第 2 編 管理運用

1. 装置へのログイン

装置の起動と停止、ログインとログアウトについて説明します。

REF: コマンドの詳細については、『コマンドリファレンス』を参照してください。

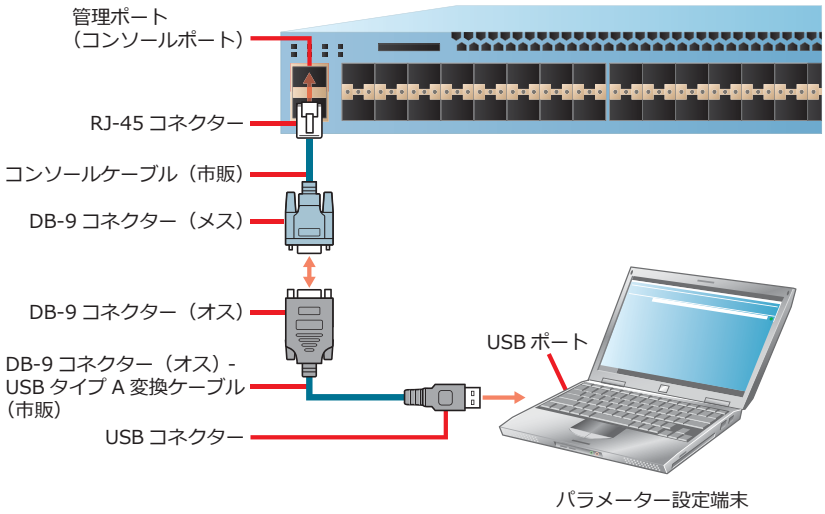
1.1 装置とパラメーター設定端末の接続

装置の監視や設定を行うには、**コンソールポート**（RJ-45 ポート）にパラメーター設定端末を接続します。パラメーター設定端末は、**RS-232C シリアルポート**を備えており、端末エミュレータを利用できる必要があります。

NOTE: パラメーター設定端末に RS-232C シリアルポートがない場合は、「DB-9 コネクター - USB タイプ A 変換ケーブル（市販）」を使用して接続します。

装置とパラメーター設定端末を接続するには、**コンソールケーブル**（一方が RJ-45 コネクターで、もう一方がメス型 DB-9 コネクター）を、装置のコンソールポートと、パラメーター設定端末の RS-232C シリアルポートに挿入します。

図 1-1 コンソールケーブルによる接続



1.2 端末エミュレータの設定

シリアル接続に対応した端末エミュレータを使用して、装置に接続します。端末エミュレータの接続プロパティを以下のように設定してください。

表 1-1 端末エミュレータの設定

項目	内容
接続先のシリアルポート	パラメーター設定端末の RS-232C シリアルポートを選択
データレート（ボー・レート）	9600bps
データ長	8bit
ストップビット	1bit
パリティー	なし
フロー制御	なし

NOTE: エミュレーションモードを選択できる場合は、「VT100」に設定してください。

1.3 装置の起動およびログイン

装置とパラメーター設定端末を接続した状態で、装置を起動して特権実行モードに遷移する操作を以下に示します。

NOTE: 他の章では、主に特権実行モードに遷移してからの操作を説明しています。

1. パラメーター設定端末で端末エミュレータを起動し、装置の電源を入れます。

```
Boot Procedure V1.00.01
  MAC Address: 00-40-66-A8-CF-10
  H/W Version: A

Power On Self Test: 100 %

Please Wait, Loading V1.00.01

Firmware: 100 %
UART init: 100 %

Starting firmware...

Device Discovery: 100 %
Configuration init: 100 %

Switch con0 is now available

Press any key to login...
```

2. 任意のキーを押します。

```
Ethernet Switch ApresiaNP7000-48X6L

Firmware: Build 1.00.01

>
```

3. 特権実行モードに遷移します。

```
> enable
#
```

1.4 ログアウトおよび装置の停止

装置の監視や設定が終了したら、ログアウトします。ログアウトする操作を以下に示します。

NOTE: 装置の電源を切る場合は、すべてのユーザーがログアウトしたことを確認してください。

1. 現在のグローバル設定モードまたはサブ設定モードを終了して、特権実行モードに遷移します。

```
(config-if-port)# end
#
```

2. ログアウトします。

```
# logout
```

3. 装置の電源を切ります。

2. コマンドの指定方法

装置の状態確認や設定のために使用するコマンドの指定方法について説明します。

REF: コマンドの詳細については、『コマンドリファレンス』を参照してください。

2.1 コマンドモードの主な種類

コマンドラインインターフェース（以後、CLI）の**プロンプト**は、ユーザーが接続している**コマンドモード**を表しています。主なコマンドモードは以下のとおりです。

表 2-1 コマンドモードの主な種類

プロンプト	コマンドモード
>	ユーザー実行モード
#	特権実行モード
(config)#	グローバル設定モード
(config-if-port)# **(config-if-vlan)#** **(config-if-port-channel)#**	サブ設定モード （左記の例は、インターフェース設定モード）

特権レベル

ユーザーアカウントには、特権レベルを割り当てることができます。各コマンドには使用できる特権レベルが設定されているため、ユーザーアカウントごとにアクセス可能なコマンドをある程度制御できます。特権レベルの概要は以下のとおりです。

表 2-2 特権レベルの概要

特権レベル	アクセス可能なコマンドモード	使用できるコマンドの概要
レベル 1	• ユーザー実行モード	• ほとんどの **show** コマンド *1 • **ping** や **telnet** などの一部の操作コマンド *2
レベル 12	• 特権実行モード（レベル 12） • グローバル設定モード • 任意の設定モード（一部除く）	• ほとんどの **show** コマンド *1 • **ping** や **telnet**、**clear** コマンドなどの一部の操作コマンド *2 • セキュリティー関連の設定コマンドを除く設定コマンド
レベル 15	• 特権実行モード（レベル 15） • グローバル設定モード • 任意の設定モード	• すべてのコマンド

*1：構成情報の表示コマンド（**show running-config**、**show startup-config**）や、技術サポート情報の表示コマンド（**show tech-support**）などは、特権レベル 15 でのみ使用できます。

*2：構成情報の保存コマンド（**write**）や、装置の再起動コマンド（**reboot**）、その他の多くの操作コマンドは、特権レベル 15 でのみ使用できます。

ユーザーアカウントを作成していない場合に、特権レベルにアクセスするためのパスワードを設定するには、**enable password** コマンドを使用します。

CAUTION: パスワードとして「ap_recovery」は使用できません。

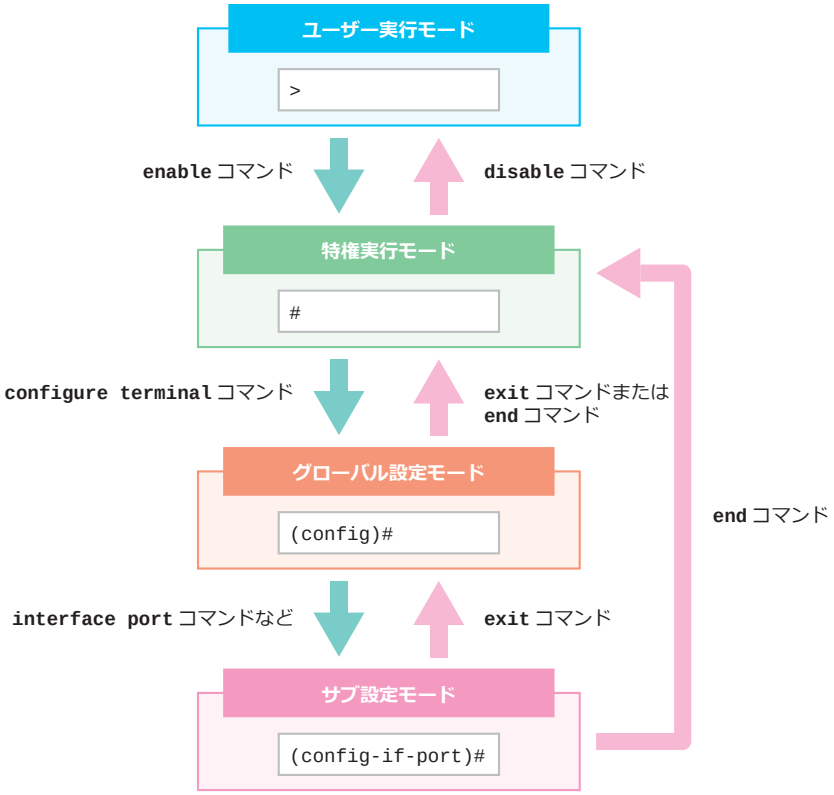
CAUTION: **enable password** コマンドを設定していない場合は、コンソールポート接続で装置にログインしているときにのみ、パスワードなしで特権レベル 15 に遷移できます。

REF: コマンドごとの特権レベルについては、『コマンドリファレンス』を参照してください。

コマンドモードの切り替え

コマンドモードを切り替えるには、下図のような適切なコマンドを使用する必要があります。たとえば、ユーザー実行モードから特権実行モードに遷移するには **enable** コマンドを使用します。逆に、特権実行モードからユーザー実行モードに遷移するには **disable** コマンドを使用します。

図 2-1 コマンドモードの遷移



NOTE: 装置に複数セッションでログインしている状態で、複数セッションから同時に設定を変更しないでください。複数セッションでログインしている状態では、グローバル設定モードに遷移するのは 1 つのセッションだけにしてください。

2.2 コマンドの編集操作

CLI でコマンドを編集する際に使用できる操作を以下に示します。

表 2-3 コマンドの編集操作

操作	説明
Enter キー	コマンドを実行します。
Delete キー	カーソル位置の文字を削除します。
Backspace キー	カーソル位置の 1 つ左の文字を削除します。
Ctrl+A キー	カーソルを行頭へ移動します。
Ctrl+E キー	カーソルを行末へ移動します。
Ctrl+K キー	カーソル位置の文字から行末までを削除します。
Ctrl+Z キー	グローバル設定モードまたはサブ設定モードの場合に、入力途中の文字列を破棄して特権実行モードに戻ります。
左矢印キー	カーソルを左へ移動します。
右矢印キー	カーソルを右へ移動します。
上矢印キーまたは Ctrl+P キー	コマンド履歴リスト（**show history** で確認可能）に記録された文字列を、新しいエントリーから順番に表示します。
下矢印キーまたは Ctrl+N キー	コマンド履歴リスト（**show history** で確認可能）に記録された文字列を、古いエントリーから順番に表示します。
Ctrl+R キー	文字の挿入モードと上書きモードを切り替えます。挿入モードの場合は、カーソル位置に入力した文字を挿入します。上書きモードの場合は、カーソル位置の文字を入力した文字に置き換えます。

2.3 コマンド入力の補助機能

CLI でコマンドを入力する際に使用できる補助機能を以下に示します。

省略形式での実行

コマンドの入力の際は、そのコマンドが認識できる最小限の文字列のみ入力することにより、コマンド文字列の入力を省略できます。

たとえば、"sh ter" と入力して実行すると、**`show terminal`** コマンドが実行されます。

```
# sh ter
Terminal Settings:
 Length: 24 lines
 Width: 255 columns
 Default Length: 24 lines
 Default Width: 255 columns
 Baud Rate: 9600 bps
```

TAB キーによるコマンド補完

コマンドの入力途中で TAB キーを押すと、その時点で選択できるコマンドが 1 つの場合は、残りのコマンド文字列が自動的に補完されます。

たとえば、"show en" と入力した時点で TAB キーを押した場合は、"show environment "（末尾に半角スペース）に補完されます。

```
# show en[TAB キー押下 ]
# show environment
```

? キーによるヘルプ機能

? キーを押した場合、選択可能なコマンド候補やパラメーターのヘルプが表示されます。

たとえば、"show m" と入力した時点で ? キーを押した場合は、"show m" 以降で選択可能なすべてのコマンド候補が表示されます。

```
# show m[? キー押下 ]
mac-address-table   mls                 mmrp-plus           monitor
multicast

# show m
```

たとえば、"show environment "（末尾に半角スペース）を入力した時点で ? キーを押した場合は、"show environment "（末尾に半角スペース）以降に選択可能なパラメーターとヘルプが表示されます。

```
# show environment [? キー押下 ]
fan                         Display fan status
health                      Display health status
memory                      Display memory status
power                       Display power status
temperature                 Display temperature status
|                           Output modifiers
<cr>

# show environment
```

2.4 show コマンドの共通操作

装置の状態および設定を確認するために各種 **show** コマンドを使用できます。

表示結果のフィルタリング

show コマンドの表示結果の表示範囲を制限できます。**show running-config** コマンドの表示結果をフィルタリングする場合を例に、動作を説明します。

NOTE: その他の **show** コマンドの表示結果をフィルタリングする場合は、「**show running-config**」を「**show environment**」にするなど、適宜読み替えてください。

NOTE: 任意の条件でフィルタリングする場合は、「**begin**」、「**include**」、「**exclude**」以降の文字列を置き換えてください。

表 2-4 表示結果のフィルタリング

コマンド	説明
show running-config | begin interface port 1/0/46	**show running-config** コマンドの表示結果のうち、「**interface port 1/0/46**」と一致する最初の行から、表示結果の最後の行までをすべて表示します。
show running-config | include ssh user	**show running-config** コマンドの表示結果のうち、「**ssh user**」を含む行をすべて表示します。
show running-config | exclude interface	**show running-config** コマンドの表示結果のうち、「**interface**」を含まない行をすべて表示します。

表示結果の確認操作

コマンド実行時に表示結果が 1 画面に収まらない場合、表示は一時停止され、以下の行が表示されます。

```
  CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

この状態では、以下の操作で表示結果をスクロールできます。

表 2-5 表示結果の確認操作

操作	説明
Ctrl+C キー、Esc キー、または Q キー	**show** コマンドの実行を終了します。
スペースキーまたは N キー	次のページを表示します。
Enter キー	次の行を表示します。
A キー	すべての情報を表示します。

CAUTION: スペースキーまたは N キーを押し続けると、Telnet が切断されることがあります。

2.5 インターフェースの表記規則

装置のインターフェースの表記規則を以下に示します。

物理ポートの表記規則

物理ポートの表記規則を以下に示します。

図 2-2 物理ポートの表記規則

- **インターフェースユニットの ID**
  スタックメンバーのボックス ID です。非スタック装置の場合は、デフォルト設定では 1 です。
- **スロットの ID**
  スロットの ID は常に 0 です。
- **ポートの ID**
  物理ポート番号です。

VLAN インターフェースの表記規則

VLAN インターフェースの表記規則を以下に示します。

図 2-3 VLAN インターフェースの表記規則

- **VLAN の ID**
  VLAN ID です。1 ～ 4094 の範囲で指定します。

  REF: 「vlan 10」のように vlan と VLAN ID の間に半角スペースが必要なコマンド、「vlan10」のように vlan と VLAN ID の間を空けない文字列のみ受け付けるコマンド、両方の文字列を受け付けるコマンドがあります。コマンドの詳細については、『コマンドリファレンス』を参照してください。

3. ファームウェアのアップデート方法

ファームウェアのアップデート方法について説明します。

REF: コマンドの詳細については、『コマンドリファレンス』を参照してください。

3.1 ファームウェアのアップデート（非スタック装置の場合）

非スタック装置のファームウェアのバージョンを 1.04.01 から 1.05.01 へ変更する場合の実施例を以下に示します。なお、この実施例では、現在のディレクトリーはデフォルト（ローカルフラッシュのルートディレクトリー）のままとします。

CAUTION: ファームウェアのアップデートを有効化するには、装置を再起動する必要があります。再起動の際は通信が停止するため、アップデートは作業時間を設けて実施してください。

1. 現在のファームウェアのバージョンを確認します。

```
sw1# show version

System MAC Address: 00-40-66-AA-52-1B

Unit ID    Module Name                    Versions
-------  --------------------------  --------------------
   1      ApresiaNP7000-48X6L          H/W:A
                                       Bootloader:1.00.01
                                       Runtime:1.04.01
                                       CPLD:13


sw1#
```

2. IP アドレスが［192.168.10.100］の TFTP サーバーから、ファイル名が［AEOS-NP7000_R10501.had］のブートイメージファイルをローカルフラッシュにコピーします。なお、コピー後のファイル名を［AEOS-NP7000_R10501.had］に設定します。

```
sw1# copy tftp: flash:

Address of remote host []? 192.168.10.100
Source filename []? AEOS-NP7000_R10501.had
Destination filename []? AEOS-NP7000_R10501.had
 Accessing tftp://192.168.10.100/AEOS-NP7000_R10501.had...
 Transmission start...
 Transmission finished, file length 10895504 bytes.
 Please wait, programming flash.............. Done.

sw1#
```

3. ダウンロードしたブートイメージファイルから、セカンダリーブートイメージファイルとして指定するブートイメージファイルをコピーします。なお、コピー後のファイル名を［AEOS-NP7000_R10501_sec.had］に設定します。

```
sw1# copy flash: flash:

Source filename []? AEOS-NP7000_R10501.had
Destination filename []? AEOS-NP7000_R10501_sec.had
 Copy in progress.......................... 100 %

sw1#
```

4. ファイル名が［AEOS-NP7000_R10501.had］と［AEOS-NP7000_R10501_sec.had］のファイルが、ローカルフラッシュに存在することを確認します。

```
sw1# dir

Directory of /c:
1    -rw      10895504 May 09 2019 15:15:20  AEOS-NP7000_R10501_sec.had
2    -rw      10895504 May 09 2019 15:14:41  AEOS-NP7000_R10501.had
3    -rw      10859044 Apr 09 2019 09:59:03  AEOS-NP7000_R10401.had
4    -rw          2216 May 09 2019 14:57:18  primary.cfg
5    -rw          2216 May 09 2019 14:57:20  secondary.cfg
6    d--             0 May 09 2019 05:58:14  system

536346624 bytes total (503234560 bytes free)

sw1#
```

5. 次回起動時のプライマリーブートイメージファイルを［AEOS-NP7000_R10501.had］に、セカンダリーブートイメージファイルを［AEOS-NP7000_R10501_sec.had］に設定します。

NOTE: この実施例では相対パスで指定していますが、絶対パス「boot image c:/AEOS-NP7000_R10501.had」で指定しても同様に設定できます。

```
sw1# configure terminal
sw1(config)# boot image AEOS-NP7000_R10501.had
sw1(config)# boot image AEOS-NP7000_R10501_sec.had secondary
sw1(config)# end
sw1#
```

6. 次回起動時のプライマリーブートイメージファイルが［/c:/AEOS-NP7000_R10501.had］に、セカンダリーブートイメージファイルが［/c:/AEOS-NP7000_R10501_sec.had］に設定されていることを確認します。

```
sw1# show boot

Unit 1
*(Configured)
 Primary boot image: /c:/AEOS-NP7000_R10501.had
 Primary boot config: /c:/primary.cfg
 Secondary boot image: /c:/AEOS-NP7000_R10501_sec.had
 Secondary boot config: /c:/secondary.cfg


Note: * indicates the used boot information.

sw1#
```

7. 装置を再起動します。

```
sw1# reboot

Are you sure you want to proceed with the system reboot?(y/n) y
Please wait, the switch is rebooting...
```

8. 再起動後、現在のファームウェアのバージョンを確認します。

```
Ethernet Switch ApresiaNP7000-48X6L

Firmware: Build 1.05.01

sw1> enable
sw1# show version

System MAC Address: 00-40-66-AA-52-1B

Unit ID    Module Name                    Versions
-------  ---------------------------  ---------------------
   1      ApresiaNP7000-48X6L           H/W:A
                                        Bootloader:1.00.01
                                        Runtime:1.05.01
                                        CPLD:13


sw1#
```

3.2 ファームウェアのアップデート（スタック構成の場合）

スタック構成のファームウェアのバージョンを 1.04.01 から 1.05.01 へ変更する場合の実施例を以下に示します。なお、この実施例では、ボックス ID 1 の装置がスタックマスターです。また、現在のディレクトリーはデフォルト（スタックマスターのローカルフラッシュのルートディレクトリー）のままとします。

> ***CAUTION:*** スタックを構成するすべての装置は、同一バージョンのファームウェアで起動する必要があります。そのため、ファームウェアのアップデートを有効化するには、スタック構成全体を再起動し、スタックを構成するすべての装置のファームウェアを同時にアップデートしてください。スタック構成全体の再起動の際は通信が停止するため、アップデートは作業時間を設けて実施してください。

1. 現在のファームウェアのバージョンを確認します。

```
sw1# show version

System MAC Address: 00-40-66-AA-52-1B

Unit ID    Module Name                    Versions
------- ---------------------------- --------------------
   1     ApresiaNP7000-48X6L          H/W:A
                                      Bootloader:1.00.01
                                      Runtime:1.04.01
                                      CPLD:13

   2     ApresiaNP7000-48X6L          H/W:A
                                      Bootloader:1.00.01
                                      Runtime:1.04.01
                                      CPLD:13


sw1#
```

2. IP アドレスが［192.168.10.100］の TFTP サーバーから、ファイル名が［AEOS-NP7000_R10501.had］のブートイメージファイルを、すべてのスタックメンバーのローカルフラッシュにコピーします。なお、コピー後のファイル名を［AEOS-NP7000_R10501.had］に設定します。

```
sw1# copy tftp: flash:

Address of remote host []? 192.168.10.100
Source filename []? AEOS-NP7000_R10501.had
Destination filename []? AEOS-NP7000_R10501.had
 Accessing tftp://192.168.10.100/AEOS-NP7000_R10501.had...
 Transmission start...
 Transmission finished, file length 10895504 bytes.
 Transmission to slave start.................. Done.
 Transmission to slave finished, file length 10895504 bytes.
 Please wait, programming flash.............. Done.
 Wait slave programming flash complete...
 Done.

sw1#
```

3. すべてのスタックメンバーで、ダウンロードしたブートイメージファイルから、セカンダリーブートイメージファイルとして指定するブートイメージファイルをコピーします。なお、コピー後のファイル名を［AEOS-NP7000_R10501_sec.had］に設定します。

```
sw1# copy flash: flash:

Source filename []? AEOS-NP7000_R10501.had
Destination filename []? AEOS-NP7000_R10501_sec.had
 Copy in progress.......................... 100 %

sw1#
sw1# copy flash: flash:

Source filename []? unit2:/c:/AEOS-NP7000_R10501.had
Destination filename []? unit2:/c:/AEOS-NP7000_R10501_sec.had
 Copy in progress.......................... 100 %

sw1#
```

4. ファイル名が［AEOS-NP7000_R10501.had］と［AEOS-NP7000_R10501_sec.had］のファイルが、すべてのスタックメンバーのローカルフラッシュに存在することを確認します。

```
sw1# dir

Directory of /c:
1   -rw      10895504 May 09 2019 15:27:55  AEOS-NP7000_R10501_sec.had
2   -rw      10895504 May 09 2019 15:27:08  AEOS-NP7000_R10501.had
3   -rw          3745 May 09 2019 15:26:06  primary.cfg
4   -rw      10859044 Apr 09 2019 09:59:03  AEOS-NP7000_R10401.had
5   -rw          2216 May 09 2019 14:57:20  secondary.cfg
6   d--             0 May 09 2019 06:22:26  system

536346624 bytes total (503228416 bytes free)

sw1#
sw1# dir unit2:/c:/

Directory of /unit2:/c:/
1   -rw      10895504 May 09 2019 15:28:41  AEOS-NP7000_R10501_sec.had
2   -rw      10895504 May 09 2019 15:27:07  AEOS-NP7000_R10501.had
3   -rw          3745 May 09 2019 15:26:06  primary.cfg
4   -rw      10859044 Dec 04 2018 13:04:05  AEOS-NP7000_R10401.had
5   -rw          2216 May 09 2019 14:57:29  secondary.cfg
6   d--             0 May 09 2019 06:22:52  system

536346624 bytes total (503232512 bytes free)

sw1#
```

5. すべてのスタックメンバーで、次回起動時のプライマリーブートイメージファイルを［AEOS-NP7000_R10501.had］に、セカンダリーブートイメージファイルを［AEOS-NP7000_R10501_sec.had］に設定します。

NOTE: この実施例では、対象がスタックマスターの場合は相対パスで指定していますが、絶対パス「boot image c:/AEOS-NP7000_R10501.had」で指定しても同様に設定できます。

NOTE: 対象がスタックマスター以外の装置の場合は、先頭に「unitX:/」（X はボックス ID）を付加した絶対パスを指定します。

```
sw1# configure terminal
sw1(config)# boot image AEOS-NP7000_R10501.had
sw1(config)# boot image AEOS-NP7000_R10501_sec.had secondary
sw1(config)#
sw1(config)# boot image unit2:/c:/AEOS-NP7000_R10501.had
sw1(config)# boot image unit2:/c:/AEOS-NP7000_R10501_sec.had secondary
sw1(config)# end
sw1#
```

6. すべてのスタックメンバーで、次回起動時のプライマリーブートイメージファイルが［/c:/AEOS-NP7000_R10501.had］に、セカンダリーブートイメージファイルが［/c:/AEOS-NP7000_R10501_sec.had］に設定されていることを確認します。

```
sw1# show boot

Unit 1
*(Configured)
 Primary boot image: /c:/AEOS-NP7000_R10501.had
 Primary boot config: /c:/primary.cfg
 Secondary boot image: /c:/AEOS-NP7000_R10501_sec.had
 Secondary boot config: /c:/secondary.cfg

Unit 2
*(Configured)
 Primary boot image: /c:/AEOS-NP7000_R10501.had
 Primary boot config: /c:/primary.cfg
 Secondary boot image: /c:/AEOS-NP7000_R10501_sec.had
 Secondary boot config: /c:/secondary.cfg


Note: * indicates the used boot information.

sw1#
```

7. スタック構成全体を再起動します。

```
sw1# reboot

Are you sure you want to proceed with the system reboot?(y/n) y
Please wait, the switch is rebooting...
```

8. 再起動後、すべてのスタックメンバーの現在のファームウェアのバージョンを確認します。

```
Ethernet Switch ApresiaNP7000-48X6L

Firmware: Build 1.05.01

sw1> enable
sw1# show version

System MAC Address: 00-40-66-AA-52-1B

Unit ID    Module Name                      Versions
-------  ---------------------------  ---------------------
   1      ApresiaNP7000-48X6L           H/W:A
                                        Bootloader:1.00.01
                                        Runtime:1.05.01
                                        CPLD:13

   2      ApresiaNP7000-48X6L           H/W:A
                                        Bootloader:1.00.01
                                        Runtime:1.05.01
                                        CPLD:13


sw1#
```

3.3 SD カードブート装置でのファームウェアのアップデート

SD カードブートを使用している装置は、SD カードに保存されたブートイメージファイル（apresia-software.had）で起動します。そのため、その装置でファームウェアのアップデートを行うには、SD カードに保存されたブートイメージファイルを以下のような方法で更新する必要があります。

- SD カードが使用可能なパソコンなどを利用して更新
- ローカルフラッシュにダウンロードした新しいプライマリーブートイメージファイルから、**backup clone** コマンドを使用して更新

ここでは、**backup clone** コマンドを使用して、SD カードに保存されたブートイメージファイルを更新し、装置を再起動してファームウェアのアップデートを行う方法を説明します。

3.3.1 非スタック装置の場合

1. 「ファームウェアのアップデート（非スタック装置の場合）」の、再起動前までの手順 1 ～ 6 を実施します。
2. **backup clone** コマンドを実行し、プライマリーブートイメージファイルとして指定したファイルを、SD カードに保存されたブートイメージファイル（apresia-software.had）として上書き更新します。
3. 念のため、**more** コマンドを使用して SD カードに保存されたランタイムバージョンテキストファイル（apresia-system-name.txt）を参照し、ブートイメージファイル（apresia-software.had）のバージョンが変更後のバージョンであることを確認します。

   NOTE: ランタイムバージョンテキストファイル（apresia-system-name.txt）には、**backup clone** コマンド実行時に SD カードに保存されたブートイメージファイル（apresia-software.had）のバージョン情報が保存されます。
4. 装置を再起動します。
5. SD カードブートで起動後、現在のファームウェアのバージョンを確認します。

3.3.2 スタック構成の場合

1. 「ファームウェアのアップデート（スタック構成の場合）」の、再起動前までの手順 1 ～ 6 を実施します。
2. **backup clone** コマンドを実行し、すべてのスタックメンバーで、プライマリーブートイメージファイルとして指定したファイルを、SD カードに保存されたブートイメージファイル（apresia-software.had）として上書き更新します。
3. 念のため、すべてのスタックメンバーで、**more** コマンドを使用して SD カードに保存されたランタイムバージョンテキストファイル（apresia-system-name.txt）を参照し、ブートイメージファイル（apresia-software.had）のバージョンが変更後のバージョンであることを確認します。

   NOTE: ランタイムバージョンテキストファイル（apresia-system-name.txt）には、**backup clone** コマンド実行時に SD カードに保存されたブートイメージファイル（apresia-software.had）のバージョン情報が保存されます。
4. スタック構成全体を再起動します。
5. SD カードブートで起動後、すべてのスタックメンバーの現在のファームウェアのバージョンを確認します。

3.4 2 台スタック構成での一時的なバージョンチェック無視機能

2 台スタック構成での一時的なバージョンチェック無視機能は、2 台スタック構成でのファームウェアのアップデート時に、一時的にスタックメンバーのバージョンチェック処理を無視する機能です。本機能を有効にするには **`stack version check ignore`** コマンドを使用します。

> ***NOTE:*** stack version check ignore は、NP7000 の 1.11.01 以降、NP5000 の 1.11.01 以降、NP3000 の 1.11.01 以降、NP2100 の 1.13.01 以降、NP2500 の 1.12.01 以降でサポートしています。

スタックを構成するすべての装置は、同一バージョンのファームウェアである必要があります。そのため、スタック構成でのファームウェアのアップデート時は、通常はスタック構成全体を再起動して、スタックを構成するすべての装置のファームウェアを同時にアップデートする必要があります。

2 台スタック構成でのファームウェアのアップデート時に stack version check ignore を有効にすると、一時的にスタックメンバーのバージョンチェック処理を無視し、スタックメンバー装置を 1 台ずつ再起動してアップデートすることができるようになります。

これにより、主にレイヤー 2 装置として利用するスタック構成において、ファームウェアのアップデート作業時のロス時間を少なくすることが期待できます。

なお、stack version check ignore はファームウェアのアップデート作業時に一時的に有効にして、アップデート作業が完了したら無効に戻すことを想定しています。そのため、stack version check ignore を有効設定のまま定常的に運用することは未サポートです。

> ***NOTE:*** stack version check ignore は、2 台スタック構成の場合のみサポートしています。3 台スタック構成、または 4 台スタック構成で使用することは未サポートです。
>
> ***NOTE:*** 本機能はあくまでスタックメンバーのバージョンチェック処理を無視する機能です。stack version check ignore を有効にしても、スタック使用時の制限事項は変わらないことに注意してください。
>
> ***NOTE:*** stack version check ignore を使用するには、ファームウェアのアップデート前とアップデート後の両方のバージョンで本機能がサポートされている必要があります。そのため、stack version check ignore が未実装のバージョンに変更する際は、本機能は使用しないでください。

3.4.1 手順例（1）プリエンプトモード無効、2 台スタック構成（その 1）

この手順例ではスタックマスターの切り替わりは 1 回ですが、ファームウェアのアップデート前とアップデート後で、マスターの役割になる装置が変更されます。

手順例の前提条件は以下のとおりです。

- プリエンプトモードは無効。
- 実施前は、装置 1（優先度 10 設定）がスタックマスター、装置 2（優先度 20 設定）がバックアップマスターになっているとする。
- ファームウェアのアップデートにおける事前作業（新ファームウェアのダウンロード、**`boot image`** コマンドによる次回起動時のブートイメージファイルの設定など）は完了済みとする。

1. ファームウェアのアップデート前の状態を確認します。
・装置 1：マスター
・装置 2：バックアップ

2. **stack version check ignore** コマンドで、一時的にスタックメンバーのバージョンチェック処理を無視するように変更します。その後、設定を保存して、**show stack** コマンドで確認します。

```
# stack version check ignore
#
# write memory

Destination filename startup-config? [y/n]:  y

Saving all configurations to NV-RAM.......... Done.

#
# show stack

Stacking Mode        : Enabled
Stack Preempt        : Disabled
Trap State           : Disabled
Port-channel mode    : All
Stack-port load-balance: default
Version check        : Disabled      ※ スタックメンバーのバージョンチェック処理を無視
~~省略~~
```

3. バックアップマスター（装置 2）を再起動、または電源 OFF/ON して、新ファームウェアにアップデートします。装置 2 が起動してスタック構成に取り込まれるのを待ちます。
・装置 1：マスター
・装置 2：バックアップ → バックアップ

4. スタックマスター（装置 1）を再起動、または電源 OFF/ON して、新ファームウェアにアップデートします。装置 1 が起動してスタック構成に取り込まれるのを待ちます。この手順の実行時にスタックマスターの切り替わりが発生します。
・装置 1：マスター → バックアップ
・装置 2：バックアップ → マスター

5. **no stack version check ignore** コマンドで、スタックメンバーのバージョンチェック処理を有効に戻します。その後、設定を保存して、**show stack** コマンドで確認します。

```
# no stack version check ignore
#
# write memory

Destination filename startup-config? [y/n]:  y

Saving all configurations to NV-RAM.......... Done.

#
# show stack

Stacking Mode        : Enabled
Stack Preempt        : Disabled
Trap State           : Disabled
Port-channel mode    : All
Stack-port load-balance: default
Version check        : Enabled       ※ スタックメンバーのバージョンチェック処理は有効
~~省略~~
```

3.4.2 手順例（2）プリエンプトモード無効、2 台スタック構成（その 2）

この手順例ではスタックマスターの切り替わりは 2 回ですが、ファームウェアのアップデート前とアップデート後で、同じ装置がマスターになります。

手順例の前提条件は以下のとおりです。

- プリエンプトモードは無効。
- 実施前は、装置 1（優先度 10 設定）がスタックマスター、装置 2（優先度 20 設定）がバックアップマスターになっているとする。
- ファームウェアのアップデートにおける事前作業（新ファームウェアのダウンロード、**boot image** コマンドによる次回起動時のブートイメージファイルの設定など）は完了済みとする。

1. ファームウェアのアップデート前の状態を確認します。
・装置 1：マスター
・装置 2：バックアップ

2. **stack version check ignore** コマンドで、一時的にスタックメンバーのバージョンチェック処理を無視するように変更します。その後、設定を保存して、**show stack** コマンドで確認します。

```
# stack version check ignore
#
# write memory

Destination filename startup-config? [y/n]:  y

Saving all configurations to NV-RAM.......... Done.

#
# show stack

Stacking Mode        : Enabled
Stack Preempt        : Disabled
Trap State           : Disabled
Port-channel mode    : All
Stack-port load-balance: default
Version check        : Disabled      ※ スタックメンバーのバージョンチェック処理を無視
～～省略～～
```

3. スタックマスター（装置 1）を再起動、または電源 OFF/ON して、新ファームウェアにアップデートします。装置 1 が起動してスタック構成に取り込まれるのを待ちます。この手順の実行時にスタックマスターの切り替わりが発生します。
・装置 1：マスター → バックアップ
・装置 2：バックアップ → マスター

4. スタックマスター（装置 2）を再起動、または電源 OFF/ON して、新ファームウェアにアップデートします。装置 2 が起動してスタック構成に取り込まれるのを待ちます。この手順の実行時にスタックマスターの切り替わりが発生します。
・装置 1：バックアップ → マスター
・装置 2：マスター → バックアップ

5. **no stack version check ignore** コマンドで、スタックメンバーのバージョンチェック処理を有効に戻します。その後、設定を保存して、**show stack** コマンドで確認します。

```
# no stack version check ignore
#
# write memory

Destination filename startup-config? [y/n]:  y

Saving all configurations to NV-RAM.......... Done.

#
# show stack

Stacking Mode        : Enabled
Stack Preempt        : Disabled
Trap State           : Disabled
Port-channel mode    : All
Stack-port load-balance: default
Version check        : Enabled      ※ スタックメンバーのバージョンチェック処理は有効
～～省略～～
```

3.4.3 手順例（3）プリエンプトモード有効、2 台スタック構成

この手順例ではスタックマスターの切り替わりは 2 回ですが、ファームウェアのアップデート前とアップデート後で、同じ装置がマスターになります。また、プリエンプトモードによるマスター切り替わり時のポート閉塞を伴うロスを避けるために、アップデート前に一時的にプリエンプトモードを無効に変更し、アップデート後にプリエンプトモードを有効に戻します。

手順例の前提条件は以下のとおりです。

- プリエンプトモードは有効。
- 実施前は、装置 1（優先度 10 設定）がスタックマスター、装置 2（優先度 20 設定）がバックアップマスターになっているとする。
- ファームウェアのアップデートにおける事前作業（新ファームウェアのダウンロード、**boot image** コマンドによる次回起動時のブートイメージファイルの設定など）は完了済みとする。

1. ファームウェアのアップデート前の状態を確認します。
・装置 1：マスター
・装置 2：バックアップ

2. **no stack preempt** コマンドで、一時的にプリエンプトモードを無効に変更します。**stack version check ignore** コマンドで、一時的にスタックメンバーのバージョンチェック処理を無視するように変更します。その後、設定を保存して、**show stack** コマンドで確認します。

```
# no stack preempt
#
# stack version check ignore
#
# write memory

Destination filename startup-config? [y/n]:  y

Saving all configurations to NV-RAM.......... Done.

#
# show stack

Stacking Mode        : Enabled
Stack Preempt        : Disabled      ※ プリエンプトモード無効
Trap State           : Disabled
Port-channel mode    : All
Stack-port load-balance: default
Version check        : Disabled      ※ スタックメンバーのバージョンチェック処理を無視
~~省略~~
```

3. スタックマスター（装置 1）を再起動、または電源 OFF/ON して、新ファームウェアにアップデートします。装置 1 が起動してスタック構成に取り込まれるのを待ちます。この手順の実行時にスタックマスターの切り替わりが発生します。
・装置 1：マスター → バックアップ
・装置 2：バックアップ → マスター

4. スタックマスター（装置 2）を再起動、または電源 OFF/ON して、新ファームウェアにアップデートします。装置 2 が起動してスタック構成に取り込まれるのを待ちます。この手順の実行時にスタックマスターの切り替わりが発生します。
・装置 1：バックアップ → マスター
・装置 2：マスター → バックアップ

5. **stack preempt** コマンドで、プリエンプトモードを有効に戻します。**no stack version check ignore** コマンドで、スタックメンバーのバージョンチェック処理を有効に戻します。その後、設定を保存して、**show stack** コマンドで確認します。

```
# stack preempt
#
# no stack version check ignore
#
# write memory

Destination filename startup-config? [y/n]:  y

Saving all configurations to NV-RAM.......... Done.

#
# show stack

Stacking Mode        : Enabled
Stack Preempt        : Enabled       ※ プリエンプトモード有効
Trap State           : Disabled
Port-channel mode    : All
Stack-port load-balance: default
Version check        : Enabled       ※ スタックメンバーのバージョンチェック処理は有効
~~省略~~
```

4. スタック

スタックの機能、設定、動作、状態の確認方法、および構成例と設定例について説明します。

REF: コマンドの詳細については、『コマンドリファレンス』を参照してください。

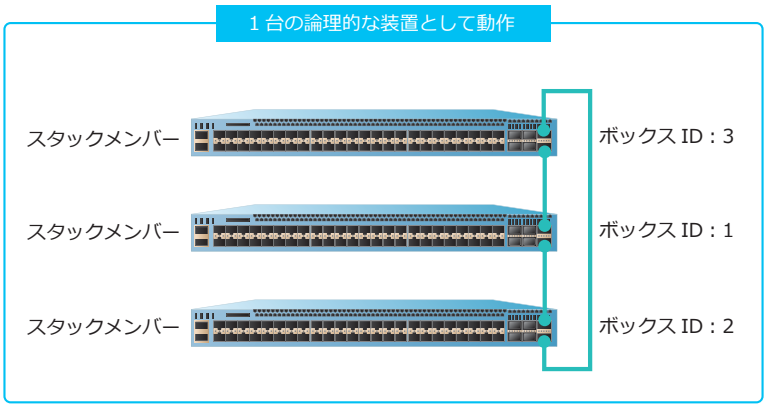
4.1 スタックの機能説明

スタックは、複数の装置を**スタックポート**で接続し、論理的に 1 台の装置として動作させる機能です。複数の装置を 1 台の装置として管理できるため、管理対象を減らすことができたり、後からスタックメンバーを増設して柔軟にポート数を増やしたりできます。

NOTE: スタック機能が有効になると、スタックポートに設定した物理ポートはスタック専用ポートになるため、通常の物理ポートのような使用はできなくなります。

スタックを構成する複数の装置それぞれを**スタックメンバー**と呼びます。スタックメンバーには、それぞれ**ボックス ID** が割り当てられます。

図 4-1 スタックの構成例



4.1.1 スタックトポロジー

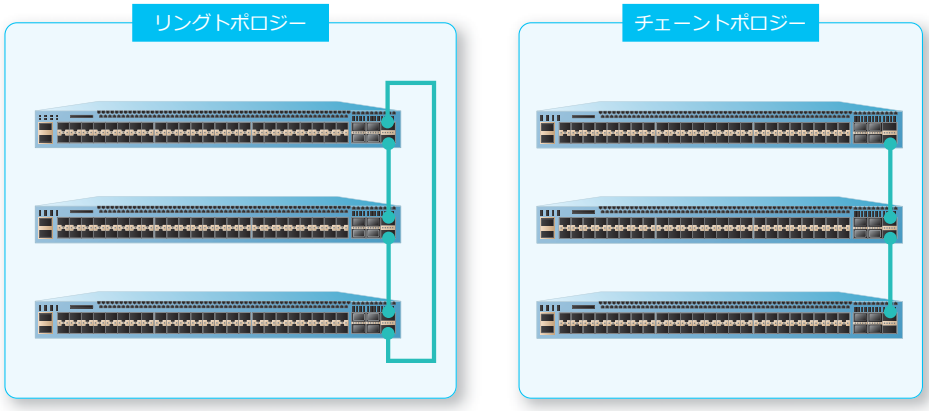
スタックを構成するには、自装置のスタックポート 1 またはスタックポート 2 と、他の装置のスタックポート 1 またはスタックポート 2 を接続して構成します。

CAUTION: スタックを構成する場合は、スタックポート間の直接接続のみをサポートしています。スタックポート間をスイッチングハブやメディアコンバーターなどの他の装置で中継する構成は、サポートしていません。

NOTE: スタック構成ではスタックマスターのみコンソール経由でログイン可能です。そのため、運用性を考慮して、スタックを構成する装置はなるべく近くに設置して運用することを推奨します。

スタックの構成方法には、リングトポロジーとチェーントポロジーの 2 種類があります。リングトポロジーは、複数の装置をリング状に接続して構成します。チェーントポロジーは、複数の装置を直線状に接続して構成します。

図 4-2 スタックトポロジー

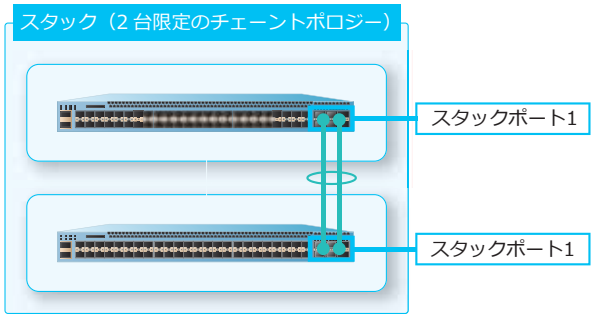


リングトポロジーでスタックリンクの 1 つに障害が発生した場合は、チェーントポロジーに変更されることで通信を継続できます。しかしながら、チェーントポロジーでスタックリンクの 1 つに障害が発生すると、スタック構成が分離されてネットワーク内に同じ設定のスタック装置が 2 台存在することになり、正常な管理や通信ができなくなる可能性があります。そのため、スタックを構成する場合は、各装置の 2 つのスタックポートを使用するリングトポロジーの接続を推奨します。

2 台限定のチェーントポロジー

スタックポートになるすべての物理ポートを 1 つのスタックポート（ポートチャネル）にする 2 台限定のチェーントポロジーという接続方法もあります。2 台限定のチェーントポロジーでは、スタックリンクの帯域幅が増加します。2 台限定のチェーントポロジーにするには、**`stack bandwidth`** コマンドで chain オプションを指定して設定します。この場合、装置のスタックポートは 1 つだけのため、chain オプションを指定して設定した 2 台の装置を接続し、スタックを構成します。

図 4-3 chain オプションを使用した接続方法



4.1.2 スタックメンバーの役割

スタックを構成すると、各スタックメンバーには「マスター」「バックアップマスター」「スレーブ」のいずれかの役割が割り当てられます。これらの役割はスタックの優先度によって決定されます。スタックの優先度は **`stack my_box_priority`** コマンド、または **`stack priority`** コマンドで設定します。値が小さいほど優先度が高くなります。各役割の説明を以下に示します。

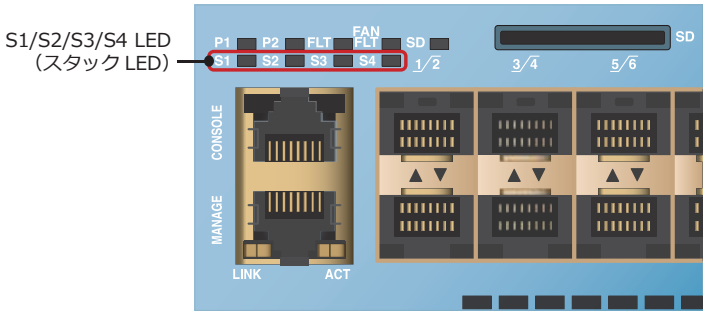
表 4-1 スタックメンバーの役割

設定	帯域幅
マスター	• マスターはスタック構成を管理し、他のスタックメンバーを制御します。 • スタック構成では、マスターのみコンソール経由でログインできます。また、マネージメントポートもマスターのみ有効になります。 • 最も優先度の高い（設定値の小さい）スタックメンバーがマスターになります。マスター決定時に同じ優先度のスタックメンバーが存在する場合、MAC アドレスの値が小さいスタックメンバーがマスターになります。 • プリエンプトモードが無効の場合は、マスターに決定したスタックメンバーの優先度は「0（最も高い優先度）」で動作するようになります。 • プリエンプトモードが有効の場合は、マスターの優先度は設定値のまま動作します。そのため、プリエンプトモードが有効なスタック構成では、後から「マスターの優先度の設定値よりも小さい設定値のスタックメンバー」を追加するとマスターが切り替わります。
バックアップマスター	• バックアップマスターは、マスターがダウンした場合に新たなマスターとして切り替わります。 • 2 番目に優先度の高い（設定値の小さい）スタックメンバーがバックアップマスターになります。バックアップマスター決定時に、同じ優先度のスタックメンバーが存在する場合、MAC アドレスの値が小さいスタックメンバーがバックアップマスターになります。
スレーブ	• マスターとバックアップマスター以外のスタックメンバーは、すべてスレーブになります。

4.1.2.1 スタック LED での確認（NP7000、NP5000、NP2500）

NP7000、NP5000、NP2500 では、装置の左上にスタック LED があります。スタックが有効化され、スタックメンバーの役割が決定すると、自装置のボックス ID に対応する S1 ～ S4 のいずれかのスタック LED が点灯します。緑色に点灯している装置がマスターで、橙色に点灯している装置がバックアップマスターまたはスレーブです。

図 4-4 スタック LED の例

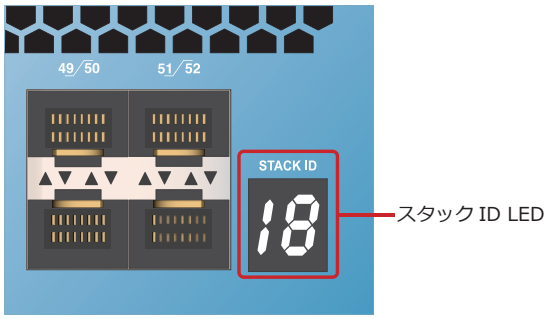


4.1.2.2 スタック ID LED での確認（NP4000、NP3000、NP2100、NP2000）

NP4000、NP3000、NP2100、NP2000 では、装置の右下にスタック ID LED があります。スタックが有効化され、スタックメンバーの役割が決定すると、スタック ID LED に以下の内容が表示されます。

- マスターに決定した装置では、ボックス ID と H（大文字）が交互に表示されます。
- バックアップマスターに決定した装置では、ボックス ID と h（小文字）が交互に表示されます。
- スレーブに決定した装置では、ボックス ID のみが表示されます。

図 4-5 スタック ID LED の例



4.1.3 スタック機能の制限事項および注意事項

- スタックを構成可能な装置の最大数は「4 台」です。
- スタック機能が有効になると、スタックポートに設定した物理ポートはスタック専用ポートになるため、通常の物理ポートのような使用はできなくなります。
- スタックを構成する場合は、スタックポート間の直接接続のみをサポートしています。スタックポート間をスイッチングハブやメディアコンバーターなどの他の装置で中継する構成は、サポートしていません。
- スタック構成ではスタックマスターのみコンソール経由でログイン可能です。
- スタックメンバーのファームウェアのバージョンはすべて同じにしてください。ファームウェアのバージョンが異なる場合はスタックを構成できません。
- NP7000、NP5000、NP3000 でスタックを構成する場合、スタックを構成するすべてのスタックメンバーで、レイヤー 3 ライセンスの有無を統一してください。
- ApresiaNP シリーズ以外の機器はスタック構成に含められません。
- 異なる ApresiaNP シリーズが混在するスタックは構成できません。同一の ApresiaNP シリーズでのみスタックを構成できます。
- ファームウェアのバージョンが AEOS-NP2000 Ver. 1.09 の場合のみ、NP2100 と NP2000 が混在するスタックを構成できます。
- ApresiaNP2100-48T4X、ApresiaNP2100-48T4X-PoE、ApresiaNP2000-48T4X、および ApresiaNP2000-48T4X-PoE では、stack bandwidth 10G 4-port 設定時は、chain オプションは併用できません。
- ApresiaNP2100-48T4X、ApresiaNP2100-48T4X-PoE、ApresiaNP2000-48T4X、および ApresiaNP2000-48T4X-PoE では、**`stack port-channel mode partial`** コマンドはサポートしていません。

プリエンプトモードに関する制限事項および注意事項

- プリエンプトモードが無効の場合は、マスターの優先度は「0（最も高い優先度）」で動作するようになります。そのため、プリエンプトモードが無効なスタック構成において、稼働状態の別の装置（マスターになっていて優先度「0」で動作中）をスタック構成に追加すると、同一優先度のため MAC アドレスの比較によるマスターの再選出が行われることに注意してください。追加した別の装置にマスターが切り替わってしまうことを防止するには、追加する装置の電源を落とした状態でスタック構成へ接続し、その後に電源を入れて起動してください。
- プリエンプトモードが有効なスタック構成において、現在のマスターより優先度の高い装置がマスターに切り替わる場合には、ポート閉塞を伴うマスター再選出プロセスが動作するため、一定の通信断時間が発生します。
- また、プリエンプトモードによってマスターが切り替わる場合には、「2 台の稼働中のマスターの優先度が比較されて、優先度の高い方がマスターとして残り、優先度の低い方がバックアップマスターになる」という動作になるため、その後のスタックの MAC アドレスはマスターになった装置の MAC アドレスになることに注意してください。

リングトポロジー構成に関する制限事項および注意事項

- 3 台以上のリングトポロジー構成でスタックメンバー装置を再起動させると、スタックの起動プロセスが終了するまで、スタック装置間を経由する学習済みユニキャストの中継が停止することがあります。

  NOTE: 3 台以上のリングトポロジー構成で、交換時などにスタックメンバー装置を復旧させる場合は、片方のスタックケーブルのみを接続した状態で起動し、一度チェーントポロジーでスタック構成に取り込みます。その後、もう片方のスタックケーブルを接続する手順で復旧させることで、本注意事項を回避できます。

FDB に関する制限事項および注意事項

- スタック構成では、各スタックメンバー装置が個々に MAC アドレスを学習します。学習した MAC アドレスは、CPU を介してスタックメンバー装置間で同期を行います。そのため、スタック構成全体で FDB 同期が完了するまでには、非スタック装置の場合よりも多くの時間を要します。
- スタック構成において、スタックメンバー装置を跨ぐポート間でステーションムーブが発生（学習済みの MAC アドレスが登録状態のまま、別のスタックメンバー装置のポートでフレームを受信して再学習）した場合、初回フレーム受信時には再学習されないことがあります。また、FDB 同期の仕組みの制限により、再学習されずに該当 MAC アドレスが MAC アドレステーブルから削除されることがあります。このような場合でも、移動先のポートで再度フレームを受信することで正常に再学習されます。

OSPFv2/OSPFv3 併用に関する制限事項および注意事項

- マスターがダウンして切り替わった場合、OSPFv2（改善前のバージョン）/OSPFv3 はリスタートします。マスター以外のスタックメンバーがダウンした場合はリスタートしません。また、スタックメンバーの復旧・新規追加時は、マスターの切り替わりの有無にかかわらず、OSPFv2/OSPFv3 はリスタートします。

  NOTE: NP7000 の 1.06.01 以降、NP5000 の 1.06.01 以降、NP3000 の 1.06.01 以降では、マスターがダウンして切り替わった場合でも、OSPFv2 がリスタートしないように改善されています。それより前のバージョンでは、マスターがダウンして切り替わった場合、OSPFv2 はリスタートします。

RIP/RIPng 併用に関する制限事項および注意事項

- プリエンプトモードが有効で、スタックメンバーの復旧・新規追加時にマスターが切り替わる場合は、ポート閉塞を伴うマスター再選出プロセスの影響で、RIP/RIPng も一度クリアされます。また、プリエンプトモードが無効で、マスターが切り替わらない場合でも、復旧・新規追加されたスタックメンバーで受信した RIP/RIPng 学習経路宛ての通信は、他装置からの RIP/RIPng パケットを一度受信するまでは中継されません。

VRRP 併用に関する制限事項および注意事項

- スタックメンバーが追加され、マスターの切り替わりが発生した場合は、VRRP 機能がリスタートします。また、装置の障害や復旧が発生し、追加されたスタックメンバーが新たにマスターになる場合も、VRRP 機能がリスタートします。

マルチキャストルーティング併用に関する制限事項および注意事項

- スタックメンバーの障害や復旧が発生したとき、および装置が追加または削除されたときに、マスターの変更が発生する場合は、PIM 機能がリスタートします。

4.2 スタック機能の設定

スタック機能を設定する方法を説明します。

4.2.1 有効化とスタックポートの設定

スタック機能を有効にするには、主に以下の設定が必要です。

- **stack bandwidth** コマンドでスタックポートを指定してスタックを有効化
- **stack my_box_id** コマンドでボックス ID を設定
- **stack my_box_priority** コマンドで優先度を設定

> ***NOTE:*** スタック機能の有効化、ボックス ID の設定などは、構成情報を保存して装置を再起動した後に反映されます。

スタックポートとして割り当てられるポートは、機種および設定によって異なります。機種ごとの **stack bandwidth** コマンド設定について以下に説明します。

4.2.1.1 NP7000 シリーズ

ApresiaNP7000 シリーズでは、ApresiaNP7000-48X6L、ApresiaNP7000-24G24X6L でスタックを構成できます。

> ***NOTE:*** レイヤー 3 ライセンスが有効な NP7000（機器レビジョン B）の対応ファームウェアは 1.08.01 以降です。そのため、レイヤー 3 ライセンスを有効にして機器レビジョン A と B の装置が混在するスタックを構成する場合は、1.08.01 以降で使用してください。

stack bandwidth コマンドでスタック機能を有効にした場合に、スタックポート 1 およびスタックポート 2 として動作するポートを以下に示します。chain オプションを指定した場合は、スタックポートのすべてのポートがスタックポート 1 になります。

表 4-2 stack bandwidth 設定（NP7000）

設定パラメーター	帯域幅	スタックポート 1	スタックポート 2
40G 2-port	40G、2 スタックポート	ポート 1/0/65	ポート 1/0/69
40G 2-port chain	40G×2、1 スタックポート	ポート 1/0/65, 1/0/69	-

4.2.1.2 NP5000 シリーズ

ApresiaNP5000 シリーズでは、ApresiaNP5000-48T4X 同士でスタックを構成できます。

> ***NOTE:*** レイヤー 3 ライセンスが有効な NP5000（機器レビジョン B）の対応ファームウェアは 1.08.01 以降です。そのため、レイヤー 3 ライセンスを有効にして機器レビジョン A と B の装置が混在するスタックを構成する場合は、1.08.01 以降で使用してください。

stack bandwidth コマンドでスタック機能を有効にした場合に、スタックポート 1 およびスタックポート 2 として動作するポートを以下に示します。chain オプションを指定した場合は、スタックポートのすべてのポートがスタックポート 1 になります。

表 4-3 stack bandwidth 設定（NP5000）

設定パラメーター	帯域幅	スタックポート 1	スタックポート 2
10G 2-port	10G、2 スタックポート	ポート 1/0/51	ポート 1/0/52

設定パラメーター	帯域幅	スタックポート 1	スタックポート 2
10G 4-port	10G×2、2 スタックポート	ポート 1/0/49, 1/0/51	ポート 1/0/50, 1/0/52
40G 2-port	40G、2 スタックポート	ポート 1/0/53	ポート 1/0/54
10G 2-port chain	10G×2、1 スタックポート	ポート 1/0/51, 1/0/52	-
10G 4-port chain	10G×4、1 スタックポート	ポート 1/0/49, 1/0/50, 1/0/51, 1/0/52	-
40G 2-port chain	40G×2、1 スタックポート	ポート 1/0/53, 1/0/54	-

4.2.1.3 NP4000 シリーズ

ApresiaNP4000 シリーズでは、ApresiaNP4000-20Xt4X 同士でスタックを構成できます。

`stack bandwidth` コマンドでスタック機能を有効にした場合に、スタックポート 1 およびスタックポート 2 として動作するポートを以下に示します。chain オプションを指定した場合は、スタックポートのすべてのポートがスタックポート 1 になります。

表 4-4 stack bandwidth 設定（NP4000）

設定パラメーター	帯域幅	スタックポート 1	スタックポート 2
10G 2-port	10G、2 スタックポート	ポート 1/0/23	ポート 1/0/24
10G 4-port	10G×2、2 スタックポート	ポート 1/0/21, 1/0/23	ポート 1/0/22, 1/0/24
10G 2-port chain	10G×2、1 スタックポート	ポート 1/0/23, 1/0/24	-
10G 4-port chain	10G×4、1 スタックポート	ポート 1/0/21, 1/0/22, 1/0/23, 1/0/24	-

4.2.1.4 NP3000 シリーズ

ApresiaNP3000 シリーズでは、ApresiaNP3000-24X4Q、ApresiaNP3000-24T8X4Q、ApresiaNP3000-48T4X でスタックを構成できます。

`stack bandwidth` コマンドでスタック機能を有効にした場合に、スタックポート 1 およびスタックポート 2 として動作するポートを以下に示します。chain オプションを指定した場合は、スタックポートのすべてのポートがスタックポート 1 になります。

表 4-5 stack bandwidth 設定（ApresiaNP3000-24X4Q）

設定パラメーター	帯域幅	スタックポート 1	スタックポート 2
10G 2-port	10G、2 スタックポート	ポート 1/0/23	ポート 1/0/24
10G 4-port	10G×2、2 スタックポート	ポート 1/0/21, 1/0/22	ポート 1/0/23, 1/0/24
25G 2-port	25G、2 スタックポート	ポート 1/0/27	ポート 1/0/28
25G 4-port	25G×2、2 スタックポート	ポート 1/0/25, 1/0/26	ポート 1/0/27, 1/0/28
10G 2-port chain	10G×2、1 スタックポート	ポート 1/0/23, 1/0/24	-
10G 4-port chain	10G×4、1 スタックポート	ポート 1/0/21, 1/0/22, 1/0/23, 1/0/24	-

設定パラメーター	帯域幅	スタックポート 1	スタックポート 2
25G 2-port chain	25G×2、1 スタックポート	ポート 1/0/27, 1/0/28	-
25G 4-port chain	25G×4、1 スタックポート	ポート 1/0/25, 1/0/26, 1/0/27, 1/0/28	-

表 4-6 stack bandwidth 設定（ApresiaNP3000-24T8X4Q）

設定パラメーター	帯域幅	スタックポート 1	スタックポート 2
10G 2-port	10G、2 スタックポート	ポート 1/0/31	ポート 1/0/32
10G 4-port	10G×2、2 スタックポート	ポート 1/0/29, 1/0/30	ポート 1/0/31, 1/0/32
25G 2-port	25G、2 スタックポート	ポート 1/0/35	ポート 1/0/36
25G 4-port	25G×2、2 スタックポート	ポート 1/0/33, 1/0/34	ポート 1/0/35, 1/0/36
10G 2-port chain	10G×2、1 スタックポート	ポート 1/0/31, 1/0/32	-
10G 4-port chain	10G×4、1 スタックポート	ポート 1/0/29, 1/0/30, 1/0/31, 1/0/32	-
25G 2-port chain	25G×2、1 スタックポート	ポート 1/0/35, 1/0/36	-
25G 4-port chain	25G×4、1 スタックポート	ポート 1/0/33, 1/0/34, 1/0/35, 1/0/36	-

表 4-7 stack bandwidth 設定（ApresiaNP3000-48T4X）

設定パラメーター	帯域幅	スタックポート 1	スタックポート 2
10G 2-port	10G、2 スタックポート	ポート 1/0/51	ポート 1/0/52
10G 4-port	10G×2、2 スタックポート	ポート 1/0/49, 1/0/50	ポート 1/0/51, 1/0/52
10G 2-port chain	10G×2、1 スタックポート	ポート 1/0/51, 1/0/52	-
10G 4-port chain	10G×4、1 スタックポート	ポート 1/0/49, 1/0/50, 1/0/51, 1/0/52	-

4.2.1.5 NP2100 シリーズ

ApresiaNP2100 シリーズでは、ApresiaNP2100-24T4X、ApresiaNP2100-24T4X-PoE、ApresiaNP2100-48T4X、ApresiaNP2100-48T4X-PoE でスタックを構成できます。

> ***NOTE:*** ファームウェアのバージョンが AEOS-NP2000 Ver. 1.09 の場合のみ、NP2100 と NP2000 が混在するスタックを構成できます。

> ***NOTE:*** ApresiaNP2100-48T4X、ApresiaNP2100-48T4X-PoE では、stack bandwidth 10G 4-port 設定時は、chain オプションは併用できません。

`stack bandwidth` コマンドでスタック機能を有効にした場合に、スタックポート 1 およびスタックポート 2 として動作するポートを以下に示します。chain オプションを指定した場合は、スタックポートのすべてのポートがスタックポート 1 になります。

表 4-8 stack bandwidth 設定（ApresiaNP2100-24T4X/ApresiaNP2100-24T4X-PoE）

設定パラメーター	帯域幅	スタックポート 1	スタックポート 2
10G 2-port	10G、2 スタックポート	ポート 1/0/27	ポート 1/0/28
10G 4-port	10G×2、2 スタックポート	ポート 1/0/25, 1/0/26	ポート 1/0/27, 1/0/28
10G 2-port chain	10G×2、1 スタックポート	ポート 1/0/27, 1/0/28	-
10G 4-port chain	10G×4、1 スタックポート	ポート 1/0/25, 1/0/26, 1/0/27, 1/0/28	-

表 4-9 stack bandwidth 設定（ApresiaNP2100-48T4X/ApresiaNP2100-48T4X-PoE）

設定パラメーター	帯域幅	スタックポート 1	スタックポート 2
10G 2-port	10G、2 スタックポート	ポート 1/0/51	ポート 1/0/52
10G 4-port	10G×2、2 スタックポート	ポート 1/0/49, 1/0/50	ポート 1/0/51, 1/0/52
10G 2-port chain	10G×2、1 スタックポート	ポート 1/0/51, 1/0/52	-

4.2.1.6 NP2000 シリーズ

ApresiaNP2000 シリーズでは、ApresiaNP2000-24T4X、ApresiaNP2000-24T4X-PoE、ApresiaNP2000-48T4X、ApresiaNP2000-48T4X-PoE でスタックを構成できます。

> ***NOTE:*** ファームウェアのバージョンが AEOS-NP2000 Ver. 1.09 の場合のみ、NP2100 と NP2000 が混在するスタックを構成できます。

> ***NOTE:*** ApresiaNP2000-48T4X、ApresiaNP2000-48T4X-PoE では、stack bandwidth 10G 4-port 設定時は、chain オプションは併用できません。

`stack bandwidth` コマンドでスタック機能を有効にした場合に、スタックポート 1 およびスタックポート 2 として動作するポートを以下に示します。chain オプションを指定した場合は、スタックポートのすべてのポートがスタックポート 1 になります。

表 4-10 stack bandwidth 設定（ApresiaNP2000-24T4X/ApresiaNP2000-24T4X-PoE）

設定パラメーター	帯域幅	スタックポート 1	スタックポート 2
10G 2-port	10G、2 スタックポート	ポート 1/0/27	ポート 1/0/28
10G 4-port	10G×2、2 スタックポート	ポート 1/0/25, 1/0/26	ポート 1/0/27, 1/0/28
10G 2-port chain	10G×2、1 スタックポート	ポート 1/0/27, 1/0/28	-
10G 4-port chain	10G×4、1 スタックポート	ポート 1/0/25, 1/0/26, 1/0/27, 1/0/28	-

表 4-11 stack bandwidth 設定（ApresiaNP2000-48T4X/ApresiaNP2000-48T4X-PoE）

設定パラメーター	帯域幅	スタックポート 1	スタックポート 2
10G 2-port	10G、2 スタックポート	ポート 1/0/51	ポート 1/0/52
10G 4-port	10G×2、2 スタックポート	ポート 1/0/49, 1/0/50	ポート 1/0/51, 1/0/52
10G 2-port chain	10G×2、1 スタックポート	ポート 1/0/51, 1/0/52	-

4.2.1.7 NP2500 シリーズ

ApresiaNP2500 シリーズでは、ApresiaNP2500-8MT4X-PoE、ApresiaNP2500-16MT4X-PoE でスタックを構成できます。

stack bandwidth コマンドでスタック機能を有効にした場合に、スタックポート 1 およびスタックポート 2 として動作するポートを以下に示します。chain オプションを指定した場合は、スタックポートのすべてのポートがスタックポート 1 になります。

表 4-12 stack bandwidth 設定（ApresiaNP2500-8MT4X-PoE）

設定パラメーター	帯域幅	スタックポート 1	スタックポート 2
10G 2-port	10G、2 スタックポート	ポート 1/0/11	ポート 1/0/12
10G 4-port	10G×2、2 スタックポート	ポート 1/0/9, 1/0/10	ポート 1/0/11, 1/0/12
10G 2-port chain	10G×2、1 スタックポート	ポート 1/0/11, 1/0/12	-
10G 4-port chain	10G×4、1 スタックポート	ポート 1/0/9, 1/0/10, 1/0/11, 1/0/12	-

表 4-13 stack bandwidth 設定（ApresiaNP2500-16MT4X-PoE）

設定パラメーター	帯域幅	スタックポート 1	スタックポート 2
10G 2-port	10G、2 スタックポート	ポート 1/0/19	ポート 1/0/20
10G 4-port	10G×2、2 スタックポート	ポート 1/0/17, 1/0/18	ポート 1/0/19, 1/0/20
10G 2-port chain	10G×2、1 スタックポート	ポート 1/0/19, 1/0/20	-
10G 4-port chain	10G×4、1 スタックポート	ポート 1/0/17, 1/0/18, 1/0/19, 1/0/20	-

4.2.2 ボックス ID の設定

ボックス ID は、スタックメンバーに割り当てられる 1 ～ 4 の一意の ID です。ボックス ID が競合した場合はスタックが正常に構成されないため、ボックス ID は競合しないように設定してください。

ボックス ID の割り当てには、以下の 2 種類の方法があります。

- 設定コマンドによる手動割り当て
- スタック起動時にルールに従って割り当てられる自動割り当て（デフォルト設定）

NOTE: 各装置のボックス ID を明示的に指定して管理しやすくするためにも、ボックス ID は設定コマンドで割り当てることを推奨します。

4.2.2.1 設定コマンドによるボックス ID の手動割り当て

自装置のボックス ID を設定するには、**stack my_box_id** コマンドを使用します。ボックス ID の設定は、構成情報を保存して装置を再起動した後に反映されます。

REF: ボックス ID は **stack renumber** コマンドでも設定できます。**stack my_box_id** コマンドをサポートする前の一部機種の古いバージョン（NP7000、NP5000、NP2000 それぞれの 1.03.01 より前のバージョン）では、**stack renumber** コマンドを使用してください。**stack renumber** コマンドの詳細については、『コマンドリファレンス』を参照してください。

4.2.2.2 ボックス ID の自動割り当て

ボックス ID が自動的に割り当てられる場合は、以下のルールに従って割り当てられます。

リングトポロジーの場合

1. スタックが構成されると、マスターになった装置にボックス ID「1」が割り当てられます。
2. その後、マスターのダウンストリームスイッチ（マスターのスタックポート 2 に接続された装置）に、マスターのボックス ID に「1」を加算したボックス ID が割り当てられます。ダウンストリームスイッチが複数存在する場合、ボックス ID は「1」ずつ増加して割り当てられます。

チェーントポロジーの場合

1. スタックが構成されると、マスターになった装置にボックス ID「1」が割り当てられます。
2. その後、マスターのダウンストリームスイッチ（マスターのスタックポート 2 に接続された装置）に、マスターのボックス ID に「1」を加算したボックス ID が割り当てられます。ダウンストリームスイッチが複数存在する場合、ボックス ID は「1」ずつ増加して割り当てられます。
3. その後、マスターのアップストリームスイッチ（マスターのスタックポート 1 に接続された装置）に、ダウンストリームスイッチに割り当てられた最後のボックス ID に「1」を加算したボックス ID が割り当てられます。アップストリームスイッチが複数存在する場合、ボックス ID は「1」ずつ増加して割り当てられます。

4.2.3 優先度の設定

スタックの優先度は、値が小さいほど高くなります。また、同じ優先度の場合は MAC アドレスが比較され、MAC アドレスの値が小さい方が優先度が高くなります。

自装置の優先度を設定するには、**`stack my_box_priority`** コマンドを使用します。優先度を変更した場合は、次回起動時にも反映されるように構成情報を保存してください。

> ***REF:*** 優先度は **`stack priority`** コマンドでも設定できます。**`stack my_box_priority`** コマンドをサポートする前の一部機種の古いバージョン（NP7000、NP5000、NP2000 それぞれの 1.03.01 より前のバージョン）では、**`stack priority`** コマンドを使用してください。**`stack priority`** コマンドの詳細については、『コマンドリファレンス』を参照してください。
>
> ***NOTE:*** プリエンプトモードが無効の場合は、マスターに決定したスタックメンバーの優先度は「0（最も高い優先度）」で動作するようになります。

4.2.4 無効化、設定削除

自装置のスタック機能を無効にするには、**no stack** コマンドを使用します。また、各種スタック設定を削除するには、**no** 形式の各コマンドを使用します。

> ***NOTE:*** スタック機能の無効化、ボックス ID の設定削除などは、構成情報を保存して装置を再起動した後に反映されます。

> ***NOTE:*** スタック機能を無効にしてもボックス ID の設定が残っている場合は、自装置のポート番号などがボックス ID の設定値のままになることに注意してください。そのため、スタック機能を無効化して非スタック装置に戻す場合は、すべてのスタック設定も削除してデフォルト設定に戻してください。

reset system コマンドを使用すると、スタック設定を含めたすべての構成情報をデフォルト設定に戻すことができます。**reset system** コマンドを実行すると装置は再起動します。

clear running-config コマンドを使用すると、スタック設定を除いた構成情報をデフォルト設定に戻すことができます。スタック設定は保持されます。

> ***NOTE:*** **clear running-config** コマンドで running-config を消去した装置を運用環境で使用する際は、設定を実施して構成情報を保存した後、念のため運用前に一度起動しなおしてから使用することを推奨します。

4.2.5 プリエンプトモード

プリエンプトモードは、「マスターの装置がダウンして復旧した際に、マスターを元の装置に切り戻す運用」を行う場合などに有効にします。デフォルト設定では無効です。プリエンプトモードを有効にするには、**stack preempt** コマンドを使用します。

プリエンプトモード無効時の動作

プリエンプトモードが無効（デフォルト設定）の場合は、マスターに決定したスタックメンバーの優先度は、設定値ではなく「0（最も高い優先度）」で動作するようになります。そのため、優先度比較において常に現状のマスターの優先度が最も高くなります。これにより、再起動などでスタックから一時的に離脱した旧マスターが復旧する場合や、スタック構成に新たに装置を追加する場合（電源 OFF の状態でスタック構成に接続してから起動する手順）に、不要なマスターの切り替わりが発生するのを防ぎます。

> ***NOTE:*** プリエンプトモードが無効なスタック構成において、稼働状態の別の装置（マスターになっていて優先度「0」で動作中）をスタック構成に追加すると、同一優先度のため MAC アドレスの比較によるマスターの再選出が行われることに注意してください。

プリエンプトモード有効時の動作

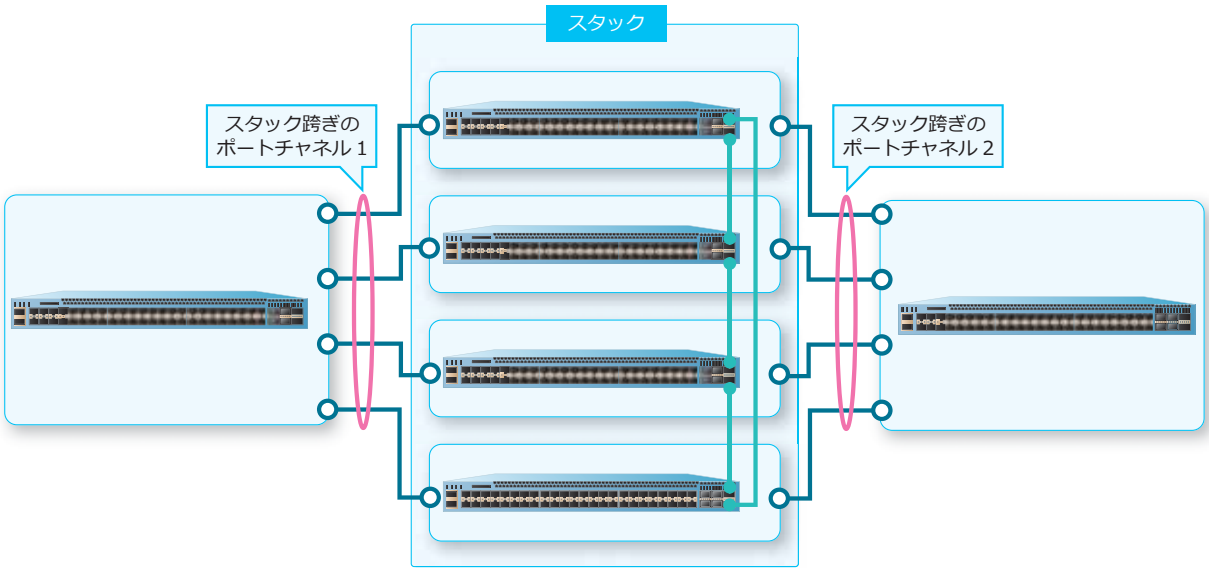
プリエンプトモードが有効の場合は、マスターに決定したスタックメンバーの優先度は設定値のまま動作します。そのため、再起動などでスタックから一時的に離脱した旧マスターが復旧する場合や、スタック構成に新たに装置を追加する場合でも、常に設定値の優先度で比較されることになるため、最も優先度の高いスタックメンバーを常にマスターとして動作させることができます。なお、優先度が同じ場合は、MAC アドレスによって比較されます。

> ***NOTE:*** プリエンプトモードによってマスターが切り替わる場合には、ポート閉塞を伴うマスター再選出プロセスが動作するため、一定の通信断時間が発生することに注意してください。

4.2.6 スタック跨ぎのポートチャネル

スタック機能では、スタックメンバー装置を跨いだポートチャネルを使用できます。スタック跨ぎのポートチャネルも通常のポートチャネルと同様に、1 つのポートチャネルに設定可能なメンバーポートは最大 8 ポートです。

図 4-6 スタック跨ぎのポートチャネル

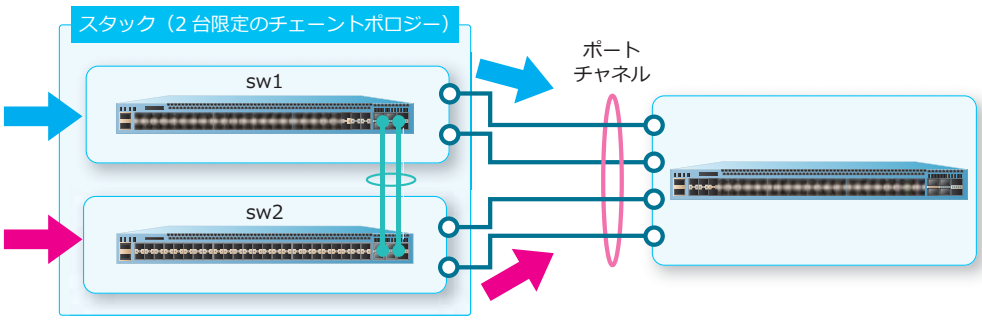


4.2.6.1 stack port-channel mode partial

スタック跨ぎのポートチャネルの負荷分散は、通常のポートチャネルと同様に、すべてのメンバーポートの中から負荷分散アルゴリズムに従って出力ポートが決定されます。そのため、入力ポートの装置と出力ポートの装置が異なる場合は、スタックポートを経由して中継されます。

2 台限定のチェーントポロジーの場合は、スタック跨ぎのポートチャネルの負荷分散を、すべてのメンバーポートではなく、入力ポートと同じ装置のメンバーポートの中から負荷分散アルゴリズムに従って決定されるように変更できます。

図 4-7 stack port-channel mode partial の動作例



この機能を有効にするには、**`stack port-channel mode partial`** コマンドを使用します。なお、リンクダウンなどで同じ装置に送信可能なメンバーポートが 1 つも残っていない場合は、別装置のメンバーポートから選択されます。

> ***CAUTION:*** ApresiaNP2100-48T4X、ApresiaNP2100-48T4X-PoE、ApresiaNP2000-48T4X、および ApresiaNP2000-48T4X-PoE では、**`stack port-channel mode partial`** コマンドはサポートしていません。

> ***NOTE:*** **`stack port-channel mode partial`** コマンドは、2 台限定のチェーントポロジーでスタックを構成した場合のみ使用できます。

NOTE: 本設定は、スタック構成に接続されている状態では設定できません。単体で起動している状態で設定してください。

NOTE: 本設定は、構成情報を保存して装置を再起動した後に反映されます。

4.2.7 スタックのオプション機能

スタックに関連するオプション機能を以下に示します。

- スタックポートの VLAN 設定のプリセット（NP7000）
- スタックポート（ポートチャネル）の負荷分散
- 2 台スタック構成での一時的なバージョンチェック無視機能

4.2.7.1 スタックポートの VLAN 設定のプリセット（NP7000）

NP7000 では、スタックポートの VLAN 設定を前もって設定できます（プリセット）。スタックポートの VLAN 設定をプリセットするには、**`stack vlan pre-setting`** コマンドを使用します。

CAUTION: NP5000、NP4000、NP3000、NP2100、NP2000、および NP2500 では、**`stack vlan pre-setting`** コマンドは使用できません。

NOTE: 本設定は、構成情報を保存して装置を再起動した後に反映されます。

4.2.7.2 スタックポート（ポートチャネル）の負荷分散

1 つのスタックポートが複数のポートで構成されている場合の負荷分散方法を設定できます。スタックポート（ポートチャネル）の負荷分散方法を設定するには、**`stack stack-port load-balance`** コマンドを使用します。

NOTE: 本設定は、構成情報を保存して装置を再起動した後に反映されます。

4.2.7.3 2 台スタック構成での一時的なバージョンチェック無視機能

2 台スタック構成での一時的なバージョンチェック無視機能は、2 台スタック構成でのファームウェアのアップデート時に、一時的にスタックメンバーのバージョンチェック処理を無視する機能です。本機能を有効にするには **`stack version check ignore`** コマンドを使用します。

REF: 本機能の詳細については、「第 2 編 管理運用」の「2 台スタック構成での一時的なバージョンチェック無視機能」を参照してください。

4.3 スタック機能の動作

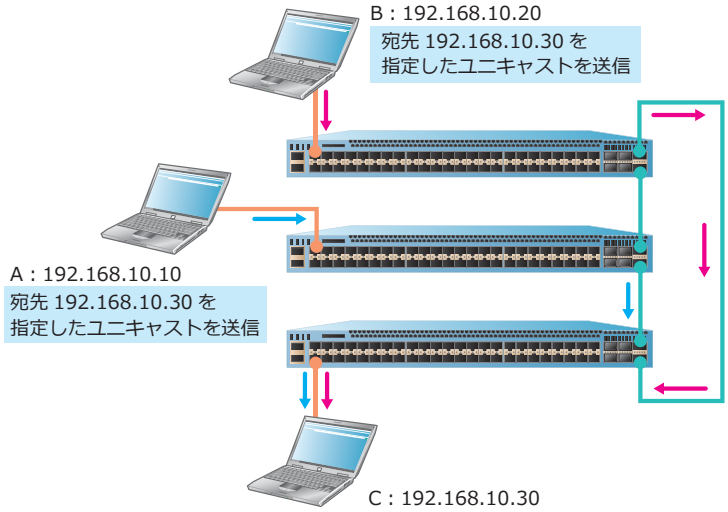
スタック機能の動作について説明します。

4.3.1 スタックメンバーを跨ぐトラフィックの中継方法

スタック構成では、受信ポートと送信ポートが異なるスタックメンバーのポートの場合は、トラフィックはスタックポートのリンクを経由して中継されます。

ユニキャストトラフィックは、最短パスで宛先のスタックメンバー装置に転送されて宛先ポートから送信されます。最短パスが 2 つある場合は、ポート番号が小さいスタックポートのパスが使用されます。リングトポロジーの場合のユニキャストトラフィックの中継例を示します。

図 4-8 ユニキャストトラフィックの中継例



ユニキャスト以外（宛先が不明なユニキャスト、マルチキャスト、ブロードキャスト）のトラフィックは、フラッディング中継されます。リングトポロジーではトラフィックループを防ぐために、スタックリンクのうちの 1 つがユニキャスト以外のトラフィック中継を抑止するパッシブリンクになります。パッシブリンクは以下の方法で自動的に決定されます。ユーザーが明示的に設定することはできません。

- リングトポロジーのスタックが起動する際には、マスターのスタックポート 1 に接続されたスタックリンクがパッシブリンクになります。
- チェーントポロジーからリングトポロジーへ変更された際には、新しく追加されたスタックリンクがパッシブリンクになります。

4.3.2 トポロジー変更時の動作

リングトポロジーでスタックリンクに障害が発生した場合、Ring to Chain イベントが発生してチェーントポロジーに変更されます。スタックトポロジーがチェーントポロジーに変更されるまで、約 1 秒を要します。

4.3.3 障害発生時と復旧時の動作

リングトポロジーのスタック構成（プリエンプトモード無効）で、マスター／バックアップマスター／スタックポートのケーブルに障害が発生した場合、および復旧した場合の動作について説明します。

> ***REF:*** マスターの切り替わりやスタックメンバーの復旧・新規追加時の制限事項については、「スタック機能の制限事項および注意事項」を参照してください。

4.3.3.1 マスターの障害発生／復旧時の動作

マスターに障害が発生した場合、バックアップマスターがマスターになり、その次に優先度の高いスレーブがバックアップマスターになります。このとき、各 VLAN インターフェースの MAC アドレスは元の MAC アドレス（最初のマスターの MAC アドレス）を引き継ぎます。これにより、レイヤー 3 中継する通信を継続できます。なお、マネージメントポートの MAC アドレスは、新マスター装置の MAC アドレスに変更されます。

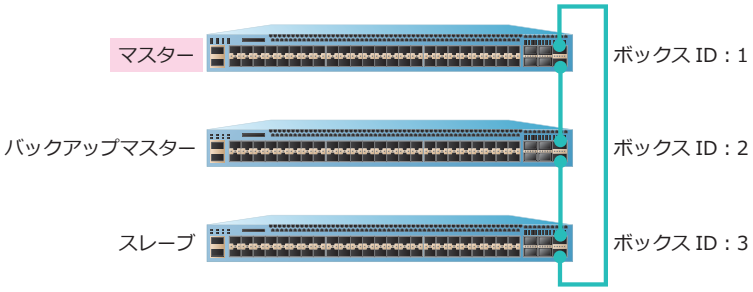
> ***NOTE:*** マスターから引き継がれた MAC アドレスは、**show version** コマンドで確認できます。なお、NP7000 は 1.06.01 以降、NP5000 は 1.05.02 以降、NP4000 は 1.02.01 以降、NP2000 は 1.07.01 以降で対応しています。

以下に、マスターの障害発生／復旧時の動作と表示例を示します。

(1) 正常時

この例では、正常時はボックス ID［1］の装置がマスター、ボックス ID［2］の装置がバックアップマスター、ボックス ID［3］の装置がスレーブになっているとします。

図 4-9 マスターに障害が発生する前の構成



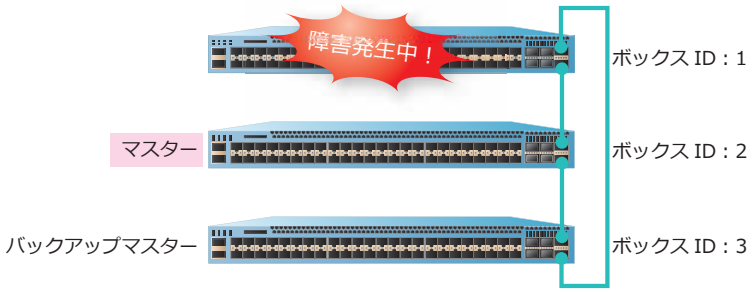
スタックの状態を **show stack** コマンドで確認した場合の例を示します。

```
Topology            : Duplex_Ring
My Box ID           : 1
Master ID           : 1
BK Master ID        : 2
Box Count           : 3

Box User Module                      Prio-                    Prom    Runtime   H/W
ID  Set  Name                  Exist rity  MAC                Version Version   Version
--- ---- --------------------- ----- ----- ------------------ ------- --------- -------
1   User ApresiaNP7000-48X6L   Exist 0     00-40-66-AA-52-1B 1.00.01 1.05.01   A
2   User ApresiaNP7000-48X6L   Exist 32    00-40-66-AA-31-00 1.00.01 1.05.01   A
3   User ApresiaNP7000-48X6L   Exist 60    00-40-66-AB-7D-5A 1.00.01 1.05.01   A
4   -    NOT_EXIST             No

 Stack Bandwidth and Unit Status:
 Box    User Set    SIO1 Active   SIO2 Active   Unit
 ID     Bandwidth   Bandwidth     Bandwidth     Status
 ----   ---------   ---------     ---------     ---------
 1      2-port(40G) 1-port        1-port        Normal
 2      2-port(40G) 1-port        1-port        Normal
 3      2-port(40G) 1-port        1-port        Normal
 4
```

(2) マスターに障害が発生した場合

マスターに障害が発生すると、バックアップマスターがマスターになり、その次に優先度の高いスレーブがバックアップマスターになります。

図 4-10 マスターに障害が発生した場合



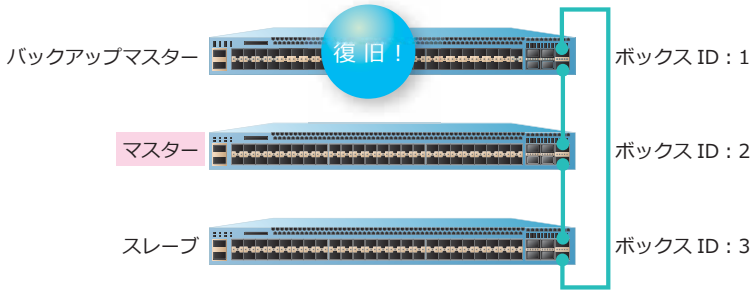
スタックの状態を **show stack** コマンドで確認した場合の例を示します。

```
Topology             : Duplex_Chain
My Box ID            : 2
Master ID            : 2
BK Master ID         : 3
Box Count            : 2

Box User Module                      Prio-                    Prom    Runtime   H/W
ID  Set  Name                   Exist rity  MAC                Version Version   Version
--- ---- ---------------------- ----- ----- ------------------ ------- --------- -------
1   -    ApresiaNP7000-48X6L    No
2   User ApresiaNP7000-48X6L    Exist 0     00-40-66-AA-31-00 1.00.01 1.05.01   A
3   User ApresiaNP7000-48X6L    Exist 60    00-40-66-AB-7D-5A 1.00.01 1.05.01   A
4   -    NOT_EXIST              No

 Stack Bandwidth and Unit Status:
 Box    User Set    SIO1 Active   SIO2 Active   Unit
 ID     Bandwidth   Bandwidth     Bandwidth     Status
 ----   ---------   ---------     ---------     ---------
 1
 2      2-port(40G) Down          1-port        Normal
 3      2-port(40G) 1-port        Down          Normal
 4
```

(3) 旧マスターの装置が復旧した場合

この例（プリエンプトモード無効）の場合、旧マスターのボックス ID［1］の装置が復旧すると、ボックス ID［1］の装置の優先度「10」が現状のバックアップマスターの優先度「60」よりも高いため、優先度の比較の結果、ボックス ID［1］の装置がバックアップマスターになり、ボックス ID［3］の装置がスレーブになります。

図 4-11 旧マスターの装置が復旧した場合



スタックの状態を **show stack** コマンドで確認した場合の例を示します。

```
Topology             : Duplex_Ring
My Box ID            : 2
Master ID            : 2
BK Master ID         : 1
Box Count            : 3

Box User Module                       Prio-                    Prom    Runtime   H/W
ID  Set  Name                  Exist  rity  MAC                Version Version   Version
--- ---- ---------------------- ----- ----- ------------------ ------- --------- -------
1   User ApresiaNP7000-48X6L   Exist 10    00-40-66-AA-52-1B 1.00.01 1.05.01   A
2   User ApresiaNP7000-48X6L   Exist 0     00-40-66-AA-31-00 1.00.01 1.05.01   A
3   User ApresiaNP7000-48X6L   Exist 60    00-40-66-AB-7D-5A 1.00.01 1.05.01   A
4   -    NOT_EXIST             No

 Stack Bandwidth and Unit Status:
 Box    User Set    SIO1 Active   SIO2 Active   Unit
 ID     Bandwidth   Bandwidth     Bandwidth     Status
 ----   ---------   ---------     ---------     ---------
 1      2-port(40G) 1-port        1-port        Normal
 2      2-port(40G) 1-port        1-port        Normal
 3      2-port(40G) 1-port        1-port        Normal
 4
```

4.3.3.2 バックアップマスターの障害発生／復旧時の動作

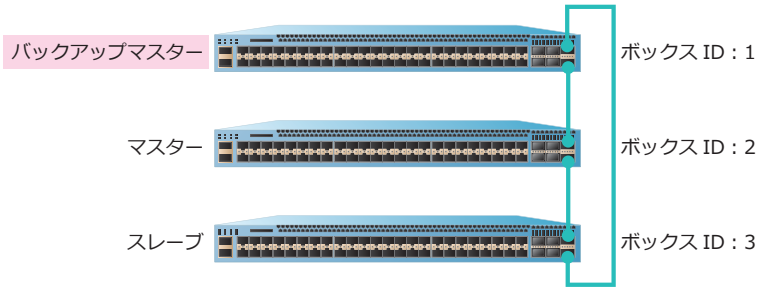
バックアップマスターに障害が発生した場合、バックアップマスターの次に優先度が高いスレーブがバックアップマスターになります。

以下に、バックアップマスターの障害発生／復旧時の動作と表示例を示します。

(1) 正常時

この例では、正常時はボックス ID［1］の装置がバックアップマスター、ボックス ID［2］の装置がマスター、ボックス ID［3］の装置がスレーブになっているとします。

図 4-12 バックアップマスターに障害が発生する前の構成



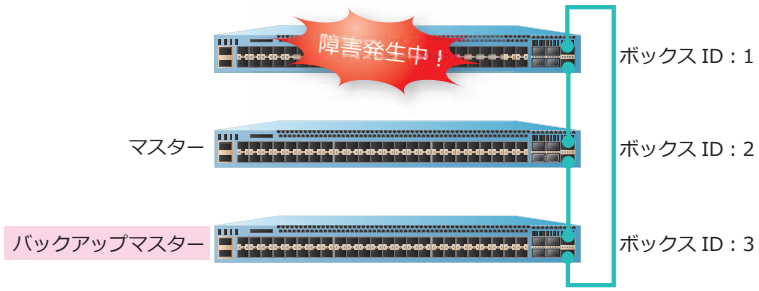
スタックの状態を **show stack** コマンドで確認した場合の例を示します。

```
Topology             : Duplex_Ring
My Box ID            : 2
Master ID            : 2
BK Master ID         : 1
Box Count            : 3

Box User Module                      Prio-                    Prom    Runtime   H/W
ID  Set  Name                  Exist rity  MAC                Version Version   Version
--- ---- --------------------- ----- ----- ------------------ ------- --------- -------
1   User ApresiaNP7000-48X6L   Exist 10    00-40-66-AA-52-1B 1.00.01 1.05.01   A
2   User ApresiaNP7000-48X6L   Exist 0     00-40-66-AA-31-00 1.00.01 1.05.01   A
3   User ApresiaNP7000-48X6L   Exist 60    00-40-66-AB-7D-5A 1.00.01 1.05.01   A
4   -    NOT_EXIST             No

 Stack Bandwidth and Unit Status:
 Box    User Set    SIO1 Active   SIO2 Active   Unit
 ID     Bandwidth   Bandwidth     Bandwidth     Status
 ----   ---------   ---------     ---------     ---------
 1      2-port(40G) 1-port        1-port        Normal
 2      2-port(40G) 1-port        1-port        Normal
 3      2-port(40G) 1-port        1-port        Normal
 4
```

(2) バックアップマスターに障害が発生した場合

バックアップマスターに障害が発生すると、バックアップマスターの次に優先度が高いスレーブがバックアップマスターになります。

図 4-13 バックアップマスターに障害が発生した場合



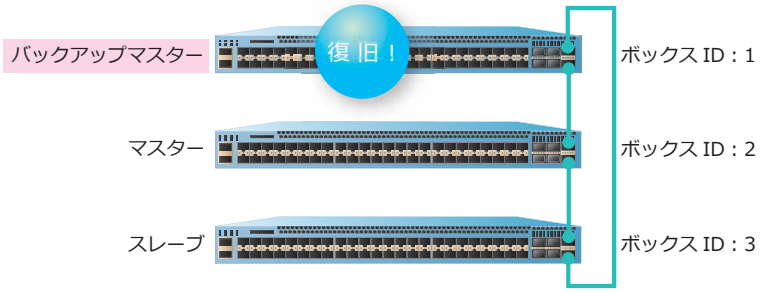
スタックの状態を **show stack** コマンドで確認した場合の例を示します。

```
Topology             : Duplex_Chain
My Box ID            : 2
Master ID            : 2
BK Master ID         : 3
Box Count            : 2

Box User Module                      Prio-                    Prom    Runtime   H/W
ID  Set  Name                   Exist rity  MAC                Version Version   Version
--- ---- ---------------------- ----- ----- ------------------ ------- --------- -------
1   -    ApresiaNP7000-48X6L    No
2   User ApresiaNP7000-48X6L    Exist 0     00-40-66-AA-31-00 1.00.01 1.05.01   A
3   User ApresiaNP7000-48X6L    Exist 60    00-40-66-AB-7D-5A 1.00.01 1.05.01   A
4   -    NOT_EXIST              No

 Stack Bandwidth and Unit Status:
 Box    User Set    SIO1 Active   SIO2 Active   Unit
 ID     Bandwidth   Bandwidth     Bandwidth     Status
 ----   ---------   ---------     ---------     ---------
 1
 2      2-port(40G) Down          1-port        Normal
 3      2-port(40G) 1-port        Down          Normal
 4
```

(3) 旧バックアップマスターの装置が復旧した場合

この例の場合、旧バックアップマスターのボックス ID［1］の装置が復旧すると、ボックス ID［1］の装置の優先度「10」が現状のバックアップマスターの優先度「60」よりも高いため、優先度の比較の結果、ボックス ID［1］の装置がバックアップマスターになり、ボックス ID［3］の装置がスレーブになります。

図 4-14 旧バックアップマスターの装置が復旧した場合



スタックの状態を **show stack** コマンドで確認した場合の例を示します。

```
Topology             : Duplex_Ring
My Box ID            : 2
Master ID            : 2
BK Master ID         : 1
Box Count            : 3

Box User Module                      Prio-                    Prom    Runtime   H/W
ID  Set  Name                  Exist rity  MAC                Version Version   Version
--- ---- --------------------- ----- ----- ------------------ ------- --------- -------
1   User ApresiaNP7000-48X6L   Exist 10    00-40-66-AA-52-1B 1.00.01 1.05.01   A
2   User ApresiaNP7000-48X6L   Exist 0     00-40-66-AA-31-00 1.00.01 1.05.01   A
3   User ApresiaNP7000-48X6L   Exist 60    00-40-66-AB-7D-5A 1.00.01 1.05.01   A
4   -    NOT_EXIST             No

 Stack Bandwidth and Unit Status:
 Box    User Set    SIO1 Active   SIO2 Active   Unit
 ID     Bandwidth   Bandwidth     Bandwidth     Status
 ----   ---------   ---------     ---------     ---------
 1      2-port(40G) 1-port        1-port        Normal
 2      2-port(40G) 1-port        1-port        Normal
 3      2-port(40G) 1-port        1-port        Normal
 4
```

4.3.3.3 スタックポートのケーブルの障害発生／復旧時の動作

スタックポートのケーブルに障害が発生すると、切り離されたスタックメンバーは、それぞれが独立したスタックとして機能し始めます。このとき、それぞれのスタックは同じ IP アドレスと MAC アドレスを使用するため、正常な通信ができなくなります。すみやかにケーブルの復旧を行ってください。

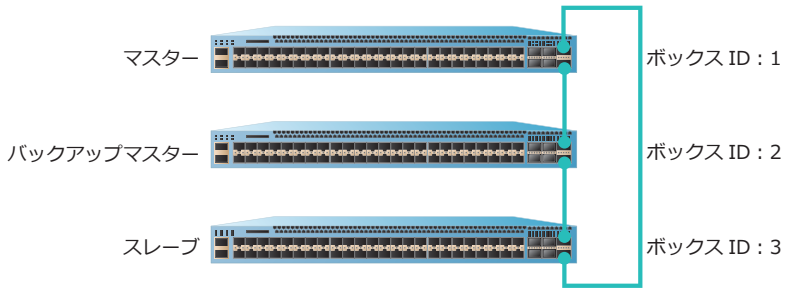
スタックポートのケーブル障害が復旧すると、それぞれの装置はお互いをスタックメンバーとして認識し、優先度と MAC アドレスに応じて役割が割り当てられます。なお、プリエンプトモードが無効の場合はマスターの優先度は「0」になるため、この例では MAC アドレスによってマスターとバックアップマスターが選出されます。

以下に、スタックポートのケーブルの障害発生／復旧時の動作と表示例を示します。

(1) 正常時

この例では、正常時はボックス ID［1］の装置がマスター、ボックス ID［2］の装置がバックアップマスター、ボックス ID［3］の装置がスレーブになっているとします。

図 4-15 スタックポートのケーブルに障害が発生する前の状態



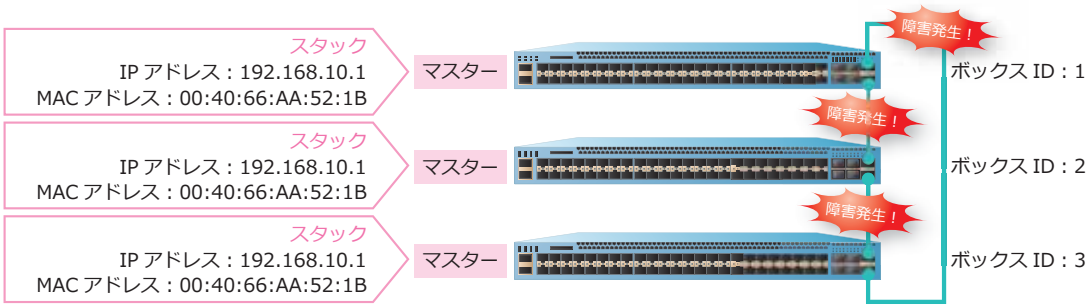
スタックの状態を **show stack** コマンドで確認した場合の例を示します。

```
Topology             : Duplex_Ring
My Box ID            : 1
Master ID            : 1
BK Master ID         : 2
Box Count            : 3

Box User Module                      Prio-                    Prom    Runtime   H/W
ID  Set  Name                  Exist rity  MAC                Version Version   Version
--- ---- --------------------- ----- ----- ------------------ ------- --------- -------
1   User ApresiaNP7000-48X6L   Exist 0     00-40-66-AA-52-1B 1.00.01 1.05.01   A
2   User ApresiaNP7000-48X6L   Exist 32    00-40-66-AA-31-00 1.00.01 1.05.01   A
3   User ApresiaNP7000-48X6L   Exist 60    00-40-66-AB-7D-5A 1.00.01 1.05.01   A
4   -    NOT_EXIST             No

 Stack Bandwidth and Unit Status:
 Box    User Set    SIO1 Active   SIO2 Active   Unit
 ID     Bandwidth   Bandwidth     Bandwidth     Status
 ----   ---------   ----------    ----------    ----------
 1      2-port(40G) 1-port        1-port        Normal
 2      2-port(40G) 1-port        1-port        Normal
 3      2-port(40G) 1-port        1-port        Normal
 4
```

(2) スタックポートのケーブル障害が発生した場合

スタックポートのケーブル障害が発生すると、切り離されたスタックメンバーは、それぞれが独立したスタックとして機能し始めます。

図 4-16 スタックポートのケーブル障害が発生した場合



ボックス ID［1］の装置の状態を **show stack** コマンドで確認した場合の例を示します。

> ***NOTE:*** **show stack** コマンドの［MAC］項目には、それぞれの装置自身のシステム MAC アドレスが表示されます。

> ***NOTE:*** マスターから引き継がれた MAC アドレスは、**show version** コマンドで確認できます。なお、NP7000 は 1.06.01 以降、NP5000 は 1.05.02 以降、NP4000 は 1.02.01 以降、NP2000 は 1.07.01 以降で対応しています。

```
Topology            : Duplex_Chain
My Box ID           : 1
Master ID           : 1
Box Count           : 1

Box User Module                      Prio-                    Prom    Runtime   H/W
ID  Set  Name                  Exist rity  MAC                Version Version   Version
--- ---- --------------------- ----- ----- ------------------ ------- --------- -------
1   User ApresiaNP7000-48X6L   Exist 0     00-40-66-AA-52-1B 1.00.01 1.05.01   A
2   -    ApresiaNP7000-48X6L   No
3   -    ApresiaNP7000-48X6L   No
4   -    NOT_EXIST             No

 Stack Bandwidth and Unit Status:
 Box    User Set    SIO1 Active   SIO2 Active   Unit
 ID     Bandwidth   Bandwidth     Bandwidth     Status
 ----   ---------   ---------     ---------     ---------
 1      2-port(40G) Down          Down          Normal
 2
 3
 4
```

ボックス ID［2］の装置の状態を **show stack** コマンドで確認した場合の例を示します。

```
Topology            : Duplex_Chain
My Box ID           : 2
Master ID           : 2
Box Count           : 1

Box User Module                      Prio-                    Prom    Runtime   H/W
ID  Set  Name                   Exist rity  MAC                Version Version   Version
--- ---- ---------------------- ----- ----- ------------------ ------- --------- -------
1   -    ApresiaNP7000-48X6L    No
2   User ApresiaNP7000-48X6L    Exist 0     00-40-66-AA-31-00 1.00.01 1.05.01   A
3   -    ApresiaNP7000-48X6L    No
4   -    NOT_EXIST              No

 Stack Bandwidth and Unit Status:
 Box    User Set    SIO1 Active   SIO2 Active   Unit
 ID     Bandwidth   Bandwidth     Bandwidth     Status
 ----   ---------   ---------     ---------     ---------
 1
 2      2-port(40G) Down          Down          Normal
 3
 4
```

ボックス ID［3］の装置の状態を **show stack** コマンドで確認した場合の例を示します。

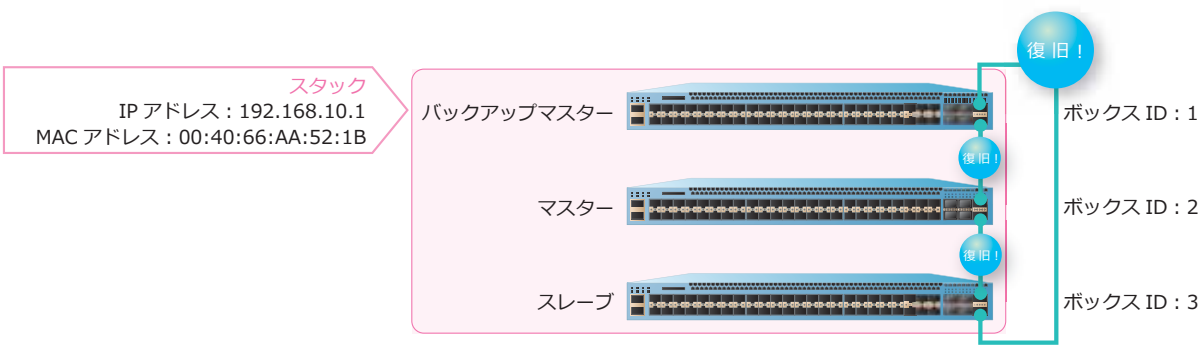
```
Topology            : Duplex_Chain
My Box ID           : 3
Master ID           : 3
Box Count           : 1

Box User Module                      Prio-                    Prom    Runtime   H/W
ID  Set  Name                   Exist rity  MAC                Version Version   Version
--- ---- ---------------------- ----- ----- ------------------ ------- --------- -------
1   -    ApresiaNP7000-48X6L    No
2   -    ApresiaNP7000-48X6L    No
3   User ApresiaNP7000-48X6L    Exist 0     00-40-66-AB-7D-5A 1.00.01 1.05.01   A
4   -    NOT_EXIST              No

 Stack Bandwidth and Unit Status:
 Box    User Set    SIO1 Active   SIO2 Active   Unit
 ID     Bandwidth   Bandwidth     Bandwidth     Status
 ----   ---------   ---------     ---------     ---------
 1
 2
 3      2-port(40G) Down          Down          Normal
 4
```

(3) スタックポートのケーブル障害が復旧した場合

この例（プリエンプトモード無効）では、切り離されたスタックメンバーはそれぞれマスターになっていて優先度「0」で動作しています。そのため、各装置が起動した状態のままスタックポートのケーブル障害が復旧すると、優先度が同じなため各装置の MAC アドレスによってマスターとバックアップマスターが選出されます。

この例の場合、MAC アドレスの値が一番小さいボックス ID［2］の装置がマスターになり、次に MAC アドレスの値が小さいボックス ID［1］の装置がバックアップマスターになります。ボックス ID［3］の装置はスレーブになります。

図 4-17 スタックポートのケーブル障害が復旧した場合



スタックの状態を **show stack** コマンドで確認した場合の例を示します。

```
Topology             : Duplex_Ring
My Box ID            : 2
Master ID            : 2
BK Master ID         : 1
Box Count            : 3

Box User Module                        Prio-                    Prom    Runtime   H/W
ID  Set  Name                  Exist   rity  MAC                Version Version   Version
--- ---- --------------------- ------- ----- ------------------ ------- --------- -------
1   User ApresiaNP7000-48X6L   Exist   10    00-40-66-AA-52-1B  1.00.01 1.05.01   A
2   User ApresiaNP7000-48X6L   Exist   0     00-40-66-AA-31-00  1.00.01 1.05.01   A
3   User ApresiaNP7000-48X6L   Exist   60    00-40-66-AB-7D-5A  1.00.01 1.05.01   A
4   -    NOT_EXIST             No

 Stack Bandwidth and Unit Status:
 Box    User Set    SIO1 Active   SIO2 Active   Unit
 ID     Bandwidth   Bandwidth     Bandwidth     Status
 ----   ---------   ---------     ---------     ----------
 1      2-port(40G) 1-port        1-port        Normal
 2      2-port(40G) 1-port        1-port        Normal
 3      2-port(40G) 1-port        1-port        Normal
 4
```

4.3.4 ボックス ID 競合時の動作

スタックを構成する場合、スタックメンバーには、それぞれユニークなボックス ID を割り当てる必要があります。ボックス ID が競合しているスタックメンバーを接続しても、スタックは構成されません。以下にボックス ID の競合ケースと、その場合の動作、および復旧方法を示します。

表 4-14 ボックス ID の競合ケース

競合ケース	競合時の動作	復旧方法
競合ケース (1) 動作中のスタック構成に、ボックス ID が競合した装置を電源 OFF の状態で追加してから、電源 ON した場合。	動作中のスタック構成はそのまま動作。 新たに追加した装置はスタック構成に取り込まれず、ボックス ID 競合モードで起動。	新たに追加した装置をスタック構成から取り外し、一度電源 OFF/ON して通常モードで単体で起動。その後、ボックス ID の競合を解消してから、スタック構成に戻す。
競合ケース (2) 動作中のスタック構成に、ボックス ID が競合した装置を電源 ON の状態で追加した場合。	動作中のスタック構成はそのまま動作。 新たに追加した装置はスタック構成に取り込まれず、通常モードで起動したまま。	新たに追加した装置をスタック構成から取り外し、ボックス ID の競合を解消してから、スタック構成に戻す。
競合ケース (3) すべての装置（ボックス ID が競合した装置を含む）を電源 OFF の状態で接続してから、電源 ON した場合。	すべての装置がボックス ID 競合モードで起動。	すべての装置をスタック構成から取り外し、一度電源 OFF/ON して通常モードで単体で起動。その後、ボックス ID の競合を解消してから、スタック構成に戻す。

4.3.4.1 ボックス ID 競合モード

稼働中のスタック構成において、スタックメンバーを追加した際などにボックス ID の競合を検出すると、ログ／トラップが通知されます。ボックス ID の競合を検出した際のログの例を示します。

```
CRIT(2) Hot insert failed, box ID conflict: Unit 1 conflict (MAC: 00-40-66-B4-97-1F and
MAC: 00-40-66-B4-96-B5)
```

ボックス ID の競合を検出した際に、マスター装置または追加した装置にコンソールを接続していると、ボックス ID が競合したことを示すメッセージが出力されます。追加した装置をスタック構成に接続して起動した際に、ボックス ID［1］の装置が 2 台検出されたことを示すメッセージの出力例を示します。

```
Boot Procedure V1.00.01
  MAC Address: 00-40-66-DE-52-A1
  H/W Version: A

Power On Self Test: 100 %

Please Wait, Loading V1.06.01

Firmware: 100 %
UART init: 100 %

Starting firmware...

