数に到達したのち、クライアントから応答を受信しない場合、装置はクライアントをログオフします。最大試行回数を設定する場合、**dot1x retry** コマンドを使用します。
- **定期的再認証タイマ**－クライアントが認証にパスしたのち、定期的なオンラインユーザの再認証が有効になったときに起動します。装置は設定された間隔でクライアントを再認証します。設定の変更を行ったのちに、オンラインになったクライアントのみ設定の変更が適用されます。

ほとんどの場合、デフォルトの設定で十分です。ネットワークの状況に応じてタイマを設定することができます。

- パフォーマンスの低いネットワークで、クライアントタイムアウトタイマを高い値に設定します。
- 異なる性能の認証サーバがあるネットワークでサーバタイムアウトタイマを調整します。

以下に 802.1X 認証タイムアウト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． クライアント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：30秒 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 “802.1X”* を参照してください。
3． サーバ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 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 “802.1X”* を参照してください。
4． ハンドシェイクタイマを設定する	**dot1x timer handshake-period** *handshake-period-value*	デフォルト：15秒 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 “802.1X”* を参照してください。

操作	コマンド	補足
5． 定期的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 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 “802.1X”* を参照してください。

5.3.6 MAC アドレス認証の認証方式の設定

以下に MAC アドレス認証の認証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． MAC アドレス認証の認証方式を設定する	**mac-authentication authentication-method { chap | pap }**	デフォルト：MACアドレス認証にPAPを使用します。 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“MACアドレス認証”* を参照してください。

5.3.7 MAC アドレス認証のユーザアカウントのフォーマットの設定

以下に MAC アドレス認証のユーザアカウントの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． MAC アドレス認証のユーザアカウントのフォーマットを設定する	● 各クライアントにMACベースのユーザアカウントを使用する： **mac-authentication user-name-format mac-address** [{ **with-hyphen** | **without-hyphen** } [**lowercase** | **uppercase**]] ● すべてのユーザに共有ユーザアカウントを使用する： **mac-authentication user-name-format fixed** [**account** *name*] [**password** { **cipher** | **simple** } *password*]	デフォルト：MACアドレス認証のユーザ名とパスワードとしてクライアントのMACアドレスを使用します。 MACアドレスは16進数でハイフンなし、小文字のみです。 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“MACアドレス認証”* を参照してください。

5.3.8 グローバルでの MAC アドレス認証ドメインの設定

クライアントで異なるアクセスポリシーを設定する場合、グローバルあるいはサービステンプレートで MAC アドレス認証の ISP ドメインを指定することができます。

WLAN クライアントの MAC アドレス認証は以下の順番で ISP ドメインを選択します。

1)　サービステンプレートで設定されたドメイン

2)　system view で設定されたグローバルの MAC アドレス認証のドメイン
3)　デフォルトドメイン

ISP ドメインの詳細はオペレーションマニュアルのセクション 9 *セキュリティ　“AAA”* を参照してください。

以下にグローバルでの MAC アドレス認証クライアントの ISP ドメ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.　グローバルでの MAC アドレス認証ドメインを設定する	**mac-authentication domain** *domain-name*	デフォルト：設定なし 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“MACアドレス認証”* を参照してください。

5.3.9 MAC アドレス認証サーバタイムアウトタイマの設定

装置が RADIUS サーバに認証リクエストを送信するとき、MAC アドレス認証はサーバタイムアウトタイマを起動します。装置がタイムアウトタイマ以内に RADIUS サーバから応答を受信しない場合、装置はサーバを到達不能と認識します。MAC アドレス認証の間、タイマが終了した場合、クライアントはネットワークにアクセスすることができません。

以下に MAC アドレス認証サーバタイムアウト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.　MAC アドレス認証サーバタイムアウトタイマを設定する	**mac-authentication timer server-timeout** *server-timeout-value*	デフォルト：100秒 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“MACアドレス認証”* を参照してください。

5.4 サービス特有のWLAN認証パラメータの設定

5.4.1 認証モードの設定

以下に認証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.　service template view に移行する	**wlan service-template** *service-template-name*	―
3.　WLAN クライアントの認証モードを設定する	**client-security authentication-mode** { **dot1x** | **dot1x-then-mac** | **mac** | **mac-then-dot1x** | **oui-then-dot1x** | **mac-and-dot1x** }	デフォルト：設定なし。装置は認証を実行しません（認証バイパスモード）。クライアントは直接装置にアクセスすることができます。

5.4.2 サーバからの許可情報の無視設定

クライアントが 802.1X 認証あるいは MAC アドレス認証にパスしたのち、サーバ（ローカル、リモート）から受信した許可情報を使用しないように無視することができます。許可情報は VLAN、ACL、ユーザプロファイルがあります。

以下にサーバからの認証情報を無視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． 認証サーバから受信した許可情報を無視する	**client-security ignore-authorization**	デフォルト：サーバから受信した許可情報を使用します。

5.4.3 WLAN 制限 VLAN の設定

以下に WLAN 制限 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． service template view に移行する	**wlan service-template** *service-template-name*	―
3． WLAN 制限 VLAN を設定する	**client-security authentication fail-vlan** *vlan-id*	デフォルト：設定なし WLAN制限VLANはサービステンプレートでのみ設定できます。

5.4.4 authorization-fail-offline 機能の有効化

authorization-fail-offline 機能は ACL あるいはユーザプロファイルで許可されていない WLAN クライアントをログオフします。

以下の状況の場合、クライアントは ACL あるいはユーザプロファイルの許可に失敗します。

- 装置あるいはサーバは、クライアントに指定した ACL あるいはユーザプロファイルの許可を失敗します。
- 許可された ACL あるいはユーザプロファイルは存在しません。

本機能は VLAN 認証に失敗したクライアントには適用されません。装置はこれらのクライアントを直接ログオフします。

以下に authorization-fail-offline 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． service template view に移行する	**wlan service-template** *service-template-name*	―

操作	コマンド	補足
3． authorization-fail-offline 機能を有効にする	**client-security authorization-fail offline**	デフォルト：無効 ACLあるいはユーザプロファイルで許可されていないクライアントをログオフしません。そしてシステムのログを出力します。

5.4.5 侵入保護の設定

以下に侵入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． service template view に移行する	**wlan service-template** *service-template-name*	―
3． 侵入保護を有効にする	**client-security intrusion-protection enable**	デフォルト：無効
4． （オプション設定項目）侵入保護のアクションを設定する	**client-security intrusion-protection action** { **service-stop** | **temporary-block** | **temporary-service-stop** }	デフォルト：**temporary-block**
5． （オプション設定項目）不正なクライアントに対するブロック期間を設定する	**client-security intrusion-protection timer temporary-block** *value*	デフォルト：180秒
6． （オプション設定項目）BSS が無効状態され続ける silence 期間を設定する	**client-security intrusion-protection timer temporary-service-stop** *value*	デフォルト：20秒

5.4.6 オンラインユーザハンドシェイク機能の設定

オンラインユーザのハンドシェイク機能はオンライン 802.1X クライアントの接続状態を確認します。装置はオンラインクライアントに、**dot1x timer handshake-period** コマンドによって設定された間隔でハンドシェイクメッセージを送信します。最大ハンドシェイク試行回数に到達したのち、クライアントから応答を受信しない場合、装置はクライアントをログオフします。

オンラインユーザハンドシェイクのセキュリティ機能はハンドシェイクメッセージに認証情報を追加します。この機能によって、偽造された 802.1X クライアントから、装置とハンドシェイクメッセージを交換する正式なクライアントを防ぐことができます。この機能において、装置はクライアントから受信したハンドシェイクレスポンスメッセージの認証情報と、認証サーバに割り当てられた認証情報を比較します。一致しない場合、装置はクライアントをログオフします。

I. 設定ガイドライン

オンラインユーザハンドシェイク機能を設定する場合、以下の制限とガイドラインに従ってください。

- オンラインユーザハンドシェイクのセキュリティ機能を使用する場合、オンラインユーザハンドシェイク機能を有効にしてください。
- オンラインユーザハンドシェイクのセキュリティ機能はオンラインで認証された802.1X クライアントのみ保護します。

II. 設定手順

以下にオンラインユーザハンドシェイ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. service template 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イク機能を設定する	**dot1x handshake enable**	デフォルト：無効
4. （オプション設定項目）オンラインユーザハンドシェイクのセキュリティ機能を設定する	**dot1x handshake secure enable**	デフォルト：無効

5.4.7 802.1X 認証ドメインの設定

WLAN クライアントの 802.1X 認証は以下の順番で ISP ドメインを選択します。

- サービステンプレートで指定されたドメイン
- ユーザ名で指定されたドメイン
- デフォルトドメイン

以下に 802.1X 認証ドメ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. service template view に移行する	**wlan service-template** *service-template-name*	―
3. 802.1X 認証ドメインを設定する	**dot1x domain** *domain-name*	デフォルト：設定なし

5.4.8 802.1X 認証クライアントの最大同時接続数の設定

サービステンプレートの 802.1X 認証クライアントの同時接続数が最大になったとき、新規の 802.1X 認証クライアントは拒否されます。

🕮 **メモ：**

- 802.1X 認証クライアント同時接続数を、サービステンプレートを設定した無線インタフェースごとに制限します。
- 1 つの無線インタフェースで同時に接続可能なクライアント最大数は 512 です。
- 無線インタフェースで同時に接続可能なクライアント最大数を超えて接続することはできません。

以下に 802.1X 認証クライアントの最大同時接続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． 802.1X 認証クライアントの最大同時接続数を設定する	**dot1x max-user** *count*	デフォルト：512

5.4.9 定期的なオンラインユーザ再認証機能の有効化

オンラインクライアントの接続状態を確認するため、定期的なオンラインユーザの再認証を行い、サーバによって割り当てられた許可属性をアップデートします。属性には ACL、VLAN、QoS ベースのユーザプロファイルが含まれます。再認証の間隔はユーザが設定できます。

サーバによって割り当てられた RADIUS 属性の Session-Timeout、Termination-Action は、定期的なオンラインユーザの再認証に影響します。サーバによって割り当てられた Session-Timeout、Termination-Action を表示する場合、**display dot1x connection** コマンドを使用します。コマンドマニュアルのセクション 9 *セキュリティ “802.1X”* を参照してください。

- Termination-Action がログオフユーザである場合、定期的な再認証は、定期再認証タイマが Session-Timeout タイマよりも小さいときのみ適用されます。Session-Timeout が定期再認証タイマより小さい場合、Session-Timeout タイマが終了したとき、装置は認証されたオンラインユーザをログオフします。
- Termination-Action が RADIUS リクエストである場合、装置で定期的な再認証は適用されません。Session-Timeout タイマが終了したのち、オンライン 802.1X ユーザを再認証します。

サーバの設定をサポートし、サーバモデルに応じて Session-Timeout タイマと Termination-Action を割り当ててください。

以下に定期的なオンラインユーザ再認証機能の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． 定期的なオンラインユーザ再認証機能を有効にする	**dot1x re-authenticate enable**	デフォルト：無効

5.4.10 MAC アドレス認証クライアントの最大同時接続数の設定

サービステンプレートの MAC アドレス認証クライアントの同時接続数が最大になったとき、新規 MAC アドレス認証クライアントは拒否されます。

🕮 **メモ：**

- MAC アドレス認証クライアント同時接続数を、サービステンプレートを設定した無線インタフェースごとに制限します。
- 1 つの無線インタフェースで同時に接続可能なクライアント最大数は 512 です。
- 無線インタフェースで同時に接続可能なクライアント最大数を超えて接続することはできません。

以下に MAC アドレス認証クライアントの最大同時接続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． MAC アドレス認証クライアントの最大同時接続数を設定する	**mac-authentication max-user** *count*	デフォルト：512

5.4.11 サービス特有の MAC アドレス認証のドメインの設定

WLAN クライアントの MAC アドレス認証は以下の順番で ISP ドメインを選択します。

- サービステンプレートで指定されたドメイン
- system view で指定されたグローバルの MAC アドレス認証のドメイン
- デフォルトドメイン

以下に MAC アドレス認証クライアントの ISP ドメ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． service template view に移行する	**wlan service-template** *service-template-name*	―
3． 802.1X 認証ドメインを設定する	**mac-authentication domain** *domain-name*	デフォルト：設定なし

5.5 Web認証(ポータル認証)の設定

Web 認証(ポータル認証)の設定に関するコンフィグについては、別紙の共通マニュアル”*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*”を参照してください。

5.6 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

5.6.1 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について

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。

5.6.2 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作業リスト

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設定するには、次の手順に従います。

作業リスト
• 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指定

5.6.3 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指定

レーダーによる通信停止回避を行うためには 1 つのサービステンプレートに対して、1 つのバックアップ用のサービステンプレートを用意します。

- バックアップ用サービステンプレートには、fail-permit 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。

以下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

5.7 失敗許可機能の有効化

5.7.1 失敗許可機能について

🕮 **メモ：**

- 失敗許可機能は、APがRADIUSサーバ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。

失敗許可機能をサービステンプレートで有効にすることで、AP が 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。

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。

5.7.2 失敗許可機能の設定

MAC アドレス認証で失敗許可機能を使用する場合、サービステンプレートを 1 つ設定します。このとき、同一サービステンプレートに PSK 認証も設定する必要があります。AP が RADIUS サーバと通信不能になってから数分後、失敗許可機能が動作します。接続済みのクライアントは、接続を維持します。新規クライアントは、失敗許可機能動作後に接続可能です。RADIUS サーバと AP の切断前は、クライアントは MAC 認証及び PSK 認証で認証されます。切断後は PSK 認証で認証されます。設定方法の詳細は、設定例（*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*）を参照してください。

802.1X 認証で失敗許可機能を使用する場合、サービステンプレートを 2 つ設定します。1 つのサービステンプレートには 802.1X 認証の設定および **fail-permit enable** コマンドを設定します。もう一方のサービステンプレートにはバックアップ用に PSK 認証および **fail-permit template** コマンドを設定します。AP が RADIUS サーバと通信不能になるまではバックアップ用の SSID は表示されません。AP が RADIUS サーバと通信不能になってから数分後に失敗許可機能が動作します。接続済みのクライアントは接続を維持します。新規クライアントは、失敗許可機能動作後に接続可能です。RADIUS サーバと AP の切断前は、クライアントは 802.1X 認証で認証されます。切断後はバックアップ用の PSK 認証で認証されます。設定方法の詳細は、設定例（*802.1X 認証時の失敗許可機能設定例*）を参照してください。

失敗許可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． service template view に移行する	**wlan service-template** *service-template-name*	―
3． 失敗許可を有効にする	**fail-permit enable** [**keep-online**]	デフォルト：無効

5.7.3 RADIUS サーバ検出の設定

失敗許可機能を利用する認証に RADIUS サーバを使用する際、RADIUS サーバが利用可能かを検出するために、RADIUS サーバ検出を設定する必要があります。

RADIUS サーバ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**	ー
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

5.8 WLAN認証の表示と維持

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
オンライン802.1Xクライアントの情報を表示する	**display dot1x connection** [**interface** *interface-type interface-number* | **user-mac** *mac-address* | **user-name** *name-string*]
802.1Xセッションの接続情報、統計情報、設定情報を表示する	**display dot1x** [**sessions** | **statistics**] [**interface** *interface-type interface-number*]
MACアドレス認証の接続を表示する	**display mac-authentication connection** [**interface** *interface-type interface-number* | **user-mac** *mac-address* | **user-name** *name-string*]
MACアドレス認証の情報を表示する	**display mac-authentication** [**interface** *interface-type interface-number*]
ブロックしたMACアドレスの情報を表示する	**display wlan client-security block-mac**
802.1Xの統計情報を削除する	**reset dot1x statistics** [**interface** *interface-type interface-number*]
MACアドレス認証の統計情報を削除する	**reset mac-authentication statistics** [**interface** *interface-type interface-number*]

🕮 **メモ：**

display dot1x connection コマンド、**display dot1x** コマンド、**reset dot1x statistics** コマンド、**display mac-authentication connection** コマンド、**display mac-authentication** コマンド、**reset mac-authentication statistics** 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 "802.1X"、"MAC アドレス認証"* を参照してください。

5.9 WLAN認証の設定例

5.9.1 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 5-1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 1 つ、バックアップ用のサービステンプレートを 1 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 5-1 ネットワーク図

II. 設定手順

1)　オリジナルの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。

```
[AP-wlan-st-service1] ssid service1
[AP-wlan-st-service1] akm mode psk
[AP-wlan-st-service1] preshared-key pass-phrase simple 12345678
[AP-wlan-st-service1] cipher-suite ccmp
[AP-wlan-st-service1] security-ie rsn
[AP-wlan-st-service1] service-template enable
[AP-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。

```
[AP-wlan-st-service1_BU] ssid service1
[AP-wlan-st-service1_BU] fail-permit template
[AP-wlan-st-service1_BU] akm mode psk
[AP-wlan-st-service1_BU] preshared-key pass-phrase simple 12345678
```

```
[AP-wlan-st-service1_BU] cipher-suite ccmp
[AP-wlan-st-service1_BU] security-ie rsn
[AP-wlan-st-service1_BU] service-template enable
[AP-wlan-st-service1_BU] quit
```

3)　オリジナルとバックアップ用のサービステンプレートを別 radio に割り当てます。

```
[AP] interface wlan-radio 1/0/2
[AP-WLAN-Radio1/0/2] undo shutdown
[AP-WLAN-Radio1/0/2] service template service1
[AP-WLAN-Radio1/0/2] service template service2_BU
[AP-WLAN-Radio1/0/2] quit
[AP] interface wlan-radio 1/0/3
[AP-WLAN-Radio1/0/3] undo shutdown
[AP-WLAN-Radio1/0/3] service template service2
[AP-WLAN-Radio1/0/3] service template service1_BU
[AP-WLAN-Radio1/0/3] quit
```

5.9.2 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 5-2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。

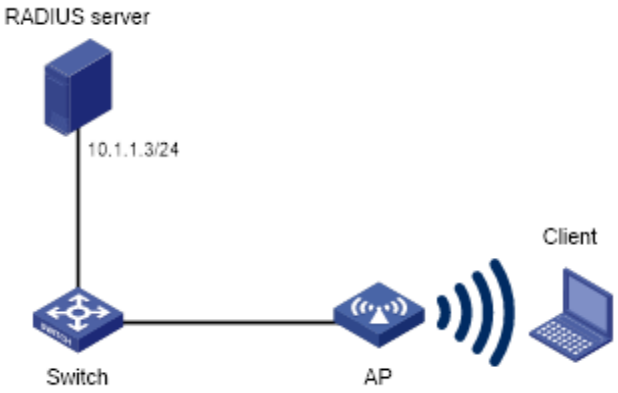


図 5-2 ネットワーク図

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 AP 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。

```
<AP> system-view
[AP] wlan service-template service1
[AP-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鍵 12345678 を指定します。

```
[AP-wlan-st-service1] akm mode psk
[AP-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。

```
[AP-wlan-st-service1] cipher-suite ccmp
[AP-wlan-st-service1] security-ie rsn
```

MAC アドレス認証を設定します。

```
[AP-wlan-st-service1] client-security authentication-mode mac
```

4) 失敗許可機能を有効にします。

```
[AP-wlan-st-service1] fail-permit enable
```

5) サービステンプレート service1 を有効にします。

```
[AP-wlan-st-service1] service-template enable
[AP-wlan-st-service1] quit
```

6) RADIUS サーバ検出を設定します。

```
[AP] radius-server test-profile 1 username nectest interval 1
```

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。

```
[AP] 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。

```
[AP-radius-radius1] primary authentication 10.1.1.3 1812 test-profile 1
[AP-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。

```
[AP-radius-radius1] key authentication simple 12345678
[AP-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。

```
[AP-radius-radius1] user-name-format without-domain
[AP-radius-radius1] 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。

```
[AP-radius-radius1] user-name-format with-domain
[AP-radius-radius1] 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。

```
[AP] domain dom1
[AP-isp-dom1] authentication lan-access radius-scheme radius1
[AP-isp-dom1] authorization lan-access radius-scheme radius1
[AP-isp-dom1] accounting lan-access radius-scheme radius1
[AP-isp-dom1] quit
```

9) MAC アドレス認証を有効にします。

```
[AP] mac-authentication
```

10) 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。

```
[AP] mac-authentication domain dom1
[AP] mac-authentication user-name-format mac-address with-hyphen lowercase
```

11) サービステンプレート service1 を AP の radio 2 に割り当て、radio 2 を有効にします。

```
[AP] interface WLAN-Radio 1/0/2
[AP-WLAN-Radio1/0/2] service-template service1
[AP-WLAN-Radio1/0/2] undo shutdown
[AP-WLAN-Radio1/0/2] quit
```

🕮 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。）

5.9.3 802.1X 認証時の失敗許可機能設定例

I. ネットワーク要件

図 5-3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。

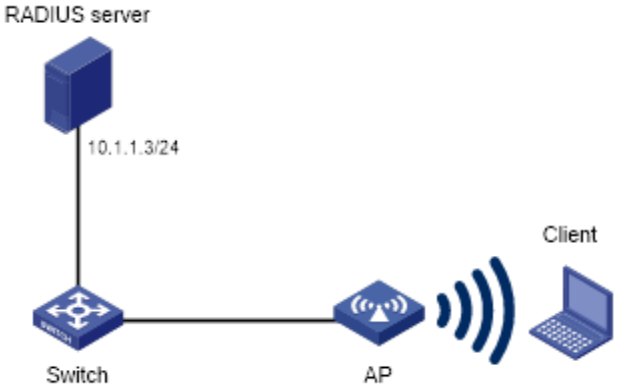


図 5-3 ネットワーク図

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 AP 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。

```
<AP> system-view
[AP] 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。

```
[AP-wlan-st-service1] ssid service_dot1x
```

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。

```
[AP-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。

```
[AP-wlan-st-service1] cipher-suite ccmp
[AP-wlan-st-service1] security-ie rsn
```

802.1X 認証モードを設定します。

```
[AP-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。

```
[AP-wlan-st-service1] dot1x domain dom1
```

6)　失敗許可機能を有効にします。

```
[AP-wlan-st-service1] fail-permit enable
```

7)　サービステンプレート service1 を有効にします。

```
[AP-wlan-st-service1] service-template enable
[AP-wlan-st-service1] quit
```

8)　802.1X を設定します。

```
[AP] dot1x
[AP] dot1x authentication-method eap
```

9)　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。

```
<AP> system-view
[AP] wlan service-template service1_bu
```

10) サービステンプレートの SSID サービスを指定します。

```
[AP-wlan-st-service1_bu] ssid service_psk
```

11) サービステンプレート service1_bu 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。

```
[AP-wlan-st-service1_bu] akm mode psk
[AP-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。

```
[AP-wlan-st-service1_bu] cipher-suite ccmp
[AP-wlan-st-service1_bu] security-ie rsn
```

12) バックアップ用に fail-permit template を設定します。

```
[AP-wlan-st-service1_bu] fail-permit template
```

13) サービステンプレート service1_bu を有効にします。

```
[AP-wlan-st-service1_bu] service-template enable
[AP-wlan-st-service1_bu] quit
```

14) RADIUS サーバ検出を設定します。

```
[AP] radius-server test-profile 1 username nectest interval 1
```

15) 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。

```
[AP] 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。

```
[AP-radius-radius1] primary authentication 10.1.1.3 1812 test-profile 1
[AP-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。

```
[AP-radius-radius1] key authentication simple 12345
[AP-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。

```
[AP-radius-radius1] user-name-format without-domain
[AP-radius-radius1] 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。

```
[AP-radius-radius1] user-name-format with-domain
[AP-radius-radius1] quit
```

16) 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。

```
[AP] domain dom1
[AP-isp-dom1] authentication lan-access radius-scheme radius1
[AP-isp-dom1] authorization lan-access radius-scheme radius1
[AP-isp-dom1] accounting lan-access radius-scheme radius1
[AP-isp-dom1] quit
```

17) サービステンプレート service1 と service1_bu を AP の radio 2 に割り当て、radio 2 を有効にします。

```
[AP] interface WLAN-Radio 1/0/2
[AP-WLAN-Radio1/0/2] service-template service1
[AP-WLAN-Radio1/0/2] service-template service1_bu
[AP-WLAN-Radio1/0/2] undo shutdown
[AP-WLAN-Radio1/0/2] quit
```

🕮 **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。）

目次

このセクションのページは**2-x-x** です。

6 章 WIPS の概要（FIT は未サポート） 6-1
6.1 概要 6-1
6.2 攻撃検出 6-1
6.2.1 フラッドアタックの検出 6-1
6.2.2 不正パケットの検出 6-2
6.2.3 なりすまし攻撃の検出 6-4
6.2.4 Weak IV の検出 6-4
6.2.5 Omerta 攻撃の検出 6-4
6.2.6 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 6-5
6.2.7 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 6-5
6.2.8 パワーセーブ攻撃の検出 6-5
6.2.9 禁止チャンネルの検出 6-5
6.2.10 ソフト AP の検出 6-5
6.2.11 Windows ブリッジの検出 6-5
6.2.12 未暗号化装置の検出 6-6
6.2.13 ホットスポット攻撃の検出 6-6
6.2.14 AP なりすまし攻撃の検出 6-6
6.2.15 HT-グリーンフィールド AP の検出 6-6
6.2.16 ハニーポット AP の検出 6-6
6.2.17 MITM 攻撃の検出 6-7
6.2.18 無線ブリッジの検出 6-7
6.2.19 アソシエーション/再アソシエーション DoS 攻撃の検出 6-7
6.2.20 AP フラッド攻撃の検出 6-7
6.2.21 装置エントリ攻撃の検出 6-7
6.2.22 シグネチャにもとづいた攻撃の検出 6-7
6.3 装置の種別 6-8
6.3.1 AP の種別 6-8
6.3.2 クライアント種別 6-11
6.4 対策 6-12

6章 WIPS の概要（FIT は未サポート）

6.1 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。

6.2 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。

6.2.1 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（電力管理ビットが 1）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。

6.2.2 不正パケットの検出

WIPS は、フレームが表 6-1 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。

表 6-1 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。
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。

6.2.3 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。

6.2.4 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。

6.2.5 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。

6.2.6 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。

6.2.7 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。

6.2.8 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ムが満了すると、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。

6.2.9 禁止チャンネルの検出

許可チャンネルリストを設定し、禁止チャンネル検出を有効にすると、WIPS は許可チャンネルリストにないチャンネルを禁止チャンネルであると判断します。

6.2.10 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。

6.2.11 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。

6.2.12 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。

6.2.13 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、ホットスポットファイルを設定できます。

6.2.14 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。

6.2.15 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。

6.2.16 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。

6.2.17 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。WIPS は、ハニーポット AP 検出と MITM 攻撃検出のそれぞれを有効にする場合にのみ、MITM 攻撃を検出できます。

6.2.18 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。

6.2.19 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。

6.2.20 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。

6.2.21 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。

6.2.22 シグネチャにもとづいた攻撃の検出

WIPS は、シグネチャにもとづいた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。

6.3 装置の種別

6.3.1 AP の種別

表 6-2 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 6-2 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。	ー
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。

種別	説明	分類ルール
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。
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。

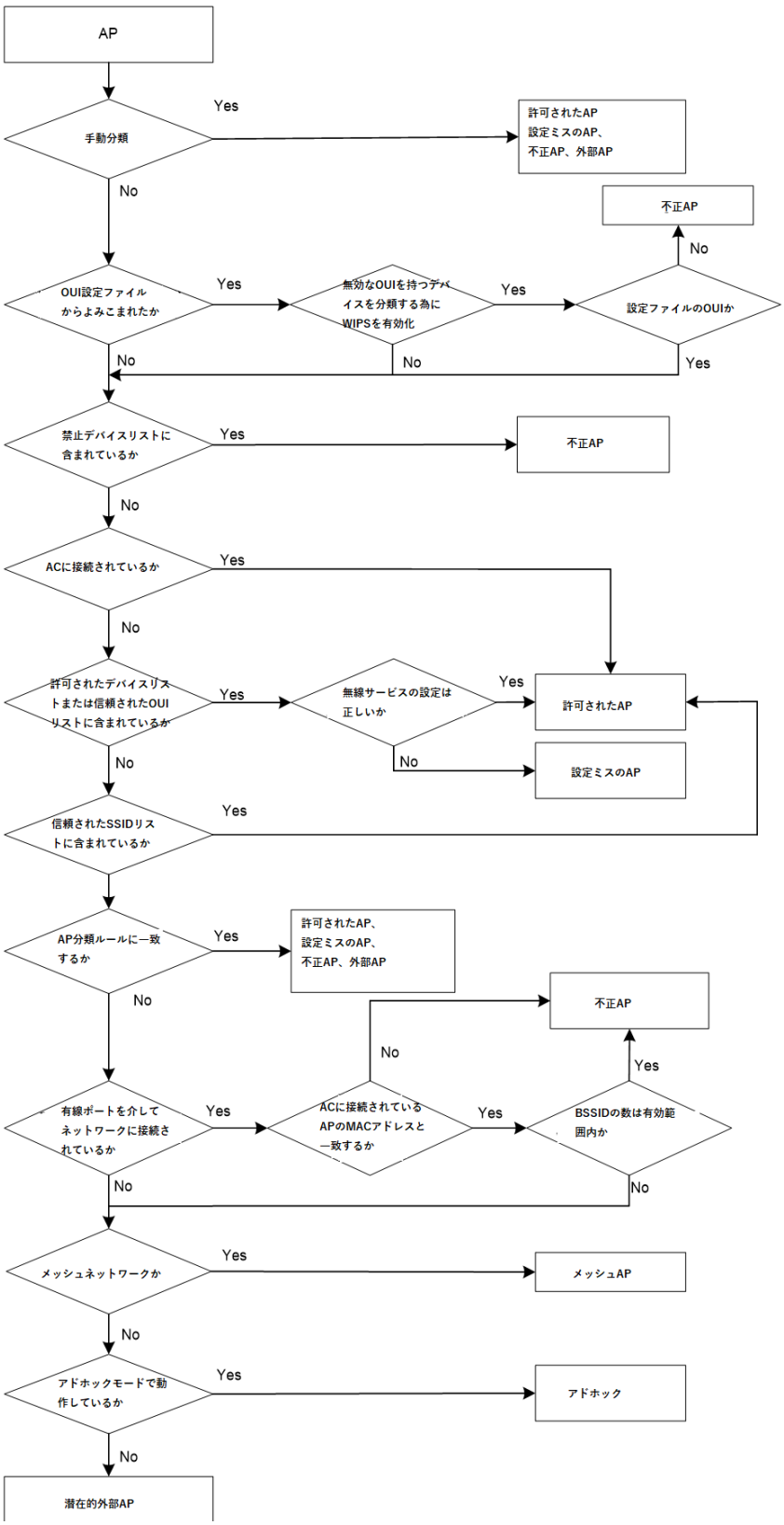


図 6-1 AP 分類フロー

6.3.2 クライアント種別

表 6-3 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 6-3 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。

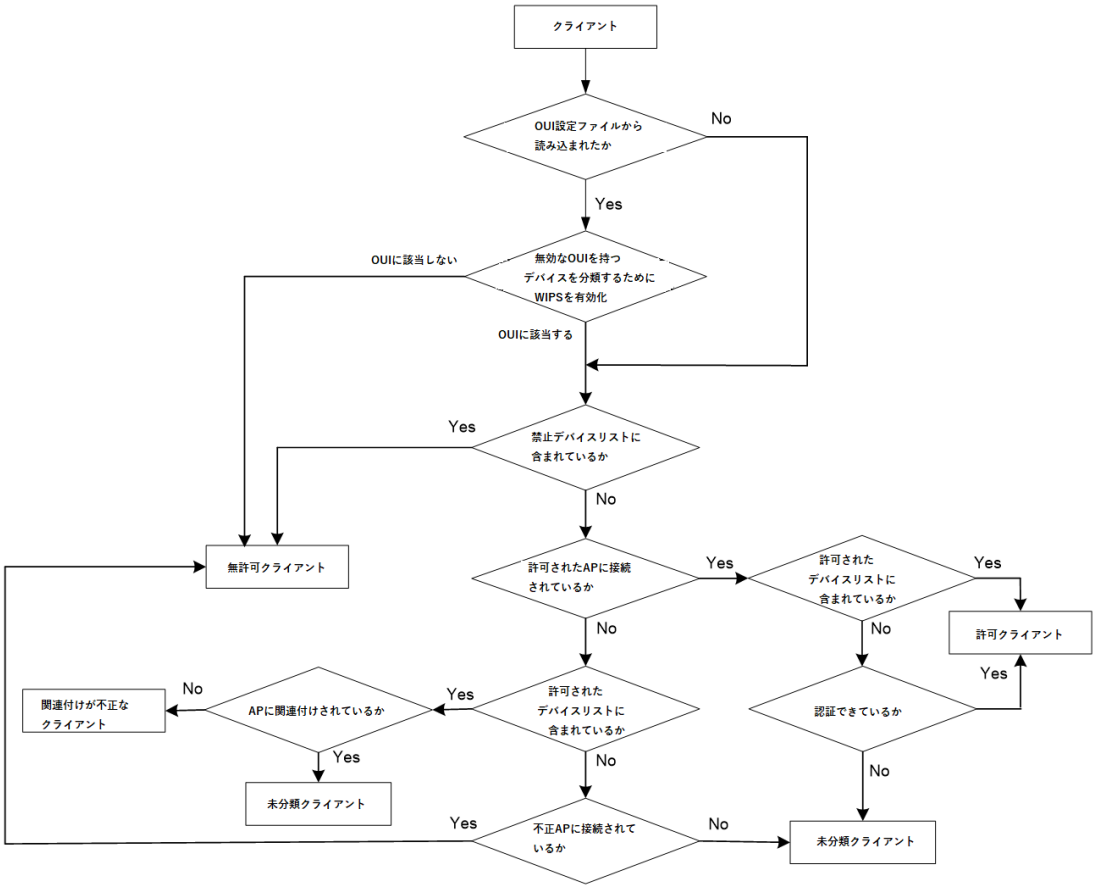


図 6-2 クライアントの分類フロー

6.4 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。

目次

このセクションのページは**2-x-x** です。

7 章 WIPS の設定（FIT は未サポート） 7-1
7.1 WIPS 設定作業リスト 7-1
7.2 WIPS 有効化 7-1
7.3 無線攻撃検出の設定 7-2
7.3.1 フラッド攻撃検出の設定 7-2
7.3.2 不正パケット検出の設定 7-3
7.3.3 装置エントリ攻撃検出の設定 7-4
7.3.4 その他の攻撃に対する検出設定 7-5
7.3.5 攻撃検知ポリシーの適用 7-6
7.3.6 シグネチャにもとづいた攻撃検出の設定 7-6
7.3.7 アラーム無視装置リストの設定 7-8
7.4 装置種別の設定 7-8
7.4.1 分類ポリシーの設定 7-8
7.4.2 分類ポリシーの適用 7-10
7.5 対策の設定 7-10
7.5.1 対策ポリシーの設定 7-10
7.5.2 対策ポリシーの適用 7-12
7.6 WIPS の表示と維持 7-12
7.7 WIPS 設定例 7-13
7.7.1 装置の分類の設定例 7-13
7.7.2 不正パケットとフラッド攻撃の検出例 7-15
7.7.3 シグネチャベースの攻撃検出設定例 7-19

7章 WIPS の設定（FIT は未サポート）

7.1 WIPS設定作業リスト

必須/オプション	作業リスト
必須	WIPSの有効化
オプション	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 • 攻撃検知ポリシーの適用 • シグネチャにもとづいた攻撃検出の設定 • アラーム無視装置リストの設定
オプション	装置種別の設定 • 分類ポリシーの設定 • 分類ポリシーの適用
オプション	対策の設定 • 対策ポリシーの設定 • 対策ポリシーの適用

7.2 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、無線インタフェースで 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。

無線インタフェースで WIPS を有効化する前に、AP を VSD に追加する必要があります。

以下に WIPS を有効に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

操作	コマンド	補足
2． AP を VSD に追加する	**wips virtual-security-domain** *vsd-name*	デフォルト：設定なし
3． VSD view から戻る	**Quit**	―
4． interface view に移行する	**interface wlan-radio** *interface-number*	―
5． WIPS を有効にする	**wips enable**	デフォルト：無効

7.3 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。

7.3.1 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**	―
2． WIPS view に移行する	**wips**	デフォルト：設定なし
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
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

操作	コマンド	補足
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

7.3.2 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
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

操作	コマンド	補足
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

7.3.3 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、クライアントエントリのしきい値は512です。
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ム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64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がエージングタイム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。

7.3.4 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
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

操作	コマンド	補足
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．WIPS view に戻る	**quit**	―
27．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。
28．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
29．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

7.3.5 攻撃検知ポリシーの適用

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 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． 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。

7.3.6 シグネチャにもとづいた攻撃検出の設定

I. 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**	―
2． WIPS view に移行する	**wips**	―

操作	コマンド	補足
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

II. シグネチャの適用

以下にシグネチャ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**	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、アラームしきい値は50です。

III. 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

操作	コマンド	補足
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

7.3.7 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、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

7.4 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。

7.4.1 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 分類ポリシーを使用して、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**	―
2． WIPS view に移行する	**wips**	―
3． OUI コンフィグファイルから OUI をインポートする	**import oui** *file-name*	デフォルト：設定なし
4． 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

操作	コマンド	補足
5. 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
6. 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
7. 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。
8. 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
9. 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
10. 指定 AP 種別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**	―
2. WIPS view に移行する	**wips**	―
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
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

III. 手動 AP 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． 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

7.4.2 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**	ー
2． WIPS view に移行する	**wips**	ー
3． VSD view に移行する	**virtual-security-domai**n *vsd-name*	デフォルト：設定なし
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。

7.5 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。

7.5.1 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 の潜在的許可 AP 対策を有効にする	**countermeasure potential-authorized-ap**	デフォルト：無効
8． 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

操作	コマンド	補足
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の悪意のある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*	デフォルト：無効
15. WIPSのドホック装置対策を有効にする	**countermeasure adhoc**	デフォルト：無効
16. WIPSのブロードキャスト認証解除攻撃を開始する装置対策を有効にする	**countermeasure attack deauth-broadcast**	デフォルト：無効
17. WIPSのブロードキャストアソシエーション攻撃を開始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のホットスポット攻撃を開始する装置対策を有効にする	**countermeasure attack hotspot-attack**	デフォルト：無効
20. WIPSの 40 MHz 帯域幅モードを無効にした装置対策を有効にする	**countermeasure attack ht-40-mhz-intolerance**	デフォルト：無効
21. WIPSの不正な形式の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攻撃を開始する装置対策を有効にする	**countermeasure attack man-in-the-middle**	デフォルト：無効
23. WIPSの Omerta 攻撃を開始する装置対策を有効にする	**countermeasure attack omerta**	デフォルト：無効
24. WIPSのパワーセーブ攻撃を開始する装置対策を有効にする	**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. WIPSの暗号化されていない許可された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. WIPSの 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

操作	コマンド	補足
28．WIPS の Windows ブリッジ攻撃を開始する装置対策を有効にする	**countermeasure attack windows-bridge**	デフォルト：無効
29．WIPS のべての攻撃者対策を有効にする	**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。

7.5.2 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
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。

7.6 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*]
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** | **mesh** | **misconfigured** | **potential-authorized** | **potential-external** | **potential-rosue** | **rogue** | **uncategorized**] | **client** [[**dissociative-client**] [**authorized** | **misassociation** | **unauthorized** | **uncategorized**]] | **mac-address** *mac-address*] [**verbose**]
検出した無線装置情報を表示する	**display client-proximity-sensor device** [**ap** | **client** | **mac-address** *mac-address*] [**verbose**]
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** }
検出した無線装置情報を削除する	**reset client-proximity-sensor device** { **ap** | **client** | **mac-address** *mac-address* | **all** }

7.7 WIPS設定例

7.7.1 装置の分類の設定例

I. ネットワーク要件

図 7-1 に示すように、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。

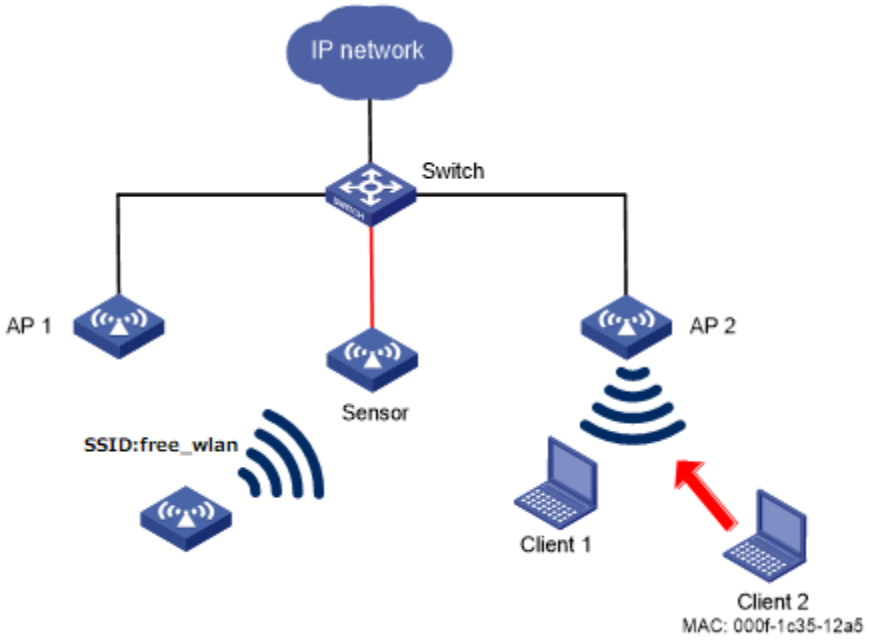


図 7-1 ネットワーク図

II. 設定手順

AP1 と AP2 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、オペレーションマニュアルのセクション 2 *WLAN "WLAN アクセスの設定"* を参照してください。

VSD vsd1 を作成します。

```
<Sensor> system-view
[Sensor] wips
[Sensor-wips] virtual-security-domain vsd1
[Sensor-wips-vsd-vsd1] quit
[Sensor-wips] quit
```

WIPS を有効にします。

```
[Sensor] interface WLAN-Radio 1/0/1
```

```
[Sensor-WLAN-Radio1/0/1] wips enable
[Sensor-WLAN-Radio1/0/1] quit
[Sensor] interface WLAN-Radio 1/0/2
[Sensor-WLAN-Radio1/0/2] wips enable
[Sensor-WLAN-Radio1/0/2] quit
[Sensor] interface WLAN-Radio 1/0/3
[Sensor-WLAN-Radio1/0/3] wips enable
[Sensor-WLAN-Radio1/0/3] quit
```

VSD vsd1 に AP Sensor を追加します。

```
[Sensor] wips virtual-security-domain vsd1
```

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。信頼できる SSID リストに SSID abc を追加します。

```
[Sensor] wips
[Sensor-wips] classification policy class1
[Sensor-wips-cls-class1] block mac-address 000f-1c35-12a5
[Sensor-wips-cls-class1] trust ssid abc
[Sensor-wips-cls-class1] quit
```

分類ポリシーclass1 を VSD vsd1 に適用します。

```
[Sensor-wips] virtual-security-domain vsd1
[Sensor-wips-vsd-vsd1] apply classification policy class1
[Sensor-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。

```
[Sensor-wips] countermeasure policy protect
[Sensor-wips-cms-protect] countermeasure unauthorized-client
[Sensor-wips-cms-protect] countermeasure potential-external-ap
[Sensor-wips-cms-protect] quit
```

対策ポリシーprotect を VSD vsd1 に適用します。

```
[Sensor-wips] virtual-security-domain vsd1
[Sensor-wips-vsd-vsd1] apply countermeasure policy protect
[Sensor-wips-vsd-vsd1] quit
[Sensor-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。

```
[Sensor] 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。

```
[Sensor] display wips virtual-security-domain vsd1 countermeasure record
Total 2 times countermeasure, current 2 countermeasure record in
virtual-security-domain vsd1
Reason: Attack; Ass - associated; Black - blacklist;
        Class - classification; Manu - manual;

MAC address    Type   Reason   Countermeasure AP      Radio ID   Time
000f-e200-5829 AP     Class    Sensor              1         2014-06-03/09:30:25
000f-e228-2528 AP     Class    Sensor              1         2014-06-03/19:31:56
000f-e223-1616 AP     Class    Sensor              1         2014-06-03/10:30:36
000f-1c35-12a5 Client Class    Sensor              1         2014-06-03/09:13:26
000f-e201-0102 Client Class    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。

7.7.2 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 7-2 に示すように、AP をセンサとして設定します。センサを VSD vsd1 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。

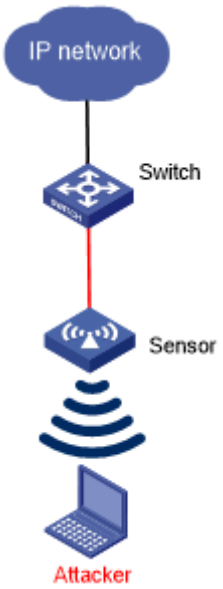


図 7-2 ネットワーク図

II. 設定手順

センサ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、オペレーションマニュアルのセクション 2 *WLAN "WLAN アクセスの設定"* を参照してください。

VSD vsd1 を作成します。

```
<Sensor> system-view
[Sensor] wips
[Sensor-wips] virtual-security-domain vsd1
[Sensor-wips-vsd-vsd1] quit
[Sensor-wips] quit
```

WIPS を有効にします。

```
[Sensor] interface WLAN-Radio 1/0/1
[Sensor-WLAN-Radio1/0/1] wips enable
[Sensor-WLAN-Radio1/0/1] quit
[Sensor] interface WLAN-Radio 1/0/2
[Sensor-WLAN-Radio1/0/2] wips enable
[Sensor-WLAN-Radio1/0/2] quit
[Sensor] interface WLAN-Radio 1/0/3
[Sensor-WLAN-Radio1/0/3] wips enable
[Sensor-WLAN-Radio1/0/3] quit
```

VSD csd1 にセンサを追加します。

```
[Sensor] wips virtual-security-domain vsd1
```

攻撃検出ポリシーdtc1 を作成します。

```
[Sensor] wips
[Sensor-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。

```
[Sensor-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。

```
[Sensor-wips-dtc-dtc1] flood beacon interval 100 quiet 50 threshold 200
[Sensor-wips-dtc-dtc1] quit
```

攻撃検出ポリシーdtc1 を VSD VSD_1 に適用します。

```
[Sensor-wips] virtual-security-domain vsd1
[Sensor-wips-vsd-vsd1] apply detect policy dtc1
[Sensor-wips-vsd-vsd1] quit
[Sensor-wips] quit
```

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。

```
<Sensor> 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。

<Sensor> 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
```

7.7.3 シグネチャベースの攻撃検出設定例

I. ネットワーク要件

図 7-3 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。

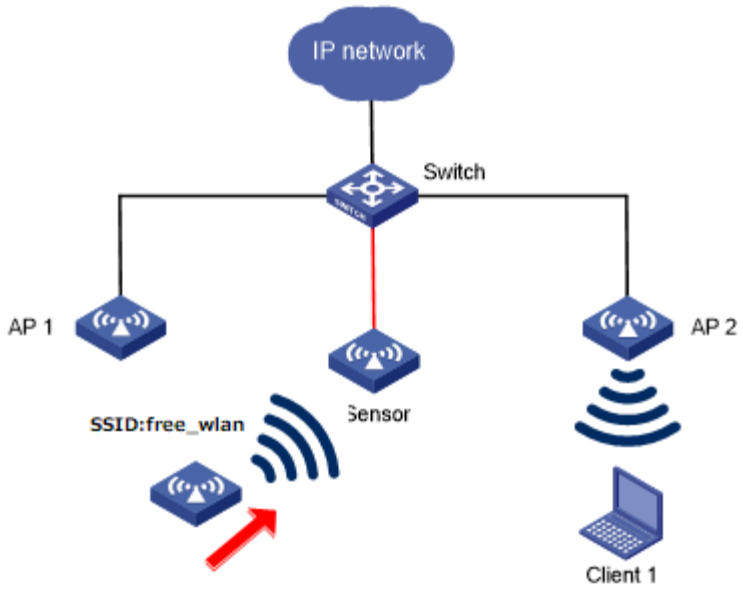


図 7-3 ネットワーク図

II. 設定手順

AP1 と AP2 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、オペレーションマニュアルのセクション 2 *WLAN "WLAN アクセスの設定"* を参照してください。

VSD vsd1 を作成します。

```
<Sensor> system-view
[Sensor] wips
[Sensor-wips] virtual-security-domain vsd1
[Sensor-wips-vsd-vsd1] quit
[Sensor-wips] quit
```

WIPS を有効にします。

```
[Sensor] interface WLAN-Radio 1/0/1
[Sensor-WLAN-Radio1/0/1] wips enable
[Sensor-WLAN-Radio1/0/1] quit
[Sensor] interface WLAN-Radio 1/0/2
[Sensor-WLAN-Radio1/0/2] wips enable
[Sensor-WLAN-Radio1/0/2] quit
[Sensor] interface WLAN-Radio 1/0/3
[Sensor-WLAN-Radio1/0/3] wips enable
[Sensor-WLAN-Radio1/0/3] quit
```

VSD vsd1 にセンサを追加します。

```
[Sensor] wips virtual-security-domain vsd1
```

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。

```
[Sensor] wips
[Sensor-wips] signature rule 1
[Sensor-wips-sig-rule-1] frame-type management frame-subtype beacon
[Sensor-wips-sig-rule-1] ssid not equal abc
[Sensor-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。

```
[Sensor-wips] signature policy sig1
[Sensor-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。

```
[Sensor-wips-sig-sig1] detect signature interval 5 quiet 60 threshold 60
[Sensor-wips-sig-sig1] quit
```

シグネチャポリシーsig1 を VSD vsd1 に適用します。

```
[Sensor] wips
[Sensor-wips] virtual-security-domain vsd1
[Sensor-wips-vsd-vsd1] apply signature policy sig1
[Sensor-wips-vsd-vsd1] quit
```

III. 設定の確認

SSID free_wlan の無線サービスを検出したときに、センサがアラームを生成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。

```
[Sensor] 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
```

目次

このセクションのページは**2-x-x** です。

8 章 WLAN QoS の設定（FIT は未サポート） 8-1
8.1 概要 8-1
8.1.1 WMM プロトコル 8-1
8.1.2 SVP 8-3
8.1.3 帯域保証 8-3
8.1.4 クライアント帯域制限 8-3
8.1.5 プロトコルと標準 8-3
8.2 設定作業リスト 8-3
8.3 WMM の設定 8-4
8.3.1 WMM の有効化 8-4
8.3.2 EDCA パラメータの設定 8-4
8.3.3 クライアントの EDCA パラメータ設定（AC-BE または AC-BK） 8-4
8.3.4 クライアントの EDCA パラメータ設定（AC-VI または AC-VO） 8-5
8.3.5 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ポートの設定 8-6
8.4 帯域保証の設定 8-6
8.5 クライアント帯域制限 8-7
8.5.1 サービステンプレートベースの帯域制限設定 8-7
8.5.2 クライアントタイプベースの帯域制限設定 8-7
8.6 U-APSD の設定 8-7
8.6.1 制限とガイドライン 8-7
8.6.2 U-APSD の設定 8-8
8.7 Air Time Fairness の設定 8-9
8.8 WMM の表示および維持 8-9
8.9 WLAN QoS の設定例 8-9
8.9.1 基本的な WMM の設定例 8-9
8.9.2 トラフィック差別化の設定例 8-10
8.9.3 帯域保証の設定例 8-12
8.9.4 サービステンプレートベースのクライアント帯域制限の設定例 8-13
8.9.5 Air Time Fairness の設定例 8-14

8章 WLAN QoS の設定（FIT は未サポート）

この章では、WLAN QoS の設定方法について説明します。

8.1 概要

802.11 ネットワークは、コンテンションベースのワイヤレス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、IEEE は 802.11 ベースの WLAN 向けに 802.11e を開発しました。

IEEE 802.11e は標準化されていますが、Wi-Fi Alliance は異なるベンダーの QoS 供給装置を相互運用させるために Wi-Fi マルチメディア（WMM）標準を定めました。WMM を使用することで、WLAN で QoS サービスを提供でき、オーディオおよびビデオアプリケーションのパフォーマンスが向上します。

8.1.1 WMM プロトコル

I. WMM について

802.11 の Distributed Coordination Function（DCF）では、AP とクライアントが carrier sense multiple access with collision avoidance （CSMA / CA）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、データを転送するためのチャネルを保持する前に、そのチャネルの使用状況を確認します。指定されたチャネルの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。最初にバックオフが終了したデバイスがチャネルを取得します。802.11 では、すべてのデバイスが同じアイドル時間とコンテンションウィンドウを持ちます。そのため、チャネルが競合する場合、すべての通信が平等に扱われることになります。

WMM では QoS サービスを提供するために、データトラフィックを異なる優先度を持つ 4 つの AC に分割します。優先度の高い AC のトラフィックは、チャネルを使用できる可能性が高くなります。

II. 用語

- **Enhanced distributed channel access**－EDCA は、優先度が高いパケットを優先的に送信しより多くの帯域幅を割り当てる、WMM によって定義されたチャネル競合メカニズムです。
- **Access category**－WMM は、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 4 つの AC を定義します。4 つの AC の優先度は降順です。
- **Connect Admission Control**－CAC は、優先度の高い AC（AC-VO および AC-VI）を使用できるクライアントの数を制限して、これらのクライアントに十分な帯域幅があることを確認します。
- **Unscheduled automatic power save delivery**－U-APSD は、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節電方法です。

III. EDCA パラメータ

- **Arbitration inter-frame spacing number**－802.11 ベースの WLAN は、各クライアントで同じアイドル時間（DIFS）を持ちますが、WMM では AC ごとに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増加します。
- **Exponent form of CWmin/Exponent form of Cwmax**－ECWmin と ECWmax の 2 つの値が増加するにつれて、バックオフスロットを増加します。
- **Transmission opportunity limit**－TXOP 制限は、競合が発生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 つのパケットのみ送信することができます。

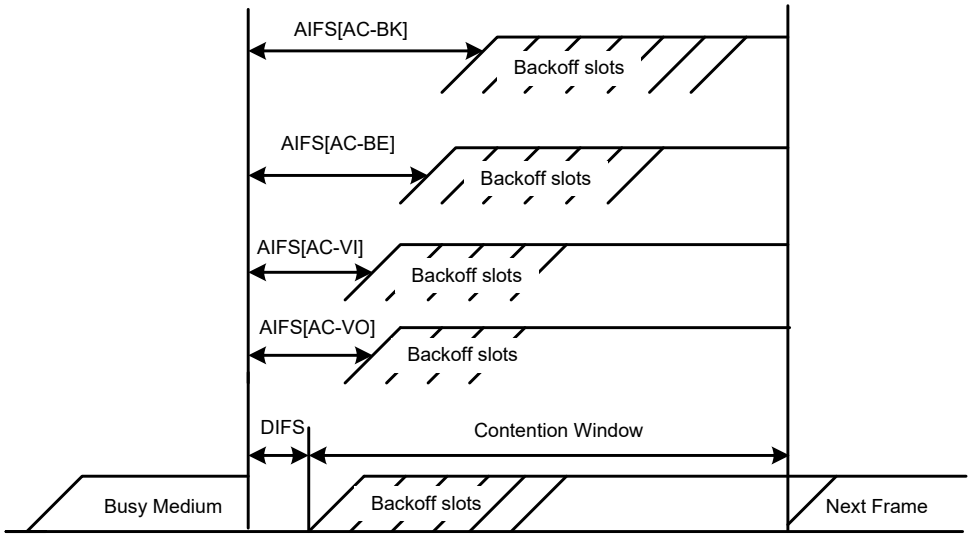


図 8-1 EDCA パラメータ

IV. U-APSD 節電方法

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受信することができます。U-APSD は 802.11 APSD 節電方法を改善します。

U-APSD は、WMM を有効にすると自動的に有効になります。

undo u-apsd enable コマンドにて U-APSD を無効にできます。

V. ACK ポリシー

WMM では、次の ACK ポリシーが定義されています。

- Normal ACK－受信者は、受信した各ユニキャストパケットの確認応答を行います。
- No ACK－受信者は、無線パケット通信中に受信パケットの確認応答を行いません。このポリシーは、通信品質が高く干渉が弱い環境での伝送効率を向上させます。通信品質が悪化した場合、パケットロス率が増加する可能性があります。802.11n クライアントから送信された 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

SpectraLink Voice Priority（SVP）は、SpectraLink によって開発され、音声トラフィックに QoS サービスを提供します。

8.1.3 帯域保証

この機能は、以下の機能を提供します。

- ネットワークが輻輳していないときは、すべての BSS からのトラフィックが自由に通過できるようにします。
- ネットワークが輻輳しているときは、各 BSS が保証された帯域幅を確保できるようにします。

この機能により、帯域幅の効率化や、WLAN サービス間で帯域幅を公正に使用することができます。たとえば、SSID1、SSID2、SSID3 には、合計帯域幅の 25%、25%、50%を割り当てます。ネットワークが輻輳していない場合、SSID1 は保証された帯域幅に加えて、未使用な帯域幅も使用することができます。ネットワークが輻輳している場合、SSID1 は帯域幅の 25%が保証されます。

この機能は、AP からクライアントへのトラフィックにのみ適用されます。

8.1.4 クライアント帯域制限

この機能は、1 つのクライアントによる帯域幅の積極的な使用を防ぎ、同じ AP に関連づけられているクライアント間で帯域幅を公正に使用することを可能にします。

クライアント帯域制限には、次のいずれかのモードを設定することができます。

- **Dynamic mode**－すべてのクライアントで共有する総帯域幅を設定します。各クライアントの帯域制限は、総帯域幅をオンラインクライアントの数で割ったものとなります。たとえば、総帯域幅が 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。
- **Static mode**－各クライアントで使用できる帯域幅を設定します。設定した帯域幅にクライアントの数を掛けた値が AP によって提供することのできる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使用することができない可能性があります。

8.1.5 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 設定作業リスト

作業リスト
必要に応じて次の作業を選択します。 • WMMの設定 • 帯域保証の設定 • クライアント帯域制限の設定

8.3 WMMの設定

8.3.1 WMM の有効化

802.11n プロトコルでは、すべての 802.11n クライアントが WLAN QoS をサポートしている必要があります。802.11n クライアントが関連する AP と通信するには、無線が 802.11an または 802.11gn モードで動作しているときに WMM を有効にします。

I. WMM の有効化

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． radio interface view に移行する	**interface wlan-radio** *interface-number*	—
3． WMM を有効にする	**wmm enable**	デフォルト：有効

8.3.2 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． radio interface view に移行する	**interface wlan-radio** *interface-number*	—
3． WMM を有効にする	**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* } *	デフォルト：EDCAパラメータのデフォルトを表 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	ECW min	ECW max	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

8.3.3 クライアントの EDCA パラメータ設定（AC-BE または AC-BK）

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． radio intereface view に移行する	**interface wlan-radio** *interface-number*	—
3． クライアントの AC-BE キューまたは AC-BK キューの EDCA パラメータを設定する	**edca client** { **ac-be** | **ac-bk** } { **aifsn** *aifsn-value* | **ecw ecwmin ecwmin-value ecwmax** *ecwmax-value* | **txoplimit** *txoplimit-value* } *	デフォルト：EDCAパラメータのデフォルトを表 8-2に示します。

表 8-2 クライアントの AC-BE キューまたは AC-BK キューの EDCA パラメータのデフォルト値

AC	AIFSN	ECW min	ECW max	TXOP Limit
AC-BK	7	4	10	0
AC-BE	3	4	10	0

8.3.4 クライアントの EDCA パラメータ設定（AC-VI または AC-VO）

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. radio interface view に移行する	**interface wlan-radio** *interface-number*	—
3. クライアントの AC-VI キューまたは AC-VO キューの EDCA パラメータを設定	**edca client** { **ac-vi** | **ac-vo** } { **aifsn** *aifsn-value* | **cac** { **disable** | **enable** } | **ecw ecwmin** *ecwmin-value* **ecwmax** *ecwmax-value* | **txoplimit** *txoplimit-value* } *	デフォルト：EDCAパラメータのデフォルトを表 8-3に示します。

表 8-3 クライアントの AC-BI キューまたは AC-VO キューの EDCA パラメータのデフォルト値

AC	AIFSN	ECW min	ECW max	TXOP Limit
AC-VI	2	3	4	94
AC-VO	2	2	3	47

8.3.5 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ポートの設定

この機能は、アップリンクパケットにのみ適用されます。

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ポート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. service template view に移行する	**wlan service-template** *service-template-name*	—
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 { dot11e | dscp }**	デフォルト：有効
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

8.4 帯域保証の設定

メモ：

wlan max-bandwidth コマンドの **dot11be**、**dot11abe**、**dot11gbe**、**dot11eax** のパラメータは、ソフトウェアバージョン 7.5.105 を含む以降のソフトウェアからサポートしています。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. 指定した無線タイプの最大帯域幅を設定する	**wlan max-bandwidth** { **dot11a** | **dot11ac** | **dot11ax** | **dot11abe** | **dot11eax** | **dot11be** | **dot11an** | **dot11b** | **dot11g** | **dot11gax** | **dot11gbe** | **dot11gn** } *bandwidth*	デフォルト：以下の設定が適用されています。 ● dot11be：1500000Kbps ● dot11abe：800000Kbps ● dot11gbe：300000Kbps ● dot11eax：700000Kbps ● dot11a、dot11g：30000Kbps ● dot11an、dot11gn、dot11gax：250000Kbps ● dot11ac、dot11ax：500000Kbps ● dot11b：7000Kbps
3. radio interface view に移行する	**interface wlan-radio** *interface-number*	—
4. 帯域保証を設定する	**bandwidth-guarantee** { **disable** | **enable** }	デフォルト：無効
5. 指定したサービステンプレートの帯域保証幅の割合を設定する	**bandwidth-guarantee service-template** *service-template-name* **percent** *percent*	デフォルト：設定なし

8.5 クライアント帯域制限

サービステンプレートベース、クライアントタイプベースの方式でクライアント帯域制限を設定できます。帯域制限モードでは、クライアント帯域制限の動的モードまたは静的モードを構成できます。

複数の方式とモードが設定されている場合、すべての設定が有効になります。 クライアント帯域は、すべてのクライアント帯域制限設定の中で最小値に制限されます。

8.5.1 サービステンプレートベースの帯域制限設定

本設定は、同じサービステンプレートに関連づけられているすべてのクライアントに影響を与えます。

サービステンプレートベースのクライアント帯域制限を設定するには、次の手順を実行します。

操作	コマンド	補足
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ベースのクライアント帯域制限を有効化する	**client-rate-limit enable**	デフォルト：無効
4. サービステンプレートベースのクライアント帯域制限値を設定する	**client-rate-limit** { **inbound** | **outbound** } **mode** { **dynamic** | **static** } **cir** *cir*	デフォルト：設定なし

8.5.2 クライアントタイプベースの帯域制限設定

本設定は、指定されたプロトコルのすべてのクライアントに影響を与えます。

クライアントタイプベースのクライアント帯域制限を設定するには、次の手順を実行します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. クライアントタイプベースのクライアント帯域制限値を設定する	**wlan client-rate-limit** { **dot11a** | **dot11ac** | **dot11ax** | **dot11an** | **dot11b** | **dot11g** | **dot11gac** | **dot11gn** } { **inbound** | **outbound** } **cir** *cir* [**cbs** *cbs*]	デフォルト：設定なし

8.6 U-APSDの設定

8.6.1 制限とガイドライン

U-APSD は、WMM を有効にすると自動的に有効になります。

クライアントが U-APSD をサポートしている場合、この機能を有効にして節電機能を向上させることを推奨します。

この機能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てください。

8.6.2 U-APSD 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． U-APSD を有効にする	**u-apsd enable**	デフォルト：有効 U-APSDを無効にする場合、**undo u-apsd enable**コマンドを実行します。

8.7 Air Time Fairnessの設定

Air Time Fairness は、すべてのクライアントが AP のカバレッジエリア内の通信時間に均等にアクセスできるようにします。この機能を使用すると、高速クライアントがワイヤレスリソースを使用する機会が増えます。これにより、ネットワーク全体の転送効率が向上します。

この機能を有効にすると、低速クライアントの転送効率が低下する可能性があります。

この機能を設定する場合は、アクセスクライアントの数と高速クライアントの転送効率を考慮してください。

この機能でネットワークの転送効率が向上するのは、AP からクライアント方向の通信のみです。

Air Time Fairness 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
1． system view に移行する	**system-view**	—
2． radio interface view へ移行する	**interface wlan-radio** *interface-number*	—
3． Air Time Fairness を設定する	**atf** { **disable** | **enable** }	デフォルト：無効

8.8 WMMの表示および維持

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
無線のWMM統計情報を表示する	**display wlan wmm radio** { **all** | **ap** *ap-name* }
クライアントのWMM統計情報を表示する	**display wlan wmm client** { **all** | **ap** *ap-name* | **mac-address** *mac-address* }
無線のWMM統計情報をリセットする	**reset wlan wmm radio** { **all** | **ap** *ap-name* }
クライアントのWMM統計情報をリセットする	**reset wlan wmm client** { **all** | **ap** *ap-name* | **mac-address** *mac-address* }

8.9 WLAN QoSの設定例

8.9.1 基本的な WMM の設定例

I. ネットワーク要件

図 8-2 に示すように、fat AP 上で WMM を有効にし、fat AP とクライアントがトラフィックに優先度を付けるようにします。

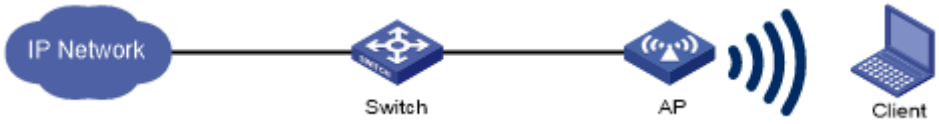


図 8-2 ネットワーク図

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します。

```
<FAT AP> system-view
[FAT AP] wlan service-template market
[FAT AP-wlan-st-market] ssid market
[FAT AP-wlan-st-market] service-template enable
[FAT AP-wlan-st-market] quit
```

WMM を有効にし、サービステンプレート market を WLAN-Radio 1/0/1 に紐づけます。

```
[FAT AP] interface wlan-radio 1/0/1
[FAT AP-WLAN-Radio1/0/1] undo shutdown
[FAT AP-WLAN-Radio1/0/1] service-template market
[FAT AP-WLAN-Radio1/0/1] wmm enable
[FAT AP-WLAN-Radio1/0/1] quit
```

III. 設定の確認

無線の WMM 統計情報を表示します。

```
[FAT AP] display wlan wmm radio
 AP ID : 1   AP Name : fatap

 Radio : 1
 Client EDCA updates : 0
 QoS mode    : WMM
 WMM status : Enabled
 Radio max AIFSN         : 0          Radio max ECWmin : 0
 Radio max TXOPLimit     : 0          Radio max ECWmax : 0
```

8.9.2 トラフィック差別化の設定例

I. ネットワーク要件

図 8-3 に示すように、クライアントから AC-VO キューに 802.11 パケットを追加するために、fat AP 上でプライオリティマッピングを設定します。

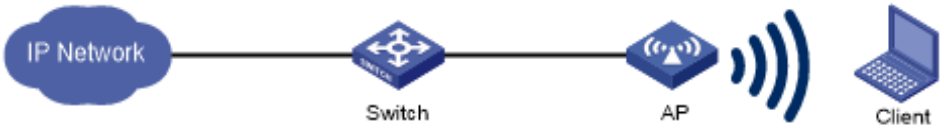


図 8-3 ネットワーク図

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します。

```
<FAT AP> system-view
[FAT AP] wlan service-template market
[FAT AP-wlan-st-market] ssid market
[FAT AP-wlan-st-market] service-template enable
[FAT AP-wlan-st-market] quit
```

#802.11 パケットの 802.11e プライオリティを 7 に設定します。

```
[FAT AP-wlan-st-market] qos priority 7
[FAT AP-wlan-st-market] quit
```

#無線 1 にサービステンプレート market を WLAN-Radio 1/0/1 に紐づけます。

```
[FAT AP] interface wlan-radio 1/0/1
[FAT AP-WLAN-Radio1/0/1] undo shutdown
[FAT AP-WLAN-Radio1/0/1] service-template market
```

#WMM を有効にします。

```
[FAT AP-WLAN-Radio1/0/1] wmm enable
[FAT AP-WLAN-Radio1/0/1] quit
```

III. 設定の確認

#クライアントからのパケットが AC-VO キューに追加されていることを確認します。

```
[FAT AP] display wlan statistics client
 MAC address                  : 0015-005e-97cc
 AP name                      : 7848-59f3-fd40
 Radio ID                     : 1
 SSID                         : market
 BSSID                        : 7848-59f3-fd40
 RSSI                         : 27
 Sent frames:
   Back ground                : 0/0 (frames/bytes)
   Best effort                : 0/0 (frames/bytes)
   Video                      : 0/0 (frames/bytes)
   Voice                      : 14/1092 (frames/bytes)
 Received frames:
   Back ground                : 0/0 (frames/bytes)
   Best effort                : 66/8177 (frames/bytes)
   Video                      : 0/0 (frames/bytes)
   Voice                      : 0/0 (frames/bytes)
 Discarded frames:
```

```
    Back ground                 : 0/0 (frames/bytes)
    Best effort                 : 0/0 (frames/bytes)
    Video                       : 0/0 (frames/bytes)
    Voice                       : 0/0 (frames/bytes)
```

8.9.3 帯域保証の設定例

I. ネットワーク要件

図 8-4 に示すように、クライアント 1、2、3 は、それぞれ SSIDresearch、office、entertain を通じてネットワークにアクセスします。

ネットワークが正常に動作するためには、SSIDoffice に帯域幅の 20%、researck に 80% を保証し、entertain の帯域幅は保証を行わないようにする必要があります。

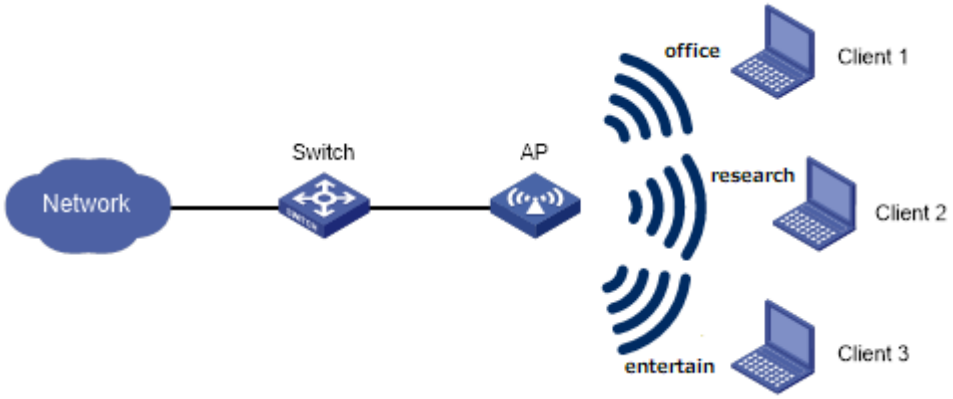


図 8-4 ネットワーク図

II. 設定手順

office という名前のサービステンプレートを作成し、SSID を office に設定し、サービステンプレートを有効にします。

```
<FAT AP> system-view
[FAT AP] wlan service-template office
[FAT AP-wlan-st-office] ssid office
[FAT AP-wlan-st-office] service-template enable
[FAT AP-wlan-st-office] quit
```

research という名前のサービステンプレートを作成し、SSID を research に設定し、サービステンプレートを有効にします。

```
[FAT AP] wlan service-template research
[FAT AP-wlan-st-research] ssid research
[FAT AP-wlan-st-research] service-template enable
[FAT AP-wlan-st-research] quit
```

entertain という名前のサービステンプレートを作成し、SSID を entertain に設定し、サービステンプレートを有効にします。

```
[FAT AP] wlan service-template entertain
```

```
[FAT AP-wlan-st-entertain] ssid entertain
[FAT AP-wlan-st-entertain] service-template enable
[FAT AP-wlan-st-entertain] quit
```

802.11ac 無線の場合、最大帯域幅を 10000 Kbps に設定します。

```
[FAT AP] wlan max-bandwidth dot11ac 10000
```

サービステンプレートの office、research、entertain を WLAN-Radio1/0/1 に紐づけます。

```
[FAT AP] interface wlan-radio 1/0/1
[FAT AP-WLAN-Radio1/0/1] undo shutdown
[FAT AP-WLAN-Radio1/0/1] service-template office
[FAT AP-WLAN-Radio1/0/1] service-template research
[FAT AP-WLAN-Radio1/0/1] service-template entertain
```

帯域保証を有効にします。

```
[FAT AP-WLAN-Radio1/0/1] bandwidth-guarantee enable
```

帯域保証する割合をサービステンプレート office は 20%、research は 80%に設定します。

```
[FAT AP-WLAN-Radio1/0/1] bandwidth-guarantee service-template office percent 20
[FAT AP-WLAN-Radio1/0/1] bandwidth-guarantee service-template research percent 80
[FAT AP-WLAN-Radio1/0/1] return
```

III. 設定の確認

#総トラフィックレートが 10000 Kbps 未満の場合、AP から任意のクライアントへのトラフィックのレートが制限されていないことを確認します。

#次の項目を確認するために、AP からクライアント 1 へ 2000Kbps 以上、クライアント 2 に 8000 Kbps 以上の速度でトラフィックを送信します。

- AP は 2000 Kbps でクライアント 1 にトラフィックを送信します。
- AP は 8000 Kbps でクライアント 2 にトラフィックを送信します。
- AP からクライアント 3 へのトラフィックの送信は制限されています。

8.9.4 サービステンプレートベースのクライアント帯域制限の設定例

I. ネットワーク要件

図 8-5 に示すように、fat AP で次の作業を実行します。

- static mode のクライアント帯域制限を設定して、着信クライアントトラフィックの帯域を制限します。
- dynamic mode のクライアント帯域制限を設定して、発信クライアントトラフィックの帯域を制限します。

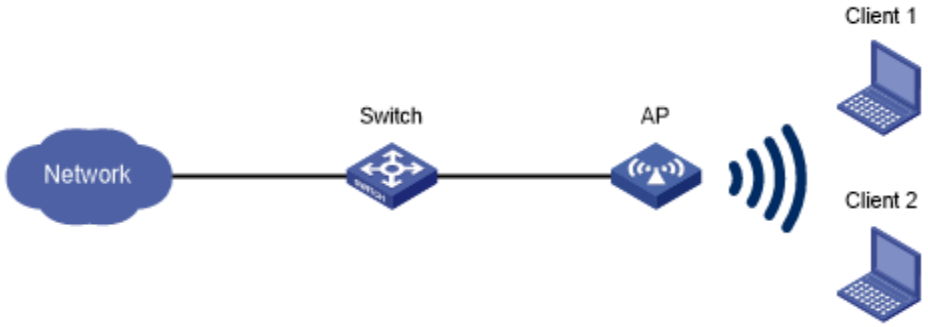


図 8-5 ネットワーク図

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、SSID を service に設定します。

```
<FAT AP> system-view
[FAT AP] wlan service-template service
[FAT AP-wlan-st-service] ssid service
```

サービステンプレート service のクライアント帯域制限を有効にし、次のようにクライアント帯域制限を構成します。

- static mode で、受信トラフィックの帯域を 8000 Kbps に制限します。
- dynamic mode で、送信トラフィックの帯域を 8000Kbps に制限します。

```
[FAT AP-wlan-st-service] client-rate-limit enable
[FAT AP-wlan-st-service] client-rate-limit inbound mode static cir 8000
[FAT AP-wlan-st-service] client-rate-limit outbound mode dynamic cir 8000
[FAT AP-wlan-st-service] service-template enable
[FAT AP-wlan-st-service] quit
```

WLAN-Radio1/0/1 にサービステンプレート service を紐づけます。

```
[FAT AP] interface wlan-radio 1/0/1
[FAT AP-WLAN-Radio1/0/1] undo shutdown
[FAT AP-WLAN-Radio1/0/1] service-template service
[FAT AP-WLAN-Radio1/0/1] return
```

8.9.5 Air Time Fairness の設定例

I. ネットワーク要件

図 8-6 に示すように、fat AP で次の作業を実行します。

- Client 1 は 802.11n に対応した低速クライアントです。
- Client 2 は 802.11ax に対応した高速クライアントです。Air Time Fairness を有効にして、Client 1 による通信速度の低下の影響を抑えます

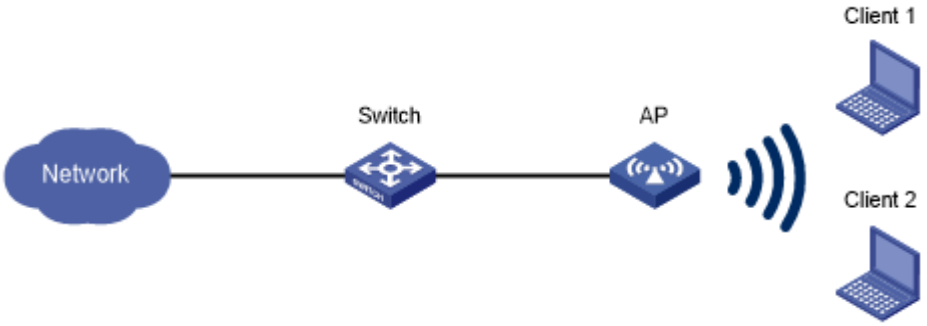


図 8-6 ネットワーク図

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、SSID を service に設定します。

```
<FAT AP> system-view
[FAT AP] wlan service-template service
[FAT AP-wlan-st-service] ssid service
[FAT AP-wlan-st-service] service-template enable
[FAT AP-wlan-st-service] quit
```

WLAN-Radio1/0/2 にサービステンプレート service を紐づけます。

```
[FAT AP] interface wlan-radio 1/0/2
[FAT AP-WLAN-Radio1/0/2] undo shutdown
[FAT AP-WLAN-Radio1/0/2] service-template service
```

Air Time Fairness を有効にします

```
[FAT AP-WLAN-Radio1/0/2] atf enable
```

目次

このセクションのページは**2-x-x** です。

9章 WLANローミングの設定（FITは未サポート） 9-1
9.1 概要 9-1
9.2 特殊な用語 9-1
9.3 WLANローミングメカニズム 9-1
9.3.1 FAT AP間ローミング 9-1
9.3.2 FAT AP間ローミングの設定 9-3
9.3.3 WLANローミング用SNMP通知機能の有効化 9-3
9.4 802.11rの設定 9-4
9.4.1 802.11r 動作メカニズム 9-4
9.4.2 プロトコルと標準 9-4
9.4.3 802.11rの設定 9-5
9.5 802.11vの設定 9-5
9.5.1 BTM (BSS移行管理) 9-6
9.5.2 BTMの設定 9-6
9.5.3 BTMアソシエーション解除の設定 9-7
9.5.4 クライアントanti-stickyの設定 9-7
9.6 802.11kの設定 9-8
9.7 WLANローミング設定例 9-8
9.7.1 FAT AP間ローミング 9-8
9.8 802.11r設定例 9-12
9.8.1 Over-the-air FTとPSK認証設定例 9-12
9.8.2 Over-the-air FTと802.1X認証設定例 9-17
9.9 802.11v設定例 9-23
9.9.1 BTMとPSK認証設定 9-23
9.9.2 BTMと802.1X認証設定 9-28

9章 WLAN ローミングの設定（FIT は未サポート）

9.1 概要

WLAN ローミングは、クライアントが、同一モビリティグループの FAT AP 間で、IP アドレスと認可情報を保持してシームレスに移動することを可能にします。

QX シリーズの AP は、RSN + 802.1X を使用した再認証不要な AP 間の移動により、高速なローミングを提供します。

9.2 特殊な用語

- IADTP（Inter Access Device Tunneling Protocol）

IADTP は、AP 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 AP 間では、IADTP 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 AP

Home AP は、クライアントが最初に接続する AP です。

- Foreign AP

Foreign AP は、クライアントがローミング後に接続する AP 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 を含むグループです。

IADTP を使用するためには、モビリティグループを設定する必要があります。

9.3 WLANローミングメカニズム

クライアントは同じモビリティグループの AP 間で移動することができます。

9.3.1 FAT AP 間ローミング

FAT AP 間ローミングは、同じモビリティグループの AP の間でクライアントが移動することを可能にします。

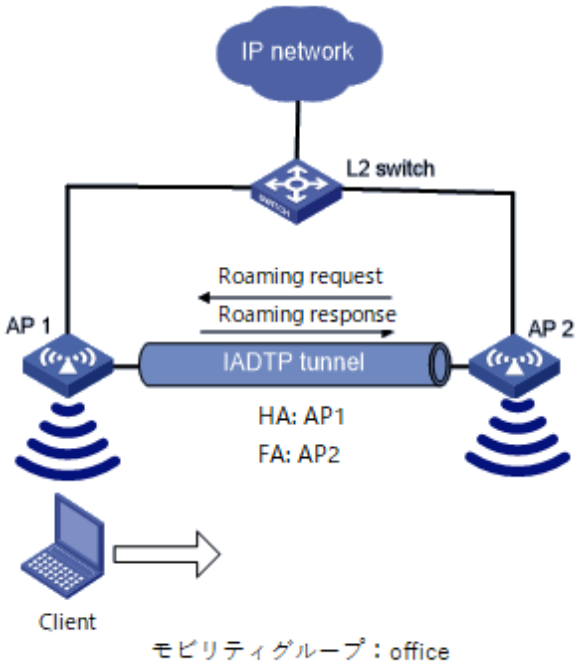


図 9-1 FAT AP 間ローミング

図 9-1に示すように、FAT AP 間ローミングは以下の処理を行います。

1) AP1 と AP2 はモビリティグループ office に所属しています。クライアントは AP 1 でオンラインになり、AP1 はクライアントのローミングエントリを作成します。
2) クライアントは AP 2 に移動します。AP2 はクライアントのローミングエントリを調査し、高速ローミング可能か決定します。クライアントが RSN + 802.1X クライアントなら、高速ローミングを使用し、再認証なしで AP 2 に移動します。RSN + 802.1X クライアントでない場合、クライアントは、AP 2 に接続するために再認証する必要があります。

9.3.2 FAT AP 間ローミングの設定

🕮 **メモ：**

- FAT モードで動作する AP 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、FAT AP 間ローミング動作は未サポートです。
- FAT モードで動作する AP と AC の組み合わせ、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。

FAT AP 間でクライアントのローミングエントリをやり取りするために、AP にモビリティグループの設定をしてください。

以下にモビリティ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**	ー
2. モビリティグループを作成し、その view に移行する	**wlan mobility group** *group-name*	デフォルト：設定なし
3. 送信元 IPv4 アドレスを指定する	**source ip** *ip-address*	デフォルト：設定なし
4. メンバ AP の IPv4 アドレスを指定する	**member ip** *ip-address*	デフォルト：設定なし
5. モビリティグループを有効にする	**group enable**	デフォルト：無効

9.3.3 WLAN ローミング用 SNMP 通知機能の有効化

WLAN ローミングイベントを NMS に通知するためには、SNMP 通知機能の有効にしてください。

以下に WLAN ローミング用 SNMP 通知機能を有効に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. WLAN ローミング用 SNMP 通知機能を有効にする	**snmp-agent trap enable wlan mobility**	デフォルト：無効

9.4 802.11rの設定

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 は以下のメッセージ交換方法を提供します。

- **Over-the-air**－クライアントは事前ローミング認証のために、ローミング先の AP と直接通信します。

9.4.1 802.11r 動作メカニズム

I. Over-the-air FT を使用した AP 間ローミング

図 9-2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 AP 間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。

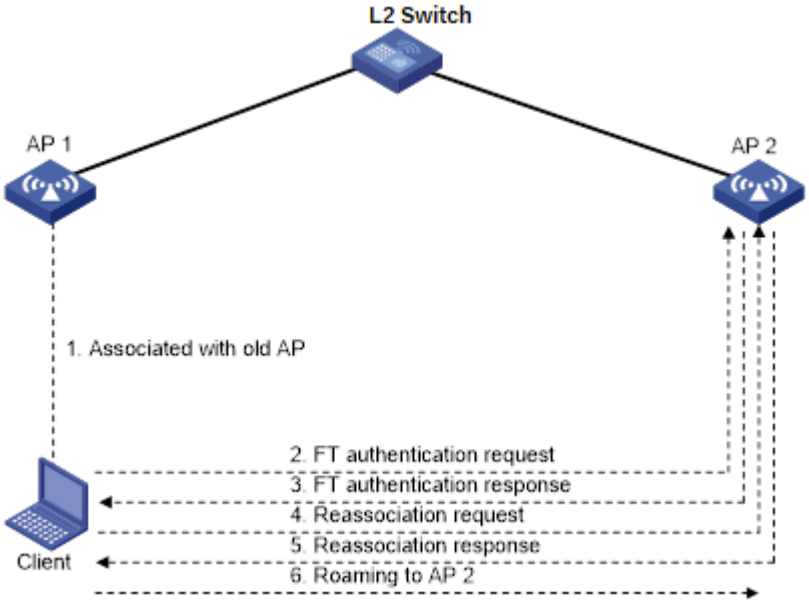


図 9-2 Over-the-air FT を使用した AP 間ローミング

9.4.2 プロトコルと標準

802.11r IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements

9.4.3 802.11r 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。
- 定期的な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 と定期的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。定期的再認証に関する詳細はオペレーションマニュアルのセクション 2 *WLAN "WLAN 認証の設定"* を参照してください。
- 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。PTK アップデートの詳細はオペレーションマニュアルのセクション 2 *WLAN "WLAN セキュリティ"* を参照してください。

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）FT の方法を設定する	**ft method over-the-air**	デフォルト：**over-the-air**
5. （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。

9.5 802.11vの設定

🕮 **メモ：**

802.11v の設定は、ソフトウェアバージョン 7.5.105 を含む以降のソフトウェアからサポートしています。

802.11v は、省電力、ロードバランシング、および BSS 移行管理(BTM) などの多数の拡張機能を定義した、ワイヤレスネットワーク管理の規格です。これにより、クライアントはネットワーク情報を交換し、常に最適な AP と関連付けることができるため、クライアントのバッテリ持続時間が長くなり、ユーザエクスペリエンスが向上します

9.5.1 BTM (BSS 移行管理)

BTM を使用すると、接続中の AP の信号強度が低い場合や、より信号強度の優れた 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 9-3に示すように、クライアントは AP に関連付いています。この時 BSS 移行管理は、以下のように動作します。

1) AP または 802.11v クライアントが BSS 移行をトリガします。

- Unsolicited request： AP は、クライアントの RSSI が RSSI しきい値よりも低いことを検出すると、クライアントに BTM request を送信します。
- Solicited request： 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。

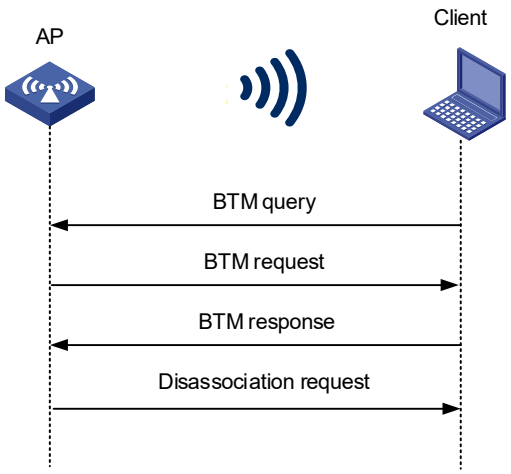


図 9-3 BSS 移行管理

9.5.2 BTM の設定

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。

- クライアント anti-sticky が無効の場合、AP はクライアントの信号強度がしきい値よりも低いかどうかを調べず、unsolicited BTM をトリガしません。
- この作業を行う前に、サービステンプレートが無効になっていることを確認してください。

BTM 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. BTM を有効にする	**bss transition-management enable**	デフォルト：無効

9.5.3 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。

- forced：アソシエーション解除タイマの期限が切れてもクライアントが AP とのアソシエーションを解除していない場合、AP はそのクライアントを強制的にログオフします。
- recommended： アソシエーション解除タイマの期限が切れてもクライアントが AP とのアソシエーションを解除していない場合、AP はクライアントを強制的にログオフしません。

bss transition-management disassociation forced を設定すると、アソシエーション解除タイマの期限が切れてもクライアントが AP とのアソシエーションを解除していない場合に、クライアントが強制的にログオフされます。この機能は慎重に使用してください。

BTM アソシエーション解除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. BTM アソシエーション解除を設定する	**bss transition-management disassociation** { **forced** | **recommended** } [**timer** *time*]	デフォルト：無効

9.5.4 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。

クライアント anti-sticky 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. radio interface view に移行する	**interface wlan-radio** *interface-number*	—
3. 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

9.6 802.11kの設定

QX-W1200 シリーズアクセスポイントオペレーションマニュアルの “*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。

9.7 WLANローミング設定例

9.7.1 FAT AP 間ローミング

I. ネットワーク要件

図 9-4に示すように、FAT AP1 と FAT AP2 間で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。

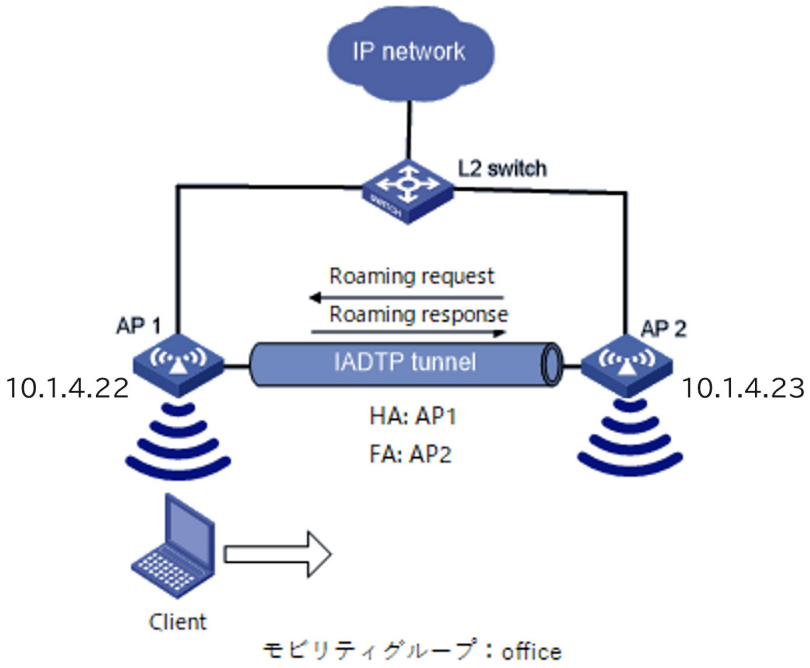


図 9-4 ネットワーク図

II. 設定手順

AP1 で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使用可能にします。

```
<AP1> system-view
[AP1] wlan service-template service
[AP1-wlan-st-service] ssid 1
[AP1-wlan-st-service] service-template enable
[AP1-wlan-st-service] quit
```

