第 4 編 レイヤー 2

1. レイヤー 2 基本機能

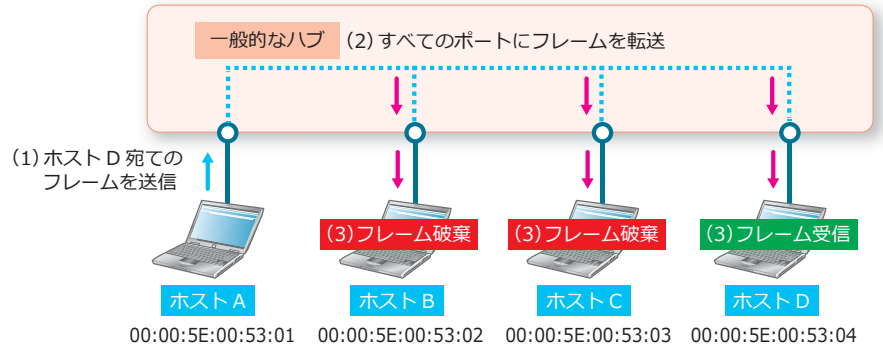
イーサネットでのレイヤー 2 スイッチとしての基本機能、MAC アドレス学習、およびジャンボフレームの機能、状態の確認方法、および構成例と設定例について説明します。

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。

1.1 レイヤー 2 基本機能の機能説明

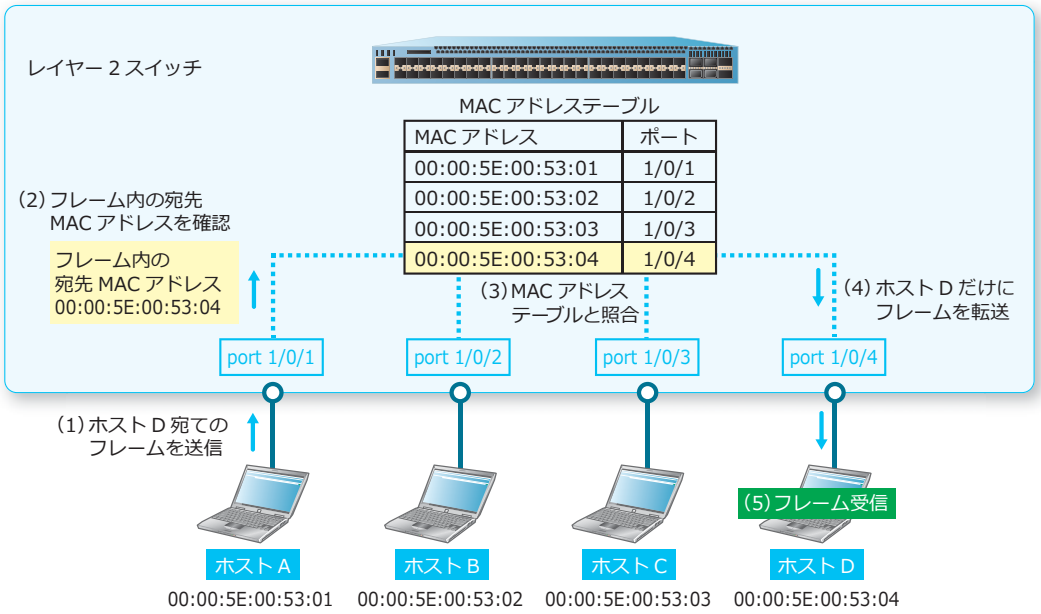
ローカルエリアネットワークでは主にイーサネットが利用されており、**フレーム**という単位でデータを送受信します。一般的なハブでは受信したフレームをすべてのホストに中継し、ホストでは宛先が自装置ではないフレームは破棄します。つまり、一般的なハブでは帯域を無駄に消費していることになります。

図 1-1 一般的なハブによるフレームの送受信



レイヤー 2 スイッチでは、**MAC アドレステーブル**に登録された情報（MAC アドレス、接続ポート、VLAN）を基に宛先のホストだけに中継します。これにより、帯域を効率よく利用できます。

図 1-2 レイヤー 2 スイッチによるフレームの送受信



1.1.1 MAC アドレステーブルの更新

レイヤー 2 スイッチは、フレームを受信すると送信元 MAC アドレスを学習して MAC アドレステーブルに登録します。登録済みエントリーからのフレームを受信すると、そのエントリーが削除されるまでの時間が更新されます。また、同一 VLAN の異なるポートで登録済みエントリーからのフレームを受信すると、接続ポート情報が更新されます。なお、VLAN が異なる場合は同じ MAC アドレスでも別エントリーとして扱われます。

また、送信元 MAC アドレスが一致する場合だけでなく、宛先 MAC アドレスが一致する場合に対象エントリーが削除されるまでの時間を更新することもできます。宛先 MAC アドレスによる更新機能は、デフォルト設定では無効です。有効にするには、**`mac-address-table aging destination-hit`** コマンドを使用します。

1.1.2 MAC アドレス学習の有効／無効

デフォルト設定では、すべてのポートで MAC アドレス学習は有効ですが、物理ポートごとに MAC アドレス学習を無効にできます。なお、ポートチャネルで MAC アドレス学習を無効にする場合は、ポートチャネルのすべてのメンバーポートで無効にしてください。

MAC アドレス学習の有効／無効を設定するには、**`mac-address-table learning`** コマンドを使用します。

1.1.3 スタティック MAC アドレスエントリー

MAC アドレステーブルには、スタティックに MAC アドレスエントリーを設定できます。スタティック MAC アドレスエントリーとして、以下の 3 種類のエントリーを設定できます。

- ユニキャスト MAC アドレス宛てのエントリー
- drop パラメーター指定のエントリー
- マルチキャスト MAC アドレス宛てのエントリー

ユニキャスト MAC アドレス宛てのスタティック MAC アドレスエントリーの場合、指定した VLAN で宛先 MAC アドレスが一致するフレームを受信した場合に、指定したインターフェースに中継されます。

drop パラメーター指定のスタティック MAC アドレスエントリーの場合、指定した VLAN で、宛先 MAC アドレスまたは送信元 MAC アドレスが指定した MAC アドレス（ユニキャスト MAC アドレスのみ指定可能）と一致するフレームを受信すると、中継されずに破棄されます。

マルチキャスト MAC アドレス宛てのスタティック MAC アドレスエントリーの場合、指定した VLAN で宛先 MAC アドレスが一致するフレームを受信した場合に、指定したインターフェース（複数指定可能）に中継されます。

スタティック MAC アドレスエントリーの最大設定数を以下に示します。

表 1-1 スタティック MAC アドレスエントリーの最大設定数

対象機種	ユニキャスト MAC アドレス宛て	drop 指定	マルチキャスト MAC アドレス宛て
NP7000 1.10.01 以降、NP5000 1.09.01 以降	2,048	2,048	128
NP7000 1.10.01 より前のバージョン NP5000 1.09.01 より前のバージョン	256	256	128
NP3000 1.10.01 以降	2,048	2,048	1,024

対象機種	ユニキャスト MAC アドレス宛て	drop 指定	マルチキャスト MAC アドレス宛て
NP3000 1.10.01 より前のバージョン	2,048	256	1,024
NP4000、NP2100、NP2000、NP2500	256	256	128

スタティック MAC アドレスエントリーを設定するには、**mac-address-table static** コマンドを使用します。

1.1.4 MAC アドレステーブルのエージングタイム

MAC アドレステーブルに登録されたエントリーは、エージングタイムとして設定した時間内のみ保持されます。エージングタイム内に送信元 MAC アドレスが一致するフレームを受信しなかった場合、そのエントリーは削除されます。

MAC アドレステーブルのエージングタイムは、デフォルト設定では 300 秒です。エージングタイムを設定するには、**mac-address-table aging-time** コマンドを使用します。なお、エージングタイムとして 0 秒を指定した場合は、エージングタイムアウトによる削除が無効化されます。

> ***NOTE:*** 実際に MAC アドレステーブルからエントリーが削除されるまでの時間は、設定値～設定値 ×2 になります。

1.1.5 ダイナミック MAC アドレスエントリーの削除

学習して MAC アドレステーブルに登録されたダイナミック MAC アドレスエントリーは、手動コマンドで削除することもできます。すべてのダイナミック MAC アドレスエントリーの削除だけでなく、MAC アドレス指定の削除、ポート指定の削除、VLAN 指定の削除も可能です。

ダイナミック MAC アドレスエントリーを削除するには、**clear mac-address-table** コマンドを使用します。

1.1.6 インターフェースへの説明の追加

インターフェースに説明を追加する場合、説明文を指定して **description** コマンドを使用します。

1.1.7 ポートのカウンターのクリア

ポート（物理ポート、CPU ポート）のカウンターをクリアするには、**clear counters** コマンドを使用します。

1.1.8 インターフェースの無効化

インターフェースは、デフォルト設定では有効です。インターフェースを無効にするには、インターフェースの設定モードで **shutdown** コマンドを使用します。

> ***CAUTION:*** **shutdown** コマンドを実行した場合、1 つのポートを無効化するために数百ミリ秒の時間を要します。そのため、同時に複数ポートに対して **shutdown** コマンドを実行した場合、すべてのポートの無効化が完了するまでに数秒から数十秒程度の時間を要します。

1.1.9 レイヤー 2 VLAN インターフェース

レイヤー 2 VLAN インターフェースは、**interface l2vlan** コマンドでインターフェース設定モードに遷移し、**description** コマンドでインターフェースの説明を設定する場合にのみ使用します。**show interfaces description** コマンドでインターフェースの説明を確認できます。

vlan コマンドで VLAN を作成すると対応するレイヤー 2 VLAN インターフェースも作成されますが、**description** コマンドを設定していない状態では、構成情報に interface l2vlan は表示されません。

1.1.10 ジャンボフレーム

ジャンボフレームは、装置が許容する最大イーサネットフレームサイズで、デフォルト設定では 1,536 バイトです。最大イーサネットフレームサイズを変更するには、**max-rcv-frame-size** コマンドを使用します。

> ***REF:*** **max-rcv-frame-size** コマンドの設定値に対する動作は、対象ポート種別や機種によって異なります。詳細については、各機種の『コマンドリファレンス』を参照してください。

1.1.11 管理用 IP アドレスの設定

レイヤー 3 ライセンスが無効な NP7000、NP5000、および NP3000 でも、ネットワーク経由で管理するために、VLAN インターフェースやマネージメントポートに IP アドレスを設定できます。また、IPv4 のデフォルトスタティックルートと IPv6 のデフォルトスタティックルートも、それぞれ 1 つずつ設定できます。

NP4000、NP2100、および NP2000 にはレイヤー 3 ライセンスはありませんが、VLAN インターフェースやマネージメントポートの IP アドレスを設定できます。また、スタティックルートも設定できます。

NP2500 では VLAN 間のレイヤー 3 中継はできませんが、管理用としてマネージメントポート以外に 1 つの VLAN にのみ IP アドレスを設定できます。また、IPv4 のデフォルトスタティックルートと IPv6 のデフォルトスタティックルートも、それぞれ 1 つずつ設定できます。

> ***REF:*** IP アドレスやスタティックルートの設定については、「第 5 編 レイヤー 3」の「レイヤー 3 基本機能」を参照してください。

1.2 レイヤー 2 基本機能の状態確認

インターフェース関連の情報、カウンター情報、および MAC アドレステーブル関連の情報を表示して確認する方法を説明します。

1.2.1 インターフェース関連の情報の表示

インターフェース関連の情報を確認する方法を説明します。

1.2.1.1 インターフェース情報の表示

show interfaces コマンドで、インターフェースの情報を確認できます。

> ***REF:*** **show interfaces** コマンドの表示は機種によって異なります。詳細については、各機種の『コマンドリファレンス』を参照してください。

NP2100 の 1.12.01 で、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 interfaces port 1/0/1
(1)                    (2)
Port1/0/1 is enabled, link status is up
  Interface type: 1000BASE-T ...(3)
  Interface description: ...(4)
  MAC Address: FC-6D-D1-00-4C-9D ...(5)
  Auto-duplex, auto-speed, auto-mdix ...(6)
  Send flow-control: off, receive flow-control: off ...(7)
  Send flow-control oper: off, receive flow-control oper: off ...(8)
  Full-duplex, 1Gb/s ...(9)
  Maximum transmit unit: 1536 bytes ...(10)
  RX rate: 2344 bits/sec, TX rate: 0 bits/sec ...(11)
  RX bytes: 916, TX bytes: 0 ...(12)
  RX rate: 3 packets/sec, TX rate: 0 packets/sec ...(13)
  RX packets: 10, TX packets: 0 ...(14)
  RX multicast: 6, RX broadcast: 4 ...(15)
  RX CRC error: 0, RX undersize: 0 ...(16)
  RX oversize: 0, RX fragment: 0 ...(17)
  RX jabber: 0, RX dropped Pkts: 3 ...(18)
  RX MTU exceeded: 0 ...(19)
  TX CRC error: 0, TX excessive deferral: 0 ...(20)
  TX single collision: 0, TX excessive collision: 0 ...(21)
  TX late collision: 0, TX collision: 0 ...(22)
```

各項目の説明は、以下のとおりです。

表 1-2 show interfaces コマンドの表示項目

項番	説明
(1)	ポートの有効／無効を表示します。 • enabled：有効（no shutdown 設定時） • disabled：無効（shutdown 設定時）

項番	説明
(2)	ポートのリンク状態を表示します。 • up：リンクアップ状態 • down：リンクダウン状態 • down（error disabled: 機能名称）：各機能による err-disabled 状態 • down（cause: Memory Error）：**memory-error fault-action shutdown-all** コマンドの機能によってポートがシャットダウンされた状態 • errDis：LLDP 疑似リンクダウン状態 • minDown：ポートチャネルのミニマムリンク機能によるダウン状態（NP7000 の 1.10.02 以降、NP5000 の 1.09.01 以降、NP3000 の 1.10.01 以降でサポート）
(3)	インターフェースの種類を表示します。 • 1000BASE-T：RJ-45 ポート（10BASE-T/100BASE-TX/1000BASE-T） • 2500BASE-T：RJ-45 ポート（100BASE-TX/1000BASE-T/2.5GBASE-T） • 10GBASE-T：RJ-45 ポート（100BASE-TX/1000BASE-T/10GBASE-T） • 1000BASE-X：SFP ポート（ApresiaNP7000-24G24X6L のポート 1 ～ 24） • 10GBASE-R：SFP/SFP+ ポート • 25GBASE-R：SFP+/SFP28 ポート、または SFP/SFP+/SFP28 ポート • 40GBASE-R：QSFP+ ポート
(4)	ポートの説明を表示します。
(5)	ポートの MAC アドレスを表示します。
(6)	デュプレックスモード、速度、および MDIX 設定を表示します。機種ごとに設定できる内容が異なるため、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。
(7)	送信時および受信時のフロー制御設定（off：無効／ on：有効）を表示します。
(8)	送信時および受信時のフロー制御の実動作（off：無効状態／ on：有効状態）を表示します。
(9)	ポートのリンク状態、デュプレックスモード、および速度を表示します。 • Full-duplex, 40Gb/s：40Gbps/Full でリンクアップ状態 • Full-duplex, 25Gb/s：25Gbps/Full でリンクアップ状態 • Full-duplex, 10Gb/s：10Gbps/Full でリンクアップ状態 • Full-duplex, 2.5Gb/s：2.5Gbps/Full でリンクアップ状態 • Full-duplex, 1Gb/s：1000Mbps/Full でリンクアップ状態 • Full-duplex, 100Mb/s：100Mbps/Full でリンクアップ状態 • Half-duplex, 100Mb/s：100Mbps/Half でリンクアップ状態 • Full-duplex, 10Mb/s：10Mbps/Full でリンクアップ状態 • Half-duplex, 10Mb/s：10Mbps/Half でリンクアップ状態 • Down：リンクダウン状態
(10)	許容する最大イーサネットフレームサイズを表示します。
(11)	1 秒あたりの受信ビット数、および 1 秒あたりの送信ビット数を表示します。
(12)	受信バイト数、および送信バイト数を表示します。
(13)	1 秒あたりの受信パケット数、および 1 秒あたりの送信パケット数を表示します。
(14)	受信パケット数、および送信パケット数を表示します。
(15)	受信マルチキャストパケット数、および受信ブロードキャストパケット数を表示します。

項番	説明
(16)	受信 FCS エラー、および受信アンダーサイズパケットエラーのパケット数を表示します。
(17)	受信オーバーサイズパケットエラー、および受信フラグメントエラーのパケット数を表示します。
(18)	受信ジャバーパケットカウンター、および受信パケットドロップカウンターを表示します。
(19)	受信ポートの最大イーサネットフレームサイズによって破棄されたパケット数を表示します。
(20)	送信 FCS エラー、および送信過剰遅延のパケット数を表示します。
(21)	1 回のコリジョンだけで送信が成功した回数、および過度のコリジョン（16 回）によって転送が失敗した回数を表示します。
(22)	遅延コリジョンの発生回数、および送信コリジョンの発生回数を表示します。

1.2.1.2 インターフェースカウンターの表示

show interfaces counters コマンドで、インターフェースカウンター（送受信オクテットカウンター、送受信パケットカウンター）を確認できます。

ポート 1/0/1 からポート 1/0/2 を指定した場合の表示例を以下に示します。

```
# show interfaces port 1/0/1-2 counters
(1)           (2)                      (4)
Port          InOctets /               InMcastPkts /
              InUcastPkts ...(3)       InBcastPkts ...(5)
------------- ------------------------ ------------------------
Port1/0/1                      110664                       413
                                    0                       402
Port1/0/2                           0                         0
                                    0                         0
              (6)                      (8)
Port          OutOctets /              OutMcastPkts /
              OutUcastPkts ...(7)      OutBcastPkts ...(9)
------------- ------------------------ ------------------------
Port1/0/1                           0                         0
                                    0                         0
Port1/0/2                           0                         0
                                    0                         0

Total Entries: 2
```

各項目の説明は、以下のとおりです。

表 1-3 show interfaces counters 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)	受信オクテットカウンターを表示します。
(3)	受信ユニキャストパケットカウンターを表示します。
(4)	受信マルチキャストパケットカウンターを表示します。
(5)	受信ブロードキャストパケットカウンターを表示します。

項番	説明
(6)	送信オクテットカウンターを表示します。
(7)	送信ユニキャストパケットカウンターを表示します。
(8)	送信マルチキャストパケットカウンターを表示します。
(9)	送信ブロードキャストパケットカウンターを表示します。

1.2.1.3 ポートの接続状態の一覧表示

show interfaces status コマンドで、ポートの接続状態の一覧を確認できます。

ポート 1/0/1 からポート 1/0/8 を指定した場合の表示例を以下に示します。

```
# show interfaces port 1/0/1-8 status
(1)            (2)            (3)          (4)      (4)              (5)
Port           Status         VLAN         Duplex   Speed            Type
-------------- -------------- ------------ -------- ---------------- -------------
Port1/0/1      connected      1            a-full   a-1000           10GBASE-R
Port1/0/2      not-connected  1            auto     auto             10GBASE-R
Port1/0/3      not-connected  1            auto     auto             10GBASE-R
Port1/0/4      not-connected  1            auto     auto             10GBASE-R
Port1/0/5      not-connected  1            auto     auto             10GBASE-R
Port1/0/6      not-connected  1            auto     auto             10GBASE-R
Port1/0/7      not-connected  1            auto     auto             10GBASE-R
Port1/0/8      not-connected  1            auto     auto             10GBASE-R