Device Discovery:     -
Stacking failed! Box ID 1 conflicts, please reconfigure it.
Device Type: ApresiaNP7000-48X6L, MAC Address: 00-40-66-DE-52-58
Device Type: ApresiaNP7000-48X6L, MAC Address: 00-40-66-DE-52-A1
```

起動時にボックス ID の競合を検出した装置は、ボックス ID 競合モードで起動します。ボックス ID 競合モードで起動した装置は、基本的には電源を一度落としてスタック構成から取り外し、単体で正常に起動させてからボックス ID の競合を修正してください。

> ***NOTE:*** ボックス ID 競合モードの状態でボックス ID を修正して設定を保存すると、再起動後にボックス ID は変更されますが、それ以外の設定は維持されません。そのため、基本的にはボックス ID 競合モードの状態で設定を保存することは推奨しません。
>
> ***NOTE:*** ボックス ID 競合モードでボックス ID を修正して設定を保存した装置をスタック構成に取り込んだ場合は、スタック構成に取り込まれた後にマスターで **`write memory`** コマンドを使用して設定を保存し、新たに追加した装置の startup-config にも設定を同期してください。

ボックス ID 競合モードでは実行できるコマンドは制限されていて、「**`login`**」「**`logout`**」「**`enable`**」「**`copy running-config startup-config`**」「**`[no] stack renumber`**」「**`stack my_box_id`**（NP7000/NP5000 は 1.03.02 以降）」「**`write memory`**（NP7000/NP5000 は 1.03.02 以降）」コマンドのみが使用できます。なお、省略形式では実行できません。

4.4 スタック機能の運用操作

スタック機能の運用操作について説明します。

4.4.1 スタックメンバーの追加

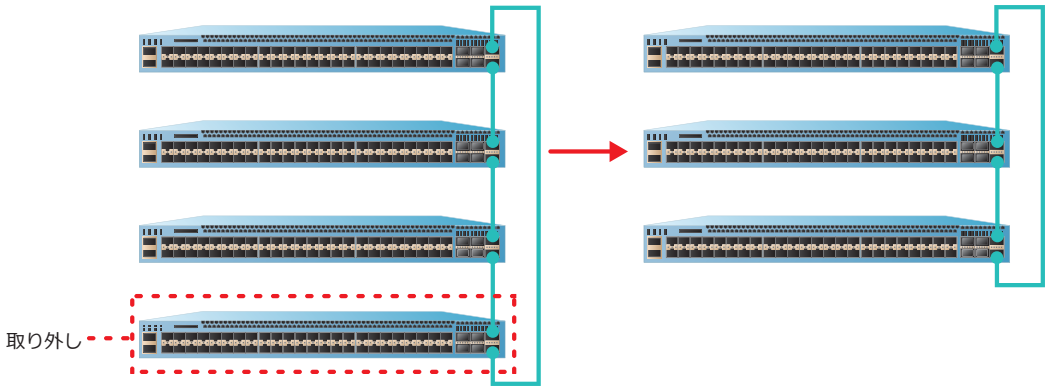
稼働中のスタックに、スタックメンバーを追加できます。スタックメンバー追加時の動作は、スタックの稼働環境によって異なります。

- 電源 ON の状態の装置をスタックに追加する場合、一時的にスタック内でマスターが重複して存在することになります。その後、再計算によってスタックメンバーがバックアップマスターまたはスレーブの役割に切り替わる場合は、バックアップマスターまたはスレーブの役割に切り替わった装置の初期化が行われ、同期をとるためにすべてのポートが一時的にリンクダウンします。
- 電源 OFF の状態の装置をスタックに追加する場合は、装置の初期化が行われた後にスタックに追加されるため、ポートのリンクダウンは発生しません。
- 追加するスタックメンバーが稼働中の場合（追加時にファームウェアが動作している場合）、スタックトポロジーの更新が終了するまで、約 24 秒を要します。
- 追加したスタックメンバーが停止中の場合（追加後にファームウェアを起動する場合）、スタックトポロジーの更新が終了するまで、約 48 秒を要します。

4.4.2 スタックメンバーの取り外し

稼働中のスタックからスタックメンバーを取り外せます。取り外す際、設定変更は不要です。ケーブルのみ、接続しなおしてください。

図 4-18 スタックメンバーの取り外し

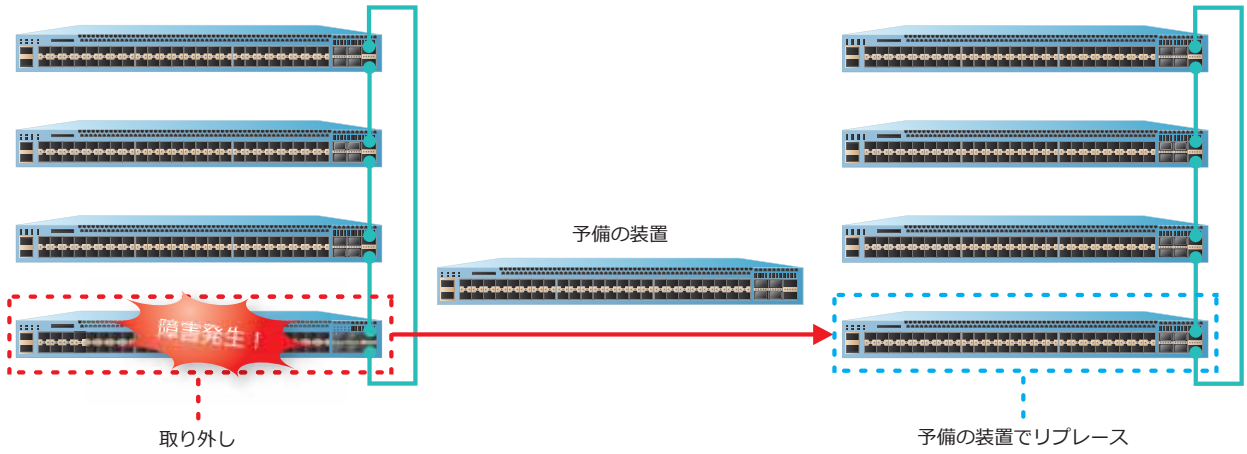


取り外したスタックメンバーに関連する設定は、構成情報に残ったままになります。構成情報から取り外したスタックメンバーに関連する設定を削除する場合は、**`stack remove`** コマンドを使用します。

4.4.3 スタックメンバーのリプレース

稼働中のスタックでスタックメンバーに障害が発生した場合は、障害が発生したスタックメンバーを取り外し、予備の装置に交換します。

図 4-19 スタックメンバーのリプレース



プリエンプトモードが無効の場合（デフォルト設定）

プリエンプトモードが無効の場合のリプレース手順例を示します。基本的には、予備の装置を単体で起動し、各種スタック設定を実施して設定を保存したら、電源を落とした状態でスタック構成に接続して起動する手順になります。スタックに接続してから予備の装置の電源を入れることにより、マスターの切り替わりを発生させずにリプレースできます。

1. 予備の装置を単体で起動します。
2. **stack bandwidth** コマンドでスタックポートを設定します。
3. ボックス ID が手動設定の場合は、**stack my_box_id** コマンドで、交換対象の装置のボックス ID を予備の装置に設定します。
4. **stack my_box_priority** コマンドで、交換対象の装置の優先度を予備の装置に設定します。
5. **write memory** コマンドで設定を保存して、予備の装置の電源を落とします。
6. 予備の装置を交換対象の装置と入れ替えてスタック構成に接続します。
7. 予備の装置の電源を入れます。
8. 予備の装置が起動してスタックメンバーとして正常に認識された後、マスターで **write memory** コマンドを使用して設定を保存し、予備の装置の startup-config にも設定を同期します。

   NOTE: リプレースした予備の装置にもスタック全体の構成情報を保存するために、予備の装置がスタックメンバーとして認識された後、マスターで **write memory** コマンドを使用して設定を一度保存してください。

   NOTE: リプレース後のスタックメンバーにはカスタマイズした認証ページ、SSL サーバー証明書（https-certificate）、および SSL サーバーの秘密鍵（https-private-key）が引き継がれません。各ファイルを使用している場合は、**copy** コマンドを使用してスタック構成全体にコピーしてください。

   REF: ボックス ID と優先度の変更には、**stack renumber** コマンドや **stack priority** コマンドも使用できます。**stack renumber** コマンドおよび **stack priority** コマンドの詳細については、『コマンドリファレンス』を参照してください。

プリエンプトモードが有効の場合

プリエンプトモードが有効なスタック構成で、交換対象が「交換する前までマスター以外だった装置」の場合は、以下の追加手順以外はプリエンプトモードが無効な場合の手順例と同じです。

- 追加手順：予備の装置を単体で起動して各種スタック設定を実施する際に、**stack preempt** コマンドでプリエンプトモードを有効にする。

プリエンプトモードが有効なスタック構成で、交換対象が「障害が発生して交換する前までマスターだった装置」の場合は、手順が複雑になることや、プリエンプトモードの仕様制限に注意してください。以下にこのケースの注意点を示します。

- プリエンプトモードが有効なスタック構成のため、交換する予備の装置の優先度が最も高い場合は、交換後はプリエンプトモードによってマスターが予備の装置に切り替わります。そのため、交換前の装置と同じ構成情報や動作に必要なファイルなどを、あらかじめ予備の装置に入れておく必要があることに注意してください。たとえば、交換前の装置で **backup** コマンドでバックアップして、予備の装置で **restore** コマンドでリストアすることが可能です。また、SD カードブート使用環境の場合は、交換前の装置の SD カードを予備の装置に入れ替えることで実現可能です。
- プリエンプトモードによってマスターが切り替わる場合には、ポート閉塞を伴うマスター再選出プロセスが動作するため、一定の通信断時間が発生することに注意してください。
- また、プリエンプトモードによってマスターが切り替わる場合には、「2 台の稼働中のマスターの優先度が比較されて、優先度の高い方がマスターとして残り、優先度の低い方がバックアップマスターになる」という動作になるため、その後のスタックの MAC アドレスはそのマスターになった装置の MAC アドレスになることに注意してください。

  REF: マスターの切り替わり時の制限事項については、「スタック機能の制限事項および注意事項」を参照してください。

4.4.4 SD カードブート使用時のスタックメンバーのリプレース

スタックを構成するすべての装置に SD カードが実装されており、かつ **backup clone** コマンドを実行済みの状態で、スタックメンバーをリプレースする場合は、以下の手順を実行します。

1. 予備の装置に、交換対象となったメンバー装置の SD カードを実装します。
2. 予備の装置をスタックに接続し、電源を入れます。
3. 予備の装置がスタックメンバーとして認識されたことを確認します。

   REF: SD カードブートの詳細については、「第 2 編 管理運用」の「SD カードブート」を参照してください。

4.4.5 スタック構成のファームウェアのアップデート

スタックを構成するすべての装置は、同一バージョンのファームウェアで起動する必要があります。そのため、ファームウェアをアップデートする場合は、スタック構成全体を再起動し、スタックを構成するすべての装置のファームウェアを同時にアップデートしてください。

2 台スタック構成の場合は、対応している機種／バージョンで、一時的なバージョンチェック無視機能（**stack version check ignore** コマンド）を利用することもできます。

REF: ファームウェアのアップデート方法については、「第 2 編 管理運用」の「ファームウェアのアップデート方法」を参照してください。

4.5 スタックの状態確認

スタックの状態を表示して確認する方法を説明します。

4.5.1 スタックの状態の表示

show stack コマンドで、スタックの状態を確認できます。

> ***NOTE:*** Unit Status 項目は、NP7000 の 1.05.01 以降、NP5000 の 1.05.01 以降、NP4000 の 1.03.01 以降、NP3000 の 1.06.01 以降、NP2100 の 1.09.02 以降、NP2000 の 1.09.01 以降、NP2500 の 1.12.01 以降で表示されます。
>
> ***NOTE:*** Unit Status 項目は、NP7000 の 1.10.02 以降、NP5000 の 1.10.02 以降、NP4000 の 1.03.03 以降、NP3000 の 1.10.01 以降、NP2100 の 1.09.10/1.12.01 以降、NP2000 の 1.09.10 以降、NP2500 の 1.12.01 以降で表示文字列が変更されています。

表示例を以下に示します。

```
# show stack

Stacking Mode        : Enabled ...(1)
Stack Preempt        : Disabled ...(2)
Trap State           : Disabled ...(3)
Port-channel mode    : All ...(4)
Stack-port load-balance: default ...(5)
Version check        : Enabled ...(6)

Topology             : Duplex_Ring ...(7)
My Box ID            : 1 ...(8)
Master ID            : 1 ...(9)
BK Master ID         : 2 ...(10)
Box Count            : 3 ...(11)
(12)(13) (14)                    (15)   (16)   (17)               (18)     (19)       (20)
Box User Module                         Prio-                    Prom     Runtime    H/W
ID  Set  Name                    Exist  rity   MAC                Version  Version    Version
--- ---- ---------------------- ------ ------ ------------------ ------- --------- -------
1   User ApresiaNP7000-48X6L    Exist  0      00-40-66-A8-CC-36  1.00.01  1.11.01    A
2   User ApresiaNP7000-48X6L    Exist  20     00-40-66-AA-52-1B  1.00.01  1.11.01    A
3   User ApresiaNP7000-48X6L    Exist  30     00-40-66-AB-7D-5A  1.00.01  1.11.01    A
4   -    NOT_EXIST              No

 Stack Bandwidth and Unit Status:
 (12)    (21)         (22)           (23)           (24)
 Box     User Set     SIO1 Active    SIO2 Active    Unit
 ID      Bandwidth    Bandwidth      Bandwidth      Status
 ----    ---------    ---------      ---------      ---------
 1       2-port(40G)  1-port         1-port         Stable
 2       2-port(40G)  1-port         1-port         Stable
 3       2-port(40G)  1-port         1-port         Stable
 4
```

各項目の説明は、以下のとおりです。

表 4-15 show stack コマンドの表示項目

項番	説明
(1)	スタックの有効 (Enabled) ／無効 (Disabled) を表示します。
(2)	プリエンプトモードの有効 (Enabled) ／無効 (Disabled) を表示します。NP7000 で l2-extend オプションを指定して有効にした場合は、Enabled(L2-Extend) と表示されます。

項番	説明
(3)	トラップの有効 (Enabled) ／無効 (Disabled) を表示します。
(4)	ポートチャネルモードを表示します。 • All：スタック跨ぎのポートチャネルにおいて、装置跨ぎの負荷分散が有効 • Partial：スタック跨ぎのポートチャネルにおいて、装置跨ぎの負荷分散が無効
(5)	スタックポートの負荷分散アルゴリズムを表示します。
(6)	スタックメンバーのバージョンチェック処理の設定を表示します。 • Enabled：バージョンチェック処理は有効（デフォルト設定） • Disabled：バージョンチェック処理を無視する設定時（stack version check ignore）
(7)	スタックトポロジーを表示します。 • Duplex_Chain：チェーントポロジー • Duplex_Ring：リングトポロジー
(8)	装置のボックス ID を表示します。
(9)	マスターのボックス ID を表示します。
(10)	バックアップマスターのボックス ID を表示します。
(11)	スタックを構成している装置の数を表示します。
(12)	ボックス ID を表示します。
(13)	ボックス ID の設定状況を表示します。 • Auto：自動割り当て • User：手動割り当て
(14)	装置の名称を表示します。
(15)	スタック構成の中に存在しているかどうかを表示します。
(16)	優先度を表示します。
(17)	スタックメンバーの MAC アドレスを表示します。
(18)	ブートローダーバージョンを表示します。
(19)	ファームウェアバージョンを表示します。
(20)	ハードウェアリビジョンを表示します。
(21)	スタックポート構成を表示します。 • 2-port(40G)：stack bandwidth 40G 2-port 設定時 • 4-port(25G)：stack bandwidth 25G 4-port 設定時 • 2-port(25G)：stack bandwidth 25G 2-port 設定時 • 4-port(10G)：stack bandwidth 10G 4-port 設定時 • 2-port(10G)：stack bandwidth 10G 2-port 設定時

項番	説明
(22)	スタックポート 1 の状態を表示します。 • 4-port：スタックポート 1 の 4 ポートがリンクアップ状態（4-port chain 設定時） • 3-port：スタックポート 1 の 3 ポートがリンクアップ状態（4-port chain 設定時） • 2-port：スタックポート 1 の 2 ポートがリンクアップ状態 • 1-port：スタックポート 1 の 1 ポートがリンクアップ状態 • Down：スタックポート 1 の全ポートがリンクダウン状態
(23)	スタックポート 2 の状態を表示します。 • 2-port：スタックポート 2 の 2 ポートがリンクアップ状態 • 1-port：スタックポート 2 の 1 ポートがリンクアップ状態 • Down：スタックポート 2 の全ポートがリンクダウン状態 • -：chain オプションが有効なスタック構成の場合
(24)	装置の状態を表示します。 • Stable：安定状態（表示文字列の変更前のバージョンでは Normal 表示） • *Unstable：不安定状態（表示文字列の変更前のバージョンでは *Abnormal 表示）

4.5.2 スタックポートの情報の表示

`show stack detail` コマンドでスタックポートの情報を確認できます。

> ***NOTE:*** 本コマンドは、NP7000 の 1.09.01 以降、NP5000 の 1.09.01 以降、NP3000 の 1.09.01 以降、NP2100 の 1.11.01 以降、NP2500 の 1.12.01 以降でサポートしています。

表示例を以下に示します。

```
# show stack detail

Unit 1, Stack Port 65 link status is up ...(1)
 Type: 40GBASE-SR4 ...(2)
 Vendor PN: AFBR-79E4Z-D ...(3)
 Vendor SN: QB240295 ...(4)

Unit 1, Stack Port 69 link status is up
 Type: 40GBASE-SR4
 Vendor PN: AFBR-79E4Z-D
 Vendor SN: QB240256

Unit 2, Stack Port 65 link status is up
 Type: 40GBASE-SR4
 Vendor PN: AFBR-79E4Z-D
 Vendor SN: QB240233

Unit 2, Stack Port 69 link status is up
 Type: 40GBASE-SR4
 Vendor PN: AFBR-79E4Z-D
 Vendor SN: QB240300
```

各項目の説明は、以下のとおりです。

表 4-16 `show stack detail` コマンドの表示項目

項番	説明
(1)	ボックス ID、スタックポートのポート番号、リンク状態（up/down）を表示します。

項番	説明
(2)	挿入されているトランシーバーの種類を表示します。
(3)	型式番号を表示します。
(4)	シリアル番号を表示します。

4.6 スタックの構成例と設定例

スタックを利用する場合の構成例と設定例を示します。

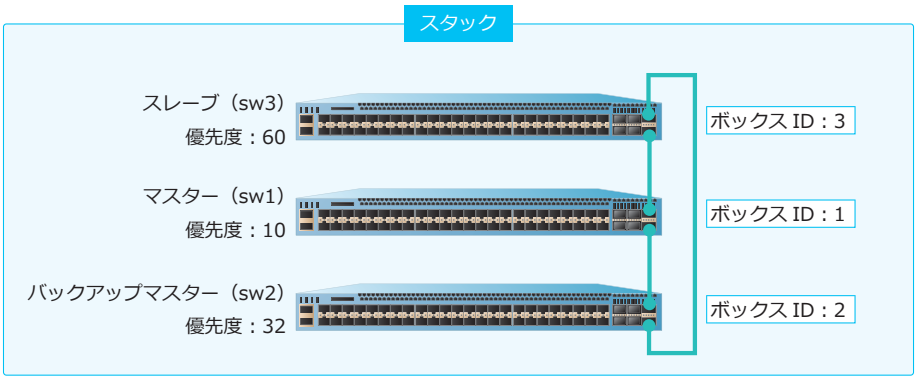
4.6.1 リングトポロジー

以下のコマンドでスタック設定を実施する場合の例を示します。各装置を単体で起動した状態でスタック設定を実施します。

- **stack bandwidth** コマンドでスタックポートを指定してスタックを有効化
- **stack my_box_id** コマンドでボックス ID を設定
- **stack my_box_priority** コマンドで優先度を設定

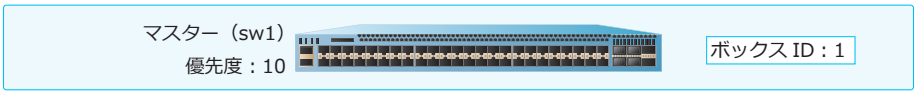
各装置でスタック設定を実施した後は、想定した装置がマスターになるように、すべてのメンバー装置を電源 OFF した状態でスタックポートを接続し、同時に起動してスタックを構成します。

図 4-20 スタックの構成例（リングトポロジー）



4.6.1.1 マスターの設定例（sw1）

図 4-21 マスターの設定例（sw1）



1. スタック機能を有効にします。

```
sw1# stack bandwidth 40G 2-port

 WARNING: The command does not take effect until the next reboot.
sw1#
```

2. ボックス ID を［1］に設定します。

```
sw1# stack my_box_id 1

 WARNING: The command does not take effect until the next reboot.
sw1#
```

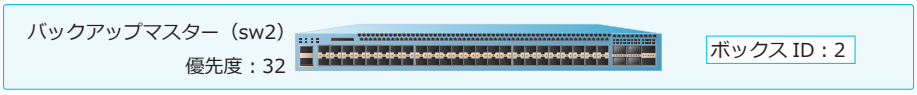
3. 優先度を［10］に設定して保存します。スタックは装置を起動し直した後に有効になります。

```
sw1# stack my_box_priority 10
sw1# write memory

Destination filename startup-config? [y/n]:  y

Saving all configurations to NV-RAM.......... Done.

sw1#
```

4. すべてのメンバー装置でスタック設定が完了したら、すべてのメンバー装置を電源 OFF した状態でスタックポートを接続し、同時に起動してスタックを構成します。

4.6.1.2 バックアップマスターの設定例（sw2）

図 4-22 バックアップマスターの設定例（sw2）



1. スタック機能を有効にします。

```
sw2# stack bandwidth 40G 2-port

 WARNING: The command does not take effect until the next reboot.
sw2#
```

2. ボックス ID を［2］に設定します。

```
sw2# stack my_box_id 2

 WARNING: The command does not take effect until the next reboot.
sw2#
```

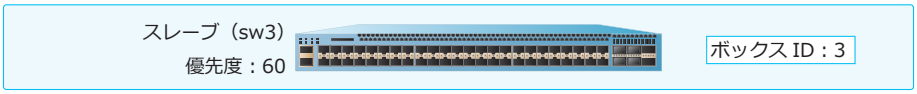
3. 優先度を［32］に設定して保存します。スタックは装置を起動し直した後に有効になります。

```
sw2# stack my_box_priority 32
sw2# write memory

Destination filename startup-config? [y/n]:  y

Saving all configurations to NV-RAM.......... Done.

sw2#
```

4. すべてのメンバー装置でスタック設定が完了したら、すべてのメンバー装置を電源 OFF した状態でスタックポートを接続し、同時に起動してスタックを構成します。

4.6.1.3 スレーブの設定例（sw3）

図 4-23 スレーブの設定例（sw3）



1. スタック機能を有効にします。

```
sw3# stack bandwidth 40G 2-port

 WARNING: The command does not take effect until the next reboot.
sw3#
```

2. ボックス ID を［3］に設定します。

```
sw3# stack my_box_id 3

 WARNING: The command does not take effect until the next reboot.
sw3#
```

3. 優先度を［60］に設定して保存します。スタックは装置を起動し直した後に有効になります。

```
sw3# stack my_box_priority 60
sw3# write memory

Destination filename startup-config? [y/n]:  y

Saving all configurations to NV-RAM.......... Done.

sw3#
```

4. すべてのメンバー装置でスタック設定が完了したら、すべてのメンバー装置を電源 OFF した状態でスタックポートを接続し、同時に起動してスタックを構成します。

4.6.2 リングトポロジー（stack renumber / stack priority コマンド）

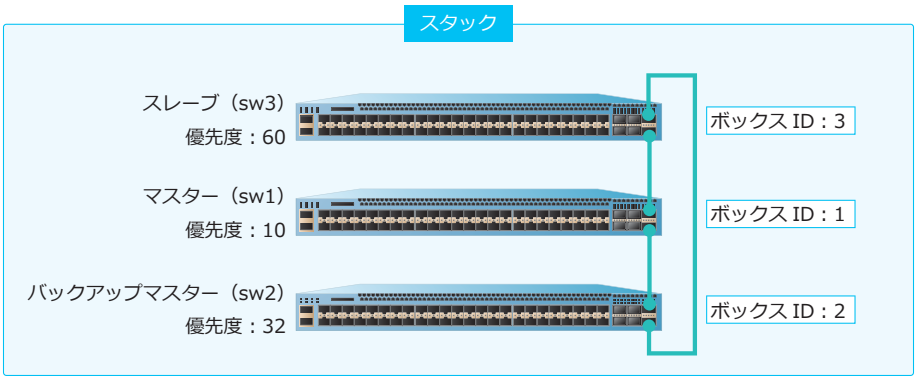
スタックのボックス ID と優先度は **stack my_box_id** コマンドおよび **stack my_box_priority** コマンドで設定しますが、**stack renumber** コマンドおよび **stack priority** コマンドでも設定できます。

以下のコマンドでスタック設定を実施する場合の例を示します。各装置を単体で起動した状態でスタック設定を実施します。

- **stack bandwidth** コマンドでスタックポートを指定してスタックを有効化
- **stack renumber** コマンドでボックス ID を設定
- **stack priority** コマンドで優先度を設定

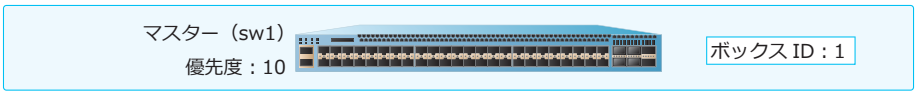
各装置でスタック設定を実施した後は、想定した装置がマスターになるように、すべてのメンバー装置を電源 OFF した状態でスタックポートを接続し、同時に起動してスタックを構成します。

図 4-24 スタックの構成例（リングトポロジー）



4.6.2.1 マスターの設定例（sw1）

図 4-25 マスターの設定例（sw1）



1. スタック機能を有効にします。

```
sw1# stack bandwidth 40G 2-port

 WARNING: The command does not take effect until the next reboot.
sw1#
```

2. 設定前の装置のボックス ID はデフォルトの［1］とします。この装置ではボックス ID を［1］のまま使用するため、ボックス ID の変更は不要です。設定を保存し、装置を再起動します。再起動後にスタックが有効になります。

```
sw1# write memory

Destination filename startup-config? [y/n]:  y

Saving all configurations to NV-RAM.......... Done.

sw1# reboot

Are you sure you want to proceed with the system reboot?(y/n) y
Please wait, the switch is rebooting...
```

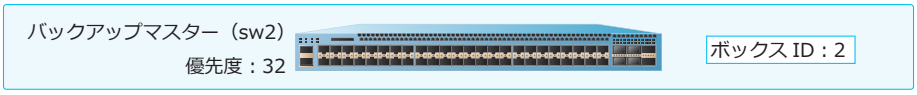
3. ボックス ID［1］の優先度を［10］に設定した後、設定を保存します。

```
sw1# stack 1 priority 10
sw1# write memory

Destination filename startup-config? [y/n]:  y

Saving all configurations to NV-RAM.......... Done.

sw1#
```

4. すべてのメンバー装置でスタック設定が完了したら、すべてのメンバー装置を電源 OFF した状態でスタックポートを接続し、同時に起動してスタックを構成します。

4.6.2.2 バックアップマスターの設定例（sw2）

図 4-26 バックアップマスターの設定例（sw2）



1. スタック機能を有効にします。

```
sw2# stack bandwidth 40G 2-port

 WARNING: The command does not take effect until the next reboot.
sw2#
```

2. 設定前の装置のボックス ID はデフォルトの［1］とします。ボックス ID を［2］に変更した後、設定を保存し、装置を再起動します。再起動後にスタックが有効になります。

```
sw2# stack 1 renumber 2

 WARNING: The command does not take effect until the next reboot.
sw2# write memory

Destination filename startup-config? [y/n]:  y

Saving all configurations to NV-RAM.......... Done.

sw2# reboot

Are you sure you want to proceed with the system reboot?(y/n) y
Please wait, the switch is rebooting...
```

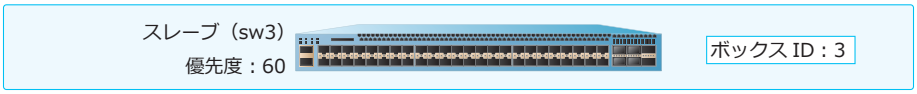
3. ボックス ID［2］の優先度を［32］に設定した後、設定を保存します。

```
sw2# stack 2 priority 32
sw2# write memory

Destination filename startup-config? [y/n]:  y

Saving all configurations to NV-RAM.......... Done.

sw2#
```

4. すべてのメンバー装置でスタック設定が完了したら、すべてのメンバー装置を電源 OFF した状態でスタックポートを接続し、同時に起動してスタックを構成します。

4.6.2.3 スレーブの設定例（sw3）

図 4-27 スレーブの設定例（sw3）



1. スタック機能を有効にします。

```
sw3# stack bandwidth 40G 2-port

 WARNING: The command does not take effect until the next reboot.
sw3#
```

2. 設定前の装置のボックス ID はデフォルトの［1］とします。ボックス ID を［3］に変更した後、設定を保存し、装置を再起動します。再起動後にスタックが有効になります。

```
sw3# stack 1 renumber 3

 WARNING: The command does not take effect until the next reboot.
sw3# write memory

Destination filename startup-config? [y/n]:  y

Saving all configurations to NV-RAM.......... Done.

sw3# reboot

Are you sure you want to proceed with the system reboot?(y/n) y
Please wait, the switch is rebooting...
```

3. ボックス ID［3］の優先度を［60］に設定した後、設定を保存します。

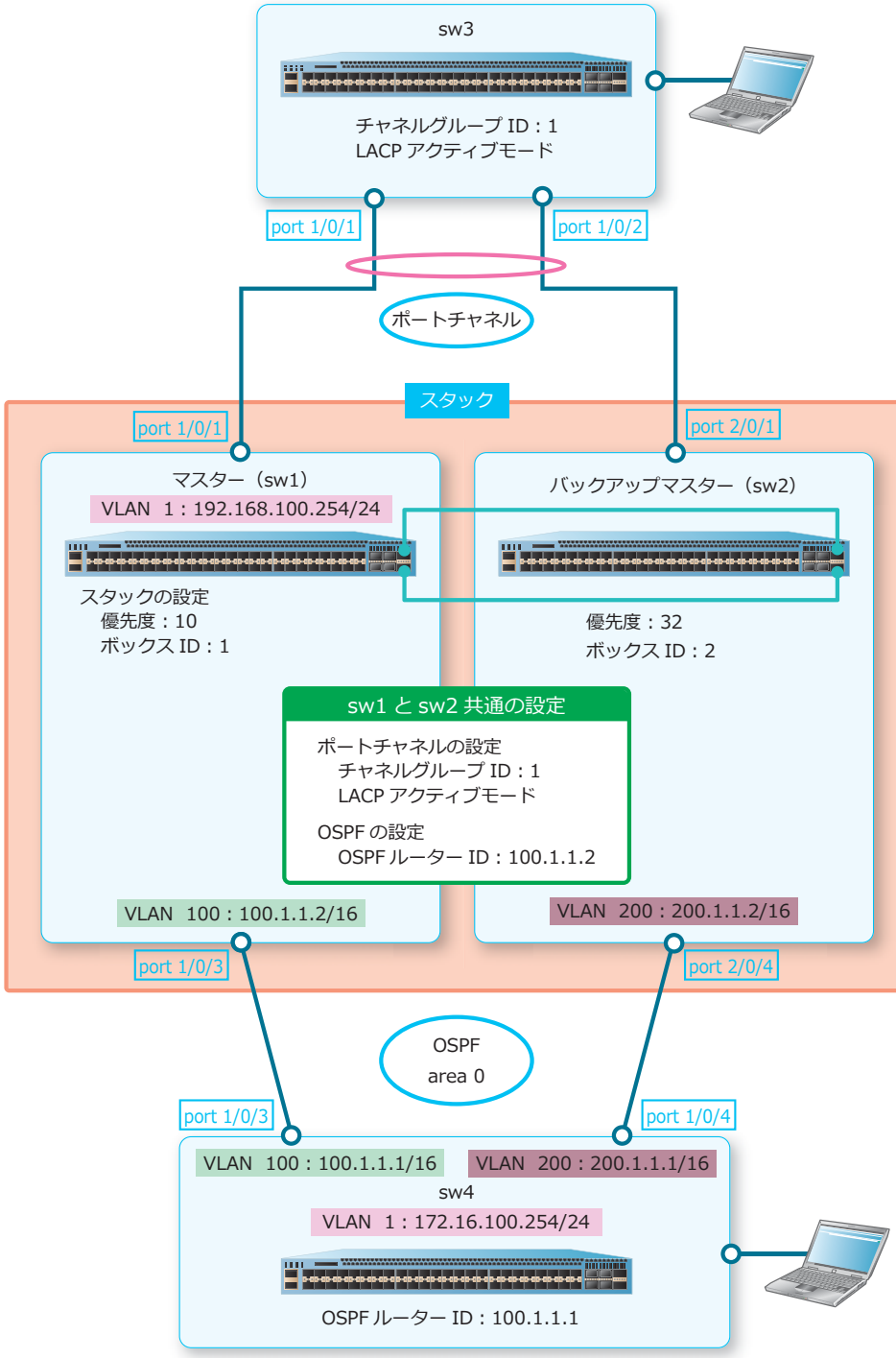
```
sw3# stack 3 priority 60
sw3# write memory

Destination filename startup-config? [y/n]:  y

Saving all configurations to NV-RAM.......... Done.

sw3#
```

4. すべてのメンバー装置でスタック設定が完了したら、すべてのメンバー装置を電源 OFF した状態でスタックポートを接続し、同時に起動してスタックを構成します。

4.6.3 リングトポロジー（OSPF、ポートチャネル併用）

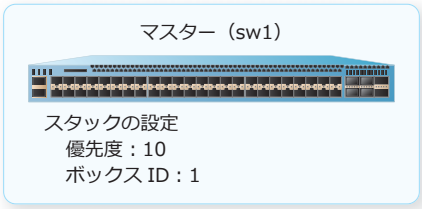
2 台の装置でリングトポロジーのスタックを構成します。各装置でスタック設定を実施した後は、想定した装置がマスターになるように、すべてのメンバー装置を電源 OFF した状態でスタックポートを接続し、同時に起動してスタックを構成します。スタックを構成した後は、マスターからスタック以外の設定を実施します。

図 4-28 スタックの構成例（リングトポロジー＋ OSPF ＋ポートチャネル）



4.6.3.1 マスターの設定例（sw1）

図 4-29 マスターの設定例（sw1）



1. スタック機能を有効にします。

```
sw1# stack bandwidth 40G 2-port

 WARNING: The command does not take effect until the next reboot.
sw1#
```

2. ボックス ID を［1］に設定します。

```
sw1# stack my_box_id 1

 WARNING: The command does not take effect until the next reboot.
sw1#
```

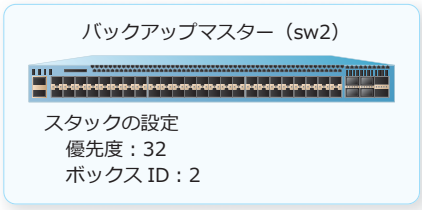
3. 優先度を［10］に設定して保存します。スタックは装置を起動し直した後に有効になります。

```
sw1# stack my_box_priority 10
sw1# write memory

Destination filename startup-config? [y/n]:  y

Saving all configurations to NV-RAM.......... Done.

sw1#
```

4. すべてのメンバー装置でスタック設定が完了したら、すべてのメンバー装置を電源 OFF した状態でスタックポートを接続し、同時に起動してスタックを構成します。

4.6.3.2 バックアップマスターの設定例（sw2）

図 4-30 バックアップマスターの設定例（sw2）



1. スタック機能を有効にします。

```
sw2# stack bandwidth 40G 2-port

 WARNING: The command does not take effect until the next reboot.
sw2#
```

2. ボックス ID を［2］に設定します。

```
sw2# stack my_box_id 2

 WARNING: The command does not take effect until the next reboot.
sw2#
```

3. 優先度を［32］に設定して保存します。スタックは装置を起動し直した後に有効になります。

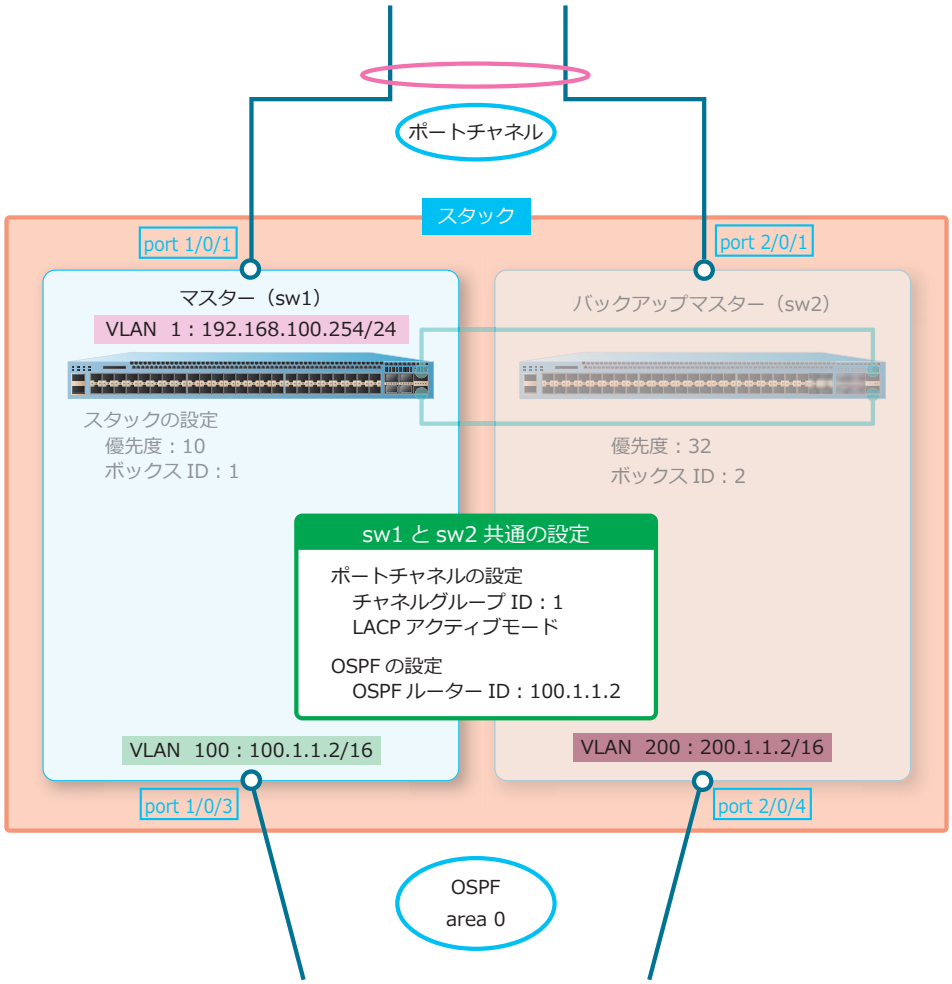
```
sw2# stack my_box_priority 32
sw2# write memory

Destination filename startup-config? [y/n]:  y

Saving all configurations to NV-RAM.......... Done.

sw2#
```

4. すべてのメンバー装置でスタック設定が完了したら、すべてのメンバー装置を電源 OFF した状態でスタックポートを接続し、同時に起動してスタックを構成します。

4.6.3.3 sw1 のポートチャネルと OSPF の設定例

スタックを構成した後は、マスターからのみ設定できます。

図 4-31 sw1 のポートチャネルと OSPF の設定例



1. ポート 1/0/1 とポート 2/0/1 をチャネルグループに登録し、チャネルグループの ID を［1］に設定します。また、チャネルグループを LACP アクティブモードで動作させます。

```
sw1# configure terminal
sw1(config)# interface range port 1/0/1,2/0/1
sw1(config-if-port-range)# channel-group 1 mode active
sw1(config-if-port-range)# exit
sw1(config)#
```

2. VLAN 1、VLAN 100、および VLAN 200 を作成します。

```
sw1(config)# vlan 1
sw1(config-vlan)# exit
sw1(config)# vlan 100
sw1(config-vlan)# exit
sw1(config)# vlan 200
sw1(config-vlan)# exit
sw1(config)#
```

3. ポート 1/0/3 をトランクポートとして設定し、トランクポートに［VLAN 100］を割り当てます。また、ポート 2/0/4 をトランクポートとして設定し、トランクポートに［VLAN 200］を割り当てます。

```
sw1(config)# interface port 1/0/3
sw1(config-if-port)# switchport mode trunk
sw1(config-if-port)# switchport trunk allowed vlan 100
sw1(config-if-port)# exit
sw1(config)# interface port 2/0/4
sw1(config-if-port)# switchport mode trunk
sw1(config-if-port)# switchport trunk allowed vlan 200
sw1(config-if-port)# exit
sw1(config)#
```

4. VLAN 1 の IP アドレスを［192.168.100.254/24］に、VLAN 100 の IP アドレスを［100.1.1.2/16］に、VLAN 200 の IP アドレスを［200.1.1.2/16］に設定します。

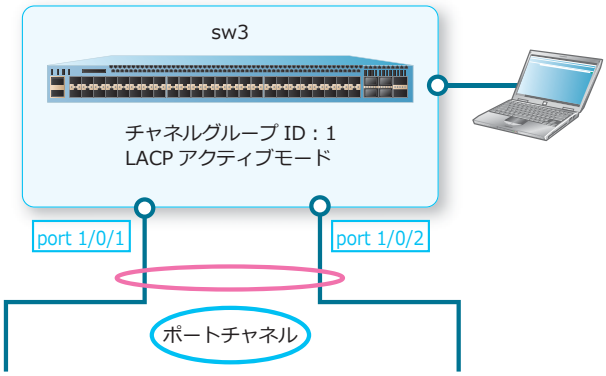
```
sw1(config)# interface vlan 1
sw1(config-if-vlan)# ip address 192.168.100.254/24
sw1(config-if-vlan)# exit
sw1(config)# interface vlan 100
sw1(config-if-vlan)# ip address 100.1.1.2/16
sw1(config-if-vlan)# exit
sw1(config)# interface vlan 200
sw1(config-if-vlan)# ip address 200.1.1.2/16
sw1(config-if-vlan)# exit
sw1(config)#
```

5. OSPF ルーター設定モードに移行し、OSPF ルーター ID を［100.1.1.2］に設定します。OSPF を有効にするネットワークを［100.1.0.0 0.0.255.255］および［200.1.0.0 0.0.255.255］に、それぞれのネットワークのエリア ID を［0］に設定します。また、直接接続された経路の再配布を設定します。

```
sw1(config)# router ospf
sw1(config-router)# router-id 100.1.1.2
sw1(config-router)# network 100.1.0.0 0.0.255.255 area 0
sw1(config-router)# network 200.1.0.0 0.0.255.255 area 0
sw1(config-router)# redistribute connected
sw1(config-router)# end
sw1#
```

4.6.3.4 sw3 のポートチャネルの設定例

図 4-32 sw3 のポートチャネルの設定例

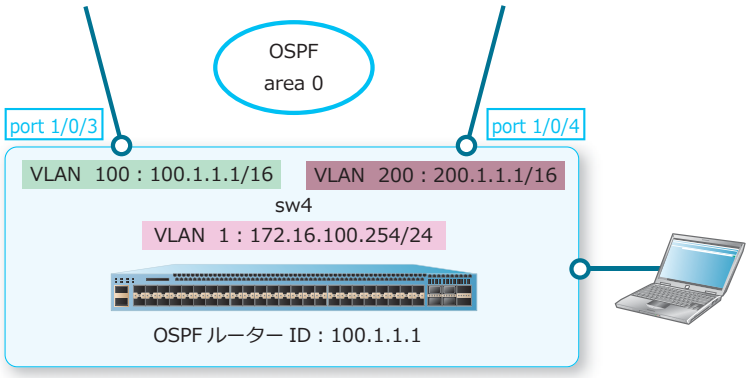


1. ポート 1/0/1 とポート 1/0/2 をチャネルグループに登録し、チャネルグループの ID を［1］に設定します。また、チャネルグループを LACP アクティブモードで動作させます。

```
sw3# configure terminal
sw3(config)# interface range port 1/0/1,1/0/2
sw3(config-if-port-range)# channel-group 1 mode active
sw3(config-if-port-range)# end
sw3#
```

4.6.3.5 sw4 の OSPF の設定例

図 4-33 sw4 の OSPF の設定例



1. VLAN 1、VLAN 100、および VLAN 200 を作成します。

```
sw4# configure terminal
sw4(config)# vlan 1
sw4(config-vlan)# exit
sw4(config)# vlan 100
sw4(config-vlan)# exit
sw4(config)# vlan 200
sw4(config-vlan)# exit
sw4(config)#
```

2. ポート 1/0/3 をトランクポートとして設定し、トランクポートに［VLAN 100］を割り当てます。また、ポート 1/0/4 をトランクポートとして設定し、トランクポートに［VLAN 200］を割り当てます。

```
sw4(config)# interface port 1/0/3
sw4(config-if-port)# switchport mode trunk
sw4(config-if-port)# switchport trunk allowed vlan 100
sw4(config-if-port)# exit
sw4(config)# interface port 1/0/4
sw4(config-if-port)# switchport mode trunk
sw4(config-if-port)# switchport trunk allowed vlan 200
sw4(config-if-port)# exit
sw4(config)#
```

3. VLAN 1 の IP アドレスを［172.16.100.254/24］に、VLAN 100 の IP アドレスを［100.1.1.1/16］に、VLAN 200 の IP アドレスを［200.1.1.1/16］に設定します。

```
sw4(config)# interface vlan 1
sw4(config-if-vlan)# ip address 172.16.100.254/24
sw4(config-if-vlan)# exit
sw4(config)# interface vlan 100
sw4(config-if-vlan)# ip address 100.1.1.1/16
sw4(config-if-vlan)# exit
sw4(config)# interface vlan 200
sw4(config-if-vlan)# ip address 200.1.1.1/16
sw4(config-if-vlan)# exit
sw4(config)#
```

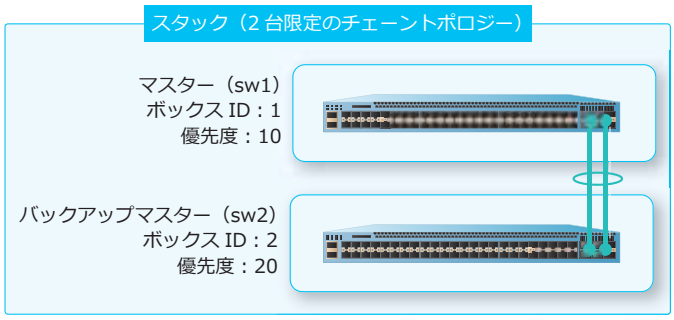
4. OSPF ルーター設定モードに移行し、OSPF ルーター ID を［100.1.1.1］に設定します。OSPF を有効にするネットワークを［100.1.0.0 0.0.255.255］および［200.1.0.0 0.0.255.255］に、それぞれのネットワークのエリア ID を［0］に設定します。また、直接接続された経路の再配布を設定します。

```
sw4 configure terminal
sw4(config)# router ospf
sw4(config-router)# router-id 100.1.1.1
sw4(config-router)# network 100.1.0.0 0.0.255.255 area 0
sw4(config-router)# network 200.1.0.0 0.0.255.255 area 0
sw4(config-router)# redistribute connected
sw4(config-router)# end
sw4#
```

4.6.4　2 台限定のチェーントポロジー

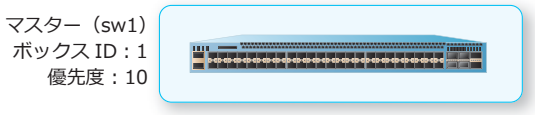
stack bandwidth コマンドの chain オプションを使用して、2 台限定のチェーントポロジーでスタックを構成します。各装置でスタック設定を実施した後は、想定した装置がマスターになるように、すべてのメンバー装置を電源 OFF した状態でスタックポートを接続し、同時に起動してスタックを構成します。

図 4-34 スタックの構成例（2 台限定のチェーントポロジー）



4.6.4.1　マスターの設定例（sw1）

図 4-35 マスターの設定例（sw1）



1. chain オプションを使用してスタック機能を有効にします。

```
sw1# stack bandwidth 40G 2-port chain

 WARNING: The command does not take effect until the next reboot.
sw1#
```

2. ボックス ID を［1］に設定します。

```
sw1# stack my_box_id 1

 WARNING: The command does not take effect until the next reboot.
sw1#
```

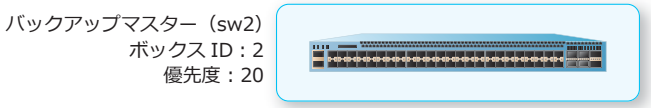
3. 優先度を［10］に設定して保存します。スタックは装置を起動し直した後に有効になります。

```
sw1# stack my_box_priority 10
sw1# write memory

Destination filename startup-config? [y/n]:  y

Saving all configurations to NV-RAM.......... Done.

sw1#
```

4. すべてのメンバー装置でスタック設定が完了したら、すべてのメンバー装置を電源 OFF した状態でスタックポートを接続し、同時に起動してスタックを構成します。

4.6.4.2 バックアップマスターの設定例（sw2）

図 4-36 バックアップマスターの設定例（sw2）



1. chain オプションを使用してスタック機能を有効にします。

```
sw2# stack bandwidth 40G 2-port chain

 WARNING: The command does not take effect until the next reboot.
sw2#
```

2. ボックス ID を［2］に設定します。

```
sw2# stack my_box_id 2

 WARNING: The command does not take effect until the next reboot.
sw2#
```

3. 優先度を［20］に設定して保存します。スタックは装置を起動し直した後に有効になります。

```
sw2# stack my_box_priority 20
sw2# write memory

Destination filename startup-config? [y/n]:  y

Saving all configurations to NV-RAM.......... Done.

sw2#
```

4. すべてのメンバー装置でスタック設定が完了したら、すべてのメンバー装置を電源 OFF した状態でスタックポートを接続し、同時に起動してスタックを構成します。

5. SNMP

SNMP の機能、状態の確認方法、および構成例と設定例について説明します。

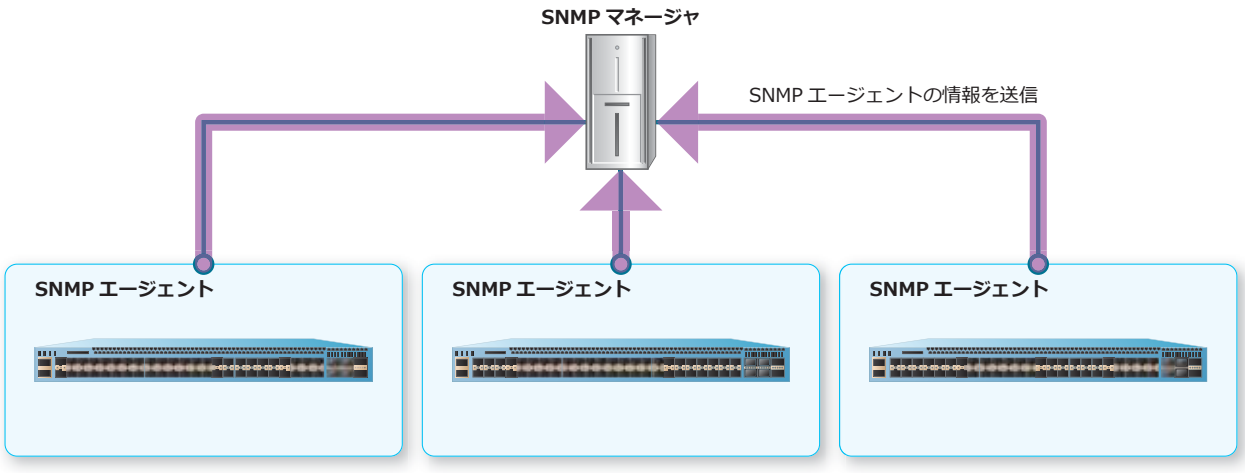
REF: コマンドの詳細については、『コマンドリファレンス』を参照してください。

5.1 SNMP の機能説明

SNMP（Simple Network Management Protocol）は、ネットワークデバイスを管理するためのプロトコルです。トランスポート層のプロトコルには、UDP（ポート番号 161 および 162）を使用します。

SNMP では、ネットワークデバイスを管理するための装置を **SNMP マネージャ**と呼び、管理されるネットワークデバイスを **SNMP エージェント**と呼びます。

図 5-1 SNMP マネージャ／ SNMP エージェント



5.1.1 SNMP エージェント

SNMP エージェントを有効に設定すると、以下の 2 種類の方式を使用して、ネットワークデバイスの情報を送受信できます。

- SNMP GetRequest/SNMP GetResponse
- SNMP トラップ

SNMP エージェントを有効に設定するには、**`snmp-server`** コマンドを使用します。

> ***NOTE:*** NP7000 の 1.08.01 以降、NP5000 の 1.08.01 以降、NP4000 の 1.03.01 以降、NP2100 の 1.09.02 以降、NP2000 の 1.09.01 以降、NP2500 の 1.08.02 以降では、デフォルトで設定されている Read/Write 権限の SNMP コミュニティー名「private」が存在する状態で **`snmp-server`** コマンドを設定すると、SNMP コミュニティー名の変更を促す警告メッセージが表示されます。

SNMP エージェントのグローバル設定

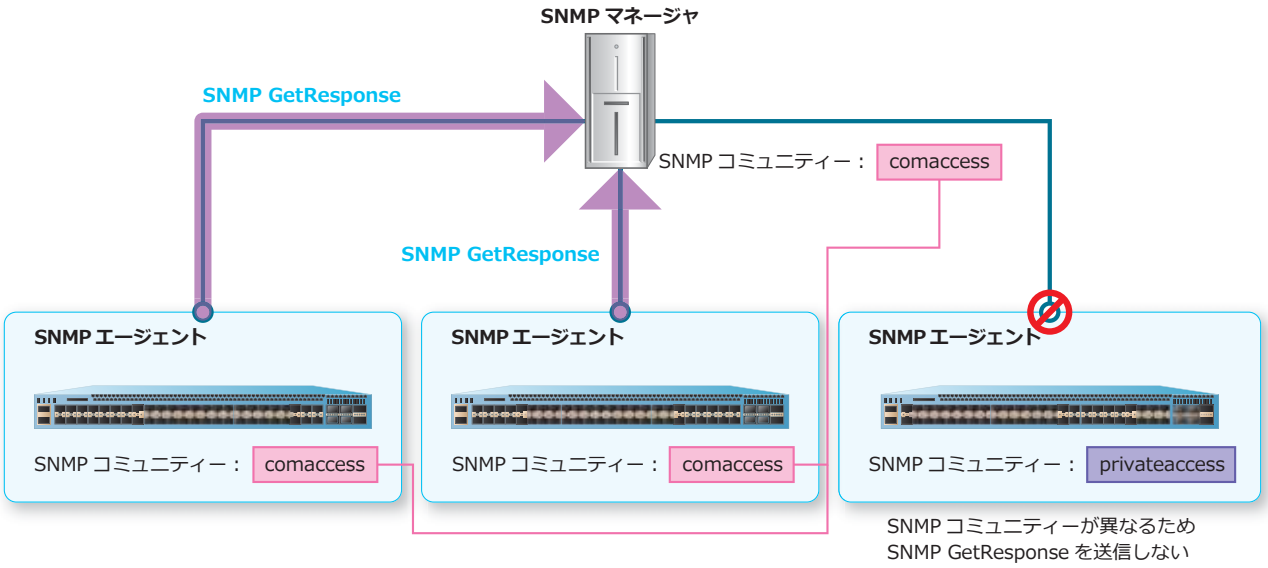
SNMP エージェントに設定できる基本的な情報は以下のとおりです。（）内は使用するコマンドです。

- 装置名（**snmp-server name** コマンド）
- 設置場所情報（**snmp-server location** コマンド）
- 障害発生時の連絡先情報（**snmp-server contact** コマンド）
- UDP ポート番号（**snmp-server service-port** コマンド）
- ブロードキャストアドレス宛ての SNMP GetRequest に対する応答設定（**snmp-server response broadcast-request** コマンド）
- SNMP コミュニティー（**snmp-server community** コマンド）
- SNMP ユーザー（**snmp-server user** コマンド）
- SNMP グループ（**snmp-server group** コマンド）

SNMP コミュニティー

SNMP コミュニティーは、SNMP マネージャが情報を読み書きできる SNMP エージェントの集合を表します。同一の SNMP コミュニティーに所属する SNMP エージェントの情報は、SNMP マネージャから読み書きできるため、SNMPv1 および SNMPv2c では、認証情報として使用されます。

図 5-2 SNMP コミュニティー



SNMP コミュニティーは、**snmp-server community** コマンドで作成します。

> ***CAUTION:*** **snmp-server community** コマンドで SNMP コミュニティーを作成すると、SNMP コミュニティー名を SNMP グループ名とする 2 つの SNMP グループが自動的に作成されます。これらの設定は変更または削除しないでください。

アクセスを許可する SNMP マネージャーを制限する場合は、**snmp-server community** コマンドの access パラメーターを使用します。access パラメーターには、標準 IP アクセスリストまたは標準 IPv6 アクセスリストを指定します。アクセスリストの permit ルールで指定した IP アドレスが許可され、deny ルールで指定した IP アドレスが拒否されます。なお、指定したアクセスリストのどのルールにもマッチしない場合はアクセスが拒否されます。

> ***CAUTION:*** **snmp-server community** コマンドの access パラメーターで指定する標準 IP アクセスリスト、または標準 IPv6 アクセスリストでは、装置のハードウェアリソースを使用しません。

SNMP ユーザー／ SNMP グループ

SNMP エージェントの MIB へアクセスする際に、SNMP ユーザー名を指定するように設定することで、セキュリティーを確保できます。また、SNMP グループを設定すると、SNMP ユーザーごとに SNMP エージェントの MIB（OID ツリー）へのアクセス権を設定できます。

SNMP ユーザーは、SNMPv3 で SNMP エージェントの MIB へアクセスするための認証情報です。SNMP エージェントとして動作させる装置に、以下の情報を設定します。

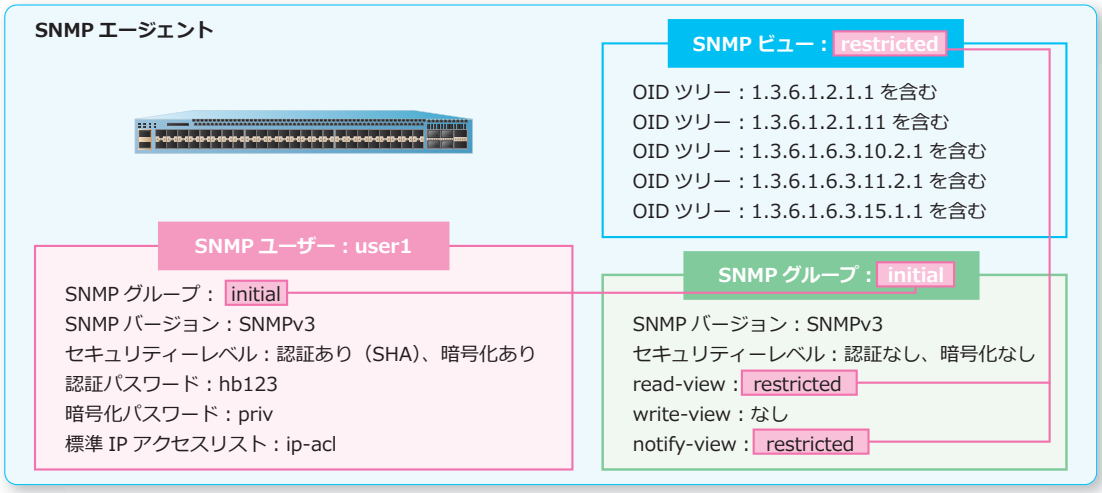
- ユーザー名
- グループ名
- SNMP バージョン
- セキュリティーレベル
- 認証パスワード
- SNMP トラップの暗号化パスワード
- 標準 IP アクセスリスト

SNMP グループでは、SNMP ユーザーに関連付ける SNMP ビューを設定します。

SNMP のバージョンごとに、SNMP ビュー（読み取り用ビュー、書き込み用ビュー、および通知用ビュー）を設定できます。SNMPv3 の場合は、認証および暗号化の要否を設定できます。

たとえば、SNMP エージェントに、SNMP ユーザー：user1 でアクセスしたときに限り、SNMP ビュー：restricted に設定した OID ツリーの読み取りと、通知を許可する場合は、以下のように設定します。

図 5-3 SNMP ユーザー／ SNMP グループ



SNMP ユーザーは、**`snmp-server user`** コマンドで作成します。SNMP グループは、**`snmp-server group`** コマンドで設定します。

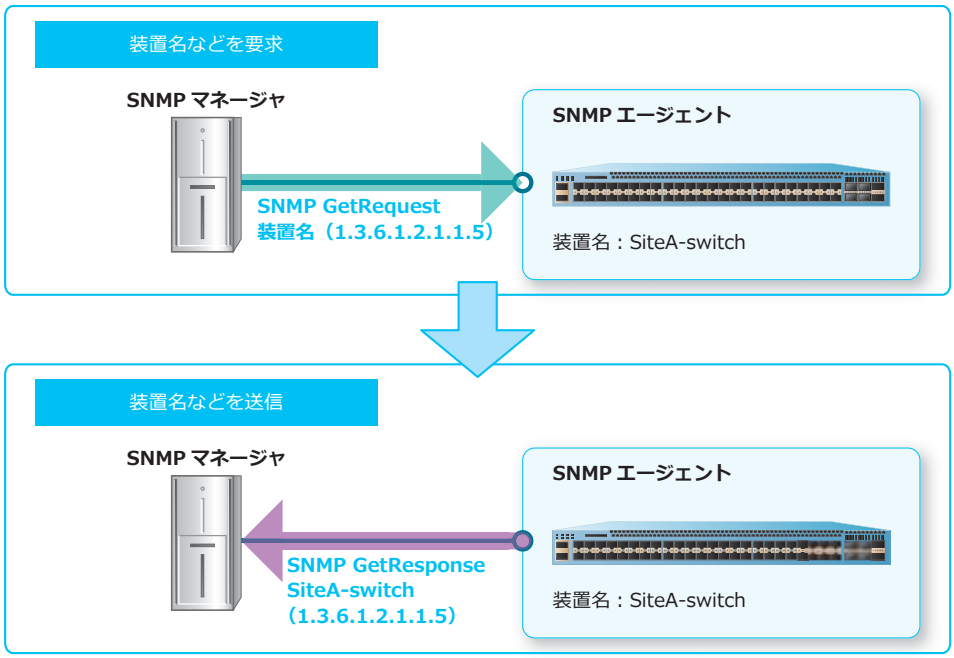
アクセスを許可する SNMP マネージャーを制限する場合は、**`snmp-server user`** コマンドの access パラメーターを使用します。access パラメーターには、標準 IP アクセスリストまたは標準 IPv6 アクセスリストを指定します。アクセスリストの permit ルールで指定した IP アドレスが許可され、deny ルールで指定した IP アドレスが拒否されます。なお、指定したアクセスリストのどのルールにもマッチしない場合はアクセスが拒否されます。

> ***CAUTION:*** **`snmp-server user`** コマンドの access パラメーターで指定する標準 IP アクセスリスト、または標準 IPv6 アクセスリストでは、装置のハードウェアリソースを使用しません。

5.1.2 SNMP GetRequest/SNMP GetResponse

SNMP マネージャから SNMP エージェントに情報を要求する際は、**SNMP GetRequest** を送信し、SNMP エージェントから情報を返送する際は、**SNMP GetResponse** を送信します。

図 5-4 SNMP GetRequest/SNMP GetResponse の概要



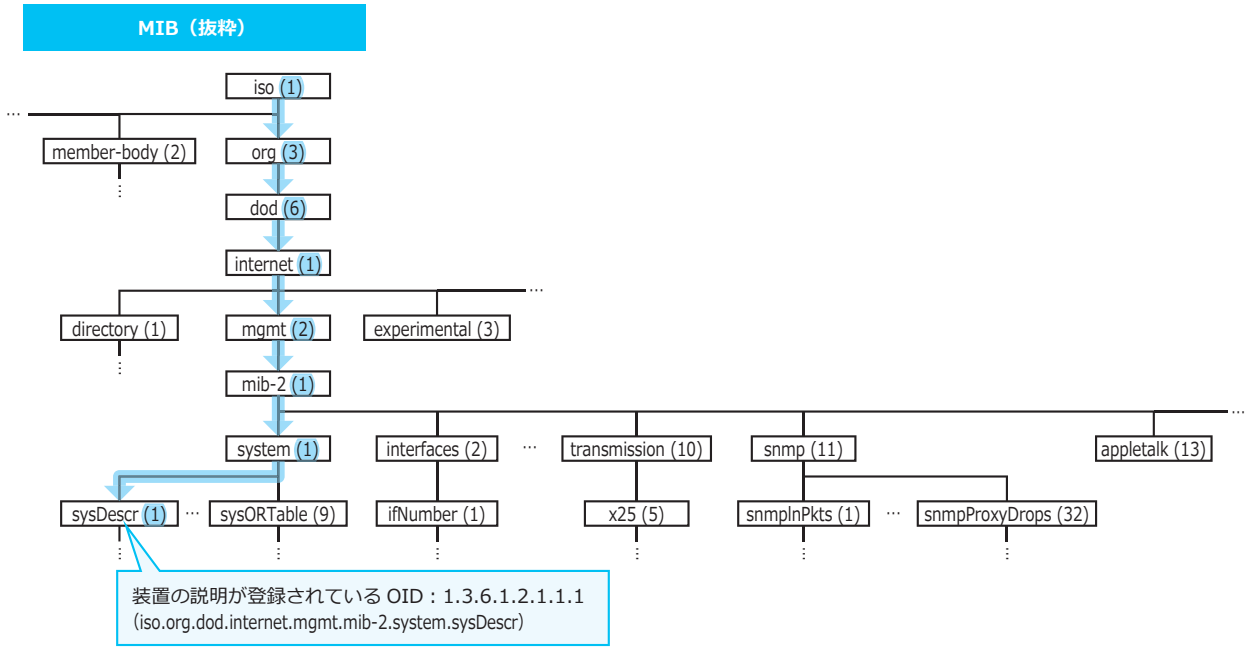
SNMP マネージャが要求できる情報は、SNMP エージェントの **MIB（Management Information Base）**に格納されている情報のうち、**SNMP ビュー**でアクセスできるように設定されている情報です。

MIB（Management Information Base）

MIB は、SNMP エージェントの情報が蓄積されるツリー構造のデータベースです。MIB 内の情報の種類は、**OID（Object ID）**を使用して特定します。OID は、下図のようにツリーの頂上からたどって、目的の情報までの経路を表したものです。たとえば、装置の説明が登録されているオブジェクト（sysDescr）の OID は「1.3.6.1.2.1.1.1」または「iso.org.dod.internet.mgmt.mib-2.system.sysDescr」と表します。

SNMP マネージャから SNMP エージェントの情報を取得する際は、OID を指定して SNMP GetRequest を送信します。

図 5-5 MIB の概要



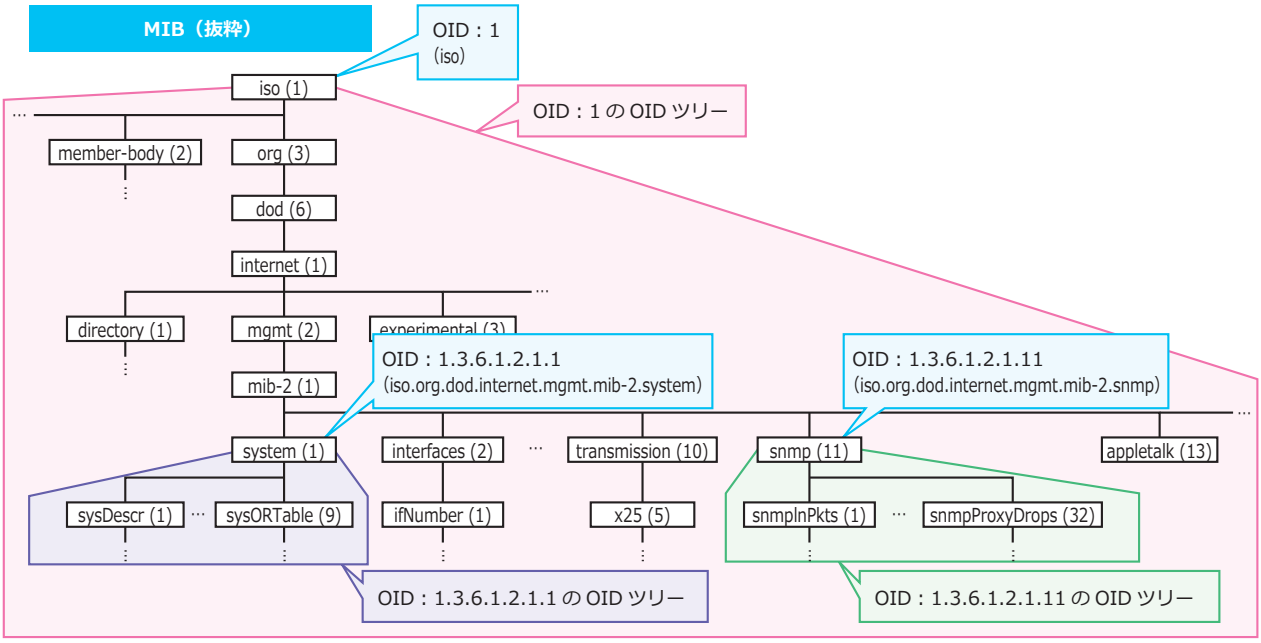
REF: MIB の詳細については、『MIB 項目の実装仕様』を参照してください。

SNMP ビュー

SNMP ビューは、SNMP マネージャがアクセスできる **OID ツリー**を制限するために作成します。OID ツリーは、指定した OID を頂点とし、それ以下のオブジェクトをすべて含むツリーを指します。

たとえば、「OID：1.3.6.1.2.1.1 の OID ツリー」には、OID：1.3.6.1.2.1.1.1、OID：1.3.6.1.2.1.1.9、および OID：1.3.6.1.2.1.1.9.1 などが含まれます。

図 5-6 OID ツリー



初期設定では、以下の SNMP ビューが設定されています。

- **restricted ビュー**

  以下の OID ツリーにアクセスできます。

  - 1.3.6.1.2.1.1（System グループ）を含む
  - 1.3.6.1.2.1.11（SNMP グループ）を含む
  - 1.3.6.1.6.3.10.2.1（SNMP Engine グループ）を含む
  - 1.3.6.1.6.3.11.2.1（SNMP MPD MIB グループ）を含む
  - 1.3.6.1.6.3.15.1.1（SNMP USER BASED SM MIB グループ）を含む

- **CommunityView ビュー**

  以下のすべての OID ツリーにアクセスできます。

  - 1（すべての OID）を含む
  - 1.3.6.1.6.3（SNMP モジュール）を除く
  - 1.3.6.1.6.3.1（SNMP MIB モジュール）を含む

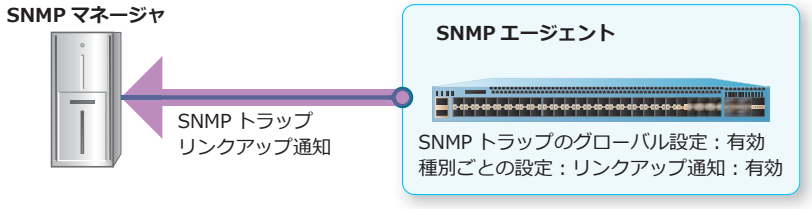
  NOTE: 1.3.6.1.6.3（SNMP モジュール）には、1.3.6.1.6.3.1（SNMP MIB モジュール）以外に、1.3.6.1.6.3.10 から 1.3.6.1.6.3.20 が含まれています。したがって、初期設定の CommunityView ビューでは、1.3.6.1.6.3.10 から 1.3.6.1.6.3.20 にはアクセスできません。

SNMP ビューは、**`snmp-server view`** コマンドで作成します。

5.1.3 SNMP トラップ

SNMP GetRequest/SNMP GetResponse とは異なり、SNMP エージェントに問題が発生した場合など、SNMP マネージャから要求されていないときに、SNMP エージェントから SNMP マネージャに向けてデバイスの状態変更などを通知する際は、**SNMP トラップ**を送信します。

図 5-7 SNMP トラップの概要



REF: SNMP トラップの詳細については、『MIB 項目の実装仕様』を参照してください。

SNMP トラップのグローバル設定の有効／無効

SNMP トラップを使用するには、SNMP トラップのグローバル設定を有効に設定します。SNMP トラップのグローバル設定は **`snmp-server enable traps`** コマンドで設定します。なお、SNMP トラップの種別ごとの有効／無効設定がある場合は、そちらも有効に設定する必要があります。

> ***NOTE:*** SNMP トラップのグローバル設定を無効に設定している場合は、種別ごとの有効／無効設定が有効に設定されていても、SNMP トラップは送信されません。

SNMP トラップの種別ごとの有効／無効設定

いくつかの SNMP トラップでは、種別ごとに SNMP トラップの有効／無効を設定できます。対応する有効／無効設定がない場合は、SNMP トラップのグローバル設定を有効にすると SNMP トラップも有効になります。

> ***NOTE:*** 種別ごとの SNMP トラップの有効／無効コマンドの有無は、機種やバージョンによって異なります。詳細については、本項末尾の「種別ごとの SNMP トラップの有効／無効コマンド対応一覧表」、または各機種の『コマンドリファレンス』を参照してください。

SNMP トラップの種別ごとの有効／無効設定を以下に示します。

- **リンクアップ通知**

  インターフェースがリンクアップしたことを通知する SNMP トラップの有効／無効は、**`snmp-server enable traps snmp linkup`** コマンドで設定します。

- **リンクダウン通知**

  インターフェースがリンクダウンしたことを通知する SNMP トラップの有効／無効は、**`snmp-server enable traps snmp linkdown`** コマンドで設定します。

  > ***NOTE:*** リンクアップ通知／リンクダウン通知は、**`snmp trap link-status`** コマンドを使用して、ポートごとに有効／無効を設定できます。

- **SNMP 認証失敗通知**

  SNMP 認証が失敗したことを通知する SNMP トラップの有効／無効は、**`snmp-server enable traps snmp authentication`** コマンドで設定します。

- **コールドスタート通知**

  装置が電源供給の停止状態から起動したことを通知する SNMP トラップの有効／無効は、**`snmp-server enable traps snmp coldstart`** コマンドで設定します。

- **ウォームスタート通知**

  装置が電源供給の停止を伴わずに再起動したことを通知する SNMP トラップの有効／無効は、**`snmp-server enable traps snmp warmstart`** コマンドで設定します。

• RMON 機能の通知

RMON 機能の上昇しきい値イベント、下降しきい値イベントが発生したことを通知する SNMP トラップの有効／無効は、**snmp-server enable traps rmon rising-alarm / falling-alarm** コマンドで設定します。

• LLDP 機能の通知

LLDP で収集した他機器の情報が変化したことを通知する SNMP トラップの有効／無効は、**snmp-server enable traps lldp** コマンドで設定します。**lldp notification enable** コマンドを使用して、インターフェースごとに有効／無効を設定できます。

• LLDP-MED 機能の通知

LLDP-MED 対応機器がインターフェースに接続されたこと、および接続が解除されたことを通知する SNMP トラップの有効／無効は、**snmp-server enable traps lldp med** コマンドで設定します。**lldp med notification enable** コマンドを使用して、インターフェースごとに有効／無効を設定できます。

• スパニングツリープロトコル機能の通知

スパニングツリープロトコル機能で、新たにルートブリッジが選出されたことを通知する SNMP トラップの有効／無効は、**snmp-server enable traps stp new-root** コマンドで設定します。トポロジーが変更されたことを通知する SNMP トラップの有効／無効は、**snmp-server enable traps stp topology-chg** コマンドで設定します。

• VRRPv2 機能の通知

VRRPv2 機能で、認証が失敗したことを通知する SNMP トラップの有効／無効は、**snmp-server enable traps vrrp auth-fail** コマンドで設定します。マスターが変更されたことを通知する SNMP トラップの有効／無効は、**snmp-server enable traps vrrp new-master** コマンドで設定します。

• 環境モニタリング通知（装置のファン、電源、温度）

装置のファン、電源、温度関連の SNMP トラップの有効／無効は、**snmp-server enable traps environment fan / power / temperature** コマンドで設定します。

• システムメモリー使用率監視機能の通知

システムメモリー使用率監視機能の SNMP トラップの有効／無効は、**snmp-server enable traps environment memory** コマンドで設定します。

• 装置のシステム状態関連の通知

装置のシステム状態関連の SNMP トラップの有効／無効は、**snmp-server enable traps environment health-status** コマンドで設定します。

• スタック機能の通知

スタック機能の SNMP トラップの有効／無効は、**snmp-server enable traps stack** コマンドで設定します。

• CPU 使用率監視機能の通知

CPU 使用率監視機能の SNMP トラップの有効／無効は、**snmp-server enable traps cpu-protect** コマンドで設定します。

• 光トランシーバー関連の通知

光トランシーバー関連の SNMP トラップの有効／無効は、**snmp-server enable traps sfp** コマンドで設定します。

• PoE 機能の通知

PoE 機能の SNMP トラップの有効／無効は、**snmp-server enable traps poe** コマンドで設定します。

• ストームコントロール機能の通知

ストームコントロール機能の SNMP トラップの有効／無効は、**snmp-server enable traps storm-control** コマンドで設定します。

- **メモリーエラー自動復旧機能の通知**

  メモリーエラー自動復旧機能に関連する通知（ログ、SNMP トラップ）の有効／無効は、**memory-error auto-recovery notify disable** コマンドで設定します。

- **CFM 機能の通知**

  CFM 機能の SNMP トラップの有効／無効は、**snmp-server enable traps cfm** コマンドで設定します。

- **ループ検知機能の通知**

  ループ検知機能の SNMP トラップの有効／無効は、**snmp-server enable traps loop-detection** コマンドで設定します。

- **MMRP-Plus 機能の通知**

  MMRP-Plus 機能の SNMP トラップの有効／無効は、**snmp-server enable traps mmrp-plus** コマンドで設定します。

SNMP トラップの種別ごとの有効／無効コマンドのサポート状況を以下に示します。○はリリース当初から有効／無効コマンドをサポートしていることを示します。数値は、途中から有効／無効コマンドをサポートした場合のバージョン情報を示します。- は有効／無効コマンドが未対応なことを、N/A は対象機能がないことを示します。

> ***REF:*** SNMP トラップをサポートしたバージョンと、SNMP トラップの有効／無効コマンドをサポートしたバージョンは異なることがあります。SNMP トラップをサポートしたバージョンの詳細については、『MIB 項目の実装仕様』を参照してください。

表 5-1 種別ごとの SNMP トラップの有効／無効コマンド対応一覧表

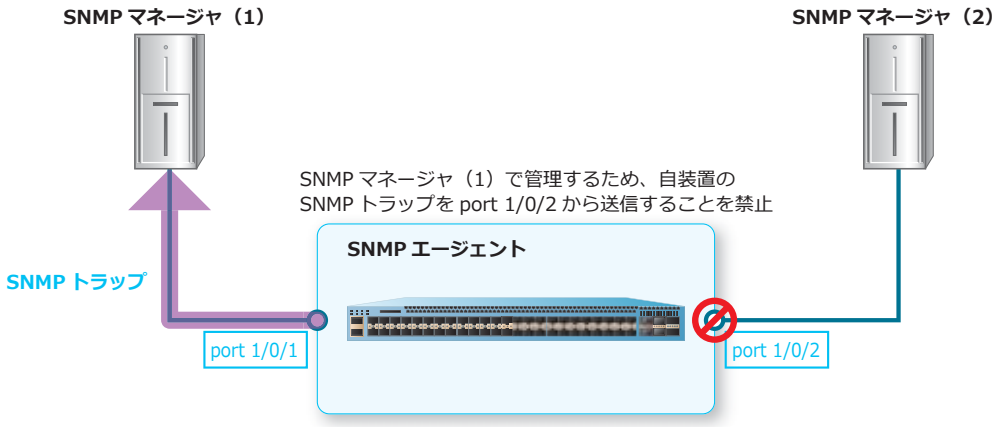
種別	NP7000	NP5000	NP4000	NP3000	NP2100	NP2000	NP2500
リンクアップ通知	○	○	○	○	○	○	○
リンクダウン通知	○	○	○	○	○	○	○
SNMP 認証失敗通知	○	○	○	○	○	○	○
コールドスタート通知	○	○	○	○	○	○	○
ウォームスタート通知	○	○	○	○	○	○	○
RMON 機能の通知	○	○	○	○	○	○	○
LLDP 機能の通知	○	○	○	○	○	○	○
LLDP-MED 機能の通知	○	○	○	○	○	○	○
スパニングツリープロトコル機能の通知	○	○	○	○	○	○	○
VRRPv2 機能の通知	○	○	N/A	○	N/A	N/A	N/A
環境モニタリング通知（装置のファン、電源、温度）	1.03.01	1.03.01	○	○	○	1.03.01	○
システムメモリー使用率監視機能の通知	1.08.01	1.08.01	1.03.01	-	○	1.09.01	-
装置のシステム状態関連の通知	1.09.01	1.09.01	-	1.09.01	1.11.01	-	-
スタック機能の通知	1.03.01	1.03.01	○	○	○	1.03.01	○

種別	NP7000	NP5000	NP4000	NP3000	NP2100	NP2000	NP2500
CPU 使用率監視機能の通知	1.06.01	1.06.01	1.03.01	○	○	1.08.01	○
光トランシーバー関連の通知	1.08.01	1.08.01	1.03.01	-	○	1.09.01	-
PoE 機能の通知	N/A	N/A	N/A	N/A	○	1.05.01	○
ストームコントロール機能の通知	1.08.01	1.08.01	1.03.01	-	○	1.09.01	1.13.01
メモリーエラー自動復旧機能の通知	1.03.01	1.03.01	○	○	○	○	○
CFM 機能の通知	1.09.01	1.09.01	-	1.09.01	1.11.01	-	-
ループ検知機能の通知	1.09.01	1.09.01	-	1.09.01	1.11.01	-	1.13.01
MMRP-Plus 機能の通知	1.09.01	1.09.01	-	1.09.01	1.11.01	-	-

SNMP トラップの送信を禁止するポートの設定

SNMP トラップの送信を禁止するポートを設定できます。送信を禁止したポートからは、自装置の SNMP トラップは送信されません。SNMP トラップの送信を禁止するポートを設定するには、**`snmp-server trap-sending disable`** コマンドを使用します。

図 5-8 SNMP トラップの送信を禁止するポートの設定



SNMP トラップの宛先設定

SNMP トラップの宛先（SNMP マネージャ）の IP アドレスまたは IPv6 アドレス、SNMP トラップの送信に使用する SNMP のバージョン、認証の有無、暗号化の有無、SNMP コミュニティー名、および UDP ポート番号を設定できます。SNMP トラップの宛先は、**`snmp-server host`** コマンドで設定します。

SNMP トラップの送信元 IP アドレス設定

SNMP トラップを送信する IP アドレスを設定できます。SNMP トラップの送信元 IP アドレスは、**`snmp-server source-interface traps`** コマンドで設定します。

5.1.4 SNMPv3 設定

SNMPv3 を利用する場合は、**SNMP エンジン ID** を設定します。SNMP エンジン ID は、SNMP エージェントを識別する 16 進数です。SNMP エージェントのプログラムが異なる場合は、異なる値を設定してください。SNMP エンジン ID は、**`snmp-server engineID local`** コマンドで設定します。

5.1.5 SNMP コンテキストマッピングテーブル

OSPFv3 MIB を取得する場合に、SNMP コンテキストマッピングテーブルを設定します。SNMP コンテキストマッピングテーブルを設定するには、**`snmp-server context-map`** コマンドを使用します。

> ***CAUTION:*** NP4000、NP2100、NP2000、および NP2500 では、SNMP コンテキストマッピングテーブルを使用できません。

5.2 SNMP の状態確認

SNMP の状態を表示して確認する方法を説明します。

5.2.1 SNMP エージェントの表示

show snmp-server コマンドで、SNMP エージェントの設定を確認できます。

表示例を以下に示します。