サービステンプレート service を AP1 の WLAN-Radio 1/0/2 に割り当てます。

```
[AP1] interface WLAN-Radio 1/0/2
[AP1-WLAN-Radio1/0/2] undo shutdown
[AP1-WLAN-Radio1/0/2] service-template service
[AP1-WLAN-Radio1/0/2] quit
```

AP1 でモビリティグループ office を作成します。

```
[AP1] wlan mobility group office
```

モビリティトンネルの確立に使用する送信元 IP として 10.1.4.22 を設定します。

```
[AP1-wlan-mg-office] source ip 10.1.4.22
```

メンバ IP 10.1.4.23 を設定します。

```
[AP1-wlan-mg-office] member ip 10.1.4.23
```

モビリティグループを有効化します。

```
[AP1-wlan-mg-office] group enable
```

AP2 で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使用可能にします。

```
<AP2> system-view
[AP2] wlan service-template service
[AP2-wlan-st-service] ssid 1
[AP2-wlan-st-service] service-template enable
[AP2-wlan-st-service] quit
```

サービステンプレート service を AP2 の WLAN-Radio 1/0/1 に割り当てます。

```
[AP2] interface WLAN-Radio 1/0/2
[AP2-WLAN-Radio1/0/2] undo shutdown
[AP2-WLAN-Radio1/0/2] service-template service
[AP2-WLAN-Radio1/0/2] quit
```

モビリティグループ office を作成します。

```
[AP2] wlan mobility group office
```

モビリティトンネルの確立に使用する送信元 IP として 10.1.4.23 を設定します。

```
[AP2-wlan-mg-office] source ip 10.1.4.23
```

メンバ IP 10.1.4.23 を設定します。

```
[AP2-wlan-mg-office] member ip 10.1.4.22
```

モビリティグループを有効化します。

```
[AP2-wlan-mg-office] group enable
```

III. 設定確認

AP1 で display wlan mobility group コマンドを使用します

```
[AP1] 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
```

AP2 で、display wlan mobility group コマンドを使用します

```
[AP2] 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
```

クライアントを AP1 に参加させます。（詳細は省略します。）

クライアントが AP1 に参加しているが、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。

```
[AP1] display wlan client verbose
Total number of clients: 1

 MAC address                     : 0103-0184-cd1e
 IPv4 address                    : 192.168.1.21
 IPv6 address                    : N/A
 Username                        : N/A
 AID                             : 1
 Radio ID                        : 2
 Channel                         : 100
 SSID                            : service
 BSSID                           : 782c-2979-7c80
 VLAN ID                         : 1
 Service VLAN ID                 : N/A
 Sleep count                     : 369
```

```
 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          : N/A
 Number of Sounding Dimensions      : N/A
 SU beamformee capability           : Not supported
 MU beamformee capability           : Not supported
 Block Ack                          : TID 0  Both
                                      TID 1  In
                                      TID 5  In
 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                               : 32
 Rx/Tx rate                         : 39/6 Mbps
 Speed                              : 4.320/1.112Kbps
 Authentication method              : Open system
 Security mode                      : RSN
 AKM mode                           : PSK
 Cipher suite                       : CCMP
 User authentication mode           : Bypass
 WPA3 status                        : Disabled
 Authorization CAR                  : N/A
 Authorization user group name      : N/A
 Authorization ACL ID               : N/A
 Authorization user profile         : N/A
 Roam status                        : N/A
 Key derivation                     : SHA256
 PMF status                         : N/A
 Forwarding policy name             : Not configured
 Online time                        : 0days 0hours 3minutes 24seconds
 FT status                          : Active
 BTM mode                           : 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 に参加し、ローミングステータスが Inter-AP roam であることを確認します。

[AC] display wlan client verbose

```
Total number of clients: 1

 MAC address                        : 0103-0184-cd1e
 IPv4 address                       : 192.168.1.21
 IPv6 address                       : N/A
 Username                           : N/A
 AID                                : 1
 Radio ID                           : 2
 Channel                            : 116
 SSID                               : service
 BSSID                              : 74ea-c8fd-bd70
 VLAN ID                            : 1
 Service VLAN ID                    : N/A
 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        : N/A
Number of Sounding Dimensions    : N/A
SU beamformee capability         : Not supported
MU beamformee capability         : Not supported
Block Ack                        : TID 0  In
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                             : 57
Rx/Tx rate                       : 780/6 Mbps
Speed                            : N/A
Authentication method            : FT
Security mode                    : RSN
AKM mode                         : PSK
Cipher suite                     : CCMP
User authentication mode         : Bypass
WPA3 status                      : Disabled
Authorization CAR                : N/A
Authorization user group name    : N/A
Authorization ACL ID             : N/A
Authorization user profile       : N/A
Roam status                      : Inter-AP roam
Key derivation                   : SHA256
PMF status                       : N/A
Forwarding policy name           : Not configured
Online time                      : 0days 0hours 0minutes 4seconds
FT status                        : Active
BTM mode                         : Inactive
```

9.8 802.11r設定例

9.8.1 Over-the-air FT と PSK 認証設定例

I. ネットワーク要件

図 9-5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 AP 間ローミングを設定します。FAT AP 間でローミングができるように、モビリティグループ office を設定します。akm モードを PSK に設定します。

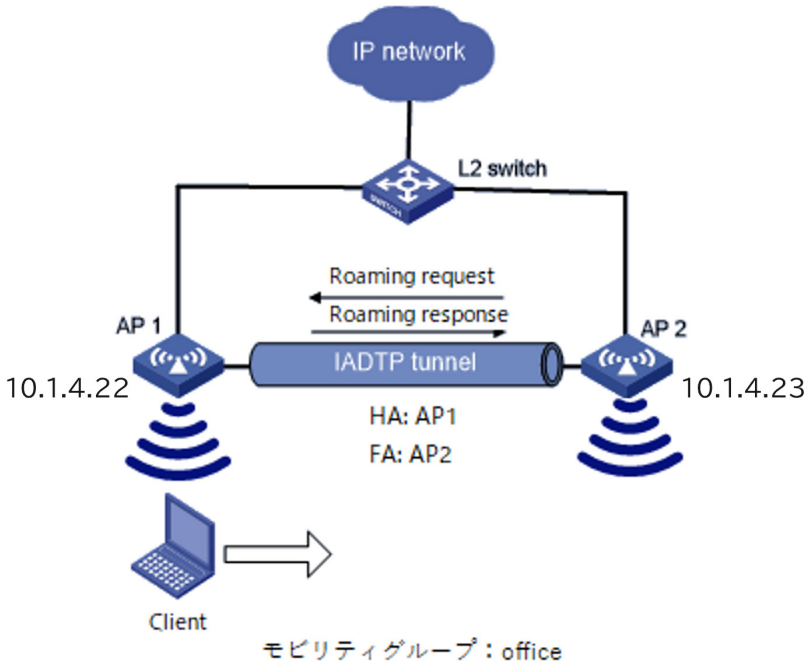


図 9-5 ネットワーク図

II. 設定手順

AP1 でサービステンプレート **service** を作成します。

```
<AP1> system-view
[AP1] wlan service-template service
```

SSID を **service** に設定します。

```
[AP1-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。

```
[AP1-wlan-st-service] akm mode psk
[AP1-wlan-st-service] 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。

```
[AP1-wlan-st-service] cipher-suite ccmp
[AP1-wlan-st-service] security-ie rsn
```

FT を有効にします。

```
[AP1-wlan-st-service] 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。

```
[AP1-wlan-st-service] ft reassociation-timeout 50
```

サービステンプレートを有効にします。

```
[AP1-wlan-st-service] service-template enable
[AP1-wlan-st-service] quit
```

サービステンプレート service を AP1 の WLAN-Radio 1/0/2 に割り当てます。

```
[AP1] interface WLAN-Radio 1/0/2
[AP1-WLAN-Radio1/0/2] undo shutdown
[AP1-WLAN-Radio1/0/2] service-template service
[AP1-WLAN-Radio1/0/2] quit
```

AP1 でモビリティグループ office を作成します。

```
[AP1] wlan mobility group office
```

モビリティトンネルの確立に使用する送信元 IP として 10.1.4.22 を設定します。

```
[AP1-wlan-mg-office] source ip 10.1.4.22
```

メンバ IP 10.1.4.23 を設定します。

```
[AP1-wlan-mg-office] member ip 10.1.4.23
```

モビリティグループを有効化します。

```
[AP1-wlan-mg-office] group enable
```

#AP2 で サービステンプレート **service** を作成します。

```
<AP2> system-view
[AP2] wlan service-template service
```

SSID を **service** に設定します。

```
[AP2-wlan-st-service] 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。

```
[AP2-wlan-st-service] akm mode psk
[AP2-wlan-st-service] 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。

```
[AP2-wlan-st-service] cipher-suite ccmp
[AP2-wlan-st-service] security-ie rsn
```

FT を有効にします。

```
[AP2-wlan-st-service] 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。

```
[AP2-wlan-st-service] ft reassociation-timeout 50
```

サービステンプレートを有効にします。

```
[AP2-wlan-st-service] service-template enable
```

```
[AP2-wlan-st-service] quit
```

サービステンプレート service を AP2 の WLAN-Radio 1/0/2 に割り当てます。

```
[AP2] interface WLAN-Radio 1/0/2
[AP2-WLAN-Radio1/0/2] undo shutdown
[AP2-WLAN-Radio1/0/2] service-template service
[AP2-WLAN-Radio1/0/2] quit
```

AP2 でモビリティグループ office を作成します。

```
[AP2] wlan mobility group office
```

モビリティトンネルの確立に使用する送信元 IP として 10.1.4.23 を設定します。

```
[AP2-wlan-mg-office] source ip 10.1.4.23
```

メンバ IP 10.1.4.23 を設定します。

```
[AP2-wlan-mg-office] member ip 10.1.4.22
```

モビリティグループを有効化します。

```
[AP2-wlan-mg-office] group enable
```

III. 設定確認

AP1 で display wlan mobility group コマンドを使用します

```
[AP1] 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
```

AP2 で、display wlan mobility group コマンドを使用します

```
[AP2] 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
```

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                     : a60a-1303-8361
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 Inter-AP roam であることを確認します。

[AC] display wlan client verbose

```
Total number of clients: 1

 MAC address                     : a60a-1303-8361
 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                       : Inter-AP roam
 Key derivation                    : SHA256
 PMF status                        : N/A
 Forward policy                     : N/A
 Online time                       : 0hr 0min 27sec
 FT status                         : Active
```

AP2 で、display wlan mobility roam-in コマンドを使用します

```
[AP2] display wlan mobility roam-in
Current entries: 1
MAC address     BSSID           VLAN ID    HA IP address
a60a-1303-8361  000f-e211-2233  1          10.1.1.114
```

9.8.2 Over-the-air FT と 802.1X 認証設定例

I. ネットワーク要件

図 9-5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 AP 間ローミングを設定します。FAT AP 間でローミングができるように、モビリティグループ office を設定します。akm モードを 802.1X に設定します。

II. 設定手順

AP1 でサービステンプレート **service** を作成します。

```
<AP1> system-view
[AP1] wlan service-template service
```

SSID を **service** に設定します。

```
[AP1-wlan-st-service] ssid service
```

akm モードを 802.1X に設定します。

```
[AP1-wlan-st-service] 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。

```
[AP1-wlan-st-service] cipher-suite ccmp
[AP1-wlan-st-service] 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。

```
[AP1-wlan-st-service] client-security authentication-mode dot1x
[AP1-wlan-st-service] dot1x domain imc
```

FT を有効にします。

```
[AP1-wlan-st-service] ft enable
```

サービステンプレートを有効にします。

```
[AP1-wlan-st-service] service-template enable
[AP1-wlan-st-service] quit
```

802.1X 認証を設定します。

```
[AP1] dot1x
[AP1] dot1x authentication-method eap
```

RADIUS スキーム imcc を作成します。

```
[AP1] 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 10.1.4.3 に設定します。

```
[AP1-radius-imcc] primary authentication 10.1.4.3
[AP1-radius-imcc] primary accounting 10.1.4.3
```

#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､AP1 に共有鍵 12345678 を設定します。

```
[AP1-radius-imcc] key authentication simple 12345678
[AP1-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。

```
[AP1-radius-imcc] user-name-format without-domain
[AP1-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。

```
[AP1] domain imc
[AP1-isp-imc] authentication lan-access radius-scheme imcc
[AP1-isp-imc] authorization lan-access radius-scheme imcc
[AP1-isp-imc] accounting lan-access radius-scheme imcc
[AP1-isp-imc] quit
```

サービステンプレート service を AP1 の WLAN-Radio 1/0/2 に割り当てます。

```
[AP1] interface WLAN-Radio 1/0/2
[AP1-WLAN-Radio1/0/2] undo shutdown
[AP1-WLAN-Radio1/0/2] service-template service
[AP1-WLAN-Radio1/0/2] quit
```

AP1 でモビリティグループ office を作成します。

```
[AP1] wlan mobility group office
```

モビリティトンネルの確立に使用する送信元 IP として 10.1.4.22 を設定します。

```
[AP1-wlan-mg-office] source ip 10.1.4.22
```

メンバ IP 10.1.4.23 を設定します。

```
[AP1-wlan-mg-office] member ip 10.1.4.23
```

モビリティグループを有効化します。

```
[AP1-wlan-mg-office] group enable
```

#AP2 で サービステンプレート **service** を作成します。

```
<AP2> system-view
[AP2] wlan service-template service
```

SSID を **service** に設定します。

```
[AP2-wlan-st-service] ssid service
```

akm モードを 802.1X に設定します。

```
[AP2-wlan-st-service] 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。

```
[AP2-wlan-st-service] cipher-suite ccmp
[AP2-wlan-st-service] 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。

```
[AP2-wlan-st-service] client-security authentication-mode dot1x
[AP2-wlan-st-service] dot1x domain imc
```

FT を有効にします。

```
[AP2-wlan-st-service] ft enable
```

サービステンプレートを有効にします。

```
[AP2-wlan-st-service] service-template enable
[AP2-wlan-st-service] quit
```

802.1X 認証モードを EAP に設定します。

```
[AP2] dot1x authentication-method eap
```

RADIUS スキーム imcc を作成します。

```
[AP2] 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 10.1.4.3 に設定します。

```
[AP2-radius-imcc] primary authentication 10.1.4.3
```

```
[AP2-radius-imcc] primary accounting 10.1.4.3
```

#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、AP1 に共有鍵 12345678 を設定します。

```
[AP2-radius-imcc] key authentication simple 12345678
[AP2-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。

```
[AP2-radius-imcc] user-name-format without-domain
[AP2-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。

```
[AP2] domain imc
[AP2-isp-imc] authentication lan-access radius-scheme imcc
[AP2-isp-imc] authorization lan-access radius-scheme imcc
[AP2-isp-imc] accounting lan-access radius-scheme imcc
[AP2-isp-imc] quit
```

サービステンプレート service を AP2 の WLAN-Radio 1/0/2 に割り当てます。

```
[AP2] interface WLAN-Radio 1/0/2
[AP2-WLAN-Radio1/0/2] undo shutdown
[AP2-WLAN-Radio1/0/2] service-template service
[AP2-WLAN-Radio1/0/2] quit
```

AP2 でモビリティグループ office を作成します。

```
[AP2] wlan mobility group office
```

モビリティトンネルの確立に使用する送信元 IP として 10.1.4.23 を設定します。

```
[AP2-wlan-mg-office] source ip 10.1.4.23
```

メンバ IP 10.1.4.23 を設定します。

```
[AP2-wlan-mg-office] member ip 10.1.4.22
```

モビリティグループを有効化します。

```
[AP2-wlan-mg-office] group enable
```

III. 設定確認

AP1 で display wlan mobility group コマンドを使用します

```
[AP1] 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
```

AP2 で、display wlan mobility group コマンドを使用します

[AP2] 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
```

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                          : a60a-1303-8361
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 19sec
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-AP roam であることを確認します。

[AC] display wlan client verbose

```
Total number of clients: 1

MAC address                     : a60a-1303-8361
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                     : Inter-AP roam
Key derivation                  : SHA256
PMF status                      : N/A
Forward policy                  : N/A
Online time                     : 0hr 0min 7sec
FT status                       : Active
```

AP2 で、display wlan mobility roam-in コマンドを使用します

[AP2] display wlan mobility roam-in

```
Current entries: 1
MAC address     BSSID           VLAN ID    HA IP address
a60a-1303-8361  000f-e211-2233  1          10.1.1.114
```

9.9 802.11v設定例

> 🕮 メモ：
> 802.11v の設定は、ソフトウェアバージョン 7.5.105 を含む以降のソフトウェアからサポートしています。

9.9.1 BTM と PSK 認証設定

I. ネットワーク要件

図 9-6に示すように、クライアントが AP1 から AP2 の方向へ移動するとき、より適切な AP にクライアントの接続先を誘導する為、BTM、BTM アソシエーション解除(forced)を設定します。クライアント anti-sticky を設定し、RSSI しきい値を 30 に設定し、検出間隔を 5 秒に設定し、非 802.11v クライアントの強制ログオフを有効にします。akm(authentication and key management)モードを PSK に設定します。

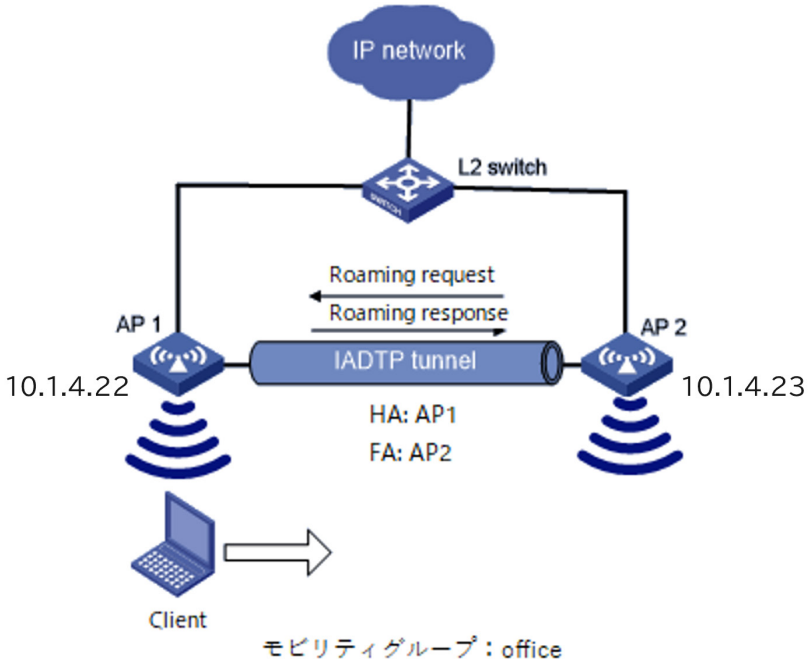


図 9-6 ネットワーク図

II. 設定手順

AP1 でサービステンプレート **service** を作成します。

```
<AP1> system-view
[AP1] wlan service-template service
```

SSID を **service** に設定します。

```
[AP1-wlan-st-service] 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。

```
[AP1-wlan-st-service] akm mode psk
[AP1-wlan-st-service] 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。

```
[AP1-wlan-st-service] cipher-suite ccmp
[AP1-wlan-st-service] security-ie rsn
```

BTM を有効にします。

```
[AP1-wlan-st-service] bss transition-management enable
```

BTM アソシエーション解除を forced で設定し、タイマを 90 秒に設定します。

```
[AP1-wlan-st-service] bss transition-management disassociation forced timer 90
```

サービステンプレートを有効にします。

```
[AP1-wlan-st-sercie] service-template enable
[AP1-wlan-st-service] quit
```

サービステンプレート service を AP1 の WLAN-Radio 1/0/2 に割り当てます。クライアント anti-sticky を有効にし、RSSI しきい値を 30 に設定し、検出間隔を 5 秒に設定し、非 802.11v クライアントの強制ログオフを有効にします。

```
[AP1] interface WLAN-Radio 1/0/2
[AP1-WLAN-Radio1/0/2] undo shutdown
[AP1-WLAN-Radio1/0/2] service-template service
[AP1-WLAN-Radio1/0/2] sacp anti-sticky enable rssi 30 interval 5 forced-logoff
[AP1-WLAN-Radio1/0/2] quit
```

AP1 でモビリティグループ office を作成します。

```
[AP1] wlan mobility group office
```

モビリティトンネルの確立に使用する送信元 IP として 10.1.4.22 を設定します。

```
[AP1-wlan-mg-office] source ip 10.1.4.22
```

メンバ IP 10.1.4.23 を設定します。

```
[AP1-wlan-mg-office] member ip 10.1.4.23
```

モビリティグループを有効化します。

```
[AP1-wlan-mg-office] group enable
```

#AP2 で サービステンプレート **service** を作成します。

```
<AP2> system-view
[AP2] wlan service-template service
```

SSID を **service** に設定します。

```
[AP2-wlan-st-service] 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。

```
[AP2-wlan-st-service] akm mode psk
[AP2-wlan-st-service] 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。

```
[AP2-wlan-st-service] cipher-suite ccmp
[AP2-wlan-st-service] security-ie rsn
```

BTM を有効にします。

```
[AP2-wlan-st-service] bss transition-management enable
```

BTM アソシエーション解除を forced で設定し、タイマを 90 秒に設定します。

```
[AP2-wlan-st-service] bss transition-management disassociation forced timer 90
```

サービステンプレートを有効にします。

```
[AP2-wlan-st-service] service-template enable
[AP2-wlan-st-service] quit
```

サービステンプレート service を AP2 の WLAN-Radio 1/0/2 に割り当てます。クライアント anti-sticky を有効にし、RSSI しきい値を 30 に設定し、検出間隔を 5 秒に設定し、非 802.11v クライアントの強制ログオフを有効にします。

```
[AP2] interface WLAN-Radio 1/0/2
[AP2-WLAN-Radio1/0/2] undo shutdown
[AP2-WLAN-Radio1/0/2] service-template service
[AP2-WLAN-Radio1/0/2] sacp anti-sticky enable rssi 30 interval 5 forced-logoff
[AP2-WLAN-Radio1/0/2] quit
```

AP2 でモビリティグループ office を作成します。

```
[AP2] wlan mobility group office
```

モビリティトンネルの確立に使用する送信元 IP として 10.1.4.23 を設定します。

```
[AP2-wlan-mg-office] source ip 10.1.4.23
```

メンバ IP 10.1.4.22 を設定します。

```
[AP2-wlan-mg-office] member ip 10.1.4.22
```

モビリティグループを有効化します。

```
[AP2-wlan-mg-office] group enable
```

III. 設定確認

AP1 で display wlan mobility group コマンドを使用します

[AP1] 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
```

AP2 で、display wlan mobility group コマンドを使用します

[AP2] 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
```

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。

- RSN IE が有効。
- AKM モードが PSK。
- Cipher スイートが CCMP。
- BTM status が有効。

[AP1] display wlan service-template service verbose

```
Service template name                              : service
Description                                        : Not configured
SSID                                               : service
SSID-hide                                          : Disabled
User-isolation                                     : Disabled
Service template status                            : Enabled
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
Service VLAN ID                                    : N/A
Service VLAN TPID                                  : dot1q
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
PPSK                                               : Disabled
PPSK Fail Permit                                   : Enabled
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                                      : Disabled
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
QoS U-APSD mode                                 : 1
BTM status                                      : Enabled
```

#802.11v 対応クライアントを AP1 に接続します。(詳細は省略します)

#クライアントの情報で、BTM mode が Active となっていることを確認します。

```
[AP1]display wlan client verbose
Total number of clients: 1

MAC address                        : a601-13af-8cc3
IPv4 address                       : N/A
IPv6 address                       : N/A
 Username                           : N/A
 AID                                : 1
 Radio ID                           : 2
 Channel                            : 132
 SSID                               : service
 BSSID                              : 1496-2d06-c220
 VLAN ID                            : 1
 Sleep count                        : 8
 Wireless mode                      : 802.11ax
 Channel bandwidth                  : 80MHz
 SM power save                      : Disabled
 Short GI for 20MHz                 : Supported
 Short GI for 40MHz                 : Supported
 Short GI for 80MHz                 : Supported
 Short GI for 160/80+80MHz          : Not supported
 STBC RX capability                 : Supported
 STBC TX capability                 : Supported
 LDPC RX capability                 : Supported
 Beamformee STS capability          : N/A
 Number of Sounding Dimensions      : N/A
 SU beamformee capability           : Not supported
 MU beamformee capability           : Not supported
 Block Ack                          : TID 0  Both
 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
 5G 40And80MHz Channel bandwidth    : Supported
 5G 160MHz Channel bandwidth        : Not Supported
 5G 80+80MHz Channel bandwidth      : Not Supported
 OFDMA random access RUs            : Not supported
```

```
 Supported HE-MCS set                : 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
 TWT scheduled                       : No
 QoS mode                            : WMM
 Listen interval                     : 250
 RSSI                                : 39
 Rx/Tx rate                          : 735/6 Mbps
 Speed                               : 0.578/0.405Kbps
 Authentication method               : Open system
 Security mode                       : RSN
 AKM mode                            : PSK
 Cipher suite                        : CCMP
 User authentication mode            : Bypass
 WPA3 status                         : Disabled
 SAE PWE Method                      : None
 Authorization CAR                   : N/A
 Authorization ACL ID                : N/A
 Authorization user profile          : N/A
 Roam status                         : N/A
 Key derivation                      : SHA1
 PMF status                          : N/A
 Forwarding policy name              : Not configured
 Online time                         : 0days 0hours 0minutes 29seconds
 FT status                           : Inactive
 BTM mode                            : Active
```

9.9.2 BTM と 802.1X 認証設定

I. ネットワーク要件

図 9-6に示すように、クライアントが AP1 から AP2 の方向へ移動するとき、より適切な AP にクライアントの接続先を誘導する為、BTM、BTM アソシエーション解除 (recommended)、クライアント anti-sticky を設定し、RSSI しきい値を 30 に設定し、検出間隔を 5 秒に設定し、非 802.11v クライアントの強制ログオフを有効にします。akm モードを 802.1X に設定します。

AP1 でサービステンプレート **service** を作成します。

```
<AP1> system-view
[AP1] wlan service-template service
```

SSID を **service** に設定します。

```
[AP1-wlan-st-service] ssid service
```

akm モードを 802.1X に設定します。

```
[AP1-wlan-st-service] 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。

```
[AP1-wlan-st-service] cipher-suite ccmp
[AP1-wlan-st-service] 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。

```
[AP1-wlan-st-service] client-security authentication-mode dot1x
```

```
[AP1-wlan-st-service] dot1x domain imc
```

BTM を有効にします。

```
[AP1-wlan-st-service] bss transition-management enable
```

BTM アソシエーション解除を recommended で設定し、タイマを 90 秒に設定します。

```
[AP1-wlan-st-service] bss transition-management disassociation recommended timer 90
```

サービステンプレートを有効にします。

```
[AP1-wlan-st-service] service-template enable
[AP1-wlan-st-service] quit
```

802.1X 認証を設定します。

```
[AP1] dot1x
[AP1] dot1x authentication-method eap
```

RADIUS スキーム imcc を作成します。

```
[AP1] 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 10.1.4.3 に設定します。

```
[AP1-radius-imcc] primary authentication 10.1.4.3
[AP1-radius-imcc] primary accounting 10.1.4.3
```

#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､AP1 に共有鍵 12345678 を設定します。

```
[AP1-radius-imcc] key authentication simple 12345678
[AP1-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。

```
[AP1-radius-imcc] user-name-format without-domain
[AP1-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。

```
[AP1] domain imc
[AP1-isp-imc] authentication lan-access radius-scheme imcc
[AP1-isp-imc] authorization lan-access radius-scheme imcc
[AP1-isp-imc] accounting lan-access radius-scheme imcc
[AP1-isp-imc] quit
```

サービステンプレート service を AP1 の WLAN-Radio 1/0/2 に割り当てます。

```
[AP1] interface WLAN-Radio 1/0/2
[AP1-WLAN-Radio1/0/2] undo shutdown
[AP1-WLAN-Radio1/0/2] service-template service
```

```
[AP1-WLAN-Radio1/0/2] quit
```

AP1 でモビリティグループ office を作成します。

```
[AP1] wlan mobility group office
```

モビリティトンネルの確立に使用する送信元 IP として 10.1.4.22 を設定します。

```
[AP1-wlan-mg-office] source ip 10.1.4.22
```

メンバ IP 10.1.4.23 を設定します。

```
[AP1-wlan-mg-office] member ip 10.1.4.23
```

モビリティグループを有効化します。

```
[AP1-wlan-mg-office] group enable
```

#AP2 で サービステンプレート **service** を作成します。

```
<AP2> system-view
[AP2] wlan service-template service
```

SSID を **service** に設定します。

```
[AP2-wlan-st-service] ssid service
```

akm モードを 802.1X に設定します。

```
[AP2-wlan-st-service] 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。

```
[AP2-wlan-st-service] cipher-suite ccmp
[AP2-wlan-st-service] 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。

```
[AP2-wlan-st-service] client-security authentication-mode dot1x
[AP2-wlan-st-service] dot1x domain imc
```

BTM を有効にします。

```
[AP2-wlan-st-service] bss transition-management enable
```

BTM アソシエーション解除を recommended で設定し、タイマを 90 秒に設定します。

```
[AP2-wlan-st-service] bss transition-management disassociation recommended timer 90
```

サービステンプレートを有効にします。

```
[AP2-wlan-st-service] service-template enable
[AP2-wlan-st-service] quit
```

802.1X を設定します。

```
[AP2] dot1x
[AP2] dot1x authentication-method eap
```

RADIUS スキーム imcc を作成します。

```
[AP2] 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 10.1.4.3 に設定します。

```
[AP2-radius-imcc] primary authentication 10.1.4.3
[AP2-radius-imcc] primary accounting 10.1.4.3
```

#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､AP1 に共有鍵 12345678 を設定します。

```
[AP2-radius-imcc] key authentication simple 12345678
[AP2-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。

```
[AP2-radius-imcc] user-name-format without-domain
[AP2-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。

```
[AP2] domain imc
[AP2-isp-imc] authentication lan-access radius-scheme imcc
[AP2-isp-imc] authorization lan-access radius-scheme imcc
[AP2-isp-imc] accounting lan-access radius-scheme imcc
[AP2-isp-imc] quit
```

サービステンプレート service を AP2 の WLAN-Radio 1/0/2 に割り当てます。

```
[AP2] interface WLAN-Radio 1/0/2
[AP2-WLAN-Radio1/0/2] undo shutdown
[AP2-WLAN-Radio1/0/2] service-template service
[AP2-WLAN-Radio1/0/2] quit
```

AP2 でモビリティグループ office を作成します。

```
[AP2] wlan mobility group office
```

モビリティトンネルの確立に使用する送信元 IP として 10.1.4.23 を設定します。

```
[AP2-wlan-mg-office] source ip 10.1.4.23
```

メンバ IP 10.1.4.22 を設定します。

```
[AP2-wlan-mg-office] member ip 10.1.4.22
```

モビリティグループを有効化します。

```
[AP2-wlan-mg-office] group enable
```

II. 設定確認

AP1 で display wlan mobility group コマンドを使用します

[AP1] 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
```

AP2 で、display wlan mobility group コマンドを使用します

[AP2] 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
```

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。
- BTM stasus が有効。

[AP1] display wlan service-template service verbose

```
Service template name                              : service
Description                                        : Not configured
SSID                                               : service
SSID-hide                                          : Disabled
User-isolation                                     : Disabled
Service template status                            : Enabled
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
Service VLAN ID                                    : N/A
Service VLAN TPID                                  : dot1q
AKM mode                                           : 802.1X
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
PPSK                                               : Disabled
PPSK Fail Permit                                   : Enabled
Enhance-open status                                : Disabled
Enhanced-open transition-mode service-template     : N/A
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 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                                    : AP
FT status                                    : Disabled
QoS trust                                    : Port
QoS priority                                 : 0
QoS U-APSD mode                              : 1
BTM status                                   : Enabled
```

#802.11v 対応クライアントを AP1 に接続します。(詳細は省略します)

#クライアントの情報で、BTM mode が Active となっていることを確認します。

[AC]display wlan client verbose

```
Total number of clients: 1

 MAC address                         : 0908-37af-8cc3
 IPv4 address                        : N/A
 IPv6 address                        : N/A
 Username                            : tester
 AID                                 : 1
 Radio ID                            : 2
 Channel                             : 132
 SSID                                : service
 BSSID                               : 1496-2d06-c220
 VLAN ID                             : 1
 Sleep count                         : 8
 Wireless mode                       : 802.11ax
 Channel bandwidth                   : 80MHz
 SM power save                       : Disabled
 Short GI for 20MHz                  : Supported
 Short GI for 40MHz                  : Supported
 Short GI for 80MHz                  : Supported
 Short GI for 160/80+80MHz           : Not supported
 STBC RX capability                  : Supported
 STBC TX capability                  : Supported
 LDPC RX capability                  : Supported
 Beamformee STS capability           : N/A
 Number of Sounding Dimensions       : N/A
 SU beamformee capability            : Not supported
 MU beamformee capability            : Not supported
 Block Ack                           : TID 0  Both
 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
 5G 40And80MHz Channel bandwidth     : Supported
 5G 160MHz Channel bandwidth         : Not Supported
 5G 80+80MHz Channel bandwidth       : Not Supported
```

```
OFDMA random access RUs          : Not supported
Supported HE-MCS set             : 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
TWT scheduled                    : No
QoS mode                         : WMM
Listen interval                  : 250
RSSI                             : 39
Rx/Tx rate                       : 735/6 Mbps
Speed                            : 0.578/0.405Kbps
Authentication method            : Open system
Security mode                    : RSN
AKM mode                         : 802.1X
Cipher suite                     : CCMP
User authentication mode         : 802.1X
WPA3 status                      : Disabled
SAE PWE Method                   : None
Authorization CAR                : N/A
Authorization ACL ID             : N/A
Authorization user profile       : N/A
Roam status                      : N/A
Key derivation                   : SHA1
PMF status                       : N/A
Forwarding policy name           : Not configured
Online time                      : 0days 0hours 0minutes 29seconds
FT status                        : Inactive
BTM mode                         : Active
```

目次

このセクションのページは**2-x-x** です。

10 章 WLAN 無線リソースの計測設定（FIT は未サポート） 10-1
10.1 概要 10-1
10.1.1 802.11h 計測 10-1
10.1.2 802.11k 計測 10-1
10.2 設定作業リスト 10-2
10.3 無線リソース計測の有効化 10-2
10.4 計測期間と計測間隔の設定 10-3
10.5 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 10-3
10.6 WLAN 無線リソース計測の表示 10-4
10.7 無線リソース計測の設定例 10-4
10.7.1 無線リソース計測の設定例 10-4

10章 WLAN 無線リソースの計測設定（FIT は未サポート）

10.1 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。

10.1.1 802.11h 計測

802.11h 計測は、5GHz 帯のチャネルを計測します。表 10-1 は、802.11h 計測がサポートする計測の一覧です。

表 10-1 802.11h 計測

タイプ		内容
スペクトル管理計測	Basic	クライアントが以下のいずれかを検出したかを計測します。 ● 別のBSSからのパケット ● OFDMプリアンブル ● レーダ信号 ● 未知の信号
	CCA（Clear Channel Assessment）	計測時間の総和に対するチャネルのビジー時間の割合を計測します。
	RPI（Receive Power Indication）	計測時間の総和に対する異なるRPI範囲の時間の割合を計測します。
TPC（Transmit Power Control）計測		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。

802.11h 計測は、以下の手順で作動します。

1) AP は、802.11h 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スペクトル計測フィールドを 1 に設定します。
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。

10.1.2 802.11k 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 10-2 は、802.11k 計測がサポートする計測の一覧です。

表 10-2 802.11k 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。

10.2 設定作業リスト

必須/オプション	作業リスト
必須	無線リソース計測の有効化
オプション	計測期間と計測間隔の設定
オプション	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

10.3 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. radio interface view に移行する	**interface wlan-radio** *interface-number*	—

操作	コマンド	補足
3． 無線リソース計測を有効にする	**resource-measure enable**	デフォルト：無効 リンク計測、ネイバ計測、無線計測を有効にする場合、無線リソース計測を有効にしなければなりません。
4． スペクトル管理を有効にする	**spectrum-management enable**	デフォルト：無効 スペクトル計測またはTPC計測は、スペクトル管理を有効にしたあとにのみ適用されます。 このコマンドに関する詳細はコマンドマニュアルのセクション2 *WLAN “スペクトル管理の設定”* を参照してください。
5． 計測タイプを有効にする	**measure** { **all** | **link** | **neighbor** | **radio** | **spectrum** | **tpc** } **enable**	デフォルト：無効 Spectrum、tpcキーワードは5GHz無線でのみ利用可能です。

10.4 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。

計測期間と計測間隔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． radio interface view に移行する	**interface wlan-radio** *interface-number*	—
3． 計測期間を設定する	**measure-duration** *time*	デフォルト：500TU
4． 計測間隔を設定する	**measure-interval** *value*	デフォルト：30秒

10.5 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。

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． radio interface view に移行する	**interface wlan-radio** *interface-number*	—
3． 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

10.6 WLAN無線リソース計測の表示

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
クライアント計測報告を表示する	**display wlan measure-report interface** *interface-type interface-number* [**client mac-address** *mac-address*]

10.7 無線リソース計測の設定例

10.7.1 無線リソース計測の設定例

I. ネットワーク要件

図 10-1 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。

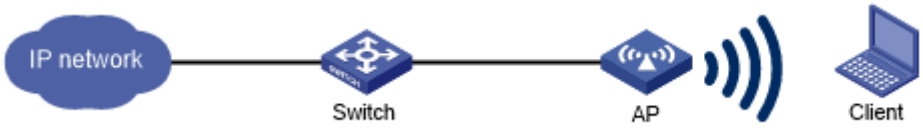


図 10-1 ネットワーク図

II. 設定手順

サービステンプレート 1 を作成します。

```
<FAT AP> system-view
[FAT AP] wlan service-template 1
```

SSID resource-measure を設定し、サービステンプレートを有効にします。

```
[FAT AP-wlan-st-1] ssid resource-measure
[FAT AP-wlan-st-1] service-template enable
[FAT AP-wlan-st-1] quit
```

WLAN-Radio 1/0/1 の radio interface view に移行します。

```
[FAT AP] interface wlan-radio 1/0/1
```

スペクトル管理を有効にします。

```
[FAT AP-WLAN-Radio1/0/1] spectrum-management enable
```

無線リソース計測を有効にします。

```
[FAT AP-WLAN-Radio1/0/1] resource-measure enable
```

すべての計測機能を有効にします。

```
[FAT AP-WLAN-Radio1/0/1] 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 partial に設定します。

```
[FAT AP-WLAN-Radio1/0/1] rm-capability mode partial
```

WLAN-Radio 1/0/1 インタフェースにサービステンプレートを設定します。

```
[FAT AP-WLAN-Radio1/0/1] service-template 1
[FAT AP-WLAN-Radio1/0/1] quit
```

III. 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。

```
[FAT AP] display wlan client
Total number of clients: 1

MAC address       Username     AP name     RID  IP address          VLAN ID
00ee-bd44-557f      N/A        ap1         1    1.1.1.1             1
```

#クライアントからの計測報告を表示します。

```
[FAT AP] display wlan measure-report interface wlan-radio 1/0/1
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**2-x-x** です。

11 章 チャネルスキャンの設定 11-1
11.1 概要 11-1
11.1.1 基本概念 11-1
11.1.2 動作メカニズム 11-1
11.2 チャネルスキャンの設定 11-2
11.2.1 スキャン期間の設定 11-2
11.2.2 最大サービス期間の設定 11-2
11.2.3 サービスアイドルタイムアウトの設定 11-2
11.2.4 チャネルスキャンのブラックリスト・ホワイトリストの設定 11-3
11.3 チャネルスキャンの設定例 11-3
11.3.1 相対的な優先転送の設定例 11-3
11.3.2 絶対的な優先転送の設定例 11-4

11章 チャネルスキャンの設定

11.1 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。AP 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。

11.1.1 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。

11.1.2 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。

たとえば図 11-1 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。

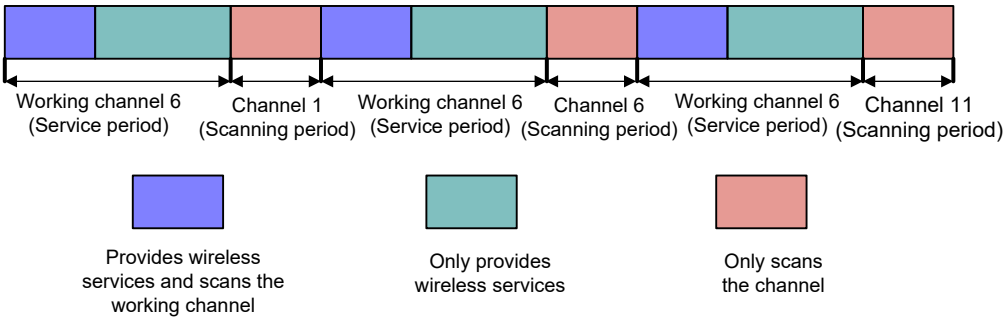


図 11-1 チャネルスキャンメカニズム

11.2 チャネルスキャンの設定

11.2.1 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． radio interface view に移行する	**interface wlan-radio** *interface-number*	—
3． 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。

11.2.2 最大サービス期間の設定

スキャンとサービスの両方の品質を確保するために、サービス期間の最大値を設定することができます。最大サービス期間に到達すると、AP は転送トラフィックの有無によらず、スキャンを開始します。無線サービスの品質を確保するためには、サービス期間を制限しないよう設定することを推奨します。AP はサービスアイドルタイムアウトの期限が切れるまではスキャン期間を開始しません。

最大サービス期間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． radio interface view に移行する	**interface wlan-radio** *interface-number*	—
3． 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： 5000ミリ秒

11.2.3 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。

サービスアイドルタイムアウト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． radio interface view に移行する	**interface wlan-radio** *interface-number*	—
3． 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： 100ミリ秒 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。

11.2.4 チャネルスキャンのブラックリスト・ホワイトリストの設定

AP にブラックリストを設定する場合、AP はブラックリスト内のチャネルをスキャンしません。AP にホワイトリストを設定する場合、AP はホワイトリスト内のチャネルのみスキャンします。同じ AP に対してブラックリストとホワイトリストの両方を設定することはできません。

チャネルスキャンのブラックリスト・ホワイトリス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． radio interface view に移行する	**interface wlan-radio** *interface-number*	—
3． 特定のチャネルをブラックリストに追加する	**scan channel blacklist** *channel-list*	デフォルト：設定なし
4． 特定のチャネルをホワイトリストに追加する	**scan channel whitelist** *channel-list*	デフォルト：設定なし

11.3 チャネルスキャンの設定例

11.3.1 相対的な優先転送の設定例

I. ネットワーク要件

図 11-2 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 に最大サービス期間を設定します。

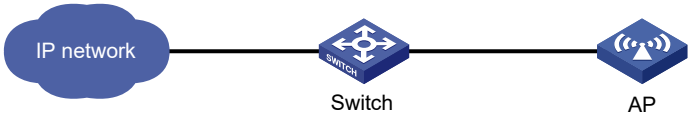


図 11-2 ネットワーク図

II. 設定手順

radio 1/0/2 の interface view に移行します。

```
<FAT AP> system-view
[FAT AP] interface wlan-radio 1/0/2
```

スキャン期間を 200 ミリ秒に設定します。

```
[FAT AP-WLAN-Radio1/0/2] scan scan-time 200
```

最大サービス期間を 5000 ミリ秒に設定します。

```
[FAT AP-WLAN-Radio1/0/2] 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。

```
[FAT AP-WLAN-Radio1/0/2] scan idle-time 100
```

11.3.2 絶対的な優先転送の設定例

I. ネットワーク要件

図 11-3 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 に対してサービス期間を制限しないようにします。

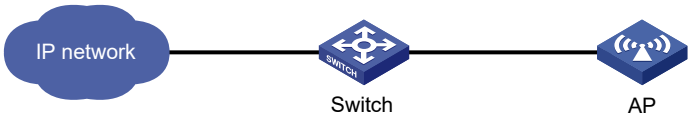


図 11-3 ネットワーク図

II. 設定手順

radio 1/0/2 の interface view に移行します。

```
<FAT AP> system-view
[FAT AP] interface wlan-radio 1/0/2
```

スキャン期間を 100 ミリ秒に設定します。

```
[FAT AP-WLAN-Radio1/0/2] 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。

```
[FAT AP-WLAN-Radio1/0/2] 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。

```
[FAT AP-WLAN-Radio1/0/2] scan idle-time 100
```

目次

このセクションのページは**2-x-x** です。

12 章 バンドナビゲーションの設定（FIT は未サポート） 12-1
12.1 概要 12-1
12.2 設定作業リスト 12-1
12.3 設定必須要件 12-1
12.4 バンドナビゲーションの設定 12-2
12.4.1 グローバルでのバンドナビゲーションの有効化 12-2
12.4.2 バンドナビゲーションに対するロードバランスの設定 12-2
12.4.3 バンドナビゲーションパラメータの設定 12-2
12.4.4 6GHz 無線のバンドナビゲーションの設定 12-3
12.5 バンドナビゲーションの設定例 12-4
12.5.1 バンドナビゲーションの設定 12-4
12.5.2 6GHz 無線のバンドナビゲーションの設定 12-5

12章 バンドナビゲーションの設定（FIT は未サポート）

12.1 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 12-1 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。

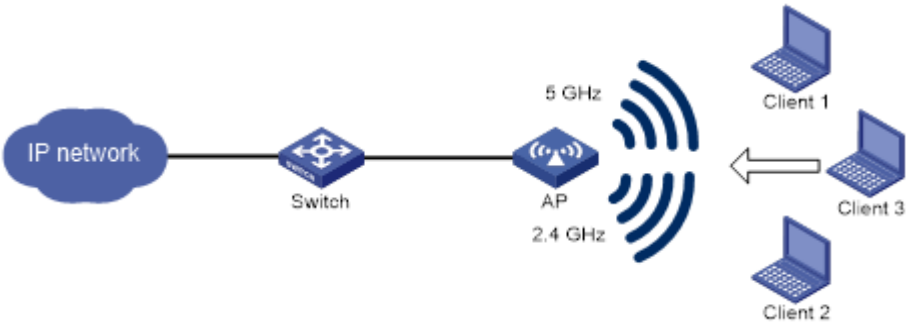


図 12-1 バンドナビゲーション

12.2 設定作業リスト

必須/オプション	作業リスト
必須	グローバルでのバンドナビゲーションの有効化
オプション	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	バンドナビゲーションパラメータの設定

12.3 設定必須要件

バンドナビゲーションの設定前に、以下を完了してください。

- クイックアソシエーションを無効にしてください。クイックアソシエーションに関する詳細は、オペレーションマニュアルのセクション 2 *WLAN “WLAN アクセスの設定”* を参照してください。
- 5GHz 無線と 2.4GHz 無線の両方が有効化され、無線に同じサービステンプレートが設定されていることを確認してください。

12.4 バンドナビゲーションの設定

WLAN 内の大半のクライアントが 2.4GHz バンドしかサポートしていない場合、またはトラフィック遅延に敏感な WLAN 内ではバンドナビゲーションを有効にしないでください。

12.4.1 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

12.4.2 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**	—
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

12.4.3 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 : APは5GHzアソシエーション要求を拒否しません。
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

12.4.4 6GHz 無線のバンドナビゲーションの設定

🕮 **メモ：**

6GHz 無線のバンドナビゲーションの設定は、ソフトウェアバージョン 7.5.105 を含む以降のソフトウェアからサポートしています。

6GHz 無線は無線ロードバランス用のバンドナビゲーションをサポートしています。

この機能を有効にすると、装置は 2.4GHz および 5GHz 無線の新しい 802.11v クライアントに BSS 移行メッセージを送信し、802.11v サービスで構成された 6GHz 無線に接続するように案内します。

BSS を切り替えるメッセージを受信した後、無線クライアントは BSS 移行アクションを実行するかどうかを自律的に決定します。

6GHz 無線のバンドナビゲーション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. 無線ロードバランス用のバンドナビゲーションを設定する	**wlan radio-load-balance band-navigation enable**	デフォルト：有効
3. Service template view に移行する	**wlan service-template** *service-template-name*	ー
4. BTM を有効にする	**bss transition-management enable**	デフォルト：無効

12.5 バンドナビゲーションの設定例

12.5.1 バンドナビゲーションの設定

I. ネットワーク要件

図 12-2 に示すように、5GHz 無線と 2.4GHz 無線の両方が FAT 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。

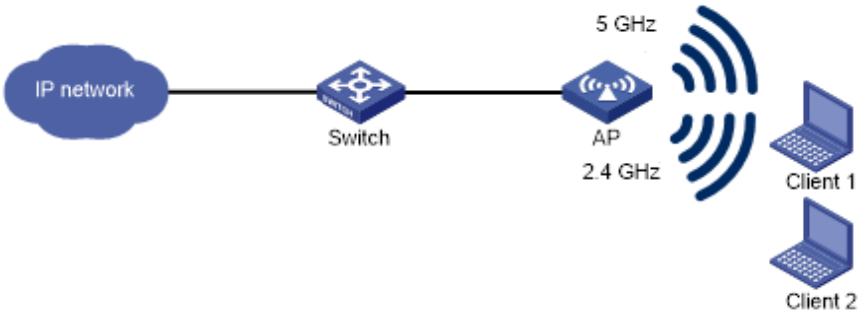


図 12-2 ネットワーク図

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。

```
<FAT AP> system-view
[FAT AP] wlan service-template 1
[FAT AP-wlan-st-1] ssid band-navigation
[FAT AP-wlan-st-1] service-template enable
[FAT AP-wlan-st-1] quit
```

WLAN-radio 1/0/1 の interface view に移行し、無線タイプを 802.11n （5 GHz）に設定します。

```
[FAT AP] interface wlan-radio 1/0/1
[FAT AP-WLAN-Radio1/0/1] type dot11an
```

サービステンプレート 1 を WLAN-radio 1/0/1 に設定します。

```
[FAT AP-WLAN-Radio1/0/1] service-template 1
[FAT AP-WLAN-Radio1/0/1] quit
```

WLAN-radio 1/0/3 の interface view に移行し、無線タイプを 802.11n （2.4 GHz）に設定します。

```
[FAT AP] interface wlan-radio 1/0/3
[FAT AP-WLAN-Radio1/0/3] type dot11gn
```

サービステンプレート 1 を WLAN-radio 1/0/3 に設定します。

```
[FAT AP-WLAN-Radio1/0/3] service-template 1
[FAT AP-WLAN-Radio1/0/3] quit
```

バンドナビゲーションをグローバルに有効化します。

```
[FAT AP] wlan band-navigation enable
```

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。

```
[FAT AP] 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。

```
[FAT AP] 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。

```
[FAT AP] wlan band-navigation rssi-threshold 30
```

クライアント情報エージングタイマを 160 秒に設定します。

```
[FAT AP] 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 に関連付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（詳細は省略します。）
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。）

12.5.2 6GHz 無線のバンドナビゲーションの設定

I. ネットワーク要件

図 12-3 に示すように、6GHz、5GHz、2.4GHz 無線が FAT AP 上で有効化されています。6GHz 無線のバンドナビゲーションを設定し、802.11v クライアントが接続されたときに 6GHz の無線に接続するように設定します。

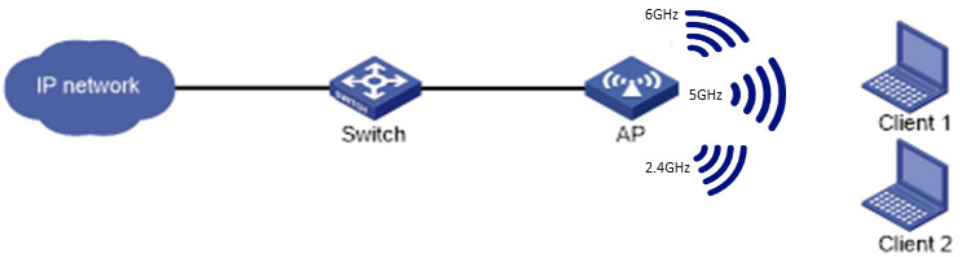


図 12-3 ネットワーク図

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。6GHz 無線のバンドナビゲーションを使用するため BTM を有効にします。

```
<FAT AP> system-view
[FAT AP] wlan service-template 1
[FAT AP-wlan-st-1] ssid band-navigation
[FAT AP-wlan-st-1] enhanced-open enable
[FAT AP-wlan-st-1] bss transition-management enable
[FAT AP-wlan-st-1] service-template enable
[FAT AP-wlan-st-1] quit
```

WLAN-radio 1/0/1 の interface view に移行し、サービステンプレート 1 を WLAN-radio 1/0/1 に設定します。

```
[FAT AP] interface WLAN-Radio 1/0/1
[FAT AP-WLAN-Radio1/0/1] service-template 1
[FAT AP-WLAN-Radio1/0/1] quit
```

WLAN-radio 1/0/2 の interface view に移行し、サービステンプレート 1 を WLAN-radio 1/0/1 に設定します。

```
[FAT AP] interface WLAN-Radio 1/0/2
[FAT AP-WLAN-Radio1/0/2] service-template 1
[FAT AP-WLAN-Radio1/0/2] quit
```

WLAN-radio 1/0/1 の interface view に移行し、サービステンプレート 1 を WLAN-radio 1/0/1 に設定します。

```
[FAT AP] interface WLAN-Radio 1/0/3
[FAT AP-WLAN-Radio1/0/3] service-template 1
[FAT AP-WLAN-Radio1/0/3] quit
```

6GHz 無線のバンドナビゲーションを有効化します。

```
[FAT AP] wlan radio-load-balance band-navigation enable
```

III. 設定の確認

6GHz 無線に対応するクライアントが AP に関連付けを要求したときに、6GHz 無線に関連付くことを確認します（詳細は省略します。）

目次

このセクションのページは **2-x-x** です。

13 章 スペクトル管理の設定（FIT は未サポート） 13-1
13.1 概要 13-1
13.2 スペクトル管理設定作業リスト 13-1
13.3 スペクトル管理の設定 13-1
13.3.1 スペクトル管理の有効化 13-1
13.3.2 電力制限モードの設定 13-1
13.3.3 チャネルスイッチモードの設定 13-2
13.3.4 伝送電力ケーパビリティマッチモードの設定 13-2
13.3.5 チャネルケーパビリティマッチモードの設定 13-3
13.4 スペクトル管理の設定例 13-4
13.4.1 スペクトル管理の設定例 13-4

13章 スペクトル管理の設定（FIT は未サポート）

13.1 概要

スペクトル管理は 802.11h に準拠しています。クライアントが 5GHz 帯で動作する際、制御要求を満たすように、スペクトル管理は 5GHz WLAN で使用されます。スペクトル管理機能により AP は、許可された最大伝送電力をクライアントに通知できます。クライアントの電力とチャネルが制御要求を満たさない場合、AP はそのクライアントからのアソシエーション要求を拒否できます。

13.2 スペクトル管理設定作業リスト

必須/オプション	作業リスト
オプション	スペクトル管理の有効化
オプション	電力制限モードの設定
オプション	チャネルスイッチモードの設定
オプション	伝送電力ケーパビリティマッチモードの設定
オプション	チャネルケーパビリティマッチモードの設定

13.3 スペクトル管理の設定

13.3.1 スペクトル管理の有効化

この機能は 5GHz 無線にのみ適用できます。

スペクトル管理を有効にする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． radio interface view に移行する	**interface wlan-radio** *interface-number*	—
3． スペクトル管理を有効化する	**spectrum-management enable**	デフォルト：無効

13.3.2 電力制限モードの設定

この機能は 5GHz 無線にのみ適用できます。

この機能により、AP に紐付いたクライアントが別の無線装置と干渉するのを防ぐために、クライアントの伝送電力を制限することができます。無線から電力制限値を含むビーコンフレームやプローブ応答を受信すると、クライアントはトラフィックを伝送するために新たなローカル最大伝送電力を使用します。新たなローカル最大電力は、チャネルに指定された最大伝送電力レベルから電力制限値を引いた値です。

無線に対して以下の電力制限モードを設定できます。

- **Manual**－電力制限値を手動で指定します。
- **Auto**－電力制限値を無線が自動で計算します。

電力制限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． radio interface view に移行する	**interface wlan-radio** *interface-number*	—
3． 電力制限モードを設定する	**power-constraint mode** { **auto** [**anpi-interval** *anpi-interval-value*] | **manual** *power-constraint* }	デフォルト：auto 電力制限モードは、スペクトル管理もしくは無線リソース管理が有効なときのみ適用されます。無線リソース管理の詳細は、オペレーションマニュアルのセクション2 *WLAN "WLAN無線リソースの計測の設定"* を参照してください。

13.3.3 チャネルスイッチモードの設定

無線が新たなチャネルに変更したとき、無線は紐付いたクライアントにチャネル切り替えの通知を送信します。通知には新たなチャネル番号と、クライアントがフレームの送信を継続できるかに関する情報が含まれます。

チャネルスイッチ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． radio interface view に移行する	**interface wlan-radio** *interface-number*	—
3． 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** チャネルの切り替え中、オンラインのクライアントはフレームの送信を停止します。

13.3.4 伝送電力ケーパビリティマッチモードの設定

クライアントは、事前に定義された一致基準に基づき無線と紐付くことができます。伝送電力ケーパビリティは、クライアントと無線が現在のチャネルでフレームを伝送できる最小/最大電力を参照します。装置は以下のクライアント電力ケーパビリティマッチモードをサポートします。

- **All**－クライアントの伝送電力ケーパビリティが、無線の伝送電力ケーパビリティとすべて一致する場合のみ、クライアントは無線への紐付けが許可されます。
- **None**－クライアントの伝送電力ケーパビリティはチェックされません。
- **Partial**－クライアントの伝送電力ケーパビリティが、無線の伝送電力ケーパビリティと 1 つでも一致する場合、クライアントは無線への紐付けが許可されます。

伝送電力ケーパビリティマッチ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． radio interface view に移行する	**interface wlan-radio** *interface-number*	—
3． 伝送電力ケーパビリティマッチモードを設定する	**power-capability mode** { **all** | **none** | **partial** }	デフォルト：**none** このモードは、スペクトル管理もしくは無線リソース管理が有効なときのみ適用されます。無線リソース管理の詳細は、オペレーションマニュアルのセクション2 *WLAN "WLAN無線リソースの計測の設定"* を参照してください。

13.3.5 チャネルケーパビリティマッチモードの設定

この機能は 5GHz 無線にのみ適用できます。

クライアントは、事前に定義された一致基準に基づき無線と紐付くことができます。チャネルケーパビリティは、クライアントと無線がそれぞれサポートするチャネルを参照します。装置は以下のクライアントチャネルケーパビリティマッチモードをサポートします。

- **All**－クライアントのサポートするチャネルが、無線のサポートするチャネルとすべて一致する場合のみ、クライアントは無線への紐付けが許可されます。
- **None**－クライアントのチャネルケーパビリティはチェックされません。
- **Partial**－クライアントのサポートするチャネルが、無線のサポートするチャネルと 1 つでも一致する場合、クライアントは無線への紐付けが許可されます。

チャネルケーパビリティマッチ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． radio interface view に移行する	**interface wlan-radio** *interface-number*	—
3． チャネルケーパビリティマッチモードを設定する	**channel-capability mode** { **all** | **none** | **partial** }	デフォルト：**none**

13.4 スペクトル管理の設定例

13.4.1 スペクトル管理の設定例

I. ネットワーク要件

図 13-1 に示すように、クライアントの伝送電力を制限し、チャネル切り替え中にクライアントがフレームの送信を継続できるようにスペクトル管理を設定します。

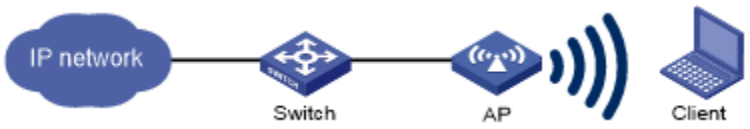


図13-1 ネットワーク図

II. 設定手順

スペクトル管理を有効にします。

```
<Fat AP> system-view
[Fat AP]  interface wlan-radio 1/0/2
[FAT AP-WLAN-Radio1/0/2] spectrum-management enable
```

チャネルケーパビリティマッチモードを partial に設定します。

```
[FAT AP-WLAN-Radio1/0/2] channel-capability mode partial
```

伝送電力ケーパビリティマッチモードを all に設定します。

```
[FAT AP-WLAN-Radio1/0/2] power-capability mode partial
```

電力制限モードを manual に設定し、電力制限値を 5dBm に設定します。

```
[FAT AP-WLAN-Radio1/0/2] power-constraint mode manual 5
```

チャネルスイッチモードを continuous に設定します。

```
[FAT AP-WLAN-Radio1/0/2] channel-switch mode continuous
```

III. 設定の確認

クライアントが無線との紐付けに成功するか確かめるために **display wlan client** コマンドを実行します。（詳細は省略します。）

目次

このセクションのページは **2-x-x** です。

14 章 WLAN 最適化（FIT は未サポート） 14-1
14.1 概要 14-1
14.2 制限事項とガイドライン:WLAN 最適化設定 14-1
14.3 AP トリガのクライアント再関連付けの設定 14-1
14.4 AP のトラフィックスケジューリングモードの設定 14-2
14.5 隠れ端末保護の設定 14-2
14.6 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 14-3
14.7 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 14-3
14.8 クライアント高速キープアライブの設定 14-4

14章 WLAN 最適化（FIT は未サポート）

14.1 概要

WLAN 導入時の適切なチャン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、重複しないチャンネル数に対し、WLAN デバイス数は常に増加するため、チャンネル重複,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。

14.2 制限事項とガイドライン:WLAN最適化設定

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、チャン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。

14.3 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

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． radio interface view に移行する	**interface wlan-radio** *interface-number*	－

操作	コマンド	補足
3. 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

14.4 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 7.5.129 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、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、指定したスケジューリングモードに基づいて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

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. radio interface view に移行する	**interface wlan-radio** *interface-number*	—
3. 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

14.5 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

隠れ端末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. radio interface view に移行する	**interface wlan-radio** *interface-number*	―
3. 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

14.6 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

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. 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：無効

14.7 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フェース経由で転送するレートを制限します。

II. 設定手順

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. 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
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値を設定する	**rrop anti-bmc { broadcast | multicast } rate-limit pps** *max-pps*	デフォルト：制限なし

14.8 クライアント高速キープアライブの設定

🕮 **メモ：**

rrop client fast-keep-alive コマンドはソフトウェアバージョン 7.5.129 を含む以降のソフトウェアからサポートしています。ソフトウェアバージョン 7.5.129 より前では本機能がデフォルトのパラメータ値で動作しており、無効にすることはできません。

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

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. radio interface view へ移行する	**interface wlan-radio** *interfacenumber*	―
3. 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 1024、interval 10)

目次

このセクションのページは**2-x-x** です。

15 章 WLAN IP スヌーピング（FIT は未サポート） 15-1
15.1 概要 15-1
15.1.1 クライアント IPv4 アドレス学習 15-1
15.2 WLAN IP スヌーピング設定作業リスト 15-1
15.3 ARP パケットスヌーピングの無効化 15-1
15.4 DHCPv4 パケットスヌーピングの無効化 15-2

15章 WLAN IP スヌーピング（FIT は未サポート）

15.1 概要

WLAN IP snooping により、AP が ARP、DHCP、ND、HTTP パケットのスヌーピングによってクライアントの IP アドレスを学習し、クライアントの IP アドレス、MAC アドレス、学習方法、を記録するスヌーピングエントリを作成することが可能になります。

エントリは 802.1X および MAC 認証クライアントのアカウンティングのために AAA により使用されるか、または、クライアントパケットを転送すべきかを IP ソースガードが決定するために使用されます。

15.1.1 クライアント IPv4 アドレス学習

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。
  DHCP 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 5 *IP サービス* を参照してください。
- 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。
  ARP 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 5 *IP サービス "ARP"* を参照してください。

IP アドレスを学習する優先度は DHCPv4 パケット、ARP パケットの順番で行われます。

15.2 WLAN IPスヌーピング設定作業リスト

作業リスト
（オプション設定項目）ARPパケットスヌーピングの無効化
（オプション設定項目）DHCPv4パケットスヌーピングの無効化

15.3 ARPパケットスヌーピングの無効化

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、view に移行する	**wlan service-template** *service-template-name*	—
3． ARP パケットスヌーピングを無効化する	**undo client ipv4-snooping arp-learning enable**	デフォルト：有効

15.4 DHCPv4パケットスヌーピングの無効化

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、view に移行する	**wlan service-template** *service-template-name*	—
3． DHCPv4 パケットスヌーピングを無効化する	**undo client ipv4-snooping dhcp-learning enable**	デフォルト：有効

目次

このセクションのページは **2-x-x** です。

16 章 Web リダイレクトの設定 16-1
16.1.1 Web リダイレクトについて 16-1
16.1.2 Web リダイレクトの設定 16-1

16章 Web リダイレクトの設定

16.1.1 Web リダイレクトについて

Web リダイレクトは、簡略化されたポータル機能です。Web リダイレクトでは、ユーザはポータル認証を実行せず、ブラウザでの最初の Web アクセス試行時に、指定された URL に直接リダイレクトされます。指定されたリダイレクト間隔が経過すると、ユーザは訪問中の Web サイトから指定された URL に再度リダイレクトされます。

Web リダイレクトは、ISP に拡張サービスを提供できます。たとえば、ISP は、リダイレクトされた Web ページに広告を配置し、情報を公開できます。

16.1.2 Web リダイレクトの設定

🕮 **メモ：**

- Web リダイレクトの機能は、デフォルトのポート番号 80 を使用する HTTP パケットに対してのみ有効です。

以下に、Web リダイレク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. 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で Web リダイレクトを設定する	**web-redirect url** *url-string* [**interval** *interval*]	デフォルト　：無効 デフォルト間隔：86400秒

目次

このセクションのページは**2-x-x** です。

17章 WLAN メッシュの設定（FITは未サポート） 17-1
17.1 概要 17-1
17.1.1 WLANメッシュネットワーク 17-1
17.1.2 メッシュプロファイル 17-2
17.1.3 ネイバ検出とメッシュリンク確立 17-2
17.1.4 無線配置システム 17-3
17.1.5 メッシュピアブラックリスト、ホワイトリスト 17-5
17.1.6 プロトコルと標準 17-5
17.2 WLANメッシュ設定作業リスト 17-6
17.3 メッシュプロファイルの設定 17-6
17.4 無線インタフェースへのメッシュプロファイルのバインド 17-7
17.5 メッシュポリシーの設定 17-7
17.6 無線インタフェースへのメッシュポリシーのバインド 17-8
17.7 メッシュピアブラックリスト・ホワイトリストの設定 17-9
17.8 メッシュインタフェースの設定 17-9
17.8.1 メッシュインタフェースの作成 17-9
17.8.2 無線インタフェースへのメッシュインタフェースのバインド 17-10
17.9 スパニングツリー機能の有効化 17-10
17.10 WLANメッシュのための表示と保守コマンド 17-11
17.11 WLANメッシュ設定例 17-11
17.11.1 WLANメッシュの設定例 17-11
17.11.2 Point-to-point WDSの設定例 17-14
17.11.3 環状トポロジの設定例 17-15

17章 WLAN メッシュの設定（FIT は未サポート）

🕮 **メモ：**

- QX-W1200 シリーズでは、WLAN メッシュの設定は、ソフトウェアバージョン 7.5.114 を含む以降のソフトウェアからサポートしています。
- WLAN メッシュ機能は、同じシリーズ、かつ、同じソフトウェアバージョンの装置同士の接続のみサポートしています。
- WLAN メッシュ機能を設定した Radio には、WIPS 機能を設定しないことを推奨します。

17.1 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。

🕮 **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。

17.1.1 WLAN メッシュネットワーク

図17-1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。

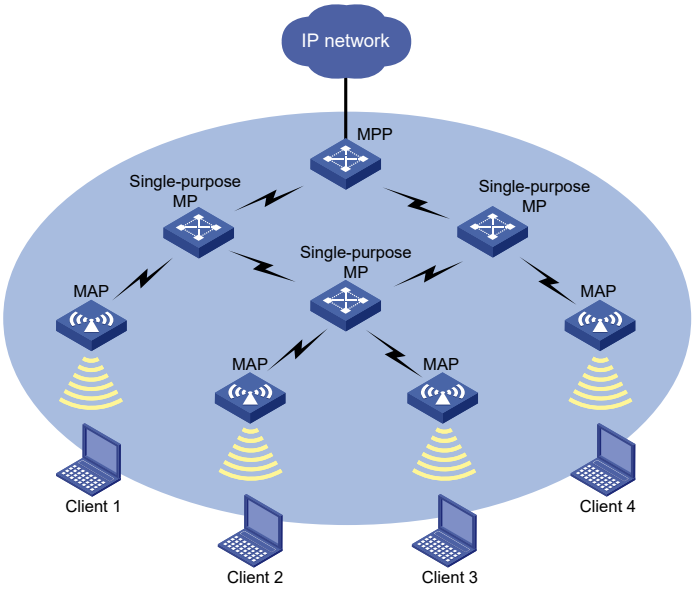


図17-1 WLAN メッシュネットワーク図

17.1.2 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ー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 間隔ー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 は、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。

17.1.3 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**ー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**ー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17-2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。

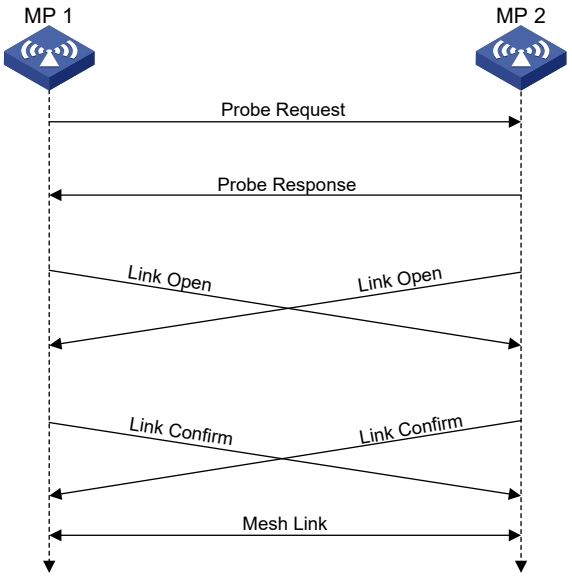


図17-2 ネイバ検出と WLAN メッシュネットワークでのメッシュリンク確立

17.1.4 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。

- Point-to-point トポロジ

図17-3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17-3 WDS point-to-point トポロジ

- スタートポロジ

図17-4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。

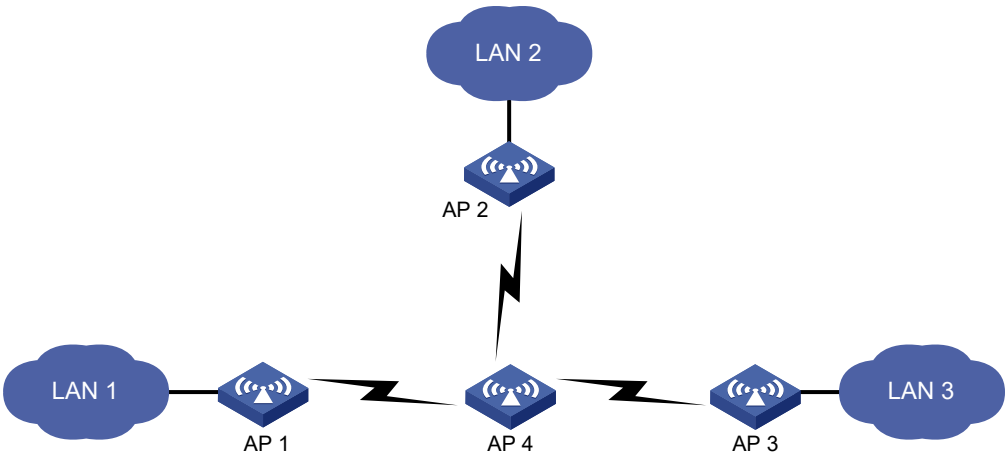


図17-4 スタートポロジ

- 自動ネイバ検出で作成されたトポロジ

接続する AP をピアメッシュホワイトリストで指定しない場合、WDS トポロジは自動ネイバ検出の結果に依存し、検出された AP 間でメッシュリンクが確立されます。

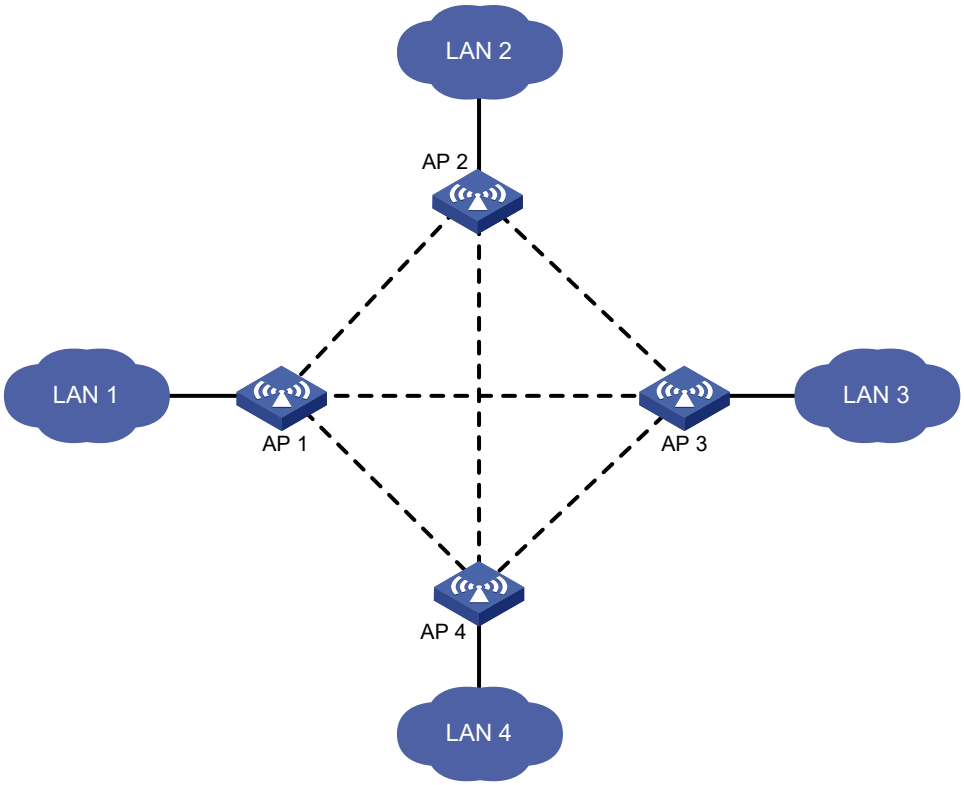


図17-5 自動トポロジ設定

17.1.5 メッシュピアブラックリスト、ホワイトリスト

ネイバ MP 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 とのみ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 とはメッシュリンクを確立できません。

17.1.6 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

17.2 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）無線インタフェース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）無線インタフェース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）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 ● メッシュインタフェースの作成 ● ラジオへのメッシュインタフェースのバインド	ー
（オプション設定項目）スパニングツリー機能の有効化	環状のトポロジを構成する場合、環状トポロジを構成するすべてのMPでこの作業を実施します。

17.3 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**	—
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

操作	コマンド	補足
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

17.4 無線インタフェース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

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. 無線インタフェースの view に移行する	**interface wlan-radio** *interface-number*	—
3. 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：バインドなし

17.5 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

操作	コマンド	補足
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）リンクレートモードを設定する	**link-rate-mode** { **fixed** | **real-time** }	デフォルト：fixedモード fixedモード：メッシュリンクのインタフェースレートは、無線インタフェースレートの現在の設定の最大値で固定されます。 real-timeモード: メッシュリンクのインタフェースレートは、自動でRSSIに適応します。
7. （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

17.6 無線インタフェース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インタフェース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。無線インタフェース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

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. 無線インタフェースの view に移行する	**interface wlan-radio** *interface-number*	—
3. 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: 無線インタフェース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。

17.7 メッシュピアブラックリスト・ホワイトリストの設定

I. メッシュピアブラックリスト・ホワイトリストの設定

本機能を設定すると、メッシュピアブラックリストに追加された装置とはメッシュリンクを確立しない、あるいはメッシュピアホワイトリストに追加された装置のみとメッシュリンクを確立します。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. 無線インタフェースの view に移行する	**interface wlan-radio** *interface-number*	—
3. 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MP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。

17.8 メッシュインタフェースの設定

17.8.1 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。VLAN1 以外で通信する場合、メッシュインタフェースを作成して任意の VLAN を割り当てる必要があります。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. 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

17.8.2 無線インタフェース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

1 つの無線インタフェースにバインドできるメッシュインタフェースは 1 つだけです。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. 無線インタフェースの view に移行する	**interface wlan-radio** *interface-number*	—
3. 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：設定なし

17.9 スパニングツリー機能の有効化

I. 制限とガイドライン

図17-5のような環状のトポロジを構成する場合、環状トポロジを構成するすべての MP でスパニングツリー機能を有効にしてください。スパニングツリー機能を有効にしない場合、ループが発生します。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. スパニングツリー機能を有効にする	**stp global enable**	デフォルト：設定なし

17.10 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** [**mesh-profile** *mesh-profile-number* | **interface** *interface-type interface-number* | **peer-mac-address** *mac-address*]
メッシュプロファイル情報を表示する	**display wlan mesh-profile** [*mesh-profile-number*]
メッシュポリシー情報を表示する	**display wlan mesh-policy** [*mesh-policy-name*]

17.11 WLANメッシュ設定例

17.11.1 WLAN メッシュの設定例

I. ネットワーク設定

図17-6にネットワーク図を示します。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。

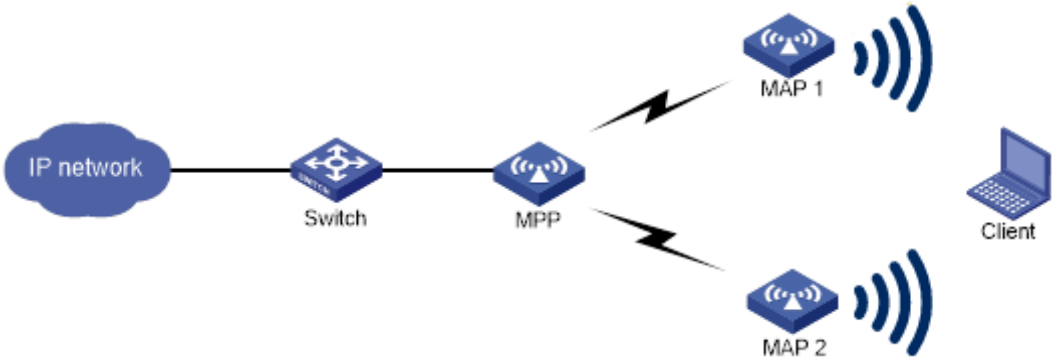


図17-6 ネットワーク図

II. 設定手順

1) MPP を設定します。

メッシュプロファイルを作成します。

```
<MPP> system-view
[MPP] wlan mesh-profile 1
```

メッシュ ID を 1 に設定します。

```
[MPP-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。

```
[MPP-wlan-mesh-profile-1] akm mode sae
```

事前共有鍵を設定します。

```
[MPP-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。

```
[MPP-wlan-mesh-profile-1] mesh-profile enable
[MPP-wlan-mesh-profile-1] quit
```

メッシュプロファイルを無線インタフェース WLAN-Radio 1/0/2 にバインドします。

```
[MPP] interface wlan-radio 1/0/2
[MPP-WLAN-Radio1/0/2] mesh-profile 1
```

無線インタフェースで無線タイプを 802.11n (5GHz)に設定します。

```
[MPP-WLAN-Radio1/0/2] type dot11an
```

無線の作動チャネルを 36 に設定します。

```
[MPP-WLAN-Radio1/0/2] channel 36
```

ラジオを有効にします。

```
[MPP-WLAN-Radio1/0/2] undo shutdown
[MPP-WLAN-Radio1/0/2] quit
```

2) MAP1 を設定します。

メッシュプロファイルを作成します。

```
<MAP1> system-view
[MAP1] wlan mesh-profile 1
```

メッシュ ID を 1 に設定します。

```
[MAP1-wlan-mesh-profile-1] mesh-id 1
```

認証と鍵管理に対して SAE を設定します。

```
[MAP1-wlan-mesh-profile-1] akm mode sae
```

MPP と同じ事前共有鍵を設定します。

```
[MAP1-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。

```
[MAP1-wlan-mesh-profile-1] mesh-profile enable
[MAP 1-wlan-mesh-profile-1] quit
```

サービステンプレートを設定します。

```
[MAP1] wlan service-template service1
[MAP1-wlan-st-service1] ssid mesh-network
[MAP1-wlan-st-service1] service-template enable
```

```
[MAP1-wlan-st-service1] quit
```

無線インタフェース WLAN-Radio 1/0/2 にメッシュプロファイルをバインドします。

```
[MAP1] interface wlan-radio 1/0/2
[MAP1-WLAN-Radio1/0/2] mesh-profile 1
```

無線インタフェース WLAN-Radio 1/0/2 にサービステンプレートをバインドします。

```
[MAP1-WLAN-Radio1/0/2] service-template service1
```

無線インタフェースで無線タイプを 802.11n (5GHz)に設定します。

```
[MAP1-WLAN-Radio1/0/2] type dot11an
```

無線の作動チャネルを 36 に設定します。

```
[MAP1-WLAN-Radio1/0/2] 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。

```
[MAP1-WLAN-Radio1/0/2] mesh peer-mac-address 4a1b-517d-23ff
```

ラジオを有効にします。

```
[MAP1-WLAN-Radio1/0/2] undo shutdown
[MAP1-WLAN-Radio1/0/2] quit
[MAP1] quit
```

3) MAP1 と同様に MAP2 を設定します。（詳細は省略します。）

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。

```
<MPP> display wlan mesh-link
 Peer MAC       RSSI BSSID          Interface        Link state Online time
 7b2d-23bb-e56f 22   4a1b-517d-23ff WLAN-MeshLink1   Active     00h 08m 31s
 6a3b-cc5a-e215 22   4a1b-517d-23ff WLAN-MeshLink2   Active     00h 40m 56s
```

MAP1 が MPP とメッシュリンクを確立することを確認します。

```
<MAP1> display wlan mesh-link
 Peer MAC       RSSI BSSID          Interface        Link state Online time
 4a1b-517d-23ff 22   7b2d-23bb-e56f WLAN-MeshLink1   Active     00h 08m 31s
```

MAP2 が MPP とメッシュリンクを確立することを確認します。

```
<MAP2> display wlan mesh-link
 Peer MAC       RSSI BSSID          Interface        Link state Online time
 4a1b-517d-23ff 22   6a3b-cc5a-e215 WLAN-MeshLink1   Active     00h 08m 31s
```

17.11.2 Point-to-point WDS の設定例

I. ネットワーク設定

図17-7に示すように、2 つの LAN 間にレイヤ 2 無線接続を提供するために、2 台の AP を point-to-point WDS として配置します。チャネル 36 で WDS リンクを確立するため、802.11a を使用するように AP を設定します。



図17-7 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。

```
<AP1> system-view
[AP1] wlan mesh-profile 1
```

メッシュ ID を 1 に設定します。

```
[AP1-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。

```
[AP1-wlan-mesh-profile-1] akm mode sae
```

事前共有鍵を設定します。

```
[AP1-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。

```
[AP1-wlan-mesh-profile-1] mesh-profile enable
[AP 1-wlan-mesh-profile-1] quit
```

無線インタフェース WLAN-Radio 1/0/2 にメッシュプロファイルをバインドします。

```
[AP1] interface wlan-radio 1/0/2
[AP1-WLAN-Radio1/0/2] mesh-profile
```

無線インタフェースで無線タイプを 802.11a に設定します。

```
[AP1-WLAN-Radio1/0/2] type dot11a
```

無線の作動チャネルを 36 に設定します。

```
[AP1-WLAN-Radio1/0/2] channel 36
```

ラジオを有効にします。

```
[AP1-WLAN-Radio1/0/2] undo shutdown
```

```
[AP1-WLAN-Radio1/0/2] quit
[AP1] quit
```

2) AP1 と同様に AP2 を設定します。（詳細は省略します。）

III. 設定の確認

AP1 のメッシュリンク情報を表示します。

```
<AP1> display wlan mesh-link
Nbr-Mac        RSSI BSSID          Interface         Linkstate Uptime(hh:mm:ss)
482b-c01d-e87f 22   a503-cc9b-418f WLAN-MeshLink1    Active    00:01:10
```

AP2 のメッシュリンク情報を表示します。

```
<AP2> display wlan mesh-link
Nbr-Mac        RSSI BSSID          Interface         Linkstate Uptime(hh:mm:ss)
a503-cc9b-418f 22   482b-c01d-e87f WLAN-MeshLink1    Active    00:01:10
```

17.11.3 環状トポロジの設定例

I. ネットワーク設定

図17-8に示すように、4 つの LAN 間にレイヤ 2 無線接続を提供するために、4 台の AP を配置します。チャネル 36 で WDS リンクを確立するため、802.11a を使用するように AP を設定します。

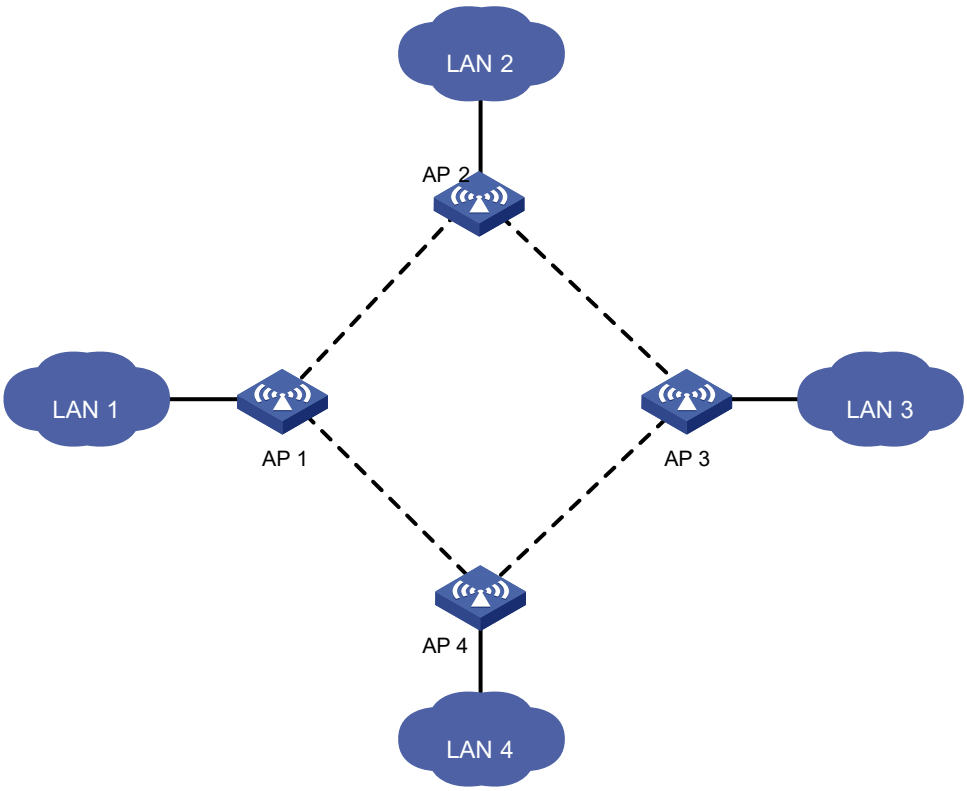


図17-8 ネットワーク図

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。

```
<AP1> system-view
[AP1] wlan mesh-profile 1
```

メッシュ ID を 1 に設定します。

```
[AP1-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。

```
[AP1-wlan-mesh-profile-1] akm mode sae
```

事前共有鍵を設定します。

```
[AP1-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。

```
[AP1-wlan-mesh-profile-1] mesh-profile enable
[AP 1-wlan-mesh-profile-1] quit
```

メッシュインタフェース 1 を作成します。

```
[AP1] interface wlan-mesh 1
[AP1-WLAN-Mesh1] quit
```

無線インタフェース WLAN-Radio 1/0/2 にメッシュプロファイルをバインドします。

```
[AP1] interface wlan-radio 1/0/2
[AP1-WLAN-Radio1/0/2] mesh-profile 1
```

無線インタフェース WLAN-Radio 1/0/1 にメッシュインタフェースをバインドします。

```
[AP1-WLAN-Radio1/0/2] mesh-interface 1
```

無線インタフェースで無線タイプを 802.11a に設定します。

```
[AP1-WLAN-Radio1/0/2] type dot11a
```

無線の作動チャネルを 36 に設定します。

```
[AP1-WLAN-Radio1/0/2] channel 36
```

AP2 と AP4 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。AP1 は AP2 と AP4 とのみメッシュリンクを確立できます。

```
[MAP1-WLAN-Radio1/0/2] mesh peer-mac-address 9ce8-9525-f2e0
[MAP1-WLAN-Radio1/0/2] mesh peer-mac-address 9ce8-9525-fee0
```

ラジオを有効にします。

```
[AP1-WLAN-Radio1/0/2] undo shutdown
[AP1-WLAN-Radio1/0/2] quit
```

```
[AP1] quit
```

グローバルでスパニングツリーを有効にします。

```
[AP1] stp global enable
```

2) AP1 と同様に AP2, AP3, AP4 を設定します。ただし、ホワイトリストの設定は AP により異なります。隣接する AP（AP2 : AP1, AP3 、AP3 : AP2, AP4、AP4 : AP1, AP3 ）の MAC アドレスを設定してください。（詳細は省略します。）

III. 設定の確認

AP1 のメッシュリンク情報を表示します。

```
<AP1> display wlan mesh-link
Peer MAC       RSSI BSSID          Interface         Link state       Online time
 9ce8-9525-f2e0 57   74ea-c8fd-bfd0 WLAN-MeshLink3    Active(an)      00h 18m 11s
 9ce8-9525-fee0 62   74ea-c8fd-bfd0 WLAN-MeshLink6    Active(an)      00h 11m 12s
```

AP2 のメッシュリンク情報を表示します。

```
<AP2> display wlan mesh-link
Peer MAC       RSSI BSSID          Interface         Link state       Online time
 74ea-c8fd-bfd0 62   9ce8-9525-f2e0 WLAN-MeshLink3    Active(an)      00h 18m 55s
 9ce8-9525-f370 54   9ce8-9525-f2e0 WLAN-MeshLink6    Active(an)      00h 07m 51s
```