Total Entries: 8
```

各項目の説明は、以下のとおりです。

表 1-4 show interfaces 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)	ポートのリンク状態を表示します。 • connected：リンクアップ状態 • not-connected：有効設定（no shutdown）で、リンクダウン状態 • disabled：無効設定（shutdown）状態 • err-disabled：err-disabled 状態 • memory-error：**memory-error fault-action shutdown-all** コマンドの機能によってポートがシャットダウンされた状態
(3)	アクセス VLAN またはネイティブ VLAN の VLAN ID を表示します。 対象ポートがポートチャネルのメンバーポートの場合は trunk と表示されます。 対象ポートがプライベート VLAN プロミスキャスポートの場合はプライマリー VLAN の、プライベート VLAN ホストポートの場合はセカンダリー VLAN の VLAN ID を表示します。
(4)	デュプレックスモードと通信速度を表示します。機種やインターフェースの種類ごとに表示内容が異なるため、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。

項番	説明
(5)	インターフェースの種類を表示します。 • 1000BASE-T：RJ-45 ポート（10BASE-T/100BASE-TX/1000BASE-T） • 2500BASE-T：RJ-45 ポート（100BASE-TX/1000BASE-T/2.5GBASE-T） • 10GBASE-T：RJ-45 ポート（100BASE-TX/1000BASE-T/10GBASE-T） • 1000BASE-X：SFP ポート（ApresiaNP7000-24G24X6L のポート 1 ～ 24） • 10GBASE-R：SFP/SFP+ ポート • 25GBASE-R：SFP+/SFP28 ポート、または SFP/SFP+/SFP28 ポート • 40GBASE-R：QSFP+ ポート

1.2.1.4 ポートの使用率の表示

show interfaces utilization コマンドで、ポートの使用率を確認できます。

ポート 1/0/1 からポート 1/0/2 を指定した場合の表示例を以下に示します。

```
# show interfaces port 1/0/1-2 utilization
(1)             (2)                 (3)                 (4)
Port            TX packets/sec /    TX bits/sec /       Utilization
                RX packets/sec      RX bits/sec
-------------   ----------------- ----------------- -----------
Port1/0/1                  6165          39048256             7
                          15413          97284024
Port1/0/2                     0                 0             0
                              0                 0

Total Entries: 2
```

各項目の説明は、以下のとおりです。

表 1-5 show interfaces utilization 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)	1 秒あたりの送信パケット数［上段］／受信パケット数［下段］を表示します。
(3)	1 秒あたりの送信ビット数［上段］／受信ビット数［下段］を表示します。
(4)	送受信あわせたポートの使用率（%）を表示します。

1.2.1.5 トランシーバーの情報の表示

show interfaces gbic コマンドで、トランシーバー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 interfaces port 1/0/1 gbic

Port1/0/1 ...(1)
 Type: H-T-SFP/R-A ...(2)
 Vendor PN: FCLF8521P2BTL ...(3)
 Vendor SN: PDR20VB ...(4)
```

各項目の説明は、以下のとおりです。

表 1-6 `show interfaces gbic` 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)	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。

1.2.1.6 インターフェースの説明とリンク状態の表示

`show interfaces description` コマンドでインターフェースの説明とリンク状態を確認できます。

表示例を以下に示します。

```
# show interfaces description
 (1)                  (2)       (3)             (4)
 Interface            Status    Administrative  Description
 -------------------  --------  --------------  ------------------------------
 Port1/0/1            up        enabled         TEST Port1/0/1
 Port1/0/2            up        enabled         3FN-04[1/0/3] to Conference ro
                                                om(ARENA-2F-003)
 Port1/0/3            down      enabled
 Port1/0/4            down      disabled
～～省略～～
 Port1/0/61           down      enabled
 Port1/0/65           down      enabled
 Port1/0/69           down      enabled
 Mgmt 0               up        enabled
 L2VLAN 1             up        enabled
 Interface vlan1      up        enabled         TEST VLAN 1 Interface

Total Entries: 57
```

各項目の説明は、以下のとおりです。

表 1-7 `show interfaces description` コマンドの表示項目

項番	説明
(1)	ポート番号などのインターフェース ID を表示します。
(2)	インターフェースのリンク状態を表示します。 • up：アップ状態 • down：ダウン状態 • errDis：LLDP 疑似リンクダウン状態（物理ポートの場合のみ） • minDown：ポートチャネルのメンバーポートがミニマムリンク機能によるダウン状態
(3)	インターフェースの有効／無効設定を表示します。ポートチャネル、レイヤー 2 VLAN インターフェース、NULL インターフェースは、常に enabled 表示です。 • enabled：有効（no shutdown 設定時） • disabled：無効（shutdown 設定時）
(4)	インターフェースの説明を表示します。**`description`** コマンドで設定した文字列（最大 64 文字）が 30 文字を超える場合、31 文字目と 61 文字目の前で改行されます。

1.2.1.7 ポートのオートネゴシエーション情報の表示

show interfaces auto-negotiation コマンドで、ポートのオートネゴシエーション情報を確認できます。

NP2500 の 1.11.01 で、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 interfaces port 1/0/1 auto-negotiation

Port1/0/1 ...(1)
 Auto Negotiation: Enabled ...(2)

 Speed auto downgrade: Disabled ...(3)
 Remote Signaling: Not detected ...(4)
 Configure Status: Complete ...(5)
 Capability Bits: 100M_Half, 100M_Full, 1000M_Full, 2500M_Full ...(6)
 Capability Advertised Bits: 100M_Half, 100M_Full, 1000M_Full, 2500M_Full ...(7)
 Capability Received Bits: 100M_Half, 100M_Full, 1000M_Full ...(8)
 RemoteFaultAdvertised: Disabled ...(9)
 RemoteFaultReceived: NoError ...(10)
```

各項目の説明は、以下のとおりです。

表 1-8 show interfaces auto-negotiation 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)	オートネゴシエーションの有効 (Enabled) ／無効 (Disabled) を表示します。
(3)	speed auto-downgrade 設定の有効 (Enabled) ／無効 (Disabled) を表示します。
(4)	リモートシグナルの状況を表示します。
(5)	オートネゴシエーションの状況を表示します。
(6)	使用可能な通信速度とデュプレックスモードを表示します。
(7)	対向装置に通知する通信速度とデュプレックスモードを表示します。
(8)	対向装置から通知された通信速度とデュプレックスモードを表示します。
(9)	本項目の表示は未サポートです。
(10)	本項目の表示は未サポートです。

1.2.2 カウンター情報の表示

指定したインターフェースのカウンターを確認する方法を説明します。

> ***REF:*** **`show counters`** コマンドの表示は機種によって異なります。詳細については、各機種の『コマンドリファレンス』を参照してください。

1.2.2.1 物理ポートのカウンターの表示

`show counters interface` コマンドで、物理ポートのカウンターを確認できます。

NP2100 の 1.12.01 で、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 counters interface port 1/0/1

Port1/0/1 counters
rxHCTotalPkts                    :                86734 ...(1)
txHCTotalPkts                    :                   73 ...(2)
rxHCUnicastPkts                  :                  158 ...(3)
txHCUnicastPkts                  :                   73 ...(4)
rxHCMulticastPkts                :                39140 ...(5)
txHCMulticastPkts                :                    0 ...(6)
rxHCBroadcastPkts                :                47436 ...(7)
txHCBroadcastPkts                :                    0 ...(8)
rxHCOctets                       :             14420412 ...(9)
txHCOctets                       :                 4992 ...(10)
rxHCPkt64Octets                  :                38554 ...(11)
rxHCPkt65to127Octets             :                23454 ...(12)
rxHCPkt128to255Octets            :                 7531 ...(13)
rxHCPkt256to511Octets            :                12541 ...(14)
rxHCPkt512to1023Octets           :                 3228 ...(15)
rxHCPkt1024to1518Octets          :                 1426 ...(16)
rxHCPkt1519to1522Octets          :                    0 ...(17)
rxHCPkt1519to2047Octets          :                    0 ...(18)
rxHCPkt2048to4095Octets          :                    0 ...(19)
rxHCPkt4096to9216Octets          :                    0 ...(20)
txHCPkt64Octets                  :                   41 ...(21)
txHCPkt65to127Octets             :                   32 ...(22)
txHCPkt128to255Octets            :                    0 ...(23)
txHCPkt256to511Octets            :                    0 ...(24)
txHCPkt512to1023Octets           :                    0 ...(25)
txHCPkt1024to1518Octets          :                    0 ...(26)
txHCPkt1519to1522Octets          :                    0 ...(27)
txHCPkt1519to2047Octets          :                    0 ...(28)
txHCPkt2048to4095Octets          :                    0 ...(29)
txHCPkt4096to9216Octets          :                    0 ...(30)

rxCRCAlignErrors                 :                    0 ...(31)
rxUndersizedPkts                 :                    0 ...(32)
rxOversizedPkts                  :                    0 ...(33)
rxFragmentPkts                   :                    0 ...(34)
rxJabbers                        :                    0 ...(35)
rxSymbolErrors                   :                    0 ...(36)
rxDropPkts                       :                50256 ...(37)
```

```
txCollisions                        :                    0 ...(38)
ifInErrors                          :                    0 ...(39)
ifOutErrors                         :                    0 ...(40)
ifInDiscards                        :                50256 ...(41)
ifInUnknownProtos                   :                    0 ...(42)
ifOutDiscards                       :                    0 ...(43)
txDelayExceededDiscards             :                    0 ...(44)
txCRC                               :                    0 ...(45)
txDropPkts                          :                    0 ...(46)
txCoS0DropPkts                      :                    0 ...(47)
txCoS1DropPkts                      :                    0 ...(48)
txCoS2DropPkts                      :                    0 ...(49)
txCoS3DropPkts                      :                    0 ...(50)
txCoS4DropPkts                      :                    0 ...(51)
txCoS5DropPkts                      :                    0 ...(52)
txCoS6DropPkts                      :                    0 ...(53)
txCoS7DropPkts                      :                    0 ...(54)

dot3StatsAlignmentErrors            :                    0 ...(55)
dot3StatsFCSErrors                  :                    0 ...(56)
dot3StatsSingleColFrames            :                    0 ...(57)
dot3StatsMultiColFrames             :                    0 ...(58)
dot3StatsSQETestErrors              :                    0 ...(59)
dot3StatsDeferredTransmisions       :                    0 ...(60)
dot3StatsLateCollisions             :                    0 ...(61)
dot3StatsExcessiveCollisions        :                    0 ...(62)
dot3StatsInternalMacTransmitErrors  :                    0 ...(63)
dot3StatsCarrierSenseErrors         :                    0 ...(64)
dot3StatsFrameTooLongs              :                    0 ...(65)
dot3StatsInternalMacReceiveErrors   :                    0 ...(66)

linkChange                          :                    2 ...(67)
```

各項目の説明は、以下のとおりです。

表 1-9 `show counters interface` コマンドの表示項目

項番	説明
(1)	受信パケットカウンターを表示します。
(2)	送信パケットカウンターを表示します。
(3)	受信ユニキャストパケットカウンターを表示します。
(4)	送信ユニキャストパケットカウンターを表示します。
(5)	受信マルチキャストパケットカウンターを表示します。
(6)	送信マルチキャストパケットカウンターを表示します。
(7)	受信ブロードキャストパケットカウンターを表示します。
(8)	送信ブロードキャストパケットカウンターを表示します。
(9)	受信オクテットカウンターを表示します。
(10)	送信オクテットカウンターを表示します。

項番	説明
(11)	受信 64 オクテットパケットカウンターを表示します。
(12)	受信 65 ～ 127 オクテットパケットカウンターを表示します。
(13)	受信 128 ～ 255 オクテットパケットカウンターを表示します。
(14)	受信 256 ～ 511 オクテットパケットカウンターを表示します。
(15)	受信 512 ～ 1,023 オクテットパケットカウンターを表示します。
(16)	受信 1,024 ～ 1,518 オクテットパケットカウンターを表示します。
(17)	受信 1,519 ～ 1,522 オクテットパケットカウンターを表示します。
(18)	受信 1,519 ～ 2,047 オクテットパケットカウンターを表示します。
(19)	受信 2,048 ～ 4,095 オクテットパケットカウンターを表示します。
(20)	受信 4,096 ～ 9,216 オクテットパケットカウンターを表示します。
(21)	送信 64 オクテットパケットカウンターを表示します。
(22)	送信 65 ～ 127 オクテットパケットカウンターを表示します。
(23)	送信 128 ～ 255 オクテットパケットカウンターを表示します。
(24)	送信 256 ～ 511 オクテットパケットカウンターを表示します。
(25)	送信 512 ～ 1,023 オクテットパケットカウンターを表示します。
(26)	送信 1,024 ～ 1,518 オクテットパケットカウンターを表示します。
(27)	送信 1,519 ～ 1,522 オクテットパケットカウンターを表示します。
(27)	送信 1,519 ～ 2,047 オクテットパケットカウンターを表示します。
(29)	送信 2,048 ～ 4,095 オクテットパケットカウンターを表示します。
(30)	送信 4,096 ～ 9,216 オクテットパケットカウンターを表示します。
(31)	受信 FCS エラーパケットカウンターを表示します。
(32)	受信アンダーサイズパケットカウンターを表示します。
(33)	受信オーバーサイズパケットカウンターを表示します。
(34)	受信フラグメントカウンターを表示します。
(35)	受信ジャバーパケットカウンターを表示します。
(36)	受信コードエラーパケットカウンターを表示します。
(37)	受信パケットドロップカウンターを表示します。
(38)	送信コリジョンカウンターを表示します。
(39)	上位レイヤープロトコルへの配信を妨げるエラーを含む、受信パケット数を表示します。
(40)	エラーのために送信できない送信パケット数を表示します。

項番	説明
(41)	上位レイヤープロトコルに配信できないエラーが検知されていない場合に、廃棄が選択された受信パケット数を表示します。
(42)	当該インターフェース経由で受信したプロトコルが不明、またはサポートされていないために廃棄されたパケット数を表示します。
(43)	送信を妨げるエラーが検知されていない場合に、廃棄を指定された送信パケット数を表示します。
(44)	送信マルチ遅延パケットカウンターを表示します。
(45)	送信 FCS エラーカウンターを表示します。
(46)	送信パケットドロップカウンターを表示します。
(47)	CoS キュー 0 の送信パケットドロップカウンターを表示します。 NP2100、NP2000、および NP2500 では、本項目はカウントしません。
(48)	CoS キュー 1 の送信パケットドロップカウンターを表示します。 NP2100、NP2000、および NP2500 では、本項目はカウントしません。
(49)	CoS キュー 2 の送信パケットドロップカウンターを表示します。 NP2100、NP2000、および NP2500 では、本項目はカウントしません。
(50)	CoS キュー 3 の送信パケットドロップカウンターを表示します。 NP2100、NP2000、および NP2500 では、本項目はカウントしません。
(51)	CoS キュー 4 の送信パケットドロップカウンターを表示します。 NP2100、NP2000、および NP2500 では、本項目はカウントしません。
(52)	CoS キュー 5 の送信パケットドロップカウンターを表示します。 NP2100、NP2000、および NP2500 では、本項目はカウントしません。
(53)	CoS キュー 6 の送信パケットドロップカウンターを表示します。 NP2100、NP2000、および NP2500 では、本項目はカウントしません。
(54)	CoS キュー 7 の送信パケットドロップカウンターを表示します。 NP2100、NP2000、および NP2500 では、本項目はカウントしません。
(55)	特定のインターフェースで受信した、整数倍ではないオクテット長で、かつ FCS チェックに合格しないパケットの数を表示します。
(56)	特定のインターフェースで受信した、整数倍のオクテット長で、かつ FCS チェックに合格にしないパケットの数を表示します。
(57)	1 回のコリジョンで送信が抑止された特定のインターフェースで、正常に送信されたパケット数を表示します。
(58)	2 回以上のコリジョンで送信が抑止された特定のインターフェースで、正常に送信されたパケット数を表示します。
(59)	特定のインターフェースに対し、PLS サブレイヤーによって SQE TEST ERROR メッセージが出力された回数を表示します。
(60)	メディアがビジー状態のため、特定のインターフェースで初回の送信が遅延したパケット数を表示します。
(61)	パケットに割り当てられたスロットタイムが経過した後に、特定のインターフェースでコリジョンが検知された回数を表示します。

項番	説明
(62)	過度なコリジョンが原因で、特定のインターフェースで送信に失敗したパケット数を表示します。
(63)	内部 MAC サブレイヤーの送信エラーが原因で、特定のインターフェースで送信に失敗したパケット数を表示します。
(64)	特定のインターフェースでパケットを送信しようとしたときに、キャリア検知状態が失われた、またはアサートされていなかった回数を表示します。
(65)	特定のインターフェースで受信した、最大許容フレームサイズを超えるパケット数を表示します。
(66)	内部 MAC サブレイヤーの受信エラーが原因で、特定のインターフェースで受信に失敗したパケット数を表示します。
(67)	ポートのステータスが変化した際にカウントされる数字を表示します。

1.2.2.2 CPU 宛てカウンターの表示

show counters cpu-port コマンドで、CPU 宛てカウンターを確認できます。NP7000 の 1.08.01 以降、NP5000 の 1.08.01 以降、NP4000 の 1.03.01 以降、NP3000 の 1.11.03 以降、NP2100 の 1.09.02 以降、NP2000 の 1.09.01 以降では、表示内容が拡張されています。

表示内容が拡張された機種／バージョンでの表示例を以下に示します。

```
# show counters cpu-port

Unit 1, CPU Port counters
(1)                (2)                  (3)                (4) cpuTxDropPkts
CoS                cpuRxPkts            cpuTxDropPkts        Last occurrence
--- ------------------------ ------------------------ --------------------
0                          0                        0                     -
1                          0                        0                     -
2                      31412                   415509    2021-04-12 13:32:42
3                          0                        0                     -
4                          0                        0                     -
5                          0                        0                     -
6                          0                        0                     -
7                          0                        0                     -

Unit 1, CPU Port counters rate (pps)
      (5)           (6)              (7)
(1)   cpuRxPkts     Maximum          Maximum rate
CoS   rate(pps)        rate       last occurrence
--- ----------- ---------- --------------------
0             0          -                     -
1             0          -                     -
2             5        580  2021-04-12 13:28:10
3             0          -                     -
4             0          -                     -
5             0          -                     -
6             0          -                     -
7             0          -                     -
     (8)                   (9)         (10)                  (11)
(1)  cpuTxDropPkts         Maximum     Maximum drop rate     Number of
CoS      rate(pps)       drop rate       last occurrence   occurrences
--- -------------- -------------- -------------------- ------------
0                0              -                    -            -
1                0              -                    -            -
2                0          82473  2021-04-12 13:32:37           21
3                0              -                    -            -
4                0              -                    -            -
5                0              -                    -            -
6                0              -                    -            -
7                0              -                    -            -
```

各項目の説明は、以下のとおりです。

表 1-10 show counters cpu-port コマンドの表示項目

項番	説明
(1)	CoS キューを表示します。
(2)	CoS ごとの CPU での受信パケットカウンターを表示します。
(3)	CoS ごとの CPU 宛てポートの送信パケットドロップカウンターを表示します。
(4)	CoS ごとの CPU 宛て送信パケットドロップが最後に発生した時刻を表示します。
(5)	CoS ごとの CPU での受信パケットレート（pps）を表示します。

項番	説明
(6)	CoS ごとの CPU での受信パケットレートの、カウンターがクリアされた以降の最大値（pps）を表示します。
(7)	CoS ごとの CPU での受信パケットレートが最大値を示した時刻を表示します。
(8)	CoS ごとの CPU 宛て送信パケットドロップレート（pps）を表示します。
(9)	CoS ごとの CPU 宛て送信パケットドロップレートの、カウンターがクリアされた以降の最大値（pps）を表示します。
(10)	CoS ごとの CPU 宛て送信パケットドロップレートが最大値を示した時刻を表示します。
(11)	CoS ごとの CPU 宛て送信パケットドロップが 1pps 以上を示した回数を表示します。