```
# show snmp-server

SNMP Server  : Enabled ...(1)
Name         : SiteA-Switch ...(2)
Location     : HQ 15F ...(3)
Contact      : MIS Department II ...(4)
SNMP UDP Port    : 161 ...(5)
SNMP Response Broadcast Request    : Disabled ...(6)
```

各項目の説明は、以下のとおりです。

表 5-2 show snmp-server コマンドの表示項目

項番	説明
(1)	SNMP エージェントが有効 (Enabled) なことを示します。
(2)	システム名（sysName）を表示します。
(3)	システムロケーション（sysLocation）を表示します。
(4)	システムコンタクト（sysContact）を表示します。
(5)	SNMP で使用する UDP ポート番号を表示します。
(6)	ブロードキャストアドレス宛ての SNMP GetRequest に対する応答設定の有効 (Enabled) ／無効 (Disabled) を表示します。

5.2.2 SNMP コミュニティー名の表示

show snmp community コマンドで、SNMP コミュニティー名の設定を確認できます。

表示例を以下に示します。

```
# show snmp community

Community : public ...(1)
 Access : read-only ...(2)
 View : CommunityView ...(3)
 IP access control list : test-IPv4-ACL ...(4)

Community : private
 Access : read-write
 View : CommunityView

Total Entries: 2
```

各項目の説明は、以下のとおりです。

表 5-3 show snmp community コマンドの表示項目

項番	説明
(1)	SNMP コミュニティー名を表示します。
(2)	MIB へのアクセス権を表示します。
(3)	SNMP ビュー名を表示します。
(4)	SNMP コミュニティー名と関連付ける標準 IP アクセスリスト、または標準 IPv6 アクセスリストを表示します。未設定の場合は表示されません。

5.2.3 SNMP トラップ設定の表示

SNMP トラップ関連の設定を確認する方法を説明します。

5.2.3.1 SNMP トラップの宛先ホストの表示

show snmp host コマンドで、SNMP トラップの宛先ホスト設定を確認できます。

表示例を以下に示します。

```
# show snmp host

Host IP Address  : 192.0.2.100 ...(1)
SNMP Version     : V2c ...(2)
Community Name   : test-public ...(3)
UDP Port         : 162 ...(4)

Host IPv6 Address: 2001:db8::100 ...(1)
SNMP Version     : V3 noauthnopriv
SNMPv3 User Name : test-user ...(5)
UDP Port         : 162

Total Entries: 2
```

各項目の説明は、以下のとおりです。

表 5-4 show snmp host コマンドの表示項目

項番	説明
(1)	SNMP トラップの宛先 IP アドレスを表示します。
(2)	SNMP トラップのバージョンを表示します。 • V1：SNMPv1 • V2c：SNMPv2c • V3 noauthnopriv：SNMPv3（認証なし、暗号化なし） • V3 authnopriv：SNMPv3（認証あり、暗号化なし） • V3 authpriv：SNMPv3（認証あり、暗号化あり）
(3)	SNMP トラップで通知する SNMP コミュニティー名を表示します。
(4)	UDP ポート番号を表示します。
(5)	SNMP トラップで通知する SNMP ユーザー名を表示します。

5.2.3.2 SNMP トラップの有効／無効の表示

show snmp-server traps コマンドで、SNMP トラップの有効／無効を確認できます。

REF: **show snmp-server traps** コマンドの表示は機種やバージョンによって異なるため、詳細については、『コマンドリファレンス』を参照してください。

NOTE: **show snmp-server traps** コマンドで表示されない有効／無効設定は、構成情報を直接確認してください。

NP5000 の 1.09.01 で、SNMP トラップの有効／無効を確認する場合の表示例を以下に示します。

```
# show snmp-server traps

Global Trap State : Enabled ...(1)
Individual Trap State:
  STACK
    Stack                     : Disabled ...(2)
  Environment
    Fan                       : Disabled ...(3)
    Power                     : Disabled ...(4)
    Temperature               : Disabled ...(5)
    Memory                    : Enabled ...(6)
    Health-status             : Enabled ...(7)
  SYSTEM
    CPU-Protect               : Disabled ...(8)
  MEAR
    Memory-error              : Enabled ...(9)
  STORM
    Storm-control             : Disabled ...(10)
  PORT
    SFP                       : Disabled ...(11)
    Link-Flap-Prevention      : Enabled ...(12)
  STP
    New-root                  : Disabled ...(13)
    Topology-change           : Disabled ...(14)
  LOOP-DETECT
    Loop-detection            : Enabled ...(15)
  SNMP
    Authentication            : Disabled ...(16)
    Linkup                    : Disabled ...(17)
    Linkdown                  : Disabled ...(18)
    Coldstart                 : Disabled ...(19)
    Warmstart                 : Disabled ...(20)
  CFM
    CFM                       : Enabled ...(21)
  LLDP
    LLDP                      : Disabled ...(22)
    LLDP-MED                  : Disabled ...(23)
  RMON
    Rising-alarm              : Disabled ...(24)
    Falling-alarm             : Disabled ...(25)
  BGP
    Established               : Disabled ...(26)
    Backward-trans            : Disabled ...(27)
  VRRP
    Auth-fail                 : Disabled ...(28)
    New-master                : Disabled ...(29)
  MMRP
    MMRP-Plus                 : Enabled ...(30)
```

各項目の説明は、以下のとおりです。

表 5-5 `show snmp-server traps` コマンドの表示項目

項番	説明
(1)	SNMP トラップのグローバル設定の有効 (Enabled) ／無効 (Disabled) を表示します。
(2)	スタック機能の SNMP トラップの有効 (Enabled) ／無効 (Disabled) を表示します。
(3)	ファン関連の SNMP トラップの有効 (Enabled) ／無効 (Disabled) を表示します。
(4)	電源関連の SNMP トラップの有効 (Enabled) ／無効 (Disabled) を表示します。
(5)	温度関連の SNMP トラップの有効 (Enabled) ／無効 (Disabled) を表示します。
(6)	システムメモリー使用率監視機能の SNMP トラップの有効 (Enabled) ／無効 (Disabled) を表示します。
(7)	装置のシステム状態関連の SNMP トラップの有効 (Enabled) ／無効 (Disabled) を表示します。
(8)	CPU 使用率監視機能の SNMP トラップの有効 (Enabled) ／無効 (Disabled) を表示します。
(9)	メモリーエラー自動復旧機能に関連する通知（ログ、SNMP トラップ）の有効 (Enabled) ／無効 (Disabled) を表示します。設定コマンドは、**`memory-error auto-recovery notify disable`** コマンドです。
(10)	ストームコントロール機能の SNMP トラップの有効 (Enabled) ／無効 (Disabled) を表示します。
(11)	光トランシーバー関連の SNMP トラップの有効 (Enabled) ／無効 (Disabled) を表示します。
(12)	リンクフラップ防止機能の SNMP トラップの有効 (Enabled) ／無効 (Disabled) を表示します。
(13)	スパニングツリープロトコル機能の、新ルートブリッジ SNMP トラップの有効 (Enabled) ／無効 (Disabled) を表示します。
(14)	スパニングツリープロトコル機能の、トポロジー変更 SNMP トラップの有効 (Enabled) ／無効 (Disabled) を表示します。
(15)	ループ検知機能の SNMP トラップの有効 (Enabled) ／無効 (Disabled) を表示します。
(16)	SNMP 認証失敗 SNMP トラップの有効 (Enabled) ／無効 (Disabled) を表示します。
(17)	リンクアップ SNMP トラップのグローバル設定の有効 (Enabled) ／無効 (Disabled) を表示します。
(18)	リンクダウン SNMP トラップのグローバル設定の有効 (Enabled) ／無効 (Disabled) を表示します。
(19)	コールドスタート SNMP トラップの有効 (Enabled) ／無効 (Disabled) を表示します。
(20)	ウォームスタート SNMP トラップの有効 (Enabled) ／無効 (Disabled) を表示します。
(21)	CFM 機能の SNMP トラップの有効 (Enabled) ／無効 (Disabled) を表示します。
(22)	LLDP 機能の SNMP トラップの有効 (Enabled) ／無効 (Disabled) を表示します。
(23)	LLDP-MED 機能の SNMP トラップの有効 (Enabled) ／無効 (Disabled) を表示します。
(24)	RMON 機能の、上昇しきい値イベントが発生した際の SNMP トラップの有効 (Enabled) ／無効 (Disabled) を表示します。
(25)	RMON 機能の、下降しきい値イベントが発生した際の SNMP トラップの有効 (Enabled) ／無効 (Disabled) を表示します。

項番	説明
(26)	現状、BGP 機能は未サポートです。
(27)	現状、BGP 機能は未サポートです。
(28)	VRRPv2 機能の認証失敗トラップの有効 (Enabled) ／無効 (Disabled) を表示します。
(29)	VRRPv2 機能のマスター変更トラップの有効 (Enabled) ／無効 (Disabled) を表示します。
(30)	MMRP-Plus 機能の SNMP トラップの有効 (Enabled) ／無効 (Disabled) を表示します。

5.2.3.3 自装置の SNMP トラップの送信可能ポート／送信禁止ポートの表示

show snmp-server trap-sending コマンドで、自装置の SNMP トラップの送信可能ポート／送信禁止ポートを確認できます。

表示例を以下に示します。

```
# show snmp-server trap-sending
(1)                  (2)
Port                 Trap Sending
-------------        -------------
Port1/0/1            Enabled
Port1/0/2            Enabled
Port1/0/3            Enabled
Port1/0/4            Disabled
Port1/0/5            Enabled
Port1/0/6            Disabled
～～省略～～
```

各項目の説明は、以下のとおりです。

表 5-6 show snmp-server trap-sending コマンドの表示項目

項番	説明
(1)	ポート番号を表示します。
(2)	自装置の SNMP トラップの送信可能ポート (Enabled) ／送信禁止ポート (Disabled) を表示します。

5.2.3.4 ポートのリンクアップ・リンクダウンの SNMP トラップ設定の表示

show snmp trap link-status コマンドで、ポートのリンクアップ・リンクダウンの SNMP トラップ設定を確認できます。

表示例を以下に示します。

```
# show snmp trap link-status
(1)                  (2)
Port                 Trap state
-------------        -------------
Port1/0/1            Enabled
Port1/0/2            Enabled
Port1/0/3            Enabled
Port1/0/4            Enabled
Port1/0/5            Enabled
Port1/0/6            Enabled
～～省略～～
```

各項目の説明は、以下のとおりです。

表 5-7 `show snmp trap link-status` コマンドの表示項目

項番	説明
(1)	ポート番号を表示します。
(2)	リンクアップ・リンクダウンの SNMP トラップの有効 (Enabled) ／無効 (Disabled) を表示します。

5.2.4 SNMP ユーザーの表示

`show snmp user` コマンドで、SNMP ユーザーの設定を確認できます。

表示例を以下に示します。

```
# show snmp user

User Name: initial ...(1)
  Security Model: 3 ...(2)
  Group Name: initial ...(3)
  Authentication Protocol: None ...(4)
  Privacy Protocol: None ...(5)
  Engine ID: 8000011603004066a8cc3600 ...(6)
  IP access control list: ...(7)

Total Entries: 1
```

各項目の説明は、以下のとおりです。

表 5-8 `show snmp user` コマンドの表示項目

項番	説明
(1)	SNMP ユーザー名を表示します。
(2)	セキュリティーモデル（3：SNMPv3）を表示します。
(3)	SNMP ユーザーが所属する SNMP グループ名を表示します。
(4)	SNMP ユーザーの認証方式を表示します。 • None：なし • md5：HMAC-MD5-96 認証 • sha：HMAC-SHA-96 認証
(5)	パケットの暗号化方式（None：暗号化なし／ DES：Data Encryption Standard）を表示します。
(6)	SNMP エンジン ID を表示します。
(7)	SNMP ユーザーと関連付ける標準 IP アクセスリスト、または標準 IPv6 アクセスリストを表示します。

5.2.5 その他の SNMP 設定の表示

その他の SNMP 関連の設定を確認する方法を説明します。

5.2.5.1 SNMP グループの表示

show snmp group コマンドで、SNMP グループの設定を確認できます。

表示例を以下に示します。

```
# show snmp group

GroupName: public ...(1)
SecurityModel: v1 ...(2)
  ReadView     : CommunityView ...(3)          WriteView    : ...(4)
  NotifyView   : CommunityView ...(5)
  IP access control list: ...(6)

GroupName: public
SecurityModel: v2c
  ReadView     : CommunityView                 WriteView    :
  NotifyView   : CommunityView
  IP access control list:

GroupName: initial
SecurityModel: v3/noauth
  ReadView     : restricted                    WriteView    :
  NotifyView   : restricted
  IP access control list:

GroupName: private
SecurityModel: v1
  ReadView     : CommunityView                 WriteView    : CommunityView
  NotifyView   : CommunityView
  IP access control list:

GroupName: private
SecurityModel: v2c
  ReadView     : CommunityView                 WriteView    : CommunityView
  NotifyView   : CommunityView
  IP access control list:

Total Entries: 5
```

各項目の説明は、以下のとおりです。

表 5-9 show snmp group コマンドの表示項目

項番	説明
(1)	SNMP グループ名を表示します。
(2)	セキュリティーモデルを表示します。 • v1：SNMPv1 • v2c：SNMPv2c • v3/noauth：SNMPv3（認証なし、暗号化なし） • v3/auth：SNMPv3（認証あり、暗号化なし） • v3/priv：SNMPv3（認証あり、暗号化あり）
(3)	グループのユーザーに読み取りを許可する SNMP ビュー（read-view）を表示します。
(4)	グループのユーザーに書き込みを許可する SNMP ビュー（write-view）を表示します。

項番	説明
(5)	グループのユーザーに SNMP トラップの送信を許可する SNMP ビュー（notify-view）を表示します。
(6)	SNMP グループと関連付ける標準 IP アクセスリスト、または標準 IPv6 アクセスリストを表示します。

5.2.5.2 SNMP ビューの表示

show snmp view コマンドで、SNMP ビューの設定を確認できます。

表示例を以下に示します。

```
# show snmp view
(1)         (2)         (3)
restricted(included) 1.3.6.1.2.1.1
restricted(included) 1.3.6.1.2.1.11
restricted(included) 1.3.6.1.6.3.10.2.1
restricted(included) 1.3.6.1.6.3.11.2.1
restricted(included) 1.3.6.1.6.3.15.1.1
CommunityView(included) 1
CommunityView(excluded) 1.3.6.1.6.3
CommunityView(included) 1.3.6.1.6.3.1

Total Entries: 8
```

各項目の説明は、以下のとおりです。

表 5-10 show snmp view コマンドの表示項目

項番	説明
(1)	SNMP ビュー名を表示します。
(2)	対象の OID ツリーの条件（included：SNMP ビューに含める／ excluded：SNMP ビューから除外する）を表示します。
(3)	OID ツリーの頂点のオブジェクト識別子を表示します。

5.2.5.3 SNMP エンジン ID の表示

show snmp engineID コマンドで、SNMP エンジン ID を確認できます。

表示例を以下に示します。

```
# show snmp engineID

Local SNMP engineID: 8000011603004066704500000 ...(1)
```

各項目の説明は、以下のとおりです。

表 5-11 show snmp engineID コマンドの表示項目

項番	説明
(1)	SNMP エンジン ID を表示します。

5.2.5.4 SNMP コンテキストマッピングテーブルの表示

show snmp context-map コマンドで、SNMP コンテキストマッピングテーブルを確認できます。

> ***CAUTION:*** NP4000、NP2100、NP2000、および NP2500 では、SNMP コンテキストマッピングテーブルを使用できません。

表示例を以下に示します。

```
# show snmp context-map

SNMP Context Mapping Table:

Context Name : snmp-context ...(1)
Instance ID : 1 ...(2)
```

各項目の説明は、以下のとおりです。

表 5-12 show snmp context-map コマンドの表示項目

項番	説明
(1)	SNMP コンテキスト名を表示します。
(2)	関連付けたインスタンス ID（OSPFv3 のプロセス ID）を表示します。

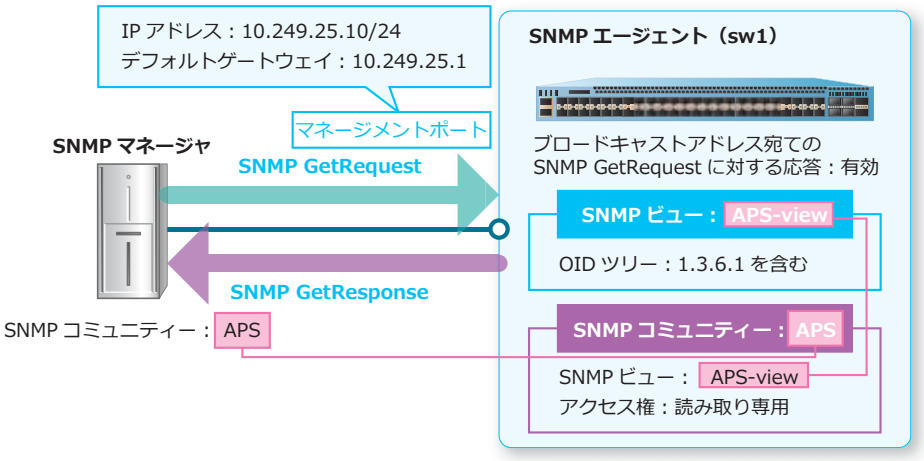
5.3 SNMP の構成例と設定例

SNMP を利用する場合の構成例と設定例を示します。

5.3.1 SNMP GetRequest/SNMP GetResponse を利用する場合

SNMP GetRequest/SNMP GetResponse を利用して、SNMP エージェントの情報を取得する場合の構成例と設定例を示します。本設定例ではブロードキャストアドレス宛ての SNMP GetRequest に対する応答も有効に設定しています。

図 5-9 SNMP GetRequest/SNMP GetResponse を利用する場合の構成例



1. マネージメントポートの IP アドレスを［10.249.25.10/24］に、デフォルトゲートウェイを［10.249.25.1］に設定します。

```
sw1# configure terminal
sw1(config)# interface mgmt 0
sw1(config-if-mgmt)# ip address 10.249.25.10/24
sw1(config-if-mgmt)# ip default-gateway 10.249.25.1
sw1(config-if-mgmt)# exit
sw1(config)#
```

2. 初期設定されている SNMP コミュニティー［private］および［public］を削除します。

```
sw1(config)# no snmp-server community private
sw1(config)# no snmp-server community public
sw1(config)#
```

3. 初期設定されている SNMP グループ［initial］の SNMP ユーザー［initial］を削除します。

```
sw1(config)# no snmp-server user initial initial v3
sw1(config)#
```

4. SNMP ビュー［APS-view］を作成し、OID ツリー［1.3.6.1］を含めます。

```
sw1(config)# snmp-server view APS-view 1.3.6.1 included
sw1(config)#
```

5. SNMP コミュニティー［APS］を作成し、SNMP ビューを［APS-view］に、アクセス権を読み取り専用に設定します。

```
sw1(config)# snmp-server community APS view APS-view ro
sw1(config)#
```

6. ブロードキャストアドレス宛ての SNMP GetRequest に対する応答を有効化します。

```
sw1(config)# snmp-server response broadcast-request
sw1(config)#
```

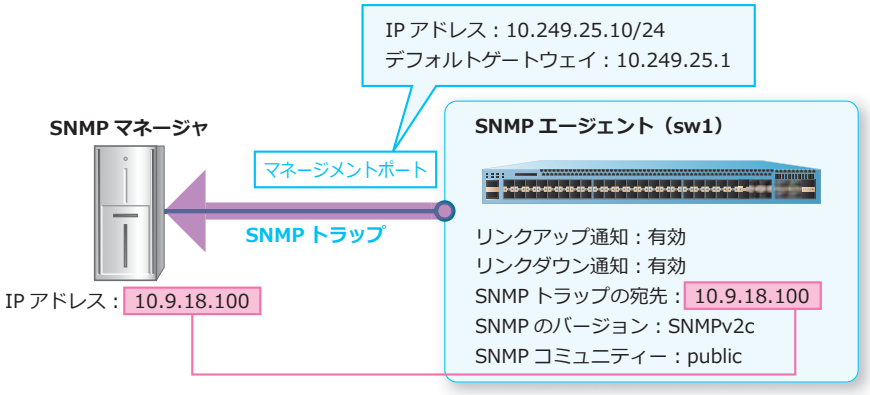
7. SNMP エージェントを有効化します。

```
sw1(config)# snmp-server
sw1(config)# end
sw1#
```

5.3.2 SNMP トラップを利用する場合

SNMP トラップを利用して、SNMP エージェントからの通知を受信する場合の構成例と設定例を示します。

図 5-10 SNMP トラップを利用する場合の構成例



1. マネージメントポートの IP アドレスを［10.249.25.10/24］に、デフォルトゲートウェイを［10.249.25.1］に設定します。

```
sw1# configure terminal
sw1(config)# interface mgmt 0
sw1(config-if-mgmt)# ip address 10.249.25.10/24
sw1(config-if-mgmt)# ip default-gateway 10.249.25.1
sw1(config-if-mgmt)# exit
sw1(config)#
```

2. リンクアップ通知およびリンクダウン通知を送信できるように設定します。

```
sw1(config)# snmp-server enable traps snmp linkdown
sw1(config)# snmp-server enable traps snmp linkup
sw1(config)#
```

3. SNMP トラップの送信を有効化します。

```
sw1(config)# snmp-server enable traps
sw1(config)#
```

4. SNMP トラップの宛先を［10.9.18.100］に、SNMP のバージョンを［SNMPv2c］に、SNMP コミュニティーを［public］に設定します。

```
sw1(config)# snmp-server host 10.9.18.100 version 2c public
sw1(config)#
```

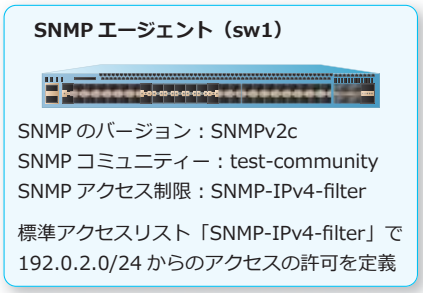
5. SNMP エージェントを有効化します。

```
sw1(config)# snmp-server
sw1(config)# end
sw1#
```

5.3.3 SNMP アクセスを許可する端末を制限する場合

SNMP アクセスを許可する端末を制限する場合の構成例と設定例を示します。

図 5-11 SNMP アクセスを許可する端末を制限する場合の構成例



1. 標準 IP アクセスリスト［SNMP-IPv4-filter］を作成します。SNMP アクセスを許可するルールを以下のように設定します。

ルール 10（許可）：送信元 IP アドレス［192.0.2.0 0.0.0.255］、宛先 IP アドレス［any］

```
sw1# configure terminal
sw1(config)# ip access-list SNMP-IPv4-filter
sw1(config-ip-acl)# 10 permit 192.0.2.0 0.0.0.255 any
sw1(config-ip-acl)# exit
sw1(config)#
```

2. 初期設定されている SNMP コミュニティー［private］および［public］を削除します。

```
sw1(config)# no snmp-server community private
sw1(config)# no snmp-server community public
sw1(config)#
```

3. 初期設定されている SNMP グループ［initial］の SNMP ユーザー［initial］を削除します。

```
sw1(config)# no snmp-server user initial initial v3
sw1(config)#
```

4. SNMP コミュニティー［test-community］を作成し、アクセス権を読み取り専用に、アクセス制限に使用するアクセスリストを［SNMP-IPv4-filter］に設定します。

```
sw1(config)# snmp-server community test-community ro access SNMP-IPv4-filter
sw1(config)#
```

5. SNMP エージェントを有効化します。

```
sw1(config)# snmp-server
sw1(config)# end
sw1#
```

6. RMON

RMON の機能、状態の確認方法、および構成例と設定例について説明します。

REF: コマンドの詳細については、『コマンドリファレンス』を参照してください。

6.1 RMON の機能説明

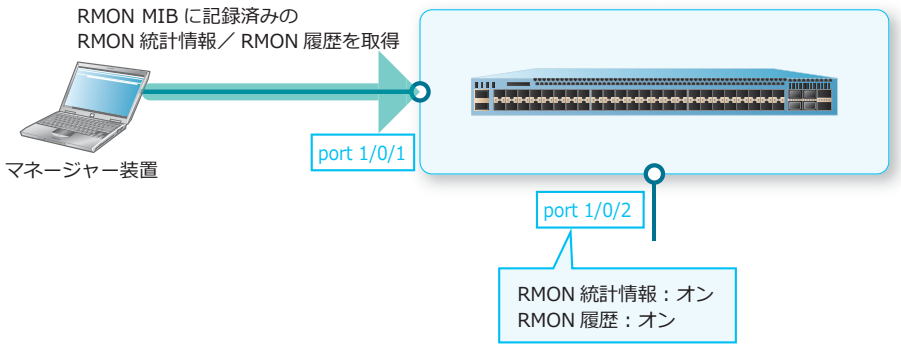
RMON（Remote network MONitoring）は、遠隔地にあるネットワークの通信状況を監視する機能です。SNMP の機能を利用して実現しています。

6.1.1 RMON 統計情報／ RMON 履歴

RMON 統計情報／ **RMON 履歴**を有効化したインターフェースは、統計情報を RMON MIB に記録します。マネージャー装置から SNMP で RMON MIB に記録された情報を取得し、ネットワークの通信状況を監視できます。

NOTE: RMON を利用するには、SNMP エージェントを有効化してください。

図 6-1 RMON 統計情報／ RMON 履歴の概要



RMON 統計情報

RMON 統計情報は、RMON MIB の statistics グループに記録されます。たとえば、ネットワーク中の総パケット数、ブロードキャストのパケット数、およびエラー数などが記録されます。RMON 統計情報を有効にするには、**`rmon collection stats`** コマンドを使用します。

RMON 履歴

RMON 履歴は、RMON 統計情報を指定した履歴数まで記録する機能です。RMON MIB の history グループに記録されます。RMON 履歴を有効にするには、**`rmon collection history`** コマンドを使用します。

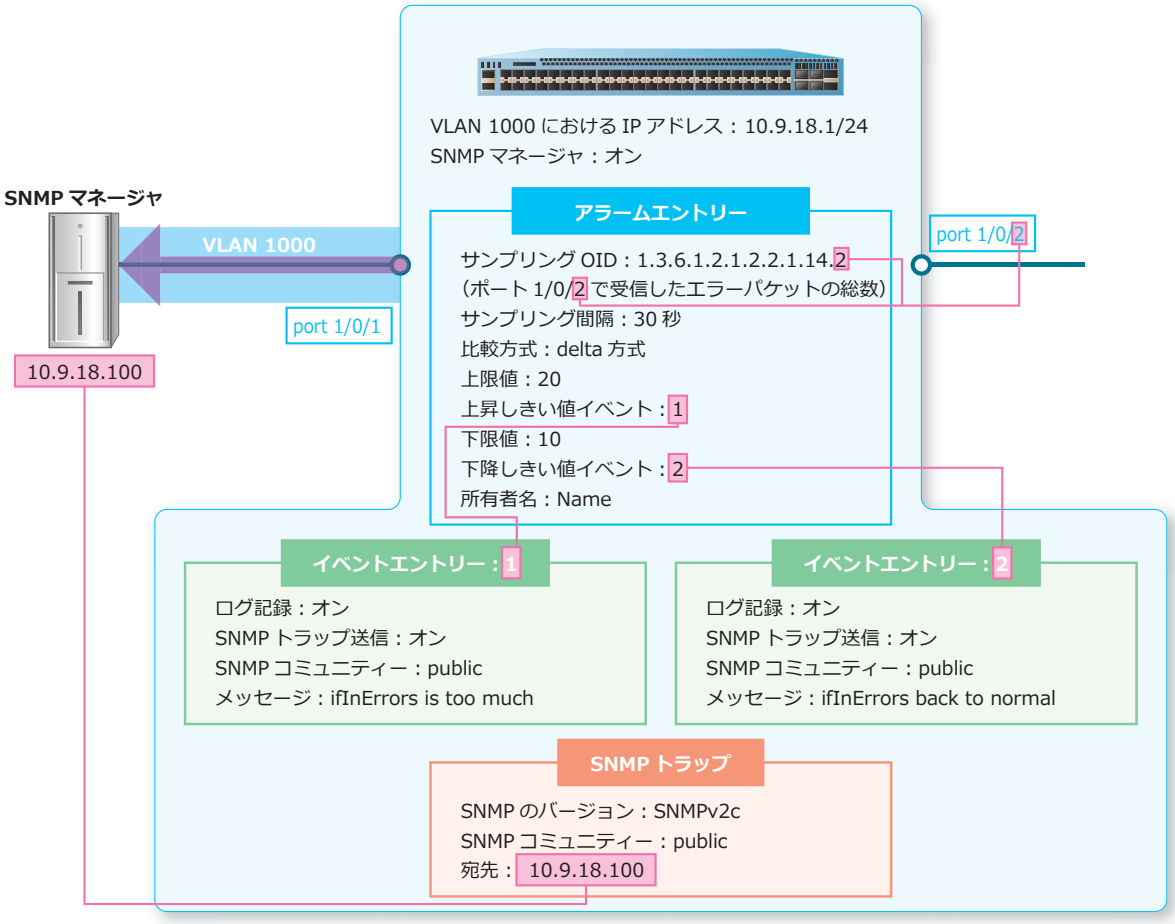
6.1.2 異常の通知（アラームエントリー／イベントエントリー）

アラームエントリーを設定すると、監視対象のオブジェクト識別子（OID）の値をサンプリング間隔で取得し、指定した比較方式でしきい値と比較します。サンプリング値が上昇しきい値（上限値）以上になった場合は、上昇しきい値イベントが実行されます。サンプリング値が下降しきい値（下限値）以下になった場合は、下降しきい値イベントが実行されます。アラームエントリーは、**`rmon alarm`** コマンドで設定します。

上昇しきい値イベント、および下降しきい値イベントに関連付けるイベントエントリーでは、ログ記録（RMON MIB の logTable）の有効／無効、SNMP トラップ送信の有効／無効、イベントの説明を設定できます。イベントエントリーは、**`rmon event`** コマンドで設定します。

NOTE: Counter64 型のオブジェクト識別子（OID）は、監視対象として指定できません。

図 6-2 アラームエントリー／イベントエントリーの概要



この例のように設定した場合は、以下のいずれかの条件を満たしたときに、ログ記録（RMON MIB の logTable）および SNMP トラップ送信が実行されます。

- ポート 1/0/2 で受信したエラーパケットの前回サンプリング値からの差分値が、上限値（20）以上になった場合
- ポート 1/0/2 で受信したエラーパケットの前回サンプリング値からの差分値が、下限値（10）以下になった場合

上昇しきい値（上限値）および下降しきい値（下限値）との比較方式

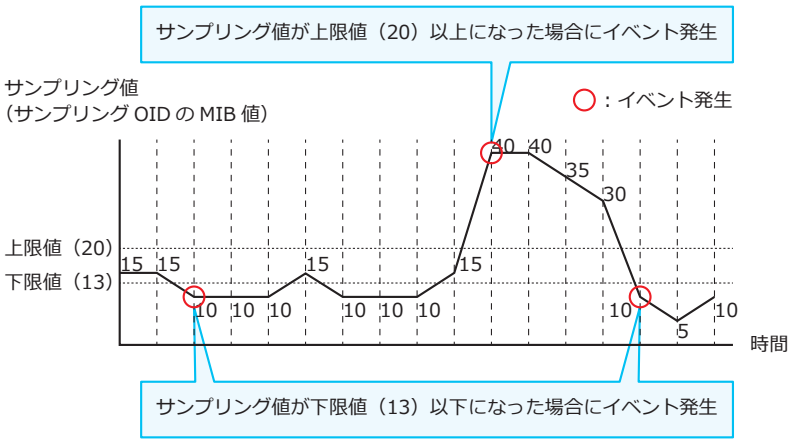
サンプリング値は、**absolute 方式**または **delta 方式**のいずれかで比較します。

- **absolute 方式**

  取得した値をそのままサンプリング値として使用します。サンプリング値が上限値以上になった場合に上昇しきい値イベントが実行され、下限値以下になった場合に下降しきい値イベントが実行されます。

  上昇しきい値イベントが発生した後は、サンプリング値が下限値以下になるまで別の上昇しきい値イベントは発生しません。下降しきい値イベントが発生した後は、サンプリング値が上限値以上になるまで別の下降しきい値イベントは発生しません。

図 6-3 比較方式が absolute 方式の場合

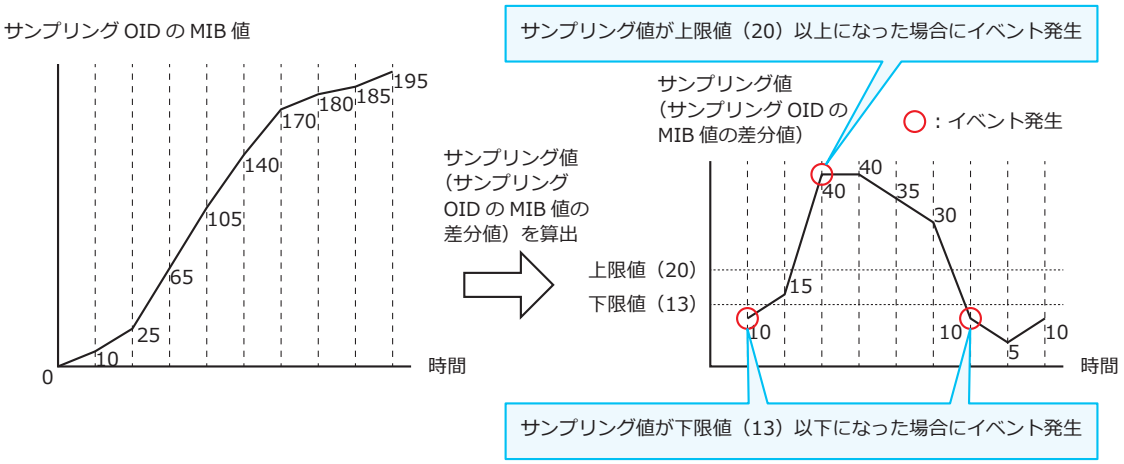


- **delta 方式**

  前回取得値と今回取得値の差分値をサンプリング値として使用します。サンプリング値が上限値以上になった場合に上昇しきい値イベントが実行され、下限値以下になった場合に下降しきい値イベントが実行されます。

  上昇しきい値イベントが発生した後は、サンプリング値が下限値以下になるまで別の上昇しきい値イベントは発生しません。下降しきい値イベントが発生した後は、サンプリング値が上限値以上になるまで別の下降しきい値イベントは発生しません。

図 6-4 比較方式が delta 方式の場合



6.2 RMON の状態確認

RMON の状態を表示して確認する方法を説明します。

6.2.1 RMON 統計情報の表示

show rmon statistics コマンドで、装置が蓄積した RMON 統計情報を確認できます。

表示例を以下に示します。

```
# show rmon statistics
(1)         (2)            (3)
Index 1, owned by guest, Data source is Port1/0/1
  Received octets: 518394321, Received packets: 5228964 ...(4)
  Broadcast packets: 2559743, Multicast packets: 988945 ...(5)
  Undersized packets: 0, Oversized packets: 0 ...(6)
  Fragments: 0, Jabbers: 0 ...(7)
  CRC alignment errors: 0, Collisions: 0 ...(8)
  Drop events: 887 ...(9)
  Packets in 64 octets: 4255288, Packets in 65-127 octets: 128250 ...(10)
  Packets in 128-255 octets: 576077, Packets in 256-511 octets: 102826 ...(10)
  Packets in 512-1023 octets: 165799, Packets in 1024-1518 octets: 724 ...(10)
```

各項目の説明は、以下のとおりです。

表 6-1 show rmon statistics コマンドの表示項目

項番	説明
(1)	RMON 統計情報 ID を表示します。
(2)	所有者名を表示します。
(3)	RMON 統計情報の対象ポート番号を表示します。
(4)	受信オクテット数、および受信パケット数を表示します。
(5)	ブロードキャストパケット数、およびマルチキャストパケット数を表示します。
(6)	アンダーサイズ（フレーム長が 64 オクテットよりも小さい）パケット数、およびオーバーサイズ（フレーム長が 1,518 オクテットよりも大きい）パケット数を表示します。
(7)	フラグメント（フレーム長が 64 オクテットよりも小さいパケットのうち、FCS エラーを伴う）パケット数、およびジャバー（フレーム長が 1,518 オクテットよりも大きいパケットのうち、FCS エラーを伴う）パケット数を表示します。
(8)	フレーム長が 64 ～ 1,518 オクテットのパケットのうち、FCS エラーを伴うパケット数、およびコリジョンの推定値を表示します。
(9)	リソース不足のために廃棄されたイベントの検出回数を表示します。
(10)	フレーム長ごとの受信パケット数を表示します。

6.2.2 RMON 履歴の表示

show rmon history コマンドで、装置が蓄積した RMON 履歴を確認できます。

表示例を以下に示します。

```
# show rmon history
(1)         (2)             (3)
Index 101, owned by test, Data source is Port1/0/1
 Interval: 60 seconds ...(4)
 Requested buckets: 50, Granted buckets: 50 ...(5)
 Sample 1 ...(6)
  Received octets: 9303, Received packets: 107 ...(7)
  Broadcast packets: 37, Multicast packets: 14 ...(8)
  Estimated utilization: 100 ...(9)
  Undersized packets: 0, Oversized packets: 0 ...(10)
  Fragments: 0, Jabbers: 0 ...(11)
  CRC alignment errors: 0, Collisions: 0 ...(12)
  Drop events: 0 ...(13)
 Sample 2
  Received octets: 11027, Received packets: 110
  Broadcast packets: 32, Multicast packets: 20
  Estimated utilization: 0
  Undersized packets: 0, Oversized packets: 0
  Fragments: 0, Jabbers: 0
  CRC alignment errors: 0, Collisions: 0
  Drop events: 0
 Sample 3
  Received octets: 8762, Received packets: 103
  Broadcast packets: 29, Multicast packets: 17
  Estimated utilization: 100
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

各項目の説明は、以下のとおりです。

表 6-2 show rmon history コマンドの表示項目

項番	説明
(1)	RMON 履歴 ID を表示します。
(2)	所有者名を表示します。
(3)	RMON 履歴の対象ポート番号を表示します。
(4)	サンプリング間隔を表示します。
(5)	RMON 統計情報を記録する履歴数を表示します。
(6)	履歴番号を表示します。
(7)	受信オクテット数、および受信パケット数を表示します。
(8)	ブロードキャストパケット数、およびマルチキャストパケット数を表示します。
(9)	サンプリング間隔におけるリンクの推定利用率 (%) を表示します。
(10)	アンダーサイズ（フレーム長が 64 オクテットよりも小さい）パケット数、およびオーバーサイズ（フレーム長が 1,518 オクテットよりも大きい）パケット数を表示します。
(11)	フラグメント（フレーム長が 64 オクテットよりも小さいパケットのうち、FCS エラーを伴う）パケット数、およびジャバー（フレーム長が 1,518 オクテットよりも大きいパケットのうち、FCS エラーを伴う）パケット数を表示します。

項番	説明
(12)	フレーム長が 64 ～ 1,518 オクテットのパケットのうち、FCS エラーを伴うパケット数、およびコリジョンの推定値を表示します。
(13)	リソース不足のために廃棄されたイベントの検出回数を表示します。

6.2.3 アラームエントリーの表示

show rmon alarm コマンドで、アラームエントリーを確認できます。

表示例を以下に示します。

```
# show rmon alarm
(1)              (2)
Alarm Index 23, owned by IT
 Monitors OID: 1.3.6.1.2.1.2.2.1.10.1 ...(3)
 every 120 second(s) ...(4)
 (5)                    (6)
 Taking delta samples, last value was 2500
 Rising threshold is 2000, assigned to event 12 ...(7)
 Falling threshold is 1100, assigned to event 12 ...(8)
 On startup enable rising or falling alarm ...(9)
```

各項目の説明は、以下のとおりです。

表 6-3 show rmon alarm コマンドの表示項目

項番	説明
(1)	アラームエントリー ID を表示します。
(2)	所有者名を表示します。
(3)	監視対象のオブジェクト識別子（OID）を表示します。
(4)	サンプリング間隔を表示します。
(5)	上昇しきい値（上限値）、および下降しきい値（下限値）との比較方式を表示します。 • Taking absolute samples：サンプリング値をそのまま比較対象にする absolute 方式 • Taking delta samples：前回のサンプリング値からの差分値を比較対象にする delta 方式
(6)	最新のサンプリング値を表示します。
(7)	上昇しきい値（上限値）、および上昇しきい値イベント発生時に使用するイベントエントリー ID を表示します。
(8)	下降しきい値（下限値）、および下降しきい値イベント発生時に使用するイベントエントリー ID を表示します。
(9)	アラームエントリーが開始してから初めてのサンプリング値を、上昇しきい値（上限値）、および下降しきい値（下限値）との判定対象として使用することを意味します。

6.2.4 イベントエントリーの表示

show rmon events コマンドで、イベントエントリーを確認できます。

表示例を以下に示します。

```
# show rmon events
(1)          (2)
Event 1001, owned by guest
 Description is Errors over 100 packets ...(3)
 Event trigger action: log & trap send to community public ...(4)
 Last triggered time: 21:59:2, 3 ...(5)
 Log: 1 ...(6)
  Log Time: 3d, 21h:57m:32s ...(7)
  Log Description: Errors over 100 packets ...(8)
 Log: 2
  Log Time: 3d, 21h:59m:2s
  Log Description: Errors over 100 packets
```

各項目の説明は、以下のとおりです。

表 6-4 show rmon events コマンドの表示項目

項番	説明
(1)	イベントエントリー ID を表示します。
(2)	所有者名を表示します。
(3)	イベントエントリーの説明を表示します。
(4)	イベントエントリーのアクションを表示します。
(5)	直近のイベント発生時の sysUpTime の値を表示します。
(6)	ログ番号を表示します。ログは、イベント発生時のログ記録（RMON MIB の logTable）を有効にしている場合に表示されます。
(7)	イベント発生時の sysUpTime の値を表示します。
(8)	イベントエントリーの説明を表示します。

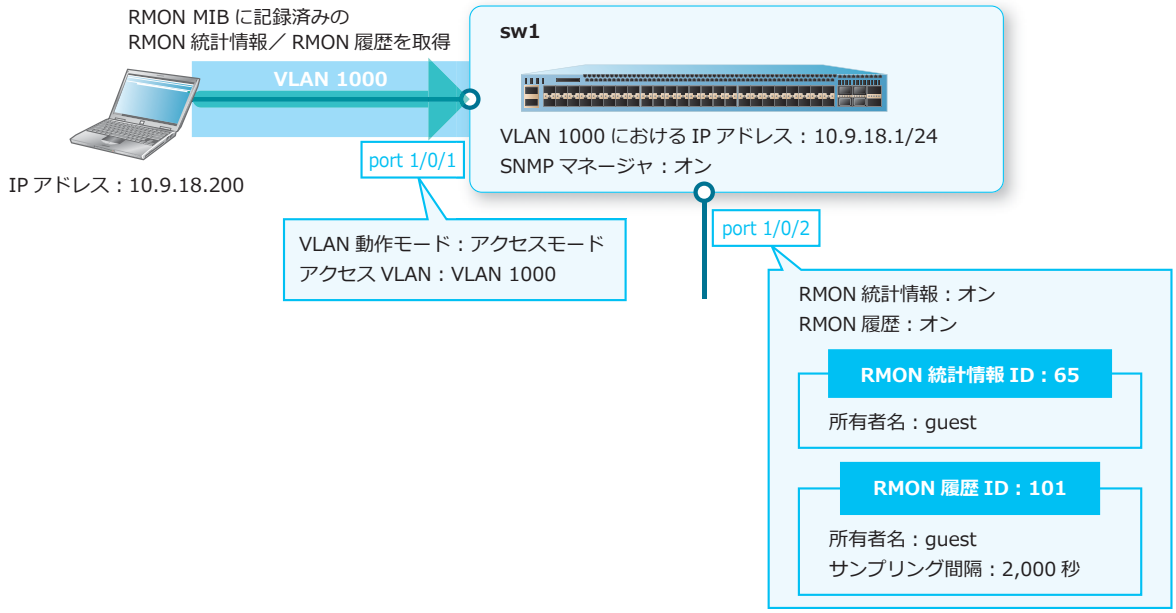
6.3 RMON の構成例と設定例

RMON を利用する場合の構成例と設定例を示します。

6.3.1 RMON 統計情報／ RMON 履歴を有効にする場合

RMON 統計情報／ RMON 履歴を有効にする場合の構成例と設定例を示します。

図 6-5 RMON 統計情報／ RMON 履歴を有効にする場合の構成例



1. VLAN 1000 を作成します。

```
sw1# configure terminal
sw1(config)# vlan 1000
sw1(config-vlan)# exit
sw1(config)#
```

2. ポート 1/0/1 をアクセスポートとして設定し、アクセスポートに［VLAN 1000］を割り当てます。

```
sw1(config)# interface port 1/0/1
sw1(config-if-port)# switchport access vlan 1000
sw1(config-if-port)# exit
sw1(config)#
```

3. VLAN 1000 における IP アドレスを［10.9.18.1/24］に設定します。

```
sw1(config)# interface vlan 1000
sw1(config-if-vlan)# ip address 10.9.18.1/24
sw1(config-if-vlan)# exit
sw1(config)#
```

4. SNMP エージェントを有効化します。

```
sw1(config)# snmp-server
sw1(config)#
```

5. ポート 1/0/2 の RMON 統計情報を以下のように設定して有効化します。

RMON 統計情報 ID［65］、所有者名［guest］

```
sw1(config)# interface port 1/0/2
sw1(config-if-port)# rmon collection stats 65 owner guest
sw1(config-if-port)#
```

6. 同様に RMON 履歴を以下のように設定して有効化します。

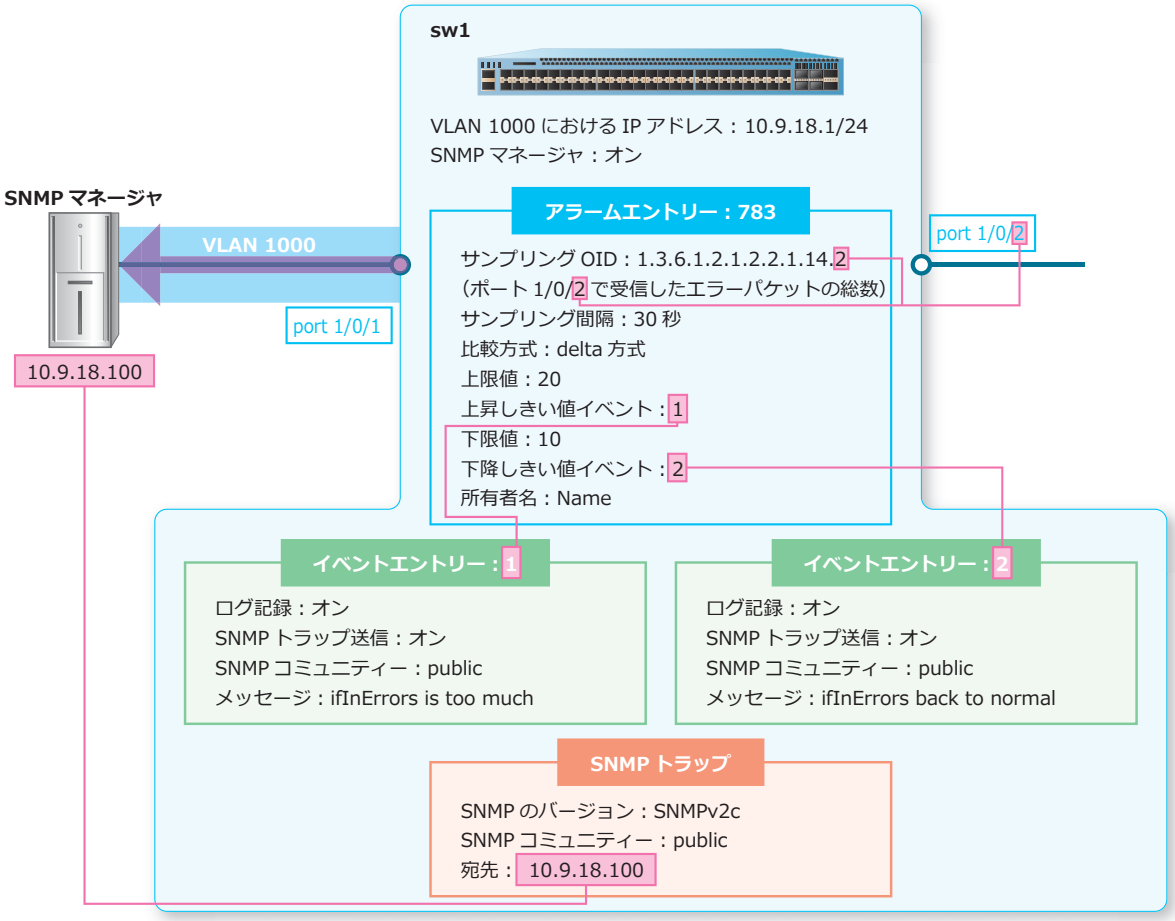
RMON 履歴 ID［101］、所有者名［guest］、サンプリング間隔［2,000 秒］

```
sw1(config-if-port)# rmon collection history 101 owner guest interval 2000
sw1(config-if-port)# end
sw1#
```

6.3.2 アラームエントリー／イベントエントリーを利用する場合

アラームエントリー／イベントエントリーを利用して、上昇しきい値イベントまたは下降しきい値イベント発生時に、ログ記録（RMON MIB の logTable）および SNMP トラップ送信を有効にする場合の構成例と設定例を示します。

図 6-6 アラームエントリー／イベントエントリーを利用する場合の構成例



1. VLAN 1000 を作成します。

```
sw1# configure terminal
sw1(config)# vlan 1000
sw1(config-vlan)# exit
sw1(config)#
```

2. ポート 1/0/1 をアクセスポートとして設定し、アクセスポートに［VLAN 1000］を割り当てます。

```
sw1(config)# interface port 1/0/1
sw1(config-if-port)# switchport access vlan 1000
sw1(config-if-port)# exit
sw1(config)#
```

3. VLAN 1000 における IP アドレスを［10.9.18.1/24］に設定します。

```
sw1(config)# interface vlan 1000
sw1(config-if-vlan)# ip address 10.9.18.1/24
sw1(config-if-vlan)# exit
sw1(config)#
```

4. SNMP トラップの送信を有効化します。

```
sw1(config)# snmp-server enable traps
sw1(config)#
```

5. SNMP エージェントを有効化します。

```
sw1(config)# snmp-server
sw1(config)#
```

6. RMON 機能の SNMP トラップを有効化します。

```
sw1(config)# snmp-server enable traps rmon
sw1(config)#
```

7. SNMP トラップの宛先を［10.9.18.100］に、SNMP のバージョンを［SNMPv2c］に、SNMP コミュニティーを［public］に設定します。

```
sw1(config)# snmp-server host 10.9.18.100 version 2c public
sw1(config)#
```

8. アラームエントリーを以下のように設定します。

アラームエントリー ID［783］、サンプリング OID［1.3.6.1.2.1.2.2.1.14.2］（ポート 1/0/2 で受信したエラーパケットの総数）、サンプリング間隔［30 秒］、比較方式［delta 方式］、上限値［20］、上昇しきい値イベントの ID［1］、下限値［10］、下降しきい値イベントの ID［2］、所有者名［Name］

```
sw1(config)# rmon alarm 783 1.3.6.1.2.1.2.2.1.14.2 30 delta rising-threshold
20 1 falling-threshold 10 2 owner Name
sw1(config)#
```

9. イベントエントリーを以下のように設定します。

イベントエントリー ID［1］、ログ記録［オン］、SNMP トラップ送信［オン］、SNMP コミュニティー［public］、所有者名［Name］、イベントエントリーの説明［ifInErrors is too much］

イベントエントリー ID［2］、ログ記録［オン］、SNMP トラップ送信［オン］、SNMP コミュニティー［public］、所有者名［Name］、イベントエントリーの説明［ifInErrors back to normal］

```
sw1(config)# rmon event 1 log trap public owner Name description ifInErrors is
too much
sw1(config)# rmon event 2 log trap public owner Name description ifInErrors
back to normal
sw1(config)# end
sw1#
```

7. sFlow

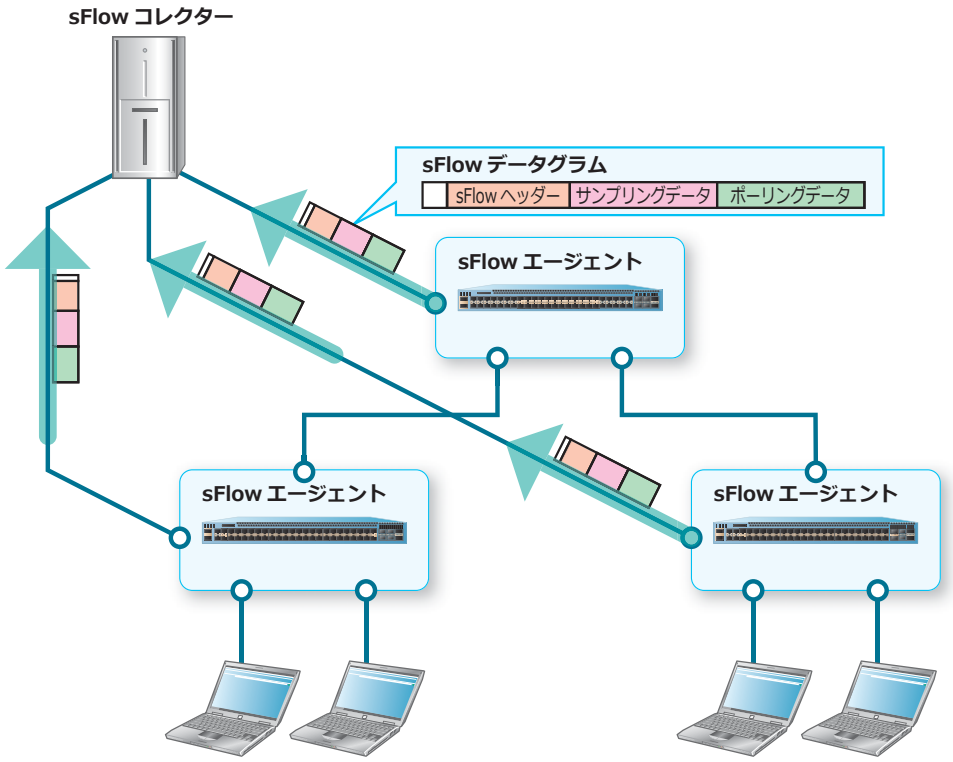
sFlow の機能、状態の確認方法、および構成例と設定例について説明します。

REF: コマンドの詳細については、『コマンドリファレンス』を参照してください。

7.1 sFlow の機能説明

sFlow はネットワーク内のトラフィックをモニタリングするプロトコルで、**sFlow コレクター**と **sFlow エージェント**から構成されます。

図 7-1 sFlow の概要



- **sFlow コレクター**

  トラフィックを分析するために sFlow データグラムを収集するデバイスです。

- **sFlow エージェント**

  トラフィックを分析するために、装置で送受信したフレームのサンプリングおよびポーリングを行うデバイスです。

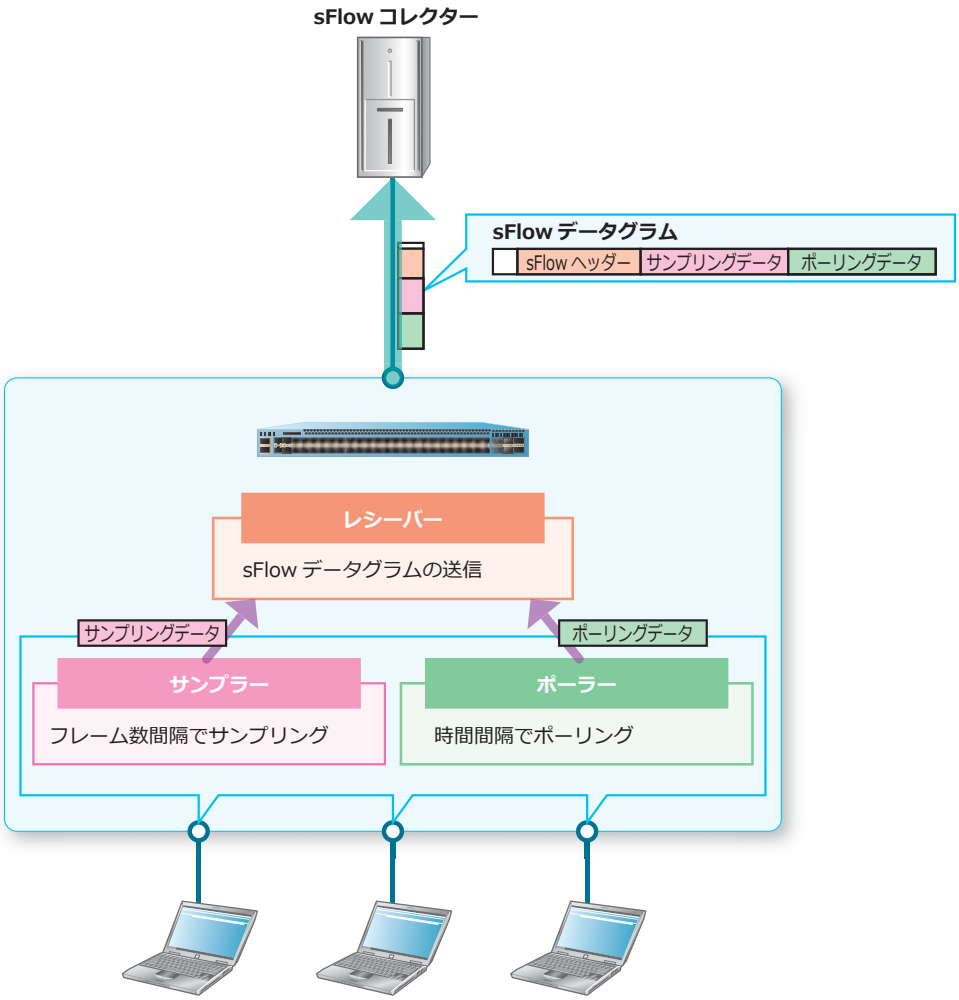
- **sFlow データグラム**

  sFlow エージェントにおいてサンプリングまたはポーリングしたデータを格納し、sFlow コレクターに送信されるパケットです。

7.1.1 sFlow エージェント

sFlow エージェントには、サンプラー、ポーラー、およびレシーバーの 3 つの機能があります。各機能によって、sFlow データグラムが作成され、sFlow コレクターに送信されます。

図 7-2 sFlow エージェントの概要



サンプラー

インターフェースで送受信されるデータをサンプリングレートで指定したフレーム数間隔でサンプリングし、sFlow データグラムに格納します。サンプラーは、sFlow エージェントのインターフェースごとに作成できます。サンプラーを作成するには、**`sflow sampler`** コマンドを使用します。

- **ポーラー**

  インターフェースで送受信されるデータを一定の時間間隔でポーリングし、sFlow データグラムに格納します。ポーラーは、sFlow エージェントのインターフェースごとに作成できます。ポーラーを作成するには、**`sflow poller`** コマンドを使用します。

- **レシーバー**

  sFlow データグラムを sFlow コレクターに送信します。レシーバーを作成するには、**`sflow receiver`** コマンドを使用します。

7.2 sFlow の状態確認

sFlow の状態を表示して確認する方法を説明します。

7.2.1 sFlow エージェントの表示

show sflow agent コマンドで、sFlow エージェントの情報を確認できます。

表示例を以下に示します。

```
# show sflow agent

sFlow Agent Version       : APRESIA Systems, Ltd Inc.;1.00 ...(1)
sFlow Agent Address       : 192.0.2.100 ...(2)
sFlow Agent IPv6 Address  :  ...(3)
```

各項目の説明は、以下のとおりです。

表 7-1 show sflow agent コマンドの表示項目

項番	説明
(1)	sFlow エージェントの情報（組織、sFlow ソフトウェアのリビジョン）を表示します。
(2)	sFlow エージェントの IPv4 アドレスを表示します。 IPv4 アドレスが設定されている VLAN インターフェースのうち、最小 VLAN ID である VLAN インターフェースの IPv4 アドレスが、sFlow エージェントの IPv4 アドレスになります。
(3)	sFlow エージェントの IPv6 アドレスを表示します。 VLAN 1 インターフェースの IPv6 リンクローカルアドレスが、sFlow エージェントの IPv6 アドレスになります。sFlow エージェントの IPv6 アドレスを使用する場合は、VLAN 1 インターフェースで IPv6 機能を有効にしてください。

7.2.2 sFlow エージェントのレシーバーの表示

show sflow receiver コマンドで、sFlow エージェントのレシーバーの情報を確認できます。

表示例を以下に示します。

```
# show sflow receiver

Receivers Information
Index                     : 1 ...(1)
Owner                     : collector1 ...(2)
Expire Time               : 86400 ...(3)
Current Countdown Time    : 85550 ...(4)
Max Datagram Size         : 1400 ...(5)
Address                   : 10.1.1.2 ...(6)
VRF Name                  :  ...(7)
Port                      : 6343 ...(8)
Datagram Version          : 5 ...(9)

Index                     : 2
～～省略～～
```

各項目の説明は、以下のとおりです。

表 7-2 `show sflow receiver` コマンドの表示項目

項番	説明
(1)	sFlow レシーバーのインデックスを表示します。
(2)	所有者名を表示します。
(3)	レシーバーの有効期限を表示します。
(4)	サンプリングおよびポーリングが停止するまでの時間（秒）を表示します。
(5)	1 つの sFlow データグラムの最大バイト数を表示します。
(6)	sFlow コレクターの IPv4 アドレスまたは IPv6 アドレスを表示します。
(7)	関連付ける VRF インスタンス名を表示します。NP7000、NP5000、および NP3000 で表示されます。
(8)	sFlow コレクターとの通信に使用する UDP ポート番号を表示します。
(9)	sFlow データグラムのバージョンを表示します。

7.2.3 sFlow エージェントのサンプラーの表示

`show sflow sampler` コマンドで、sFlow エージェントのサンプラーの情報を確認できます。

表示例を以下に示します。

```
# show sflow sampler

Samplers Information
(1)          (2)       (3)       (4)       (5)          (6)          (7)
Interface    Instance Receiver Mode      Admin Rate  Active Rate  Max Header Size
------------ -------- -------- -------- ----------  -----------  ---------------
Port1/0/1           1        1 inbound         1024         1024              128
Port1/0/5         105        1 outbound        1024         1024              128
```

各項目の説明は、以下のとおりです。

表 7-3 `show sflow sampler` コマンドの表示項目

項番	説明
(1)	サンプラーを設定したポート番号を表示します。
(2)	サンプラーのインデックスを表示します。
(3)	サンプラー用のレシーバーのインデックスを表示します。
(4)	サンプリング対象（inbound：受信パケット／ outbound：送信パケット）を表示します。
(5)	設定したサンプリングレートを表示します。実際のサンプリングレートは「設定値（表示されている値）×256」パケットで動作します。
(6)	アクティブなサンプリングレートを表示します。実際のサンプリングレートは「表示されている値 ×256」パケットで動作します。
(7)	サンプリングしたパケットからコピーするデータの最大バイト数を表示します。

7.2.4 sFlow エージェントのポーラーの表示

show sflow poller コマンドで、sFlow エージェントのポーラーの情報を確認できます。

表示例を以下に示します。

```
# show sflow poller

Pollers Information
(1)          (2)        (3)        (4)
Interface    Instance   Receiver   Interval
-----------  --------   --------   --------
Port1/0/1           1          1         60
Port1/0/5         105          1         60
```

各項目の説明は、以下のとおりです。

表 7-4 show sflow poller コマンドの表示項目

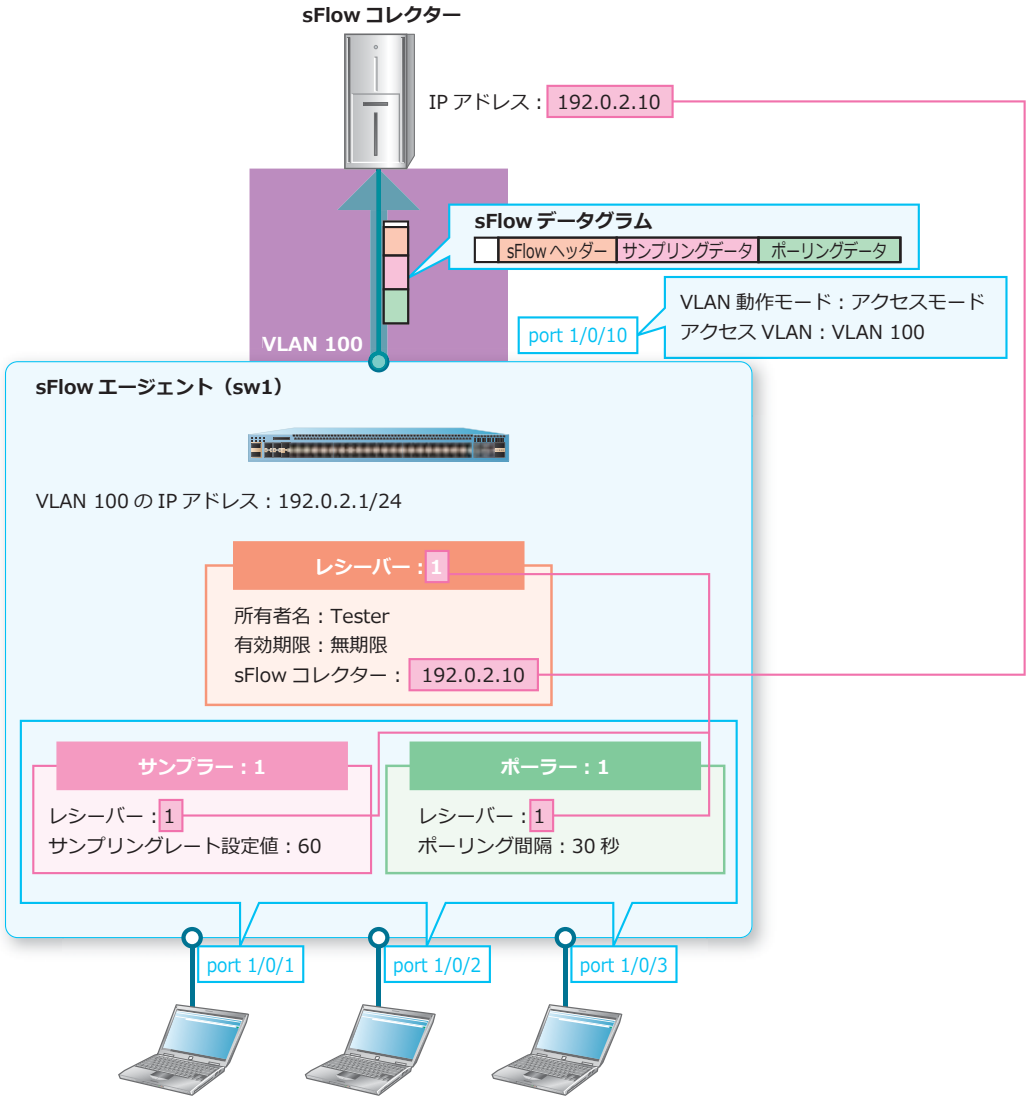
項番	説明
(1)	ポーラーを設定したポート番号を表示します。
(2)	ポーラーのインデックスを表示します。
(3)	ポーラー用のレシーバーのインデックスを表示します。
(4)	ポーリング間隔を表示します。

7.3 sFlow の構成例と設定例

sFlow エージェントを利用する場合の構成例と設定例を示します。

- レシーバー：レシーバー ID = 1、所有者名 = Tester、有効期限 = 無期限（infinite）、sFlow コレクターの IP アドレス = 192.0.2.10
- ポート 1/0/1 からポート 1/0/3 でサンプラーを設定：サンプラー ID = 1、レシーバー ID = 1、サンプリング対象は受信パケット、サンプリングレート設定値 = 60
- ポート 1/0/1 からポート 1/0/3 でポーラーを設定：ポーラー ID = 1、レシーバー ID = 1、ポーリング間隔 = 30 秒

図 7-3 sFlow の構成例



1. VLAN 100 を作成し、ポート 1/0/10 をアクセスポートとして［VLAN 100］を割り当てます。また、VLAN 100 の IP アドレスを［192.0.2.1/24］に設定します。

```
sw1# configure terminal
sw1(config)# vlan 100
sw1(config-vlan)# exit
sw1(config)# interface port 1/0/10
sw1(config-if-port)# switchport mode access
sw1(config-if-port)# switchport access vlan 100
sw1(config-if-port)# exit
sw1(config)# interface vlan 100
sw1(config-if-vlan)# ip address 192.0.2.1/24
sw1(config-if-vlan)# exit
sw1(config)#
```

2. sFlow エージェントのレシーバーを、レシーバー ID［1］、所有者名［Tester］、有効期限［infinite］、sFlow コレクターの IP アドレス［192.0.2.10］で設定します。

```
sw1(config)# sflow receiver 1 owner Tester expiry infinite host 192.0.2.10
sw1(config)#
```

3. ポート 1/0/1 からポート 1/0/3 で sFlow エージェントのサンプラーを、サンプラー ID［1］、レシーバー ID［1］、サンプリングレート設定値［60］で設定します。サンプリング対象を指定しない場合は、受信パケットが対象になります。

```
sw1(config)# interface range port 1/0/1-3
sw1(config-if-port-range)# sflow sampler 1 receiver 1 sampling-rate 60
sw1(config-if-port-range)#
```

4. ポート 1/0/1 からポート 1/0/3 で sFlow エージェントのポーラーを、ポーラー ID［1］、レシーバー ID［1］、ポーリング間隔［30 秒］で設定します。

```
sw1(config-if-port-range)# sflow poller 1 receiver 1 interval 30
sw1(config-if-port-range)# end
sw1#
```

5. 実施後の sFlow 関連の設定を以下に抜粋します。

```
# SFLOW

sflow receiver 1 owner Tester host 192.0.2.10
interface port 1/0/1
 sflow sampler 1 receiver 1 sampling-rate 60
 sflow poller 1 receiver 1 interval 30
interface port 1/0/2
 sflow sampler 1 receiver 1 sampling-rate 60
 sflow poller 1 receiver 1 interval 30
interface port 1/0/3
 sflow sampler 1 receiver 1 sampling-rate 60
 sflow poller 1 receiver 1 interval 30
```

8. 時刻同期（NTP/SNTP）

NTP（Network Time Protocol）および SNTP（Simple Network Time Protocol）の機能、状態の確認方法、および構成例と設定例について説明します。また、手動での時刻設定方法についても説明します。

REF: コマンドの詳細については、『コマンドリファレンス』を参照してください。

8.1 時刻同期（NTP/SNTP）の機能説明

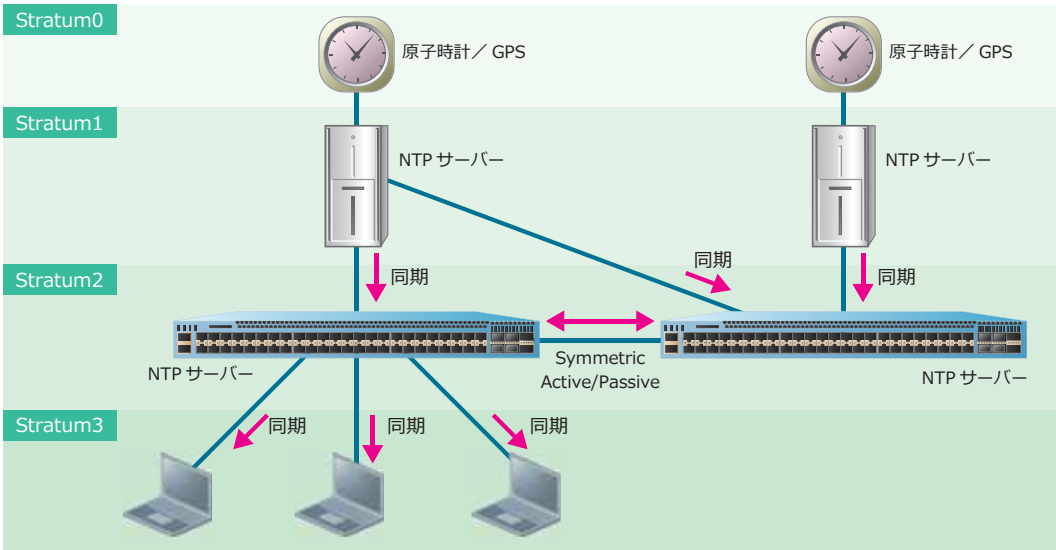
NTP および **SNTP** の機能、および手動での時刻設定方法を説明します。

8.1.1 NTP の機能説明

NTP はネットワーク経由で時刻を同期する機能です。NTP サーバーとの遅延時間などを考慮した仕組みで、より正確な時刻同期を実現します。

NTP は Stratum という階層構造（Stratum 0 ～ Stratum 15）になっており、基本的には上位の（Stratum が小さい）NTP サーバーに問い合わせて時刻を同期します。また、同じ階層の NTP サーバー同士をお互いを信頼できる情報源として関係付けることもできます。

図 8-1 NTP の概要



NTP サービスを有効にすると、NTP サーバーおよび NTP クライアントとしての動作が有効になります。NTP サービスを有効にするには、**`service ntp`** コマンドを使用します。クライアントモードで時刻を問い合わせる NTP サーバーを設定するには、**`ntp server`** コマンドを使用します。また、Symmetric Active モードで関係付ける NTP サーバーを設定するには **`ntp peer`** コマンドを使用します。

CAUTION: 本装置を NTP サーバーとして使用する場合は、NTP クライアントごとに最も近い IP アドレスを NTP サーバーとして指定してください。それ以外の IP アドレスを指定しても時刻同期できません。また、ループバックインターフェースに設定した IP アドレスを指定しても時刻同期できません。

ハードウェアクロックの定期的な更新

NTP で取得した時刻を用いて、定期的にハードウェアクロックを更新するには、**`ntp update-calendar`** コマンドを使用します。

自装置のハードウェアクロックを情報源にする場合

装置を NTP サーバーとして使用するには、信頼できる情報源（上位の NTP サーバーなど）から時刻を取得し同期している必要がありますが、上位の NTP サーバーなどを利用できない場合に自装置のハードウェアクロックを利用できます。自装置のハードウェアクロックを情報源として使用するには、**ntp master** コマンドを使用します。

8.1.2 NTP のオプション機能

NTP に関連するオプション機能を以下に示します。各コマンドの詳細については、『コマンドリファレンス』を参照してください。

- NTP の認証
- NTP の制限

8.1.2.1 NTP の認証

NTP 認証を有効にすると、認証キーが不一致の問い合わせに対する時刻同期を制限できます。NTP 認証を有効にするには、**ntp authenticate** コマンドを使用します。認証キーを定義するには **ntp authentication-key** コマンドを、使用する認証キーを指定するには **ntp trusted-key** コマンドを使用します。また、**ntp server** コマンドや **ntp peer** コマンドでも認証キーを指定します。

> ***NOTE:*** NTP サーバーは、認証なしの問い合わせを受信するとデフォルトでは応答します。認証なしの問い合わせを制限するには、**ntp access-group** コマンドで notrust パラメーターを指定して設定してください。

8.1.2.2 NTP の制限

VLAN インターフェースごとに NTP サービスを無効にできます。NTP サービスを無効にするには、**ntp disable** コマンドを使用します。

すべての送信元または特定の送信元からの NTP サービスへのアクセスを制限できます。NTP サービスへのアクセスを制限するには、**ntp access-group** コマンドを使用します。

自装置に設定するアソシエーションの最大数を設定できます。アソシエーションの最大数を設定するには、**ntp max-associations** コマンドを使用します。

8.1.3 時刻同期（SNTP）の機能説明

SNTP は NTP 同様にネットワーク経由で時刻を同期する機能で、NTP よりも簡易化されています。同期に用いるパケットは NTP と共通のため、NTP サーバーから時刻同期できます。

> ***NOTE:*** SNTP クライアント機能のみ対応しています。

> ***NOTE:*** NTP サービスと SNTP クライアント機能は同時に有効にできません。

SNTP で時刻を問い合わせる NTP/SNTP サーバーを設定するには、**sntp server** コマンドを使用します。時刻の問い合わせ間隔（デフォルト 720 秒）を変更するには、**sntp interval** コマンドを使用します。SNTP クライアント機能を有効にするには、**sntp enable** コマンドを使用します。

8.1.4 手動での時刻設定

手動で時刻を設定するには、**clock set** コマンドを使用します。NTP/SNTP を利用して外部の信頼できる情報源と時刻同期している場合は、手動で時刻を設定する必要はありません。手動での時刻設定は、NTP/SNTP による時刻同期が利用できない場合に使用してください。

> ***NOTE:*** タイムゾーンはデフォルトで日本標準時（UTC +09:00）に設定されています。

8.2 時刻同期（NTP/SNTP）の状態確認

NTP および SNTP の状態を表示して確認する方法を説明します。

8.2.1 NTP の状態の表示

show ntp status コマンドで、NTP の状態を確認できます。

表示例を以下に示します。

```
# show ntp status

Leap Indicator:       Synchronized...(1)
Stratum:              6...(2)
Precision:            -11...(3)
Root Distance:        0.02306 s...(4)
Root Dispersion:      0.10722 s...(5)
Reference ID:         [172.31.2.41]...(6)
Reference Time:       d9bf3265.9889d2dc  Wed, Oct  7 2015 14:55:49.00595...(7)
System Flags:         Auth Monitor NTP Kernel Stats...(8)
Jitter:               0.000488 s...(9)
Stability:            0.000 ppm...(10)
Auth Delay:           0.000000 s...(11)
```

各項目の説明は、以下のとおりです。

表 8-1 show ntp status コマンドの表示項目

項番	説明
(1)	Leap Indicator フィールドの情報を表示します。 • Synchronized：信頼できる情報源と時刻を同期している状態 • Unsynchronized：信頼できる情報源と時刻を同期できていない状態
(2)	自装置の Stratum を表示します。
(3)	精度値を表示します。
(4)	最上位の NTP サーバーへの往復遅延時間（秒）を表示します。
(5)	最上位の NTP サーバーとの通信における揺らぎ（秒）を表示します。
(6)	自装置が同期している NTP サーバーの IP アドレスを表示します。
(7)	自装置が最後に時刻同期を実施した時刻を表示します。
(8)	システムフラグを表示します。
(9)	システムジッター（秒）を表示します。
(10)	周波数の安定性を表示します。
(11)	認証遅延（秒）を表示します。

8.2.2 NTP アソシエーションの状態の表示

show ntp associations コマンドで、NTP アソシエーションの状態を確認できます。

表示例を以下に示します。

```
# show ntp associations
(1)(2)           (3)              (4)(5)   (6)    (7)      (8)        (9)
 Remote          Local            St Poll  Reach Delay   Offset     Disp
 =============== ================ == ===== ===== ======= ========== =======
*192.168.10.254  192.168.10.101    2    16   377 0.00003 0.002101   0.06461
+192.168.30.102  192.168.30.101    4    16   377 0.00027 -0.003163  0.11024
+ Symmetric active, - Symmetric passive, = Client, * System Peer
```

各項目の説明は、以下のとおりです。

表 8-2 show ntp associations コマンドの表示項目

項番	説明
(1)	NTP アソシエーションのモードを表示します。 • + : Symmetric active モード • - : Symmetric passive モード • = : クライアントモード • * : 同期対象
(2)	対象の IP アドレスを表示します。対象が IPv6 アドレスで、アドレス文字数が 16 文字以上の場合は、15 文字目以降が省略表記になります。
(3)	自装置の IP アドレスを表示します。対象が IPv6 アドレスで、アドレス文字数が 16 文字以上の場合は、15 文字目以降が省略表記になります。
(4)	対象の Stratum を表示します。
(5)	NTP パケットのポーリング間隔（秒）を表示します。
(6)	対象の到達可能性（過去 8 回のポーリング結果）を 8 進数で表示します。
(7)	対象への往復遅延時間（秒）を表示します。
(8)	対象との時刻オフセット（秒）を表示します。
(9)	対象との通信における揺らぎ（秒）を表示します。

8.2.3 NTP アソシエーションの詳細情報の表示

show ntp associations detail コマンドで、NTP アソシエーションの詳細情報を確認できます。

表示例を以下に示します。

```
# show ntp associations detail
(1)                    (2)
Remote 10.249.23.215, Local 10.249.24.175
(3)              (4)               (5)        (6)
Our mode client, Peer mode server, Stratum 3, Precision -18
(7)      (8)                    (9)                    (10)
Leap 00, RefID [10.249.45.11], RootDistance 0.03513, RootDispersion 0.09491
(11)     (12)     (13)     (14)       (15)
PPoll 6, HPoll 6, KeyID 0, Version 4, Association 8355
(16)       (17)       (18)          (19)       (20)
Reach 377, Unreach 0, Flash 0x0000, Timer 51s, flags  System_Peer, Config
Reference Timestamp : e34f45f6.9a3b3072  Fri, Nov  6 2020 12:48:06.60247 ...(21)
Originate Timestamp : e34f4ac8.cf9728ee  Fri, Nov  6 2020 13:08:40.81090 ...(22)
Receive Timestamp   : e34f4ac8.d97adc9e  Fri, Nov  6 2020 13:08:40.84953 ...(23)
Transmit Timestamp  : e34f4ac8.d97ada2b  Fri, Nov  6 2020 13:08:40.84953 ...(24)
Filter Delay:  0.00000  0.00032  0.00113  0.00122  ...(25)
               0.00124  0.00127  0.00127  0.00111
Filter Offset: 0.038631 0.040588 0.043037 0.045680 ...(26)
               0.049074 0.049002 0.049015 0.049231
Filter Order:  0        1        7        2        ...(27)
               3        4        5        6
(28)             (29)           (30)                (31)
Offset 0.038631, Delay 0.00000, Error Bound 0.04013, Filter Error 0.09238
```

各項目の説明は、以下のとおりです。

表 8-3 show ntp associations details コマンドの表示項目

項番	説明
(1)	対象の IP アドレスを表示します。
(2)	自装置の IP アドレスを表示します。
(3)	自装置の NTP アソシエーションのモードを表示します。 • server：サーバーモード • client：クライアントモード • active：Symmetric active モード • passive：Symmetric passive モード
(4)	対象の NTP アソシエーションのモードを表示します。 • server：サーバーモード • client：クライアントモード • active：Symmetric active モード • passive：Symmetric passive モード
(5)	対象の Stratum を表示します。
(6)	精度値を表示します。
(7)	対象から受信した NTP パケットの Leap Indicator フィールドの情報を表示します。
(8)	対象から受信した NTP パケットの Reference ID フィールドの情報を表示します。
(9)	対象から受信した NTP パケットの Root Delay フィールドの情報を表示します。

項番	説明
(10)	対象から受信した NTP パケットの Root Dispersion フィールドの情報を表示します。
(11)	対象のポーリング間隔の値を表示します。
(12)	自装置のポーリング間隔の値を表示します。
(13)	認証キー ID を表示します。
(14)	NTP バージョンを表示します。
(15)	アソシエーション ID を表示します。
(16)	対象の到達可能性（過去 8 回のポーリング結果）を 8 進数で表示します。
(17)	未到達カウンターを表示します。
(18)	問題点を診断するためのフラッシュステータスワードを表示します。
(19)	ピアタイマー（秒単位）を表示します。
(20)	ピアのフラグを表示します。
(21)	対象から受信した NTP パケットの Reference Timestamp フィールドの情報を表示します。
(22)	対象から受信した NTP パケットの Origin Timestamp フィールドの情報を表示します。
(23)	対象から受信した NTP パケットの Receive Timestamp フィールドの情報を表示します。
(24)	対象から受信した NTP パケットの Transmit Timestamp フィールドの情報を表示します。
(25)	各サンプルの往復遅延時間（秒）を表示します。
(26)	各サンプルの時刻オフセット（秒）を表示します。
(27)	各サンプルのフィルタリング順序を表示します。
(28)	対象との時刻オフセット（秒）を表示します。
(29)	対象への往復遅延時間（秒）を表示します。
(30)	対象との通信における揺らぎ（秒）を表示します。
(31)	各サンプルの近似誤差（秒）を表示します。

8.2.4 SNTP の状態の表示

show sntp コマンドで、SNTP の情報を確認できます。

表示例を以下に示します。

```
# show sntp

SNTP Status               : Enabled ...(1)
SNTP Poll Interval        : 720 seconds ...(2)

SNTP Server Status:
(3)                                              (4)     (5)     (6)
SNTP Server                                      Stratum Version Last Receive
------------------------------------------------ ------- ------- ---------------
192.0.2.100                                      ------- ------- ---------------
172.16.10.200                                    5       3       00:10:28 Synced
2001:db8:10::100                                 ------- ------- ---------------
fe80::240:66ff:aaaa:bbbb%vlan10                  ------- ------- ---------------
------------------------------------------------ ------- ------- ---------------
Total Entries: 4
```

各項目の説明は、以下のとおりです。

表 8-4 show sntp コマンドの表示項目

項番	説明
(1)	SNTP クライアント機能の有効 (Enabled) ／無効 (Disabled) を表示します。
(2)	SNTP での時刻の問い合わせ間隔を表示します。
(3)	設定した NTP/SNTP サーバーの IP アドレスを表示します。リストの先頭に登録された NTP/SNTP サーバーから問い合わせが行われます。
(4)	NTP/SNTP サーバーの Stratum を表示します。
(5)	NTP/SNTP のバージョンを表示します。
(6)	最後に時刻を同期してから経過した時間を表示します。現在の同期対象の NTP/SNTP サーバーには Synced が表示されます。

8.2.5 日時情報の表示

show clock コマンドで、装置の日時情報を確認できます。

表示例を以下に示します。

```
# show clock

     Current Time Source    : System Clock...(1)
     Current Time           : 12:27:51, 2015-03-10...(2)
     Time Zone              : UTC +09:00...(3)
     Daylight Saving Time   : Disabled...(4)
```

各項目の説明は、以下のとおりです。

表 8-5 `show clock` コマンドの表示項目

項番	説明
(1)	時刻情報の情報源を表示します。 • System Clock：システムクロック • SNTP：SNTP 有効、時刻が同期されている場合 • NTP(Synchronized)：NTP サービス有効、時刻が同期されている場合 • NTP(Unsynchronized)：NTP サービス有効、時刻が同期されていない場合
(2)	現在の時刻および年月日を表示します。
(3)	タイムゾーンを表示します。
(4)	サマータイムの有効／無効を表示します。有効な場合は、サマータイムの「オフセット」「開始日」「終了日」も表示されます。 • Disabled：無効 • Recurring：サマータイムを recurring パラメーターを指定して有効にした場合 • Date：サマータイムを date パラメーターを指定して有効にした場合

8.3 時刻同期（NTP/SNTP）の構成例と設定例

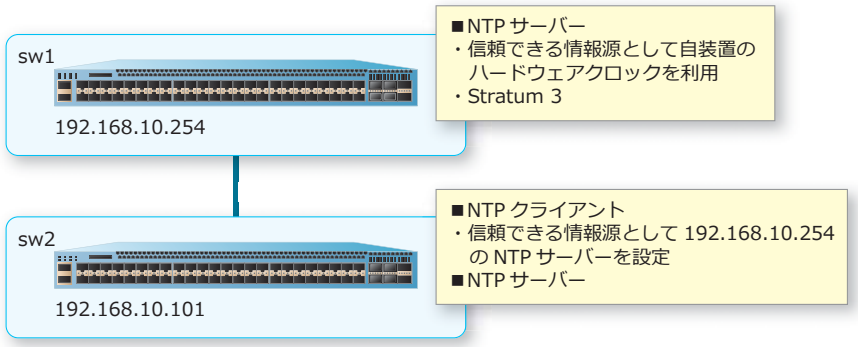
NTP および SNTP で時刻同期を行う場合の構成例と設定例を示します。

8.3.1 NTP を使用する場合

NTP を使用する場合の構成例と設定例を示します。本設定例では、VLAN や IP アドレスの設定は省略しています。

sw1 は自装置のハードウェアクロックを信頼できる情報源とした NTP サーバーとして設定しています。また、sw2 は時刻を問い合わせる NTP サーバーとして sw1 を指定して、NTP サービスを有効にしています。

図 8-2 NTP を使用する場合の構成例



8.3.1.1 NTP：sw1 の設定例

1. 自装置のハードウェアクロックを信頼できる情報源として設定します。また、自装置の Stratum を 3 に設定します。

```
sw1# configure terminal
sw1(config)# ntp master 3
sw1(config)#
```

2. NTP サービスを有効にします。

```
sw1(config)# service ntp
sw1(config)# end
sw1#
```

3. 実施後の NTP の状態を確認します。

```
sw1# show ntp status

Leap Indicator:         Synchronized
Stratum:                3
Precision:              -22
Root Distance:          0.00000 s
Root Dispersion:        0.00000 s
Reference ID:           [127.0.0.1]
Reference Time:         00000000.00000000  Thu, Feb  7 2036 15:28:16.00000
System Flags:           Auth Monitor NTP Kernel Stats
Jitter:                 0.000000 s
Stability:              0.000 ppm
Auth Delay:             0.000000 s
```

8.3.1.2 NTP：sw2 の設定例

1. NTP サーバー［192.168.10.254］宛てに時刻問い合わせを行うように設定します。

```
sw2# configure terminal
sw2(config)# ntp server 192.168.10.254
sw2(config)#
```

2. ハードウェアクロックの定期的な同期を有効にします。

```
sw2(config)# ntp update-calendar
sw2(config)#
```

3. NTP サービスを有効にします。

```
sw2(config)# service ntp
sw2(config)# end
sw2#
```

4. 実施後、しばらくして時刻同期した後の NTP の状態を確認します。

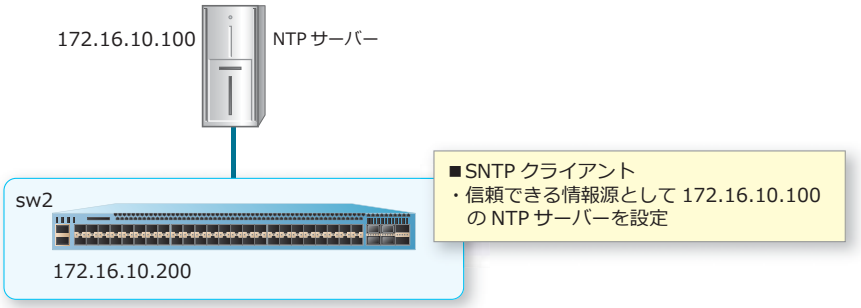
```
sw2# show ntp status

Leap Indicator:       Synchronized
Stratum:              4
Precision:            -22
Root Distance:        0.00000 s
Root Dispersion:      0.95081 s
Reference ID:         [192.168.10.254]
Reference Time:       e29da313.900b996b  Wed, Jun 24 2020 19:01:55.562
System Flags:         Auth Monitor NTP Kernel Stats
Jitter:               0.002884 s
Stability:            0.000 ppm
Auth Delay:           0.000000 s
```

8.3.2 SNTP を使用する場合

SNTP を使用する場合の構成例と設定例を示します。本設定例では、VLAN や IP アドレスの設定は省略しています。

sw1 は時刻を問い合わせる NTP サーバーとして 172.16.10.100 を指定して、SNTP クライアント機能を有効にしています。

図 8-3 SNTP を使用する場合の構成例



1. NTP サーバー［172.16.10.100］宛てに時刻問い合わせを行うように設定します。

```
sw1# configure terminal
sw1(config)# sntp server 172.16.10.100
sw1(config)#
```

2. SNTP クライアント機能を有効にします。

```
sw1(config)# sntp enable
sw1(config)# end
sw1#
```

3. 実施後、しばらくして時刻同期した後の SNTP の状態を確認します。

```
sw1# show sntp

SNTP Status                : Enabled
SNTP Poll Interval         : 720 seconds

SNTP Server Status:

SNTP Server                                        Stratum Version Last Receive
-------------------------------------------------- ------- ------- ---------------
172.16.10.100                                      11      1       00:01:18 Synced
-------------------------------------------------- ------- ------- ---------------
Total Entries: 1
```

9. SSH/Telnet

SSH/Telnet の機能、状態の確認方法、および構成例と設定例について説明します。

REF: コマンドの詳細については、『コマンドリファレンス』を参照してください。

9.1 SSH/Telnet の機能説明

SSH/Telnet の機能、および SSH/Telnet で装置に接続するための設定について説明します。

NOTE: SSH の最大セッション数は、マネージメントポート専用が 1、それ以外が 8 です。

NOTE: NP7000、NP4000、NP2100、NP2000、および NP2500 では、Telnet の最大セッション数は、マネージメントポート専用が 1、それ以外が 8 です。

NOTE: NP5000 および NP3000 では、Telnet の最大セッション数は 8 です。

9.1.1 SSH の機能説明

SSH は、暗号や認証を利用して装置（SSH サーバー）と SSH クライアントが安全に通信するためのプロトコルです。SSH では、パスワードなどを含め、すべての通信が暗号化されます。

9.1.1.1 SSH サーバーの設定

SSH サーバーの設定について、以下に説明します。

NOTE: 鍵交換方式、暗号化方式、メッセージ認証符号の設定は、NP7000 の 1.10.02 以降、NP3000 の 1.10.01 以降、NP2100 の 1.11.01 以降、NP2500 の 1.12.01 以降でサポートしています。

SSH サーバーの有効化

装置に SSH で接続するには、SSH サーバーを有効化します。デフォルト設定では無効です。SSH サーバーを有効化するには、**`ip ssh server`** コマンドを使用します。

SSH プロトコルの TCP ポート番号

SSH プロトコルの TCP ポート番号のデフォルト設定は 22 です。SSH プロトコルの TCP ポート番号を変更するには、**`ip ssh service-port`** コマンドを使用します。

SSH 接続のネゴシエーション時の応答待ち時間

SSH 接続のネゴシエーション時のクライアントからの応答待ち時間は、デフォルト設定では 120 秒です。応答待ち時間を変更するには、**`ip ssh timeout`** コマンドを使用します。

SSH 認証の再試行回数の変更

SSH 認証の再試行回数のデフォルト設定は 3 回です。SSH 認証の再試行回数を変更するには、**`ip ssh authentication-retries`** コマンドを使用します。

鍵交換方式の有効／無効

鍵交換方式（Key exchange algorithms）の有効／無効を設定できます。デフォルト設定ではすべて有効です。鍵交換方式の有効／無効を変更するには、**`ip ssh key-exchange enable`** コマンドを使用します。

暗号化方式の有効／無効

暗号化方式（Cipher algorithms）の有効／無効を設定できます。デフォルト設定ではすべて有効です。暗号化方式の有効／無効を変更するには、**ip ssh cipher enable** コマンドを使用します。

メッセージ認証符号の有効／無効

メッセージ認証符号（Message Authentication Code）の有効／無効を設定できます。デフォルト設定ではすべて有効です。メッセージ認証符号の有効／無効を変更するには、**ip ssh mac enable** コマンドを使用します。

9.1.1.2 SSH サーバー認証の設定

SSH サーバー認証のために、あらかじめ SSH サーバーのホストキー（RSA 鍵対／ DSA 鍵対）を作成しておく必要があります。ApresiaNP シリーズでは、RSA 鍵対／ DSA 鍵対のどちらも「SSH プロトコル version2」でのみ使用できます。

SSH サーバーの RSA 鍵対を作成する場合は **crypto key generate rsa** コマンドを、DSA 鍵対を作成する場合は **crypto key generate dsa** コマンドを使用します。また、SSH サーバーの RSA 鍵対を削除する場合は **crypto key zeroize rsa** コマンドを、DSA 鍵対を削除する場合は **crypto key zeroize dsa** コマンドを使用します。