AP3 のメッシュリンク情報を表示します。

```
<AP3> display wlan mesh-link
Peer MAC       RSSI BSSID          Interface         Link state       Online time
 9ce8-9525-f2e0 53   9ce8-9525-f370 WLAN-MeshLink4    Active(an)      00h 09m 40s
 9ce8-9525-fee0 57   9ce8-9525-f370 WLAN-MeshLink5    Active(an)      00h 07m 37s
```

AP4 のメッシュリンク情報を表示します。

```
<AP4> display wlan mesh-link
Peer MAC       RSSI BSSID          Interface         Link state       Online time
 74ea-c8fd-bfd0 70   9ce8-9525-fee0 WLAN-MeshLink3    Active(an)      00h 13m 08s
 9ce8-9525-f370 58   9ce8-9525-fee0 WLAN-MeshLink5    Active(an)      00h 06m 59s
```

目次

このセクションのページは**2-x-x** です。

18 章 WLAN 無線ロードバランス（FIT は未サポート） 18-1
18.1 概要 18-1
18.1.1 ネットワークスキーム 18-1
18.1.2 無線ロードバランスのモードとタイプ 18-1
18.2 制限とガイドライン 18-2
18.3 5GHz 無線ロードバランス機能 18-2

18章 WLAN 無線ロードバランス（FIT は未サポート）

18.1 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。

18.1.1 ネットワークスキーム

図 18-1 に示すように同じ AP の Radio1 と Radio2 が有効になっています。2 つの 5GHz 無線で同じ SSID を使用している場合、WLAN 無線ロードバランスを使用することで、Client4 が Radio1 に接続するのを避け、Radio2 への接続に誘導します。

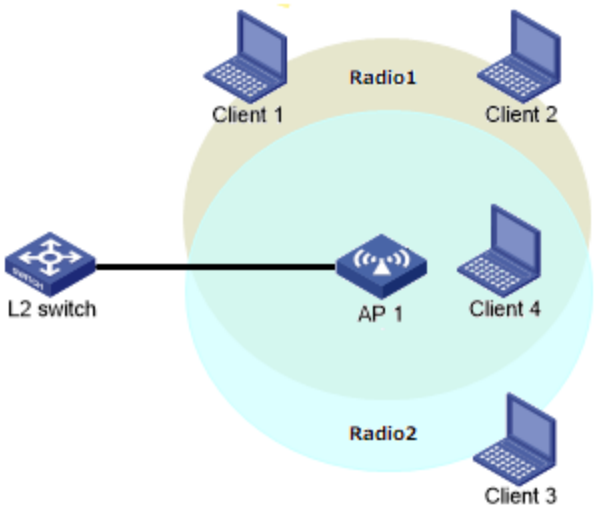


図 18-1 ネットワーク図

18.1.2 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

⚠ **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。

18.2 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。

WLAN 無線ロードバランスとバンドナビゲーションは、互いに排他的です。バンドナビ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 2 *WLAN “バンドナビゲーションの設定”* を参照してください。

18.3 5GHz無線ロードバランス機能

🕮 **メモ：**
この機能は QX-W1240 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
1． system view に移行する	**system-view**	—
2． 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*]] } [**force-logoff**]	デフォルト有効

QX-W1200 シリーズ アクセスポイント

オペレーションマニュアル

3. 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-Ethernet インタフェース

02-ループバックインタフェースと Null インタフェース

03-Interface range

目次

このセクションのページは**3-x-x** です。

1 章 Ethernet インタフェース 1-1
1.1 Ethernet インタフェースの共通設定 1-1
1.1.1 Ethernet インタフェースの基本設定 1-1
1.1.2 ジャンボフレームの設定 1-2
1.1.3 統計情報のポーリング間隔の設定 1-3
1.1.4 ストーム抑制機能の設定 1-4
1.2 Ethernet インタフェースの表示および維持 1-5

1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。

1.1 Ethernetインタフェースの共通設定

1.1.1 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。

- **全二重モード**：パケットを同時に送受信することができます。
- **半二重モード**：パケットの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**：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。

I. Ethernet インタフェースの設定 (ポート 1)

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 Ten-GigabitEthernet 1/0/1**	―
3． 説明を設定する	**description** *text*	デフォルト：Ten-GigabitEthernet 1/0/1 Interface
4． 通信モードを設定する	**duplex** { **auto** | **full** | **half** }	デフォルト：auto
5． 通信速度を設定する	**speed** { **100** | **1000** | **2500** | **5000** | **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**	―

II. Ethernet インタフェースの設定 (ポート 2)

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 Gigabit-Ethernet 1/0/2**	―
3． 説明を設定する	**description** *text*	デフォルト：GigabitEthernet 1/0/2 Interface
4． 通信モードを設定する	**duplex** { **auto** | **full** | **half** }	デフォルト：auto
5． 通信速度を設定する	**speed** { **10** | **100** | **1000** | **auto** }	デフォルト：auto
6． Ethernet インタフェースを有効にする	**undo shutdown**	―

1.1.2 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：1600バイト

1.1.3 統計情報のポーリング間隔の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． Ethernet interface view に移行する	**interface** *interface-type interface-number*	ー
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

設定したポーリング間隔によって収集された統計情報を表示するには、**display interface** コマンドを使用します。

1.1.4 ストーム抑制機能の設定

I. ストーム抑制機能

ストーム抑制機能により、特定のタイプのトラフィック(ブロードキャスト、またはマルチキャスト)のサイズがインタフェースのしきい値を超えないようにします。インタフェース上のブロードキャストまたはマルチキャストがこのしきい値を超えると、トラフィックがこのしきい値を下回るまで、システムはパケットを廃棄します。

II. 設定手順

以下にストーム抑制の設定を示します。

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． ブロードキャストパケット転送抑制を設定し、しきい値を設定する	**broadcast-suppression { ratio | pps** *max-pps* **| kbps** *max-kbps* **}**	デフォルト：無効
4． マルチキャストパケット転送抑制を設定し、しきい値を設定する	**multicast-suppression { ratio | pps** *max-pps* **| kbps** *max-kbps* **}**	デフォルト：無効

1.2 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**]]
指定されたEthernetインタフェースで破棄したパケットの情報を表示する	**display packet-drop** { **interface** [*interface-type* [*interface-number*]] | **summary** }
Ethernet統計情報を表示する	**display ethernet statistics slot** *slot-number*
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**3-x-x** です。

2 章 ループバックインタフェースと Null インタフェース 2-1
2.1 ループバックインタフェースの設定 2-1
2.2 Null インタフェースの設定 2-1
2.3 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 2-2

2章 ループバックインタフェースと Null インタフェース

本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。

2.1 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。

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 **LoopBack1 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

2.2 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。

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

2.3 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**3-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* | *interface-number.subnumber* } 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*]

QX-W1200 シリーズ アクセスポイント

オペレーションマニュアル

4. 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-MAC アドレステーブル

02-リンクアグリゲーション

03-VLAN

04-STP

05-ループ検出

06-LLDP

目次

このセクションのページは**4-x-x** です。

1 章 MAC アドレステーブル 1-1
1.1 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 1-3
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 1-4
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 1-5
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 1-6
1.9 MAC アドレステーブルの SNMP 通知の有効化 1-7
1.10 MAC アドレステーブルの表示と維持 1-8

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(または egress RB)、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
（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

操作	コマンド	補足
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**	―
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*	―
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**	―
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**	―
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*	―
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**	―
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*	―
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 のループが発生してい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。
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、オペレーションマニュアルのセクション 10 *システム管理 "SNMP"、"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**
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**

目次

このセクションのページは**4-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
2.1.1 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
2.1.2 アグリゲーショングループのメンバポートの状態 2-1
2.1.3 オペレーショナルキー 2-2
2.1.4 コンフィグレーションタイプ 2-2
2.1.5 リンクアグリゲーションモード 2-3
2.1.6 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
2.1.7 アグリゲーショングループの負荷分散 2-4
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 設定の制限とガイドライン 2-5
2.3.2 アグリゲーショングループの設定 2-6
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
2.4.3 アグリゲートインタフェースのシャットダウン 2-7
2.5 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
2.5.1 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 2-8
2.5.2 グループ単位でのロードシェアリングモードの設定 2-8
2.6 リンクアグリゲーションの表示と維持 2-8
2.7 リンクアグリゲーションの設定例 2-9
2.7.1 スタティックアグリゲーション設定例 2-9

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。

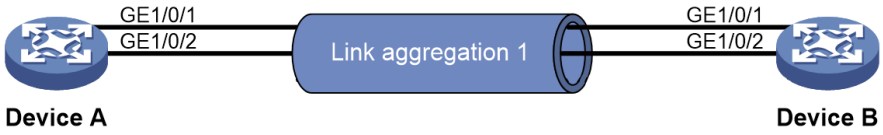


図 2-1 リンクアグリゲーション図

2.1.1 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。アグリゲーショングループのメンバポートの状態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 4 *アクセス　“リンクアグリゲーション”* の *“アグリゲーショングループのメンバポートの状態”* を参照してください。

2.1.2 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。
- **Individual**：通常の物理ポートのようにトラフィックを転送できます。ポートは以下の状況にある場合、Individual 状態になります。
  - アグリゲートインタフェースがエッジアグリゲートインタフェースとして設定されている
  - ポートが Link Aggregation Control Protocol Data Units (LACPDUs) をピアのポートから受信していない

2.1.3 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。

2.1.4 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
ポートアイソレーション	• アイソレーションの設定有無
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、オペレーションマニュアルのセクション4 *アクセス “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。

2.1.5 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。

🕮 **メモ：**

- 本装置はダイナミックアグリゲーションモードをサポートしておりません。

2.1.6 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) 全二重/高速
3) 全二重/低速
4) 半二重/高速
5) 半二重/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。

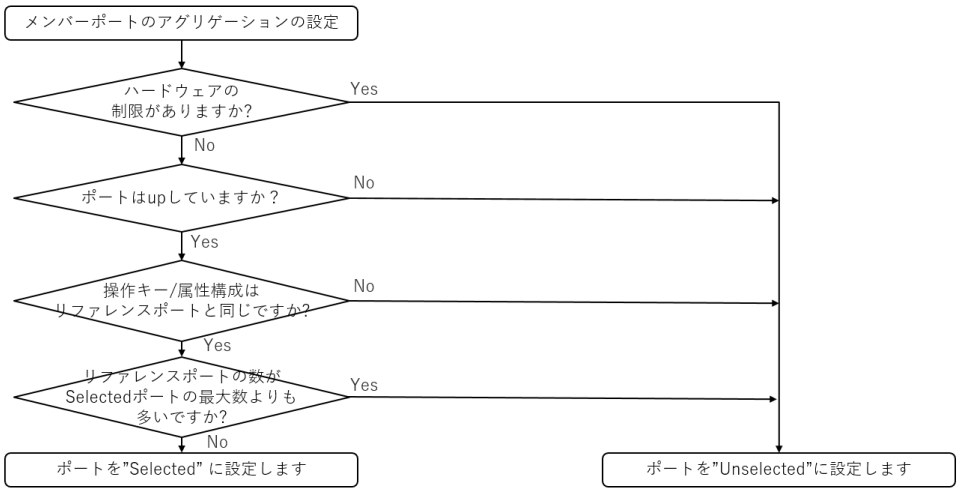


図 2-2 スタティックアグリゲーショングループのアグリゲーション状態の設定

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。

2.1.7 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 • アグリゲーショングループのSelectedポートの最小と最大数の設定 • 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）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

この章ではアグリゲーショングループの設定方法について説明します。

2.3.1 設定の制限とガイドライン

I. アグリゲーションメンバインタフェースの制限

インタフェースで表 2-2 に示す機能が設定されている場合、アグリゲーショングループにインタフェースを割り当てることができません。

表 2-2 アグリゲーションメンバインタフェースで設定できない機能

インタフェースの機能	参照
MACアドレス認証	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* *“MACアドレス認証”* を参照してください。
802.1X	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* *“802.1X”* を参照してください。

II. 設定の整合性の要件

- アグリゲーションリンクのエンド間に同じアグリゲーションモードを設定する必要があります。
- スタティックアグリゲーションを正常に動作させるには、各アグリゲーションリンクポートの両端に同じアグリゲーション状態を設定する必要があります。
- アグリゲートインタフェースを削除すると、アグリゲーショングループも削除され、すべてのメンバポートがアグリゲーショングループから削除されます。

2.3.2 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**	ー
2. aggregate interface view に移行する	**interface bridge-aggregation** *interface-number*	ー
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。

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。

2.4.3 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**

2.5 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。

2.5.1 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** | **source-ip** | **source-mac** } *	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。

2.5.2 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** } *	―

2.6 リンクアグリゲーションの表示と維持

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
1つ以上のアグリゲートインタフェースを表示する	**display interface bridge-aggregation** [*interface-number*] [**brief** [**description** | **down**]]

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*]
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*]]
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*]]

2.7 リンクアグリゲーションの設定例

2.7.1 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。

- AP とスイッチ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。
- 送信元および宛先 MAC アドレスに基づいてトラフィックを配送するアグリゲーショングループを設定します。

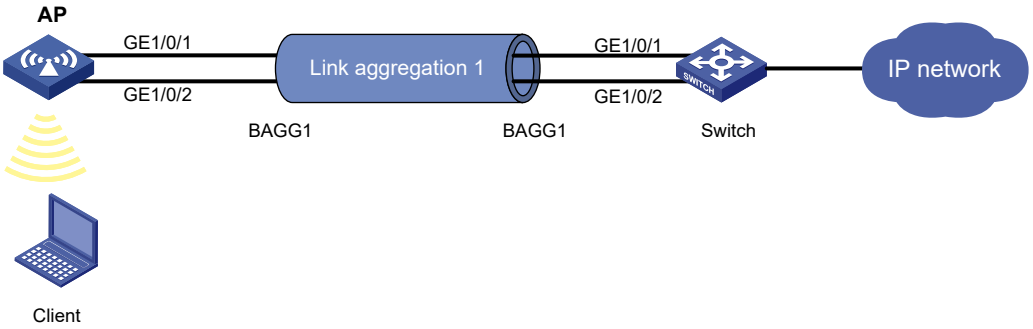


図 2-3 ネットワーク図

II. 設定手順

1)　AP を設定します。

レイヤ 2 アグリゲートインタフェース Bridge-Aggregation 1 を作成します。

```
<AP> system-view
[AP] interface bridge-aggregation 1
[AP-Bridge-Aggregation1] quit
```

リンクアグリゲーショングループ 1 に GigabitEthernet 1/0/1 と GigabitEthernet 1/0/2 を割り当てます。

```
[AP] interface gigabitethernet 1/0/1
```

```
[AP-GigabitEthernet1/0/1] port link-aggregation group 1
[AP-GigabitEthernet1/0/1] quit
[AP] interface gigabitethernet 1/0/2
[AP-GigabitEthernet1/0/2] port link-aggregation group 1
[AP-GigabitEthernet1/0/2] quit
```

送信元および宛先 MAC アドレスに基づいてトラフィックを配送するアグリゲーショングループを設定します。

```
[AP] interface bridge-aggregation 1
[AP-Bridge-Aggregation1] link-aggregation load-sharing mode source-mac destination-mac
```

2)　スイッチを AP と同様に設定します。（詳細は省略します。）

III. 設定の確認

AP 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。

```
[AP] display link-aggregation verbose
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected, I -- Individual
Flags:  A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
        D -- Synchronization, E -- Collecting, F -- Distributing,
        G -- Defaulted, H -- Expired

Aggregate Interface: Bridge-Aggregation1
Aggregation Mode: Static
Loadsharing Type: Shar
  Port             Status  Priority Oper-Key
--------------------------------------------------------------------------------
  GE1/0/1          S       32768    1
  GE1/0/2          S       32768    1
```

出力はリンクアグリゲーショングループ 1 が、2 つの Selected ポートを含むレイヤ 2 スタティックアグリゲーショングループ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**4-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 3-3
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 3-6
3.5 VLAN の表示と維持 3-7

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**－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**－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**－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。

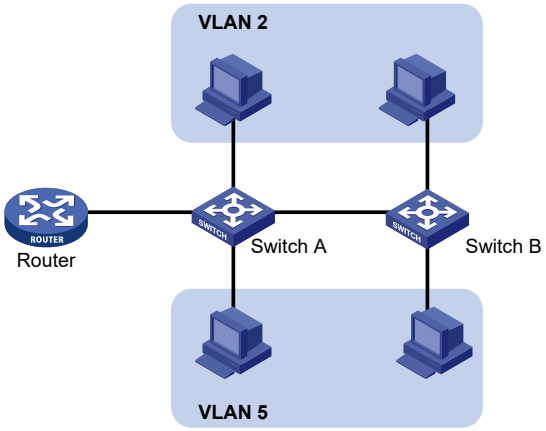


図 3-1 VLAN ネットワーク図

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。

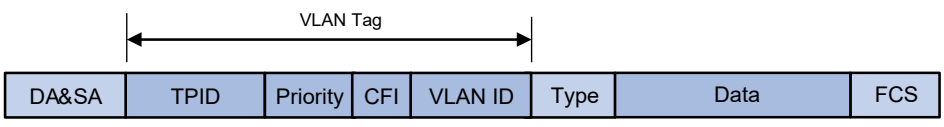


図 3-2 VLAN タグの位置とフォーマット

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。詳細はオペレーションマニュアルのセクション 8 *ACL and QoS “プライオリティマッピング”* を参照してください。
- **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。詳細はオペレーションマニュアルのセクション 4 *アクセス “VLAN” の “ポートベース VLAN の設定”* を参照してください。

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。

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**	ー
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-id1* [**to** *vlan-id2*] }	デフォルト： デフォルト VLAN（VLAN1）のみ

操作	コマンド	補足
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

VLAN の異なるホスト間で通信を行うには、ルータまたはレイヤ 3 スイッチでレイヤ 3 転送を行う必要があります。これを実現するために、VLAN インタフェースが使用されます。VLAN インタフェースは異なる VLAN 間でレイヤ 3 通信を行うための仮想インタフェースです。装置上の VLAN インタフェースは物理的には存在しません。各 VLAN は、1 つの VLAN インタフェースを作成することができます。VLAN インタフェースには IP アドレスを割り当てることができ、そしてそれをゲートウェイとすることで、異なる IP ネットワークセグメントへのトラフィックを転送することが可能となります。

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** *vlan-interface-id*	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（例：Vlan-interface1 Interface）
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：手動でシャットダウン状態になっていません。 ● VLANのすべてのポートがdownしている場合、VLANインタフェースはdownになります。 ● 1つ以上のVLANがupである場合、VLANインタフェースはupになります。

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**－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**－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**－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**	―
2． VLAN view 移行する	**vlan** *vlan-id*	―
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**	―
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*	―

操作	コマンド	補足
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**	―
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*	―
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** [**description** | **down**]]
VLAN情報を表示する	**display vlan** [*vlan-id1* [**to** *vlan-id2*] | **all** | **dynamic** | **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*]

目次

このセクションのページは **4-x-x** です。

4 章 STP 4-1
4.1 STP 4-1
4.1.1 STP のプロトコルパケット 4-1
4.1.2 STP の基本概念 4-3
4.1.3 STP アルゴリズムの計算プロセス 4-4
4.2 RSTP 4-11
4.3 MSTP 4-12
4.3.1 MSTP の特徴 4-12
4.3.2 MSTP の基本概念 4-12
4.3.3 MSTP の原理 4-17
4.3.4 装置での MSTP の実行 4-18
4.4 プロトコルと規格 4-18
4.5 スパニングツリー設定作業リスト 4-18
4.5.1 STP 設定作業リスト 4-19
4.5.2 RSTP 設定作業リスト 4-19
4.5.3 MSTP 設定作業リスト 4-20
4.6 動作モードの設定 4-21
4.6.1 設定手順 4-21
4.7 MST region の設定 4-21
4.8 Root Bridge と Secondary Root Bridge の設定 4-22
4.8.1 Root Bridge の設定 4-23
4.8.2 Secondary Root Bridge の設定 4-23
4.9 Bridge プライオリティの設定 4-23
4.10 MST region の最大ホップ数の設定 4-24
4.11 ネットワークダイアメータの設定 4-24
4.12 スパニングツリータイマの設定 4-25
4.12.1 設定の制限とガイドライン 4-25
4.12.2 設定手順 4-26
4.13 タイムアウトファクタの設定 4-26
4.14 BPDU 最大送出レートの設定 4-26
4.15 Edge ポートの設定 4-27
4.15.1 設定の制限とガイドライン 4-27
4.15.2 設定手順 4-27
4.16 Port Path Cost の設定 4-28
4.16.1 デフォルト Path Cost の計算時の基準指定 4-28
4.16.2 Path Cost の設定 4-29
4.17 Port priority の設定 4-29
4.18 Point-to-Point リンクの設定 4-30
4.18.1 設定の制限とガイドライン 4-30
4.18.2 設定手順 4-30
4.19 MSTP パケットのフォーマット設定 4-31
4.20 スパニングツリー機能の有効化 4-31
4.20.1 STP/RSTP/MSTP モードでのスパニングツリー機能の有効化 4-32
4.21 mCheck 機能の設定 4-32
4.21.1 設定の制限とガイドライン 4-32

4.21.2 設定手順 4-33
4.22 Digest Snooping の設定 4-33
4.22.1 設定の制限とガイドライン 4-34
4.22.2 設定手順 4-34
4.22.3 Digest Snooping 設定例 4-34
4.23 No Agreement Check の設定 4-35
4.23.1 設定要件 4-37
4.23.2 設定手順 4-37
4.23.3 No Agreement Check 設定例 4-37
4.24 保護機能の設定 4-38
4.24.1 BPDU ガードの有効化 4-38
4.24.2 Root ガードの有効化 4-39
4.24.3 Loop ガードの有効化 4-39
4.24.4 TC-BPDU ガードの有効化 4-40
4.24.5 PVST BPDU ガード機能の有効化 4-41
4.25 スパニングツリーの表示と維持 4-41

4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。

4.1 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。

4.1.1 STP のプロトコルパケット

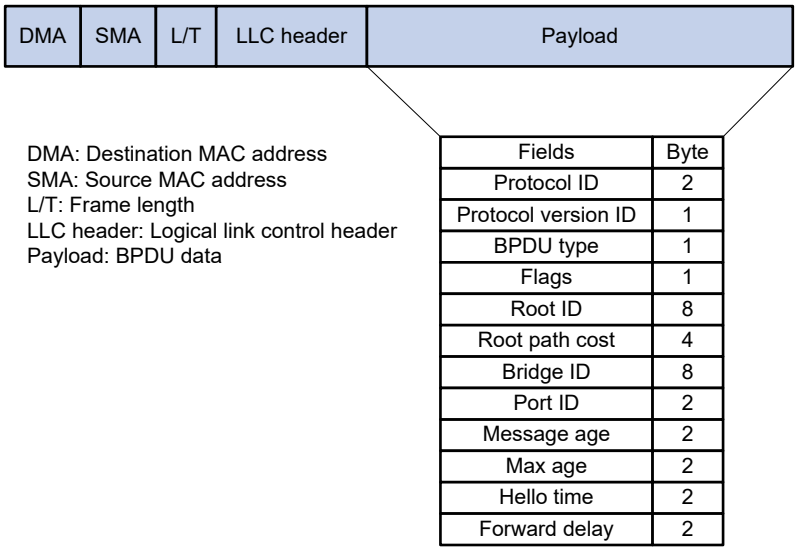
スパニングツリープロトコルでは、リンクレイヤパケットの BPDU（Bridge Protocol Data Units）を使用して、情報交換・状態の維持管理を行います。IEEE802.1d で規定される STP では、以下 2 種類の BPDU を使用します。STP が有効なネットワークの装置は BPDU を交換してスパニングツリーを確立します。BPDU はスパニングツリーの計算を行うために十分な情報を含みます。

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 4-1 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 4-2 に TCN BPDU の形式を示します。

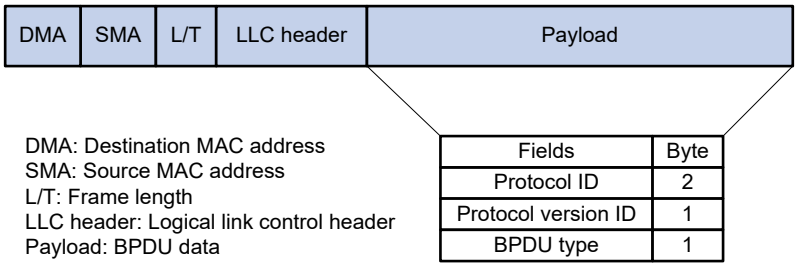


図 4-2 TCN BPDU の形式

TCN BPDU には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**－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。

4.1.2 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 4-3 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。

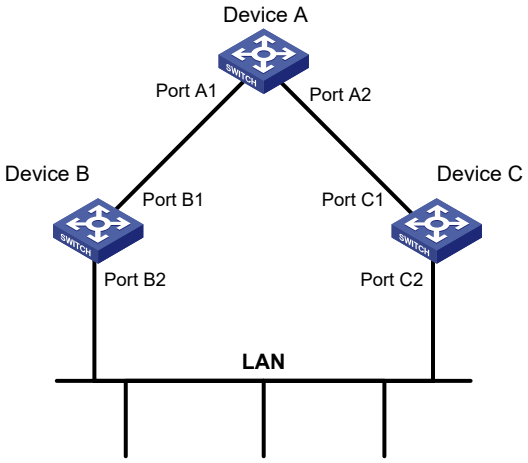


図 4-3 Designated bridge と Designated port

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。

4.1.3 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 を自身のデバイス 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 4-1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 4-1 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 4-4 に STP アルゴリズムの計算例を示します。

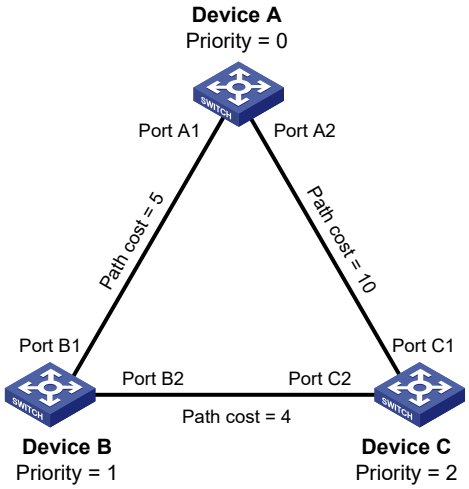


図 4-4 STP アルゴリズム

図 4-4 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 4-2 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 4-2 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 4-3 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 4-3 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A1: {0, 0, 0,ポート A1} • ポートA2: {0, 0, 0,ポート A2}

装置	比較プロセス	比較後のポートの Configuration BPDU
	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。	
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}
	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}

装置	比較プロセス	比較後のポートの Configuration BPDU
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}
	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}
	Device Cは、ポートC1のルートパスコスト (10)	● Blocked port (ポートC1): {0, 0, 0, ポートA2}

装置	比較プロセス	比較後のポートの Configuration BPDU
	(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。	• Root port (ポートC2): {0, 5, 1, ポートB2}

表 4-3 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 4-5 のように確立されます。

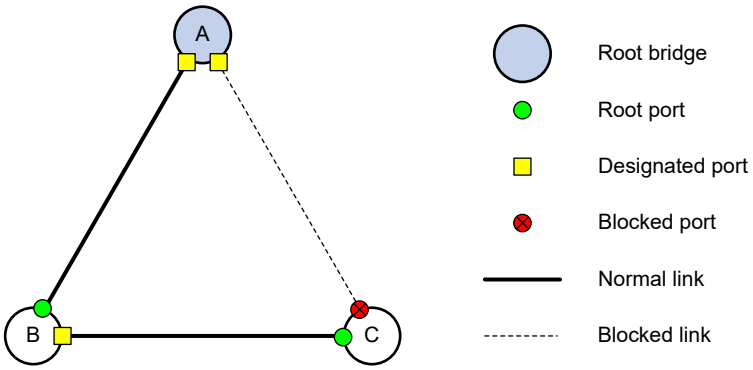


図 4-5 比較プロセス後のスパニングツリー

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。

4.2 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。

4.3 MSTP

MSTP は以下の STP、RSTP 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。

4.3.1 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 に互換性があります。

4.3.2 MSTP の基本概念

図 4-6 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 4-7 は MST region3 のネットワークトポロジを示します。

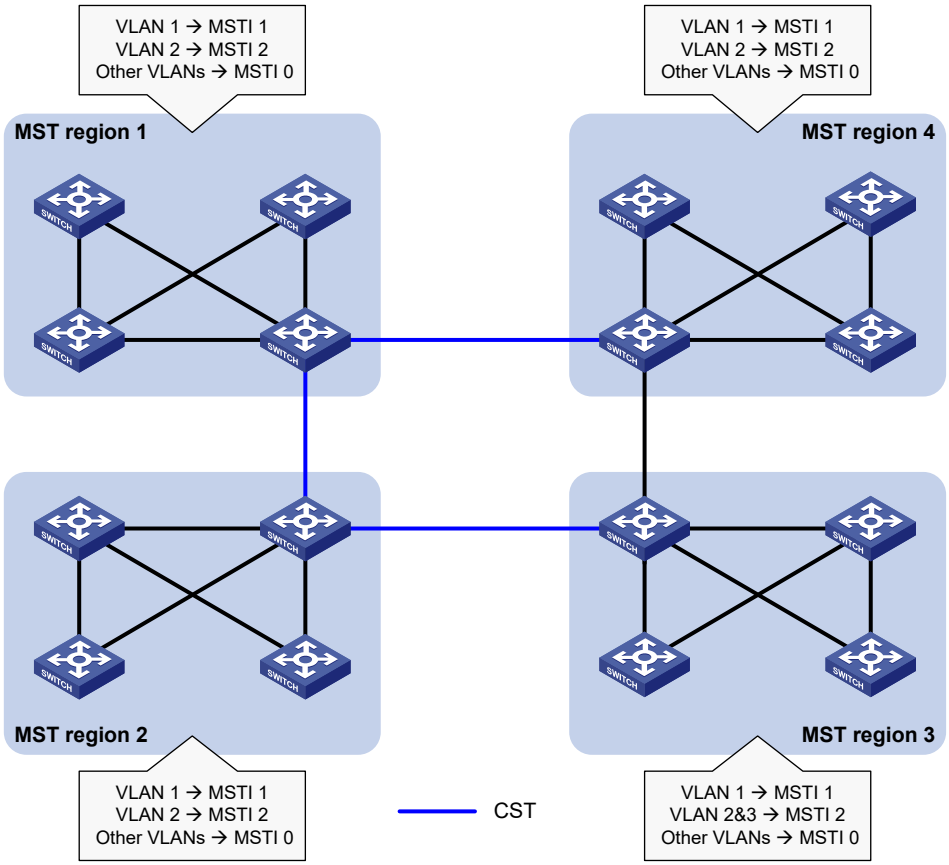


図 4-6 MSTP の基本概念

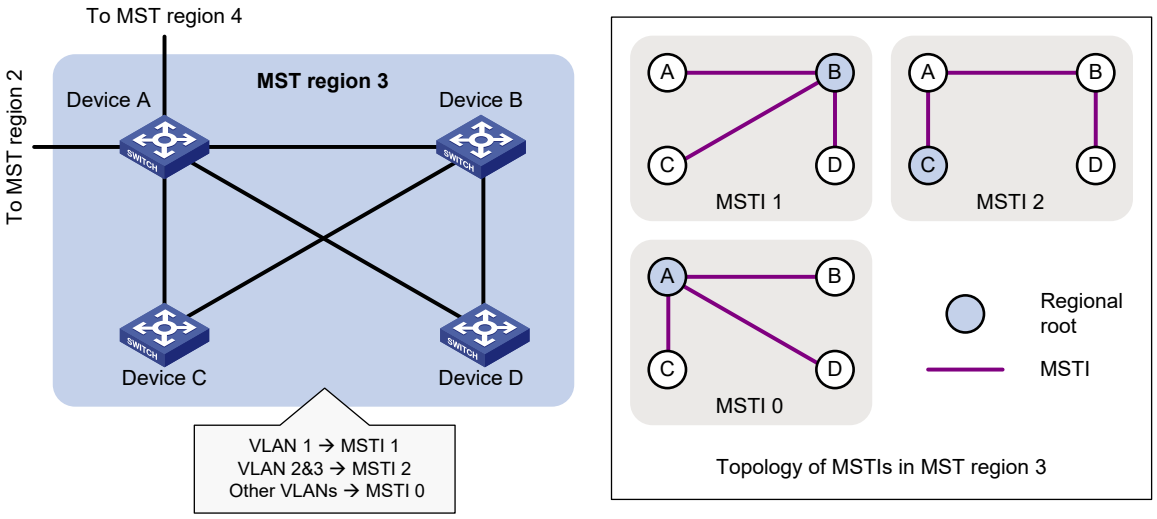


図 4-7 MST region 3 のネットワーク図とトポロジ

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 4-6 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 4-7 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 4-7 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 4-6 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 4-6 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 4-6 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 4-7 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 4-6 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 4-8 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。

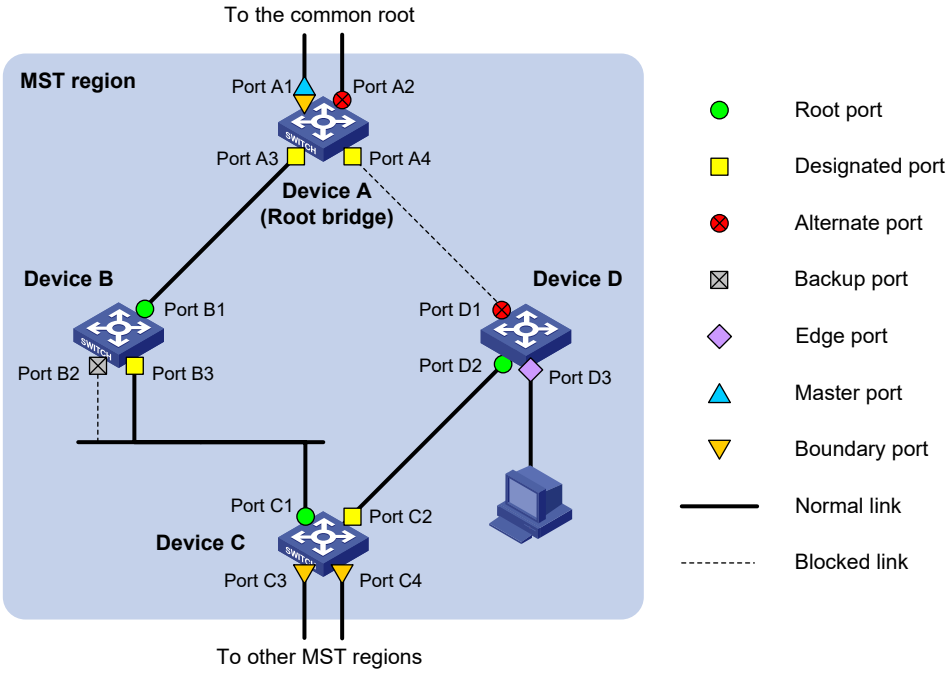


図 4-8 ポートの役割

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 4-4 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 4-4 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

4.3.3 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

- 最も優先度の高いデバイスを、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 つのデバイスとみなして､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、オペレーションマニュアルのセクション 4 *アクセス “STP”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。

4.3.4 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

4.4 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*

4.5 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)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。

4.5.1 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

4.5.2 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

作業リスト
• (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

4.5.3 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

作業リスト
• (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

4.6 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。

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。

4.6.1 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** | **rstp** | **stp** }	デフォルト：MSTP

4.7 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 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**	―

4.8 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、オペレーションマニュアルのセクション 4 *アクセス "STP" の "Bridge プライオリティの設定"* を参照してください。

4.8.1 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** • 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。

4.8.2 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** • 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。

4.9 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、そのデバイスを 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
2. Bridge プライオリティを設定する	• STP/RSTPモード: **stp priority** *priority* • MSTPモード: **stp** [**instance** *instance-list*] **priority** *priority*	デフォルト：32768

4.10 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デバイスを経由する度に、-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

4.11 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。

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**	―
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*	デフォルト：7

4.12 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。

4.12.1 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デバイス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、デバイス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デバイス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。

4.12.2 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*	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*	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*	デフォルト： 20秒

4.13 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、上位のデバイス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**	ー
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

4.14 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

4.15 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、接続デバイスが 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。

4.15.1 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。

4.15.2 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

4.16 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。

4.16.1 デフォルト Path Cost の計算時の基準指定

⚠ **注意:**

デバイスがデフォルト 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。(オペレーションマニュアルのセクション 4 *アクセス “STP” 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**	ー
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 4-5 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	ー	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

4.16.2 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**	ー
2. Ethernet あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	ー
3. Path Cost を設定する	• STP/RSTPモード: **stp 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

4.17 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* • MSTPモード: **stp** [**instance** *instance-list*] **port priority** *priority*	デフォルト：128

4.18 Point-to-Pointリンクの設定

Point-to-Point リンクは、2 台のデバイス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。

4.18.1 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 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 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。

4.18.2 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*	―

操作	コマンド	補足
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。

4.19 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デバイスと通信します。

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**

4.20 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。

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。

4.20.1 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
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

4.21 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 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 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 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。

4.21.1 設定の制限とガイドライン

mCheck 機能は MSTP、RSTP モードで動作する装置で適用されます。

4.21.2 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**

4.22 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。

4.22.1 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。

4.22.2 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

4.22.3 Digest Snooping 設定例

I. ネットワーク要件

図 4-9 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。

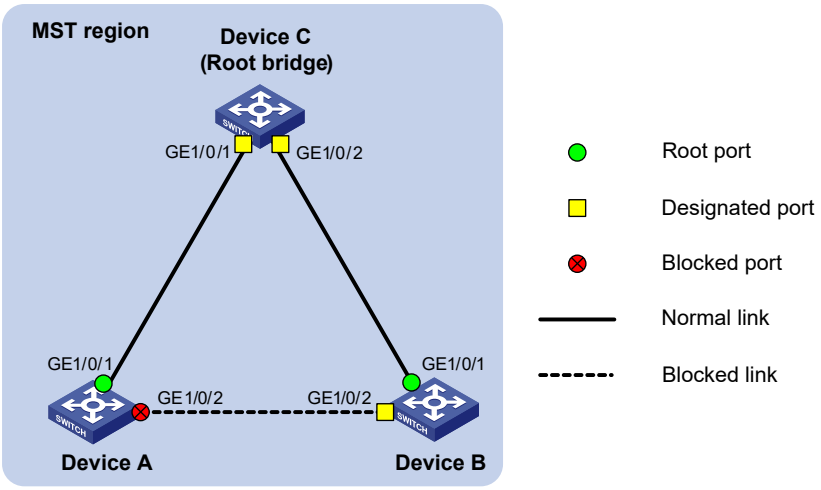


図 4-9 ネットワーク図

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
```

4.23 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。

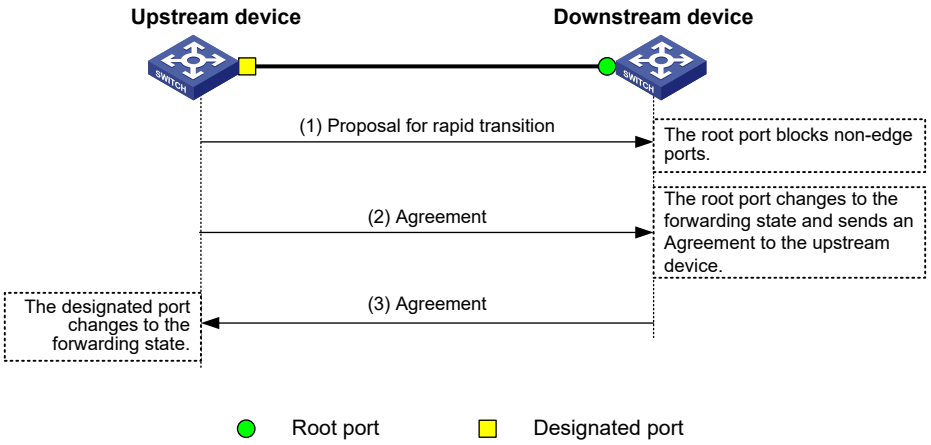


図 4-10 MSTP の designated port の高速状態遷移のメカニズム

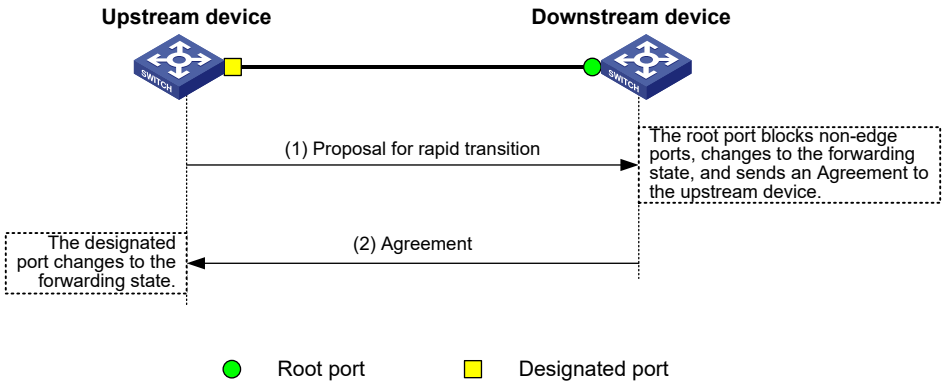


図 4-11 RSTP の designated port の高速状態遷移のメカニズム

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。

4.23.1 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。

4.23.2 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

4.23.3 No Agreement Check 設定例

I. ネットワーク要件

図 4-12 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。

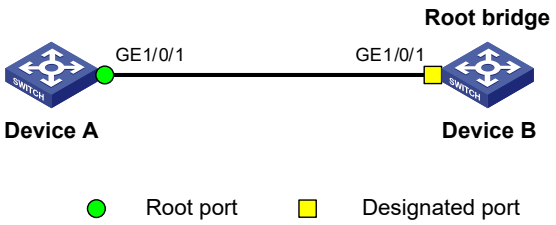


図 4-12 ネットワーク図

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
```

4.24 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
- TC-BPDU ガード
- PVST BPDU ガード

4.24.1 BPDU ガードの有効化

アクセスポートは通常、ユーザ端末(PC など)やファイルサーバに直接接続されており、高速な遷移を実現するために、Edge ポートに設定されています。こうしたポートで BPDU パケットを受信すると、装置はそのポートを自動的に非 Edge ポートに設定し、スパニングツリーの再計算を開始します。その結果、ネットワーク全体でトポロジ変更が発生する可能性があります。通常の状況下ではこれらのポートは configuration BPDU を受信すべできではありません。しかし不正な装置への攻撃によって configuration BPDU を偽造した場合、ネットワークは不安定となります。

この点を狙った悪意のユーザからの攻撃を防止するための機能として、BPDU ガード機能をサポートします。

本機能を設定することで、Edge ポートに設定しているポートで BPDU パケットを受信すると、装置は以下の操作をします。

- Edge ポートに設定しているポートを shutdown 状態にします。
- NMS に shutdown 状態であることを通知します。

装置は検出の間隔後に、shutdown 状態のポートの解除を行います。検出の間隔についての詳細は、オペレーションマニュアルのセクション 1 *はじめに* *“装置管理”* を参照してください。

loopback test が設定されたポートでは、BPDU ガードを有効にすることができません。

BPDU ガードは、Edge ポートが設定された装置で設定します。

以下に 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**	―

操作	コマンド	補足
2． BPDU ガードを有効にする	**stp bpdu-protection**	デフォルト：無効

4.24.2 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、不正なデバイス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

4.24.3 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

4.24.4 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**	―
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

4.24.5 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

4.25 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** [**slot** *slot-number*]
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** [**slot** *slot-number*]
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* | **slot** *slot-number*] [**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*]

目次

このセクションのページは**4-x-x** です。

5 章 ループ検出 5-1
5.1 概要 5-1
5.1.1 ループ検出メカニズム 5-1
5.1.2 ループ検出間隔 5-2
5.1.3 ループ保護アクション 5-2
5.1.4 ポート状態自動回復 5-3
5.2 ループ検出設定作業リスト 5-3
5.3 ループ検出の有効化 5-3
5.3.1 グローバルでのループ検出の有効化 5-3
5.3.2 ポートでのループ検出の有効化 5-4
5.4 ループ保護アクションの設定 5-4
5.4.1 グローバルでのループ保護アクションの設定 5-4
5.4.2 Ethernet インタフェースでのループ保護アクションの設定 5-4
5.4.3 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 5-5
5.5 ループ検出間隔の設定 5-5
5.6 ループ検出の表示と維持 5-5
5.7 ループ検出設定例 5-5
5.7.1 ネットワーク要件 5-5
5.7.2 設定手順 5-6
5.7.3 設定の確認 5-8

5章 ループ検出

5.1 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。詳細はオペレーションマニュアルのセクション 10 *システム管理 “Information Center”* を参照してください。

5.1.1 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。

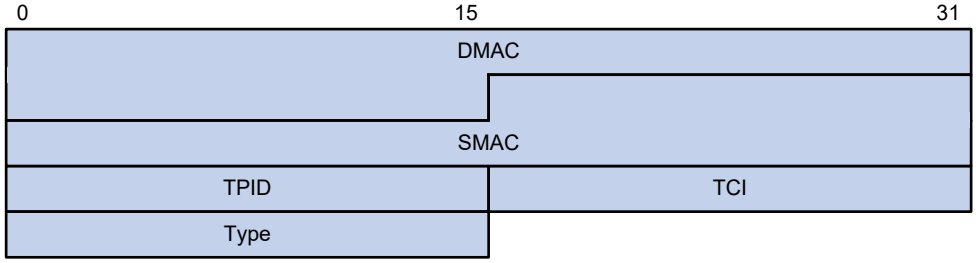


図 5-1 ループ検出のイーサネットフレームヘッダ

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。

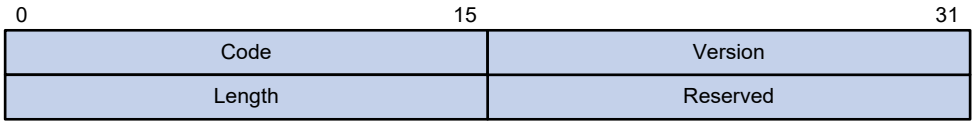


図 5-2 ループ検出の内部フレームヘッダ

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 5-1 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

5.1.2 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。

5.1.3 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。

5.1.4 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。

5.2 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

5.3 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。

5.3.1 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**	―

操作	コマンド	補足
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。

5.3.2 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**	―
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

5.4 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。

5.4.1 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**	―
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。

5.4.2 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。

5.4.3 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。

5.5 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

5.6 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**

5.7 ループ検出設定例

5.7.1 ネットワーク要件

図 5-3 に示すように AP はスイッチ A を介してネットワークにアクセスします。スイッチ A、スイッチ B、スイッチ C がループ接続された時にネットワーク管理者はネットワーク内のループを防止します。

- 不正な設定によるループが発生した場合、AP はログ情報を出力してトラップメッセージを送信することにより、ネットワーク接続を確認するようユーザに通知することができるよう、AP 上でループバック検出を設定します。

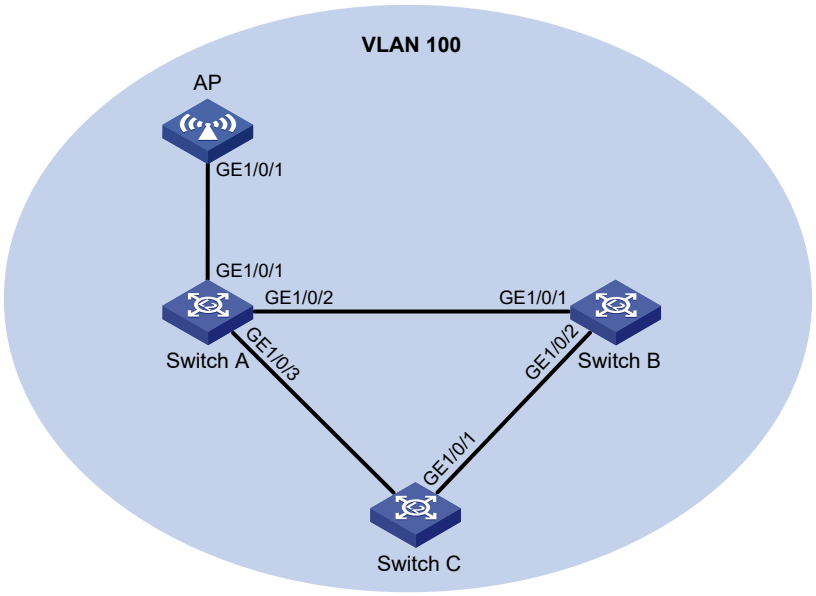


図 5-3 ネットワーク図

5.7.2 設定手順

1)　AP を設定します。

GigabitEthernet 1/0/1 をトランクポートに設定し、VLAN 100 を割り当てます。インタフェースがループを検出すると、GigabitEthernet 1/0/1 をシャットダウンしてパケットを破棄します。

```
<AP> system-view
[AP] interface GigabitEthernet 1/0/1
[AP] vlan 100
[AP-vlan100] quit
[AP] interface GigabitEthernet1/0/1
[AP-GigabitEthernet1/0/1] port link-type trunk
[AP-GigabitEthernet1/0/1] port trunk permit vlan 100
[AP-GigabitEthernet1/0/1] loopback-detection enable Vlan 100
```

ループ保護アクションをシャットダウンに設定します。

```
[AP-GigabitEthernet1/0/1] loopback-detection action shutdown
[AP-GigabitEthernet1/0/1] quit
```

ループ検出間隔を 35 秒に設定します。

```
[AP] loopback-detection interval-time 35
```

2)　スイッチ A を設定します。

VLAN 100 を作成します。

```
<SwitchA> system-view
[SwitchA] vlan 100
```

```
[SwitchA–vlan100] quit
```

GigabitEthernet 1/0/2、GigabitEthernet 1/0/3 をトランクポートとして設定し、VLAN 100 を割り当てます。

```
[SwitchA] interface GigabitEthernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] port link-type trunk
[SwitchA-GigabitEthernet1/0/2] port trunk permit vlan 100
[SwitchA-GigabitEthernet1/0/2] quit
[SwitchA] interface GigabitEthernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] port link-type trunk
[SwitchA-GigabitEthernet1/0/3] port trunk permit vlan 100
[SwitchA-GigabitEthernet1/0/3] quit
```

3)　スイッチ B を設定します。

VLAN 100 を作成します。

```
<SwitchB> system-view
[SwitchB] vlan 100
[SwitchB–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。

```
[SwitchB] interface GigabitEthernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] port link-type trunk
[SwitchB-GigabitEthernet1/0/1] port trunk permit vlan 100
[SwitchB-GigabitEthernet1/0/1] quit
[SwitchB] interface GigabitEthernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] port link-type trunk
[SwitchB-GigabitEthernet1/0/2] port trunk permit vlan 100
[SwitchB-GigabitEthernet1/0/2] quit
```

GigabitEthernet 1/0/1 はシャットダウンを想定します。

```
[SwitchB] interface GigabitEthernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] shutdown
[SwitchB-GigabitEthernet1/0/1] quit
```

1)　スイッチ C を設定します。

VLAN 100 を作成します。

```
<SwitchC> system-view
[SwitchC] vlan 100
[SwitchC–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。

```
[SwitchC] interface GigabitEthernet 1/0/1
[SwitchC-GigabitEthernet1/0/1] port link-type trunk
[SwitchC-GigabitEthernet1/0/1] port trunk permit vlan 100
```

```
[SwitchC-GigabitEthernet1/0/1] quit
[SwitchC] interface GigabitEthernet 1/0/2
[SwitchC-GigabitEthernet1/0/2] port link-type trunk
[SwitchC-GigabitEthernet1/0/2] port trunk permit vlan 100
[SwitchC-GigabitEthernet1/0/2] quit
```

5.7.3 設定の確認

設定の完了後に、**display loopback-detection** コマンドを使用して、各装置のループ検出の状態を確認します。

AP でループ検出の状態を表示します。

```
[AP] display loopback-detection
Loopback-detection is enabled.
Loopback detection interval is 35 second(s).
No loopback is detected.
```

AP でループ検出が有効になっていることと、ループが検出されていことを確認します。

スイッチ A でループ検出の状態を表示します。

```
[SwitchA] display loopback-detection
Loopback-detection is disabled.
```

スイッチ B でループ検出の状態を表示します。

```
[SwitchB] display loopback-detection
Loopback-detection is disabled.
```

スイッチ C でループ検出の状態を表示します。

```
[SwitchC] display loopback-detection
Loopback-detection is disabled.
```

スイッチ A、スイッチ B、スイッチ C でループ検出が有効になっていないことを確認します。

この状態からスイッチ A とスイッチ B の GigabitEthernet 1/0/1 が誤って接続されたしてスイッチ B の GigabitEthernet 1/0/1 を Linkup させます。AP はループ検出間隔内にループを検出します。その結果、自動的にポートをシャットダウンし、ログ情報を出力します。

```
%Feb 24 15:04:29:663 2013 AP LPDT/4/LPDT_LOOPED: Loopback exists on
GigabitEthernet1/0/1.
%Feb 24 15:04:44:243 2013 AP LPDT/4/LPDT_RECOVERED: Loopback on
GigabitEthernet1/0/1 recovered.
```

ログ情報の表示後、AP で **display loopback-detection** コマンドを再度使用して、ループ検出の状態を表示します。

AP でループ検出の操作状態を表示します。

```
[AP] display loopback-detection
Loopback-detection is enabled.
Loopback detection interval is 35 second(s).
Loopback is detected on following interfaces:
Interface                Action mode
GigabitEthernet1/0/1     Shutdown
```

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。

目次

このセクションのページは**4-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 6-8
6.3.1 LLDP の有効化 6-8
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 6-9
6.3.5 アドバタイズ可能な TLV の設定 6-10
6.3.6 管理アドレスの設定とカプセル化フォーマットの設定 6-11
6.3.7 LLDP に関する他のパラメータの設定 6-12
6.3.8 LLDP フレームのカプセル化フォーマットの設定 6-12
6.4 LLDP トラップの設定 6-13
6.5 LLDP の表示と維持 6-13
6.6 LLDP の設定例 6-14
6.6.1 LLDP の基本的な設定例 6-14

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。

Link Layer Discovery Protocol (LLDP) 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、オペレーションマニュアルのセクション 10 *システム管理 “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。

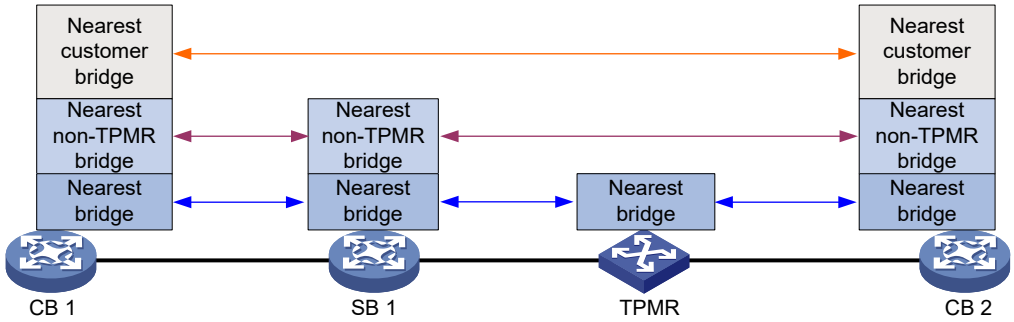


図 6-1 LLDP 隣接関係

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

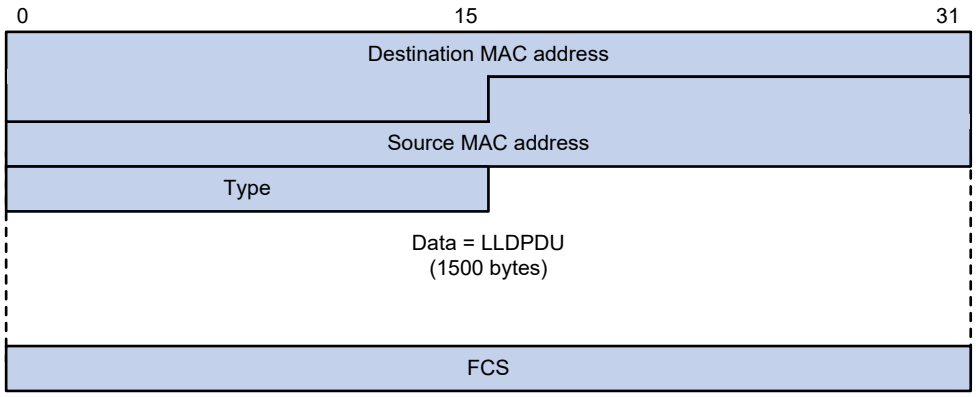


図 6-2 Ethernet II にカプセル化した LLDP フレーム

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。
Data	LLDPDUです。

フィールド	説明
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

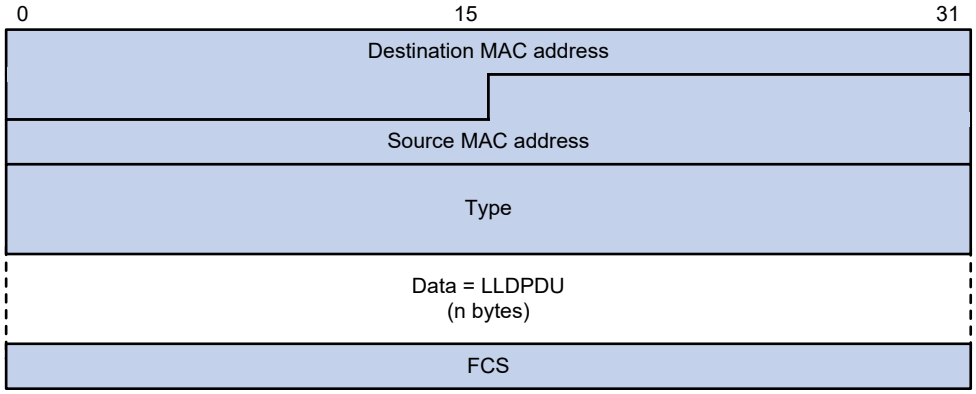


図 6-3 SNAP にカプセル化したフレーム

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。

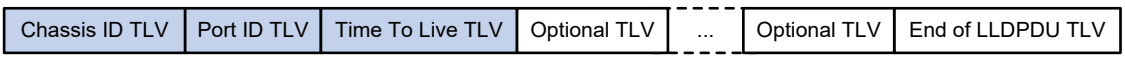


図 6-4 LLDPDU カプセルフォーマット

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 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。
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。

タイプ	説明
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。
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オペレーションマニュアルのセクション 8 *ACL and QoS “トラフィックポリシング”* 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） 管理アドレスの設定とカプセル化フォーマットの設定 ● （オプション設定項目） LLDPに関する他のパラメータの設定 ● （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） LLDPトラップ、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． Layer 2 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）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. Layer 2 Ethernet interface view あるいは aggregate 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 Ethernet interface view での設定： **lldp** [**agent nearest-customer**] **admin-status** { **disable** | **rx** | **tx** | **txrx** } ● 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**	―
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. Layer 2 Ethernet interface view 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. LLDP ポーリングの有効化を設定する	• Layer 2 Ethernet interface view での設定： **lldp** [**agent nearest-customer**] **check-change-interval** *interval* • 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. Layer 2 Ethernet interface view あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	—
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*] } | **dot1-tlv** { **all** | **congestion-notification** | **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** | **power** } | **med-tlv** { **all** | **capability** | **inventory** | **network-policy** [*vlan-id*] | **power-over-ethernet** | **location-id** { **civic-address** *device-type country-code* { *ca-type ca-value* }&<1-10> | **elin-address** *tel-number* } } } • **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** | **congestion-notification** | **port-vlan-id** | **link-aggregation** } }	デフォルト： • Nearest bridgeエージェントはlocation identification TLV, port VLAN ID TLV、protocol VLAN ID TLV、VLAN name TLV、management VLAN ID 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。

操作	コマンド	補足
4. LLDPDU TLV を設定する（aggregate interface view）	• **lldp agent nearest-nontpmr 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 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** } }	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 管理アドレスの設定とカプセル化フォーマットの設定

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。

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. Layer 2 Ethernet interface view あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	—
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での設定： **lldp** [**agent nearest-customer**] **tlv-enable basic-tlv management-address-tlv** [*ip-address*] • 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 Ethernet interface viewでの設定： **lldp** [**agent nearest-customer**] **management-address-format string** • 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 に関する他のパラメータの設定

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
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

LLDPDU は Ethernet II または SNAP フレームにカプセル化されます。

- **Ethernet II**－カプセル化フォーマットを Ethernet II に設定した場合、LLDP ポートは Ethernet II フレームで LLDP フレームを送信します。
- **SNAP**－カプセル化フォーマットを SNAP に設定した場合、LLDP ポートは SNAP フレームで LLDP フレームを送信します。

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． Layer 2 Ethernet interface view あるいは Layer 2 aggregate 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 Ethernet interface view での設定： **lldp** [**agent nearest-customer**] **encapsulation snap** ● aggregate interface viewでの設定： **lldp agent nearest-customer encapsulation snap**	デフォルト： Ethernet II

6.4 LLDPトラップの設定

LLDP 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。

トポロジが不安定なとき、LLDP トラップの送信間隔の設定を変更することで、指定した時間内での過度な LLDP トラップの送信を防ぐことができます。

以下に LLDP 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. Layer 2 Ethernet interface view あるいは aggregate interface view に移行する	**interface** *interface-type interface-number*	―
3. LLDP トラップの送信を有効にする	● Layer 2 Ethernet interface view での設定： **lldp** [**agent nearest-customer**] **notification remote-change enable** ● aggregate interface viewでの設定： **lldp agent nearest-customer notification remote-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、スイッチおよび AP 上で LLDP をグローバルに有効にして、次の作業を実行します。

- NMS 上のスイッチと AP 間のリンクを監視します。
- NMS 上のスイッチと MED 装置間のリンクを監視します。

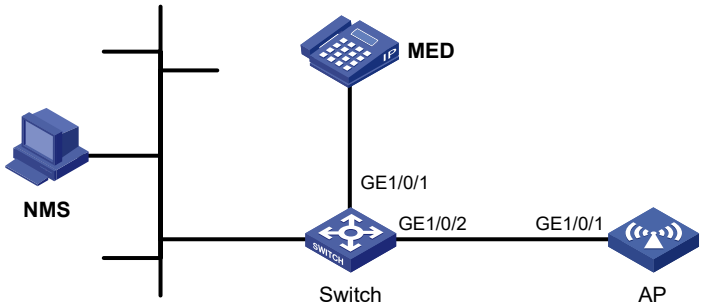


図 6-5 ネットワーク図

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)　AP を設定します。

グローバルで LLDP を有効にします。

```
<AP> system-view
[AP] 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。

```
[AP] interface gigabitethernet 1/0/1
[AP-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。

```
[AP-GigabitEthernet1/0/1] lldp admin-status tx
[AP-GigabitEthernet1/0/1] quit
```

III. 設定の確認

次の条件を満たしていることを確認します。

- スイッチの GigabitEthernet 1/0/1 が MED 装置に接続します。
- スイッチの GigabitEthernet 1/0/2 は、非 MED 装置に接続します。
- それぞれのポートは Rx モードで動作し、LLDP フレームを受信できますが LLDP フレームは送信できません。

```
[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 1 [GigabitEthernet1/0/1]:
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        : 1
Number of CDP neighbors        : 0
Number of sent optional TLV    : 21
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
```

```
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
```

スイッチと AP のリンクを切断します。

スイッチの 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 1 [GigabitEthernet1/0/1]:
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         : 1
Number of CDP neighbors         : 0
Number of sent optional TLV     : 0
Number of received unknown TLV : 5

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 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
```

QX-W1200 シリーズ アクセスポイント

オペレーションマニュアル

5. IP サービス

本マニュアルは以下に示す章で構成されています。

01-ARP

02-Gratuitous ARP

03-Proxy ARP

04-IP アドレス

05-DHCP の概要

06-DHCP サーバ

07-DHCP リレー

08-DHCP クライアント

09-BOOTP クライアント

10-DNS

11-IP パフォーマンスの最適化

12-NAT の概要

13-NAT の設定

目次

このセクションのページは **5-x-x** です。

1 章 ARP 1-1
1.1 概要 1-1
1.1.1 ARP メッセージフォーマット 1-1
1.1.2 ARP 動作メカニズム 1-1
1.1.3 ARP テーブル 1-3
1.2 スタティック ARP エントリの設定 1-3
1.3 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 1-4
1.4 ダイナミック ARP エントリのエージングタイマの設定 1-4
1.5 ARP エントリチェックの有効化 1-5
1.6 ARP ロギング機能の有効化 1-5
1.7 ARP の表示と維持 1-6
1.8 ロングスタティック ARP エントリ設定例 1-6
1.8.1 ネットワーク要求 1-6
1.8.2 設定手順 1-7
1.8.3 設定の確認 1-7

1章 ARP

1.1 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。

1.1.1 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 1-1 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。

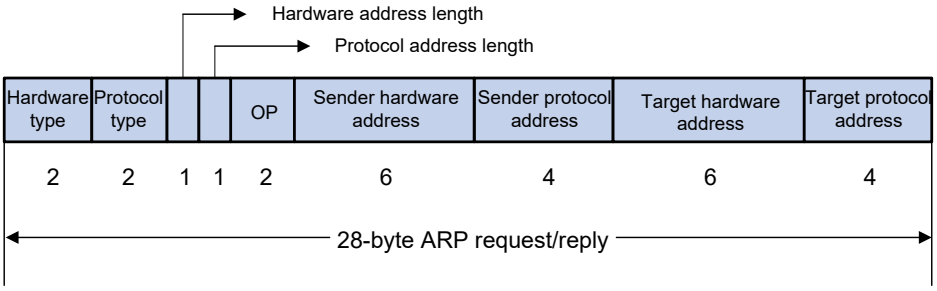


図 1-1 ARP メッセージフォーマット

- **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。

1.1.2 ARP 動作メカニズム

図 1-2 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** ー Host A の IP アドレスと MAC アドレス
   - **宛先 IP アドレス** ー Host B の IP アドレス
   - **宛先 MAC アドレス** ー 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。

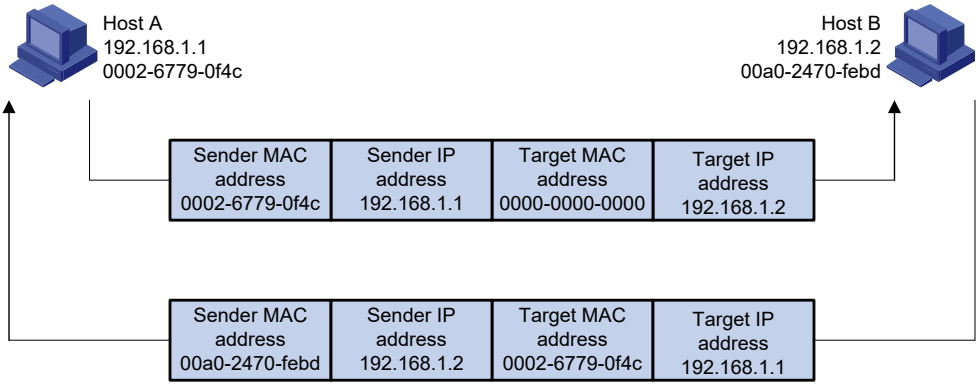


図 1-2 ARP アドレス解決プロセス

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。

1.1.3 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。

1.2 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

1.3 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*	―
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。

1.4 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-time*	デフォルト：20分

1.5 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

1.6 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 リプライの送信元 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、オペレーションマニュアルのセクション 10 *システム管理 “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**	―
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

1.7 ARPの表示と維持

重要：

ARP テーブルから ARP エントリをクリアすると、通信障害を引き起こす恐れがあります。ARP エントリを削除した場合は、その後の通信に影響がないことを確認してください。

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**]
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** }

1.8 ロングスタティックARPエントリ設定例

1.8.1 ネットワーク要求

図 1-3 に示すように、ホストは AP に接続されています。AP は VLAN 10 の interface GigabitEthernet 1/0/1 を介してルータと接続されています。

ルータと AP 間のセキュアな通信を保証するために、ルータにロングスタティック ARP エントリを設定します。

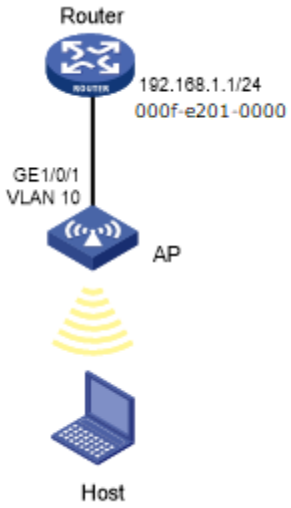


図 1-3 ネットワーク図

1.8.2 設定手順

AP で無線サービスを設定します。詳細はオペレーションマニュアルのセクション 2 *WLAN* “*WLAN アクセスの設定*”を参照してください。

VLAN 10 を作成します。

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

interface GigabitEthernet 1/0/1 を VLAN 10 に追加します。

```
[AP] interface gigabitethernet 1/0/1
[AP-GigabitEthernet1/0/1] port access vlan 10
[AP-GigabitEthernet1/0/1] quit
```

VLAN-interface 10 を作成し、IP アドレスを設定します。

```
[AP] interface vlan-interface 10
[AP-vlan-interface10] ip address 192.168.1.2 8
[AP-vlan-interface10] quit
```

VLAN 10 に、IP アドレス 192.168.1.1、MAC アドレス 000f-e201-0000、出力インタフェース GigabitEthernet 1/0/1 をもつ、ロングスタティック ARP エントリを設定します。

```
[AP] arp static 192.168.1.1 000f-e201-0000 10 gigabitethernet 1/0/1
```

1.8.3 設定の確認

AP がルータに対してロングスタティック ARP エントリをもつことを確認します。

```
[AP] display arp static
  Type: S-Static   D-Dynamic   O-Openflow   R-Rule          I-Invalid
IP address       MAC address     SVID     Interface             Aging Type
192.168.1.1      000f-e201-0000  10       GE1/0/1               --    S
```

目次

このセクションのページは **5-x-x** です。

2 章 Gratuitous ARP 2-1
2.1 概要 2-1
2.1.1 Gratuitous ARP パケットの学習 2-1
2.1.2 Gratuitous ARP パケットの送信間隔の設定 2-1
2.2 設定手順 2-2
2.3 IP 重複通知の有効化 2-2

2章 Gratuitous ARP

2.1 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。

2.1.1 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。

2.1.2 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。

2.2 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

2.3 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**	―

操作	コマンド	補足
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。

3 章 Proxy ARP 3-1
3.1 一般的な Proxy ARP の有効化 3-1
3.2 ローカル Proxy ARP の有効化 3-1
3.3 Proxy ARP の表示と維持 3-1
3.4 一般的な Proxy ARP 設定例 3-2
3.4.1 ネットワーク要件 3-2
3.4.2 設定手順 3-2
3.4.3 設定の確認 3-3

3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。

3.1 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**	－
2． interface view に移行する	**interface** *interface-type interface-number*	－
3． 一般的な Proxy ARP を有効にする	**proxy-arp enable**	デフォルト：無効

3.2 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**	－
2． interface view に移行する	**interface** *interface-type interface-number*	－
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

3.3 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*]

3.4 一般的なProxy ARP設定例

3.4.1 ネットワーク要件

図 3-1 に示すように、Host A と Host D は同一 IP プレフィックスとマスクを持ちますが、AP によって異なるサブネットに分離されています。Host A は VLAN 1、Host D は VLAN 2 に所属しています。Host A と Host D 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 Host 間で通信ができるように AP で一般的な Proxy ARP を設定します。

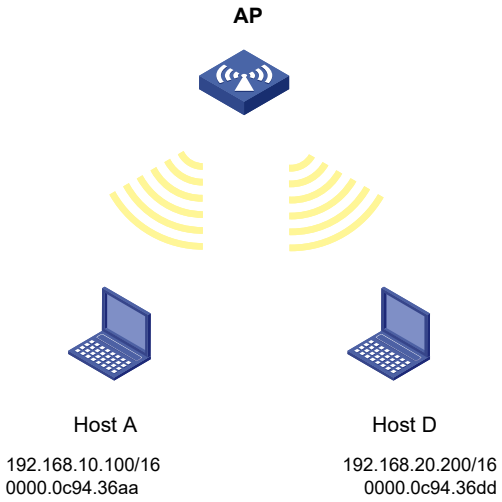


図 3-1 ネットワーク図

3.4.2 設定手順

AP で無線サービスを設定します。詳細はオペレーションマニュアルのセクション 2 *WLAN* “*WLAN アクセスの設定*”してください。

VLAN 2 を作成します。

```
<AP> system-view
[AP] vlan 2
[AP-vlan2] quit
```

VLAN インタフェース 1 の IP アドレスを設定します。

```
[AP] interface vlan-interface 1
[AP-Vlan-interface1] ip address 192.168.10.99 255.255.255.0
```

VLAN インタフェース 1 で一般的な Proxy ARP を有効にします。

```
[AP-Vlan-interface1] proxy-arp enable
[AP-Vlan-interface1] quit
```

VLAN インタフェース 2 の IP アドレスを設定します。

```
[AP] interface vlan-interface 2
[AP-Vlan-interface2] ip address 192.168.20.99 255.255.255.0
```

VLAN インタフェース 2 で一般的な Proxy ARP を有効にします。

```
[AP-Vlan-interface2] proxy-arp enable
```

3.4.3 設定の確認

Host A と Host D 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。

4 章 IP アドレス 4-1
4.1 概要 4-1
4.1.1 IP アドレスクラス 4-1
4.1.2 特別な IP アドレス 4-2
4.1.3 サブネットとマスク 4-2
4.2 インタフェースへの IP アドレスの割り当て 4-3
4.2.1 設定ガイドライン 4-3
4.2.2 設定手順 4-3
4.3 IP アドレスの表示と維持 4-3
4.4 設定例 4-4
4.4.1 IP アドレス設定例 4-4

4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。

4.1 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。3 先ほどの 32 ビットの 2 進数は、10.1.1.1 となります。

4.1.1 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 4-1 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。

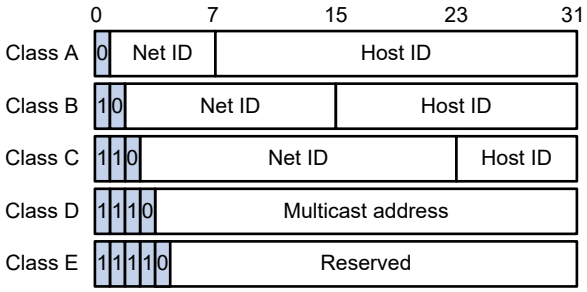


図 4-1 IP アドレスクラス

表 4-1 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

クラス	アドレス範囲	補足
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。

4.1.2 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** － 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** － 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** － 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。

4.1.3 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。

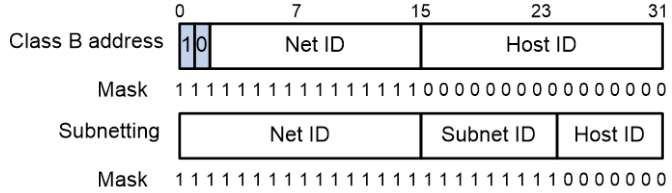


図 4-2 クラス B ネットワークのサブネット

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。

4.2 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。

4.2.1 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 または DHCP、PPP アドレスネゴシエーションにより 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。

4.2.2 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

4.3 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*]

操作	コマンド
指定した、またはすべてのレイヤ3インタフェースの概要情報を表示する	**display ip interface** [*interface-type* [*interface-number*]] **brief**

4.4 設定例

4.4.1 IP アドレス設定例

I. ネットワーク要件

図 4-3 に示すように、VLAN1 の AP は、2 つのネットワーク 172.16.1.0/24 と 172.16.2.0/24 で構成された LAN に接続されています。

2 つのネットワーク要素のホストが、AP を介して外部ネットワークと通信できるようにするため、および LAN のホストが互いに通信できるようにするために、以下の設定を行います。

- プライマリ IP アドレスとセカンダリ IP アドレスを AP の VLAN-interface 1 に割り当てます。
- AP のプライマリ IP アドレスを、サブネット 172.16.1.0/24 の PC のゲートウェイアドレスとして設定します。また、AP のセカンダリ IP アドレスを、サブネット 172.16.2.0/24 の PC のゲートウェイアドレスとして設定します。
- AP の無線サービスを設定します。

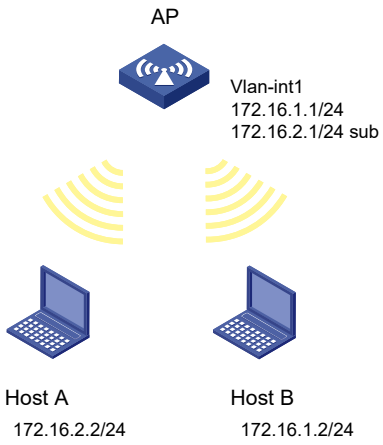


図 4-3 ネットワーク図

II. 設定手順

プライマリ IP アドレスとセカンダリ IP アドレスを VLAN-interface 1 に割り当てます。

```
<AP> system-view
[AP] interface vlan-interface 1
[AP-Vlan-interface1] ip address 172.16.1.1 255.255.255.0
[AP-Vlan-interface1] ip address 172.16.2.1 255.255.255.0 sub
```

サブネット 172.16.1.0/24 に割り振られた PC で、ゲートウェイアドレスを 172.16.1.1 に設定します。またサブネット 172.16.2.0/24 に割り振られた PC で、ゲートウェイアドレスを 172.16.2.1 に設定します。

III. 設定の確認

サブネット 172.16.1.0/24 のホストと AP の通信状況を確認します。

```
<AP> ping 172.16.1.2
Ping 172.16.1.2 (172.16.1.2): 56 data bytes, press CTRL_C to break
56 bytes from 172.16.1.2: icmp_seq=0 ttl=128 time=7.000 ms
56 bytes from 172.16.1.2: icmp_seq=1 ttl=128 time=2.000 ms
56 bytes from 172.16.1.2: icmp_seq=2 ttl=128 time=1.000 ms
56 bytes from 172.16.1.2: icmp_seq=3 ttl=128 time=1.000 ms
56 bytes from 172.16.1.2: icmp_seq=4 ttl=128 time=2.000 ms

--- Ping statistics for 172.16.1.2 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.000/2.600/7.000/2.245 ms
```

サブネット 172.16.2.0/24 のホストと AP の通信状況を確認します。

```
<AP> ping 172.16.2.2
Ping 172.16.2.2 (172.16.2.2): 56 data bytes, press CTRL_C to break
56 bytes from 172.16.2.2: icmp_seq=0 ttl=128 time=2.000 ms
56 bytes from 172.16.2.2: icmp_seq=1 ttl=128 time=7.000 ms
56 bytes from 172.16.2.2: icmp_seq=2 ttl=128 time=1.000 ms
56 bytes from 172.16.2.2: icmp_seq=3 ttl=128 time=2.000 ms
56 bytes from 172.16.2.2: icmp_seq=4 ttl=128 time=1.000 ms

--- Ping statistics for 172.16.2.2 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.000/2.600/7.000/2.245 ms
```

サブネット 172.16.1.0/24 のホストとサブネット 172.16.2.0/24 のホストの通信状況を確認します。Ping 動作は成功します。

目次

このセクションのページは **5-x-x** です。

5 章 DHCP の概要 5-1
5.1 DHCP アドレスの割り当て 5-1
5.1.1 割り当てメカニズム 5-1
5.1.2 IP アドレスの割り当てプロセス 5-2
5.1.3 IP アドレスのリース延長 5-3
5.2 DHCP メッセージフォーマット 5-3
5.3 DHCP オプション 5-4
5.3.1 一般的な DHCP オプション 5-4
5.3.2 自己定義 DHCP オプション 5-5
5.4 プロトコルと標準 5-7

5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 5-1 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。

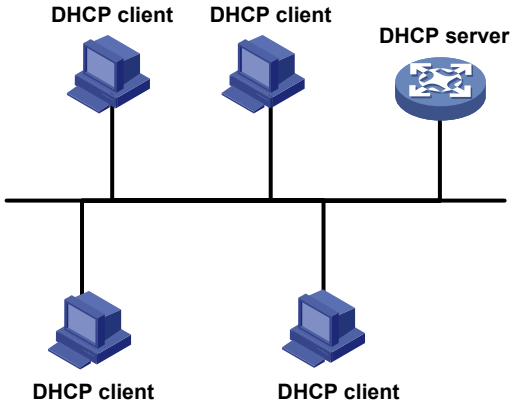


図 5-1 一般的な DHCP の構成

5.1 DHCPアドレスの割り当て

5.1.1 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。

5.1.2 IP アドレスの割り当てプロセス

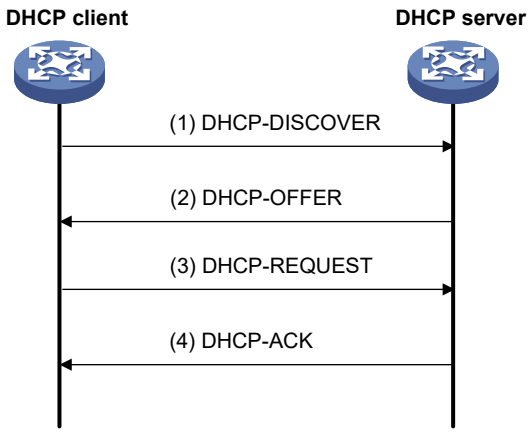


図 5-2 IP アドレスの割り当てプロセス

図 5-2 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、オペレーションマニュアルのセクション 5 *IP サービス "DHCP の概要"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。

5.1.3 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。

5.2 DHCPメッセージフォーマット

図 5-3 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。

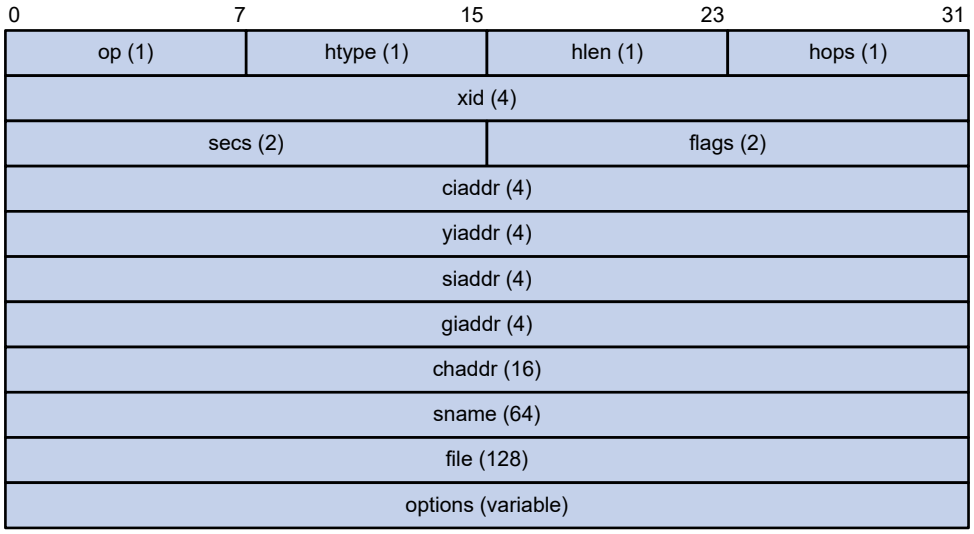


図 5-3 DHCP メッセージフォーマット

- **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。

5.3 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。

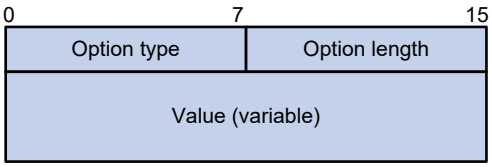


図 5-4 DHCP オプションフォーマット

5.3.1 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。

5.3.2 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

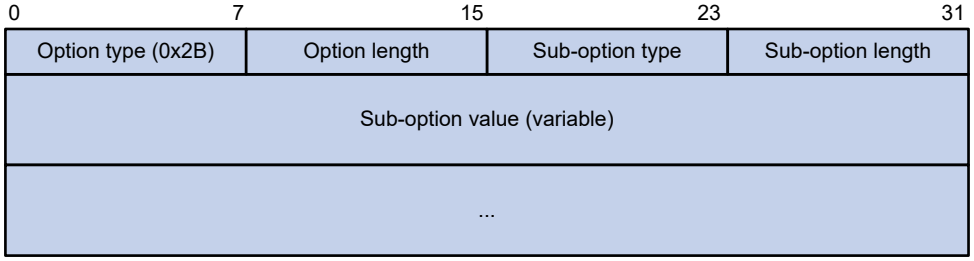


図 5-5 オプション 43 のフォーマット

図 5-5 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** – 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** – 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** – 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 5-6 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。

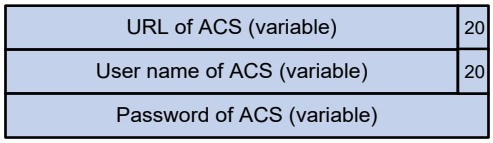


図 5-6 サブオプションフィールドのフォーマット

- **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** – 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** – 図 5-7 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。

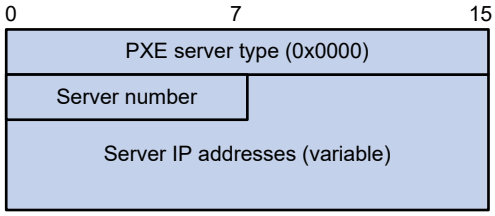


図 5-7 PXE サーバアドレスのサブオプションフィールド

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）、サブオプション 5（Link Selection）の 3 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、ダウンロード可能なプログラムを提供するサーバです。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** － プライマリネットワークコーリングプロセッサが到達不可能な場合に、DHCP クライアントがコンタクトをとるバックアップのネットワークコーリングプロセッサの IP アドレスです。
- **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 ID 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** － ターゲットユーザの IP アドレスと呼び出し番号を含むファイルオーバルートを指定します。プライマリとバックアップのコーリングプロセッサが両方とも到達不可能な場合、SIP VoIP ユーザは直接ターゲットの SIP ユーザに接続を確立するために使用する宛先 IP アドレスと呼び出し番号（SIP ユーザは IP アドレスとナンバを使用して相互に通信する）を指定します。

5.4 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。

6 章 DHCP サーバ 6-1
6.1 概要 6-1
6.1.1 DHCP アドレスプール 6-1
6.1.2 IP アドレス割り当て順序 6-2
6.2 DHCP サーバ設定作業リスト 6-3
6.3 DHCP ユーザクラスの作成 6-3
6.4 DHCP サーバのアドレスプールの設定 6-4
6.4.1 設定作業リスト 6-4
6.4.2 DHCP アドレスプールの作成 6-4
6.4.3 DHCP アドレスプールの IP アドレス範囲の設定 6-4
6.4.4 DHCP クライアントのゲートウェイの設定 6-6
6.4.5 クライアントへのドメイン名サフィックスの設定 6-7
6.4.6 DHCP クライアントの DNS サーバの設定 6-7
6.4.7 DHCP クライアントの WINS サーバと NetBIOS ノードタイプの設定 6-7
6.4.8 DHCP クライアントの BIMS サーバ情報の設定 6-8
6.4.9 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 6-8
6.4.10 DHCP クライアントのサーバの設定 6-9
6.4.11 DHCP クライアントのオプション 184 パラメータの設定 6-9
6.4.12 カスタマイズ DHCP オプションの設定 6-10
6.5 DHCP の有効化 6-11
6.6 インタフェースでの DHCP サーバの有効化 6-12
6.7 インタフェースでのアドレスプールの適用 6-12
6.8 IP アドレス競合検出の設定 6-12
6.9 オプション 82 の処理モードの有効化 6-13
6.10 DHCP サーバが送信した DHCP パケットの DSCP 値の設定 6-13
6.11 DHCP サーバの表示と維持 6-14
6.12 DHCP サーバ設定例 6-14
6.12.1 ダイナミック IP アドレスの割り当て設定例 6-15
6.12.2 自己定義オプション設定例 6-17
6.13 DHCP サーバ設定のトラブルシューティング 6-18
6.13.1 症状 6-18
6.13.2 分析 6-18
6.13.3 解決策 6-18

6章 DHCP サーバ

6.1 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

6.1.1 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。

6.1.2 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。

6.2 DHCPサーバ設定作業リスト

作業リスト
（オプション設定項目）DHCPユーザクラスの設定
（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

6.3 DHCPユーザクラスの作成

DHCP サーバは、受信した DHCP 要求のハードウェアアドレス、オプション情報、または giaddr フィールドに従って、DHCP ユーザをさまざまなユーザクラスに分類します。サーバは、異なるユーザクラスの DHCP クライアントに IP アドレスと設定パラメータを割り当てます。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. DHCP ユーザクラスを作成し、その view に移行する	**dhcp class** *class-name*	—

操作	コマンド	補足
3. DHCP ユーザクラスの一致ルールを設定します。	**if-match rule** *rule-number* **{ hardware-address** *hardware-address* **mask** *hardware-address-mask* **| option** *option-code* **[ascii** *ascii-string* **[offset** *offset* **| partial]] | hex** *hex-string* **[mask** *mask* **| offset** *offset* **length** *length* **| partial]] | relay-agent** *gateway-address* **}**	デフォルト：設定なし

6.4 DHCPサーバのアドレスプールの設定

6.4.1 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
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

6.4.2 DHCP アドレスプールの作成

操作	コマンド	補足
4. system view に移行する	**system-view**	ー
5. 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

6.4.3 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** { **day** *day* [**hour** *hour* [**minute** *minute* [**second** *second*]]] | **unlimited** }	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**	―
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**] }	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** { **day** *day* [**hour** *hour* [**minute** *minute* [**second** *second*]]] | **unlimited** }	デフォルト：1日

6.4.4 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**	―
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

操作	コマンド	補足
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

6.4.5 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。DNS の詳細は、オペレーションマニュアルのセクション 5 *IP サービス "DNS"* を参照してください。

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

6.4.6 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

6.4.7 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**	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. 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

6.4.8 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**	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. 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

6.4.9 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**	―
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

6.4.10 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**	―
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

6.4.11 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 の詳細はオペレーションマニュアルのセクション 5 *IP サービス　“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**	―

操作	コマンド	補足
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）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

6.4.12 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 6-1 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。

II. DHCP オプショングループでのカスタマイズ 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 オプショングループを作成し、その view に移行する	**dhcp option-group** *option-group-number*	―
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。
4． system view に移行する	**quit**	―
5． 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
6． DHCP ユーザクラスに DHCP オプショングループを指定する。	**class** *class-name* **option-group** *option-group-number*	デフォルト：設定なし DHCPユーザクラスは事前に作成しておく必要があります。

6.5 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

6.6 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

6.7 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**	―
2． interface view に移行する	**interface** *interface-type interface-number*	―
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。

6.8 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**	―
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。

6.9 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、オペレーションマニュアルのセクション 5 *IP サービス “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**	―
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

6.10 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**	―
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

6.11 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**

6.12 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。

6.12.1 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

0 に示すように、DHCP サーバ（Switch）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。

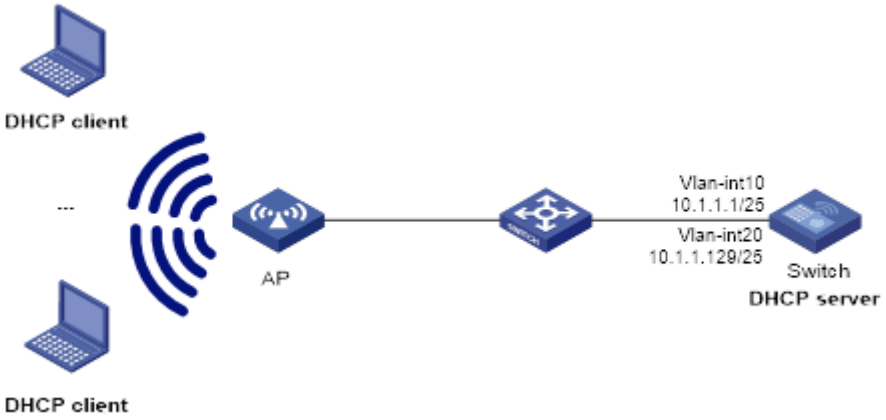


図 6-1 ネットワーク図

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。