1.2.2.3 受信ポートごとの CPU 宛てカウンターの表示

show counters cpu-port detail コマンドで、受信ポートごとの CPU 宛てカウンターを確認できます。

> ***NOTE:*** 受信ポートごとの CPU 宛てカウンターは、NP7000 の 1.07.01 以降、NP5000 の 1.07.01 以降、NP4000 の 1.03.01 以降、NP3000 の 1.12.01 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。

表示例を以下に示します。

```
# show counters cpu-port detail

cpuRxPkts:          (1)        (2)        (3)        (4)        (5)        (6)        (7)        (8)
                   CoS0       CoS1       CoS2       CoS3       CoS4       CoS5       CoS6       CoS7
             ---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------
port 1/0/1            0          0          0          0          0          0          0          0
port 1/0/2            0          0          0          0          0          0          0          0
port 1/0/3            0          0          0          0          0          0          0          0
port 1/0/4            0          0          0          0          0          0          0          0
port 1/0/5            0          0          0          0          0          0          0          0
port 1/0/6            0          0          0          0          0          0          0          0
port 1/0/7            0          0          0          0          0          0          0          0
port 1/0/8            0          0          0          0          0          0          0          0
port 1/0/9            0          0          0          0          0          0          0          0
port 1/0/10           0          0          0          0          0          0          0          0
port 1/0/11           0          0          0          0          0          0          0          0
port 1/0/12           0          0          0          0          0          0          0          0
port 1/0/13           0          0          0          0          0          0          0          0
port 1/0/14           0          0          0          0          0          0          0          0
port 1/0/15           0          0          0          0          0          0          0          0
port 1/0/16           0          0          0          0          0          0          0          0
port 1/0/17           0          0          0          0          0          0          0          0
port 1/0/18           0          0          0          0          0          0          0          0
port 1/0/19           0          0          0          0          0          0          0          0
port 1/0/20           0          0          0          0          0          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 1-11 show counters cpu-port detail コマンドの表示項目

項番	説明
(1)	CoS キュー 0 の CPU での受信パケットカウンターを表示します。
(2)	CoS キュー 1 の CPU での受信パケットカウンターを表示します。

項番	説明
(3)	CoS キュー 2 の CPU での受信パケットカウンターを表示します。
(4)	CoS キュー 3 の CPU での受信パケットカウンターを表示します。
(5)	CoS キュー 4 の CPU での受信パケットカウンターを表示します。
(6)	CoS キュー 5 の CPU での受信パケットカウンターを表示します。
(7)	CoS キュー 6 の CPU での受信パケットカウンターを表示します。
(8)	CoS キュー 7 の CPU での受信パケットカウンターを表示します。

1.2.3 MAC アドレステーブル関連の情報の表示

MAC アドレステーブル関連の情報を確認する方法を説明します。

1.2.3.1 MAC アドレステーブルの表示

show mac-address-table コマンドで、MAC アドレステーブルを確認できます。

MAC アドレス 00-00-5E-00-53-F2 を指定した場合の表示例と、VLAN 10 を指定した場合の表示例を以下に示します。

```
# show mac-address-table address 00-00-5E-00-53-F2
(1)   (2)                 (3)          (4)
VLAN  MAC Address         Type         Ports
----  ------------------  ----------   -------------------------
  10  00-00-5E-00-53-F2   Dynamic      Port1/0/11

Total Entries: 1

# show mac-address-table vlan 10
(1)   (2)                 (3)          (4)
VLAN MAC Address          Type         Ports
----  ------------------  ----------   -------------------------
  10  00-00-5E-00-53-F1   Dynamic      Port1/0/4
  10  00-00-5E-00-53-F2   Dynamic      Port1/0/11
  10  00-40-66-A8-CC-41   Dynamic      Port1/0/12

Total Entries: 3
```

各項目の説明は、以下のとおりです。

表 1-12 show mac-address-table コマンドの表示項目

項番	説明
(1)	VLAN ID を表示します。
(2)	MAC アドレスを表示します。
(3)	エントリーのタイプ（Static：スタティック／ Dynamic：ダイナミック）を表示します。
(4)	ポート番号を表示します。

1.2.3.2 スタティックエントリーの表示

show mac-address-table static コマンドで、MAC アドレステーブルのスタティックエントリーを確認できます。

表示例を以下に示します。

```
# show mac-address-table static
(1)   (2)                (3)          (4)
VLAN  MAC Address        Type         Ports
----  -----------------  ----------   -------------------------
   1  00-40-66-B4-96-B5  Static       CPU
   4  00-00-5E-00-53-11  Static       Port1/0/1
   4  00-00-5E-00-53-22  Static       port-channel2

Total Entries: 3
```

各項目の説明は、以下のとおりです。

表 1-13 show mac-address-table static コマンドの表示項目

項番	説明
(1)	VLAN ID を表示します。
(2)	MAC アドレスを表示します。
(3)	エントリーのタイプ（Static：スタティック／ Dynamic：ダイナミック）を表示します。
(4)	ポート番号を表示します。

1.2.3.3 エージングタイムの設定値の表示

show mac-address-table aging-time コマンドで、MAC アドレステーブルのエージングタイムの設定値を確認できます。

表示例を以下に示します。

```
# show mac-address-table aging-time

 Aging Time is 300 seconds....(1)
```

各項目の説明は、以下のとおりです。

表 1-14 show mac-address-table aging-time コマンドの表示項目

項番	説明
(1)	MAC アドレステーブルのエージングタイムの設定値を表示します。

1.2.3.4 MAC アドレス学習の有効／無効の表示

show mac-address-table learning コマンドで MAC アドレス学習の有効／無効を確認できます。

ポート 1/0/1 からポート 1/0/6 を指定した場合の表示例を以下に示します。

```
# show mac-address-table learning interface port 1/0/1-6
(1)                          (2)
Port                         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
```

各項目の説明は、以下のとおりです。

表 1-15 show mac-address-table learning コマンドの表示項目

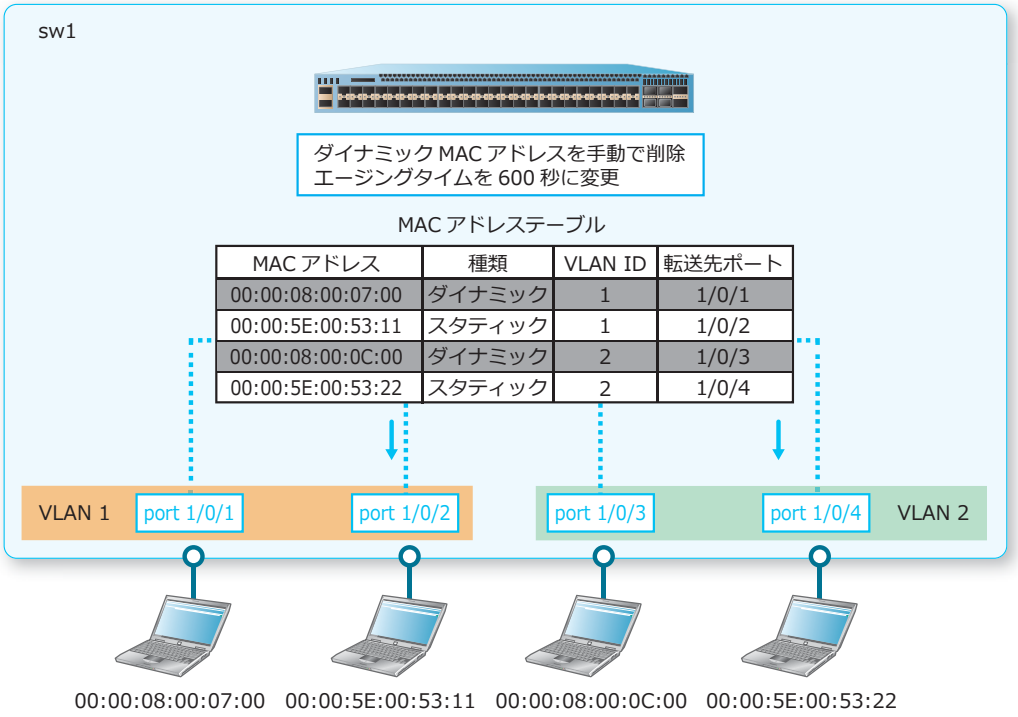
項番	説明
(1)	ポート番号を表示します。
(2)	MAC アドレス学習の有効 (Enabled) ／無効 (Disabled) を表示します。

1.3 レイヤー 2 基本機能の構成例と設定例

MAC アドレステーブルに、以下の変更を行う場合の構成例と設定例を示します。

- すべてのダイナミック MAC アドレスを手動で削除する
- エージングタイムを変更する
- スタティック MAC アドレスを追加する

図 1-3 MAC アドレステーブルの構成例



1. VLAN 1 および VLAN 2 を作成します。

```
sw1# configure terminal
sw1(config)# vlan 1
sw1(config-vlan)# exit
sw1(config)# vlan 2
sw1(config-vlan)# exit
sw1(config)#
```

2. ポート 1/0/1 およびポート 1/0/2 をアクセスポートとして設定し、アクセスポートに［VLAN 1］を割り当てます。また、ポート 1/0/3 およびポート 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 2］を割り当てます。

```
sw1(config)# interface range port 1/0/1-2
sw1(config-if-port-range)# switchport mode access
sw1(config-if-port-range)# switchport access vlan 1
sw1(config-if-port-range)# exit
sw1(config)# interface range port 1/0/3-4
sw1(config-if-port-range)# switchport mode access
sw1(config-if-port-range)# switchport access vlan 2
sw1(config-if-port-range)# end
sw1#
```

3. すべてのダイナミック MAC アドレスを削除します。

```
sw1# clear mac-address-table dynamic all
sw1#
```

4. MAC アドレステーブルのエージングタイムを［600 秒］に変更します。

```
sw1# configure terminal
sw1(config)# mac-address-table aging-time 600
sw1(config)#
```

5. スタティック MAC アドレス［00:00:5E:00:53:11］を［VLAN 1］の［port 1/0/2］指定で設定します。

```
sw1(config)# mac-address-table static 00:00:5e:00:53:11 vlan 1 interface port
1/0/2
sw1(config)#
```

6. スタティック MAC アドレス［00:00:5E:00:53:22］を［VLAN 2］の［port 1/0/4］指定で設定します。

```
sw1(config)# mac-address-table static 00:00:5e:00:53:22 vlan 2 interface port
1/0/4
sw1(config)# end
sw1#
```

2. VLAN

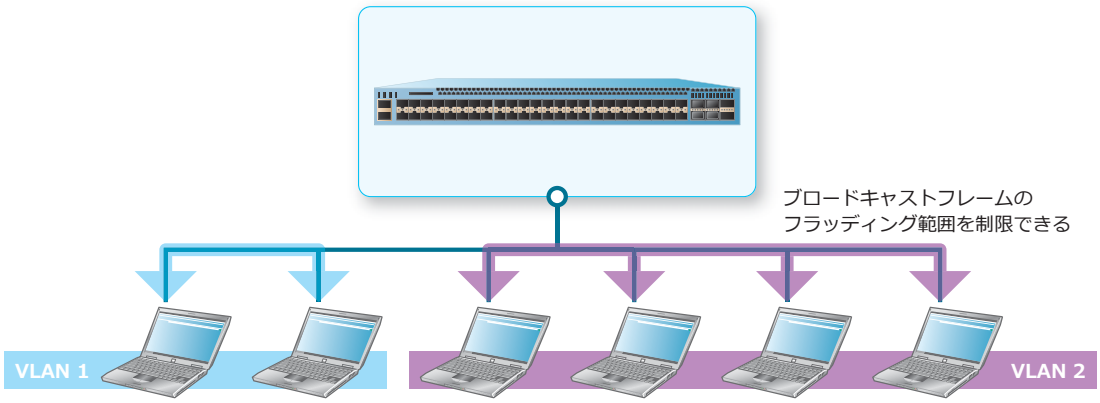
VLAN の機能、状態の確認方法、および構成例と設定例について説明します。

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。

2.1 VLAN の機能説明

VLAN は、装置のトラフィックを仮想的なグループに分割する機能です。ブロードキャストドメインを分割し、ブロードキャストフレームのフラッディング範囲を制限するために使用します。

図 2-1 VLAN の概要



VLAN を作成するには、**vlan** コマンドを使用します。VLAN の名前を設定するには、**name** コマンドを使用します。

タグ付き VLAN とタグなし VLAN

VLAN はフレームに付与された VLAN タグの VLAN ID によって判別されます。送受信するフレームの形式（タグ付き／タグなし）は、対象インターフェースの VLAN 動作モードによって決まります。タグ付きフレームを送受信する VLAN のことをタグ付き VLAN と呼びます。また、タグなしフレームを送受信する VLAN のことをタグなし VLAN と呼びます。

プロトコル VLAN

フレームタイプを基に定義する VLAN をプロトコル VLAN と呼びます。プロトコルグループを作成し、インターフェースごとに、プロトコルグループに一致したフレームを振り分ける VLAN を設定すると、プロトコル VLAN が有効になります。プロトコルグループの作成は、**protocol-vlan profile** コマンドを使用します。プロトコルグループに一致したフレームを振り分ける VLAN を設定するには、**protocol-vlan profile (interface)** コマンドを使用します。

受信可能なフレームタイプの制限

ポートごとに受信可能なフレームタイプ（タグ付きフレームのみ許可、タグなしフレームのみ許可、すべて許可）を設定できます。受信可能なフレームタイプを設定するには、**acceptable-frame** コマンドを使用します。

受信可能な VLAN ID チェックの有効／無効

ポートごとに、受信可能な VLAN ID チェックの有効／無効を設定できます。デフォルトでは VLAN ID チェックは有効で、受信したタグ付きフレームの VLAN ID に一致する VLAN が対象ポートに割り当てられている場合にのみ受信できます。割り当てられていない場合は受信できません。受信可能な VLAN ID チェックの有効／無効を設定するには、**ingress-checking** コマンドを使用します。

2.1.1 VLAN 動作モード

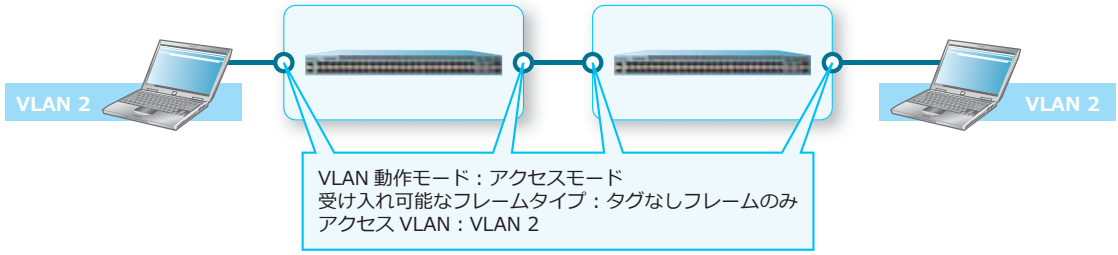
インターフェースには、以下の VLAN 動作モードがあります。なお、アクセスモードのインターフェースをアクセスポートと呼びます。また、その他の VLAN 動作モードのインターフェースも同様に、ハイブリッドポート、トランクポート、およびトンネルポートと呼びます。

VLAN 動作モードは、**`switchport mode`** コマンドで設定します。

- **アクセスモード（アクセスポート）**

  1 つの VLAN を割り当てるためのモードで、主に端末を収容するために使用します。対象ポートではこの VLAN をアクセス VLAN と呼びます。アクセス VLAN では基本的にはタグなしフレームを送受信します。

図 2-2 アクセスモード

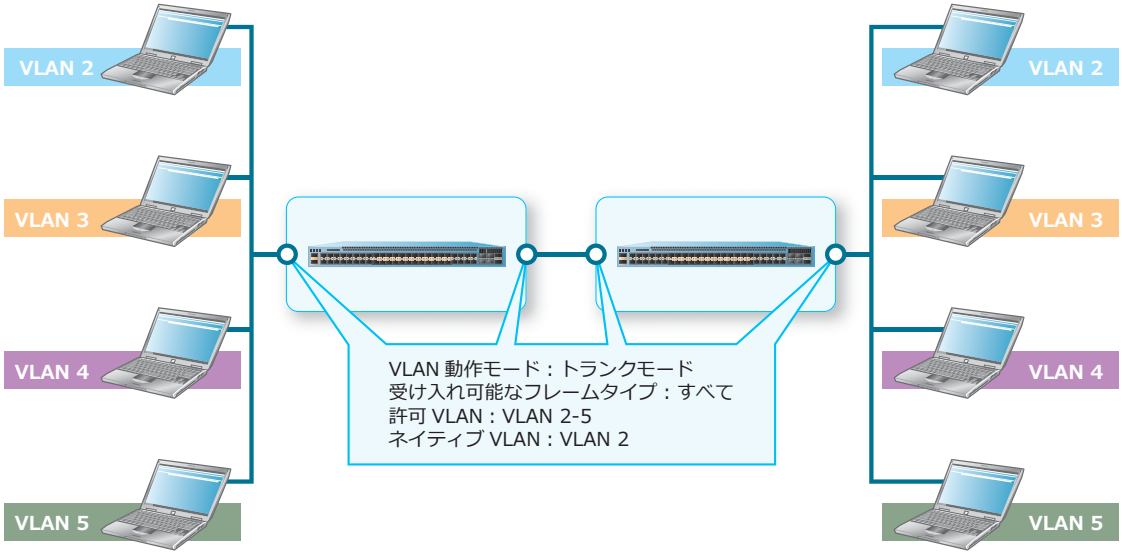


アクセスモード（switchport mode access）のポートに VLAN を割り当てるには、**`switchport access vlan`** コマンドを使用します。

- **トランクモード（トランクポート）**

  同一ポートに複数のタグ付き VLAN（タグ付きフレームを送受信）と、1 つのネイティブ VLAN（基本的にはタグなしフレームを送受信）を割り当てることが可能なモードで、主に装置間の接続で使用します。

図 2-3 トランクモード



トランクモード（switchport mode trunk）のポートに VLAN を割り当てるには、**`switchport trunk allowed vlan`** コマンドを使用して、許可する VLAN をネイティブ VLAN も含めてすべて割り当てます。

> ***NOTE:*** **`switchport trunk allowed vlan`** コマンドのデフォルト設定は「すべての VLAN を許可する設定」のため、任意のポートをトランクポートに設定した時点で、設定済みのすべての VLAN が割り当てられることに注意してください。

すでに **`switchport trunk allowed vlan`** コマンドが設定されている状態で再度コマンドを実施すると、上書き設定されることに注意してください。たとえば、**`switchport trunk allowed`**

vlan 10,20 が設定されている状態で **switchport trunk allowed vlan 30** を実施すると、上書き設定されて **switchport trunk allowed vlan 30** になります。

そのため、既存の設定に VLAN を追加／削除する場合は、add パラメーター／ remove パラメーターを指定してコマンドを実施してください。たとえば、**switchport trunk allowed vlan 10,20** が設定されている状態で **switchport trunk allowed vlan add 30** を実施すると、VLAN 30 が追加されて **switchport trunk allowed vlan 10,20,30** になります。また、この状態から **switchport trunk allowed vlan remove 20** を実施すると、VLAN 20 が削除されて **switchport trunk allowed vlan 10,30** になります。

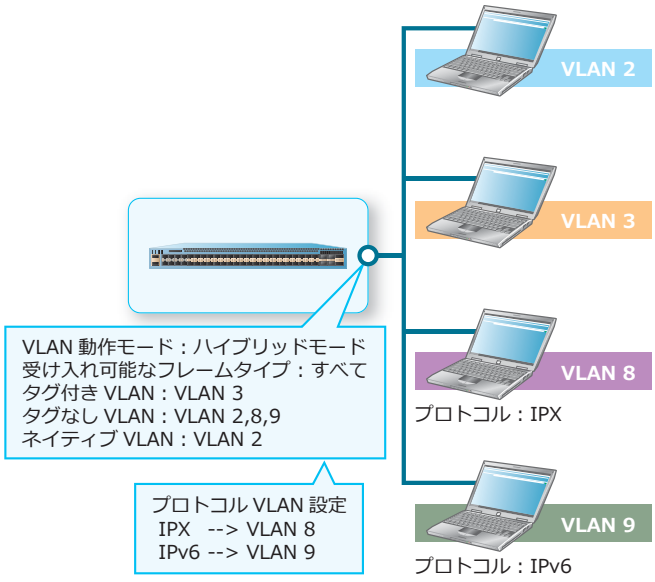
> ***CAUTION:*** **no switchport trunk allowed vlan** コマンドで設定を削除すると、デフォルト設定（**switchport trunk allowed vlan all**）の「すべての VLAN を許可する設定」になることに注意してください。

トランクポートのネイティブ VLAN を設定するには、**switchport trunk native vlan** コマンドを使用します。ネイティブ VLAN から送信するフレームをタグ付きフレームに変更するには、**switchport trunk native vlan tag** コマンドを使用します。デフォルトでは VLAN 1 がタグなしモードでネイティブ VLAN に設定されています。

- **ハイブリッドモード（ハイブリッドポート）**

  同一ポートに複数のタグ付き VLAN（タグ付きフレームを送受信）と、複数のタグなし VLAN（基本的にはタグなしフレームを送受信）を割り当てることが可能なモードで、主にプロトコル VLAN で使用します。

図 2-4 ハイブリッドモード



この例では、VLAN 3 をタグ付き VLAN として登録し、VLAN 2,8,9 をタグなし VLAN として登録しています。また、受信したタグなしフレームを受信する VLAN を決定するために、プロトコルが IPX の場合は VLAN 8 で受信し、プロトコルが IPv6 の場合は VLAN 9 で受信するように、プロトコル VLAN を設定しています。また、どちらのプロトコル VLAN 設定にもマッチしないタグなしフレームを VLAN 2 で受信するように、VLAN 2 はネイティブ VLAN として設定しています。

ハイブリッドモード（switchport mode hybrid）のポートにタグ付き VLAN を割り当てるには、tagged パラメーターを指定して **switchport hybrid allowed vlan** コマンドを使用します。タグなし VLAN を割り当てるには、untagged パラメーターを指定して **switchport hybrid allowed vlan** コマンドを使用します。ハイブリッドポートのネイティブ VLAN を設定するには、**switchport hybrid native vlan** コマンドを使用します。

すでに **switchport hybrid allowed vlan** コマンドが設定されている状態で再度コマンドを実施すると、上書き設定されることに注意してください。たとえば、**switchport hybrid allowed vlan untagged 10,20**が設定されている状態で**switchport hybrid allowed vlan untagged 30** を実施すると、上書き設定されて **switchport hybrid allowed vlan untagged 30** になります。

そのため、既存の設定に VLAN を追加／削除する場合は、add パラメーター／ remove パラメーターを指定してコマンドを実施してください。たとえば、**switchport hybrid allowed vlan untagged 10,20**が設定されている状態で**switchport hybrid allowed vlan add untagged 30** を実施すると、VLAN 30 が追加されて **switchport hybrid allowed vlan untagged 10,20,30** になります。また、この状態から **switchport hybrid allowed vlan remove 20** を実施すると、VLAN 20 が削除されて **switchport hybrid allowed vlan untagged 10,30** になります。

- **トンネルモード（トンネルポート）**

  VLAN トンネル使用時に、サービス VLAN の UNI ポートとして動作させるためのモードです。詳細については、「第 4 編 レイヤー 2」の「VLAN トンネル／ VLAN 変換」を参照してください。

2.2 VLAN の状態確認

VLAN の状態を表示して確認する方法を説明します。

2.2.1 VLAN の表示

show vlan コマンドで、すべての VLAN の設定を確認できます。

表示例を以下に示します。