9.1.1.3 SSH ユーザー認証の設定

SSH ユーザー認証方式には、**パスワード認証方式**、**公開鍵認証方式**、および**ホストベース認証方式**があります。それぞれの SSH ユーザー認証方式の設定について、以下に説明します。

パスワード認証方式の設定

SSH ユーザー認証のデフォルト設定はパスワード認証方式です。ログインする際にユーザー名とパスワードを入力し、許可されたアカウントの場合にログインできます。他の認証方式に設定している状態からパスワード認証方式に変更するには、password パラメーターを指定して **ssh user authentication-method** コマンドを使用します。

公開鍵認証方式の設定

SSH ユーザー認証で公開鍵認証方式を使用する場合、SSH クライアントで公開鍵対を生成し、SSH サーバーにクライアントの公開鍵を保存しておきます。公開鍵認証方式に変更するには、publickey パラメーターとクライアントの公開鍵を指定して **ssh user authentication-method** コマンドを使用します。

ホストベース認証方式の設定

SSH ユーザー認証でホストベース認証方式を使用するには、SSH クライアントでホスト鍵を生成し、SSH サーバーにホスト鍵を保存しておきます。ホストベース認証方式に変更するには、hostbased パラメーターとクライアントのホスト鍵およびホスト名を指定して **ssh user authentication-method** コマンドを使用します。

9.1.1.4 AAA 無効時の SSH のアクセス設定

AAA が無効（**no aaa new-model**）で認証方式がパスワード認証の場合、SSH アクセスは **login** コマンドの設定によって以下の認証ルールが適用されます。いずれの場合も、**username** コマンドでユーザー名の設定が必要です。

- **login コマンドが local 指定で有効設定の場合（login local）**

  ローカルのユーザーアカウント（**username** コマンドで設定したユーザー名とパスワード）でログインします。

- **login コマンドが有効設定の場合（login）**

  username コマンドで設定したユーザー名と、SSH ライン設定モードの **password** コマンドで設定したパスワードを入力すると、レベル 1 の特権レベルでログインします。

- **login コマンドが無効設定の場合（no login）**

  認証時にパスワードが無視されます。**username** コマンドで設定したユーザー名と、パスワードとして任意の文字列を入力すると、レベル 1 の特権レベルでログインします。

9.1.2 Telnet の機能説明

ホストから装置に Telnet で接続する場合の設定方法を説明します。

9.1.2.1 Telnet サーバーの設定

Telnet サーバーの設定について、以下に説明します。

Telnet サーバーの有効化

装置に Telnet で接続するには、Telnet サーバーを有効化します。Telnet サーバーは、デフォルト設定で有効です。Telnet サーバーが無効な状態から有効化するには、**ip telnet server** コマンドを使用します。

Telnet のサービスポートの変更

Telnet プロトコルのウェルノウン TCP ポートは 23 です。Telnet プロトコル用のサービスポートを変更するには、**ip telnet service-port** コマンドを使用します。

9.1.2.2 Telnet クライアントの設定

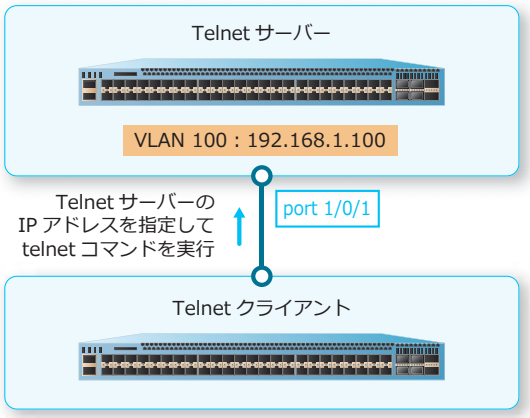
Telnet クライアントから装置に Telnet で接続する場合、Telnet 接続で使用するインターフェースを指定します。

Telnet 接続で使用するインターフェースは、デフォルト設定では接続先に最も近いインターフェースの IP アドレスです。Telnet 接続で使用するインターフェースを指定するには、**ip telnet source-interface** コマンドを使用します。指定したインターフェースの IP アドレスが Telnet パケットの送信元アドレスとして使用されます。

9.1.2.3 Telnet 接続の実行

装置を Telnet クライアントとして別の装置の Telnet サーバーへ接続するには、**`telnet`** コマンドを使用します。

図 9-1 Telnet 接続の実行



9.1.2.4 AAA 無効時の Telnet のアクセス設定

AAA が無効（**`no aaa new-model`**）の場合、Telnet アクセスは **`login`** コマンドの設定によって以下の認証ルールが適用されます。

- **`login` コマンドが local 指定で有効設定の場合（login local）**

  ローカルのユーザーアカウント（**`username`** コマンドで設定したユーザー名とパスワード）でログインします。

- **`login` コマンドが有効設定の場合（login）**

  Telnet ライン設定モードの **`password`** コマンドで設定したパスワードを入力すると、レベル 1 の特権レベルでログインします。

- **`login` コマンドが無効設定の場合（no login）**

  ユーザー名とパスワードの入力なしで、レベル 1 の特権レベルでログインします。

9.1.3 SSH/Telnet 接続の制限

SSH/Telnet 接続による装置へのアクセスを許可する端末を制限できます。アクセスを許可する端末の IP アドレスを定義したアクセスリストを **`ip access-list`** コマンドまたは **`ipv6 access-list`** コマンドで作成し、アクセスリストを **`access-class`** コマンドで指定します。

> ***CAUTION:*** 本設定で指定する標準 IP アクセスリスト、または標準 IPv6 アクセスリストでは、装置のハードウェアリソースを使用しません。

9.2 SSH/Telnet の状態確認

SSH/Telnet の状態を表示して確認する方法を説明します。

9.2.1 SSH の接続情報の表示

show ssh コマンドで SSH の接続情報を確認できます。

表示例を以下に示します。

```
# show ssh
(1) (2)  (3)                          (4)              (5)
SID Ver. Cipher                       Userid           Client IP Address
--- --- ---------------------------- ---------------- -------------------------
0   V2  3des-cbc/sha1-96              user1            192.168.0.100
1   V2  3des-cbc/hmac-sha1            user2            2000::243

Total Entries: 2
```

各項目の説明は、以下のとおりです。

表 9-1 show ssh コマンドの表示項目

項番	説明
(1)	SSH セッションを識別する一意の番号を表示します。
(2)	SSH のバージョンを表示します。
(3)	使用している暗号化方式とメッセージ認証符号を表示します。
(4)	ログインユーザー名を表示します。
(5)	SSH クライアントの IP アドレスを表示します。

9.2.2 SSH サーバーの設定の表示

show ip ssh コマンドで SSH サーバーの設定を確認できます。

表示例を以下に示します。

```
# show ip ssh

IP SSH server              : Enabled...(1)
IP SSH service port        : 22...(2)
SSH server mode            : V2...(3)
Authentication timeout     : 120 secs...(4)
Authentication retries     : 3 times...(5)
```

各項目の説明は、以下のとおりです。

表 9-2 show ip ssh コマンドの表示項目

項番	説明
(1)	SSH サーバーの有効 (Enabled) ／無効 (Disabled) を表示します。
(2)	SSH の TCP ポート番号を表示します。
(3)	SSH サーバーのバージョンを表示します。
(4)	認証タイムアウト時間を表示します。
(5)	認証リトライ回数を表示します。

9.2.3 鍵交換方式、暗号化方式、メッセージ認証符号の設定の表示

show ssh algorithm コマンドで、鍵交換方式の各アルゴリズムの有効／無効、暗号化方式の各アルゴリズムの有効／無効、各メッセージ認証符号の有効／無効を確認できます。

> ***NOTE:*** 鍵交換方式、暗号化方式、メッセージ認証符号の設定は、NP7000 の 1.10.02 以降、NP3000 の 1.10.01 以降、NP2100 の 1.11.01 以降、NP2500 の 1.12.01 以降でサポートしています。

表示例を以下に示します。

```
# show ssh algorithm

Key Exchange ...(1)                        State ...(2)
-----------------------------------------  --------
diffie-hellman-group1-sha1                 Enabled
diffie-hellman-group14-sha1                Enabled
diffie-hellman-group14-sha256              Enabled
diffie-hellman-group16-sha512              Enabled
diffie-hellman-group18-sha512              Enabled
diffie-hellman-group-exchange-sha1         Enabled
diffie-hellman-group-exchange-sha256       Enabled
ecdh-sha2-nistp256                         Enabled
ecdh-sha2-nistp384                         Enabled
ecdh-sha2-nistp521                         Enabled
curve25519-sha256                          Enabled
curve25519-sha256@libssh.org               Enabled

Cipher ...(3)                              State ...(4)
-----------------------------------------  --------
3des-cbc                                   Enabled
aes128-cbc                                 Enabled
aes192-cbc                                 Enabled
aes256-cbc                                 Enabled
aes128-ctr                                 Enabled
aes192-ctr                                 Enabled
aes256-ctr                                 Enabled
arcfour                                    Enabled
blowfish-cbc                               Enabled
cast128-cbc                                Enabled
aes128-gcm@openssh.com                     Enabled
aes256-gcm@openssh.com                     Enabled
chacha20-poly1305@openssh.com              Enabled
twofish-cbc                                Enabled
twofish256-cbc                             Enabled
twofish192-cbc                             Enabled
twofish128-cbc                             Enabled

Message Authentication Code ...(5)         State ...(6)
-----------------------------------------  --------
hmac-sha1                                  Enabled
hmac-sha1-96                               Enabled
hmac-sha2-256                              Enabled
hmac-sha2-512                              Enabled
hmac-md5                                   Enabled
hmac-md5-96                                Enabled
umac-64@openssh.com                        Enabled
umac-128@openssh.com                       Enabled
hmac-sha1-etm@openssh.com                  Enabled
hmac-sha1-96-etm@openssh.com               Enabled
hmac-sha2-256-etm@openssh.com              Enabled
hmac-sha2-512-etm@openssh.com              Enabled
hmac-md5-etm@openssh.com                   Enabled
hmac-md5-96-etm@openssh.com                Enabled
umac-64-etm@openssh.com                    Enabled
umac-128-etm@openssh.com                   Enabled

Public Key Algorithm ...(7)
-----------------------------------------
ssh-rsa
ssh-dss
```

各項目の説明は、以下のとおりです。

表 9-3 `show ssh algorithm` コマンドの表示項目

項番	説明
(1)	鍵交換方式（Key exchange algorithms）を表示します。
(2)	各鍵交換方式の有効 (Enabled) ／無効 (Disabled) を表示します。
(3)	暗号化方式（Cipher algorithms）を表示します。
(4)	各暗号化方式の有効 (Enabled) ／無効 (Disabled) を表示します。
(5)	メッセージ認証符号（Message Authentication Code）を表示します。
(6)	各メッセージ認証符号の有効 (Enabled) ／無効 (Disabled) を表示します。
(7)	公開鍵アルゴリズム（Public Key Algorithm）を表示します。

9.2.4 SSH サーバーのホストキーの表示

`show crypto key mypubkey` コマンドで SSH サーバーの RSA 鍵、または DSA 鍵を確認できます。

SSH サーバーの RSA 鍵の表示例を以下に示します。

```
# show crypto key mypubkey rsa

% Key pair was generated at: 13:02:23, 2024-07-23 ...(1)
Key Size: 2048 bits ...(2)
Key Data: ...(3)
AAAAB3Nz aC1yc2EA AAADAQAB AAABAQD2 tE2iMT+e urUzKLjr 2xx1DENl jPdk3W4Z
6Mpg5btT haFksJfr +JRfbkq+ cMt4zOur /vO5etKR NdsTuHco czdo8M/6 kvPYQlp3
j0+uyPaU bYxRHdrY mZs+lVP9 xUZnf9IE t2CB11FF GSq9deIP mKtZsCn+ nfHo6DMf
iMAuJy4O TK/3gFY0 Qpsp8G3o PdEK5gKu n2iKnLEh F4ZXni3p OYnVJsj9 bE9jlbT1
yB5dtad+ wcy0Ko85 F2THjcJ/ 5+nKsk0Z XjHVm2m8 MVXet39h aVHj9Krz I9LU6L18
BWnyzVCc eY1Wh9Ft UkrzKnY+ XapB15aH 8UuyeTF4 PJQ6Uy15 R/cL
```

各項目の説明は、以下のとおりです。

表 9-4 `show crypto key mypubkey rsa` コマンドの表示項目

項番	説明
(1)	RSA 鍵対が生成された日時を表示します。 **`restore`** コマンドを実行して装置を起動し直した後は、**`restore`** コマンド実行時の時刻（RSA 鍵が置き換えられた時刻）に変更されます。 SD カードブートで起動した場合は、RSA 鍵が置き換えられた起動時の時刻に変更されます。なお、この場合は UTC 時刻が記録されます。
(2)	RSA 鍵の鍵長を表示します。
(3)	RSA 鍵の情報を表示します。

SSH サーバーの DSA 鍵の表示例を以下に示します。

```
# show crypto key mypubkey dsa

% Key pair was generated at: 14:55:01, 2020-06-02 ...(1)
Key Size: 1024 bits ...(2)
Key Data: ...(3)
AAAAB3Nz aC1kc3MA AACBAL7+ Pi0IEeTE 57pUbmuy XfyUultm T1IP/vvP ebFLRMRF
57gyjM/v RUpipRs5 zz4xOuyl 5gT5Jfkm wyfhPUsJ mA3wW3U4 fMYCHoHx qzGYRey1
/uIce7wU vORSLc/o kgRDYbfu AvvvMqCh Hn72k1n/ D6ftT324 kHfVymGg 4GQ/ICwP
AAAAFQDM cz4dZV/Q Tv/QbTj8 oZTLiRpb FwAAAIEA gS1wH5Jf 8FngnwDg 21QfXRGW
40MoIO4H h+g6E1MF NdFxruOf QG3++sj0 rcEMsqpW T2lqu5zF K4n5J6tj YD1Ep7fn
2Q+vidj7 A9PFI5KQ x1aASrQA AedExUMQ zpuXA94/ jJbNR3TM MKC/YtkK S0Vd3sUF
QyiAjV8t RG7gT2mH Gp8AAACB AKBCupVR +XyOtk53 6HFqp6gZ wHygUgNq ue5m6XIn
yG6zFgln j78yf0q2 7HqfXRlh lWDjKisx d8makEme u/ecwoTN fWFfxC7j V0Qvfzdz
MrtHSca9 AFenLAw7 PX9eNieh 73D8G8PW ws9FT+C0 EkBtA7ly uJrqj4/D +FnLH7dy
PfXD
```

各項目の説明は、以下のとおりです。

表 9-5 `show crypto key mypubkey dsa` コマンドの表示項目

項番	説明
(1)	DSA 鍵対が生成された日時を表示します。 **`restore`** コマンドを実行して装置を起動し直した後は、**`restore`** コマンド実行時の時刻（DSA 鍵が置き換えられた時刻）に変更されます。 SD カードブートで起動した場合は、DSA 鍵が置き換えられた起動時の時刻に変更されます。なお、この場合は UTC 時刻が記録されます。
(2)	DSA 鍵の鍵長を表示します。DSA の場合は 1024 ビット固定です。
(3)	DSA 鍵の情報を表示します。

9.2.5 Telnet サーバーの設定の表示

show ip telnet server コマンドで Telnet サーバーの設定を確認できます。

表示例を以下に示します。

```
# show ip telnet server

Server State: Enabled ...(1)
```

各項目の説明は、以下のとおりです。

表 9-6 show ip telnet server コマンドの表示項目

項番	説明
(1)	Telnet サーバーの有効 (Enabled) ／無効 (Disabled) を表示します。

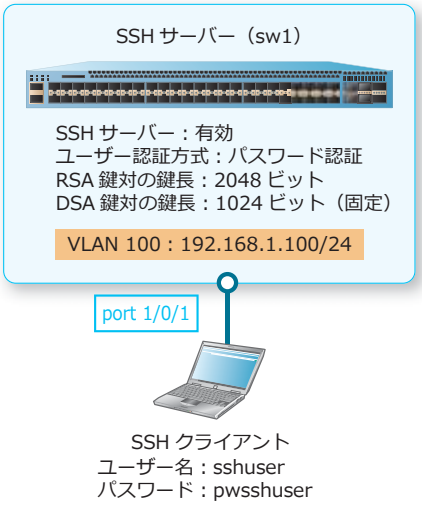
9.3 SSH/Telnet の構成例と設定例

SSH/Telnet で装置に接続する場合の構成例と設定例を示します。

9.3.1 SSH 接続をパスワード認証方式で行う場合

AAA が無効な装置において、パスワード認証方式で SSH 接続する場合の構成例と設定例を示します。
なお、SSH サーバー（sw1）では「鍵長 2048 ビットの RSA 鍵対」と「DSA 鍵対」を生成します。

図 9-2 SSH 接続をパスワード認証方式で行う場合の構成例



1. SSH 接続で使用する VLAN 100 を作成し、ポート 1/0/1 をアクセスポートとして［VLAN 100］を割り当てます。また、VLAN 100 の IP アドレスを［192.168.1.100/24］に設定します。

```
sw1# configure terminal
sw1(config)# vlan 100
sw1(config-vlan)# exit
sw1(config)# interface port 1/0/1
sw1(config-if-port)# switchport mode access
sw1(config-if-port)# switchport access vlan 100
sw1(config-if-port)# exit
sw1(config)# interface vlan 100
sw1(config-if-vlan)# ip address 192.168.1.100/24
sw1(config-if-vlan)# exit
sw1(config)#
```

2. SSH クライアントのユーザーアカウントとして、ユーザー名を［sshuser］に、パスワードを［pwsshuser］に設定します。また、設定したユーザーアカウントを使用するために、SSH ライン設定モードでローカル認証［local］を設定します。

```
sw1(config)# username sshuser password pwsshuser
sw1(config)# line ssh
sw1(config-line)# login local
sw1(config-line)# exit
sw1(config)#
```

3. SSH サーバーを有効にします。また、ユーザー名［sshuser］の SSH 認証方式をパスワード認証方式に設定します。なお、**username** コマンドでユーザーアカウントを設定すると、そのユーザーアカウントに対応した ssh user authentication-method 設定がデフォルト設定で自動的に作成されます。

```
sw1(config)# ip ssh server
sw1(config)# ssh user sshuser authentication-method password
sw1(config)# end
sw1#
```

4. SSH サーバーの RSA 鍵対を鍵長［2048］ビットで生成します。

```
sw1# crypto key generate rsa modulus 2048

Generating RSA key...Done.

sw1#
```

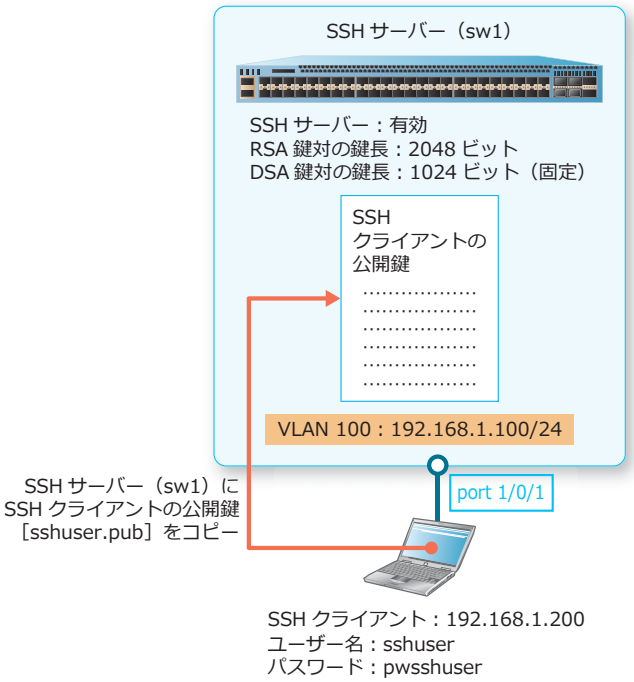
5. SSH サーバーの DSA 鍵対を生成します。

```
sw1# crypto key generate dsa

Generating DSA key...Done.

sw1#
```

9.3.2 SSH 接続を公開鍵認証方式で行う場合

AAA が無効な装置において、公開鍵認証方式で SSH 接続する場合の構成例と設定例を示します。なお、SSH サーバー（sw1）では「鍵長 2048 ビットの RSA 鍵対」と「DSA 鍵対」を生成します。

図 9-3 SSH 接続を公開鍵認証方式で行う場合の構成例



1. SSH 接続で使用する VLAN 100 を作成し、ポート 1/0/1 をアクセスポートとして［VLAN 100］を割り当てます。また、VLAN 100 の IP アドレスを［192.168.1.100/24］に設定します。

```
sw1# configure terminal
sw1(config)# vlan 100
sw1(config-vlan)# exit
sw1(config)# interface port 1/0/1
sw1(config-if-port)# switchport mode access
sw1(config-if-port)# switchport access vlan 100
sw1(config-if-port)# exit
sw1(config)# interface vlan 100
sw1(config-if-vlan)# ip address 192.168.1.100/24
sw1(config-if-vlan)# exit
sw1(config)#
```

2. SSH クライアントのユーザーアカウントとして、ユーザー名を［sshuser］に、パスワードを［pwsshuser］に設定します。また、設定したユーザーアカウントを使用するために、SSH ライン設定モードでローカル認証［local］を設定します。

```
sw1(config)# username sshuser password pwsshuser
sw1(config)# line ssh
sw1(config-line)# login local
sw1(config-line)# exit
sw1(config)#
```

3. SSH サーバーを有効にします。

```
sw1(config)# ip ssh server
sw1(config)# end
sw1#
```

4. SSH サーバーの RSA 鍵対を鍵長［2048］ビットで生成します。

```
sw1# crypto key generate rsa modulus 2048

Generating RSA key...Done.

sw1#
```

5. SSH サーバーの DSA 鍵対を生成します。

```
sw1# crypto key generate dsa

Generating DSA key...Done.

sw1#
```

6. SSH クライアントの公開鍵を SSH サーバー（sw1）にコピーします。なお、この例では TFTP サーバー［192.168.1.200］に SSH クライアントの公開鍵［id_rsa.pub］が保存されている前提で、TFTP サーバーからコピーしています。また、コピー後のファイル名は［sshuser.pub］としています。

```
sw1# copy tftp: flash:

Address of remote host []? 192.168.1.200
Source filename []? id_rsa.pub
Destination filename []? sshuser.pub
Accessing tftp://192.168.1.200/id_rsa.pub...
Transmission start...
Transmission finished, file length 234 bytes.
Please wait, programming flash.............. Done.
```

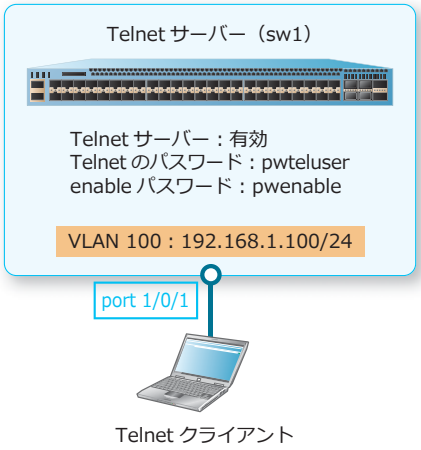
7. ユーザー名［sshuser］の SSH 認証方式を公開鍵認証方式に設定します。SSH クライアントの公開鍵のファイルパスは［c:/sshuser.pub］に設定します。

```
sw1# configure terminal
sw1(config)# ssh user sshuser authentication-method publickey c:/sshuser.pub
sw1(config)# end
sw1#
```

9.3.3 Telnet 接続を共通パスワードで行う場合

AAA が無効な装置において、共通パスワードを使用して、装置に Telnet 接続する場合の構成例と設定例を示します。

図 9-4 Telnet 接続を共通パスワードで行う場合の構成例



1. Telnet 接続で使用する VLAN 100 を作成し、ポート 1/0/1 をアクセスポートとして［VLAN 100］を割り当てます。また、VLAN 100 の IP アドレスを［192.168.1.100/24］に設定します。

```
sw1# configure terminal
sw1(config)# vlan 100
sw1(config-vlan)# exit
sw1(config)# interface port 1/0/1
sw1(config-if-port)# switchport mode access
sw1(config-if-port)# switchport access vlan 100
sw1(config-if-port)# exit
sw1(config)# interface vlan 100
sw1(config-if-vlan)# ip address 192.168.1.100/24
sw1(config-if-vlan)# exit
sw1(config)#
```

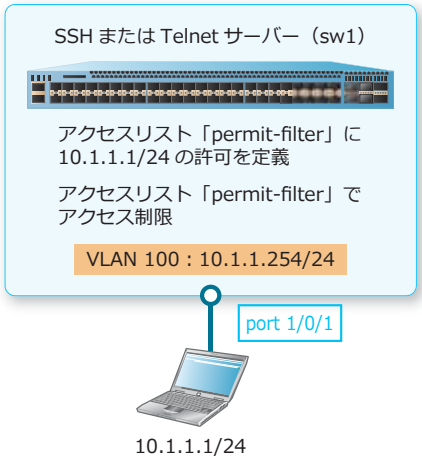
2. Telnet サーバーを有効にして、Telnet ライン設定モードで Telnet のパスワードを［pwteluser］に設定します。また、enable パスワードを［pwenable］に設定します。

```
sw1(config)# ip telnet server
sw1(config)# line telnet
sw1(config-line)# password pwteluser
sw1(config-line)# exit
sw1(config)# enable password pwenable
sw1(config)# end
sw1#
```

9.3.4 SSH/Telnet 接続でアクセスを許可する端末を制限する場合

SSH/Telnet 接続で、10.1.1.1/24 の端末にのみアクセスを許可する場合の構成例と設定例を示します。

図 9-5 SSH/Telnet でアクセスを許可する端末を制限する場合の構成例



NOTE: 以下の操作は、アクセスを許可する端末を制限するための手順です。SSH サーバーと Telnet サーバーの設定は、別途行ってください。

1. アクセスリスト［permit-filter］を作成し、［10.1.1.1 0.0.0.0］の許可を定義します。

```
sw1# configure terminal
sw1(config)# ip access-list permit-filter
sw1(config-ip-acl)# permit 10.1.1.1 0.0.0.0
sw1(config-ip-acl)# exit
sw1(config)#
```

2. SSH/Telnet 接続を制限するアクセスリスト［permit-filter］を適用します。

```
sw1(config)# line ssh
sw1(config-line)# access-class permit-filter
sw1(config-line)# exit
sw1(config)# line telnet
sw1(config-line)# access-class permit-filter
sw1(config-line)# end
sw1#
```

10. RADIUS/TACACS+

RADIUS/TACACS+ の機能、状態の確認方法、および構成例と設定例について説明します。

REF: コマンドの詳細については、『コマンドリファレンス』を参照してください。

10.1 RADIUS/TACACS+ の機能説明

RADIUS と **TACACS+** は、装置とホストの通信で **AAA**（認証／認可／アカウンティング）を実現するためのセキュリティープロトコルです。

AAA を実現するために、以下のサービスを実行します。

- **認証**

  ユーザーアカウントとパスワードを確認し、装置へのホストのアクセスを許可してよいかどうかを決定します。

- **認可**

  ユーザーごとに装置上で使用できるコマンドを制限します。

- **アカウンティング**

  装置にログインしたユーザーが使用したコマンド、接続時間、システムイベントなどにタイムスタンプを付加してログとして記録します。

RADIUS と TACACS+ を利用した AAA では、それぞれのプロトコルに対応した RADIUS サーバー／ TACACS+ サーバーで AAA の情報を一元管理します。装置は、ホストからのログインやコマンドの使用の要求が発生するたびに RADIUS サーバー／ TACACS+ サーバーに問い合わせ、ホストが装置上で実行する動作を制限します。

RADIUS または TACACS+ を利用するには、装置で AAA を有効にする必要があります。

10.1.1 AAA の各種設定

AAA の有効化、認証／認可／アカウンティングの設定、および AAA と RADIUS サーバー／ TACACS+ サーバーの関連付けについて、以下に説明します。

10.1.1.1 AAA の有効化

RADIUS または TACACS+ を利用するには、装置で AAA を有効にする必要があります。デフォルト設定では、AAA は無効です。AAA を有効にするには、**`aaa new-model`** コマンドを使用します。

AAA 機能を有効にすると、各ラインセッションへのログイン方法は **`aaa authentication login`** コマンドと **`login authentication`** コマンドによって決定されます。デフォルト設定の場合は、ログイン認証方式が「**`username`** コマンドで作成したユーザーアカウント」になります。

また、AAA 機能を有効にすると、enable パスワードの認証方式は **`aaa authentication enable`** コマンドによって決定されます。デフォルト設定の場合は、認証方式が「**`enable password`** コマンドで設定したパスワード」になります。

> ***NOTE:*** AAA 機能が有効、ログイン認証方式がデフォルト設定、かつ **`username`** コマンドで作成したユーザーアカウントがまだ存在しない状態では、コンソールの場合のみ「ユーザー名／パスワードを未入力で Enter 実施、または任意の文字列を入力して Enter 実施」でログインできます。

> ***NOTE:*** AAA 機能が有効、enable パスワードの認証方式がデフォルト設定、かつ **`enable password`** コマンドが未設定の状態では、コンソールの場合のみ「enable パスワードを未入力で Enter 実施、または任意の文字列を入力して Enter 実施」で特権レベル 15 に遷移できます。

10.1.1.2 ログイン認証

装置にログインする場合、デフォルト設定では **username** コマンドで作成したユーザーアカウントで認証します。

ログイン認証の認証方式を設定するには、**aaa authentication login** コマンドで以下の認証方式を指定して認証方式リストを設定します。また、**login authentication** コマンドで認証方式リストを各ラインセッションに適用します。

- **local**

  username コマンドで作成したユーザーアカウント

- **group radius**

  radius-server host コマンドで設定したすべての RADIUS サーバー

- **group tacacs+**

  tacacs-server host コマンドで設定したすべての TACACS+ サーバー

- **group グループ名**

  aaa group server radius コマンドで設定した RADIUS サーバーグループに登録されている RADIUS サーバー、または **aaa group server tacacs+** コマンドで設定した TACACS+ サーバーグループに登録されている TACACS+ サーバー

- **none**

  認証なしで許可する

10.1.1.3 enable パスワードの認証方式

enable パスワードは、デフォルト設定では **enable password** コマンドで設定したパスワードで認証します。

enable パスワードの認証方式を設定するには、**aaa authentication enable default** コマンドで以下の認証方式を指定して認証方式リストを設定します。

- **enable**

  enable password コマンドで設定したパスワード

- **group radius**

  radius-server host コマンドで設定したすべての RADIUS サーバー

- **group tacacs+**

  tacacs-server host コマンドで設定したすべての TACACS+ サーバー

- **group グループ名**

  aaa group server radius コマンドで設定した RADIUS サーバーグループに登録されている RADIUS サーバー、または **aaa group server tacacs+** コマンドで設定した TACACS+ サーバーグループに登録されている TACACS+ サーバー

- **none**

  認証なしで許可する

10.1.1.4 アカウンティングの設定

装置にログインしたホストが使用したコマンド、ホストの接続時間、発生したシステムイベントなどにタイムスタンプを付加してログとして記録するには、アカウンティングを設定します。デフォルト設定ではアカウンティングは無効です。

アカウンティングの設定では、以下のアカウンティング方式を指定できます。

- **group radius**

  radius-server host コマンドで設定したすべての RADIUS サーバー

- **group tacacs+**

  tacacs-server host コマンドで設定したすべての TACACS+ サーバー

- **group グループ名**

  aaa group server radius コマンドで設定した RADIUS サーバーグループに登録されている RADIUS サーバー、または **aaa group server tacacs+** コマンドで設定した TACACS+ サーバーグループに登録されている TACACS+ サーバー

- **none**

  方式の指定なし

特権レベル内のコマンドのアカウンティングの設定

指定した特権レベル内のコマンドのアカウンティングを設定するには、**aaa accounting commands** コマンドでアカウンティング方式リストを設定します。また、**accounting commands** コマンドでアカウンティング方式リストを各ラインセッションに適用します。

> ***NOTE:*** 特権レベル内のコマンドのアカウンティングは、TACACS+ で実行できます。RADIUS では実行できません。方式には、group tacacs+、TACACS+ サーバーのグループ名、または none のいずれかを指定できます。

ユーザー EXEC ターミナルセッションのアカウンティングの設定

ユーザー EXEC ターミナルセッションのアカウンティングを設定するには、**aaa accounting exec** コマンドでアカウンティング方式リストを設定します。また、**accounting exec** コマンドでアカウンティング方式リストを各ラインセッションに適用します。

システムイベントのアカウンティングの設定

システムイベントのアカウンティングを設定するには、**aaa accounting system** コマンドでアカウンティング方式リストを設定します。

AccessDefender のアカウンティングの設定

AccessDefender のアカウンティングを設定するには、**aaa accounting network** コマンドでアカウンティング方式リストを設定します。

10.1.1.5 サーバーグループの設定

認証方式リストとアカウンティング方式リストで使用するサーバーグループを設定するには、RADIUS サーバーグループの場合は **aaa group server radius** コマンドを、TACACS+ サーバーグループの場合は **aaa group server tacacs+** コマンドを使用します。

サーバーグループは、RADIUS サーバーグループと TACACS+ サーバーグループを合わせて最大 8 グループまで設定できます。なお、8 グループには 2 つのデフォルトのサーバーグループ「radius」「tacacs+」も含まれます。

1 つの RADIUS サーバーグループには、最大 16 個の RADIUS サーバーを登録できます。また、1 つの TACACS+ サーバーグループには、最大 16 個の TACACS+ サーバーを登録できます。

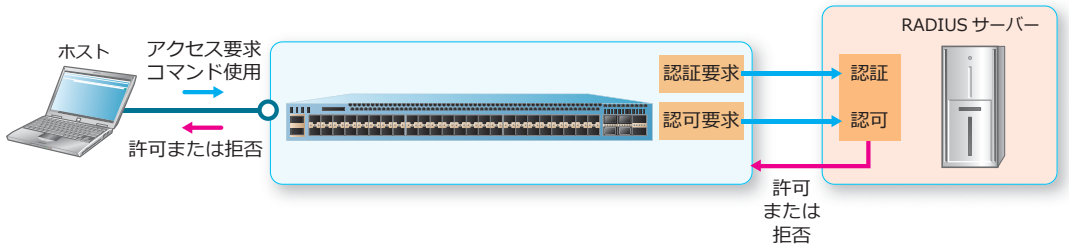
10.1.1.6 サーバーの統計情報の消去

認証とアカウンティングで使用するサーバーの統計情報を消去するには、**clear aaa counters servers** コマンドを使用します。

10.1.2 RADIUS の機能説明

RADIUS は、装置に接続するホストを認証および認可するセキュリティープロトコルです。RADIUS プロトコルに対応した RADIUS サーバーには AAA の情報が登録されています。ホストから装置へのアクセスが発生するたび、装置は RADIUS サーバーに問い合わせを行います。RADIUS サーバーは、ホストの接続やコマンド使用の許可または拒否を決定し、装置に返信します。

図 10-1 RADIUS サーバーの機能



10.1.2.1 RADIUS パケットの送信元インターフェースの設定

装置が RADIUS パケットを送信するインターフェースを設定します。RADIUS パケットを送信するインターフェースは、デフォルト設定では RADIUS サーバーに最も近い IP アドレスが設定されています。

装置が RADIUS パケットを送信するインターフェースを設定するには、IPv4 の場合は **ip radius source-interface** コマンド、IPv6 の場合は **ipv6 radius source-interface** コマンドを使用します。

10.1.2.2 RADIUS サーバーのデッドタイムの設定

問い合わせした RADIUS サーバーからの応答がない場合に、その RADIUS サーバーをオフラインとみなす期間（デッドタイム）を設定します。オフラインと判断された RADIUS サーバーには、デッドタイムが満了するまで問い合わせは行われません。デッドタイムが満了すると、再び問い合わせ候補になります。

RADIUS サーバーをオフラインとみなす期間（デッドタイム）を設定するには、**radius-server deadtime** コマンドを使用します。

10.1.2.3 RADIUS サーバーの IP アドレスと共有鍵（Shared Secret）の設定

RADIUS サーバーの IP アドレスと共有鍵（Shared Secret）を設定します。デフォルト設定では、RADIUS サーバーは設定されていません。RADIUS サーバーは TACACS+ サーバーと合わせて 16 台まで設定できます。

RADIUS サーバーの IP アドレスと共有鍵（Shared Secret）を設定するには、**`radius-server host`** コマンドを使用します。

10.1.2.4 RADIUS サーバーグループに登録する RADIUS サーバーの設定

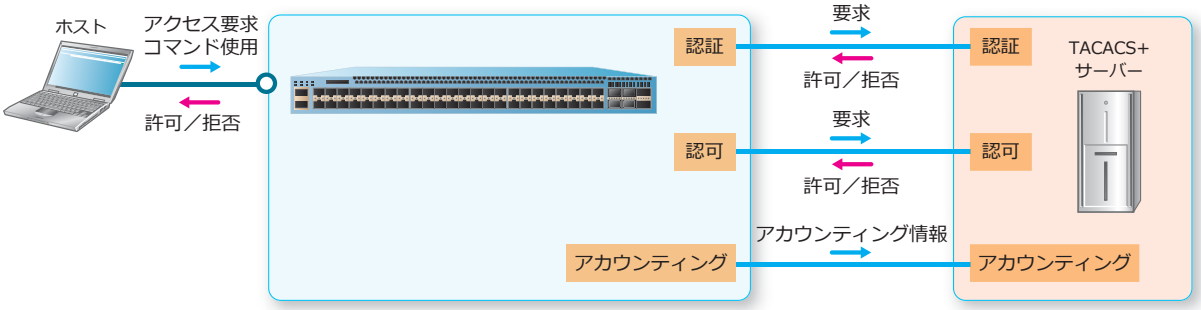
任意に作成した RADIUS サーバーグループに RADIUS サーバーを登録します。デフォルト設定では、RADIUS サーバーは登録されていません。

任意の RADIUS サーバーグループを作成するには、**`aaa group server radius`** コマンドを使用します。任意に作成した RADIUS サーバーグループに RADIUS サーバーを登録するには、**`server`** コマンドを使用します。

10.1.3 TACACS+ の機能説明

TACACS+ は、AAA の認証、認可、およびアカウンティングのそれぞれを独立したサービスとして個別に利用できるセキュリティープロトコルです。TACACS+ プロトコルに対応した TACACS+ サーバーには、AAA の認証、認可、およびアカウンティングのそれぞれの情報が、個別のデータベースに記録されています。これにより、認証だけを利用したり、認可だけを利用したりできます。

図 10-2 TACACS+ サーバーの機能



10.1.3.1 TACACS+ パケットの送信元インターフェースの設定

装置が TACACS+ パケットを送信するインターフェースを設定します。TACACS+ パケットを送信するインターフェースは、デフォルト設定では TACACS+ サーバーに最も近い IP アドレスが設定されています。

装置が TACACS+ パケットを送信するインターフェースを設定するには、**`ip tacacs source-interface`** コマンドを使用します。

10.1.3.2 TACACS+ サーバーの IP アドレスと共有鍵（Shared Secret）の設定

TACACS+ サーバーの IP アドレスと共有鍵（Shared Secret）を設定します。デフォルト設定では、TACACS+ サーバーは設定されていません。TACACS+ サーバーは RADIUS サーバーと合わせて 16 台まで設定できます。

TACACS+ サーバーの IP アドレスと共有鍵（Shared Secret）を設定するには、**`tacacs-server host`** コマンドを使用します。

CAUTION: IPv6 アドレスは設定できません。

10.1.3.3 TACACS+ サーバーグループに登録する TACACS+ サーバーの設定

任意に作成した TACACS+ サーバーグループに TACACS+ サーバーを登録します。デフォルト設定では、TACACS+ サーバーは登録されていません。

任意の TACACS+ サーバーグループを作成するには、**aaa group server tacacs+** コマンドを使用します。任意に作成した TACACS+ サーバーグループに TACACS+ サーバーを登録するには、**server** コマンドを使用します。

10.2 RADIUS/TACACS+ の状態確認

RADIUS/TACACS+ の状態を表示して確認する方法を説明します。

10.2.1 AAA 機能の設定の表示

show aaa コマンドで AAA 機能の設定を確認できます。

表示例を以下に示します。

```
# show aaa

AAA is enabled....(1)
```

各項目の説明は、以下のとおりです。

表 10-1 show aaa コマンドの表示項目

項番	説明
(1)	AAA 機能の有効 (enabled) ／無効 (disabled) を表示します。

10.2.2 RADIUS サーバーの統計情報の表示

show radius statistics コマンドで RADIUS サーバーの状態を確認できます。

表示例を以下に示します。

```
# show radius statistics
                 (1)             (2)              (3)
 RADIUS Server: 10.249.23.119: Auth-Port 1812, Acct-Port 1813
 State is Up...(4)        (5)         (6)
                          Auth.       Acct
 Round Trip Time:         10          0...(7)
 Access Requests:         1           NA...(8)
 Access Accepts:          1           NA...(9)
 Access Rejects:          0           NA...(10)
 Access Challenges:       0           NA...(11)
 Acct Request:            NA          0...(12)
 Acct Response:           NA          0...(13)
 Retransmissions:         0           0...(14)
 Malformed Responses:     0           0...(15)
 Bad Authenticators:      0           0...(16)
 Pending Requests:        0           0...(17)
 Timeouts:                0           0...(18)
 Unknown Types:           0           0...(19)
 Packets Dropped:         0           0...(20)
```

各項目の説明は、以下のとおりです。

表 10-2 show radius statistics コマンドの表示項目

項番	説明
(1)	RADIUS サーバーの IP アドレスを表示します。
(2)	RADIUS サーバーの認証用の UDP ポート番号を表示します。

項番	説明
(3)	RADIUS サーバーのアカウンティング用の UDP ポート番号を表示します。
(4)	RADIUS サーバーの状態を表示します。 • Up：問い合わせ対象として使用可能な状態 • Down：オフラインとみなして、問い合わせ対象から除外している状態
(5)	認証パケットの統計情報を表示します。
(6)	アカウンティングパケットの統計情報を表示します。
(7)	RADIUS サーバーからの直近の応答と、応答と一致した要求との間の時間間隔（100 分の 1 秒単位）を表示します。
(8)	サーバーに送信された RADIUS アクセス要求パケットの数を表示します。再送されたパケットは含まれません。
(9)	サーバーから受信した RADIUS Access-Accept パケットの数を表示します。
(10)	サーバーから受信した RADIUS Access-Reject パケットの数を表示します。
(11)	サーバーから受信した RADIUS Access-Challenge パケットの数を表示します。
(12)	送信された RADIUS Accounting-Request パケットの数を表示します。再送されたパケットは含まれません。
(13)	アカウンティングポートで受信したサーバーからの RADIUS パケットの数を表示します。
(14)	RADIUS サーバーに再送された RADIUS 要求パケットの数を表示します。再送には、識別子と Acct-Delay が更新されたリトライ状態が同じままのリトライが含まれます。
(15)	サーバーから受信した誤った形式の RADIUS 応答パケットの数を表示します。長さが無効なパケットも数に含まれます。なお、誤った Authenticator、署名属性、または不明なタイプは、誤った形式の応答の数には含まれません。
(16)	サーバーから受信した無効な Authenticator または署名属性を含んだ RADIUS 応答パケットの数を表示します。
(17)	サーバー宛てでタイムアウト前または応答未受信の RADIUS 要求パケットの数を表示します。要求の送信によって増えます。また、要求の受信、タイムアウト、または再送によって減少します。
(18)	サーバーのタイムアウト回数を表示します。タイムアウト後のクライアントに想定される動作は、同じサーバーへのリトライ、別のサーバーへの送信、または断念のいずれかです。同じサーバーへのリトライは、再送とタイムアウトとしてカウントします。別のサーバーへの送信は、要求とタイムアウトとしてカウントします。
(19)	サーバーから受信したタイプ不明の RADIUS パケットの数を表示します。
(20)	サーバーから受信し、何らかの理由で廃棄された RADIUS パケットの数を表示します。

10.2.3 TACACS+ サーバーの統計情報の表示

show tacacs statistics コマンドで TACACS+ サーバーの状態を確認できます。

CAUTION: TACACS+ サーバーによる認証時のみ、カウントされます。

表示例を以下に示します。

```
# show tacacs statistics
                 (1)                (2)
TACACS+ Server: 10.249.22.182/49, State is Up
Socket Opens: 0...(3)
Socket Closes: 0...(4)
Total Packets Sent: 0...(5)
Total Packets Recv: 0...(6)
Reference Count: 0...(7)
```

各項目の説明は、以下のとおりです。

表 10-3 show tacacs statistics コマンドの表示項目

項番	説明
(1)	TACACS+ サーバーの IP アドレスを表示します。
(2)	TACACS+ サーバーの状態を表示します。
(3)	TACACS+ サーバーへの TCP ソケット接続に成功した回数を表示します。
(4)	TCP ソケットを閉じようとして成功した回数を表示します。
(5)	TACACS+ サーバーに送信されたパケットの数を表示します。
(6)	TACACS+ サーバーから受信したパケットの数を表示します。
(7)	TACACS+ サーバーからの認証要求の数を表示します。

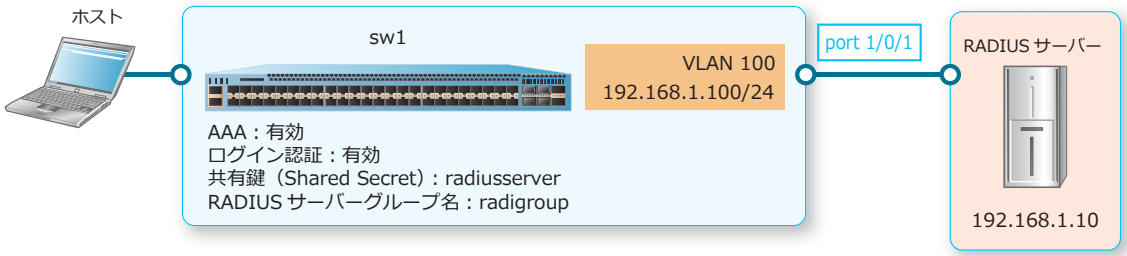
10.3 RADIUS/TACACS+ の構成例と設定例

RADIUS サーバーと TACACS+ サーバーを利用する場合の構成例と設定例を示します。

10.3.1 RADIUS サーバーの構成例と設定例

装置で RADIUS サーバーを利用する場合の構成例と設定例を示します。

図 10-3 RADIUS サーバーの構成例



1. VLAN 100 を作成し、ポート 1/0/1 をアクセスポートとして［VLAN 100］を割り当てます。また、VLAN 100 の IP アドレスを［192.168.1.100/24］に設定します。

```
sw1# configure terminal
sw1(config)# vlan 100
sw1(config-vlan)# exit
sw1(config)# interface port 1/0/1
sw1(config-if-port)# switchport mode access
sw1(config-if-port)# switchport access vlan 100
sw1(config-if-port)# exit
sw1(config)# interface vlan 100
sw1(config-if-vlan)# ip address 192.168.1.100/24
sw1(config-if-vlan)# exit
sw1(config)#
```

2. 装置の AAA を有効化します。また、RADIUS サーバーグループのデフォルトの認証方式リストを指定し、ログイン認証を有効化します。

```
sw1(config)# aaa new-model
sw1(config)# aaa authentication login default group radius none
```

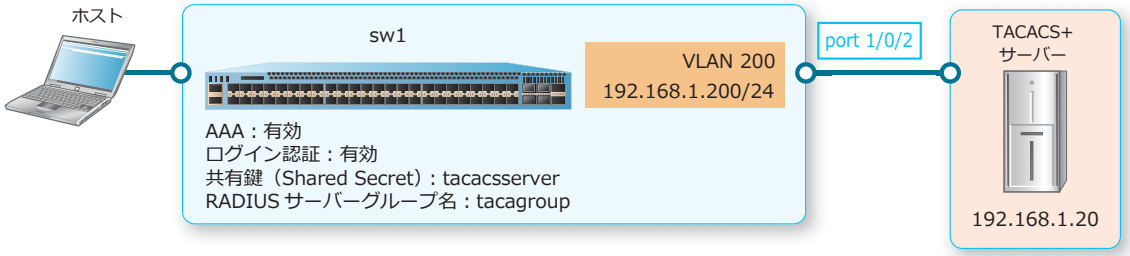
3. RADIUS パケットの送信元インターフェースとして［VLAN 100］を設定します。また、RADIUS サーバーの IP アドレス［192.168.1.10］と共有鍵［radiusserver］を設定し、RADIUS サーバーグループを［radigroup］に設定して RADIUS サーバーを登録します。

```
sw1(config)# ip radius source-interface vlan 100
sw1(config)# radius-server host 192.168.1.10 key radiusserver
sw1(config)# aaa group server radius radigroup
sw1(config-sg-radius)# server 192.168.1.10
sw1(config-sg-radius)# end
sw1#
```

10.3.2 TACACS+ サーバーの構成例と設定例

装置で TACACS+ サーバーを利用する場合の構成例と設定例を示します。

図 10-4 TACACS+ サーバーの構成例



1. VLAN 200 を作成し、ポート 1/0/2 をアクセスポートとして［VLAN 200］を割り当てます。また、VLAN 200 の IP アドレスを［192.168.1.200］に設定します。

```
sw1# configure terminal
sw1(config)# vlan 200
sw1(config-vlan)# exit
sw1(config)# interface port 1/0/2
sw1(config-if-port)# switchport mode access
sw1(config-if-port)# switchport access vlan 200
sw1(config-if-port)# exit
sw1(config)# interface vlan 200
sw1(config-if-vlan)# ip address 192.168.1.200/24
sw1(config-if-vlan)# exit
sw1(config)#
```

2. 装置の AAA を有効化します。また、TACACS+ サーバーグループのデフォルトの認証方式リストを指定してログイン認証を有効化します。

```
sw1(config)# aaa new-model
sw1(config)# aaa authentication login default group tacacs+ none
```

3. TACACS+ パケットの送信元インターフェースとして［VLAN 200］を設定します。また、TACACS+ サーバーの IP アドレス［192.168.1.20］と共有鍵［tacacsserver］を設定し、TACACS+ サーバーグループを［tacagroup］に設定して TACACS+ サーバーを登録します。

```
sw1(config)# ip tacacs source-interface vlan 200
sw1(config)# tacacs-server host 192.168.1.20 key tacacsserver
sw1(config)# aaa group server tacacs+ tacagroup
sw1(config-sg-tacacs+)# server 192.168.1.20
sw1(config-sg-tacacs+)# end
sw1#
```

11. システムファイル

システムファイルの機能、仕様と動作、状態の確認方法、および実施例について説明します。

REF: コマンドの詳細については、『コマンドリファレンス』を参照してください。

11.1 システムファイルの機能説明

装置を動作させるためのシステムファイルには、**構成情報**と**ブートイメージファイル**があります。

11.1.1 構成情報

装置の設定を変更すると、running-config に反映されます。装置の設定を保存すると、running-config の内容が startup-config に保存されます。設定を保存するには、**`write memory`** コマンドを使用します。

`write memory` コマンドは、running-config をプライマリーで指定した構成情報ファイルにのみ上書き保存します。running-config をセカンダリーで指定した構成情報ファイルに上書き保存する場合は、**`write memory secondary`** コマンドを使用してください。また、**`copy primary-config secondary-config`** コマンドを使用すると、プライマリーで指定した構成情報ファイルをセカンダリーで指定した構成情報ファイルに上書き保存できます。

> ***NOTE:*** **`write memory`** コマンドおよび **`copy running-config startup-config`** コマンドは、SD カードが挿入されている場合、現在の設定を SD カードにも「apresia-startup-config.txt」として保存します。その際、「apresia-startup-config.txt」が存在している場合は、上書きされます。

• startup-config

装置が起動する際に使用される、初期設定用の構成情報を指します。

startup-config の内容を更新するには、現在動作中の設定（running-config）を更新して、running-config を startup-config に保存します。

startup-config として使用する構成情報には、プライマリー構成情報およびセカンダリー構成情報があります。装置が起動するときに最初に読み込まれるのは、プライマリー構成情報です。プライマリー構成情報が読み込めない場合は、セカンダリー構成情報が読み込まれます。

startup-config として使用する構成情報のファイル名は、**`boot config`** コマンドで設定します。

> ***CAUTION:*** ローカルフラッシュのブートスクリプトで、SD カード上の構成情報ファイルを指定する場合は、SD カードを取り外さないでください。この状態で SD カードを取り外すと、startup-config にはローカルフラッシュ内で有効な構成情報と判定されたファイルのうち、最新日時のファイルが適用されます。
>
> ***NOTE:*** startup-config は直接編集できません。
>
> ***NOTE:*** **`boot config`** コマンドを実行するとすぐに、指定したファイルが装置の NVRAM に格納されます。
>
> ***NOTE:*** プライマリー構成情報およびセカンダリー構成情報が読み込めない場合は、ローカルフラッシュ内で有効な構成情報と判定されたファイルのうち、最新日時のファイルが適用されます。ローカルフラッシュにも起動時に使用できる構成情報が存在しない場合は、デフォルト設定で起動します。運用中の装置がデフォルト設定で起動した場合、ループを含む重大な障害につながる恐れがあるため、構成情報はプライマリーとセカンダリーの双方を指定して保存してください。

• running-config

現在動作中の設定が自動的に記録される構成情報を指します。グローバル設定モードやサブ設定モードで、設定を変更するコマンドを使用すると、running-config の内容が変更されます。

NOTE: 装置を再起動すると、running-config は削除され、startup-config のコマンド設定に従って装置が起動します。

装置設定の削除（デフォルト設定での再起動）

startup-config をデフォルト設定に戻し、再起動させる場合は **`reset system`** コマンドを使用します。装置を再起動せずに装置のデフォルト設定で動作させる場合は、**`clear running-config`** コマンドを使用します。

NOTE: **`reset system`** コマンドを使用した場合は、スタックに関する設定も削除されます。**`clear running-config`** コマンドを使用した場合は、スタックに関する設定は削除されません。

NOTE: **`clear running-config`** コマンドで running-config を消去した装置を運用環境で使用する際は、設定を実施して構成情報を保存した後、念のため運用前に一度起動しなおしてから使用することを推奨します。

NOTE: 装置の設定を削除すると、IP アドレスも削除され、Telnet や SSH による接続ができなくなります。

NOTE: 設定のバックアップが必要な場合は、装置の設定を削除する前に、**`copy`** コマンドなどを使用してバックアップしてください。

`default port-shutdown` コマンドを設定してから **`reset system`** コマンドを使用すると、再起動後に **`shutdown`** コマンドが全ポートに設定された状態で起動できます。再起動後の running-config と startup-config の全ポートに **`shutdown`** コマンドが設定されます。

running-config の置き換え

running-config を削除し、指定した構成情報の内容に置き換えます。構成情報が、他のネットワークデバイスに保存されている場合は、TFTP/FTP/SFTP のいずれかのプロトコルを利用してコピーできます。running-config を置き換えるには、**`configure replace`** コマンドを使用します。

CAUTION: **`configure replace`** コマンドを使用すると、装置の再起動を伴わずに running-config の置き換えが発生します。装置の設定が置き換わる際に通信断やループが発生する可能性がありますので、運用中の使用は避けてください。

CAUTION: スタック機能が無効となっている装置では、**`configure replace`** コマンドを使用する際、スタック機能が有効となっている構成情報に置き換えないでください。

NOTE: 設定のバックアップが必要な場合は、running-config を置き換える前に、**`copy`** コマンドなどを使用してバックアップしてください。

11.1.2 ブートイメージファイル

ブートイメージファイルは、装置が起動する際に使用されるファームウェアイメージです。ブートイメージファイルには、プライマリーブートイメージファイルおよびセカンダリーブートイメージファイルがあります。

装置が起動すると、最初にプライマリーブートイメージファイルが読み込まれます。プライマリーブートイメージファイルが読み込めない場合は、セカンダリーブートイメージファイルが読み込まれます。

装置が起動する際に使用されるブートイメージファイルは、**`boot image`** コマンドで設定します。

> ***CAUTION:*** ローカルフラッシュのブートスクリプトで、SD カード上のブートイメージファイルを指定する場合は、SD カードを取り外さないでください。この状態で SD カードを取り外すと、ブートイメージファイルにはローカルフラッシュ内で有効なイメージファイルと判定されたファイルのうち、最新日時のファイルが適用されます。
>
> ***CAUTION:*** ローカルフラッシュには、有効なブートイメージファイルを必ず 1 つは残しておいてください。
>
> ***NOTE:*** **`boot image`** コマンドを実行するとすぐに、指定したファイルが装置の NVRAM に格納されます。
>
> ***NOTE:*** プライマリーブートイメージファイルおよびセカンダリーブートイメージファイルが読み込めない場合は、ローカルフラッシュ内で有効なイメージファイルと判定されたファイルのうち、最新日時のファイルが適用されます。

11.1.3 ファイルシステム

装置で利用できるファイルシステムには、ローカルフラッシュおよび外部ストレージがあります。ブートイメージファイル、構成情報、およびシステムログ情報はすべて、ファイルシステムにファイルとして保存されます。

操作対象のファイルシステムは、以下のように指定します。

表 11-1 操作対象のファイルシステムの指定方法

操作対象のファイルシステム	指定方法
• 非スタック装置のローカルフラッシュ • スタックメンバー（マスター）のローカルフラッシュ	c:
• 非スタック装置の外部ストレージ • スタックメンバー（マスター）の外部ストレージ	d:
スタックメンバー（マスター以外）のローカルフラッシュ	unit2:/c: （ボックス ID が 2 の装置の場合）
スタックメンバー（マスター以外）の外部ストレージ	unit2:/d: （ボックス ID が 2 の装置の場合）

ローカルフラッシュのメモリーサイズは、以下のように装置ごとに異なります。

表 11-2 ローカルフラッシュのメモリーサイズ

装置	メモリーサイズ
NP7000	512 メガバイト
NP5000	256 メガバイト

装置	メモリーサイズ
NP4000	512 メガバイト
NP3000	128 メガバイト
NP2100	128 メガバイト
NP2000	• ApresiaNP2000-24T4X および ApresiaNP2000-48T4X：32 メガバイト • ApresiaNP2000-24T4X-PoE および ApresiaNP2000-48T4X-PoE：128 メガバイト
NP2500	128 メガバイト

NOTE: ローカルフラッシュの空き容量は **dir** コマンドで確認できます。

NOTE: SD メモリーカードを再初期化する際は、FAT16 でフォーマットしてください。フォーマットには SD メモリーカードメーカー各社より提供されている SD メモリーカードフォーマットソフトウェアをご使用ください。

11.1.4 動作に必要なファイルのバックアップおよびリストア

装置が動作するために必要なファイル（以後、**動作に必要なファイル**）を、装置のローカルフラッシュから TFTP/FTP/SFTP サーバーまたは SD カードにバックアップしたり、逆にローカルフラッシュにリストアしたりできます。

バックアップされるファイルは以下のとおりです。

- ブートイメージファイル
- startup-config
- running-config
- ランタイムバージョンテキストファイル
- SSHv2 RSA 鍵対ファイル
- SSHv2 DSA 鍵対ファイル
- 以下の Web ページ
  ログイン認証ページ
  認証成功ページ
  認証失敗ページ
  ログアウト成功ページ
  ログアウト失敗ページ
  リダイレクト失敗ページ
- AccessDefender のローカルデータベース
- SSL サーバー証明書
- SSL サーバーの秘密鍵
- Web ページ画像 01 ～ 10

  NOTE: NP2100 の 1.09.02 以降、NP2000 の 1.09.01 以降では、個別 Web 認証ページ（180 ファイル）、および Web アクセス拒否通知ページも処理対象になります。

  NOTE: NP2500 の 1.10.01 以降では、Web アクセス拒否通知ページも処理対象になります。

11.1.4.1 動作に必要なファイルのバックアップ

動作に必要なファイルを、装置のローカルフラッシュから TFTP/FTP/SFTP サーバーまたは SD カードにバックアップできます。動作に必要なファイルをバックアップするには、**backup** コマンドを使用します。

CAUTION: スタックを構成している場合、マスター以外のスタックメンバーは、**backup** コマンドでは動作に必要なファイルをバックアップできません。

CAUTION: IPv6 アドレスで TFTP/FTP サーバーを指定して **backup** コマンドを使用する場合、および IPv4 アドレスで FTP サーバーを指定して **backup ftp:** コマンドを使用する場合は、「AccessDefender のローカルデータベース」「SSL サーバー証明書」「SSL サーバーの秘密鍵」はバックアップ処理の対象外になります。これらを含めて実施する場合は、IPv4 アドレスで TFTP サーバーを指定して **backup tftp:** コマンドを使用するか、SD カードを利用して **backup memory-card:** コマンドを使用してください。

NOTE: 各ファイルのバックアップはそれぞれ独立して実行されます。1 つのファイルのバックアップに失敗した場合でも、その他のファイルのバックアップは行われます。

11.1.4.2 動作に必要なファイルのリストア

TFTP/FTP/SFTP サーバーまたは SD カードにバックアップした動作に必要なファイルを、装置のローカルフラッシュにリストアできます。動作に必要なファイルをリストアするには、**restore** コマンドを使用します。**restore** コマンドを実施した後は、ファームウェアや設定などを反映させるために、装置を再起動または電源 OFF/ON を実施して起動しなおしてください。

CAUTION: スタックを構成している場合、マスター以外のスタックメンバーは、**restore** コマンドでは動作に必要なファイルをリストアできません。

CAUTION: IPv6 アドレスで TFTP/FTP サーバーを指定して **restore** コマンドを使用する場合、および IPv4 アドレスで FTP サーバーを指定して **restore ftp:** コマンドを使用する場合は、「AccessDefender のローカルデータベース」「SSL サーバー証明書」「SSL サーバーの秘密鍵」はリストア処理の対象外になります。これらを含めて実施する場合は、IPv4 アドレスで TFTP サーバーを指定して **restore tftp:** コマンドを使用するか、SD カードを利用して **restore memory-card:** コマンドを使用してください。

NOTE: 動作に必要なファイルをリストアすると、プライマリー構成情報はリストアされた startup-config に置き換わり、プライマリーブートイメージファイルはリストアされたブートイメージファイルに置き換わります。装置に同じ名前のファイルが存在した場合は、既存のファイルは上書きされます。

NOTE: SSHv2 RSA/DSA 鍵対ファイルは、装置を起動しなおした後にリストアされたファイルに置き換わります。

NOTE: 装置のローカルフラッシュに十分な空き容量があることを確認してから行ってください。

11.1.5 ブートスクリプト

ブートスクリプトは装置起動時に使用される情報です。装置起動時に使用するブートイメージファイルと、装置起動時に使用する構成情報のファイル名が記載されています。

ブートスクリプトに記載されているブートイメージファイルのファイル名を書き替えるには、**boot image** コマンドを使用します。同様に、startup-config として使用する構成情報のファイル名を書き替えるには、**boot config** コマンドを使用します。

11.1.6 SD カードへのブートスクリプトの保存

装置のローカルフラッシュから SD カードにブートスクリプトのみを保存できます。SD カードにブートスクリプトのみを保存するには、**copy boot** コマンドを使用します。

11.1.7 ローカルフラッシュのブートスクリプトの消去

装置のローカルフラッシュからブートスクリプトを消去できます。ローカルフラッシュからブートスクリプトを消去するには、**erase boot** コマンドを使用します。

> ***CAUTION:*** ローカルフラッシュからブートスクリプトを消去すると、正しく使用できるブートスクリプトが保存されている SD カードを装置に挿入しない限り、装置起動時にブートスクリプトの読み込みに失敗します。

11.1.8 システムの復旧（パスワードのリセット）

ネットワーク管理者は、システム復旧機能を利用してパスワードをリセットできます。

システム復旧の手順は、装置にユーザーアカウントが存在する場合と、存在しない場合で異なります。

> ***CAUTION:*** **username** コマンドおよび **enable password** コマンドで設定するユーザー名およびパスワードに、「ap_recovery」を使用することはできません。「ap_recovery」は、設定の初期化を実行するための特別なユーザー名およびパスワードです。
>
> ***NOTE:*** システム復旧手順を実行すると、保存されている設定はデフォルト設定に戻ります。また、SSH サーバーの RSA 鍵対と DSA 鍵対も削除されます。

11.1.8.1 装置にユーザーアカウントが存在する場合の復旧手順

装置にユーザーアカウントが存在する場合のシステム復旧手順を示します。

1. パラメーター設定端末を、装置のコンソールポートに接続します。
2. 装置の電源を入れます。
3. ログイン画面が表示された後、Username フィールドに「**ap_recovery**」と入力して、Enter キーを押します。

```
Ethernet Switch ApresiaNP7000-48X6L

Firmware: Build 1.05.01

User Verification Access
Username:ap_recovery
System will be reset, save and reboot!
Saving configurations and logs to NV-RAM...... Done.
Please wait, the switch is rebooting...
```

装置が再起動した後は設定がデフォルト設定に戻っているため、ユーザーアカウントおよびパスワードを入力せずにユーザー実行モードで CLI にアクセスが許可されます。

11.1.8.2 装置にユーザーアカウントが存在しない場合の復旧手順

装置にユーザーアカウントが存在しないが、enable パスワードが設定されている場合のシステム復旧手順を、以下に示します。

1. パラメーター設定端末を、装置のコンソールポートに接続します。
2. 装置の電源を入れます。
3. ユーザー実行モードにログインした後、**enable** コマンドを使用し、Password フィールドに「**ap_recovery**」と入力して、Enter キーを押します。

```
Ethernet Switch ApresiaNP7000-48X6L

Firmware: Build 1.05.01

> enable
Password:ap_recovery

System will be reset, save and reboot!
Saving configurations and logs to NV-RAM...... Done.
Please wait, the switch is rebooting...
```

> ***NOTE:*** この手順例では、説明のために Password フィールドに入力した文字列を表示していますが、実際には「**********」と表示されます。

装置が再起動した後は設定がデフォルト設定に戻っているため、enable パスワード設定もデフォルトの未設定になります。

11.2 システムファイルの仕様と動作

システムファイルの仕様と運用時の動作について説明します。

外部ストレージのマッピングルール

ファイルシステムは、複数のドライブに対応しています。

装置の外部ストレージは 1 つのドライブに割り当てられ、ドライブごとにドライブ文字が割り当てられます。ローカルフラッシュには「c:」が割り当てられ、外部ストレージには「d:」以降のドライブ文字が割り当てられます。

予約ファイル

システムモジュールが使用するファイルは参照できません。予約ファイルが占有する領域は **dir** コマンドで確認できます。

ディレクトリー名およびファイル名のルール

ディレクトリー名およびファイル名には、以下の制限があります。ディレクトリー名およびファイル名を変更するには、**rename** コマンドを使用します。

- **大文字と小文字**
  ファイル名では大文字と小文字が区別されます。
- **使用不可文字**
  以下の文字は使用できません。
  / \ : * ? " < > | スペース
- **予約済みファイル名**
  以下の名前はシステムで予約済みです。これらの名前をディレクトリー名およびファイル名として使用することはできません。

表 11-3 予約済みファイル名

名前	用途
.	現在のディレクトリーを表すファイル名
..	上位レベルのディレクトリーを表す
ルートディレクトリー配下の「system」	システムで予約済み

- **文字数**
  ディレクトリー名およびファイル名の最小文字数は 1 文字、最大文字数は 32 文字です。
- **その他のルール**
  同じディレクトリー内の異なるディレクトリーまたはファイルに、同じ名前を付けられません。

ファイル属性

ファイルの以下の属性を確認できます。

- **作成日時**
  ファイルが作成された日時です。

11.3 システムファイルの状態確認

システムファイルの状態を表示して確認する方法を説明します。

11.3.1 ブートスクリプトの表示

show boot コマンドで、ブートスクリプトを確認できます。

表示例を以下に示します。この例では「apresia-loader.conf」が保存されている SD カードが挿入されています。

```
# show boot

Unit 1 ...(1)
(Configured)
 Primary boot image:/c:/image1.had ...(2)
 Primary boot config:/c:/config1.cfg ...(3)
 Secondary boot image:No valid boot image. ...(4)
 Secondary boot config:No valid boot config. ...(5)
*(SD Card)
 Primary boot image:/d:/apresia-software.had ...(6)
 Primary boot config:/d:/apresia-startup-config.txt ...(7)


Note:* indicates the used boot information.
```

各項目の説明は、以下のとおりです。

表 11-4 show boot コマンドの表示項目

項番	説明
(1)	装置のボックス ID を表示します。スタックを構成していない場合は「1」が表示されます。
(2)	プライマリーブートイメージファイルとして使用するファイルのパスを表示します。
(3)	プライマリー構成情報として使用するファイルのパスを表示します。
(4)	セカンダリーブートイメージファイルとして使用するファイルのパスを表示します。
(5)	セカンダリー構成情報として使用するファイルのパスを表示します。
(6)	SD カードブート利用時の、プライマリーブートイメージファイルとして使用するファイルのパスを表示します。
(7)	SD カードブート利用時の、プライマリー構成情報として使用するファイルのパスを表示します。

11.3.2 startup-config の表示

show startup-config コマンドで、起動時に使用する構成情報を確認できます。

表示例を以下に示します。

```
# show startup-config

#------------------------------------------------------------------------------
#                 ApresiaNP7000-48X6L TenGigabit Ethernet Switch
#                                Configuration
#
#                            Firmware: Build 1.04.01
#          Copyright(C) 2016 APRESIA Systems, Ltd. All rights reserved.
#------------------------------------------------------------------------------

# Date: Fri Nov 02 10:37:14 2018


# STACK

no stack
no stack my_box_id
stack my_box_priority 32
no stack preempt
no stack port-channel mode partial
no stack stack-port load-balance
no stack vlan pre-setting

# PORT

CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

11.3.3 running-config の表示

show running-config コマンドで、現在動作中の構成情報を確認できます。

表示例を以下に示します。

```
# show running-config
Building configuration...

Current configuration : 3299 bytes ...(1)

#------------------------------------------------------------------------------
#                 ApresiaNP7000-48X6L TenGigabit Ethernet Switch
#                                Configuration
#
#                            Firmware: Build 1.04.01
#          Copyright(C) 2016 APRESIA Systems, Ltd. All rights reserved.
#------------------------------------------------------------------------------

# Date: Mon Nov 12 11:24:28 2018


# STACK

no stack
no stack my_box_id
stack my_box_priority 32
no stack preempt
no stack port-channel mode partial
no stack stack-port load-balance
no stack vlan pre-setting
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

各項目の説明は、以下のとおりです。

表 11-5 show running-config コマンドの表示項目

項番	説明
(1)	running-config のサイズを表示します。

11.3.4 構成情報の差分の表示

show config differences コマンドで、指定した 2 つの構成情報の差分を確認できます。

running-config と startup-config の差分を確認する場合の表示例を以下に示します。

```
# show config differences running-config startup-config

Config differences: ...(1)
+vlan 10,20,500
+interface port 1/0/25
+ switchport access vlan 500
-vlan 10,20
-logging server 10.249.234.112 severity debugging facility 23 port 514
```

各項目の説明は、以下のとおりです。

表 11-6 show config differences コマンドの表示項目

項番	説明
(1)	**show config differences A B** と実行した場合、差分は以下のように表示されます。 • A に含まれていて、B に含まれていない設定：先頭に "+" が付与されて表示 • A に含まれず、B に含まれている設定：先頭に "-" が付与されて表示

11.3.5 現在のディレクトリーおよびディレクトリー情報の表示

ファイルシステムの現在のディレクトリーおよびディレクトリー情報を確認できます。

現在のディレクトリーの表示

cd コマンドは、現在のディレクトリーを変更するコマンドです。ディレクトリーの URL の指定を省略した場合は、現在のディレクトリーを確認できます。

表示例を以下に示します。

```
# cd
Current directory is /c:/log ...(1)
```

各項目の説明は、以下のとおりです。

表 11-7 cd コマンドの表示項目

項番	説明
(1)	現在のディレクトリーを表示します。

ディレクトリー情報の表示

dir コマンドで、ディレクトリー情報を確認できます。

表示例を以下に示します。

```
# dir

Directory of /c: ...(1)
(2) (3)       (4)       (5)                    (6)
1   d--             0 Mar 10 2016 07:00:01  log
2   -rw      12036316 Mar 10 2016 08:00:01  FW-1.00.01.0002.had
3   -rw         55131 Mar 10 2016 09:00:01  config.cfg
4   d--             0 Mar 10 2016 10:00:01  system

536346624 bytes total (523964416 bytes free) ...(7)
```

各項目の説明は、以下のとおりです。

表 11-8 dir コマンドの表示項目

項番	説明
(1)	ディレクトリー情報を表示するパスを表示します。
(2)	ディレクトリーまたはファイルの通し番号を表示します。
(3)	ディレクトリーまたはファイルの種別、およびアクセス権を表示します。 • d：ディレクトリー • r：読み出し可能 • w：書き込み可能
(4)	ファイルサイズを表示します。ディレクトリーの場合は、「0」を表示します。
(5)	ディレクトリーまたはファイルの更新日時を表示します。
(6)	ディレクトリーまたはファイルの名前を表示します。
(7)	ファイルが使用している容量および未使用容量を表示します。

ファイル内容の表示

more コマンドで、ファイルの内容を確認できます。

「/c:/config.cfg」を指定した場合の表示例を以下に示します。

```
# more /c:/config.cfg


#------------------------------------------------------------------------------
#                  ApresiaNP7000-48X6L TenGigabit Ethernet Switch
#                                  Configuration
#
#                              Firmware: Build 1.02.02
#          Copyright(C) 2016 APRESIA Systems, Ltd. All rights reserved.
#------------------------------------------------------------------------------

# Date: Wed Jan 18 09:12:08 2017


# STACK

no stack
no stack my_box_id
stack my_box_priority 32
no stack preempt

# PORT

interface port 1/0/1
interface port 1/0/2
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

11.3.6 ローカルフラッシュおよび外部ストレージの情報の表示

show storage media-info コマンドで、ローカルフラッシュおよび外部ストレージの情報を確認できます。

表示例を以下に示します。

```
# show storage media-info
(1)   (2)    (3)          (4)       (5)      (6)
Unit  Drive  Media-Type   Size      FS-Type  Label
----  -----  ----------   --------  -------  -----------
1     c:     Flash        511 MB    FFS
1     d:     SD Card      1888 MB   FAT16
```

各項目の説明は、以下のとおりです。

表 11-9 show storage media-info コマンドの表示項目

項番	説明
(1)	装置のボックス ID を表示します。スタックを構成していない場合は「1」が表示されます。
(2)	ドライブ文字を表示します。
(3)	メディアの種類（Flash：ローカルフラッシュ／ SD Card：外部ストレージ）を表示します。
(4)	総容量を表示します。

項番	説明
(5)	ファイルシステムを表示します。
(6)	ラベルを表示します。

11.4 システムファイルの実施例

システムファイルを利用する場合の実施例を示します。

11.4.1 ファイルリストを表示する場合

ローカルフラッシュのファイルリストを表示する場合の実施例を示します。

> ***NOTE:*** その他のファイルシステムのファイルリストを表示する場合は、「c:」（ローカルフラッシュ）を「d:」（外部ストレージ）や「unit2:/c:」（ボックス ID が 2 の装置のローカルフラッシュ）にするなど、適宜読み替えてください。

現在のディレクトリーを［c:］に移動して、ファイルリストを表示します。

```
sw1# cd c:
sw1# dir
```

現在のディレクトリーを移動しないで、ファイルリストを表示します。

```
sw1# dir c:
```

11.4.2 ファイルをコピーする場合

ローカルフラッシュの file.txt を、外部ストレージにコピーする場合の実施例を示します。

> ***NOTE:*** その他のファイルシステムのファイルをコピーする場合は、以下の表を参考に、適宜コマンドを読み替えてください。

表 11-10 ファイルの指定方法

ファイル	指定方法
• 非スタック装置のローカルフラッシュの file.txt • スタックメンバー（マスター）のローカルフラッシュの file.txt	c:/file.txt
• 非スタック装置の外部ストレージの file.txt • スタックメンバー（マスター）の外部ストレージの file.txt	d:/file.txt
スタックメンバー（マスター以外でボックス ID が 2）のローカルフラッシュの file.txt	unit2:/c:/file.txt
スタックメンバー（マスター以外でボックス ID が 2）の外部ストレージの file.txt	unit2:/d:/file.txt

1. 現在のディレクトリーがローカルフラッシュ［/c:］であることを確認します。

```
sw1# cd
Current directory is /c:
sw1#
```

2. ［ローカルフラッシュの file.txt］を、［外部ストレージ］にファイル名［new-file.txt］でコピーします。

```
sw1# copy flash: flash:

Source filename []? file.txt
Destination filename []? d:/new-file.txt
 Copy in progress.......................... 100 %

sw1#
```

11.4.3 running-config をコピーする場合

running-config を、スタックメンバー（マスター以外でボックス ID が 2）の外部ストレージにコピーする場合の実施例を示します。

NOTE: その他のファイルシステムのファイルにコピーする場合は、以下の表を参考に、適宜コマンドを読み替えてください。

表 11-11 ファイルの指定方法

ファイル	指定方法
• 非スタック装置のローカルフラッシュの master_run.cfg • スタックメンバー（マスター）のローカルフラッシュの master_run.cfg	c:/master_run.cfg
• 非スタック装置の外部ストレージの master_run.cfg • スタックメンバー（マスター）の外部ストレージの master_run.cfg	d:/master_run.cfg
スタックメンバー（マスター以外でボックス ID が 2）のローカルフラッシュの master_run.cfg	unit2:/c:/master_run.cfg
スタックメンバー（マスター以外でボックス ID が 2）の外部ストレージの master_run.cfg	unit2:/d:/master_run.cfg

running-config を、［スタックメンバー（マスター以外でボックス ID が 2）の外部ストレージ］にファイル名［master_run.cfg］でコピーします。

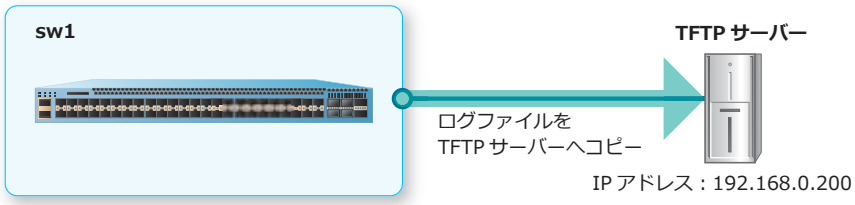
```
sw1# copy running-config flash:

Destination filename []? unit2:/d:/master_run.cfg
Saving all configurations to NV-RAM.......... Done.

sw1#
```

11.4.4 ログファイルを TFTP サーバーにコピーする場合

ログファイルを、IP アドレスが 192.168.0.200 の TFTP サーバーにコピーする場合の実施例を示します。

NOTE: コピー元として log を指定した場合は、コピー先には TFTP サーバーのみ指定できます。

図 11-1 ログファイルを TFTP サーバーにコピーする場合の構成例



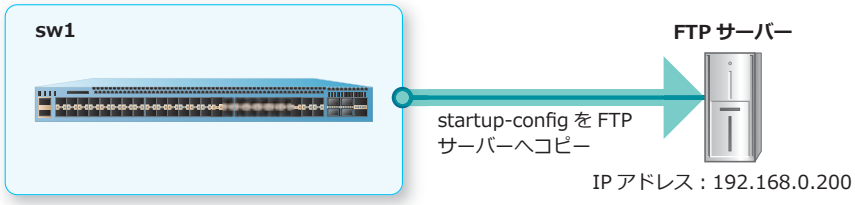
ログファイルを、IP アドレスが［192.168.0.200］の TFTP サーバーに、ファイル名を［log.txt］としてコピーします。

```
sw1# copy log tftp:

Address of remote host []? 192.168.0.200
Destination filename []? log.txt
 Accessing tftp://192.168.0.200/log.txt...
 Transmission start...
 Transmission finished, file length 9595 bytes.

sw1#
```

11.4.5 startup-config を FTP サーバーにコピーする場合

startup-config を、IP アドレスが 192.168.0.200 の FTP サーバーにコピーする場合の実施例を示します。

図 11-2 startup-config を FTP サーバーにコピーする場合の構成例



startup-config を、IP アドレスが［192.168.0.200］の FTP サーバーに、ファイル名を［config.cfg］としてコピーします。FTP サーバーにコピーする場合は FTP サーバーのユーザーアカウントとパスワードが必要ですが、この例ではユーザーアカウント［apresia-user］とパスワードを入力しています。

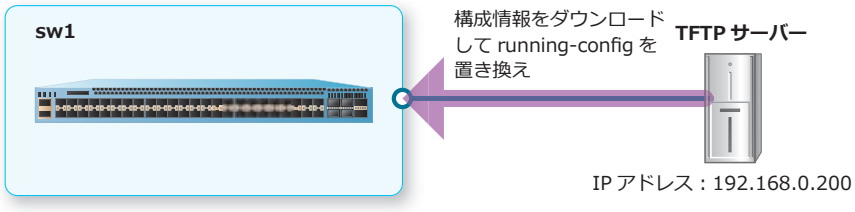
```
sw1# copy startup-config ftp:

Address of remote host []? 192.168.0.200
Destination username [Anonymous]? apresia-user
Destination password []? *******
TCP port number of remote host [default]?
Destination filename []? config.cfg
 Accessing ftp://192.168.0.200/config.cfg...
 Transmission start...
 Transmission finished, file length 2456 bytes.

sw1#
```

11.4.6 TFTP サーバーから構成情報をダウンロードして反映する場合

TFTP サーバーから構成情報をダウンロードして running-config の内容を置き換え、その設定を startup-config に保存する場合の実施例を示します。

> ***CAUTION:*** `configure replace` コマンドを使用すると、装置の再起動を伴わずに running-config の置き換えが発生します。装置の設定が置き換わる際に通信断やループが発生する可能性がありますので、運用中の使用は避けてください。

図 11-3 TFTP サーバーから構成情報をダウンロードする場合の構成例



1. IP アドレスが［192.168.0.200］の TFTP サーバーから構成情報［config.cfg］をダウンロードして、running-config の内容を置き換えます。

```
sw1# configure replace tftp: //192.168.0.200/config.cfg

This will apply all necessary additions and deletions
to replace the current running configuration with the
contents of the specified configuration file, which is
assumed to be a complete configuration, not a partial
configuration. [y/n]:  y

 Accessing tftp://192.168.0.200/config.cfg...
 Transmission start...
 Transmission finished, file length 2456 bytes.
 Executing script file config.cfg ......
 Executing done

sw1#
```

2. 現在動作中の設定（running-config）を startup-config に保存します。

```
sw1# write memory

Destination filename startup-config? [y/n]:  y

Saving all configurations to NV-RAM.......... Done.

sw1#
```

12. SD カードブート

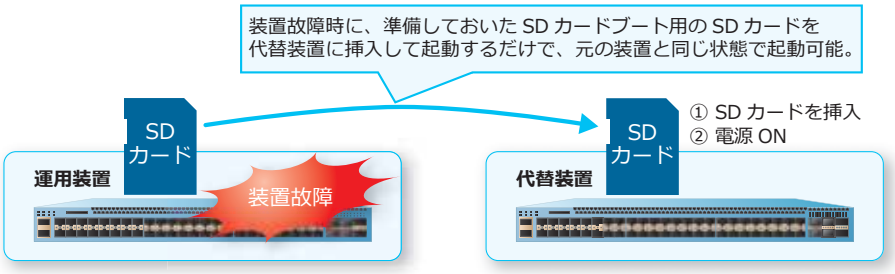
SD カードブートの機能、準備方法、および装置故障時の交換手順について説明します。

REF: コマンドの詳細については、『コマンドリファレンス』を参照してください。

12.1 SD カードブートの機能説明

装置が故障した際、通常の装置交換では、故障した装置と同じブートイメージファイルや構成情報を代替装置に設定する必要があります。この作業時間を短縮するための機能が、**SD カードブート**です。SD カードブートでは、準備しておいた SD カードブート用の SD カードを代替装置に挿入して起動するだけで、故障した装置と同じ状態に設定された代替装置を簡単に起動できます。

図 12-1 SD カードブートの概要



12.2 SD カードブートの準備

SD カードブートでは、ブートスクリプト、および動作に必要なファイルを、あらかじめ SD カードにコピーしておきます。SD カードブートの準備を行うには、**backup clone** コマンドを使用します。

backup clone コマンド実行時に SD カードにコピーされるファイルとファイル名（固定）は、以下のとおりです。なお、元々存在しないファイルはコピーされません。

> ***NOTE:*** ランタイムバージョンテキストファイル（apresia-system-name.txt）には、**backup clone** コマンド実行時に SD カードに保存されたブートイメージファイル(apresia-software.had)のバージョン情報が保存されます。

- ブートスクリプト：apresia-loader.conf
- ブートイメージファイル：apresia-software.had
- startup-config：apresia-startup-config.txt
- ランタイムバージョンテキストファイル：apresia-system-name.txt
- SSHv2 RSA 鍵対ファイル：apresia-rsa-key
- SSHv2 DSA 鍵対ファイル：apresia-dsa-key
- 以下の Web 認証ページ
  ログイン認証ページ：apresia-login-page
  認証成功ページ：apresia-login-success-page
  認証失敗ページ：apresia-login-failure-page
  ログアウト成功ページ：apresia-logout-success-page
  ログアウト失敗ページ：apresia-logout-failure-page
  リダイレクト失敗ページ：apresia-redirect-error-page
- AccessDefender のローカルデータベース：apresia-aaa-local-db
- SSL サーバー証明書：apresia-https-certificate
- SSL サーバーの秘密鍵：apresia-https-private-key
- Web ページ画像 01 ～ 10：apresia-webpage-image01 ～ apresia-webpage-image10

  > ***NOTE:*** NP2100 の 1.09.02 以降、NP2000 の 1.09.01 以降では、個別 Web 認証ページ（180 ファイル）、および Web アクセス拒否通知ページも処理対象になります。

  > ***NOTE:*** NP2500 の 1.10.01 以降では、Web アクセス拒否通知ページも処理対象になります。

12.2.1 非スタック装置の場合の動作例

非スタック装置で **backup clone** コマンドを実行した場合の動作例を以下に示します。この動作例の条件は、以下のとおりです。

- SSHv2 RSA 鍵対ファイル、DSA 鍵対ファイルは作成済み
- ユーザーで準備したカスタム Web 認証ページを装置にダウンロード済み
- ユーザーで準備した SSL 証明書 / 秘密鍵を装置にダウンロード済み
- ユーザーで準備した Web ページ画像 01 を装置にダウンロード済み
- AccessDefender のローカルデータベース、Web ページ画像 02 ～ 10 はなし

  NOTE: **backup clone** コマンド実行時に、SD カードにすでに同名のファイルが存在する場合は上書きされます。

1. 装置に SD カードを挿入します。

```
sw1# show storage media-info

Unit  Drive  Media-Type  Size      FS-Type  Label
----  -----  ----------  --------  -------  -----------
1     c:     Flash       29 MB     FFS
1     d:     SD Card     944 MB    FAT16

sw1#
sw1# dir d:/

Directory of /d:/
1   d--             0 Nov 21 2018 10:40:04  System Volume Information

990576640 bytes total (990265344 bytes free)

sw1#
```

2. **backup clone** コマンドを実行します。

```
sw1# backup clone

 Uploading boot information (apresia-loader.conf)..... Done.
 Uploading firmware image file (apresia-software.had)..... Done.
 Uploading start-up configuration file (apresia-startup-config.txt)..... Done.
 Uploading system name file (apresia-system-name.txt)..... Done.
 Uploading SSH RSA key file (apresia-rsa-key)..... Done.
 Uploading SSH DSA key file (apresia-dsa-key)..... Done.
 Uploading web authentication login-page file (apresia-login-page)..... Done.
 Uploading web authentication login-success-page file
(apresia-login-success-page)..... Done.
 Uploading web authentication login-failure-page file
(apresia-login-failure-page)..... Done.
 Uploading web authentication logout-success-page file
(apresia-logout-success-page)..... Done.
 Uploading web authentication logout-failure-page file
(apresia-logout-failure-page)..... Done.
 Uploading web authentication redirect-error-page file
(apresia-redirect-error-page)..... Done.
 Uploading access defender local database settings file
(apresia-aaa-local-db)..... Fail.
 Uploading SSL server certificate file (apresia-https-certificate)..... Done.
 Uploading SSL server private key file (apresia-https-private-key)..... Done.
 Uploading web authentication webpage-image01 file
(apresia-webpage-image01)..... Done.
 Uploading web authentication webpage-image02 file
(apresia-webpage-image02)..... Fail.
 Uploading web authentication webpage-image03 file
(apresia-webpage-image03)..... Fail.
 Uploading web authentication webpage-image04 file
(apresia-webpage-image04)..... Fail.
 Uploading web authentication webpage-image05 file
(apresia-webpage-image05)..... Fail.
 Uploading web authentication webpage-image06 file
(apresia-webpage-image06)..... Fail.
 Uploading web authentication webpage-image07 file
(apresia-webpage-image07)..... Fail.
 Uploading web authentication webpage-image08 file
(apresia-webpage-image08)..... Fail.
 Uploading web authentication webpage-image09 file
(apresia-webpage-image09)..... Fail.
 Uploading web authentication webpage-image10 file
(apresia-webpage-image10)..... Fail.
 ERROR: File not found.

sw1#
```

3. **backup clone** コマンド実行後の状態を確認します。

```
sw1# dir d:/

Directory of /d:/
1   -rw          1576 Oct 08 2019 15:55:18  apresia-loader.conf
2   -rw       7179528 Oct 08 2019 15:56:58  apresia-software.had
3   -rw          2212 Oct 08 2019 15:57:02  apresia-startup-config.txt
4   -rw             8 Oct 08 2019 15:56:04  apresia-system-name.txt
5   -rw          2391 Oct 08 2019 15:56:10  apresia-rsa-key
6   -rw           905 Oct 08 2019 15:56:14  apresia-dsa-key
7   -rw          2427 Oct 08 2019 15:56:20  apresia-login-page
8   -rw          1332 Oct 08 2019 15:56:26  apresia-login-success-page
9   -rw          1084 Oct 08 2019 15:56:30  apresia-login-failure-page
10  -rw          1013 Oct 08 2019 15:56:36  apresia-logout-success-page
11  -rw          1084 Oct 08 2019 15:56:42  apresia-logout-failure-page
12  -rw          1023 Oct 08 2019 15:56:48  apresia-redirect-error-page
13  d--             0 Nov 21 2018 10:40:04  System Volume Information
14  -rw          4474 Oct 08 2019 15:56:54  apresia-https-certificate
15  -rw          1679 Oct 08 2019 15:57:06  apresia-https-private-key
16  -rw          5434 Oct 08 2019 15:57:10  apresia-webpage-image01

990576640 bytes total (982843392 bytes free)

sw1#
sw1# show boot

Unit 1
*(Configured)
 Primary boot image: /c:/AEOS-NP2000_R10701.had
 Primary boot config: /c:/primary.cfg
 Secondary boot image: /c:/AEOS-NP2000_R10701_sec.had
 Secondary boot config: /c:/secondary.cfg
(SD Card)
 Primary boot image: /d:/apresia-software.had
 Primary boot config: /d:/apresia-startup-config.txt


Note: * indicates the used boot information.

sw1#
```

12.2.2 スタック構成の場合の動作例

スタック構成で **backup clone** コマンドを実行した場合の動作例を以下に示します。この動作例の条件は、以下のとおりです。

- ApresiaNP2000-48T4X×3 台のスタック構成
- SSHv2 RSA 鍵対ファイル、DSA 鍵対ファイルは作成済み
- ユーザーで準備したカスタム Web 認証ページを装置にダウンロード済み
- ユーザーで準備した SSL 証明書 / 秘密鍵を装置にダウンロード済み
- ユーザーで準備した Web ページ画像 01 を装置にダウンロード済み
- AccessDefender のローカルデータベース、Web ページ画像 02 ～ 10 はなし

NOTE: **backup clone** コマンド実行時に、SD カードにすでに同名のファイルが存在する場合は上書きされます。

1. スタックを構成するすべての装置に SD カードを挿入します。

```
sw1# show storage media-info

Unit  Drive  Media-Type  Size      FS-Type  Label
----  -----  ----------  --------  -------  -----------
1     c:     Flash       29 MB     FFS
1     d:     SD Card     944 MB    FAT16
2     c:     Flash       29 MB     FFS
2     d:     SD Card     944 MB    FAT16
3     c:     Flash       29 MB     FFS
3     d:     SD Card     944 MB    FAT16

sw1#
sw1# dir d:/

Directory of /d:/
1   d--              0 Nov 21 2018 10:40:04  System Volume Information

990576640 bytes total (990265344 bytes free)

sw1#
sw1# dir unit2:/d:/

Directory of /unit2:/d:/
1   d--              0 Dec 14 2017 13:58:28  System Volume Information

990560256 bytes total (990248960 bytes free)

sw1#
sw1# dir unit3:/d:/

Directory of /unit3:/d:/
1   d--              0 Oct 08 2019 17:05:12  System Volume Information

990560256 bytes total (990265344 bytes free)

sw1#
```

2. **backup clone** コマンドを実行します。

```
sw1# backup clone

Master (Unit 1)
 Uploading boot information (apresia-loader.conf)..... Done.
 Uploading firmware image file (apresia-software.had)..... Done.
 Uploading start-up configuration file (apresia-startup-config.txt)..... Done.
 Uploading system name file (apresia-system-name.txt)..... Done.
 Uploading SSH RSA key file (apresia-rsa-key)..... Done.
 Uploading SSH DSA key file (apresia-dsa-key)..... Done.
 Uploading web authentication login-page file (apresia-login-page)..... Done.
 Uploading web authentication login-success-page file
(apresia-login-success-page)..... Done.
 Uploading web authentication login-failure-page file
(apresia-login-failure-page)..... Done.
 Uploading web authentication logout-success-page file
(apresia-logout-success-page)..... Done.
 Uploading web authentication logout-failure-page file
(apresia-logout-failure-page)..... Done.
 Uploading web authentication redirect-error-page file
(apresia-redirect-error-page)..... Done.
 Uploading access defender local database settings file
(apresia-aaa-local-db)..... Fail.
 Uploading SSL server certificate file (apresia-https-certificate)..... Done.
 Uploading SSL server private key file (apresia-https-private-key)..... Done.
 Uploading web authentication webpage-image01 file
(apresia-webpage-image01)..... Done.
 Uploading web authentication webpage-image02 file
(apresia-webpage-image02)..... Fail.
 Uploading web authentication webpage-image03 file
(apresia-webpage-image03)..... Fail.
 Uploading web authentication webpage-image04 file
(apresia-webpage-image04)..... Fail.
 Uploading web authentication webpage-image05 file
(apresia-webpage-image05)..... Fail.
 Uploading web authentication webpage-image06 file
(apresia-webpage-image06)..... Fail.
 Uploading web authentication webpage-image07 file
(apresia-webpage-image07)..... Fail.
 Uploading web authentication webpage-image08 file
(apresia-webpage-image08)..... Fail.
 Uploading web authentication webpage-image09 file
(apresia-webpage-image09)..... Fail.
 Uploading web authentication webpage-image10 file
(apresia-webpage-image10)..... Fail.
 ERROR: File not found.

Unit 2
 Uploading boot information (apresia-loader.conf)..... Done.
 Uploading firmware image file (apresia-software.had)..... Done.
 Uploading start-up configuration file (apresia-startup-config.txt)..... Done.
 Uploading system name file (apresia-system-name.txt)..... Done.
 Uploading SSH RSA key file (apresia-rsa-key)..... Done.
 Uploading SSH DSA key file (apresia-dsa-key)..... Done.
 Uploading web authentication login-page file (apresia-login-page)..... Done.
 Uploading web authentication login-success-page file
(apresia-login-success-page)..... Done.
 Uploading web authentication login-failure-page file
(apresia-login-failure-page)..... Done.
 Uploading web authentication logout-success-page file
```

```
(apresia-logout-success-page)..... Done.
 Uploading web authentication logout-failure-page file
(apresia-logout-failure-page)..... Done.
 Uploading web authentication redirect-error-page file
(apresia-redirect-error-page)..... Done.
 Uploading access defender local database settings file
(apresia-aaa-local-db)..... Fail.
 Uploading SSL server certificate file (apresia-https-certificate)..... Done.
 Uploading SSL server private key file (apresia-https-private-key)..... Done.
 Uploading web authentication webpage-image01 file
(apresia-webpage-image01)..... Done.
 Uploading web authentication webpage-image02 file
(apresia-webpage-image02)..... Fail.
 Uploading web authentication webpage-image03 file
(apresia-webpage-image03)..... Fail.
 Uploading web authentication webpage-image04 file
(apresia-webpage-image04)..... Fail.
 Uploading web authentication webpage-image05 file
(apresia-webpage-image05)..... Fail.
 Uploading web authentication webpage-image06 file
(apresia-webpage-image06)..... Fail.
 Uploading web authentication webpage-image07 file
(apresia-webpage-image07)..... Fail.
 Uploading web authentication webpage-image08 file
(apresia-webpage-image08)..... Fail.
 Uploading web authentication webpage-image09 file
(apresia-webpage-image09)..... Fail.
 Uploading web authentication webpage-image10 file
(apresia-webpage-image10)..... Fail.
 ERROR: File not found.