```
<Switch> system-view
[Switch] vlan 10
[Switch -vlan10] quit
[Switch] vlan 20
[Switch -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。

```
[Switch] interface gigabitethernet 1/0/1
[Switch -GigabitEthernet1/0/2] port link-type trunk
[Switch -GigabitEthernet1/0/2] port trunk permit vlan 10
[Switch -GigabitEthernet1/0/2] port trunk pvid vlan 10
[Switch -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。

```
[Switch] interface vlan-interface 10
[Switch-Vlan-interface10] ip address 10.1.1.1 25
[Switch-Vlan-interface10] quit
[Switch-interface vlan-interface 20
[Switch-Vlan-interface20] ip address 10.1.1.129 25
```

```
[Switch-Vlan-interface20] quit
```

2)　DHCP サーバを設定します。

DHCP を有効にします。

```
[Switch] 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。

```
[Switch] interface vlan-interface 10
[Switch-Vlan-interface10] dhcp select server
[Switch-Vlan-interface10] quit
[Switch] interface vlan-interface 20
[Switch-Vlan-interface20] dhcp select server
[Switch-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。

```
[Switch] dhcp server ip-pool 1
[Switch-dhcp-pool-1] network 10.1.1.0 mask 255.255.255.128
[Switch-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。

```
[Switch] dhcp server ip-pool 2
[Switch-dhcp-pool-2] network 10.1.1.128 mask 255.255.255.128
[Switch-dhcp-pool-2] quit
```

3)　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。

```
[AP] wlan service-template service
[AP-wlan-st-service] ssid service
[AP-wlan-st-service] vlan 20
[AP-wlan-st-service] service-template enable
[AP-wlan-st-service] quit
```

AP を設定します。

```
[AP] interface WLAN-Radio1/0/1
[AC-WLAN-Radio1/0/1] service-template service1
[AC-WLAN-Radio1/0/1] radio enable
[AC-WLAN-Radio1/0/1] return
```

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。）

6.12.2 自己定義オプション設定例

I. ネットワーク要件

図 6-2 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。

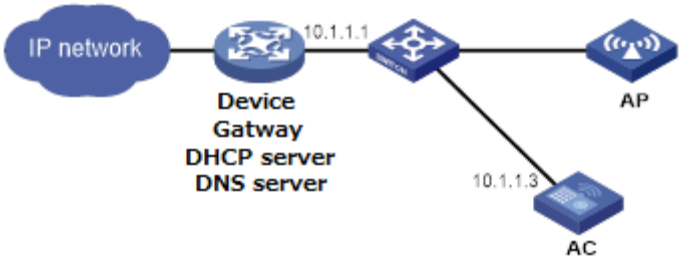


図 6-2 ネットワーク図

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
```

6.13 DHCPサーバ設定のトラブルシューティング

6.13.1 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。

6.13.2 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。

6.13.3 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。

7 章 DHCP リレー 7-1
7.1 概要 7-1
7.1.1 動作 7-1
7.1.2 DHCP リレーエージェントのオプション 82 のサポート 7-2
7.2 DHCP リレーエージェント設定作業リスト 7-2
7.3 DHCP の有効化 7-3
7.4 インタフェースでの DHCP リレーエージェントの有効化 7-3
7.5 リレーエージェントの DHCP サーバの指定 7-3
7.6 DHCP リレーエージェントセキュリティ機能の設定 7-4
7.6.1 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 7-4
7.6.2 ダイナミックリレーエントリの定期的な更新の有効化 7-4
7.7 DHCP リレーエージェントでの IP アドレスのリリース設定 7-5
7.8 オプション 82 の設定 7-5
7.9 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 7-6
7.10 DHCP クライアントのゲートウェイアドレスの設定 7-6
7.11 リレーされた DHCP 要求の送信元 IP アドレスの指定 7-7
7.12 オプション 82 に基づいた DHCP 応答を転送するための DHCP リレーエージェントの設定 7-7
7.13 DHCP リレーエージェントの表示と維持 7-8
7.14 DHCP リレーエージェント設定例 7-9
7.14.1 DHCP リレーエージェント設定例 7-9
7.15 オプション 82 の設定例 7-10
7.16 DHCP リレーエージェントのトラブルシューティング 7-11
7.16.1 症状 7-11
7.16.2 分析 7-11
7.16.3 解決策 7-11

7章 DHCP リレー

7.1 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 7-1 に DHCP リレーエージェントの標準的な構成を示します。

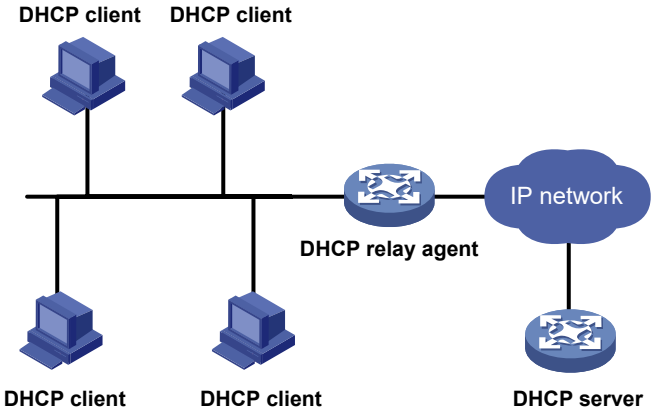


図 7-1 DHCP リレーエージェント構成

7.1.1 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、オペレーションマニュアルのセクション 5 *IP サービス　“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。

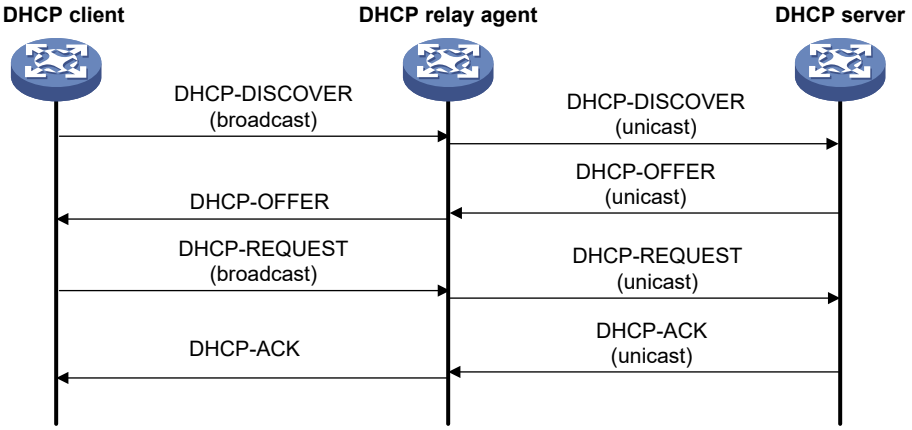


図 7-2 DHCP リレーエージェントの動作

7.1.2 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、オペレーションマニュアルのセクション 5 *IP サービス　“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 7-1 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 7-1 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。

7.2 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

作業リスト
（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
（オプション設定項目）DHCPクライアントのゲートウェイアドレスの設定
（オプション設定項目）リレーされたDHCP要求の送信元IPアドレスの指定
（オプション設定項目）オプション82に基づいたDHCP応答を転送するためのDHCPリレーエージェントの設定

7.3 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

7.4 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。

7.5 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

7.6 DHCPリレーエージェントセキュリティ機能の設定

7.6.1 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。

ARP アドレスチェック、IP ソースガードのようないくつかのセキュリティ機能は、入力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。たとえば、セキュリティ機能には ARP アドレスの確認、許可 ARP、IP ソースガードがあります。

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

🕮 **メモ：**

DHCP リレーエージェントは、同期／非同期シリアルインタフェース上で動作している DHCP クライアントに対しては、IP-MAC バインディングを記録しません。

7.6.2 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

7.7 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** *client-ip*	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。

7.8 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。DHCP サーバのオプション 82 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 5 *IP サービス “DHCP サーバ”* を参照してください。
- 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。

7.9 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

7.10 DHCPクライアントのゲートウェイアドレスの設定

デフォルトでは、DHCP DISCOVER 及び REQUEST パケットの giaddr フィールドには、リレーインタフェースのプライマリ IP アドレスが入ります。DHCP クライアントのリレーエージェントのゲートウェイアドレスを指定することができます。DHCP リレーエージェントは、DHCP DISCOVER 及び REQUEST パケットの giaddr フィールドに指摘されたゲートウェイアドレスを使います。

以下に DHCP クライアントの DHCP 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． DHCP クライアントのゲートウェイアドレスを指定する	**dhcp relay gateway ip-address**	デフォルト : リレーインタフェースのプライマリIPアドレス

7.11 リレーされたDHCP要求の送信元IPアドレスの指定

この作業は、複数のリレーインタフェースが同じ IP アドレスを共有している場合、またはリレーインタフェースに DHCP サーバへのルートがない場合に必要です。この作業を実行することで、リレーされた DHCP 要求の送信元 IP アドレスとして、DHCP リレーエージェント上の別インタフェースの IP アドレスまたは IP アドレスを指定することができます。DHCP リレーエージェントに認可アドレスプールが存在する場合、**dhcp relay source-address ip-address** コマンドは送信元 IP アドレスだけでなく **giaddr** フィールドも変更します。ユーザの認可 IP アドレスプールの構成の詳細については、オペレーションマニュアルのセクション 9 *セキュリティ　"AAA"* を参照してください。

以下に、リレーされた DHCP 要求の送信元 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． interface view に移行する	**interface** *interface-type interface-number*	―
3． リレーされた DHCP 要求の送信元 IP アドレスを指定します。	**dhcp relay source-address** { *ip-address* | **gateway** | **relay-interface** }	デフォルト：DHCPリレーエージェントは、リレーされたDHCP要求の送信元IPアドレスとして、DHCPサーバに接続するインタフェースのIPアドレスを使用します。 インタフェース上でリレーされたDHCP要求には、送信元IPアドレスを1つだけ指定できます。

7.12 オプション82に基づいたDHCP応答を転送するためのDHCPリレーエージェントの設定

DHCP リレーエージェントがオプション 82 に基づいて DHCP クライアントに DHCP 応答を転送する必要がある場合、この機能を設定します。

以下にオプション 82 に基づいて DHCP 応答を転送す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**	―
2． interface view に移行する	**interface** *interface-type interface-number*	―
3． リレーエージェントがオプション 82 を処理できるようにします。	**dhcp relay information enable**	デフォルト：無効

操作	コマンド	補足
4． Circuit ID サブオプションのパディングモードとパディングフォーマットを設定します。	**dhcp relay information circuit-id** { **bas** [**sub-interface-vlan**] | **string** *circuit-id* | { **normal** | **verbose** [**node-identifier** { **mac** | **sysname** | **user-defined** *node-identifier* }] [**interface**] } [**sub-interface-vlan**] [**format** { **ascii** | **hex** }] }	デフォルト：Circuit IDサブオプションのパディングモードは**normal**で、パディングフォーマットは**hex**です。 サブオプション1のパディングコンテンツとして設定されている場合は、装置名（**sysname**コマンドを使用して設定）にスペースを含めないでください。含めた場合、DHCPリレーエージェントはオプション82の追加または置換に失敗します。 パディングモードを**bas**、**normal**、**verbose**に設定する場合、**sub-interface-vlan**キーワードを指定する必要があります。
5． オプション 82 に基づいて DHCP 応答を転送するように DHCP リレーエージェントを設定します。	**dhcp relay forward reply by-oputionn82**	デフォルト：DHCPリレーエージェントはオプション82に基づくDHCP応答を転送しません。

7.13 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*]
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*]

7.14 DHCPリレーエージェント設定例

7.14.1 DHCP リレーエージェント設定例

I. ネットワーク要件

図 7-3 に示すように、AP の VLAN インタフェース 10 に DHCP リレーエージェントを設定します。VLAN インタフェース 10 の IP アドレスは 10.10.1.1/24 です。DHCP リレーエージェントを使用すると、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ことができます。

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、オペレーションマニュアルのセクション 5 *IP サービス　"DHCP サーバ"* を参照してください。

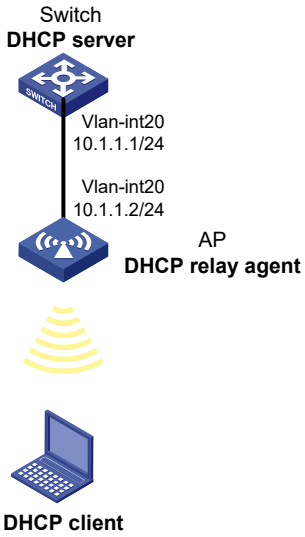


図 7-3 ネットワーク図

II. 設定手順

1)　インタフェースの IP アドレスを指定します（詳細は省略します。）
2)　AP を設定します。

AP に無線サービスの基本設定を行います。詳細は、オペレーションマニュアルのセクション 2 *WLAN* を参照してください。

DHCP を有効にします。

```
<AP> system-view
[AP] 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。

```
[AP] interface vlan-interface 10
[AP-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。

```
[AP-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。

```
[AP] 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。

```
[AP] display dhcp relay client-information
```

7.15 オプション82の設定例

I. ネットワーク要件

図 3-3 に示すように、DHCP リレーエージェント（AP）は、DHCP 要求を DHCP サーバ（スイッチ B）に転送する前に、DHCP 要求のオプション 82 を置き換えます。

- Circuit ID サブオプションは **company001** です。
- リモート ID サブオプションは **device001** です。

オプション 82 を使用するには、DHCP サーバでもオプション 82 を有効にする必要があります。

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。）

DHCP を有効にします。

```
<AP> system-view
[AP] 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。

```
[AP] interface vlan-interface 10
[AP-Vlan-interface10] dhcp select relay
```

DHCP サーバの IP アドレスを指定します。

```
[AP-Vlan-interface10] dhcp relay server-address 10.1.1.1
```

オプション 82 の処理方法とパディングの内容を設定します。

```
[AP-Vlan-interface10] dhcp relay information enable
[AP-Vlan-interface10] dhcp relay information strategy replace
[AP-Vlan-interface10] dhcp relay information circuit-id string company001
[AP-Vlan-interface10] dhcp relay information remote-id string device001
```

7.16 DHCPリレーエージェントのトラブルシューティング

7.16.1 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。

7.16.2 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。

7.16.3 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。

8 章 DHCP クライアント 8-1
8.1 インタフェースでの DHCP クライアントの有効化 8-1
8.2 アドレス重複検出の有効化 8-1
8.3 DHCP クライアントが送信する DHCP パケットの DSCP の設定 8-2
8.4 DHCP クライアントの表示と維持 8-2
8.5 DHCP クライアントの設定例 8-2

8章 DHCP クライアント

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することができます。

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。

8.1 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*	デフォルト：設定なし FITモードではデフォルトでVlan1のインタフェースが作成されています。
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 FITモードではデフォルト有効です。

8.2 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 : インタフェースで有効

8.3 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**	―
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

8.4 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*]

8.5 DHCPクライアントの設定例

I. ネットワーク要件

図 8-1 に示すように、AP は DHCP を介して IP アドレス、AC のアドレス、ゲートウェイアドレス、DNS サーバアドレスを取得します。

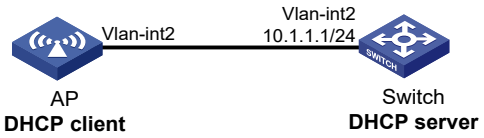


図 8-1 ネットワーク図

II. 設定手順

AP の設定をします

IP アドレス取得に DHCP を使用するように VLAN インタフェース 2 を設定します。

```
<AP> system-view
[AP] interface vlan-interface 2
[AP-Vlan-interface2] ip address dhcp-alloc
```

III. 設定の確認

AP に割り当てられた IP アドレスおよびその他のネットワークパラメータを表示します。

```
[AP] display dhcp client
```

目次

このセクションのページは **5-x-x** です。

9 章 BOOTP クライアント 9-1
9.1 BOOTP アプリケーション 9-1
9.2 動的 IP アドレスの取得 9-1
9.3 プロトコルと標準 9-1
9.4 インタフェースでの BOOTP を使用した IP アドレスの取得の設定 9-2
9.5 BOOTP クライアントの表示と維持 9-2

9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。

9.1 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。

9.2 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。

9.3 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*

9.4 インタフェースでの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

9.5 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。

10 章 DNS 10-1
10.1 概要 10-1
10.1.1 スタティックドメイン名解決 10-1
10.1.2 ダイナミックドメイン名解決 10-1
10.1.3 DNS プロキシ 10-3
10.2 DNS 設定作業リスト 10-4
10.3 IPv4 DNS クライアントの設定 10-4
10.3.1 スタティックドメイン名解決の設定 10-4
10.3.2 ダイナミックドメイン名解決の設定 10-4
10.4 DNS プロキシの設定 10-5
10.5 送信される DNS パケットの DSCP 値の設定 10-5
10.6 IPv4 DNS の表示と維持 10-6
10.7 IPv4 DNS 設定例 10-6
10.7.1 スタティックドメイン名解決の設定例 10-6
10.7.2 ダイナミックドメイン名解決の設定例 10-7
10.7.3 DNS プロキシの設定例 10-11
10.8 IPv4 DNS 設定のトラブルシューティング 10-12
10.8.1 症状 10-12
10.8.2 解決策 10-12

10章 DNS

10.1 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）な名前解決の場合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。

10.1.1 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。

10.1.2 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 10-1 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。

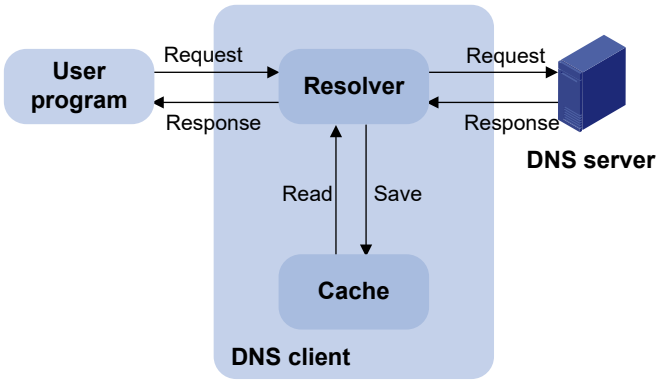


図 10-1 ダイナミックドメイン名解決

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 aabbcc.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、aabbcc を入力するだけで aabbcc.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 aabbcc）、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 aabbcc）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.aabbcc）、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、aabbcc.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。

10.1.3 DNS プロキシ

図 10-2 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。

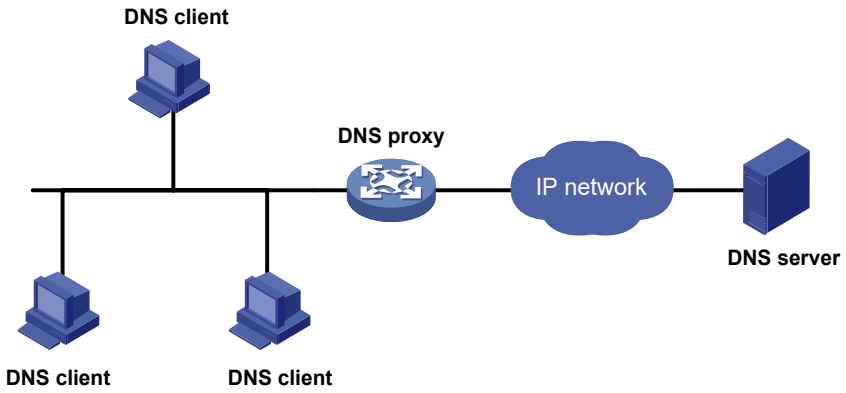


図 10-2 DNS プロキシアプリケーション

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は、DNS プロキシから指定の DNS サーバに要求が送信され、ドメイン名の解決を行います。
4) DNS サーバから応答を受け取ると、DNS プロキシは IP アドレスー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。

10.2 DNS設定作業リスト

作業リスト
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

10.3 IPv4 DNSクライアントの設定

10.3.1 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**	ー
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

10.3.2 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**	ー
2. （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。
3. DNS サーバの IPv4 アドレスを system view で設定する	**dns server** *ip-address*	デフォルト：設定なし

10.4 DNSプロキシの設定

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 プロキシの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. DNS プロキシを有効にする	**dns proxy enable**	デフォルト：無効
3. DNS サーバの IPv4 アドレスを指定する	**dns server** *ip-address*	デフォルト：指定なし

10.5 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。

10.6 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**]

10.7 IPv4 DNS設定例

10.7.1 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 10-3 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。

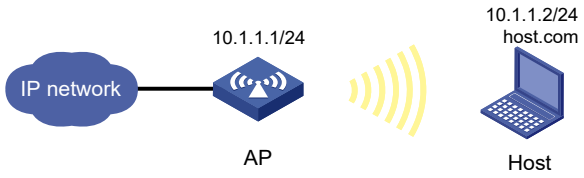


図 10-3 ネットワーク図

II. 設定手順

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。

```
<AP> system-view
[AP] 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。

```
[AP] 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
```

10.7.2 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 10-4 に示すように、以下のような設定をします。

- ホストのドメイン名 host と、com ドメイン内の IPv4 アドレス 3.1.1.1/16 間のマッピングを保管するように、DNS サーバを設定します。
- AP でダイナミック IPv4 DNS と DNS サフィックス com を設定し、AP が、ホストにアクセスするためのドメイン名 host を使用できるようにします。

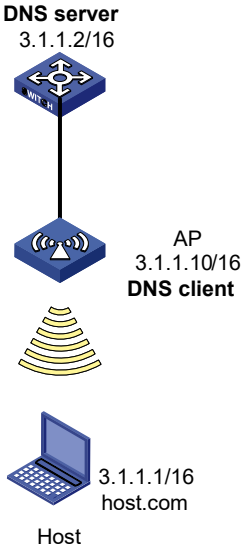


図 10-4 ネットワーク図

II. 設定手順

設定を行う前に、以下を確認してください。

- AP と Host が互いに通信可能でき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 10-4 に示すように設定されていることを確認してください。

1) DNS server を設定します。

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。

a) “Start”>“Programs”>“Administrative Tools”>“DNS”を選択します。図 10-5 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。

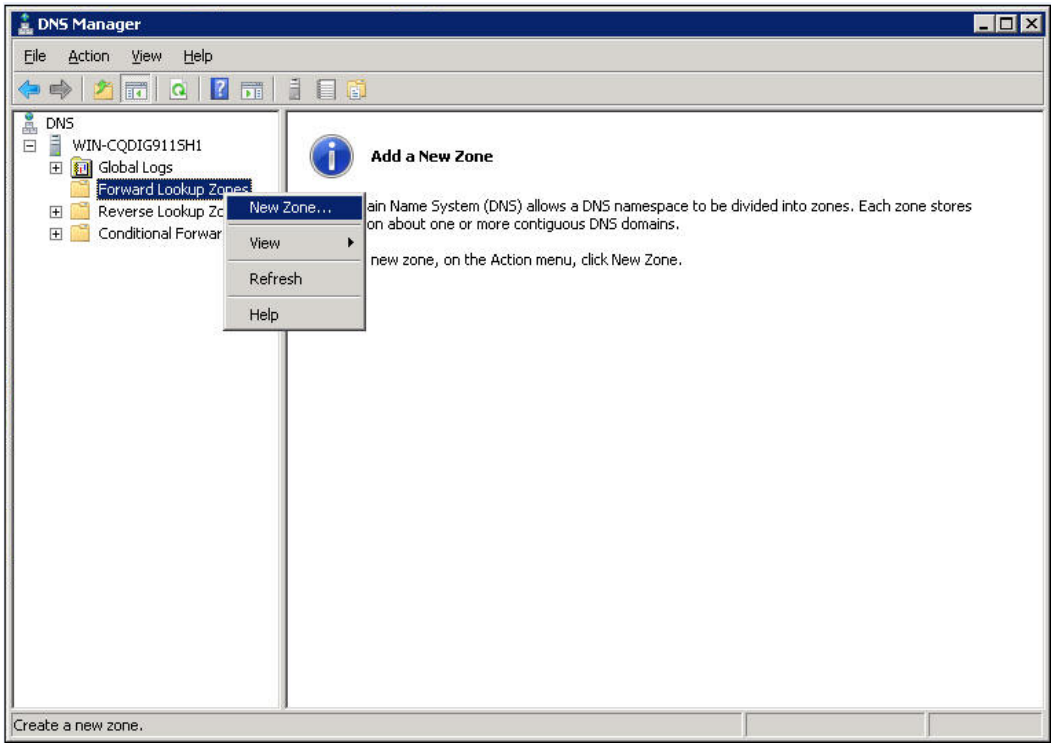


図 10-5 ゾーンの作成

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。

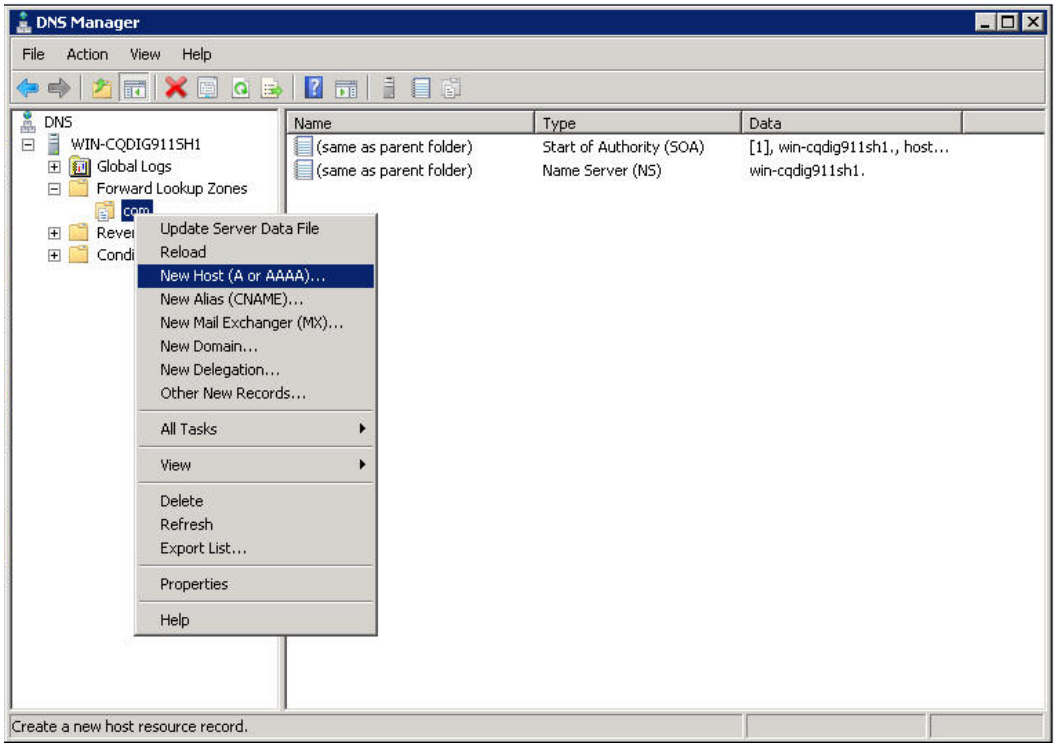


図 10-6 ホストの追加

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。

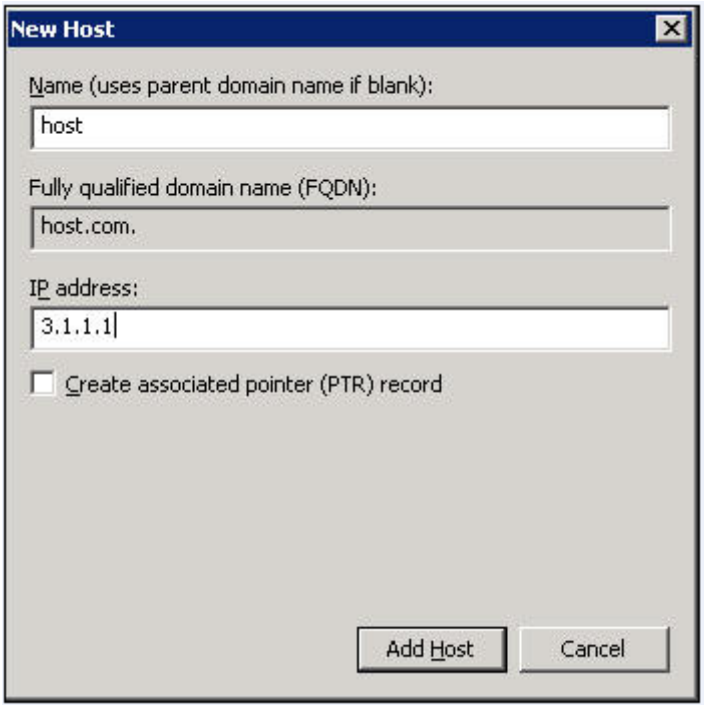


図 10-7 IP アドレスとホスト名間のマッピングの作成

2)　DNS client を設定します。

IP アドレスとして 3.1.1.2 を指定します。

```
<AP> system-view
[AP] dns server 3.1.1.2
```

#ドメイン名のサフィックスとして com を設定します。

```
[AP] dns domain com
```

III. 設定の確認

AP がダイナミックドメイン名解決を使用し、ドメイン名 host.com を IP アドレス 3.1.1.1 に変換できることを確認します。

```
[AP] ping host
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 ---
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
```

10.7.3 DNS プロキシの設定例

I. ネットワーク要件

図 10-8 に示すように DNS client（Device B）と DNS Server 間で DNS パケットを転送する DNS プロキシとして AP を設定します。DNS Server の IP アドレスは 4.1.1.1 です。

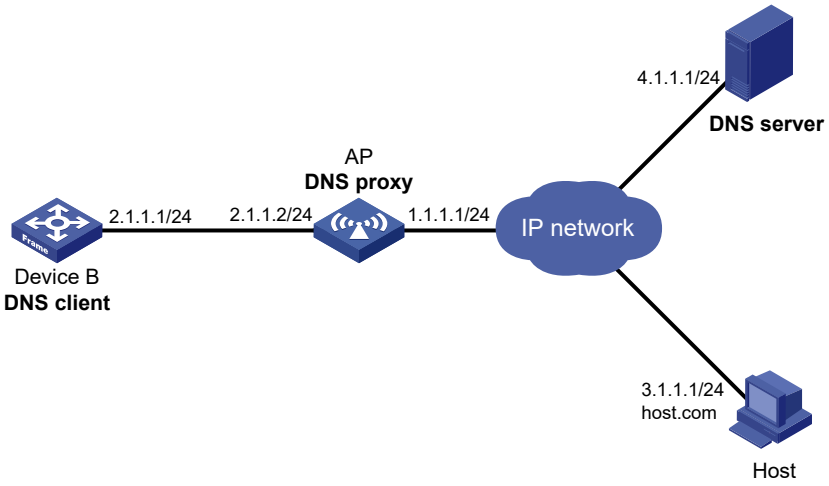


図 10-8 ネットワーク図

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。

- AP 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 10-8 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) 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 2008 R2 サーバを DNS サーバとして使用する場合、オペレーションマニュアルのセクション 5 *IP サービス "DNS" 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。

2) 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。

```
<AP> system-view
[AP] dns server 4.1.1.1
```

DNS プロキシを有効にします。

```
[AP] dns proxy enable
```

3) 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。

```
<DeviceB> system-view
[DeviceB] dns server 2.1.1.2
```

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。

[DeviceB] 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
```

10.8 IPv4 DNS設定のトラブルシューティング

10.8.1 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。

10.8.2 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。

11 章 IP パフォーマンスの最適化 11-1
11.1 ダイレクトブロードキャストの送受信の有効化 11-1
11.1.1 設定手順 11-1
11.2 インタフェースの MTU サイズの設定 11-1
11.3 TCP path MTU discovery の設定 11-2
11.4 TCP バッファサイズの設定 11-3
11.5 TCP タイマの設定 11-3
11.6 ICMP エラーパケットの送信設定 11-3
11.7 ICMP エラーメッセージのレートリミットの設定 11-5
11.8 ICMP パフォーマンスの最適化の表示と維持 11-6

11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。

11.1 ダイレクトブロードキャストの送受信の有効化

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パケットの宛先 IP アドレスの、ネットワーク ID は宛先ネットワークを識別し、ホスト ID は値がすべて 1 です。

直接接続されたネットワークに対して定義されたダイレクトブロードキャストの転送を、インタフェースが許可されている場合、ハッカーはこの脆弱性を利用して目標のネットワークに攻撃することができます。

11.1.1 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送受信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送受信を有効にする	**ip forward-broadcast**	デフォルト：無効

11.2 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

11.3 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**	ー
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

11.4 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**	ー
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：63KB

11.5 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**	ー
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

11.6 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。

- 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。
- 選択したルートがリダイレクトパケットで作成されていない、あるいは変更されていません。
- 選択されたルートが 0.0.0.0 の装置へのデフォルトルートではありません。
- 受信したパケットに送信元ルートオプションがありません。

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 宛先不能パケットを送信します。

- パケットを転送するためのルートとデフォルトルートが入手できない場合、
- 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 の詳細はオペレーションマニュアルのセクション 5 *IP サービス "DHCP の概要"* 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**	ー
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。

11.7 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** *interval* [*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。

11.8 ICMP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** [**pcb** *pcb-index*]
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** [**pcb** *pcb-index*]
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** [**pcb** *pcb-index*]
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。

12 章 NAT の概要 12-1
12.1 NAT の基本概念 12-1
12.2 基本的な NAT 操作メカニズム 12-2
12.3 NAT アプリケーション 12-2
12.3.1 従来の NAT 12-2
12.3.2 Twice NAT 12-2
12.3.3 双方向 NAT 12-2
12.4 NAT 制御 12-3
12.5 NAT 変換方式 12-3
12.5.1 スタティック NAT 12-3
12.5.2 ダイナミック NAT 12-3
12.5.3 NO-PAT 12-3
12.5.4 PAT 12-3
12.6 NAT エントリ 12-4
12.6.1 NAT セッションエントリ 12-4
12.6.2 EIM エントリ 12-5
12.6.3 NO-PAT エントリ 12-5
12.7 NAT ALG 12-5

12章 NAT の概要

NAT (Network Address Translation) は、IP パケットヘッダー内の 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。

12.1 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。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。
- **NAT 規則**ーアドレス変換の実行方法を定義する規則。
- **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、*"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 または PPPoE 経由で取得することもできます。

12.2 基本的なNAT操作メカニズム

図 12-1 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。

Direction	Before NAT	After NAT
Outbound	192.168.1.3	20.1.1.1
Inbound	20.1.1.1	192.168.1.3

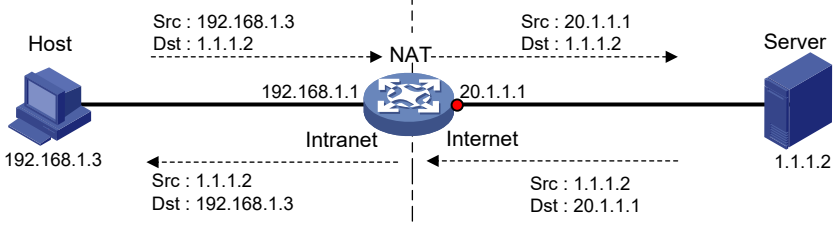


図 12-1 基本的な NAT 動作

12.3 NATアプリケーション

12.3.1 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。

12.3.2 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。

12.3.3 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。

12.4 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。

12.5 NAT変換方式

12.5.1 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。

12.5.2 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。

12.5.3 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。

12.5.4 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

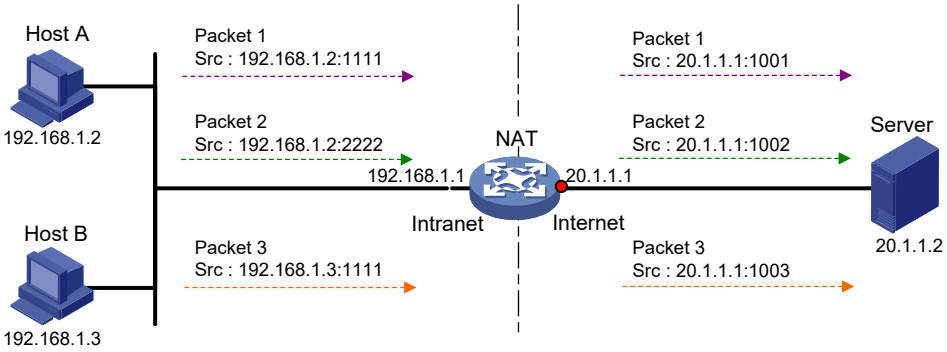


図 12-2 PAT 動作

図 12-2 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、次のマッピングがサポートされています。

- **EIM（Endpoint-Independent Mapping）**–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。

12.6 NATエントリ

12.6.1 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。

12.6.2 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、次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。

12.6.3 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。

NAT の ALG プロセス中に NO-PAT エントリを作成することもできます。

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。

12.7 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。

目次

このセクションのページは **5-x-x** です。

13 章 NAT の設定 13-1
13.1 制限とガイドライン 13-1
13.2 NAT 設定作業リスト 13-1
13.3 インタフェースでのスタティック NAT の設定 13-2
13.3.1 制限とガイドライン 13-2
13.3.2 前提条件 13-2
13.3.3 送信 1 対 1 スタティック NAT の設定 13-2
13.3.4 送信 net-to-net スタティック NAT の設定 13-3
13.3.5 受信 1 対 1 スタティック NAT の設定 13-3
13.3.6 受信 net-to-net スタティック NAT の設定 13-4
13.4 インタフェースでのダイナミック NAT の設定 13-5
13.4.1 制限とガイドライン 13-5
13.4.2 前提条件 13-5
13.4.3 送信ダイナミック NAT の設定 13-5
13.4.4 受信ダイナミック NAT の設定 13-6
13.5 NAT ALG の設定 13-7
13.6 NAT ログの設定 13-8
13.6.1 NAT セッションログの設定 13-8
13.6.2 NAT アラームログの設定 13-9
13.7 NAT 障害に対する ICMP エラーメッセージの送信の有効化 13-10
13.8 NAT の表示およびメンテナンスコマンド 13-10
13.9 NAT の設定例 13-11
13.9.1 送信 1 対 1 スタティック NAT の設定例（FAT モード） 13-11
13.9.2 送信ダイナミック NAT の設定例（FAT モード） 13-12
13.9.3 送信 1 対 1 スタティック NAT の設定例（Anchor-AC モード） 13-15
13.9.4 送信ダイナミック NAT の設定例（Anchor-AC モード） 13-16

13章 NAT の設定

13.1 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が含まれます。
- インタフェースですべての変換方式を実行する場合、NAT 規則は次の降順でソートされます。

a) スタティックNAT。

b) ダイナミックNAT。

NAT は、同じタイプのルールを NAT プライオリティ値の降順でソートします。プライオリティ値が小さいNATルールは､パケット変換のプライオリティが高いことを表します。同じタイプの NAT ルールを移動して、パケットマッチングのプライオリティを変更できます。

参照 NAT ルールの前後の行にルールを移動すると、移動したルールのプライオリティは変更されますが、参照 NAT ルールのプライオリティは変更されません。

- ルールが参照 NAT ルールの前の行に移動された場合、移動されたルールのプライオリティは、参照ルールのプライオリティ値から 1 を引いた値と等しくなります。
- ルールが参照 NAT ルールの後の行に移動された場合、移動されたルールのプライオリティは、参照ルールのプライオリティ値に 1 を加えた値と等しくなります。

13.2 NAT設定作業リスト

作業リスト
（必須設定項目）アドレス変換方式の設定 • インタフェースでのスタティックNATの設定 • インタフェースでのダイナミックNAT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ログの構成
（オプション設定項目） NAT失敗時のICMPエラーメッセージの送信の有効化

13.3 インタフェースでのスタティックNATの設定

13.3.1 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、または送信スタティック NAT とともに設定します。

13.3.2 前提条件

スタティック NAT を設定する前に、次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 の詳細については、オペレーションマニュアル セクション 8　*ACL and QoS*“*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。

13.3.3 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. 設定手順

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*] [**disable**] [**counting**]	—
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*	—
4． interface view に移行する	**interface** *interface-type interface-number*	—

操作	コマンド	補足
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

13.3.4 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. 設定手順

送信 net-to-net スタティック NAT 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 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*] [**disable**] [**counting**]	—
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

13.3.5 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. 設定手順

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*] [**disable**] [**counting**]	―
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

13.3.6 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. 設定手順

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 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*] [**disable**] [**counting**]	―
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

13.4 インタフェースでのダイナミックNATの設定

13.4.1 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 規則を設定できます。

- ACL を持つ NAT ルールは、ACL を持たないルールよりも優先されます。
- ACL ベースのダイナミック NAT ルールが 2 つ設定されている場合、ACL 番号が大きい方のルールのプライオリティが高くなります。

13.4.2 前提条件

ダイナミック NAT を設定する前に、次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。
- 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。

13.4.3 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。

- 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. 設定手順

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. NAT アドレスグループを作成し、そのビューに移行する	**nat address-group** *group-id* [**name** *group-name*]	―
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*	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**	―

操作	コマンド	補足
5． interface view に移行する	**interface** *interface-type interface-number*	―
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* | **name** *group-name* } **no-pat** [**reversible**] [**rule** *rule-name*] [**priority** *priority*] [**disable**] [**description** *text*] [**counting**] ● PATを設定する **nat outbound** [*ipv4-acl-number* | **name** *ipv4-acl-name*] [**address-group** { *group-id* | **name** *group-name* }] [**port-preserved**] [**rule** *rule-name*] [**priority** *priority*] [**disable**] [**description** text] [**counting**]	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) PAT マッピングモードを設定する	a) system viewに戻る **quit** b) 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* }]	デフォルトのマッピングモードは、Address and Port-Dependent Mappingです。このコマンドは、PATの送信ダイナミックNATだけで有効になります。
8． (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*	―

13.4.4 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、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

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**	―

操作	コマンド	補足
2． NAT アドレスグループを作成し、そのビューに移行する	**nat address-group** *group-id* [**name** *group-name*]	
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*	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*	―
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* | **name** *group-name* } [**no-pat** [**reversible**] [**add-route**]] [**rule** *rule-name*] [**priority** *priority*] [**disable**] [**description** *text*] [**counting**]	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。 **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ダイナミックに追加できます。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*	―

13.5 NAT ALGの設定

I. NAT ALG について

NAT ALG は、アプリケーション層ペイロード内のアドレスまたはポート情報を変換して、接続の確立を保証します。

たとえば、FTP アプリケーションには、データ接続と制御接続が含まれます。データ接続の IP アドレスとポート番号は、制御接続のペイロード情報によって異なります。これには、NAT ALG がアドレスおよびポート情報を変換してデータ接続を確立する必要があります。

II. 設定手順

以下に NAT ヘアピ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． 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** | **icmp-error** | **ils** | **mgcp** | **nbt** | **pptp** | **rsh** | **rtsp** | **sccp** | **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。

13.6 NATログの設定

13.6.1 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、次のイベントの 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

操作	コマンド	補足
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

13.6.2 NAT アラームログの設定

I. NAT アラームログについて

NAT リソースが十分でない場合、変換が必要なパケットはドロップされます。NO-PAT では、NAT リソースはパブリック IP アドレスを参照します。EIM PAT では、NAT リソースはパブリック IP アドレスおよびポートを参照します。NAT アラームログは NAT リソースの使用状況を監視し、NAT リソースが十分でない場合はログを出力します。

II. 制限とガイドライン

nat log alarm コマンドは、nat log enable コマンドを使用して NAT ログを有効にした後にだけ有効になります。

III. 前提条件

NAT アラームログを設定する前に、カスタム NAT ログ生成および出力機能を設定する必要があります。

IV. 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 aclキーワードは、NATアラームログでは有効になりません。
3． NAT アラームログを有効にする	**nat log alarm**	デフォルト：無効

13.7 NAT障害に対するICMPエラーメッセージの送信の有効化

I. NAT 障害に対する ICMP エラーメッセージの送信について

デフォルトでは、NAT が失敗した場合、装置は ICMP エラーメッセージを送信しません。NAT 障害に対する ICMP エラーメッセージの送信を無効にすると、不要なパケットが減少し、帯域幅が節約され、ファイアウォール IP アドレスがパブリックネットワークに公開されなくなります。

II. 制限とガイドライン

traceroute 機能には ICMP エラーパケットが必要なため、traceroute に対してこの機能を有効にします。

III. 設定手順

以下に AT 障害に対する ICMP エラーメッセージ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**	ー
2． NAT 障害に対する ICMP エラーメッセージの送信を有効にする	**nat icmp-error reply**	デフォルト：無効

13.8 NATの表示およびメンテナンスコマンド

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 EIMエントリに関する情報を表示します。	**display nat eim**
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**

操作	コマンド
NATセッションを表示します。	**display nat session** [[**responder**] { **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**

13.9 NATの設定例

13.9.1 送信 1 対 1 スタティック NAT の設定例（FAT モード）

I. ネットワーク要件

図 13-1 に示すように、192.168.1.10/24 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。

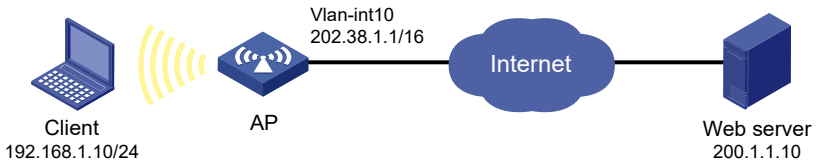


図 13-1 ネットワーク図

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 192.168.1.10 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。

```
<AP>system-view
[AP] nat static outbound 192.168.1.10 202.38.1.100
```

VLAN インタフェース 10 でスタティック NAT を有効にします。

```
[AP] interface vlan-interface 10
[AP-Vlan-interface10] nat static enable
```

III. 設定の確認

スタティック NAT の設定を確認します。

```
[AP] display nat static
           Static NAT mappings:
             Totally 1 outbound static NAT mappings.
             IP-to-IP:
               Local IP     : 192.168.1.10
               Global IP    : 202.38.1.100
               Config status: Active

           Interfaces enabled with static NAT:
             Totally 1 interfaces enabled with static NAT.
             Interface: Vlan-interface10
               Config status: Active
```

NAT セッション情報を表示します。

```
[AP] display nat session verbose
           Initiator:
             Source      IP/port: 192.168.1.10/42496
             Destination IP/port: 202.38.1.111/2048
             DS-Lite tunnel peer: -
             VPN instance/VLAN ID/Inline ID: -/-/-
             Protocol: ICMP(1)
             Inbound interface: Vlan-interface1
           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-interface10
           State: ICMP_REPLY
           Application: INVALID
           Rule ID: -/-/-
           Rule name:
           Start time: 2017-08-16 09:30:49  TTL: 27s
           Initiator->Responder:            5 packets        420 bytes
           Responder->Initiator:            5 packets        420 bytes

           Total sessions found: 1
```

13.9.2 送信ダイナミック NAT の設定例（FAT モード）

I. ネットワーク要件

図 13-2 にネットワーク図を示します。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。

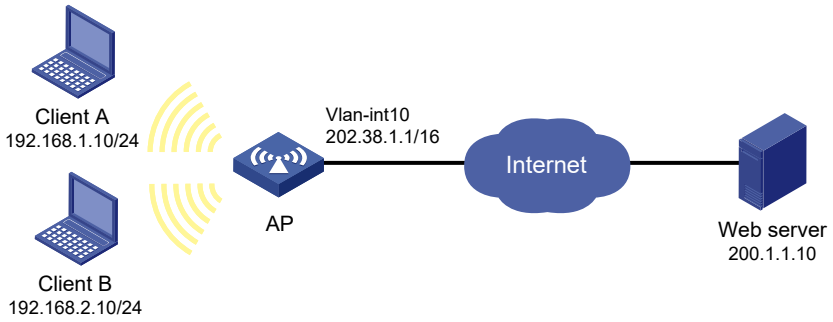


図 13-2 ネットワーク図

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。

```
<AP> system-view
[AP] nat address-group 0
[AP-address-group-0] address 202.38.1.2 202.38.1.3
[AP-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。

```
[AP] acl basic 2000
[AP-acl-ipv4-basic-2000] rule permit source 192.168.1.0 0.0.0.255
[AP-acl-ipv4-basic-2000] quit
```

VLAN インタフェース 10 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。

```
[AP] interface vlan-interface 10
[AP-Vlan-interface10] nat outbound 2000 address-group 0
```

III. 設定の確認

クライアント A は WWW サーバにアクセスできるが、クライアント 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。

```
[AP] 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

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
```

クライアント 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。

[AP] 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-interface1
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-interface10
State: ICMP_REPLY
Application: INVALID
Rule ID: -/-/-
Rule name:
Start time: 2017-08-15 14:53:29  TTL: 12s
Initiator->Responder:            1 packets         84 bytes
Responder->Initiator:            1 packets         84 bytes
```

```
Total sessions found: 1
```

13.9.3 送信 1 対 1 スタティック NAT の設定例（Anchor-AC モード）

I. ネットワーク要件

図 13-3 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。

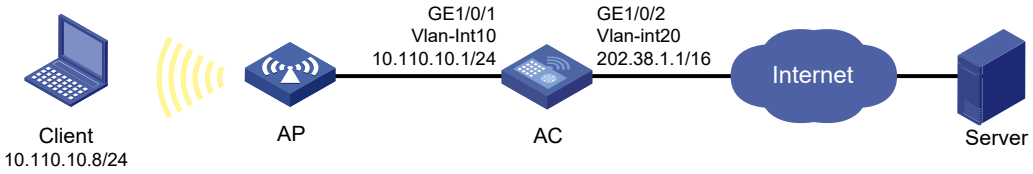


図 13-3 ネットワーク図

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

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
```

13.9.4 送信ダイナミック NAT の設定例（Anchor-AC モード）

I. ネットワーク要件

図 13-4 にネットワーク図を示します。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。

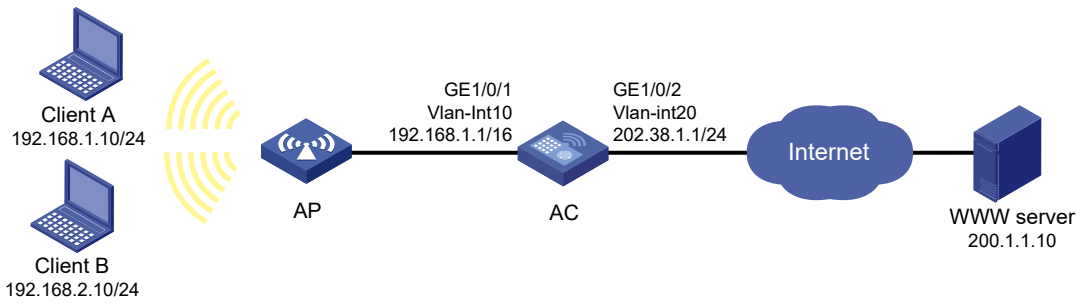


図 13-4 ネットワーク図

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

クライアント A は WWW サーバにアクセスできるが、クライアント 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
```

クライアント 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
```

QX-W1200 シリーズ アクセスポイント

オペレーションマニュアル

6. ルーティングプロトコル

本マニュアルは以下に示す章で構成されています。

01-IP ルーティングの基本
02-スタティックルーティング
03-デフォルトルート

目次

このセクションのページは**6-x-x** です。

1 章 IP ルーティングの基本 1-1
1.1 ルーティングテーブル 1-1
1.2 ルートの優先度 1-2
1.3 ロードバランス 1-2
1.4 ルートバックアップ 1-2
1.5 ルート再帰 1-3
1.6 ルート再分配 1-3
1.7 ルーティングテーブルの表示と維持 1-3

1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、オペレーションマニュアルのセクション *7 IP マルチキャスト “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。

1.1 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 1-1 にルートのカテゴリを示します。

表 1-1 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。

```
<AP> 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
...
```

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。

1.2 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 1-2 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 1-2 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
RIP	100
Unknown(信用されていない送信元からのルート)	256

1.3 ロードバランス

ルーティングプロトコルは、同一宛先への複数の最適な同一コストのルートを持ちます。これらのルートの優先順位は同じであり、同一コストで複数パス(ECMP)のロードバランス（負荷分散）を行い転送できます。

スタティックルーティングがロードバランスをサポートしています。

1.4 ルートバックアップ

ルートバックアップはネットワークの信頼性を向上させます。ルートバックアップを用いて、最も優先度が高いルートをプライマリルートに設定し、残りをセカンダリルートにすることで、同一宛先に複数のルートを設定することができます。

通常時、パケットはプライマリルートで転送されます。障害などが発生したとき、セカンダリルートの中で最も優先度が高いルートでパケットが転送されます。障害が復旧したとき、ルートの選択が行われ、プライマリルートでパケットが転送されます。

1.5 ルート再帰

ネクストホップに直接接続されていない、スタティックルートを使用する場合、ルータはネクストホップに届く送信インタフェースを検索するため、ルート再帰を行う必要があります。

RIB は、関連したルート、ルート再帰のパス、およびルート再帰の depth についての概要情報を含めて、ルート再帰情報を記録し、保存します。

1.6 ルート再分配

ルート再分配はお互いにルート情報を学習するルーティングプロトコルで有効となります。ダイナミックルーティングプロトコルは、ダイレクト、スタティックルーティングを含む他のルーティングプロトコルからのルートを再分配することができます。詳細は、オペレーションマニュアルの関連する章を参照してください。

RIB はルーティングプロトコルの再分配の情報を記録します。

1.7 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**]
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 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**6-x-x** です。

2 章 スタティックルーティング..... 2-1
2.1 スタティックルートの設定..... 2-1
2.2 スタティックルートの表示と維持..... 2-1
2.3 基本的なスタティックルートの設定例..... 2-2

2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。

2.1 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*] [**tag** *tag-value*] [**description** *description-text*]	デフォルト：設定なし
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-value*	デフォルト：60
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。

2.2 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**]

2.3 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 2-1 に示すように、ホストとクライアント間で相互接続できるように、Switch A、Switch B、AP にスタティックルートを設定します。

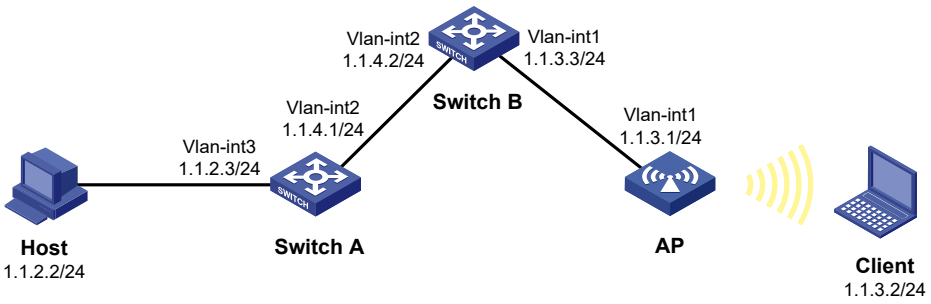


図 2-1 ネットワーク図

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。

Switch A にデフォルトルートを設定します。

```
<SwitchA> system-view
[SwitchA] ip route-static 0.0.0.0 0.0.0.0 1.1.4.2
```

Switch B に 2 つのスタティックルートを設定します。

```
<SwitchB> system-view
[SwitchB] ip route-static 1.1.2.0 255.255.255.0 1.1.4.1
```

AP にデフォルトルートを設定します。

```
<AP> system-view
[AP] ip route-static 0.0.0.0 0.0.0.0 1.1.3.3
```

3) Host と Client にそれぞれ 1.1.2.3 と 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

Switch A のルーティングテーブル情報を表示します。

```
[SwitchA] display ip routing-table

Destinations : 7        Routes : 7

Destination/Mask    Proto   Pre  Cost         NextHop         Interface

0.0.0.0/0           Static 60   0            1.1.4.2         Vlan2
1.1.2.0/24          Direct 0    0            1.1.2.3         Vlan3
1.1.2.3/32          Direct 0    0            127.0.0.1       InLoop0
1.1.4.0/30          Direct 0    0            1.1.4.1         Vlan2
1.1.4.1/32          Direct 0    0            127.0.0.1       InLoop0
```

```
127.0.0.0/8          Direct 0    0            127.0.0.1       InLoop0
127.0.0.1/32         Direct 0    0            127.0.0.1       InLoop0
```

Switch B のルーティングテーブル情報を表示します。

```
[SwitchB] display ip routing-table

Destinations : 7        Routes : 7

Destination/Mask    Proto  Pre  Cost         NextHop         Interface

1.1.2.0/24          Static 60   0            1.1.4.1         Vlan2
1.1.3.0/24          Direct 0    0            1.1.3.3         Vlan1
1.1.3.3/32          Direct 0    0            127.0.0.1       InLoop0
1.1.4.0/30          Direct 0    0            1.1.4.2         Vlan2
1.1.4.2/32          Direct 0    0            127.0.0.1       InLoop0
127.0.0.0/8         Direct 0    0            127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0            127.0.0.1       InLoop0
```

AP のルーティングテーブル情報を表示します。

```
[AP] display ip routing-table

Destinations : 5        Routes : 5

Destination/Mask    Proto  Pre  Cost         NextHop         Interface

0.0.0.0/0           Static 60   0            1.1.3.3         Vlan1
1.1.3.0/24          Direct 0    0            1.1.3.1         Vlan1
1.1.3.1/32          Direct 0    0            127.0.0.1       InLoop0
127.0.0.0/8         Direct 0    0            127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0            127.0.0.1       InLoop0
```

Host 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 XP で動作していると仮定します。)

```
C:\Documents and Settings\Administrator>ping 1.1.3.2

Pinging 1.1.3.2 with 32 bytes of data:

Reply from 1.1.3.2: bytes=32 time=1ms TTL=125
Reply from 1.1.3.2: bytes=32 time=1ms TTL=125
Reply from 1.1.3.2: bytes=32 time=1ms TTL=125
Reply from 1.1.3.2: bytes=32 time=1ms TTL=125

Ping statistics for 1.1.3.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

目次

このセクションのページは**6-x-x** です。

3 章 デフォルトルート 3-1

3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。詳細はオペレーションマニュアルのセクション 6 *ルーティングプロトコル “スタティックルーティング”* を参照してください。

QX-W1200 シリーズ アクセスポイント

オペレーションマニュアル

7. IP マルチキャスト

本マニュアルは以下に示す章で構成されています。

01-マルチキャストの概要
02-IGMP スヌーピング

目次

このセクションのページは **7-x-x** です。

1 章 マルチキャストの概要 1-1
1.1 マルチキャストの導入 1-1
1.1.1 情報通信技術 1-1
1.1.2 マルチキャストの機能 1-3
1.1.3 マルチキャストの一般的な表記方法 1-4
1.1.4 マルチキャストの利点とアプリケーション 1-4
1.2 マルチキャストモデル 1-5
1.3 マルチキャストアーキテクチャ 1-6
1.3.1 マルチキャストアドレス 1-6
1.3.2 マルチキャストプロトコル 1-10

1章 マルチキャストの概要

1.1 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。

1.1.1 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。

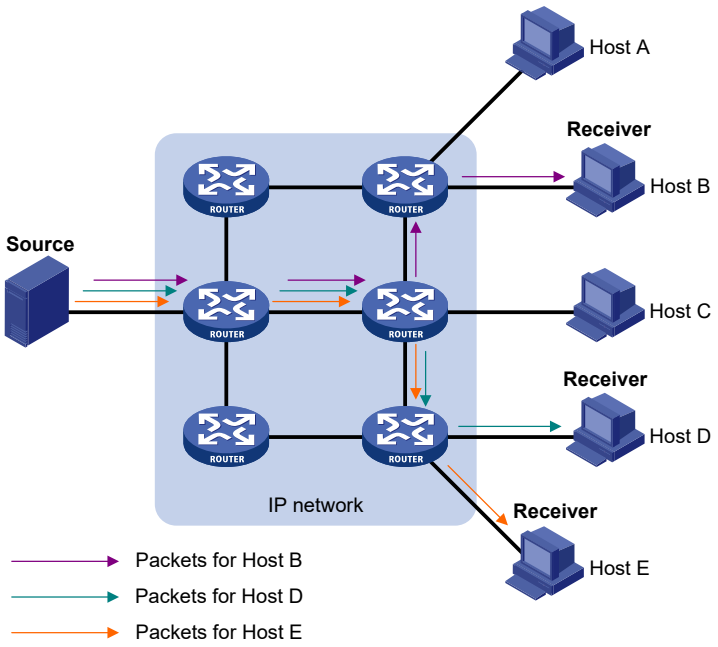


図 1-1 ユニキャスト通信

図 1-1 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。

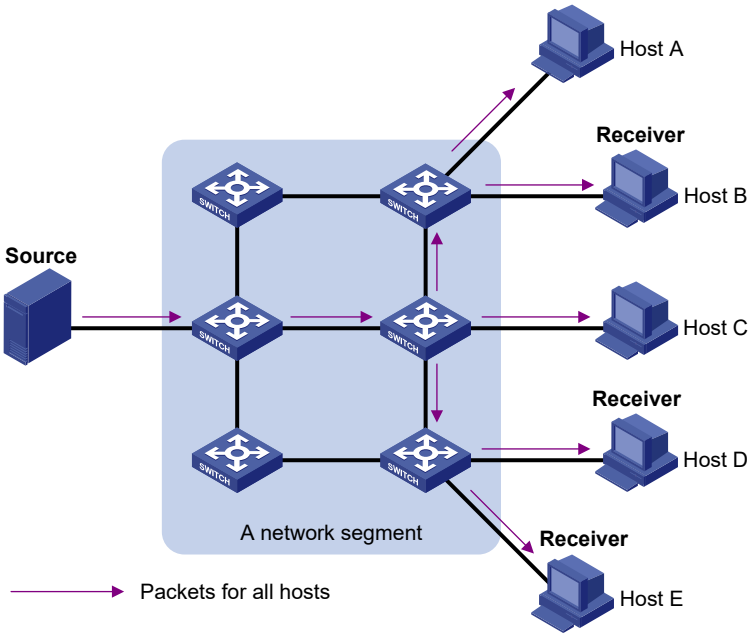


図 1-2 ブロードキャスト通信

図 1-2 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。

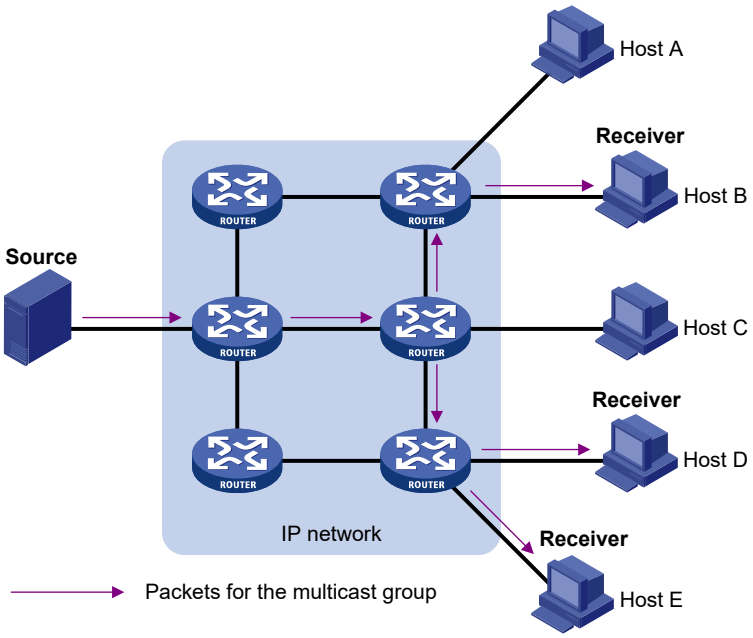


図 1-3 マルチキャスト通信

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。

1.1.2 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、マルチキャストソース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。
- マルチキャストソースは情報の送信者です。マルチキャストソース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

ャストソース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 1-1 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。	マルチキャストソース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。	ソース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。

1.1.3 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ソース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ソース、(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、マルチキャストソース 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ソース、（G）は特定のマルチキャストグループを表します。

1.1.4 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。

1.2 マルチキャストモデル

レシーバ（受信者）がマルチキャストソース（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。

I. ASM モデル

ASM モデルでは、すべてのマルチキャストソース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ソースの位置を認識していません。

II. SFM モデル

SFM モデルは ASM モデルから派生しています。センダ（送信者）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ソースからのだけ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、マルチキャストソース（送信元）がすべて有効というわけではありません。マルチキャストソースはフィルタされます。

III. 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ソース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ソース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ソースの間に専用のマルチキャスト転送パスが確立されます。

1.3 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。

- マルチキャストソース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ソース(送信元）がどこにいるのか？（マルチキャストソースディスカバリ）
- 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** － マルチキャストソース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** － マルチキャストソース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、マルチキャストソース（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。

1.3.1 マルチキャストアドレス

I. IP マルチキャストアドレス

- 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 1-2 クラス D 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のために使用されることができます。一般的な永久グループアドレスの一覧は表 1-3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。

アドレスブロック	説明
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	管理上、範囲指定された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 1-3 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のDRまたはバックアップDR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。
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。

- IPv6 マルチキャストアドレス

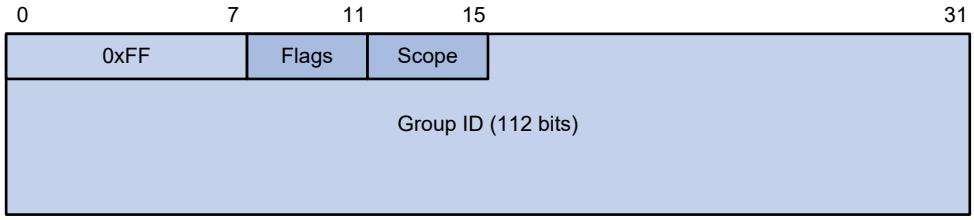


図 1-4 IPv6 マルチキャストフォーマット

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** － 8 ビットで 11111111 です。このアドレスが IPv6 マルチキャストアドレスであることを示します。
- **Flags** － 4 ビットのフラグフィールドです。



図 1-5 Flags フィールドフォーマット

表 1-4 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）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 1-5 Scope フィールドの値

値	意味
0、F	予約済み
1	インタフェースノードローカル
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

値	意味
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。

II. イーサネットマルチキャスト MAC アドレス

- 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。

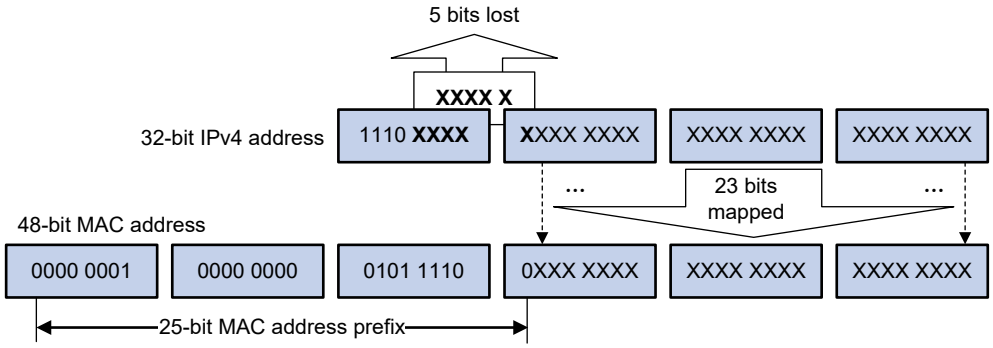


図 1-6 IPv4 アドレスと MAC アドレスのマッピング

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。

- 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。

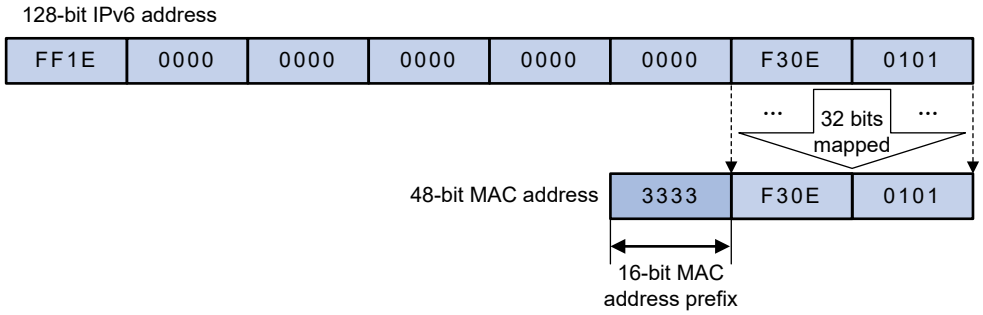


図 1-7 IPv6 アドレスと MAC アドレスのマッピング例

1.3.2 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。

I. 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。

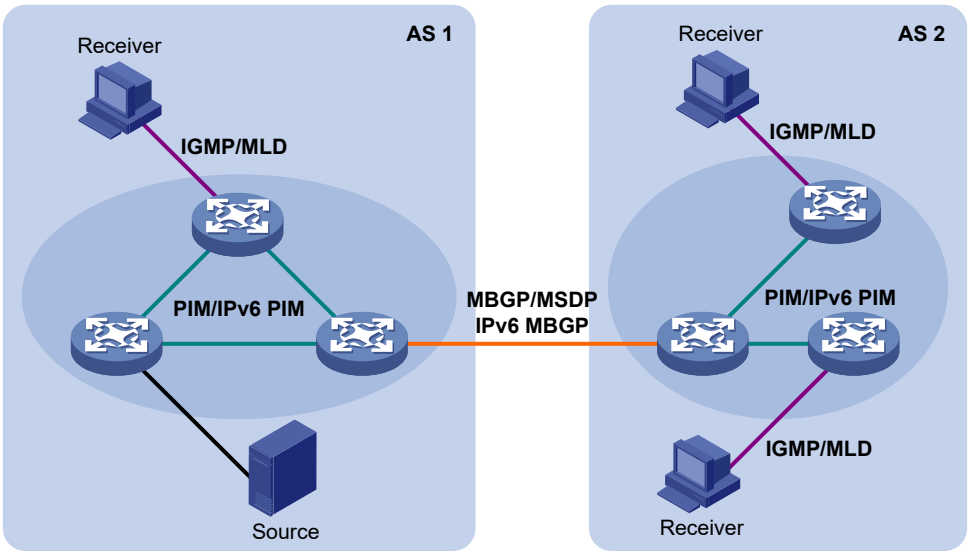


図 1-8 レイヤ 3 マルチキャストプロトコルの位置

- 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、データソース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。

II. 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。

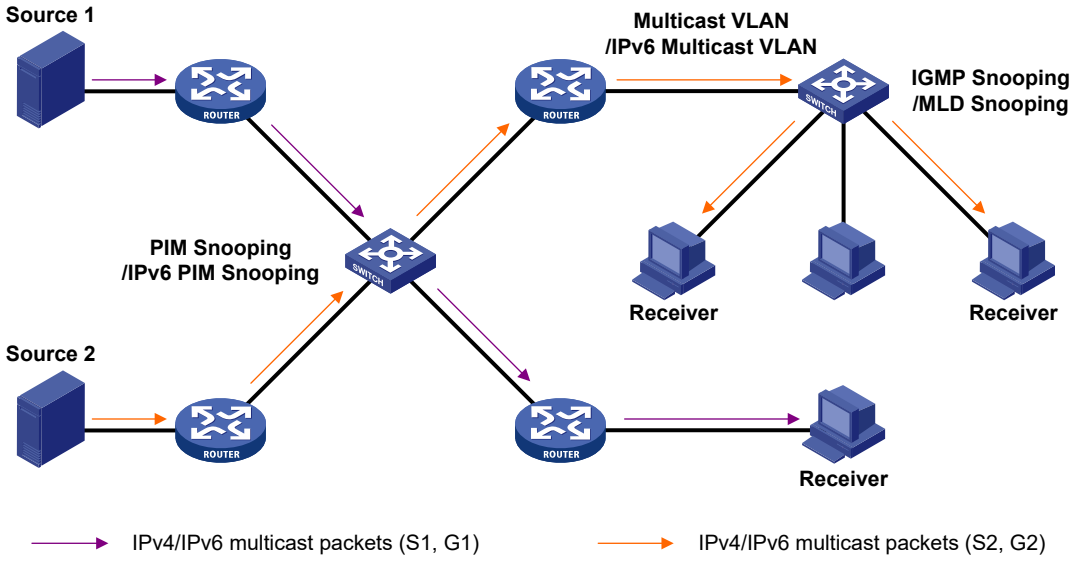


図 1-9 レイヤ 2 マルチキャストプロトコルの位置

- IGMP snooping、MLD snooping

マルチキャストの転送効率を改良するため PIM Snooping および IPv6 PIM 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。受信した PIM メッセージを解析するため、PIM snooping や IPv6 PIM snooping を動作させます。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。

目次

このセクションのページは **7-x-x** です。

2 章 IGMP スヌーピング 2-1
2.1 概要 2-1
2.1.1 IGMP snooping のポート 2-1
2.1.2 IGMP snooping の動作 2-3
2.2 プロトコルと標準 2-5
2.3 IGMP snooping 設定作業リスト 2-5
2.4 IGMP snooping の基本機能の設定 2-5
2.4.1 IGMP snooping の有効化 2-6
2.4.2 IGMP snooping のバージョンの設定 2-6
2.4.3 IGMP snooping 転送エントリの最大数の設定 2-7
2.4.4 IGMP last member クエリ間隔の設定 2-7
2.5 IGMP snooping ポート機能の設定 2-8
2.5.1 ダイナミックポートのエージングタイマの設定 2-8
2.5.2 スタティックポートの設定 2-9
2.5.3 シミュレーティッドメンバホストの設定 2-9
2.5.4 fast-leave 処理の有効化 2-10
2.6 IGMP snooping クエリの設定 2-11
2.6.1 設定要件 2-11
2.6.2 IGMP snooping クエリアの有効化 2-11
2.6.3 IGMP クエリと response のパラメータの設定 2-12
2.7 IGMP メッセージのパラメータの設定 2-13
2.7.1 設定要件 2-13
2.7.2 IGMP メッセージの送信元 IP アドレスの設定 2-13
2.7.3 IGMP メッセージの 802.1p 優先度の設定 2-14
2.8 IGMP snooping ポリシーの設定 2-15
2.8.1 マルチキャストグループポリシーの設定 2-15
2.8.2 未知のマルチキャストデータ廃棄機能の有効化 2-16
2.8.3 IGMP report 抑制機能の有効化 2-17
2.8.4 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 2-17
2.8.5 マルチキャストグループ置き換え機能の有効化 2-18
2.9 IGMP snooping の表示と維持 2-19
2.10 IGMP snooping 設定例 2-19
2.10.1 ネットワーク要件 2-19
2.10.2 設定手順 2-20
2.11 IGMP snooping のトラブルシューティング 2-21
2.11.1 レイヤ 2 マルチキャスト転送ができない 2-21
2.11.2 マルチキャストグループポリシーが動作しない 2-22

2章 IGMP スヌーピング

2.1 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 2-1 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。レイヤ 2 装置で 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 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。

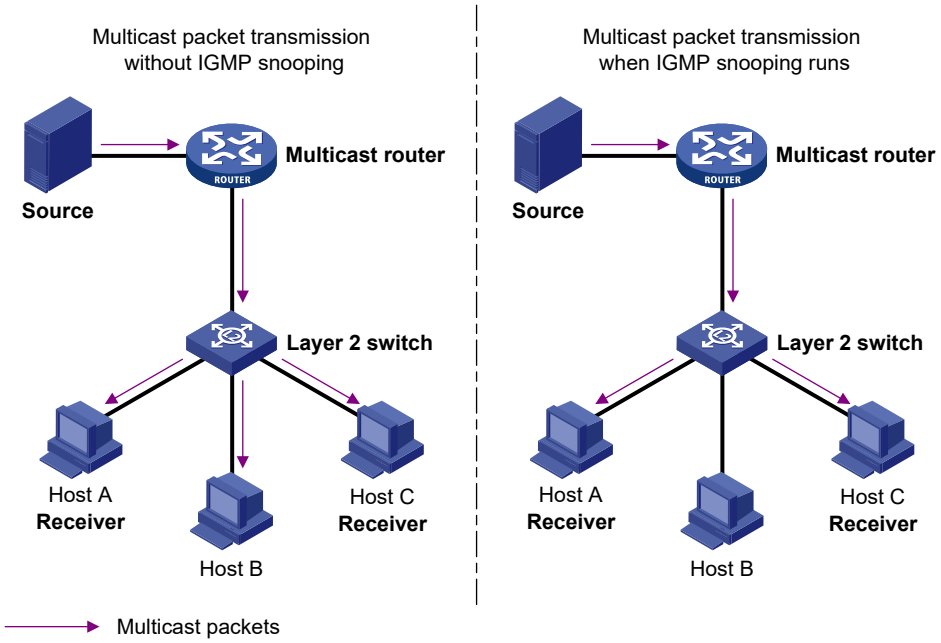


図 2-1 IGMP snooping を有効にする前と有効にした後のマルチキャストパケットの転送

2.1.1 IGMP snooping のポート

図 2-2 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。

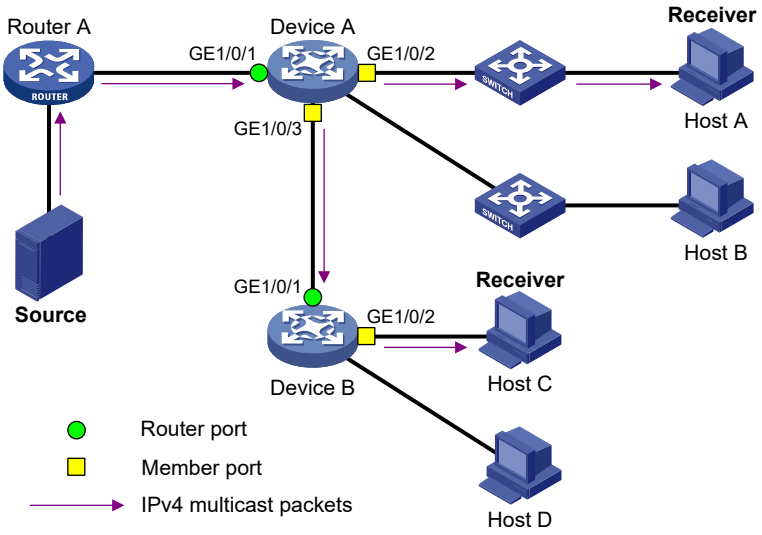


図 2-2 IGMP snooping 関連ポート

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 2-2 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 2-2 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。

2.1.2 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、オペレーションマニュアルのセクション 7 *マルチキャスト “IGMP スヌーピング”* 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。

2.2 プロトコルと標準

RFC 4541, *Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches*

2.3 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

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。

2.4 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。

2.4.1 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**	―
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**	―
4． VLAN view に移行する	**vlan** *vlan-id*	―
5． VLAN で IGMP snooping を有効にする	**igmp-snooping enable**	デフォルト：無効

2.4.2 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、オペレーションマニュアルのセクション 7 *マルチキャスト “IGMP スヌーピング”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**	―
2． VLAN view に移行する	**vlan** *vlan-id*	―
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

2.4.3 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

2.4.4 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

2.5 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。

2.5.1 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

2.5.2 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

2.5.3 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

2.5.4 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

2.6 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。

2.6.1 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。

2.6.2 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

2.6.3 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

操作	コマンド	補足
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

2.7 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。

2.7.1 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。

2.7.2 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**	ー
2. VLAN view に移行する	**vlan** *vlan-id*	ー
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。

2.7.3 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**	ー

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-number*	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-number*	デフォルト：設定なし

2.8 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。

2.8.1 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

2.8.2 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。IGMP-snooping view での drop-unknown コマンドと VLAN view での **igmp-snooping drop-unknown** コマンドは互いに排他的です。同一装置にこれらのコマンドを設定することはできません。
- この機能を VLAN で有効にするために、装置は VLAN に対する未知の IPv4 マルチキャストデータを、VLAN 内の別のルータポートに転送します。

II. グローバル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． IGMP-snooping view に移行する	**igmp-snooping**	―
3． 未知のマルチキャストデータ廃棄機能をグローバルで有効にする	**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。

III. 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。

2.8.3 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

2.8.4 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**	―

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

2.8.5 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

2.9 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*] [**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** [**verbose** | **vlan** *vlan-id*]
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**

2.10 IGMP snooping設定例

2.10.1 ネットワーク要件

図 2-3 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 AP を設定します。

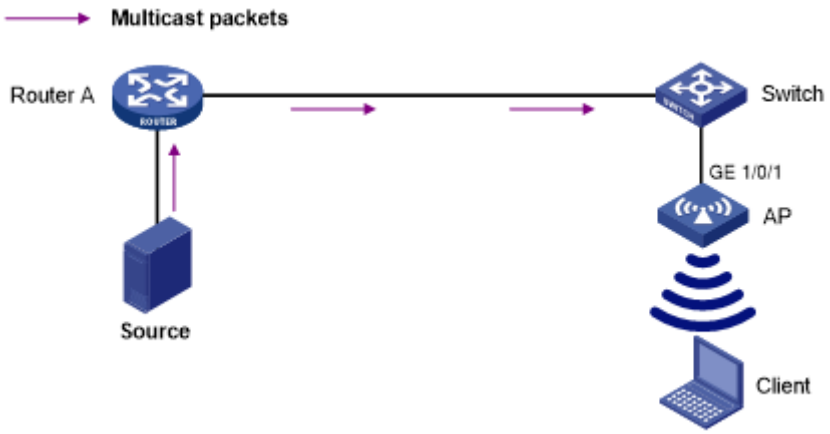


図 2-3 ネットワーク図

2.10.2 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有効にします。また、Switch と接続したポートで PIM-DM と IGMP を有効にします。（詳細は省略します。）

II. WLAN サービスの設定

1)　WLAN サービスの設定

VLAN 100 を作成します。

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

service template 1 を作成し、service template のために SSID を Multicast に設定します。

```
[AP] wlan service-template 1
[AP-wlan-st-1] ssid Multicast
```

service template 1 を経由してオンラインになるクライアントに VLAN 100 を割り当て、service template を有効にします。

```
[AP-wlan-st-1] vlan 100
[AP-wlan-st-1] service-template enable
[AP-wlan-st-1] quit
```

service template 1 を WLAN-Radio 1/0/1 に結び付けます。

```
[AP] interface WLAN-Radio 1/0/1
[AP-WLAN-Radio1/0/1] service-template 1
```

```
[AP-WLAN-Radio1/0/1] quit
```

2) VLAN 100 で IGMP snooping を有効にし、IGMP snooping のバージョンを 3 に設定します。

```
[AP] igmp-snooping
[AP-igmp-snooping] quit
[AP] vlan 100
[AP-vlan100] igmp-snooping enable
[AP-vlan100] igmp-snooping version 3
[AP-vlan100] quit
```

3) GigabitEthernet 1/0/1 を trunk ポートに設定し、ポートに VLAN 100 を割り当てます。

```
[AP] interface GigabitEthernet 1/0/1
[AP-GigabitEthernet1/0/1] port link-type trunk
[AP-GigabitEthernet1/0/1] port trunk permit vlan 100
[AP-GigabitEthernet1/0/1] quit
```

III. 設定の確認

無線クライアントが 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 に対するマルチキャストデータを受信できるか確認します。（詳細は省略します。）

2.11 IGMP snoopingのトラブルシューティング

2.11.1 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、販売店もしくは担当営業に問い合わせてください。

2.11.2 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、販売店もしくは担当営業に問い合わせてください。

QX-W1200 シリーズ アクセスポイント

オペレーションマニュアル

8. ACL and QoS

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-QoS の概要
03-QoS ポリシー
04-プライオリティマッピング
05-トラフィックポリシング
06-トラフィックフィルタリング
07-プライオリティマーキング
08-タイムレンジ
09-付録

目次

このセクションのページは**8-x-x** です。

1 章 ACL 1-1
1.1 概要 1-1
1.1.1 ACL タイプ 1-1
1.1.2 ACL の番号づけと命名 1-2
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 1-3
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 1-4
1.4 標準 ACL の設定 1-4
1.5 拡張 ACL の設定 1-5
1.6 L2 ACL の設定 1-6
1.7 WLAN client ACL の設定 1-7
1.8 WLAN AP ACL の設定 1-7
1.9 ACL のコピー 1-8
1.10 ACL によるパケットフィルタリングの設定 1-9
1.11 サービステンプレートに適用するパケットフィルタの設定 1-9
1.12 ACL の表示と維持 1-10

1章 ACL

🕮 **メモ：**
IPv6 ACL はサポートしていません。

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ます。ACL を使用して、モジュールにおけるパケットの廃棄、転送を決定します。

⚠ **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 タイプ

タイプ	ACL 番号	IP バージョン	マッチング基準
WLAN client ACL	100～199	IPv4	SSID
標準ACL	2000～2999	IPv4	送信元IPアドレス
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
L2 ACL	4000～4999	IPv4	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（QoS など）は暗黙の permit となり、ソフトウェアベースの ACL（telnet, snmp など）は暗黙の deny になります。

1.1.2 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。

標準 IPv4 ACL と拡張 IPv4 ACL では、IPv4 で固有の ACL 番号と名前を使用する必要があります。

L2、WLAN client では、固有の ACL 番号と名前を使用する必要があります。

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。

IPv4 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 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. VPN インスタンス 2. 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。） 3. ルールが作成された順
拡張IPv4 ACL	1. VPN インスタンス 2. プロトコルタイプが IP よりも高いレイヤかどうか 3. 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 4. 宛先 IP アドレスのワイルドカードマスクの 0 が多い順 5. TCP/UDP のポート番号の範囲が小さい順 6. 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によるパケットフィルタの設定
（オプション設定項目）サービステンプレートに適用するパケットフィルタの設定

1.4 標準ACLの設定

標準 IPv4 ACL は送信元 IP 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 IPv4 ACL を作成し、その view に移行する	● **acl basic** { *acl-number* | **name** *acl-name* } [**match-order** { **auto** | **config** }] ● **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。
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

操作	コマンド	補足
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

1.5 拡張ACLの設定

拡張 IPv4 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 IPv4 ACL と比較すると、拡張 IPv4 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。

以下に拡張 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． 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** }] • **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。
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

操作	コマンド	補足
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

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**	―
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** }] • **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。
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

操作	コマンド	補足
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

1.7 WLAN client ACLの設定

WLAN client ACL は、WLAN クライアントが WLAN にアクセスするために使用する SSID にもとづいてパケットを照合します。WLAN client ACL を使用することで、WLAN クライアントのアクセス制御行うことが出来ます。

以下に WLAN client 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. WLAN client ACL を作成し、その view に移行する	**acl wlan client** { *acl-number* | **name** *acl-name* }	デフォルト：設定なし 設定範囲は100～199です。 WLAN client ACLの番号を指定する場合、**acl wlan client** *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。 WLAN client ACLの名前を指定する場合、**acl wlan client 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）WLAN client 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** } [**ssid** *ssid-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

1.8 WLAN AP ACLの設定

WLAN AP ACL は、MAC アドレスまたはシリアル ID にもとづいて WLAN AP からのパケットを照合します。

以下に WLAN AP 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

操作	コマンド	補足
2. WLAN AP ACL を作成し、その view に移行する	**acl wlan ap** { *acl-number* | **name** *acl-name* }	デフォルト：設定なし 設定範囲は200～299です。 WLAN AP ACLの番号を指定する場合、**acl wlan ap** *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。 WLAN client ACLの名前を指定する場合、**acl wlan ap 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）WLAN AP 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 0から開始します。
5. ルールを作成/修正する	**rule** [*rule-id*] { **deny** | **permit** } [**mac** *mac-address mac-mask*] [**serial-id** *serial-id*]	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

1.9 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** [**mac**] **copy** { *source-acl-number* | **name** *source-acl-name* } **to** { *dest-acl-number* | **name** *dest-acl-name* }

1.10 ACLによるパケットフィルタリングの設定

🕮 **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。

ここでは、ACL を適用して、指定したインタフェースで送信または受信するパケットをフィルタリングする手順について説明します。この機能は、アグリゲートメンバーポートでは有効になりません。

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． パケットをフィルタするために ACL をインタフェースに適用する	**packet-filter** [**mac**] { *acl-number* | **name** *acl-name* } { **inbound** | **outbound** }	デフォルト：設定なし インタフェースの同じ方向に、最大32のACLを適用できます。

1.11 サービステンプレートに適用するパケットフィルタの設定

🕮 **メモ：**

この機能を FIT または Anchor-FIT AP にバインドしたサービステンプレートで動作させる場合、AC ではなく、FIT または Anchor-FIT AP 側に ACL を設定する必要があります。コンフィグレーションプロファイル機能、または **map-configuration** コマンドを使用して ACL を設定してください。

ここでは、サービステンプレートに ACL を適用して、帰属したクライアントが送信または受信するパケットをフィルタリングする手順について説明します。

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． パケットをフィルタするために ACL をサービステンプレートに適用する	**packet-filter** { *acl-number* | **name** *acl-name* } { **inbound** | **outbound** }	デフォルト：設定なし サービステンプレートの同じ方向に、最大1のACLを適用できます。

1.12 ACL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
ACLの設定とマッチした統計情報を表示する	**display acl** [**mac** | **wlan**] { *acl-number* | **all** | **name** *acl-name* }

目次

このセクションのページは**8-x-x** です。

2 章 QoS の概要 2-1
2.1 QoS サービスモデル 2-1
2.1.1 ベストエフォートサービスモデル 2-1
2.1.2 IntServ モデル 2-1
2.1.3 DiffServ モデル 2-2
2.2 QoS 技術の概要 2-2
2.2.1 ネットワークの QoS 技術の展開 2-2
2.2.2 装置の QoS 処理フロー 2-2