```
# show vlan

 VLAN 1 ...(1)
    Name : default ...(2)
    Description : ...(3)
    Tagged Member Ports   : ...(4)
    Untagged Member Ports : 1/0/21-1/0/49,1/0/53,1/0/57,1/0/61,1/0/65,1/0/69 ...(5)
 VLAN 100
    Name : VLAN0100
    Description :
    Tagged Member Ports   : 1/0/49,1/0/53
    Untagged Member Ports : 1/0/1-1/0/10
 VLAN 200
    Name : VLAN0200
    Description :
    Tagged Member Ports   : 1/0/49,1/0/53
    Untagged Member Ports : 1/0/11-1/0/20
Total Entries: 3
```

各項目の説明は、以下のとおりです。

表 2-1 show vlan コマンドの表示項目

項番	説明
(1)	VLAN ID を表示します。
(2)	VLAN 名を表示します。
(3)	対応するレイヤー 2 VLAN インターフェースの description 設定を表示します。
(4)	VLAN のタグ付きメンバーポートを表示します。
(5)	VLAN のタグなしメンバーポートを表示します。

2.2.2 VLAN の詳細情報の表示

show vlan detail コマンドで、VLAN の詳細情報を確認できます。

表示例を以下に示します。

```
# show vlan detail

--- vlan port information --- ...(1)
               a = access  t = trunk  h = hybrid
               p = private-vlan  d = dot1q-tunnel
               C Port
                 1      8 9     16 17    24 25    32 33    40 41    48 49    56
                 +------+ +------+ +------+ +------+ +------+ +------+ +------+
                 57    64 65    72
                 +------+ +------+
 Port Mode     1 aaaaaaaa aaaaaaaa aaaaaaaa aaaaaaaa aaaaaaaa aaaaaaaa txxxtxxx
                 axxxaxxx axxxaxxx

--- vlan mapping information --- ...(2)
               u = untag  t = tag
               C Port
                 1      8 9     16 17    24 25    32 33    40 41    48 49    56
                 +------+ +------+ +------+ +------+ +------+ +------+ +------+
                 57    64 65    72
 Name      VID   +------+ +------+
default      1 1 ........ ........ ....uuuu uuuuuuuu uuuuuuuu uuuuuuuu uxxxuxxx
                 uxxxuxxx uxxxuxxx
VLAN0100   100 1 uuuuuuuu uu...... ........ ........ ........ ........ txxxtxxx
                 .xxx.xxx .xxx.xxx
VLAN0200   200 1 ........ ..uuuuuu uuuu.... ........ ........ ........ txxxtxxx
                 .xxx.xxx .xxx.xxx
```

各項目の説明は、以下のとおりです。

表 2-2 show vlan detail コマンドの表示項目

項番	説明
(1)	ポートの VLAN モードを表示します。 "C" 列はスタックのボックス ID を示します。スタックが無効な場合は 1 が表示されます。
(2)	VLAN ID ごとに、ポートのタグなし、またはタグ付きを表示します。 "C" 列はスタックのボックス ID を示します。スタックが無効な場合は 1 が表示されます。

2.2.3 VLAN 関連のインターフェース設定の表示

show vlan interface コマンドで、VLAN 関連のインターフェース設定を確認できます。

ポート 1/0/1 からポート 1/0/6 を指定した場合の表示例を以下に示します。

```
# show vlan interface port 1/0/1-6

 Port1/0/1 ...(1)
   VLAN mode              : Access ...(2)
   Access VLAN            : 10 ...(3)
   Ingress checking       : Enabled ...(4)
   Acceptable frame type  : Untagged-Only ...(5)

 Port1/0/2
   VLAN mode              : Trunk
   Native VLAN            : 1 (Untagged) ...(6)
   Trunk allowed VLAN     : 1-4094 ...(7)
   Ingress checking       : Enabled
   Acceptable frame type  : Admit-All

 Port1/0/3
   VLAN mode              : Hybrid
   Native VLAN            : 1 ...(8)
   Hybrid untagged VLAN   : 1,50,60 ...(9)
   Hybrid tagged VLAN     : 10,20 ...(10)
   Ingress checking       : Enabled
   Acceptable frame type  : Admit-All

 Port1/0/4
   VLAN mode              : Dot1q-Tunnel
   Access VLAN            : 10 ...(11)
   Hybrid untagged VLAN   : 50,60 ...(12)
   Ingress checking       : Enabled
   Acceptable frame type  : Admit-All

 Port1/0/5
   VLAN mode              : Promiscuous
   Native VLAN            : 100 ...(13)
   Ingress checking       : Enabled
   Acceptable frame type  : Admit-All

 Port1/0/6
   VLAN mode              : Host
   Native VLAN            : 101 ...(14)
   Ingress checking       : Enabled
   Acceptable frame type  : Admit-All
```

各項目の説明は、以下のとおりです。

表 2-3 show vlan interface コマンドの表示項目

項番	説明
(1)	ポート番号またはポートチャネル番号を表示します。
(2)	インターフェースの VLAN 動作モードを表示します。 • Access：アクセスモード • Trunk：トランクモード • Hybrid：ハイブリッドモード • Dot1q-Tunnel：トンネルモード • Promiscuous：プライベート VLAN のプロミスキャスポート • Host：プライベート VLAN のホストポート

項番	説明
(3)	アクセスモードのポートにおいて、**switchport access vlan** コマンドで設定したアクセス VLAN を表示します。
(4)	受信したフレームの受け入れチェックの有効 (Enabled) ／無効 (Disabled) を表示します。
(5)	受け入れ可能なフレームタイプを表示します。 • Tagged-Only：タグ付きフレームのみ • Untagged-Only：タグなしフレームのみ • Admit-All：すべてのフレーム
(6)	トランクモードのポートにおいて、**switchport trunk native vlan** コマンドで設定したネイティブ VLAN を表示します。 • (Untagged)：ネイティブ VLAN はタグなしモード • (tagged)：ネイティブ VLAN はタグ付きモード
(7)	トランクモードのポートにおいて、**switchport trunk allowed vlan** コマンドで許可した VLAN を表示します。
(8)	ハイブリッドモードのポートにおいて、**switchport hybrid native vlan** コマンドで設定したネイティブ VLAN を表示します。
(9)	ハイブリッドモードのポートにおいて、**switchport hybrid allowed vlan** コマンドの untagged 指定で許可した VLAN を表示します。
(10)	ハイブリッドモードのポートにおいて、**switchport hybrid allowed vlan** コマンドの tagged 指定で許可した VLAN を表示します。
(11)	トンネルモードのポートにおいて、**switchport access vlan** コマンドで設定したアクセス VLAN を表示します。
(12)	トンネルモードのポートにおいて、**switchport hybrid allowed vlan** コマンドの untagged 指定で許可した VLAN を表示します。
(13)	プライベート VLAN のプロミスキャスポートにおいて、**switchport private-vlan mapping** コマンドで設定したプライマリー VLAN を表示します。
(14)	プライベート VLAN のホストポートにおいて、**switchport private-vlan host-association** コマンドで設定したセカンダリー VLAN を表示します。

2.2.4 プロトコル VLAN の表示

プロトコル VLAN の設定を確認する方法を説明します。

2.2.4.1 プロトコルグループ設定の表示

show protocol-vlan profile コマンドで、プロトコルグループ設定を確認できます。

表示例を以下に示します。

```
# show protocol-vlan profile
 (1)          (2)           (3)
 Profile ID   Frame-type    Ether-type
 ----------   -----------   ----------------
 1            Ethernet2     0x86DD(IPv6)
 2            Ethernet2     0x0800(IP)
 3            Ethernet2     0x0806(ARP)
```

各項目の説明は、以下のとおりです。

表 2-4 show protocol-vlan profile コマンドの表示項目

項番	説明
(1)	プロトコルグループ ID を表示します。
(2)	フレームタイプの種類を表示します。
(3)	フレームタイプの値を表示します。

2.2.4.2 プロトコル VLAN 識別設定の表示

show protocol-vlan interface コマンドで、インターフェースに適用したプロトコル VLAN 識別設定を確認できます。

ポート 1/0/1 からポート 1/0/3 を指定した場合の表示例を以下に示します。

```
# show protocol-vlan interface port 1/0/1-3
 (1)              (2)                 (3)    (4)
 Interface        Protocol Group ID   VLAN   Priority
 --------------   -----------------   ----   --------
 Port1/0/1        1                   1      5
 Port1/0/2        10                  3      0
                  11                  2001   4
                  12                  3002   1
 Port1/0/3        2                   100    6
```

各項目の説明は、以下のとおりです。

表 2-5 show protocol-vlan interface コマンドの表示項目

項番	説明
(1)	ポート番号またはポートチャネル番号を表示します。
(2)	インターフェースに割り当てられているプロトコルグループ ID を表示します。
(3)	プロトコルグループにマッチした場合に受信する VLAN の VLAN ID を表示します。
(4)	受信フレームの CoS 値を表示します。

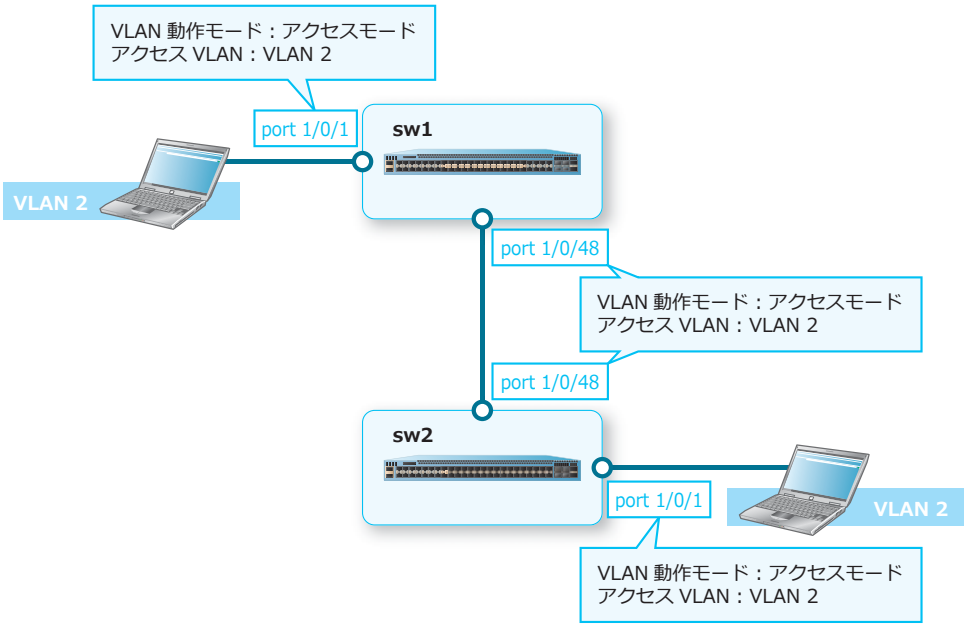
2.3 VLAN の構成例と設定例

VLAN を利用する場合の構成例と設定例を示します。

2.3.1 アクセスモードを利用する場合

アクセスポートを設定する場合の構成例と設定例を示します。この設定例では、PC を収容するポートと装置間の接続ポートの両方をアクセスポートで構成しています。なお、本設定例では sw1 の設定のみ示します。

図 2-5 アクセスモードの場合の構成例



1. VLAN 2 を作成します。

```
sw1# configure terminal
sw1(config)# vlan 2
sw1(config-vlan)# exit
sw1(config)#
```

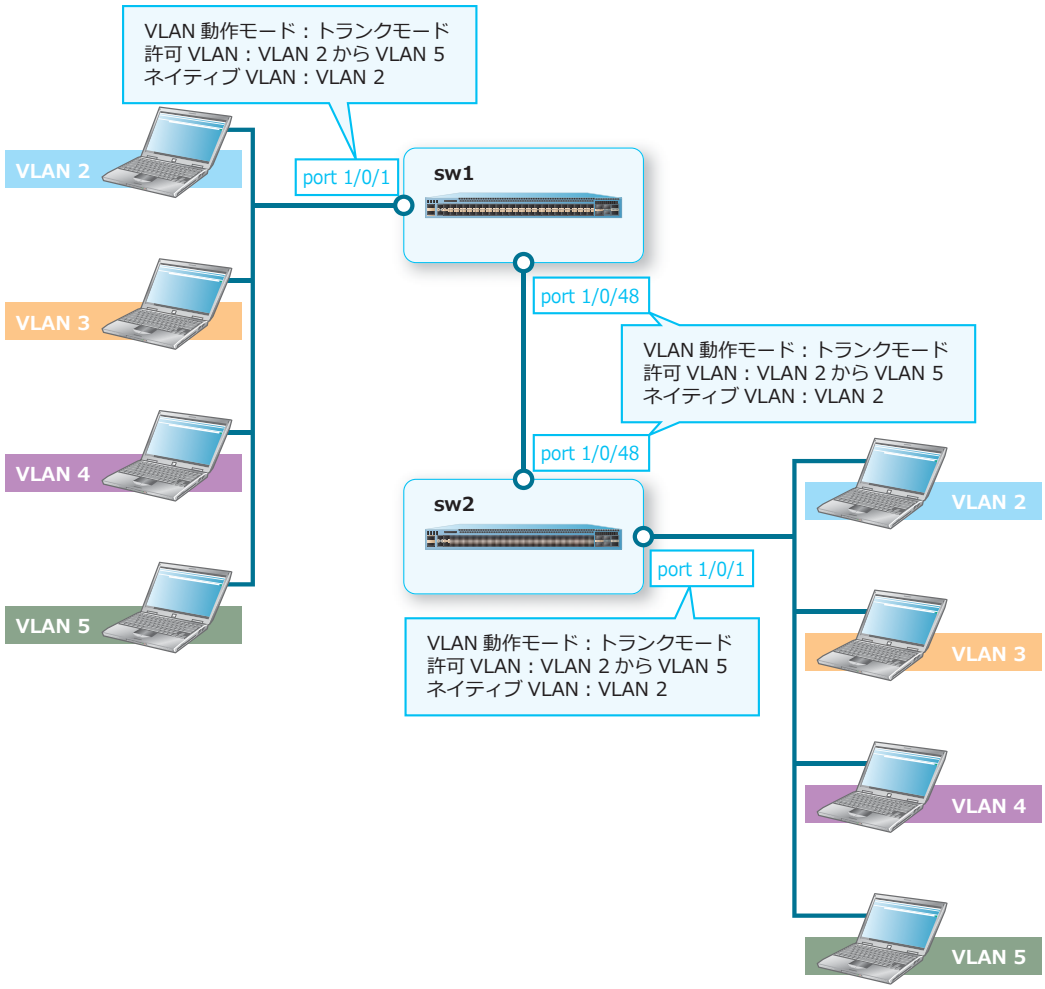
2. ポート 1/0/1 およびポート 1/0/48 をアクセスポートとして設定し、アクセスポートに［VLAN 2］を割り当てます。

```
sw1(config)# interface range port 1/0/1,1/0/48
sw1(config-if-port-range)# switchport mode access
sw1(config-if-port-range)# switchport access vlan 2
sw1(config-if-port-range)# end
sw1#
```

2.3.2 トランクモードを利用する場合

トランクポートを設定する場合の構成例と設定例を示します。この設定例では、PC を収容するポートと装置間の接続ポートの両方をトランクポートで構成しています。なお、本設定例では sw1 の設定のみ示します。

図 2-6 トランクモードの場合の構成例



1. VLAN 2 から VLAN 5 を作成します。