Unit 3
 Uploading boot information (apresia-loader.conf)..... Done.
 Uploading firmware image file (apresia-software.had)..... Done.
 Uploading start-up configuration file (apresia-startup-config.txt)..... Done.
 Uploading system name file (apresia-system-name.txt)..... Done.
 Uploading SSH RSA key file (apresia-rsa-key)..... Done.
 Uploading SSH DSA key file (apresia-dsa-key)..... Done.
 Uploading web authentication login-page file (apresia-login-page)..... Done.
 Uploading web authentication login-success-page file
(apresia-login-success-page)..... Done.
 Uploading web authentication login-failure-page file
(apresia-login-failure-page)..... Done.
 Uploading web authentication logout-success-page file
(apresia-logout-success-page)..... Done.
 Uploading web authentication logout-failure-page file
(apresia-logout-failure-page)..... Done.
 Uploading web authentication redirect-error-page file
(apresia-redirect-error-page)..... Done.
 Uploading access defender local database settings file
(apresia-aaa-local-db)..... Fail.
 Uploading SSL server certificate file (apresia-https-certificate)..... Done.
 Uploading SSL server private key file (apresia-https-private-key)..... Done.
 Uploading web authentication webpage-image01 file
(apresia-webpage-image01)..... Done.
 Uploading web authentication webpage-image02 file
(apresia-webpage-image02)..... Fail.
 Uploading web authentication webpage-image03 file
(apresia-webpage-image03)..... Fail.
 Uploading web authentication webpage-image04 file
```

```
(apresia-webpage-image04)..... Fail.
 Uploading web authentication webpage-image05 file
(apresia-webpage-image05)..... Fail.
 Uploading web authentication webpage-image06 file
(apresia-webpage-image06)..... Fail.
 Uploading web authentication webpage-image07 file
(apresia-webpage-image07)..... Fail.
 Uploading web authentication webpage-image08 file
(apresia-webpage-image08)..... Fail.
 Uploading web authentication webpage-image09 file
(apresia-webpage-image09)..... Fail.
 Uploading web authentication webpage-image10 file
(apresia-webpage-image10)..... Fail.
 ERROR: File not found.

sw1#
```

3. **backup clone** コマンド実行後の状態を確認します。

```
sw1# dir d:/

Directory of /d:/
1   -rw          1576 Oct 08 2019 17:06:38  apresia-loader.conf
2   -rw       7179528 Oct 08 2019 17:07:28  apresia-software.had
3   -rw          5771 Oct 08 2019 17:07:34  apresia-startup-config.txt
4   -rw             8 Oct 08 2019 17:07:40  apresia-system-name.txt
5   -rw          2391 Oct 08 2019 17:07:46  apresia-rsa-key
6   -rw           905 Oct 08 2019 17:07:54  apresia-dsa-key
7   -rw          2427 Oct 08 2019 17:08:00  apresia-login-page
8   -rw          1332 Oct 08 2019 17:07:02  apresia-login-success-page
9   -rw          1011 Oct 08 2019 17:07:08  apresia-login-failure-page
10  -rw          1013 Oct 08 2019 17:07:16  apresia-logout-success-page
11  -rw          1084 Oct 08 2019 17:07:22  apresia-logout-failure-page
12  -rw          1023 Oct 08 2019 17:07:28  apresia-redirect-error-page
13  d--             0 Nov 21 2018 10:40:04  System Volume Information
14  -rw          4474 Oct 08 2019 17:07:38  apresia-https-certificate
15  -rw          1679 Oct 08 2019 17:07:46  apresia-https-private-key
16  -rw          5434 Oct 08 2019 17:07:52  apresia-webpage-image01

990576640 bytes total (982843392 bytes free)

sw1#
sw1# dir unit2:/d:/

Directory of /unit2:/d:/
1   -rw          1576 Oct 08 2019 17:06:34  apresia-loader.conf
2   -rw       7179528 Oct 08 2019 17:07:18  apresia-software.had
3   -rw          5771 Oct 08 2019 17:07:22  apresia-startup-config.txt
4   -rw             8 Oct 08 2019 17:07:26  apresia-system-name.txt
5   -rw          2391 Oct 08 2019 17:07:28  apresia-rsa-key
6   -rw           905 Oct 08 2019 17:07:32  apresia-dsa-key
7   -rw          2427 Oct 08 2019 17:07:36  apresia-login-page
8   -rw          1332 Oct 08 2019 17:07:38  apresia-login-success-page
9   -rw          1011 Oct 08 2019 17:07:42  apresia-login-failure-page
10  -rw          1013 Oct 08 2019 17:07:46  apresia-logout-success-page
11  -rw          1084 Oct 08 2019 17:07:48  apresia-logout-failure-page
12  -rw          1023 Oct 08 2019 17:07:52  apresia-redirect-error-page
13  -rw          4474 Oct 08 2019 17:07:56  apresia-https-certificate
14  -rw          1679 Oct 08 2019 17:08:00  apresia-https-private-key
15  -rw          5434 Oct 08 2019 17:07:00  apresia-webpage-image01
```

```
16  d--              0 Dec 14 2017 13:58:28  System Volume Information

990560256 bytes total (982827008 bytes free)

sw1#
sw1# dir unit3:/d:/

Directory of /unit3:/d:/
1   d--              0 Oct 08 2019 17:05:12  System Volume Information
2   -rw           1576 Oct 08 2019 17:06:34  apresia-loader.conf
3   -rw        7179528 Oct 08 2019 17:07:18  apresia-software.had
4   -rw           5771 Oct 08 2019 17:07:20  apresia-startup-config.txt
5   -rw              8 Oct 08 2019 17:07:22  apresia-system-name.txt
6   -rw           2391 Oct 08 2019 17:07:24  apresia-rsa-key
7   -rw            905 Oct 08 2019 17:07:26  apresia-dsa-key
8   -rw           2427 Oct 08 2019 17:07:28  apresia-login-page
9   -rw           1332 Oct 08 2019 17:07:28  apresia-login-success-page
10  -rw           1011 Oct 08 2019 17:07:30  apresia-login-failure-page
11  -rw           1013 Oct 08 2019 17:07:32  apresia-logout-success-page
12  -rw           1084 Oct 08 2019 17:07:36  apresia-logout-failure-page
13  -rw           1023 Oct 08 2019 17:07:38  apresia-redirect-error-page
14  -rw           4474 Oct 08 2019 17:07:40  apresia-https-certificate
15  -rw           1679 Oct 08 2019 17:07:44  apresia-https-private-key
16  -rw           5434 Oct 08 2019 17:07:46  apresia-webpage-image01

990560256 bytes total (982843392 bytes free)

sw1#
sw1# show boot

Unit 1
*(Configured)
 Primary boot image: /c:/AEOS-NP2000_R10701.had
 Primary boot config: /c:/primary.cfg
 Secondary boot image: /c:/AEOS-NP2000_R10701_sec.had
 Secondary boot config: /c:/secondary.cfg
(SD Card)
 Primary boot image: /d:/apresia-software.had
 Primary boot config: /d:/apresia-startup-config.txt

Unit 2
*(Configured)
 Primary boot image: /c:/AEOS-NP2000_R10701.had
 Primary boot config: /c:/primary.cfg
 Secondary boot image: /c:/AEOS-NP2000_R10701_sec.had
 Secondary boot config: /c:/secondary.cfg
(SD Card)
 Primary boot image: /d:/apresia-software.had
 Primary boot config: /d:/apresia-startup-config.txt

Unit 3
*(Configured)
 Primary boot image: /c:/AEOS-NP2000_R10701.had
 Primary boot config: /c:/primary.cfg
 Secondary boot image: /c:/AEOS-NP2000_R10701_sec.had
 Secondary boot config: /c:/secondary.cfg
(SD Card)
 Primary boot image: /d:/apresia-software.had
 Primary boot config: /d:/apresia-startup-config.txt
```

```
Note: * indicates the used boot information.

sw1#
```

12.3 SD カードブート使用装置での設定保存動作

SD カードブートを使用する装置は、SD カードを挿入したまま運用します。**write memory** コマンドまたは **copy running-config startup-config** コマンドを実行して設定を保存すると、ローカルフラッシュのプライマリーで指定した構成情報だけでなく、SD カードの「apresia-startup-config.txt」にも設定が保存されます。スタック構成で **write memory** コマンドを実行した場合も同様に、すべてのスタックメンバーで、ローカルフラッシュのプライマリーで指定した構成情報と SD カードの「apresia-startup-config.txt」に設定が保存されます。

SD カードを挿入した状態で **write memory** コマンドを実行した場合の動作例を以下に示します。

```
sw1# write memory

Destination filename startup-config? [y/n]:  y

Saving all configurations to NV-RAM.......... Done.
Saving all configurations to SD-Card......... Done.

sw1#
```

12.4 装置故障時の交換手順

準備しておいた SD カードブート用の SD カードを代替装置に挿入して起動するだけで、元の装置と同じ状態で代替装置を起動できます。

> ***NOTE:*** SD カードブートを使用して代替装置を起動する場合は、交換前と同じ製品名の装置に挿入して使用してください。同じシリーズでも、異なる製品名の装置への挿入はサポートしていません。

1. 故障した装置から SD カードを取り外します。
2. 故障した装置からすべてのケーブルを取り外します。
3. 代替装置に SD カードを挿入します。
4. 代替装置にすべてのケーブルを接続します。
5. 代替装置の電源を入れます。

ローカルフラッシュの構成情報とブートイメージファイルを更新する場合

SD カードブートで代替装置を起動した後も、ローカルフラッシュのプライマリーで指定した構成情報とブートイメージファイルは更新されません。SD カードを挿入したまま運用するため問題ありませんが、万一 SD カードが故障した場合などに備え、ローカルフラッシュのプライマリーで指定した構成情報とブートイメージファイルを更新することもできます。たとえば、以下の更新方法があります。

- ローカルフラッシュのプライマリーで指定した構成情報を更新するには、**`write memory`** コマンドまたは **`copy running-config startup-config`** コマンドで設定を保存してください。
- ローカルフラッシュのプライマリーで指定したブートイメージファイルを更新するには、**`copy`** コマンドなどでブートイメージファイルをローカルフラッシュにコピーしてから、**`boot image`** コマンドで再設定してください。

13. ミラーリング

ミラーリングの機能、状態の確認方法、および構成例と設定例について説明します。

REF: コマンドの詳細については、『コマンドリファレンス』を参照してください。

13.1 ミラーリングの機能説明

ミラーリングは、指定した送信元インターフェースで送受信するトラフィックをコピーし、ミラーリングトラフィックを宛先インターフェースから送信する機能です。

13.1.1 送信元インターフェースと宛先インターフェースの設定

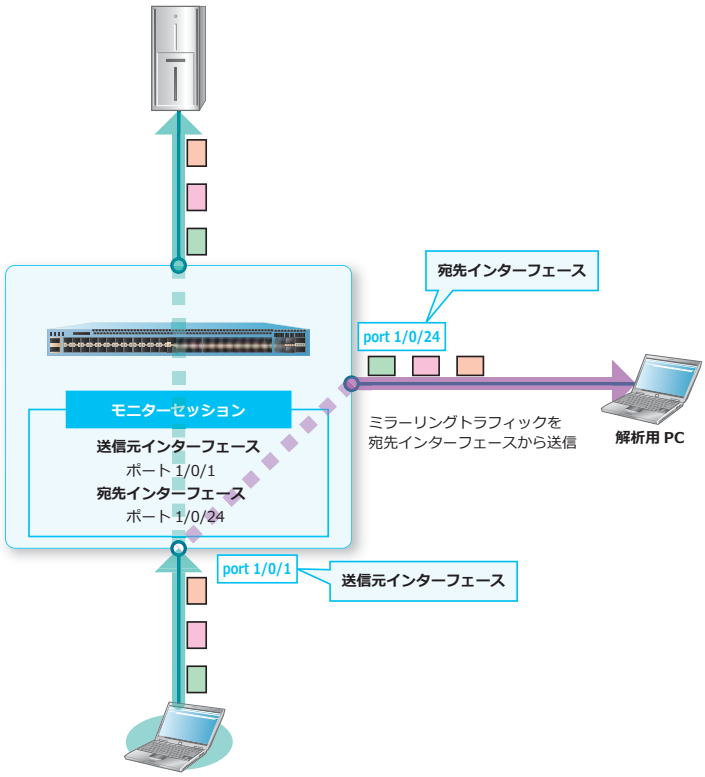
ミラーリングを利用するには、モニターセッションを作成し、送信元インターフェースと宛先インターフェースを設定します。1 つのモニターセッションには、複数の送信元インターフェースを設定できます。また、1 つのモニターセッションには、宛先インターフェースを 1 つだけ設定できます。

ローカルモニターセッション

送信元インターフェースと宛先インターフェースが同じ装置にある場合は、**ローカルモニターセッション**を使用します。送信元インターフェースを設定するには、**`monitor session source interface`** コマンドを使用します。宛先インターフェースを設定するには、**`monitor session destination interface`** コマンドを使用します。

NOTE: NP5000 の 1.08.01 以降では、最大 2 個のローカルモニターセッションまで、同一インターフェースをそれぞれのモニターセッションに送信元インターフェースとして設定できます。

図 13-1 ローカルモニターセッションの概要



リモートモニターセッション

ネットワーク上にある他の装置で送受信されているトラフィックをミラーリングする場合は、**リモートモニターセッション**を使用します。

リモートモニターセッションでは、ミラーリングトラフィックをリモートモニター VLAN のタグ付きフレームとして伝送します。また、リモートモニター VLAN に設定した VLAN では、MAC アドレス学習が無効になります。VLAN をリモートモニター VLAN として設定するには、**remote-span** コマンドを使用します。

リモートモニターセッションの各装置では、以下のように設定します。

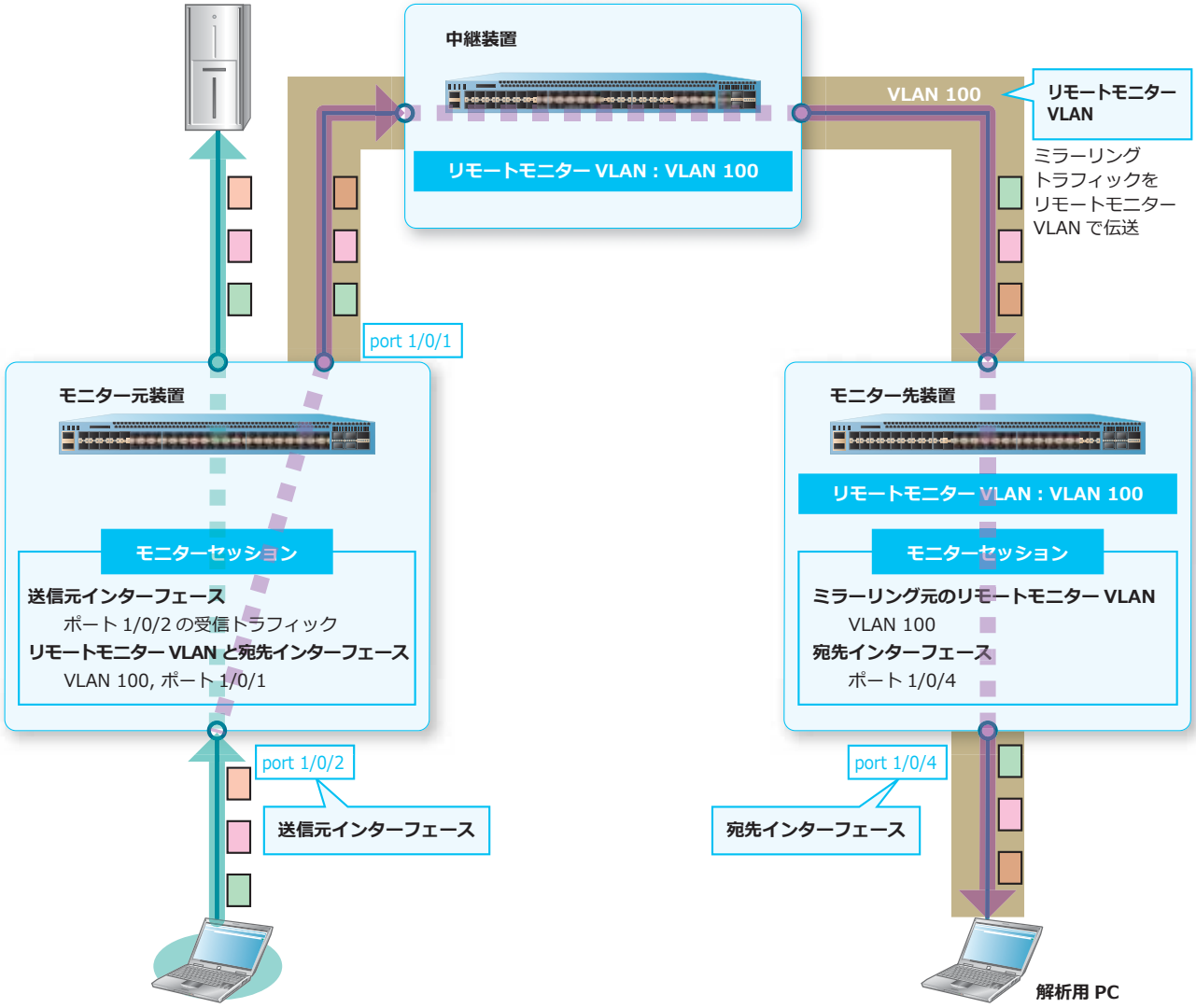
表 13-1 リモートモニターセッションの各装置の設定

装置種別	設定内容とコマンド
モニター元装置 *1	• 送信元インターフェースの設定 **monitor session source interface** コマンド • リモートモニター VLAN と宛先インターフェースの設定 **monitor session destination remote vlan** コマンド
中継装置	• リモートモニター VLAN の設定 **remote-span** コマンド、各種 VLAN 設定（リモートモニター VLAN のタグ付きフレームを送受信できるように VLAN 設定を行う）
モニター先装置	• リモートモニター VLAN の設定 **remote-span** コマンド、各種 VLAN 設定（リモートモニター VLAN のタグ付きフレームを送受信できるように VLAN 設定を行う） • ミラーリング元のリモートモニター VLAN の設定 **monitor session source remote vlan** コマンド • 宛先インターフェースの設定 **monitor session destination interface** コマンド

*1：モニター元装置では、リモートモニター VLAN を設定しなくても動作します。

CAUTION: モニター先装置では、ミラーリングトラフィック（リモートモニター VLAN のタグ付きフレーム）を受信するインターフェースに、**switchport trunk allowed vlan** コマンドでリモートモニター VLAN を設定してください。また、**monitor session destination interface** コマンドで設定した宛先インターフェースにも、**switchport access vlan** コマンドでリモートモニター VLAN を設定してください。

図 13-2 リモートモニターセッションの概要

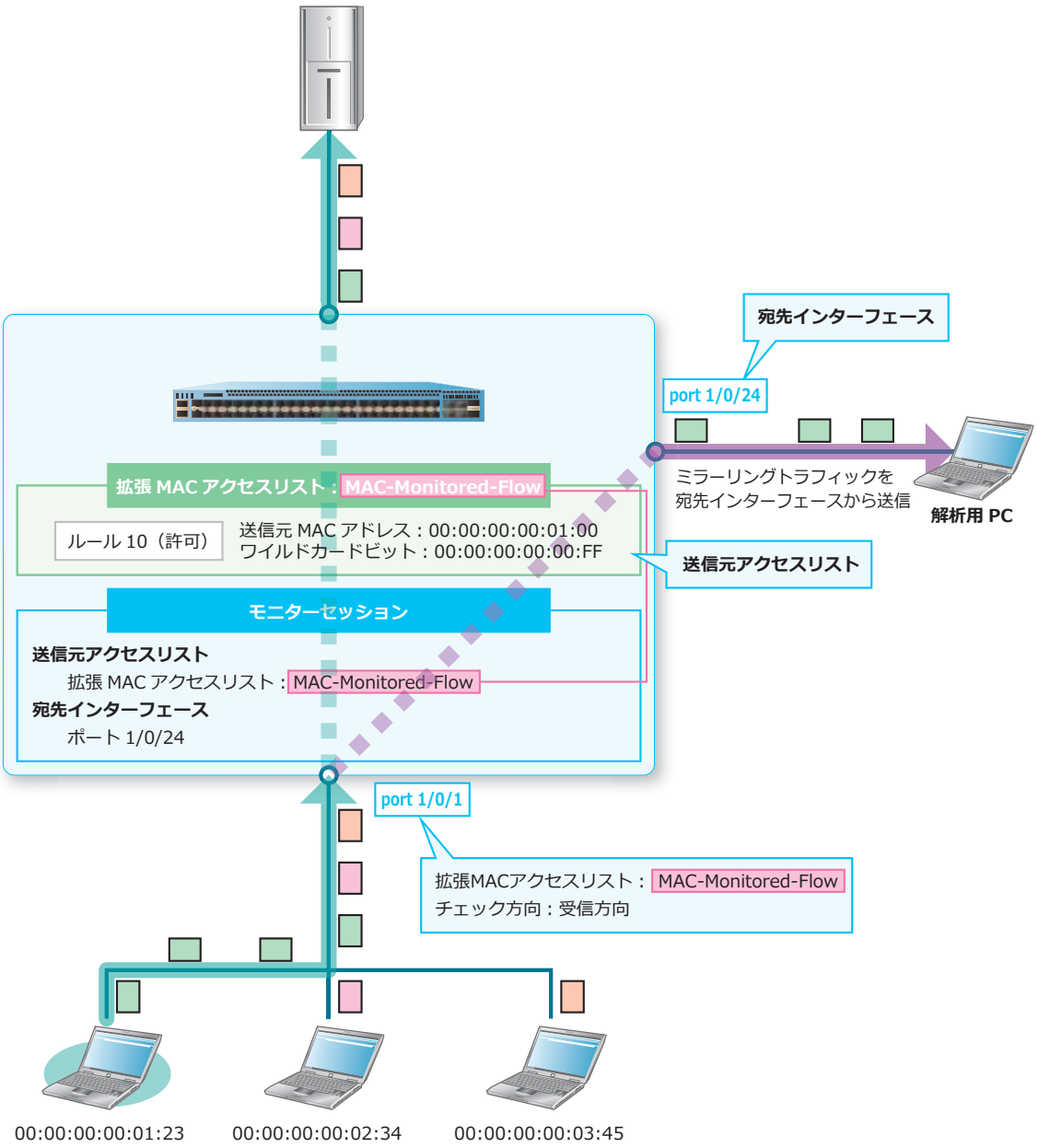


13.1.2 送信元アクセスリストによるミラーリング対象の指定

送信元アクセスリストを使用して、ミラーリングする受信トラフィックを指定できます。指定するアクセスリストは、**expert access-group** コマンド、**mac access-group** コマンド、**ip access-group** コマンド、**arp access-group** コマンド、または **ipv6 access-group** コマンドで受信方向を指定してモニター対象のポートに適用するか、または VLAN アクセスマップコマンドを介してモニター対象の VLAN に適用する必要があります。

送信元アクセスリストを利用する場合は、**monitor session source acl** コマンドを使用します。

図 13-3 送信元アクセスリストの概要



NOTE: **monitor session source acl** コマンドでは、受信方向に適用されたアクセスリスト（例：ip access-group TEST in）を指定します。送信方向に適用されたアクセスリスト（例：ip access-group TEST out）を指定しても、送信トラフィックはミラーリングできません。

NOTE: 指定したアクセスリストの permit ルールにマッチしたトラフィックだけでなく、deny ルールにマッチしたトラフィックもミラーリングされます。

NOTE: 拡張エキスパートアクセスリスト／ IP アクセスリストを使用した場合は、IPv4 パケットが対象になります。

NOTE: 拡張 MAC アクセスリストを使用した場合は、非 IP パケットが対象になります。拡張 MAC アクセスリストの IP パケット対象化機能を有効にした場合は、IPv4 パケットおよび IPv6 パケットも対象になります。

NOTE: ARP アクセスリストを使用した場合は、ARP パケットが対象になります。

NOTE: IPv6 アクセスリストを使用した場合は、IPv6 パケットが対象になります。

13.1.3 モニターセッションの上限

NP3000、NP2100、NP2000、および NP2500 では、モニターセッションは装置全体で最大 4 個まで設定できます。なお、送信元インターフェース設定に tx 指定を含めることができるモニターセッションは、1 個だけです。

NP7000、NP5000、および NP4000 では、モニターセッションは装置全体で最大 4 リソースまで設定できます。リソースの数え方は以下のとおりです。

- 送信元インターフェース設定に rx 指定（送信元アクセスリスト含む）と tx 指定の両方を含むモニターセッションの場合は、2 リソース
- 送信元インターフェース設定が rx 指定（送信元アクセスリスト含む）のみのモニターセッションの場合は、1 リソース
- 送信元インターフェース設定が tx 指定のみのモニターセッションの場合は、1 リソース

13.2 ミラーリングの状態確認

ミラーリングの状態を表示して確認する方法を説明します。

13.2.1 モニターセッションの設定の表示

show monitor session コマンドで、モニターセッションの設定を確認できます。

モニターセッション 1 を指定した場合の表示例を以下に示します。

```
# show monitor session 1

 Session 1 ...(1)
     Session Type: local session ...(2)
     Destination Port: Port1/0/1 ...(3)
     Flow Based Source: IPv4-Monitor-List ...(4)
     Source Ports: ...(5)
         Both:
             Port1/0/4
         RX:
             Port1/0/3
         TX:
             Port1/0/2

 Total Entries: 1
```

各項目の説明は、以下のとおりです。

表 13-2 show monitor session コマンドの表示項目

項番	説明
(1)	セッション番号を表示します。
(2)	セッションタイプを表示します。 • local session：ローカルモニターセッション • remote source session：リモートモニターセッション（モニター元装置） • remote destination session：リモートモニターセッション（モニター先装置）
(3)	モニターセッションの宛先インターフェース（ポート番号またはポートチャネル番号）を表示します。
(4)	モニターセッションの送信元アクセスリストを表示します。
(5)	モニターセッションの送信元インターフェース（ポート番号またはポートチャネル番号）を表示します。 • Both：ミラーリング対象が受信フレームおよび送信フレームの送信元インターフェース • RX：ミラーリング対象が受信フレームのみの送信元インターフェース • TX：ミラーリング対象が送信フレームのみの送信元インターフェース

13.2.2 リモートモニターセッションの設定の表示

show monitor session remote コマンドで、リモートモニターセッションの設定を確認できます。

表示例を以下に示します。

```
# show monitor session remote

 Session 1 ...(1)
     Session Type: remote source session ...(2)
     Destination Remote VLAN: VLAN 2001 ...(3)
     Destination Port: Port1/0/19 ...(4)
     Source Ports: ...(5)
         RX:
             Port1/0/10

 Session 4 ...(1)
     Session Type: remote destination session ...(2)
     Source Remote VLAN: VLAN 4090 ...(6)
     Destination Port: Port1/0/48 ...(4)

 Total Entries: 2
```

各項目の説明は、以下のとおりです。

表 13-3 show monitor session remote コマンドの表示項目

項番	説明
(1)	セッション番号を表示します。
(2)	セッションタイプを表示します。 • local session：ローカルモニターセッション • remote source session：リモートモニターセッション（モニター元装置） • remote destination session：リモートモニターセッション（モニター先装置）
(3)	リモートモニターセッション（モニター元装置）で設定した、リモートモニター VLAN を表示します。
(4)	モニターセッションの宛先インターフェース（ポート番号またはポートチャネル番号）を表示します。
(5)	モニターセッションの送信元インターフェース（ポート番号またはポートチャネル番号）を表示します。 • Both：ミラーリング対象が受信フレームおよび送信フレームの送信元インターフェース • RX：ミラーリング対象が受信フレームのみの送信元インターフェース • TX：ミラーリング対象が送信フレームのみの送信元インターフェース
(6)	リモートモニターセッション（モニター先装置）で設定した、ミラーリング元のリモートモニター VLAN を表示します。

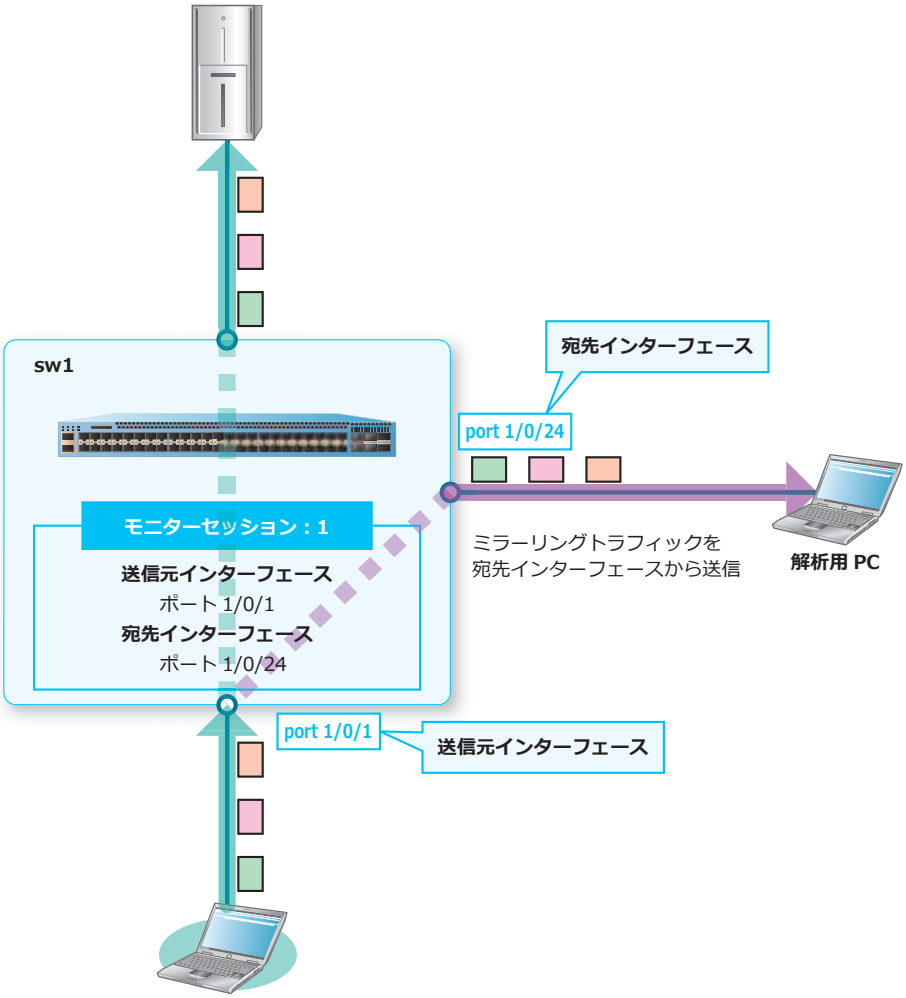
13.3 ミラーリングの構成例と設定例

ミラーリングを利用する場合の構成例と設定例を示します。

13.3.1 ローカルモニターセッションを利用する場合

ローカルモニターセッションを作成して、ポート 1/0/1 で送受信するトラフィックをミラーリングする場合の構成例と設定例を示します。

図 13-4 ローカルモニターセッションを利用する場合の構成例



1. モニターセッション［1］の送信元インターフェースを［ポート 1/0/1］に設定します。

```
sw1# configure terminal
sw1(config)# monitor session 1 source interface port 1/0/1
sw1(config)#
```

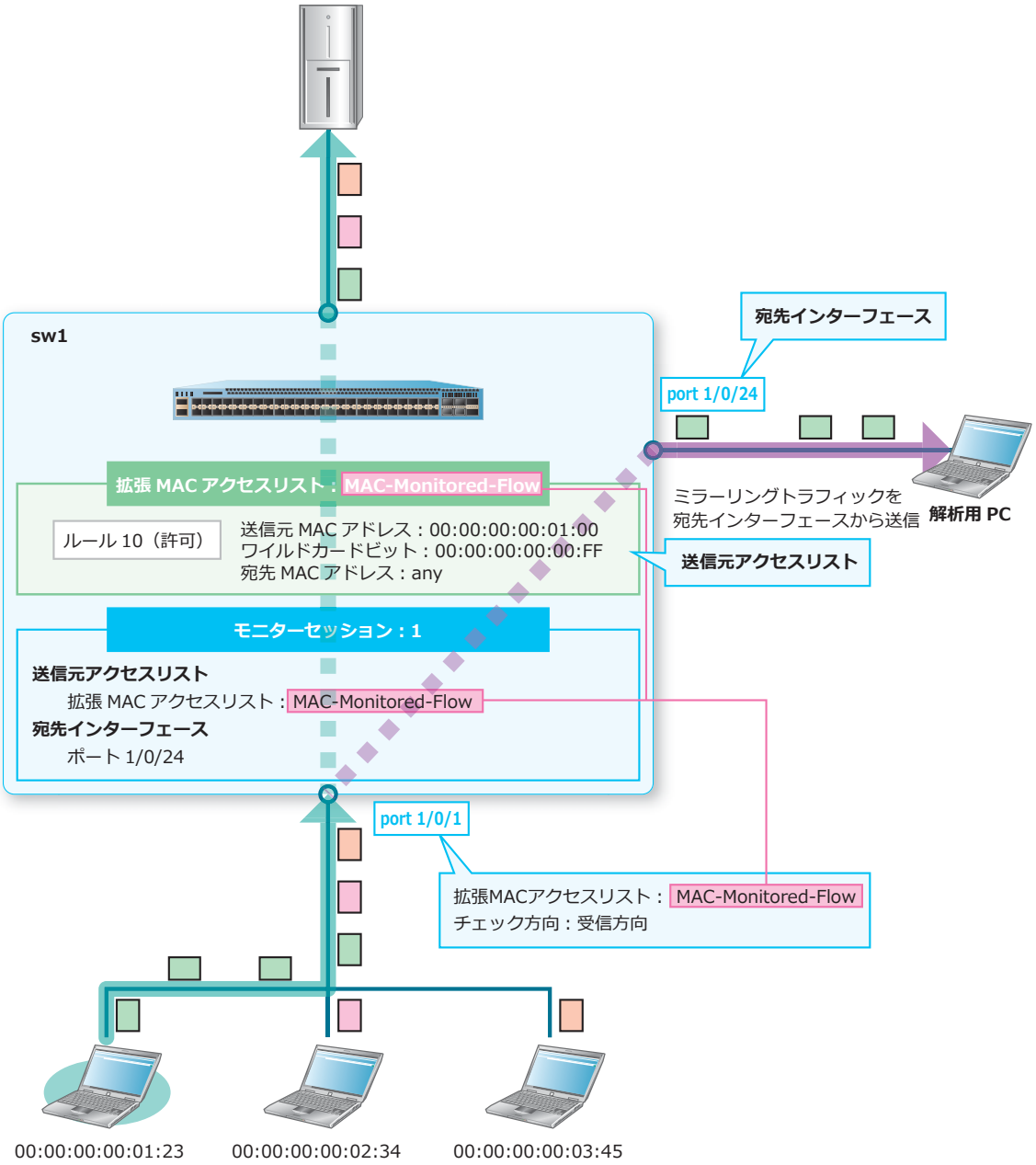
2. モニターセッション［1］の宛先インターフェースを［ポート 1/0/24］に設定します。

```
sw1(config)# monitor session 1 destination interface port 1/0/24
sw1(config)# end
sw1#
```

13.3.2 送信元アクセスリストを使用してミラーリングする場合

ローカルモニターセッションを作成して、ポート 1/0/1 で受信する MAC アドレスが 00:00:00:00:01:XX（XX の部分は任意）の非 IP パケットのトラフィックをミラーリングする場合の構成例と設定例を示します。

図 13-5 送信元アクセスリストを使用してミラーリングする場合の構成例



1. 拡張 MAC アクセスリスト［MAC-Monitored-Flow］を作成します。

```
sw1# configure terminal
sw1(config)# mac access-list extended MAC-Monitored-Flow
sw1(config-mac-ext-acl)#
```

2. ミラーリング対象として指定するルールを以下のように設定します。

ルール 10（許可）：送信元 MAC アドレス［00:00:00:00:01:00］、ワイルドカードビット［00:00:00:00:00:FF］、宛先 MAC アドレス［any］

```
sw1(config-mac-ext-acl)# 10 permit 0000.0000.0100 0000.0000.00ff any
sw1(config-mac-ext-acl)# exit
sw1(config)#
```

3. 設定した拡張 MAC アクセスリストを、ポート 1/0/1 に受信方向で適用します。

```
sw1(config)# interface port 1/0/1
sw1(config-if-port)# mac access-group MAC-Monitored-Flow in
sw1(config-if-port)# exit
sw1(config)#
```

4. モニターセッション［1］の送信元アクセスリストを［拡張 MAC アクセスリスト：MAC-Monitored-Flow］に設定します。

```
sw1(config)# monitor session 1 source acl MAC-Monitored-Flow
sw1(config)#
```

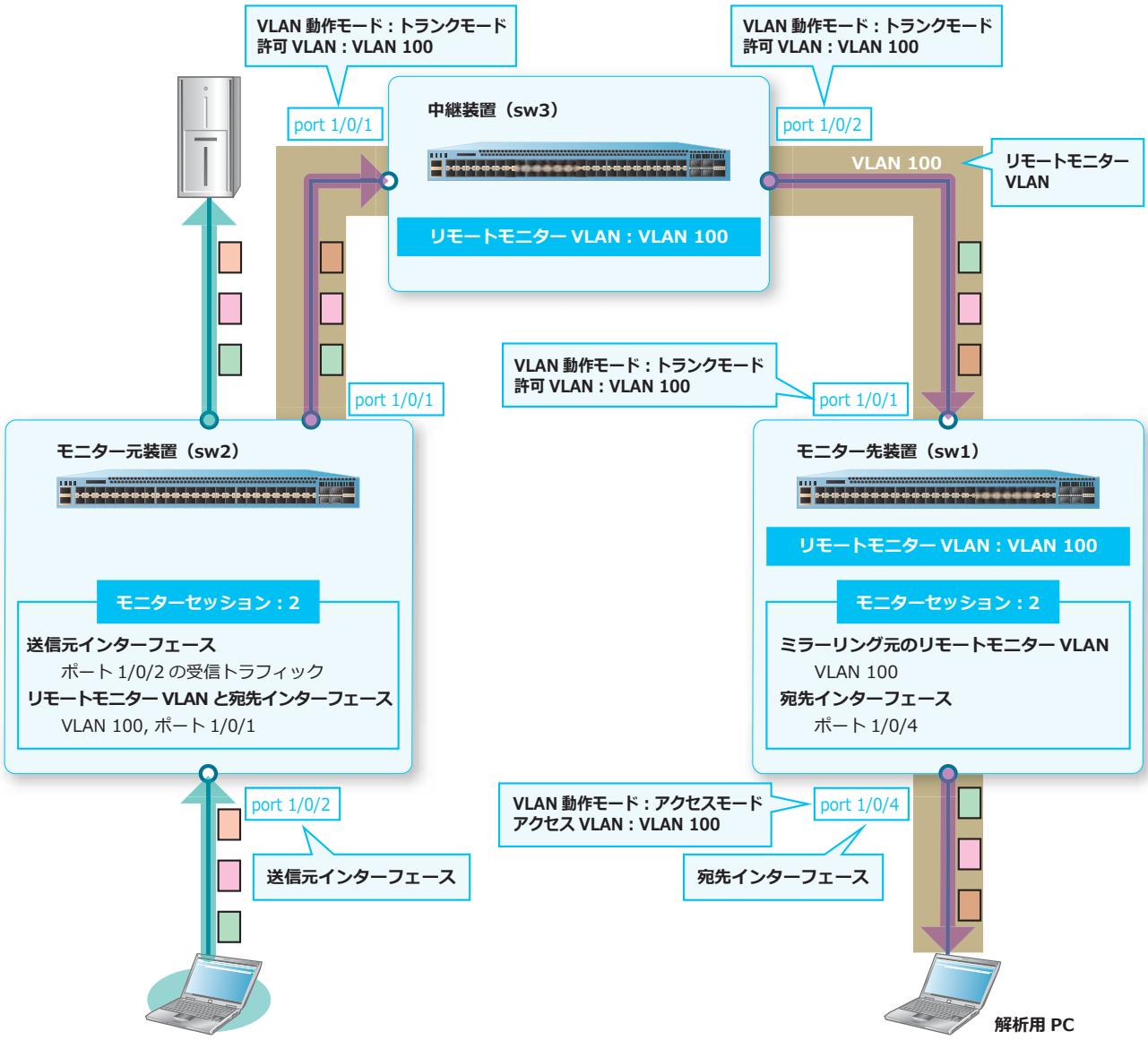
5. モニターセッション［1］の宛先インターフェースを［ポート 1/0/24］に設定します。

```
sw1(config)# monitor session 1 destination interface port 1/0/24
sw1(config)# end
sw1#
```

13.3.3 リモートモニターセッションを利用する場合

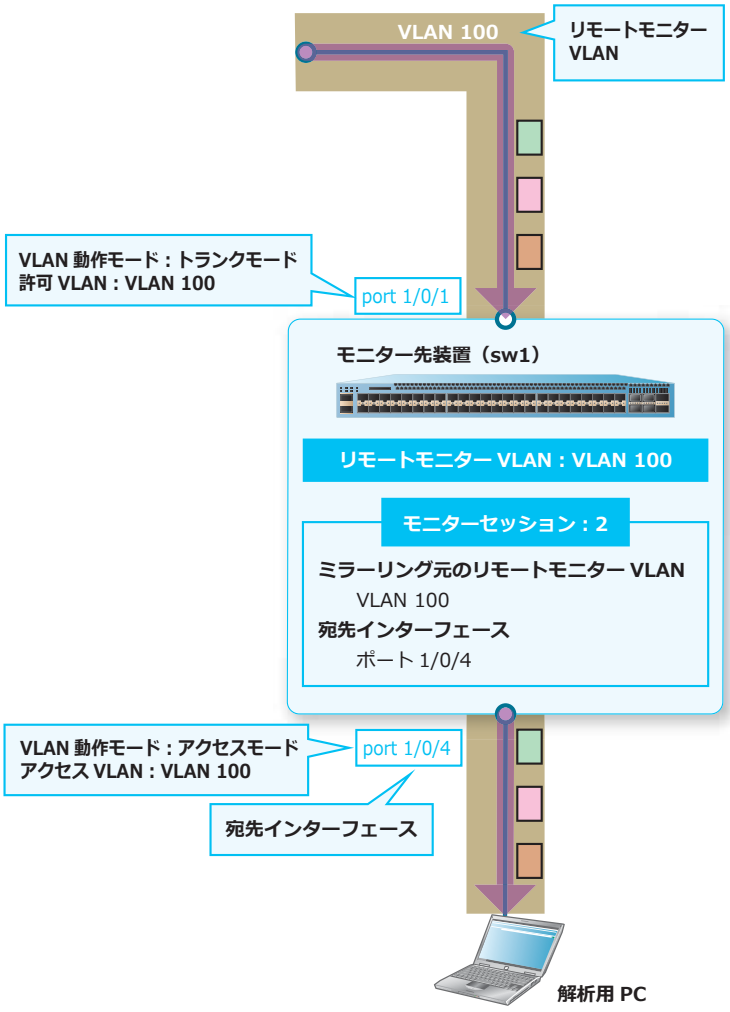
リモートモニターセッションを作成して、他の装置で送受信されているトラフィックをミラーリングする場合の構成例と設定例を示します。この例では、sw2 のポート 1/0/2 で受信したトラフィックを、sw1 のポート 1/0/4 にミラーリングしています。

図 13-6 リモートモニターセッションを利用する場合の構成例



13.3.3.1 宛先インターフェースが存在するモニター先装置の設定例（sw1）

図 13-7 リモートモニターセッションを利用する場合の設定例（sw1）



1. VLAN 100 を作成し、リモートモニター VLAN として設定します。

```
sw1# configure terminal
sw1(config)# vlan 100
sw1(config-vlan)# remote-span
sw1(config-vlan)# exit
sw1(config)#
```

2. ポート 1/0/1 をトランクポートとして設定し、トランクポートに［VLAN 100］を割り当てます。

```
sw1(config)# interface port 1/0/1
sw1(config-if-port)# switchport mode trunk
sw1(config-if-port)# switchport trunk allowed vlan 100
sw1(config-if-port)# exit
sw1(config)
```

3. ポート 1/0/4 をアクセスポートとして設定し、アクセスポートに［VLAN 100］を割り当てます。

```
sw1(config)# interface port 1/0/4
sw1(config-if-port)# switchport mode access
sw1(config-if-port)# switchport access vlan 100
sw1(config-if-port)# exit
sw1(config)
```

4. モニターセッション［2］のミラーリング元のリモートモニター VLAN を［VLAN 100］に設定します。

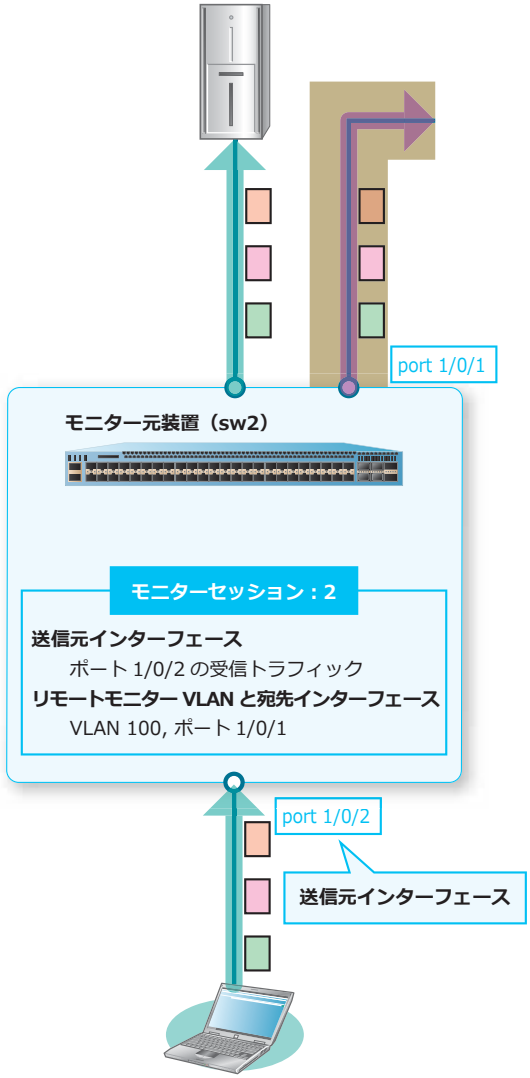
```
sw1(config)# monitor session 2 source remote vlan 100
sw1(config)
```

5. モニターセッション［2］の宛先インターフェースを［ポート 1/0/4］に設定します。

```
sw1(config)# monitor session 2 destination interface port 1/0/4
sw1(config)# end
sw1#
```

13.3.3.2 送信元インターフェースが存在するモニター元装置の設定例（sw2）

図 13-8 リモートモニターセッションを利用する場合の設定例（sw2）



1. モニターセッション［2］の送信元インターフェースを［ポート 1/0/2 の受信トラフィック］に設定します。

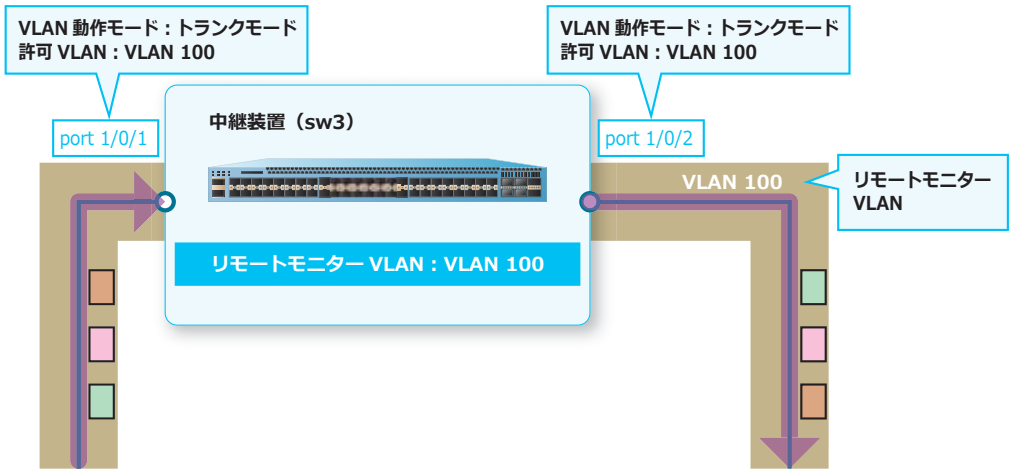
```
sw2# configure terminal
sw2(config)# monitor session 2 source interface port 1/0/2 rx
sw2(config)#
```

2. モニターセッション［2］のリモートモニター VLAN と宛先インターフェースを［VLAN 100、ポート 1/0/1］に設定します。

```
sw2(config)# monitor session 2 destination remote vlan 100 interface port 1/0/1
sw2(config)# end
sw2#
```

13.3.3.3 リモートモニターセッションの中継装置の設定例（sw3）

図 13-9 リモートモニターセッションを利用する場合の設定例（sw3）



1. VLAN 100 を作成し、リモートモニター VLAN として設定します。

```
sw3# configure terminal
sw3(config)# vlan 100
sw3(config-vlan)# remote-span
sw3(config-vlan)# exit
sw3(config)#
```

2. ポート 1/0/1 およびポート 1/0/2 をトランクポートとして設定し、トランクポートに［VLAN 100］を割り当てます。

```
sw3(config)# interface port 1/0/1
sw3(config-if-port)# switchport mode trunk
sw3(config-if-port)# switchport trunk allowed vlan 100
sw3(config-if-port)# exit
sw3(config)# interface port 1/0/2
sw3(config-if-port)# switchport mode trunk
sw3(config-if-port)# switchport trunk allowed vlan 100
sw3(config-if-port)# end
sw3#
```

14. TFTP/FTP/SFTP

TFTP/FTP/SFTP の機能、および実施例について説明します。

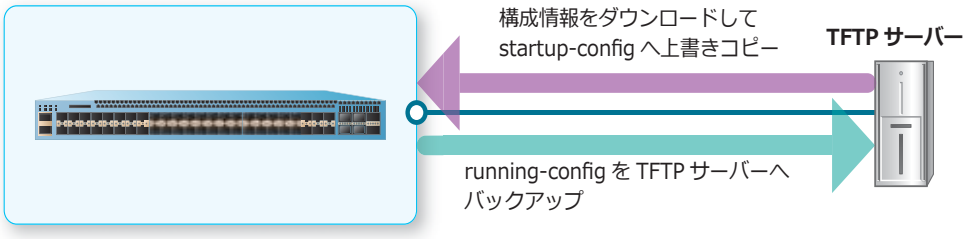
REF: コマンドの詳細については、『コマンドリファレンス』を参照してください。

14.1 TFTP/FTP/SFTP の機能説明

NOTE: SFTP は、NP7000 の 1.10.02 以降、NP2100 の 1.11.01 以降、NP2500 の 1.13.01 以降でサポートしています。

startup-config、running-config、システムログ、およびその他のファイルを転送（コピー）できます。たとえば、構成情報を TFTP サーバーからダウンロードして、装置の startup-config へ上書きコピーしたり、装置の running-config を TFTP サーバーへバックアップしたりできます。

図 14-1 TFTP サーバーとのファイル転送（コピー）



ファイルを転送（コピー）するには、**copy** コマンドを使用します。

コピー元として指定できるファイル

コピー元として指定できるファイルは以下のとおりです。

- startup-config
- running-config
- ローカルフラッシュまたは外部ストレージに保存されているファイル
- システムログ
- TFTP/FTP/SFTP サーバーに保存されているファイル

コピー先として指定できるファイル

コピー先として指定できるファイル、ファイルシステム、およびサーバーは以下のとおりです。

- startup-config
- running-config
- ローカルフラッシュまたは外部ストレージ
- TFTP/FTP/SFTP サーバー

TFTP/FTP/SFTP で実施できる操作

TFTP/FTP/SFTP で実施できる主な操作を以下に示します。

- ファイルシステム内のファイルを、別のファイルにコピーする
- startup-config または running-config をバックアップする（ファイルシステム内のファイルにコピーする、または TFTP/FTP/SFTP サーバーにアップロードする）
- startup-config または running-config を、TFTP/FTP/SFTP サーバーからダウンロードする
- ブートイメージファイルを、TFTP/FTP/SFTP サーバーからダウンロードする
- システムログを、TFTP/SFTP サーバーにアップロードする

CAUTION: SFTP の IPv6 アドレスでの使用は未サポートです。SFTP は IPv4 アドレスで使用してください。

CAUTION: SIZE コマンド（RFC 3659 規格）に対応する FTP サーバーのみ指定できます。

CAUTION: **copy {tftp: | ftp: | sftp:} startup-config** コマンドは、指定した構成情報のスタック設定を含めてコピーします。そのため、スタック構成の装置に対しては実行しないでください。

NOTE: コピー先として startup-config を指定した場合は、コピー元ファイルが保存されている場所によって動作が異なります。ローカルフラッシュまたは外部ストレージに保存されているファイルをコピー元に指定したときは、**boot config** コマンドで設定したファイル名がコピー元ファイル名に変更されます。一方、その他の場所に保存されているファイルをコピー元に指定したときは、**boot config** コマンドで設定したファイルの内容が上書きされます。

NOTE: コピー先として running-config を指定した場合は、現在動作中の設定（running-config）に、コピー元に指定した構成情報ファイルの内容が流し込みされます。そのため、上書き可能な設定は上書きされますが、上書き不可の設定は設定されません。

NOTE: コピー元として log を指定した場合は、コピー先には TFTP/SFTP サーバーのみ指定できます。

NOTE: ダウンロードしたブートイメージファイルを次回起動時に使用する場合は、**boot image** コマンドで指定してください。

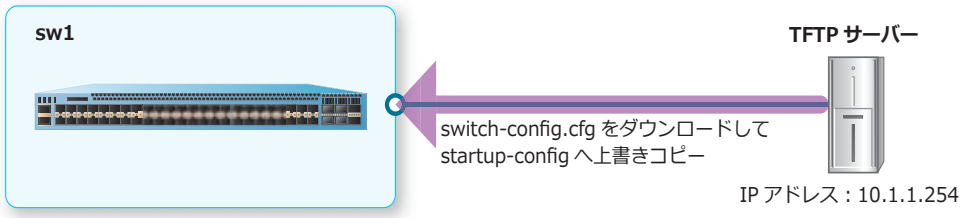
14.2 TFTP/FTP/SFTP の実施例

TFTP/FTP/SFTP を利用する場合の実施例を示します。

14.2.1 TFTP サーバーから startup-config へダウンロードする場合

TFTP サーバーから構成情報をダウンロードして、startup-config に上書きする場合の実施例を示します。

図 14-2 TFTP サーバーから startup-config へダウンロードする場合の構成例



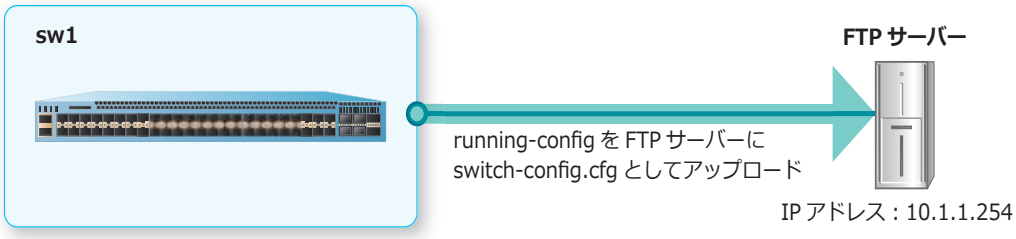
IP アドレスが［10.1.1.254］の TFTP サーバーから構成情報［switch-config.cfg］をダウンロードして、startup-config へ上書きコピーします。

```
sw1# copy tftp: //10.1.1.254/switch-config.cfg startup-config

Address of remote host [10.1.1.254]?
Source filename [switch-config.cfg]?
Destination filename startup-config? [y/n]:  y

 Accessing tftp://10.1.1.254/switch-config.cfg...
 Transmission start...
 Transmission finished, file length 2830 bytes.
 Please wait, programming flash.............. Done.

sw1#
```

14.2.2 running-config を FTP サーバーへアップロードする場合

running-config をバックアップするために、FTP サーバーへアップロードする場合の実施例を示します。

図 14-3 running-config を FTP サーバーへアップロードする場合の構成例



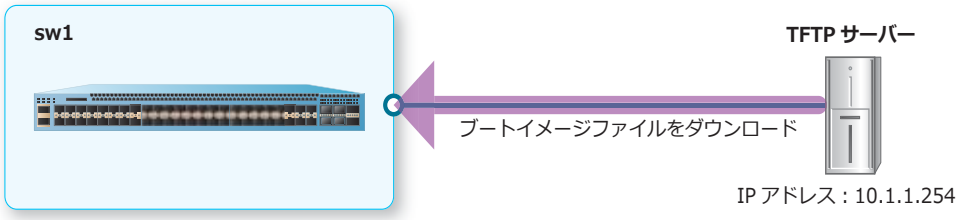
running-config を、IP アドレスが［10.1.1.254］の FTP サーバーに、ファイル名を［switch-config.cfg］としてアップロードします。FTP サーバーにコピーする場合は FTP サーバーのユーザーアカウントとパスワードが必要ですが、この例ではユーザーアカウント［apresia-user］とパスワードを入力しています。

```
sw1# copy running-config ftp:

Address of remote host []? 10.1.1.254
Destination username [Anonymous]? apresia-user
Destination password []? ******
TCP port number of remote host [default]?
Destination filename []? switch-config.cfg
 Accessing ftp://10.1.1.254/switch-config.cfg...
 Transmission start...
 Transmission finished, file length 2885 bytes.

sw1#
```

14.2.3 TFTP サーバーからブートイメージファイルをダウンロードする場合

TFTP サーバーからブートイメージファイルをダウンロードする場合の実施例を示します。

図 14-4 TFTP サーバーからブートイメージファイルをダウンロードする場合の構成例



1. IP アドレスが［10.1.1.254］の TFTP サーバーからブートイメージファイル［AEOS-NP7000_R10601.had］をダウンロードして、ファイル名を［R10601.had］として保存します。

```
sw1# copy tftp: //10.1.1.254/AEOS-NP7000_R10601.had flash: R10601.had

Address of remote host [10.1.1.254]?
Source filename [AEOS-NP7000_R10601.had]?
Destination filename [R10601.had]?
 Accessing tftp://10.1.1.254/AEOS-NP7000_R10601.had...
 Transmission start...
 Transmission finished, file length 11037236 bytes.
 Please wait, programming flash.............. Done.

sw1#
```

2. 次回起動時のブートイメージファイルを［c:/R10601.had］に設定します。

```
sw1# configure terminal
sw1(config)# boot image c:/R10601.had
sw1(config)# end
sw1#
```

15. LLDP

LLDP の機能、状態の確認方法、および構成例と設定例について説明します。

REF: コマンドの詳細については、『コマンドリファレンス』を参照してください。

15.1 LLDP の機能説明

LLDP（Link Layer Discovery Protocol）は、自装置の情報を TLV（type, length, value）形式で定期的に隣接装置に通知したり、隣接装置からの情報を収集したりするプロトコルです。通知できる情報の例は、以下のとおりです。

- シャーシ ID（必須）
- ポート番号（必須）
- ポートの説明（オプション）
- システム名（オプション）
- システムの説明（オプション）

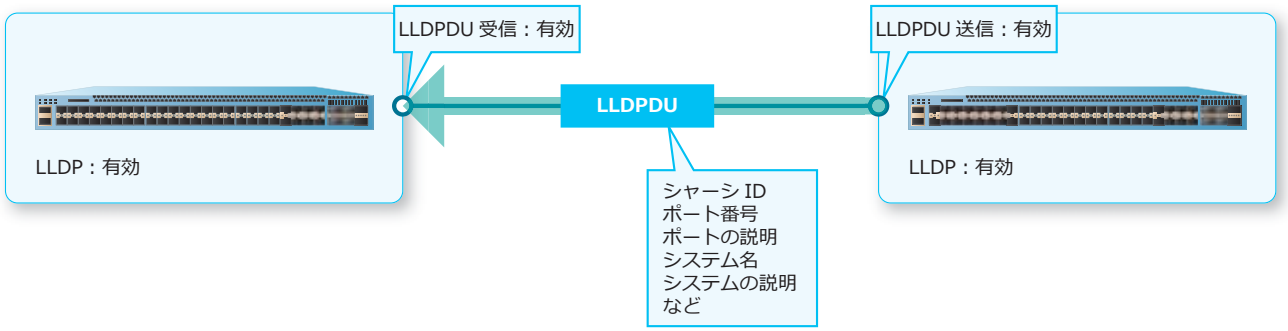
LLDP を使用すると、接続されている隣接装置の情報を、隣接装置にログインすることなく簡単に確認できるようになるため、機器の接続確認や設定変更の際に役立ちます。

15.1.1 LLDP の有効化

LLDP を使用するには、装置全体で LLDP を有効化します。物理ポートごとの LLDPDU（LLDP data unit）の送受信設定はデフォルトで有効です。特定の物理ポートで LLDP を無効にする場合は、その物理ポートの LLDPDU の送受信設定を無効にしてください。

装置全体で LLDP を有効化するには、**`lldp run`** コマンドを使用します。物理ポートごとの LLDPDU 送信設定を変更するには、**`lldp transmit`** コマンドを使用します。物理ポートごとの LLDPDU 受信設定を変更するには、**`lldp receive`** コマンドを使用します。

図 15-1 LLDP の有効化

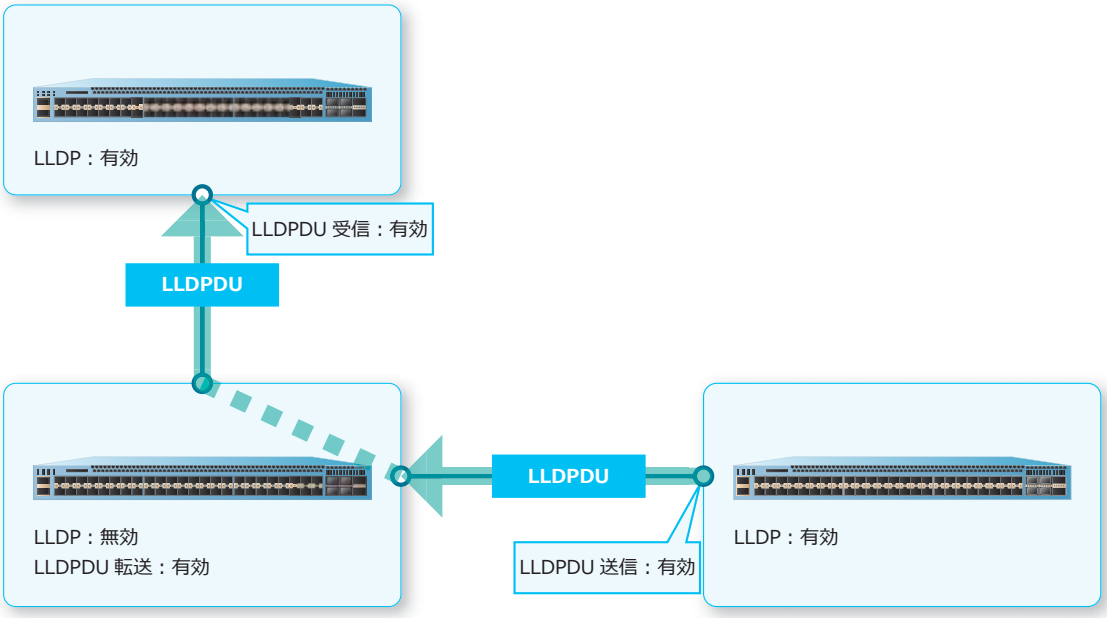


LLDPDU 転送の有効化

装置全体の LLDP を無効にしている装置では、LLDPDU 転送を有効化すると、他の装置から受信した LLDPDU を中継できます。デフォルト設定では、LLDPDU 転送は無効です。LLDPDU 転送の有効／無効を設定するには、**`lldp forward`** コマンドを使用します。

> ***CAUTION:*** 転送される LLDPDU は、送信ポートの種別にかかわらず常にタグなしフレームの形式で転送されます。

図 15-2 LLDPDU 転送の有効化



LLDP 再初期化の遅延時間の設定

LLDP の無効化と有効化を頻繁に実行した際、LLDP の初期化が繰り返し実行されることを避けるために、LLDP 再初期化の遅延時間を設定できます。LLDP が最後に無効化されてから、遅延時間の間は LLDP が有効化されません。LLDP 再初期化の遅延時間は、**`lldp reinit`** コマンドで設定します。

15.1.2 隣接装置に通知する情報の設定

物理ポートごとに、LLDPDU に付加して隣接装置に通知する情報を設定できます。通知できる情報は以下のとおりです。（）内は使用するコマンドです。

- **管理用アドレス（`lldp management-address` コマンド）**

  Management address TLV で通知する管理用アドレスは、装置の VLAN インターフェースまたはループバックインターフェースに設定済みの IP アドレスを指定できます。未設定の IP アドレスや、マネージメントポートに設定した IP アドレスは指定できません。

- **Port ID TLV のサブタイプ（`lldp subtype port-id` コマンド）**

  Port ID TLV のサブタイプを、ポート番号（例：Port1/0/21）または対象ポートの MAC アドレスから選択できます。

- **基本情報（`lldp tlv-select` コマンド）**

  ポートの説明を通知する Port Description TLV（**`port-description`**）、システムの利用可能な能力を通知する System Capabilities TLV（**`system-capabilities`**）、システムの説明を通知する System Description TLV（**`system-description`**）、システム名を通知する System Name TLV（**`system-name`**）のそれぞれを、LLDPDU に付加するかどうかを設定できます。

- **IEEE 802.1 Organizationally Specific TLVs（`lldp dot1-tlv-select` コマンド）**

  Port VLAN ID TLV（**`port-vlan`**）、Port and Protocol VLAN ID TLV（**`protocol-vlan`**）、VLAN Name TLV（**`vlan-name`**）、Protocol Identity TLV（**`protocol-identity`**）のそれぞれを、LLDPDU に付加するかどうかを設定できます。

- **IEEE 802.3 Organizationally Specific TLVs（`lldp dot3-tlv-select` コマンド）**

  MAC/PHY Configuration/Status TLV（**`mac-phy-cfg`**）、Link Aggregation TLV（**`link-aggregation`**）、Maximum Frame Size TLV（**`max-frame-size`**）、Power Via MDI TLV（**`power`**、PoE 対応ポートのみ）のそれぞれを、LLDPDU に付加するかどうかを設定できます。

- **LLDP-MED TLV（`lldp med-tlv-select` コマンド）**

  LLDP-MED Capabilities TLV（**`capabilities`**）、LLDP-MED Inventory Management TLV（**`inventory-management`**）、LLDP-MED Extended Power-via-MDI TLV（**`power-management`**、PoE 対応ポートのみ）のそれぞれを、LLDPDU に付加するかどうかを設定できます。

15.1.3 LLDP で通知する情報の TTL（Time To Live）値

LLDP で通知する情報の **TTL 値**（隣接装置での情報保持時間）を設定できます。TTL 値を超過すると、学習した LLDP 情報は削除されます。

TTL 値は、LLDPDU 送信間隔（秒数）と乗数（Message TX Hold Multiplier）の積で決定されます。たとえば、LLDPDU 送信間隔を 12 秒、乗数を 4 に設定した場合は、TTL 値は、12×4 = 48（秒）となります。

LLDPDU 送信間隔（秒数）は、**`lldp tx-interval`** コマンドで設定します。乗数は、**`lldp hold-multiplier`** コマンドで設定します。

NOTE: LLDPDU 送信間隔は、LLDPDU の送信遅延間隔の 4 倍以上に設定してください。

LLDPDU の送信遅延間隔

装置の情報が変更されてから、LLDPDU を送信するまでの遅延時間を設定できます。この時間を適切に設定することで、装置の情報が短時間に頻繁に変更された際に送信される LLDPDU の数を抑えられます。LLDPDU の送信遅延間隔を設定するには、**`lldp tx-delay`** コマンドを使用します。

NOTE: LLDPDU の送信遅延間隔は、LLDPDU 送信間隔の 4 分の 1 以下に設定してください。

15.1.4 LLDP-MED 対応機器を新規に検出したときの処理回数

LLDP-MED（LLDP for media endpoint discovery）は、機器の設定や管理を効率化するための仕組みです。LLDP-MED 対応機器を新規に検出すると、LLDP-MED TLV が付加された LLDPDU を送信するようになります。ただし、LLDP-MED 対応機器が必要な情報を受信したことを確認できないため、LLDP-MED fast start 処理を一定回数繰り返して実行します。LLDP-MED fast start 処理の実行回数は、**`lldp fast-count`** コマンドで設定します。

15.1.5 LLDP 情報のクリア

LLDPDU を受信して学習した隣接装置の LLDP 情報は TTL 値を超過すると削除されますが、**clear lldp table** コマンドを使用すると手動で削除できます。また、LLDP に関する統計情報は、**clear lldp counters** コマンドで消去できます。

15.1.6 LLDP 疑似リンクダウン機能

LLDP 疑似リンクダウン機能を使用する場合は、自装置と対向装置の両方のポートで有効にして使用してください。LLDP 疑似リンクダウン機能を有効にすると、LLDPDU の受信状態や受信内容に基づいて、ポートを LLDP 疑似リンクダウン状態に遷移／復旧します。

LLDP 疑似リンクダウン機能を有効にしたポートで、リンク障害などによって対向装置からの LLDPDU を受信しなくなったり、対向装置からリンク異常を検知した内容の LLDPDU を受信したりすると、ポートは LLDP 疑似リンクダウン状態に遷移します。

LLDP 疑似リンクダウン機能を有効にしたポートがリンクアップすると、まだ対向装置の情報を取得していない状態では LLDP 疑似リンクダウン状態になります。対向装置の情報を取得すると、LLDP 疑似リンクダウン状態は復旧します。LLDPDU の送信タイミングは対向装置と同期しているわけではないため、自装置側のポートと対向装置側のポートの LLDP 疑似リンクダウン状態の復旧タイミングには時間差が発生することに注意してください。

LLDP 疑似リンクダウン機能を有効にするには、**lldp err-disable** コマンドを使用します。

LLDP 疑似リンクダウン状態の物理ポートは、**show interfaces status** コマンドの Status 項目では "connected" と表示されますが、**show interfaces** コマンドでは "link status is errDis" と表示されます。また、**show interfaces description** コマンドの Status 項目では "errDis" と表示されます。

ポートチャネルのメンバーポートが LLDP 疑似リンクダウン状態になった場合は、**show channel-group channel** コマンドのメンバーポートのステータスは hot-sby になります。

物理ポートで指定した MMRP-Plus のリングポートが LLDP 疑似リンクダウン状態になった場合は、**show mmrp-plus status ring** コマンドや **show mmrp-plus status port** コマンドのポートのリンク状態（Link Status 項目）は "errDis" と表示され、その MMRP-Plus リングポートはダウンします。

15.1.6.1 LLDP 疑似リンクダウン使用時の制限事項

- LLDP 疑似リンクダウン機能と LACP は、同一ポートで併用できません。
- 物理ポートで LLDP 疑似リンクダウン機能と STP/RSTP/MSTP/RPVST+/ERPS 機能は併用できません。
- LLDP 疑似リンクダウン状態の物理ポートは、VLAN インターフェースではリンクアップしているポートとして扱われます。
- ポートチャネル（スタティックモード）のメンバーポートで LLDP 疑似リンクダウン機能を使用している場合、LLDP 疑似リンクダウン状態の復旧タイミングは自装置と対向装置で同期していないため、リンクアップ後にポートチャネルのメンバーポートとして復旧するタイミングも同期しないことに注意してください。たとえば、自装置側ポートが先にメンバーポートとして復旧し、対向装置側ポートがまだ復旧していない状態では、自装置側のそのポートから送信したトラフィックは対向装置側で破棄されます。
- ApresiaNP シリーズでは、「Chassis ID と Port ID の組み合わせが同じ LLDPDU」を複数ポートで受信するような使い方はできません。各ポートで受信する LLDPDU は、「Chassis ID と Port ID の組み合わせがユニークな LLDPDU」になるようにして使用してください。

15.2 LLDP の状態確認

LLDP の状態を表示して確認する方法を説明します。

15.2.1 隣接装置の LLDP 情報の表示

学習した隣接装置の LLDP 情報を確認できます。

隣接装置の LLDP 情報の表示（標準モード）

show lldp neighbors interface コマンドで、隣接装置の LLDP 情報を標準モードで確認できます。

ポート 1/0/15 を指定した場合の表示例を以下に示します。

```
# show lldp neighbors interface port 1/0/15

Port ID: Port1/0/15 ...(1)
------------------------------------------------------------------------------
Remote Entities Count : 1 ...(2)
Entity 1 ...(3)
    Chassis ID Subtype                          : MAC Address ...(4)
    Chassis ID                                  : 00-40-66-AC-2C-90 ...(5)
    Port ID Subtype                             : Local ...(6)
    Port ID                                     : Port1/0/49 ...(7)
    Port Description                            : APRESIA Systems, Ltd ApresiaNP5
                                                  000-48T4X HW A firmware 1.05.01
                                                   Port 20 on Unit 1 ...(8)
    System Name                                 : Test-NP5000 ...(9)
    System Description                          : ApresiaNP5000-48T4X Gigabit Eth
                                                  ernet Switch Ver.1.05.01 ...(10)
    System Capabilities                         : Bridge, Router ...(11)
    Management Address Count                    : 1 ...(12)
    Port PVID                                   : 0 ...(13)
    PPVID Entries Count                         : 0 ...(14)
    VLAN Name Entries Count                     : 2 ...(15)
    Protocol ID Entries Count                   : 0 ...(16)
    MAC/PHY Configuration/Status                : (None) ...(17)
    Power Via MDI                               : (None) ...(18)
    Link Aggregation                            : (None) ...(19)
    Maximum Frame Size                          : 1536 ...(20)
    Link Fault                                  : - ...(21)
    LLDP-MED capabilities                       : (See Detail) ...(22)
    Extended power via MDI                      : (See Detail) ...(23)
    Network policy                              : (See Detail) ...(24)
    Inventory Management                        : (See Detail) ...(25)
    Unknown TLVs Count                          : 0 ...(26)
```

各項目の説明は、以下のとおりです。

表 15-1 show lldp neighbors interface コマンドの表示項目

項番	説明
(1)	自装置のポート番号を表示します。
(2)	登録された隣接装置の数を表示します。
(3)	登録番号を表示します。
(4)	隣接装置から通知された、Chassis ID TLV のサブタイプを表示します。

項番	説明
(5)	隣接装置から Chassis ID TLV で通知された、Chassis ID 情報を表示します。
(6)	隣接装置から通知された、Port ID TLV のサブタイプを表示します。
(7)	隣接装置から Port ID TLV で通知された、Port ID 情報を表示します。
(8)	隣接装置から Port Description TLV で通知された、ポートの説明を表示します。
(9)	隣接装置から System Name TLV で通知された、システム名を表示します。
(10)	隣接装置から System Description TLV で通知された、システムの説明を表示します。
(11)	隣接装置から System Capabilities TLV で通知された、システムの利用可能な能力を表示します。
(12)	隣接装置から Management Address TLV で通知された、管理用 IP アドレスの数を表示します。
(13)	隣接装置から Port VLAN ID TLV で通知された、ポートの VLAN ID を表示します。
(14)	隣接装置から Port and Protocol VLAN ID (PPVID) TLV で通知された、プロトコル VLAN の数を表示します。
(15)	隣接装置から VLAN Name TLV で通知された、VLAN の数を表示します。
(16)	隣接装置から Protocol Identity TLV で通知された、プロトコルの数を表示します。
(17)	隣接装置から MAC/PHY Configuration/Status TLV で通知された情報は、詳細モードで確認します。
(18)	隣接装置から Power Via MDI TLV で通知された情報は、詳細モードで確認します。
(19)	隣接装置から Link Aggregation TLV で通知された情報は、詳細モードで確認します。
(20)	隣接装置から Maximum Frame Size TLV で通知された、最大フレームサイズを表示します。
(21)	隣接装置からベンダー独自の Link Fault TLV で通知された、LLDP 疑似リンクダウンに関する情報を表示します。 • -：隣接装置側ポートは無効設定 • Normal：隣接装置側ポートは正常状態 • Fault：隣接装置側ポートは LLDP 疑似リンクダウン状態
(22)	隣接装置から LLDP-MED Capabilities TLV で通知された情報は、詳細モードで確認します。
(23)	隣接装置から LLDP-MED Extended Power-via-MDI TLV で通知された情報は、詳細モードで確認します。
(24)	隣接装置から LLDP-MED Network Policy TLV で通知された情報は、詳細モードで確認します。
(25)	隣接装置から LLDP-MED Inventory Management TLV で通知された情報は、詳細モードで確認します。
(26)	隣接装置から通知された、未知の TLV の数を表示します。

隣接装置の LLDP 情報の表示（要約モード）

show lldp neighbors interface brief コマンドで、隣接装置の LLDP 情報を要約モードで確認できます。

ポート 1/0/15 を指定した場合の表示例を以下に示します。

```
# show lldp neighbors interface port 1/0/15 brief

Port ID: Port1/0/15 ...(1)
--------------------------------------------------------------------------------
Remote Entities Count : 1 ...(2)
Entity 1 ...(3)
    Chassis ID Subtype                          : MAC Address ...(4)
    Chassis ID                                  : 00-40-66-AC-2C-90 ...(5)
    Port ID Subtype                             : Local ...(6)
    Port ID                                     : Port1/0/49 ...(7)
    Port Description                            : APRESIA Systems, Ltd ApresiaNP5
                                                  000-48T4X HW A firmware 1.05.01
                                                   Port 20 on Unit 1 ...(8)
```

各項目の説明は、以下のとおりです。

表 15-2 show lldp neighbors interface brief コマンドの表示項目

項番	説明
(1)	自装置のポート番号を表示します。
(2)	登録された隣接装置の数を表示します。
(3)	登録番号を表示します。
(4)	隣接装置から通知された、Chassis ID TLV のサブタイプを表示します。
(5)	隣接装置から Chassis ID TLV で通知された、Chassis ID 情報を表示します。
(6)	隣接装置から通知された、Port ID TLV のサブタイプを表示します。
(7)	隣接装置から Port ID TLV で通知された、Port ID 情報を表示します。
(8)	隣接装置から Port Description TLV で通知された、ポートの説明を表示します。

隣接装置の LLDP 情報の表示（詳細モード）

show lldp neighbors interface detail コマンドで、隣接装置の LLDP 情報を詳細モードで確認できます。

ポート 1/0/15 を指定した場合の表示例を以下に示します。

```
# show lldp neighbors interface port 1/0/15 detail

Port ID: Port1/0/15 ...(1)
--------------------------------------------------------------------------------
Remote Entities Count : 1 ...(2)
Entity 1 ...(3)
    Chassis ID Subtype                          : MAC Address ...(4)
    Chassis ID                                  : 00-40-66-AC-2C-90 ...(5)
    Port ID Subtype                             : Local ...(6)
    Port ID                                     : Port1/0/49 ...(7)
    Port Description                            : APRESIA Systems, Ltd ApresiaNP5
                                                  000-48T4X HW A firmware 1.05.01
                                                   Port 20 on Unit 1 ...(8)
    System Name                                 : Test-NP5000 ...(9)
    System Description                          : ApresiaNP5000-48T4X Gigabit Eth
                                                  ernet Switch Ver.1.05.01 ...(10)
    System Capabilities                         : Bridge, Router ...(11)
    Management Address Count                    : 1 ...(12)
        Entry 1 :
            Subtype                             : IPv4
            Address                             : 192.168.10.100
            IF Type                             : IfIndex
            OID                                 : 1.3.6.1.4.1.278.1.42.2.0


    Port PVID                                   : 0 ...(13)
    PPVID Entries Count                         : 0 ...(14)
        (None)

    VLAN Name Entries Count                     : 2 ...(15)
        Entry 1 :
            VLAN ID                             : 1
            VLAN Name                           : default
        Entry 2 :
            VLAN ID                             : 10
            VLAN Name                           : Test-VLAN10

    Protocol ID Entries Count                   : 0 ...(16)
        (None)

    MAC/PHY Configuration/Status                : (None) ...(17)
    Power Via MDI                               : (None) ...(18)
    Link Aggregation                            : (None) ...(19)
    Maximum Frame Size                          : 1536 ...(20)
    Link Fault                                  : - ...(21)
    Unknown TLVs Count                          : 0 ...(22)
        (None)

        LLDP-MED Capabilities Enabled: ...(23)
            Capabilities                    : Not Support
            Network Policy                  : Not Support
            Location Identification         : Not Support
            Extended Power Via MDI          : Not Support
            Inventory                       : Not Support


    Inventory Management: ...(24)
        None
```

各項目の説明は、以下のとおりです。

表 15-3 `show lldp neighbors interface detail` コマンドの表示項目

項番	説明
(1)	自装置のポート番号を表示します。
(2)	登録された隣接装置の数を表示します。
(3)	登録番号を表示します。
(4)	隣接装置から通知された、Chassis ID TLV のサブタイプを表示します。
(5)	隣接装置から Chassis ID TLV で通知された、Chassis ID 情報を表示します。
(6)	隣接装置から通知された、Port ID TLV のサブタイプを表示します。
(7)	隣接装置から Port ID TLV で通知された、Port ID 情報を表示します。
(8)	隣接装置から Port Description TLV で通知された、ポートの説明を表示します。
(9)	隣接装置から System Name TLV で通知された、システム名を表示します。
(10)	隣接装置から System Description TLV で通知された、システムの説明を表示します。
(11)	隣接装置から System Capabilities TLV で通知された、システムの利用可能な能力を表示します。
(12)	隣接装置から Management Address TLV で通知された、管理用 IP アドレスの数と IP アドレス情報を表示します。0 個の場合は、IP アドレス情報は (None) と表示されます。
(13)	隣接装置から Port VLAN ID TLV で通知された、ポートの VLAN ID を表示します。
(14)	隣接装置から Port and Protocol VLAN ID (PPVID) TLV で通知された、プロトコル VLAN の数と VLAN 情報を表示します。0 個の場合は、VLAN 情報は (None) と表示されます。
(15)	隣接装置から VLAN Name TLV で通知された、VLAN の数と VLAN 情報を表示します。0 個の場合は、VLAN 情報は (None) と表示されます。
(16)	隣接装置から Protocol Identity TLV で通知された、プロトコルの数とプロトコル情報を表示します。0 個の場合は、プロトコル情報は (None) と表示されます。
(17)	隣接装置から MAC/PHY Configuration/Status TLV で通知された情報を表示します。
(18)	隣接装置から Power Via MDI TLV で通知された情報を表示します。
(19)	隣接装置から Link Aggregation TLV で通知された情報を表示します。
(20)	隣接装置から Maximum Frame Size TLV で通知された、最大フレームサイズを表示します。
(21)	隣接装置からベンダー独自の Link Fault TLV で通知された、LLDP 疑似リンクダウンに関する情報を表示します。 • -：隣接装置側ポートは無効設定 • Normal：隣接装置側ポートは正常状態 • Fault：隣接装置側ポートは LLDP 疑似リンクダウン状態
(22)	隣接装置から通知された、未知の TLV の数と TLV 情報を表示します。
(23)	隣接装置から LLDP-MED Capabilities TLV で通知された情報を表示します。
(24)	隣接装置から LLDP-MED Inventory Management TLV で通知された情報を表示します。

15.2.2 LLDP で隣接装置に通知する情報の表示

各 TLV の通知が有効になっている場合に、LLDP TLV に含めて隣接装置に通知する情報を確認できます。

隣接装置に通知する情報の表示（標準モード）

show lldp local interface コマンドで、隣接装置に通知する情報を標準モードで確認できます。

ポート 1/0/15 を指定した場合の表示例を以下に示します。

```
# show lldp local interface port 1/0/15

Port ID: Port1/0/15 ...(1)
------------------------------------------------------------------------------
Port ID Subtype                              : Local ...(2)
Port ID                                      : Port1/0/15 ...(3)
Port Description                             : APRESIA Systems, Ltd
                                               ApresiaNP7000-48X6L HW A firmware
                                               1.05.01 Port 15 on Unit 1 ...(4)
Port PVID                                    : 1 ...(5)
Management Address Count                     : 1 ...(6)
PPVID Entries Count                          : 0 ...(7)
VLAN Name Entries Count                      : 2 ...(8)
Protocol Identity Entries Count              : 0 ...(9)
MAC/PHY Configuration/Status                 : (See Detail) ...(10)
Link Aggregation                             : (See Detail) ...(11)
Maximum Frame Size                           : 1536 ...(12)
Link Fault                                   : - ...(13)
LLDP-MED capabilities                        : (See Detail) ...(14)
```

各項目の説明は、以下のとおりです。

表 15-4 show lldp local interface コマンドの表示項目

項番	説明
(1)	ポート番号を表示します。
(2)	Port ID TLV のサブタイプを表示します。 • Local：Locally assigned(7) • MAC Address：MAC address(3)
(3)	Port ID TLV のサブタイプが local 設定の場合は、ポート番号を表示します。Port ID TLV のサブタイプが mac-address 設定の場合は、対象ポートの MAC アドレスを表示します。
(4)	Port Description TLV で通知される、ポートの説明を表示します。
(5)	Port VLAN ID TLV で通知される、ポートの VLAN ID を表示します。
(6)	Management Address TLV で通知される、管理用 IP アドレスの数を表示します。
(7)	Port and Protocol VLAN ID (PPVID) TLV で通知される、プロトコル VLAN の数を表示します。
(8)	VLAN Name TLV で通知される、VLAN の数を表示します。
(9)	Protocol Identity TLV で通知される、プロトコルの数を表示します。
(10)	MAC/PHY Configuration/Status TLV で通知される情報は、詳細モードで確認します。
(11)	Link Aggregation TLV で通知される情報は、詳細モードで確認します。
(12)	Maximum Frame Size TLV で通知される、最大フレームサイズを表示します。

項番	説明
(13)	LLDP 疑似リンクダウンに関する情報を表示します。 • -：自装置側ポートは無効設定 • Normal：自装置側ポートは正常状態 • Fault：自装置側ポートは LLDP 疑似リンクダウン状態
(14)	LLDP-MED Capabilities TLV で通知される情報は、詳細モードで確認します。

隣接装置に通知する情報の表示（要約モード）

show lldp local interface brief コマンドで、隣接装置に通知する情報を要約モードで確認できます。

ポート 1/0/15 を指定した場合の表示例を以下に示します。

```
# show lldp local interface port 1/0/15 brief

Port ID: Port1/0/15 ...(1)
--------------------------------------------------------------------------------
Port ID Subtype                          : Local ...(2)
Port ID                                  : Port1/0/15 ...(3)
Port Description                         : APRESIA Systems, Ltd
                                           ApresiaNP7000-48X6L HW A firmware
                                           1.05.01 Port 15 on Unit 1 ...(4)
```

各項目の説明は、以下のとおりです。

表 15-5 show lldp local interface brief コマンドの表示項目

項番	説明
(1)	ポート番号を表示します。
(2)	Port ID TLV のサブタイプを表示します。 • Local：Locally assigned(7) • MAC Address：MAC address(3)
(3)	Port ID TLV のサブタイプが local 設定の場合は、ポート番号を表示します。Port ID TLV のサブタイプが mac-address 設定の場合は、対象ポートの MAC アドレスを表示します。
(4)	Port Description TLV で通知される、ポートの説明を表示します。

隣接装置に通知する情報の表示（詳細モード）

show lldp local interface detail コマンドで、隣接装置に通知する情報を詳細モードで確認できます。

ポート 1/0/15 を指定した場合の表示例を以下に示します。

```
# show lldp local interface port 1/0/15 detail

Port ID: Port1/0/15 ...(1)
------------------------------------------------------------------------------
Port ID Subtype                              : Local ...(2)
Port ID                                      : Port1/0/15 ...(3)
Port Description                             : APRESIA Systems, Ltd
                                               ApresiaNP7000-48X6L HW A firmware
                                               1.05.01 Port 15 on Unit 1 ...(4)
Port PVID                                    : 1 ...(5)
Management Address Count                     : 1 ...(6)

    Address 1 : (default)
        Subtype                              : IPv4
        Address                              : 192.168.10.100
        IF Type                              : IfIndex
        OID                                  : 1.3.6.1.4.1.278.1.42.1

PPVID Entries Count                          : 0 ...(7)
    (None)
VLAN Name Entries Count                      : 2 ...(8)
    Entry 1 :
        VLAN ID                              : 1
        VLAN Name                            : default

    Entry 2 :
        VLAN ID                              : 10
        VLAN Name                            : VLAN0010

Protocol Identity Entries Count              : 0 ...(9)
    (None)
MAC/PHY Configuration/Status                 : ...(10)
    Auto-Negotiation Support                 : Supported
    Auto-Negotiation Enabled                 : Enabled
    Auto-Negotiation Advertised Capability   : 8000(hex)
    Auto-Negotiation Operational MAU Type    : 0000(hex)

Link Aggregation                             : ...(11)
    Aggregation Capability                   : Aggregated
    Aggregation Status                       : Not Currently in Aggregation
    Aggregation Port ID                      : 0

Maximum Frame Size                           : 1536 ...(12)

Link Fault                                   : - ...(13)

LLDP-MED Capabilities Support: ...(14)
    Capabilities               :Support
    Network Policy             :Not Support
    Location Identification    :Not Support
    Extended Power Via MDI PSE :Not Support
    Extended Power Via MDI PD  :Not Support
    Inventory                  :Support
```

各項目の説明は、以下のとおりです。

表 15-6 `show lldp local interface detail` コマンドの表示項目

項番	説明
(1)	ポート番号を表示します。
(2)	Port ID TLV のサブタイプを表示します。 • Local：Locally assigned(7) • MAC Address：MAC address(3)
(3)	Port ID TLV のサブタイプが local 設定の場合は、ポート番号を表示します。Port ID TLV のサブタイプが mac-address 設定の場合は、対象ポートの MAC アドレスを表示します。
(4)	Port Description TLV で通知される、ポートの説明を表示します。
(5)	Port VLAN ID TLV で通知される、ポートの VLAN ID を表示します。
(6)	Management Address TLV で通知される、管理用 IP アドレスの数と IP アドレス情報を表示します。0 個の場合は、IP アドレス情報は (None) と表示されます。
(7)	Port and Protocol VLAN ID (PPVID) TLV で通知される、プロトコル VLAN の数と VLAN 情報を表示します。0 個の場合は、VLAN 情報は (None) と表示されます。
(8)	VLAN Name TLV で通知される、VLAN の数と VLAN 情報を表示します。
(9)	Protocol Identity TLV で通知される、プロトコルの数とプロトコル情報を表示します。0 個の場合は、プロトコル情報は (None) と表示されます。
(10)	MAC/PHY Configuration/Status TLV で通知される情報を表示します。
(11)	Link Aggregation TLV で通知される情報を表示します。
(12)	Maximum Frame Size TLV で通知される、最大フレームサイズを表示します。
(13)	LLDP 疑似リンクダウンに関する情報を表示します。 • -：自装置側ポートは無効設定 • Normal：自装置側ポートは正常状態 • Fault：自装置側ポートは LLDP 疑似リンクダウン状態
(14)	LLDP-MED Capabilities TLV で通知される情報を表示します。

15.2.3 装置全体の LLDP 設定の表示

show lldp コマンドで、装置全体の LLDP 設定を確認できます。

表示例を以下に示します。

```
# show lldp

LLDP System Information
    Chassis ID Subtype        : MAC Address ...(1)
    Chassis ID                : 00-40-66-AA-52-1B ...(2)
    System Name               : Switch ...(3)
    System Description        : ApresiaNP7000-48X6L TenGigabit Ethernet Switch V
                                er.1.04.01 ...(4)
    System Capabilities Supported: Bridge, Router ...(5)
    System Capabilities Enabled  : Bridge, Router ...(6)
LLDP-MED System Information:
    Device Class              : Network Connectivity Device ...(7)
    Hardware Revision         : A ...(8)
    Firmware Revision         : 1.00.01 ...(9)
    Software Revision         : 1.04.01 ...(10)
    Serial Number             : 187550000006 ...(11)
    Manufacturer Name         : APRESIA Systems, Ltd ...(12)
    Model Name                : ApresiaNP7000-48X6L TenGigabit E ...(13)
    Asset ID                  : ...(14)

LLDP Configurations
    LLDP State                : Disabled ...(15)
    LLDP Forward State        : Disabled ...(16)
    Message TX Interval       : 30 ...(17)
    Message TX Hold Multiplier: 4 ...(18)
    ReInit Delay              : 2 ...(19)
    TX Delay                  : 2 ...(20)

LLDP-MED Configuration:
    Fast Start Repeat Count   : 4 ...(21)
```

各項目の説明は、以下のとおりです。

表 15-7 show lldp コマンドの表示項目

項番	説明
(1)	Chassis ID TLV のサブタイプを表示します。ApresiaNP シリーズでは、Chassis ID TLV のサブタイプは MAC address(4) で送信します。
(2)	Chassis ID TLV で通知する情報を表示します。サブタイプが MAC Address のため、自装置の MAC アドレスを表示します。
(3)	System Name TLV で通知されるシステム名を表示します。
(4)	System Description TLV を通知される自装置の説明を表示します。
(5)	System Capabilities TLV で通知される、自装置で利用可能な機能の情報を表示します。
(6)	自装置で有効化されている機能の情報を表示します。
(7)	LLDP-MED 対応機器として動作する際に通知するデバイスクラスを表示します。
(8)	LLDP-MED 対応機器として動作する際に通知するハードウェアリビジョンを表示します。
(9)	LLDP-MED 対応機器として動作する際に通知するファームウェアリビジョンを表示します。

項番	説明
(10)	LLDP-MED 対応機器として動作する際に通知するソフトウェアリビジョンを表示します。
(11)	LLDP-MED 対応機器として動作する際に通知するシリアル番号を表示します。
(12)	LLDP-MED 対応機器として動作する際に通知するメーカー名を表示します。
(13)	LLDP-MED 対応機器として動作する際に通知するモデル名を表示します。
(14)	LLDP-MED 対応機器として動作する際に通知するアセット ID を表示します。
(15)	装置全体の LLDP 設定の有効 (Enabled) ／無効 (Disabled) を表示します。
(16)	LLDPDU 転送の有効 (Enabled) ／無効 (Disabled) を表示します。
(17)	LLDPDU の送信間隔（秒）を表示します。
(18)	送信する LLDPDU の TTL 値を決定するための、LLDPDU 送信間隔の乗数を表示します。
(19)	LLDP 再初期化の遅延時間（秒）を表示します。
(20)	LLDPDU の送信遅延間隔（秒）を表示します。
(21)	LLDP-MED fast start 処理の実行回数を表示します。

15.2.4 物理ポートの LLDP 設定の表示

show lldp interface コマンドで、物理ポートの LLDP 設定を確認できます。

ポート 1/0/1 を指定した場合の表示例を以下に示します。

```
# show lldp interface port 1/0/1

Port ID: Port1/0/1 ...(1)
------------------------------------------------------------------------------
Port ID                                                    :Port1/0/1 ...(2)
Admin Status                                               :TX and RX ...(3)
Error disable                                              :Disabled ...(4)
Notification                                               :Disabled ...(5)
Basic Management TLVs:
    Port Description                                       :Disabled ...(6)
    System Name                                            :Disabled ...(7)
    System Description                                     :Disabled ...(8)
    System Capabilities                                    :Disabled ...(9)
    Enabled Management Address: ...(10)
        (None)
IEEE 802.1 Organizationally Specific TLVs:

    Port VLAN ID                                           :Disabled ...(11)
    Enabled Port_and_Protocol_VLAN_ID ...(12)
        (None)
    Enabled VLAN Name ...(13)
        (None)
    Enabled Protocol_Identity ...(14)
        (None)
IEEE 802.3 Organizationally Specific TLVs:

    MAC/PHY Configuration/Status                           :Disabled ...(15)
    Link Aggregation                                       :Disabled ...(16)
    Maximum Frame Size                                     :Disabled ...(17)

Organizationally Specific TLVs:

    Link Fault TLV                                         :Disabled ...(18)

LLDP-MED Organizationally Specific TLVs:

    LLDP-MED Capabilities TLV                              :Disabled ...(19)
    LLDP-MED Inventory TLV                                 :Disabled ...(20)
```

各項目の説明は、以下のとおりです。

表 15-8 show lldp interface コマンドの表示項目

項番	説明
(1)	ポート番号を表示します。
(2)	ポート番号を表示します。
(3)	LLDPDU の送受信それぞれについて有効／無効を表示します。 • TX and RX：送受信ともに有効 • TX Only：送信のみ有効 • RX Only：受信のみ有効 • Disabled：送受信ともに無効
(4)	LLDP 疑似リンクダウン機能の有効 (Enabled) ／無効 (Disabled) を表示します。

項番	説明
(5)	LLDP 関連と LLDP-MED 関連の SNMP トラップの有効／無効を表示します。 • Disabled：無効 • LLDP：LLDP 関連の SNMP トラップのみ有効 • LLDP-MED：LLDP-MED 関連の SNMP トラップのみ有効 • LLDP and LLDP-MED：LLDP 関連と LLDP-MED 関連の SNMP トラップが有効
(6)	Port Description TLV 付加の有効 (Enabled) ／無効 (Disabled) を表示します。
(7)	System Name TLV 付加の有効 (Enabled) ／無効 (Disabled) を表示します。
(8)	System Description TLV 付加の有効 (Enabled) ／無効 (Disabled) を表示します。
(9)	System Capabilities TLV 付加の有効 (Enabled) ／無効 (Disabled) を表示します。
(10)	Management Address TLV で通知する管理用 IP アドレスを表示します。Management Address TLV を通知しない場合は (None) と表示されます。
(11)	Port VLAN ID TLV 付加の有効 (Enabled) ／無効 (Disabled) を表示します。
(12)	Port and Protocol VLAN ID (PPVID) TLV で通知する VLAN ID を表示します。PPVID TLV を通知しない場合は (None) と表示されます。
(13)	VLAN Name TLV で通知する VLAN ID を表示します。VLAN Name TLV を通知しない場合は (None) と表示されます。
(14)	Protocol Identity TLV で通知するプロトコルを表示します。Protocol Identity TLV を通知しない場合は (None) と表示されます。
(15)	MAC/PHY Configuration/Status TLV 付加の有効 (Enabled) ／無効 (Disabled) を表示します。
(16)	Link Aggregation TLV 付加の有効 (Enabled) ／無効 (Disabled) を表示します。
(17)	Maximum Frame Size TLV 付加の有効 (Enabled) ／無効 (Disabled) を表示します。
(18)	ベンダー独自の Link Fault TLV（LLDP 疑似リンクダウンに関する情報）付加の有効 (Enabled) ／無効 (Disabled) を表示します。
(19)	LLDP-MED Capabilities TLV 付加の有効 (Enabled) ／無効 (Disabled) を表示します。
(20)	LLDP-MED Inventory Management TLV 付加の有効 (Enabled) ／無効 (Disabled) を表示します。

15.2.5 管理用アドレス情報の表示

show lldp management-address コマンドで、管理用アドレス情報を確認できます。

表示例を以下に示します。

```
# show lldp management-address

Address 1 : (default)
-----------------------------------------------
    Subtype                              : IPv4 ...(1)
    Address                              : 192.0.2.100 ...(2)
    IF Type                              : IfIndex ...(3)
    OID                                  : 1.3.6.1.4.1.278.1.42.1 ...(4)
    Advertising Ports                    : - ...(5)

Address 2 :
-----------------------------------------------
    Subtype                              : IPv4
    Address                              : 192.0.2.100
    IF Type                              : IfIndex
    OID                                  : 1.3.6.1.4.1.278.1.42.1
    Advertising Ports                    : -
      Port1/0/1,Port1/0/5

Total Entries: 2
```

各項目の説明は、以下のとおりです。

表 15-9 show lldp management-address コマンドの表示項目

項番	説明
(1)	管理用アドレスのサブタイプ（IPv4 ／ IPv6）を表示します。
(2)	管理用アドレスを表示します。
(3)	管理用アドレスのインターフェースタイプを表示します。
(4)	管理用アドレスの装置を判別する OID を表示します。
(5)	対象の管理用アドレスを Management Address TLV で通知するポートを表示します。

15.2.6 グローバルな LLDP 統計情報の表示

show lldp traffic コマンドで、グローバルな LLDP 統計情報を確認できます。

表示例を以下に示します。

```
# show lldp traffic

Last Change Time    : 1910843 ...(1)
Total Inserts       : 1 ...(2)
Total Deletes       : 0 ...(3)
Total Drops         : 0 ...(4)
Total Ageouts       : 0 ...(5)
```

各項目の説明は、以下のとおりです。

表 15-10 `show lldp traffic` コマンドの表示項目

項番	説明
(1)	lldpStatsRemTablesLastChangeTime の MIB の値（sysUpTime）を表示します。
(2)	LLDP テーブルに登録した回数を表示します。
(3)	クリアコマンドや、TTL 値が 0 秒の LLDPDU を受信して LLDP テーブルから削除した回数を表示します。
(4)	リソース不足のため、LLDP テーブルに登録されなかった回数を表示します。
(5)	TTL expired により LLDP テーブルから削除された回数を表示します。

15.2.7 物理ポートの LLDP 統計情報の表示

`show lldp traffic interface` コマンドで、物理ポートの LLDP 統計情報を確認できます。

ポート 1/0/1 を指定した場合の表示例を以下に示します。

```
# show lldp traffic interface port 1/0/1

Port ID : Port1/0/1 ...(1)
-------------------------------------------
    Total Transmits      : 0 ...(2)
    Total Discards       : 0 ...(3)
    Total Errors         : 0 ...(4)
    Total Receives       : 0 ...(5)
    Total TLV Discards   : 0 ...(6)
    Total TLV Unknowns   : 0 ...(7)
    Total Ageouts        : 0 ...(8)
```

各項目の説明は、以下のとおりです。

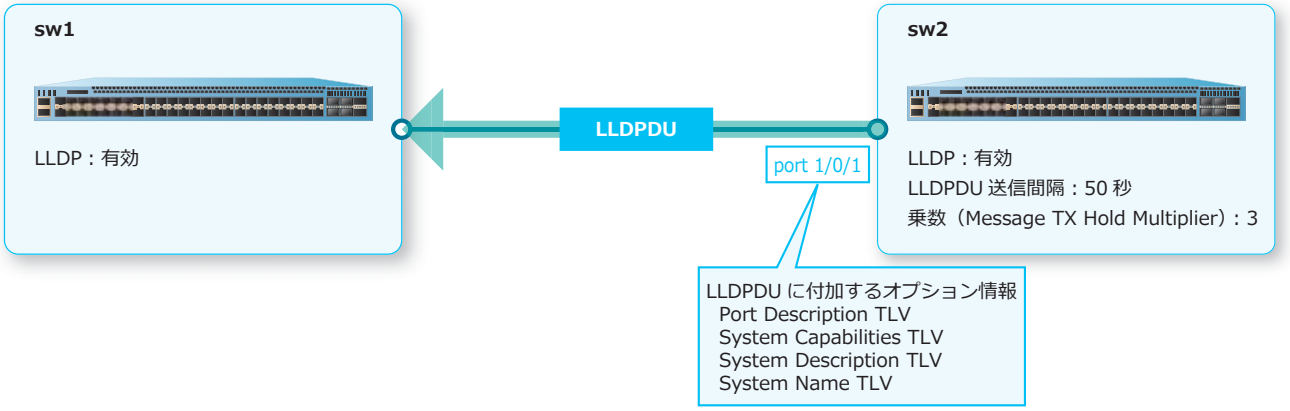
表 15-11 `show lldp traffic interface` コマンドの表示項目

項番	説明
(1)	ポート番号を表示します。
(2)	送信した LLDPDU の数を表示します。
(3)	廃棄した LLDPDU の数を表示します。
(4)	受信した無効な LLDPDU の数を表示します。
(5)	受信した LLDPDU の数を表示します。
(6)	廃棄した情報（TLV）の数を表示します。
(7)	受信した未知の情報（TLV）の数を表示します。
(8)	TTL expired により LLDP テーブルから削除された回数を表示します。

15.3 LLDP の構成例と設定例

LLDP を有効化し、LLDPDU 送信間隔や、通知する情報を設定する場合の構成例と設定例を示します。

図 15-3 LLDP を有効化する場合の構成例



1. 受信側の装置全体の LLDP を有効化します。

```
sw1# configure terminal
sw1(config)# lldp run
sw1(config)# end
sw1#
```

2. 送信側の装置全体の LLDP を有効化します。

```
sw2# configure terminal
sw2(config)# lldp run
sw2(config)#
```

3. ポート 1/0/1 で、[Port Description TLV]、[System Capabilities TLV]、[System Description TLV]、[System Name TLV] を LLDPDU に付加するように設定します。パラメーターを指定しないで **lldp tlv-select** コマンドを実行すると、すべてのパラメーターが有効になります。

```
sw2(config)# interface port 1/0/1
sw2(config-if-port)# lldp tlv-select
sw2(config-if-port)# exit
sw2(config)#
```

4. LLDPDU 送信間隔を［50 秒］に設定し、LLDPDU の TTL 値を決定するための乗数を［3］に設定します。

```
sw2(config)# lldp tx-interval 50
sw2(config)# lldp hold-multiplier 3
sw2(config)# end
sw2#
```

16. Ethernet OAM/CFM

Ethernet OAM/CFM の機能、状態の確認方法、および構成例と設定例について説明します。

REF: コマンドの詳細については、『コマンドリファレンス』を参照してください。

16.1 Ethernet OAM の機能説明

イーサネット上で動作する OAM（Operations, Administration, Maintenance）には、いくつかの規格が存在します。この章では、IEEE 802.3ah で規格化された、「2 つの隣接する装置間の回線状態を監視する機能（以後、**Ethernet OAM**）」について説明します。

Ethernet OAM では、以下のようなことが可能です。

- リンクモニタリングとイベント通知
- リモートループバック
- Ethernet OAM を利用した単方向リンク検出

Ethernet OAM を有効化するには、**`ethernet oam`** コマンドを使用します。Ethernet OAM の動作モードを設定するには、**`ethernet oam mode`** コマンドを使用します。

16.1.1 リンクモニタリングとイベント通知

リンクモニタリングイベントを有効にすると、有効にしたポートのリンクモニタリングが開始されます。設定した監視条件を満たすと、イベント記録と対向装置へのイベント通知が行われます。以下に、各リンクモニタリングイベントを示します。

• Errored Symbol Period イベント

しきい値はシンボルエラー数です。設定した監視期間中に発生したシンボルエラー数がしきい値を超えた場合に、Errored Symbol Period イベントが記録され、Errored Symbol Period Event TLV を含む Event Notification OAMPDU が送信されます。**`ethernet oam link-monitor error-symbol`** コマンドで設定します。

• Errored Frame イベント

しきい値はエラーフレーム数です。設定した監視期間中に発生したエラーフレーム数がしきい値を超えた場合に、Errored Frame イベントが記録され、Errored Frame Event TLV を含む Event Notification OAMPDU が送信されます。**`ethernet oam link-monitor error-frame`** コマンドで設定します。

• Errored Frame Period イベント

しきい値はエラーフレーム数です。設定した監視フレーム数を受信する間に発生したエラーフレーム数がしきい値を超えた場合に、Errored Frame Period イベントが記録され、Errored Frame Period Event TLV を含む Event Notification OAMPDU が送信されます。**`ethernet oam link-monitor error-frame-period`** コマンドで設定します。

• Errored Frame Seconds Summary イベント

しきい値は、「1 秒以内に少なくとも 1 個のエラーフレームを検出したことがある秒数」です。設定した監視期間中に「エラーフレームを検出した秒数」がしきい値を超えた場合に、Errored Frame Seconds Summary イベントが記録され、Errored Frame Seconds Summary Event TLV を含む Event Notification OAMPDU が送信されます。**`ethernet oam link-monitor error-frame-seconds`** コマンドで設定します。

その他、Flags フィールドの「Link Fault ビット」「Dying Gasp ビット」「Critical Event ビット」のいずれかがセットされた OAMPDU を受信した場合にも、それぞれのイベントが記録されます。

記録されたイベントログは、**show ethernet oam event-log** コマンドで確認できます。また、dot3OamEventLogTable MIB でも確認できます。イベントログをクリアするには、**clear ethernet oam event-log** コマンドを使用します。

16.1.2 リモートループバック

リモートループバックは、対向の隣接装置のポートをループバックモードに変更する機能です。ループバックモードに変更すると通常のフレーム中継はできなくなるため、使用する場合は十分に注意して使用してください。

対向の隣接装置のポートに対してループバックモードの開始／終了を要求するには、**ethernet oam remote-loopback** コマンドを使用します。また、隣接装置から受信したループバックモード設定要求に対する動作を設定するには、**ethernet oam received-remote-loopback** コマンドを使用します。

16.1.3 Ethernet OAM を利用した単方向リンク検出

Ethernet OAM を利用して、単方向リンク（双方向通信不可の場合も含む）を検出できます。また、単方向リンクとして検出されたインターフェースを自動的にシャットダウン（err-disabled 状態に変更）できます。

単方向リンク検出機能を有効化するには、**uld enable** コマンドを使用します。Discovery プロセスの完了待機時間を設定するには、**uld discovery-time** コマンドを使用します。単方向リンクとして検出されたインターフェースを自動的にシャットダウン（err-disabled 状態に変更）するには、**uld action** コマンドを使用します。

> ***CAUTION:*** 単方向リンク検出機能は独自仕様のため、他社製品の同等機能との相互接続はサポートしていません。
>
> ***NOTE:*** 単方向リンク検出機能で err-disabled 状態にされたポートのリンク状態は、**show interfaces** コマンドでは "link status is down (error disabled: OAM Unidirectional Link)" と表示されます。また、**show interfaces status** コマンドの Status 項目では "err-disabled" と表示されます。

障害を検出してシャットダウン（err-disabled 状態に変更）されたインターフェースは、**shutdown** コマンドと **no shutdown** コマンドを使用すると手動で復旧できます。また、**errdisable recovery cause uld** コマンドを使用して自動復旧を有効にしておくと、障害を検出してインターフェースが err-disabled 状態になっても、一定時間経過後に自動的に復旧されます。

> ***NOTE:*** **errdisable recovery cause uld** コマンドは、NP7000 の 1.06.01 以降、NP5000 の 1.06.01 以降、NP4000 の 1.02.01 以降、NP3000 の 1.06.01 以降、NP2100 の 1.09.02 以降、NP2000 の 1.07.01 以降、NP2500 の 1.08.02 以降でサポートしています。

16.2 CFM の機能説明

IEEE 802.1ag で規格化された Connectivity Fault Management（以後、**CFM**）は、「レイヤー 2 ネットワークにおける、複数の装置間での障害監視」を目的とした機能です。

CFM では、以下のようなことが可能です。

- CCM（Continuity Check Message）による定常監視
- CFM ループバックテスト（レイヤー 2 ネットワークでの疎通確認）
- CFM リンクトレース（レイヤー 2 ネットワークでの経路探索）

装置全体で CFM を有効化するには、**`cfm global enable`** コマンドを使用します。インターフェースごとに CFM を有効化するには、**`cfm enable`** コマンドを使用します。

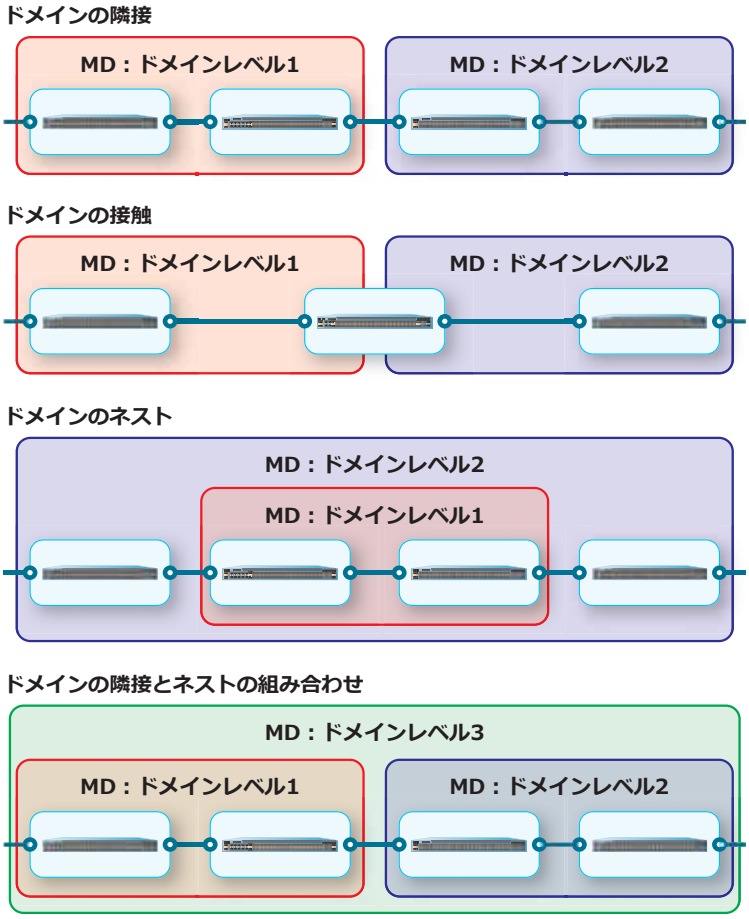
> ***CAUTION:*** MMRP-Plus のリングポートでは、CFM を有効化しないでください。
>
> ***NOTE:*** CFM 機能を使用する場合、CFM PDU を送受信するポートはトランクポート（**`switchport mode trunk`** コマンド）に設定してください。

16.2.1 メンテナンスドメイン（MD）およびメンテナンスアソシエーション（MA）

メンテナンスドメイン（以後、**MD**）は、レイヤー 2 ネットワークをドメインレベルで階層的に管理するための管理グループです。ドメインレベルの範囲は 0 ～ 7 で、0 が最も低いレベル、7 が最も高いレベルです。また、**メンテナンスアソシエーション**（以後、**MA**）は、MD に監視対象 VLAN を紐付けた管理グループで、MD ごとに最低でも 1 つは MA を設定する必要があります。

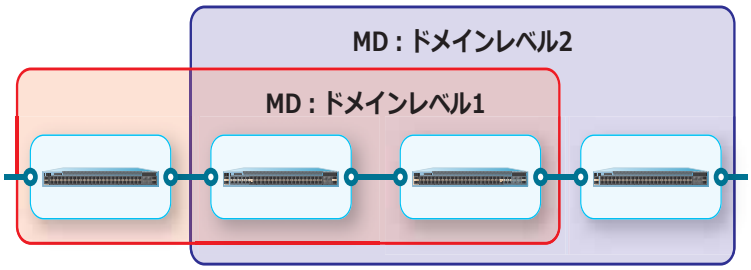
同一監視対象 VLAN でドメインレベルの異なる MD を使用する場合は、MD が隣接している構成や、低いレベルの MD が高いレベルの MD よりも内側に入れ子になっている構成を設計できます。

図 16-1 設計可能な MD の構成例



なお、同一監視対象 VLAN でドメインレベルの異なる MD が交差するような構成はできません。

図 16-2 設計不可能な MD の構成例



MD を作成するには、**cfm domain** コマンドを使用します。MA を作成するには、**cfm ma** コマンドを使用します。

16.2.2 メンテナンスエンドポイント（MEP）およびメンテナンス中間ポイント（MIP）

CFM を使用するには、同一ドメインレベルで同一監視対象 VLAN の MA に、複数の**メンテナンスポイント**を設定して配置する必要があります。メンテナンスポイントには、以下の 2 種類が存在します。

- **メンテナンスエンドポイント（以後、MEP）**

  MEP は MA の管理境界（終端ポイント）に配置され、CFM PDU の送受信とフィルタリング（破棄）を行います。

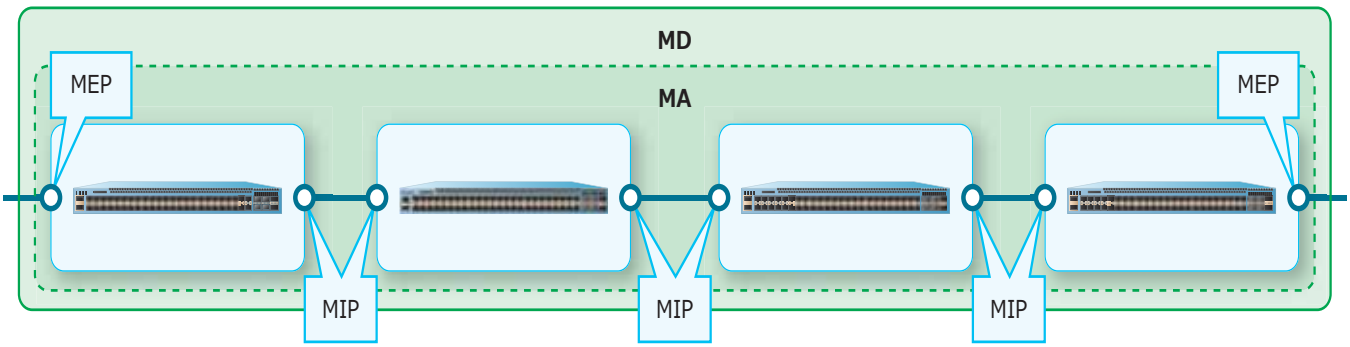
  MEP は、配置する方向によって Up MEP と Down MEP の 2 種類に分けられます。Up MEP は、Up 方向（配置したポートの装置内部方向）で同一ドメインレベルの CFM PDU を送受信します。Down MEP は、Down 方向（配置したポートの装置外部方向）で同一ドメインレベルの CFM PDU を送受信します。どちらの場合も、自身のドメインレベルより低いレベルの CFM PDU や、逆方向から受信した同一ドメインレベル以下の CFM PDU はフィルタリング（破棄）され、中継しません。しかし、自身のドメインレベルより高いレベルの CFM PDU は中継します。

  CAUTION: 同一 MA では Up MEP と Down MEP を同時に設定できません。

- **メンテナンス中間ポイント（以後、MIP）**

  MIP は MA の中間ポイントに配置され、一部の CFM PDU への応答処理を行います。

図 16-3 MEP および MIP

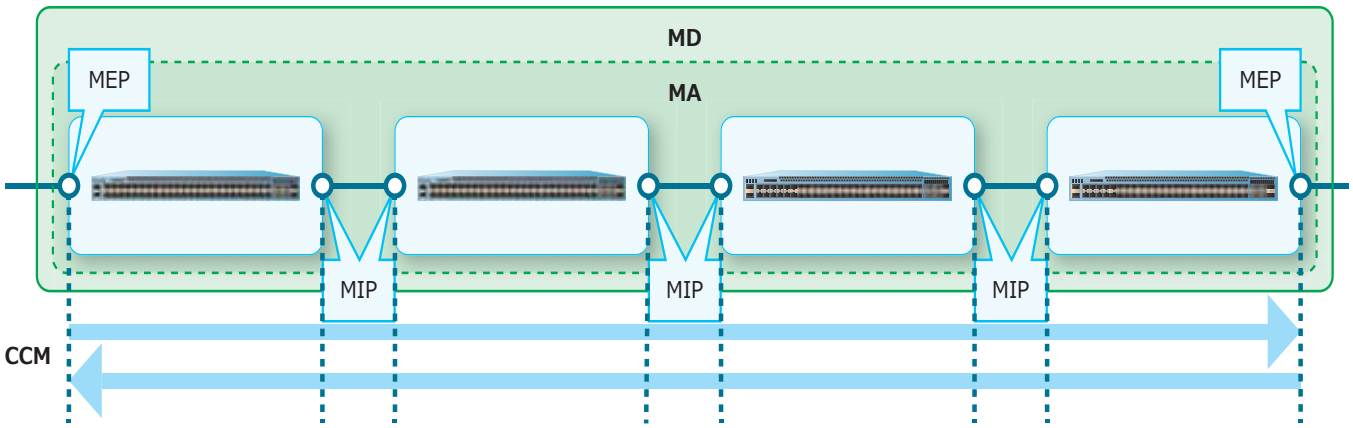


MEP を作成して有効にするには、あらかじめ **mepid-list** コマンドで MEP ID リストに登録してから **cfm mep** コマンドで作成し、**mep enable** コマンドで有効化します。また、MIP の作成方法を設定するには、**mip creation** コマンドを使用します。

16.2.3 CCM（Continuity Check Message）による定常監視

CCM は、各 MEP 間の定常監視を行うためのメッセージです。各 MEP から定期的に送信され、レイヤー 2 ネットワークの障害監視を行います。CCM を有効化するには、**`ccm enable`** コマンドを使用します。CCM の送信間隔を設定するには、**`ccm interval`** コマンドを使用します。

図 16-4 CCM による定常監視



16.2.3.1 MEP で検出できる障害種別

MEP で検出できる障害は、以下のとおりです。優先度が低い順に記載しています。（）内は **`show cfm mep fault`** コマンドのStatus項目、または **`show cfm mepid`** コマンドのHighest Fault項目で表示される情報です。

- **DefRDICCM（Some Remote MEP Defect Indication）**
  RDI ビットがセットされた CCM を受信。
- **DefMACstatus（Some Remote MEP MAC Status Error）**
  Port Status TLV または Interface Status TLV を介してエラー状態を示す CCM を受信。
- **DefRemoteCCM（Some Remote MEP Down）**
  設定した MEP ID リストに所属する MEP からの CCM を受信できていない状態。
- **DefErrorCCM（Error CCM Received）**
  MEP ID が重複した CCM、MEP ID リストにない MEP ID の CCM、CCM 送信間隔設定が異なる CCM など、無効な CCM を受信。
- **DefXconCCM（Cross-connect CCM Received）**
  他の MA からの可能性がある CCM を受信。

16.2.3.2 障害アラーム（SNMP トラップ）

障害アラーム（SNMP トラップ）の送信対象にする障害種別を指定するには、**`fault-alarm`** コマンドを使用します。

MEP で障害を検出すると、障害アラームの送信遅延タイマーが開始されます。送信待機時間が経過しても障害が存在している場合に、障害アラームが送信されます。なお、送信待機時間の間に複数の障害が検出された場合は、最も優先度の高い障害の障害アラームのみが送信されます。

障害アラームが送信された後に新たな障害を検出すると、前の障害よりも優先度が高い場合は、新しい障害アラームがすぐに送信されます。前の障害よりも優先度が低い場合は、新しい障害アラームは送信されません。

MEP で検出したすべての障害がなくなると、障害アラームのリセットタイマーが開始されます。リセット待機時間が経過しても障害が存在していない場合に、障害アラームはリセットされます。

障害アラームの送信待機時間、およびリセット待機時間を設定するには、**alarm-time** コマンドを使用します。

16.2.3.3 AIS（Alarm Indication Signal）機能

AIS 機能は、MEP で検出した障害を、よりドメインレベルが高い MEP に通知する機能です。AIS の有効／無効、AIS フレームの送信間隔とドメインレベルを設定するには、**ais** コマンドを使用します。

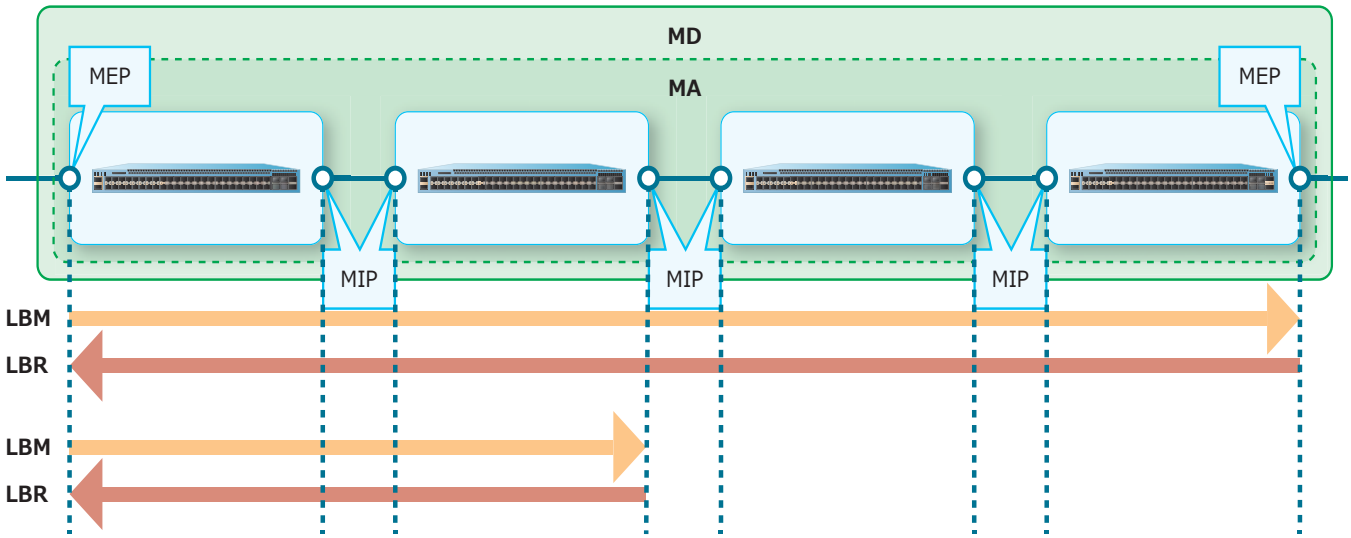
16.2.3.4 LCK（Lock Signal）機能

LCK 機能は、メンテナンスなどの目的で対象の MEP が使用不可状態になる可能性があることを、よりドメインレベルが高い MEP に対して手動で通知する機能です。LCK フレーム送信の開始／停止を行うには、**cfm lck start/stop** コマンドを使用します。LCK の有効／無効、LCK フレームの送信間隔とドメインレベルを設定するには、**lck** コマンドを使用します。

16.2.4 CFM ループバックテスト

CFM ループバックテストは、レイヤー 2 ネットワークでの疎通確認機能です。CFM ループバックテストを実施した MEP から LBM（Loop Back Message）を送信し、LBM を受信した宛先の MEP または MIP が LBR（Loop Back Reply）を応答します。CFM ループバックテストを実行するには、**cfm loopback test** コマンドを使用します。

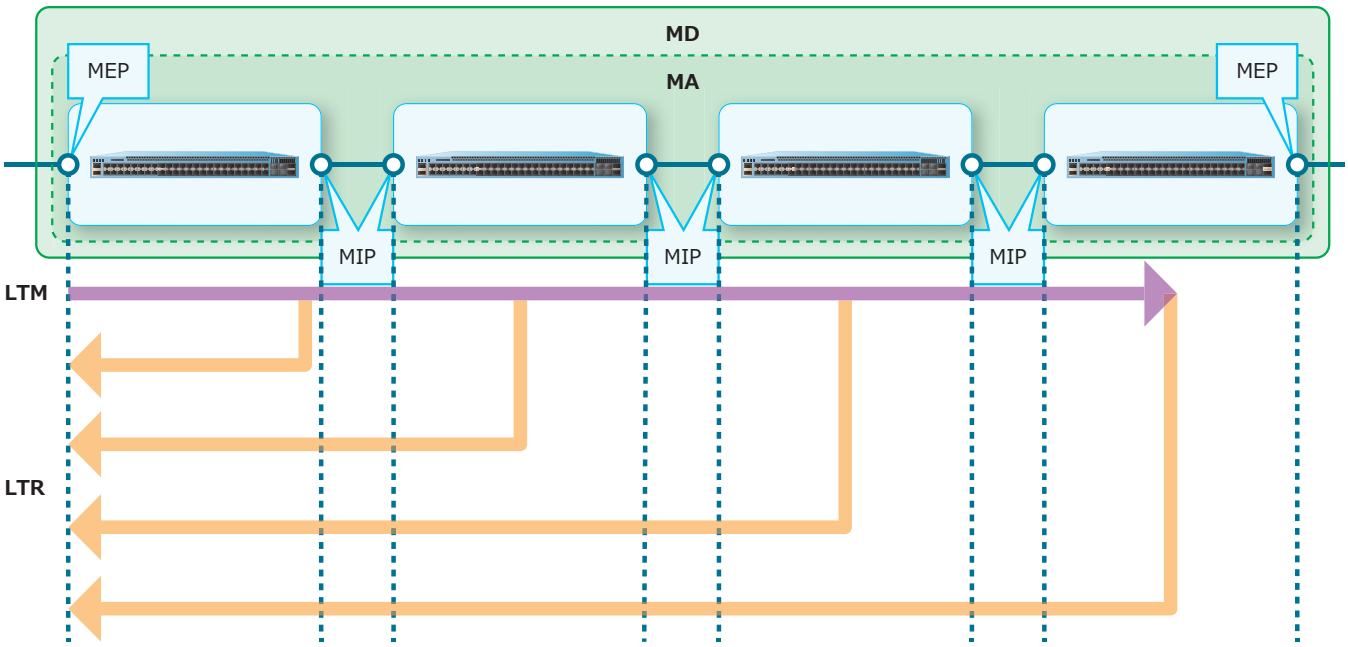
図 16-5 CFM ループバックテスト



16.2.5 CFM リンクトレース

CFM リンクトレースは、レイヤー 2 ネットワークでの経路探索機能です。CFM リンクトレースを実施した MEP から LTM（Link Trace Message）を送信し、LTM を処理した MIP または MEP が LTR（Link Trace Reply）を応答します。CFM リンクトレースを実行するには、**`cfm linktrace`** コマンドを使用します。結果を表示するには **`show cfm linktrace`** コマンドを、結果を削除するには **`clear cfm linktrace`** コマンドを使用します。

図 16-6 CFM リンクトレース



16.3 Ethernet OAM/CFM の状態確認

Ethernet OAM/CFM の状態を表示して確認する方法を説明します。

16.3.1 Ethernet OAM の設定の表示

show ethernet oam configuration コマンドで、Ethernet OAM の設定を確認できます。

ポート 1/0/1 を指定した場合の表示例を以下に示します。

```
# show ethernet oam configuration interface port 1/0/1

Port1/0/1 ...(1)
------------------------------------------------------------
OAM                       : Disabled ...(2)
Mode                      : Active ...(3)
Dying Gasp                : Enabled ...(4)
Critical Event            : Enabled ...(5)
Remote Loopback OAMPDU    : Not Processed ...(6)

Symbol Error ...(7)
  Notify State              : Enabled ...(8)
  Window                    : 10 deciseconds ...(9)
  Threshold                 : 1 Error Symbol ...(10)

Frame Error ...(11)
  Notify State              : Enabled
  Window                    : 10 deciseconds
  Threshold                 : 1 Error Frame

Frame Period Error ...(12)
  Notify State              : Enabled
  Window                    : 1488100 Frames
  Threshold                 : 1 Error Frame

Frame Seconds Error ...(13)
  Notify State              : Enabled
  Window                    : 600 deciseconds
  Threshold                 : 1 Error Seconds
```

各項目の説明は、以下のとおりです。

表 16-1 show ethernet oam configuration コマンドの表示項目

項番	説明
(1)	ポート番号を表示します。
(2)	Ethernet OAM の有効 (Enabled) ／無効 (Disabled) を表示します。
(3)	Ethernet OAM の動作モード（Active：アクティブモード／ Passive：パッシブモード）を表示します。
(4)	Dying Gasp イベント通知の有効 (Enabled) ／無効 (Disabled) を表示します。
(5)	クリティカルイベント通知の有効 (Enabled) ／無効 (Disabled) を表示します。
(6)	ピアから受信したリモートループバック設定要求の処理方法を表示します。 • Processed：リモートループバックモード設定要求を処理する • Not Processed：リモートループバックモード設定要求を無視する

項番	説明
(7)	Errored Symbol Period イベントに関する情報を表示します。
(8)	イベントの有効 (Enabled) ／無効 (Disabled) を表示します。
(9)	対象イベントの監視ウィンドウの設定値を表示します。
(10)	対象イベントのしきい値を表示します。
(11)	Errored Frame イベントに関する情報を表示します。
(12)	Errored Frame Period イベントに関する情報を表示します。
(13)	Errored Frame Seconds Summary イベントに関する情報を表示します。

16.3.2 Ethernet OAM の状態の表示

show ethernet oam status コマンドで、Ethernet OAM の状態を確認できます。

ポート 1/0/1 を指定した場合の表示例を以下に示します。

```
# show ethernet oam status interface port 1/0/1

Port1/0/1 ...(1)
  Local client ...(2)
    Admin state                   : Enabled ...(3)
    Mode                          : Active ...(4)
    Max OAMPDU size               : 1518 bytes ...(5)
    Remote loopback               : Supported ...(6)
    Unidirectional                : Not supported ...(7)
    Link monitoring               : Supported ...(8)
    Variable request              : Not supported ...(9)
    PDU revision                  : 0 ...(10)
    Operation status              : Operational ...(11)
    Loopback status               : No loopback ...(12)

  Remote client ...(13)
    Mode                          : Passive
    MAC address                   : 0040.66A8.C9A6 ...(14)
    Vendor (OUI)                  : 004066 ...(15)
    Max OAMPDU size               : 1518 bytes
    Unidirection                  : Not supported
    Link monitoring               : Supported
    Variable request              : Not supported
    PDU revision                  : 0
```

各項目の説明は、以下のとおりです。

表 16-2 show ethernet oam status コマンドの表示項目

項番	説明
(1)	ポート番号を表示します。
(2)	自装置側の情報を表示します。
(3)	Ethernet OAM の有効 (Enabled) ／無効 (Disabled) を表示します。
(4)	Ethernet OAM の動作モード（Active：アクティブモード／ Passive：パッシブモード）を表示します。

項番	説明
(5)	OAMPDU の最大サイズを表示します。
(6)	ループバックモードの対応状況（Supported ／ Not supported）を表示します。
(7)	単方向リンクでの OAMPDU 送信の対応状況（Supported ／ Not supported）を表示します。
(8)	Event Notification 送受信の対応状況（Supported ／ Not supported）を表示します。
(9)	Variable Request 送受信の対応状況（Supported ／ Not supported）を表示します。
(10)	OAMPDU のリビジョンを表示します。
(11)	Ethernet OAM の状態を表示します。 • Disable：Ethernet OAM が無効 • LinkFault：リンク障害を検出 • PassiveWait：パッシブモードのポートでピアが Ethernet OAM に対応しているか確認中 • ActiveSendLocal：アクティブモードのポートでローカル情報を送信中 • SendLocalAndRemote：ピアを検出済み（設定待ち） • SendLocalAndRemoteOk：ピアを検出済み（設定済み） • PeeringLocallyRejected：ローカル OAM エンティティーはピアを拒否 • PeeringRemotelyRejected：リモート OAM エンティティーはローカル装置を拒否 • Operational：Ethernet OAM を利用可能（ローカル装置とピアの両方が接続を受け入れ） • NonOperHalfDuplex：ポートが半二重ポートのため不完全動作
(12)	ポートのループバック状態を表示します。 • No loopback：非ループバック状態 • Local loopback：自装置側のポートがループバック状態 • Remote loopback：隣接装置側のポートがループバック状態
(13)	隣接装置側の情報を表示します。
(14)	MAC アドレスを表示します。
(15)	MAC アドレスのベンダー識別子を表示します。

16.3.3 Ethernet OAM の統計情報の表示

show ethernet oam statistics コマンドで、Ethernet OAM の統計情報を確認できます。

ポート 1/0/1 を指定した場合の表示例を以下に示します。

```
# show ethernet oam statistics interface port 1/0/1

Port1/0/1 ...(1)
------------------------------------------------------------
  Information OAMPDU TX                 : 0 ...(2)
  Information OAMPDU RX                 : 0 ...(3)
  Unique Event Notification OAMPDU TX   : 0 ...(4)
  Unique Event Notification OAMPDU RX   : 0 ...(5)
  Duplicate Event Notification OAMPDU TX: 0 ...(6)
  Duplicate Event Notification OAMPDU RX: 0 ...(7)
  Loopback Control OAMPDU TX            : 0 ...(8)
  Loopback Control OAMPDU RX            : 0 ...(9)
  Variable Request OAMPDU TX            : 0 ...(10)
  Variable Request OAMPDU RX            : 0 ...(11)
  Variable Response OAMPDU TX           : 0 ...(12)
  Variable Response OAMPDU RX           : 0 ...(13)
  Organization Specific OAMPDUs TX      : 0 ...(14)
  Organization Specific OAMPDUs RX      : 0 ...(15)
  Unsupported OAMPDU TX                 : 0 ...(16)
  Unsupported OAMPDU RX                 : 0 ...(17)
  Frames Lost Due To OAM                : 0 ...(18)
```

各項目の説明は、以下のとおりです。

表 16-3 show ethernet oam statistics コマンドの表示項目

項番	説明
(1)	ポート番号を表示します。
(2)	Information OAMPDU の送信数を表示します。
(3)	Information OAMPDU の受信数を表示します。
(4)	Unique Event Notification OAMPDU の送信数を表示します。
(5)	Unique Event Notification OAMPDU の受信数を表示します。
(6)	Duplicate Event Notification OAMPDU の送信数を表示します。
(7)	Duplicate Event Notification OAMPDU の受信数を表示します。
(8)	Loopback Control OAMPDU の送信数を表示します。
(9)	Loopback Control OAMPDU の受信数を表示します。
(10)	Variable Request OAMPDU の送信数を表示します。
(11)	Variable Request OAMPDU の受信数を表示します。
(12)	Variable Response OAMPDU の送信数を表示します。
(13)	Variable Response OAMPDU の受信数を表示します。
(14)	Organization Specific OAMPDU の送信数を表示します。
(15)	Organization Specific OAMPDU の受信数を表示します。

項番	説明
(16)	非対応な OAMPDU の送信数を表示します。
(17)	非対応な OAMPDU の受信数を表示します。
(18)	Ethernet OAM によって廃棄されたフレーム数を表示します。

16.3.4 Ethernet OAM のイベントログの表示

show ethernet oam event-log コマンドで、Ethernet OAM のイベントログを確認できます。

ポート 1/0/1 を指定した場合の表示例を以下に示します。

```
# show ethernet oam event-log interface port 1/0/1

Port1/0/1 ...(1)
    Local Faults: ...(2)
    -------------
      0 Link Fault records ...(3)
      0 Dying Gasp records ...(4)
      0 Critical Event records ...(5)

    Remote Faults: ...(6)
    -------------
      0 Link Fault records
      0 Dying Gasp records
      1 Critical Event records
         Event index : 1 ...(7)
         Time stamp  : 2022-07-07 11:14 ...(8)


    Local event logs: ...(9)
    -------------
      0 Errored Symbol records ...(10)
      1 Errored Frame records ...(11)
         Event index         : 2
         Time stamp          : 2022-07-07 11:20
         Error frame/symbol  : 542 ...(12)
         Window              : 1000 (millisecond) ...(13)
         Threshold           : 1 ...(14)
         Accumulated errors  : 542 ...(15)

      0 Errored Frame Period records ...(16)
      1 Errored Frame Second records ...(17)
         Event index         : 3
         Time stamp          : 2022-07-07 11:20
         Error frame/symbol  : 1
         Window              : 60000 (millisecond)
         Threshold           : 1
         Accumulated errors  : 1


    Remote event logs: ...(18)
    -------------
      0 Errored Symbol records
      0 Errored Frame records
      0 Errored Frame Period records
      0 Errored Frame Second records
```

各項目の説明は、以下のとおりです。

表 16-4 `show ethernet oam event-log` コマンドの表示項目

項番	説明
(1)	ポート番号を表示します。
(2)	自装置側で生成した Fault イベントの情報を表示します。
(3)	リンク障害のイベントログ数を表示します。
(4)	Dying Gasp のイベントログ数を表示します。
(5)	クリティカルイベントのログ数を表示します。
(6)	隣接装置側で生成した Fault イベントの情報を表示します。
(7)	イベントログ番号を表示します。
(8)	イベント発生時のタイムスタンプを表示します。
(9)	自装置側で生成したイベントログの情報を表示します。
(10)	Errored Symbol Period イベントログの数を表示します。
(11)	Errored Frame イベントログの数を表示します。
(12)	しきい値を比較する値（シンボルエラー数、エラーフレーム数、エラーフレームを検出した秒数）を表示します。
(13)	設定した監視ウィンドウの値を表示します。
(14)	設定したしきい値を表示します。
(15)	しきい値を比較する値の累積数を表示します。
(16)	Errored Frame Period イベントログの数を表示します。
(17)	Errored Frame Seconds Summary イベントログの数を表示します。
(18)	隣接装置側で生成したイベントログの情報を表示します。

16.3.5 単方向リンク検出機能の情報の表示

`show uld` コマンドで、単方向リンク検出機能の情報を確認できます。

ポート 1/0/1 を指定した場合の表示例を以下に示します。

```
# show uld interface port 1/0/1

Port1/0/1 ...(1)
    Admin State             : Enabled ...(2)
    Oper Status             : Enabled ...(3)
    Action                  : Shutdown ...(4)
    Link Status             : Bidirectional ...(5)
    Discovery Time(Sec)     : 5 ...(6)
```

各項目の説明は、以下のとおりです。

表 16-5 `show uld` コマンドの表示項目

項番	説明
(1)	ポート番号を表示します。
(2)	単方向リンク検出機能の有効 (Enabled) ／無効 (Disabled) を表示します。
(3)	動作状態を表示します。 • Enabled：対応した OAMPDU を受信している状態 • Disabled：対応した OAMPDU を未受信の状態
(4)	単方向リンク検出機能のアクション設定を表示します。 • Shutdown：単方向リンク検出時に対象ポートをシャットダウン（err-disabled 状態に変更） • Normal：単方向リンク検出時にログのみ出力
(5)	対向とのネゴシエーション状態を表示します。 • Bidirectional：お互いを正常に認識している状態 • RX Fault：受信方向の通信障害（双方向通信不可の場合も含む）を検出した状態 • TX Fault：送信方向の通信障害を検出した状態 • Link Down：対象ポートがリンクダウンしている状態（err-disabled 状態は除く） • Unknown：ネゴシエーションが完了していない状態
(6)	Discovery プロセスの完了待機時間を表示します。

16.3.6 CFM のグローバル設定の表示

`show cfm` コマンドで、CFM のグローバル設定を確認できます。

表示例を以下に示します。

```
# show cfm

CFM State: Enabled ...(1)
(2)                                    (3)
Domain Name: md5                       Level: 5
Domain Name: md6                       Level: 2
```

各項目の説明は、以下のとおりです。

表 16-6 `show cfm` コマンドの表示項目

項番	説明
(1)	CFM のグローバル設定の有効 (Enabled) ／無効 (Disabled) を表示します。
(2)	MD 名を表示します。
(3)	ドメインレベルを表示します。

16.3.7 インターフェースの CFM 情報の表示

show cfm interface コマンドで、インターフェースの CFM 情報を確認できます。

ポート 1/0/12 を指定した場合の表示例を以下に示します。

```
# show cfm interface port 1/0/12

Port1/0/12 ...(1)
CFM is enabled ...(2)
MAC Address: 00-40-66-A8-D5-62 ...(3)

  Domain Name: md5 ...(4)
  Level: 5 ...(5)
  MA Name: ma5 ...(6)
  VID: 10 ...(7)
  MEPID: 2 ...(8)
  Direction: Down ...(9)

  Domain Name: md6
  Level: 6
  MA Name: ma6
  VID: 10
  MEPID: MIP
```

各項目の説明は、以下のとおりです。

表 16-7 show cfm interface コマンドの表示項目

項番	説明
(1)	ポート番号を表示します。
(2)	CFM のポートごとの有効 (CFM is enabled) ／無効 (CFM is disabled) を表示します。
(3)	MAC アドレスを表示します。
(4)	MD 名を表示します。
(5)	ドメインレベルを表示します。
(6)	MA 名を表示します。
(7)	監視対象 VLAN を表示します。
(8)	MEP ID を表示します。対象が MIP の場合は MIP と表示されます。
(9)	MEP の配置方向（Up ／ Down）を表示します。

16.3.8 MD 情報の表示

show cfm domain コマンドで、MD 情報を確認できます。

MD 名 op-domain を指定した場合の表示例を以下に示します。

```
# show cfm domain op-domain

Domain Name: op-domain ...(1)
Domain Level: 2 ...(2)
MIP Creation: Auto ...(3)
SenderID TLV: Chassis ...(4)
MA Name: op1 ...(5)
MA Name: op-mal
```

各項目の説明は、以下のとおりです。

表 16-8 show cfm domain コマンドの表示項目

項番	説明
(1)	MD 名を表示します。
(2)	ドメインレベルを表示します。
(3)	MIP の作成方法を表示します。 • Auto：自動作成 • Explicit：既存の下位の MEP が設定されているポートで MIP を作成 • None：MIP を作成しない
(4)	Sender ID TLV の付加ルールを表示します。 • Chassis：Chassis ID 情報を含む Sender ID TLV を付加 • Chassis_manage：Chassis ID 情報と Management Address 情報を含む Sender ID TLV を付加 • Manage：Management Address 情報を含む Sender ID TLV を付加 • None：Sender ID TLV を付加しない
(5)	MD 内に存在する MA を表示します。

16.3.9 MA 情報の表示

show cfm ma コマンドで、MA 情報を確認できます。

MD 名 md5、MA 名 ma5 を指定した場合の表示例を以下に示します。

```
# show cfm ma name ma5 domain md5

MA Name: ma5 ...(1)
MA VID: 10 ...(2)
MIP Creation: Auto ...(3)
CCM Interval: 10 seconds ...(4)
SenderID TLV: Chassis ...(5)
MEPID List  : 1-2 ...(6)
   (7)       (8)          (9)
   MEPID: 1  Port: 1/0/2  Direction: Up
```

各項目の説明は、以下のとおりです。

表 16-9 show cfm ma コマンドの表示項目

項番	説明
(1)	MA 名を表示します。
(2)	監視対象 VLAN を表示します。
(3)	MIP の作成方法を表示します。 • Auto：自動作成 • Explicit：既存の下位の MEP が設定されているポートで MIP を作成 • None：MIP を作成しない • Defer：MD の設定に従う
(4)	CCM の送信間隔を表示します。
(5)	Sender ID TLV の付加ルールを表示します。 • Chassis：Chassis ID 情報を含む Sender ID TLV を付加 • Chassis_manage：Chassis ID 情報と Management Address 情報を含む Sender ID TLV を付加 • Manage：Management Address 情報を含む Sender ID TLV を付加 • None：Sender ID TLV を付加しない • Defer：MD の設定に従う
(6)	MEP ID リストを表示します。
(7)	MEP ID を表示します。
(8)	ポート番号を表示します。
(9)	MEP の配置方向（Up ／ Down）を表示します。

16.3.10 MEP 情報の表示

show cfm mepid コマンドで、MEP 情報を確認できます。

MD 名 op-domain、MA 名 op-ma、MEP ID 2 を指定した場合の表示例を以下に示します。

```
# show cfm mepid 2 ma name op-ma domain op-domain

MEPID: 2 ...(1)
Port: 1/0/9 ...(2)
Direction: Up ...(3)
CFM Port Status: Enabled ...(4)
MAC Address: 00-40-66-20-24-0D ...(5)
MEP State: Enabled ...(6)
CCM State: Enabled ...(7)
PDU Priority: 7 ...(8)
Fault Alarm: Disabled ...(9)
Alarm Time: 250 centisecond((1/100)s) ...(10)
Alarm Reset Time: 1000 centisecond((1/100)s) ...(11)
Highest Fault: Some Remote MEP MAC Status Error ...(12)
AIS State: Disabled ...(13)
AIS Period: 1 Second ...(14)
AIS Client Level: Invalid ...(15)
AIS Status: Not Detected ...(16)
LCK State: Disabled ...(17)
LCK Period: 1 Second ...(18)
LCK Client Level: Invalid ...(19)
LCK Status: Not Detected ...(20)
LCK Action: Stop ...(21)
Out-of-Sequence CCMs Received: 0 ...(22)
Cross-connect CCMs Received: 0 ...(23)
Error CCMs Received: 0 ...(24)              Normal CCMs Received: 0 ...(25)
Port Status CCMs Received: 0 ...(26)        If Status CCMs Received: 0 ...(27)
CCMs transmitted: 14813 ...(28)             In-order LBRs Received: 0 ...(29)
Out-of-order LBRs Received: 0 ...(30)       Next LTM Trans ID: 1 ...(31)
Unexpected LTRs Received: 0 ...(32)         LBMs Transmitted: 0 ...(33)
AIS PDUs Received: 0 ...(34)                AIS PDUs Transmitted: 0 ...(35)
LCK PDUs Received: 0 ...(36)                LCK PDUs Transmitted: 0 ...(37)
```

各項目の説明は、以下のとおりです。

表 16-10 show cfm mepid コマンドの表示項目

項番	説明
(1)	MEP ID を表示します。
(2)	ポート番号を表示します。
(3)	MEP の配置方向（Up ／ Down）を表示します。
(4)	CFM のポートごとの有効 (Enabled) ／無効 (Disabled) を表示します。
(5)	MAC アドレスを表示します。
(6)	MEP の有効 (Enabled) ／無効 (Disabled) を表示します。
(7)	CCM の有効 (Enabled) ／無効 (Disabled) を表示します。
(8)	CCM の IEEE 802.1p 優先度を表示します。

項番	説明
(9)	障害アラームの送信設定を表示します。 • Disabled：障害アラームを送信しない • All：すべての障害に対して送信 • Some Remote MEP MAC Status Error：「DefMACstatus」以上の障害に対して送信 • Some Remote MEP Down：「DefRemoteCCM」以上の障害に対して送信 • Error CCM Received：「DefErrorCCM」以上の障害に対して送信 • Cross-connect CCM Received：「DefXconCCM」の障害に対してのみ送信
(10)	障害アラームの送信待機時間を表示します。
(11)	障害アラームのリセット待機時間を表示します。
(12)	MEP で検出された最高優先度の障害を表示します。 • None：障害を検出していない状態 • Some Remote MEP Defect Indication：「DefRDICCM」を検出 • Some Remote MEP MAC Status Error：「DefMACstatus」を検出 • Some Remote MEP Down：「DefRemoteCCM」を検出 • Error CCM Received：「DefErrorCCM」を検出 • Cross-connect CCM Received：「DefXconCCM」を検出
(13)	AIS 機能の有効 (Enabled) ／無効 (Disabled) を表示します。
(14)	AIS フレームの送信間隔を表示します。
(15)	AIS フレームを送信するドメインレベルを表示します。ドメインレベルが未決定の場合は Invalid と表示されます。
(16)	AIS フレームの受信状況（Not Detected：未検出／ Detected：検出）を表示します。
(17)	LCK 機能の有効 (Enabled) ／無効 (Disabled) を表示します。
(18)	LCK フレームの送信間隔を表示します。
(19)	LCK フレームを送信するドメインレベルを表示します。ドメインレベルが未決定の場合は Invalid と表示されます。
(20)	LCK フレームの受信状況（Not Detected：未検出／ Detected：検出）を表示します。
(21)	LCK フレームの送信状況（Stop：停止／ Start：開始）を表示します。
(22)	不正な順序で受信した CCM の数を表示します。
(23)	他の MA から受信した CCM の数を表示します。
(24)	無効な CCM の数を表示します。
(25)	通常の CCM の数を表示します。
(26)	ポート状態を含めて送信された CCM の数を表示します。
(27)	ステータスを含めて送信された CCM の数を表示します。
(28)	送信済み CCM の数を表示します。
(29)	有効なメッセージおよび有効な順序で受信した LBR の数を表示します。

項番	説明
(30)	不正な順序で受信した LBR の数を表示します。
(31)	LTM の次の送信先を表示します。
(32)	装置で受信した予期しない LTR の数を表示します。
(33)	送信した LBM の数を表示します。
(34)	受信した AIS フレームの数を表示します。
(35)	送信した AIS フレームの数を表示します。
(36)	受信した LCK フレームの数を表示します。
(37)	送信した LCK フレームの数を表示します。

16.3.11 MEP で検出した障害情報の表示

`show cfm mep fault` コマンドで、MEP で検出した障害情報を確認できます。

表示例を以下に示します。

```
# show cfm mep fault

Domain Name: md5 ...(1)
MA Name: ma5 ...(2)
MEPID: 2 ...(3)
Status: Some Remote MEP Down ...(4)
AIS Status: Normal ...(5)
LCK Status: Normal ...(6)
```

各項目の説明は、以下のとおりです。

表 16-11 `show cfm mep fault` コマンドの表示項目

項番	説明
(1)	MD 名を表示します。
(2)	MA 名を表示します。
(3)	障害を検出した MEP ID を表示します。
(4)	MEP で検出された最高優先度の障害を表示します。 • None：障害を検出していない状態 • Some Remote MEP Defect Indication：「DefRDICCM」を検出 • Some Remote MEP MAC Status Error：「DefMACstatus」を検出 • Some Remote MEP Down：「DefRemoteCCM」を検出 • Error CCM Received：「DefErrorCCM」を検出 • Cross-connect CCM Received：「DefXconCCM」を検出
(5)	AIS フレームの受信状況（AIS Received：受信中／ Normal：未受信）を表示します。
(6)	LCK フレームの受信状況（LCK Received：受信中／ Normal：未受信）を表示します。

16.3.12 すべての MEP の CCM 受信カウンターの表示

show cfm counter ccm コマンドで、すべての MEP の CCM 受信カウンターを確認できます。

表示例を以下に示します。

```
# show cfm counter ccm

CCM counters:
(1)           (2)         (3)           (4)               (5)
MEPID: 1      VID: 10     Level: 5      Direction: Up     Port: 1/0/1
 XCON: 0 ...(6)     Error: 10 ...(7)    Normal: 1862 ...(8)
MEPID: 1002   VID: 210    Level: 3      Direction: Down   Port: 1/0/21
 XCON: 7            Error: 0            Normal: 431

Total:
 XCON: 7            Error: 10           Normal: 2293
```

各項目の説明は、以下のとおりです。

表 16-12 show cfm counter ccm コマンドの表示項目

項番	説明
(1)	MEP ID を表示します。
(2)	監視対象 VLAN を表示します。
(3)	ドメインレベルを表示します。
(4)	MEP の配置方向（Up ／ Down）を表示します。
(5)	ポート番号を表示します。
(6)	他の MA からの可能性がある CCM の受信数を表示します。
(7)	無効な CCM の受信数を表示します。
(8)	有効な CCM の受信数を表示します。

16.3.13 リモート MEP 情報の表示

show cfm remote-mep コマンドで、リモート MEP 情報を確認できます。

MD 名 op-domain、MA 名 op-ma、MEP ID 1 を指定した場合の表示例を以下に示します。

```
# show cfm remote-mep mepid 1 ma name op-ma domain op-domain

Remote MEPID: 2 ...(1)
MAC Address: 00-40-66-20-48-0F ...(2)
(3)          (4)
Status: OK,  RDI: Yes
(5)                  (6)
Port State: Blocked, Interface Status: Up
Last CCM Serial Number: 180 ...(7)
Sender Chassis ID: None ...(8)
Sender Management Address: None ...(9)
Detect Time: 2016-07-06 10:29:02 ...(10)

Remote MEPID: 3
MAC Address: FF-FF-FF-FF-FF-FF
Status: FAILED,  RDI: No
Port State: No, Interface Status: No
Last CCM Serial Number: 0
Sender Chassis ID: None
Sender Management Address: None
Detect Time: 2016-07-06 10:27:46
```

各項目の説明は、以下のとおりです。

表 16-13 show cfm remote-mep コマンドの表示項目

項番	説明
(1)	MEP ID リストに登録されているリモート MEP の MEP ID を表示します。
(2)	リモート MEP の MAC アドレスを表示します。一度も有効な CCM を受信したことがない状態では FF-FF-FF-FF-FF-FF と表示されます。
(3)	リモート MEP からの CCM 受信状態を表示します。 • IDLE：アイドル状態（自装置の MEP がまだ使用できない状態） • START：自装置の MEP が使用可能になってからタイムアウトタイマーがまだ満了しておらず、かつ有効な CCM を受信していない状態 • FAILED：有効な CCM を受信していない状態 • OK：有効な CCM を受信している状態
(4)	最後に受信した有効な CCM の RDI ビットを表示します。 • Yes：RDI ビットがセットされている（リモート MEP が障害を検出している状態） • No：RDI ビットがセットされていない（リモート MEP が障害を検出していない状態）
(5)	最後に受信した有効な CCM に含まれる、Port Status TLV の値を表示します。 • No：CCM 未受信、または受信した CCM に Port Status TLV が含まれていない • Blocked：psBlocked(1) • Up：psUp(2)

項番	説明
(6)	最後に受信した有効な CCM に含まれる、Interface Status TLV の値を表示します。 • No：CCM 未受信、または受信した CCM に Interface Status TLV が含まれていない • Up：isUp(1) • Down：isDown(2) • Testing：isTesting(3) • Unknown：isUnknown(4) • Dormant：isDormant(5) • Notpresent：isNotPresent(6) • Lowerlayerdown：isLowerLayerDown(7)
(7)	最後に受信した有効な CCM の Sequence Number を表示します。
(8)	最後に受信した有効な CCM に含まれる、Sender ID TLV の Chassis ID の値を表示します。含まれない場合は None と表示されます。
(9)	最後に受信した有効な CCM に含まれる、Sender ID TLV の Management Address の値を表示します。含まれない場合は None と表示されます。
(10)	最後に有効な CCM を受信した時間を表示します。自装置の MEP が使用可能になってから一度も有効な CCM を受信したことがない場合は、リモート MEP からの CCM 受信状態が FAILED になった時間を表示します。

16.3.14 MIP の CCM データベースエントリーの表示

show cfm mip ccm コマンドで、MIP の CCM データベースエントリーを確認できます。

表示例を以下に示します。

```
# show cfm mip ccm

      VID: 10 ...(1)
      MAC Address: 00-40-66-00-00-1C ...(2)
      Port: Port1/0/12 ...(3)

      VID: 10
      MAC Address: 00-40-66-00-00-1E
      Port: Port1/0/14

      Total: 2 ...(4)
```

各項目の説明は、以下のとおりです。

表 16-14 show cfm mip ccm コマンドの表示項目

項番	説明
(1)	監視対象 VLAN を表示します。
(2)	受信した CCM の送信元 MEP の MAC アドレスを表示します。
(3)	CCM を受信したポート番号を表示します。
(4)	MIP の CCM データベースエントリー数を表示します。

16.3.15 CFM カウンターの表示

show cfm pkt-cnt interface コマンドで、CFM カウンターを確認できます。

ポート 1/0/1 を指定した場合の表示例を以下に示します。

```
# show cfm pkt-cnt interface port 1/0/1

Port1/0/1 ...(1)
  CFM RX Statistics
    AllPkt:498 ...(2)  CCM:484 ...(3)
    LBR:8 ...(4)       LBM:4 ...(5)
    LTR:2 ...(6)       LTM:0 ...(7)
    VidDrop:0 ...(8)   OpcoDrop:0 ...(9)
  CFM TX Statistics
    AllPkt:257 ...(10) CCM:243 ...(11)
    LBR:4 ...(12)      LBM:8 ...(13)
    LTR:0 ...(14)      LTM:2 ...(15)
```

各項目の説明は、以下のとおりです。

表 16-15 show cfm pkt-cnt interface コマンドの表示項目

項番	説明
(1)	ポート番号を表示します。
(2)	受信したすべての CFM PDU 数を表示します。
(3)	受信 CCM 数を表示します。
(4)	受信 LBR 数を表示します。
(5)	受信 LBM 数を表示します。
(6)	受信 LTR 数を表示します。
(7)	受信 LTM 数を表示します。
(8)	監視対象 VLAN で受信できず廃棄された CFM PDU 数を表示します。
(9)	予期しない OP コードのために廃棄された CFM PDU 数を表示します。
(10)	送信したすべての CFM PDU 数を表示します。
(11)	送信 CCM 数を表示します。
(12)	送信 LBR 数を表示します。
(13)	送信 LBM 数を表示します。
(14)	送信 LTR 数を表示します。
(15)	送信 LTM 数を表示します。

16.3.16 CFM リンクトレース結果の表示

show cfm linktrace コマンドで、CFM リンクトレース結果を確認できます。

MD 名 op-domain、MA 名 op-ma、MEP ID 1、トランザクション ID 1 を指定した場合の表示例を以下に示します。

```
# show cfm linktrace mepid 1 ma name op-ma domain op-domain trans-id 1

Transaction ID: 1 ...(1)
From MEPID 1 to 00-40-66-A8-C9-A6 ...(2)
Start Time: 2015-11-20 16:49:30 ...(3)
Hop: 1 ...(4)
   Ingress MAC Address: 00-00-00-00-00-00 ...(5)
   Egress MAC Address : 00-40-66-A8-D5-59 ...(6)
   (7)              (8)
   Forwarded: Yes  Relay Action: FDB
Hop: 2
   Ingress MAC Address: 00-40-66-A8-C9-A6
   Egress MAC Address : 00-00-00-00-00-00
   Forwarded: No  Relay Action: Hit
```

各項目の説明は、以下のとおりです。

表 16-16 show cfm linktrace コマンドの表示項目

項番	説明
(1)	トランザクション ID を表示します。
(2)	LTM の送信元 MEP ID および宛先 MAC アドレスを表示します。
(3)	CFM リンクトレースの開始日時を表示します。
(4)	CFM リンクトレースの経路の順番を表示します。
(5)	LTM を受信したメンテナンスポイントの MAC アドレスを表示します。
(6)	LTM を送信したメンテナンスポイントの MAC アドレスを表示します。
(7)	メンテナンスポイントにおける CFM リンクトレースの転送状態（Yes：転送状態／ No：非転送状態）を表示します。
(8)	CFM リンクトレースの状態を表示します。 • FDB：MAC アドレステーブルによって、送信ポートを決定 • MPDB：MIP の CCM データベースによって、送信ポートを決定 • Hit：LTM の宛先と一致するメンテナンスポイントに到達

16.3.17 すべてのメンテナンスポイントが LTR を応答する機能の設定の表示

show cfm mp-ltr-all コマンドで、すべてのメンテナンスポイントが LTR を応答する機能の設定を確認できます。

表示例を以下に示します。

```
# show cfm mp-ltr-all

All MPs reply LTRs: Enabled ...(1)
```

各項目の説明は、以下のとおりです。

表 16-17 show cfm mp-ltr-all コマンドの表示項目

項番	説明
(1)	すべてのメンテナンスポイントが LTR を応答する機能の有効 (Enabled) ／無効 (Disabled) を表示します。

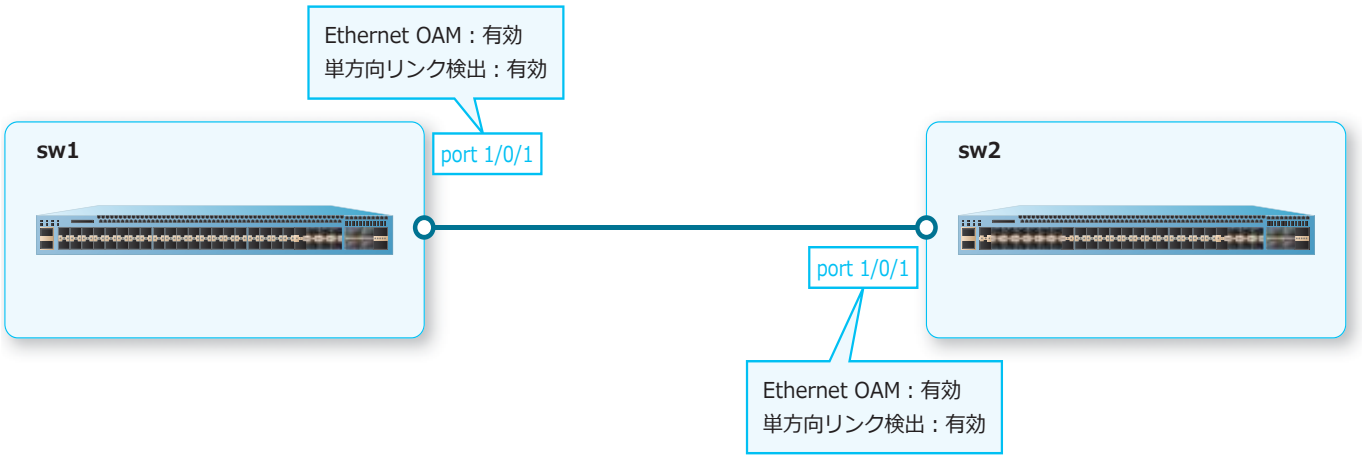
16.4 Ethernet OAM/CFM の構成例と設定例

Ethernet OAM/CFM を利用する場合の構成例と設定例を示します。

16.4.1 Ethernet OAM の構成例と設定例

Ethernet OAM と単方向リンク検出機能を利用して、2 台の隣接する装置間の回線状態を監視する場合の構成例と設定例を示します。

図 16-7 Ethernet OAM の構成例



1. ポート 1/0/1 の Ethernet OAM を有効化し、単方向リンク検出を有効化します。

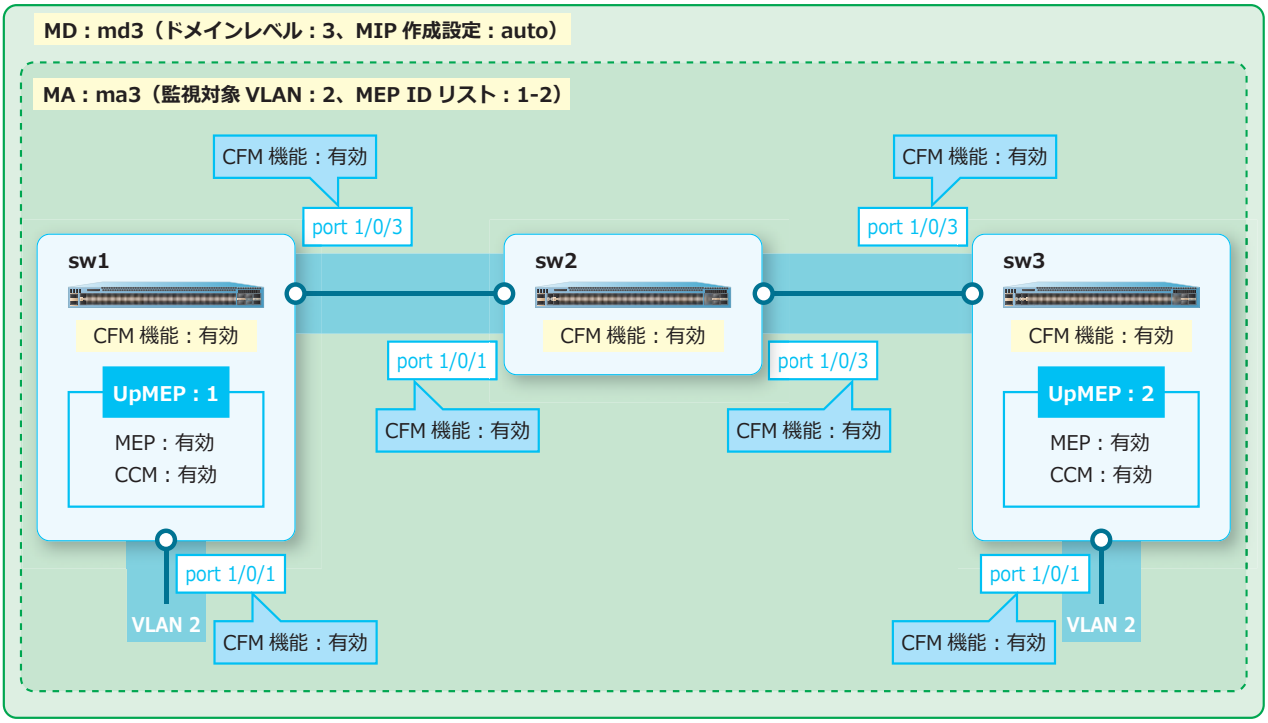
```
sw1# configure terminal
sw1(config)# interface port 1/0/1
sw1(config-if-port)# ethernet oam
sw1(config-if-port)# uld enable
sw1(config-if-port)# end
sw1#
```

2. sw2 も同様に設定します。

16.4.2 CFM の構成例と設定例

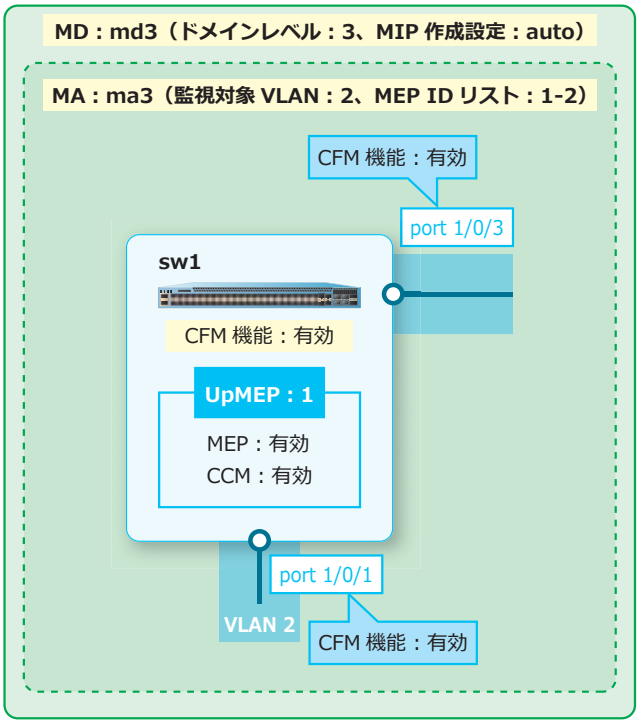
CFM によるレイヤー 2 ネットワークでの障害監視の構成例と設定例を示します。

図 16-8 CFM の構成例



16.4.2.1 CFM : sw1 の設定例

図 16-9 CFM : sw1 の設定例



1. VLAN 2 を作成します。

```
sw1# configure terminal
sw1(config)# vlan 2
sw1(config-vlan)# exit
sw1(config)#
```

2. ポート 1/0/1 およびポート 1/0/3 をトランクポートとして設定し、トランクポートに［VLAN 2］を割り当てます。

```
sw1(config)# interface range port 1/0/1,1/0/3
sw1(config-if-port-range)# switchport mode trunk
sw1(config-if-port-range)# switchport trunk allowed vlan 2
sw1(config-if-port-range)# exit
sw1(config)#
```

3. ドメインレベル［3］の MD［md3］を作成し、MIP 作成設定を［auto］に設定します。

```
sw1(config)# cfm domain md3 level 3
sw1(config-cfm-md)# mip creation auto
sw1(config-cfm-md)#
```

4. MD［md3］に、以下のような MA を設定します。

MA：MA 名［ma3］、監視対象 VLAN［VLAN 2］、MEP ID リスト［MEP ID 1 から MEP ID 2］

```
sw1(config-cfm-md)# cfm ma name ma3 vlan 2
sw1(config-cfm-ma)# mepid-list add 1-2
sw1(config-cfm-ma)# exit
sw1(config-cfm-md)# exit
sw1(config)#
```

5. ポート 1/0/1 に、以下のような MEP を設定し、MEP を有効化します。

MEP：MEP ID［1］、MA［ma3］、MD［md3］、配置方向［up］、CCM［有効］

```
sw1(config)# interface port 1/0/1
sw1(config-if-port)# cfm mep mepid 1 ma name ma3 domain md3 direction up
sw1(config-cfm-mep)# ccm enable
sw1(config-cfm-mep)# mep enable
sw1(config-cfm-mep)# exit
sw1(config-if-port)# exit
sw1(config)#
```

6. ポート 1/0/1 およびポート 1/0/3 の CFM 機能を有効化します。

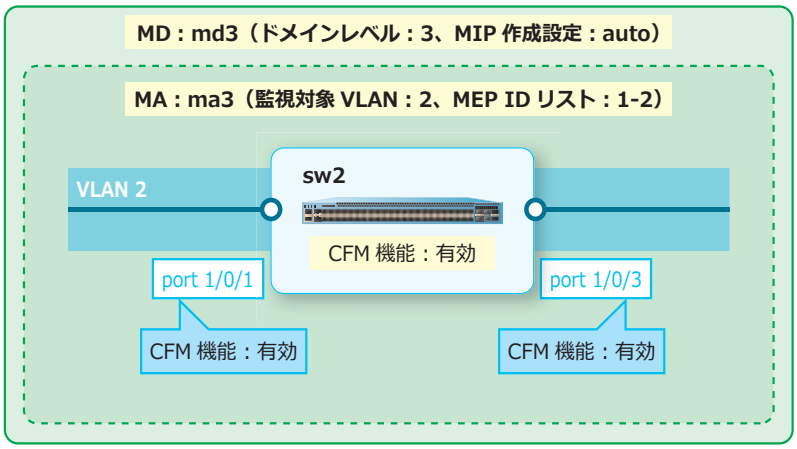
```
sw1(config)# interface range port 1/0/1,1/0/3
sw1(config-if-port-range)# cfm enable
sw1(config-if-port-range)# exit
sw1(config)#
```

7. CFM 機能を有効化します。

```
sw1(config)# cfm global enable
sw1(config)# end
sw1#
```

16.4.2.2 CFM：sw2 の設定例

図 16-10 CFM：sw2 の設定例



1. VLAN 2 を作成します。

```
sw2# configure terminal
sw2(config)# vlan 2
sw2(config-vlan)# exit
sw2(config)#
```

2. ポート 1/0/1 およびポート 1/0/3 をトランクポートとして設定し、トランクポートに［VLAN 2］を割り当てます。

```
sw2(config)# interface range port 1/0/1,1/0/3
sw2(config-if-port-range)# switchport mode trunk
sw2(config-if-port-range)# switchport trunk allowed vlan 2
sw2(config-if-port-range)# exit
sw2(config)#
```

3. ドメインレベル［3］の MD［md3］を作成し、MIP 作成設定を［auto］に設定します。

```
sw2(config)# cfm domain md3 level 3
sw2(config-cfm-md)# mip creation auto
sw2(config-cfm-md)#
```

4. MD［md3］に、以下のような MA を設定します。

MA：MA 名［ma3］、監視対象 VLAN［VLAN 2］

```
sw2(config-cfm-md)# cfm ma name ma3 vlan 2
sw2(config-cfm-ma)# exit
sw2(config-cfm-md)# exit
sw2(config)#
```

5. ポート 1/0/1 およびポート 1/0/3 の CFM 機能を有効化します。

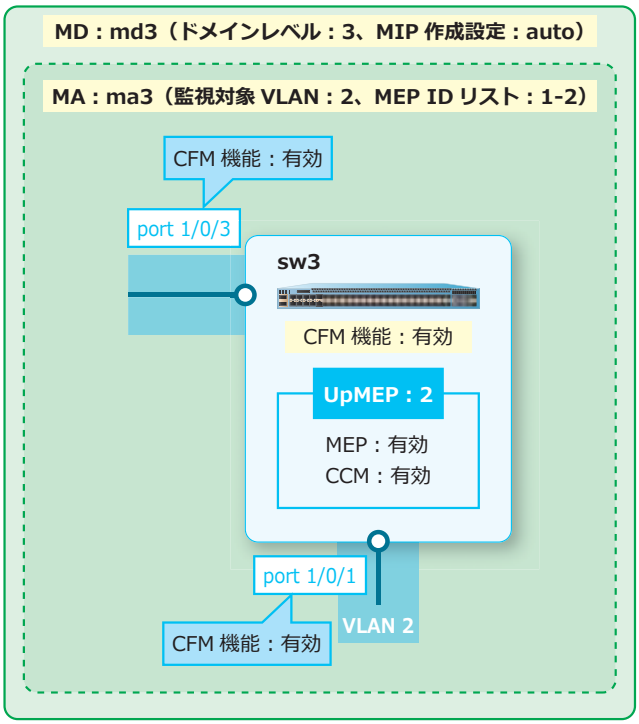
```
sw2(config)# interface range port 1/0/1,1/0/3
sw2(config-if-port-range)# cfm enable
sw2(config-if-port-range)# exit
sw2(config)#
```

6. CFM 機能を有効化します。

```
sw2(config)# cfm global enable
sw2(config)# end
sw2#
```

16.4.2.3 CFM：sw3 の設定例

図 16-11 CFM：sw3 の設定例



1. VLAN 2 を作成します。

```
sw3# configure terminal
sw3(config)# vlan 2
sw3(config-vlan)# exit
sw3(config)#
```

2. ポート 1/0/1 およびポート 1/0/3 をトランクポートとして設定し、トランクポートに［VLAN 2］を割り当てます。

```
sw3(config)# interface range port 1/0/1,1/0/3
sw3(config-if-port-range)# switchport mode trunk
sw3(config-if-port-range)# switchport trunk allowed vlan 2
sw3(config-if-port-range)# exit
sw3(config)#
```

3. ドメインレベル［3］の MD［md3］を作成し、MIP 作成設定を［auto］に設定します。

```
sw3(config)# cfm domain md3 level 3
sw3(config-cfm-md)# mip creation auto
sw3(config-cfm-md)#
```

4. MD［md3］に、以下のような MA を設定します。

MA：MA 名［ma3］、監視対象 VLAN［VLAN 2］、MEP ID リスト［MEP ID 1 から MEP ID 2］

```
sw3(config-cfm-md)# cfm ma name ma3 vlan 2
sw3(config-cfm-ma)# mepid-list add 1-2
sw3(config-cfm-ma)# exit
sw3(config-cfm-md)# exit
sw3(config)#
```

5. ポート 1/0/1 に、以下のような MEP を設定し、MEP を有効化します。

MEP：MEP ID［2］、MA［ma3］、MD［md3］、配置方向［up］、CCM［有効］

```
sw3(config)# interface port 1/0/1
sw3(config-if-port)# cfm mep mepid 2 ma name ma3 domain md3 direction up
sw3(config-cfm-mep)# ccm enable
sw3(config-cfm-mep)# mep enable
sw3(config-cfm-mep)# exit
sw3(config-if-port)# exit
sw3(config)#
```

6. ポート 1/0/1 およびポート 1/0/3 の CFM 機能を有効化します。

```
sw3(config)# interface range port 1/0/1,1/0/3
sw3(config-if-port-range)# cfm enable
sw3(config-if-port-range)# exit
sw3(config)#
```

7. CFM 機能を有効化します。

```
sw3(config)# cfm global enable
sw3(config)# end
sw3#
```

17. DHCP

DHCP（Dynamic Host Configuration Protocol）の機能、状態の確認方法、および構成例と設定例について説明します。

REF: コマンドの詳細については、『コマンドリファレンス』を参照してください。

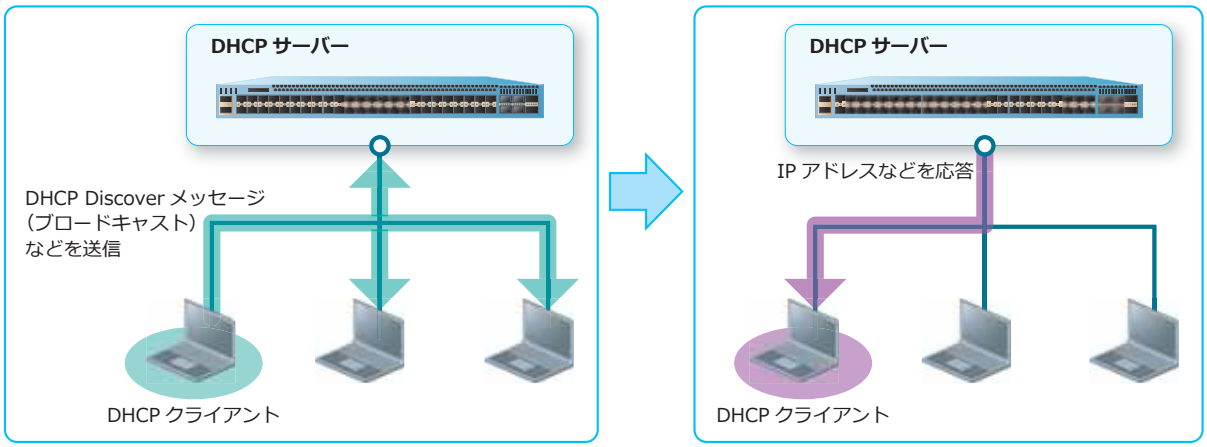
17.1 DHCP サーバーの機能説明

DHCP サーバーは、クライアントに割り当てる IP アドレスなどの情報を自動的に発行する機能です。DHCP サーバーを使用するには、必要な情報を設定してから **service dhcp** コマンドで有効にします。

CAUTION: セカンダリー IP アドレスで指定したサブネットでは、DHCP サーバー機能は動作しません。

CAUTION: DHCP サーバーが有効な状態では、設定の変更内容が反映されません。変更内容を反映するには、**no service dhcp** コマンドを使用して DHCP サーバーを一度無効にした後、再度 DHCP サーバーを有効にしてください。

図 17-1 DHCP サーバーの概要



DHCP サーバーは、DHCP クライアントに IP アドレスを割り当てる前に、その IP アドレスがすでに使用されているかどうかを ping によって確認します。ping による事前確認で応答がない場合、その IP アドレスは割り当て可能と判断され、DHCP クライアントに割り当てられます。ping による事前確認で応答があった場合は、その IP アドレスは割り当て候補から除外され、DHCP 競合エントリーとして登録されます。

ping による事前確認の送信回数を変更するには、**ip dhcp ping packets** コマンドを使用します。応答タイムアウト時間を変更するには、**ip dhcp ping timeout** コマンドを使用します。

NOTE: DHCP 競合エントリーとして登録された IP アドレスは、**clear ip dhcp conflict** コマンドで手動で削除されるまでリース対象になりません。

17.1.1 DHCP アドレスプール

クライアントに割り当てる IP アドレスなどの情報は、DHCP アドレスプールを作成してその中で設定します。サブネットごとに 1 つの DHCP アドレスプールを作成し、DHCP アドレスプールごとに DHCP クライアントに提供する情報を設定できます。DHCP アドレスプールは、**ip dhcp pool** コマンドで作成します。

> ***NOTE:*** 動的割り当てのための DHCP アドレスプールは最大 32 個設定でき、1 つのプールあたり最大 1,024 個のアドレスをリースできます。ただし、NP2100、NP2000、および NP2500 でサポートする動的割り当てのための DHCP アドレスプールは、最大 23 個です。

> ***NOTE:*** DHCP プール（動的割り当てのための DHCP アドレスプール、手動バインディングエントリーのための DHCP アドレスプール、DHCP リレーのための DHCP リレープール）は、装置全体であわせて最大 96 個まで設定できます。

DHCP アドレスプールごとに設定できる情報は以下のとおりです。（）内は使用するコマンドです。

- ネットワークアドレスとサブネットマスク（**network**）
- DHCP クラス（**class**）
- リース期間（**lease**）
- デフォルトルーター（**default-router**）
- ドメイン名（**domain-name**）
- DNS サーバー（**dns-server**）
- NetBIOS ノードタイプ（**netbios-node-type**）
- WINS サーバー（**netbios-name-server**）
- ブートサーバー（**next-server**）
- ブートファイル（**bootfile**）
- オプション（**option**）

DHCP クラス

DHCP クラスは、DHCP クライアントが送信した DHCP パケットのオプション情報を基に、DHCP クライアントを分類する機能です。分類した DHCP クラスごとに、DHCP サーバーがリースする IP アドレスの範囲を指定したり、DHCP リレーのリレー先 IP アドレスを指定したりできます。

DHCP クラスは、**ip dhcp class** コマンドで作成します。DHCP クラスを利用する場合は、**ip dhcp use class** コマンドを使用して、DHCP クラスの利用設定を有効化する必要があります。

> ***NOTE:*** 装置全体で設定できる DHCP クラスは最大 10 個ですが、DHCP クラスは複数の異なる DHCP プールに適用できます。また、1 つの DHCP アドレスプールでは最大 10 個の DHCP クラスを利用できます。

DHCP クラスの一致条件を設定するには、**option hex** コマンドを使用します。なお、一致条件が未設定の DHCP クラスは「一致条件 = any」の扱いになり、すべての DHCP クライアントが対象になります。

DHCP サーバーにおいて、分類した DHCP クラスごとにリースする IP アドレスの範囲を指定するには、**address range** コマンドを使用します。

17.1.2 IP アドレスのリース範囲の限定方法

IP アドレスのリース範囲を限定するには、以下の 2 種類の方法が使用できます。

- リース除外範囲の指定（**`ip dhcp excluded-address`**）
- DHCP クラスを利用したリースする IP アドレスの範囲指定

> ***NOTE:*** 自装置に設定した IP アドレス、または手動バインディングエントリーとして設定済みの IP アドレスは、リース対象から自動的に除外されます。

リース除外範囲の指定（ip dhcp excluded-address）

`ip dhcp excluded-address` コマンドを使用すると、リースする IP アドレスから除外する範囲を設定できます。

> ***NOTE:*** **`ip dhcp excluded-address`** コマンドは、装置全体で最大 5 個設定できます。

DHCP クラスを利用したリースする IP アドレスの範囲指定

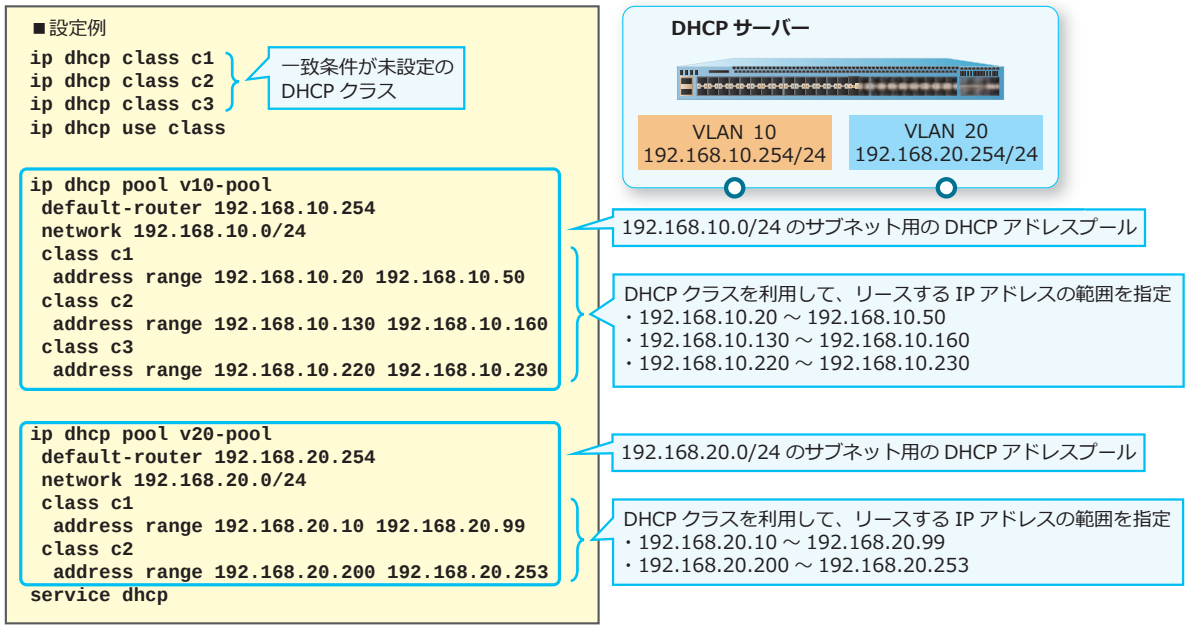
DHCP クラスは、一致条件が未設定の場合はすべての DHCP クライアントが対象になります。そのため、一致条件が未設定の DHCP クラスを利用することにより、1 つの DHCP アドレスプールあたり最大 10 個のリースする IP アドレスの範囲指定ができます。

> ***NOTE:*** 装置全体で設定できる DHCP クラスは最大 10 個ですが、DHCP クラスは複数の異なる DHCP プールに適用できます。また、1 つの DHCP アドレスプールでは最大 10 個の DHCP クラスを利用できます。

リースする IP アドレスの範囲指定を行う例を以下に示します。

- 192.168.10.0/24 のサブネットでは、リースする IP アドレスの範囲を「192.168.10.20 ～ 192.168.10.50」「192.168.10.130 ～ 192.168.10.160」「192.168.10.220 ～ 192.168.10.230」に限定
- 192.168.20.0/24 のサブネットでは、リースする IP アドレスの範囲を「192.168.20.10 ～ 192.168.20.99」「192.168.20.200 ～ 192.168.20.253」に限定

図 17-2 DHCP クラスを利用したリースする IP アドレスの範囲指定の例



17.1.3 手動バインディングエントリー

手動バインディングエントリーは、特定の MAC アドレスまたは特定のクライアント ID からの要求に対して、リースする IP アドレスを固定できます。

> ***NOTE:*** 手動バインディングエントリーのための DHCP アドレスプールは最大 64 個設定でき、1 つのプールあたり 1 個の手動バインディングエントリーを設定できます。
>
> ***NOTE:*** DHCP プール（動的割り当てのための DHCP アドレスプール、手動バインディングエントリーのための DHCP アドレスプール、DHCP リレーのための DHCP リレープール）は、装置全体で合わせて最大 96 個まで設定できます。

手動バインディングエントリーのための DHCP アドレスプールでは、以下のいずれかの方法でリースする IP アドレスを手動で設定します。

- **host** コマンドで「手動バインディングエントリーの IP アドレス」を設定し、それをリースする MAC アドレスを **hardware-address** コマンドで紐付ける。
- **host** コマンドで「手動バインディングエントリーの IP アドレス」を設定し、それをリースするクライアント ID を **client-identifier** コマンドで紐付ける。

また、「ネットワークアドレスとサブネットマスク（**network**）」「DHCP クラス（**class**）」以外の情報は、手動バインディングエントリーのための DHCP アドレスプールでも設定できます。

17.1.4 バインディングエントリーの手動削除

DHCP サーバーからリースされた IP アドレスは、DHCP サーバーのバインディングエントリーとして登録されます。登録されているバインディングエントリーを削除するには、**clear ip dhcp binding** コマンドを使用します。

17.1.5 競合エントリーの手動削除

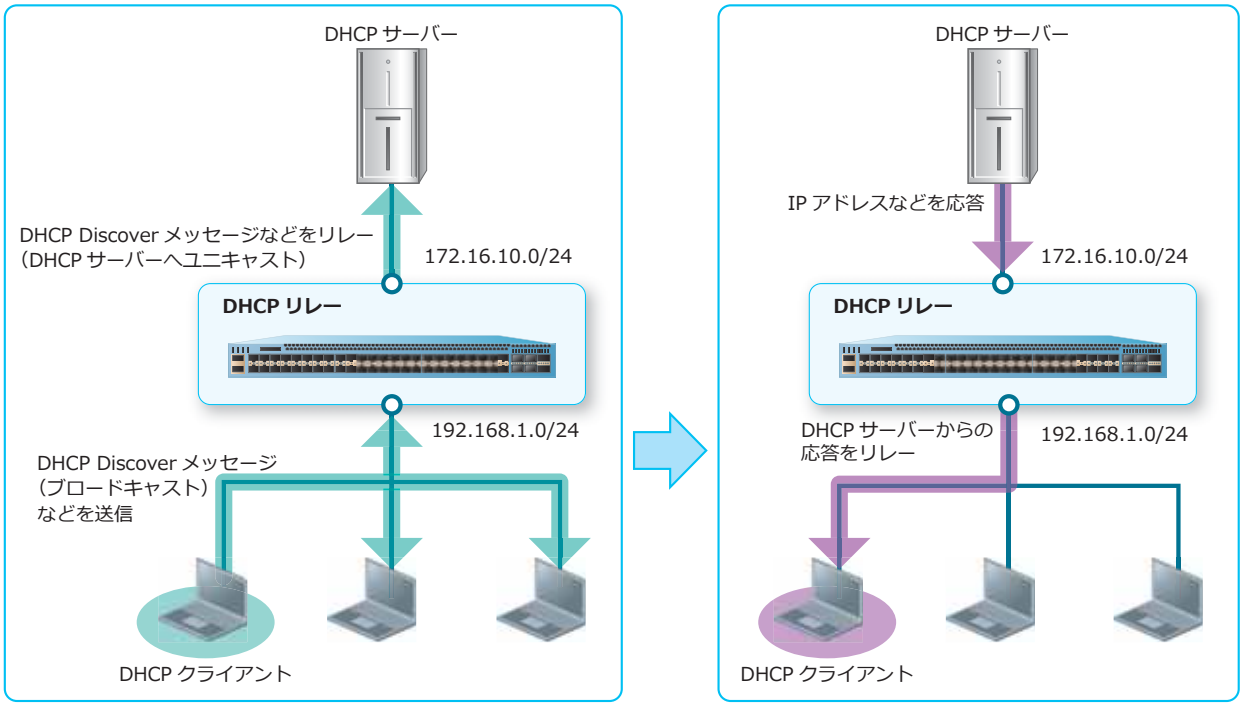
リース時の ping による事前確認で応答がない場合、対象の IP アドレスは DHCP 競合エントリーとして登録されます。登録されている DHCP 競合エントリーを削除するには、**clear ip dhcp conflict** コマンドを使用します。

17.2 DHCP リレーの機能説明

DHCP リレーは、クライアントとサーバーが異なるセグメントに存在する場合に、クライアントとサーバー間の DHCP メッセージをリレーする機能です。DHCP リレーを使用するには、必要な情報を設定してから **service dhcp** コマンドで有効にします。

> ***CAUTION:*** 送信元サブネットにセカンダリー IP アドレスのサブネットを指定しても、DHCP リレーは動作しません。

図 17-3 DHCP リレーの概要



DHCP リレーを使用するには、**ip dhcp pool** コマンドで DHCP リレープールを作成し、「DHCP リレー対象の送信元サブネット（**relay source** コマンド）」「リレー先 DHCP サーバーの IP アドレス（**relay destination** コマンド）」を設定します。

> ***NOTE:*** DHCP リレーのための DHCP リレープールは最大 16 個設定できます。1 つの DHCP リレープールにつき、「リレー対象の送信元サブネット」は最大 4 個、「リレー先 DHCP サーバーの IP アドレス」は最大 4 個設定できます。

> ***NOTE:*** 1 つの DHCP リレープールに設定可能な「リレー対象の送信元サブネット」は、NP7000 の 1.10.01 以降、NP5000 の 1.09.01 以降では最大 16 個に拡張されています。また、NP3000 の 1.10.01 以降では最大 12 個に拡張されています。

> ***NOTE:*** DHCP プール（動的割り当てのための DHCP アドレスプール、手動バインディングエントリーのための DHCP アドレスプール、DHCP リレーのための DHCP リレープール）は、装置全体で合わせて最大 96 個まで設定できます。

また、DHCP クラスを利用すると、分類した DHCP クラスごとにリレー先 IP アドレスを指定できます。DHCP リレーにおいて、分類した DHCP クラスごとにリレー先の IP アドレスを指定するには、**relay target** コマンドを使用します。

DHCP リレーでは、以下のオプション機能にも対応しています。詳細については、『コマンドリファレンス』を参照してください。

- DHCP クライアントユニキャストパケットの取り扱いに関する設定
- Relay Agent Information（Option 82）の挿入、およびポリシーの設定

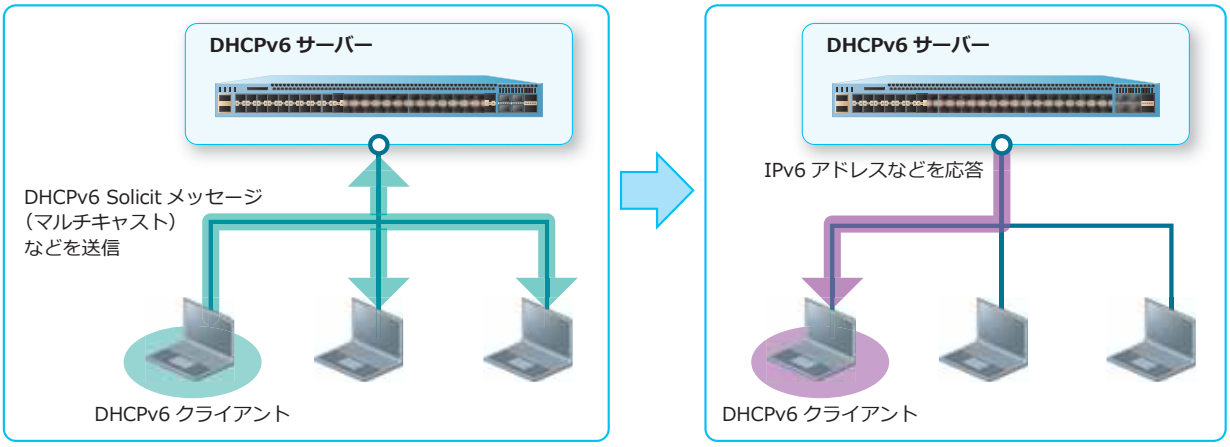
17.3 DHCPv6 サーバーの機能説明

DHCPv6 サーバーは、クライアントに割り当てる IPv6 アドレスなどの情報を自動的に発行する機能です。IPv6 アドレスのリースだけでなく、DHCPv6-PD によるプレフィックス委譲も可能です。DHCPv6 サーバーを使用するには、必要な情報を設定してから **ipv6 dhcp server** コマンドおよび **service ipv6 dhcp** コマンドで有効にします。

> ***CAUTION:*** DHCPv6 サーバーが有効な状態では、設定の変更内容が反映されません。変更内容を反映するには、**no service ipv6 dhcp** コマンドを使用して DHCP サーバーを一度無効にした後、再度 DHCPv6 サーバーを有効にしてください。

> ***NOTE:*** 1 つの VLAN インターフェースで有効にできる DHCPv6 プレフィックスプールは 1 個です。

図 17-4 DHCPv6 サーバーの概要



17.3.1 DHCPv6 プレフィックスプール

クライアントに割り当てる DHCPv6 アドレスなどの情報は、DHCPv6 プレフィックスプールを作成してその中で設定します。プレフィックスごとに 1 つの DHCPv6 プレフィックスプールを作成し、DHCPv6 プレフィックスプールごとに DHCPv6 クライアントに提供する情報を設定できます。DHCPv6 プレフィックスプールは、**ipv6 dhcp pool** コマンドで作成します。

> ***NOTE:*** DHCPv6 プレフィックスプールは、IPv6 アドレスを割り当てるための DHCPv6 プレフィックスプールと、プレフィックス委譲のための DHCPv6 プレフィックスプールを、装置全体で合わせて最大 16 個まで設定できます。

DHCPv6 プレフィックスプールごとに設定できる情報は以下のとおりです。() 内は使用するコマンドです。

- プレフィックスと有効期間、推奨期間（**address prefix**）
- 手動バインディングエントリー（**address-assignment**）
- ドメイン名（**domain-name**）
- DNS サーバー（**dns-server**）

DHCPv6 手動バインディングエントリー

DHCPv6 手動バインディングエントリーは、特定の DUID（DHCP Unique Identifier）からの要求に対して、リースする IPv6 アドレスを固定できます。DHCPv6 手動バインディングエントリーを設定するには、DHCPv6 プレフィックスプールで **address-assignment** コマンドを使用します。

NOTE: 手動割り当てのエントリーは、DHCPv6 手動バインディングエントリーと手動プレフィックス委譲エントリーを、装置全体で合わせて最大 64 個まで設定できます。

リース除外範囲の指定（ipv6 dhcp excluded-address）

`ipv6 dhcp excluded-address` コマンドを使用すると、リースする IPv6 アドレスから除外する範囲を設定できます。

NOTE: リース除外範囲の設定は、1 つの DHCPv6 プレフィックスプールにつき最大 4 個設定でき、装置全体で最大 64 個まで設定できます。

NOTE: 自装置に設定した IPv6 アドレス、または DHCPv6 手動バインディングエントリーとして設定済みの IPv6 アドレスは、リース対象から自動的に除外されます。

17.3.2 DHCPv6-PD によるプレフィックス委譲

DHCPv6 サーバーでは、単一の IPv6 アドレスのリースだけでなく、プレフィックスを委譲することもできます。プレフィックスを委譲するには、まず **`ipv6 local pool`** コマンドでローカル IPv6 プレフィックスプールを作成し、委譲するプレフィックス情報を設定します。次に、DHCPv6 プレフィックスプールで **`prefix-delegation pool`** コマンドを使用して、プレフィックス委譲に使用するローカル IPv6 プレフィックスプールを設定します。

NOTE: DHCPv6 プレフィックスプールは、IPv6 アドレスを割り当てるための DHCPv6 プレフィックスプールと、プレフィックス委譲のための DHCPv6 プレフィックスプールを、装置全体であわせて最大 16 個まで設定できます。

NOTE: ローカル IPv6 プレフィックスプールは最大 16 個設定できます。また、1 つの DHCPv6 プレフィックスプールあたり、1 個のローカル IPv6 プレフィックスプールを設定できます。

手動プレフィックス委譲エントリー

手動プレフィックス委譲エントリーは、特定の DUID（DHCP Unique Identifier）からの要求に対して、リースするプレフィックスを固定できます。手動プレフィックス委譲エントリーを設定するには、DHCPv6 プレフィックスプールで **`prefix-delegation`** コマンドを使用します。

NOTE: 手動割り当てのエントリーは、DHCPv6 手動バインディングエントリーと手動プレフィックス委譲エントリーを、装置全体で合わせて最大 64 個まで設定できます。

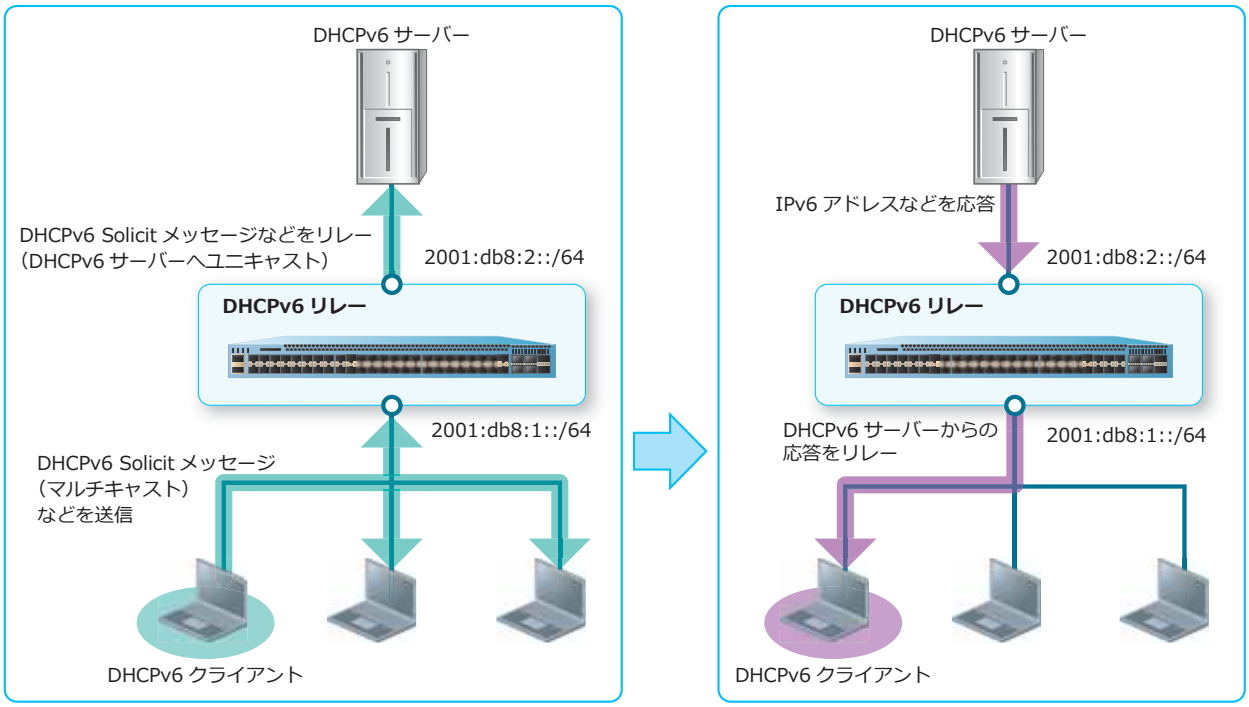
17.3.3 DHCPv6 バインディングエントリーの手動削除

DHCPv6 サーバーからリースされた IPv6 アドレスまたはプレフィックスは、DHCPv6 サーバーのバインディングエントリーとして登録されます。登録されているバインディングエントリーを削除するには、**`clear ipv6 dhcp binding`** コマンドを使用します。

17.4 DHCPv6 リレーの機能説明

DHCPv6 リレーは、クライアントとサーバーが異なるセグメントに存在する場合に、クライアントとサーバー間の DHCPv6 メッセージをリレーする機能です。DHCPv6 リレーを使用するには、**`ipv6 dhcp relay destination`** コマンドおよび **`service ipv6 dhcp`** コマンドで有効にします。

図 17-5 DHCPv6 リレーの概要



DHCPv6 リレーでは、以下のオプション機能にも対応しています。詳細については、『コマンドリファレンス』を参照してください。

- Interface-Id オプション（Option 18）の挿入、およびポリシーの設定
- Relay Agent Remote-ID（Option 37）の挿入、およびポリシーの設定

17.5 DHCP Auto Configuration の機能説明

DHCP Auto Configuration を有効化すると、装置起動時に VLAN 1 インターフェースは自動的に DHCP クライアントになります。装置は、DHCP サーバーから IP アドレスを取得する際に、TFTP サーバーの IP アドレスと構成情報ファイル名も取得します。取得した TFTP サーバーの IP アドレスと構成情報ファイル名を基に、装置は TFTP サーバーから構成情報をダウンロードし、その構成情報で装置を起動できます。

構成情報ファイル名は、DHCP メッセージに DHCP オプション 67（Bootfile name）が付与されている場合は、その値が適用されます。DHCP オプション 67 が付与されていない場合は、file フィールドの値が適用されます。file フィールドにも値が入っていない場合は、DHCP Auto Configuration プロセスは中断されます。

TFTP サーバーの IP アドレスは、「DHCP オプション 150（TFTP Server Address）の IP アドレス（複数可、最大 3 個）」「siaddr フィールドの IP アドレス」の順番で、構成情報ファイルのダウンロードが成功するまで順次適用されます。いずれも失敗した場合は、DHCP Auto Configuration プロセスは中断されます。

構成情報ファイルを正常に取得できず、DHCP Auto Configuration プロセスが中断された場合は、startup-config として指定されていた構成情報が適用されます。

DHCP Auto Configuration を有効化するには、**`autoconfig enable`** コマンドを使用します。

> ***NOTE:*** 構成情報を保存し、装置を再起動するまでは、DHCP Auto Configuration は有効になりません。

17.6 DHCP の状態確認

DHCP の状態を表示して確認する方法を説明します。

17.6.1 DHCP サーバーのバインディングエントリーの表示

show ip dhcp binding コマンドで、DHCP サーバーのバインディングエントリーを確認できます。

表示例を以下に示します。