2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。

2.1 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。

2.1.1 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。

2.1.2 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。

2.1.3 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。

2.2 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ー

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。

2.2.1 ネットワークの QoS 技術の展開

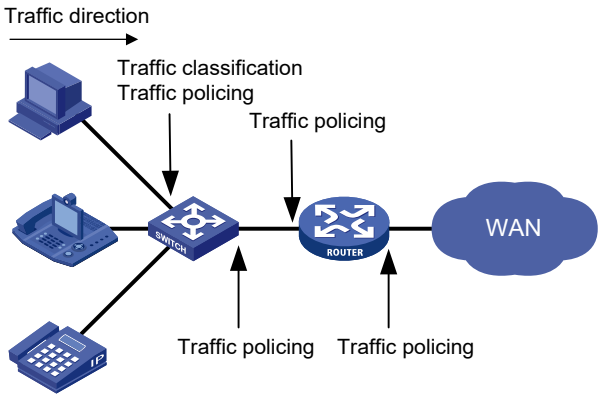


図 2-1 ネットワークの QoS 技術の位置

図 2-1 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ー**－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。

2.2.2 装置の QoS 処理フロー

図 2-2 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。

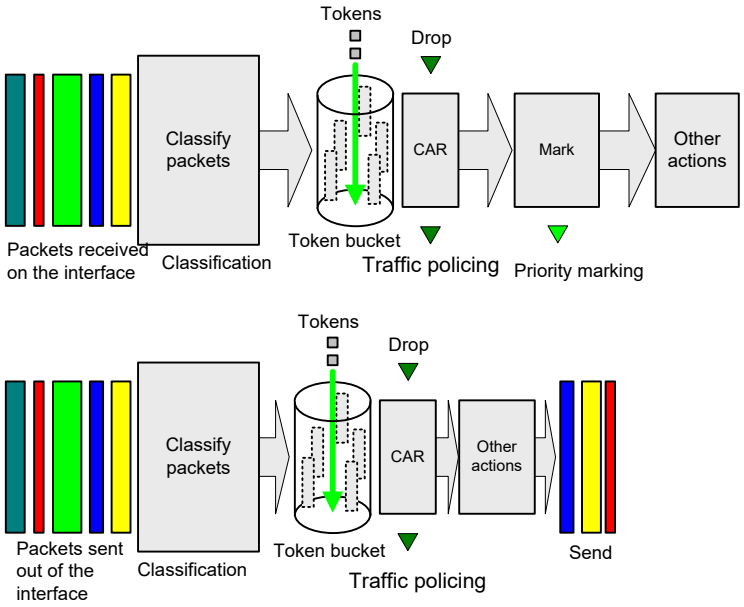


図 2-2 QoS 処理フロー

目次

このセクションのページは**8-x-x** です。

3 章 QoS ポリシー 3-1
3.1 非ポリシーベースのアプローチ 3-1
3.2 ポリシーベースのアプローチ 3-1
3.3 QoS ポリシーの設定手順 3-1
3.4 トラフィッククラスの定義 3-2
3.5 トラフィック動作の定義 3-2
3.6 QoS ポリシーの定義 3-3
3.7 QoS ポリシーの適用 3-3
3.7.1 インタフェースへの QoS ポリシーの適用 3-3
3.7.2 グローバル QoS ポリシーの適用 3-4
3.8 QoS ポリシーの情報表示と維持 3-4

3章 QoS ポリシー

QoS 設定は、ポリシーベースあるいは非ポリシーベースの 2 つのアプローチが利用可能です。ただし一部の機能は 1 つだけのサポートとなります。

3.1 非ポリシーベースのアプローチ

QoS ポリシーを使用せずに QoS サービスパラメータを使用する設定を非ポリシーベースと呼びます。

3.2 ポリシーベースのアプローチ

QoS ポリシーによる QoS サービスパラメータを使用して設定する設定をポリシーベース MQC（Modular QoS Configuration）と呼びます。ポリシーベースは、トラフィックの異なるクラスに対応するため、トラフィックポリシーやほかの QoS アクションを定義します。

トラフィッククラスはトラフィックを特定するための条件を定義し、論理積（AND）または論理和（OR）の演算子（オペレータ）を使用します。

- オペレータが AND である場合、パケットはトラフィッククラスの一致条件すべてにマッチする必要があります。
- オペレータが OR である場合、パケットはトラフィッククラスの一致条件のいずれかにマッチします。

トラフィック動作（traffic behavior）でパケットの優先順位のマーキング等の QoS アクションを定義します。

QoS ポリシーでトラフィッククラスとトラフィック動作を関連づけます。トラフィッククラスで定義した条件で特定されたトラフィックをトラフィック動作で定義した QoS アクションで処理させることができます。

3.3 QoSポリシーの設定手順

図 3-1 に QoS ポリシーの設定手順を示します。

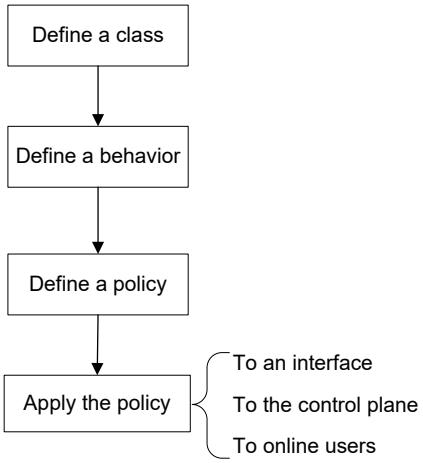


図 3-1 QoS ポリシーの設定手順

3.4 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**	―
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． 一致条件を設定する	**if-match** *match-criteria*	デフォルト：設定なし **if-match**コマンドの詳細はコマンドマニュアルのセクション8 *ACL and QoS “QoSポリシー”* を参照してください。

3.5 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、オペレーションマニュアルのセクション8 *ACL and QoS* を参照してください。	デフォルト：設定なし

3.6 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。

3.7 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。
- **グローバル**－QoS ポリシーはすべてのポートで送受信したトラフィックに適用します。

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）

3.7.1 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*	―

操作	コマンド	補足
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

3.7.2 グローバル QoS ポリシーの適用

すべてのポートのインバウンド/アウトバウンド方向に QoS ポリシーを適用できます。

以下にグローバル 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**	ー
2． QoS ポリシーを適用する	**qos apply policy** *policy-name* **global** { **inbound** | **outbound** }	デフォルト：設定なし

3.8 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**8-x-x** です。

4 章 プライオリティマッピング 4-1
4.1 概要 4-1
4.1.1 プライオリティの導入 4-1
4.1.2 プライオリティマッピング 4-1
4.2 プライオリティマッピングの設定作業リスト 4-2
4.3 プライオリティマッピングの設定 4-2
4.4 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4-3
4.5 インタフェースのポートプライオリティの変更 4-3
4.6 プライオリティマッピングの表示と維持 4-3

4章 プライオリティマッピング

4.1 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

4.1.1 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オペレーションマニュアルのセクション 8 *ACL and QoS “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。

4.1.2 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（オペレーションマニュアルのセクション 8 *ACL and QoS “付録”* の *“デフォルトプライオリティ”* を参照してください）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。

4.2 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

4.3 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**	－
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、オペレーションマニュアルのセクション8 *ACL and QoS "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。

4.4 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

4.5 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

4.6 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**8-x-x** です。

5 章 トラフィックポリシング 5-1
5.1 概要 5-1
5.1.1 トラフィックレートの検証とトークンバケット 5-1
5.1.2 トラフィックポリシング 5-2
5.2 トラフィックポリシングの設定 5-3
5.2.1 QoS ポリシーを使用したトラフィックポリシングの設定 5-3
5.3 トラフィックポリシングの表示と維持 5-3

5章 トラフィックポリシング

5.1 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、ある時間範囲内で設定したリソースのみを使用するようにフローを設定することができます。これにより、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。

5.1.1 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。

5.1.2 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 5-1 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。

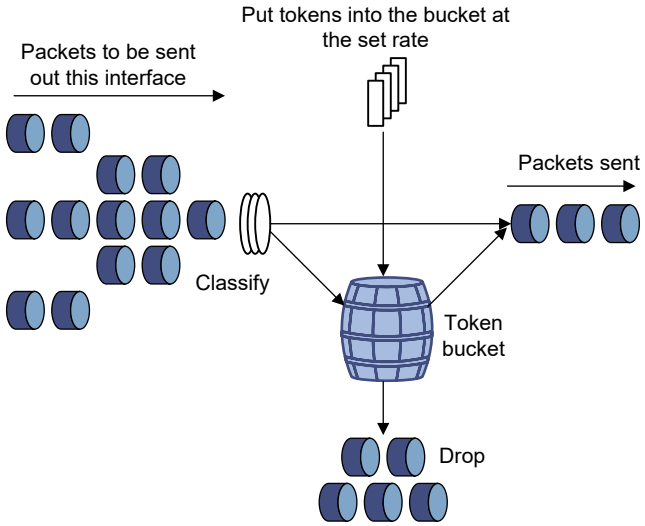


図 5-1 トラフィックポリシング

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。
- 検証結果が適合である場合、リマークしたプレシーデンスに従ってパケットを転送します。(QX-W では未サポート)

5.2 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。

5.2.1 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**	―
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**コマンドの詳細はコマンドマニュアルのセクション*8 ACL and QoS “QoSポリシー”*を参照してください。
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**	―
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**	―
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

5.3 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**8-x-x** です。

6 章 トラフィックフィルタリング 6-1
6.1 設定手順 6-1
6.2 設定例 6-1
6.2.1 ネットワーク要件 6-1
6.2.2 設定手順 6-2

6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。

6.1 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**	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
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**	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**	ー
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。

6.2 設定例

6.2.1 ネットワーク要件

図 6-1 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。

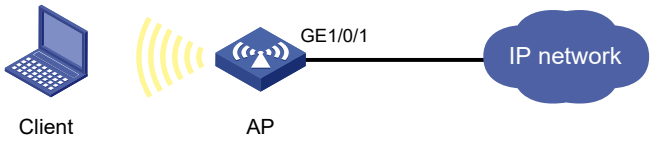


図 6-1 ネットワーク図

6.2.2 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。

```
<AP> system-view
[AP] acl advanced 3000
[AP-acl-ipv4-adv-3000] rule 0 permit tcp source-port neq 21
[AP-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。

```
[AP] traffic classifier classifier_1
[AP-classifier-classifier_1] if-match acl 3000
[AP-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。

```
[AP] traffic behavior behavior_1
[AP-behavior-behavior_1] filter deny
[AP-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。

```
[AP] qos policy policy
[AP-qospolicy-policy] classifier classifier_1 behavior behavior_1
[AP-qospolicy-policy] quit
```

GigabitEthernet 1/0/1 の出力トラフィックに QoS ポリシー **policy** を適用します。

```
[AP] interface gigabitethernet 1/0/1
[AP-GigabitEthernet1/0/1] qos apply policy policy outbound
```

目次

このセクションのページは**8-x-x** です。

7 章 プライオリティマーキング..... 7-1
7.1 概要 7-1
7.2 設定手順..... 7-1
7.2.1 ネットワーク要件..... 7-2
7.2.2 設定手順 7-2

7章 プライオリティマーキング

7.1 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、オペレーションマニュアルのセクション 8 *ACL and QoS “プライオリティマッピング”* を参照してください。

7.2 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、コマンドマニュアルのセクション8 *ACL and QoS “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. 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* ● IPプレシーデンスを設定する： **remark ip-precedence** *ip-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

操作	コマンド	補足
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。

7.2.1 ネットワーク要件

図 7-1 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。

宛先	プライオリティ
Data server	High
Mail server	Medium
File server	Low

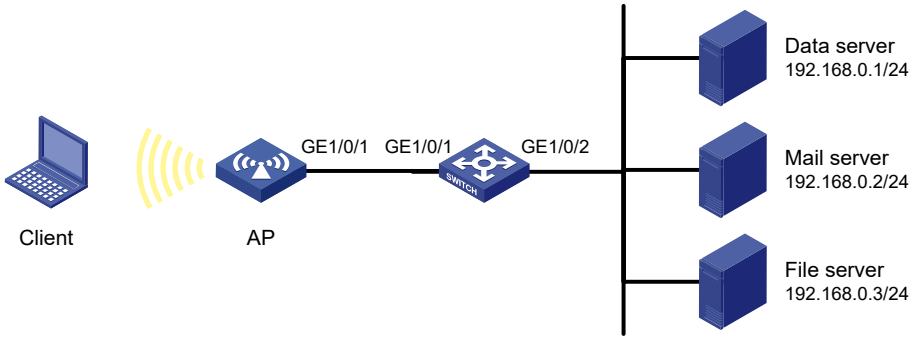


図 7-1 ネットワーク図

7.2.2 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。

```
<AP> system-view
[AP] acl advanced 3000
[AP-acl-ipv4-adv-3000] rule permit ip destination 192.168.0.1 0
[AP-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。

```
[AP] acl advanced 3001
```

```
[AP-acl-ipv4-adv-3001] rule permit ip destination 192.168.0.2 0
[AP-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。

```
[AP] acl advanced 3002
[AP-acl-ipv4-adv-3002] rule permit ip destination 192.168.0.3 0
[AP-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。

```
[AP] traffic classifier classifier_dbserver
[AP-classifier-classifier_dbserver] if-match acl 3000
[AP-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。

```
[AP] traffic classifier classifier_mserver
[AP-classifier-classifier_mserver] if-match acl 3001
[AP-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。

```
[AP] traffic classifier classifier_fserver
[AP-classifier-classifier_fserver] if-match acl 3002
[AP-classifier-classifier_fserver] quit
```

トラフィック動作 **behavior_dbserver** を作成し、DSCP 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。

```
[AP] traffic behavior behavior_dbserver
[AP-behavior-behavior_dbserver] remark dscp 4
[AP-behavior-behavior_dbserver] quit
```

トラフィック動作 **behavior_mserver** を作成し、DSCP の値を 3 としたアクションを設定します。

```
[AP] traffic behavior behavior_mserver
[AP-behavior-behavior_mserver] remark dscp 3
[AP-behavior-behavior_mserver] quit
```

トラフィック動作 **behavior_fserver** を作成し、DSCP の値を 2 としたアクションを設定します。

```
[AP] traffic behavior behavior_fserver
[AP-behavior-behavior_fserver] remark dscp 2
[AP-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。

```
[AP] qos policy policy_server
[AP-qospolicy-policy_server] classifier classifier_dbserver behavior behavior_dbserver
[AP-qospolicy-policy_server] classifier classifier_mserver behavior behavior_mserver
[AP-qospolicy-policy_server] classifier classifier_fserver behavior behavior_fserver
[AP-qospolicy-policy_server] quit
```

GigabitEthernet 1/0/1 の出力トラフィックに QoS ポリシー**policy_server** を適用します。

```
[AP] interface gigabitethernet 1/0/1
[AP-GigabitEthernet1/0/1] qos apply policy policy_server outbound
[AP-GigabitEthernet1/0/1] quit
```

目次

このセクションのページは**8-x-x** です。

8 章 タイムレンジ 8-1
8.1 設定手順 8-1
8.2 タイムレンジの表示と維持 8-1

8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。

8.1 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

8.2 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** }

目次

このセクションのページは**8-x-x** です。

9 章 付録 9-1
9.1 付録 A 頭字語 9-1
9.2 付録 B デフォルトプライオリティマップ 9-1
9.3 付録 C パケットプレシーデンスの概要 9-3
9.3.1 IP プレシーデンスと DSCP フィールドの値 9-3
9.3.2 802.1p プライオリティ 9-4
9.3.3 802.11e プライオリティ 9-5

9章 付録

9.1 付録A 頭字語

頭字語	フルスペル
BE	Best Effort
CAR	Committed Access Rate
CBS	Committed Burst Size
CIR	Committed Information Rate
CQ	Custom Queuing
DiffServ	Differentiated Service
DSCP	Differentiated Services Code Point
EBS	Excess Burst Size
FIFO	First in First out
IntServ	Integrated Service
ISP	Internet Service Provider
PIR	Peak Information Rate
PQ	Priority Queuing
QoS	Quality of Service
ToS	Type of Service

9.2 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 9-1 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 9-2 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	dot1e-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 9-3 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-lp マッピング
dscp	lp
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 9-4 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 9-5 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

9.3 付録C パケットプレシーデンスの概要

9.3.1 IP プレシーデンスと DSCP フィールドの値

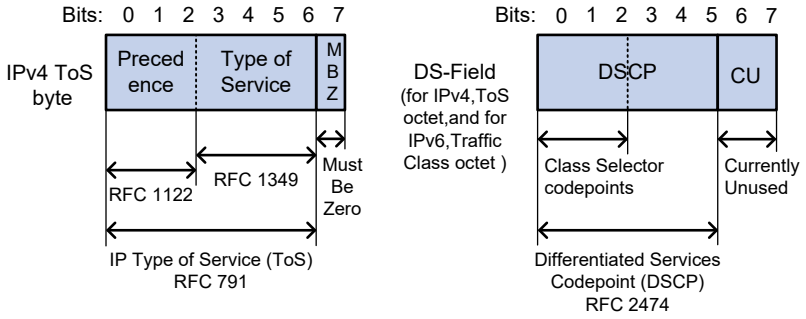


図 9-1 ToS、DS フィールド

図 9-1 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 9-6 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 9-7 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

DSCP 値(10 進表示)	DSCP 値(2 進表示)	説明
40	101000	cs5
48	110000	cs6
56	111000	cs7
0	000000	be (default)

9.3.2 802.1p 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。

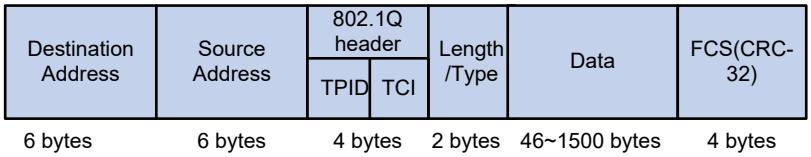


図 9-2 802.1Q タグヘッダの Ethernet フレーム

図 9-2 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 9-3 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 9-8 に 802.1p プライオリティの値を示します。

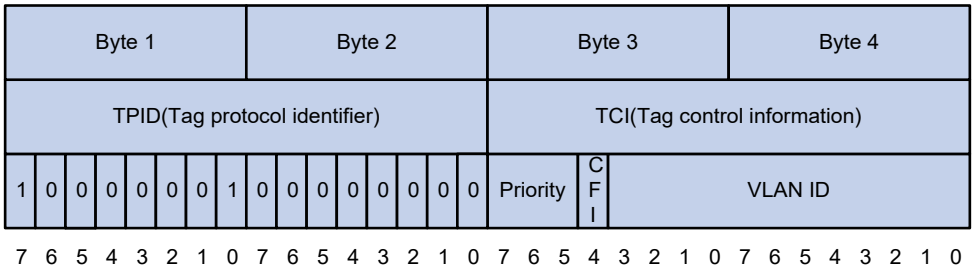


図 9-3 802.1Q タグヘッダ

表 9-8 802.1p 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

9.3.3 802.11e 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。

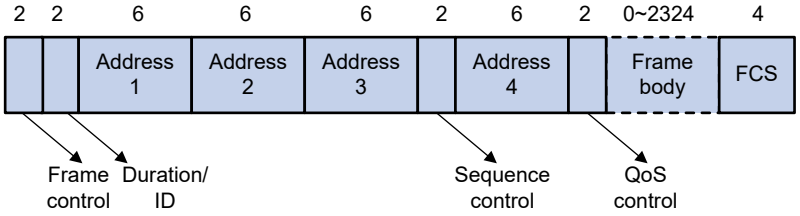


図 9-4 802.11e フレームの構造

QX-W1200 シリーズ アクセスポイント

オペレーションマニュアル

9. 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-AAA
02-802.1X の概要
03-802.1X
04-MAC アドレス認証
05-パスワード管理
06-公開鍵
07-SSH
08-PKI 設定
09-SSL 設定
10-ユーザアイソレーション
11-ユーザプロファイル

目次

このセクションのページは **9-x-x** です。

1 章 AAA 1-1
1.1 概要 1-1
1.1.1 RADIUS 1-2
1.1.2 装置の AAA 実装 1-6
1.1.3 プロトコルと標準 1-8
1.1.4 RADIUS 属性 1-8
1.2 AAA 設定要件と設定作業リスト 1-11
1.3 ローカルユーザの設定 1-12
1.4 RADIUS クライアント機能の設定 1-15
1.4.1 RADIUS スキームの設定 1-15
1.5 ISP ドメインの設定 1-22
1.5.1 設定要件 1-23
1.5.2 ISP ドメインの作成 1-23
1.5.3 ISP ドメインの属性の設定 1-24
1.5.4 ISP ドメインの認証方式の設定 1-24
1.5.5 ISP ドメインの許可方式の設定 1-25
1.5.6 ISP ドメインのアカウンティング方式の設定 1-26
1.5.7 ISP ドメインの NAS-ID の設定 1-27
1.5.8 ISP ドメインの表示と維持 1-27
1.6 同時ログインユーザの最大数の設定 1-27
1.7 EAP プロファイルの設定 1-28
1.7.1 EAP プロファイルの概要 1-28
1.7.2 EAP プロファイルの制約事項とガイドライン 1-28
1.7.3 EAP プロファイルの前提条件 1-28
1.7.4 EAP プロファイルの設定 1-28
1.8 RADIUS サーバ機能の設定 1-29
1.8.1 RADIUS サーバ機能のタスク一覧 1-29
1.8.2 RADIUS ユーザの設定 1-29
1.8.3 RADIUS クライアントの指定 1-30
1.8.4 EAP 認証の設定 1-31
1.8.5 RADIUS サーバの認証ログ出力の設定 1-31
1.8.6 RADIUS サーバ設定の有効化 1-32
1.8.7 RADIUS サーバ設定の無効化 1-32
1.8.8 RADIUS サーバ機能の確認とメンテナンス 1-32
1.9 AAA の設定例 1-33
1.9.1 SSH ユーザの RADIUS 認証、アカウンティングの設定例 1-33
1.9.2 802.1X EAP-PEAP 認証を RADIUS サーバとして機能する AP で構成する 1-34
1.9.3 802.1X EAP-TLS 認証を RADIUS サーバとして機能する AP で構成する 1-38
1.10 RADIUS のトラブルシューティング 1-41
1.10.1 RADIUS 認証の失敗 1-41
1.10.2 RADIUS パケットが到達不能 1-41
1.10.3 RADIUS アカウンティングエラー 1-42
1.11 付録 1-42
1.11.1 付録 A 一般的に使用される RADIUS 属性 1-42
1.11.2 付録 B 一般的に使用される標準 RADIUS 属性の説明 1-43

1章 AAA

1.1 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取得します。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 1-1 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。

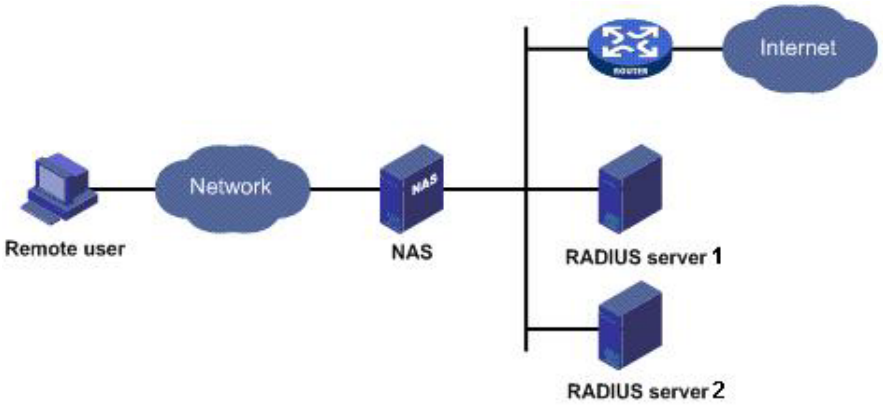


図 1-1 AAA のネットワーク構成

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 1-1 に示すように、RADIUS サーバ 1 と RADIUS サーバ 2 があります。このとき、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。

1.1.1 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。

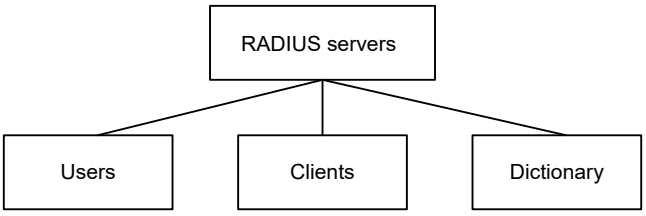


図 1-2 RADIUS サーバデータベース

- **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 1-3 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。

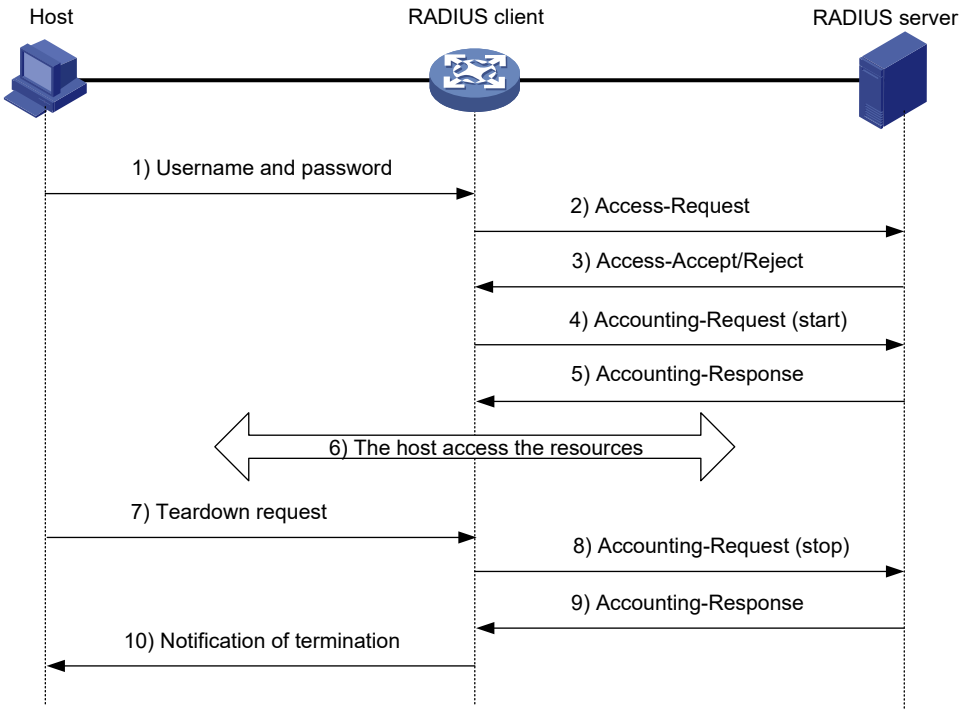


図 1-3 RADIUS の標準的なパケット交換プロセス

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 1-4 に RADIUS パケットのフォーマットを示します。

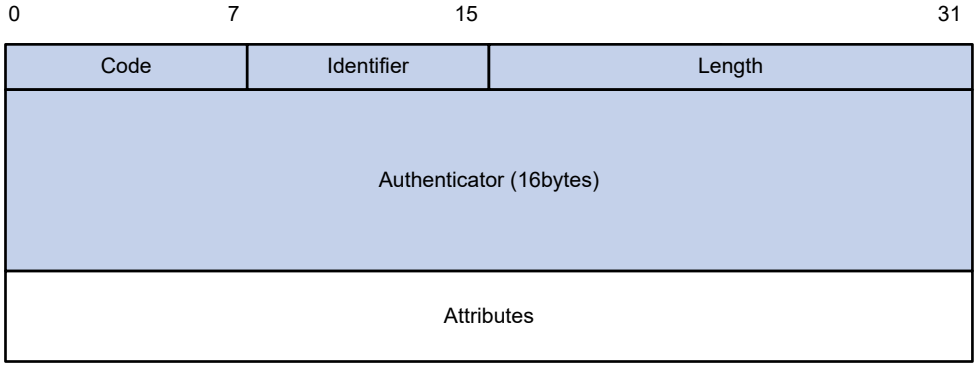


図 1-4 RADIUS パケットフォーマット

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 1-1 にコードフィールドと主な値について説明します。

表 1-1 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。

Code	パケットタイプ	説明
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、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”の“一般的に使われる標準 RADIUS 属性”*を参照してください。

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 1-5 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、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” の “QX シリーズ用 RADIUS 属性”* を参照してください。

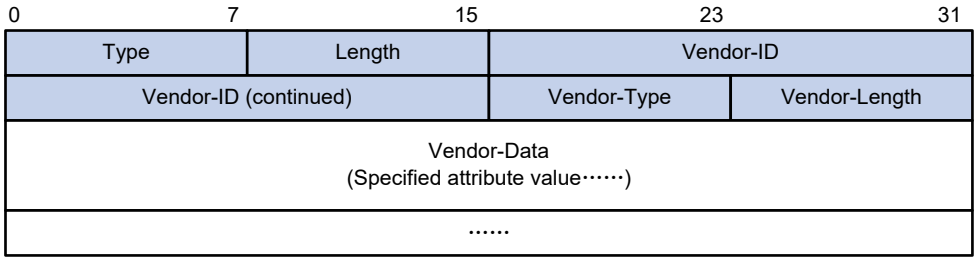


図 1-5 属性番号 26 の拡張 RADIUS 属性フォーマット

1.1.2 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アクセスタイプ

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。

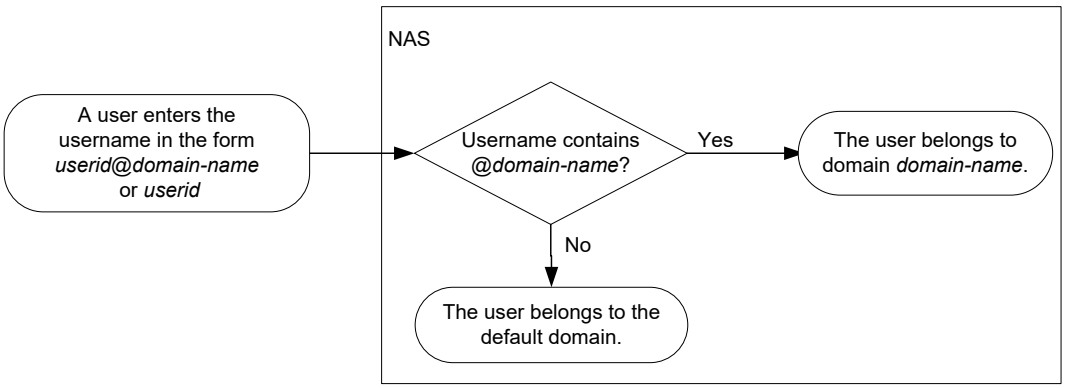


図 1-6 ユーザ名を用いた ISP ドメインの決定

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。

1.1.3 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)*

1.1.4 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	ユーザアクセスを行うNASインタフェースのIPアドレスです。
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。

番号	属性	説明
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。
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。

番号	属性	説明
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。

1.2 AAA設定要件と設定作業リスト

AAA を設定するため、NAS で以下の作業を完了している必要があります。

1) 必要な AAA スキームの設定
   - □ **ローカル認証** － ユーザのユーザ名、パスワードを含む、認証するために必要なローカルユーザと、属性を設定します。
   - □ **リモート認証** － 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。
2) ユーザの ISP ドメインの AAA 方式を設定します。リモート AAA 方式は ISP domain view で設定された RADIUS スキームを参照します。

以下に AAA 認証の設定作業リストを示します。

ローカル認証作業リスト
（必須設定項目）ローカルユーザの設定
（必須設定項目）ISPドメインの設定 ISPドメインの作成 ISPドメインの属性の設定 ISPドメインの認証方式の設定 ISPドメインの許可方式の設定 ISPドメインのアカウンティング方式の設定 ISPドメインのNAS-IDの設定
（オプション設定項目）同時ログインユーザの最大数の設定

リモート認証作業リスト
（必須設定項目）RADIUSクライアント機能の設定
（必須設定項目）ISPドメインの設定 ISPドメインの作成 ISPドメインの属性の設定 ISPドメインの認証方式の設定 ISPドメインの許可方式の設定 ISPドメインのアカウンティング方式の設定 ISPドメインのNAS-IDの設定

リモート認証作業リスト
（オプション設定項目）同時ログインユーザの最大数の設定

認証サーバ機能作業リスト
（必須設定項目）ローカルユーザの設定
（必須設定項目）EAPプロファイルの設定
（必須設定項目）RADIUSサーバ機能の設定

🕮 **メモ：**

認証サーバ機能は、ソフトウェアバージョン 7.5.142a を含む以降のソフトウェアからサポートしています。AP を認証サーバとして動作させる場合、自装置及び管理対象の AP のための認証クライアントとしての利用のみをサポートします。

1.3 ローカルユーザの設定

ローカルユーザ認証、許可、アカウンティングを実装するため、装置で、ローカルユーザを作成し、ユーザの属性の設定を行う必要があります。ローカルユーザと属性は装置のローカルユーザデータベースに記録されます。ローカルユーザはユーザ名で識別されます。

ローカルユーザは以下のタイプに分類されます。

- **装置管理**－装置にログインする装置管理ユーザをサポートします。
- **ネットワークアクセスユーザ**－装置を通してネットワークリソースにアクセスするユーザをサポートします。

設定可能なローカルユーザ属性を以下に示します。

- **サービスタイプ**－ユーザが使用できるサービスタイプです。ローカル認証はローカルユーザのサービスタイプをチェックします。もしサービスタイプが有効でない場合、ユーザは認証にパスできません。

  サービスタイプは FTP、HTTP、HTTPS、LAN アクセス、SSH、Telnet、ターミナルがあります。

- **ユーザ状態**－ローカルユーザがネットワークサービスをリクエストできるかどうかを示します。active と blocked の 2 つの状態があります。active 状態のユーザはネットワークサービスをリクエストできますが、blocked のユーザはリクエストできません。
- **同一ユーザ名を使用する同時ログインユーザの上限**－同一ユーザ名を使用して同時に装置にアクセスすることができるユーザの最大の数です。同一ユーザ名を使用するローカルユーザの数が上限に達するとき、ローカルユーザは、そのユーザ名を使用して装置にアクセスすることができません。
- **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と、パスワード管理属性、許可属性のようなグループのすべての属性を運んでいます。ローカルユーザグループの詳細は、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”* の *“ユーザグループ属性の設定”* を参照してください。
- **許可属性**－許可属性は、ローカル認証をパスした後、ユーザの権利を示します。許可属性は ACL、アイドルカット機能、ユーザロール、VLAN、FTP/SFTP/SCP 作業ディレクトリを含みます。許可属性の詳細は、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”* の *“ローカルユーザ属性の設定”* を参照してください。

  ローカルユーザのサービスタイプにもとづいて許可属性を設定します。

user group view ですべてのローカルユーザに適用される属性、local user view でローカルユーザのみに適用される属性となるように、許可属性を設定することができます。local user view で設定した許可属性の設定は、user group view で設定した許可属性よりも優先されます。

- □ user group view で設定した属性はユーザグループのすべてのローカルユーザに適用します。
- □ local user view で設定した属性はローカルユーザのみ適用します。

- **パスワード管理属性**－パスワード管理属性は装置管理ユーザのパスワードのセキュリティを容易に管理するようにするサービスタイプです。パスワード管理属性は、パスワードの有効期限、最小パスワード長、パスワード構成の確認、パスワードの複雑さの確認、ログイン試行制限を含みます。

  system view、user group view、local user view でパスワード管理属性を設定することができます。狭い範囲の view で設定した許可属性の設定は、優先度が高くなります。

I. ローカルユーザ設定作業リスト

作業リスト
（必須設定項目）ローカルユーザ属性の設定
（オプション設定項目）ユーザグループ属性の設定
（オプション設定項目）ローカルユーザとローカルユーザグループの表示と維持

II. ローカルユーザ属性の設定

ローカルユーザ属性の設定を行うとき、以下のガイドラインに従ってください。

- local user view あるいは user group view で許可属性、パスワード管理属性を設定することができます。local user view で設定した値が user group view で設定した値よりも優先されます。
- 許可属性はアプリケーションの環境と目的に従って設定してください。ユーザのサービスタイプにもとづいて許可属性をサポートします。
  - □ 802.1X ユーザは、ユーザが装置にアクセスする際に、802.1X が有効な Ethernet インタフェースを指定してください。
  - □ MAC アドレス認証ユーザは、ユーザが装置にアクセスする際に、MAC アドレス認証が有効な Ethernet インタフェースを指定してください。

以下にローカルユーザ属性の設定を示します。

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** | **network** }]	デフォルト：設定なし
3. （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 ローカルユーザは、正しいユーザ名を入力して属性チェックをパスした後に認証を通過します。

操作	コマンド	補足
4. ローカルユーザのサービスタイプを指定する	● ネットワークアクセスユーザ： **service-type lan-access** ● 装置管理ユーザ： **service-type** { **ftp** | { **http** | **https** | **ssh** | **telnet** | **terminal** } * }	デフォルト：設定なし
5. （オプション設定項目）ローカルユーザを active あるいは blocked に設定する	**state** { **active** | **block** }	デフォルト：**active** ネットワークサービスを要求することができます。
6. （オプション設定項目）同時にログインするローカルユーザの上限を設定する	**access-limit** *max-user-number*	デフォルト：制限なし ローカルユーザの設定のみ適用され、アカウンティングをサポートしていない FTP、SFTP、SCPユーザには適用しません。
7. （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、SFTP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。
8. （オプション設定項目）ローカルユーザのユーザグループを指定する	**group** *group-name*	デフォルト：ローカルユーザはデフォルトユーザグループのsystemに属しています。

III. 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略化します。ユーザグループはローカルユーザのグループから構成され、ローカルユーザ属性の構成があります。グループ内のローカルユーザを集中化してユーザ属性の管理を行うため、ユーザグループ用のローカルユーザ属性を設定することができます。パスワード管理属性と許可属性を含んだユーザ属性を設定できます。

デフォルトでは、新しく追加された各ローカルユーザは、システムデフォルトユーザグループ system に属し、グループのすべての属性に対応します。ローカルユーザが属しているユーザグループを割り当てる場合、local user view で **group** コマンドを使用します。

以下にユーザグループ属性の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. ユーザグループを作成し、その view に移行する	**user-group** *group-name*	デフォルト：デフォルトユーザグループとしてsystemがあります

操作	コマンド	補足
3. ユーザグループの許可属性を設定する	**authorization-attribute** { **acl** *acl-number* | **idle-cut** *minutes* | **user-profile** *profile-name* | **vlan** *vlan-id* | **work-directory** *directory-name* }*	デフォルト：設定なし

IV. ローカルユーザとローカルユーザグループの表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
ローカルユーザの設定とオンラインユーザに関する統計情報を表示する	**display local-user** [**class** { **manage** | **network** } | **idle-cut** { **disable** | **enable** } | **service-type** { **ftp** | **http** | **https** | **lan-access** | **ssh** | **telnet** | **terminal** } | **state** { **active** | **block** } | **user-name** *user-name* **class** { **manage** | **network** } | **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* }

1.4 RADIUSクライアント機能の設定

1.4.1 RADIUS スキームの設定

Radius クライアント機能は、RADIUS スキームによって RADIUS サーバを指定し、RADIUS サーバの情報を交換するのに使われるパラメータを定義します。パラメータは、サーバの IP アドレス、UDP ポート番号、共有鍵、サーバタイプを含んでいます。

I. 設定作業リスト

作業リスト
（必須設定項目）RADIUSスキームの作成
（必須設定項目） RADIUS認証サーバの指定
（オプション設定項目）RADIUSアカウンティングサーバと関連パラメータの指定
（オプション設定項目）セキュアなRADIUS通信を行うための共有鍵の指定
（オプション設定項目） ユーザ名フォーマットとトラフィック統計情報ユニットの設定
（オプション設定項目） RADIUS要求の再送信の最大試行回数の設定
（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）出力するRADIUSパケットの送信元IPアドレスの指定
（オプション設定項目）RADIUSサーバのタイマ機能の設定
（オプション設定項目）RADIUSアカウンティング機能の設定
（オプション設定項目）RADIUSの表示と維持

II. RADIUS スキームの作成

ほかの RADIUS 設定を行う前に、RADIUS スキームを作成してください。RADIUS スキームを 16 まで作成することができます。RADIUS スキームは複数の ISP ドメインから参照することができます。

以下に RADIUS スキ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**	ー

操作	コマンド	補足
2． RADIUS スキームを作成し、その view に移行する	**radius scheme** *radius-scheme-name*	デフォルト：設定なし

III. RADIUS 認証サーバの指定

許可情報は認証の応答パケットに含めて RADIUS クライアントに送信されるため、RADIUS 認証サーバは、認証、許可を一緒に扱います。

1 つのプライマリ認証サーバと 16 のセカンダリ認証/許可サーバを指定することができます。プライマリサーバが有効でないとき、装置は、順番に設定されたセカンダリサーバと通信を行い、**active** 状態の最初のセカンダリサーバと通信を行います。

冗長性を必要としない場合、プライマリサーバのみ指定します。RADIUS 認証サーバは同時に、1 つのスキーム用にプライマリ認証サーバとして機能させ、ほかのスキーム用にセカンダリ認証サーバとして機能させることができます。

以下に RADIUS スキームの RADIUS 認証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**	—
2． RADIUS scheme view に移行する	**radius scheme** *radius-scheme-name*	—
3． RADIUS 認証サーバを指定する	• プライマリRADIUS認証サーバを指定する：**primary authentication** *ipv4-address* [*port-number*	**key** { **cipher**	**simple** } *string*] * • セカンダリRADIUS認証サーバを指定する：**secondary authentication** *ipv4-address* [*port-number*	**key** { **cipher**	**simple** } *string*] *	デフォルト：指定なし 少なくとも1つのコマンドを設定してください。 プライマリ認証サーバとセカンダリ認証サーバで、同一のIPアドレス、ポート番号を設定することはできません。

IV. RADIUS アカウンティングサーバと関連パラメータの指定

RADIUS スキームに、1 つのプライマリアカウンティングサーバと 16 のセカンダリアカウンティングサーバを指定することができます。プライマリサーバが有効でないとき、装置は、順番に設定されたセカンダリサーバと通信を行い、**active** 状態の最初のセカンダリサーバと通信を行います。

冗長性を必要としない場合、プライマリサーバのみします。RADIUS アカウンティングサーバは同時に、1 つのスキーム用にプライマリアカウンティングサーバとして機能させ、ほかのスキーム用にセカンダリアカウンティングサーバとして機能させることができます。

装置は以下の状況でアカウンティングサーバにアカウンティング停止要求（stop-accounting request）を送信します。

- ホストから接続切断要求を受信
- 管理者から接続切断通知を受信

アカウンティング要求に対して、指定した試行回数の上限に達しても応答がない場合、ユーザを切断します。

RADIUS は FTP、SFTP ユーザのアカウンティングをサポートしていません。

以下に RADIUS スキームのアカウンティングサーバと関連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. RADIUS scheme view に移行する	**radius scheme** *radius-scheme-name*	―
3. RADIUS アカウンティングサーバを指定する	• プライマリRADIUSアカウンティングサーバを指定する： **primary accounting** *ipv4-address* [*port-number* | **key** { **cipher** | **simple** } *string*] * • セカンダリRADIUSアカウンティングサーバを指定する： **secondary accounting** *ipv4-address* [*port-number* | **key** { **cipher** | **simple** } *string*] *	デフォルト：指定なし 少なくとも1つのコマンドを設定してください。 プライマリアカウンティングサーバとセカンダリアカウンティングサーバで、同一のIPアドレス、ポート番号を設定することはできません。
4. （オプション設定項目）アカウンティング要求の最大試行回数を設定する	**retry realtime-accounting** *retry-times*	デフォルト：5

V. セキュアな RADIUS 通信を行うための共有鍵の指定

RADIUS クライアントと RADIUS サーバは、パケット認証とユーザパスワードの暗号化を行うため、MD5 アルゴリズムを使用して、クライアントとサーバ間で交換するパケットと共有鍵を暗号化し、パケットの検証を行います。同じ共有鍵が使用される場合のみ、パケットを適切に受信し、応答を返すことができます。

スキームで同じタイプ（アカウンティングあるいは認証）のすべてのサーバで、共有鍵が設定されます。RADIUS サーバ用に個別に設定された共有鍵よりも優先度は低くなります。

以下にセキュアな RADIUS 通信を行うための共有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. RADIUS scheme view に移行する	**radius scheme** *radius-scheme-name*	―
3. セキュアな RADIUS 通信を行うための共有鍵を指定する	**key** { **accounting** | **authentication** } { **cipher** | **simple** } *string*	デフォルト：指定なし 装置とRADIUSサーバで必ず同じ共有鍵を設定するようにしてください。

VI. ユーザ名フォーマットとトラフィック統計情報ユニットの設定

ユーザ名は、一般的に *userid@isp-name* のフォーマットで表されます。*isp-name* はユーザが属している ISP ドメイン名で、ユーザがどこの ISP ドメインに属しているか装置が認識するのに使われます。しかし初期の RADIUS サーバは ISP ドメイン名が含まれていないユーザ名を認識することはできません。この場合、ユーザ名を送信する前に各ユーザ名のドメイン名を削除する必要があります。

同一 RADIUS スキームを参照するために 2 つ以上の ISP ドメインを使用する場合、ドメインを識別するため、ユーザ名の中の ISP ドメイン名を削除しないでください。

装置は、アカウンティングパケットのオンラインユーザのトラフィックの統計情報を RADIUS アカウンティングサーバに周期的に通知します。正しいトラフィック統計情報を行うため、装置でのデータフローのユニットとパケットのユニットが、RADIUS サーバのユニットと同一になっていることを確認してください。

以下にユーザ名フォーマットとトラフィック統計情報ユニ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. RADIUS scheme view に移行する	**radius scheme** *radius-scheme-name*	―
3. RADIUS サーバに送信されるユーザ名の形式を指定する	**user-name-format** { **keep-original** | **with-domain** | **without-domain** }	デフォルト：**with-domain** 起動時の設定の詳細についてはオペレーションマニュアルのセクション1 *はじめに "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。
4. （オプション設定項目）RADIUS サーバへ送信されるデータフロー、またはパケットの単位を指定する	**data-flow-format** { **data** { **byte** | **giga-byte** | **kilo-byte** | **mega-byte** } | **packet** { **giga-packet** | **kilo-packet** | **mega-packet** | **one-packet** } }*	データフロー：**byte** パケット：**one-packet**

VII. RADIUS 要求の再送信の最大試行回数の設定

RADIUS はデータ送信に UDP を使用しているため、通信に信頼性がありません。応答タイムアウト時間（**timer response-timeout** コマンドで設定されます。）が切れる前に RADIUS サーバから応答がなかった場合、NAS は RADIUS リクエストを再送します。再送の試行回数が上限に達しても、RADIUS サーバから応答がない場合、**active** 状態の他の RADIUS サーバと通信を試みます。**active** 状態の他の RADIUS サーバから応答がない場合、装置は認証あるいはアカウンティングが失敗したとみなします。RADIUS サーバ応答タイムアウト時間についての詳細は、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" の "RADIUS サーバのタイマ機能の設定"* を参照してください。

以下に RADIUS 要求の再送信の最大試行回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. RADIUS scheme view に移行する	**radius scheme** *radius-scheme-name*	―
3. RADIUS 要求の再送信の最大試行回数を設定する	**retry** *retry-times*	デフォルト：3

VIII. RADIUS サーバのステータスの設定

RADIUS サーバのステータスを blocked 状態あるいは active 状態に設定することで、装置と通信を行う現在のサーバが有効でなくなったときに、接続先の制御ができます。実際には、1 つのプライマリ RADIUS サーバと、プライマリサーバのバックアップとして動作す

る複数のセカンダリ RADIUS サーバを指定することができます。一般的に装置は、以下のルールにもとづいてサーバを選択します。

- プライマリサーバが active 状態のとき、装置はプライマリサーバと通信します。
  - プライマリサーバが故障したとき装置は以下の処理を行います。
  - サーバのステータスを blocked 状態に変更します。
  - サーバの quiet タイマを開始します。
- active 状態のセカンダリサーバと通信を行います。（最初に設定されたセカンダリサーバが高い優先度を持ちます）
- セカンダリサーバが有効でなくなったとき、装置は以下の処理を行います。
  - サーバのステータスを blocked 状態に変更します。
  - サーバの quiet タイマを開始します。
  - active 状態の次のセカンダリサーバのチェックを行います。このプロセスは、装置が有効なセカンダリサーバを見つける、あるいは active 状態のすべてのセカンダリサーバのチェックを完了するまで行います。
- quiet タイマの時間が経過した場合あるいは手動で active 状態に設定した場合、サーバは active 状態になります。しかし装置は認証あるいはアカウンティングプロセスの間、サーバを再度チェックしません。

  もし 1 回の検索プロセスで通信可能なサーバが見つからない場合、認証あるいはアカウンティングの試みが失敗したと認識します。
- もし使用している認証あるいはアカウンティングサーバが削除された場合、サーバと装置の通信はタイムアウトとなります。装置は最初から active 状態のサーバを検索します。最初にプライマリサーバ（もしある場合）をチェックし、次にセカンダリサーバをチェックする順番で確認します。
- プライマリとセカンダリサーバの両方が blocked 状態の場合、装置はすべてのサーバと通信しません。
- 1 つのサーバが active 状態で、ほかのすべてのサーバが blocked 状態の場合、装置は、たとえサーバが有効でない場合でも active 状態のサーバのみと通信します。
- RADIUS サーバの状態が自動的に変更する場合、装置はすべての RADIUS スキームに従いサーバの状態を変更します。

デフォルトでは、すべての RADIUS サーバの状態は active となります。必要に応じて、サーバの状態を変更できます。たとえば、サーバが故障している場合、サーバとの通信を防ぐために blocked となっているサーバの状態を変更することができます。

以下に RADIUS サーバのステータ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. RADIUS scheme 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** } • 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**	少なくとも1つのコマンドを設定します。 デフォルト：RADIUSスキームに指定されたサーバはactive状態です。 設定されたサーバのステータスは設定ファイルに保存することができません。**display radius scheme**コマンドを使用して表示することのみ可能です。 装置の再起動後、すべてのサーバはactive状態に戻ります。

操作	コマンド	補足
	authentication [*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** [*ipv4-address* [*port-number*] *] { **active** | **block** }	

IX. 出力する RADIUS パケットの送信元 IP アドレスの指定

NAS が送信した RADIUS パケットの送信元 IP アドレスは、RADIUS サーバで設定された NAS の IP アドレスとマッチする必要があります。RADIUS パケットを受信する際、RADIUS サーバはパケットの送信元 IP アドレスが管理された NAS の IP アドレスかどうか確認します。

- パケットの送信元 IP アドレスが管理された NAS の IP アドレスとマッチしている場合、サーバは処理を行います。
- パケットの送信元 IP アドレスが管理された NAS の IP アドレスとマッチしていない場合、パケットを廃棄します。

一般的に、RADIUS パケットの送信元アドレスは NAS のいずれかの出力インタフェースの IP アドレスです。ある状況においては、送信元 IP アドレスを変更する必要があります。

RADIUS scheme view、または system view で出力する RADIUS パケットの送信元 IP アドレスを指定することができます。

- RADIUS scheme view で指定された IP アドレスは、1 つの RADIUS scheme のみに適用されます。
- system view で指定された IP アドレスは、すべての RADIUS scheme に適用されます。

RADIUS パケットを送信する前に、NAS は以下の順番で送信元 IP アドレスを選択します。

1) RADIUS スキーム用に指定された送信元 IP アドレス
2) system view で指定された送信元 IP アドレス
3) ルートで指定された出力インタフェースの IP アドレス

以下にすべての RADIUS スキームの送信元 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. 出力する RADIUS パケットの送信元 IP アドレスを指定する	**radius nas-ip** *ipv4-address*	デフォルト : RADIUSパケットを送信するインタフェースのIPアドレスが指定されます。

以下に指定された RADIUS スキームの送信元 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. RADIUS scheme view に移行する	**radius scheme** *radius-scheme-name*	—

操作	コマンド	補足
3. 出力する RADIUS パケットの送信元 IP アドレスを指定する	**nas-ip** *ipv4-address*	デフォルト：system view で **radius nas-ip**コマンドが設定されたIPアドレスが使用されます。設定されていない場合、RADIUSパケットを送信するインタフェースのIPアドレスが指定されます。

X. RADIUS サーバのタイマ機能の設定

装置は、RADIUS サーバとの通信を管理するため、以下のタイマを使用します。

- **RADIUS サーバの応答タイムアウトタイマ**（**response-timeout**） – RADIUS リクエスト再送信間隔です。このタイマは RADIUS リクエストが送信された後、すぐに開始します。装置はタイマが満了する前に RADIUS サーバから応答を受信しない場合、リクエストを再送します。
- **サーバ停止タイマ**（**quiet**） – block 状態にある到達不能のサーバを保持する時間です。1 つのサーバが到達不能である場合、装置はサーバのステータスを blocked 状態に変更し、サーバ停止タイマを開始します。active 状態の別のサーバと通信しようとします。サーバ停止タイマが満了した後、装置はサーバの状態を active に戻します。
- **リアルタイムのアカウンティング間隔**（**realtime-accounting**） – ユーザのリアルタイムアカウンティングを実行する間隔を定義します。このタイマが設定されると、装置は指定された間隔で、オンラインユーザのアカウンティング情報を RADIUS サーバに送信します。装置がサーバからの応答を受信しない場合、ユーザの接続が強制的に切断されます。

RADIUS サーバの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。

- RADIUS パケットの再送信の最大試行回数の設定と RADIUS サーバ応答タイムアウトタイマの設定を行うとき、セカンダリサーバの数を考慮してください。再送プロセスに十分な時間がない場合、Telnet のようなアクセスモジュールのクライアント接続では、有効なサーバを検索しようとしている間にタイムアウトしてしまう可能性があります。
- セカンダリサーバ数が設定されたとき、たとえパケット転送試行制限とサーバ応答タイムアウト期間が小さい値で設定されている場合でも、クライアント接続タイムアウトの時間を短く設定している、アクセスモジュールのクライアント接続は、初期認証あるいはアカウンティングの間にタイムアウトしてしまう可能性があります。この場合、装置はブロックする到達不能サーバの状態と短くした到達可能サーバを検索する時間を設定しているため、次の認証あるいはアカウンティングの試行は成功します。
- サーバ停止タイマは、適切に設定してください。短すぎると、サーバは active 状態の到達不能なサーバの通信を繰り返し試みる必要があるため、頻繁に認証あるいはアカウンティングが失敗します。タイマの時間を長くすると、タイマの期間が満了する間に blocked 状態になるため、一時的に故障から回復した到達可能なサーバをブロックする可能性があります。
- リアルタイムのアカウンティング間隔の設定は、NAS と RADIUS サーバの性能によって代わります。短い間隔にすると、より正確なアカウンティングを行うことができますが、高い性能が必要となります。ユーザの最大数が多い（1000 以上）の場合、間隔を長くしてください。

以下に RADIUS サーバのタイマ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. RADIUS scheme view に移行する	**radius scheme** *radius-scheme-name*	—
3. 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
4. サーバの停止タイマを設定する	**timer quiet** *minutes*	デフォルト：5分
5. リアルタイムアカウンティング間隔を設定する	**timer realtime-accounting minutes** *interval* [**second**]	デフォルト：12分

XI. RADIUS アカウンティング機能の設定

アカウンティング機能を有効にした場合、装置は再起動した後に RADIUS サーバに accounting-on パケットを自動的に送信します。accounting-on パケットを受信すると、RADIUS サーバは装置に対して再ログインできるように全オンラインユーザをログアウトします。この機能を使用しない場合、RADIUS サーバはユーザがオンライン中とみなしているため再起動後にユーザが再ログインすることができません。

装置が accounting-on パケットを再送するために待機する間隔と最大試行回数を設定できます。

以下に RADIUS スキームのアカウンティング機能設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. RADIUS scheme view に移行する	**radius scheme** *radius-scheme-name*	—
3. RADIUS サーバの応答タイムアウトタイマを設定する	**accounting-on enable** [**interval** *seconds* | **send** *send-times*] *	デフォルト：無効

XII. RADIUS 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
RADIUSスキームの設定を表示する	**display radius scheme** [*radius-scheme-name*]
RADIUSパケットの統計情報を表示する	**display radius statistics**
RADIUSパケットの統計情報をクリアする	**reset radius statistics**

1.5 ISPドメインの設定

ISP domain view で設定された AAA スキームを使用して、ISP ドメインの AAA 方式を、設定することができます。各 ISP ドメインは、デフォルトの AAA 方式を持っています。この AAA 方式は、デフォルトでローカル認証、ローカル許可、ローカルアカウンティン

グとなっており、設定することができます。もし ISP ドメインを設定しない場合、ユーザの認証、許可、アカウンティングがデフォルトの AAA 方式を使用します。

1.5.1 設定要件

ISP ドメインでユーザのローカル認証を使用する場合、最初に装置でローカルユーザのアカウントを設定してください。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" の "ローカルユーザ属性の設定"* を参照してください。

リモート認証、許可、アカウンティングを使用する場合、要求される RADIUS スキームを作成してください。RADIUS スキームについて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" の "RADIUS スキームの設定"* を参照してください。

1.5.2 ISP ドメインの作成

複数の ISP を持つネットワークシナリオでは、装置に各 ISP のユーザを接続する可能性があります。各 ISP ユーザはそれぞれのユーザ属性（たとえば、ユーザ名、パスワードの構成、サービスタイプ、権限）を持ち、ユーザを識別するために ISP ドメインを設定する必要がある可能性があります。そして ISP ドメインのために AAA 方式を含む各属性を設定する必要があります。

ドメインはあらかじめ定義されているデフォルト ISP ドメイン system を含む最大 16 の ISP ドメインを設定することができます。デフォルトのドメインとして ISP ドメインを指定することができます。ISP ドメインの設定を修正することができますが、削除することはできません。

装置では、各ユーザは ISP ドメインに属します。もしユーザがログインするとき、ISP ドメイン名がない場合、装置はデフォルト ISP ドメインに属していると認識します。

装置は以下の順にそれぞれの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を指定された認証ドメイン
2) ユーザ名の ISP ドメイン
3) 装置のデフォルト ISP ドメイン

選択されたドメインが装置に存在しない場合、装置は存在しないドメインに割り当てられるユーザを収容する ISP ドメインを検索します。そのような 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。

🕮 **メモ：**

認証ドメインのサポートはアクセスモジュールによって異なります。802.1X、MAC アドレス認証の認証ドメインを指定することができます。

ISP ドメインの設定をする場合、以下の制限とガイドラインに従ってください

- デフォルトの ISP ドメインを削除することはできません。**undo domain** コマンドを使用する前に **undo domain default enable** コマンドを使用して、デフォルト以外の ISP ドメインに変更してください。
- ISP ドメイン **system** の設定変更はできますが、ドメインを削除することはできません。

以下に ISP ドメ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. ISP ドメインを作成し、ISP domain view に移行する	**domain** *isp-name*	―
3. system view に戻る	**quit**	―
4. （オプション設定項目）デフォルト ISP ドメインを指定する	**domain default enable** *isp-name*	デフォルト：system

1.5.3 ISP ドメインの属性の設定

ISP ドメインで以下の属性を設定することができます。

- **ドメイン状態**－ISP ドメインを active あるいは blocked 状態にすることによって、ユーザからのネットワークサービス要求の許可あるいは拒否することができます。

ISP ドメインの属性はドメインのすべてのユーザに適用します。

以下に ISP ドメインの属性の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. ISP domain view に移行する	**domain** *isp-name*	―
3. ISP ドメインを **active** あるいは **blocked** 状態に設定する	**state** { **active** | **block** }	デフォルト：**active** ドメインのユーザはネットワークサービスをリクエストすることができます。

1.5.4 ISP ドメインの認証方式の設定

I. 設定要件

認証方式を設定する前に、以下の作業を行ってください。

1) 設定するアクセスタイプ、またはサービスタイプを定義してください。AAA では、各アクセスタイプとサービスタイプのために認証方式を設定することができます。
2) すべてのアクセスタイプとサービスタイプでデフォルトの認証方式を設定するかどうか定義してください。デフォルト認証方式はすべてのアクセスユーザに適用しますが、指定された認証方式よりもプライオリティは低くなります。

II. 設定ガイドライン

認証方式を設定するとき、以下のガイドラインに従ってください。

- 認証方式が RADIUS スキームを使用し、許可方式が RADIUS スキームを使用しない場合、AAA は RADIUS サーバから認証結果のみを受け取ります。RADIUS サーバからの Access-Accept メッセージは許可情報を含みますが、装置は許可情報を無視します。
- ユーザロール認証のスキームを指定する場合、ユーザロールが level-*n* のフォーマットにあることを確認してください。RADIUS スキームを指定する場合、装置はロール

認証の RADIUS サーバのユーザ名$**enab***n*$を使います。ここで *n* はユーザロール level-*n* の *n* と同一です。

III. 設定手順

以下に ISP ドメインの認証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. ISP domain view に移行する	**domain** *isp-name*	―
3. ユーザのすべてのタイプのためのデフォルト認証方式を指定する	**authentication default** { **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }	デフォルト：**local**
4. LAN ユーザのための認証方式を指定する	**authorization lan-access** { **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }	デフォルト：LANユーザのためのデフォルト認証方式
5. ログインユーザのための認証方式を指定する	**authentication login** { **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }	デフォルト：ログインユーザのためのデフォルト認証方式

1.5.5 ISP ドメインの許可方式の設定

I. 設定要件

許可方式を設定する前に、以下の作業を行ってください。

1) 設定されるアクセスタイプあるいはサービスタイプを定義してください。AAA では各アクセスタイプとサービスタイプに許可スキームを設定することができます。
2) すべてのアクセスタイプとサービスタイプでデフォルトの許可方式を設定するかどうか定義してください。デフォルト許可方式はすべてのアクセスユーザに適用しますが、指定された許可方式よりもプライオリティは低くなります。

II. 設定ガイドライン

認証方式を設定するとき、以下のガイドラインに従ってください。

- RADIUS 許可を設定するため、RADIUS 認証を設定し、RADIUS 認証と許可で同じ RADIUS スキームを参照してください。RADIUS 許可の設定に間違いがある場合や RADIUS 許可に失敗する場合は、RADIUS 認証も失敗します。

III. 設定手順

以下に ISP ドメインの許可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. ISP domain view に移行する	**domain** *isp-name*	―

操作	コマンド	補足
3. すべてのタイプのユーザのためにデフォルト許可方式を指定する	**authorization default** { **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }	デフォルト：**local**
4. コマンド許可方式を指定する	**authorization command** { **local** [**none**] | **none** }	デフォルト：コマンド許可のためのデフォルト許可方式
5. LAN ユーザの許可方式を指定する	**authorization lan-access** { **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }	デフォルト：LANユーザのためのデフォルト許可方式
6. ログインユーザのために許可方式を指定する	**authorization login** { **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }	デフォルト：ログインユーザのためのデフォルト許可方式

1.5.6 ISP ドメインのアカウンティング方式の設定

I. 設定要件

アカウンティング方式を設定する前に、以下の作業を行ってください。

1) 設定されるアクセスタイプあるいはサービスタイプを定義してください。AAA では各アクセスタイプとサービスタイプにアカウンティング方式を設定することができます。
2) すべてのアクセスタイプとサービスタイプで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定義してください。デフォルト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しますが、指定されたアカウンティング方式よりもプライオリティは低くなります。

II. 設定ガイドライン

アカウンティング方式を設定するとき、以下のガイドラインに従ってください。

- FTP、SFTP サービスを使用するログイン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は、アカウンティングの統計情報を提供しません。同じローカルユーザアカウントを使用するユーザ数のカウントと管理を行います。しきい値は **access-limit** コマンドによって設定されます。

III. 設定手順

以下に ISP ドメインのアカウンティング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. ISP domain view に移行する	**domain** *isp-name*	—
3. すべてのタイプのユーザに使用するデフォルトアカウンティング方式を指定する	**accounting default** { **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. LAN ユーザにアカウンティング方式を指定する	**accounting lan-access** { **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }	デフォルト：LANユーザのためのデフォルトアカウンティング方式
5. ログインユーザに使用するアカウンティング方式を指定する	**accounting login** { **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }	デフォルト：ログインユーザのためのデフォルトアカウンティング方式

1.5.7 ISP ドメインの NAS-ID の設定

以下に ISP ドメインの NAS-ID 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. ISP domain view に移行する	**domain** *isp-name*	―
3. ISP ドメインの NAS-ID を設定する	**nas-id** *nas-identifier*	デフォルト：設定なし

1.5.8 ISP ドメインの表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
ISP ドメインの設定を表示する	**display domain** [*isp-name*]

1.6 同時ログインユーザの最大数の設定

認証方法に関わらず、FTP、SSH、Telnet プロトコルを使用して、装置にログインできる最大ユーザ数を設定することができます。

以下に同時ログインユーザ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. 同時ログインユーザの最大数を設定する	**aaa session-limit** { **ftp** | **ssh** | **telnet** } *max-sessions*	デフォルト：32

1.7 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 7.5.142a を含む以降のソフトウェアからサポートしています。

1.7.1 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。

1.7.2 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。

1.7.3 EAP プロファイルの前提条件

ローカル証明書、秘密鍵、CA 証明書、または CRL ファイルを指定する前に、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。

1.7.4 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**	—
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*	—
3. デフォルトの EAP 認証方式を設定する	**method** { **md5** | **peap-mschapv2** | **tls** | **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

操作	コマンド	補足
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
8. EAP 認証用の CRL ファイルを設定する	**crl-file** *file-name*	デフォルト：設定なし 🕮 メモ：EAP認証用のCRLファイルの設定はソフトウェアバージョン7.5.143bを含む以降のソフトウェアからサポートしています。

1.8 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 7.5.142a を含む以降のソフトウェアからサポートしています。

1.8.1 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	
(オプション設定項目) RADIUSサーバの認証ログ出力の設定	
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	

1.8.2 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

1.8.3 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。

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。

🕮 **メモ：**

AP を認証サーバとして動作させる場合、自装置及び管理対象 AP(FIT)のための利用のみをサポートします。認証装置は自装置(FAT または Anchor-AC)で使用し、Radius クライアントで指定するアドレスは自装置の IP アドレスのみ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. 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

1.8.4 EAP 認証の設定

🕮 **メモ：**

EAP-TLS の EAP 認証方式は、ソフトウェアバージョン 7.5.143b を含む以降のソフトウェアからサポートしています。

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
- TLS
- 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 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

1.8.5 RADIUS サーバの認証ログ出力の設定

RADIUS サーバ機能の認証ログ出力機能を有効にします。

I. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. RADIUS サーバの認証ログ出力を有効化する	**radius-server auth-log enable**	デフォルト：無効

1.8.6 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、CRL ファイルの内容、RADIUS サーバの認証ログ出力設定を含む 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。
- デバイスに保存した CRL ファイルを変更する。
- RADIUS サーバの認証ログ出力の設定を変更する。

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**	―

1.8.7 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**	―

1.8.8 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*]

1.9 AAAの設定例

1.9.1 SSH ユーザの RADIUS 認証、アカウンティングの設定例

I. ネットワーク要件

図 1-7 に示すように、設定します。

- SSH サーバ用に RADIUS 認証、許可、アカウンティングを実行するように設定します。
- 認証にパスした後、SSH ユーザにデフォルトユーザロール network-operator を割り当てます。
- ユーザ名からドメイン名を削除してサーバに送信するように設定します。
- RADIUS サーバとセキュアな通信を行うため、共有鍵 **expert** を設定します。

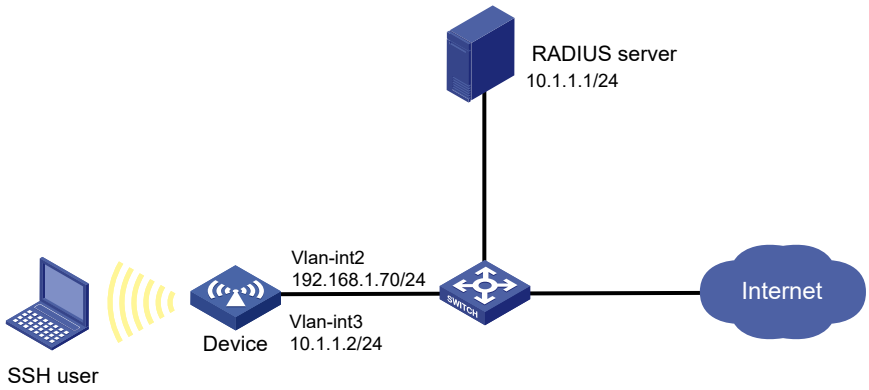


図 1-7 ネットワーク図

II. 設定手順

1)　RADIUS サーバを設定します。（詳細は省略します。）

装置とセキュアな通信を行うため共有鍵 export を設定します。

SSH ユーザのアカウントとパスワードを設定します。

2)　Device を設定します。

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。）

RADIUS スキームを設定します。

```
<Device> system-view
 [Device] radius scheme rd
```

プライマリ認証サーバを設定します。

```
[Device-radius-rd] primary authentication 10.1.1.1 1813
```

プライマリ許可サーバを設定します。

```
[Device-radius-rd] primary authorization 10.1.1.1 1813
```

プライマリアカウンティングサーバを設定します。

```
[Device-radius-rd] primary accounting 10.1.1.1 1813
```

セキュアな RADIUS 通信を行うため、プレーンテキストで共有鍵 export を設定します。

```
[Device-radius-rd] key authentication simple expert
[Device-radius-rd] key authorization simple expert
[Device-radius-rd] key accounting simple expert
```

RADIUS サーバから送信されたドメイン名からユーザ名を除外します。

```
[Device-radius-rd] user-name-format without-domain
[Device-radius-rd] quit
```

ログインユーザの認証、許可、アカウンティングの RADIUS スキームを使用するドメイン bbb を設定します。

```
[Device] domain bbb
[Device-isp-bbb] authentication login radius-scheme rd
[Device-isp-bbb] authorization login radius-scheme rd
[Device-isp-bbb] accounting login radius-scheme rd
```

ローカル RSA、DSA 鍵ペアを作成します。

```
[Device] public-key local create rsa
[Device] public-key local create dsa
```

SSH サービスを有効にします。

```
[Device] ssh server enable
```

ユーザロール VTY0～63 のスキーム認証を有効にします。

```
[Device] line vty 0 63
[Device-line-vty0-63] authentication-mode scheme
[Device-line-vty0-63] quit
```

認証にパスした後、SSH ユーザがデフォルトユーザロール network-operator を取得できるようにデフォルトユーザロール許可機能を有効にします。

```
[Device] role default-role enable
```

III. 設定の確認

ユーザが、Device への SSH 接続を開始し、ユーザ名 **hello@bbb** と正しいパスワードを入力したとき、ユーザが正常にログインし、network-operator ユーザロールでコマンドを使用することができます。

1.9.2 802.1X EAP-PEAP 認証を RADIUS サーバとして機能する AP で構成する

I. ネットワーク要件

図 1-8 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。

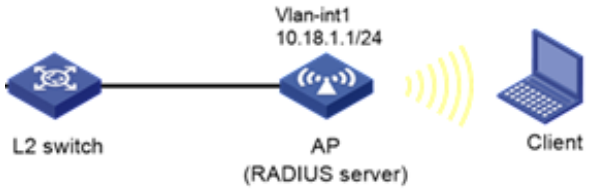


図 1-8 ネットワーク構成

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 AP に保存しておく必要があります。

本設定例では、AP 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. AP 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
[AP] dot1x
[AP] 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。

```
[AP] radius scheme freeradius
[AP-radius-freeradius] primary authentication 10.18.1.1 1812
[AP-radius-freeradius] key authentication simple 12345678
[AP-radius-freeradius] user-name-format without-domain
[AP-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。

```
[AP] domain freeradius
[AP-isp-freeradius] authentication lan-access radius-scheme freeradius
[AP-isp-freeradius] authorization lan-access radius-scheme freeradius
[AP-isp-freeradius] accounting lan-access none
[AP-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。

```
[AP] wlan service-template wlas_freeradius_peap
[AP-wlan-st-wlas_freeradius_peap] client-security authentication-mode dot1x
[AP-wlan-st-wlas_freeradius_peap] dot1x domain freeradius
[AP-wlan-st-wlas_freeradius_peap] ssid wlas_freeradius_peap
[AP-wlan-st-wlas_freeradius_peap] akm mode dot1x
[AP-wlan-st-wlas_freeradius_peap] cipher-suite ccmp
[AP-wlan-st-wlas_freeradius_peap] security-ie rsn
[AP-wlan-st-wlas_freeradius_peap] service-template enable
[AP-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。

```
[AP] wlan ap ap1 model QX-W1240
[AP-wlan-ap-ap1] serial-id 219801A28N819CE0002T
[AP-wlan-ap-ap1] radio 2
[AP-wlan-ap-ap1-radio-2] radio enable
[AP-wlan-ap-ap1-radio-2] service-template wlas_freeradius_peap
[AP-wlan-ap-ap1-radio-2] quit
[AP-wlan-ap-ap1] quit
```

4. PC 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。

```
[AP] local-user dot1x class network
[AP-luser-network-dot1x] password simple 123456
[AP-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。

```
[AP] eap-profile dot1x
[AP-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。

```
[AP-eap-profile-dot1x] ca-file ca.pem
[AP-eap-profile-dot1x] certificate-file server.pem
[AP-eap-profile-dot1x] private-key-file server-key.pem
[AP-eap-profile-dot1x] private-key-password simple whatever
[AP-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。

```
[AP] 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。

```
[AP] 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。

```
[AP] radius-server activate
```

III. 設定の確認

AP 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。

```
[AP] 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。）

AP 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。

```
[AP] 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
```

AP 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。

```
[AP] 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
```

1.9.3 802.1X EAP-TLS 認証を RADIUS サーバとして機能する AP で構成する

I. ネットワーク要件

図 1-8 に示すように AP は L2 スイッチと接続されています。

AP 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-TLS 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。

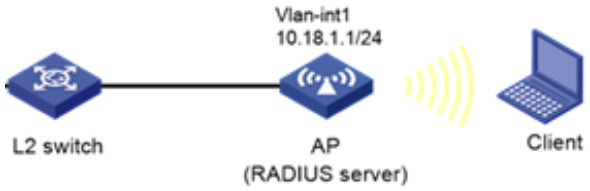


図 1-9 ネットワーク構成

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、CRL ファイルは、FTP などを使用してあらかじめ AP に保存しておく必要があります。

本設定例では、AP 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)、CRL ファイル(crl.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 証明書とクライアント証明書をインストールしておく必要があります。

1. AP 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。

```
<AP> system-view
[AP] dot1x
[AP] 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。

```
[AP] radius scheme freeradius
[AP-radius-freeradius] primary authentication 10.18.1.1 1812
[AP-radius-freeradius] key authentication simple 12345678
[AP-radius-freeradius] user-name-format without-domain
[AP-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。AP 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。

```
[AP] domain freeradius
[AP-isp-freeradius] authentication lan-access radius-scheme freeradius
[AP-isp-freeradius] authorization lan-access radius-scheme freeradius
[AP-isp-freeradius] accounting lan-access none
[AP-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。

```
[AP] wlan service-template wlas_freeradius_tls
[AP-wlan-st-wlas_freeradius_tls] client-security authentication-mode dot1x
[AP-wlan-st-wlas_freeradius_tls] dot1x domain freeradius
[AP-wlan-st-wlas_freeradius_tls] ssid wlas_freeradius_tls
[AP-wlan-st-wlas_freeradius_tls] akm mode dot1x
[AP-wlan-st-wlas_freeradius_tls] cipher-suite ccmp
[AP-wlan-st-wlas_freeradius_tls] security-ie rsn
[AP-wlan-st-wlas_freeradius_tls] service-template enable
[AP-wlan-st-wlas_freeradius_tls] 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_tls)をバインドします。

```
[AP] Interface WLAN-Radio 1/0/1
[AP-WLAN-Radio1/0/1] service-template wlas_freeradius_tls
[AP-WLAN-Radio1/0/1] quit
[AP] quit
```

4. 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 EAP-TLS に設定します。

```
[AP] eap-profile dot1x
[AP-eap-profile-dot1x] method tls
```

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、CRL 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。

```
[AP-eap-profile-dot1x] ca-file ca.pem
[AP-eap-profile-dot1x] certificate-file server.pem
[AP-eap-profile-dot1x] private-key-file server-key.pem
[AP-eap-profile-dot1x] crl-file crl.pem
[AP-eap-profile-dot1x] private-key-password simple whatever
[AP-eap-profile-dot1x] quit
```

AP 上の RADIUS サーバに EAP プロファイル dot1x を適用します。

```
[AP] 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。

```
[AP] 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。

```
[AP] radius-server activate
```

III. 設定の確認

AP 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。

```
[AP] display radius-server active-client
Total 1 RADIUS clients.
Client IP: 10.18.1.1
```

端末側で、SSID wlas_freeradius_tls に 802.1X 接続を通じて接続します。クライアント証明書を使用して認証します。（詳細は省略。）

AP 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証明書のユーザ名と同じであることを確認します。

```
[AP] 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
```

AP 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。

```
[AP] 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
```

1.10 RADIUSのトラブルシューティング

1.10.1 RADIUS 認証の失敗

I. 症状

認証が常に失敗します。

II. 分析

可能性のある理由を以下に示します。

- NAS と RADIUS サーバ間で通信障害が存在します。
- ユーザ名が userid@isp-name のフォーマットではありません、あるいは NAS で ISP ドメインが正しく設定されていません。
- ユーザが RADIUS サーバで設定されていません。
- ユーザで入力したパスワードが間違っています。
- RADIUS サーバと NAS が異なる共有鍵で設定されています。

III. 解決策

以下を確認してください。

- NAS と RADIUS サーバがお互いに ping できることを確認してください。
- ユーザ名が userid@isp-name のフォーマットで、NAS で ISP ドメインが正しく設定されていることを確認してください。
- ユーザが RADIUS サーバで設定されていることを確認してください。
- 正しいパスワードを入力してください。
- RADIUS サーバと NAS の両方で同じ共有鍵が設定されていることを確認してください。

問題が解決しない場合、販売店もしくは担当営業に問い合わせてください。

1.10.2 RADIUS パケットが到達不能

I. 症状

RADIUS パケットが RADIUS サーバに到達できません。

II. 分析

可能性のある理由を以下に示します。

- NAS と RADIUS サーバ間で通信障害が存在します。
- NAS に RADIUS サーバの IP アドレスが設定されていません。
- NAS の認証、アカウンティングの UDP ポートが正しくありません。
- RADIUS サーバの認証、アカウンティングのためのポート番号がほかのアプリケーションで使用されています。

III. 解決策

以下を確認してください。

- NAS と RADIUS サーバ間のリンクが物理レイヤ、データリンクレイヤの両方で正しく動作することを確認してください。

- RADIUS サーバの IP アドレスが NAS で正しく設定されていることを確認してください。
- NAS で設定された認証、アカウンティングの UDP ポートが RADIUS サーバで設定されているものと同じであることを確認してください。
- RADIUS サーバの認証、アカウンティングのためのポート番号が使用可能であることを確認してください。

問題が解決しない場合、販売店もしくは担当営業に問い合わせてください。

1.10.3 RADIUS アカウンティングエラー

I. 症状

ユーザは認証と許可されましたが、アカウンティングが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の設定が間違っています。可能性のある理由を以下に示します。

- NAS で設定されたアカウンティングのためのポート番号が間違っています。
- NAS で設定されたアカウンティングサーバの IP アドレスが間違っています。たとえば、NAS が認証、許可、アカウンティングサービスを提供するために、1 つのサーバを使用するように設定されていますが、実際のサービスは異なるサーバによって提供されています。

III. 解決策

以下を確認してください。

- アカウンティングのためのポート番号が正しく設定されていることを確認してください。
- 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ことを確認してください。

問題が解決しない場合、販売店もしくは担当営業に問い合わせてください。

1.11 付録

1.11.1 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 1-2 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)

No	属性	No	属性
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
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)

1.11.2 付録 B 一般的に使用される標準 RADIUS 属性の説明

表 1-3 一般的に使用される標準 RADIUS 属性

No	属性	説明
1	ユーザ名	認証されるユーザの名前。

No	属性	説明
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タイプまたは提供されるサービスタイプ。
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。
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。

No	属性	説明
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。
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。

目次

このセクションのページは **9-x-x** です。

2章 802.1Xの概要 2-1
2.1 802.1Xの構成 2-1
2.2 制御/非制御ポートとポート許可状態 2-1
2.3 802.1X関連プロトコル 2-2
2.3.1 パケットフォーマット 2-2
2.3.2 EAP over RADIUS 2-4
2.4 802.1X認証の開始 2-4
2.4.1 802.1Xクライアントからの認証開始 2-5
2.4.2 アクセスデバイスからの認証開始 2-5
2.5 802.1Xの認証プロセス 2-5
2.5.1 EAP relayとEAP terminationの比較 2-6
2.5.2 EAP relay 2-6
2.5.3 EAP termination 2-8

2章 802.1X の概要

802.1X は、ポートベースのネットワークアクセス制御プロトコルです。

802.1X は、802.1X が有効な LAN ポートに接続された装置を、認証サーバ(RADIUS サーバなど)による認証することでネットワークを保護します。

2.1 802.1Xの構成

802.1X は、クライアント/サーバモデルで動作します。図 2-1に示すように 802.1X 認証は以下の構成要素があります。

- **クライアント（サプリカント）**－クライアントは、LAN へアクセスしようとするユーザの端末です。端末はネットワークアクセスデバイスを認証する 802.1X ソフトウェアが必要です。
- **アクセスデバイス（オーセンティケータ）**－ネットワークアクセスデバイスは、クライアントを認証し、LAN へのアクセスを制御します。通常の 802.1X 環境では、ネットワークアクセスデバイスは、認証サーバを使用して認証を実行します。
- **認証サーバ**－認証サーバは、ネットワークアクセスデバイスの認証サービスを提供するエンティティです。ネットワークアクセスデバイスから送信されたデータを使用して 802.1X クライアントを認証し、ネットワークアクセスデバイスがアクセスするための認証結果を返します。認証サーバは通常、RADIUS（Remote Authentication Dial-in User Service）サーバです。小規模な LAN では、認証サーバとしてネットワークアクセスデバイスを使用することもできます。

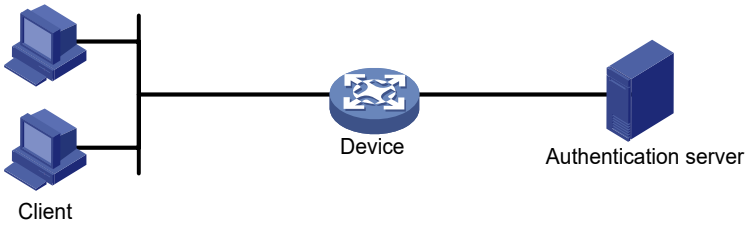


図 2-1 802.1X の構成

2.2 制御/非制御ポートとポート許可状態

802.1X は、ネットワークのアクセスポートのために、制御ポートと非制御ポートの 2 つの論理ポートを定義しています。ネットワークのアクセスポートに受信するパケットはすべて、両方の論理ポートに表示されます。

- **非制御ポート**－非制御ポートは常にオープン状態で、認証パケットを送信します。
- **制御ポート**－ポートの状態に依存してパケットをフィルタします。
  - **許可状態**－クライアントが認証にパスしたとき、ポートは authorized 状態になります。このポートはトラフィックを通過させることができます。

- **非許可状態**－クライアントが認証にパスしないとき、ポートは unauthorized 状態になります。以下の方法の 1 つによってトラフィックを制御します。
  - クライアントへのトラフィックとクライアントからのトラフィックを拒否するように、双方向のトラフィックを制御します。
  - クライアントからのトラフィックを拒否するように、片方向のトラフィックを制御します。本デバイスは片方向のトラフィック制御のみをサポートしています。

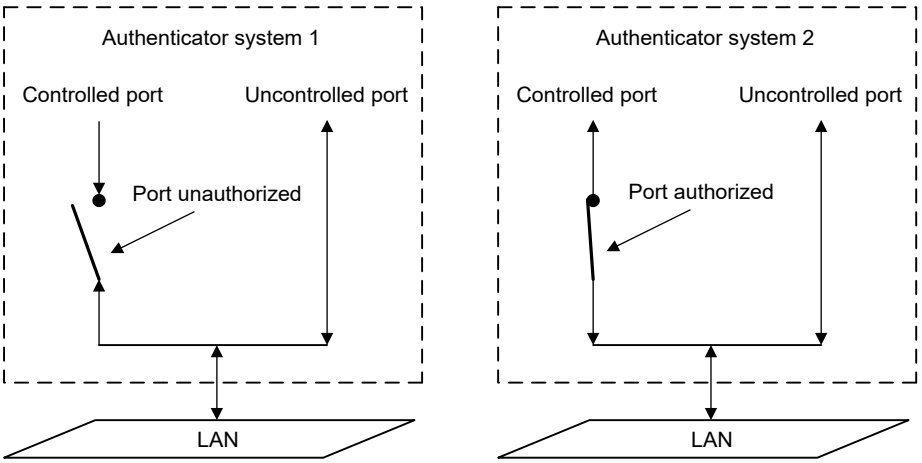


図 2-2 制御ポートの許可/非許可状態

2.3 802.1X関連プロトコル

802.1X は、クライアント、ネットワークアクセスデバイス、認証サーバの認証情報を転送するために EAP（Extensible Authentication Protocol）を使用しています。 EAP は、クライアント/サーバモデルを使用する認証フレームワークです。MD5-Challenge、EAP-TLS（EAP-Transport Layer Security）、PEAP（Protected EAP）を含む様々な認証方式をサポートしています。

802.1X は、有線または無線 LAN 経由で、クライアントとアクセスデバイス間で EAPOL（EAP over LAN）を定義します。アクセスデバイスと認証サーバとの間で、802.1X は、次のいずれかの方法で認証情報を提供します。

- **EAP relay**：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 termination**：EAP パケットから認証情報を抽出し、標準的な RADIUS パケット内の情報をカプセル化します。

2.3.1 パケットフォーマット

I. EAP パケットのフォーマット

図 2-3に EAP パケットのフォーマットを示します。

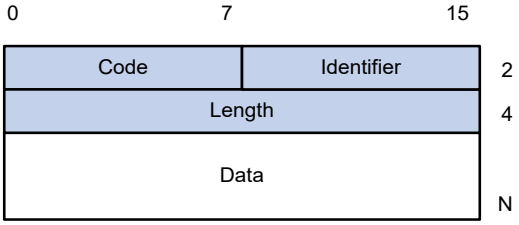


図 2-3 EAP パケットのフォーマット

- **Code**－EAP パケットのタイプです。Request(1)、Response(2)、Success(3)、Failure(4)があります。
- **Identifier**－リクエストとレスポンスを対応づけます。
- **Length**－EAP パケット長（byte）です。Code、Identifier、Length、Data フィールドの合計です。
- **Data**－EAP パケットの中身です。このフィールドは、リクエストまたはレスポンス EAP パケットにのみあります。リクエストタイプ（またはレスポンスタイプ）とタイプデータで構成されています。タイプ 1（Identify）とタイプ 4（MD5-Challenge）はタイプフィールドの 2 つの例です。

II. EAPOL パケットのフォーマット

図 2-4に EAPOL パケットのフォーマットを示します。

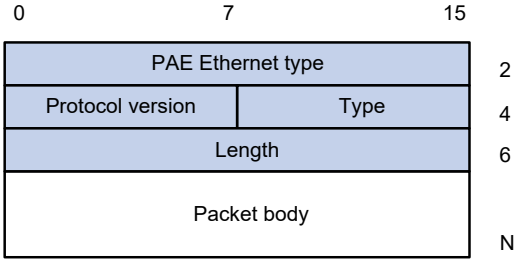


図 2-4 EAPOL パケットのフォーマット

- **PAE Ethernet type**－プロトコルタイプです。EAPOL の値は 0x888E です。
- **Protocol version**－EAPOL パケットの送信元がサポートする EAPOL プロトコルのバージョンです。
- **Type**－EAPOL パケットのタイプです。表 2-1に装置がサポートする EAPOL パケットのタイプを示します。

表 2-1 EAPOL パケットのタイプ

値	タイプ	説明
0x00	EAP-Packet	クライアントとネットワークアクセスデバイスは、認証情報を運ぶためにEAP-Packetを使用します。
0x01	EAPOL-Start	クライアントは、802.1X認証を開始させるために、ネットワークアクセスデバイスにEAPOL-Startメッセージを送ります。
0x02	EAPOL-Logoff	クライアントは、ログオフを通知するために、アクセスデバイスにEAPOL-Logoffメッセージを送ります。

- **Length**－データ長（byte）です。Packet body フィールド長を示します。パケットタイプが EAPOL-Start か EAPOL-Logoff の場合、このフィールドに 0 がセットされ、Packet body フィールドは存在しません。
- **Packet body**－パケットの中身です。EAPOL パケットタイプが EAP-Packet の時、Packet body フィールドが EAP パケットの中身です。

2.3.2 EAP over RADIUS

RADIUS は EAP 認証をサポートするため、EAP-Message と Message-Authenticator の 2 つの属性を追加します。RADIUS パケットのフォーマットについての詳細は、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。

I. EAP-Message

図 2-5に示すように RADIUS は、EAP-Message 属性に EAP パケットをカプセル化します。このパケットの Type フィールドの値は 79 です。String フィールドには最大 253 バイトまで入ります。EAP パケット長が 253 バイト以上である場合、複数の EAP-Message 属性にカプセル化されます。

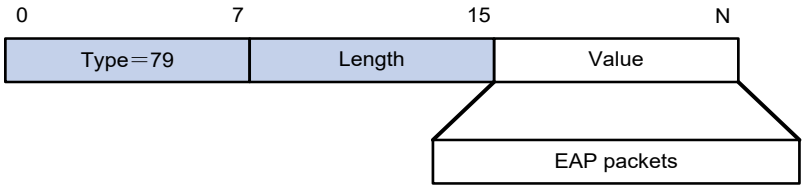


図 2-5 EAP-Message の属性フォーマット

II. Message-Authenticator

RADIUS は、整合性をチェックするため EAP-Message 属性を持つすべてのパケットに Message-Authenticator 属性を含めます。

計算されたパケットの整合性チェックサムが Message-Authenticator 属性の値と異なる場合、パケットの受信者はパケットを廃棄します。Message-Authenticator は、EAP 認証中に EAP 認証パケットが改ざんされることを防ぎます。

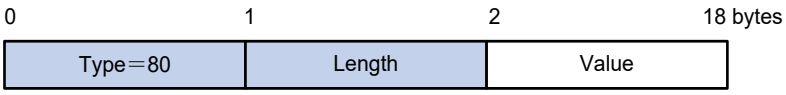


図 2-6 Message-Authenticator の属性フォーマット

2.4 802.1X認証の開始

802.1X 認証は、802.1X クライアントと装置のどちらからでも開始させることができます。

2.4.1 802.1X クライアントからの認証開始

クライアントは、アクセスデバイスに EAPOL-Start パケットを送信することで、802.1X 認証を開始します。このパケットの宛先 MAC アドレスは、IEEE 802.1X で指定されたマルチキャストアドレス 01-80-C2-00-00-03 またはブロードキャスト MAC アドレスです。クライアントと認証サーバ間のすべての中間デバイスがマルチキャストアドレスをサポートしていない場合、ブロードキャスト EAPOL-Start パケットを送信できる 802.1X クライアントを使用する必要があります。