```
sw1# configure terminal
sw1(config)# vlan 2-5
sw1(config-vlan)# exit
sw1(config)#
```

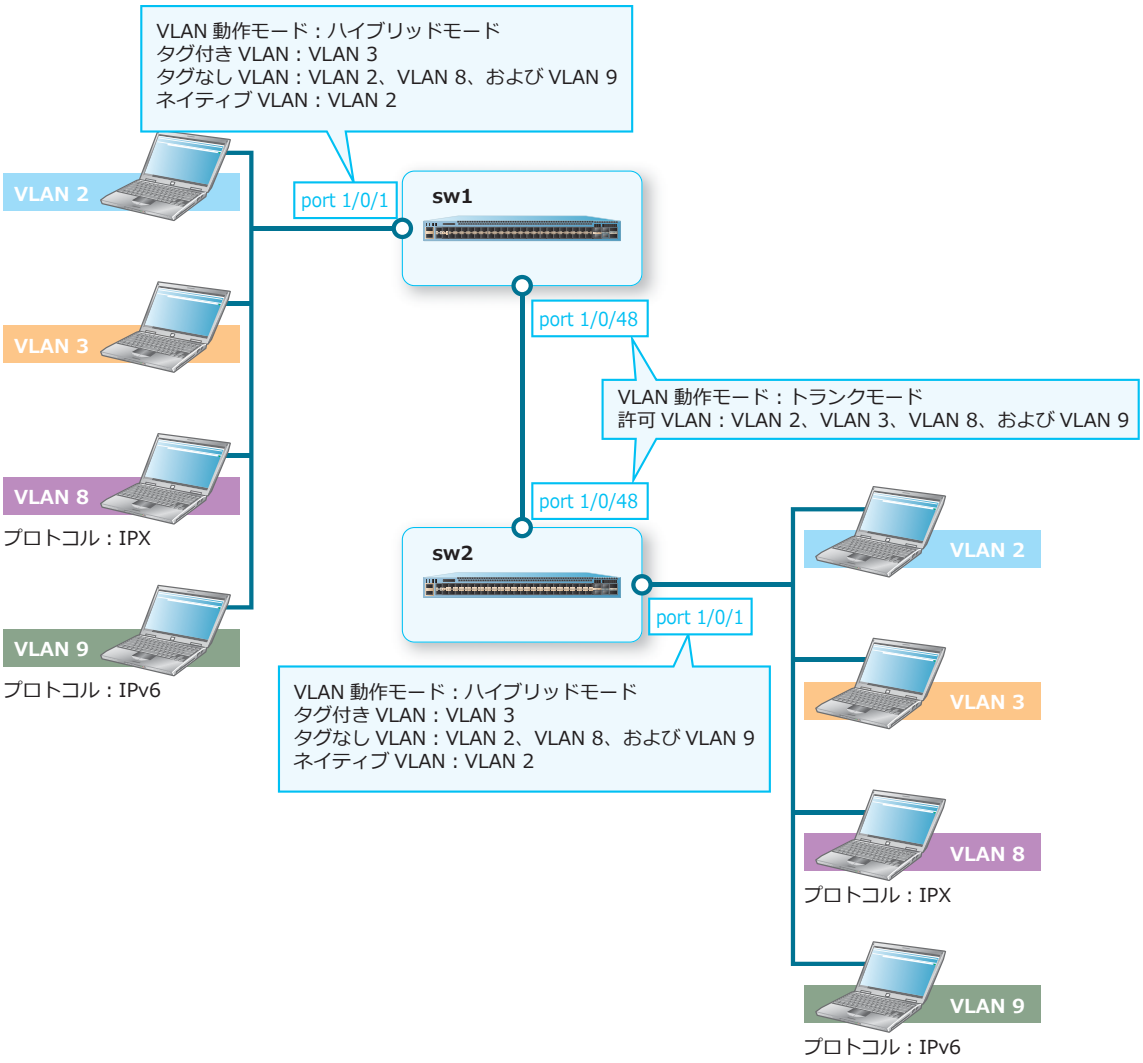
2. ポート 1/0/1 およびポート 1/0/48 をトランクポートとして設定し、トランクポートに［VLAN 2 から VLAN 5］を割り当てます。また、トランクポートのネイティブ VLAN を［VLAN 2］に設定します。

```
sw1(config)# interface port 1/0/1
sw1(config-if-port)# switchport mode trunk
sw1(config-if-port)# switchport trunk allowed vlan 2-5
sw1(config-if-port)# switchport trunk native vlan 2
sw1(config-if-port)# exit
sw1(config)# interface port 1/0/48
sw1(config-if-port)# switchport mode trunk
sw1(config-if-port)# switchport trunk allowed vlan 2-5
sw1(config-if-port)# switchport trunk native vlan 2
sw1(config-if-port)# exit
sw1(config)#
```

2.3.3 ハイブリッドモードを利用する場合

ハイブリッドポートを設定する場合の構成例と設定例を示します。この設定例では、PC を収容するポートをハイブリッドポートで、装置間の接続ポートをトランクポートで構成しています。ハイブリッドポートでは、受信したタグなしフレームのプロトコルが IPX の場合は VLAN 8 で受信し、プロトコルが IPv6 の場合は VLAN 9 で受信します。また、IPX と IPv6 以外の場合は、VLAN 2 で受信するようにします。なお、本設定例では sw1 の設定のみ示します。

図 2-7 ハイブリッドモードの場合の構成例



1. VLAN 2、VLAN 3、VLAN 8、および VLAN 9 を作成します。

```
sw1# configure terminal
sw1(config)# vlan 2,3,8,9
sw1(config-vlan)# exit
sw1(config)#
```

2. プロトコルグループを以下のように設定します。

プロトコルグループ ID［1］：フレームタイプの種類［ethernet2］、フレームタイプの値［0x8137］

プロトコルグループ ID［2］：フレームタイプの種類［ethernet2］、フレームタイプの値［0x86DD］

```
sw1(config)# protocol-vlan profile 1 frame-type ethernet2 ether-type 0x8137
sw1(config)# protocol-vlan profile 2 frame-type ethernet2 ether-type 0x86dd
sw1(config)#
```

3. ポート 1/0/1 をハイブリッドポートとして設定し、ハイブリッドポートのタグ付き VLAN に［VLAN 3］を、タグなし VLAN に［VLAN 2、VLAN 8、および VLAN 9］を割り当てます。また、ハイブリッドポートのネイティブ VLAN を［VLAN 2］に設定します。

```
sw1(config)# interface port 1/0/1
sw1(config-if-port)# switchport mode hybrid
sw1(config-if-port)# switchport hybrid allowed vlan tagged 3
sw1(config-if-port)# switchport hybrid allowed vlan untagged 2,8,9
sw1(config-if-port)# switchport hybrid native vlan 2
sw1(config-if-port)# exit
sw1(config)#
```

4. ポート 1/0/48 をトランクポートとして設定し、トランクポートに［VLAN 2、VLAN 3、VLAN 8、および VLAN 9］を割り当てます。

```
sw1(config)# interface port 1/0/48
sw1(config-if-port)# switchport mode trunk
sw1(config-if-port)# switchport trunk allowed vlan 2,3,8,9
sw1(config-if-port)# exit
sw1(config)#
```

5. ポート 1/0/1 で、プロトコルグループ ID［1］の設定に一致したフレームを VLAN 8 として設定し、プロトコルグループ ID［2］の設定に一致したフレームを VLAN 9 として設定します。

```
sw1(config)# interface port 1/0/1
sw1(config-if-port)# protocol-vlan profile 1 vlan 8
sw1(config-if-port)# protocol-vlan profile 2 vlan 9
sw1(config-if-port)# end
sw1#
```

3. プライベート VLAN

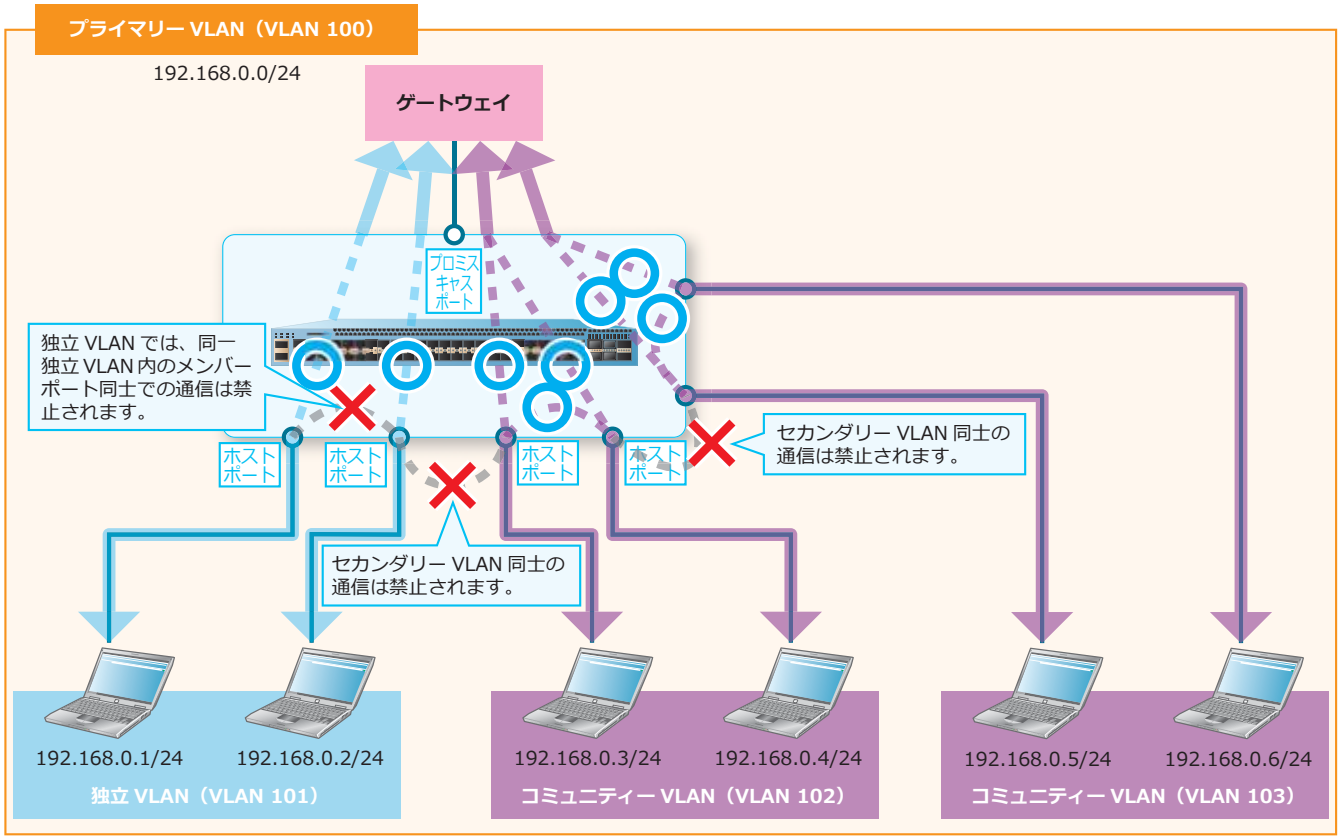
プライベート VLAN の機能、状態の確認方法、および構成例と設定例について説明します。

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。

3.1 プライベート VLAN の機能説明

プライベート VLAN は、レイヤー 2 レベルでトラフィックを分離するための機能です。1 つの**プライマリー VLAN** に、1 つ以上の**セカンダリー VLAN**（1 つの独立 VLAN、複数のコミュニティー VLAN）を関連付けて設定します。異なるセカンダリー VLAN 間での通信が制限されることにより、トラフィックの中継可能範囲を分離します。

図 3-1 プライベート VLAN の概要



プライマリー VLAN、セカンダリー VLAN（独立 VLAN、コミュニティー VLAN）に割り当てるポートの種別と動作について、以下に示します。

NOTE: プライベート VLAN のポート (プロミスキャスポート、ホストポート) では、タグなしフレーム形式で送受信します。

- **プライマリー VLAN**

  プライマリー VLAN のポートは、プロミスキャスポート（Promiscuous Port）として設定します。プロミスキャスポートで受信したトラフィックは、すべてのプロミスキャスポートとホストポートに中継可能です。

- **独立 VLAN（Isolated VLAN）**

  独立 VLAN のホストポート（Isolated Port）で受信したトラフィックは、プロミスキャスポートにのみ中継可能です。独立 VLAN の別のホストポートや、コミュニティー VLAN のホストポートには中継しません。

- **コミュニティー VLAN（Community VLAN）**

  コミュニティー VLAN のホストポート（Community Port）で受信したトラフィックは、プロミスキャスポート、および同じコミュニティー VLAN の別のホストポートに中継可能です。異なるコミュニティー VLAN のホストポートや、独立 VLAN のホストポートには中継しません。

プライベート VLAN の種別は、**private-vlan** コマンドで設定します。プライマリー VLAN に、セカンダリー VLAN を関連付けるには、**private-vlan association** コマンドを使用します。

プライベート VLAN のポート種別は、**switchport mode private-vlan** コマンドで設定します。プロミスキャスポートとして割り当てるには、**switchport private-vlan mapping** コマンドを使用します。ホストポートとして割り当てるには、**switchport private-vlan host-association** コマンドを使用します。

3.1.1 プライベート VLAN の制限事項

プライベート VLAN を使用する場合は、以下の制限事項があります。

- プライベート VLAN では、通常の VLAN より多くの MAC アドレステーブルを使用します。
- VLAN 1 はプライベート VLAN として使用できません。
- セカンダリー VLAN では、VLAN インターフェースを作成して IP アドレスを設定することはできません。プライマリー VLAN では設定できますが、ホストポート経由ではその IP アドレスとの通信（Telnet や ping など、すべての IP 通信）はできません。

また、プライベート VLAN では、以下の機能との併用は不可、または未サポートです。

- プライベート VLAN と他 VLAN との間のレイヤー 3 中継
- OSPF や VRRP など、すべてのレイヤー 3 関連機能（ただし、プロミスキャスポート経由の管理用のスタティックルートは除く）
- DHCP 関連機能、CFM 機能、IGMP スヌーピング機能、MLD スヌーピング機能、RPVST+ 機能、VLAN ベースモードのループ検知機能
- AccessDefender 機能のダイナミック VLAN、Gateway 認証、DHCP スヌーピング
- その他、ホストポート経由で装置の IP アドレスとの通信が関連する機能

3.1.2 スイッチを跨いでプライベート VLAN を構築する場合

プライベート VLAN では、基本的にプロミスキャスポートとホストポートを使用しますが、スイッチを跨いで同じポリシーのプライベート VLAN を構築する場合のみ、スイッチ間を接続するポートはトランクポート設定で接続します。この場合、スイッチを跨いでもプライベート VLAN の動作を維持するために、通常のトランクポートの動作ではなく、以下のような動作になります。

- トランクポートで受信したプライマリー VLAN のタグ付きフレームは、すべてのポートに中継可能です。
- トランクポートで受信した独立 VLAN のタグ付きフレームは、プロミスキャスポートと別のトランクポートにのみ中継可能です。独立 VLAN のホストポートや、コミュニティー VLAN のホストポートには中継しません。
- トランクポートで受信したコミュニティー VLAN のタグ付きフレームは、プロミスキャスポート、トランクポート、および同じコミュニティー VLAN のホストポートに中継可能です。異なるコミュニティー VLAN のホストポートや、独立 VLAN のホストポートには中継しません。

ただし、この構成の場合、以下のようなフラッディングトラフィックが増える仕様制限があることに注意してください。以下では、2 台のスイッチ（SW1 と SW2）をトランクポート設定で接続している構成を例に説明します。

- SW1 のプロミスキャスポートで受信し、宛先 MAC アドレスの端末が SW2 のホストポートの先に存在する場合、そのトラフィックは SW1 では常にフラッディング中継動作になります。
- SW1 のホストポートで受信し、宛先 MAC アドレスの端末が SW2 のプロミスキャスポートの先に存在する場合、そのトラフィックは SW1 では常にフラッディング中継動作になります。

3.2 プライベート VLAN の状態確認

show vlan private-vlan コマンドで、プライベート VLAN の設定を確認できます。

表示例を以下に示します。

```
# show vlan private-vlan
(1)             (2)               (3)        (4)
Primary VLAN    Secondary VLAN    Type       Interface
------------------------------------------------------
300             200               Isolated     1/0/9-1/0/16,1/0/24
300             100               Community    1/0/1-1/0/8,1/0/24

Total Entries: 2
```

各項目の説明は、以下のとおりです。

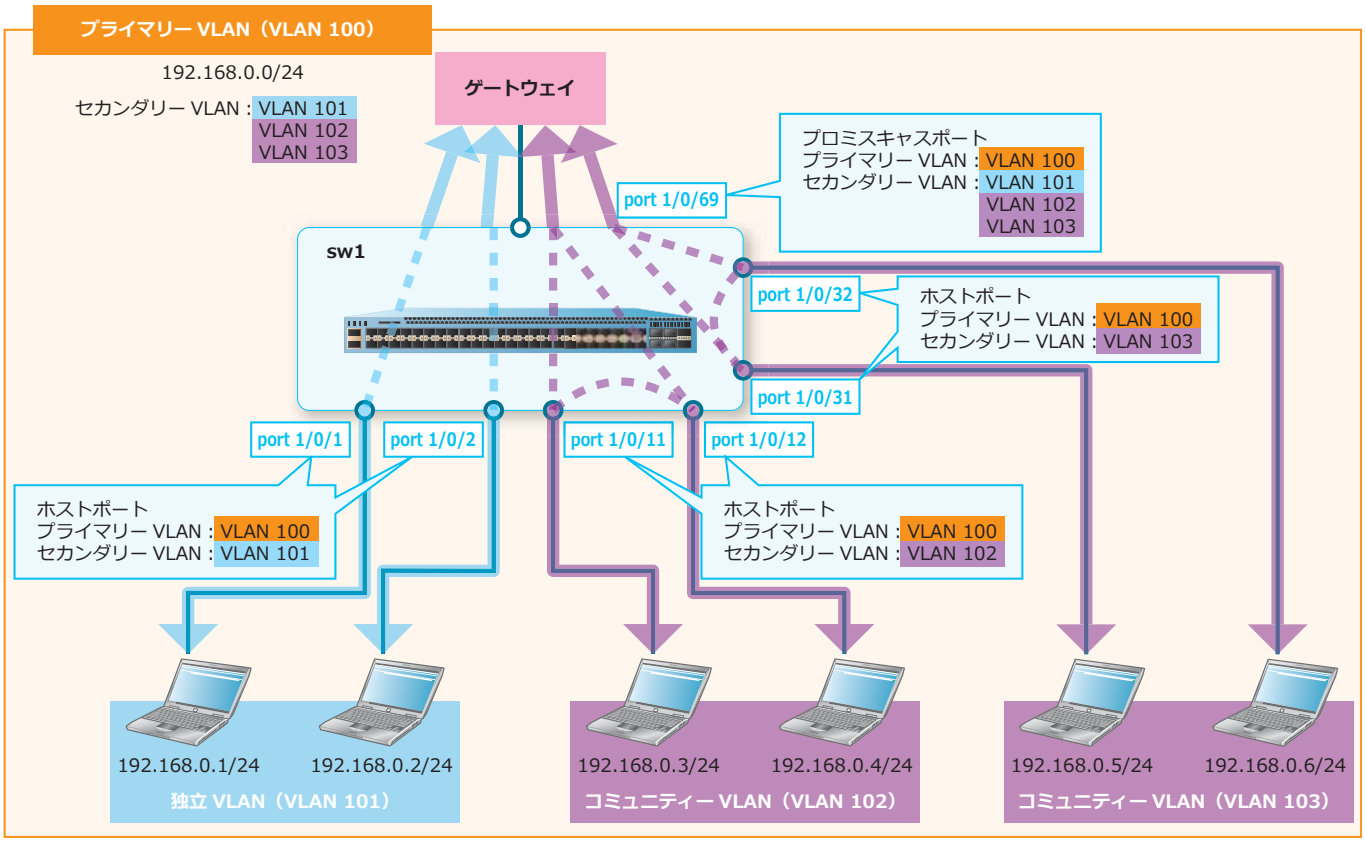
表 3-1 show vlan private-vlan コマンドの表示項目

項番	説明
(1)	プライマリー VLAN の VLAN ID を表示します。
(2)	セカンダリー VLAN の VLAN ID を表示します。
(3)	セカンダリー VLAN のタイプを表示します。 • Isolated：独立 VLAN • Community：コミュニティー VLAN
(4)	ポート番号を表示します。ポートチャネルでプライベート VLAN を設定した場合は、すべてのメンバーポートのポート番号が表示されます。

3.3 プライベート VLAN の構成例と設定例

独立 VLAN および 2 つのコミュニティー VLAN を利用する場合の構成例と設定例を示します。

図 3-2 プライベート VLAN の構成例



1. VLAN 101 を作成し、独立 VLAN として設定します。