```
# show ip dhcp binding

 VRF Name: vrf10 ...(1)
 (2)             (3)               (4)                   (5)
 IP address          Client-ID/    Lease expiration      Type
                 Hardware address
 --------------- ----------------- -------------------- ---------
 192.0.2.103     010000005DFD3A    Oct 05 2019 11:16 AM Automatic
 192.0.2.104     010000005DFD39    Oct 05 2019 11:16 AM Automatic
 192.0.2.65      00-00-5E-00-53-00 Infinite             Manual
```

各項目の説明は、以下のとおりです。

表 17-1 show ip dhcp binding コマンドの表示項目

項番	説明
(1)	VRF インスタンス名を表示します。NP7000、NP5000、および NP3000 で表示されます。
(2)	DHCP クライアントに割り当てた IP アドレスを表示します。
(3)	DHCP クライアント ID または MAC アドレスを表示します。
(4)	リース満了日時を表示します。
(5)	IP アドレスの割り当て方法（Automatic：自動／ Manual：固定）を表示します。

17.6.2 DHCP サーバーの競合エントリーの表示

show ip dhcp conflict コマンドで、DHCP 競合エントリーを確認できます。

表示例を以下に示します。

```
# show ip dhcp conflict
 (1)             (2)             (3)                  (4)
 IP address      Detected Method Detection time       VRF
 --------------- --------------- -------------------- ------------
 192.0.2.101     Ping            Oct 04 2019 11:16 AM vrf10
 192.0.2.102     Ping            Oct 04 2019 11:16 AM vrf10
```

各項目の説明は、以下のとおりです。

表 17-2 `show ip dhcp conflict` コマンドの表示項目

項番	説明
(1)	DHCP 競合エントリーに記録された IP アドレスを表示します。
(2)	競合の検出方法を表示します。 • Gratuitous ARP：DHCP クライアントが送信する DHCP Decline メッセージで検出した場合 • Ping：DHCP サーバーが送信する ping による事前確認で検出した場合
(3)	競合の検出日時を表示します。
(4)	VRF インスタンス名を表示します。NP7000、NP5000、および NP3000 で表示されます。

17.6.3 DHCP アドレスプールの表示

`show ip dhcp pool` コマンドで、DHCP アドレスプールの設定を確認できます。

> ***NOTE:*** 本コマンドでは DHCP リレープールも表示されますが、リレー対象の送信元サブネットやリレー先 DHCP サーバーの IP アドレスは表示されません。DHCP リレープールの設定を確認する場合は、**`show running-config function DHCP-RELAY`** コマンドなどで構成情報を直接確認してください。

表示例を以下に示します。

```
# show ip dhcp pool

 Pool name: server-vrf10 ...(1)
   VRF name: vrf10 ...(2)
   Network: 192.0.2.0/24 ...(3)
   Boot file: ...(4)
   Default router: 192.0.2.254 ...(5)
   DNS server: 192.168.0.11 ...(6)
   NetBIOS server: ...(7)
   Domain name: ...(8)
   Lease: 1 days 0 hours 0 minutes 0 seconds ...(9)
   NetBIOS node type: ...(10)
   Next server: 0.0.0.0 ...(11)
   Class c1 ...(12)
     address-range 192.0.2.101 192.0.2.130 ...(13)
   Remaining unallocated address number: 252 ...(14)
   Number of leased addresses: 2 ...(15)
```

各項目の説明は、以下のとおりです。

表 17-3 `show ip dhcp pool` コマンドの表示項目

項番	説明
(1)	DHCP アドレスプール名を表示します。
(2)	VRF インスタンス名を表示します。NP7000、NP5000、および NP3000 で表示されます。
(3)	サブネットを表示します。
(4)	ブートイメージファイルのパスを表示します。
(5)	デフォルトゲートウェイの IP アドレスを表示します。

項番	説明
(6)	DNS サーバーの IP アドレスを表示します。
(7)	WINS サーバーの IP アドレスを表示します。
(8)	ドメイン名を表示します。
(9)	IP アドレスのリース期間を表示します。
(10)	NetBIOS ノードタイプを表示します。
(11)	ブートイメージファイルを取得するためのブートサーバーの IP アドレスを表示します。
(12)	関連付けられた DHCP クラスを表示します。
(13)	DHCP クラスに関連付ける IP アドレスの範囲を表示します。
(14)	リースされていない IP アドレスの個数を表示します。
(15)	リースされた IP アドレスの個数を表示します。

17.6.4 DHCP サーバーの設定の表示

show ip dhcp server コマンドで、DHCP サーバーの設定を確認できます。

表示例を以下に示します。

```
# show ip dhcp server

 DHCP Service: Disabled ...(1)
 Ping packets number: 3 ...(2)
 Ping timeout: 500 ms ...(3)
 Excluded Addresses ...(4)
  10.1.1.1 - 10.1.1.255

 List of DHCP server configured address pool ...(5)
  pool1  pool10  pool11  pool12
  pool2  pool3  pool4  pool5
  pool6  pool7  pool8  pool9
```

各項目の説明は、以下のとおりです。

表 17-4 show ip dhcp server コマンドの表示項目

項番	説明
(1)	DHCP サーバーまたは DHCP リレーの有効 (Enabled) ／無効 (Disabled) を表示します。
(2)	ping による事前確認の送信回数を表示します。
(3)	ping による事前確認の応答タイムアウト時間を表示します。
(4)	除外 IP アドレスの範囲を表示します。
(5)	DHCP プール（動的割り当てのための DHCP アドレスプール、手動バインディングエントリーのための DHCP アドレスプール、DHCP リレーのための DHCP リレープール）を表示します。

17.6.5 DHCP サーバーの統計情報の表示

show ip dhcp server statistics コマンドで、DHCP サーバーの統計情報を確認できます。

表示例を以下に示します。

```
# show ip dhcp server statistics

Address pools               3 ...(1)
Automatic bindings          100 ...(2)
Manual binding              2 ...(3)
Malformed messages          0 ...(4)
Renew messages              0 ...(5)

Message                     Received ...(6)
BOOTREQUEST                 12
DHCPDISCOVER                200
DHCPREQUEST                 178
DHCPDECLINE                 0
DHCPRELEASE                 0
DHCPINFORM                  0

Message                     Sent ...(7)
BOOTREPLY                   12
DHCPOFFER                   190
DHCPACK                     172
DHCPNAK                     6
```

各項目の説明は、以下のとおりです。

表 17-5 show ip dhcp server statistics コマンドの表示項目

項番	説明
(1)	DHCP プール（動的割り当てのための DHCP アドレスプール、手動バインディングエントリーのための DHCP アドレスプール、DHCP リレーのための DHCP リレープール）の個数を表示します。
(2)	動的に割り当てられた IP アドレスの個数を表示します。
(3)	手動バインディングエントリーの個数を表示します。
(4)	DHCP サーバーが受信した不正な DHCP メッセージの個数を表示します。
(5)	リースされた IP アドレスを更新する DHCP メッセージの個数を表示します。
(6)	受信した DHCP メッセージの個数を、DHCP メッセージの種類ごとに表示します。
(7)	送信した DHCP メッセージの個数を、DHCP メッセージの種類ごとに表示します。

17.6.6 DHCP リレーのオプション機能の表示

DHCP リレーのオプション機能の設定を確認する方法を説明します。

Relay Agent Information 付き DHCP パケットの信頼設定の表示

show ip dhcp relay information trusted-sources コマンドで、Relay Agent Information（Option 82）が付与されたクライアントからの DHCP パケットを信頼するインターフェースを確認できます。

表示例を以下に示します。

```
# show ip dhcp relay information trusted-sources

List of trusted sources of relay agent information option:
vlan100     vlan200     vlan300     vlan400     vlan500     vlan600
vlan700     vlan800

Total Entries: 8
```

すべてのインターフェースが信頼するインターフェースの場合は、以下のように表示されます。

```
# show ip dhcp relay information trusted-sources

All interfaces are trusted source of relay agent information option
```

Relay Agent Information の挿入設定の表示

show ip dhcp relay information option-insert コマンドで、クライアントからの DHCP パケットをリレーする際の、Relay Agent Information（Option 82）の挿入設定を確認できます。

表示例を以下に示します。

```
# show ip dhcp relay information option-insert

(1)            (2)
Interface      Option-Insert
-------------- ----------
vlan1          Enabled
vlan2          Disabled
vlan3          Not Configured

Total Entries: 3
```

各項目の説明は、以下のとおりです。

表 17-6 show ip dhcp relay information option-insert コマンドの表示項目

項番	説明
(1)	インターフェース名を表示します。
(2)	Relay Agent Information（Option 82）の挿入設定を表示します。 • Enabled：有効 • Disabled：無効 • Not Configured：未設定

Relay Agent Information 付き DHCP パケットの処理ポリシーの表示

show ip dhcp relay information policy-action コマンドで、すでに Relay Agent Information（Option 82）が付与されたクライアントからの DHCP パケットを受信した場合の、リレー時の処理ポリシーを確認できます。

表示例を以下に示します。

```
# show ip dhcp relay information policy-action
(1)           (2)
Interface     Policy
------------- ---------
vlan1         Keep
vlan2         Drop
vlan3         Replace
vlan4         Not Configured

Total Entries: 4
```

各項目の説明は、以下のとおりです。

表 17-7 show ip dhcp relay information policy-action コマンドの表示項目

項番	説明
(1)	インターフェース名を表示します。
(2)	すでに Relay Agent Information（Option 82）が付与された DHCP パケットを受信した場合の、リレー時の処理ポリシーを表示します。 • Drop：対象の DHCP パケットを破棄 • Keep：対象の DHCP パケットをそのままリレー処理 • Replace：Relay Agent Information（Option 82）を置き換えてリレー処理 • Not configured：未設定

17.6.7 DHCPv6 の DUID の表示

show ipv6 dhcp コマンドで、自装置の DUID（DHCP Unique Identifier）を確認できます。

表示例を以下に示します。

```
# show ipv6 dhcp

This device's DUID is 00030006000205040608 ...(1)
```

各項目の説明は、以下のとおりです。

表 17-8 show ipv6 dhcp コマンドの表示項目

項番	説明
(1)	DUID（DHCP Unique Identifier）を表示します。

17.6.8 インターフェースの DHCPv6 関連の設定の表示

show ipv6 dhcp interface コマンドで、インターフェースの DHCPv6 関連の設定を確認できます。

DHCPv6 サーバーとして動作している場合

VLAN 1 インターフェースが DHCPv6 サーバーとして動作している場合の表示例を以下に示します。

```
# show ipv6 dhcp interface vlan1

vlan1 is in server mode ...(1)
  IPv6 DHCP pool is pool1 ...(2)
  Preference value: 0 ...(3)
  Hint from client: ignored ...(4)
  Rapid-Commit is disabled ...(5)
```

各項目の説明は、以下のとおりです。

表 17-9 show ipv6 dhcp interface コマンドの表示項目（DHCPv6 サーバーの場合）

項番	説明
(1)	インターフェースの DHCPv6 関連の設定を表示します。 <IF-NAME> is not in DHCPv6 mode：DHCPv6 関連の設定が未設定 <IF-NAME> is in server mode：DHCPv6 サーバーモード
(2)	DHCPv6 プレフィックスプール名を表示します。
(3)	アドバタイズメントメッセージ内のプリファレンス（優先度）を表示します。
(4)	DHCP SOLICIT メッセージ内のクライアントからのヒントの扱い（allowed：利用する／ ignored：無視する）を表示します。
(5)	DHCPv6 の Rapid Commit オプションの有効 (enabled) ／無効 (disabled) を表示します。

DHCPv6 リレーとして動作している場合

VLAN 1 インターフェースが DHCPv6 リレーとして動作している場合の表示例を以下に示します。

```
# show ipv6 dhcp interface vlan1

vlan1 is in relay mode ...(1)
    Relay destinations: ...(2)
      fe80::20a:bbff:fecc:102 via vlan2
```

各項目の説明は、以下のとおりです。

表 17-10 show ipv6 dhcp interface コマンドの表示項目（DHCPv6 リレーの場合）

項番	説明
(1)	インターフェースの DHCPv6 関連の設定を表示します。 <IF-NAME> is not in DHCPv6 mode：DHCPv6 関連の設定が未設定 <IF-NAME> is in relay mode：DHCPv6 リレーモード
(2)	DHCPv6 リレーのリレー先 IPv6 アドレスを表示します。

DHCPv6 クライアントとして動作している場合

VLAN 1 インターフェースが DHCPv6 クライアントとして動作し、DHCPv6-PD でプレフィックス委譲された場合の表示例を以下に示します。

```
# show ipv6 dhcp interface

vlan1 is in client mode ...(1)
  State is OPEN
  List of known servers:
    Reachable via address: fe80::240:66ff:feac:31e9 ...(2)
    Configuration parameters:
        IA PD: IA ID 2, T1 302400, T2 483840 ...(3)
          Prefix: fd00:10:10:10:10::/96 ...(4)
                (5)                       (6)
               preferred lifetime 604800, valid lifetime 2592000
  Prefix name: test-001 ...(7)
  Rapid-Commit: disabled ...(8)
```

また、VLAN 1 インターフェースが DHCPv6 クライアントとして動作し、DHCPv6 で IPv6 アドレスを割り当てられた場合の表示例を以下に示します。

```
# show ipv6 dhcp interface

vlan1 is in client mode ...(1)
  State is OPEN
  List of known servers:
    Reachable via address: fe80::240:66ff:feac:31e9 ...(2)
    Configuration parameters:
        IA NA: IA ID 2, T1 302400, T2 483840 ...(9)
          Address: fd00:192:168:10::1001/64 ...(10)
                   (5)                          (6)
                  preferred lifetime 604800, valid lifetime 2592000
  Rapid-Commit: disabled ...(8)
```

各項目の説明は、以下のとおりです。

表 17-11 `show ipv6 dhcp interface` コマンドの表示項目（DHCPv6 クライアントの場合）

項番	説明
(1)	インターフェースの DHCPv6 関連の設定を表示します。 <IF-NAME> is not in DHCPv6 mode：DHCPv6 関連の設定が未設定 <IF-NAME> is in client mode：DHCPv6 クライアントモード
(2)	DHCPv6 サーバーのリンクローカルアドレスを表示します。
(3)	DHCPv6-PD で委譲された IPv6 アドレスプレフィックスの情報を表示します。
(4)	IPv6 アドレスプレフィックスを表示します。
(5)	IPv6 アドレスプレフィックスまたは IPv6 アドレスの推奨期間を表示します。
(6)	IPv6 アドレスプレフィックスまたは IPv6 アドレスの有効期間を表示します。
(7)	IPv6 アドレスプレフィックス名を表示します。
(8)	DHCPv6 の Rapid Commit オプションの有効 (enabled) ／無効 (disabled) を表示します。
(9)	割り当てられた IPv6 アドレスの情報を表示します。

項番	説明
(10)	IPv6 アドレスを表示します。

17.6.9 DHCPv6 サーバーのバインディングエントリーの表示

show ipv6 dhcp binding コマンドで、DHCPv6 サーバーのバインディングエントリーを確認できます。

表示例を以下に示します。

```
# show ipv6 dhcp binding

Client DUID : 00030006004066ac2c90 ...(1)
                address: 2001:db8:200::100 ...(2)
                         (3)                          (4)
                         preferred lifetime 604800 ,valid lifetime 2592000

Client DUID : 00030006004066ac31e9
                prefix: 2001:db8:aaaa::/64 ...(5)
                         preferred lifetime 604800 ,valid lifetime 2592000


Total Entries: 2
```

各項目の説明は、以下のとおりです。

表 17-12 show ipv6 dhcp binding コマンドの表示項目

項番	説明
(1)	DHCPv6 クライアントの DUID（DHCP Unique Identifier）を表示します。
(2)	リースした IPv6 アドレスを表示します。
(3)	IPv6 アドレスまたはプレフィックスの推奨期間を表示します。
(4)	IPv6 アドレスまたはプレフィックスの有効期間を表示します。
(5)	委譲したプレフィックスを表示します。

17.6.10 DHCPv6 プレフィックスプールの表示

show ipv6 dhcp pool コマンドで、DHCPv6 プレフィックスプールの設定を確認できます。

IPv6 アドレス割り当て用の場合

IPv6 アドレスを割り当てるための DHCPv6 プレフィックスプールの場合の表示例を以下に示します。

```
# show ipv6 dhcp pool

DHCPv6 pool: address-pool ...(1)
        Static bindings:
           Binding for client 00030006004066aaaaaa ...(2)
           IA NA: IA ID not specified ...(3)
              Address: 2001:db8:200::aaaa ...(4)
              (5)                          (6)
               preferred lifetime 604800, valid lifetime 2592000
           Binding for client 00030006004066bbbbbb
           IA NA: IA ID not specified
              Address: 2001:db8:200::bbbb
               preferred lifetime 604800, valid lifetime 2592000
        Address prefix: 2001:db8:200::/64 ...(7)
              (8)                         (9)
              preferred lifetime 604800, valid lifetime 2592000
        DNS server: 1:db8:3000:3000::42 ...(10)
        Domain name: v6domain ...(11)
        Active clients: 0 ...(12)
```

各項目の説明は、以下のとおりです。

表 17-13 show ipv6 dhcp pool コマンドの表示項目（IPv6 アドレス割り当て用）

項番	説明
(1)	DHCPv6 プレフィックスプール名を表示します。
(2)	DHCPv6 手動バインディングエントリーの DUID（DHCP Unique Identifier）を表示します。
(3)	DHCPv6 手動バインディングエントリーの IAID（Identity Association Identifier）を表示します。
(4)	DHCPv6 手動バインディングエントリーに割り当てる IPv6 アドレスを表示します。
(5)	DHCPv6 手動バインディングエントリーの推奨期間を表示します。
(6)	DHCPv6 手動バインディングエントリーの有効期間を表示します。
(7)	DHCPv6 クライアントに IPv6 アドレスを割り当てるプレフィックスを表示します。
(8)	IPv6 アドレスの推奨期間を表示します。
(9)	IPv6 アドレスの有効期間を表示します。
(10)	DNS サーバーの IPv6 アドレスを表示します。
(11)	ドメイン名を表示します。
(12)	アクティブな DHCPv6 クライアントの個数を表示します。

プレフィックス委譲用の場合

プレフィックス委譲のための DHCPv6 プレフィックスプールの場合の表示例を以下に示します。

```
# show ipv6 dhcp pool

DHCPv6 pool: pd-pool ...(1)
        Static bindings:
           Binding for client 00030006004066aabbcc ...(2)
           IA PD: IA ID not specified ...(3)
              Prefix: 2001:db8:aaaa:ff11::/64 ...(4)
                (5)                          (6)
                preferred lifetime 604800, valid lifetime 2592000
           Binding for client 00030006004066ddeeff
           IA PD: IA ID 0x1001
              Prefix: 2001:db8:aaaa:ff22::/64
                preferred lifetime 604800, valid lifetime 2592000
        Prefix delegation pool: pd01 ...(7)
              (8)                          (9)
              preferred lifetime 604800, valid lifetime 2592000
        DNS server:
        Domain name:
        Active clients: 0
```

各項目の説明は、以下のとおりです。

表 17-14 `show ipv6 dhcp pool` コマンドの表示項目（プレフィックス委譲用）

項番	説明
(1)	DHCPv6 プレフィックスプール名を表示します。
(2)	手動プレフィックス委譲エントリーの DUID（DHCP Unique Identifier）を表示します。
(3)	手動プレフィックス委譲エントリーの IAID（Identity Association Identifier）を表示します。
(4)	手動プレフィックス委譲エントリーに割り当てるプレフィックスを表示します。
(5)	手動プレフィックス委譲エントリーの推奨期間を表示します。
(6)	手動プレフィックス委譲エントリーの有効期間を表示します。
(7)	プレフィックス委譲で使用するローカル IPv6 プレフィックスプールを表示します。
(8)	委譲するプレフィックスの推奨期間を表示します。
(9)	委譲するプレフィックスの有効期間を表示します。

17.6.11 DHCPv6 サーバーの除外 IPv6 アドレスの表示

show ipv6 excluded-address コマンドで、リースする範囲から除外する IPv6 アドレスを確認できます。

表示例を以下に示します。

```
# show ipv6 excluded-address

 IPv6 excluded address: ...(1)
        1.      2001:db8:200::1 - 2001:db8:200::ff
        2.      2001:db8:200::abcd:1 - 2001:db8:200::abcd:ffff

 Total Entries: 2
```

各項目の説明は、以下のとおりです。

表 17-15 show ipv6 excluded-address コマンドの表示項目

項番	説明
(1)	リースする範囲から除外する IPv6 アドレスを表示します。

17.6.12 ローカル IPv6 プレフィックスプールの表示

show ipv6 local pool コマンドで、ローカル IPv6 プレフィックスプールの情報を確認できます。

表示例を以下に示します。

```
# show ipv6 local pool
(1)          (2)                                        (3)    (4)
Pool         Prefix                                     Free   In use
------------ ------------------------------------------ ------ ------
pd01         2001:db8:aaaa::/48                         65535  1
pd02         2001:db8:1234:5678::/64                    256    0
------------ ------------------------------------------ ------ ------
Total Entries: 2
```

各項目の説明は、以下のとおりです。

表 17-16 show ipv6 local pool コマンドの表示項目

項番	説明
(1)	ローカル IPv6 プレフィックスプール名を表示します。
(2)	委譲元のプレフィックスを表示します。
(3)	指定したプレフィックス長で分割した、委譲可能なプレフィックスの残り数を表示します。
(4)	委譲したプレフィックス数を表示します。

17.6.13 DHCPv6 サーバーの設定の表示

show ipv6 dhcp operation コマンドで、DHCPv6 サーバーの設定を確認できます。

表示例を以下に示します。

```
# show ipv6 dhcp operation

DHCPv6 pool: address-pool ...(1)
        Address prefix: 2001:db8:200::/64 ...(2)
        Static bindings:
           Binding for client 00030006004066aaaaaa ...(3)
            IA NA: IA ID not specified ...(4)
              Address: 2001:db8:200::aaaa ...(5)
               (6)                        (7)
               preferred lifetime 604800, valid lifetime 2592000
           Binding for client 00030006004066bbbbbb
            IA NA: IA ID not specified
              Address: 2001:db8:200::bbbb
               preferred lifetime 604800, valid lifetime 2592000
        IPv6 excluded address: 2001:db8:200::1 - 2001:db8:200::ff ...(8)
                               2001:db8:200::abcd:1 - 2001:db8:200::abcd:ffff
        (9)                         (10)
        preferred lifetime 604800, valid lifetime 2592000
        DNS server: 1:db8:3000:3000::42 ...(11)
        Domain name: v6domain ...(12)

DHCPv6 pool: pd-pool
        Prefix delegation pool: pd01, prefix is 2001:db8:aaaa::/48 64 ...(13)
        Static bindings:
           Binding for client 00030006004066aabbcc ...(14)
             IA PD: IA ID not specified ...(15)
             Prefix: 2001:db8:aaaa:ff11::/64 ...(16)
             (17)                        (18)
             preferred lifetime 604800, valid lifetime 2592000
           Binding for client 00030006004066ddeeff
             IA PD: IA ID 0x1001
             Prefix: 2001:db8:aaaa:ff22::/64
             preferred lifetime 604800, valid lifetime 2592000
        (19)                        (20)
        preferred lifetime 604800, valid lifetime 2592000
        DNS server:
        Domain name:
```

各項目の説明は、以下のとおりです。

表 17-17 show ipv6 dhcp operation コマンドの表示項目

項番	説明
(1)	DHCPv6 プレフィックスプール名を表示します。
(2)	DHCPv6 クライアントに IPv6 アドレスを割り当てるプレフィックスを表示します。
(3)	DHCPv6 手動バインディングエントリーの DUID（DHCP Unique Identifier）を表示します。
(4)	DHCPv6 手動バインディングエントリーの IAID（Identity Association Identifier）を表示します。
(5)	DHCPv6 手動バインディングエントリーに割り当てる IPv6 アドレスを表示します。
(6)	DHCPv6 手動バインディングエントリーの推奨期間を表示します。
(7)	DHCPv6 手動バインディングエントリーの有効期間を表示します。

項番	説明
(8)	リースする範囲から除外する IPv6 アドレスを表示します。
(9)	IPv6 アドレスの推奨期間を表示します。
(10)	IPv6 アドレスの有効期間を表示します。
(11)	DNS サーバーの IPv6 アドレスを表示します。
(12)	ドメイン名を表示します。
(13)	プレフィックス委譲で使用するローカル IPv6 プレフィックスプールの情報を表示します。
(14)	手動プレフィックス委譲エントリーの DUID（DHCP Unique Identifier）を表示します。
(15)	手動プレフィックス委譲エントリーの IAID（Identity Association Identifier）を表示します。
(16)	手動プレフィックス委譲エントリーに割り当てるプレフィックスを表示します。
(17)	手動プレフィックス委譲エントリーの推奨期間を表示します。
(18)	手動プレフィックス委譲エントリーの有効期間を表示します。
(19)	委譲するプレフィックスの推奨期間を表示します。
(20)	委譲するプレフィックスの有効期間を表示します。

17.6.14 DHCPv6 リレーのオプション機能の表示

show ipv6 dhcp relay information option コマンドで、DHCPv6 リレーのオプション機能の設定を確認できます。

表示例を以下に示します。

```
# show ipv6 dhcp relay information option

IPv6 DHCP relay remote-id
  Policy : keep ...(1)
IPv6 DHCP relay interface-id
  Policy : keep ...(2)
```

各項目の説明は、以下のとおりです。

表 17-18 show ipv6 dhcp relay information option コマンドの表示項目

項番	説明
(1)	すでに Relay Agent Remote-ID（Option 37）が付与されたクライアントからの DHCPv6 パケットを受信した場合の、リレー時の処理ポリシーを表示します。 • drop：対象の DHCPv6 パケットを破棄 • keep：対象の DHCPv6 パケットをそのままリレー処理
(2)	すでに Interface-Id オプション（Option 18）が付与されたクライアントからの DHCPv6 パケットを受信した場合の、リレー時の処理ポリシーを表示します。 • drop：対象の DHCPv6 パケットを破棄 • keep：対象の DHCPv6 パケットをそのままリレー処理

17.6.15 DHCP Auto Configuration の設定の表示

show autoconfig コマンドで、DHCP Auto Configuration の設定を確認できます。

表示例を以下に示します。

```
# show autoconfig

Autoconfig State: Disabled ...(1)
```

各項目の説明は、以下のとおりです。

表 17-19 show autoconfig コマンドの表示項目

項番	説明
(1)	DHCP Auto Configuration の有効 (Enabled) ／無効 (Disabled) を表示します。

17.7 DHCP の構成例と設定例

DHCP を利用する場合の構成例と設定例を示します。

17.7.1 DHCP サーバーの設定

DHCP サーバーの構成例と設定例を示します。この例では以下のように 2 個の DHCP アドレスプールを設定しています。

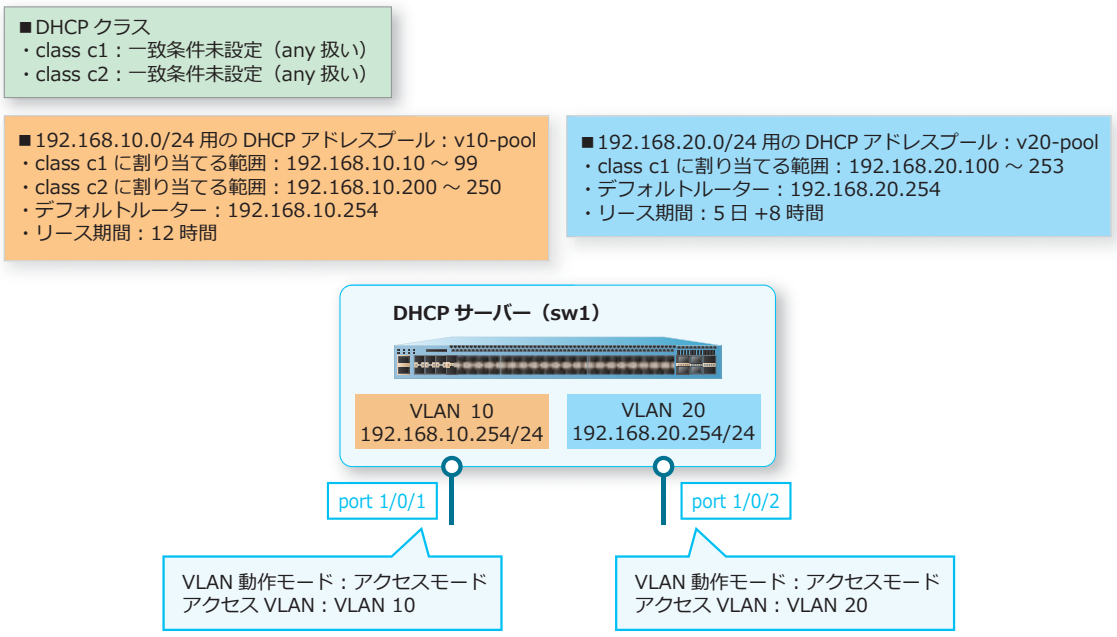
192.168.10.0/24 用の DHCP アドレスプール［v10-pool］を以下の条件で設定します。

- リースするアドレス範囲は［192.168.10.10 ～ 192.168.10.99］［192.168.10.200 ～ 192.168.10.250］
- デフォルトルーターは［192.168.10.254］
- リース期間は 12 時間

192.168.20.0/24 用の DHCP アドレスプール［v20-pool］を以下の条件で設定します。

- リースするアドレス範囲は［192.168.20.100 ～ 192.168.20.253］
- デフォルトルーターは［192.168.20.254］
- リース期間は 5 日 +8 時間

図 17-6 DHCP サーバーの構成例



1. VLAN 10、VLAN 20 を作成します。

```
sw1# configure terminal
sw1(config)# vlan 10,20
sw1(config-vlan)# exit
sw1(config)#
```

2. ポート 1/0/1 をアクセスポートとして設定し、アクセスポートに［VLAN 10］を割り当てます。また、ポート 1/0/2 をアクセスポートとして設定し、アクセスポートに［VLAN 20］を割り当てます。

```
sw1(config)# interface port 1/0/1
sw1(config-if-port)# switchport mode access
sw1(config-if-port)# switchport access vlan 10
sw1(config-if-port)# exit
sw1(config)# interface port 1/0/2
sw1(config-if-port)# switchport mode access
sw1(config-if-port)# switchport access vlan 20
sw1(config-if-port)# exit
sw1(config)#
```

3. VLAN 10 の IP アドレスを［192.168.10.254/24］に、VLAN 20 の IP アドレスを［192.168.20.254/24］に設定します。

```
sw1(config)# interface vlan 10
sw1(config-if-vlan)# ip address 192.168.10.254/24
sw1(config-if-vlan)# exit
sw1(config)# interface vlan 20
sw1(config-if-vlan)# ip address 192.168.20.254/24
sw1(config-if-vlan)# exit
sw1(config)#
```

4. DHCP クラス［c1］と［c2］を、一致条件未設定で作成します。

```
sw1(config)# ip dhcp class c1
sw1(config-dhcp-class)# exit
sw1(config)# ip dhcp class c2
sw1(config-dhcp-class)# exit
sw1(config)#
```

5. DHCP クラスの利用設定を有効化します。

```
sw1(config)# ip dhcp use class
sw1(config)#
```

6. DHCP アドレスプール［v10-pool］を作成し、ネットワークアドレスとサブネットを［192.168.10.0/24］に、デフォルトルーターを［192.168.10.254］に、リース期間を［12 時間］に設定します。

```
sw1(config)# ip dhcp pool v10-pool
sw1(config-dhcp-pool)# network 192.168.10.0/24
sw1(config-dhcp-pool)# default-router 192.168.10.254
sw1(config-dhcp-pool)# lease 0 12 0 0
sw1(config-dhcp-pool)#
```

7. DHCP アドレスプール［v10-pool］において、DHCP クラス［c1］を使用してリースするアドレス範囲［192.168.10.10 ～ 192.168.10.99］を割り当てます。また、DHCP クラス［c2］を使用してリースするアドレス範囲［192.168.10.200 ～ 192.168.10.250］を割り当てます。

```
sw1(config-dhcp-pool)# class c1
sw1(config-dhcp-pool-class)# address range 192.168.10.10 192.168.10.99
sw1(config-dhcp-pool-class)# exit
sw1(config-dhcp-pool)# class c2
sw1(config-dhcp-pool-class)# address range 192.168.10.200 192.168.10.250
sw1(config-dhcp-pool-class)# exit
sw1(config-dhcp-pool)# exit
sw1(config)#
```

8. DHCP アドレスプール［v20-pool］を作成し、ネットワークアドレスとサブネットを［192.168.20.0/24］に、デフォルトルーターを［192.168.20.254］に、リース期間を［5 日 +8 時間］に設定します。

```
sw1(config)# ip dhcp pool v20-pool
sw1(config-dhcp-pool)# network 192.168.20.0/24
sw1(config-dhcp-pool)# default-router 192.168.20.254
sw1(config-dhcp-pool)# lease 5 8 0 0
sw1(config-dhcp-pool)#
```

9. DHCP アドレスプール［v20-pool］において、DHCP クラス［c1］を使用してリースするアドレス範囲［192.168.20.100 ～ 192.168.20.253］を割り当てます。

```
sw1(config-dhcp-pool)# class c1
sw1(config-dhcp-pool-class)# address range 192.168.20.100 192.168.20.253
sw1(config-dhcp-pool-class)# exit
sw1(config-dhcp-pool)# exit
sw1(config)#
```

10. DHCP サーバーを有効にします。

```
sw1(config)# service dhcp
sw1(config)# end
sw1#
```

11. 実施後の「DHCP サーバーの設定」を確認します。

```
sw1# show ip dhcp server

 DHCP Service: Enabled
 Ping packets number: 2
 Ping timeout: 500 ms

 List of DHCP server configured address pool
  v10-pool  v20-pool
```

12. 実施後の DHCP アドレスプール［v10-pool］を確認します。

```
sw1# show ip dhcp pool v10-pool

 Pool name: v10-pool
   VRF name:
   Network: 192.168.10.0/24
   Boot file:
   Default router: 192.168.10.254
   DNS server:
   NetBIOS server:
   Domain name:
   Lease: 0 days 12 hours 0 minutes 0 seconds
   NetBIOS node type:
   Next server: 0.0.0.0
   Class c1
     address-range 192.168.10.10 192.168.10.99
   Class c2
     address-range 192.168.10.200 192.168.10.250
   Remaining unallocated address number: 254
   Number of leased addresses: 0
```

13.実施後の DHCP アドレスプール［v20-pool］を確認します。

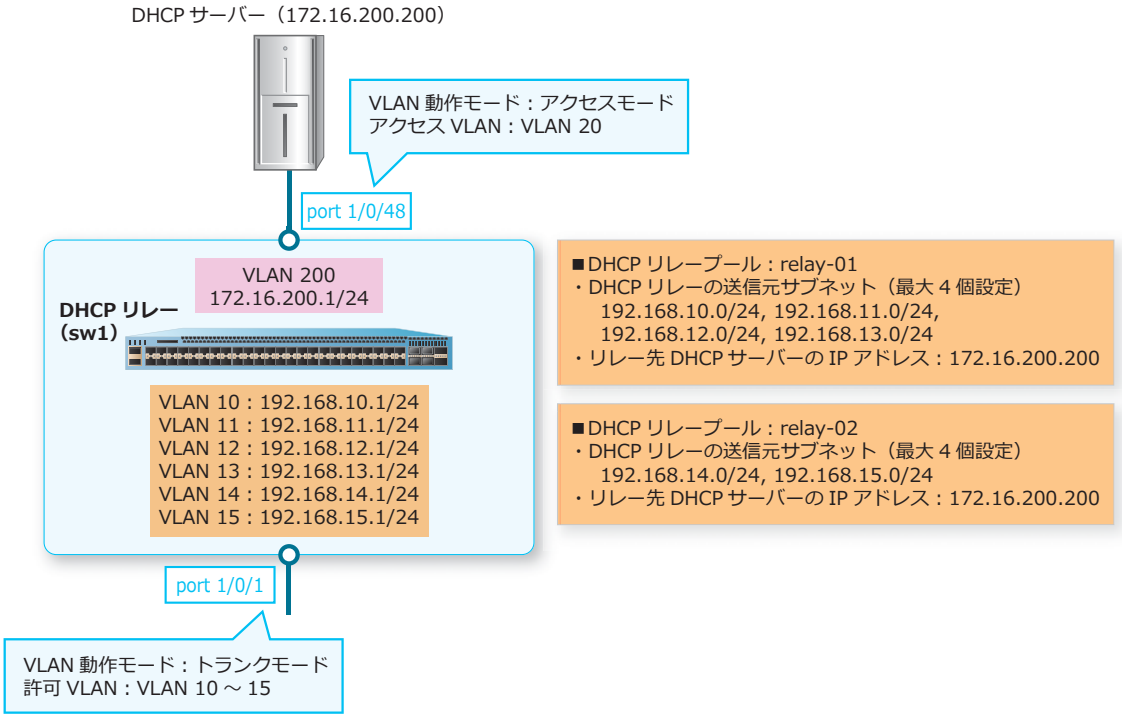
```
sw1# show ip dhcp pool v20-pool

 Pool name: v20-pool
   VRF name:
   Network: 192.168.20.0/24
   Boot file:
   Default router: 192.168.20.254
   DNS server:
   NetBIOS server:
   Domain name:
   Lease: 5 days 8 hours 0 minutes 0 seconds
   NetBIOS node type:
   Next server: 0.0.0.0
   Class c1
     address-range 192.168.20.100 192.168.20.253
   Remaining unallocated address number: 254
   Number of leased addresses: 0
```

17.7.2 DHCP リレーの設定

DHCP リレーの構成例と設定例を示します。この例では以下のように DHCP リレーを設定するために、2 個の DHCP リレープールを設定しています。

- DHCP リレーの送信元サブネット：192.168.10.0/24, 192.168.11.0/24, 192.168.12.0/24, 192.168.13.0/24, 192.168.14.0/24, 192.168.15.0/24
- リレー先 DHCP サーバーの IP アドレス：172.16.200.200

図 17-7 DHCP リレーの構成例



1. VLAN 10 ～ VLAN 15、VLAN 200 を作成します。

```
sw1# configure terminal
sw1(config)# vlan 10-15,200
sw1(config-vlan)# exit
sw1(config)#
```

2. ポート 1/0/1 をトランクポートとして設定し、トランクポートに［VLAN 10 ～ VLAN 15］を割り当てます。また、ポート 1/0/48 をアクセスポートとして設定し、アクセスポートに［VLAN 200］を割り当てます。

```
sw1(config)# interface port 1/0/1
sw1(config-if-port)# switchport mode trunk
sw1(config-if-port)# switchport trunk allowed vlan 10-15
sw1(config-if-port)# exit
sw1(config)# interface port 1/0/48
sw1(config-if-port)# switchport mode access
sw1(config-if-port)# switchport access vlan 200
sw1(config-if-port)# exit
sw1(config)#
```

3. 各 VLAN インターフェースの IP アドレスを、構成例のように設定します。

```
sw1(config)# interface vlan 10
sw1(config-if-vlan)# ip address 192.168.10.1/24
sw1(config-if-vlan)# exit
sw1(config)# interface vlan 11
sw1(config-if-vlan)# ip address 192.168.11.1/24
sw1(config-if-vlan)# exit
sw1(config)# interface vlan 12
sw1(config-if-vlan)# ip address 192.168.12.1/24
sw1(config-if-vlan)# exit
sw1(config)# interface vlan 13
sw1(config-if-vlan)# ip address 192.168.13.1/24
sw1(config-if-vlan)# exit
sw1(config)# interface vlan 14
sw1(config-if-vlan)# ip address 192.168.14.1/24
sw1(config-if-vlan)# exit
sw1(config)# interface vlan 15
sw1(config-if-vlan)# ip address 192.168.15.1/24
sw1(config-if-vlan)# exit
sw1(config)# interface vlan 200
sw1(config-if-vlan)# ip address 172.16.200.1/24
sw1(config-if-vlan)# exit
sw1(config)#
```

4. DHCP リレープール［relay-01］を作成し、DHCP リレーの送信元サブネットを［192.168.10.0/24］［192.168.11.0/24］［192.168.12.0/24］［192.168.13.0/24］に、リレー先 DHCP サーバーの IP アドレスを［172.16.200.200］に設定します。

```
sw1(config)# ip dhcp pool relay-01
sw1(config-dhcp-pool)# relay source 192.168.10.0/24
sw1(config-dhcp-pool)# relay source 192.168.11.0/24
sw1(config-dhcp-pool)# relay source 192.168.12.0/24
sw1(config-dhcp-pool)# relay source 192.168.13.0/24
sw1(config-dhcp-pool)# relay destination 172.16.200.200
sw1(config-dhcp-pool)# exit
sw1(config)#
```

5. DHCP リレープール［relay-02］を作成し、DHCP リレーの送信元サブネットを［192.168.14.0/24］［192.168.15.0/24］に、リレー先 DHCP サーバーの IP アドレスを［172.16.200.200］に設定します。

```
sw1(config)# ip dhcp pool relay-02
sw1(config-dhcp-pool)# relay source 192.168.14.0/24
sw1(config-dhcp-pool)# relay source 192.168.15.0/24
sw1(config-dhcp-pool)# relay destination 172.16.200.200
sw1(config-dhcp-pool)# exit
sw1(config)#
```

6. DHCP リレーを有効にします。

```
sw1(config)# service dhcp
sw1(config)# end
sw1#
```

7. 実施後の DHCP リレーの設定を、構成情報で確認します。

```
sw1# show running-config function DHCP-RELAY
Building configuration...

Current configuration : 320 bytes


# DHCP-RELAY

ip dhcp pool relay-01
 relay source 192.168.10.0/24
 relay source 192.168.11.0/24
 relay source 192.168.12.0/24
 relay source 192.168.13.0/24
 relay destination 172.16.200.200
ip dhcp pool relay-02
 relay source 192.168.14.0/24
 relay source 192.168.15.0/24
 relay destination 172.16.200.200

sw1# show running-config function DHCP-SERVER
Building configuration...

Current configuration : 79 bytes


# DHCP-SERVER

ip dhcp pool relay-01
ip dhcp pool relay-02
service dhcp

sw1#
```

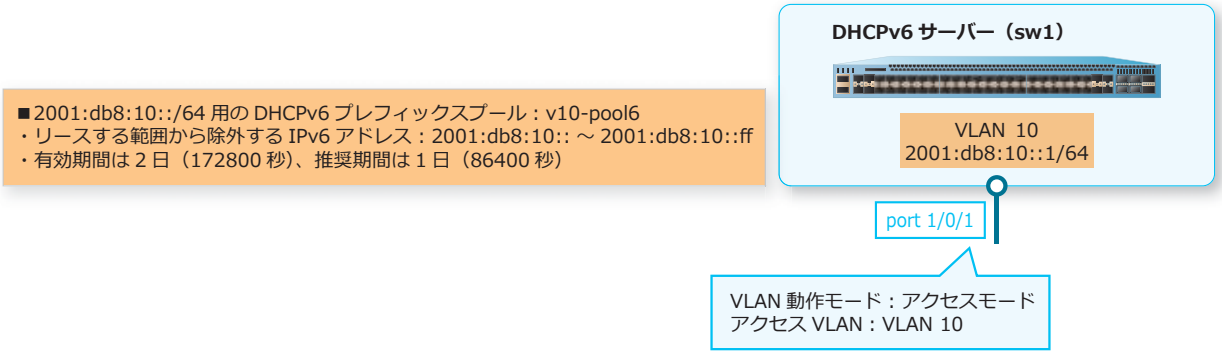
17.7.3 DHCPv6 サーバーの設定

DHCPv6 サーバーの構成例と設定例を示します。

2001:db8:10::/64 用の DHCPv6 プレフィックスプール［v10-pool6］を以下の条件で設定します。

- リースするアドレス範囲は［2001:db8:10::/64］から［2001:db8:10:: ～ 2001:db8:10::ff］を除外した範囲
- 有効期間は 2 日（172800 秒）、推奨期間は 1 日（86400 秒）

図 17-8 DHCPv6 サーバーの構成例



1. VLAN 10 を作成します。

```
sw1# configure terminal
sw1(config)# vlan 10
sw1(config-vlan)# exit
sw1(config)#
```

2. ポート 1/0/1 をアクセスポートとして設定し、アクセスポートに［VLAN 10］を割り当てます。

```
sw1(config)# interface port 1/0/1
sw1(config-if-port)# switchport mode access
sw1(config-if-port)# switchport access vlan 10
sw1(config-if-port)# exit
sw1(config)#
```

3. VLAN 10 の IPv6 アドレスを［2001:db8:10::1/64］に設定します。

```
sw1(config)# interface vlan 10
sw1(config-if-vlan)# ipv6 address 2001:db8:10::1/64
sw1(config-if-vlan)# exit
sw1(config)#
```

4. DHCPv6 プレフィックスプール［v10-pool6］を作成し、プレフィックスを［2001:db8:10::/64］に、有効期間を［2 日（172800 秒）］に、推奨期間を［1 日（86400 秒）］に設定します。

```
sw1(config)# ipv6 dhcp pool v10-pool6
sw1(config-dhcp)# address prefix 2001:db8:10::/64 lifetime 172800 86400
sw1(config-dhcp)# exit
sw1(config)#
```

5. リースする範囲から除外する IPv6 アドレスを［2001:db8:10:: ～ 2001:db8:10::ff］に設定します。

```
sw1(config)# ipv6 dhcp excluded-address 2001:db8:10:: 2001:db8:10::ff
sw1(config)#
```

6. VLAN 10 インターフェースで使用する DHCPv6 プレフィックスプールとして［v10-pool6］を指定し、DHCPv6 サーバーを有効にします。

```
sw1(config)# interface vlan 10
sw1(config-if-vlan)# ipv6 dhcp server v10-pool6
sw1(config-if-vlan)# exit
sw1(config)# service ipv6 dhcp
sw1(config)# end
sw1#
```

7. 実施後の「DHCPv6 サーバーの設定」を確認します。

```
sw1# show ipv6 dhcp operation

DHCPv6 pool: v10-pool6
        Address prefix: 2001:db8:10::/64
        IPv6 excluded address: 2001:db8:10::1 - 2001:db8:10::ff
        preferred lifetime 86400, valid lifetime 172800
        DNS server:
        Domain name:
```

8. 実施後の DHCPv6 プレフィックスプール［v10-pool6］を確認します。

```
sw1# show ipv6 dhcp pool

DHCPv6 pool: v10-pool6
        Address prefix: 2001:db8:10::/64
              preferred lifetime 86400, valid lifetime 172800
        DNS server:
        Domain name:
        Active clients: 0
```

17.7.4 DHCPv6 サーバーでプレフィックス委譲を使用する場合

DHCPv6 サーバーでプレフィックス委譲を使用する場合の構成例と設定例を示します。

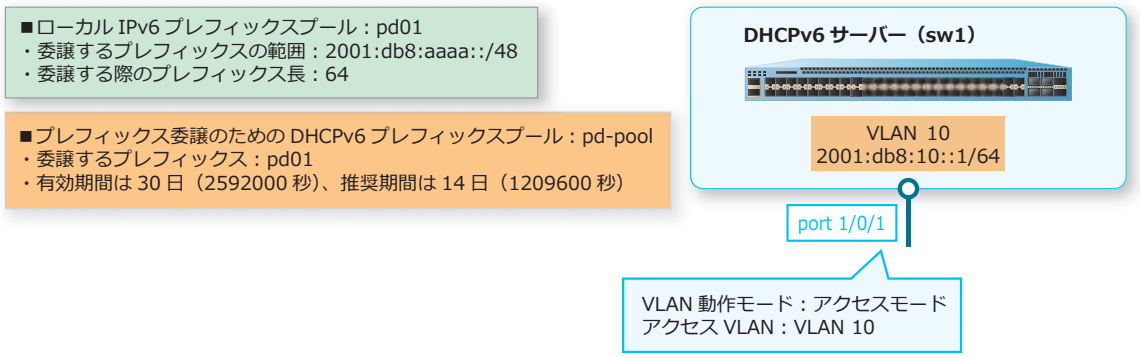
ローカル IPv6 プレフィックスプール［pd01］を以下の条件で設定します。

- 委譲するプレフィックスの範囲：2001:db8:aaaa::/48
- 委譲する際のプレフィックス長：64

プレフィックス委譲のための DHCPv6 プレフィックスプール［pd-pool］を以下の条件で設定します。

- 委譲するプレフィックス：pd01
- 有効期間は 30 日（2592000 秒）、推奨期間は 14 日（1209600 秒）

図 17-9 DHCPv6 サーバーでプレフィックス委譲を使用する場合の構成例



1. VLAN 10 を作成します。

```
sw1# configure terminal
sw1(config)# vlan 10
sw1(config-vlan)# exit
sw1(config)#
```

2. ポート 1/0/1 をアクセスポートとして設定し、アクセスポートに［VLAN 10］を割り当てます。

```
sw1(config)# interface port 1/0/1
sw1(config-if-port)# switchport mode access
sw1(config-if-port)# switchport access vlan 10
sw1(config-if-port)# exit
sw1(config)#
```

3. VLAN 10 の IPv6 アドレスを［2001:db8:10::1/64］に設定します。

```
sw1(config)# interface vlan 10
sw1(config-if-vlan)# ipv6 address 2001:db8:10::1/64
sw1(config-if-vlan)# exit
sw1(config)#
```

4. ローカル IPv6 プレフィックスプール［pd01］を作成し、委譲するプレフィックスの範囲を［2001:db8:aaaa::/48］に、委譲する際のプレフィックス長を［64］に設定します。

```
sw1(config)# ipv6 local pool pd01 2001:db8:aaaa::/48 64
sw1(config)#
```

5. DHCPv6 プレフィックスプール［pd-pool］を作成し、委譲するプレフィックスを［pd01］に、有効期間を［30 日（2592000 秒）］に、推奨期間を［14 日（1209600 秒）］に設定します。

```
sw1(config)# ipv6 dhcp pool pd-pool
sw1(config-dhcp)# prefix-delegation pool pd01 lifetime 2592000 1209600
sw1(config-dhcp)# exit
sw1(config)#
```

6. VLAN 10 インターフェースで使用する DHCPv6 プレフィックスプールとして［pd-pool］を指定し、DHCPv6 サーバーを有効にします。

```
sw1(config)# interface vlan 10
sw1(config-if-vlan)# ipv6 dhcp server pd-pool
sw1(config-if-vlan)# exit
sw1(config)# service ipv6 dhcp
sw1(config)# end
sw1#
```

7. 実施後の「DHCPv6 サーバーの設定」を確認します。

```
sw1# show ipv6 dhcp operation

DHCPv6 pool: pd-pool
        Prefix delegation pool: pd01, prefix is 2001:db8:aaaa::/48 64
        preferred lifetime 1209600, valid lifetime 2592000
        DNS server:
        Domain name:
```

8. 実施後の DHCPv6 プレフィックスプール［pd-pool］を確認します。

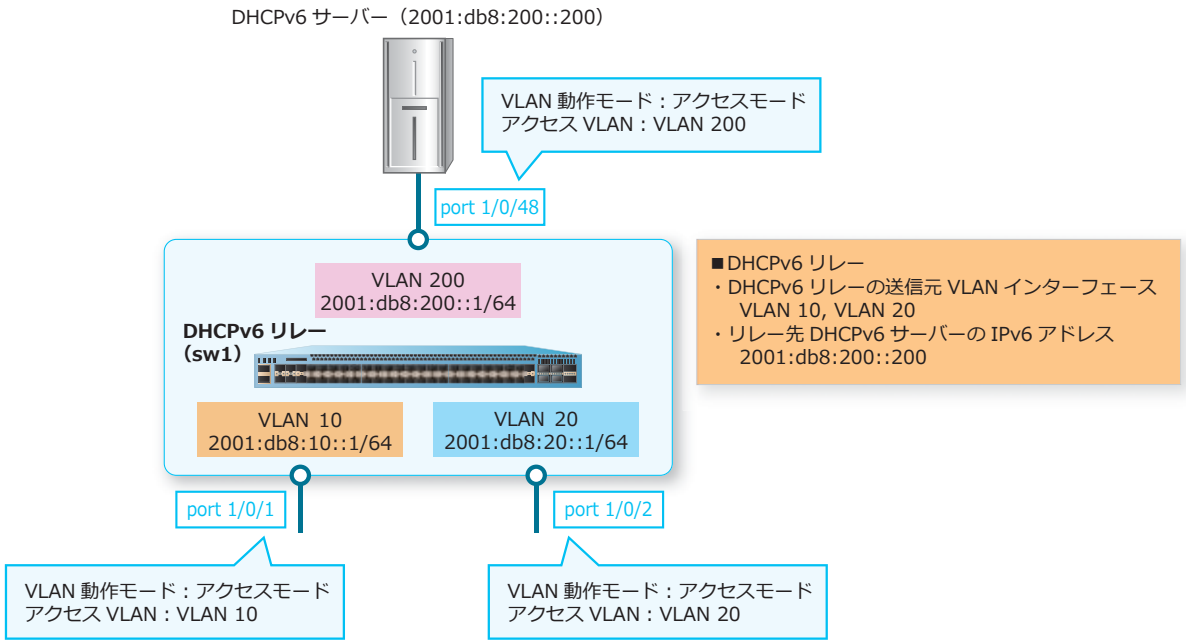
```
sw1# show ipv6 dhcp pool pd-pool

DHCPv6 pool: pd-pool
        Prefix delegation pool: pd01
              preferred lifetime 1209600, valid lifetime 2592000
        DNS server:
        Domain name:
        Active clients: 0
```

17.7.5 DHCPv6 リレーの設定

DHCPv6 リレーの構成例と設定例を示します。

- DHCPv6 リレーの送信元 VLAN インターフェース：VLAN 10、VLAN 20
- リレー先 DHCPv6 サーバーの IPv6 アドレス：2001:db8:200::200

図 17-10 DHCPv6 リレーの構成例



1. VLAN 10、VLAN 20、VLAN 200 を作成します。

```
sw1# configure terminal
sw1(config)# vlan 10,20,200
sw1(config-vlan)# exit
sw1(config)#
```

2. ポート 1/0/1 をアクセスポートとして設定し、アクセスポートに［VLAN 10］を割り当てます。ポート 1/0/2 をアクセスポートとして設定し、アクセスポートに［VLAN 20］を割り当てます。また、ポート 1/0/48 をアクセスポートとして設定し、アクセスポートに［VLAN 200］を割り当てます。

```
sw1(config)# interface port 1/0/1
sw1(config-if-port)# switchport mode access
sw1(config-if-port)# switchport access vlan 10
sw1(config-if-port)# exit
sw1(config)# interface port 1/0/2
sw1(config-if-port)# switchport mode access
sw1(config-if-port)# switchport access vlan 20
sw1(config-if-port)# exit
sw1(config-if-port)# interface port 1/0/48
sw1(config-if-port)# switchport mode access
sw1(config-if-port)# switchport access vlan 200
sw1(config-if-port)# exit
sw1(config)#
```

3. 各 VLAN インターフェースの IPv6 アドレスを、構成例のように設定します。

```
sw1(config)# interface vlan 10
sw1(config-if-vlan)# ipv6 address 2001:db8:10::1/64
sw1(config-if-vlan)# exit
sw1(config)# interface vlan 20
sw1(config-if-vlan)# ipv6 address 2001:db8:20::1/64
sw1(config-if-vlan)# exit
sw1(config)# interface vlan 200
sw1(config-if-vlan)# ipv6 address 2001:db8:200::1/64
sw1(config-if-vlan)# exit
sw1(config)#
```

4. VLAN 10 インターフェースで、リレー先 DHCPv6 サーバーの IPv6 アドレスを［2001:db8:200::200］に設定します。同様に、VLAN 20 インターフェースで、リレー先 DHCPv6 サーバーの IPv6 アドレスを［2001:db8:200::200］に設定します。

```
sw1(config)# interface vlan 10
sw1(config-if-vlan)# ipv6 dhcp relay destination 2001:db8:200::200
sw1(config-if-vlan)# exit
sw1(config)# interface vlan 20
sw1(config-if-vlan)# ipv6 dhcp relay destination 2001:db8:200::200
sw1(config-if-vlan)# exit
sw1(config)#
```

5. DHCPv6 リレーを有効にします。

```
sw1(config)# service ipv6 dhcp
sw1(config)# end
sw1#
```

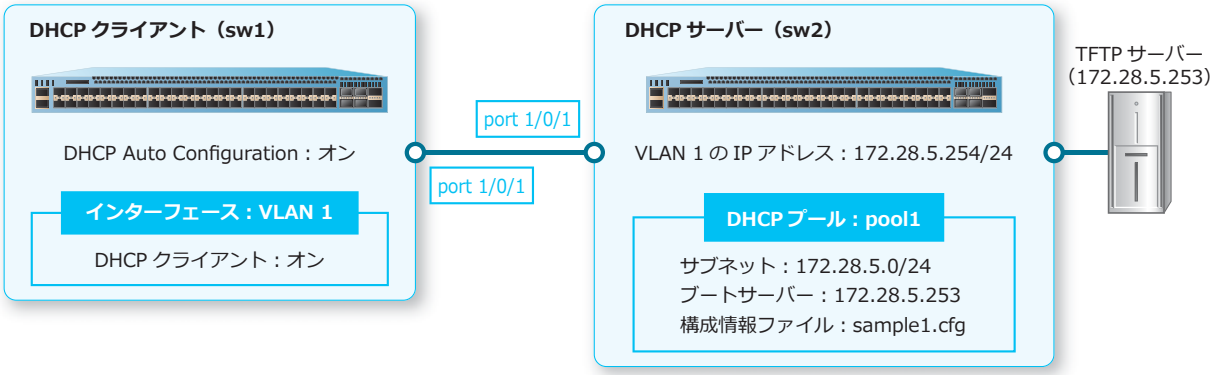
6. 実施後の DHCP リレーの設定を、構成情報で確認します。

```
sw1# show running-config function RELAY6
Building configuration...

Current configuration : 150 bytes


# RELAY6

interface vlan 10
 ipv6 dhcp relay destination 2001:db8:200::200
interface vlan 20
 ipv6 dhcp relay destination 2001:db8:200::200

sw1# show running-config function DHCPV6-SERVER
Building configuration...

Current configuration : 40 bytes


# DHCPV6-SERVER

service ipv6 dhcp

sw1#
```

17.7.6 DHCP Auto Configuration を利用する場合

DHCP Auto Configuration を利用する場合の構成例と設定例を示します。

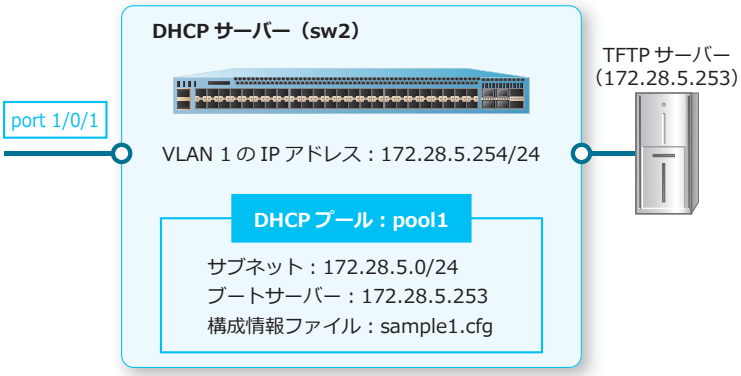
図 17-11 DHCP Auto Configuration を利用する場合の構成例



17.7.6.1 DHCP サーバーの設定例

DHCP サーバーで DHCP Auto Configuration を利用するための設定を行います。

図 17-12 DHCP サーバーの設定例



1. VLAN 1 の IP アドレスを［172.28.5.254/24］に設定します。

```
sw2# configure terminal
sw2(config)# interface vlan 1
sw2(config-if-vlan)# ip address 172.28.5.254/24
sw2(config-if-vlan)# exit
sw2(config)#
```

2. DHCP アドレスプール［pool1］を作成し、サブネットを［172.28.5.0/24］に、ブートサーバーを［172.28.5.253］に、構成情報ファイルを［sample1.cfg］に設定します。

```
sw2(config)# ip dhcp pool pool1
sw2(config-dhcp-pool)# network 172.28.5.0/24
sw2(config-dhcp-pool)# next-server 172.28.5.253
sw2(config-dhcp-pool)# bootfile sample1.cfg
sw2(config-dhcp-pool)# exit
sw2(config)#
```

3. DHCP サーバーサービスを有効化します。

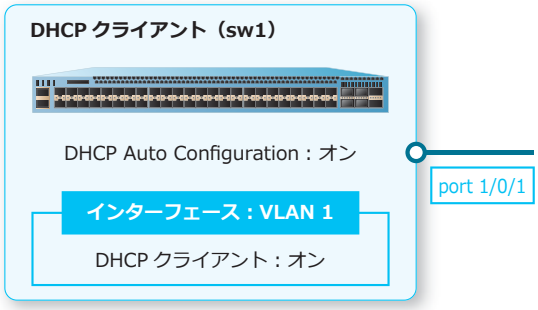
```
sw2(config)# service dhcp
sw2(config)# end
sw2#
```

17.7.6.2 DHCP クライアントの設定例

DHCP クライアントで DHCP Auto Configuration を有効化し、DHCP クライアントを再起動すると、DHCP Auto Configuration が実行されます。

なお、DHCP Auto Configuration 実行時に VLAN 1 インターフェースは自動的に DHCP クライアントになるため、本設定例の手順 1 を実行しなくても、DHCP Auto Configuration は動作します。

図 17-13 DHCP クライアントの設定例



1. インターフェース［VLAN 1］上で、DHCP クライアントを有効化します。

```
sw1# configure terminal
sw1(config)# interface vlan 1
sw1(config-if-vlan)# ip address dhcp
sw1(config-if-vlan)# exit
sw1(config)#
```

2. DHCP Auto Configuration を有効化します。

```
sw1(config)# autoconfig enable
sw1(config)# exit
sw1#
```

3. running-config を startup-config へコピーします。

```
sw1# write memory

Destination filename startup-config? [y/n]:  y

Saving all configurations to NV-RAM.......... Done.

sw1#
```

4. 装置を再起動します。

```
sw1# reboot

Are you sure you want to proceed with the system reboot?(y/n) y
Please wait, the switch is rebooting...
```

18. 管理運用機能

管理運用機能、状態の確認方法、および実施例について説明します。

REF: コマンドの詳細については、『コマンドリファレンス』を参照してください。

18.1 管理運用機能の機能説明

使用できるコマンドをユーザーごとに制限できます。

18.1.1 マネージメントポートへの IP アドレス設定とデフォルトルート設定

マネージメントポートのポート設定モードに遷移するには、**interface mgmt** コマンドを使用します。

NOTE: マネージメントポートのポート設定モードに遷移するには、**interface mgmt** コマンドで 0 を指定する必要があります。

装置のマネージメントポートに管理用の IP アドレスを設定するには、**ip address** コマンドを使用します。マネージメントポートにデフォルトルートを設定する場合には、**ip default-gateway** コマンドを使用します。

NOTE: マネージメントポートに設定したデフォルトルートは、装置のルーティングテーブルには登録されません。

NOTE: マネージメントポートに IPv6 アドレスを設定することはできません。

18.1.2 ユーザーアカウントの作成

ユーザー名、特権レベル、およびパスワードを設定してユーザーアカウントを作成できます。ユーザーアカウントを作成するには、**username** コマンドを使用します。パスワードを設定するには、password パラメーターで指定します。

CAUTION: ユーザー名として「ap_recovery」は使用できません。

18.1.3 コンフィグ上で表示されるパスワードの暗号化

show running-config コマンドなどのコンフィグ情報に表示されるパスワードを暗号化して表示するには、**service user-account encryption** コマンドを使用します。このコマンドで暗号化される情報は、以下のコマンドで設定したパスワード、SNMP コミュニティー名、SNMP グループ名、および共有鍵（Shared Secret）です。

- **username** コマンドのパスワード
- **enable password** コマンドのパスワード
- **password** コマンドのパスワード
- **aaa-local-db user** コマンドのパスワード
- **mac-authentication password** コマンドのパスワード
- **snmp-server community** コマンド、**snmp-server host** コマンドの SNMP コミュニティー名
- **snmp-server user** コマンド、**snmp-server group** コマンドの SNMP グループ名
- **radius-server host** コマンド、**tacacs-server host** コマンドの共有鍵（Shared Secret）

18.1.4 システムログ

システムメッセージをローカルメッセージバッファーにロギングできます。ローカルメッセージバッファーへのロギングを有効にするには、**logging on** コマンドと **logging buffered** コマンドを使用します。

ローカルメッセージバッファーの内容は、**logging buffered** コマンドで指定する周期的書き込み間隔で SRAM に保存されます。なお、NP7000 および NP5000 の 1.04.01 以前、NP4000 の 1.01.02 以前、NP2000 の 1.05.01 以前のバージョンでは、フラッシュメモリーに保存されます。

ローカルメッセージバッファーと SRAM のシステムメッセージを削除するには、**clear logging** コマンドを使用します。

> ***NOTE:*** ローカルメッセージバッファーでのログの最大保存数は約 10,000 件です。また、SRAM でのログの最大保存数は約 3,000 件です。

18.1.5 SYSLOG サーバー

ローカルメッセージバッファーにロギングされたシステムメッセージを、SYSLOG サーバーに送信できます。SYSLOG サーバーを設定するには、**logging server** コマンドを使用します。

> ***NOTE:*** SYSLOG サーバーを使用する場合は、ローカルメッセージバッファーへのロギングを有効にする必要があります。
>
> ***NOTE:*** SYSLOG サーバーホストは 4 個まで設定できます。
>
> ***NOTE:*** SYSLOG サーバーに送信されるログは、起動時に出力するログ「System warm start」以降です。また、SYSLOG サーバーとの通信が可能になった後は、通信が可能になる前に保存されていたログも送信されます。

18.1.6 装置の再起動

装置を再起動するには、**reboot** コマンドを使用します。装置を強制的に再起動するには、**reboot force_agree** コマンドを使用します。

> ***CAUTION:*** **reboot** コマンドの実行時には、設定の保存確認を行いません。設定を保存してから、本コマンドを実行してください。

18.1.7 日時指定の装置の自動再起動

指定した時間に装置を自動的に再起動することができます。

> ***NOTE:*** 装置の自動再起動は、NP7000 の 1.10.02 以降、NP5000 の 1.10.01 以降、NP2100 の 1.12.01 以降でサポートしています。

指定した日時に一度だけ自動再起動を実行する場合は、repeat パラメーターを指定しないで **reboot time** コマンドを使用します。一定期間ごとに自動再起動を繰り返し実行する場合は、「初回の実行日時」と repeat パラメーターで「実行間隔（日単位）」を指定して **reboot time** コマンドを使用します。

18.2 管理運用機能の状態確認

管理運用機能の状態を表示して確認する方法を説明します。

18.2.1 装置の状態の表示

show environment コマンドで、装置のファンや電源の状態などを確認できます。

非スタック装置の場合

非スタック装置のファンや電源の状態などを確認する場合の表示例を以下に示します。

```
# show environment

Detail Temperature Status:
(1)      (2)          (3)
Unit     Status       Current Temperature
-----    ---------    --------------------
1        Normal       28C

Detail Fan Status: ...(4)
-----------------------------------------------------------------
Unit 1:
  Module 1:    Normal
  Module 2:    Normal
  Module 3:    Normal
  Module 4:    Normal

Detail Power Status:
(1)      (5)                (6)              (7)
Unit     Power Module       Power Status     Consumption
-----    ----------------   -------------    -----------
1        PWR-460-ACF        in-operation         85 W
1        Power 2            empty                 0 W

Detail Memory-Error Auto-Recovery Status:
-----------------------------------------------------------------
Auto Recovery Mode          : Enabled ...(8)
Auto Recovery Notification : Enabled ...(9)
Fault Action Configuration : - ...(10)
(1)      (11)         (12)               (13)
Unit     Status       Recovery Count     ECC Uncorrectable Error Count
-----    ---------    ---------------    ------------------------------
1        Normal       0                  0

Health Status:
(1)      (14)         (15)
Unit     Status       Failure Code
-----  ---------      --------------------
1      Abnormal       0x00400
```

各項目の説明は、以下のとおりです。

表 18-1 show environment コマンドの表示項目

項番	説明
(1)	装置のボックス ID を表示します。スタックを構成していない場合は「1」が表示されます。

項番	説明
(2)	装置の温度状態を表示します。 • Normal：装置の温度が正常範囲 • Abnormal：装置の温度が正常範囲外
(3)	現在の温度を表示します。
(4)	ファンユニットの状態を表示します。 • Normal：正常状態 • Failure：異常あり、またはファンユニット未実装状態
(5)	電源ユニットを表示します。
(6)	電源の状態を表示します。 • in-operation：通常動作中 • failed：異常あり • empty：電源ユニット未実装状態
(7)	消費電力量を表示します。 NP7000 の 1.06.01 以降、NP5000 の 1.06.01 以降で表示されます。
(8)	メモリーエラー自動復旧機能の有効 (Enabled) ／無効 (Disabled) を表示します。
(9)	メモリーエラー自動復旧機能に関連する通知（ログ、SNMP トラップ）の有効 (Enabled) ／無効 (Disabled) を表示します。
(10)	SW-LSI メモリーの状態が「異常」になった場合に、すべてのポートをシャットダウンする機能の有効 (Shutdown-all) ／無効 (-) を表示します。
(11)	SW-LSI メモリーの状態を表示します。 • Normal：正常 • Abnormal：メモリーエラー発生状態（メモリーエラー自動復旧機能無効：メモリーエラーの発生を検知、メモリーエラー自動復旧機能有効：メモリーエラーの多発を検知）
(12)	メモリーエラーが検出されたときに、実行された復旧アクションの回数を表示します。
(13)	復旧不能なメモリーエラーが検出された回数を表示します。
(14)	装置の正常性を表示します。 • Normal：正常 • Abnormal：1 つ以上のコンポーネントでエラーを検出

項番	説明
(15)	装置によって検出された障害コードを表示します。 • すべての bit=0（0x00000）：正常状態 • bit[8]=1（0x00100）：電源の障害 • bit[10]=1（0x00400）：ファンの障害 • bit[11]=1（0x00800）：温度異常 • bit[14]=1（0x04000）：SW-LSI のメモリーエラー • bit[15]=1（0x08000）：SW-LSI の復旧不能なメモリーエラー • bit[16]=1（0x10000）：SW-LSI のメモリーエラー（ハードエラー） • bit[17]=1（0x20000）：SW-LSI の復旧不能なメモリーエラー（ハードエラー） ※ メモリーエラー自動復旧機能が無効で、「復旧可能なメモリーエラーを検出した場合」は、bit[14]=1（0x04000）を表示します。 ※ メモリーエラー自動復旧機能が無効で、「復旧不能なメモリーエラーを検出した場合」は、bit[15]=1（0x08000）を表示します。 ※ メモリーエラー自動復旧機能が有効で、「SW-LSI の同じメモリー領域で、メモリーエラーの検出および復旧アクションが 10 回以上動作して、監視対象外になった場合」は、bit[16]=1（0x10000）を表示します。 ※ メモリーエラー自動復旧機能が有効で、「復旧不能なメモリーエラーを検出した場合」は、bit[17]=1（0x20000）を表示します。

スタック構成の場合

スタック構成のファンや電源の状態などを確認する場合の表示例を以下に示します。

```
# show environment

Detail Temperature Status:
(1)      (2)          (3)
Unit     Status       Current Temperature
-----    ---------    --------------------
1        Normal       26C
2        Normal       27C

Detail Fan Status: ...(4)
-----------------------------------------------------------------
Unit 1:
  Module 1:   Normal
  Module 2:   Normal
  Module 3:   Normal
  Module 4:   Normal
Unit 2:
  Module 1:   Normal
  Module 2:   Normal
  Module 3:   Normal
  Module 4:   Failure

Detail Power Status:
(1)      (5)                (6)              (7)
Unit     Power Module       Power Status     Consumption
-----    ----------------   -------------    -----------
1        PWR-460-ACF        in-operation         85 W
1        Power 2            empty                 0 W
2        PWR-460-ACF        in-operation         53 W
2        PWR-460-ACF        in-operation         46 W

Detail Memory-Error Auto-Recovery Status:
-----------------------------------------------------------------
Auto Recovery Mode          : Enabled ...(8)
Auto Recovery Notification : Enabled ...(9)
Fault Action Configuration : - ...(10)
(1)      (11)         (12)                (13)
Unit     Status       Recovery Count      ECC Uncorrectable Error Count
-----    ---------    ---------------     -------------------------------
1        Normal       0                   0
2        Normal       0                   0

Health Status:
(1)      (14)         (15)
Unit     Status       Failure Code
-----    ---------    --------------------
1        Normal       0x00000
2        Abnormal     0x00400
```

各項目の説明は、非スタック装置の場合と同じです。

18.2.2 装置の情報の表示

show unit コマンドで、装置の情報を確認できます。

表示例を以下に示します。

```
# show unit
(1)            (2)
Unit           Model Name
----  -----------------------------
 1     ApresiaNP7000-48X6L
(1)           (3)                              (4)            (5)
Unit          Serial-Number                    Status         Up Time
----  --------------------------------  ---------  -----------------
 1     187552150014                      ok          0DT0H5M20S
(1)         (6)                      (7)                        (8)
Unit        Module Type              Serial-Number              Product Name
----  ----------------------  -------------------------  ------------------
 1     Power Module 1          DZRD1510045143              PWR-460-ACF
 1     Power Module 2          DZRD1510045140              PWR-460-ACF
 1     Fan Module 1            187572150079                FAN-0402-F
 1     Fan Module 2            187572150078                FAN-0402-F
 1     Fan Module 3            187572150073                FAN-0402-F
 1     Fan Module 4            187572150063                FAN-0402-F
(1)    (9)          (10)         (11)         (12)
Unit   Memory       Total        Used         Free
----  --------  -----------  -----------  -----------
 1     DRAM      2097152 K    209084 K   1888068 K
 1     FLASH      523776 K     46004 K    477772 K
```

各項目の説明は、以下のとおりです。

表 18-2 show unit コマンドの表示項目

項番	説明
(1)	装置のボックス ID を表示します。スタックを構成していない場合は「1」が表示されます。
(2)	装置名を表示します。
(3)	シリアル番号を表示します。
(4)	ステータスを表示します。
(5)	連続稼働時間（sysUpTime）を、（日）DT（時）H（分）M（秒）S 形式で表示します。
(6)	モジュールタイプを表示します。
(7)	モジュールのシリアル番号を表示します。
(8)	モジュールのプロダクトコードを表示します。
(9)	メモリー種別を表示します。
(10)	メモリー容量を表示します。
(11)	使用中のメモリー容量を表示します。
(12)	未使用のメモリー容量を表示します。

18.2.3 CPU 使用率の表示

show cpu utilization コマンドで、装置の CPU 使用率を確認できます。

表示例を以下に示します。

```
# show cpu utilization

CPU Utilization
(1)                          (2)                          (3)
Five seconds -  30 %         One minute -  25 %           Five minutes -  24 %
Maximum - 31 %               Minimum - 8 %
(4)                          (5)
```

各項目の説明は、以下のとおりです。

表 18-3 show cpu utilization コマンドの表示項目

項番	説明
(1)	5 秒間の平均の CPU 使用率を表示します。
(2)	1 分間の平均の CPU 使用率を表示します。
(3)	5 分間の平均の CPU 使用率を表示します。
(4)	CPU 使用率の最大値を表示します。
(5)	CPU 使用率の最小値を表示します。

すべてのスタックメンバーの CPU 使用率を表示する場合

スタック構成において、**show cpu utilization unit** コマンドで、すべてのスタックメンバーの CPU 使用率を確認できます。

表示例を以下に示します。

```
# show cpu utilization unit

CPU Utilization
(1)       (2)      (3)      (4)      (5)    (6)
          5 sec    1 min    5 min    Max    Min
-----------------------------------------
Unit 1:     27%      23%      23%    33%    10%
Unit 2:     28%      23%      23%    33%    9%
Unit 3:       -        -        -      -     -
Unit 4:       -        -        -      -     -
```

各項目の説明は、以下のとおりです。

表 18-4 show cpu utilization unit コマンドの表示項目

項番	説明
(1)	ボックス ID を表示します。
(2)	5 秒間の平均の CPU 使用率を表示します。
(3)	1 分間の平均の CPU 使用率を表示します。

項番	説明
(4)	5 分間の平均の CPU 使用率を表示します。
(5)	CPU 使用率の最大値を表示します。
(6)	CPU 使用率の最小値を表示します。

18.2.4 プロセスごとの CPU 使用率の表示

debug show cpu utilization コマンドで、プロセスごとの CPU 使用率を確認できます。

> ***NOTE:*** 本コマンドはトラブルシューティング用のコマンドです。技術サポート担当者が問題の分析を行うために収集をお願いすることがあります。

表示例を以下に示します。

```
# debug show cpu utilization
(1)                          (2)                          (3)
Five seconds -  21 %         One minute -  17 %           Five minutes -  17 %
(4)                   (5)      (6)      (7)
Process Name          5Sec     1Min     5Min
-----------------   ------   ------   ------
OS_UTIL               71 %     67 %     67 %
GBIC_Pooling           8 %      7 %      8 %
FAN_Pooling            2 %      1 %      1 %
bcmCNTR.0              1 %      1 %      1 %
CLI                    0 %      0 %      0 %
ST_PERI                0 %      0 %      0 %
bcmL2X.0               0 %      0 %      0 %
SYS_Ctr                0 %      0 %      0 %
cpuprotect             0 %      0 %      0 %
CNT_TASK               0 %      0 %      0 %
socdmadesc.0           0 %      0 %      0 %
tBulkClnt              0 %      0 %      0 %
bcmRX                  0 %      0 %      0 %
MAUMIB_TASK            0 %      0 %      0 %
NICLinkScan            0 %      0 %      0 %
radius_reader          0 %      0 %      0 %
HISR1                  0 %      0 %      0 %
IP-Msg                 0 %      0 %      0 %
IP6-Tic                0 %      0 %      0 %
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

各項目の説明は、以下のとおりです。

表 18-5 debug show cpu utilization コマンドの表示項目

項番	説明
(1)	5 秒間の平均の CPU 使用率を表示します。
(2)	1 分間の平均の CPU 使用率を表示します。
(3)	5 分間の平均の CPU 使用率を表示します。
(4)	プロセス名を表示します。
(5)	5 秒間の平均の CPU 使用率を表示します。
(6)	1 分間の平均の CPU 使用率を表示します。

項番	説明
(7)	5 分間の平均の CPU 使用率を表示します。

18.2.5 バージョン情報の表示

show version コマンドで、バージョン情報を確認できます。

表示例を以下に示します。

```
# show version

System MAC Address: 00-40-66-A8-CF-10 ...(1)
(2)         (3)                              (4)
Unit ID     Module Name                      Versions
-------  ---------------------------  ---------------------
   1       ApresiaNP7000-48X6L          H/W:A
                                        Bootloader:1.00.00
                                        Runtime:1.00.00
                                        CPLD:01
```

各項目の説明は、以下のとおりです。

表 18-6 show version コマンドの表示項目

項番	説明
(1)	システム MAC アドレスを表示します。 非スタック装置の場合は、自装置の MAC アドレスを表示します。 スタック構成の場合、「そのスタック構成が最初に起動したときのマスター装置の MAC アドレス」を表示します（NP7000 は 1.06.01 以降、NP5000 は 1.05.02 以降、NP4000 は 1.02.01 以降、NP2000 は 1.07.01 以降で対応しています。それより前のバージョンでは、「コマンド実行時点のマスター装置（自装置）の MAC アドレス」を表示します）。
(2)	装置のボックス ID を表示します。スタックを構成していない場合は「1」が表示されます。
(3)	装置名を表示します。
(4)	バージョン情報を表示します。

18.2.6 技術サポート情報の表示

show tech-support コマンドで、技術サポート情報（装置の各種情報）を確認できます。

NOTE: 本コマンドの実行結果は、テクニカルサポートにお問い合わせの際、送付を依頼する場合があります。

NOTE: NP7000 および NP5000 の 1.03.01 より前のバージョン、NP2000 の 1.02.01 より前のバージョンでは、**show tech-support** コマンドではなく、**debug show tech-support** コマンドを使用します。

表示例を以下に示します。

```
# show tech-support

#------------------------------------------------------------------------------
#                 ApresiaNP7000-48X6L TenGigabit Ethernet Switch
#                          Technical Support Information
#
#                            Firmware: Build 1.03.01
#   Copyright(C) 2016  APRESIA Systems, Ltd. All rights reserved.
#------------------------------------------------------------------------------


********************   Basic System Information   ********************

[SYS 2017-5-11 10:02:52]

Boot Time           : 11 May 2017  09:56:42
RTC Time            : 2017/05/11 01:02:52
Boot PROM Version   : Build 1.00.01
Firmware Version    : Build 1.03.01
Hardware Version    : A
Serial number       : 700010000021
MAC Address         : 00-40-66-A8-CF-10
MAC Address Number  : 73

Unit          Model Name
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

18.2.7 エラーログの表示

debug show error-log コマンドで、エラーログを確認できます。

> ***NOTE:*** 本コマンドの実行結果は、テクニカルサポートにお問い合わせの際、送付を依頼する場合があります。

表示例を以下に示します。

```
# debug show error-log
# Persistent memory area

# Error level: DEBUG (2)
# Firmware version: 1.00.01
# Clock: 40280 ms
# Characters lost: 0
# UTC 2016/03/17 04:13:44

====================== SOFTWARE FATAL ERROR =======================
file=./src/proj_led.c,line=2508,Invalid semaphore handle : 00000000

Current TASK : FAN_Pooling
------------------------- TASK STACKTRACE ------------------------
-> 1003694
-> 37001B0
-> 2D584AC
-> 2D57DE8
-> 2D40BE4
-> 2D40A0C
-> 215D638
-> 215D158
-> 214C0A0
-> 214BF84

CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

18.2.8 システムメッセージの表示

show logging コマンドで、ローカルメッセージバッファーにロギングされたシステムメッセージを確認できます。

表示例を以下に示します。

```
# show logging

Total number of buffered messages:6 ...(1)
(2)
#6      2016-03-03 14:49:36 INFO(6) "exit" executed by 15 from Console
#5      2016-03-03 14:49:35 INFO(6) "configure terminal" executed by 15 from Console
#4      2016-03-03 14:49:29 INFO(6) Successful login through Console (Username: 15)
#3      2016-03-03 14:49:27 INFO(6) Logout through Console (Username: 15)
#2      2016-03-03 14:49:27 INFO(6) "logout" executed by 15 from Console
#1      2016-03-03 14:49:22 INFO(6) "clear logging" executed by 15 from Console
```

各項目の説明は、以下のとおりです。

表 18-7 show logging コマンドの表示項目

項番	説明
(1)	システムメッセージ数を表示します。
(2)	オプションパラメーターを指定しないで実行した場合は、最新メッセージから最大 200 個のログが表示されます。

指定したシーケンス番号以降のシステムメッセージを表示する場合

表示を開始するシーケンス番号と「+」指定の表示数を指定すると、指定したシーケンス番号以降の新しいメッセージが、指定した数だけ表示されます。

シーケンス番号 2 以降の新しいメッセージを 4 個確認する場合の表示例を以下に示します。

```
# show logging 2 + 4

Total number of buffered messages:8 ...(1)
(2)
#2      2016-03-03 14:49:27 INFO(6) "logout" executed by 15 from Console
#3      2016-03-03 14:49:27 INFO(6) Logout through Console (Username: 15)
#4      2016-03-03 14:49:29 INFO(6) Successful login through Console (Username: 15)
#5      2016-03-03 14:49:35 INFO(6) "configure terminal" executed by 15 from Console
```

各項目の説明は、以下のとおりです。

表 18-8 show logging 開始番号 + 表示数コマンド表示項目

項番	説明
(1)	システムメッセージ数を表示します。
(2)	表示を開始するシーケンス番号と「+」指定の表示数を指定した場合は、指定したシーケンス番号以降の新しいメッセージが指定した数だけ表示されます。

指定したシーケンス番号以前のシステムメッセージを表示する場合

表示を開始するシーケンス番号と「-」指定の表示数を指定すると、指定したシーケンス番号以前の古いメッセージが、指定した数だけ表示されます。

シーケンス番号 4 以前の古いメッセージを 3 個確認する場合の表示例を以下に示します。

```
# show logging 4 - 3

Total number of buffered messages:9 ...(1)
(2)
#4      2016-03-03 14:49:29 INFO(6) Successful login through Console (Username: 15)
#3      2016-03-03 14:49:27 INFO(6) Logout through Console (Username: 15)
#2      2016-03-03 14:49:27 INFO(6) "logout" executed by 15 from Console
```