2.4.2 アクセスデバイスからの認証開始

クライアントが EAPOL-Start パケットを送信できない場合、アクセスデバイスが認証を開始するよう設定します。たとえば 802.1X クライアントは Windows XP で使用できます。

アクセスデバイスは、以下のモードをサポートしています。

- **マルチキャストトリガモード**－アクセスデバイスが、定期的に（デフォルトでは 30 秒ごと）EAP-Request/Identity パケットをマルチキャスト送信することで、802.1X 認証を開始します。
- **ユニキャストトリガモード**－MAC アドレステーブルにない送信元 MAC アドレスのフレームを受信したとき、アクセスデバイスは受信ポートから未知の MAC アドレスへ EAP-Request/Identity パケットを送信します。応答を一定時間内に受信しない場合、パケットを再送します。

2.5 802.1Xの認証プロセス

802.1X 認証には、EAP relay と EAP termination の 2 つのアプローチがあります。EAP パケットと EAP 認証方式のために RADIUS サーバのサポートに応じていずれかのモードを選択してください。

- EAP relay モード

EAP relay は、IEEE802.1X で定義されています。このモードでは、ネットワークデバイスは、図 2-7に示すように、RADIUS サーバに認証情報を送信するために EAPOR パケットを使用します。

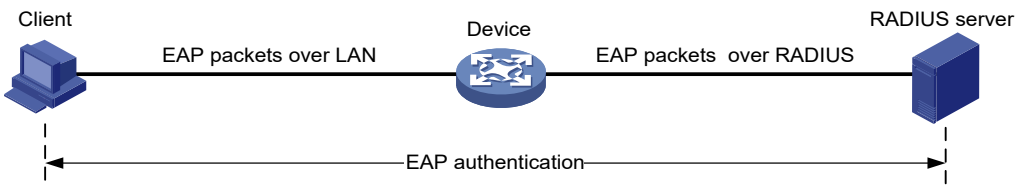


図 2-7 EAP relay

EAP relay モードでは、クライアントは RADIUS サーバと同じ認証方式を用いる必要があります。ネットワークアクセスを行うデバイス上では、EAP relay で利用するために **dot1x authentication-method eap** コマンドのみが必要です。

- EAP termination モード

図 2-8に示すように、アクセスデバイスは EAP termination モードで以下の動作を行います。

a) クライアントから受信したEAPパケットを終端します。

b) 標準RADIUSパケットにクライアント認証情報をカプセル化します。

c) RADIUSサーバに認証するため、PAPあるいはCHAPを使用します。

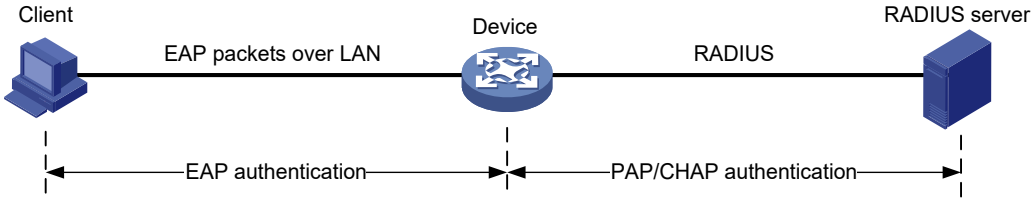


図 2-8 EAP termination

2.5.1 EAP relay と EAP termination の比較

パケット交換方式	利点	制限
EAP relay	• 様々なEAP認証方法をサポートしています。 • アクセスデバイス上の設定と処理が簡単です。	RADIUSサーバはEAP-MessageとMessage-Authenticator属性と、クライアントに使用されるEAP認証方式をサポートする必要があります。

EAP termination	PAPまたはCHAP認証をサポートしている任意のRADIUSサーバと連携して動作します。	• 以下のEAP認証方式のみをサポートします。
		  • MD5-Challenge EAP認証
		  • ユーザ名とパスワードのEAP認証
		• アクセスデバイス上の処理が複雑です。

2.5.2 EAP relay

図 2-9に EAP-MD5 を使用した、EAP relay モードでの基本的な 802.1X 認証プロセスを示します。

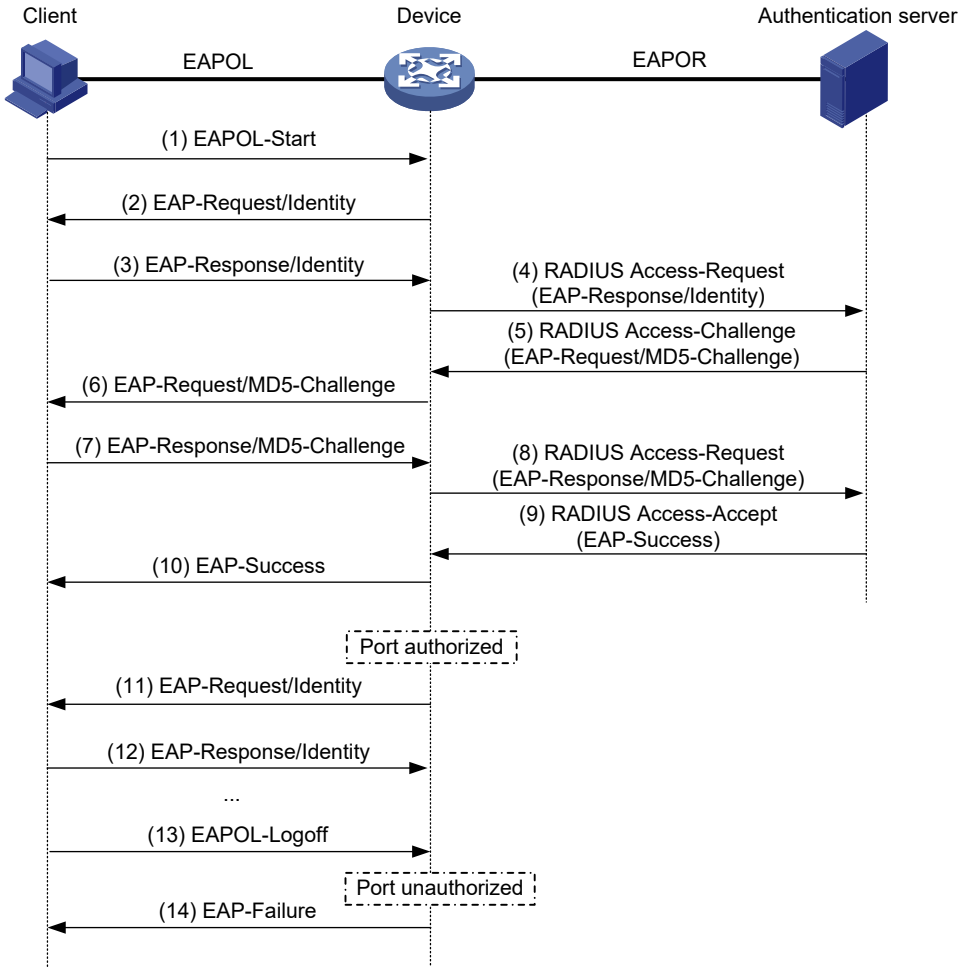


図 2-9 EAP relay モードでの 802.1X 認証プロセス

以下に 802.1X 認証プロセスを記載します。

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、アクセスデバイスに EAPOL-Start パケットを送信します。
2) アクセスデバイスは、応答としてクライアントのユーザ名を要求するために EAP-Request/Identity パケットを送信します。
3) EAP-Request/Identity パケットの応答として、クライアントは EAP-Request/Identity パケットの中にユーザ名を入れて、アクセスデバイスに送信します。
4) アクセスデバイスは、RADIUS Access-Request パケットの EAP-Request/Identity パケットを認証サーバに伝搬します。
5) 認証サーバは、ユーザのデータベースを検索するため、RADIUS Access-Request パケットの identify 情報を使用します。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るチャレンジ（EAP-Request/MD5 challenge）を使用してパスワード情報を暗号化し、RADIUS Access-Challenge パケットを通してネットワークアクセスデバイスにチャレンジ情報を送信します。
6) アクセスデバイスは、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情報を使用してパスワードを暗号化します。そして EAP-Response/MD5 Challenge パケットの暗号化したパスワードをアクセスデバイスに送信します。
8) アクセスデバイスは、RADIUS Access-Request パケットの EAP-Response/MD5 Challenge パケットを認証サーバに伝搬します。
9) 認証サーバは、受信したパスワード情報と、5)で自身が生成したパスワード情報を比較します。2 つのパスワード情報が一致する場合、認証サーバはクライアントが有効であるとみなし、アクセスデバイスに RADIUS Access-Accept パケットを送信します。
10) RADIUS Access-Accept パケットを受信すると、アクセスデバイスは、以下の動作を行います。

a) クライアントにEAP-Successパケットを送ります。

b) 制御ポートをauthorized状態に設定します。

クライアントはネットワークにアクセスできます。

11) クライアントがオンラインになった後、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ために、アクセスデバイスは定期的にハンドシェイク要求を送信します。デフォルトでは、2 回連続してハンドシェイクが失敗すると、デバイスはクライアントをログオフします。
12) ハンドシェイク要求を受け取ると、クライアントは応答を返します。クライアントが特定の回数（デフォルトで 2 回）連続してハンドシェイク応答に失敗した場合、アクセスデバイスは、クライアントをログオフします。このハンドシェイクメカニズムにより、異常にオフラインになった 802.1X ユーザによって使用されるネットワークリソースをタイムリーにリリースすることが可能になります。
13) クライアントは、アクセスデバイスにログオフを依頼する EAPOL-Logoff パケットを送信することもできます。
14) EAPOL-Logoff パケットに応答して、アクセスデバイスは、制御ポートの状態を authorized から unauthorized に変更し、クライアントへ EAP-Failure パケットを送信します。

2.5.3 EAP termination

図 2-10に CHAP 認証を使用した、EAP termination モードでの基本的な 802.1X 認証プロセスを示します。

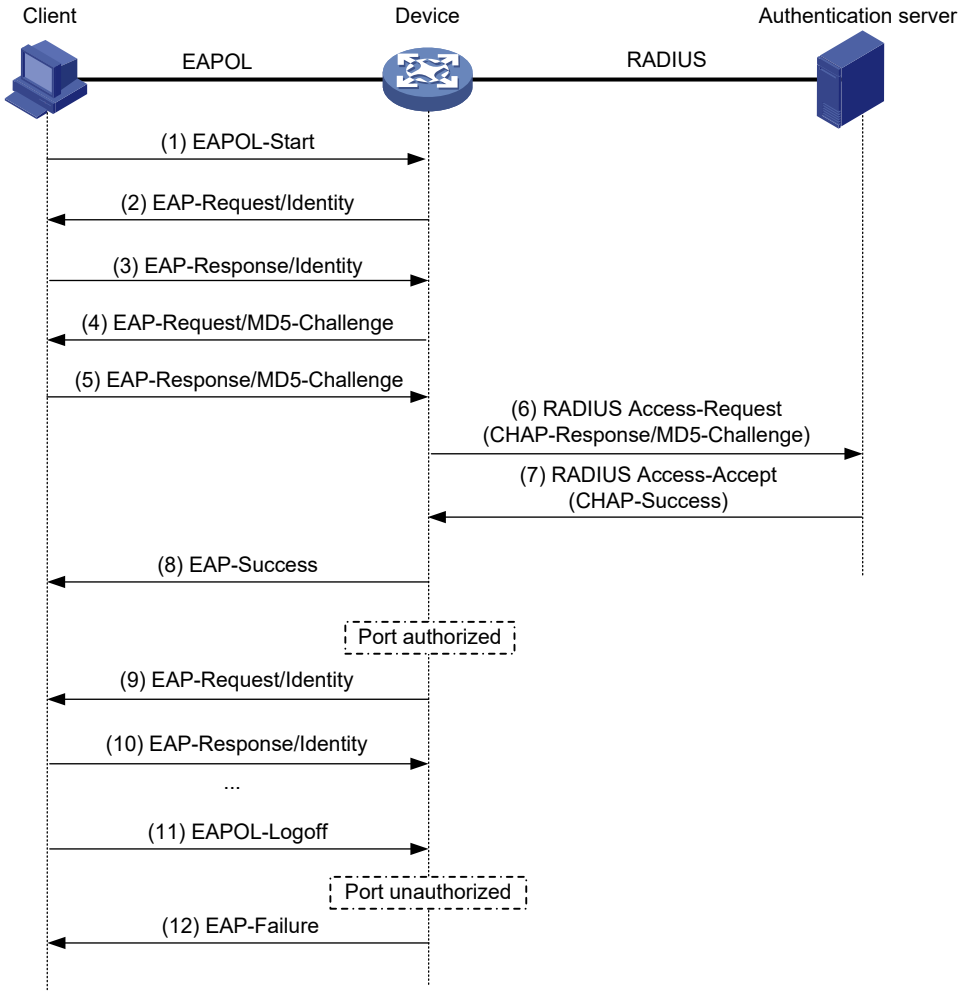


図 2-10 EAP termination での 802.1X 認証プロセス

EAP termination モードでは、パスワードを暗号化するために MD5 challenge を生成するのは認証サーバでなく、アクセスデバイスです。アクセスデバイスは次に、MD5 challenge をユーザ名と暗号化されたパスワードと一緒に標準の RADIUS パケットに入れて RADIUS サーバへ送信します。

目次

このセクションのページは **9-x-x** です。

3章 802.1X 3-1
3.1 アクセス制御方式 3-1
3.2 802.1XのVLAN操作 3-1
3.2.1 許可VLAN 3-1
3.2.2 ゲストVLAN 3-4
3.2.3 制限VLAN 3-5
3.3 他の機能を用いた802.1X認証 3-5
3.3.1 ACLの割り当て 3-5
3.4 設定要件 3-6
3.5 802.1X設定作業リスト 3-6
3.6 802.1X認証の有効化 3-6
3.7 EAP relayまたはEAP terminationの有効化 3-7
3.8 ポート許可状態の設定 3-8
3.9 アクセス制御方式の指定 3-8
3.10 ポートの802.1Xユーザの最大同時接続数の設定 3-8
3.11 認証リクエストの最大送信数の設定 3-9
3.12 802.1X認証タイムアウトタイマの設定 3-9
3.13 オンラインユーザハンドシェイク機能の設定 3-9
3.13.1 設定ガイドライン 3-10
3.13.2 設定手順 3-10
3.14 認証トリガ機能の設定 3-10
3.14.1 設定ガイドライン 3-10
3.14.2 設定手順 3-11
3.15 ポートでの強制認証ドメインの設定 3-11
3.16 quietタイマの設定 3-11
3.17 802.1X再認証の設定 3-12
3.17.1 概要 3-12
3.17.2 設定ガイドライン 3-12
3.17.3 802.1X定期的な再認証の設定 3-13
3.18 802.1X制限VLANの設定 3-13
3.18.1 設定ガイドライン 3-13
3.18.2 設定要件 3-14
3.18.3 設定手順 3-14
3.19 802.1Xの表示と維持 3-14
3.20 802.1X認証の設定例 3-15
3.20.1 基本的な802.1X認証の設定例 3-15

3章 802.1X

この章は、装置上で 802.1X を設定する方法について説明します。802.1X を実行時に、ポートセキュリティ機能を設定することもできます。ポートセキュリティは 802.1X と MAC アドレス認証を組み合わせて拡張します。ポート上でユーザごとに異なる認証方法を必要とするネットワークや WLAN に適用します。

🕮 **メモ：**

ポートセキュリティ機能はサポートしていません。

3.1 アクセス制御方式

802.1X プロトコルで定義されたポートベースのアクセス制御を実装しており、MAC ベースのアクセス制御をサポートするためにプロトコルを拡張します。

- **ポートベースアクセス制御**－ポートベースのアクセス制御では、一度 802.1X ユーザがポート上で認証を通過すると、後続のユーザは、認証なしでポートを介してネットワークにアクセスできます。認証されたユーザがログオフすると、他のすべてのユーザはログオフされます。
- **MAC ベースアクセス制御**－MAC ベースのアクセス制御では、各ユーザは個別にポート上で認証されます。ユーザがログオフしても、他のオンラインのユーザは影響を受けません。

3.2 802.1XのVLAN操作

3.2.1 許可 VLAN

802.1X ユーザが許可されたネットワークリソースへのアクセスを制御するため、許可 VLAN を指定することができます。802.1X ユーザが認証にパスしたのち、認証サーバは許可 VLAN あるいは VLAN グループをユーザに割り当てます。

I. サポートされる VLAN タイプと形式

VLAN タイプと形式は許可タイプに依存してサポートされます。

- ローカル VLAN 許可

  アクセス装置で user view あるいは user group view で VLAN ID によって 1 つの許可 VLAN のみを指定することができます。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 9 *セキュリティ “AAA”* を参照してください。
- リモート VLAN 許可

802.1X ユーザの AAA サーバで VLAN あるいは VLAN グループを指定することができます。アクセス装置は以下の形式の VLAN をサポートします。

- VLAN ID
- VLAN 名

VLAN 名はアクセス装置で VLAN の特徴を示します。

- VLAN ID と VLAN 名の組み合わせ

文字列で、ある VLAN は VLAN ID で示し、ある VLAN は VLAN 名で示します。

- VLAN グループ名

VLAN グループの詳細は、オペレーションマニュアルのセクション 4 *アクセス "VLAN"* を参照してください。

- サフィックスを持つ VLAN ID

サフィックスは、t あるいは u が使用できます。VLAN がタグづけされるポートかどうかを示します。たとえば、2u は VLAN2 がタグづけされていないメンバに割り当てられていることを示します。

🕮 **メモ：**

アクセス装置は、VLAN の割り当てを行う前に、VLAN 名と VLAN グループ名を VLAN ID に置き換えます。

II. サポートされない VLAN タイプ

VLAN 許可では以下のタイプを指定することができません。アクセス装置は、802.1X ユーザに VLAN を割り当てることができません。

- ダイナミックに学習された VLAN
- 作成されていない VLAN
- 予約された VLAN

III. VLAN の選択と割り当て

サーバが VLAN のグループを割り当てるとき、アクセス装置は VLAN ID のフォーマットに従って VLAN を選択し、割り当てます。表 3-1に許可 VLAN のグループの選択と割り当てルールを記載します。

表 3-1 許可 VLAN のグループの VLAN の選択と割り当て

許可 VLAN のタイプ	VLAN の選択と割り当てルール
• VLAN ID • VLAN名 • VLANグループ名	デバイスは、ポートで他のオンラインユーザがいるかどうかに依存して、許可VLANとしてVLANを選択します。 • ポートで他のオンラインユーザがいない場合、デバイスはVLANのグループからもっとも小さいIDのVLANを選択します。 • ポートで他のオンラインユーザがいる場合、以下の処理によってVLANを選択します。 1. デバイスはオンラインユーザから一番遠い番号を持つ VLAN を選択します。 2. 2 つの VLAN がオンライン 802.1X ユーザと同じ番号を持

許可 VLAN のタイプ	VLAN の選択と割り当てルール
	っている場合、デバイスはもっとも小さい ID の VLAN を選択します。 表 3-2にデバイスがVLANの割り当てを行うルールを示します。
サフィックスを持つVLAN ID	1. デバイスはサフィックスを除いた一番左の VLAN ID、あるいは、タグなしとして u のサフィックスが付いた一番左の VLAN ID を選択します。 2. デバイスは PVID としてポートにタグなしの VLAN を割り当て、タグづけられた VLAN はそのまま割り当てます。もしタグなし VLAN が割り当てられていない場合、ポートの PVID は変更しません。ポートは、タグづけ VLAN とタグなし VLAN からのトラフィックを通過するように許可します。 たとえば、認証サーバはユーザ用に、1u 2t 3の文字列をアクセス装置に送信します。デバイスはタグなしVLANとしてVLAN1を割り当てし、タグづけVLANとして他のVLANを割り当てます。VLAN1はPVIDになります。

メモ：

サフィックスを持つ VLAN ID は、ポートベースのアクセス制御を行うハイブリッドポートあるいはトランクポートのみ割り当てることができます。

表 3-2にアクセス装置が 802.1X が有効なポートで VLAN を処理する方法を記載します。（サフィックスを持つ VLAN を除きます。）

表 3-2 VLAN 操作

ポートアクセス制御方式	VLAN 操作
ポートベース	デバイスは最初の認証ユーザの許可VLANをポートVLAN（PVID）に割り当てます。後続のすべての802.1Xユーザは認証なしでアクセスできます。 最初に認証されたユーザがログオフすると、前のPVIDが復元され、他のすべてのオンラインユーザはログオフされます。
MACベース	デバイスは最初の認証ユーザの認可VLANをPVIDとしてポートに割り当てます。他のVLANが後続のユーザに対して許可されている場合、ユーザが認証に成功できません。後続のユーザが認証に成功するためには、同じVLANを全てのポートの802.1Xユーザに許可する必要があります。

メモ：

802.1X が有効なアクセスポートは、タグなしメンバとしてのみ許可 VLAN を割り当てられます。ハイブリッドポートは、常にタグなしメンバとして VLAN に割り当ててください。割り当てられたのち、VLAN のタグ付きメンバとしてポートを再設定しないでください。

3.2.2 ゲスト VLAN

🕮 **メモ：**
この機能は、MAC ベースのアクセスコントロールを実行する 802.1X 有効化ポートには適用されません。

ポート上の 802.1X ゲスト VLAN は、802.1X 認証を実行していないユーザに対応します。

ゲスト VLAN のユーザは、アンチウィルスソフトウェアやシステムパッチをダウンロードするためにソフトウェアサーバなどの制限されたネットワークリソースにアクセスすることができます。ゲスト VLAN でユーザが一度 802.1X 認証にパスすると、ゲスト VLAN から削除され、許可されたネットワークリソースにアクセスすることができます。

802.1X ゲスト VLAN は、ポートベースアクセス制御を実行するポートでのみ有効です。

次の表は、アクセスデバイスがポートベースアクセス制御を実行する 802.1X 対応ポート上で VLAN を処理する方法を示しています。

認証状態	VLAN 操作
ユーザが802.1X認証にパスしていない	デバイスはPVIDとして802.1Xゲスト VLANをポートに割り当てます。ポートのすべての802.1Xユーザはゲスト VLANのリソースのみアクセスできます。802.1Xゲスト VLANが設定されていない場合、アクセス装置は任意のVLANの操作を実行しません。
802.1Xゲスト VLANのユーザが802.1X認証に失敗した	802.1X制限VLAN（Auth-Fail VLAN、オペレーショマニュアルのセクション9 *セキュリティ “802.1X” の “制限VLAN”* を参照してください）が有効である場合、デバイスはPVIDとして制限VLANを割り当てます。 制限VLANが設定されていない場合、ポートのPVIDは802.1Xゲスト VLANのままとなります。ポートのすべてのユーザはゲスト VLANの中にいます。
802.1Xゲスト VLANのユーザが802.1X認証に成功した	• デバイスはPVIDとしてユーザの認証VLANを割り当てます。802.1Xゲスト VLANからポートを削除します。ユーザがログオフしたのち、ポートの最初のPVIDがもとに戻ります。 • 認証サーバがVLANを許可しない場合、初期のPVIDを適用します。ユーザと後続のすべての802.1Xユーザは初期ポートに割り当てられます。ユーザがログオフしたのち、ポート VLANは変更されません。 🕮 **メモ：** 802.1Xが有効なポートの初期のPVIDは、ポートが任意の802.1X VLANに割り当てられる前にポートで使用されたPVIDです。

ネットワークデバイスはハイブリッドポートをタグなしメンバとして 802.1X ゲスト VLAN に割り当てます。

VLAN の設定の詳細は、オペレーションマニュアルのセクション 4 *アクセス “VLAN”* を参照してください。

3.2.3 制限 VLAN

🕮 **メモ：**

この機能は、MAC ベースのアクセスコントロールを実行する 802.1X 有効化ポートには適用されません。

組織のセキュリティ戦略に適合できずに失敗したことが原因で 802.1X 認証に失敗したユーザに対応するため、制限 VLAN を設定することができます。たとえば間違ったパスワードを入力したユーザに VLAN が適応します。制限 VLAN は、アンチウィルスソフトウェアやシステムパッチをダウンロードするためにソフトウェアサーバなどの制限されたネットワークリソースのみアクセスすることができます。

制限 VLAN は、ポートベースアクセス制御を実行するポートでのみ有効です。

次の表は、アクセス装置がポートベースアクセス制御を実行する 802.1X 対応ポート上で VLAN を処理する方法を示しています。

認証状態	VLAN 操作
ユーザが802.1X認証に失敗した	デバイスはPVIDとしてポートに制限VLANを割り当てます。ポートのすべての802.1Xユーザは制限VLANのリソースのみアクセスすることができます。
サーバ到達不能の理由を除いた他の理由によって、802.1X制限VLANのユーザが802.1X認証に失敗した	制限VLANが設定されている場合、ポートのPVIDは制限VLAN IDに変更されます。ポートのすべての802.1Xユーザはこの VLANにいます。
ユーザが802.1X認証にパスした	• デバイスはPVIDとしてポートにユーザの許可VLANを割り当て、制限VLANからポートを削除します。ユーザがログオフしたのち、ゲストVLANがPVIDとしてポートに割り当てられます。ゲストVLANが設定されていない場合、初期のPVIDに戻ります。 • 認証サーバがVLANを許可しない場合、ポートの初期のPVIDが適用されます。ユーザと後続のすべての802.1Xユーザは初期のPVIDに割り当てられますユーザがログオフしたのち、PVIDは変更されません。

アクセス装置はハイブリッドポートをタグなしメンバとして 802.1X ゲスト VLAN に割り当てます。

VLAN の設定の詳細は、オペレーションマニュアルのセクション 4 *アクセス “VLAN”* を参照してください。

3.3 他の機能を用いた802.1X認証

3.3.1 ACL の割り当て

ネットワークリソースへのアクセスを制御するため、802.1X ユーザに ACL を指定することができます。ユーザが 802.1X 認証にパスしたのち、認証サーバはユーザのトラフィッ

クをフィルタするためアクセスポートに ACL を割り当てます。認証サーバはローカルアクセス装置あるいは RADIUS サーバで行えます。どちらの場合でも、アクセス装置で ACL を設定する必要があります。ユーザはオンライン中に ACL を変更することができます。ACL の詳細は、オペレーションマニュアルのセクション 8 *ACL and QoS "ACL"* を参照してください。

3.4 設定要件

802.1X を設定する前に、以下の作業を完了してください。

- 802.1X ユーザのために ISP ドメインと AAA スキーム（ローカルまたは RADIUS 認証）を設定してください。
- RADIUS 認証を使用する場合は、RADIUS サーバにユーザアカウントを作成してください。
- ローカル認証を使用する場合は、アクセス装置に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 に設定してください。

RADIUS クライアントの設定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。

3.5 802.1X設定作業リスト

作業リスト
（必須設定項目）802.1X認証の有効化
（必須設定項目）EAP relayまたはEAP terminationの有効化
（オプション設定項目）ポート許可状態の設定
（オプション設定項目）アクセス制御方式の指定
（オプション設定項目）ポートの802.1Xユーザの最大同時接続数の設定
（オプション設定項目）認証リクエストの最大送信数の設定
（オプション設定項目）802.1X認証タイムアウトタイマの設定
（オプション設定項目）オンラインユーザハンドシェイク機能の設定
（オプション設定項目）認証トリガ機能の設定
（オプション設定項目） ポートでの強制認証ドメインの設定
（オプション設定項目） quietタイマの設定
（オプション設定項目）802.1X再認証の設定
（オプション設定項目） 802.1X制限VLANの設定

3.6 802.1X認証の有効化

802.1X 認証を有効にするとき、以下のガイドラインに従ってください。

- PVID が Voice VLAN である場合、802.1X 機能はポートに適用できません。
- 802.1X 認証が有効なポートでリンクアグリゲーションまたはループバックグループサービスを設定することができません。

以下に 802.1X 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． グローバルで 802.1X 認証を有効にする	**dot1x**	デフォルト：無効
3． interface view に移行する	**interface** *interface-type interface-number*	―
4． ポートで 802.1X 認証を有効にする	**dot1x**	デフォルト：無効

3.7 EAP relayまたはEAP terminationの有効化

EAP relay または EAP termination を設定するときに、以下の点を考慮してください。

- EAP パケットに関する RADIUS サーバのサポート
- 802.1X クライアントと RADIUS サーバでサポートされている認証方式

以下の状況では EAP relay と EAP termination の両方を設定することができます。

- クライアントが MD5-Challenge EAP 認証のみを使用します。
- クライアントが"ユーザ名+パスワード"の EAP 認証のみを使用します。

EAP-TLS、PEAP、またはその他の EAP 認証方式を使用するには、EAP relay を使用する必要があります。

EAP relay と EAP termination 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 “802.1X の概要”* を参照してください。

以下に EAP relay と EAP termination 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． EAP relay または EAP termination を設定する	**dot1x authentication-method** { **chap** | **eap** | **pap** }	デフォルトでは、ネットワークアクセス装置は、EAP terminationを実行し、RADIUSサーバとの通信にCHAPを使用します。 EAP terminationを有効にするためには、**chap**または**pap**パラメータを指定してください。 CHAP対応またはPAP対応のEAP relayを有効にするためには、**eap**パラメータを指定してください。

🕮 **メモ：**

EAP relay モードが使用されている場合、RADIUS scheme view で設定された **user-name-format** コマンドは適用されません。アクセス装置はクライアントからの認証データを何も変更せずにサーバに送信します。

3.8 ポート許可状態の設定

ポートの許可状態は、クライアントがネットワークへのアクセスを許可されているかどうかを決定します。**dot1x port-control** コマンドと以下のキーワードを使用して、ポートの認証状態を制御できます。

- **authorized-force**－ポートを authorized 状態にすると、認証なしでネットワークにアクセスするポート上のユーザを有効にします。
- **unauthorized-force**－ポートを unauthorized 状態にすると、ポート上のユーザからのアクセス要求を拒否します。
- **auto**－EAPOL パケットのみの通過を許可するために、最初にポートを unauthorized 状態にし、ユーザが認証を通過した後、ネットワークへのアクセスを許可するために、ポートを authorized 状態にします。ほとんどの場合で、このオプションを使用することができます。

以下にポート許可状態の設定を示します。

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． ポート認証状態を設定する	**dot1x port-control** { **authorized-force** | **auto** | **unauthorized-force** }	デフォルト：**auto**

3.9 アクセス制御方式の指定

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． アクセス制御方式を指定する	**dot1x port-method** { **macbased** | **portbased** }	デフォルト：**macbased**

3.10 ポートの802.1Xユーザの最大同時接続数の設定

この設定を行うことにより、ユーザ過多によりシステムリソース不足になることを防ぎます。

以下にポートでの 802.1X ユーザの最大同時接続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*	－
3． ポートでの 802.1X ユーザの最大同時接続数を設定する	**dot1x max-user** *user-number*	デフォルト：設定なし

3.11 認証リクエストの最大送信数の設定

アクセス装置は、指定した時間内にクライアントからの応答がない場合、認証リクエストの再送信を行います。この時間を設定する場合、**dot1x timer tx-period** *tx-period-value* コマンドまたは **dot1x timer supp-timeout** *supp-timeout-value* コマンドを使用します。

アクセス装置からリクエストの最大送信数まで再送信しても応答がない場合、リクエストの再送信を停止します。

以下に認証リクエストの最大送信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． クライアントへの認証リクエストの最大送信数を設定する	**dot1x retry** *max-retry-value*	デフォルト：2

3.12 802.1X認証タイムアウトタイマの設定

ネットワークデバイスは、以下の 802.1X 認証タイムアウトタイマを使用しています。

- **クライアントタイムアウトタイマ**－アクセス装置がクライアントに EAP-Request/MD5 Challenge パケットを送信するときに起動します。このタイマが時間切れになるまで応答がなかった場合、アクセス装置は、クライアントにリクエストを再送します。
- **サーバタイムアウトタイマ**－アクセス装置が認証サーバに RADIUS Access-Request パケットを送信するときに起動します。このタイマが時間切れになるまでに応答がなかった場合、アクセス装置は、サーバにリクエストを再送します。

ほとんどの場合、デフォルトの設定で十分です。ネットワークの状況に応じてタイマを設定することができます。

- パフォーマンスの低いネットワークで、クライアントタイムアウトタイマを高い値に設定します。
- 異なる性能の認証サーバがあるネットワークでサーバタイムアウトタイマを調整します。

以下に 802.1X 認証タイムアウト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． クライアント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：30秒
3． サーバ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

3.13 オンラインユーザハンドシェイク機能の設定

オンラインユーザハンドシェイク機能は、オンラインの 802.1X ユーザの接続状態をチェックします。ネットワークアクセス装置は、**dot1x timer handshake-period** コマンドで

指定された間隔でオンラインユーザにハンドシェイクメッセージを送信します。ハンドシェイクの最大試行回数後もオンラインユーザから応答を受信しない場合、ネットワークアクセス装置は、ユーザを offline 状態に設定します。ハンドシェイクの最大試行回数を設定する場合、**dot1x retry** コマンドを使用します。

また、本装置はデフォルトでオンラインユーザからの EAP-response に対する EAP-success を返しません。EAP-response に対する EAP-success を返すには、**dot1x handshake reply enable** コマンドを使用します。

3.13.1 設定ガイドライン

オンラインユーザハンドシェイク機能を設定するとき、以下の制限とガイドラインに従ってください。

- ネットワークに、ネットワークアクセス装置とのハンドシェイクパケットを交換できない 802.1X クライアントがある場合、オンラインユーザハンドシェイク機能を無効にしてください。これは 802.1X 接続が不適切に切断されることを防ぎます。

3.13.2 設定手順

以下にオンラインユーザハンドシェイ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. （オプション設定項目）ハンドシェイクタイマを設定する	**dot1x timer handshake-period** *handshake-period-value*	デフォルト：15秒
3. interface view に移行する	**interface** *interface-type interface-number*	―
4. オンラインユーザハンドシェイク機能を有効にする	**dot1x handshake**	デフォルト：有効
5. ハンドシェイクリプライ機能を有効にする	**dot1x handshake reply enable**	デフォルト：無効

3.14 認証トリガ機能の設定

認証トリガ機能は、802.1X クライアントが認証を開始できない場合、802.1X 認証を開始するためにネットワークアクセス装置を有効にします。

この機能はマルチキャストトリガとユニキャストトリガをサポートします。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 “802.1X の概要”* を参照してください。

3.14.1 設定ガイドライン

認証トリガ機能を設定するときは、以下のガイドラインに従ってください。

- ポートに接続されたクライアントが、802.1X 認証を開始するために EAPOL-Start パケットを送信できない場合、ポート上でマルチキャストトリガを有効にします。
- 無線 LAN でマルチキャストトリガを無効にします。無線クライアントとアクセス装置のワイヤレスモジュールは、それぞれ 802.1X 認証を開始できます。
- 802.1X クライアントがほとんどいないポートに接続され、これらのクライアントが認証を開始できない場合は、ポート上でユニキャストトリガを有効にします。
- 重複した認証パケットを避けるために、ポート上で両方のトリガを有効にしないでください。

3.14.2 設定手順

以下にポートでの認証トリガ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. （オプション設定項目）ユーザ名リクエスト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：30秒
3. interface view に移行する	**interface** *interface-type interface-number*	―
4. 認証トリガ機能を有効にする	**dot1x** { **multicast-trigger** | **unicast-trigger** }	デフォルト： • マルチキャストトリガ有効 • ユニキャストトリガ無効

3.15 ポートでの強制認証ドメインの設定

ポート上で認証、許可、アカウンティングのための強制認証ドメイン内にすべての 802.1X ユーザを配置することができます。ユーザは、他のドメイン内のアカウントを使用して、ポートを介してネットワークにアクセスすることはできません。強制認証ドメインの実装で、802.1X アクセス制御の導入時の柔軟性を高めます。

以下にポートでの強制認証ドメ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. interface view に移行する	**interface** *interface-type interface-number*	―
3. ポートで 802.1X 強制認証ドメインを指定する	**dot1x mandatory-domain** *domain-name*	デフォルト：設定なし

3.16 quietタイマの設定

quiet タイマを有効にすると、アクセス装置は、802.1X 認証に失敗したクライアントからの認証リクエストを処理する前に一定時間待ちます。

ネットワークの状況に応じて quiet タイマを設定することができます。

- 脆弱なネットワークでは高い値を設定してください。
- 認証応答を速くするためには低い値を設定してください。

以下に quiet 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. quiet タイマを有効にする	**dot1x quiet-period**	デフォルト：無効
3. （オプション設定項目）quiet タイマを設定する	**dot1x timer quiet-period** *quiet-period-value*	デフォルト：60秒

3.17 802.1X再認証の設定

3.17.1 概要

802.1X 再認証は、オンラインユーザの接続状態をトラッキングし、サーバによって割り当てられた属性を更新します。属性は ACL、VLAN が含まれます。

802.1X 再認証では、再認証の間隔はユーザが設定できます。

デフォルトでは、802.1X 再認証のサーバが到達不能である場合、装置はユーザをログオフします。オンライン保持機能は、サーバが到達不能な場合、802.1X ユーザの再認証を継続します。

3.17.2 設定ガイドライン

802.1X 再認証を設定するときは、以下のガイドラインに従ってください。

サーバで割り当てられたセッションタイムアウトタイマ（セッションタイムアウト属性）と終了行動（終了行動属性）は定期的な再認証に影響することがあります。サーバで割り当てられたセッションタイムアウトと終了行動の属性を表示するには、**display dot1x connection** コマンドを使用してください。

- 終了行動が **Default**（ログオフ）の場合、session timeout タイマよりも定期的な再認証タイマが短い際に効果があります。
- 終了行動が **Radius-request** の場合、定期的な再認証は効果がありません。session timeout タイマが終了後にオンライン 802.1X ユーザを再認証します。

session timeout と termination action 属性の割り当てサポートは、サーバモデルによります。

- **dot1x timer reauth-period** コマンドを使用して、定期的な再認証タイマをシステム view とインタフェース view のどちらでも設定できます。

  デバイスは、以下の順に定期的な再認証タイマを選択します。

a) サーバ割り当てされた再認証タイマ

b) ポート指定の再認証タイマ

c)　グローバル再認証タイマ

デフォルト再認証タイマ

- 認証前後でオンラインユーザに割り当てられた VLAN は、同一でも異なっても可能です。

3.17.3 802.1X 定期的な再認証の設定

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）定期的な認証タイマを設定する	**dot1x timer reauth-period** *reauth-period-value*	デフォルト：3600秒
3． interface view に移行する	**interface** *interface-type interface-number*	―
4． 定期的なオンラインユーザの再認証を設定する	**dot1x re-authenticate**	デフォルト：無効
5． （オプション設定項目）ポートに定期的な認証タイマを設定する	**dot1x timer reauth-period** *reauth-period-value*	デフォルト：無効 グローバルの定期的な802.1X再認証タイマを使用します。

3.18 802.1X制限VLANの設定

3.18.1 設定ガイドライン

802.1X 制限 VLAN を設定する前に、以下の制限とガイドラインに従ってください。

- ポートで Voice VLAN、ポート VLAN、802.1X 制限 VLAN に異なる ID を割り当ててください。ポートで、VLAN にタグづけられた入力トラフィックの処理を正しく処理できるように割り当ててください。
- ポートに 1 つのみ 802.1X 制限 VLAN を設定することができます。異なるポートで異なる 802.1X 制限 VLAN を設定することができます。
- ポートで複数のセキュリティ機能を設定するとき、表 3-3に示すガイドラインに従ってください。

表 3-3 802.1X 制限 VLAN と他のセキュリティ機能の関係

機能	関係	補足
MACベースのアクセス制御を行うポート上のMACアドレス認証ゲストVLAN	802.1X制限VLANは優先順位が高くなります。	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“MACアドレス認証”*を参照してください。
MACベースのアクセス制御を行うポート上のポート侵入防御	802.1X制限VLAN機能は、MAC動作のブロックよりも優先順位が高くなります。ポート侵入保護機能のポートシャットダウン動作よりも優先順位が低いです。	ポートセキュリティ機能はサポートしていません。

3.18.2 設定要件

802.1X 制限 VLAN を設定する前に、以下の作業を完了してください。

- 802.1X 制限 VLAN として指定される VLAN を作成してください。
- 802.1X 対応ポートが MAC ベースのアクセス制御を行う場合、以下の作業を完了してください。
  - ハイブリッドポートとして設定してください。
  - ポートで MAC ベース VLAN を有効にしてください。MAC ベース VLAN の詳細はオペレーションマニュアルのセクション 4 *アクセス “VLAN”* を参照してください。
  - ポートをタグなしメンバとして 802.1X 制限 VLAN に割り当ててください。

3.18.3 設定手順

以下に 802.1X 制限 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. interface view に移行する	**interface** *interface-type interface-number*	―
3. ポートで 802.1X 制限 VLAN を設定する	**dot1x auth-fail vlan** *authfail-vlan-id*	デフォルト：設定なし

3.19 802.1X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
特定、またはすべてのポートの802.1X認証情報、統計情報、設定情報を表示する	**display dot1x** [**sessions** | **statistics**] [**ap** *ap-name* [**radio** *radio-id*] | **interface** *interface-type interface-number*]
オンライン802.1Xユーザ情報を表示する	**display dot1x connection** [**ap** *ap-name* [**radio** *radio-id*] | **interface** *interface-type interface-number* | **user-mac mac-addr** | **user-name** *name-string*]
802.1X統計情報を削除する	**reset dot1x statistics** [**ap** *ap-name* [**radio** *radio-id*] | **interface** *interface-type interface-number*]

3.20 802.1X認証の設定例

3.20.1 基本的な 802.1X 認証の設定例

I. ネットワーク要件

図 2-2 に示すように、アクセス装置は、GigabitEthernet 1/0/1 に接続するユーザ用に 802.1X 認証を実行します。ポート上で MAC ベースのアクセス制御を行ってください。1 ユーザのログオフは、他のオンラインの 802.1X ユーザには影響しません。

802.1X ユーザの認証、許可、アカウンティングを実行するために RADIUS サーバを使用してください。 RADIUS 認証が失敗した場合、アクセス装置上でローカル認証を実行します。

プライマリ認証およびアカウンティングサーバとして 10.1.1.1/24 のホスト、セカンダリ認証とアカウンティングサーバとして 10.1.1.2/24 のホストを設定します。すべてユーザを収容できる ISP ドメイン bbb にすべてのユーザを割り当てます。

アクセス装置と認証サーバ間のパケットに name という名称で共有鍵を、アクセス装置とアカウンティングサーバ間のパケットに money という名称で共有鍵を設定します。

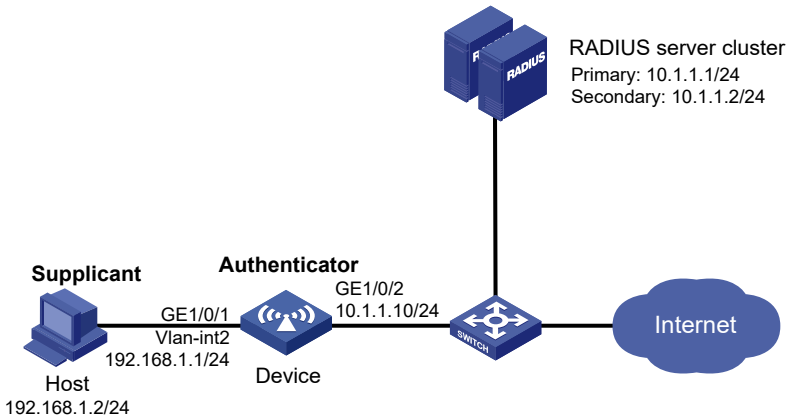


図 3-1 ネットワーク図

II. 設定手順

1) 802.1X クライアントを設定します。（詳細は省略）
2) RADIUS サーバを設定し、802.1X ユーザ用のユーザアカウントを追加します。（詳細は省略します。）

AC で使用される RADIUS コマンドについての詳細は、コマンドマニュアルのセクション 9 *セキュリティ　"AAA"* を参照してください。

3) アクセス装置上の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。）
4) アクセス装置上で 802.1X ユーザ用のユーザアカウントを設定します。

ユーザ名とパスワードがそれぞれ localuser と localpass のローカルユーザをプレーンテキストで追加します。（ユーザ名とパスワードは RADIUS サーバに設定されたものと同じにしてください。）

```
<Device> system-view
[Device] local-user localuser class network
[Device-luser-network-localuser] password simple localpass
```

サービスタイプに lan-access を選択します。

```
[Device-luser-network-localuser] service-type lan-access
[Device-luser-network-localuser] 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。

```
[Device] radius scheme radius1
```

プライマリ認証/アカウンティング RADIUS サーバの IP アドレスを指定します。

```
[Device-radius-radius1] primary authentication 10.1.1.1
[Device-radius-radius1] primary accounting 10.1.1.1
```

セカンダリ認証/アカウンティング RADIUS サーバの IP アドレスを指定します。

```
[Device-radius-radius1] secondary authentication 10.1.1.2
[Device-radius-radius1] secondary accounting 10.1.1.2
```

AC と認証サーバ間の共有鍵を指定します。

```
[Device-radius-radius1] key authentication simple name
```

AC とアカウンティングサーバ間の共有鍵を指定します。

```
[Device-radius-radius1] key accounting simple money
```

RADIUS サーバに送信されるユーザ名から ISP のドメイン名を除外します。

```
[Device-radius-radius1] user-name-format without-domain
[Device-radius-radius1] quit
```

メモ：

アクセス装置は、RADIUS サーバと同じユーザ名のフォーマットを使用する必要があります。RADIUS サーバがユーザ名に ISP のドメイン名を含む場合、アクセス装置です。

---

6) ISP ドメインを設定します。

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

```
[Device] domain bbb
```

RADIUS スキーム radius1 を ISP ドメインに適用し、セカンダリ認証方式としてローカル認証を指定します。

```
[Device-isp-bbb] authentication lan-access radius-scheme radius1 local
[Device-isp-bbb] authorization lan-access radius-scheme radius1 local
```

```
[Device-isp-bbb] accounting lan-access radius-scheme radius1 local
[Device-isp-bbb] quit
```

7) 802.1X を設定します。

GigabitEthernet 1/0/1 で 802.1X を有効にします。

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] dot1x
```

802.1X をグローバルで有効にします。

```
[Device] dot1x
```

III. 設定の確認

GigabitEthernet 1/0/1 の 802.1X 認証の設定を確認します。

```
[Device] display dot1x interface gigabitethernet 1/0/1
```

802.1X ユーザが RADIUS 認証を通過した後、ユーザ接続情報を表示します。

```
[Device] display dot1x connection
```

目次

このセクションのページは **9-x-x** です。

4 章 MAC アドレス認証 4-1
4.1 概要 4-1
4.1.1 ユーザアカウントポリシー 4-1
4.1.2 認証方式 4-1
4.1.3 VLAN の割り当て 4-2
4.1.4 ACL の割り当て 4-3
4.2 設定要件 4-4
4.3 設定作業リスト 4-4
4.4 MAC アドレス認証ドメインの指定 4-4
4.5 MAC アドレス認証の認証方式の設定 4-5
4.6 ユーザアカウントフォーマットの設定 4-5
4.7 MAC アドレス認証タイマの設定 4-6
4.8 ポート上の MAC アドレス認証ユーザの同時接続最大数の設定 4-6
4.9 MAC アドレス認証の表示と維持 4-7
4.10 MAC アドレス認証の設定例 4-7
4.10.1 ローカル MAC アドレス認証の設定例 4-7
4.10.2 RADIUS ベースの MAC アドレス認証の設定例 4-9
4.10.3 ACL の割り当ての設定例 4-11

4章 MAC アドレス認証

4.1 概要

MAC アドレス認証はポート上で送信元 MAC アドレスを認証することによって、ネットワークアクセスを制御します。

クライアントソフトウェアを必要とせず、ネットワークアクセス用のユーザ名とパスワードを入力する必要はありません。MAC アドレス認証が有効になっているポート上で未知の送信元 MAC アドレスが検出された場合、装置は MAC アドレス認証プロセスを開始します。

- 認証が成功した場合、ユーザは、許可されたネットワークリソースにアクセスすることができます。
- 認証が失敗した場合、装置はユーザの MAC アドレスをサイレント MAC アドレスとして登録し、パケットをドロップし、Quiet タイマを開始します。Quiet タイマは、サイレント MAC に登録された MAC アドレスからのすべての後続のパケットを破棄することで、短時間に何度も認証が行われることを回避します。

🕮 **メモ：**

認証に失敗した MAC アドレスがスタティック MAC アドレスまたは任意のセキュリティ認証をパスした MAC アドレスである場合、装置はその MAC アドレスをサイレントアドレスとして記憶しません。

4.1.1 ユーザアカウントポリシー

MAC アドレス認証は、以下のユーザアカウントポリシーをサポートしています。

- **各ユーザのための MAC ベースのユーザアカウント**－アクセス装置は、MAC アドレス認証するユーザのユーザ名とパスワードとして、パケットの送信元 MAC アドレスを使用します。このポリシーは、非セキュアな環境に適しています。
- **すべてのユーザのための共有のユーザアカウント**－アクセス装置上のすべての MAC アドレス認証ユーザのために、必ずしも MAC アドレスでないユーザ名とパスワードを指定します。このポリシーは、セキュアな環境に適しています。

4.1.2 認証方式

アクセス装置上（ローカル認証）または、RADIUS （Remote Authentication Dial-In User Service） サーバを介して、MAC アドレス認証を行うことができます。

ローカル認証：

- **MAC ベースアカウント**－アクセス装置は、一致するローカルアカウントデータベースを検索するためのユーザ名とパスワードとして、パケットの送信元 MAC アドレスを使用します。

- **共有アカウント**－アクセス装置は、一致するローカルアカウントデータベースを検索するために、共有アカウントのユーザ名とパスワードを使用します。

RADIUS 認証：

- **MAC ベースアカウント**－アクセス装置は、認証用の RADIUS サーバにユーザ名とパスワードとして送信元 MAC アドレスを送信します。
- **共有アカウント**－アクセス装置は、認証用の RADIUS サーバに共有アカウントのユーザ名とパスワードを送信します。

ローカル認証と RADIUS 認証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。

4.1.3 VLAN の割り当て

MAC アドレス認証は許可 VLAN、ゲスト VLAN をサポートします。

I. 許可 VLAN

MAC アドレス認証ユーザの許可されたネットワークリソースへのアクセスを制御するため、許可 VLAN を使用します。

- RADIUS サーバにおいて、許可 VLAN は VLAN ID もしくは VLAN 名のフォームで指定することができます。
- ローカルアクセス装置において、許可 VLAN は VLAN ID のフォームで指定しなければなりません。許可 VLAN は、Local user view と User group view で指定できます。

  詳細は、オペレーションマニュアルのセクション 9 *セキュリティ "AAA"* を参照してください。

表 4-1 にネットワークアクセス装置が MAC アドレス認証ユーザの許可 VLAN 処理方法を示します。

表 4-1 VLAN 操作

ポートタイプ	VLAN 操作
• アクセスポート • トランクポート • ハイブリッドポート	• ポートがタグなしメンバとして許可VLANに割り当てられている場合、装置はポートを最初の認証ユーザの許可VLANに割り当てます。許可VLANはPVIDになります。ポート上のすべてのMAC認証ユーザは、同一の認証VLANを割り当てられている必要があります。異なる許可VLANが後続のユーザに割り当てられている場合、ユーザはMAC認証を通過できません。 • ポートがタグありメンバとして許可VLANに割り当てられている場合、ポートのPVIDは変更されません。装置は各ユーザのMACアドレスを、それぞれの許可VLANにマッピングします。 アクセスポートは、タグなしVLANメンバとしてのみ許可VLANに割り当て可能です。

⚠ **重要**：

ハイブリッドポートは、常にタグなしメンバとして VLAN を割り当てることを推奨します。割り当て後は、VLAN でタグメンバとしてポートを再設定しないでください。

II. ゲスト VLAN

ポート上の MAC アドレス認証ゲスト VLAN は、MAC アドレス認証に失敗したユーザをオーガニゼーションセキュリティストラテジに準じて適応させます。例えば、VLAN は間違ったパスワードを入力した VLAN を適応します。MAC アドレス認証ゲスト VLAN 内のユーザは、ソフトウェアサーバ、ダウンロードソフトウェア、システムパッチといった限られたネットワーク資源にアクセスすることができます。MAC アドレス認証ゲスト VLAN が設定されていない場合、MAC アドレス認証に失敗した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ません。

ハイブリッドポートは、常に、タグなしメンバとして MAC アドレス認証ゲスト VLAN に割り当てられます。割り当て後、VLAN のタグづけメンバとしてポートを再設定しないでください。

表 4-2 にネットワークアクセス装置が MAC アドレス認証ユーザのゲスト VLAN を処理する方法を示します。

表 4-2 VLAN 操作

ポートタイプ	VLAN 操作
サーバに到達不能以外の理由でMACアドレス認証に失敗したMACアドレス認証ゲストVLANのユーザ	ユーザはMACアドレス認証ゲストVLANに属します。
MACアドレス認証にパスしたMACアドレス認証ゲストVLANのユーザ	装置はユーザのMACアドレスを認証ユーザによって割り当てられた許可VLANに再マッピングします。 ユーザ用の許可VLANが認証サーバで設定されていない場合、ユーザのMACアドレスをポートのPVIDに再マッピングします。

4.1.4 ACL の割り当て

ネットワークリソースへのアクセスを制御するため、MAC アドレス認証ユーザに ACL を指定することができます。ユーザが MAC アドレス認証にパスしたのち、認証サーバ（ローカルあるいはリモート）はユーザのアクセスポートに許可された ACL を割り当てます。ACL はユーザのトラフィックをフィルタします。ACL の割り当て機能のために、アクセス装置で許可 ACL の ACL を設定する必要があります。

ユーザのアクセス制御を変更するために、以下の方法の 1 つを使用することができます。

- アクセス装置の ACL ルールを修正します。
- 認証サーバで別の許可 ACL を指定します。

ACL の詳細は、オペレーションマニュアルのセクション 8 *ACL and QoS “ACL”* を参照してください。

4.2 設定要件

MAC アドレス認証を設定する前に、以下の作業を完了してください。

1) 認証ドメイン（ISP ドメイン）を設定し、AAA 方式を指定してください。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。
   - □ 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みます。）を作成し、lan-access サービスを指定してください。
   - □ RADIUS 認証の場合、装置と RADIUS サーバ間のルートで通信が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てください。MAC ベースアカウントを使用する場合、それぞれのアカウントのユーザ名とパスワードは MAC アドレス認証ユーザの MAC アドレスと同じにしてください。
2) ポートセキュリティが無効であることを確認してください。

🕮 **メモ：**

ポートセキュリティ機能はサポートしていません。

4.3 設定作業リスト

作業リスト
（オプション設定項目）MACアドレス認証ドメインの指定
（オプション設定項目）MACアドレス認証の認証方式の設定
（オプション設定項目）ユーザアカウントフォーマットの設定
（オプション設定項目）MACアドレス認証タイマの設定

4.4 MACアドレス認証ドメインの指定

デフォルトでは、MAC アドレス認証ユーザはシステムデフォルト認証ドメイン内にあります。ユーザごとに異なるアクセスポリシーを適用するには、次の方法で MAC アドレス認証ユーザ用の認証ドメインを指定することができます。

- system view でグローバルの認証ドメインを指定します。このドメインの設定は、MAC アドレス認証が有効なすべてのサービステンプレートに適用されます。
- service template view で個別のサービステンプレートに認証ドメインを指定します。

MAC アドレス認証は、サービステンプレート固有のドメイン、グローバルドメイン、デフォルトドメインの順序でポート上のユーザの認証ドメインを選択します。認証ドメインの詳細はオペレーションマニュアルのセクション 9 *セキュリティ　"AAA"* を参照してください。

以下に MAC アドレス認証ユーザの認証ドメ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**	—

操作	コマンド	補足
2． MAC アドレス認証ユーザの認証ドメインを指定する	● system viewで設定する：**mac-authentication domain** *domain-name* ● service template viewで設定する： 1． **wlan service-template** *service-template-name* 2． **mac-authentication domain** *domain-name*	デフォルト：システムのデフォルト認証ドメインが使われます。

4.5 MACアドレス認証の認証方式の設定

RADIUS ベースの MAC 認証では、次の認証方式がサポートされています。

PAP:ユーザ名とパスワードをプレーンテキストで転送します。認証方法は、高度なセキュリティを必要としないシナリオに適用されます。

CHAP:ユーザ名をプレーンテキストで、パスワードを暗号化してネットワーク経由で転送します。CHAP は PAP よりも安全です。

RADIUS サーバと同じ認証方式を使用する必要があります。

以下に MAC アドレス認証の認証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． MAC アドレス認証の認証方式を指定する	**mac-authentication authentication-method { chap | pap }**	デフォルト：MACアドレス認証にPAPを使用します

4.6 ユーザアカウントフォーマットの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． MAC アドレス認証ユーザアカウントフォーマットを設定する	● 各ユーザにMACベースユーザアカウントを使用する：**mac-authentication user-name-format mac-address** [{ **with-hyphen** | **without-hyphen** } [**lowercase** | **uppercase**]] ● すべてのユーザに共有ユーザアカウントを使用する：**mac-authentication user-name-format fixed** [**account** *name*] [**password** { **cipher** | **simple** } *string*]	デフォルト：MACアドレス認証のユーザ名とパスワードとしてユーザのMACアドレスを使用します。 MACアドレスは16進数でハイフンなし、小文字のみです。

4.7 MACアドレス認証タイマの設定

MAC アドレス認証では以下のタイマを使用します。

- **Offline detect timer**－ユーザがアイドル状態であることを検出するために、装置がユーザからのトラフィックを待つ期間を設定します。装置はタイマが終了するとユーザをログオフし、ユーザのアカウントの停止を要求します。このタイマは、MAC 認証オフライン検出機能が有効な場合にのみ効果があります。

  オフライン検出タイマを設定した後、mac-address timer コマンドを用いて MAC アドレスエージングタイマに同じ値を設定します。この操作をすることで、オフライン検出タイマ内でオフラインとなった MAC 認証ユーザが MAC アドレスのエントリが終了することを避けられます。
- **Quiet timer**－MAC アドレス認証に失敗したユーザが MAC アドレス認証を実行できるようになるまで、装置が待つ時間をタイマに設定します。 Quiet タイムの間は、MAC アドレスからのパケットはすべて廃棄されます。この Quiet メカニズムは、認証が繰り返されシステムのパフォーマンスに影響を与えることを防ぎます。
- **Server timeout timer**－RADIUS サーバが使用不能であることを検出するために、アクセス装置が RADIUS サーバからの応答を待つ時間をタイマに設定します。MAC アドレス認証中にタイムアウトした場合、ユーザはネットワークにアクセスすることはできません。

以下に MAC アドレス認証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． MAC アドレス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： offline detect timer：300秒 quiet timer：60秒 server timeout timer：100秒

4.8 ポート上のMACアドレス認証ユーザの同時接続最大数の設定

同時に接続する認証ユーザを制限することで、システムリソース不足になることを防ぎます。

以下にポート上の MAC アドレス認証ユーザの同時接続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． Ethernet interface view に移行する	**interface** *interface-type interface-number*	
3． ポート上の MAC アドレス認証ユーザの同時接続最大数を設定する	**mac-authentication max-user** *user-number*	デフォルト：設定なし

4.9 MACアドレス認証の表示と維持

display コマンドはすべての view で、**reset** コマンドは user view で使用できます。

操作	コマンド
MACアドレス認証情報を表示する	**display mac-authentication** [**ap** *ap-name* [**radio** *radio-id*]]
MACアドレス認証接続を表示する	**display mac-authentication connection** [**ap** *ap-name* [**radio** *radio-id*] | **user-mac** *mac-addr* | **user-name** *user-name*]
MACアドレス認証の統計情報を削除する	**reset mac-authentication statistics** [**ap** *ap-name* [**radio** *radio-id*]]

4.10 MACアドレス認証の設定例

4.10.1 ローカル MAC アドレス認証の設定例

I. ネットワーク要件

図 4-1 に示すように、ユーザのインターネットアクセスを制御するためにポート GigabitEthernet 1/0/1 でローカル MAC アドレス認証を設定します。

以下の要件に従うように装置を設定します。

- ユーザが 180 秒ごとにオフラインになっているかどうかを検出します。
- ユーザが認証に失敗した場合、180 秒間、ユーザを拒否します。
- すべてのユーザは ISP ドメイン bbb に属します。
- ローカルユーザは、MAC アドレス認証のユーザ名とパスワードとして、ユーザ自身の MAC アドレスを使用します。MAC アドレスは 16 進数でハイフン付き、小文字を使用します。



図 4-1 ネットワーク図

II. 設定手順

ローカルユーザを追加します。この例ではホストの MAC アドレス 11-11-11-11-11-11 をユーザ名とパスワードに設定し、LAN アクセスサービスを有効にします。

```
<Device> system-view
[Device] local-user 11-11-11-11-11-11 class network
```

```
[Device-luser-network-11-11-11-11-11-11] password simple 11-11-11-11-11-11
```

ユーザの LAN アクセスサービスを指定します。

```
[Device-luser-network-11-11-11-11-11-11] service-type lan-access
[Device-luser-network-11-11-11-11-11-11] quit
```

LAN ユーザのローカル認証を実行するため、ISP ドメイン bbb を設定します。

```
[Device] domain bbb
[Device-isp-bbb] authentication lan-access local
[Device-isp-bbb] quit
```

GigabitEthernet 1/0/1 で MAC アドレス認証を有効にします。

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] mac-authentication
[Device-GigabitEthernet1/0/1] quit
```

ISP ドメイン bbb として MAC アドレス認証ドメインを指定します。

```
[Device] mac-authentication domain bbb
```

MAC アドレス認証タイマを設定します。

```
[Device] mac-authentication timer offline-detect 180
[Device] mac-authentication timer quiet 180
```

MAC ベースのアカウントを使うよう MAC アドレス認証を設定します。MAC アドレスのユーザ名とパスワードはハイフンありで、小文字です。

```
[Device] mac-authentication user-name-format mac-address with-hyphen lowercase
```

MAC アドレス認証をグローバルで有効にします。

```
[Device] mac-authentication
```

III. 設定の確認

MAC アドレス認証の設定と統計情報を表示します。

```
[Device] display mac-authentication
Global MAC authentication parameters:
   MAC authentication     : Enabled
   User name format       : MAC address in lowercase(xx-xx-xx-xx-xx-xx)
            Username      : mac
            Password      : Not configured
   Offline detect period  : 180 s
   Quiet period           : 180 s
   Server timeout         : 100 s
   Authentication domain  : bbb
 Online MAC-auth wired users    : 1

 Silent MAC users:
          MAC address       VLAN ID  From port               Port index
          2222-2222-2222    8        GigabitEthernet1/0/1    1
 GigabitEthernet1/0/1 is link-up
```

```
   MAC authentication          : Enabled
   Carry User-IP               : Disabled
   Authentication domain       : Not configured
   Auth-delay timer            : Disabled
   Re-auth server-unreachable  : Logoff
   Host mode                   : Single VLAN
   Max online users            : 4294967295
   Authentication attempts     : successful 1, failed 0
   Current online users        : 1
          MAC address       Auth state
          1111-1111-1111    Authenticated
```

出力では、Host A が MAC アドレス認証にパスし、オンラインになっています。Host B は MAC アドレス認証に失敗し、サイレント MAC アドレスとして MAC アドレスが記録されます。

4.10.2 RADIUS ベースの MAC アドレス認証の設定例

I. ネットワーク要件

図 4-2 に示すように、装置はユーザの認証、許可、アカウンティングを実行するため、RADIUS サーバを使用します。

MAC アドレス認証によってインタネットにアクセスするユーザを制御するため、以下の作業を実行します。

- グローバルと GigabitEthernet 1/0/1 で MAC アドレス認証を有効にします。
- ユーザが 180 秒ごとにオフラインになっているかどうかを検出します。
- ユーザが認証に失敗した場合、装置は 180 秒間ユーザを拒否します。
- すべてのユーザは ISP ドメイン bbb に属します。
- すべてのユーザは、ユーザ名 aaa、パスワード 123456 の共有ユーザアカウントを使用します。

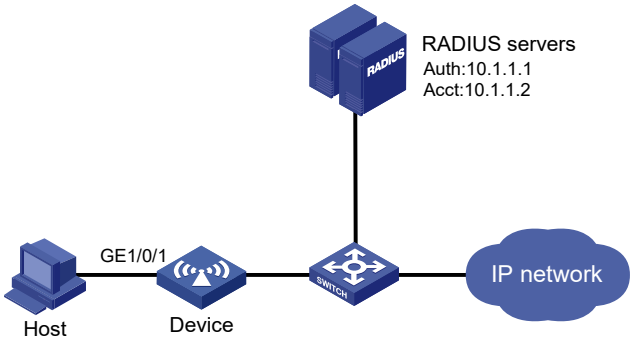


図 4-2 ネットワーク図

II. 設定手順

1) RADIUS サーバとアクセス装置で互いに通信できることを確認してください。（詳細は省略します。）
2) RADIUS サーバを設定します。

MAC アドレス認証ユーザの共有アカウントを作成します。（詳細は省略します。）

アカウントにユーザ名 aaa、パスワード 123456 を設定します。（詳細は省略します。）

3)　装置上で RADIUS ベースの MAC アドレス認証を設定します。

RADIUS スキームを設定します。

```
<Device> system-view
[Device] radius scheme 2000
[Device-radius-2000] primary authentication 10.1.1.1 1812
[Device-radius-2000] primary accounting 10.1.1.2 1813
[Device-radius-2000] key authentication simple abc
[Device-radius-2000] key accounting simple abc
[Device-radius-2000] user-name-format without-domain
[Device-radius-2000] quit
```

認証、許可、アカウンティング用の ISP ドメイン bbb の RADIUS スキームを適用します。

```
[Device] domain bbb
[Device-isp-bbb] authentication default radius-scheme 2000
[Device-isp-bbb] authorization default radius-scheme 2000
[Device-isp-bbb] accounting default radius-scheme 2000
[Device-isp-bbb] quit
```

GigabitEthernet 1/0/1 で MAC アドレス認証を有効にします。

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] mac-authentication
[Device-GigabitEthernet1/0/1] quit
```

ISP ドメイン bbb として MAC アドレス認証ドメインを指定します。

```
[Device] mac-authentication domain bbb
```

MAC アドレス認証タイマを設定します。

```
[Device] mac-authentication timer offline-detect 180
[Device] mac-authentication timer quiet 180
```

MAC アドレス認証のユーザによって共有されるアカウントのユーザ名 aaa とパスワード 123456 を指定します。

```
[Device] mac-authentication user-name-format fixed account aaa password simple 123456
```

MAC アドレス認証をグローバルで有効にします。

```
[Device] mac-authentication
```

III. 設定の確認

MAC アドレス認証の設定を表示します。

```
[Device] display mac-authentication
Global MAC authentication parameters:
   MAC authentication      : Enabled
   User name format        : Fixed account
           Username        : aaa
           Password        : ******
   Offline detect period   : 180 s
   Quiet period            : 180 s
   Server timeout          : 100 s
   Authentication domain   : bbb
 Online MAC-auth wired users    : 1

 Silent MAC users:
          MAC address       VLAN ID  From port                Port index

 GigabitEthernet1/0/1  is link-up
   MAC authentication          : Enabled
   Carry User-IP               : Disabled
   Authentication domain       : Not configured
   Auth-delay timer            : Disabled
   Re-auth server-unreachable  : Logoff
   Host mode                   : Single VLAN
   Max online users            : 4294967295
   Authentication attempts     : successful 1, failed 0
   Current online users        : 1
          MAC address       Auth state
          1111-1111-1111    Authenticated
```

4.10.3 ACL の割り当ての設定例

I. ネットワーク要件

図 4-3 に示すように、以下の要件に従うように装置を設定します。

- ユーザの認証、許可、アカウンティングを実行する RADIUS サーバを使用します。
- インターネットアクセスを制御するため、GigabitEthernet 1/0/1 で MAC アドレス認証を実行します。
- MAC アドレス認証ユーザの MAC ベースユーザアカウントを使用します。各 MAC アドレスは 16 進数でハイフンあり、小文字を使用します。
- FTP サーバ 10.0.0.1 にアクセスする認証ユーザを拒否するように ACL を設定します。

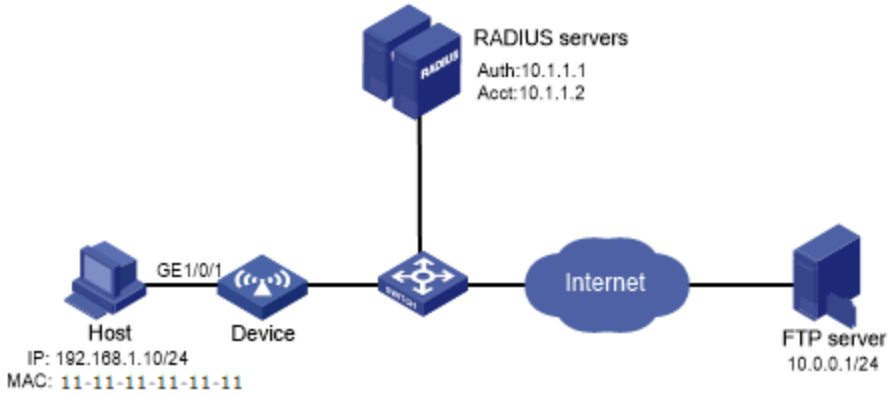


図 4-3 ネットワーク図

II. 設定手順

RADIUS サーバとアクセス装置が互いに通信できることを確認してください。

1)　10.0.0.1 へのパケットを拒否するように ACL 3000 を設定します。

```
<Device> system-view
[Device] acl advanced 3000
[Device-acl-ipv4-adv-3000] rule 0 deny ip destination 10.0.0.1 0
[Device-acl-ipv4-adv-3000] quit
```

2)　装置で RADIUS ベース MAC アドレス認証を設定します。

RADIUS スキームを設定します。

```
[Device] radius scheme 2000
[Device-radius-2000] primary authentication 10.1.1.1 1812
[Device-radius-2000] primary accounting 10.1.1.2 1813
[Device-radius-2000] key authentication simple abc
[Device-radius-2000] key accounting simple abc
[Device-radius-2000] user-name-format without-domain
```

認証、許可、アカウンティングの RADIUS スキームを ISP ドメインに適用します。

```
[Device] domain bbb
[Device-isp-bbb] authentication default radius-scheme 2000
[Device-isp-bbb] authorization default radius-scheme 2000
[Device-isp-bbb] accounting default radius-scheme 2000
[Device-isp-bbb] quit
```

MAC アドレス認証の ISP ドメインを指定します。

```
[Device] mac-authentication domain bbb
```

MAC ベースユーザアカウントを使用するために装置を設定します。各 MAC アドレスは 16 進数でハイフンあり、小文字を使用します。

```
[Device] mac-authentication user-name-format mac-address with-hyphen lowercase
```

GigabitEthernet 1/0/1 で MAC アドレス認証を有効にします。

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] mac-authentication
[Device-GigabitEthernet1/0/1] quit
```

MAC アドレス認証をグローバルで有効にします。

```
[Device] mac-authentication
```

3)　RADIUS サーバを設定します。

各 RADIUS サーバでユーザ名とパスワードが 11-11-11-11-11-11 のユーザアカウントを追加します。（詳細は省略します。）

ユーザアカウントに ACL 3000 を許可します。（詳細は省略します。）

III. 設定の確認

MAC アドレス認証の設定を確認します。

```
[Device] display mac-authentication
Global MAC authentication parameters:
   MAC authentication     : Enabled
   User name format       : MAC address in lowercase(xx-xx-xx-xx-xx-xx)
            Username      : mac
            Password      : Not configured
   Offline detect period  : 300 s
   Quiet period           : 60 s
   Server timeout         : 100 s
   Authentication domain  : bbb
 Online MAC-auth wired users    : 1

 Silent MAC users:
          MAC address       VLAN ID  From port               Port index

 GigabitEthernet1/0/1  is link-up
   MAC authentication         : Enabled
   Carry User-IP              : Disabled
   Authentication domain      : Not configured
   Auth-delay timer           : Disabled
   Re-auth server-unreachable : Logoff
   Host mode                  : Single VLAN
   Max online users           : 4294967295
   Authentication attempts    : successful 1, failed 0
   Current online users       : 1
          MAC address       Auth state
          1111-1111-1111    Authenticated
```

ホストから FTP サーバへの ping ができないことを確認します。

```
C:\>ping 10.0.0.1

Pinging 10.0.0.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.0.0.1:
   Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

出力は、FTP サーバにアクセスを拒否するため、ACL 3000 が GigabitEthernet 1/0/1 に割り当てられていることを示します。

目次

このセクションのページは **9-x-x** です。

5 章 パスワード管理 5-1
5.1 概要 5-1
5.1.1 パスワードの設定 5-1
5.1.2 パスワードのアップデートと有効期限の終了 5-3
5.1.3 ユーザログイン管理 5-4
5.1.4 すべての形式でのパスワードの非表示 5-5
5.1.5 ロギング 5-5
5.2 制限とガイドライン 5-5
5.3 パスワード管理設定作業リスト 5-6
5.4 パスワード管理の有効化 5-6
5.5 グローバルパスワード管理パラメータの設定 5-7
5.6 ユーザグループパスワード管理パラメータの設定 5-8
5.7 ローカルユーザパスワード管理パラメータの設定 5-8
5.8 super パスワード管理パラメータの設定 5-9
5.9 パスワード管理の表示と維持 5-10
5.10 パスワード管理の設定例 5-10
5.10.1 パスワード管理の設定例 5-10

5章 パスワード管理

5.1 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、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。super パスワードについては、オペレーションマニュアルのセクション 1 *はじめに*”*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）

5.1.1 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 5-1 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 5-2 にパスワード設定のポリシーを示します。

表 5-2 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。

5.1.2 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。

5.1.3 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。

5.1.4 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。

5.1.5 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。

5.2 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。

5.3 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

5.4 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**	ー
2. グローバルパスワード制御機能を有効にする	**password-control enable**	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。

5.5 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. 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
3. 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
4. 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
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：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。
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： **same-character** は無効、**user-name**は有効
7. 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
8. 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。
9. 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
10. 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

操作	コマンド	補足
11．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。
12．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

5.6 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**	―
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、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。
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。

5.7 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**	―

操作	コマンド	補足
2. 装置管理ユーザを作成し、local user view に移行する	**local-user** *user-name* **class manage**	ローカルユーザパスワード管理は、ネットワークアクセスユーザではなく、装置管理ユーザに適用されます。ローカルユーザを設定する方法については、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。
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。
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。

5.8 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**	―
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

操作	コマンド	補足
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。

5.9 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** [**user-name** *user-name* | **super** [**role** *role-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。

5.10 パスワード管理の設定例

5.10.1 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 **9-x-x** です。

6 章 公開鍵 6-1
6.1 概要 6-1
6.2 ローカル鍵ペアの作成 6-1
6.2.1 設定ガイドライン 6-1
6.2.2 設定手順 6-2
6.3 ローカルホスト公開鍵の配布 6-2
6.3.1 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 6-3
6.3.2 ホスト公開鍵の表示 6-3
6.4 ローカル鍵ペアの削除 6-3
6.5 ピア公開鍵の設定 6-3
6.5.1 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 6-4
6.5.2 ピアの公開鍵の入力 6-4
6.6 公開鍵の表示と維持 6-4

6章 公開鍵

6.1 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）アルゴリズム
- DSA（Digital Signature Algorithm）アルゴリズム

SSH、SSL を含む多くのセキュリティアプリケーションは、図 6-1 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。

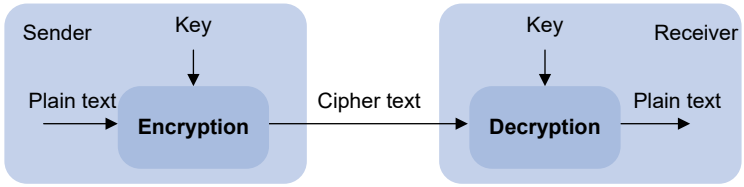


図 6-1 暗号化と複号化

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。

6.2 ローカル鍵ペアの作成

6.2.1 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。
- 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 6-1 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。

🕮 **メモ：**

SSH 1.5 のみが RSA サーバ鍵ペアを使用します。

6.2.2 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**	―
2． ローカル DSA あるいは RSA 鍵ペアを作成する	**public-key local create** { **dsa** | **rsa** } [**name** *key-name*]	デフォルト：作成なし

6.3 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。

6.3.1 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*] • 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*]

6.3.2 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。

6.4 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** | **rsa** } [**name** *key-name*]	—

6.5 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）

6.5.1 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、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”* 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。

6.5.2 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。

6.6 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** | **rsa** } **public**
ピアのホスト公開鍵を表示する	**display public-key peer** [**brief** | **name** *publickey-name*]

目次

このセクションのページは **9-x-x** です。

7 章 SSH（FIT は未サポート） 7-1
7.1 概要 7-1
7.1.1 SSH の動作 7-1
7.1.2 SSH 認証方式 7-2
7.2 SSH サーバの設定 7-3
7.2.1 ローカル鍵ペアの作成 7-4
7.2.2 Stelnet サーバ機能の有効化 7-5
7.2.3 SFTP サーバ機能の有効化 7-5
7.2.4 SSH ログインのユーザラインの設定 7-5
7.2.5 クライアントのホスト公開鍵の設定 7-6
7.2.6 SSH ユーザの設定 7-7
7.2.7 SSH 管理パラメータの設定 7-8
7.3 Stelnet クライアントの設定 7-9
7.3.1 Stelnet クライアントの作業設定リスト 7-9
7.3.2 ローカル鍵ペアの作成 7-10
7.3.3 SSH パケットの送信元 IP アドレスの指定 7-10
7.3.4 Stelnet サーバとの接続の確立 7-10
7.4 SFTP クライアントの設定 7-11
7.4.1 SFTP クライアントの設定作業リスト 7-11
7.4.2 ローカル鍵ペアの作成 7-11
7.4.3 SFTP パケットの送信元 IP アドレスの指定 7-12
7.4.4 SFTP サーバとの接続の確立 7-12
7.4.5 SFTP ディレクトリの操作 7-13
7.4.6 SFTP ファイルの操作 7-13
7.4.7 ヘルプ情報の表示 7-13
7.4.8 SFTP サーバの接続の切断 7-14
7.5 SSH の表示と維持 7-14
7.6 Stelnet 設定例 7-14
7.6.1 公開鍵認証を有効にした Stelnet サーバの設定例 7-14
7.6.2 パスワード認証を有効にした Stelnet クライアント設定例 7-20
7.6.3 公開鍵認証を有効にした Stelnet クライアント設定例 7-22
7.7 SFTP 設定例 7-24
7.7.1 パスワード認証を有効にした SFTP サーバの設定例 7-24
7.7.2 公開鍵認証を有効にした SFTP クライアント設定例 7-26

7章 SSH（FIT は未サポート）

本マニュアルに登場する「FIT」という用語は、特に断りがない場合、Anchor-FIT モードで動作する AP のことを含みます。

7.1 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や、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。

7.1.1 SSH の動作

表 7-1 に、SSH2 を使用した SSH セッションの確立に関連するステージの例を示します。

表 7-1 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。

ステージ	説明
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。

7.1.2 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。

7.2 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	―
（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。

作業リスト	補足
（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	–

7.2.1 ローカル鍵ペアの作成

DSA または 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。

装置の DSA 鍵ペアあるいは 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 と 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 と 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。

II. 設定手順

以下に SSH サーバでローカル DSA あるいは 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**	―
2． ローカル DSA または RSA 鍵ペアを作成する	**public-key local create** { **dsa** | **rsa** }	デフォルト：鍵ペアは存在しません。

7.2.2 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**	―
2． Stelnet サーバ機能を有効にする	**ssh server enable**	デフォルト：無効

7.2.3 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

7.2.4 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*]	―

操作	コマンド	補足
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1 *はじめに “ログイン”* を参照してください。

7.2.5 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**	—
2. public key view に移行する	**public-key peer** *keyname*	—

操作	コマンド	補足
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9 *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**	―

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*

7.2.6 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** | **sftp** | **stelnet** } **authentication-type** { **password** | { **any** | **password-publickey** | **publickey** } [**assign publickey** *keyname*&<1-6>] }

7.2.7 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

操作	コマンド	補足
3. RSA サーバ鍵ペアの最小アップデート間隔を設定する	**ssh server rekey-interval** *hours*	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。 このコマンドはSSH1ユーザのみ適用します。
4. 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。
5. 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
6. 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
7. 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。
8. 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。
9. 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。

7.3 Stelnetクライアントの設定

7.3.1 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**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	―

7.3.2 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**	ー
2． ローカル鍵ペアを作成する	**public-key local create** { **dsa** | **rsa** }	デフォルト : 鍵ペアは存在しません。

7.3.3 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**	ー
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。

7.3.4 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* }] *	どちらか一方の設定を使用します。 user viewで実行できます。

7.4 SFTPクライアントの設定

7.4.1 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**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） 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	―

7.4.2 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。

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** | **rsa** }	デフォルト : 鍵ペアは存在しません。

7.4.3 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	• SFTPパケットの送信元IPv4アドレスを指定する: **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。

7.4.4 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サーバの接続を確立する： **sftp** *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* | **public-key** *keyname* | **source** { **interface** *interface-type interface-number* | **ip** *ip-address* }] *	user viewで実行できます。

7.4.5 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。

7.4.6 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。

7.4.7 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。

7.4.8 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。

7.5 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*]
SSHピアの公開鍵を表示する	**display public-key peer** [**brief** | **name** *publickey-name*]

7.6 Stelnet設定例

7.6.1 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 7-1 に示すように設定します。

- AP 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。
- クライアントは SSH2（Stelnet client software）を使用します。ユーザが Stelnet を経由してクライアントで AP にログインすると、ユーザは AP の設定と管理ができます。

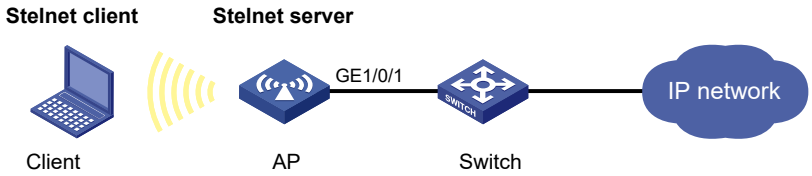


図 7-1 ネットワーク図

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。

d)　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 7-2 クライアントの鍵ペアの作成

e)　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 7-3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。

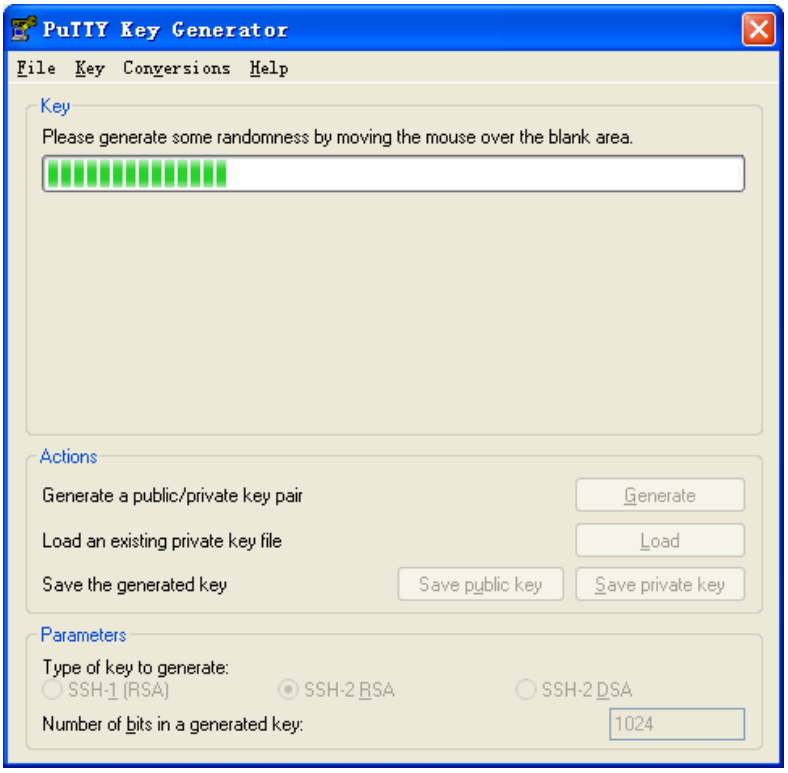


図 7-3 プロセスの作成

f)　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。

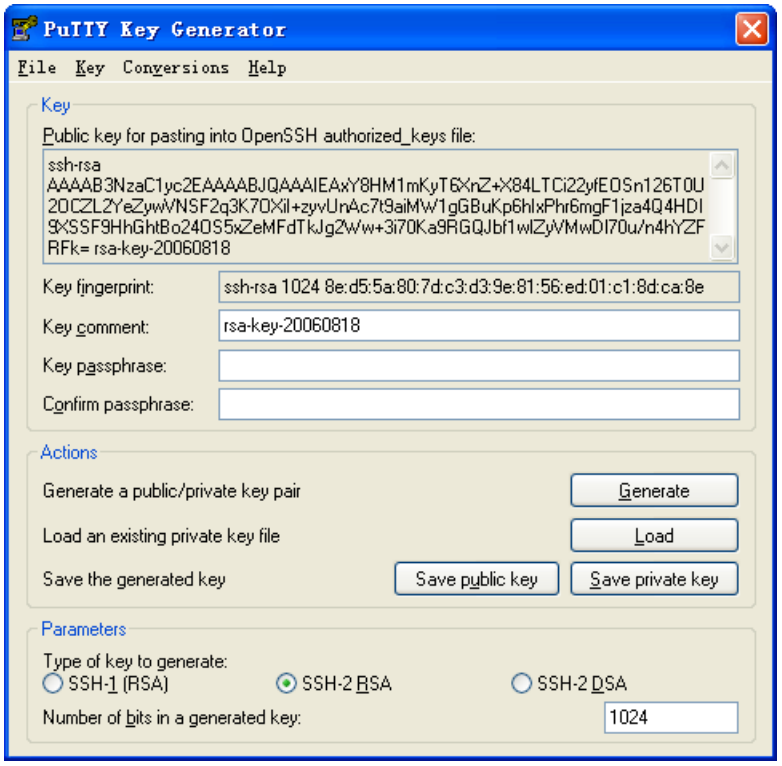


図 7-4 クライアントの鍵ペアの保存

g)　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。

h)　図 7-4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。

i)　**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。

j)　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。

k)　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。

```
<AP> system-view
[AP] 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.
```

SSH サーバ機能を有効にします。

```
[AP] 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。

```
[AP] vlan 2
[AP-vlan2] quit
[AP] interface vlan-interface 2
[AP-Vlan-interface2] ip address 192.168.1.40 255.255.255.0
[AP-Vlan-interface2] quit
```

ユーザラインの認証モードを AAA に設定します。

```
[AP] line vty 0 4
[AP-ui-vty0-4] authentication-mode scheme
```

SSH をサポートするためにユーザラインを設定します。

```
[AP-ui-vty0-4] protocol inbound ssh
[AP-ui-vty0-4] quit
```

クライアントの公開鍵を公開鍵ファイル **key.pub** からインポートし、**AP001** と名付けます。

```
[AP] public-key peer AP001 import sshkey key.pub
```

ローカルユーザ **client002** を作成します。

```
[AP] local-user client002
```

#に対してプレーンテキストのパスワード **aabbcc** を設定します。

```
[AP-luser-manage-client002] password simple aabbcc
```

SSH サービスを使用するためにローカルユーザ **client002** を許可します。

```
[AP-luser-manage-client002] service-type ssh
```

ユーザロール **network-admin** をローカルユーザ **client002** に割り当てます。

```
[AP-luser-manage-client002] authorization-attribute user-role network-admin
[AP-luser-manage-client002] quit
```

SSH ユーザ **client002** を作成し、認証方法を **publickey** に指定します。公開鍵 **AP001** をユーザに割り当てます。

```
[AP] ssh user client002 service-type stelnet authentication-type publickey assign publickey AP001
```

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。

l) 図 7-5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。

m) **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。

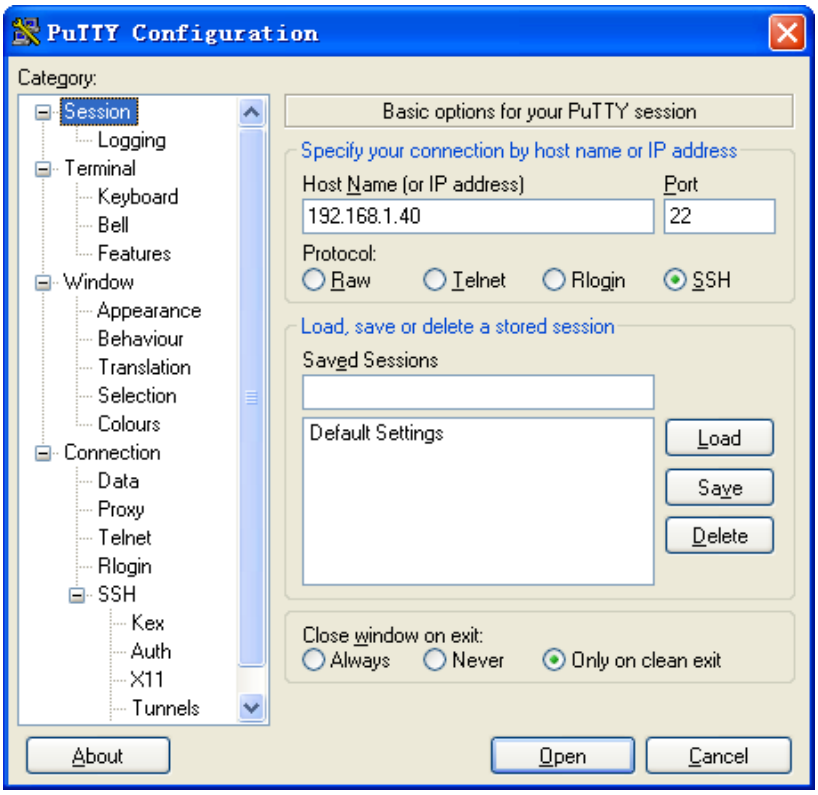


図 7-5 ホスト名（あるいは IP アドレス）の指定

n) 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 7-6に示すようにウィンドウ画面が表示されます。

o) 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。

p) **Open**をクリックします。

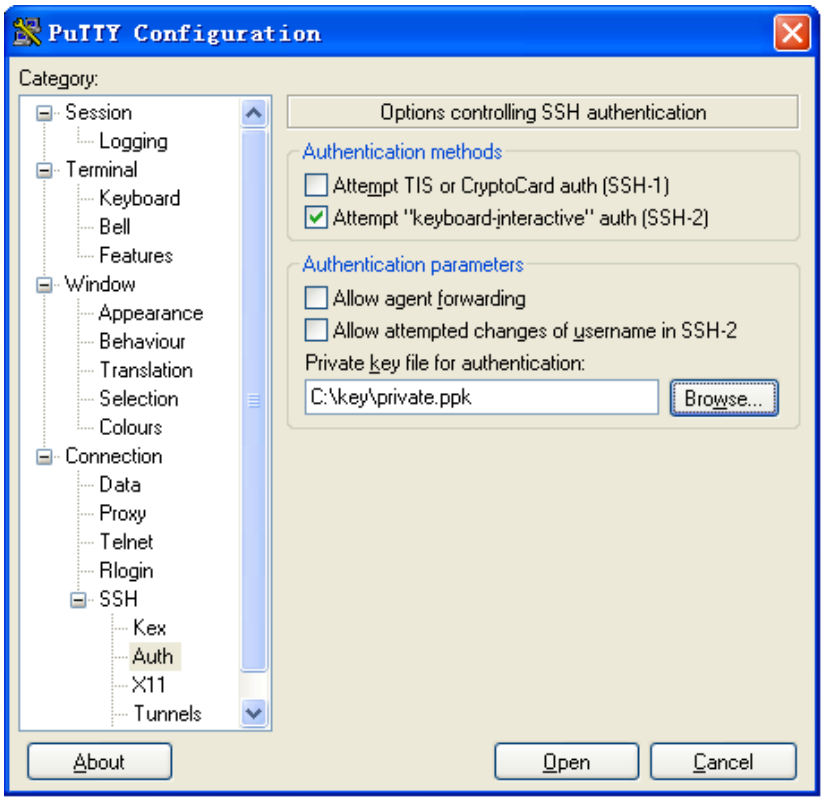


図 7-6 秘密鍵ファイルの指定

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。

7.6.2 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 7-7 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。
- AP は Stelnet クライアントとして動作します。ユーザが Stelnet を経由して AP でスイッチにログインすると、ユーザはスイッチの設定と管理が可能です。

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。

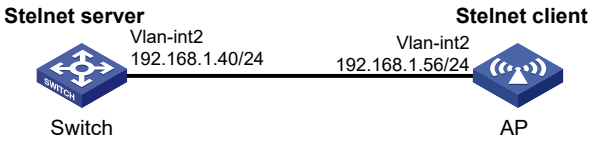


図 7-7 ネットワーク図

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 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.
```

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 4
[Switch-ui-vty0-4] authentication-mode scheme
```

ローカルユーザ **client001** を作成します。

```
[Switch] local-user client001
```

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。

```
<AP> system-view
[AP] interface vlan-interface 2
[AP-Vlan-interface2] ip address 192.168.1.56 255.255.255.0
[AP-Vlan-interface2] quit
```

```
[AP] quit
```

サーバへの SSH 接続を確立します。

```
<AP> ssh2 192.168.1.40
Username: client001
Trying 192.168.1.40 ...
Press CTRL+K to abort
Connected to 192.168.1.40 ...