```
sw1# configure terminal
sw1(config)# vlan 101
sw1(config-vlan)# private-vlan isolated
sw1(config-vlan)# exit
sw1(config)#
```

2. VLAN 102 および VLAN 103 を作成し、コミュニティー VLAN として設定します。

```
sw1(config)# vlan 102,103
sw1(config-vlan)# private-vlan community
sw1(config-vlan)# exit
sw1(config)#
```

3. VLAN 100 を作成し、プライマリー VLAN として設定します。また、VLAN 100 のセカンダリー VLAN として［VLAN 101 から VLAN 103］を登録します。

```
sw1(config)# vlan 100
sw1(config-vlan)# private-vlan primary
sw1(config-vlan)# private-vlan association add 101-103
sw1(config-vlan)# exit
sw1(config)#
```

4. ポート 1/0/69 をプロミスキャスポートとして設定し、プライマリー VLAN に［VLAN 100］を、セカンダリー VLAN に［VLAN 101 から VLAN 103］を割り当てます。

```
sw1(config)# interface port 1/0/69
sw1(config-if-port)# switchport mode private-vlan promiscuous
sw1(config-if-port)# switchport private-vlan mapping 100 add 101-103
sw1(config-if-port)# exit
sw1(config)#
```

5. ポート 1/0/1 およびポート 1/0/2 をホストポートとして設定し、プライマリー VLAN に［VLAN 100］を、セカンダリー VLAN に［VLAN 101］を割り当てます。

```
sw1(config)# interface range port 1/0/1,1/0/2
sw1(config-if-port-range)# switchport mode private-vlan host
sw1(config-if-port-range)# switchport private-vlan host-association 100 101
sw1(config-if-port-range)# exit
sw1(config)#
```

6. ポート 1/0/11 およびポート 1/0/12 をホストポートとして設定し、プライマリー VLAN に［VLAN 100］を、セカンダリー VLAN に［VLAN 102］を割り当てます。

```
sw1(config)# interface range port 1/0/11,1/0/12
sw1(config-if-port-range)# switchport mode private-vlan host
sw1(config-if-port-range)# switchport private-vlan host-association 100 102
sw1(config-if-port-range)# exit
sw1(config)#
```

7. ポート 1/0/31 およびポート 1/0/32 をホストポートとして設定し、プライマリー VLAN に［VLAN 100］を、セカンダリー VLAN に［VLAN 103］を割り当てます。