各項目の説明は、以下のとおりです。

表 18-9 `show logging` 開始番号 - 表示数コマンドの表示項目

項番	説明
(1)	システムメッセージ数を表示します。
(2)	表示を開始するシーケンス番号と「-」指定の表示数を指定した場合は、指定したシーケンス番号以前の古いメッセージが指定した数だけ表示されます。

18.2.9 SRAM に保存されたシステムメッセージの表示

`show logging sram` コマンドで、SRAM に保存されたシステムメッセージを確認できます。

表示例を以下に示します。

```
# show logging sram

Total number of buffered messages:6 ...(1)
(2)
#6      2016-03-03 14:49:36 INFO(6) "exit" executed by 15 from Console
#5      2016-03-03 14:49:35 INFO(6) "configure terminal" executed by 15 from Console
#4      2016-03-03 14:49:29 INFO(6) Successful login through Console (Username: 15)
#3      2016-03-03 14:49:27 INFO(6) Logout through Console (Username: 15)
#2      2016-03-03 14:49:27 INFO(6) "logout" executed by 15 from Console
#1      2016-03-03 14:49:22 INFO(6) "clear logging" executed by 15 from Console
```

各項目の説明は、以下のとおりです。

表 18-10 `show logging sram` コマンドの表示項目

項番	説明
(1)	システムメッセージ数を表示します。
(2)	システムメッセージを新しい順に表示します。

18.2.10 ラインセッション情報の表示

show users コマンドで、ラインセッション情報を確認できます。また、**clear line** コマンドで、指定したラインセッションを手動で切断できます。

表示例を以下に示します。

```
# show users
(1)   (2)       (3)             (4)       (5)                (6)
ID    Type      User-Name       Privilege Login-Time         IP address
-------------------------------------------------------------------------------
0       console Anonymous       1         16H9M36S
1     * telnet  example         1         11M48S             192.0.2.100
10      SSH     test            15        4M54S              10.250.21.112

Total Entries: 3
```

各項目の説明は、以下のとおりです。

表 18-11 show users コマンドの表示項目

項番	説明
(1)	ラインセッション ID を表示します。
(2)	ラインセッションのタイプを表示します。自セッションの場合はアスタリスク (*) が表示されます。 • console：コンソール経由のログイン • telnet：Telnet 経由のログイン • SSH：SSH 経由のログイン
(3)	ユーザー名を表示します。
(4)	特権レベルを表示します。
(5)	ログインしてからの経過時間を表示します。
(6)	クライアントの IP アドレスを表示します。

18.2.11 装置の自動再起動設定の表示

show reboot コマンドで自動再起動設定を確認できます。

> ***NOTE:*** 本コマンドは、NP7000 の 1.10.02 以降、NP5000 の 1.10.01 以降、NP2100 の 1.12.01 以降でサポートしています。

repeat パラメーターを使用しない場合の表示例を以下に示します。

```
# show reboot

    Reboot Time            : Enabled ...(1)
    Previous Reboot Time   : N/A
    Next Reboot Time       : N/A
    First-day              : 02:00 2023-12-01 ...(2)
    Repeat Interval-days   : N/A
```

各項目の説明は、以下のとおりです。

表 18-12 `show reboot` コマンドの表示項目

項番	説明
(1)	自動再起動の有効 (Enabled) ／無効 (Disabled) を表示します。
(2)	自動再起動を実行する日時を表示します。

repeat パラメーターを使用する場合の表示例を以下に示します。

```
# show reboot

    Reboot Time            : Enabled ...(1)
    Previous Reboot Time   : N/A ...(2)
    Next Reboot Time       : 01:00 2023-10-31 ...(3)
    First-day              : 01:00 2023-10-31 ...(4)
    Repeat Interval-days   : 30 ...(5)
```

各項目の説明は、以下のとおりです。

表 18-13 repeat パラメーター使用時の `show reboot` コマンドの表示項目

項番	説明
(1)	自動再起動の有効 (Enabled) ／無効 (Disabled) を表示します。
(2)	前回の自動再起動を実行した日時を表示します。まだ一度も自動再起動が実行されていない場合は、N/A と表示されます。
(3)	次回の自動再起動を実行する予定日時を表示します。
(4)	**`reboot time`** コマンドで設定した、初回の自動再起動の実行日時を表示します。
(5)	一定期間ごとに自動再起動を繰り返し実行する場合の実行間隔（日単位）を表示します。

18.3 管理運用機能の実施例

管理運用機能を利用する場合の実施例を示します。

18.3.1 技術サポート情報を外部ストレージへコピーする場合

技術サポート情報を外部ストレージにコピーする場合の実施例を以下に示します。

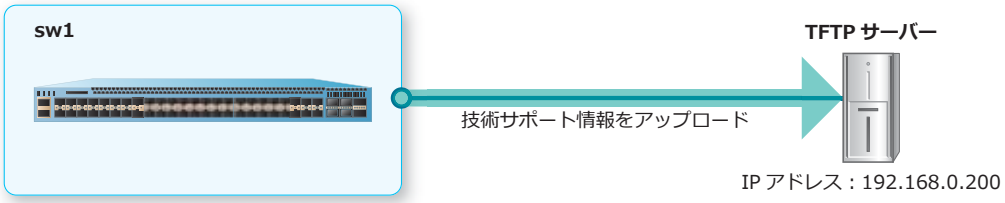
技術サポート情報を、[外部ストレージ] にファイル名 [tech_support.log] でコピーします。

```
sw1# debug copy tech-support d:/tech_support.log

Copy tech-support to /d:/tech_support.log ? (y/n) [n]  y

Please wait, copy tech-support to flash......100 %
```

18.3.2 技術サポート情報を TFTP サーバーへアップロードする場合

技術サポート情報を TFTP サーバーへアップロードする場合の実施例を示します。

図 18-1 技術サポート情報を TFTP サーバーへアップロードする場合の構成例



技術サポート情報を、IP アドレスが [192.168.0.200] の TFTP サーバーに、ファイル名を [tech_support.log] としてアップロードします。

```
sw1# debug copy tech-support tftp: //192.168.0.200/tech_support.log

Address of remote host [192.168.0.200]?
Destination filename [tech_support.log]?
 Connecting to server..................... Done.
 Upload tech-support................. 100 %

 Success.
```

18.3.3 装置の自動再起動の設定例

装置の自動再起動を、2023/11/30 1:00 に 1 回だけ実施する場合の設定例を示します。

1. 自動再起動する時刻を「2023/11/30 1:00」に設定します。

```
sw1# configure terminal
sw1(config)# reboot time 1:00 30 nov 2023
sw1(config)# end
sw1#
```

2. 実施後の自動再起動設定を確認します。

```
sw1# show reboot

    Reboot Time            : Enabled
    Previous Reboot Time   : N/A
    Next Reboot Time       : N/A
    First-day              : 01:00 2023-11-30
    Repeat Interval-days   : N/A

sw1#
```

3. 実施後の自動再起動関連の設定を以下に抜粋します。

```
# REBOOT

reboot time 01:00 30 nov 2023
```

19. メモリーエラー自動復旧機能

メモリーエラー自動復旧機能、および状態の確認方法について説明します。

REF: コマンドの詳細については、『コマンドリファレンス』を参照してください。

19.1 メモリーエラー自動復旧機能の機能説明

装置では、スイッチの大規模集積（LSI）メモリー（以後、**SW-LSI メモリー**）を監視できます。メモリーエラーが検出されると、自動的に復旧アクションが動作します。

エラーが検出されたメモリーにおいて、過去に同一箇所で規定回数のメモリーエラーが検出されていた場合、そのメモリーを監視対象外とし、SW-LSI メモリーの状態を「異常」とします。監視対象外になったメモリーでは、復旧アクションが動作しません。

19.1.1 メモリーエラー自動復旧機能の無効化

メモリーエラー自動復旧機能を無効にできます。無効にすると、SW-LSI メモリーの状態、すべてのカウンター、メモリー領域の監視はリセットされます。メモリーエラー自動復旧機能を無効にするには、**`memory-error auto-recovery mode disable`** コマンドを使用します。

19.1.2 メモリーエラー自動復旧機能の通知の無効化

SW-LSI メモリーにメモリーエラーが検出され、自動的に復旧した場合は、システムログエントリーが出力されます。システムログエントリーの出力を止めるには、**`memory-error auto-recovery notify disable`** コマンドを使用します。

19.1.3 メモリー状態が「異常」と検知された際のアクション設定

SW-LSI メモリーの状態が「異常」になったときに、すべてのポートを自動的にシャットダウンできます。メモリー状態が「異常」になった場合に、すべてのポートを自動的にシャットダウンするには、**`memory-error fault-action shutdown-all`** コマンドを使用します。

> ***NOTE:*** SW-LSI メモリーの状態が「異常」になりシャットダウンされたポートを復旧するには、**`clear memory-error`** コマンドまたは **`no memory-error fault-action shutdown-all`** コマンドを使用します。
>
> ***NOTE:*** 本機能でシャットダウンされたポートのリンク状態は、**`show interfaces`** コマンドでは "link status is down (cause: Memory Error)" と表示されます。また、**`show interfaces status`** コマンドの Status 項目では "memory-error" と表示されます。

19.1.4 メモリーエラー自動復旧機能のリストア

メモリーエラー自動復旧機能の状態をリストアできます。メモリーエラー自動復旧機能の状態をリストアするには、**`clear memory-error`** コマンドを使用します。

19.2 メモリーエラー自動復旧機能の状態確認

show environment memory コマンドで、メモリーエラー自動復旧機能の詳細状態を確認できます。

表示例を以下に示します。

```
# show environment memory

Detail Memory-Error Auto-Recovery Status:
-------------------------------------------------------------
Auto Recovery Mode          : Enabled ...(1)
Auto Recovery Notification : Enabled ...(2)
Fault Action Configuration : - ...(3)
(4)      (5)          (6)                (7)
Unit     Status       Recovery Count     ECC Uncorrectable Error Count
-----    ---------    ---------------    -------------------------------
1        Normal       0                  0
2        Normal       0                  0
```

各項目の説明は、以下のとおりです。

表 19-1 show environment memory コマンドの表示項目

項番	説明
(1)	メモリーエラー自動復旧機能の有効 (Enabled) ／無効 (Disabled) を表示します。
(2)	メモリーエラー自動復旧機能に関連する通知（ログ、SNMP トラップ）の有効 (Enabled) ／無効 (Disabled) を表示します。
(3)	SW-LSI メモリーの状態が「異常」になった場合に、すべてのポートをシャットダウンする機能の有効 (Shutdown-all) ／無効 (-) を表示します。
(4)	装置のボックス ID を表示します。スタックを構成していない場合は「1」が表示されます。
(5)	SW-LSI メモリーの状態を表示します。 • Normal：正常 • Abnormal：メモリーエラー発生状態（メモリーエラー自動復旧機能無効：メモリーエラーの発生を検知、メモリーエラー自動復旧機能有効：メモリーエラーの多発を検知）
(6)	メモリーエラーが検出されたときに、実行された復旧アクションの回数を表示します。
(7)	復旧不能なメモリーエラーが検出された回数を表示します。

20. カットスルー

カットスルーの機能、および状態の確認方法について説明します。

REF: コマンドの詳細については、『コマンドリファレンス』を参照してください。

20.1 カットスルーの機能説明

カットスルーは、パケット転送方式の 1 つです。デフォルトのパケット転送方式は、**ストアアンドフォワード**です。

ストアアンドフォワードと、カットスルーの違いは以下のとおりです。

- **ストアアンドフォワード**
  パケット全体を受信後、エラーがないことが確認できたらパケットを転送します。

  通信品質は良いが、カットスルーと比べて低速です。
- **カットスルー**
  パケット全体を受信し終わる前に中継処理を開始します。ストアアンドフォワードより遅延が少なくなります。

  CAUTION: NP5000、NP4000、NP3000、NP2100、NP2000、および NP2500 では、カットスルーは使用できません。

20.1.1 カットスルーの有効化

パケット転送方式をカットスルー方式に設定します。カットスルー方式に設定するには、**`packet-forwarding cut-through`** コマンドを使用します。

REF: 他機能との併用に制限があります。詳細については、『コマンドリファレンス』を参照してください。

20.2 カットスルーの状態確認

show packet-forwarding コマンドで、カットスルーの状態を確認できます。

表示例を以下に示します。

```
# show packet-forwarding

Cut-through:Disabled ...(1)
```

各項目の説明は、以下のとおりです。

表 20-1 show packet-forwarding コマンドの表示項目

項番	説明
(1)	カットスルー機能の有効 (Enabled) ／無効 (Disabled) を表示します。

21. ブザーおよびアラーム LED による障害通知

ブザーおよびアラーム LED による障害通知の機能、状態の確認方法、および構成例と設定例について説明します。

REF: コマンドの詳細については、『コマンドリファレンス』を参照してください。

REF: ブザーおよびアラーム LED による障害通知の設定例については、「第 4 編 レイヤー 2」の「ループ検知」や「ストームコントロール」も参照してください。

21.1 ブザーおよびアラーム LED による障害通知の機能説明

NP3000（1.09.01 以降）、NP2100、NP2000、および NP2500 では、ブザーおよびアラーム LED（ALM LED）を有効にすると、ループ検知機能やストームコントロール機能で障害を検知したときに、それぞれブザーおよびアラーム LED の動作で障害を通知できます。

NP4000 では、アラーム LED を有効にすると、ループ検知機能やストームコントロール機能で障害を検知したときに、アラーム LED の動作で障害を通知できます。

CAUTION: NP7000 および NP5000 では、ブザーおよびアラーム LED による障害通知を使用できません。

CAUTION: NP4000 では、ブザーによる障害通知を使用できません。

21.1.1 ブザーおよびアラーム LED の有効化

ブザーを有効にするには、まず装置全体に対して **alarm buzzer global enable** コマンドを使用します。次に、インターフェースに対して **alarm buzzer state enable** コマンドを使用して、ループ検知時またはストーム検知時にブザーによる通知が動作するように設定を有効にします。ブザーの動作時間を設定するには、**alarm buzzer duration** コマンドを使用します。ブザーの動作タイプを設定するには、**alarm buzzer beep-type** コマンドを使用します。

アラーム LED を有効にするには、まず装置全体に対して **alarm warn-led global enable** コマンドを使用します。次に、インターフェースに対して **alarm warn-led state enable** コマンドを使用して、ループ検知時またはストーム検知時にアラーム LED による通知が動作するように設定を有効にします。アラーム LED 動作時間を設定するには、**alarm warn-led duration** コマンドを使用します。

NOTE: NP3000（1.09.01 以降）、NP2100、NP2000、および NP2500 で buzzer または warn-led を指定しないコマンド（**alarm global enable** コマンド、**alarm state enable** コマンド、**alarm duration** コマンド）を使用した場合は、ブザーとアラーム LED の両方に対して設定されます。

21.1.2 ブザーおよびアラーム LED の手動操作

ブザーが鳴動している、またはアラーム LED が点滅している状態で、設定した動作時間を待たずに手動で動作を停止するには、以下のコマンドを実行します。

- **debug alarm buzzer test コマンド**
  鳴動しているブザーが停止します。
- **debug alarm warn-led test コマンド**
  点滅しているアラーム LED が消灯します。本コマンドはインターフェースを指定できます。

NOTE: **debug alarm buzzer test** コマンドまたは **debug alarm warn-led test** コマンドを実行する前に、ループおよびストームを解消してください。

NOTE: ループまたはストームを認識してアラーム LED が点滅しているときに、**debug alarm warn-led test** コマンドで点滅を消灯させる場合は、インターフェースを指定してください。

NOTE: **debug alarm test** コマンドは、装置のブザーとアラーム LED を任意のタイミングで動作させることもできます。コマンドを一度入力するとブザーとアラーム LED の両方または指定した一方が動作し、もう一度同じコマンドを入力すると動作が停止します。アラーム LED のみ動作させる場合には、ポートまたはチャネルグループ ID も指定できます。

21.1.3 ループ検知機能による障害通知

ループ検知機能によってループを検知した場合、ブザーおよびアラーム LED によって通知できます。ループを検知したポートが err-disabled 状態になっても、ブザーおよびアラーム LED は動作し続けます。ブザーおよびアラーム LED は、以下のトリガーによって停止するまで動作し続けます。

- **alarm buzzer duration** コマンド、**alarm warn-led duration** コマンドで設定した時間が経過した場合
- ループ検知機能によるループ検知状態が解消された場合
- **debug alarm buzzer test** コマンド、**debug alarm warn-led test** コマンドによって、手動で停止した場合

21.1.4 ストームコントロール機能による障害通知

ストームコントロール機能によってストームを検知した場合、ブザーおよびアラーム LED によって通知できます。ストームコントロールによる帯域制限が動作している間は、ブザーおよびアラーム LED は動作し続けます。ブザーおよびアラーム LED は、以下のトリガーによって停止するまで動作し続けます。

- **alarm buzzer duration** コマンド、**alarm warn-led duration** コマンドで設定した時間が経過した場合
- ストームが解消され、ストームコントロールによる帯域制限が解除された場合
- ストームコントロール機能のアクションを shutdown に設定している場合に、ストームを検知したポートがシャットダウン（err-disabled 状態に変更）された場合
- **debug alarm buzzer test** コマンド、**debug alarm warn-led test** コマンドによって、手動で停止した場合

21.2 ブザーおよびアラーム LED による障害通知の状態確認

ブザーおよびアラーム LED による障害通知の状態を表示して確認する方法を説明します。

21.2.1 ブザーによる障害通知の状態の表示

show alarm buzzer コマンドで、ブザーによる障害通知の状態を確認できます。

表示例を以下に示します。

```
# show alarm buzzer

 Alarm Buzzer:
 ----------------------------------------------------------------
 Global State     : Enabled ...(1)
 Duration         : 60 second(s) ...(2)
 Warning Time Left: 35 second(s) ...(3)
 Current Status   : Warning ...(4)
 (5)              (6)       (7)
 Interface        State     Cause Enabled
 ---------------  --------  --------------
 Port1/0/1        Enabled   Loop Detection
 Port1/0/2        Enabled   Loop Detection
 Port1/0/3        Enabled   Storm Control
 Port1/0/4        Disabled  -
～～省略～～
 Port1/0/26       Disabled  -
 Port1/0/27       Disabled  -
 Port1/0/28       Disabled  -

 Alarm Events:
 (8)              (9)
 Interface        Reason
 ----------------------------------------------------------------
 Port 1/0/1       Loop
```

各項目の説明は、以下のとおりです。

表 21-1 show alarm buzzer コマンドの表示項目

項番	説明
(1)	グローバル設定モードのブザーの有効 (Enabled) ／無効 (Disabled) を表示します。
(2)	ブザーの鳴動時間を表示します。infinite 設定の場合は infinite と表示されます。
(3)	ブザーが停止するまでの残り時間を表示します。infinite 設定の場合は infinite と表示されます。
(4)	ブザーの状態を表示します。 • Inactive：ブザーが無効 • Ready：ブザーが有効で、鳴動していない状態 • Warning：ブザーが有効で、鳴動している状態
(5)	ポート番号またはポートチャネル番号を表示します。
(6)	ブザーの有効 (Enabled) ／無効 (Disabled) を表示します。

項番	説明
(7)	ブザーで通知する対象の機能を表示します。 • All：ループ検知機能、ストームコントロール機能 • Loop Detection：ループ検知機能 • Storm Control：ストームコントロール機能
(8)	ブザーおよびアラーム LED が動作する原因を検知した、ポート番号またはポートチャネル番号を表示します。
(9)	ブザーおよびアラーム LED が動作している原因を表示します。 • Loop：ループ検知 • Storm(BC)：ブロードキャストストームを検知 • Storm(MC)：マルチキャストストームを検知 • Storm(DLF)：未知のユニキャストストームを検知 • Storm(BC&MC)：ブロードキャストストームおよびマルチキャストストームを検知 • Storm(BC&DLF)：ブロードキャストストームおよび未知のユニキャストストームを検知 • Storm(MC&DLF)：マルチキャストストームおよび未知のユニキャストストームを検知 • Storm(BC&MC&DLF)：ブロードキャストストーム、マルチキャストストーム、および未知のユニキャストストームを検知 • All (Storm Type: ストーム種別)：ループ検知機能が notify-only モードで、ループとストームの両方を検知している場合

21.2.2 アラーム LED による障害通知の状態の表示

show alarm warn-led コマンドで、アラーム LED による障害通知の状態を確認できます。

表示例を以下に示します。

```
# show alarm warn-led

 Alarm Warning LEDs:
 ------------------------------------------------------------------
 Global State     : Enabled ...(1)
 Duration         : 60 second(s) ...(2)
 (3)              (4)       (5)              (6)       (7)
 Interface        State     Cause Enabled    Current   Warning
                                             Status    Time Left
 ---------------  --------  ---------------  --------  ------------
 Port1/0/1        Enabled   Loop Detection   Ready     60 second(s)
 Port1/0/2        Enabled   Loop Detection   Ready     60 second(s)
 Port1/0/3        Enabled   Storm Control    Warning   43 second(s)
 Port1/0/4        Disabled  -                Inactive  60 second(s)
～～省略～～
 Port1/0/26       Disabled  -                Inactive  60 second(s)
 Port1/0/27       Disabled  -                Inactive  60 second(s)
 Port1/0/28       Disabled  -                Inactive  60 second(s)

 Alarm Events:
 (8)              (9)
 Interface        Reason
 ------------------------------------------------------------------
 Port 1/0/3       Storm(BC)
```

各項目の説明は、以下のとおりです。

表 21-2 `show alarm warn-led` コマンドの表示項目

項番	説明
(1)	グローバル設定モードのアラーム LED の有効 (Enabled) ／無効 (Disabled) を表示します。
(2)	アラーム LED の動作時間を表示します。infinite 設定の場合は infinite と表示されます。
(3)	ポート番号またはポートチャネル番号を表示します。
(4)	アラーム LED の有効 (Enabled) ／無効 (Disabled) を表示します。
(5)	アラーム LED で通知する対象の機能を表示します。 • All：ループ検知機能、ストームコントロール機能 • Loop Detection：ループ検知機能 • Storm Control：ストームコントロール機能
(6)	アラーム LED の状態を表示します。 • Inactive：アラーム LED が無効 • Ready：アラーム LED が有効で、アラーム LED が消灯している状態 • Warning：アラーム LED が有効で、アラーム LED が点滅している状態
(7)	アラーム LED が停止するまでの残り時間を表示します。infinite 設定の場合は infinite と表示されます。
(8)	ブザーおよびアラーム LED が動作する原因を検知した、ポート番号またはポートチャネル番号を表示します。
(9)	ブザーおよびアラーム LED が動作している原因を表示します。 • Loop：ループ検知 • Storm(BC)：ブロードキャストストームを検知 • Storm(MC)：マルチキャストストームを検知 • Storm(DLF)：未知のユニキャストストームを検知 • Storm(BC&MC)：ブロードキャストストームおよびマルチキャストストームを検知 • Storm(BC&DLF)：ブロードキャストストームおよび未知のユニキャストストームを検知 • Storm(MC&DLF)：マルチキャストストームおよび未知のユニキャストストームを検知 • Storm(BC&MC&DLF)：ブロードキャストストーム、マルチキャストストーム、および未知のユニキャストストームを検知 • All (Storm Type: ストーム種別)：ループ検知機能が notify-only モードで、ループとストームの両方を検知している場合

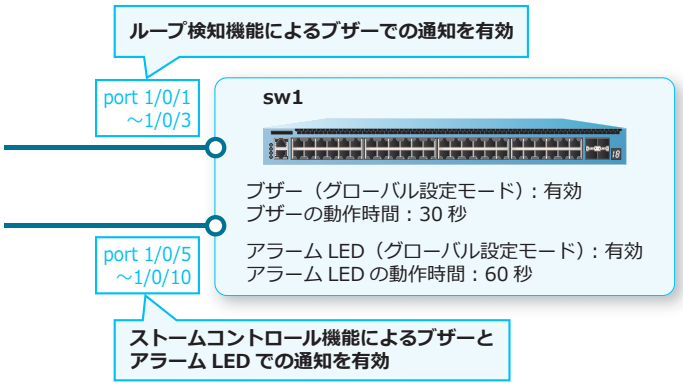
21.3 ブザーおよびアラーム LED による障害通知の構成例と設定例

以下の設定内容で、ブザーおよびアラーム LED による障害通知の構成例と設定例を示します。

- ポート 1/0/1 からポート 1/0/3 で、ループ検知機能によるブザーでの通知を有効にする
- ポート 1/0/5 からポート 1/0/10 で、ストームコントロール機能によるブザーとアラーム LED での通知を有効にする
- ブザーの動作時間は 30 秒に、アラーム LED の動作時間は 60 秒に設定する

REF: ループ検知機能、およびストームコントロール機能の設定は、「第 4 編 レイヤー 2」のそれぞれの章を参照してください。

図 21-1 ブザーおよびアラーム LED による障害通知の構成例



1. ブザーのグローバル設定を有効にします。

```
sw1# configure terminal
sw1(config)# alarm buzzer global enable
sw1(config)#
```

2. ブザーの動作時間を 30 秒に設定します。

```
sw1(config)# alarm buzzer duration 30
sw1(config)#
```

3. ポート 1/0/1 からポート 1/0/3 で、ループ検知機能によるブザーでの通知を有効にします。

```
sw1(config)# interface range port 1/0/1-3
sw1(config-if-port-range)# alarm buzzer state enable cause loop-detection
sw1(config-if-port-range)# exit
sw1(config)#
```

4. アラーム LED のグローバル設定を有効にします。

```
sw1(config)# alarm warn-led global enable
sw1(config)#
```

5. アラーム LED の動作時間を 60 秒に設定します。

```
sw1(config)# alarm warn-led duration 60
sw1(config)#
```

6. ポート 1/0/5 からポート 1/0/10 で、ストームコントロール機能によるブザーとアラーム LED での通知を有効にします。

```
sw1(config)# interface range port 1/0/5-10
sw1(config-if-port-range)# alarm buzzer state enable cause storm-control
sw1(config-if-port-range)# alarm warn-led state enable cause storm-control
sw1(config-if-port-range)# end
sw1#
```

22. CPU 使用率監視機能

CPU 使用率監視機能、および状態の確認方法について説明します。

REF: コマンドの詳細については、『コマンドリファレンス』を参照してください。

22.1 CPU 使用率監視機能の機能説明

CPU 使用率、システムメモリー（SYS_MEM、SYS_HUGE、または SEC_MEM）の割り当て状態、およびシステムメモリー（SYS_MEM、SYS_HUGE、または SEC_MEM）の使用率を監視できます。

22.1.1 CPU 使用率監視機能の有効化

CPU 使用率監視機能を有効にすると、CPU 使用率が監視されます。CPU 使用率が、あらかじめ指定したしきい値を超えると、障害解析用情報が記録され、しきい値を超えたことを示すログおよびトラップを出力します。

NOTE: ログおよびトラップの出力は、NP7000 の 1.06.01 以降、NP5000 の 1.06.01 以降、NP4000 の 1.03.01 以降、NP3000 の 1.06.01 以降、NP2100 の 1.09.02 以降、NP2000 の 1.08.01 以降、NP2500 の 1.08.02 以降でサポートしています。

NOTE: しきい値上昇前後の CPU に関する履歴ログは、NP7000 の 1.07.01 以降、NP5000 の 1.07.01 以降、NP2100 の 1.10.01 以降、NP2500 の 1.10.01 以降でサポートしています。

CPU 使用率監視機能を有効にするには、**`cpu-protect trace trigger`** コマンドを使用します。トラップの出力を有効にするには、**`snmp-server enable traps cpu-protect`** コマンドを使用します。

なお、記録された障害解析用情報は、**`show tech-support`** コマンドの技術サポート情報の一部として出力されます。

22.1.2 システムメモリー割り当て状態監視機能の有効化

システムメモリー割り当て状態監視機能を有効にすると、システムメモリーの割り当て状態が監視されます。システムメモリーを割り当てられない状態が 1 分間続いた場合、装置が再起動されます。

NOTE: システムメモリー割り当て状態監視機能は、NP7000 の 1.05.01 以降、NP5000 の 1.05.01 以降、NP4000 の 1.03.01 以降、NP3000 の 1.06.01 以降、NP2100 の 1.09.02 以降、NP2000 の 1.05.01 以降、NP2500 の 1.08.02 以降でサポートしています。

システムメモリー割り当て状態監視機能を有効にするには、**`cpu-protect system-memory limit-check fault-action reboot`** コマンドを使用します。

NOTE: NP7000 の 1.08.02 以降、NP5000 の 1.08.01 以降、NP2100 の 1.09.05/1.10.01 以降、NP2000 の 1.09.05 以降、NP2500 の 1.08.04 以降では、**`cpu-protect system-memory limit-check fault-action reboot`** コマンドは削除され、デフォルトで有効設定相当の動作に仕様変更されています。また、監視対象のシステムメモリーも追加されています。

22.1.3 システムメモリー使用率監視機能の有効化

システムメモリー使用率監視機能を有効にすると、システムメモリー使用率を 60 秒ごとにチェックします。システムメモリー使用率があらかじめ指定したしきい値を超えると、ログとトラップが出力されます。

> ***NOTE:*** システムメモリー使用率監視機能は、NP7000 の 1.05.01 以降、NP5000 の 1.05.01 以降、NP4000 の 1.03.01 以降、NP3000 の 1.06.01 以降、NP2100 の 1.09.02 以降、NP2000 の 1.05.01 以降、NP2500 の 1.08.02 以降でサポートしています。

システムメモリー使用率監視機能を有効にするには、**`cpu-protect system-memory limit-check threshold`** コマンドを使用します。

> ***NOTE:*** NP7000 の 1.08.02 以降、NP5000 の 1.08.01 以降、NP2100 の 1.09.05/1.10.01 以降、NP2000 の 1.09.05 以降、NP2500 の 1.08.04 以降では、監視対象のシステムメモリーが追加されています。

22.2 CPU 使用率監視機能の状態確認

show cpu-protect trace コマンドで、CPU 使用率監視機能の状態を確認できます。

> ***NOTE:*** CPU に関する履歴ログの項目は、NP7000 の 1.07.01 以降、NP5000 の 1.07.01 以降、NP2100 の 1.10.01 以降、NP2500 の 1.10.01 以降で表示されます。

表示例を以下に示します。

```
# show cpu-protect trace

CPU Protect Trace Trigger State     : Enabled ...(1)
CPU Protect Trace Trigger Status    : Exhausted ...(2)
Utilization Thresholds              : 100% ...(3)
Utilization polling                 : 60s ...(4)
CPU Protect Trace History State     : Enabled ...(5)
Traced log                          : Collected ...(6)
[2020-06-26 15:17:55]CPU Utilization: 65% ...(7)
[2020-06-26 15:23:16]CPU Utilization: 62%
[2020-06-26 15:24:05]CPU Utilization: 75%
```

各項目の説明は、以下のとおりです。

表 22-1 show cpu-protect trace コマンドの表示項目

項番	説明
(1)	CPU 使用率監視機能の有効 (Enabled) ／無効 (Disabled) を表示します。
(2)	CPU 使用率監視機能の状態を表示します。 • Normal：CPU 使用率がしきい値を上回っていない状態 • Exhausted：CPU 使用率がしきい値を上回っている状態
(3)	CPU 使用率のしきい値を表示します。
(4)	CPU 使用率の監視間隔を表示します。
(5)	CPU に関する履歴ログの採取機能の有効 (Enabled) ／無効 (Disabled) を表示します。
(6)	CPU に関する履歴ログの記録状態を表示します。 • No collection：履歴ログが記録されていない状態 • Collected：履歴ログが記録されている状態
(7)	指定した監視間隔の平均 CPU 使用率がしきい値を上回った履歴を表示します。

23. ZTP（Zero Touch Provisioning）

ZTP の機能、および状態の確認方法について説明します。

REF: コマンドの詳細については、『コマンドリファレンス』を参照してください。

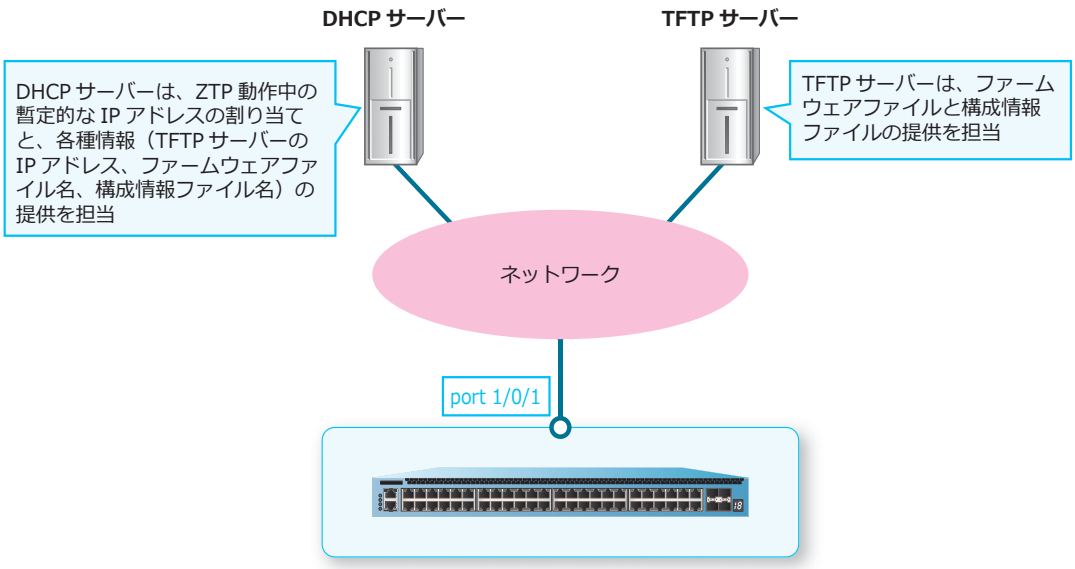
23.1 ZTP の機能説明

ZTP（Zero Touch Provisioning）は、ネットワーク構築作業を自動化する仕組みです。ZTP を使用すると、装置をネットワークに接続して起動するだけで、自動的にファームウェアファイルと構成情報ファイルをネットワーク経由で取得し、取得したファームウェアと構成情報で装置を起動させることができるようになります。

CAUTION: スタック構成の装置では、ZTP 機能は使用できません。

NOTE: ZTP は、NP4000 の 1.03.01 以降、NP3000 の 1.11.01 以降、NP2100 の 1.09.02 以降、NP2000 の 1.07.01 以降、NP2500 の 1.08.02 以降でサポートしています。

図 23-1 ZTP 使用時の基本構成



23.1.1 ZTP の基本動作

ZTP の基本動作、および動作中の ZTP 処理について説明します。

NP4000、NP2000 の ZTP の動作条件

NP4000、NP2000 では、以下のどちらかの条件を満たす場合に、装置起動時に ZTP が動作します。

- ztp enable（デフォルト設定）で、startup-config が工場出荷状態の場合
- ztp enable force 設定の場合

また、以下のいずれかの条件を満たす場合は、装置起動時に ZTP は動作しません。

- SD カードブート用の SD カードが挿入されている場合（SD カードブートによる起動が優先）
- ztp enable（デフォルト設定）でも、startup-config が工場出荷状態以外の場合
- no ztp enable 設定の場合

- ZTP によってダウンロードされたファームウェアファイル（現在のバージョンと異なるバージョン）に更新するため、ZTP の動作で自動的に再起動された場合

NP3000、NP2100、NP2500 の ZTP の動作条件

NP3000、NP2100、NP2500 では、本体付属の ZTP スイッチによって ZTP の ON/OFF が可能です。以下のどちらかの条件を満たす場合に、装置起動時に ZTP が動作します。

- ZTP スイッチが ON 状態
- ZTP スイッチが OFF 状態でも、ztp enable force 設定の場合

また、以下のいずれかの条件を満たす場合は、装置起動時に ZTP は動作しません。

- SD カードブート用の SD カードが挿入されている場合（SD カードブートによる起動が優先）
- ZTP スイッチが OFF 状態
- ZTP スイッチが ON 状態でも、no ztp enable 設定の場合
- ZTP によってダウンロードされたファームウェアファイル（現在のバージョンと異なるバージョン）に更新するため、ZTP の動作で自動的に再起動された場合

ZTP の動作と中断

ZTP が動作する条件を満たした装置をネットワークに接続して起動すると、ZTP が動作を開始します。

- 「ztp enable（デフォルト設定）で、startup-config が工場出荷状態」で ZTP が動作する場合は、ZTP が動作を開始してから終了するまでで間は、すべてのポート間のトラフィック中継は抑止されます。
- 「ztp enable force 設定」で ZTP が動作する場合は、トラフィック中継の抑止は行われません。

CAUTION: startup-config が工場出荷状態の装置で ZTP が失敗した場合は、装置は工場出荷状態の設定で起動します。そのため、ZTP が失敗した場合にループが発生するようなケーブル接続状態では、ZTP を使用しないでください。

NOTE: マネージメントポート経由での ZTP はサポートしていません。

ZTP を途中で中断する場合は、コンソールポートに接続した端末で Ctrl+C キーを入力してください。

NOTE: ファームウェアファイルまたは構成情報ファイルの更新中は、中断できません。

23.1.2 ZTP 処理の流れ

ZTP の動作開始後の処理について説明します。

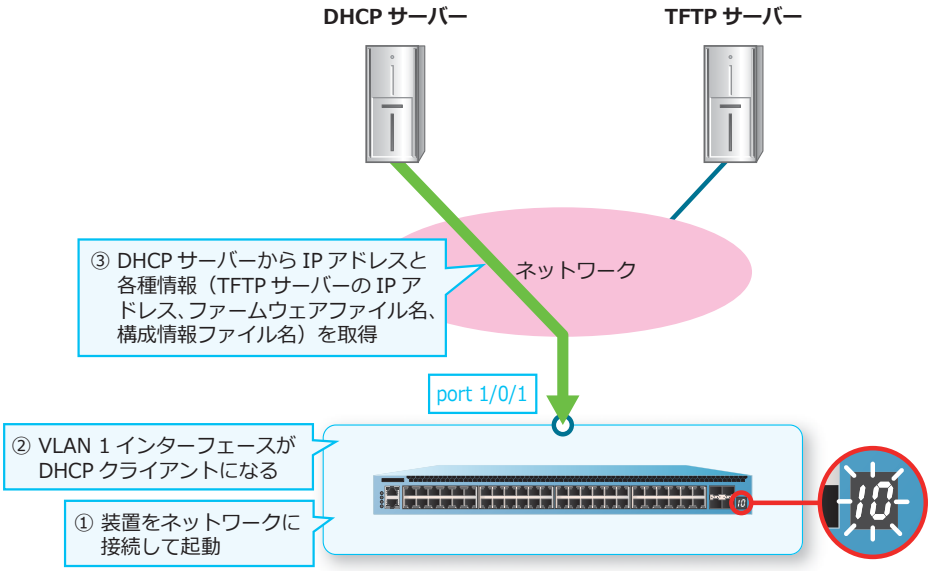
NOTE: スタック ID LED による ZTP 動作状態の表示は、NP4000、NP3000、NP2100、NP2000 でサポートしています。

NOTE: NP3000、NP2100、NP2500 では、ZTP 動作中は ZTP LED が緑点灯します。ZTP に失敗した場合は ZTP LED が 3 分間赤点灯します。

ZTP 処理（1/4）DHCP サーバーからの情報取得［LED［10］点滅］

ZTP が動作を開始すると、VLAN 1 インターフェースは自動的に DHCP クライアントになります。また、DHCP サーバーから IP アドレスを取得する際に、各種情報（TFTP サーバーの IP アドレス、ファームウェアファイル名、構成情報ファイル名）も取得します。この ZTP 処理中は、スタック ID LED に［10］が点滅します。

図 23-2 ZTP 処理（1/4）



各種情報（TFTP サーバーの IP アドレス、ファームウェアファイル名、構成情報ファイル名）は、DHCP サーバーから取得します。そのため、DHCP サーバーでは、提供する情報を事前に設定しておく必要があります。

表 23-1 DHCP サーバーでの各種情報の設定

情報	概要
TFTP サーバーの IP アドレス	• DHCP オプション 150（TFTP Server Address）で最大 3 個、siaddr フィールドの IP アドレスで 1 個の、合計最大 4 個の IP アドレスを指定可能。 • DHCP オプション 150 で指定された IP アドレス、siaddr フィールドの IP アドレスの順番で、TFTP サーバーからダウンロードが成功するまで順次適用される。
ファームウェアファイル名	• DHCP オプション 125（Vendor-Identifying Vendor-Specific Information）で指定可能。 • enterprise-number は 278 固定、subopt-code は 1 固定。 • ファームウェアファイル名は最大 32 文字。 • DHCP オプション 125 に複数のデータが含まれている場合は、最初のデータのみ使用。 • DHCP メッセージに DHCP オプション 125 が付与されていない場合は、ファームウェアファイル名は取得しない。
構成情報ファイル名	• DHCP オプション 67（Bootfile name）で指定可能。 • DHCP メッセージに DHCP オプション 67 が付与されていない場合は、file フィールドの値を構成情報ファイル名として取得。 • 構成情報ファイル名は最大 32 文字。 • DHCP オプション 67 が付与されておらず、file フィールドにも値が入っていない場合は、構成情報ファイル名は取得しない。

DHCP サーバーからの情報取得に失敗した場合は、ZTP は処理を終了します。また、現地作業者に失敗したことを伝えるために、スタック ID LED に［14］を 3 分間点滅させます。

表 23-2 DHCP サーバーからの情報取得に失敗した場合

スタック ID LED	要因
［14］を 3 分間点滅	• DHCP サーバーからの応答がない場合。 • DHCP サーバーから TFTP サーバーの IP アドレスを取得できなかった場合。 • リースされた暫定 IP アドレスと、取得した TFTP サーバーの IP アドレスが別セグメントだが、デフォルトゲートウェイの IP アドレスを取得できなかった場合。 • 取得した TFTP サーバー、またはデフォルトゲートウェイの IP アドレスに対して、ARP 解決ができなかった場合。 • DHCP サーバーから取得したファームウェアファイル名が 33 文字以上だった場合。

ZTP 処理（2/4）TFTP サーバーからのファームウェアファイルのダウンロード［LED［11］点滅］

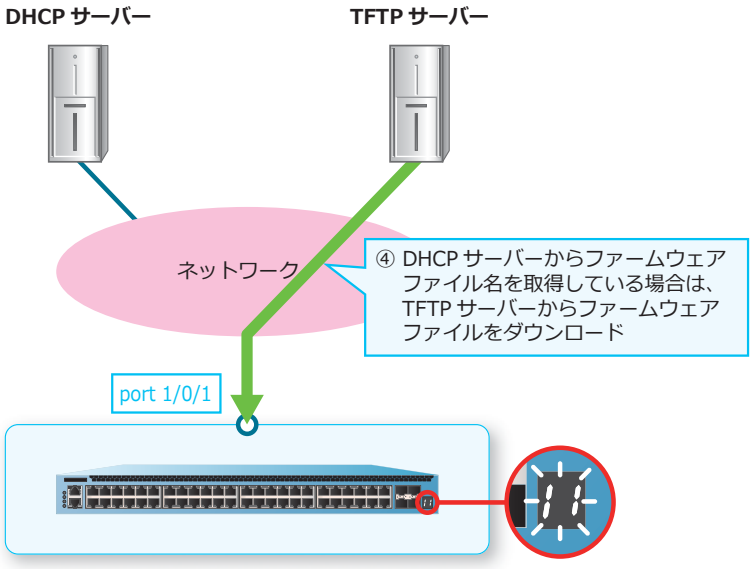
DHCP サーバーからファームウェアファイル名を取得している場合は、TFTP サーバーからファームウェアファイルをダウンロードします。この ZTP 処理中は、スタック ID LED に［11］が点滅します。

複数の TFTP サーバーの IP アドレスを取得している場合は、優先順位の高い TFTP サーバーからファームウェアファイルのダウンロードを試します。ファームウェアファイルをダウンロードできた場合は次の処理に移行します。失敗した場合は、次に優先度の高い TFTP サーバーからのダウンロードを試します。

ダウンロードしたファームウェアファイルのバージョンが現在のバージョンと同じ場合は、何もせずに次の処理に移行します。現在のバージョンと異なる場合は、ダウンロードしたファームウェアファイルを装置に保存します。

なお、DHCP サーバーからファームウェアファイル名を取得していない場合は、本処理はスキップされます。

図 23-3 ZTP 処理（2/4）



TFTP サーバーからのファームウェアファイルのダウンロードに失敗した場合は、ZTP 処理は終了します。また、現地作業者に失敗したことを伝えるために、スタック ID LED に［15］を 3 分間点滅させます。

表 23-3 TFTP サーバーからのファームウェアファイルのダウンロードに失敗した場合

スタック ID LED	要因
［15］を 3 分間点滅	• TFTP サーバーからの応答がタイムアウトするなどして、正常にファームウェアファイルをダウンロードできなかった場合。 • 取得したファームウェアファイルが不正なファイルの場合。 • 取得したファームウェアファイルを正常に保存できなかった場合。

ZTP 処理（3/4）TFTP サーバーからの構成情報ファイルのダウンロード［LED［12］点滅］

NOTE: ファームウェアファイルと構成情報ファイルは、同じ TFTP サーバーに保存しておく必要があります。

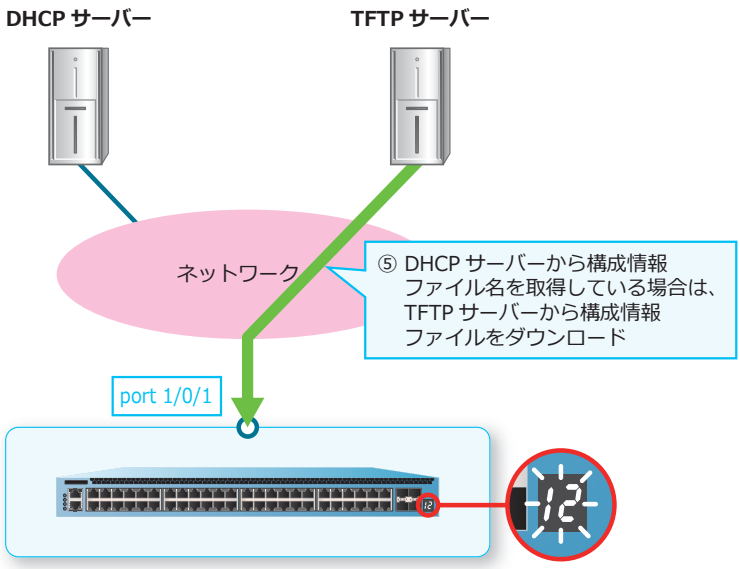
DHCP サーバーから構成情報ファイル名を取得している場合は、TFTP サーバーから構成情報ファイルをダウンロードします。この ZTP 処理中は、スタック ID LED に［12］が点滅します。

前の処理でファームウェアファイルをダウンロードしている場合は、ダウンロードに成功した TFTP サーバーから構成情報ファイルをダウンロードします。複数の TFTP サーバーの IP アドレスを取得していても、他の TFTP サーバーからのダウンロードは行われません。

前の処理がスキップされてファームウェアファイルのダウンロードを実施していない場合は、優先順位の高い TFTP サーバーから構成情報ファイルのダウンロードを試します。構成情報ファイルをダウンロードできた場合は次の処理に移行します。失敗した場合は、次に優先度の高い TFTP サーバーからのダウンロードを試します。

なお、DHCP サーバーから構成情報ファイル名を取得していない場合は、本処理はスキップされます。

図 23-4 ZTP 処理（3/4）



TFTP サーバーからの構成情報ファイルのダウンロードに失敗した場合は、ZTP 処理は終了します。また、現地作業者に失敗したことを伝えるために、スタック ID LED に［16］を 3 分間点滅させます。

表 23-4 TFTP サーバーからの構成情報ファイルのダウンロードに失敗した場合

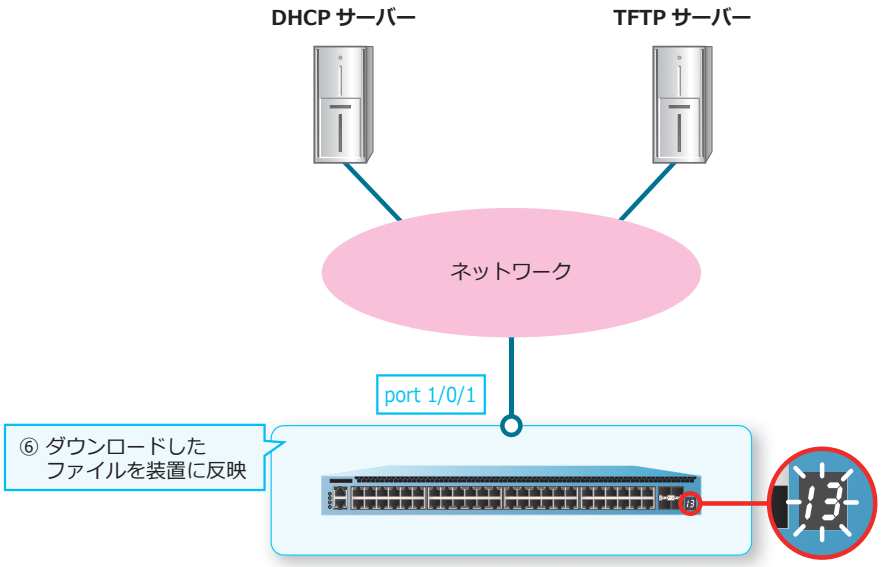
スタック ID LED	要因
［16］を 3 分間点滅	• DHCP サーバーから取得した構成情報ファイル名が 33 文字以上だった場合。 • TFTP サーバーからの応答がタイムアウトするなどして、正常に構成情報ファイルを取得できなかった場合。 • 取得した構成情報ファイルが不正なファイルの場合。 • 取得した構成情報ファイルを正常に保存できなかった場合。

ZTP 処理（4/4）ダウンロードしたファイルの反映［LED［13］点滅］

NOTE: ダウンロードしたファームウェアファイルのバージョンが現在のバージョンと同じ場合は、反映されません。

ファームウェアファイル（現在のバージョンと異なるバージョン）と構成情報ファイルをダウンロードした後は、それらのファイルを装置に反映します。この ZTP 処理中で自動的に再起動が実施されるまでは、スタック ID LED に［13］が点滅します。なお、構成情報ファイルはこのステップで保存処理されます。

図 23-5 ZTP 処理（4/4）



ファームウェアファイル（現在のバージョンと異なるバージョン）と構成情報ファイルの両方を取得した場合は、ブートスクリプトの内容が「プライマリーブートイメージファイル：ダウンロードしたファームウェアファイル」、「プライマリー構成情報ファイル：ダウンロードした構成情報ファイル」に変更され、自動的に再起動が実行されて反映されます。

ファームウェアファイル（現在のバージョンと異なるバージョン）だけを取得した場合は、ブートスクリプトの内容が「プライマリーブートイメージファイル：ダウンロードしたファームウェアファイル」に変更され、自動的に再起動が実行されて反映されます。

構成情報ファイルだけを取得した場合は、「プライマリー構成情報ファイル：ダウンロードした構成情報ファイル」に変更され、さらに running-config に反映されます。このケースでは再起動は発生しません。

なお、どちらのファイルも取得していない場合は、何も反映されずに ZTP 処理は終了します。

23.1.3 LED による ZTP の動作状態の確認

ZTP 動作中は、スタック ID LED によって進行状況や失敗状況を確認できます。

NOTE: スタック ID LED による ZTP 動作状態の表示は、NP4000、NP3000、NP2100、NP2000 でサポートしています。

NOTE: NP3000、NP2100、NP2500 では、ZTP 動作中は ZTP LED が緑点灯します。ZTP に失敗した場合は ZTP LED が 3 分間赤点灯します。

表 23-5 ZTP 動作中のスタック ID LED 表示

スタック ID LED	概要
［10］点滅	DHCP サーバーからの情報取得中。
［11］点滅	TFTP サーバーからのファームウェアファイルのダウンロード中。
［12］点滅	TFTP サーバーからの構成情報ファイルのダウンロード中。
［13］点滅	ダウンロードしたファイルの反映中。
［14］を 3 分間点滅	以下の理由で ZTP が失敗して終了。 • DHCP サーバーからの応答がない場合。 • DHCP サーバーから TFTP サーバーの IP アドレスを取得できなかった場合。 • リースされた暫定 IP アドレスと、取得した TFTP サーバーの IP アドレスが別セグメントだが、デフォルトゲートウェイの IP アドレスを取得できなかった場合。 • 取得した TFTP サーバー、またはデフォルトゲートウェイの IP アドレスに対して、ARP 解決ができなかった場合。 • DHCP サーバーから取得したファームウェアファイル名が 33 文字以上だった場合。
［15］を 3 分間点滅	以下の理由で ZTP が失敗して終了。 • TFTP サーバーからの応答がタイムアウトするなどして、正常にファームウェアファイルをダウンロードできなかった場合。 • 取得したファームウェアファイルが不正なファイルの場合。 • 取得したファームウェアファイルを正常に保存できなかった場合。
［16］を 3 分間点滅	以下の理由で ZTP が失敗して終了。 • DHCP サーバーから取得した構成情報ファイル名が 33 文字以上だった場合。 • TFTP サーバーからの応答がタイムアウトするなどして、正常に構成情報ファイルを取得できなかった場合。 • 取得した構成情報ファイルが不正なファイルの場合。 • 取得した構成情報ファイルを正常に保存できなかった場合。

23.1.4 ZTP の制限事項

- スタック構成の装置では、ZTP 機能は使用できません。
- ZTP が失敗して終了した場合にループが発生するような設定／ケーブル接続状態では、ZTP を使用しないでください。
- マネージメントポート経由での ZTP はサポートしていません。
- DHCP サーバーや TFTP サーバーとの通信は、IPv4 のみサポートしています。
- ファームウェアおよび構成情報ファイルは、同じ TFTP サーバーに保存しておく必要があります。
- NP3000（1.11.01 以降）で、VLAN 1 インターフェースに設定した IP アドレスで RIP 機能または OSPFv2 機能を使用する場合は、ZTP スイッチを OFF 状態にするなどして、起動時に ZTP が動作しないようにして使用してください。起動時に ZTP が動作／中断してから起動すると、ZTP 処理仕様の関係で、VLAN 1 インターフェースの IP アドレスに関連したレイヤー 3 機能の一部の設定（RIP 機能の **network** コマンド、OSPFv2 機能の **network area** コマンド）が、起動後に反映されない仕様制限があります。

23.1.5 ZTP の動作例

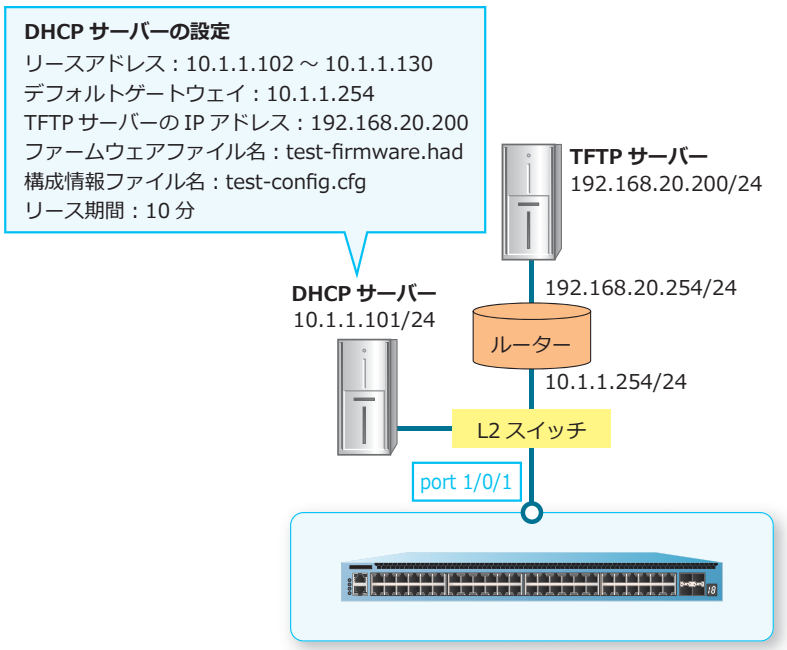
ZTP の動作例を、以下に示します。

23.1.5.1 ファームウェアと構成情報の両方を対象とする ZTP の動作例

ファームウェアと構成情報の両方を対象として ZTP を動作させる場合は、DHCP サーバーでファームウェアファイル名と構成情報ファイル名の両方が提供できるように準備しておく必要があります。

ファームウェアと構成情報の両方を対象として ZTP を動作させる場合の構成例と動作例を以下に示します。この例では、DHCP サーバー（10.1.1.101）を同一セグメントに、TFTP サーバーを別セグメント（192.168.20.200）に配置しています。

図 23-6 ファームウェアと構成情報を対象とする ZTP 動作例



この動作例のコンソールログ、および LED の点滅について、以下に示します。

```
 (1)
Press any key to login...


 Start ZTP, lock CLI for process!
 Exit ZTP process by CTRL+C.

(2)
 Try to download image from TFTP://192.168.20.200/test-firmware.had.......
 Accessing tftp:...
 Transmission start...
 Transmission finished, file length 7102392 bytes.Done
 Please wait, programming flash for save image...Done.
(3)
 Try to download configure from TFTP://192.168.20.200/test-config.cfg.......
 Accessing tftp:...
 Transmission start...
 Transmission finished, file length 2160 bytes.Done
(4)
 Please wait, save configure to file test-config.cfg ...      Done.
 Set /c:/test-config.cfg as boot configure OK.
 Set /c:/test-firmware.had as boot image OK.
 ZTP process OK.

(5)
 Reboot system, please wait......
```

各項目の説明は、以下のとおりです。

表 23-6 ファームウェアと構成情報を対象とする ZTP 動作例のコンソールログの説明

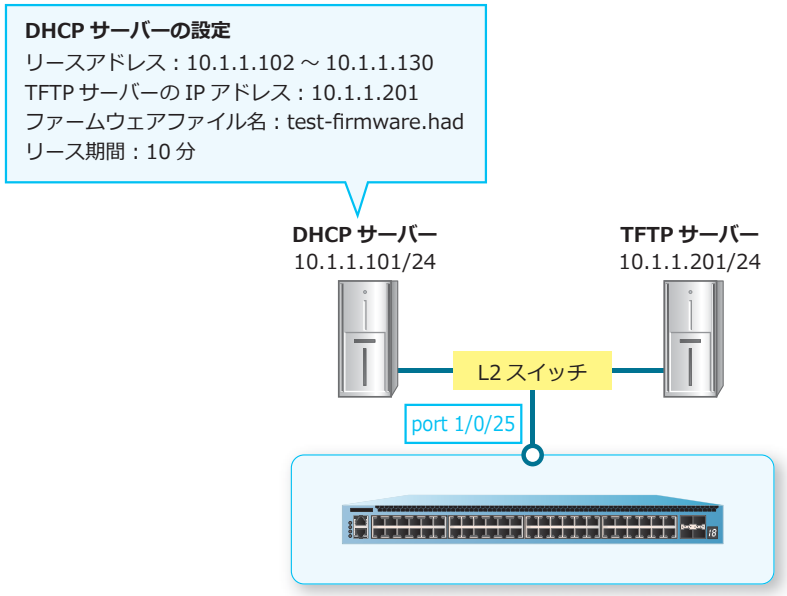
項番	説明
(1)	［LED［10］点滅］ DHCP サーバーからの情報取得中
(2)	［LED［11］点滅］ TFTP サーバーからファームウェアファイルをダウンロード中
(3)	［LED［12］点滅］ TFTP サーバーから構成情報ファイルをダウンロード中
(4)	［LED［13］点滅］ ダウンロードしたファイルの反映中
(5)	ダウンロードしたファームウェアファイルが現在のバージョンと異なるバージョンの場合は、自動的に再起動

23.1.5.2 ファームウェアのみを対象とする ZTP の動作例

ファームウェアのみを対象として ZTP を動作させる場合は、DHCP サーバーでファームウェアファイル名のみを提供できるように準備しておく必要があります。

ファームウェアのみを対象として ZTP を動作させる場合の構成例と動作例を以下に示します。この例では、DHCP サーバー（10.1.1.101）と TFTP サーバー（10.1.1.201）を同一セグメントに配置しています。

図 23-7 ファームウェアのみを対象とする ZTP 動作例



この動作例のコンソールログ、および LED の点滅について、以下に示します。

```
 (1)
Press any key to login...


 Start ZTP, lock CLI for process!
 Exit ZTP process by CTRL+C.

(2)
 Try to download image from TFTP://10.1.1.201/test-firmware.had.......
 Accessing tftp:...
 Transmission start...
 Transmission finished, file length 7102392 bytes.Done
 Please wait, programming flash for save image...Done.
(3)
 DHCP does not specify CFG File name.
 Set /c:/test-firmware.had as boot image OK.
 ZTP process OK.

(4)
 Reboot system, please wait......
```

各項目の説明は、以下のとおりです。

表 23-7 ファームウェアのみを対象とする ZTP 動作例のコンソールログの説明

項番	説明
(1)	［LED［10］点滅］ DHCP サーバーからの情報取得中

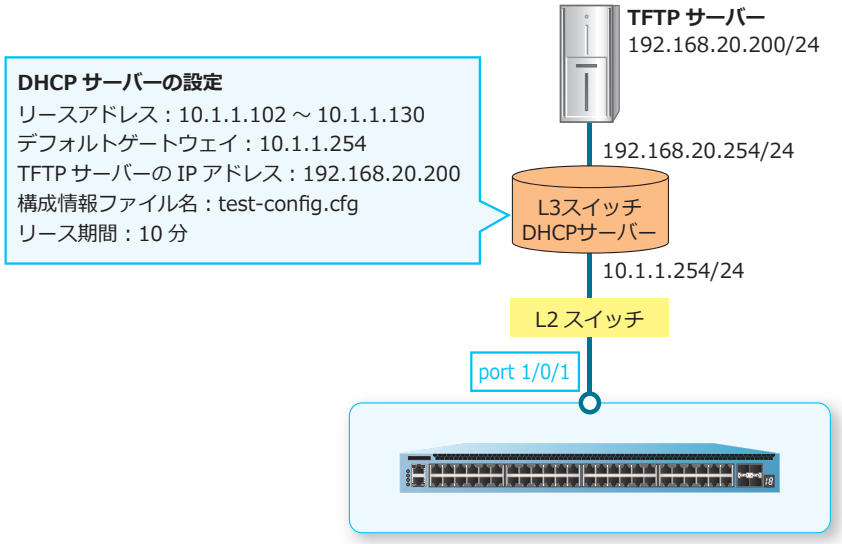
項番	説明
(2)	［LED［11］点滅］ TFTP サーバーからファームウェアファイルをダウンロード中
(3)	［LED［13］点滅］ ダウンロードしたファイルの反映中
(4)	ダウンロードしたファームウェアファイルが現在のバージョンと異なるバージョンの場合は、自動的に再起動

23.1.5.3 構成情報のみを対象とする ZTP の動作例

構成情報のみを対象として ZTP を動作させる場合は、DHCP サーバーで構成情報ファイル名のみを提供できるように準備しておく必要があります。

構成情報のみを対象として ZTP を動作させる場合の構成例と動作例を以下に示します。この例では、DHCP サーバー（10.1.1.254）を同一セグメントに、TFTP サーバーを別セグメント（192.168.20.200）に配置しています。

図 23-8 構成情報のみを対象とする ZTP 動作例



この動作例のコンソールログ、および LED の点滅について、以下に示します。

```
 (1)
Press any key to login...


 Start ZTP, lock CLI for process!
 Exit ZTP process by CTRL+C.

(2)
 Try to download configure from TFTP://192.168.20.200/test-config.cfg.......
 Accessing tftp:...
 Transmission start...
 Transmission finished, file length 2160 bytes.Done
(3)
 Please wait, save configure to file test-config.cfg ...      Done.
 Set /c:/test-config.cfg as boot configure OK.
 ZTP process OK.
 ZTP OK: Unlock CLI and use config from TFTP.
```

各項目の説明は、以下のとおりです。

表 23-8 構成情報のみを対象とする ZTP 動作例のコンソールログの説明

項番	説明
(1)	［LED［10］点滅］ DHCP サーバーからの情報取得中
(2)	［LED［12］点滅］ TFTP サーバーから構成情報ファイルをダウンロード中
(3)	［LED［13］点滅］ ダウンロードしたファイルの反映中

23.2 ZTP の状態確認

show ztp コマンドで、ZTP の状態を確認できます。

> ***NOTE:*** 複数の TFTP サーバーの IP アドレスを取得して ZTP が動作した場合は、**show ztp** コマンドの ZTP Process Result には、最後にダウンロードを試した TFTP サーバーでの結果が表示されます。それ以外の TFTP サーバーでの失敗理由は、ログを参照してください。

NP2000 の 1.09.01 の場合の表示例を以下に示します。

```
# show ztp

ZTP Bootup State      : Enabled ...(1)
ZTP Current State     : Enabled Force ...(2)
Current Firmware      : /c:/test-firmware.had ...(3)
Current Configure     : /c:/test-config.cfg ...(4)

Result of last time: ...(5)
  ZTP Process Result    : - ...(6)
  DHCP Server           : - ...(7)
  DHCP Discover Retry   : - ...(8)
  TFTP Server           : - ...(9)
  Gateway IP address    : - ...(10)
  Download Firmware     : - ...(11)
  Download Configure    : - ...(12)
  Download Other Files  : - ...(13)
  SNMP Server Address 1: - ...(14)
  SNMP Comminity Name 1: - ...(15)
  SNMP Server Version 1: - ...(16)
  SNMP Server Address 2: - ...(17)
  SNMP Comminity Name 2: - ...(18)
  SNMP Server Version 2: - ...(19)

Result of this time: ...(20)
  ZTP Process Result    : Success (Same image) ...(6)
  DHCP Server           : 10.1.1.101 ...(7)
  DHCP Discover Retry   : 0 ...(8)
  TFTP Server           : 192.168.20.200 ...(9)
  Gateway IP address    : 10.1.1.254 ...(10)
  Download Firmware     : //192.168.20.200/test-firmware.had ...(11)
  Download Configure    : //192.168.20.200/test-config.cfg ...(12)
  Download Other Files  : - ...(13)
  SNMP Server Address 1: 10.1.1.200 ...(14)
  SNMP Comminity Name 1: public ...(15)
  SNMP Server Version 1: 2c ...(16)
  SNMP Server Address 2: - ...(17)
  SNMP Comminity Name 2: - ...(18)
  SNMP Server Version 2: - ...(19)
```

各項目の説明は、以下のとおりです。

表 23-9 `show ztp` コマンドの表示項目

項番	説明
(1)	起動時の ZTP 設定を表示します。 【NP4000、NP2000 の場合】 Enabled：ztp enable 設定 Enabled Force：ztp enabe force 設定 Disabled：no ztp enable 設定 【NP3000、NP2100、NP2500 の場合】 Enabled Force Slide Switch：ZTP スイッチが ON 状態で ztp enable 設定 Enabled Force：ztp enabe force 設定 Disabled：以下のいずれかの状態 ・ZTP スイッチが OFF 状態で ztp enable 設定 ・ZTP スイッチが OFF 状態で no ztp enable 設定 ・ZTP スイッチが ON 状態で no ztp enable 設定
(2)	現在の ZTP 設定を表示します。表示内容は項番 (1) を参照してください。
(3)	現在のプライマリーブートイメージファイル設定を表示します。
(4)	現在のプライマリー構成情報ファイル設定を表示します。
(5)	前回の ZTP の動作結果を表示します。
(6)	ZTP の動作結果を表示します。 • Success：ZTP が動作成功 • Success (Same image)：ZTP が動作成功（ファームウェアファイルが同じバージョン） • Not default config：ztp enable 設定で、startup-config が工場出荷状態以外のため ZTP 未動作 • interrupted ZTP processing from console：コンソールから Ctrl+C キーで ZTP 中断 • SD-card boot：SD カードブートで起動したため ZTP 未動作 • Fail (DHCP connection timeout)：DHCP サーバーから応答なし • Fail (DHCP <ip-address> : TFTP Server information was not found):TFTP サーバーの IP アドレスを未取得 • Fail (DHCP no gateway IP address)：TFTP サーバーが別セグメントの場合に、デフォルトゲートウェイの IP アドレスを未取得 • Fail (TFTP server ARP no reply)：TFTP サーバー、またはデフォルトゲートウェイの ARP 解決に失敗 【各種ファイルの取得失敗時の表示】 XX はファイル種別ごとに表示が異なります。ファイル種別は、IMAGE（ファームウェアファイル）、CONFIG（構成情報ファイル）、OTHER（その他のファイル）で、OTHER は NP4000 の 1.03.01 以降、NP2100 の 1.09.02 以降、NP2000 の 1.09.01 以降で表示されます。 • Fail (XX <file> file name size over)：ファイル名が 33 文字以上 • Fail (XX <file> TFTP connection failed)：TFTP サーバーへの接続に失敗 • Fail (XX <file> file not found)：指定ファイルが TFTP サーバーに存在しない（TFTP Error Codes 1 を受信） • Fail (XX <file> file access error)：指定ファイルにアクセス失敗（TFTP Error Codes 1 以外を受信） • Fail (XX <file> TFTP timeout)：転送途中にタイムアウト発生 • Fail (XX <file> invalid file)：ダウンロードしたファイルが不適切 • Fail (XX <file> disk full or allocation exceeded)：フラッシュメモリーの空き容量不足で保存に失敗 • Fail (XX <file> flash access error)：フラッシュメモリーへの書き込みアクセスに失敗
(7)	DHCP サーバーの IP アドレスを表示します。

項番	説明
(8)	DHCP Discover メッセージを再送した回数を表示します。
(9)	TFTP サーバーの IP アドレスを表示します。
(10)	デフォルトゲートウェイの IP アドレスを表示します。
(11)	ファームウェアファイル名を表示します。
(12)	構成情報ファイル名を表示します。
(13)	ダウンロード一覧ファイル情報を表示します。 NP4000 の 1.03.01 以降、NP2100 の 1.09.02 以降、NP2000 の 1.09.01 以降で表示されます。
(14)	ZTP 処理中の SNMP トラップ用 宛先 IP アドレス情報 (1) を表示します。 NP4000 の 1.03.01 以降、NP2100 の 1.09.02 以降、NP2000 の 1.09.01 以降で表示されます。
(15)	ZTP 処理中の SNMP トラップ用 SNMP コミュニティー名情報 (1) を表示します。 NP4000 の 1.03.01 以降、NP2100 の 1.09.02 以降、NP2000 の 1.09.01 以降で表示されます。
(16)	ZTP 処理中の SNMP トラップ用 SNMP バージョン情報 (1) を表示します。 NP4000 の 1.03.01 以降、NP2100 の 1.09.02 以降、NP2000 の 1.09.01 以降で表示されます。
(17)	ZTP 処理中の SNMP トラップ用 宛先 IP アドレス情報 (2) を表示します。 NP4000 の 1.03.01 以降、NP2100 の 1.09.02 以降、NP2000 の 1.09.01 以降で表示されます。
(18)	ZTP 処理中の SNMP トラップ用 SNMP コミュニティー名情報 (2) を表示します。 NP4000 の 1.03.01 以降、NP2100 の 1.09.02 以降、NP2000 の 1.09.01 以降で表示されます。
(19)	ZTP 処理中の SNMP トラップ用 SNMP バージョン情報 (2) を表示します。 NP4000 の 1.03.01 以降、NP2100 の 1.09.02 以降、NP2000 の 1.09.01 以降で表示されます。
(20)	今回の ZTP の動作結果を表示します。

24. タイムレンジ

タイムレンジの機能、状態の確認方法、および構成例と設定例について説明します。

REF: コマンドの詳細については、『コマンドリファレンス』を参照してください。

24.1 タイムレンジの機能説明

タイムレンジは、期間を定義する機能です。以下の 2 種類の方法で設定できます。

- daily 指定：「開始時刻」と「終了時刻」を設定可能
- weekly 指定：「開始曜日・時刻」と「終了曜日・時刻」を設定可能

定義したタイムレンジを使用して、適用した対象機能の ON/OFF をスケジューリングできるようになります。タイムレンジを適用できる対象機能を以下に示します。

表 24-1 タイムレンジ対象機能

対象機能	対象機種と対象バージョン
タイムベース PoE	• ApresiaNP2100-24T4X-PoE（1.09.02 以降） • ApresiaNP2100-48T4X-PoE（1.09.02 以降） • ApresiaNP2000-24T4X-PoE（1.09.01 以降） • ApresiaNP2000-48T4X-PoE（1.09.01 以降） • ApresiaNP2500-8MT4X-PoE（1.10.01 以降） • ApresiaNP2500-16MT4X-PoE（1.10.01 以降）

タイムレンジプロファイルを作成するには、**time-range** コマンドを使用します。指定したタイムレンジプロファイルにおいてタイムレンジを設定するには、**periodic** コマンドを使用します。

CAUTION: 対象機能が有効／無効になる時刻は、タイムレンジで指定した開始時刻および終了時刻から最大 60 秒遅れる場合があります。

NOTE: **periodic** コマンドによるタイムレンジの設定は、装置全体で最大 64 個設定できます。

NOTE: 1 つのタイムレンジプロファイルに複数のタイムレンジを設定できますが、指定範囲が重複している場合は、動作がマージされます。

24.2 タイムレンジの状態確認

show time-range コマンドで、タイムレンジの状態を確認できます。

表示例を以下に示します。

```
# show time-range

Time Range Profile: ip-phone ...(1)
Daily 09:00 to 19:00 ...(2)

Time Range Profile: other_device ...(1)
Weekly Monday     07:00 to Friday     23:00 ...(2)

Total Entries: 2
```

各項目の説明は、以下のとおりです。

表 24-2 show time-range コマンドの表示項目

項番	説明
(1)	タイムレンジプロファイル名を表示します。
(2)	タイムレンジを表示します。

24.3 タイムレンジの構成例と設定例

タイムレンジを利用する場合の構成例と設定例を示します。

24.3.1 daily 指定のタイムレンジプロファイルの設定例

タイムレンジプロファイル［test-daily］において、daily 指定のタイムレンジを以下の内容で設定する場合の設定例を示します。

- 開始時刻［09:45］、終了時刻［15:15］
- 開始時刻［16:45］、終了時刻［22:15］

1. タイムレンジプロファイル［test-daily］を設定します。

```
sw1# configure terminal
sw1(config)# time-range test-daily
sw1(config-time-range)#
```

2. タイムレンジプロファイル［test-daily］において、daily 指定で以下のタイムレンジを設定します。

開始時刻［09:45］、終了時刻［15:15］

開始時刻［16:45］、終了時刻［22:15］

```
sw1(config-time-range)# periodic daily 09:45 to 15:15
sw1(config-time-range)# periodic daily 16:45 to 22:15
sw1(config-time-range)# end
sw1#
```

3. 実施後のタイムレンジプロファイル［test-daily］を確認します。

```
sw1# show time-range test-daily

Time Range Profile: test-daily
Daily 09:45 to 15:15
Daily 16:45 to 22:15
```

24.3.2 weekly 指定のタイムレンジプロファイルの設定例

タイムレンジプロファイル［test-weekly］において、weekly 指定のタイムレンジを以下の内容で設定する場合の設定例を示します。

- 開始曜日・時刻［月曜日 1:00］、終了曜日・時刻［金曜日 23:00］
- 開始曜日・時刻［土曜日 6:00］、終了曜日・時刻［土曜日 13:00］

1. タイムレンジプロファイル［test-weekly］を設定します。

```
sw1# configure terminal
sw1(config)# time-range test-weekly
sw1(config-time-range)#
```

2. タイムレンジプロファイル［test-weekly］において、weekly 指定で以下のタイムレンジを設定します。

開始曜日・時刻［月曜日 1:00］、終了曜日・時刻［金曜日 23:00］

開始曜日・時刻［土曜日 6:00］、終了曜日・時刻［土曜日 13:00］

```
sw1(config-time-range)# periodic weekly monday 01:00 to friday 23:00
sw1(config-time-range)# periodic weekly saturday 06:00 to saturday 13:00
sw1(config-time-range)# end
sw1#
```

3. 実施後のタイムレンジプロファイル［test-weekly］を確認します。

```
sw1# show time-range test-weekly

Time Range Profile: test-weekly
Weekly Monday     01:00 to Friday     23:00
Weekly Saturday   06:00 to Saturday   13:00
```

25. Web アクセス拒否通知

Web アクセス拒否通知の機能、および構成例と設定例について説明します。

REF: コマンドの詳細については、『コマンドリファレンス』を参照してください。

25.1 Web アクセス拒否通知の機能説明

Web アクセス拒否通知は、特定端末からの Web アクセスを拒否し、端末に対して拒否されたことを示す Web ページを応答する機能です。

対象端末は、拡張エキスパートアクセスリストで以下のように設定します。

- web-deny-notify tcp 指定で設定。
- 送信元 IPv4 アドレス、または送信元 MAC アドレス条件は host 指定で特定端末を設定。マスク指定は未サポート。
- 宛先 IPv4 アドレス条件と宛先 MAC アドレス条件は any で設定。
- 宛先 TCP ポート番号は、web-deny-notify http-port（デフォルト 80）、および web-deny-notify https-port（デフォルト 443）で指定された宛先 TCP ポート番号と一致するように設定。

web-deny-notify で設定したルールにマッチした IPv4 パケットは、CPU 宛てにリダイレクトされるようになります。対象端末からのそれ以外のトラフィック中継も制限する場合は、web-deny-notify で指定したルールよりも後にマッチするシーケンス番号で、deny ルールを設定してください。

NOTE: Web アクセス拒否通知機能は、NP2100 の 1.09.02 以降、NP2000 の 1.09.01 以降、NP2500 の 1.10.01 以降でサポートしています。

NOTE: 拡張エキスパートアクセスリストの対象は、IPv4 パケットです。

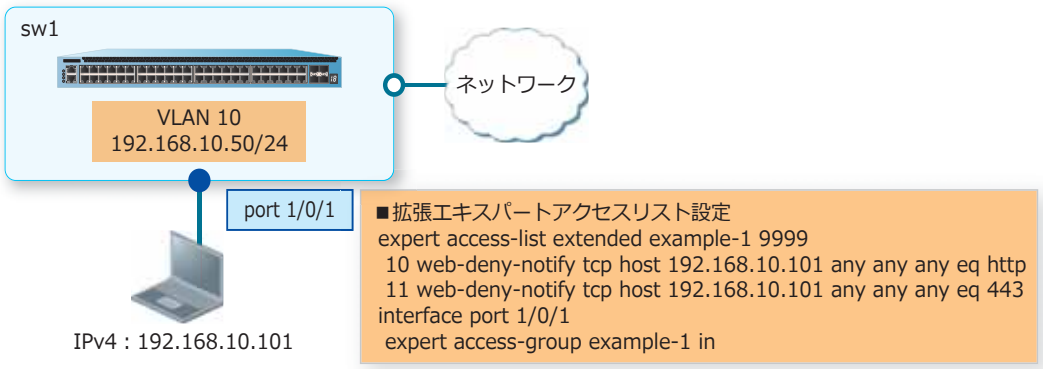
NOTE: Web アクセス拒否通知は、IPv4 アドレスでの使用をサポートしています。IPv6 アドレスには対応していません。

NOTE: Web アクセス拒否通知を使用する場合は、IPv4 アドレスを設定した任意の VLAN インターフェースを少なくとも 1 つ作成してください。また、IPv4 アドレスを設定した VLAN インターフェースが 1 つもアップしていない場合、Web アクセス拒否通知ページは応答できません。

25.1.1 対象 VLAN の実 IPv4 アドレスを利用する方法

対象端末が所属する VLAN の VLAN インターフェースに IPv4 アドレスを設定し、その IPv4 アドレスで応答処理をする場合の使用例を示します。

図 25-1 対象 VLAN の実 IPv4 アドレスを利用する場合



この例の場合、IPv4 アドレスが 192.168.10.101 の端末から HTTP（80）アクセスをポート 1/0/1 で受信すると、シーケンス番号 10 のルールにマッチするため、HTTP（80）アクセスは CPU 宛てに中継されます。
また、Web アクセス拒否通知ページ「http://192.168.10.50/www/web-deny-notify.html」にリダイレクトするよう、装置から応答が返されます。

同様に、IPv4 アドレスが 192.168.10.101 の端末から HTTPS（443）アクセスをポート 1/0/1 で受信すると、シーケンス番号 11 のルールにマッチするため、HTTPS（443）アクセスは CPU 宛てに中継されます。
また、Web アクセス拒否通知ページ「https://192.168.10.50/www/web-deny-notify.html」にリダイレクトするよう、装置から応答が返されます。

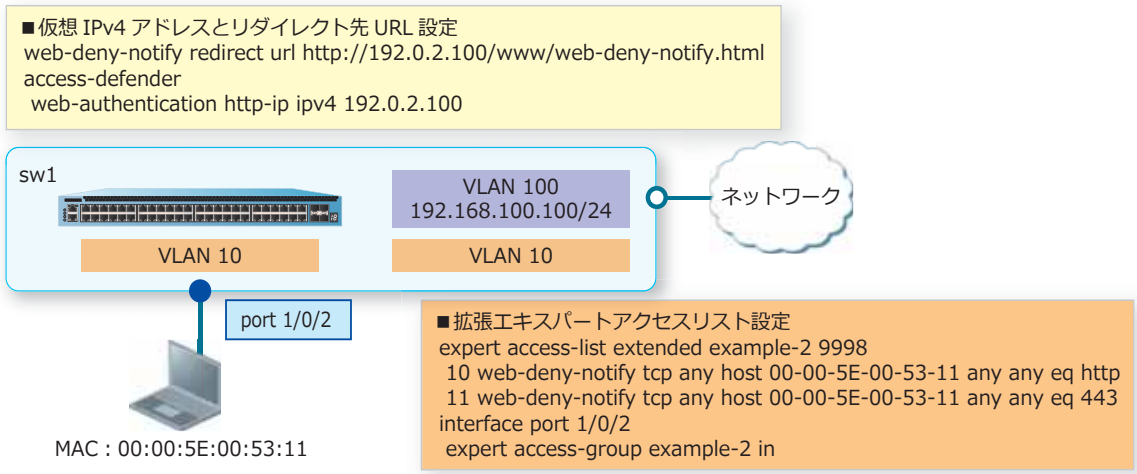
25.1.2 仮想 IPv4 アドレスを利用する方法

Web 認証の **web-authentication http-ip ipv4** コマンドを利用して仮想 IPv4 アドレスを設定し、その仮想 IPv4 アドレスで応答処理をする場合の使用例を示します。この場合は、**web-deny-notify redirect url** コマンドで、リダイレクト先 URL を以下のいずれかに設定する必要があります。

- http://「**web-authentication http-ip ipv4** コマンドの設定値」:「**web-deny-notify http-port** コマンドの設定値」/www/web-deny-notify.html
- https://「**web-authentication http-ip ipv4** コマンドの設定値」:「**web-deny-notify https-port** コマンドの設定値」/www/web-deny-notify.html

NOTE: リダイレクト先が装置の Web アクセス拒否通知ページの場合の「/www/web-deny-notify.html」は、装置内部の設定値を参照しており、変更できません。

図 25-2 対象 VLAN の実 IPv4 アドレスを利用する場合



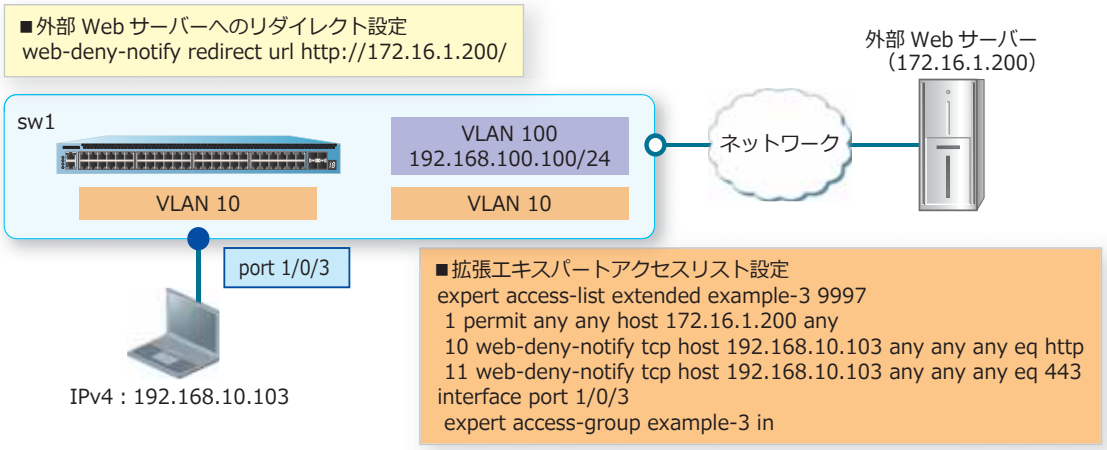
この例の場合、MAC アドレスが 00:00:5E:00:53:11 の端末から HTTP（80）アクセスをポート 1/0/2 で受信すると、シーケンス番号 10 のルールにマッチするため、HTTP（80）アクセスは CPU 宛てに中継されます。
また、Web アクセス拒否通知ページ「http://192.0.2.100/www/web-deny-notify.html」にリダイレクトするよう、装置から応答が返されます。

同様に、MAC アドレスが 00:00:5E:00:53:11 の端末から HTTPS（443）アクセスをポート 1/0/2 で受信すると、シーケンス番号 11 のルールにマッチするため、HTTPS（443）アクセスは CPU 宛てに中継されます。
また、Web アクセス拒否通知ページ「http://192.0.2.100/www/web-deny-notify.html」にリダイレクトするよう、装置から応答が返されます。

25.1.3 外部 Web サーバーにリダイレクトする方法

Web アクセス拒否通知ページを外部 Web サーバーに用意してリダイレクトする場合の使用例を示します。この場合は、拡張エキスパートアクセスリストの web-deny-notify で指定したルールよりも先にマッチするシーケンス番号で、外部 Web サーバー宛ての通信を permit または permit authentication-bypass で許可してください。

図 25-3 外部 Web サーバーにリダイレクトする場合



この例の場合、IPv4 アドレスが 192.168.10.103 の端末から HTTP（80）アクセスをポート 1/0/3 で受信すると、シーケンス番号 10 のルールにマッチするため、HTTP（80）アクセスは CPU 宛てに中継されます。
また、Web アクセス拒否通知ページ「http://172.16.1.200/」にリダイレクトするよう、装置から応答が返されます。

同様に、IPv4 アドレスが 192.168.10.103 の端末から HTTPS（443）アクセスをポート 1/0/3 で受信すると、シーケンス番号 11 のルールにマッチするため、HTTPS（443）アクセスは CPU 宛てに中継されます。
また、Web アクセス拒否通知ページ「http://172.16.1.200/」にリダイレクトするよう、装置から応答が返されます。

25.1.4 Web アクセス拒否通知ページのカスタマイズ

カスタマイズした Web アクセス拒否通知ページを装置にダウンロードするには、**copy** コマンドで web-access-deny-page パラメーターを指定して実施します。

装置にダウンロードしたカスタマイズした Web アクセス拒否通知ページを削除するには、**access-defender erase web-access-deny-page** コマンドを使用します。

> ***CAUTION:*** Web アクセス拒否通知ページでは、Web 認証ページ用として装置にダウンロードできる画像ファイル（webpage-image01 ～ webpage-image10）は使用できません。

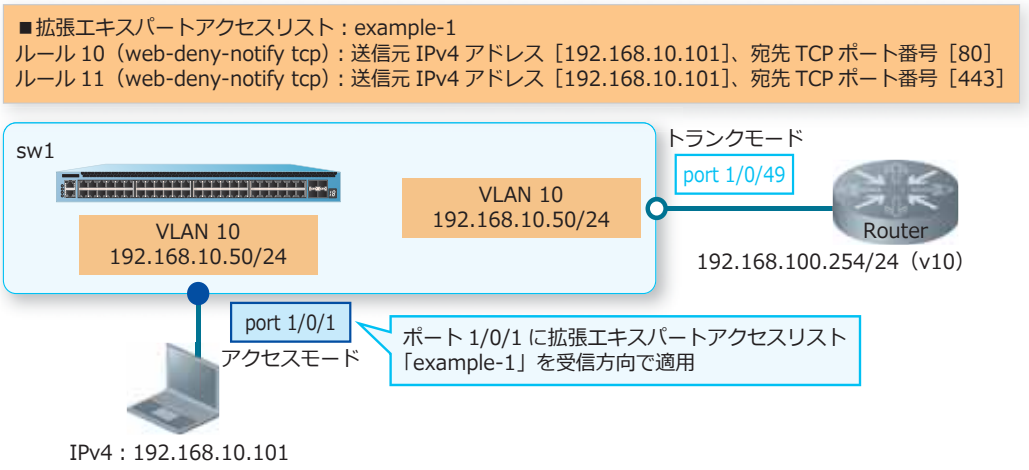
25.2 Web アクセス拒否通知の構成例と設定例

Web アクセス拒否通知の構成例と設定例を示します。

25.2.1 Web アクセス拒否通知の設定例（実 IPv4 アドレス）

Web アクセス拒否通知の対象端末が所属する VLAN の VLAN インターフェースに IPv4 アドレスが設定されていて、その IPv4 アドレスで応答処理をする場合の構成例と設定例を示します。

図 25-4 Web アクセス拒否通知の構成例（実 IPv4 アドレス）



1. VLAN 10 を作成し、構成例のように VLAN を割り当てます。

```
sw1# configure terminal
sw1(config)# vlan 10
sw1(config-vlan)# exit
sw1(config)#
sw1(config)# interface port 1/0/1
sw1(config-if-port)# switchport mode access
sw1(config-if-port)# switchport access vlan 10
sw1(config-if-port)# exit
sw1(config)#
sw1(config)# interface port 1/0/49
sw1(config-if-port)# switchport mode trunk
sw1(config-if-port)# switchport trunk allowed vlan 10
sw1(config-if-port)# exit
sw1(config)#
```

2. VLAN 10 インターフェースに IPv4 アドレス［192.168.10.50/24］を設定します。

```
sw1(config)# interface vlan 10
sw1(config-if-vlan)# ip address 192.168.10.50/24
sw1(config-if-vlan)# exit
sw1(config)#
```

3. Web アクセス拒否通知のための拡張エキスパートアクセスリスト［example-1］を作成し、以下のルールを設定します。

ルール 10（web-deny-notify tcp）：送信元 IPv4 アドレス［192.168.10.101］、宛先 TCP ポート番号［80］

ルール 11（web-deny-notify tcp）：送信元 IPv4 アドレス［192.168.10.101］、宛先 TCP ポート番号［443］

```
sw1(config)# expert access-list extended example-1
sw1(config-exp-nacl)# 10 web-deny-notify tcp host 192.168.10.101 any any any eq 80
sw1(config-exp-nacl)# 11 web-deny-notify tcp host 192.168.10.101 any any any eq 443
sw1(config-exp-nacl)# exit
sw1(config)#
```

4. 設定したアクセスリストをポート 1/0/1 に適用します。

```
sw1(config)# interface port 1/0/1
sw1(config-if-port)# expert access-group example-1 in
sw1(config-if-port)# end
sw1#
```

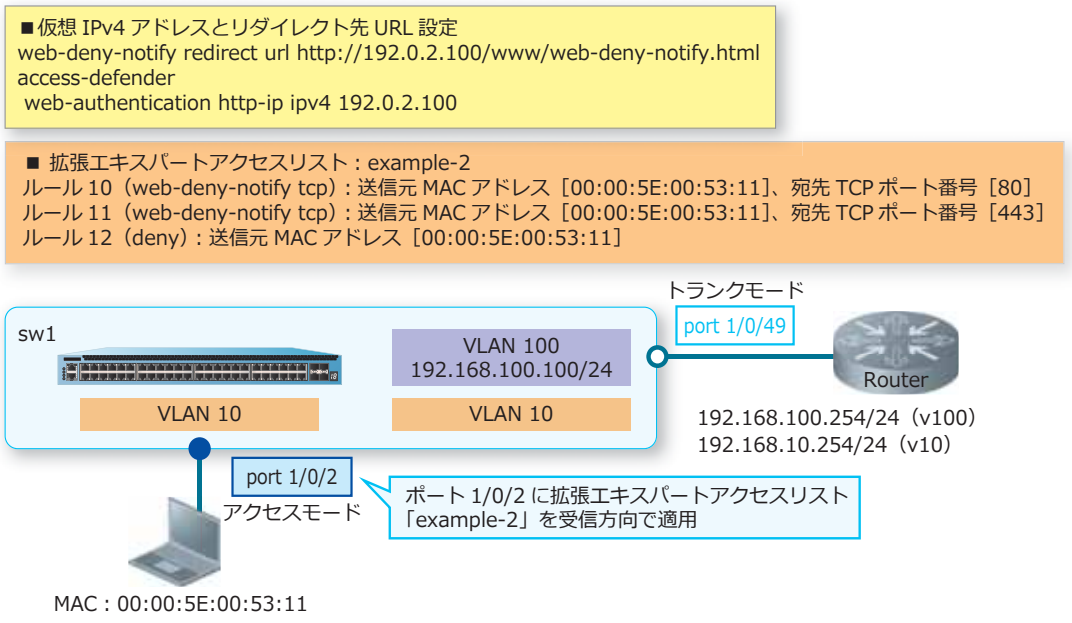
5. 実施後の Web アクセス拒否通知関連の設定を以下に抜粋します。

```
# ACL

expert access-list extended example-1 9999
 10 web-deny-notify tcp host 192.168.10.101 any any any eq http
 11 web-deny-notify tcp host 192.168.10.101 any any any eq 443
interface port 1/0/1
 expert access-group example-1 in
```

25.2.2 Web アクセス拒否通知の設定例（仮想 IPv4 アドレス）

Web 認証の **web-authentication http-ip ipv4** コマンドを利用して仮想 IPv4 アドレスを設定し、その仮想 IPv4 アドレスで応答処理をする場合の構成例と設定例を示します。また、この設定例では、対象端末からの IPv4 パケットを破棄する deny ルールも設定しています。

図 25-5 Web アクセス拒否通知の構成例（仮想 IPv4 アドレス）



1. VLAN 10、VLAN 100 を作成し、構成例のように VLAN を割り当てます。

```
sw1# configure terminal
sw1(config)# vlan 10,100
sw1(config-vlan)# exit
sw1(config)#
sw1(config)# interface port 1/0/2
sw1(config-if-port)# switchport mode access
sw1(config-if-port)# switchport access vlan 10
sw1(config-if-port)# exit
sw1(config)#
sw1(config)# interface port 1/0/49
sw1(config-if-port)# switchport mode trunk
sw1(config-if-port)# switchport trunk allowed vlan 10,100
sw1(config-if-port)# exit
sw1(config)#
```

2. VLAN 100 インターフェースに管理用 IPv4 アドレス［192.168.100.100/24］を設定します。

```
sw1(config)# interface vlan 100
sw1(config-if-vlan)# ip address 192.168.100.100/24
sw1(config-if-vlan)# exit
sw1(config)#
```

3. Web 認証の **web-authentication http-ip ipv4** コマンドを利用して仮想 IPv4 アドレス［192.0.2.100］を設定します。

```
sw1(config)# access-defender
sw1(config-a-def)# web-authentication http-ip ipv4 192.0.2.100
sw1(config-a-def)# exit
sw1(config)#
```

4. Web アクセス拒否通知のためのリダイレクト先 URL を［http://192.0.2.100/www/web-deny-notify.html］に設定します。

```
sw1(config)# web-deny-notify redirect url http://192.0.2.100/www/web-deny-notify.html
sw1(config)#
```

5. Web アクセス拒否通知のための拡張エキスパートアクセスリスト［example-2］を作成し、以下のルールを設定します。

ルール 10（web-deny-notify tcp）：送信元 MAC アドレス［00:00:5E:00:53:11］、宛先 TCP ポート番号［80］

ルール 11（web-deny-notify tcp）：送信元 MAC アドレス［00:00:5E:00:53:11］、宛先 TCP ポート番号［443］

ルール 12（deny）：送信元 MAC アドレス［00:00:5E:00:53:11］

```
sw1(config)# expert access-list extended example-2
sw1(config-exp-nacl)# 10 web-deny-notify tcp any host 0000.5e00.5311 any any eq 80
sw1(config-exp-nacl)# 11 web-deny-notify tcp any host 0000.5e00.5311 any any eq 443
sw1(config-exp-nacl)# 12 deny any host 0000.5e00.5311 any any
sw1(config-exp-nacl)# exit
sw1(config)#
```

6. 設定したアクセスリストをポート 1/0/2 に適用します。

```
sw1(config)# interface port 1/0/2
sw1(config-if-port)# expert access-group example-2 in
sw1(config-if-port)# end
sw1#
```

7. 実施後の Web アクセス拒否通知関連の設定を以下に抜粋します。

```
# ACL

expert access-list extended example-2 9999
 10 web-deny-notify tcp any host 00-00-5E-00-53-11 any any eq http
 11 web-deny-notify tcp any host 00-00-5E-00-53-11 any any eq 443
 12 deny any host 00-00-5E-00-53-11 any any
interface port 1/0/2
 expert access-group example-2 in

# WEB-AUTHENTICATION

web-deny-notify redirect url http://192.0.2.100/www/web-deny-notify.html
access-defender
 web-authentication http-ip ipv4 192.0.2.100
```