The Server is not authenticated. Continue? [Y/N]:y
Do you want to save the server public key? [Y/N]:n
Enter password:
```

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。

7.6.3 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 7-8 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 RSA 公開鍵アルゴリズムを使用します。
- AP は Stelnet クライアントとして動作します。ユーザが Stelnet を経由して AP でスイッチにログインすると、ユーザはスイッチの設定と管理が可能になります。

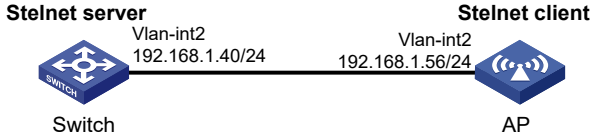


図 7-8 ネットワーク図

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。

```
<AP> system-view
[AP] interface vlan-interface 2
[AP-Vlan-interface2] ip address 192.168.1.56 255.255.255.0
[AP-Vlan-interface2] quit
```

RSA 鍵ペアを作成します。

```
[AP] public-key local create rsa
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.
Create the key pair successfully.
```

RSA ホスト公開鍵をファイル **key.pub** にエクスポートします。

```
[AP] public-key local export rsa ssh2 key.pub
[AP] 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 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.
```

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 4
[Switch-ui-vty0-4] authentication-mode scheme
```

SSH をサポートするためにユーザラインを設定します。

```
[Switch-ui-vty0-4] protocol inbound ssh
[Switch-ui-vty0-4] 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 **AP001** とします。

```
[Switch] public-key peer AP001 import sshkey key.pub
```

ローカルユーザ **client002** を作成します。

```
[Switch] local-user client002
```

パスワードをプレーンテキストで aabbcc に設定します。

```
[Switch-luser-manage-client002] password simple aabbcc
```

SSH サービスを使用するために client002 を許可します。

```
[Switch-luser-manage-client002] service-type ssh
```

ユーザにユーザロール **network-admin** を割り当てます。

```
[Switch-luser-manage-client002] authorization-attribute user-role network-admin
```

```
[Switch-luser-manage-client002] quit
```

SSH ユーザ client002 を作成します。認証方法を publickey に指定し、公開鍵 AP001 を割り当てます。

```
[Switch] ssh user client002 service-type stelnet authentication-type publickey assign publickey AP001
```

3)　Stelnet サーバ 192.168.1.40 に SSH 接続を確立します。

```
<AP> ssh2 192.168.1.40
Username: client002
Trying 192.168.1.40 ...
Press CTRL+K to abort
Connected to 192.168.1.40 ...

The Server is not authenticated. Continue? [Y/N]:y
Do you want to save the server public key? [Y/N]:n
```

ユーザ名 client002 を入力後、y を入力すると、サーバへのアクセスを継続し、サーバに正常にログインできます。

7.7 SFTP設定例

7.7.1 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 7-9 に示すように設定します。

- AP は SFTP サーバとして動作し、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 AP に保存されます。
- ユーザが SFTP を経由してクライアントで AP にログインすると、ユーザはファイル管理と伝送操作を AP で行うことができます。

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。

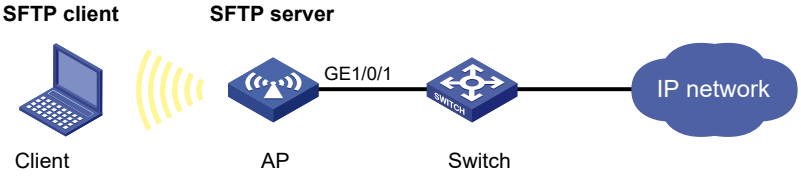


図 7-9 ネットワーク図

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。

```
<AP> system-view
[AP] public-key local create rsa
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
```

```
Generating Keys...
.
Create the key pair successfully.
```

SFTP サーバ機能を有効にします。

```
[AP] 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。

```
[AP] interface vlan-interface 2
[AP-Vlan-interface2] ip address 192.168.1.45 255.255.255.0
[AP-Vlan-interface2] quit
```

ローカルユーザ **client002** を作成します。

```
[AP] local-user client002
```

プレーンテキストのパスワードを **aabbcc** に設定します。

```
[AP-luser-manage-client002] password simple aabbcc
```

SSH サービスを使用するためにローカルユーザ **client002** を許可します。

```
[AP-luser-manage-client002] 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。

```
[AP-luser-manage-client002] authorization-attribute user-role network-admin work-directory flash:/
[AP-luser-manage-client002] quit
```

SSH 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。

```
[AP] 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 7-10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。

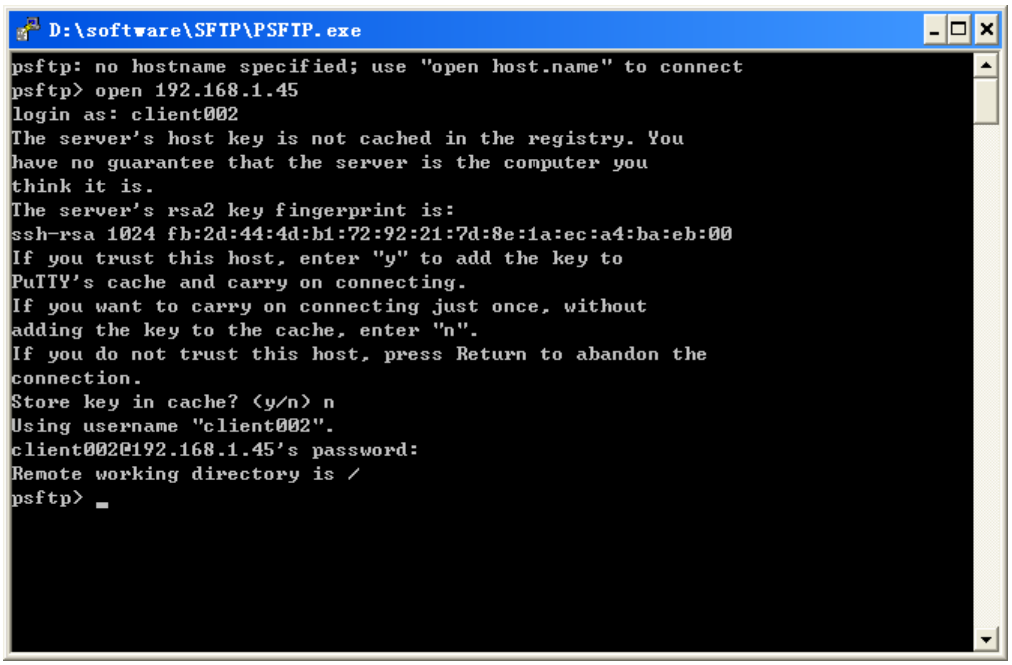


図 7-10 SFTP クライアントインタフェース

7.7.2 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 7-11 に示すように設定します。

- スイッチは SFTP サーバとして動作し、公開鍵認証と RSA 公開鍵アルゴリズムを使用します。
- AP は SFTP クライアントとして動作します。ユーザが SFTP を経由して AP でスイッチにログインすると、ユーザはファイル管理と伝送操作をスイッチで行うことができます。

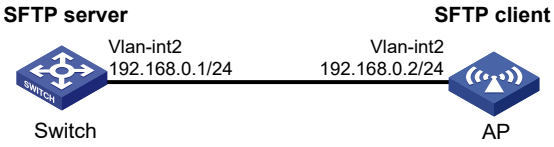


図 7-11 ネットワーク図

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。

```
<AP> system-view
```

```
[AP] interface vlan-interface 2
[AP-Vlan-interface2] ip address 192.168.0.2 255.255.255.0
[AP-Vlan-interface2] quit
```

RSA 鍵ペアを作成します。

```
[AP] public-key local create rsa
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.
Create the key pair successfully.
```

ホスト公開鍵をファイル **pubkey** にエクスポートします。

```
[AP] public-key local export rsa ssh2 pubkey
[AP] 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。

```
<Switch> system-view
[Switch] 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.
```

SFTP サーバ機能を有効にします。

```
[Switch] 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。

```
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ip address 192.168.0.1 255.255.255.0
[Switch-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 **AP001** とします。

```
[Switch] public-key peer AP001 import sshkey pubkey
```

ローカル装置管理ユーザ **client001** を作成します。

```
[Switch] local-user client001
```

パスワードをプレーンテキストで aabbcc に設定します。

```
[Switch-luser-manage-client001] password simple aabbcc
```

SSH サービスを使用するためにローカルユーザ client001 を許可します。

```
[Switch-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。

```
[Switch-luser-manage-client001] authorization-attribute user-role network-admin work-directory flash:/
[Switch-luser-manage-client001] quit
```

SSH ユーザ **client001** を作成します。サービスタイプを **sftp**、認証方式を **publickey**、公開鍵を **AP001** に設定します。

```
[Switch] ssh user client001 service-type sftp authentication-type publickey assign publickey AP001
```

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。

```
<AP> sftp 192.168.0.1 identity-key rsa
Input Username: client001
Trying 192.168.0.1 ...
Press CTRL+K to abort
Connected to 192.168.0.1 ...

The Server is not authenticated. Continue? [Y/N]:y
Do you want to save the server public key? [Y/N]:n

sftp-client>
```

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-client> dir
-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-client> delete z
The following File will be deleted:
/z
Are you sure to delete it? [Y/N]:y
This operation may take a long time.Please wait...

File successfully Removed
sftp-client> dir
-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-client> mkdir new1
New directory created
sftp-client> dir
-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-client> rename new1 new2
File successfully renamed
sftp-client> dir
-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-client> get pubkey2 public
Remote  file:/pubkey2 --->  Local file: public
Downloading file successfully ended
```

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-client> put pu puk
Local file:pu --->  Remote file: /puk
Uploading file successfully ended
sftp-client> dir
-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-client>
```

SFTP client view から戻ります。

```
sftp> quit
Bye
Connection closed.
<AP>
```

目次

このセクションのページは **9-x-x** です。

8章 PKI設定 8-1
8.1 概要 8-1
8.1.1 PKI 用語 8-1
8.1.2 PKIのアーキテクチャ 8-2
8.1.3 PKIのアプリケーション 8-3
8.1.4 PKIの動作 8-3
8.2 PKI 設定手順リスト 8-4
8.3 エンティティのDNの設定 8-4
8.4 PKIドメインの設定 8-5
8.5 PKI証明書リクエストの提出 8-7
8.5.1 証明書リクエストの提出 8-8
8.6 手動での証明書の取得 8-9
8.7 PKI証明書の確認の設定 8-9
8.8 ローカルRSA鍵ペアの廃棄 8-11
8.9 証明書の削除 8-11
8.10 PKIの表示 8-12
8.11 PKI 設定例 8-12
8.11.1 CAからローカル証明書を手動で取得する 8-12
8.12 PKIのトラブルシューティング 8-15
8.12.1 CA証明書の取得に失敗 8-15
8.12.2 ローカル証明書のリクエストに失敗 8-15
8.12.3 CRLの取得に失敗 8-16

8章 PKI 設定

8.1 概要

Public Key Infrastructure(PKI)は公開鍵技術を用いて、情報セキュリティを提供する一般的なセキュリティ方式です。

PKI は、非対称鍵方式とも呼ばれ、データの暗号化と復号化の鍵ペアを用います。鍵ペアは秘密鍵と公開鍵から構成されます。秘密鍵は秘密を保つ必要がありますが、公開鍵は分配する必要があります。2 つの鍵の 1 つを用いて暗号化されたデータはもう一方の鍵のみによって、復号化されます。

PKI の鍵の問題点は、公開鍵の管理方法です。この問題を解決するため、PKI はデジタル証明書を使用します。デジタル証明書のメカニズムは、公開鍵がオーナのものであることを結びつけ、安全で大規模なネットワークで公開鍵を配布できるようにします。

デジタル証明書において、PKI システムは、ユーザ認証、データ否認拒否、データの機密性、データの完全性のようなセキュリティサービスを行うネットワーク通信と e-コマースを提供します。

PKI システムは、Secure Sockets Layer (SSL)のため、証明書管理を提供します。

8.1.1 PKI 用語

I. デジタル証明書

デジタル証明書は、エンティティのため、認証局(CA)によってファイルの署名が行われます。主に認証情報、エンティティの公開鍵、CA 名、CA の署名、証明書の有効期間が含まれます。CA の署名が、証明書の有効性を保証します。デジタル証明書は、ITU-T X.509 の国際標準に準拠していなくてはいけません。一般的な標準は X.509 v3 です。

本文書で用いるローカル証明書と CA 証明書について説明します。ローカル証明書は、エンティティのため、CA によってデジタル証明書に署名されます。CA 証明書は CA が証明書に署名します。複数の CA が PKI システムの異なるユーザによって信頼されると、CA はトップレベルがルート CA となる CA ツリーの形となります。ルート CA はそれ自体 CA 証明書をもっており、低レベルの CA は次に高いレベルの CA によって、CA 証明書に署名されます。

II. CRL

発行されている証明書は、ユーザ名の変更、秘密鍵の漏洩、ユーザがビジネスを停止するときなどによって、取り消される必要があります。証明書の取り消しは、ユーザが正しいことを示す情報の公開鍵との結合を削除します。PKI において、取り消しは証明書失効リスト(CRL)によって行われます。証明書が取り消されるとき、CA は、すべての証明書が取り消されたということを示すため、ひとつあるいは複数の CRL を発行します。CRL はすべての取り消された証明書のシリアル番号を含んでおり、証明書が正しいかをチェックするのに効果的です。

CA は取り消された証明書の数が大きく、複数の CRL が配布されると、ネットワークに悪影響が起こる可能性があるときに、1 つのみ CRL が発行されます。CRL の URL を示すために、CRL 配布ポイントを使います。

III. CA ポリシー

CA ポリシーは CA が証明書リクエスト、失効証明書のプロセスや、CRL の配布を行うための基準です。一般的に CA は証明書実行ステート(CPS)の形式でポリシーを配布します。CA ポリシーは電話、ディスク、電子メールなどの通信外の方法を経由して取得できます。エンティティの公開鍵の結合をチェックする際、異なる CA は、異なる方法を使用します。そのため、信頼された CA を選択する前に、証明書リクエスト用の CA ポリシーを理解する必要があります。

8.1.2 PKI のアーキテクチャ

図 2-1に示すように PKI システムは、エンティティ、CA、登録局(RA)、PKI リポジトリ(repository)から構成されます。

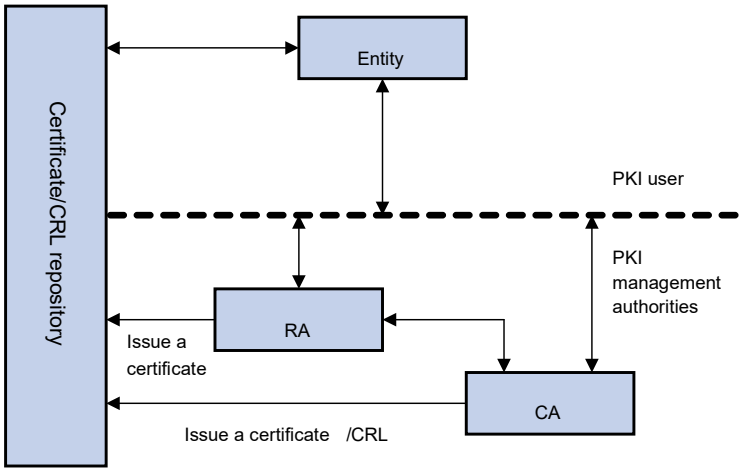


図 8-1 PKI アーキテクチャ

I. エンティティ

エンティティは、人や組織、ルータやスイッチやコンピュータで動作するプロセスのようなデバイスなどの PKI の製品やサービスのエンドユーザです。

II. CA

CA はデジタル証明書を発行したり管理したりするための、信頼された機関です。CA は CRL の配布に必要となるため、証明書の発行、証明書の有効期間を指定、失効証明書の取り消しを行います。

III. RA

登録局(RA)は CA の拡張機関、あるいは独立な機関です。CRL 管理、鍵ペア生成、鍵ペアのバックアップを含んだ機能を実装しています。PKI 標準では、アプリケーションシステ

ムの、より高度なセキュリティを実現するため、独立な RA が登録管理されることを推奨しています。

IV. PKI リポジトリ

PKI リポジトリは Lightweight Directory Access Protocol(LDAP)サーバや共通データベースで使われます。単一のクエリ機能を提供している間、証明書リクエスト、証明書、鍵、CRL、ログなどの情報を保存し、管理します。

LDAP は PKI 情報をアクセスし、管理するためのプロトコルです。LDAP サーバは、RA サーバからユーザ情報、デジタル証明書を保存します。ディレクトリナビゲーションサービスを提供します。エンティティは他のエンティティの証明書と同様に、そのローカル証明書と CA 証明書を取得することができます。

8.1.3 PKI のアプリケーション

PKI テクノロジーはオンライン処理のセキュリティ要求事項を満足させます。基盤として PKI は広い範囲のアプリケーションをもっています。ここではいくつかのアプリケーション例をあげます。

I. セキュア(安全)な email

Email は機密性、完全性、認証、非拒否性が必要とされます。PKI はこれらのニーズに取り組むことができます。安全な Email プロトコルは、Secure/Multipurpose Internet Mail Extensions (S/MIME)で、急速に発展しています。このプロトコルは PKI ベースを基にしており、署名に暗号化されたメールの転送を行うために使われます。

II. Web セキュリティ

Web セキュリティにおいて、トランスペアレントでセキュアな通信を行うために、アプリケーションレイヤで、最初に 2 つのピアが SSL 通信を確立できます。PKI において、SSL はブラウザとサーバ間で暗号化した通信を有効にします。通信グループの両方は、デジタル証明書を用いて、互いが正しいかアイデンティティを検証することができます。

8.1.4 PKI の動作

PKI が有効であるネットワークにおいて、エンティティは CA からローカル証明書をリクエストできます。デバイスは証明書が正しいかどうかをチェックします。以下に動作を示します。

1) エンティティは RA に証明書リクエストを提出します。
2) RA はエンティティが正しいかアイデンティティを再チェックし、アイデンティティ情報とデジタル署名の公開鍵を CA に送信します。
3) CA はデジタル署名をチェックします。アプリケーションを確認し、証明書を配布します。
4) RA は CA から証明書を受信し、ディレクトリナビゲーションサービスを提供するために LDAP サーバに証明書を送信します。証明書の発行に成功したことをエンティティに通知します。

5) エンティティは証明書を回収します。エンティティは、証明書を使用し、暗号化とデジタル署名によって、安全に他のエンティティと通信することができます。
6) 証明書の取り消しが必要なとき、エンティティは、CA にリクエストします。CA はリクエストを確認します。CRL をアップデートし、LDAP サーバの CRL を公表します。

8.2 PKI 設定手順リスト

以下に PKI を設定する手順を示します。

表 8-1 PKI 設定手順リスト

作業	補足
エンティティのDNの設定	必須設定項目
PKIドメインの設定	必須設定項目
PKI証明書リクエストの提出	必須設定項目
手動での証明書の取得	オプション設定項目
PKI証明書の確認の設定	オプション設定項目
ローカルRSA鍵ペアの廃棄	オプション設定項目
証明書の削除	オプション設定項目

8.3 エンティティのDNの設定

証明書は、公開鍵とエンティティのアイデンティティ情報を組み合わせます。そしてエンティティ識別名(DN)によって、アイデンティティ情報が、正常かどうか判断します。CA はエンティティ DN によって証明書申請者を独自に識別します。

エンティティ DN は以下のパラメータによって定義されます。

- エンティティの共通名
- 標準 2 文字で表されたエンティティのカントリーコード。たとえば CN は中国、US はアメリカ、JP は日本と表します。
- エンティティの完全修飾ドメイン名(FQDN)、ネットワーク上でエンティティの一意な識別子。ホスト名とドメイン名で構成され、IP アドレスに変換されます。たとえば www.whatever.com は FQDN、www はホスト名、whatever.com はドメイン名です。
- エンティティの IP アドレス
- エンティティがある所在地
- エンティティが所属している組織
- 組織内のエンティティのユニット
- エンティティがある州、県

🕮 **メモ：**

エンティティ DN の設定は、CA 証明書のポリシーに従う必要があります。たとえば、どのエンティティ DN パラメータが必須なのか、オプションなのかを決定する必要があります。そうでないと証明書は拒否されます。

以下にエンティティ DN を設定する手順を示します。

表 8-2 エンティティの DN の設定

操作	コマンド	補足
1. system view へ移行する	**system-view**	―
2. エンティティを作成し、その view に移行する	**pki entity** *entity-name*	デフォルト：なし
3. （オプション設定項目）エンティティの共通名を設定する	**common-name** *name*	デフォルト：なし
4. （オプション設定項目）エンティティのカントリーコードを設定する	**country** *country-code-str*	デフォルト：なし
5. （オプション設定項目）エンティティの FQDN を設定する	**fqdn** *name-str*	デフォルト：なし
6. （オプション設定項目）エンティティの IP アドレスを設定する	**ip** *ip-address*	デフォルト：なし
7. （オプション設定項目）エンティティの所在地を設定する	**locality** *locality-name*	デフォルト：なし
8. （オプション設定項目）エンティティの組織を設定する	**organization** *org-name*	デフォルト：なし
9. （オプション設定項目）エンティティのユニット名を設定する	**organization-unit** *org-unit-name*	デフォルト：なし
10. （オプション設定項目）エンティティの州あるいは県を設定する	**state** *state-name*	デフォルト：なし

🕮 **メモ：**

- Windows 2000 CA サーバは証明書リクエストのデータ長にいくつかの制限があります。もし証明書のエンティティ DN が、証明書のリクエストの制限を越える場合、サーバは証明書のリクエストに応答しません。

8.4 PKIドメインの設定

PKI 証明書のリクエストを行う前に、エンティティは登録情報の設定をする必要があります。登録情報は PKI ドメインとして参照されます。IKE、SSL のような他のアプリケーションにとって、PKI ドメインは参照を行う場合に役立ちます。デバイスに設定された PKI ドメインは、CA と他のデバイスには知られません。各 PKI ドメインはそれ自体のパラメータをもちます。

PKI ドメインは以下のパラメータで定義されます。

- trusted CAーエンティティは trusted CA.から証明書をリクエストします。

- エンティティー証明書アプリカント(申請者)は、CA にアイデンティティ情報を提供するためのエンティティを使用します。
- RAー一般的に独立した登録局(RA)は証明書リクエストマネジメントを管理しています。エンティティから登録リクエストを受信し、その資格をチェックします。デジタル証明書に署名するために CA に確認していいかどうかを決めます。RA はエンティティのアプリケーションの資格をチェックするだけで、いかなる証明書も発行しません。独立した RA が必要でない場合、登録の管理は CA が行いますが、独立した RA を配置すべきです。
- 登録サーバの URLーエンティティは、エンティティが CA と通信するために使われる SCEP (Simple Certification Enrollment Protocol)を通して、登録サーバに証明書リクエストを送信します。
- ポーリング間隔と総数ーアプリカントが証明書リクエストを作成した後、手動で証明書リクエストを確認する場合、CA は長い時間かかります。証明書の署名が行われた後、アプリカントができるだけ早く証明書を取得できるように、周期的にリクエストの状態を問い合わせする必要があります。ポーリング間隔と総数を設定することができます。
- LDAP サーバの IP アドレスーLDAP サーバは、普通、証明書と CRL を記録するのに使われます。このため、LDAP サーバの IP アドレスを設定する必要があります。
- ルート証明書が改ざんされていないための証明書データ(フィンガープリント)ーCA のルート証明書を取得した際、エンティティはルート証明書のフィンガープリントを検証する必要があります。これはルート証明書のデータのハッシュ値です。このハッシュ値は、証明書ごとに一意に決まります。ルート証明書のフィンガープリントが PKI ドメイン用に設定されたものと異なる場合、エンティティはルート証明書を拒否します。

PKI ドメインを設定する手順を以下に示します。

表 8-3 PKI ドメインの設定

操作	コマンド	補足
1. system view へ移行する	**system-view**	ー
2. PKI ドメインを作成し、その view へ移行する	**pki domain** *domain-name*	デフォルト：なし
3. trusted CA を指定する	**ca identifier** *name*	デフォルト：なし
4. 証明書リクエスト用のエンティティを指定する	**certificate request entity** *entity-name*	デフォルト：なし 指定されたエンティティは必要です。
5. 証明書リクエスト用の機関を指定する	**certificate request from** { **ca** | **ra** }	デフォルト：なし
6. 証明書リクエスト用のサーバの URL を設定する	**certificate request url** *url-string*	デフォルト：なし
7. （オプション設定項目）証明書リクエスト問い合わせ用のポーリング間隔と総数を設定する	**certificate request polling** { **count** *count* | **interval** *minutes* }	デフォルト：ポーリングは20分の間隔で50回です。

操作	コマンド	補足
8. ルート証明書検証のためのフィンガープリントを設定する	**root-certificate fingerprint** { **md5** | **sha1** } *string*	証明書リクエストモードが自動の場合は必須設定項目です。 証明書リクエストモードが手動の場合はオプション設定項目。 証明書リクエストモードが手動で、このコマンドが設定されていない場合、ルート証明書のフィンガープリントは手動で検証する必要があります。 デフォルト：なし。
9. 証明書要求のためにキーペアを指定する	• RSAキーペア： **public-key rsa** { { **encryption name** *encryption-key-name* [**length** *key-length*] | **signature name** *signature-key-name* [**length** *key-length*] } * | **general name** *key-name* [**length** *key-length*] } • ECDSAキーペア： **public-key ecdsa name** *key-name* [**secp192r1** | **secp256r1** | **secp384r1** | **secp521r1**] • DSAキーペア **public-key dsa name** *key-name* [**length** *key-length*]	デフォルト：なし

🕮 **メモ：**

- CA 証明書を取得するときのみ、CA 名が要求されます。ローカル証明書リクエストの時には使われません。

8.5 PKI証明書リクエストの提出

証明書を要求する際、エンティティは、アイデンティティ情報と公開鍵を提供することによって、CA に通知します。その情報は証明書の重要な構成要素となります。証明書リクエストは、オンラインモードあるいはオフラインモードでも CA に提出できます。オフラインモードにおいて、証明書リクエストは、電話、ディスク、Email などのような通信外の手段によって、提供されます。

オンライン証明書リクエストは手動モードと自動モードに分けられます。しかし本装置では手動モードのみサポートしています。

8.5.1 証明書リクエストの提出

エンティティ用に、CA 証明書を取得し、ローカル RSA 鍵ペアを作成し、ローカル証明書リクエストを提出する必要があります。

CA 証明書の取得の目的は、ローカル証明書の確実性と妥当性を検証するためです。

RSA 鍵ペアの作成は、証明書リクエストの重要な手順です。鍵ペアは公開鍵と秘密鍵をもっています。秘密鍵はユーザによって保持され、公開鍵は他の情報と一緒に CA に転送されます。

証明書リクエストを提出する手順を以下に示します。

表 8-4 証明書リクエストの提出

操作	コマンド	補足
1． system view へ移行する	**system-view**	―
2． PKI domain view へ移行する	**pki domain** *domain-name*	―
3． （オプション設定項目）証明書リクエストモードの手動設定を行う	**certificate request mode manual**	デフォルト：手動
4． system view へ戻る	**quit**	―
5． 手動での CA 証明書を取得する	手動での証明書の取得を参照してください。	―
6． ローカル RSA 鍵ペアを作成する	**public-key local create rsa**	デフォルト：なし
7． 手動のローカル証明書リクエストを提出する	**pki request-certificate domain** *domain-name* [*password*] [**pkcs10** [**filename** *filename*]]	―

🕮 **メモ：**

- PKI ドメインがすでにローカル証明書をもっている場合、RSA 鍵ペアの作成は、鍵ペアと証明書が矛盾します。新しい RSA 鍵ペアを作成するため、ローカル証明書を削除した後、**public-key local create** コマンドを実行します。
- 新しく作成された鍵ペアはすでに存在している鍵ペアに上書きされます。もしローカル RSA 鍵ペアを作成する際に、**public-key local create** コマンドを実行する場合、システムは上書きするかどうかの確認メッセージが表示されます。
- もし PKI ドメインがすでにローカル証明書をもっている場合､そのためにまた別の証明書を要求することはできません。これは設定の変更によって証明書と登録情報の間で矛盾が起こらないようにします。
- SCEP を通して、CA から証明書を要求することができないとき、**pki request-certificate domain** コマンドの pkcs10、ファイル名のキーワードを使用することによって、リクエスト情報を保存します。そして通信外の手段によって CA にファイルを送信します。
- エンティティと CA のクロックが同期されていることを確認してください｡同期していないと証明書期間が異常となります。
- PKI リクエスト証明書ドメイン設定は、コンフィグファイルに保存されません。

8.6 手動での証明書の取得

CA 証明書とローカル証明書をダウンロードし、それをローカルに保存することができます。オンラインモードやオフラインモードのどちらかで行います。オフラインモードではFTP、disk、Email のような通信外の手段を用いて証明書を取得する必要があります。ローカル PKI システムに、証明書を取り入れます。

証明書の取得は 2 つの目的に利用されます。

- 取得クエリの効率化とクエリ総数の削減を行うため、ローカルセキュリティドメインに関連した証明書をローカルに保存します。
- 証明書の確認用の準備を行います。

オンラインモードでローカル証明書の取得を行う前に、LDAP サーバの設定を行う必要があります。

手動証明書の取得の手順を以下に示します。

表 8-5 手動での証明書の取得

操作		コマンド	補足
1． system view へ移行する		**system-view**	ー
2． 手動証明書を取得する	オンライン	**pki retrieve-certificate domain** *domain-name* { **ca** | **local** }	どちらかのコマンドを使用します。
	オフライン	**pki import domain** *domain-name* { **der** { **ca** | **local** | **peer** } **filename** *filename* | **p12 local filename** *filename* | **pem** { **ca** | **local** | **peer** } [**filename** *filename*] }	

注意:

- PKI ドメインがすでに CA 証明書をもっている場合、また別の CA 証明書を取得することはできません。これは設定の変更ができないようにすることで証明書と登録情報が矛盾を生じないようにします。
- 新しい CA 証明書を取得するためには、**pki delete-certificate** コマンドを用い、存在する CA 証明書とローカル証明書を最初に削除します。
- PKI の取得と証明書の設定は、コンフィグファイルに保存されません。
- 証明書を有効とさせるため、デバイスのシステム時間が証明書の妥当な期間内にあることを確認してください。

8.7 PKI証明書の確認の設定

証明書は使用する前に確認する必要があります。証明書が CA によって署名されており、証明書の期限が切れていないことや無効でないことを確認します。

証明書の確認を行う前に、CA 証明書を取得する必要があります。

CRL のチェックは、証明書の確認で使うか指定することができます。もし CRL チェックを有効にした場合、CRL は証明書の確認に使われます。

I. CRL チェック機能有効時の PKI 証明書の確認の設定

CRL チェック有効時の PKI 証明書の確認の設定手順を以下に示します。

表 8-6 CRL チェック機能有効時の PKI 証明書の確認の設定

操作	コマンド	補足
1． system view へ移行する	**system-view**	―
2． PKI domain view へ移行する	**pki domain** *domain-name*	―
3． （オプション設定項目）CRL 発行ポイントの URL を指定する	**crl url** *url-string*	デフォルト：指定なし
4． （オプション設定項目）CRL チェックを有効にする	**crl check enable**	デフォルト：有効
5． system view へ戻る	**quit**	―
6． CA 証明書を取得する	手動での証明書の取得を参照してください。	―
7． CRL を取得する	**pki retrieve-crl domain** *domain-name*	―
8． 証明書の有効性をチェックする	**pki validate-certificate domain** *domain-name* { **ca** | **local** }	―

II. CRL チェック機能無効時の PKI 証明書の確認の設定

CRL チェック無効時の PKI 証明書の確認の設定の手順を以下に示します。

表 8-7 CRL チェック機能無効時の PKI 証明書の確認の設定

操作	コマンド	補足
1． system view へ移行する	**system-view**	―
2． PKI domain view へ移行する	**pki domain** *domain-name*	―
3． CRL チェックを無効にする	**undo crl check enable**	デフォルト：有効
4． system view へ戻る	**quit**	―
5． CA 証明書を取得する	手動での証明書の取得を参照してください。	―
6． 証明書の有効性をチェックする	**pki validate-certificate domain** *domain-name* { **ca** | **local** }	―

🕮 **メモ：**

- CRL アップデート期間は、エンティティが CRL サーバから CRL をダウンロードする間隔を参考にしています。CRL アップデート期間は、CRL で指定された期間よりも優先して設定されます。
- PKI 取得 CRL ドメインの設定は、設定ファイルに保存されません。
- CRL 発行ポイントの URL はドメイン名解決をサポートしていません。

8.8 ローカルRSA鍵ペアの廃棄

証明書はライフタイムをもっています。ライフタイムは CA によって決められます。秘密鍵が漏洩したり、証明書が期限切れとなったりする場合、古い RSA 鍵ペアの破棄を行います。そして新しい証明書を要求するリクエストのペアを作成します。

ローカル RSA ペアを廃棄する手順を以下に示します。

表 8-8 ローカル RSA 鍵ペアの廃棄

操作	コマンド	補足
1． system view への移行する	**system-view**	―
2． ローカル RSA 鍵ペアを廃棄する	**public-key local destroy rsa**	―

🕮 **メモ：**

古い RSA 鍵ペアを完全に削除するためには装置の再起動が必要です。新しい RSA 鍵ペアを作成する場合は再起動の必要はありません。

8.9 証明書の削除

手動でリクエストされた証明書が期限切れとなったり、新しい証明をリクエストしたりする場合、現在のローカル証明書あるいは CA 証明書を削除します。

証明書を削除する手順を以下に示します。

表 8-9 証明書の削除

操作	コマンド	補足
1． system view へ移行する	**system-view**	―
2． 証明書を削除する	**pki delete-certificatedomain** *domain-name* { **ca** | **local** }	―

🕮 **メモ：**

証明書を完全に削除するためには装置の再起動が必要です。新しい証明書を取得する場合は再起動の必要はありません。

8.10 PKIの表示

表 8-10 PKI の表示

操作	コマンド	補足
証明書のコンテンツを表示する	**display pki certificate domain** *domain-name* { **ca** | **local** }	すべてのviewで実行可能です。
証明書リクエストステータスを表示する	**display pki certificate request-status**	すべてのviewで実行可能です。
CRLを表示する	**display pki crl domain** *domain-name*	すべてのviewで実行可能です。

8.11 PKI 設定例

⚠ **注意:**

SCEP アドオンは CA として Windows サーバを使用するときに必要となります。この場合、PKI ドメインの設定を行うとき、エンティティが RA から証明書をリクエストするために、ra コマンドで証明書リクエストを使用する必要があります。

8.11.1 CA からローカル証明書を手動で取得する

I. ネットワーク要件

CA サーバからローカル証明書をリクエストする AP の PKI エンティティを設定します。

AP で証明書要求を作成した後、手動で CA から証明書を取得し、AP にインポートします。

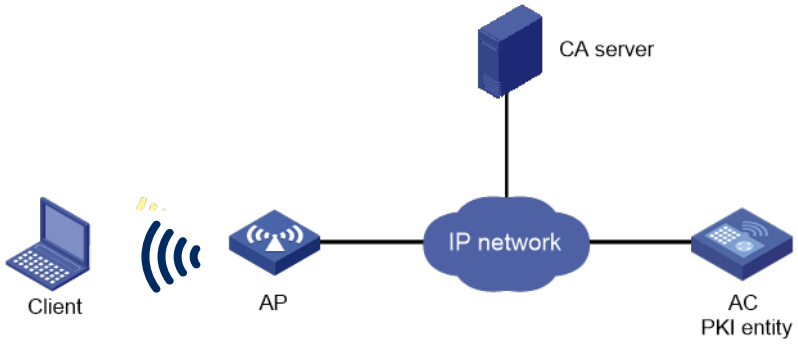


図 8-2 ネットワーク図

II. 設定手順

1) AP の設定

- エンティティ DN の設定

エンティティ名を aaa、共通名を AP と設定します。

<AP> system-view

```
[AP] pki entity aaa
[AP-pki-entity-aaa] common-name AP
[AP-pki-entity-aaa] quit
```

- PKI ドメインの設定

#PKI ドメイン torsa を作成し、PKI ドメインに移行します。

```
[AP] pki domain torsa
```

trusted CA 名 myca を設定します。

```
[AC-pki-domain-torsa] ca identifier myca
```

CA に証明書機関を設定します。

```
[AC-pki-domain-torsa] certificate request from ca
```

証明書リクエスト用のエンティティ aaa を指定します。

```
[AC-pki-domain-torsa] certificate request entity aaa
```

#RSA を使用してローカル鍵ペア hostkey を作成します。

```
[AC] public-key local create rsa name hostkey
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
It will take a few minutes.
Press CTRL+C to abort.
Input the bits in the modulus [default = 1024]:
Generating Keys...
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
++++++++++++++++++++++++++++++++++++
++++++++++++++++++++++++++++++++++++++++++++++++
++++++++++++++++++++++
```

証明書リクエスト用のローカル鍵ペアとして hostkey を指定します。

```
[AC-pki-domain-torsa] public-key rsa general name hostkey
```

- CA 証明書、ローカル証明書の取得

#CA 証明書を取得し、FTP 等を用いて AP に保存します。(詳細は省略します。)

以降の手順では、Flash 直下に cacert.pem というファイル名で保存している前提で説明します。

#CA 証明書をインポートします。

```
[AC] pki import domain torsa pem ca filename cacert.pem
```

PKCS10 のローカル証明書要求を作成します。表示された文字列を CA に提出してローカル証明書を入手します。 (詳細は省略します。)

```
[AC] pki request-certificate domain torsa pkcs10
```

```
-----BEGIN CERTIFICATE REQUEST-----
（※内容は省略します）
-----END CERTIFICATE REQUEST-----
```

入手したローカル証明書を、FTP 等を用いて AP の Flash に格納します 。(詳細は省略します。)

以降の手順では、ローカル証明書は、”localcert.pem”というファイル名で、AP の Flash 直下に保存してあるものとして説明します。

#ローカル証明書をインポートします。

```
[AP] pki import domain torsa pem local filename localcert.pem
```

2) 設定の確認

#以下のコマンドを用いて、取得されたローカル証明書の情報を表示します。

[AC] display pki certificate domain torsa local

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            48FA0FD9 00000000 000C
        Signature Algorithm: sha1WithRSAEncryption
        Issuer:
            CN=myca
        Validity
            Not Before: Nov 21 12:32:16 2007 GMT
            Not After : Nov 21 12:42:16 2008 GMT
        Subject:
            CN=AC
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00A6637A 8CDEA1AC B2E04A59 F7F6A9FE
                    5AEE52AE 14A392E4 E0E5D458 0D341113
                    0BF91E57 FA8C67AC 6CE8FEBB 5570178B
                    10242FDD D3947F5E 2DA70BD9 1FAF07E5
                    1D167CE1 FC20394F 476F5C08 C5067DF9
                    CB4D05E6 55DC11B6 9F4C014D EA600306
                    81D403CF 2D93BC5A 8AF3224D 1125E439
                    78ECEFE1 7FA9AE7B 877B50B8 3280509F
                    6B
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
            B68E4107 91D7C44C 7ABCE3BA 9BF385F8 A448F4E1
            X509v3 Authority Key Identifier:
            keyid:9D823258 EADFEFA2 4A663E75 F416B6F6 D41EE4FE

            X509v3 CRL Distribution Points:
            URI:http://l00192b/CertEnroll/CA%20server.crl
            URI:file://\\l00192b\CertEnroll\CA server.crl

            Authority Information Access:
            CA Issuers - URI:http://l00192b/CertEnroll/l00192b_CA%20server.crt
            CA Issuers - URI:file://\\l00192b\CertEnroll\l00192b_CA server.crt

            1.3.6.1.4.1.311.20.2:
                .0.I.P.S.E.C.I.n.t.e.r.m.e.d.i.a.t.e.O.f.f.l.i.n.e
    Signature Algorithm: sha1WithRSAEncryption
        81029589 7BFA1CBD 20023136 B068840B
（省略）
```

他の display コマンドー**display pki certificate domain ca** コマンドを使用できます。CA 証明書の詳細な情報を表示します。

8.12 PKIのトラブルシューティング

8.12.1 CA 証明書の取得に失敗

I. 現象

CA 証明書の取得に失敗しました。

II. 解析

以下の原因が考えられます。

- ネットワーク接続が正しくありません。たとえばネットワークケーブルの損傷あるいは切断。
- trusted CA が指定されていません。
- 証明書リクエスト用の証明書サーバの URL が不正あるいは設定されていません。
- 証明書リクエスト用の機関が設定されていません。
- デバイスのシステムクロックが CA のシステムクロックと同期していません。

III. 解決方法

- ネットワーク接続が物理的に正しいか確認します。
- 必要とされるコマンドが正しく設定されたか確認します。
- ping コマンドを用いて、RA サーバに通信可能か確認します。
- 証明書リクエスト用の機関を指定します。
- デバイスのシステムクロックを CA のシステムクロックと同期させます。

8.12.2 ローカル証明書のリクエストに失敗

I. 現象

ローカル証明書のリクエストに失敗しました。

II. 解析

以下の原因が考えられます。

- ネットワーク接続が正しくありません。たとえばネットワークケーブルの損傷あるいは切断。
- CA 証明書が取得されていません。
- 現在の鍵ペアが証明書と関連付けられていません。
- trusted CA が指定されていません。
- 証明書リクエスト用の証明書サーバの URL が不正あるいは設定されていません。
- 証明書リクエスト用の機関が設定されていません。
- エンティティ DN の必要なパラメータが設定されていません。

III. 解決方法

- ネットワーク接続が物理的に正しいか確認します。
- CA 証明書を取得します。
- 鍵ペアを再度作成します。
- trusted CA を指定します。
- ping コマンドを用いて、RA サーバに通信可能か確認します。
- 証明書リクエスト用の機関を指定します。
- エンティティ DN の必要なパラメータを設定します。

8.12.3 CRL の取得に失敗

I. 現象

CRL の取得に失敗しました。

II. 解析

以下の原因が考えられます。

- ネットワーク接続が正しくありません。たとえばネットワークケーブルの損傷あるいは切断。
- CRL の取得をする前に、CA 証明書が取得されていません。
- LDAP サーバの IP アドレスが設定されていません。
- CRL 配布 URL が設定されていません。
- LDAP サーババージョンが間違っています。

III. 解決方法

- ネットワーク接続が物理的に正しいか確認します。
- CA 証明書を取得します。
- LDAP サーバの IP アドレスを指定します。
- CRL 配布 URL を指定します。
- LDAP バージョンの再設定を行います。

目次

このセクションのページは**9-x-x** です。

9章 SSL設定 9-1
9.1 SSL概要 9-1
9.1.1 SSLセキュリティメカニズム 9-1
9.1.2 SSLプロトコルスタック 9-2
9.2 SSL設定作業リスト 9-2
9.3 SSLサーバポリシーの設定 9-3
9.3.1 設定必要条件 9-3
9.3.2 設定手順 9-3
9.4 SSLサーバのSSLプロトコルバージョンの無効化 9-4
9.5 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 9-4
9.6 SSLクライアントポリシーの設定 9-4
9.6.1 設定必要条件 9-5
9.6.2 設定手順 9-5
9.7 SSLの表示 9-5

9章 SSL 設定

9.1 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。

9.1.1 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 9-1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。

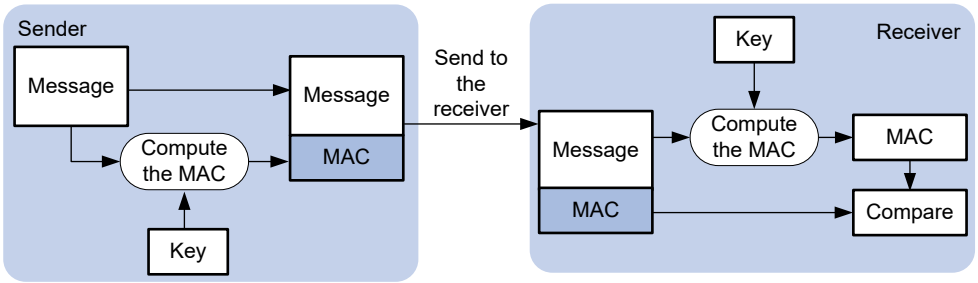


図 9-1 MAC アルゴリズムによるメッセージの完全性の検証

9.1.2 SSL プロトコルスタック

図 9-2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。

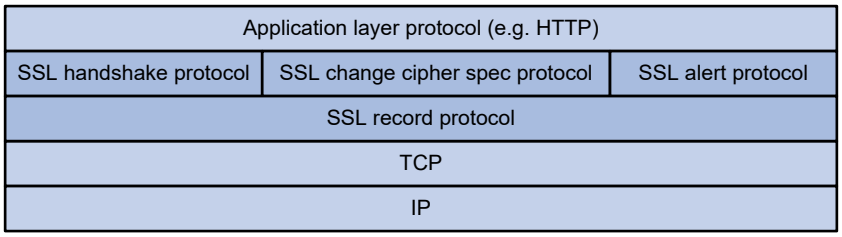


図 9-2 SSL プロトコルスタック

- **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。

9.2 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クライアントポリシーの設定	必須設定項目

作業	補足
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

9.3 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。

9.3.1 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。

9.3.2 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*	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。
- SSL は主に SSL3.0、TLS1.0、1.1、1.2 のバージョンを使用します。TLS1.0、1.1、1.2 は SSL3.1 に対応します。装置が SSL サーバとして動作するとき、SSL3.0 や TLS1.0、1.1、1.2 で動作するクライアントと通信することができます。そしてクライアントからの Hello パケットを識別することで、クライアントが SSL3.0、TLS1.0、1.1、1.2 をサポートすることを識別します。サーバは、クライアントに SSL3.0 あるいは TLS1.0、1.1、1.2 を使用して通信するということを通知します。

9.4 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**	―
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** } **disable**	デフォルト：SSL3.0、TLS1.0、TLS1.1、TLS1.2が有効

9.5 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**	―
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*	―
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

9.6 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。

9.6.1 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。

9.6.2 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**	ー
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*	ー
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** }	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

9.7 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 **9-x-x** です。

10 章 ユーザアイソレーション 10-1
10.1 概要 10-1
10.2 SSID ベースユーザアイソレーション 10-1
10.3 VLAN ベースユーザアイソレーション 10-2
10.3.1 無線のユーザから受信したパケットの扱い 10-2
10.3.2 有線のユーザから受信したパケットの扱い 10-3
10.4 SSID ベースのユーザアイソレーションの設定 10-4
10.5 VLAN ベースのユーザアイソレーションの設定 10-4
10.6 ユーザアイソレーションの表示と維持 10-5
10.7 ユーザアイソレーションの設定例 10-5
10.7.1 SSID ベースのユーザアイソレーションの設定例 10-5
10.7.2 VLAN ベースのユーザアイソレーションの設定例 10-6

10章 ユーザアイソレーション

Anchor-AC でのユーザアイソレーションについては *QX-W2120AC アクセスコントローラ オペレーションマニュアル*を参照してください。

10.1 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。

10.2 SSIDベースユーザアイソレーション

SSID ベースのユーザアイソレーションを有効にすると、AP は同一 SSID に所属するクライアントの通信を隔離します。

図 10-1 のように、クライアント 1～m が AP 配下の同一 SSID に所属している状態で、AP で SSID ベースのユーザアイソレーションを有効にします。

- クライアント 1 が VLAN100 でブロードキャストもしくはマルチキャストを送付した場合、AP は無線ネットワーク上の別クライアントへのパケット転送は行わずに、有線ポートからスイッチにのみパケット転送を行います。
- クライアント 1 が VLAN100 でクライアント 2 宛のユニキャストを送付した場合、AP はクライアント 2 への転送を行わずにパケットを廃棄します。

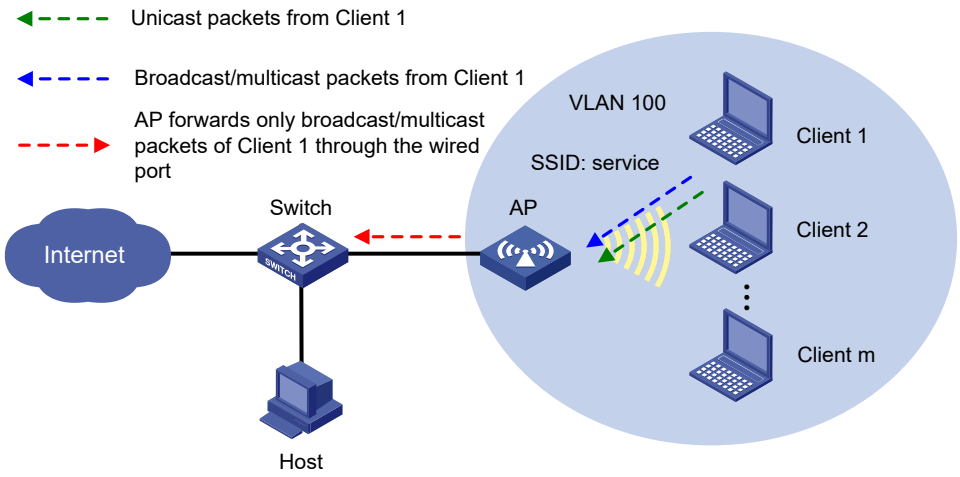


図 10-1 パケット転送例

10.3 VLANベースユーザアイソレーション

VLAN ベースのユーザアイソレーションを有効にすると、AP は同一 VLAN のパケットを以下の通り扱います。

- 受信したユニキャストパケットは、廃棄します。
- 受信したブロードキャストもしくはマルチキャストは、ローカルでない有線ネットワークの先にいる同一 VLAN の有線/無線ユーザに転送します。ローカルの無線ユーザにはパケット転送しません。

10.3.1 無線のユーザから受信したパケットの扱い

図 10-2 のように、AP1 で VLAN100 のユーザアイソレーションを有効にします。

- クライアント 1 が VLAN100 でブロードキャストもしくはマルチキャスト送付します。
  - AP1 がパケットを受け取ると、同パケットを有線ネットワークの VLAN100 を通じてサーバ / AP2 / ホストに転送します。しかし、AP1 は同パケットをクライアント 2 には転送しません。
  - AP2 がパケットを受け取ると、同パケットをクライアント 3 に転送します。これは、AP2 においてユーザアイソレーションが有効になっていないためです。
- クライアント 1 が VLAN100 でクライアント 3 宛のユニキャストを送付します。
  - AP1 がパケットを受け取ると、AP2 への転送を行わずにパケットを廃棄します。

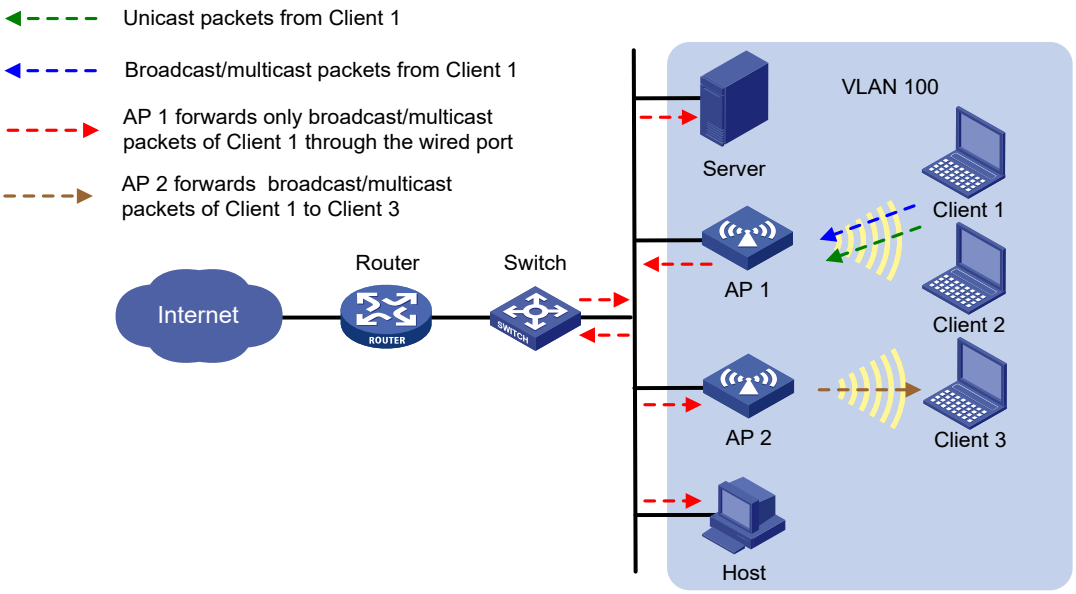


図 10-2 パケット転送例

10.3.2 有線のユーザから受信したパケットの扱い

図 10-3 のように、AP1 で VLAN100 のユーザアイソレーションを有効にします。

- ホストが VLAN100 でブロードキャストもしくはマルチキャスト送付すると、AP1 と AP2 はパケットを受け取ります。
  - AP1 がパケットを受け取ると、クライアント 1/クライアント 2 への転送を行わずにパケットを廃棄します。
  - AP2 がパケットを受け取ると、同パケットをクライアント 3 に転送します。これは、AP2 においてユーザアイソレーションが有効になっていないためです。
- ホストが VLAN100 でクライアント 1 宛のユニキャストを送付します。
  - AP1 がパケットを受け取ると、クライアント 1 への転送を行わずにパケットを廃棄します。

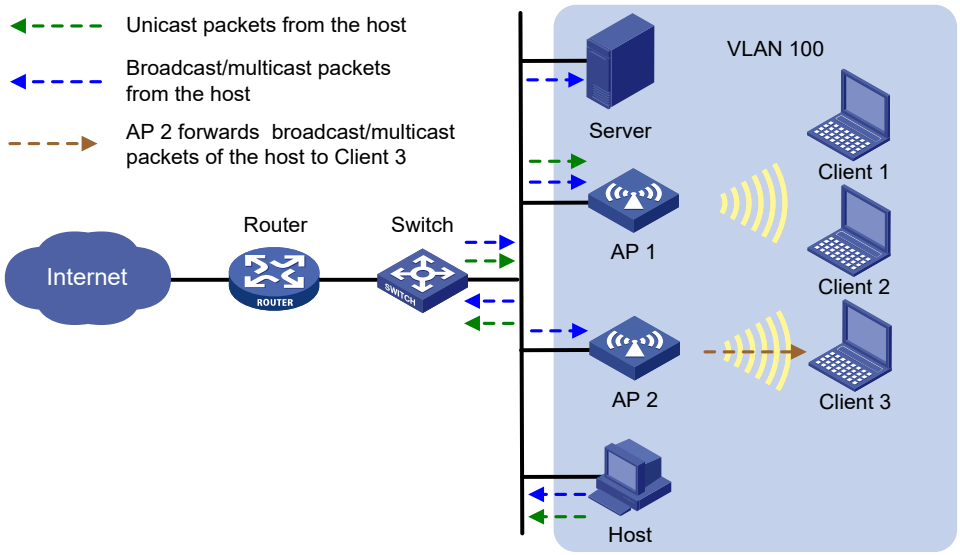


図 10-3 パケット転送例

10.4 SSIDベースのユーザアイソレーションの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. service template view に移行する	**wlan service-template** *service-template-name*	—
3. SSID ベースの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

10.5 VLANベースのユーザアイソレーションの設定

VLAN ベースのユーザアイソレーション時にユーザの外部ネットワークへのアクセスを有効にするためには、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 ゲートウェイの MAC アドレスを許可 MAC アドレスのリストに登録する必要あります。

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 リスト内で通信を許可する MAC リストを設定する	**user-isolation vlan** *vlan-list* **permit-mac** *mac-list*	デフォルト：許可されたMAC リスト無し
3. VLAN リストのユーザアイソレーションを有効化する	**user-isolation vlan** *vlan-list* **enable** [**permit-unicast**]	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）VLAN ベースのアイソレーション有効時にブロードキャストおよびマルチキャストの転送を許可する	**user-isolation permit-broadcast**	デフォルト：無効

10.6 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。

User view で reset コマンドを実行できます。

操作	コマンド
ユーザアイソレーションの統計を表示する	**display user-isolation statistics** [**vlan** *vlan-id*]
ユーザアイソレーションの統計をリセットする	**reset user-isolation statistics** [**vlan** *vlan-id*]

10.7 ユーザアイソレーションの設定例

10.7.1 SSID ベースのユーザアイソレーションの設定例

I. ネットワーク要件

図 10-4 に示すように、クライアント 1、クライアント 2 がインターネットアクセスのために同一の SSID を使用します。

クライアントにインターネットアクセスを提供しながら、レイヤ 2 で互いのクライアントを分離するよう、AP でユーザアイソレーションを設定します。

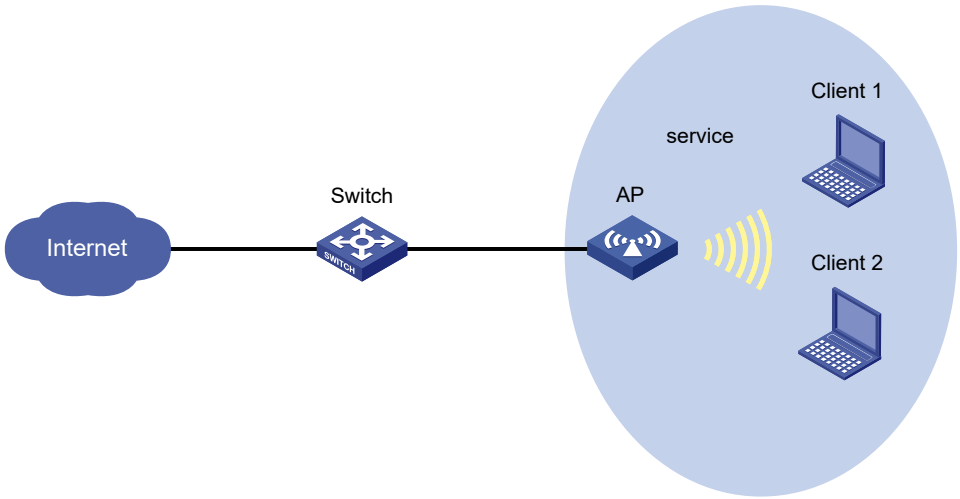


図 10-4 ネットワーク図

II. 設定手順

クライアント 1 とクライアント 2 でサービステンプレート service を作成し、インターネットアクセスの接続を確立します。詳細はオペレーションマニュアルのセクション 2 *WLAN* “*WLAN アクセスの設定*”を参照してください。

サービステンプレート service で、ユーザアイソレーションを有効化します。

```
<AP> system-view
[AP] wlan service-template service
[AP-wlan-st-service] user-isolation enable
[AP-wlan-st-service] quit
```

10.7.2 VLAN ベースのユーザアイソレーションの設定例

I. ネットワーク要件

図 10-5 に示すように、ルータを VLAN100 のデバイス群のゲートウェイとして動作させます。ゲートウェイの MAC アドレスは 000f-e202-7788 です。

AP に VLAN100 ベースのユーザアイソレーション設定を行います。クライアント 1/クライアント 2/ホスト/サーバがインターネットアクセス出来るように、ゲートウェイの MAC アドレスを許可 MAC アドレスリストに登録します。

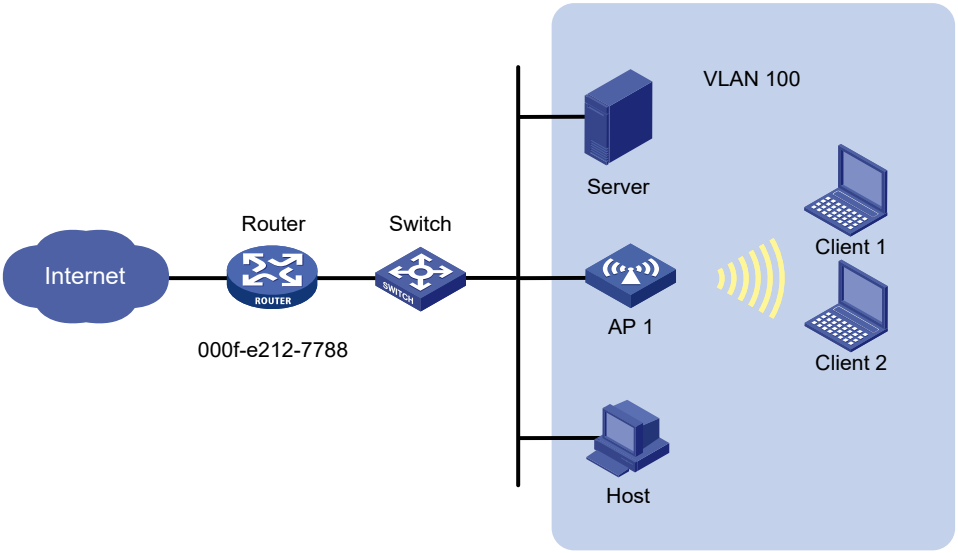


図 10-5 ネットワーク図

II. 設定手順

クライアント 1 とクライアント 2 でインターネットアクセスが出来るように設定します。詳細はオペレーションマニュアルのセクション 2 *WLAN* “*WLAN アクセスの設定*”を参照してください。

ゲートウェイの MAC アドレスを許可 MAC リストに登録します。

```
<AP> system-view
[AP] user-isolation vlan 100 permit-mac 000f-e212-7788
```

VLAN100 について、VLAN ベースのユーザアイソレーションを有効にします。

```
[AP] user-isolation vlan 100 enable
```

目次

このセクションのページは **9-x-x** です。

11 章 ユーザプロファイル..... 11-1
11.1 概要..... 11-1
11.2 ユーザプロファイルの前提条件..... 11-1
11.3 ユーザプロファイルの設定..... 11-1
11.4 ユーザプロファイルの表示とメンテナンスコマンド..... 11-2

11章 ユーザプロファイル

11.1 概要

ユーザプロファイルは、ユーザまたはユーザのクラスに対して QoS ポリシーなどのパラメータを定義します。ユーザプロファイルは、ユーザが別のインタフェースのネットワークに接続したときに再利用できます。

ユーザプロファイルアプリケーションでは、ユーザごとに柔軟なトラフィックポリシングが可能です。ユーザが認証に合格するたびに、サーバはユーザに指定さ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。デバイスは、ユーザプロファイルのパラメータをユーザに適用します。

デバイスは認証サーバと連携して、リモートユーザ認証を実行します。認証サーバ上のユーザに関連付けられたユーザプロファイルを指定する必要があります。

ユーザは、オンラインになった後、ユーザプロファイル関連付けの対象となります。ユーザプロファイルは、オンラインユーザのアクセス動作を制限します。ユーザがオンラインでない場合、ユーザプロファイルの設定は有効になりません。

ユーザプロファイルは、次の目的で使用できます。

- ユーザごとのシステムリソースの割り当て: インタフェースベースのトラフィックポリシングでは、ユーザグループが使用できる帯域幅の合計量が制限されます。ただし、ユーザプロファイルベースのトラフィックポリシングでは、1 人のユーザが使用できる帯域幅の量を制限できます。
- システムリソースへのアクセスを柔軟に制限する: インタフェースベースのトラフィックポリシングでは、ユーザが別のインタフェースでオンラインになった場合、トラフィックポリシング設定を削除し、新しいインタフェーストラフィックポリシングを再設定する必要があります。ユーザプロファイルベースのトラフィックポリシングの場合、トラフィックポリシング設定は、ユーザがオンラインになったときに自動的にユーザに発行されます。ユーザがオフラインになると、トラフィックポリシング設定は自動的に削除されます。

11.2 ユーザプロファイルの前提条件

ユーザプロファイルは認証方式で動作します。ユーザプロファイルの認証を設定する必要があります。サポートされている認証方式の詳細については、関連する認証モジュールの設定ガイドを参照してください。

11.3 ユーザプロファイルの設定

以下にユーザ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**	―
2. ユーザプロファイルを作成し、user profile view に移行する	**user-profile** *profile-name*	設定なし

11.4 ユーザプロファイルの表示とメンテナンスコマンド

すべての View で display コマンドを実行できます。

操作	コマンド	補足
指定したユーザプロファイルまたはすべてのユーザプロファイルの設定およびオンラインユーザ情報を表示します。	**display user-profile [name** *profile-name* **]**	–

QX-W1200 シリーズ アクセスポイント

オペレーションマニュアル

10. 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-システムの保守とデバッグ

02-NQA

03-NTP

04-SNMP

05-NETCONF

06-プロセスモニタリングとメンテナンス

07-Information Center

08-NetMeister

09-パケットキャプチャ

目次

このセクションのページは **10-x-x** です。

1 章 システムの保守とデバッグ 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
1.3 iPerf 1-6
1.3.2 iPerf クライアントとしてのテスト実行 1-7
1.3.3 iPerf サーバの有効化 1-7
1.3.4 iPerf 設定例 1-7
1.4 システムのデバッグ 1-8
1.4.1 スイッチのデバッグ情報の制御 1-8
1.4.2 システムデバッグの設定 1-9

1章 システムの保守とデバッグ

この章は ping、tracert、iperf を使用したシステムのデバッグ情報について記載します。

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	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。 • 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*	低速ネットワークで**ping**コマンドを使用するとき、タイムアウトタイマの値を大きな値に設定してください。（コマンドの**-t**キーワードで示されます。）

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 C 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 C のルートについての詳細な情報を取得します。

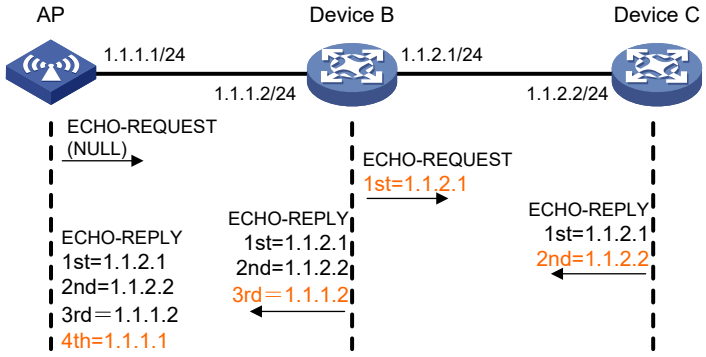


図 1-1 ネットワーク図

II. 設定手順

AP で **ping** コマンドを使用し、Device C と通信可能かどうか確認します。

```
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。

- AP が Device C に 5 つの ICMP パケットを送信､AP 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。

AP から Device C の詳細なルート情報を取得します。

```
<AP> ping -r 1.1.2.2
Ping 1.1.2.2 (1.1.2.2): 56 data bytes, press CTRL_C to break
56 bytes from 1.1.2.2: icmp_seq=0 ttl=254 time=4.685 ms
RR:     1.1.2.1
        1.1.2.2
        1.1.1.2
        1.1.1.1
56 bytes from 1.1.2.2: icmp_seq=1 ttl=254 time=4.834 ms  (same route)
56 bytes from 1.1.2.2: icmp_seq=2 ttl=254 time=4.770 ms  (same route)
56 bytes from 1.1.2.2: icmp_seq=3 ttl=254 time=4.812 ms  (same route)
56 bytes from 1.1.2.2: icmp_seq=4 ttl=254 time=4.704 ms  (same route)

--- Ping statistics for 1.1.2.2 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 4.685/4.761/4.834/0.058 ms
```

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（AP）は RR オプションを空で ICMP エコーリクエストを宛先（Device C）に対して送信します。
2) 中間デバイス（Device B）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 AP～Device C 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。

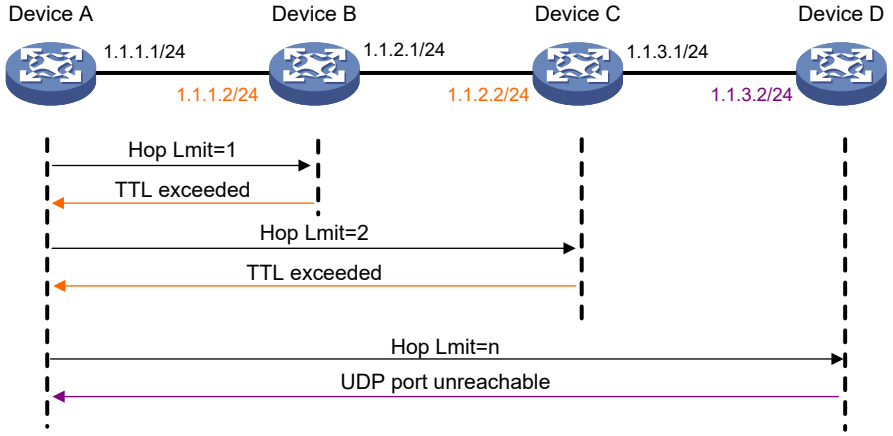


図 1-2 Tracert の動作

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。このコマンドの詳細は、コマンドマニュアルのセクション 5 *IP サービス "IP パフォーマンスの最適化"*を参照してください。
- 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。このコマンドの詳細は、コマンドマニュアルのセクション 5 *IP サービス "IP パフォーマンスの最適化"*を参照してください。

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、AP は Device B への Telnet が失敗しています。

AP 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) AP でスタティックルートを設定します。

```
<AP> system-view
[AP] ip route-static 0.0.0.0 0.0.0.0 1.1.1.2
[AP] quit
```

3) **ping** コマンドを使用して AP と Device B 間の接続性を確認します。

```
<AP> ping 1.1.2.2
Ping 1.1.2.2(1.1.2.2): 56 -data bytes, press CTRL_C to break
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、AP 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
```

AP で **tracert** コマンドを実行します。

```
<AP> tracert 1.1.2.2
traceroute to 1.1.2.2 (1.1.2.2) 30 hops at most,40 bytes each packet, press CTRL_C
to break
 1  1.1.1.2 (1.1.1.2) 1 ms 2 ms 1 ms
 2  * * *
 3  * * *
 4  * * *
 5
<AP>
```

出力は、AP と Device A は互いに通信できますが、AP 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 AP 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 AP 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 AP と Device B のルートがあるか確認します。

1.3 iPerf

🕮 **メモ：**

本機能はソフトウェアバージョン 7.5.142a を含む以降のソフトウェアからサポートしています。

iPerf 機能は、ネットワークパフォーマンスの品質を総合的に評価するために設計されたネットワークパフォーマンステストツールです。本機能は、iPerfv3 を用いて従来の TCP ネットワーク通信の最大速度をテストするだけでなく、UDP プロトコルのテスト機能も提供します。iPerf を使用することで、ネットワーク帯域幅、データ伝送遅延時間、ネットワークジッタ、パケット損失率などのパフォーマンス指標を測定でき、ネットワークの状態を把握することができます。

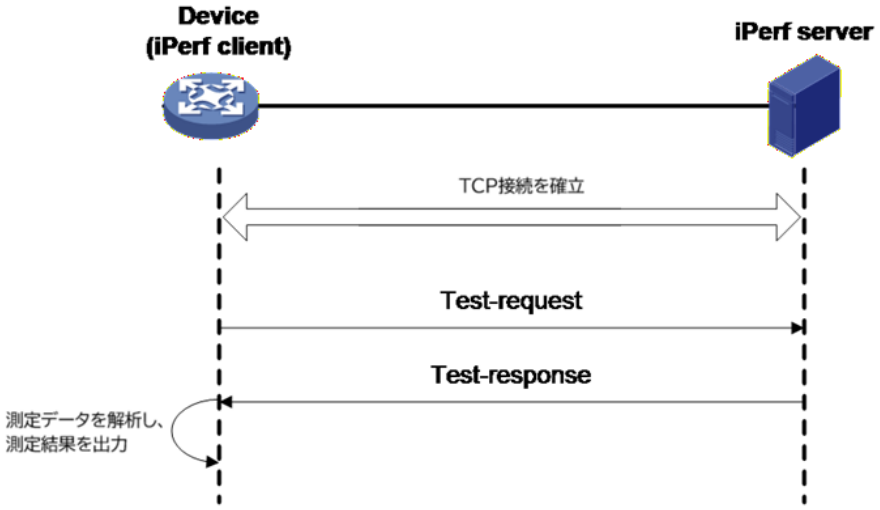


図 1-4 iPerf の動作

iPerf はクライアント／サーバモデルを使用してネットワーク性能テストを実施します。テストを行う前に、被測定ホスト上で iPerf サーバを起動し、装置は iPerf クライアントとして動作する必要があります。装置と iPerf サーバ間は TCP プロトコルで通信を行います。

以下に iPerf の動作原理を示します：

1)　デバイス（クライアント）がテスト要求を送信

デバイス上で iPerf のテストコマンドを実行すると、デバイスは iPerf クライアントとして、指定された iPerf サーバに対してテスト要求を送信し、TCP 接続の確立を要求します。

2)　サーバが要求を受信し応答

iPerf サーバはクライアントからのテスト要求を受信すると、TCP 接続を確立し、クライアントへ応答メッセージを送信します。

3)　テストデータの転送

TCP 接続が確立されると、iPerf はデータ転送テストを開始します。クライアントはバイトストリームデータを送信し、TCP のスループットを測定します。デバイスは 1 秒単位

で平均帯域を測定し、これを 10 回連続で実施します。そして各回における送信方向のバイト数、平均帯域、さらに 10 秒間の送信方向平均帯域および受信方向平均帯域を表示します。

4)　テスト結果の出力

テスト終了後、デ iPerf クライアントは結果を集計し、表示情報としてユーザに出力します。ユーザは出力結果からスループットなどの性能指標を取得し、ネットワーク性能の評価および最適化に活用できます。

総じて、iPerf はクライアント／サーバモデルによるデータ転送と測定を通じて結果を出力し、ネットワーク性能の測定や問題の特定を支援します。

1.3.2 iPerf クライアントとしてのテスト実行

操作	コマンド	補足
装置から iPerf サーバまでのネットワークをテストする。	● IPv4ネットワーク： **iperf** [**host** *host* [**port** *port-number*]] [**bidirection** | **duration** *seconds* | **flow-count** *count* | **interface** *interface-type interface-number* | [**tcp** [**window** *window-size*] | **udp** [**bandwidth** *bandwidth*]]]	テスト結果はiPerfクライアント側のみ表示されます。

1.3.3 iPerf 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**	ー
2． iPerf サーバ機能を有効にする。	● IPv4ネットワーク： **iperf server ip** *ip-address* [**port** *port-number*]	デフォルト：無効

1.3.4 iPerf 設定例

I. ネットワーク要件

図 1-5 に示すように、ネットワークの先にある iPerf サーバに対し、帯域テストを行います。装置の IP アドレスやルーティングはあらかじめ設定され、各デバイス間の通信経路は到達可能な状態とします。（詳細は省略します。）

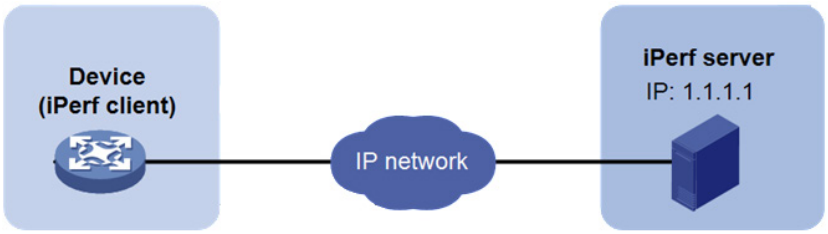


図 1-5 ネットワーク図

II. 設定手順

iPerf サーバ側で iPerf サービスを起動します。（詳細は省略します。）

#AP(iPerf クライアント)から iPerf サーバまでのネットワーク帯域をテストします。

```
<AP> iperf host 1.1.1.1
Press CTRL_C to break
Connecting to host 1.1.1.1, port 5201
Local 1.1.1.2 port 64065 connected to 1.1.1.1 port 5201
Interval(sec)    Transfer      Bitrate
 0.00-1.00       12.6 MBytes    106 Mbps
 1.00-2.00       16.1 MBytes    135 Mbps
 2.00-3.00       11.6 MBytes   97.0 Mbps
 3.00-4.00       8.92 MBytes   74.8 Mbps
 4.00-5.00       11.4 MBytes   95.8 Mbps
 5.00-6.00       13.7 MBytes    115 Mbps
 6.00-7.00       9.32 MBytes   78.2 Mbps
 7.00-8.00       13.6 MBytes    114 Mbps
 8.00-9.00       11.5 MBytes   96.2 Mbps
 9.00-10.00      11.4 MBytes   95.5 Mbps
Summary:
Interval(sec)     Transfer      Bitrate        Direction
 0.00-10.00        120 MBytes    101 Mbps      Outbound
 0.00-10.00        120 MBytes    101 Mbps      Inbound
```

上記の表示結果から、直近 10 秒間において、デバイスから iPerf サーバまでのスループットは 120 MBytes、通信速度は 101 Mbps であることが分かります。

1.4 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。

1.4.1 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。これらのコマンドの詳細は、コマンドマニュアルのセクション 10 *システム管理* "*Information center*"を参照してください。

図 1-6 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。詳細は、オペレーションマニュアルのセクション 10 *システム管理* "*Information center*"を参照してください。

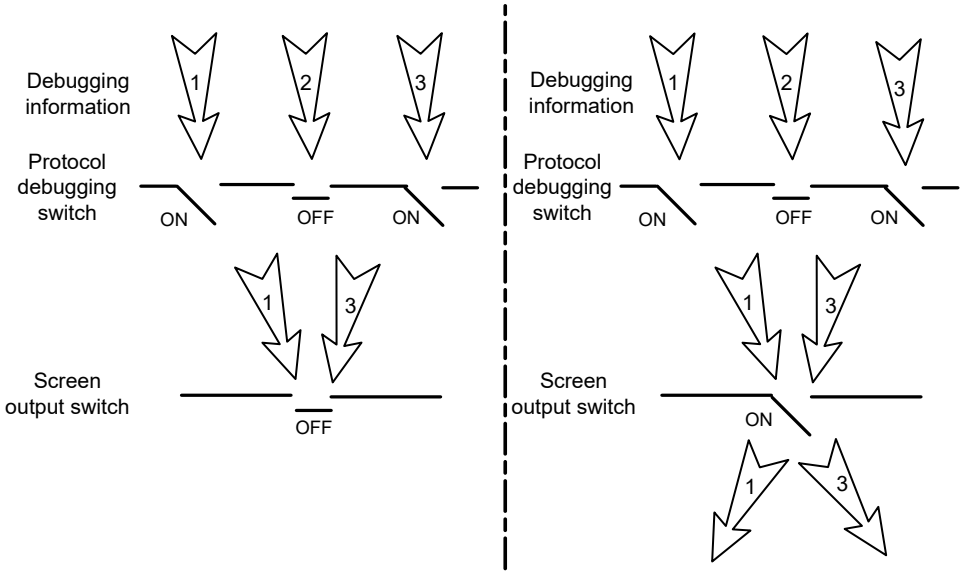


図 1-6 モジュールデバッグスイッチと画面出力スイッチの関係

1.4.2 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 **10-x-x** です。

2 章 NQA 2-1
2.1 概要 2-1
2.1.1 NQA のテストタイプ 2-1
2.1.2 しきい値監視機能 2-2
2.2 NQA 設定作業リスト 2-2
2.3 NQA サーバの設定 2-2
2.4 NQA クライアントの有効化 2-3
2.5 NQA クライアントの NQA テストの設定 2-4
2.5.1 NQA テストの設定作業リスト 2-4
2.5.2 ICMP エコーテストの設定 2-4
2.5.3 DHCP テストの設定 2-5
2.5.4 DNS テストの設定 2-6
2.5.5 FTP テストの設定 2-7
2.5.6 HTTP テストの設定 2-8
2.5.7 UDP ジッタテストの設定 2-9
2.5.8 SNMP テストの設定 2-10
2.5.9 TCP テストの設定 2-11
2.5.10 UDP エコーテストの設定 2-12
2.5.11 音声テストの設定 2-13
2.5.12 DLSw テストの設定 2-15
2.5.13 NQA テストのオプションパラメータの設定 2-16
2.5.14 しきい値監視機能の設定 2-17
2.5.15 NQA 統計情報収集機能の設定 2-19
2.5.16 NQA 履歴記録保存の設定 2-20
2.5.17 NQA クライアントにおける NQA テストのスケジューリング 2-21
2.6 NQA の表示と維持 2-21
2.7 NQA 設定例 2-21
2.7.1 ICMP エコーテスト設定例 2-21
2.7.2 DHCP テスト設定例 2-23
2.7.3 DNS テスト設定例 2-25
2.7.4 FTP テスト設定例 2-26
2.7.5 HTTP テスト設定例 2-27
2.7.6 UDP ジッタテスト設定例 2-29
2.7.7 SNMP テスト設定例 2-31
2.7.8 TCP テスト設定例 2-33
2.7.9 UDP エコーテスト設定例 2-34
2.7.10 音声テスト設定例 2-36
2.7.11 DLSw テスト設定例 2-38

2章 NQA

2.1 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 2-1 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 2-1 ネットワーク図

2.1.1 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。

2.1.2 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 2-1 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 2-1 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
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）（詳細はオペレーションマニュアルのセクション10 *システム管理"NQA"の"音声テストの設定"*を参照してください。）	音声テスト
MOS（Mean Opinion Scores）（詳細はオペレーションマニュアルのセクション10 *システム管理"NQA"の"音声テストの設定"*を参照してください。）	音声テスト

2.2 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

2.3 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

2.4 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。

2.5 NQAクライアントのNQAテストの設定

2.5.1 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 • 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 • 音声テストの設定 • DLSwテストの設定
（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

2.5.2 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**	―
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	**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

操作	コマンド	補足
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 IP 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	**next-hop ip** *ip-address*	デフォルト：設定なし

2.5.3 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**	―
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.　DHCP タイプを指定し、その view に移行する	**type dhcp**	―

操作	コマンド	補足
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。 詳細はオペレーションマニュアルのセクション5 *IPサービス* "*DHCP リレー*"を参照してください。

2.5.4 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

2.5.5 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。

2.5.6 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

2.5.7 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、コマンドマニュアルのセクション 10 *システム管理* "*NQA*"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	**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 パケットの送信元ポート番号を指定する	**source port** *port-number*	デフォルト：設定なし
8.　（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
9.　（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）
10.　（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
11.　（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
12.　（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。

2.5.8 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**	―
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**	―
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。

2.5.9 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、オペレーションマニュアルのセクション 10 *システム管理* "*NQA*"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**	―
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**	―
4． TCP 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	**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。

2.5.10 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。UDP リスニングサービスの詳細は、コマンドマニュアルのセクション 10 *システム管理* "*NQA*"の"*NQA サーバの設定*"を参照してください。

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	**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：0001020304050607080 9（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	**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。

2.5.11 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、コマンドマニュアルのセクション 10 *システム管理*"*NQA*"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**	―
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**	―
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

操作	コマンド	補足
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）
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。

2.5.12 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

操作	コマンド	補足
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。

2.5.13 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

操作	コマンド	補足
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。

2.5.14 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、コマンドマニュアルのセクション 10 *システム管理* "*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**	―
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 operation view に移行する	**type** { **dhcp** | **dlsw** | **dns** | **ftp** | **http** | **icmp-echo** | **snmp** | **tcp** | **udp-echo** | **udp-jitter** | **voice** }	―
4. 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** { **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。
5. しきい値監視機能を設定する	• 故障回数を監視する（UDPジッタテストと音声テストは未サポート）： **reaction** *item-number* **checked-element probe-fail threshold-type** { **accumulate** *accumulate-occurrences* | **consecutive** *consecutive-occurrences* } [**action-type none**] • オペレーション期間を監視する（UDPジッタテストと音声テストでは未サポート） **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** }] • 往復時間を監視する（UDPジッタテストと音声テストでのみサポート） **reaction** *item-number* **checked-element rtt threshold-type** { **accumulate** *accumulate-occurrences* | **average** } **threshold-value** *upper-threshold lower-threshold* [**action-type** { **none** | **trap-only** }]	―

操作	コマンド	補足
	• パケットロスを監視する（UDPジッタテストと音声テストでのみサポート） **reaction** *item-number* **checked-element packet-loss threshold-type accumulate** *accumulate-occurrences* [**action-type** { **none** | **trap-only** }] • 一方向ジッタを監視する（UDPジッタテストと音声テストでのみサポート） **reaction** *item-number* **checked-element** { **jitter-ds** | **jitter-sd** } **threshold-type** { **accumulate** *accumulate-occurrences* | **average** } **threshold-value** *upper-threshold lower-threshold* [**action-type** { **none** | **trap-only** }] • 一方向遅延を監視する（UDPジッタテストと音声テストでのみサポート） **reaction** *item-number* **checked-element** { **owd-ds** | **owd-sd** } **threshold-value** *upper-threshold lower-threshold* • ICPIF値を監視する（音声テストでのみサポート） **reaction** *item-number* **checked-element icpif threshold-value** *upper-threshold lower-threshold* [**action-type** { **none** | **trap-only** }] • MOS 値を監視する（音声テストでのみサポート） **reaction** *item-number* **checked-element mos threshold-value** *upper-threshold lower-threshold* [**action-type** { **none** | **trap-only** }]	–

2.5.15 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。
6. （オプション設定項目）統計情報グループの保持時間を指定する	**statistics hold-time** *hold-time*	デフォルト：120分 保持時間が終了したとき、統計グループは削除されます。

2.5.16 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**	―
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** }	UDPジッタテストと音声テストは無効です。
4. 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
5. （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。
6. （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。
7. （オプション設定項目）履歴記録を表示する	**display nqa history**	―

2.5.17 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**]

2.6 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**

2.7 NQA設定例

2.7.1 ICMP エコーテスト設定例

I. ネットワーク要件

図 2-2 に示すように、AP から Device B を通して Device A へのラウンドトリップ時間をテストするため、NQA クライアントから ICMP エコーテストを設定します。AP のネクストホップは Device B です。

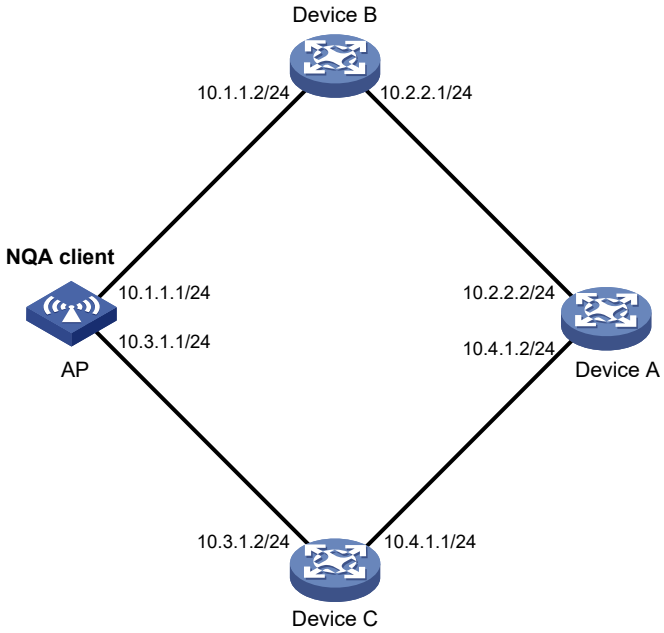


図 2-2 ネットワーク図

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。）

Device が互いに通信できるようにスタティックルートあるい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。

```
<AP> system-view
[AP] nqa entry admin test1
[AP-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。

```
[AP-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。

```
[AP-nqa-admin-test1-icmp-echo] next-hop ip 10.1.1.2
```

ICMP エコーテストの検査回数を 10 回実行します。

```
[AP-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。

```
[AP-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。

```
[AP-nqa-admin-test1-icmp-echo] frequency 5000
```

NQA 履歴記録の保存を有効にします。

```
[AP-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。

```
[AP-nqa-admin-test1-icmp-echo] history-record number 10
[AP-nqa-admin-test1-icmp-echo] quit
```

ICMP エコーテストを開始します。

```
[AP] 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。

```
[AP] undo nqa schedule admin test1
```

ICMP エコーテストの最新の結果を表示します。

```
[AP] 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。