```
sw1(config)# interface range port 1/0/31,1/0/32
sw1(config-if-port-range)# switchport mode private-vlan host
sw1(config-if-port-range)# switchport private-vlan host-association 100 103
sw1(config-if-port-range)# end
sw1#
```

4. VLAN トンネル／ VLAN 変換

VLAN トンネルと VLAN 変換の機能、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。

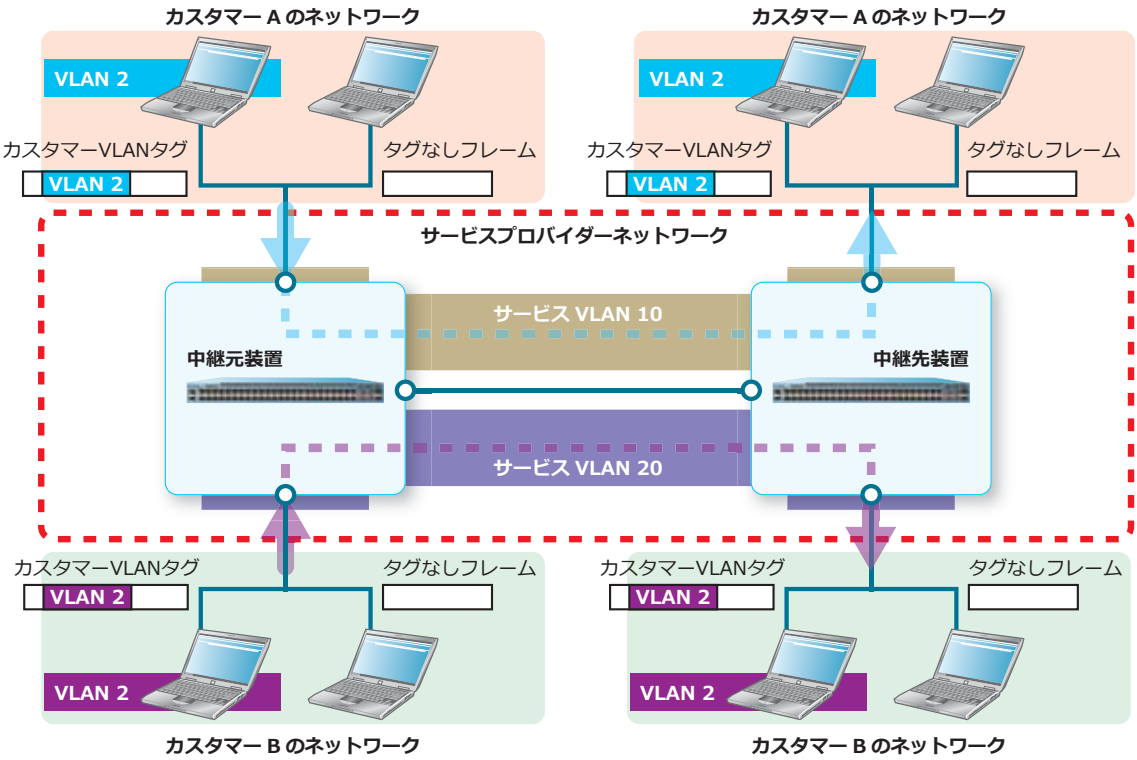
REF: コマンドの詳細については、『コマンドリファレンス』を参照してください。

4.1 VLAN トンネルの機能説明

VLAN トンネルは、VLAN タグ付きフレームにさらに VLAN タグを付与して中継する機能で、**Q-in-Q** とも呼ばれます。サービスプロバイダーで複数のカスタマーに広域 VLAN サービスを提供する際などに使用されます。

カスタマーネットワークで送受信するタグ付きフレームの VLAN タグのことを、**カスタマー VLAN タグ**と呼びます。また、サービスプロバイダーネットワークで送受信するタグ付きフレームの VLAN タグ、または 2 段タグ付きフレームの外側の VLAN タグのことを、**サービスプロバイダー VLAN タグ**（以後、**サービス VLAN タグ**）と呼びます。

図 4-1 VLAN トンネルの概要

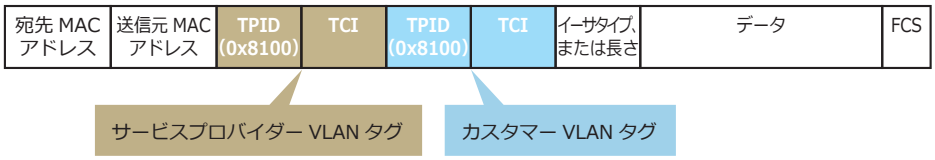


VLAN トンネルを使用すると、中継元装置で受信したカスタマーネットワークからのトラフィック（カスタマー VLAN のタグ付きフレーム、タグなしフレーム）は、サービスプロバイダーネットワークでは**サービスプロバイダー VLAN**（以後、**サービス VLAN**）で中継され、中継先装置からカスタマーネットワークに送信します。これにより、透過的にカスタマーのトラフィックを中継します。

4.1.1 TPID（Tag Protocol Identifier）の設定

TPID は、受信したフレームに VLAN タグが付与されているかどうかを判断するための識別子です。デフォルト設定では、カスタマー VLAN タグとサービス VLAN タグの TPID は 0x8100 に設定されています。

図 4-2 2 段タグ付きフレームのフレームフォーマット



カスタマー VLAN タグの TPID を設定するには、**dot1q inner ethertype** コマンドを使用します。サービス VLAN タグの TPID を設定するには、**dot1q tunneling ethertype** コマンドを使用します。

NOTE: カスタマー VLAN タグの TPID 設定は、装置全体の設定です。

NOTE: サービス VLAN タグの TPID 設定は、トランクポートでのみ設定できます。

NOTE: 2 段タグ付きフレームを受信した場合、MAC アドレステーブルではサービス VLAN タグの VLAN ID で学習します。カスタマー VLAN タグの VLAN ID で学習することはできません。

4.1.2 シンプルな VLAN トンネル

VLAN トンネルを使用する場合は、ポートの役割ごとに以下のように設定します。以下の設定方法の場合は、1 つのトンネルポートに 1 つのサービス VLAN を登録できます。

表 4-1 シンプルな VLAN トンネルの設定コマンド

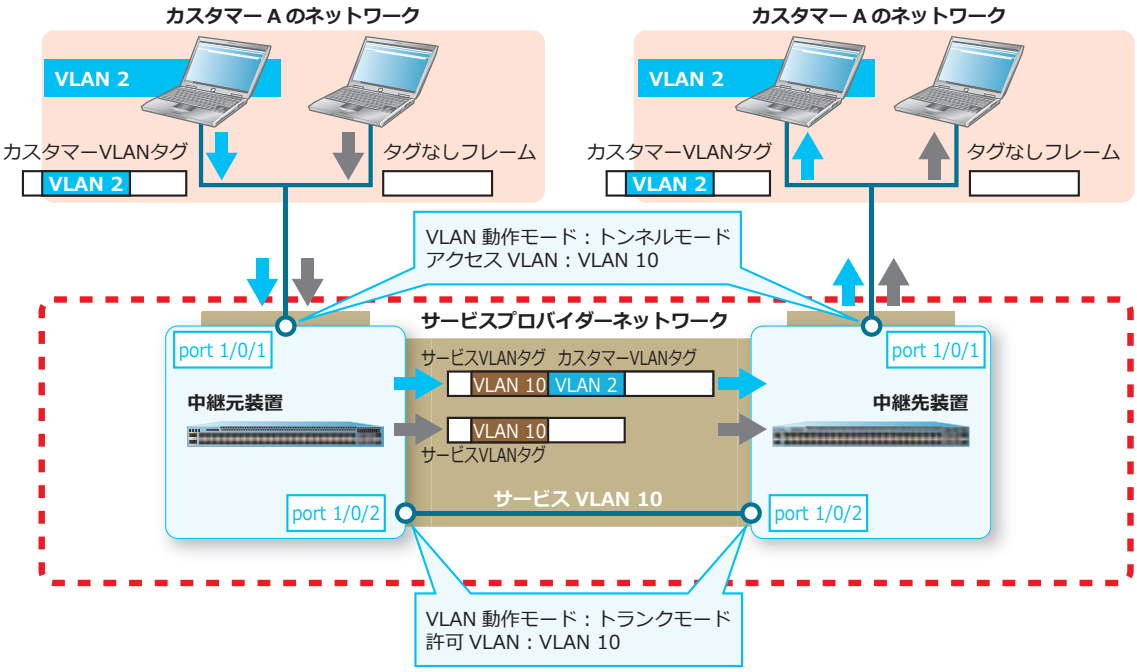
ポートの役割	概要と設定コマンド
カスタマーを収容するポート	• VLAN 動作モード：トンネルモード（**switchport mode dot1q-tunnel** コマンド） • VLAN 登録コマンド：**switchport access vlan** コマンド
装置間で VLAN を多重化して中継するポート	• VLAN 動作モード：トランクモード（**switchport mode trunk** コマンド） • VLAN 登録コマンド：**switchport trunk allowed vlan** コマンド

VLAN トンネルの中継元装置では、カスタマーを収容するトンネルポートで、タグなしフレームまたはカスタマー VLAN のタグ付きフレームを受信します。受信したフレームにはサービス VLAN タグが付与され、トランクポートからサービスプロバイダーネットワークに送信されます。サービスプロバイダーネットワークでは、サービス VLAN のタグ付きフレームとして中継されます。

NOTE: トンネルポートで受信したフレームをカスタマー VLAN のタグ付きフレームとして識別するための TPID は、**dot1q inner ethertype** コマンドで設定した TPID です。

VLAN トンネルの中継先装置では、トランクポートでサービス VLAN のタグ付きフレームを受信します。受信したフレームからサービス VLAN タグが削除され、トンネルポートからカスタマーネットワークに送信されます。

図 4-3 シンプルな VLAN トンネルの例



4.1.3 サービス VLAN マッピングエントリー

switchport vlan mapping original-vlan dot1q-tunnel コマンドでサービス VLAN マッピングエントリーを設定した場合は、トンネルポートで受信したフレームのカスタマー VLAN から受信サービス VLAN を指定できます。この使用方法の場合は、ポートの役割ごとに以下のように設定します。1 つのトンネルポートに、複数のサービス VLAN を登録できます。

表 4-2 サービス VLAN マッピングエントリーによる VLAN トンネルの設定コマンド

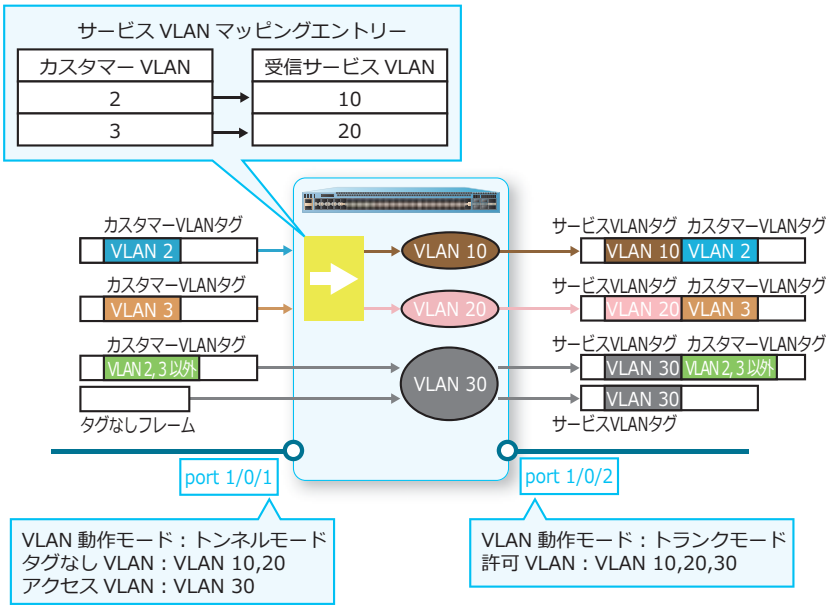
ポートの役割	概要と設定コマンド
カスタマーを収容するポート	• VLAN 動作モード：トンネルモード（**switchport mode dot1q-tunnel** コマンド） • **switchport vlan mapping original-vlan 受信フレームのカスタマーVLAN dot1q-tunnel 受信サービス VLAN [priority COS]** コマンドで、サービス VLAN マッピングエントリーを設定する。 • サービス VLAN マッピングエントリー対象の受信サービス VLAN の場合は、**switchport hybrid allowed vlan untagged** コマンドで登録する。複数登録可能。 • サービス VLAN マッピングエントリーの対象外のフレームを受信するサービス VLAN は、**switchport access vlan** コマンドで 1 つだけ登録可能。
装置間で VLAN を多重化して中継するポート	• VLAN 動作モード：トランクモード（**switchport mode trunk** コマンド） • VLAN 登録コマンド：**switchport trunk allowed vlan** コマンド

NOTE: **switchport vlan mapping original-vlan dot1q-tunnel** コマンドは、トンネルポートでのみサポートしています。

NOTE: 同一インターフェースで、1 つの受信サービス VLAN に対して複数のサービス VLAN マッピングエントリーを設定できます。

NOTE: priority パラメーターを指定しないで設定すると、priority 0 が自動的に設定されます。

図 4-4 サービス VLAN マッピングエントリーによる VLAN トンネルの例



この例では、トンネルポートに設定したポート 1/0/1 でカスタマー VLAN 2 のタグ付きフレームを受信した場合はサービス VLAN 10 で受信し、カスタマー VLAN 3 のタグ付きフレームを受信した場合はサービス VLAN 20 で受信します。また、サービス VLAN マッピングエントリーに一致しない場合は、サービス VLAN 30 で受信します。

4.1.4 トンネルポートでの VLAN 変換エントリー

トンネルポートで、**`switchport vlan mapping original-vlan resultant-vlan`** コマンドで VLAN 変換エントリーを設定した場合は、受信したフレームのカスタマー VLAN から受信サービス VLAN を指定でき、カスタマー VLAN タグを削除して受信します。さらに、そのトンネルポートから送信する際に、カスタマー VLAN タグを付与して送信します。この使用方法の場合は、ポートの役割ごとに以下のように設定します。1 つのトンネルポートに、複数のサービス VLAN を登録できます。

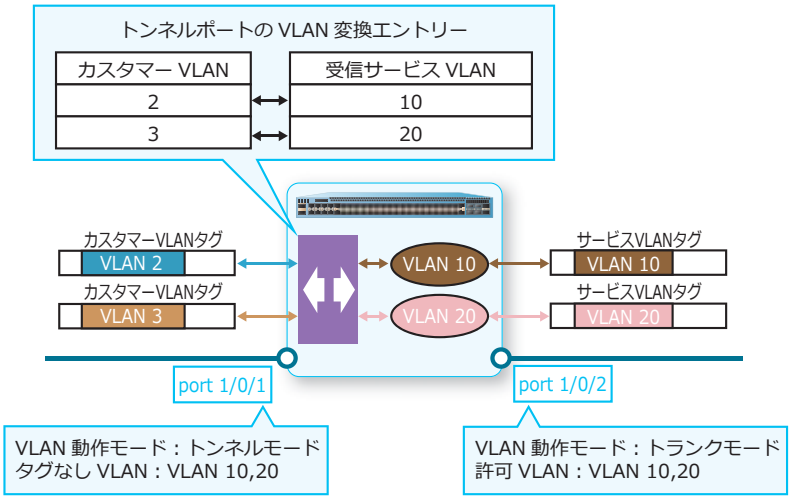
表 4-3 トンネルポートの VLAN 変換エントリーによる VLAN トンネルの設定コマンド

ポートの役割	概要と設定コマンド
カスタマーを収容するポート	• VLAN 動作モード：トンネルモード（**`switchport mode dot1q-tunnel`** コマンド） • **`switchport vlan mapping original-vlan`** **受信フレームのカスタマー VLAN** **`resultant-vlan`** **受信サービス VLAN** **`[priority COS]`** コマンドで、VLAN 変換エントリーによる VLAN マッピングを設定する。 • VLAN マッピング対象の受信サービス VLAN の場合は、**`switchport hybrid allowed vlan untagged`** コマンドで登録する。複数登録可能。 • VLAN マッピングの対象外のフレームを受信するサービス VLAN は、**`switchport access vlan`** コマンドで 1 つだけ登録可能。
装置間で VLAN を多重化して中継するポート	• VLAN 動作モード：トランクモード（**`switchport mode trunk`** コマンド） • VLAN 登録コマンド：**`switchport trunk allowed vlan`** コマンド

NOTE: 同一インターフェースでは、1 つの装置内のサービス VLAN に対して設定できる VLAN 変換エントリーは、1 エントリーのみです。

NOTE: priority パラメーターを指定しないで設定すると、priority 0 が自動的に設定されます。

図 4-5 VLAN 変換エントリーによる VLAN トンネルの設定コマンド



この例では、トンネルポートに設定したポート 1/0/1 でカスタマー VLAN 2 のタグ付きフレームを受信した場合は、カスタマー VLAN タグを削除してサービス VLAN 10 で受信します。ポート 1/0/1 のサービス VLAN 10 から送信する場合には、カスタマー VLAN 2 のタグ付きフレームとして送信します。同様に、トンネルポートに設定したポート 1/0/1 でカスタマー VLAN 3 のタグ付きフレームを受信した場合は、カスタマー VLAN タグを削除してサービス VLAN 20 で受信します。ポート 1/0/1 のサービス VLAN 20 から送信する場合には、カスタマー VLAN 3 のタグ付きフレームとして送信します。

4.1.5 VLAN マッピングプロファイル

VLAN マッピングプロファイルで VLAN マッピングルールを設定した場合は、トンネルポートで受信したフレームの任意の情報から受信サービス VLAN を指定できます。この使用方法の場合は、ポートの役割ごとに以下のように設定します。1 つのトンネルポートに、複数のサービス VLAN を登録できます。

表 4-4 VLAN マッピングプロファイルによる LAN トンネルの設定コマンド

ポートの役割	概要と設定コマンド
カスタマーを収容するポート	• VLAN 動作モード：トンネルモード（**`switchport mode dot1q-tunnel`** コマンド） • VLAN マッピングプロファイルを **`vlan mapping profile`** コマンドで作成し、**`vlan mapping rule`** コマンドで VLAN マッピングルールを登録する。そして、**`switchport vlan mapping profile`** コマンドでインターフェースに VLAN マッピングプロファイルを適用する。 • VLAN マッピングルール対象の受信サービス VLAN の場合は、**`switchport hybrid allowed vlan untagged`** コマンドで登録する。複数登録可能。 • VLAN マッピングルールの対象外のフレームを受信するサービス VLAN は、**`switchport access vlan`** コマンドで 1 つだけ登録可能。
装置間で VLAN を多重化して中継するポート	• VLAN 動作モード：トランクモード（**`switchport mode trunk`** コマンド） • VLAN 登録コマンド：**`switchport trunk allowed vlan`** コマンド

NOTE: VLAN マッピングプロファイルは、トンネルポートでのみサポートしています。

NOTE: **`vlan mapping rule`** コマンドで priority パラメーターを指定しないで設定すると、priority 0 が自動的に設定されます。

VLAN マッピングプロファイルの作成

VLAN マッピングプロファイルを最初に作成する際に、プロファイルタイプを指定します。指定するプロファイルタイプによって、使用できる抽出条件が異なります。VLAN マッピングプロファイルを作成するには、**vlan mapping profile** コマンドを使用します。

表 4-5 VLAN マッピングプロファイルのタイプと抽出条件

プロファイルタイプ	使用できる抽出条件（設定パラメーター）
ethernet	送信元 MAC アドレス（src-mac）、宛先 MAC アドレス（dst-mac）、カスタマー VLAN タグの CoS 値（priority）、カスタマー VLAN タグの VLAN ID（inner-vid）、イーサタイプ（ether-type）
ip	送信元 IP アドレス（src-ip）、宛先 IP アドレス（dst-ip）、DSCP（dscp）、送信元 L4 ポート番号（src-port）、宛先 L4 ポート番号（dst-port）、IP プロトコル番号（ip-protocol）
ipv6	送信元 IPv6 アドレス（src-ipv6）、宛先 IPv6 アドレス（dst-ipv6）
ethernet & ip	送信元 MAC アドレス（src-mac）、宛先 MAC アドレス（dst-mac）、カスタマー VLAN タグの CoS 値（priority）、カスタマー VLAN タグの VLAN ID（inner-vid）、イーサタイプ（ether-type）、送信元 IP アドレス（src-ip）、宛先 IP アドレス（dst-ip）、DSCP（dscp）、送信元 L4 ポート番号（src-port）、宛先 L4 ポート番号（dst-port）、IP プロトコル番号（ip-protocol）

NOTE: 1 つの VLAN マッピングルールで複数の抽出条件を指定する場合は、表に記載の順番でパラメーターを指定してください。

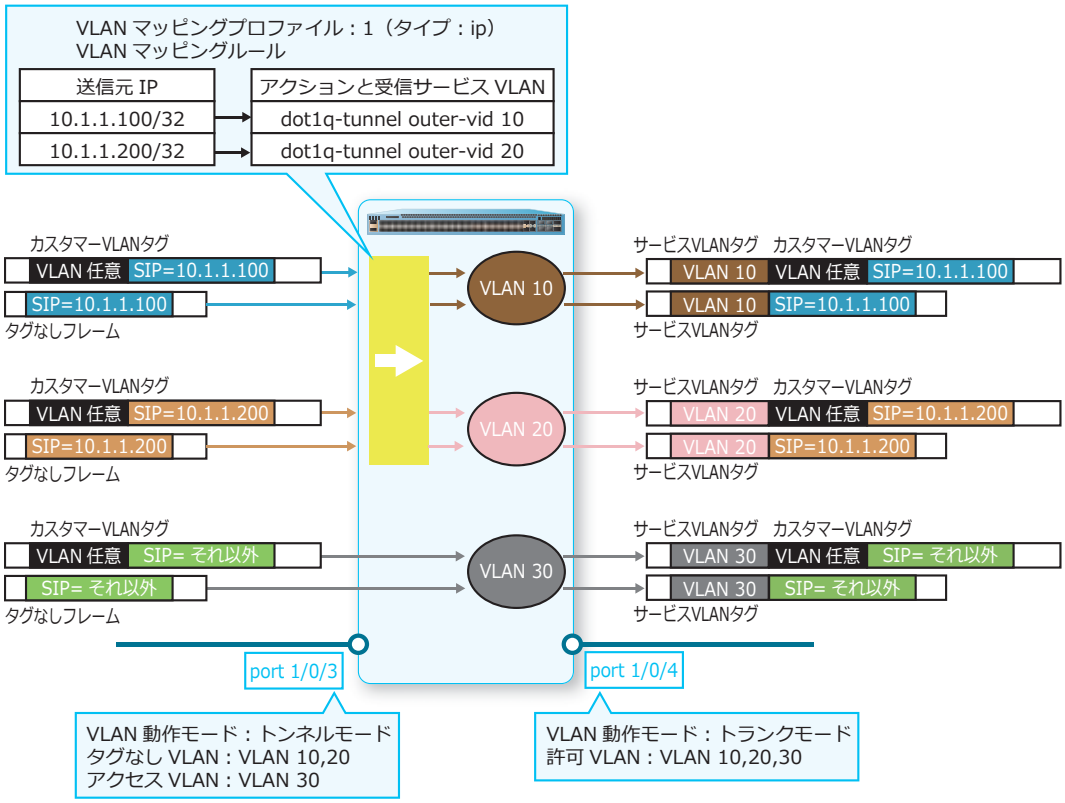
VLAN マッピングルールの設定

作成した VLAN マッピングプロファイルに、VLAN マッピングルールを設定します。各ルールでは、抽出条件とアクションを設定します。VLAN マッピングルールを設定するには、**vlan mapping rule** コマンドを使用します。

- アクションを dot1q-tunnel outer-vid **受信サービス VLAN** [priority COS] [inner-vid VLAN-ID] パラメーターで指定した場合は、受信したフレームをそのままの形式で受信します。
- アクションを translate outer-vid **受信サービス VLAN** [priority COS] パラメーターで指定した場合は、受信したフレームがカスタマー VLAN のタグ付きフレームの場合、カスタマー VLAN タグを削除して受信します。

NOTE: **vlan mapping rule** コマンドでシーケンス番号を指定しない場合は、開始値 10 から増分値 10 でインクリメントした番号のうち、まだ使用されていない最も小さい番号が自動的に割り当てられます。

図 4-6 VLAN マッピングプロファイルによる VLAN トンネルの例



この例では、トンネルポートに設定したポート 1/0/3 で送信元 IP アドレスが 10.1.1.100 のパケットを受信した場合はサービス VLAN 10 で受信し、送信元 IP アドレスが 10.1.1.200 のパケットを受信した場合はサービス VLAN 20 で受信します。また、VLAN マッピングルールに一致しない場合は、サービス VLAN 30 で受信します。

4.1.6 VLAN マッピングのオプション

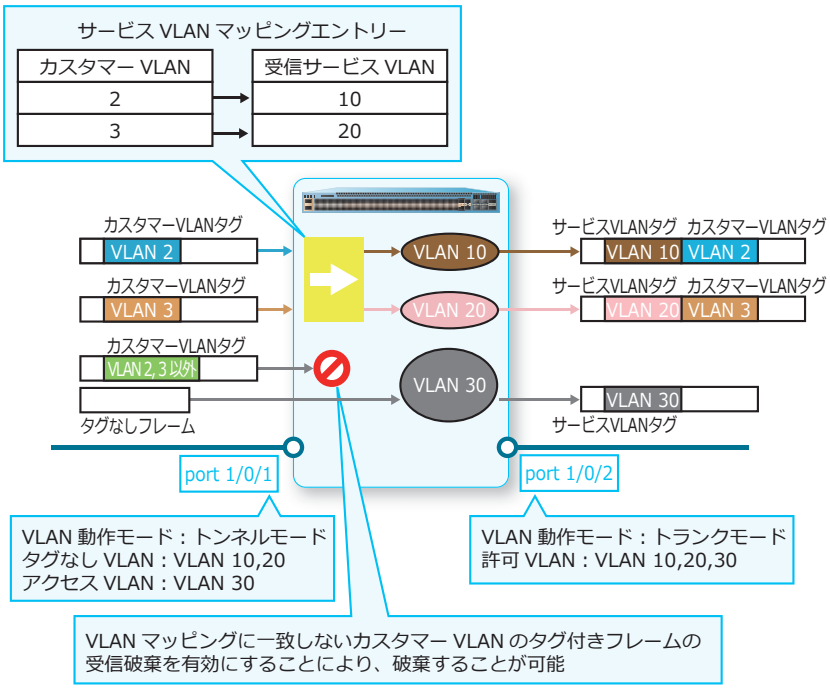
VLAN マッピングのオプションについて説明します。

VLAN マッピングに一致しないカスタマー VLAN タグ付きフレームの受信破棄オプション

サービス VLAN マッピングエントリー、トンネルポートの VLAN 変換エントリー、または VLAN マッピングルールに一致しないカスタマー VLAN のタグ付きフレームを受信した場合、そのフレームを破棄できます。なお、受信フレームがタグなしフレームの場合は対象外です。このオプションを有効にするには、**`vlan mapping miss drop`** コマンドを使用します。

NOTE: **`vlan mapping miss drop`** コマンドは、トンネルポートでのみサポートしています。

図 4-7 VLAN マッピングに一致しないカスタマー VLAN タグ付きフレームの受信破棄の例



受信カスタマー VLAN タグの優先度の反映オプション

トンネルポートでカスタマー VLAN のタグ付きフレームを受信した場合、そのカスタマー VLAN タグの優先度を CoS 値として反映できます。このオプションを有効にするには、**`dot1q-tunnel trust inner-priority`** コマンドを使用します。

> ***NOTE:*** **`dot1q-tunnel trust inner-priority`** コマンドは、トンネルポートでのみサポートしています。

> ***NOTE:*** 受信カスタマー VLAN タグの優先度の反映オプションは、サービス VLAN マッピングエントリー（**`switchport vlan mapping original-vlan dot1q-tunnel`** コマンド）、またはトンネルポートの VLAN 変換エントリー（**`switchport vlan mapping original-vlan resultant-vlan`** コマンド）の priority オプションよりも優先されます。

> ***NOTE:*** 受信カスタマー VLAN タグの優先度の反映オプションと、VLAN マッピングルール（**`vlan mapping rule`** コマンド）の priority オプションでは、VLAN マッピングルールの priority オプションが優先されます。

受信タグなしフレームへのカスタマー VLAN タグの付加オプション

トンネルポートでタグなしフレームを受信した場合に、指定した VLAN ID のカスタマー VLAN タグを付加して受信できます。なお、本オプションを有効に設定したトンネルポートからフレームを送信する際には、すべてのカスタマー VLAN タグが削除されて送信されるようになります。このオプションを有効にするには、**`dot1q-tunnel insert dot1q-tag`** コマンドを使用します。

> ***NOTE:*** **`dot1q-tunnel insert dot1q-tag`** コマンドは、トンネルポートでのみサポートしています。

> ***NOTE:*** トンネルポートの VLAN 変換エントリー（**`switchport vlan mapping original-vlan resultant-vlan`** コマンド）に一致する場合は、本オプションを有効に設定してもカスタマー VLAN タグを付与してトンネルポートからフレームを送信します。

> ***NOTE:*** 受信タグなしフレームへのカスタマー VLAN タグの付加オプションは、VLAN マッピングルール（**`vlan mapping rule`** コマンド）に一致して受信したタグなしフレームに対しては動作しません。VLAN マッピングルールの場合は、**`vlan mapping rule`** コマンドの inner-vid オプションを使用してください。

4.2 VLAN 変換の機能説明

トランクポートで、**switchport vlan mapping original-vlan resultant-vlan** コマンドで VLAN 変換エントリーを設定した場合は、送受信する VLAN タグ付きフレームの VLAN ID を双方向に変換できます。VLAN 変換の動作パターンと設定コマンドは、以下のとおりです。

表 4-6 VLAN 変換と設定コマンド

VLAN 変換	概要と設定コマンド
サービス VLAN タグの VLAN 変換	• VLAN 動作モード：トランクモード（**switchport mode trunk** コマンド） • VLAN 登録コマンド：**switchport trunk allowed vlan** コマンド • **switchport vlan mapping original-vlan 装置外のサービス VLAN resultant-vlan 装置内のサービス VLAN [priority COS]** コマンドで、サービス VLAN タグの VLAN 変換エントリーを設定する。
2 段タグフレームの VLAN 変換	• VLAN 動作モード：トランクモード（**switchport mode trunk** コマンド） • VLAN 登録コマンド：**switchport trunk allowed vlan** コマンド • **switchport vlan mapping original-vlan 装置外のサービス VLAN 装置外のカスタマー VLAN resultant-vlan 装置内のサービス VLAN 装置内のカスタマー VLAN [priority COS]** コマンドで、2 段タグフレームの両方の VLAN タグの VLAN 変換エントリーを設定する。

NOTE: 同一インターフェースでは、1 つの装置内のサービス VLAN に対して設定できる VLAN 変換エントリーは、1 エントリーのみです。

NOTE: 2 段タグフレームの VLAN 変換設定コマンドで、装置内のカスタマー VLAN を指定しない形式で設定した場合は、装置内のカスタマー VLAN を装置外のカスタマー VLAN の値で設定した場合と同じ動作になります。たとえば、**switchport vlan mapping original-vlan 10 1234 resultant-vlan 50** と設定した場合は、**switchport vlan mapping original-vlan 10 1234 resultant-vlan 50 1234** と設定した場合と同じ動作になります。

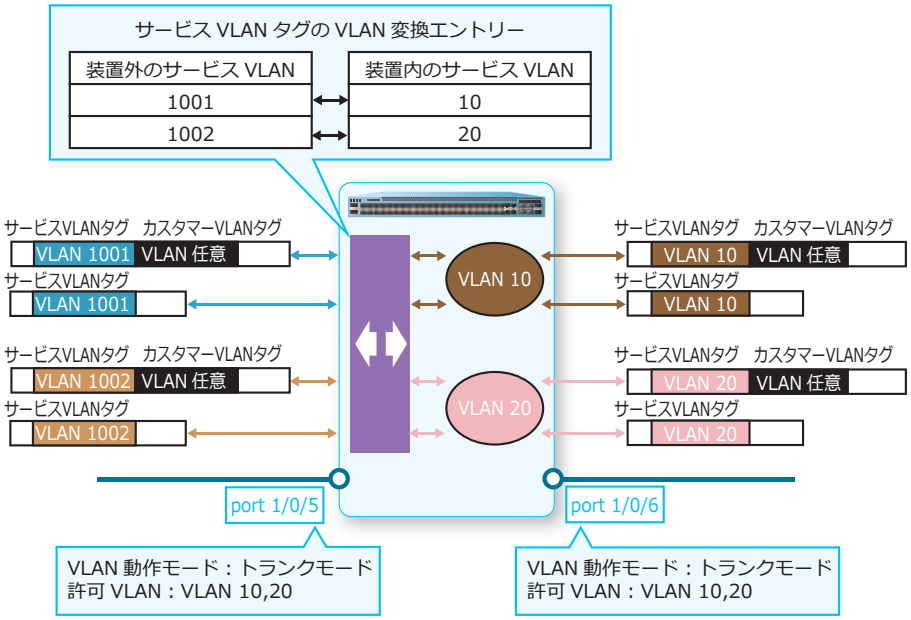
NOTE: priority パラメーターを指定しないで設定すると、priority 0 が自動的に設定されます。

NOTE: priority オプションは受信時のみ反映されます。また、サービス VLAN タグの VLAN 変換エントリーでは受信フレームが 1 段タグフレームの場合のみ、2 段タグフレームの VLAN 変換エントリーでは受信フレームが 2 段タグフレームの場合のみ、反映されます。

サービス VLAN タグの VLAN 変換の例を以下に示します。

以下の例では、トランクポートに設定したポート 1/0/5 でサービス VLAN 10 で送受信するタグ付きフレームの VLAN ID を 1001 に変換し、サービス VLAN 20 で送受信するタグ付きフレームの VLAN ID を 1002 に変換します。

図 4-8 サービス VLAN タグの VLAN 変換の例

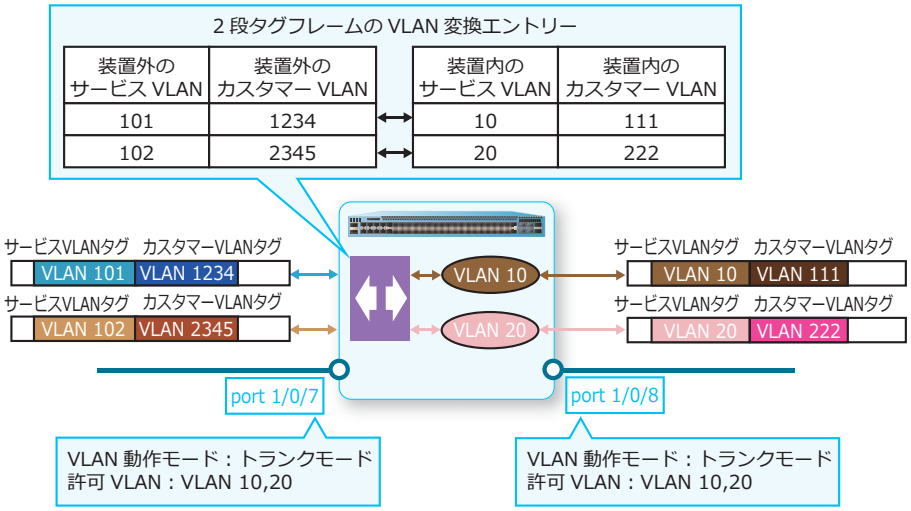


2 段タグフレームの VLAN 変換の例を以下に示します。

以下の例では、トランクポートに設定したポート 1/0/7 で「サービス VLAN 101、カスタマー VLAN 1234」の 2 段タグフレームを受信した場合は、「サービス VLAN 10、カスタマー VLAN 111」に変換してサービス VLAN 10 で受信します。また、サービス VLAN 10 のポート 1/0/7 から送信する前の形式が「サービス VLAN 10、カスタマー VLAN 111」の場合は、「サービス VLAN 101、カスタマー VLAN 1234」に変換して送信します。

同様に、ポート 1/0/7 で「サービス VLAN 102、カスタマー VLAN 2345」の 2 段タグフレームを受信した場合は、「サービス VLAN 20、カスタマー VLAN 222」に変換してサービス VLAN 20 で受信します。また、サービス VLAN 20 のポート 1/0/7 から送信する前の形式が「サービス VLAN 20、カスタマー VLAN 222」の場合は、「サービス VLAN 102、カスタマー VLAN 2345」に変換して送信します。

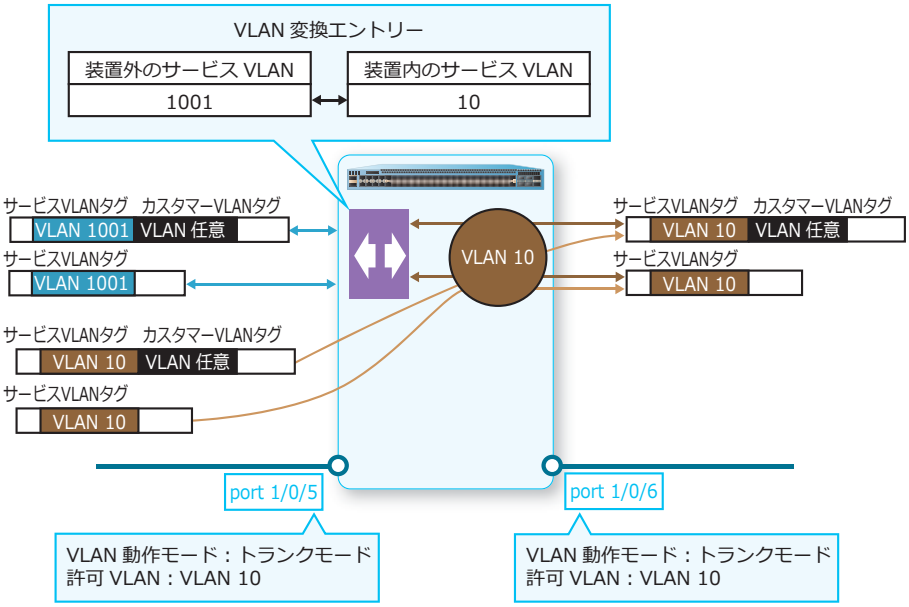
図 4-9 2 段タグフレームの VLAN 変換の例



VLAN 変換の注意事項

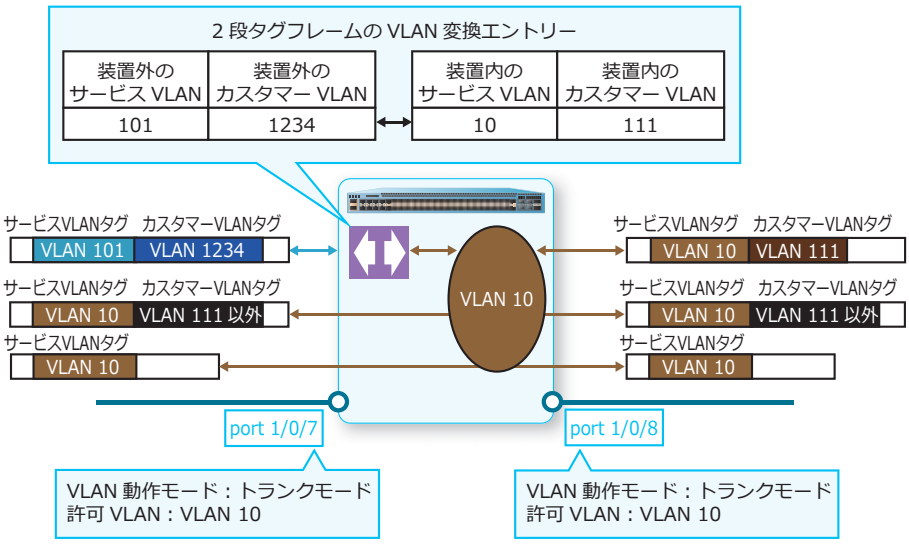
一致する VLAN 変換エントリーが存在しない場合でも、受信トランクポートにサービス VLAN と一致する VLAN が登録されている場合は、その VLAN で受信することに注意してください。以下の例のように、ポート 1/0/5 でサービス VLAN 10 のタグ付きフレームを受信した場合、「装置外のサービス VLAN=10」に一致する VLAN 変換エントリーがないため、VLAN 変換は行われませんが、ポート 1/0/5 に VLAN 10 を登録しているため、そのまま VLAN 10 で受信します。

図 4-10 VLAN 変換の注意事項の例（1）



また、2 段タグフレームの VLAN 変換エントリーの場合は、送信時に一致するエントリーがなくても、VLAN 変換しないでそのまま送信されることに注意してください。以下の例のように、サービス VLAN 10 のポート 1/0/7 から送信する前の形式が「サービス VLAN 10、カスタマー VLAN 111 以外」の 2 段タグフレーム、またはサービス VLAN 10 の 1 段タグフレームの場合は、VLAN 変換しないでそのまま送信されます。

図 4-11 VLAN 変換の注意事項の例（2）



4.3 VLAN トンネル／ VLAN 変換の状態確認

VLAN トンネル／ VLAN 変換の状態を表示して確認する方法を説明します。

4.3.1 TPID 設定の表示

show dot1q ethertype コマンドで、TPID 設定を確認できます。

表示例を以下に示します。