```
[AP] 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
```

出力では、Device A からのパケットが Device C を通して Device B に送信できる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。

2.7.2 DHCP テスト設定例

I. ネットワーク要件

図 2-3 に示すように、AP が DHCP サーバ（Switch）から IP アドレスを取得する時間をテストするため DHCP テストを設定します。

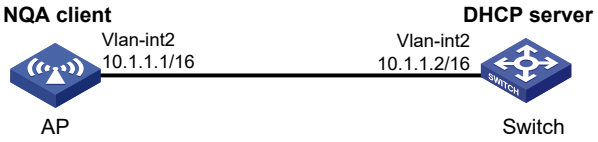


図 2-3 ネットワーク図

II. 設定手順

DHCP テストを作成します。

```
<AP> system-view
[AP] nqa entry admin test1
[AP-nqa-admin-test1] type dhcp
```

宛先アドレスとして DHCP サーバの IP アドレス 10.1.1.2 を指定します。

```
[AP-nqa-admin-test1-dhcp] destination ip 10.1.1.2
```

履歴記録を保存するように設定します。

```
[AP-nqa-admin-test1-dhcp] history-record enable
[AP-nqa-admin-test1-dhcp] quit
```

DHCP テストを開始します。

```
[AP] nqa schedule admin test1 start-time now lifetime forever
```

DHCP テストを一定の期間実行したのち、テストを停止します。

```
[AP] undo nqa schedule admin test1
```

DHCP テストの最新の結果を表示します。

```
[AP] 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: 512/512/512
    Square-Sum of round trip time: 262144
    Last succeeded probe time: 2011-11-22 09:56:03.2
  Extended results:
    Packet loss ratio: 0%
    Failures due to timeout: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
```

DHCP テストの履歴記録を表示します。

```
[AP] display nqa history admin test1
NQA entry (admin admin, tag test1) history records:
  Index      Response     Status           Time
  1          512          Succeeded        2011-11-22 09:56:03.2
```

出力では、AP が DHCP サーバから IP アドレスを取得するのに 512 ミリ秒かかることを示します。

2.7.3 DNS テスト設定例

I. ネットワーク要件

図 2-4 に示すように、AP が DHCP サーバから IP アドレスを取得するため DNS 解決時間の測定を行う DNS テストを設定します。



図 2-4 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あるい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。）

DNS テストを作成します。

```
<AP> system-view
[AP] nqa entry admin test1
[AP-nqa-admin-test1] type dns
```

宛先アドレスとして DNS サーバの IP アドレス 10.2.2.2 を指定します。

```
[AP-nqa-admin-test1-dns] destination ip 10.2.2.2
```

host.com のドメイン名に変換されるように指定します。

```
[AP-nqa-admin-test1-dns] resolve-target host.com
```

履歴記録を保存するように設定します。

```
[AP-nqa-admin-test1-dns] history-record enable
[AP-nqa-admin-test1-dns] quit
```

DNS テストを開始します。

```
[AP] nqa schedule admin test1 start-time now lifetime forever
```

DNS テストを一定の期間実行したのち、テストを停止します。

```
[AP] undo nqa schedule admin test1
```

DNS テストの最新の結果を表示します。

```
[AP] 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: 62/62/62
```

```
    Square-Sum of round trip time: 3844
    Last succeeded probe time: 2011-11-10 10:49:37.3
  Extended results:
    Packet loss ratio: 0%
    Failures due to timeout: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
```

DNS テストの履歴記録を表示します。

```
[AP] display nqa history admin test1
NQA entry (admin admin, tag test) history records:
  Index      Response     Status           Time
  1          62           Succeeded        2011-11-10 10:49:37.3
```

出力では、AP がドメイン名 host.com を IP アドレスに変換するのに 62 ミリ秒かかることを示します。

2.7.4 FTP テスト設定例

I. ネットワーク要件

図 2-5 に示すように、AP 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 2-5 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あるい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。

```
<AP> system-view
[AP] nqa entry admin test1
[AP-nqa-admin-test1] type ftp
```

FTP サーバの URL を指定します。

```
[AP-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。

```
[AP-nqa-admin-test1-ftp] source ip 10.1.1.1
```

装置が 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。

```
[AP-nqa-admin-test1-ftp] operation put
[AP-nqa-admin-test1-ftp] filename config.txt
```

FTP テストのユーザ名 admin を指定します。

```
[AP-nqa-admin-test1-ftp] username admin
```

FTP テストのパスワード systemtest を指定します。

```
[AP-nqa-admin-test1-ftp] password simple systemtest
```

履歴記録を保存するように設定します。

```
[AP-nqa-admin-test1-ftp] history-record enable
[AP-nqa-admin-test1-ftp] quit
```

FTP テストを開始します。

```
[AP] 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。

```
[AP] undo nqa schedule admin test1
```

FTP テストの最新の結果を表示します。

```
[AP] 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。

```
[AP] 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
```

出力では、AP が FTP サーバにファイルをアップロードするのに 173 ミリ秒かかることを示しています。

2.7.5 HTTP テスト設定例

I. ネットワーク要件

図 2-6 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 2-6 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あるい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。

```
<AP> system-view
[AP] nqa entry admin test1
[AP-nqa-admin-test1] type http
```

HTTP サーバの URL を指定します。

```
[AP-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。

```
[AP-nqa-admin-test1-http] operation get
```

HTTP version 1.0 を使用するように設定します。

```
[AP-nqa-admin-test1-http] version v1.0
```

履歴記録を保存するように設定します。

```
[AP-nqa-admin-test1-http] history-record enable
[AP-nqa-admin-test1-http] quit
```

HTTP テストを開始します。

```
[AP] 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。

```
[AP] undo nqa schedule admin test1
```

HTTP テストの最新の結果を表示します。

```
[AP] 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。

```
[AP] 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
```

出力では、AP が HTTP サーバからデータを取得するのに 64 ミリ秒かかることを示します。

2.7.6 UDP ジッタテスト設定例

I. ネットワーク要件

図 2-7 に示すように、AP 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 2-7 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) 各装置間で通信可能になるように、スタティックルートあるいはルーティングテーブルを設定します。（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 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
```

4) AP を設定します。

UDP ジッタテストを作成します。

```
<AP> system-view
[AP] nqa entry admin test1
[AP-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。

```
[AP-nqa-admin-test1-udp-jitter] destination ip 10.2.2.2
```

宛先ポート 9000 を設定します。

```
[AP-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。

```
[AP-nqa-admin-test1-udp-jitter] frequency 1000
[AP-nqa-admin-test1-udp-jitter] quit
```

UDP ジッタテストを開始します。

```
[AP] 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。

```
[AP] undo nqa schedule admin test1
```

UDP ジッタテストの最新の結果を表示します。

```
[AP] 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。

```
[AP] 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
```

2.7.7 SNMP テスト設定例

I. ネットワーク要件

図 2-8 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 2-8 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) 各装置間で通信可能になるように、スタティックルートあるいはルーティングテーブルを設定します。（詳細は省略します。）
3) SNMP エージェント（Device）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
```

read コミュニティを public に設定します。

```
[Device] snmp-agent community read public
```

write コミュニティを private に設定します。

```
[Device] snmp-agent community write private
```

4)　AP を設定します。

SNMP テストを作成します。

```
<AP> system-view
[AP] nqa entry admin test1
[AP-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。

```
[AP-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。

```
[AP-nqa-admin-test1-snmp] history-record enable
[AP-nqa-admin-test1-snmp] quit
```

SNMP テストを開始します。

```
[AP] 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。

```
[AP] undo nqa schedule admin test1
```

SNMP テストの最新の結果を表示します。

```
[AP] 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。

```
[AP] 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
```

出力では、AP が SNMP エージェントから応答を受信するのに 50 ミリ秒かかることを示します。

2.7.8 TCP テスト設定例

I. ネットワーク要件

図 2-9 に示すように、NQA クライアントが Device の NQA サーバに 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 2-9 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) 各装置間で通信可能になるように、スタティックルートあるいはルーティングテーブルを設定します。（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) AP を設定します。

TCP テストを作成します。

```
<AP> system-view
[AP] nqa entry admin test1
[AP-nqa-admin-test1] type tcp
```

宛先 IP アドレスを 10.2.2.2 に設定します。

```
[AP-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。

```
[AP-nqa-admin-test1-tcp] destination port 9000
```

履歴記録を保存するように設定します。

```
[AP-nqa-admin-test1-tcp] history-record enable
[AP-nqa-admin-test1-tcp] quit
```

TCP テストを開始します。

```
[AP] 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。

```
[AP] undo nqa schedule admin test1
```

TCP テストの最新の結果を表示します。

```
[AP] 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。

```
[AP] 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
```

出力では、AP が NQA サーバのポート 9000 と TCP 接続を確立するのに 13 ミリ秒かかることを示します。

2.7.9 UDP エコーテスト設定例

I. ネットワーク要件

図 2-10 に示すように、AP と Device 間のラウンドトリップ時間をテストするように、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 2-10 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) 装置が互いに通信できるようにスタティックルートあるい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 をリスニングするように設定します。

```
[Device] nqa server udp-echo 10.2.2.2 8000
```

4) AP を設定します。

UDP エコーテストを作成します。

```
<AP> system-view
[AP] nqa entry admin test1
[AP-nqa-admin-test1] type udp-echo
```

宛先 IP アドレスを 10.2.2.2 に設定します。

```
[AP-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。

```
[AP-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。

```
[AP-nqa-admin-test1-udp-echo] history-record enable
[AP-nqa-admin-test1-udp-echo] quit
```

UDP エコーテストを開始します。

```
[AP] 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。

```
[AP] undo nqa schedule admin test1
```

UDP エコーテストの最新の結果を表示します。

```
[AP] 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。

```
[AP] 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、AP と Device のポート 8000 番の間のラウンドトリップ時間が 25ms であることを示します。

2.7.10 音声テスト設定例

I. ネットワーク要件

図 2-11 に示すように、AP と Device 間のジッタ、遅延、MOS、ICPIF をテストするため音声テストを設定します。



図 2-11 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) 各装置間で通信可能になるように、スタティックルートあるいはルーティングテーブルを設定します。（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 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
```

4) AP を設定します。

音声テストを作成します。

```
<AP> system-view
[AP] nqa entry admin test1
[AP-nqa-admin-test1] type voice
```

宛先 IP アドレスを 10.2.2.2 に設定します。

```
[AP-nqa-admin-test1-voice] destination ip 10.2.2.2
```

宛先ポート番号を 9000 に設定します。

```
[AP-nqa-admin-test1-voice] destination port 9000
[AP-nqa-admin-test1-voice] quit
```

音声テストを開始します。

```
[AP] nqa schedule admin test1 start-time now lifetime forever
```

音声テストを一定期間実行したのち、テストを停止します。

```
[AP] undo nqa schedule admin test1
```

音声テストの最新の結果を表示します。

[AP] display nqa result admin test1

```
NQA entry (admin admin, tag test1) test results:
    Send operation times: 1000           Receive response times: 1000
    Min/Max/Average round trip time: 31/1328/33
    Square-Sum of round trip time: 2844813
    Last packet received time: 2011-06-13 09:49:31.1
  Extended results:
    Packet loss ratio: 0%
    Failures due to timeout: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
Packets out of sequence: 0
    Packets arrived late: 0
  Voice results:
   RTT number: 1000
    Min positive SD: 1                    Min positive DS: 1
    Max positive SD: 204                  Max positive DS: 1297
    Positive SD number: 257               Positive DS number: 259
    Positive SD sum: 759                  Positive DS sum: 1797
    Positive SD average: 2                Positive DS average: 6
    Positive SD square-sum: 54127         Positive DS square-sum: 1691967
    Min negative SD: 1                    Min negative DS: 1
    Max negative SD: 203                  Max negative DS: 1297
    Negative SD number: 255               Negative DS number: 259
    Negative SD sum: 759                  Negative DS sum: 1796
    Negative SD average: 2                Negative DS average: 6
    Negative SD square-sum: 53655         Negative DS square-sum: 1691776
  One way results:
    Max SD delay: 343                     Max DS delay: 985
    Min SD delay: 343                     Min DS delay: 985
    Number of SD delay: 1                 Number of DS delay: 1
    Sum of SD delay: 343                  Sum of DS delay: 985
    Square-Sum of SD delay: 117649        Square-Sum of DS delay: 970225
    SD lost packets: 0                   DS lost packets: 0
    Lost packets for unknown reason: 0
  Voice scores:
    MOS value: 4.38                       ICPIF value: 0
```

音声テストの統計情報を表示します。

[AP] display nqa statistics admin test1

```
NQA entry (admin admin, tag test1) test statistics:
  NO. : 1

    Start time: 2011-06-13 09:45:37.8
    Life time: 331 seconds
    Send operation times: 4000           Receive response times: 4000
    Min/Max/Average round trip time: 15/1328/32
    Square-Sum of round trip time: 7160528
  Extended results:
    Packet loss ratio: 0%
    Failures due to timeout: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
Packets out of sequence: 0
    Packets arrived late: 0
  Voice results:
   RTT number: 4000
    Min positive SD: 1                    Min positive DS: 1
    Max positive SD: 360                  Max positive DS: 1297
    Positive SD number: 1030              Positive DS number: 1024
    Positive SD sum: 4363                 Positive DS sum: 5423
    Positive SD average: 4                Positive DS average: 5
    Positive SD square-sum: 497725        Positive DS square-sum: 2254957
    Min negative SD: 1                    Min negative DS: 1
    Max negative SD: 360                  Max negative DS: 1297
    Negative SD number: 1028              Negative DS number: 1022
```

```
    Negative SD sum: 1028                  Negative DS sum: 1022
    Negative SD average: 4                 Negative DS average: 5
    Negative SD square-sum: 495901         Negative DS square-sum: 5419
  One way results:
    Max SD delay: 359                      Max DS delay: 985
    Min SD delay: 0                        Min DS delay: 0
    Number of SD delay: 4                  Number of DS delay: 4
    Sum of SD delay: 1390                  Sum of DS delay: 1079
    Square-Sum of SD delay: 483202         Square-Sum of DS delay: 973651
    SD lost packets: 0                   DS lost packets: 0
    Lost packets for unknown reason: 0
  Voice scores:
    Max MOS value: 4.38                    Min MOS value: 4.38
    Max ICPIF value: 0                     Min ICPIF value: 0
```

2.7.11 DLSw テスト設定例

I. ネットワーク要件

図 2-12 に示すように、DLSw 装置の応答時間を測定するため、DLSw テストを設定します。



図 2-12 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あるい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。）

DLSw テストを作成します。

```
<AP> system-view
[AP] nqa entry admin test1
[AP-nqa-admin-test1] type dlsw
```

宛先 IP アドレスを 10.2.2.2 に設定します。

```
[AP-nqa-admin-test1-dlsw] destination ip 10.2.2.2
```

履歴記録を保存するように設定します。

```
[AP-nqa-admin-test1-dlsw] history-record enable
[AP-nqa-admin-test1-dlsw] quit
```

DLSw テストを開始します。

```
[AP] nqa schedule admin test1 start-time now lifetime forever
```

DLSw テストを一定期間実行したのち、テストを停止します。

```
[AP] undo nqa schedule admin test1
```

DLSw テストの最新の結果を表示します。

```
[AP] 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: 19/19/19
    Square-Sum of round trip time: 361
    Last succeeded probe time: 2011-11-22 10:40:27.7
  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
```

DLSw テストの履歴記録を表示します。

```
[AP] display nqa history admin test1
NQA entry (admin admin, tag test1) history records:
  Index      Response     Status           Time
  1          19           Succeeded        2011-11-22 10:40:27.7
```

出力では、DLSw 装置の応答時間が 19 ミリ秒であることを示します。

目次

このセクションのページは **10-x-x** です。

3 章 NTP（FIT は未サポート） 3-1
3.1 概要 3-1
3.1.1 NTP の動作 3-1
3.1.2 NTP アーキテクチャ 3-2
3.1.3 運用モード 3-3
3.1.4 NTP セキュリティ 3-5
3.1.5 プロトコルと標準 3-6
3.2 設定の制限とガイドライン 3-7
3.3 設定作業リスト 3-7
3.4 NTP サービスの有効化 3-7
3.5 NTP 運用モードの設定 3-7
3.5.1 NTP クライアント/サーバモードの設定 3-7
3.5.2 NTP シンメトリックアクティブ/パッシブモードの設定 3-8
3.5.3 NTP ブロードキャストモードの設定 3-8
3.5.4 NTP マルチキャストモードの設定 3-9
3.6 NTP サービスアクセス制御権の設定 3-10
3.7 NTP 認証の設定 3-10
3.7.1 クライアント/サーバモードの NTP 認証の設定 3-10
3.7.2 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 3-12
3.7.3 ブロードキャストモードの NTP 認証の設定 3-13
3.7.4 マルチキャストモードの NTP 認証の設定 3-15
3.8 NTP オプションパラメータの設定 3-17
3.8.1 NTP メッセージの送信元インタフェースの設定 3-17
3.8.2 インタフェースでの NTP メッセージ処理の無効化 3-18
3.8.3 ダイナミックアソシエーションの最大数の設定 3-18
3.8.4 NTP パケットの DSCP 値の設定 3-19
3.9 NTP の表示と維持 3-19
3.10 NTP 設定例 3-19
3.10.1 NTP クライアント/サーバモードの設定例 3-19
3.10.2 NTP シンメトリックアクティブ/パッシブモードの設定例 3-21
3.10.3 NTP 認証を使用したクライアント/サーバモードの設定例 3-22

3章 NTP（FIT は未サポート）

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。

本マニュアルに登場する「FIT」という用語は、特に断りがない場合、Anchor-FIT モードで動作する AP のことを含みます。

3.1 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、高いクロックの精度が保証されます。NTP を有効に利用することで、装置間で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 プロトコルで、UDP ポート 123 を使用します。

🕮 **メモ：**

NTP は、以下のレイヤ 3 イーサネットインタフェースでサポートします。

- 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
- トンネルインタフェース

3.1.1 NTP の動作

図 3-1 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。

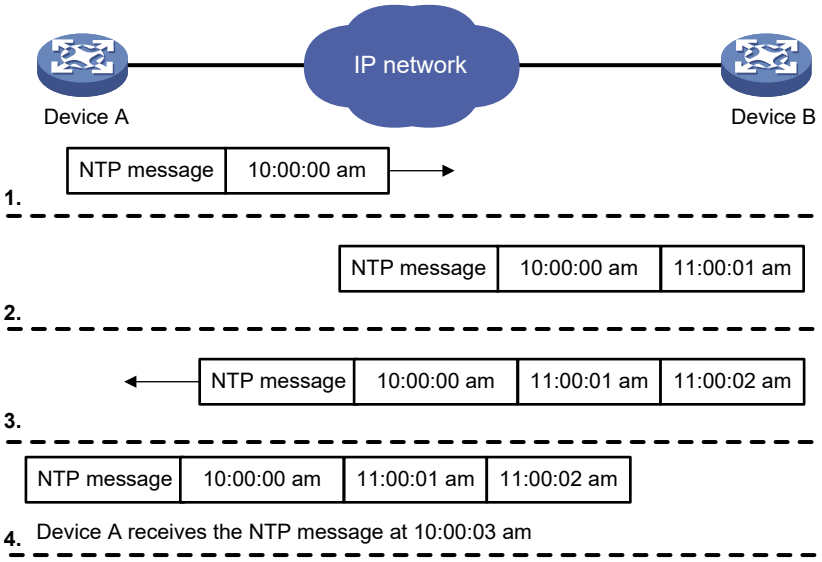


図 3-1 基本ワークフロー

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。

3.1.2 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 3-2 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。

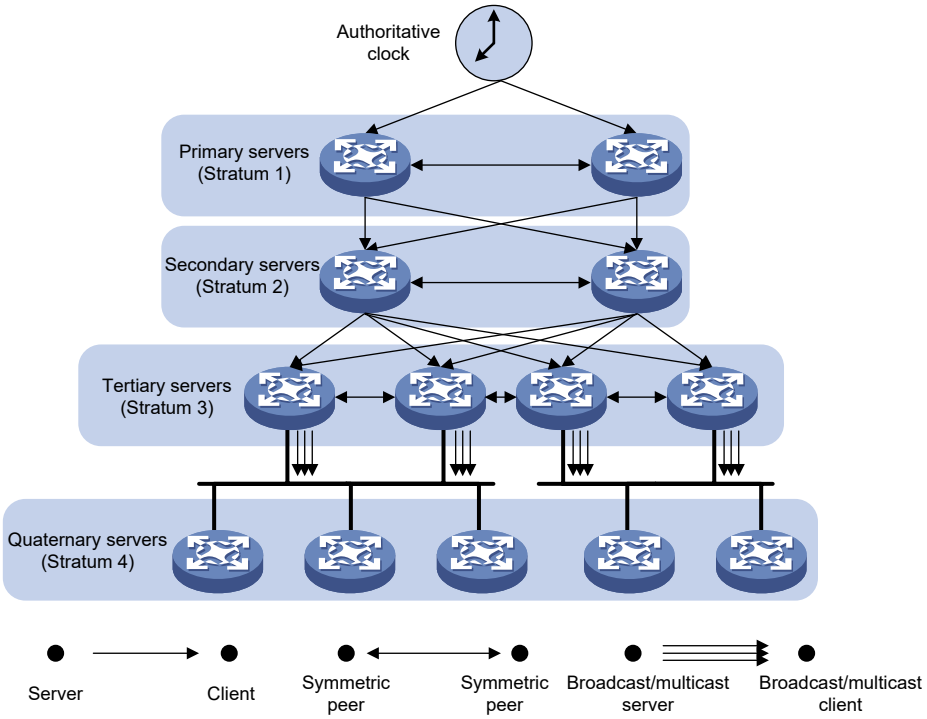


図 3-2 NTP アーキテクチャ

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。

3.1.3 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 3-1 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 3-2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 3-2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。
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 3-2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。

モード	作業処理	原則	アプリケーションシナリオ
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。

3.1.4 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。

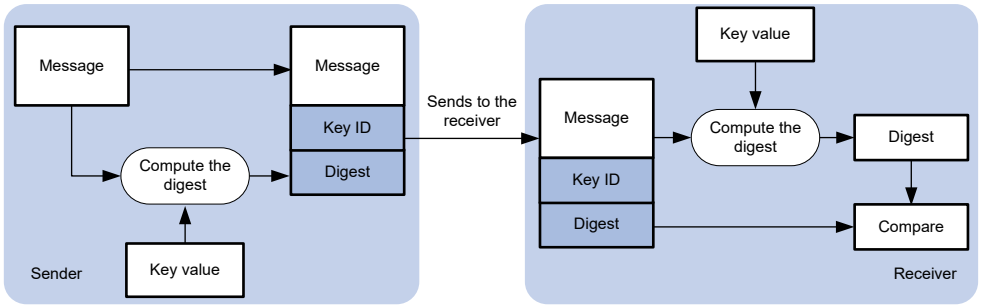


図 3-3 NTP 認証

図 3-3 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 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。

3.1.5 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*

3.2 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。

3.3 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） 以下のうちの1つを実行します。 • NTP運用モードの設定 • 参照ソース用ローカルクロックの設定
（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

3.4 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**	ー
2． NTP サービスを有効にする	**ntp-service enable**	デフォルト：無効

3.5 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。

3.5.1 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**	―
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

3.5.2 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

3.5.3 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**	ー
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**	ー
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。

3.5.4 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**	ー
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。

3.6 NTPサービスアクセス制御権の設定

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 access { peer | query | server | synchronization } acl** *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。詳細はコマンドマニュアルのセクション 8 *ACL and QoS*” *ACL*”を参照してください。

3.7 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。

3.7.1 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 と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 md5** { **cipher** | **simple** } *value*	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

操作	コマンド	補足
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 md5** { **cipher** | **simple** } *value*	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

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 3-2 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 3-2 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	―	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	―	―	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	―	―	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	―	―	―	―	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。

3.7.2 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 と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**	―
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 md5** { **cipher** | **simple** } *value*	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 md5** { **cipher** | **simple** } *value*	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 3-3 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 3-3 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。

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	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	―	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。

3.7.3 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 と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**	―

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 md5** { **cipher** | **simple** } *value*	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 md5** { **cipher** | **simple** } *value*	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 3-4 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 3-4 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。

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	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。
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。

3.7.4 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 と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 md5** { **cipher** | **simple** } *value*	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**	―
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 md5** { **cipher** | **simple** } *value*	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 3-5 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 3-5 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。

3.8 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。

3.8.1 NTP メッセージの送信元インタフェースの設定

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． NTP メッセージの送信元インタフェースを指定する	**ntp-service source** *interface-type interface-number*	デフォルト：設定なし

3.8.2 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

3.8.3 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**	―
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

3.8.4 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**	―
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

3.9 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**

3.10 NTP設定例

3.10.1 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 3-4 に示すように設定します。

- デバイスの 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。
- AP をクライアントモードで設定し、デバイスを NTP サーバとして設定します。

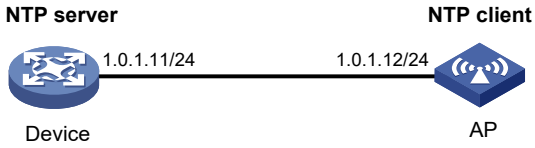


図 3-4 ネットワーク図

II. 設定手順

1) 図 3-4 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) デバイスを設定します。

NTP サービスを有効にします。

```
<Device> system-view
[Device] 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。

```
[Device] ntp-service refclock-master 2
```

3) AP を設定します。

NTP サービスを有効にします。

```
<AP> system-view
[AP] ntp-service enable
```

AP がデバイスに同期されるように、AP の NTP サーバとしてデバイスを指定します。

```
[AP] ntp-service unicast-server 1.0.1.11
```

III. 設定の確認

AP がデバイスに同期化され、AP の stratum レベルが 3 であることを確認します。

```
[AP] 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^-10
 Root delay: 0.00383 ms
 Root dispersion: 16.26572 ms
 Reference time: d0c6033f.b9923965  Wed, Dec 29 2010 18:58:07.724
```

AP とデバイス間で 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。

```
[AP] 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
```

3.10.2 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 3-5 に示すように、設定します。

- 参照ソースとしてデバイス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デバイスを設定し、デバイスのパッシブピアとして AP を指定します。



図 3-5 ネットワーク図

II. 設定手順

1) 図 3-5 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) AP を設定します。

NTP サービスを有効にします。

```
<AP> system-view
[AP] ntp-service enable
```

3) デバイスを設定します。

NTP サービスを有効にします。

```
<Device> system-view
[Device] 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。

```
[Device] ntp-service refclock-master 2
```

シンメトリックパッシブピアとして AP を設定します。

```
[Device] ntp-service unicast-peer 3.0.1.32
```

III. 設定の確認

AP がデバイス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。

```
[AP] 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^-19
 Root delay: 0.00609 ms
 Root dispersion: 1.95859 ms
 Reference time: 83aec681.deb6d3e5  Wed, Jan  8 2014 14:33:11.081
```

AP とデバイス間の 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。

```
[AP] 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
```

3.10.3 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 3-6 に示すように、デバイスの 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。
- AP はクライアントモードで動作し、デバイスは AP の NTP サーバとして使用されます。
- デバイスと AP の両方で NTP 認証を設定します。

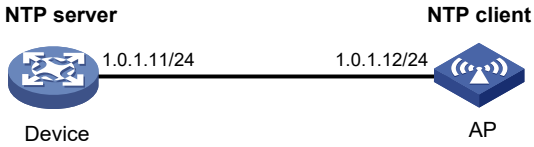


図 3-6 ネットワーク図

II. 設定手順

1) 図 3-6 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) デバイスを設定します。

NTP サービスを有効にします。

```
<Device> system-view
[Device] 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-W2120AC ではサポートしていません。

```
[Device] ntp-service refclock-master 2
```

3) AP を設定します。

NTP サービスを有効にします。

```
<AP> system-view
```

```
[AP] ntp-service enable
```

AP で NTP 認証を有効にします。

```
[AP] 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。

```
[AP] 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。

```
[AP] ntp-service reliable authentication-keyid 42
```

AP の NTP サーバとしてデバイスを指定し、キーID を 42 としてサーバと関連づけます。

```
[AP] ntp-service unicast-server 1.0.1.11 authentication-keyid 42
```

AP がデバイスのクロックの同期を行う前に、デバイスの NTP 認証を有効にします。

4) デバイスで NTP 認証を設定します。

NTP 認証を有効にします。

```
[Device] 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。

```
[Device] 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。

```
[Device] ntp-service reliable authentication-keyid 42
```

III. 設定の確認

AP がデバイスに同期化され、Switch の stratum レベルが 3 であることを確認します。

```
[AP] 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^-10
 Root delay: 0.00655 ms
 Root dispersion: 1.15869 ms
 Reference time: d0c62687.ab1bba7d  Wed, Dec 29 2010 21:28:39.668
```

AP とデバイス間で 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。

```
[AP] 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 **10-x-x** です。

4 章 SNMP（FIT は未サポート） 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 4-4
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 4-7
4.5 SNMP の表示と維持 4-9
4.6 設定例 4-9
4.6.1 SNMPv1/SNMPv2c の設定例 4-9
4.6.2 SNMPv3 の設定例 4-11

4章 SNMP（FIT は未サポート）

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。

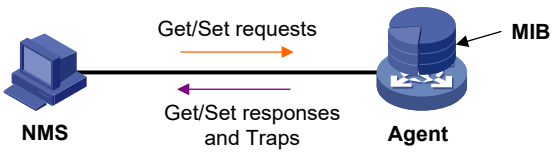


図 4-1 NMS、エージェント、MIB の関係

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。

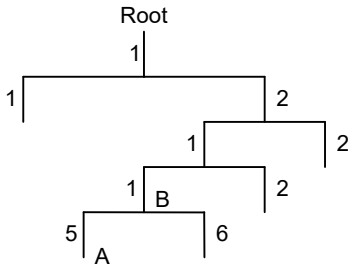


図 4-2 MIB ツリー

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
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。

操作	コマンド	補足
		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：SNMPv3が有効です。
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

操作	コマンド	補足
		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** – 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 の詳細はオペレーションマニュアルのセクション 10 *システム管理 "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**	―
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**	―
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*	―
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 | interface-number.subnumber }*	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。

操作	コマンド	補足
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**] *
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*]

4.6 設定例

4.6.1 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。

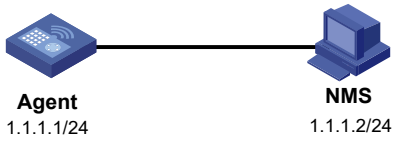


図 4-3 ネットワーク図

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。

```
<Agent> system-view
[Agent] snmp-agent sys-info version v1
[Agent] snmp-agent community read public
[Agent] 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。

```
[Agent] snmp-agent sys-info contact NEC
[Agent] 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。）

```
[Agent] snmp-agent trap enable
[Agent] 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
```

4.6.2 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。

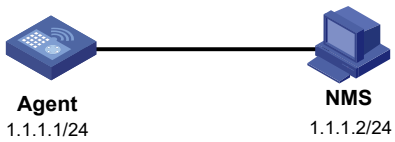


図 4-4 ネットワーク図

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。

```
<Agent> system-view
[Agent] undo snmp-agent mib-view ViewDefault
[Agent] snmp-agent mib-view included test snmp
```

```
[Agent] 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 private ノード(OID : 1.3.6.1.4)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。

```
[Agent] snmp-agent mib-view included test 1.3.6.1.2.1.1
[Agent] snmp-agent mib-view included test .1.3.6.1.4
[Agent] 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。

```
[Agent] 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。

```
[Agent] snmp-agent sys-info contact NEC
[Agent] 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 **managev3user** に設定します。

```
[Agent] snmp-agent trap enable
[Agent] snmp-agent target-host trap address udp-domain 1.1.1.2 params securityname managev3user v3 privacy
```

2) SNMP NMS を設定します。
   - □ SNMPv3 を指定します。
   - □ SNMPv3 ユーザ **managev3user** 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 **10-x-x** です。

5 章 NETCONF（FIT は未サポート） 5-1
5.1 概要 5-1
5.1.1 NETCONF の構成 5-1
5.1.2 NETCONF メッセージフォーマット 5-2
5.1.3 NETCONF の使用方法 5-3
5.1.4 プロトコルと標準 5-3
5.2 NETCONF の設定作業リスト 5-4
5.3 NETCONF over SOAP の有効化 5-4
5.4 NETCONF ロギング の有効化 5-4
5.5 NETCONF セッションの確立 5-5
5.5.1 NETCONF セッションアイドルタイムアウト時間の設定 5-5
5.5.2 xml view への移行 5-5
5.5.3 capability の交換 5-5
5.6 イベント通知の設定 5-6
5.6.1 登録手順 5-6
5.6.2 イベント通知の登録例 5-7
5.7 設定のロック/ロック解除 5-8
5.7.1 コンフィグレーションのロック 5-9
5.7.2 コンフィグレーションのロック解除 5-9
5.7.3 コンフィグレーションのロック例 5-9
5.8 サービスオペレーションの実行 5-10
5.8.1 get/get-bulk の実行 5-11
5.8.2 get-config/get-bulk-config の実行 5-12
5.8.3 edit-config オペレーションの実行 5-12
5.8.4 全てのモジュールのコンフィグレーション取得例 5-13
5.8.5 シスログのコンフィグレーション取得例 5-15
5.8.6 インタフェーステーブルのデータ取得例 5-15
5.8.7 パラメータ値の変更例 5-16
5.9 コンフィグレーションの保存、ロールバックと読み込み 5-17
5.9.1 コンフィグレーションの保存 5-17
5.9.2 コンフィグレーションファイルからのロールバック 5-18
5.9.3 ロールバックポイントからのロールバック 5-19
5.9.4 コンフィグレーションの読み込み 5-22
5.9.5 コンフィグレーションの保存例 5-23
5.10 データのフィルタリング 5-24
5.10.1 テーブルベースフィルタリング 5-24
5.10.2 コラムベースフィルタリング 5-24
5.10.3 正規表現によるデータのフィルタリング例 5-26
5.10.4 条件一致によるデータのフィルタリング例 5-28
5.11 NETCONF 経由の CLI 実行 5-29
5.11.1 実行手順 5-29
5.11.2 CLI 実行例 5-29
5.12 NETCONF セッション情報の取得 5-30
5.13 他の NETCONF セッション排除 5-31
5.13.1 実行例 5-32

5.14 CLI への復帰 5-32
5.15 付録 5-33
5.15.1 NETCONF サポートオペレーション 5-33

5章 NETCONF（FIT は未サポート）

5.1 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。

5.1.1 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 5-1 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5-4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。
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。

5.1.2 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>
```

5.1.3 NETCONF の使用方法

NETCONF の表 5-2 に示した方法で、デバイスの運用と設定が可能です。

表 5-2 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。

5.1.4 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

5.2 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) get-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

5.3 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。

5.4 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。

5.5 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、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。

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。

5.5.1 NETCONF セッションアイドルタイムアウト時間の設定

NETCONF セッションアイドルタイムアウト時間内に NETCONF セッションで NETCONF パケットが交換されない場合、装置はセッションを切断します。

以下に、NETCONF セッションアイドルタイムアウト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**	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セッション、NETCONF overコンソールセッションはタイムアウトしません。

5.5.2 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。

5.5.3 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。

5.6 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。 どのイベント通知を登録できるかについては、デバイスのシステムログメッセージリファレンスを参照してください。

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。

5.6.1 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。

5.6.2 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。

```
<Switch> xml
```

クライアントでサポートされている NETCONF 機能を装置に通知します。

```
<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>
```

5.7 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。

5.7.1 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>
```

5.7.2 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>
```

5.7.3 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。

```
<Switch> xml
```

クライアントでサポートされている NETCONF 機能を装置に通知します。

```
<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。

5.8 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。

5.8.1 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>
```

5.8.2 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>
```

5.8.3 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、オペレーショ

ンマニュアルのセクション 10 *システム管理 ”NECONF”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>
   error-option
</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)。

5.8.4 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。

```
<Switch> xml
```

クライアントでサポートされている NETCONF 機能を装置に通知します。

```
<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>
```

5.8.5 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。

```
<Switch> xml
```

クライアントでサポートされている NETCONF 機能を装置に通知します。

```
<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>
```

5.8.6 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。

```
<Switch> xml
```

クライアントでサポートされている NETCONF 機能を装置に通知します。

```
<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>
```

5.8.7 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。

```
<Switch> xml
```

クライアントでサポートされている NETCONF 機能を装置に通知します。

```
<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>
```

5.9 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。

5.9.1 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" Binary-only="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。

Binary-onry 属性は、現在の構成を指定されたテキスト構成ファイルに保存するかどうかを決定します。

- 属性のデフォルト値 false を使用する場合、装置はテキストとバイナリの両方の設定ファイルに設定を保存します。
- この属性を true に設定すると、装置は設定をバイナリファイルにのみ保存し、対応するテキストファイルを次回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設定します。
  - 指定されたテキストファイルが存在しない場合、save 操作は失敗します。
  - ファイル列が含まれていない場合、装置はタートアップコンフィグレーションファイルがあるかどうかを識別します。次の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、装置はコンフィグレーションを対応するバイナリファイルにのみ保存します。次の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、save 操作は失敗します。

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>
```

5.9.2 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>
```

5.9.3 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。詳細は、“*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。詳細は、“*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。詳細は、“*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。詳細は、“*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。詳細は、“*save-point/end オペレーションの実行*”を参照してください。
7) ロックの解放。

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>
```

5.9.4 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>
```

5.9.5 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。

```
<Switch> xml
```

#クライアントでサポートされている NETCONF 機能を装置に通知します。

```
<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>
```

5.10 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。

5.10.1 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="vrf vpn1 IP 1.1.1.0 MaskLen 24 longer/>
          </Ipv4Routes>
        </Route>
      </top>
    </filter>
  </get>
</rpc>
```

5.10.2 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 5-3 は条件一致のオペレーション一覧です。

表 5-3 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>
```

5.10.3 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。

```
<Switch> xml
```

クライアントでサポートされている NETCONF 機能を装置に通知します。

```
<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>
```

5.10.4 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。

```
<Switch> xml
```

クライアントでサポートされている NETCONF 機能を装置に通知します。

```
<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>
```

5.11 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。

5.11.1 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>
```

5.11.2 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。

```
<Switch> xml
```

クライアントでサポートされている NETCONF 機能を装置に通知します。

```
<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[
<AP>display current-configuration
#
version 7.1.045, ESS 2305
#
 sysname AP
#
 (省略)
return
   ]]>
   </Execution>
  </CLI>
</rpc-reply>
```

5.12 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。

```
<Switch> xml
```

クライアントでサポートされている NETCONF 機能を装置に通知します。

```
<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。

5.13 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>
```

5.13.1 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。

```
<Switch> xml
```

クライアントでサポートされている NETCONF 機能を装置に通知します。

```
<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>
```

5.14 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>
```

5.15 付録

5.15.1 NETCONF サポートオペレーション

表 5-4 は、NETCONF で使用可能なオペレーションの一覧です。

表 5-4 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"> <lfmgr> <Interfaces> <Interface/> </Interfaces> </lfmgr> </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 xmlns="http://www.nec.com/netconf/data:1.0"> <lfmgr> <Interfaces xc:count=”5” xmlns:xc=” http://www.nec.com/netconf/base:1.0”> <Interface/>

オペレーション	説明	XML 例
		</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。	バッファサイズを120に変更します。 <rpc message-id ="101" 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/>

オペレーション	説明	XML 例
	● 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。	</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	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
	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	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
	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"> <Ifmgr> <Interfaces> <Interface> <Index>262</Index> <Description>222222</Description> </Interface> </Interfaces> </Ifmgr> </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	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" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"> <edit-config> <target> <running/> </target>

オペレーション	説明	XML 例
	一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。	<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>2</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れます。	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>1000000</ConfigSpeed> <ConfigDuplex>1</ConfigDuplex> </Interface> </Interfaces> </lfmgr> </top> </config> </edit-config> </rpc>
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">

オペレーション	説明	XML 例
		<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からログオフします。	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>
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	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">

オペレーション	説明	XML 例
	終了できません。	<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。 Bynary-onry属性は、現在の設定を指定されたテキスト設定ファイルに保存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" Binary-only="true"> <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 **10-x-x** です。

6 章 プロセスモニタリングとメンテナンス 6-1
6.1 ユーザプロセスの表示と維持 6-1

6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。

6.1 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**
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**

目次

このセクションのページは **10-x-x** です。

7 章 Information Center 7-1
7.1 概要 7-1
7.1.1 ログタイプ 7-1
7.1.2 ログレベル 7-1
7.1.3 ログの出力先 7-2
7.1.4 デフォルト出力ルール 7-2
7.1.5 Diagnostic ログのデフォルト出力ルール 7-2
7.1.6 hidden ログのデフォルト出力ルール 7-3
7.1.7 ログフォーマット 7-3
7.2 Information Center 設定作業リスト 7-5
7.3 コンソールへのログの出力 7-5
7.4 モニタ端末へのログの出力 7-6
7.5 ログホストへのログの出力 7-7
7.6 ログバッファへのログの出力 7-7
7.7 ログファイルへのログの保存 7-8
7.8 ログの最小記録期間の設定 7-9
7.9 情報の同期出力の設定 7-9
7.10 重複ログの抑制の設定 7-10
7.11 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 7-10
7.12 ログメッセージの SNMP notification の送信の有効化 7-11
7.13 キープアライブログ送信の設定の有効化 7-11
7.14 Information Center の表示と維持 7-12
7.15 設定例 7-12
7.15.1 コンソールへのログ出力の設定例 7-12
7.15.2 UNIX ログホストへのログ出力の設定例 7-13
7.15.3 Linux ログホストへのログ出力の設定例 7-14
7.15.4 ログホストへの SSL で暗号化したログ出力の設定例(証明書によるサーバ認証無し) 7-16
7.15.5 ログホストへの SSL で暗号化したログ出力の設定例(証明書によるサーバ認証あり) 7-17

7章 Information Center

7.1 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。

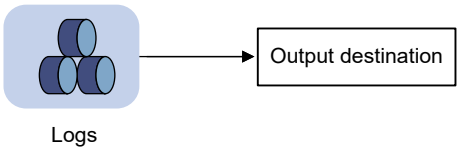


図 7-1 Information center の図

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。

7.1.1 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。

7.1.2 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 7-1 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。
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。

重要度	レベル	説明
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。

7.1.3 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。

7.1.4 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 7-2 にデフォルト出力ルールを示します。

表 7-2 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

7.1.5 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 7-3 に Diagnostic ログのデフォルト出力ルールを示します。

表 7-3 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	無効	Debugging

7.1.6 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 7-4 に hidden ログのデフォルト出力ルールを示します。

表 7-4 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

7.1.7 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 7-5 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 7-5 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	• 標準フォーマット(カスタムなし) <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 7-6 にログメッセージのフィールドの説明を示します。

表 7-6 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 7-1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 7-7と表 7-8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 7-1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。このフィールドは下記の値のうち1つを含みます。 ● IRFスタックメンバ装置のID ● 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 7-7 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 7-8 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 2003 Sysname FTPD/5/FTPD_LOGIN: User ftp (192.168.1.23) has logged in successfully. May 30 05:36:29:579 2003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>2003-05-30T06:42:44 Sysname %%10FTPD/5/FTPD_LOGIN(l): User ftp (192.168.1.23) has logged in successfully. 2003-05-30T06:42:44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	年を除いた現在時間と時間です。フォーマットはMMM DD hh:mm:ss:xxx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(l): 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。

7.2 Information Center設定作業リスト

作業リスト
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
（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）重複ログの抑制の設定
（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

7.3 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. Information Center を有効にする	**info-center enable**	デフォルト：有効

操作	コマンド	補足
3. 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** { **deny** | **level** *severity* }	デフォルト出力ルールについての詳細は、オペレーションマニュアルのセクション 10 *システム管理”Information Center”の”概要”の”デフォルト出力ルール”*を参照してください。
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** { **boot** | **date** | **none** }	デフォルト：**date**
5. user view に戻る	**quit**	ー
6. （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。
7. 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
8. （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）

7.4 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. Information Center を有効にする	**info-center enable**	デフォルト：有効
3. 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** } **monitor** { **deny** | **level** *severity* }	デフォルト出力ルールについての詳細は、オペレーションマニュアルのセクション 10 *システム管理”Information Center”の”概要”の”デフォルト出力ルール”*を参照してください。
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** { **boot** | **date** | **none** }	デフォルト：**date**
5. user view に戻る	**quit**	ー
6. 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。
7. 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

操作	コマンド	補足
8. （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）

7.5 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
2. Information Center を有効にする	**info-center enable**	デフォルト：有効
3. 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** } **loghost** { **deny** | **level** *severity* }	デフォルト出力ルールについての詳細は、オペレーションマニュアルのセクション 10 *システム管理”Information Center”の”概要”の”デフォルト出力ルール”*を参照してください。
4. （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。
5. （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** | **iso** | **no-year-date** | **none** }	デフォルト：**date**
6. 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* } [**facility** *local-number* | **format** { **default** | **rfc5424** } | **port** *port-number* | **source-ip** *source-ip-address* | **tcp** [**ssl-client-policy** *policy-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。 SSLプロトコルを使用してログを暗号化形式で送信する場合、事前にSSLクライアントポリシーを設定する必要があります。SSLクライアントポリシーの詳細は、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“SSL”*を参照してください。 装置は最大20のログホストをサポートします。

7.6 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. Information Center を有効にする	**info-center enable**	デフォルト：有効
3. 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

操作	コマンド	補足
4.　（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.　ログバッファの出力ルールを設定する	**info-center source** { *module-name* | **default** } **logbuffer** { **deny** | **level** *severity* }	デフォルト出力ルールについての詳細は、オペレーションマニュアルのセクション 10 *システム管理*”*Information Center*”の”*概要*”の”*デフォルト出力ルール*”を参照してください。
6.　（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**

7.7 ログファイルへのログの保存

システムは指定された間隔（デフォルトで 24 時間）でログバッファのログをログファイルに保存します。また手動で保存することができます。ログファイルバッファ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。

装置は 1 個のログファイルしかサポートしません。ログファイルが容量に達すると、システムは最初のログに新しいログを上書きします。

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。

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**	―
2.　Information Center を有効にする	**info-center enable**	デフォルト：有効
3.　ログファイル機能を有効にする	**info-center logfile enable**	デフォルト：無効
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：装置モデルにより異なります。 ログファイルの動作を正常に行うため、1MB～10MBのサイズに設定してください。

操作	コマンド	補足
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 : ストレージデバイスのルート直下のlogfileディレクトリ 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。

7.8 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。

- 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**	ー
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

7.9 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

7.10 重複ログの抑制の設定

重複したログが 30 秒未満の期間で連続して出力されると、システム/ネットワークのリソースの浪費となります。

機能を有効にすることにより、重複ログの出力を抑制します。

- 抑止期間中は、システムは 1 つ前に出力されたログと同一の module / name / level / mnemonic / locaton / txt 情報を有するログの出力を抑止します。
- 抑止期間終了後に同一の情報を持つログが発生した場合は、これを出力して再度、抑止を開始します。1 回目の抑止期間は 30 秒間、2 回目の抑止期間は 2 分間、以降の抑止期間は 10 分間となります。
- もし抑止期間中に別の新たなログが発生した場合、既存のログの抑止を終了して新たなログの抑止期間に移行します。

以下に重複ログの抑止の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. 重複ログの抑制を設定する	**info-center logging suppress duplicates**	デフォルト：無効

7.11 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*	―

操作	コマンド	補足
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。

7.12 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 10 *システム管理*“*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**	ー
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

7.13 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 7.5.129 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

操作	コマンド	補足
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 7.5.129のソフトウェア：有効 ソフトウェアバージョン 7.5.130を含む以降のソフトウェア：無効

7.14 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**
ログバッファを削除する	**reset logbuffer**

7.15 設定例

7.15.1 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。

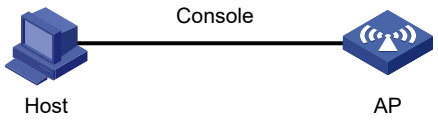


図 7-2 ネットワーク図

II. 設定手順

Information Center を有効にします。

```
<AP> system-view
[AP] info-center enable
```

コンソールへのログ出力を無効にします。

```
[AP] 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。

```
[AP] info-center source ftp console level warning
[AP] quit
```

コンソールでログの表示を有効にします。（この機能はデフォルトで有効です。）

```
<AP> terminal logging level 6
<AP> 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。

7.15.2 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

AP 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 7-3 ネットワーク図

II. 設定手順

設定を行う前に、AP 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。）

1)　AP を設定します。

Information Center を有効にします。

```
<AP> system-view
[AP] 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。

```
[AP] 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。

```
[AP] 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。

```
[AP] info-center source ftp loghost level informational
```

2)　ログホストを設定します。

以下の設定は Solaris で行ったものです。ほかの UNIX システムの設定は同様に行います。

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**AP**を作成します。ディレクトリ**AP**にファイル**info.log**を作成し、**AP**からログを保存します。

```
# mkdir /var/log/AP
# touch /var/log/AP/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。

```
# AP configuration messages
local4.info /var/log/AP/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/AP/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 AP 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、AP 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。

7.15.3 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

AP 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 7-4 ネットワーク図

II. 設定手順

設定を行う前に、AP 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。）

1)　AP を設定します。

Information Center を有効にします。

```
<AP> system-view
[AP] 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。

```
[AP] 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。

```
[AP] 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。

```
[AP] info-center source ftp loghost level informational
```

2)　ログホストを設定します。

以下の設定は Solaris で行ったものです。ほかの UNIX システムの設定は同様に行います。

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APを作成します。ディレクトリAPにファイル**info.log**を作成し、APからログを保存します。

```
# mkdir /var/log/AP
# touch /var/log/ AP /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。

```
# AP configuration messages
local5.info /var/log/AP/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**/**AP**/**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 AP 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、AP 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。

7.15.4 ログホストへの SSL で暗号化したログ出力の設定例(証明書によるサーバ認証無し)

I. ネットワーク要件

AP が SSL で暗号化したログをログホスト 1.2.0.1/16 の TCP ポート番号 514 に出力するように設定します。

AP には CA の証明書をインストールします。

ログホストには CA の証明書、サーバ証明書、秘密鍵をインストールします。(詳細は省略します)



図 7-5 ネットワーク図

II. 設定手順

設定を行う前に、AP 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。)

AP とログホストの時刻が正しく設定されていることを確認してください。(詳細は省略します。)

1)　PKI ドメインと SSL クライアントポリシーを設定します。

pki ドメイン **tls** を作成します。

```
<AP> system-view
[AP] pki domain tls
```

#CRL チェックを無効にします。

```
[AP-pki-domain-tls] undo crl check enable
[AP-pki-domain-tls] quit
```

SSL クライアントポリシー **tls-test** を作成します。

```
[AP] ssl client-policy tls-test
```

pki ドメイン **tls** を指定します。

```
[AP-ssl-client-policy-tls-test] pki-domain tls
```

証明書による SSL サーバの認証を無効にします。

```
[AP-ssl-client-policy-tls-test] undo server-verify enable
[AP-ssl-client-policy-tls-test] quit
```

2)　CA の証明書をインポートします。

CAの証明書を取得し、FTP等を用いて装置のFlashに格納します 。(詳細は省略します。)

以降の手順では、CA の証明書は、”cacert.pem”というファイル名で、Flash の直下に保存してあるものとして説明します。

#CA の証明書をインポートします。

```
[AP] pki import domain tls pem ca filename cacert.pem
```

3)　Information Center を設定します。

#info-center を有効にします。

```
[AP] info-center enable
```

ログホスト 1.2.0.1/16 を指定し、プロトコルは TCP、SSL クライアントポリシーとして tls-test を指定します。

```
[AP] info-center loghost 1.2.0.1 tcp ssl-client-policy tls-test
```

設定を行った後、Information Center はログホストの TCP514 ポートをあて先としてログを送信します。送信されるログの情報は SSL で暗号化されます。

7.15.5 ログホストへの SSL で暗号化したログ出力の設定例(証明書によるサーバ認証あり)

I. ネットワーク要件

AP が SSL で暗号化したログをログホスト 1.2.0.1/16 の TCP ポート番号 10514 に出力するように設定します。

AP には CA の証明書とローカルの証明書をインストールします。

ログホストには CA の証明書、サーバ証明書、秘密鍵をインストールします。(詳細は省略します)



図 7-6 ネットワーク図

II. 設定手順

設定を行う前に、AP 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。)

AP とログホストの時刻が正しく設定されていることを確認してください。(詳細は省略します。)

1)　PKI ドメインと SSL クライアントポリシーを設定します。

pki ドメイン **tls** を作成します。

```
<AP> system-view
[AP] pki domain tls
```

#CRL チェックを無効にします。

```
[AP-pki-domain-tls] undo crl check enable
[AP-pki-domain-tls] quit
```

SSL クライアントポリシー **tls-test** を作成します。

```
[AP] ssl client-policy tls-test
```

pki ドメイン **tls** を指定します。

```
[AP-ssl-client-policy-tls-test] pki-domain tls
```

2)　CA の証明書をインポートします。

CAの証明書を取得し、FTP等を用いて装置のFlashに格納します 。(詳細は省略します。)

以降の手順では、CA の証明書は、”cacert.pem”というファイル名で、AP の Flash の直下に保存してあるものとして説明します。

#CA の証明書をインポートします。

```
[AP] pki import domain tls pem ca filename cacert.pem
```

3)　PKI ドメインと PKI エンティティを設定し、証明書要求を作成します。

#PKI ドメイン **tls** に CA の情報を設定します。公開鍵 **hostkey** を鍵長 2048bit で生成します。PKI エンティティとして **syslog-over-tls** を指定します。

```
[AP] pki domain tls
[AP-pki-domain-tls] ca identifier CA-name
[AP-pki-domain-tls] certificate request from ca
[AP-pki-domain-tls] certificate request entity syslog-over-tls
[AP-pki-domain-tls] public-key rsa general name hostkey length 2048
[AP-pki-domain-tls] quit
```

#PKI エンティティ syslog-over-tls を作成します。

パラメータは利用環境に合わせたものを設定してください。

```
[AP] pki entity syslog-over-tls
[AP-pki-entity-syslog-over-tls] common-name test.com
[AP-pki-entity-syslog-over-tls] country JP
[AP-pki-entity-syslog-over-tls] state xxxx
[AP-pki-entity-syslog-over-tls] locality xxxx
[AP-pki-entity-syslog-over-tls] organization-unit xxxxx
[AP-pki-entity-syslog-over-tls] organization xxxxx
[AP-pki-entity-syslog-over-tls] ip 1.1.0.1
[AP-pki-entity-syslog-over-tls] quit
```

4)　ローカル証明書を入手し、インポートします。

#PKCS10 の証明書要求を作成します。表示された文字列を CA に提出してローカル証明書を入手します。 (詳細は省略します。)

```
[AP] pki request-certificate domain tls pkcs10
-----BEGIN CERTIFICATE REQUEST-----
（※内容は省略します）
-----END CERTIFICATE REQUEST-----
```

入手したローカル証明書を、FTP等を用いてAPのFlashに格納します 。(詳細は省略しま

す。)

以降の手順では、ローカル証明書は、”localcert.pem”というファイル名で、AP の Flash 直下に保存してあるものとして説明します。

#ローカル証明書をインポートします。

```
[AP] pki import domain tls pem local filename localcert.pem
```

5)　Information Center を設定します。

#info-center を有効にします。

```
[AP] info-center enable
```

ログホスト 1.2.0.1/16 を指定し、プロトコルは TCP、SSL クライアントポリシーとして tls-test を指定します。

```
[AP] info-center loghost 1.2.0.1 port 10514 tcp ssl-client-policy tls-test
```

設定を行った後、Information Center はログホストの TCP10514 ポートをあて先としてログを送信します。送信されるログの情報は SSL で暗号化されます。

目次

このセクションのページは **10-x-x** です。

8 章 NetMeister 8-1
8.1 概要 8-1
8.1.1 NetMeister の利用 8-1
8.1.2 設定手段について 8-3
8.2 設定作業リスト 8-4
8.2.1 手動設定による NetMeister の利用 8-5
8.2.2 ゼロタッチプロビジョニング機能による NetMeister の利用 8-8
8.3 NetMeister による管理 8-17
8.3.1 タブ一覧 8-17
8.4 NetMeister の表示と維持 8-19
8.5 NetMeister の設定例 8-19
8.6 NetMeister 利用のトラブルシューティング 8-21
8.6.1 NetMeister に QX が登録できない 8-21
8.6.2 NetMeister でグラフが正しく表示されない。 8-21
8.6.3 NetMeister のリモートログインが使えない 8-22
8.6.4 ファームウェア更新が成功しない 8-22
8.6.5 NetMeisterPrime 機能が使用できない 8-23

8章 NetMeister

8.1 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://support.necplatforms.co.jp/netmeister/manual/

8.1.1 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 8-1 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。

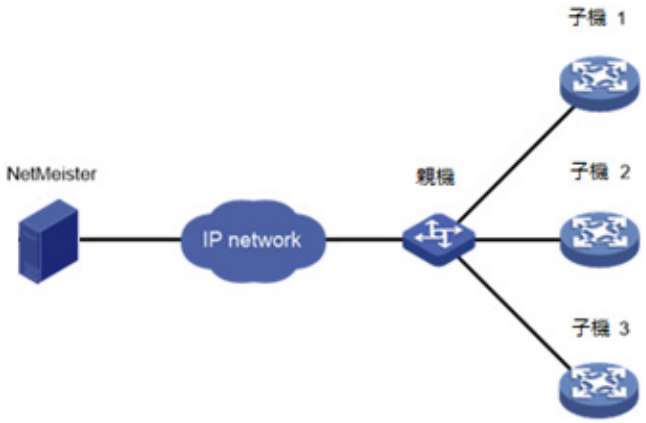


図 8-1 NetMeister との接続イメージ

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 8-2 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)

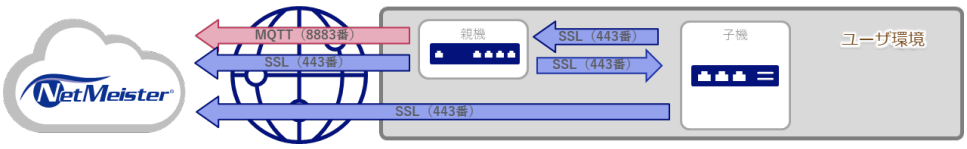


図 8-2 NetMeister への通信イメージ

図 8-3 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。

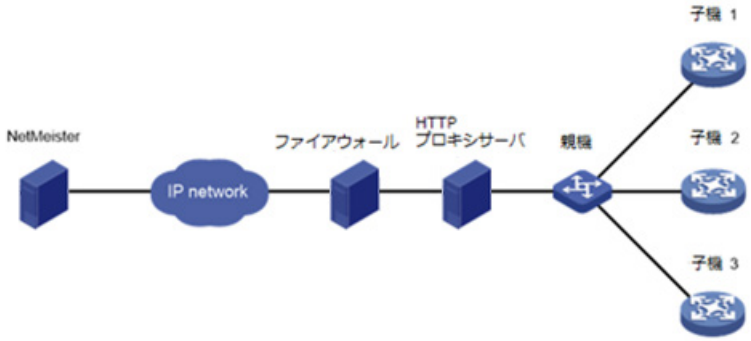


図 8-3 プロキシサーバを用いた NetMeister の利用環境

図 8-4 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。

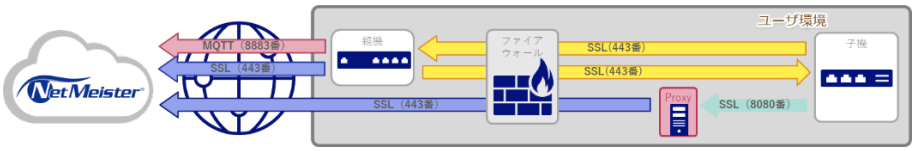


図 8-4 プロキシサーバを用いた NetMeister の通信イメージ

8.1.2 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 8-5 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。

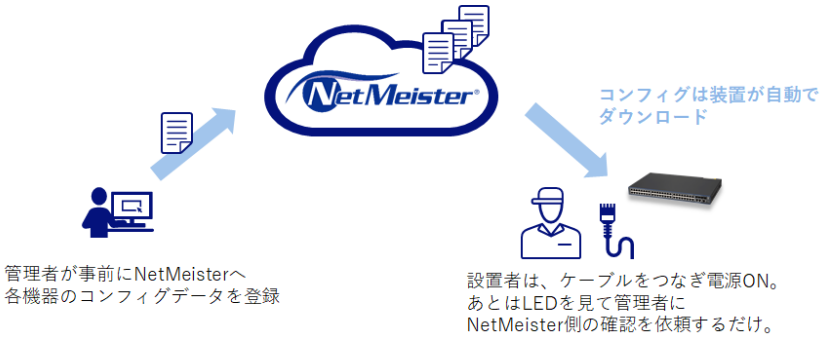


図 8-5 ゼロタッチプロビジョニングのイメージ

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 機能についてはオペレーションマニュアルのセクション 1 *はじめに* “*Auto Config*” を参照してください。

🕮 **メモ:**

QX-W シリーズでゼロタッチプロビジョニングを利用する場合、AP としての動作モード(Anchor-AC/FAT 等)の変更は予め必要です。設置作業者に渡す前に動作モードを変えておくことをお勧めします。

8.2 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 ● (オプション設定項目) NGN 閉域網経由の NetMeister 接続の有効化 ● (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

8.2.1 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）	装置時刻が正しくない場合、正しいグラフを表示できません。 v7.5.129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 v7.5.105 を含む以降のソフトウェアからサポートしています。

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 本コマンドによって 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：送信
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：v7.5.129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 v7.5.105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

🕮 **メモ:**

親機モードがおこなう MQTT 通信も **netmeister proxy** コマンドによって proxy サーバを利用します。

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：送信
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：v7.5.129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 v7.5.105以降のソフトウェアから有効にできます。
9． (オプション設定項目) NGN 閉域網経由の NetMeister 接続の有効化	**netmeister ngn enable**	デフォルト：無効 v7.5.143b以降のソフトウェアから有効にできます。
10．NetMeister 機能の有効化	**netmeister enable**	デフォルト：無効

🕮 **メモ:**

QX を NGN 閉域網経由で NetMeister に接続するためには、NGN 閉域網コントロール子機収容に対応し、NGN 閉域網経由で NetMeister に接続している IX-R(親機)が必要です。ま

た、QX を NGN 閉域網経由で NetMeister に接続するために、proxy サーバ指定(netmeister proxy)を、IX-R に設定されている子機接続用 HTTP プロキシアドレス設定(tunnel nm-child-ngn-proxy)のアドレス、ポート番号に合わせて設定する必要があります。

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**

8.2.2 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、FAT モードまたは Anchor-AC モードの場合にゼロタッチプロビジョニングが動作します。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。v7.5.129 以降のソフトウェアでは NetMeister 上のゼロタッチプロビジョニング設定で AP モード指定をすることで、ゼロタッチプロビジョニングの処理内で FAT または Anchor-AC モードから任意のモードに切り替えることが可能です。

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。

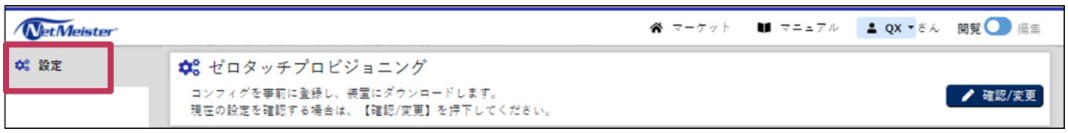


図 8-6 設定メニューの表示

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。

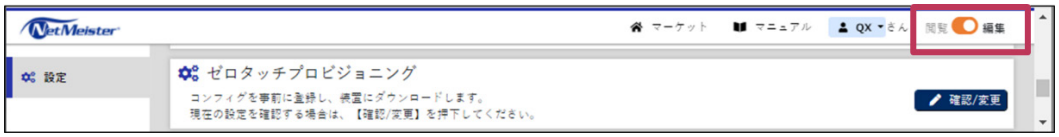


図 8-7 編集モードへの変更

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 8-8 コンフィグ登録画面

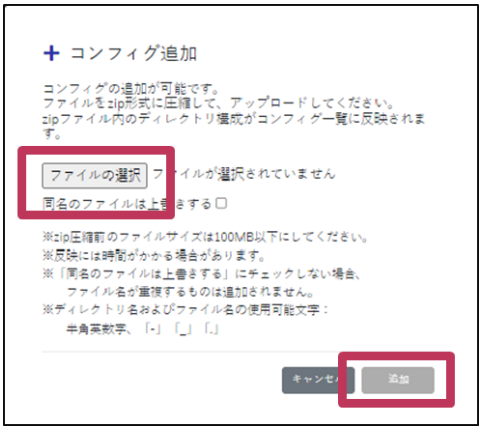


図 8-9 コンフィグの選択

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。

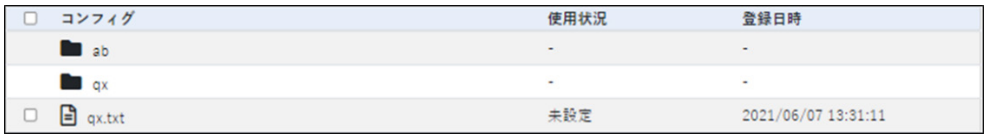


図 8-10 コンフィグ登録後の表示

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。

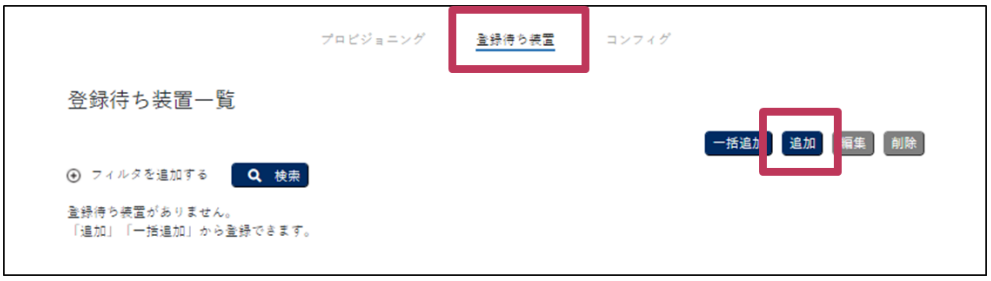


図 8-11 登録待ち装置設定画面



図 8-12 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 8-13 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 8-14 プロビジョニングの設定画面

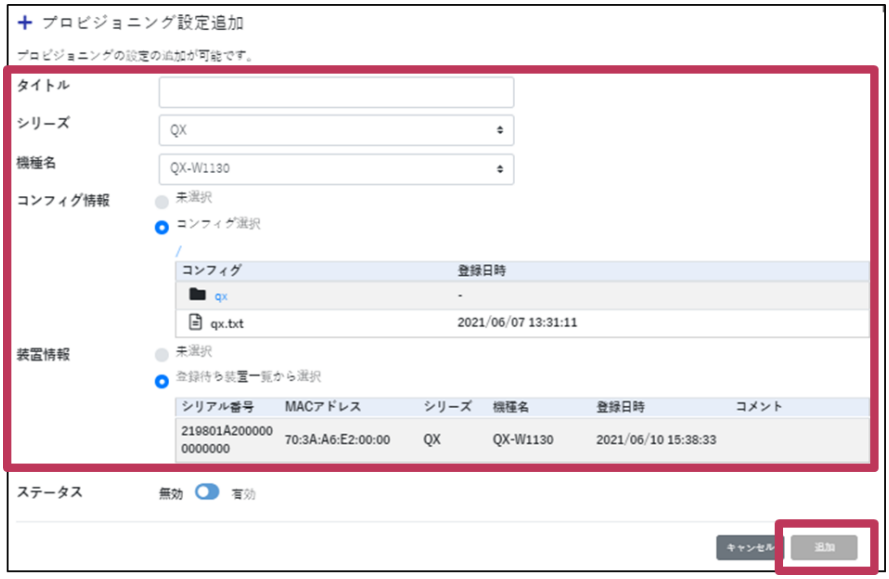


図 8-15 装置とコンフィグの選択

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 8-16 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 8-17 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 8-1 QX-W1240 LED 表示

状態	LED
Boot/System 起動中、	オレンジ点灯
ゼロタッチプロビジョニング中	緑点灯
ゼロタッチプロビジョニング成功時	(自動再起動)オレンジ点灯
コンフィグ読み込み中	緑点灯
起動完了	6 回オレンジ点灯、その後、緑点灯

9)　NetMeister 上で状態を確認します。



図 8-18 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 8-19 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。

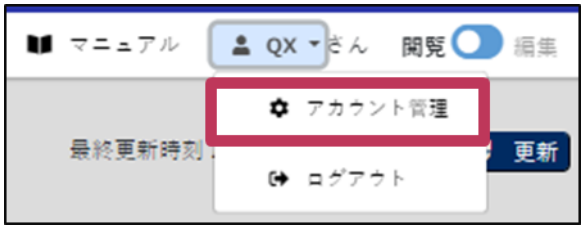


図 8-20 アカウント管理



図 8-21 通知の設定

8.3 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/

8.3.1 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 の利用によって利用可能になる機能もあります。詳細は NetMeister が提供する操作ガイドをご確認ください。

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。

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。
アラーム一覧	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/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。 その他の対応アラームはNetMeisterが提供する操作ガイドをご確認ください。
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	v7.5.105 を含む以降のソフトウェアで表示されます。 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	v7.5.105 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。 再起動履歴部分は、取得押下時に Anchor-AC が保持している情報が最新化を確認し、最新であれば表示されます。再起動履歴の更新がおこなわれる際は一時的に再起動履歴情報部分の情報は表示されません。履歴情報部分が表示されない場合は、情報収集のために 3 分程度待った後、再度取得ボタンを押してください。 オプション装置は対象外です。
接続フェーズ	v7.5.105 を含む以降のソフトウェアで表示されます。 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、取得している情報を表示します。 オプション装置の情報は Anchor-AC の情報に含まれます。
VLAN	display vlan コマンド、及び、display interface Vlan-interface brief コマンド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。

タブ名	説明
ファイル管理	v7.5.129 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。

8.4 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。

8.5 NetMeisterの設定例

I. ネットワーク要件

図 8-22 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。

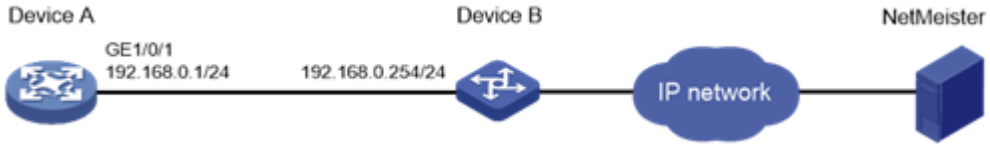


図 8-22 ネットワーク図

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。

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
```

8.6 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。

8.6.1 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、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。

8.6.2 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:**

v7.5.129 を含む以降の送付とウェアでは、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。

8.6.3 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。

8.6.4 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:**

Anchor-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、Anchor-AC がバージョンアップされた後に Anchor-AC と Anchor-FIT 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は、NetMeister から ipe 形式のソフトウェアを取得し、bin 形式に解凍して装置にセットするため、その分のディレクトリの空き容量が必要です。
v7.5.129 以降のソフトウェアでは Netmeister 機能[ファイルを管理する]によって不要なデータの削除ができます。
Netmeister 機能[ファイルを管理する]を利用できない場合、下記のいずれかの方法でディレクトリの空き容量の確認とファイル削除ができます。

- 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**)を実行する。
- NetMeister 機能[リモートログイン]やコンソールケーブル接続等して、直接装置でコマンドを実行する。

3) 問題が解決しない場合、NEC に問い合わせてください。

8.6.5 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。v7.5.105 以降のソフトウェアでは、**netmeister updae** コマンドによって周期的な装置情報更新を即座におこなうことができます。
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。

目次

このセクションのページは **10-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 9-6
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 9-10
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 9-11
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 9-12
9.8.1 ローカルパケットキャプチャ設定例 (Anchor-AC モード) 9-12
9.8.2 ローカルパケットキャプチャ設定例 (FAT モード) 9-13

9章 パケットキャプチャの設定

🕮 **メモ：**

この機能は、ソフトウェアバージョン 7.5.143b を含む以降のソフトウェアからサポートしています。

本章では、パケットキャプチャの設定コマンドについて説明します。本章のコマンドは、QX-W1200 シリーズの Anchor-AC と FAT モードで実行することができます。

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。

⚠ **注意:**

Anchor-AC 自身の radio を指定したパケットキャプチャはできません。

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。

カテゴリー	説明	例
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。
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。

変数タイプ	説明	例
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。
<<	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。

- インタフェー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。
- インタフェー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 は発信インタフェースのデフォルト VLAN ID を表します。レイヤ 2 パケットの場合、xx は着信インタフェースのデフォルト 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**
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。
&&	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。(Anchor-ACの場合)	**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。 FTPサーバ上にファイルを保存できるのは、Anchor-FITのapのみです。Anchoor-ACのapは保存できません。
AP無線でローカルパケットキャプチャを設定します。(FATの場合)	**packet-capture local interface** *interface-type interface-number* [**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 (Anchor-AC モード)

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。

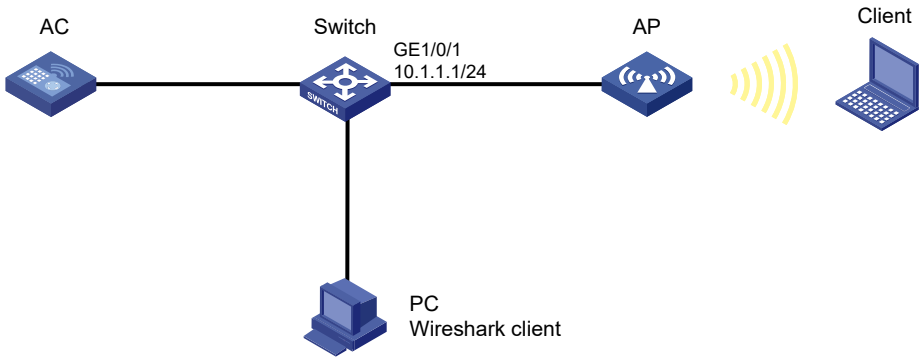


図 9-1 ネットワーク図

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 cfa0:/
```

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。）

9.8.2 ローカルパケットキャプチャ設定例 (FAT モード)

I. ネットワーク要件

図 9-2に示すように、AP の無線インタフェース 1/0/1 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。

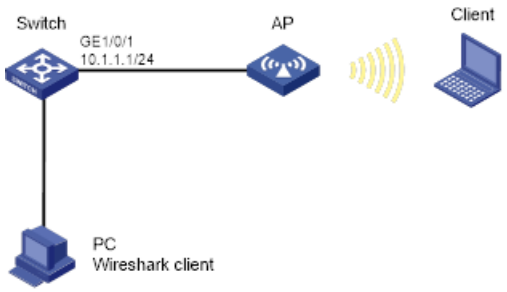


図 9-2 ネットワーク図

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 cfa0:/
```

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 の無線インタフェース 1/0/1 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。

```
<AP> packet-capture local interface WLAN-Radio 1/0/1 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。）

QX-W1200 シリーズ アクセスポイント

オペレーションマニュアル

11. 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 **11-x-x** です。

1 章 謝辞（Acknowledgments） 1-1
1.1 QX-W1200 シリーズ 謝辞 (Acknowledgments)..... 1-1

1章 謝辞（Acknowledgments）

1.1 QX-W1200シリーズ 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.

The following software(s) may be included in this product:

[aes.js 3.1.2 (part of crypto-js 3.1.2)]
[COPYRIGHT]
 (c) 2009-2013 by Jeff Mott. 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 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.

[aws-iot-device-sdk-embedded-C 3.1.1]

[COPYRIGHT]
    Copyright (C) 2020 Amazon.com, Inc. or its affiliates. All Rights Reserved.

[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.

[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]
[COPYRIGHT]
Copyright 2012 Stefan Petre

[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.
-------------------------------------------------------------------------------
---
[bootstrap-modal 2.1]
/* ============================================================
 *[Copyright]
 * Copyright 2011-2012 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.
 *                  ============================================================
*/-------------------------------------------------------------------------------
-----
[bootstrapSwitch 1.3.0]
[COPYRIGHT]
  bootstrapSwitch v1.3 by Larentis Mattia @spiritualGuru

[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

[busybox 1.20.1]
[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.
------------------------------------------------------------------------------
---
[cjson 1.7.12]
[COPYRIGHT]
  Copyright (c) 2009-2017 Dave Gamble and cJSON contributors

[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.

[cpio 2.11]
[COPYRIGHT]
Copyright (C) 1994, 1995, 1996, 1999, 2000, 2001, 2002, 2004, 2005,
2006, 2007, 2008, 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>.

[curl 7.21.2]
[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.


------------------------------------------------------------------------------
---
[domain stack framework 8.0.0 (part of FreeBSD 8.0.0)]
[COPYRIGHT]
  Copyright (c) 1992-2009 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

[dosfstools 3.0.12]
[COPYRIGHT]
Copyright (C) 1998-2005 Roman Hodek <Roman.Hodek@informatik.uni-erlangen.de>

[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>.

[dynamic linking loader 0.9.32 (part of uclibc 0.9.32)]
[Copyright]
Copyright (C) 1991, 1999 Free Software Foundation, Inc.
Copyright (C) 2000-2006 Erik Andersen <andersen@uclibc.org>
Copyright (C) 2000-2005 Manuel Novoa III <mjn3@uclibc.org>
Copyright (C) 2000-2005 David K. Williams <kodoman@wanadoo.es>
Copyright (C) 2005-2024 Waldemar Brodkorb <wbx@uclibc-ng.org>
Copyright (C) 2006-2014 Bernhard Reutner-Fischer <uclibc@btmx.net>
Copyright (C) 2014-2024 Waldemar Brodkorb and uclibc-ng contributors

[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!

[echarts.js 2.2.7 (part of echarts 2.2.7)]
[COPYRIGHT]
Copyright (c) 2013, Baidu Inc.
All rights reserved.

[LICENSE]
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.css 4.1.0 (part of font-awesome 4.1.0)]
[COPYRIGHT]
Font Awesome 4.1.0 by @davegandy - http://fontawesome.io - @fontawesome

[LICENSE]
http://fontawesome.io/license (Font: SIL OFL 1.1, CSS: MIT License)

SIL OFL 1.1

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.

MIT 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.

[freeradius-server3.0.27]
[COPYRIGHT]
  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.

[ftp client 8.0.0 (part of FreeBSD 8.0.0)]
[COPYRIGHT]
Copyright (c) 1992-2009 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

[grpc 1.4.2]
[COPYRIGHT]
Copyright 2015, Google Inc.
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 Google 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 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.

[inet stack 8.0.0 (part of FreeBSD 8.0.0)]
[COPYRIGHT]
Copyright (c) 1992-2009 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

[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.

--------------------------------------------------------------------------
---
[jquery.event.drag 2.2]
[COPYRIGHT]
  Copyright (c) 2008-2023 ThreeDubMedia

[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.
--------------------------------------------------------------------------
---
[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.

[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 1.13.1]
[LICENSE]
GNU LIBRARY GENERAL PUBLIC LICENSE
Version 2, June 1991

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.]

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.

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.

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.

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 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.

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.

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.

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

```
      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!
--------------------------------------------------------------------------
---
[libssh2 1.4.3]
[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
  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.

--------------------------------------------------------------------------------
---
[libyang2.0.7]
[COPYRIGHT]
  Copyright (c) 2015-2021, CESNET
  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 CESNET nor the names of
  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.

--------------------------------------------------------------------------------
---
[lz4 r120]
[COPYRIGHT]
  Copyright (c) 2011-2014, Yann Collet
  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.

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.

--------------------------------------------------------------------------------
---
[multi-select 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.
--------------------------------------------------------------------------------
---
[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 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.

--------------------------------------------------------------------------
---
[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]Takao Abe <takao_abe@xurb.jp> Clock driver for JJY receivers
2. [2]Mark Andrews <mark_andrews@isc.org> Leitch atomic clock controller
3. [3]Bernd Altmeier <altmeier@atlsoft.de> hopf Elektronik serial line and PCI-bus devices
4. [4]Viraj Bais <vbais@mailman1.intel.com> and [5]Clayton Kirkwood <kirkwood@striderfm.intel.com> port to WindowsNT 3.5
5. [6]Michael Barone <michael,barone@lmco.com> GPSVME fixes
6. [7]Karl Berry <karl@owl.HQ.ileaf.com> syslog to file option
7. [8]Greg Brackley <greg.brackley@bigfoot.com> Major rework of WINNT port. Clean up recvbuf and iosignal code into separate modules.
8. [9]Marc Brett <Marc.Brett@westgeo.com> Magnavox GPS clock driver
9. [10]Piete Brooks <Piete.Brooks@cl.cam.ac.uk> MSF clock driver, Trimble PARSE support
10. [11]Nelson B Bolyard <nelson@bolyard.me> update and complete broadcast and crypto features in sntp
11. [12]Jean-Francois Boudreault <Jean-Francois.Boudreault@viagenie.qc.ca> IPv6 support
12. [13]Reg Clemens <reg@dwf.com> Oncore driver (Current maintainer)
13. [14]Steve Clift <clift@ml.csiro.au> OMEGA clock driver
14. [15]Casey Crellin <casey@csc.co.za> vxWorks (Tornado) port and help with target configuration
15. [16]Sven Dietrich <sven_dietrich@trimble.com> Palisade reference clock driver, NT adj. residuals, integrated Greg's Winnt port.
16. [17]John A. Dundas III <dundas@salt.jpl.nasa.gov> Apple A/UX port
17. [18]Torsten Duwe <duwe@immd4.informatik.uni-erlangen.de> Linux port
18. [19]Dennis Ferguson <dennis@mrbill.canet.ca> foundation code for NTP Version 2 as specified in RFC-1119
19. [20]John Hay <jhay@icomtek.csir.co.za> IPv6 support and testing
20. [21]Dave Hart <davehart@davehart.com> General maintenance, Windows port interpolation rewrite
21. [22]Claas Hilbrecht <neoclock4x@linum.com> NeoClock4X clock driver
22. [23]Glenn Hollinger <glenn@herald.usask.ca> GOES clock driver
23. [24]Mike Iglesias <iglesias@uci.edu> DEC Alpha port
24. [25]Jim Jagielski <jim@jagubox.gsfc.nasa.gov> A/UX port
25. [26]Jeff Johnson <jbj@chatham.usdesign.com> massive prototyping overhaul
26. [27]Hans Lambermont <Hans.Lambermont@nl.origin-it.com> or [28]<H.Lambermont@chello.nl> ntpsweep
27. [29]Poul-Henning Kamp <phk@FreeBSD.ORG> Oncore driver (Original author)
28. [30]Frank Kardel [31]<kardel (at) ntp (dot) org> PARSE <GENERIC> driver (>14 reference clocks), STREAMS modules for PARSE, support scripts, syslog cleanup, dynamic interface handling
29. [32]William L. Jones <jones@hermes.chpc.utexas.edu> RS/6000 AIX modifications, HPUX modifications
30. [33]Dave Katz <dkatz@cisco.com> RS/6000 AIX port
31. [34]Craig Leres <leres@ee.lbl.gov> 4.4BSD port, ppsclock, Magnavox GPS clock driver
32. [35]George Lindholm <lindholm@ucs.ubc.ca> SunOS 5.1 port
33. [36]Louis A. Mamakos <louie@ni.umd.edu> MD5-based authentication
34. [37]Lars H. Mathiesen <thorinn@diku.dk> adaptation of foundation code for Version 3 as specified in RFC-1305
35. [38]Danny Mayer <mayer@ntp.org>Network I/O, Windows Port, Code Maintenance
36. [39]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
37. [40]Wolfgang Moeller <moeller@gwdgv1.dnet.gwdg.de> VMS port

38. [41]Jeffrey Mogul <mogul@pa.dec.com> ntptrace utility
39. [42]Tom Moore <tmoore@fievel.daytonoh.ncr.com> i386 svr4 port
40. [43]Kamal A Mostafa <kamal@whence.com> SCO OpenServer port
41. [44]Derek Mulcahy <derek@toybox.demon.co.uk> and [45]Damon Hart-Davis <d@hd.org> ARCRON MSF clock driver
42. [46]Rob Neal <neal@ntp.org> Bancomm refclock and config/parse code maintenance
43. [47]Rainer Pruy <Rainer.Pruy@informatik.uni-erlangen.de> monitoring/trap scripts, statistics file handling
44. [48]Dirce Richards <dirce@zk3.dec.com> Digital UNIX V4.0 port
45. [49]Wilfredo Snchez <wsanchez@apple.com> added support for NetInfo
46. [50]Nick Sayer <mrapple@quack.kfu.com> SunOS streams modules
47. [51]Jack Sasportas <jack@innovativeinternet.com> Saved a Lot of space on the stuff in the html/pic/ subdirectory
48. [52]Ray Schnitzler <schnitz@unipress.com> Unixware1 port
49. [53]Michael Shields <shields@tembel.org> USNO clock driver
50. [54]Jeff Steinman <jss@pebbles.jpl.nasa.gov> Datum PTS clock driver
51. [55]Harlan Stenn <harlan@pfcs.com> GNU automake/autoconfigure makeover, various other bits (see the ChangeLog)
52. [56]Kenneth Stone <ken@sdd.hp.com> HP-UX port
53. [57]Ajit Thyagarajan <ajit@ee.udel.edu>IP multicast/anycast support
54. [58]Tomoaki TSURUOKA <tsuruoka@nc.fukuoka-u.ac.jp>TRAK clock driver
55. [59]Paul A Vixie <vixie@vix.com> TrueTime GPS driver, generic TrueTime clock driver
56. [60]Ulrich Windl <Ulrich.Windl@rz.uni-regensburg.de> corrected and validated HTML documents according to the HTML DTD

[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.
--------------------------------------------------------------------------
---
[OpenNHRP 0.14.1]
[COPYRIGHT]
  Copyright (c) 2007-2012 Timo Teräs

[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.
--------------------------------------------------------------------------
---
[openpam 20071221]
[COPYRIGHT]
  Copyright (c) 2002-2003 Networks Associates Technology, Inc.
  Copyright (c) 2004-2007 Dag-Erling Smørgrav
  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 Yrjl? 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.                                                            *
 *****************************************************************************
/

-------------------------------------------------------------------------------
---
[openssl 1.0.2n]
  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. Actually both licenses are BSD-style
  Open Source licenses. In case of any license issues related to OpenSSL
  please contact openssl-core@openssl.org.

  OpenSSL License
```

```
 --------------

/* ====================================================================
 * Copyright (c) 1998-2017 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.]
 */

--------------------------------------------------------------------------------
---
[ping 8.0.0 (part of FreeBSD 8.0.0)]
[COPYRIGHT]
  Copyright (c) 1992-2009 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 8.0.0 (part of FreeBSD 8.0.0)]
[COPYRIGHT]
Copyright (c) 1992-2009 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

[pthread 0.9.32 (part of uclibc 0.9.32)]
[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!

[pure-ftpd 1.0.29]
[COPYRIGHT]
Copyright (c) 2001 - 2010
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) 1995-2000 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

[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.

--------------------------------------------------------------------------
---
[result.h 1.73]
[COPYRIGHT]
  Copyright (C) 2004-2009, 2012, 2014  Internet Systems Consortium, Inc. ("ISC")
  Copyright (C) 1998-2001, 2003  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.

--------------------------------------------------------------------------
---
[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]
[LICENSE]
** 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.
**
******************************************************************************
--------------------------------------------------------------------------------
---
[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) 1989-1994 The Regents of the University of California
  Copyright (c) 1992-1999 Karl Lehenbauer & Mark Diekhans
  Copyright (c) 1992-1999 Karl Lehenbauer and Mark Diekhans
  Copyright (c) 1993-1997 Bell Labs Innovations for Lucent Technologies
  Copyright (c) 1994 The Australian National University
  Copyright (c) 1994-2000 Sun Microsystems, Inc
  Copyright (c) 1995-1997 Roger E. Critchlow Jr
  Copyright (c) 1997-2000 Ajuba Solutions
  Copyright (c) 1997-2000 Scriptics Corporation
  Copyright (c) 1998 Mark Harrison
  Copyright (c) 2000 Jeffrey Hobbs
  Copyright (c) 2001 ActiveState Tool Corp
  Copyright (c) 2001 Vincent Darley
  Copyright (c) 2001-2004 ActiveState Corporation
  Copyright (c) 2001-2005 Kevin B. Kenny <kennykb(at)acm.org>
  Copyright (c) 2001-2008 Donal K. Fellows
  Copyright          (c)          2002-2008          Andreas          Kupries
<andreas_kupries(at)users.sourceforge.net>
  Copyright (c) 2003 George Petasis <petasis(at)iit.demokritos.gr>
  Copyright (c) 2003 Simon Geard
  Copyright (c) 2003-2006 Joe English
  Copyright (c) 2006 Miguel Sofer
  Copyright (c) 2006-2007 Daniel A. Steffen <das(at)users.sourceforge.net>
  Copyright (c) 2006-2008 ActiveState Software Inc
  Copyright (c) 2008 Pat Thoyts

[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 7.2.0 (part of FreeBSD 7.2.0)]
[COPYRIGHT]
  Copyright (c) 1992-2009 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 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 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
--------------------------------------------------------------------------------
---
[timer 0.9.32 (part of uclibc 0.9.32)]
[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!

[traceroute 8.0.0 (part of FreeBSD 8.0.0)]
[COPYRIGHT]
Copyright (c) 1992-2009 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 8.0.0 (part of FreeBSD 8.0.0)]
[COPYRIGHT]
Copyright (c) 1992-2009 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
--------------------------------------------------------------------------------
---
[twitter-bootstrap-wizard-1.0]
[COPYRIGHT]
  Copyright (c) 2013 - Vincent Gabriel & Jason Gill

[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.
--------------------------------------------------------------------------------
---
[u-boot 1.1.4]
[COPYRIGHT]
   (C) Copyright 2000 - 2005
   Wolfgang Denk, DENX Software Engineering, wd@denx.de.

[NOTE]
  NOTE! This copyright does *not* cover the so-called "standalone"
applications that use U-Boot services by means of the jump table
provided by U-Boot exactly for this purpose - this is merely
considered normal use of U-Boot, and does *not* fall under the
heading of "derived work".

  The header files "include/image.h" and "include/asm-*/u-boot.h"
define interfaces to U-Boot. Including these (unmodified) header
files in another file is considered normal use of U-Boot, and does
*not* fall under the heading of "derived work".

  Also note that the GPL below is copyrighted by the Free Software
Foundation, but the instance of code that it refers to (the U-Boot
source code) is copyrighted by me and others who actually wrote it.
-- Wolfgang Denk

[LICENSE]
          GNU GENERAL PUBLIC LICENSE
             Version 2, June 1991

 Copyright (C) 1989, 1991 Free Software Foundation, Inc.
     59 Temple Place, Suite 330, Boston, MA  02111-1307  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

[uclibc 0.9.32 (part of uclibc 0.9.32)]
[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!

[unix stack 8.0.0 (part of FreeBSD 8.0.0)]
[COPYRIGHT]
Copyright (c) 1992-2009 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 1.2.3]
[COPYRIGHT]
  Copyright (C) 1995-2004 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