```
# show dot1q ethertype

 802.1q inner Ethernet Type is 0x8100 ...(1)
Port1/0/2 ...(2)
  802.1q tunneling Ethernet Type is 0x8100 ...(3)
Port1/0/11
  802.1q tunneling Ethernet Type is 0x8100
Port-channel2
  802.1q tunneling Ethernet Type is 0x8100
```

各項目の説明は、以下のとおりです。

表 4-7 show dot1q ethertype コマンドの表示項目

項番	説明
(1)	装置全体のカスタマー VLAN タグの TPID 設定を表示します。
(2)	VLAN 動作モードがトランクモードのポート番号またはポートチャネル番号を表示します。
(3)	サービスプロバイダー VLAN タグの TPID 設定を表示します。

4.3.2 トンネルポート関連設定の表示

show dot1q-tunnel コマンドで、トンネルポート関連の設定を確認できます。

表示例を以下に示します。

```
# show dot1q-tunnel

dot1q Tunnel Interface: Port1/0/1 ...(1)
  Trust inner priority       : Disabled ...(2)
  VLAN mapping miss drop     : Disabled ...(3)
  Insert dot1q tag           : VLAN 111 ...(4)
  VLAN mapping profiles      : 1 ...(5)

dot1q Tunnel Interface: Port1/0/12
  Trust inner priority       : Disabled
  VLAN mapping miss drop     : Enabled

dot1q Tunnel Interface: Port-channel1
  Trust inner priority       : Enabled
  VLAN mapping miss drop     : Disabled
```

各項目の説明は、以下のとおりです。

表 4-8 `show dot1q-tunnel` コマンドの表示項目

項番	説明
(1)	VLAN 動作モードがトンネルモードのポート番号またはポートチャネル番号を表示します。
(2)	受信カスタマー VLAN タグの優先度反映オプションの有効 (Enabled) ／無効 (Disabled) を表示します。
(3)	VLAN マッピングに一致しないカスタマー VLAN タグ付きフレームの、受信破棄オプションの有効 (Enabled) ／無効 (Disabled) を表示します。
(4)	受信タグなしフレームへのカスタマー VLAN タグの付加オプション有効時に、付加するカスタマー VLAN タグの VLAN ID を表示します。無効（デフォルト設定）の場合は表示されません。
(5)	インターフェースに適用されている VLAN マッピングプロファイルを表示します。未設定の場合は表示されません。

4.3.3 サービス VLAN マッピングエントリー／ VLAN 変換エントリー設定の表示

`show vlan mapping` コマンドで、サービス VLAN マッピングエントリーと VLAN 変換エントリーの設定を確認できます。

表示例を以下に示します。

```
# show vlan mapping
(1)               (2)             (3)                   (4)       (5)
Interface         Original VLAN   Translated VLAN       Priority  Status
---------------   -------------   -------------------   -------   --------
Port1/0/1         2               dot1q-tunnel 10       5         Active
Port1/0/1         3               dot1q-tunnel 20       0         Active
Port1/0/5         1001            translate 10          0         Active
Port1/0/5         1002            translate 20          3         Active
Port1/0/7         101/1234        translate 10/111      2         Active
Port1/0/7         102/2345        translate 20/222      0         Active
Port-channel1     500             dot1q-tunnel 600      5         Active
Port-channel2     2001            translate 30          0         Active
Port-channel2     2002/50         translate 40/555      3         Active

Total Entries: 9
```

各項目の説明は、以下のとおりです。

表 4-9 `show vlan mapping` コマンドの表示項目

項番	説明
(1)	ポート番号またはポートチャネル番号を表示します。
(2)	サービス VLAN マッピングエントリーの場合は「受信フレームのカスタマー VLAN」を表示します。 トランクポートに適用した VLAN 変換エントリーの場合は、「装置外でのサービス VLAN」または「装置外でのサービス VLAN ／装置外でのカスタマー VLAN」を表示します。 トンネルポートに適用した VLAN 変換エントリーの場合は「装置外でのカスタマー VLAN」を表示します。

項番	説明
(3)	dot1q-tunnel はサービス VLAN マッピングエントリーを、translate は VLAN 変換エントリーを意味します。 サービス VLAN マッピングエントリーの場合は「受信するサービス VLAN」を表示します。 VLAN 変換エントリーの場合は「装置内でのサービス VLAN」または「装置内でのサービス VLAN ／装置内でのカスタマー VLAN」を表示します。
(4)	受信時にエントリーに一致したフレームに反映する優先度を表示します。
(5)	エントリーのステータスを表示します。

4.3.4 VLAN マッピングプロファイル設定の表示

show vlan mapping profile コマンドで、VLAN マッピングプロファイルの設定を確認できます。

表示例を以下に示します。

```
# show vlan mapping profile
(1)                    (2)
VLAN mapping profile:1  type:ip
    rule 10 match src-ip 10.1.1.100/32, action dot1q-tunnel outer-vid 10, priority 4 ...(3)
    rule 20 match src-ip 10.1.1.200/32, action dot1q-tunnel outer-vid 20, priority 0
Total Entries: 2
VLAN mapping profile:2  type:ethernet
    rule 10 match src-mac 00-00-11-11-22-22, action translate outer-vid 30, priority 3
    rule 20 match src-mac 00-AA-BB-CC-DD-EE, action translate outer-vid 40, priority 1
Total Entries: 2
```

各項目の説明は、以下のとおりです。

表 4-10 show vlan mapping profile コマンドの表示項目

項番	説明
(1)	VLAN マッピングプロファイル ID を表示します。
(2)	VLAN マッピングプロファイルタイプを表示します。
(3)	VLAN マッピングルールを表示します。

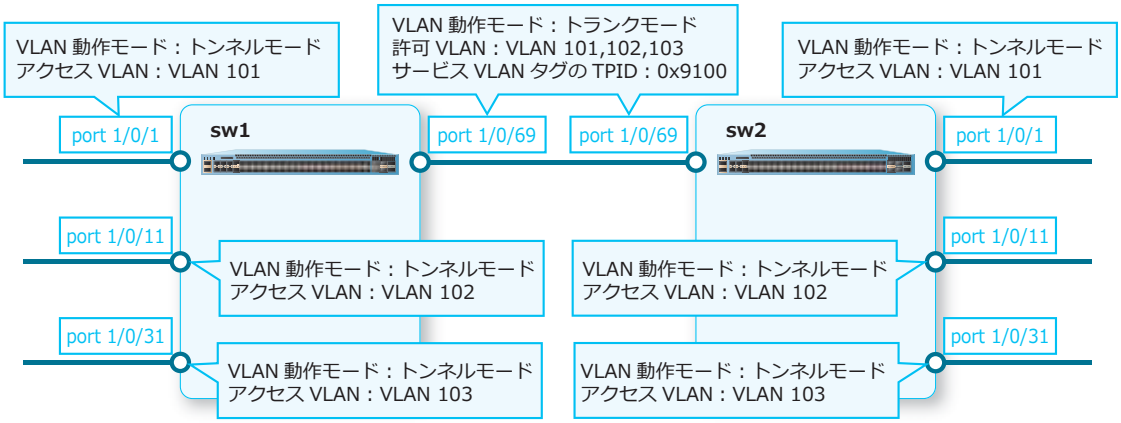
4.4 VLAN トンネル／ VLAN 変換の構成例と設定例

VLAN トンネル／ VLAN 変換を利用する場合の構成例と設定例を示します。

4.4.1 シンプルな VLAN トンネルの構成例と設定例

シンプルな VLAN トンネルの構成例と設定例を示します。この設定例では、ポート 1/0/1、ポート 1/0/11、ポート 1/0/31 をトンネルポートに設定し、それぞれアクセス VLAN 101、102、103 を登録しています。また、ポート 1/0/69 をトランクポートに設定し、VLAN 101、102、103 を登録しています。ポート 1/0/69 のサービス VLAN の TPID は 0x9100 に設定しています。ここでは、sw1 の設定例のみ示します。

図 4-12 シンプルな VLAN トンネルの構成例



1. VLAN 101 から VLAN 103 を作成します。

```
sw1# configure terminal
sw1(config)# vlan 101-103
sw1(config-vlan)# exit
sw1(config)#
```

2. ポート 1/0/69 をトランクポートとして設定し、トランクポートに［VLAN 101 から VLAN 103］を割り当てます。また、サービス VLAN タグの TPID を［0x9100］に設定します。

```
sw1(config)# interface port 1/0/69
sw1(config-if-port)# switchport mode trunk
sw1(config-if-port)# switchport trunk allowed vlan 101-103
sw1(config-if-port)#
sw1(config-if-port)# dot1q tunneling ethertype 0x9100
sw1(config-if-port)# exit
sw1(config)#
```

3. ポート 1/0/1 をトンネルポートとして設定し、トンネルポートに［VLAN 101］を割り当てます。

```
sw1(config)# interface port 1/0/1
sw1(config-if-port)# switchport mode dot1q-tunnel
sw1(config-if-port)# switchport access vlan 101
sw1(config-if-port)# exit
sw1(config)#
```

4. ポート 1/0/11 をトンネルポートとして設定し、トンネルポートに［VLAN 102］を割り当てます。

```
sw1(config)# interface port 1/0/11
sw1(config-if-port)# switchport mode dot1q-tunnel
sw1(config-if-port)# switchport access vlan 102
sw1(config-if-port)# exit
sw1(config)#
```

5. ポート 1/0/31 をトンネルポートとして設定し、トンネルポートに［VLAN 103］を割り当てます。

```
sw1(config)# interface port 1/0/31
sw1(config-if-port)# switchport mode dot1q-tunnel
sw1(config-if-port)# switchport access vlan 103
sw1(config-if-port)# end
sw1#
```

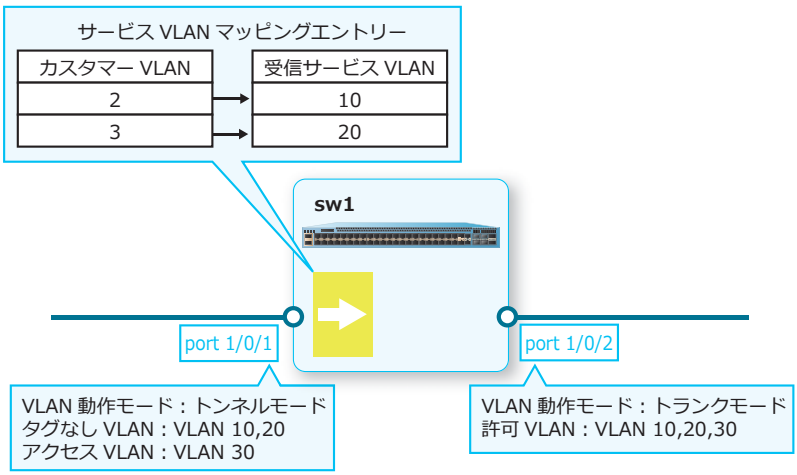
4.4.2 サービス VLAN マッピングエントリーを使用する場合

サービス VLAN マッピングエントリーを使用して、受信フレームのカスタマー VLAN から受信する VLAN を決定する方法の構成例と設定例を示します。この設定例では、ポート 1/0/1 をトンネルポートに設定し、VLAN 10、20 をタグなし VLAN として、VLAN 30 をアクセス VLAN として登録しています。また、以下のサービス VLAN マッピングエントリーを設定しています。

- 受信フレームのカスタマー VLAN が 2 の場合、VLAN 10 で受信
- 受信フレームのカスタマー VLAN が 3 の場合、VLAN 20 で受信

ポート 1/0/2 はトランクポートに設定し、VLAN 10、20、30 を登録しています。

図 4-13 サービス VLAN マッピングエントリーを使用する場合の構成例



1. VLAN 10、20、30 を作成します。

```
sw1# configure terminal
sw1(config)# vlan 10,20,30
sw1(config-vlan)# exit
sw1(config)#
```

2. 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 10、20、30］を割り当てます。

```
sw1(config)# interface port 1/0/2
sw1(config-if-port)# switchport mode trunk
sw1(config-if-port)# switchport trunk allowed vlan 10,20,30
sw1(config-if-port)# exit
sw1(config)#
```

3. ポート 1/0/1 をトンネルポートとして設定し、タグなし VLAN として［VLAN 10、20］を割り当てます。また、アクセス VLAN として［VLAN 30］を割り当てます。

```
sw1(config)# interface port 1/0/1
sw1(config-if-port)# switchport mode dot1q-tunnel
sw1(config-if-port)# switchport hybrid allowed vlan untagged 10,20
sw1(config-if-port)# switchport access vlan 30
sw1(config-if-port)# exit
sw1(config)#
```

4. ポート 1/0/1 で以下のサービス VLAN マッピングエントリーを設定します。

受信フレームのカスタマー VLAN が 2 の場合、VLAN 10 で受信

受信フレームのカスタマー VLAN が 3 の場合、VLAN 20 で受信

```
sw1(config)# interface port 1/0/1
sw1(config-if-port)# switchport vlan mapping original-vlan 2 dot1q-tunnel 10
sw1(config-if-port)# switchport vlan mapping original-vlan 3 dot1q-tunnel 20
sw1(config-if-port)# end
sw1#
```

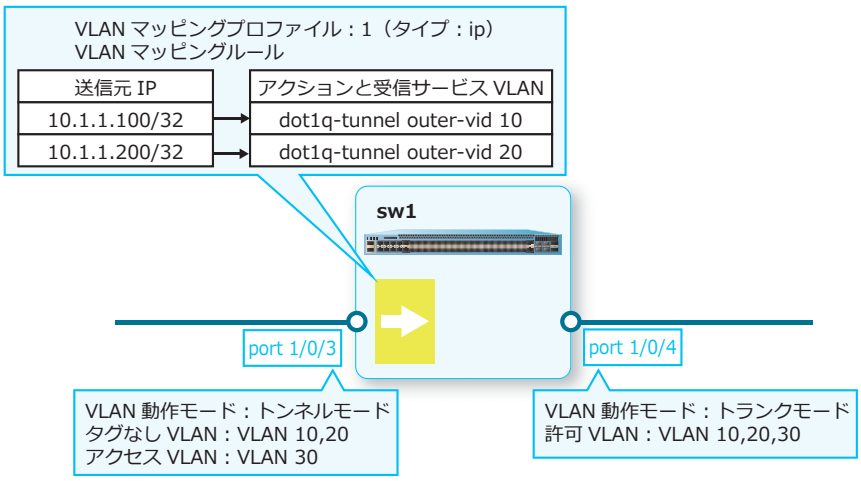
4.4.3 VLAN マッピングプロファイルを使用する場合

VLAN マッピングプロファイルを使用して、受信フレームの任意の情報から受信する VLAN を決定する方法の構成例と設定例を示します。この設定例では、ポート 1/0/3 をトンネルポートに設定し、VLAN 10、20 をタグなし VLAN として、VLAN 30 をアクセス VLAN として登録しています。また、VLAN マッピングプロファイル 1 をプロファイルタイプ ip で作成し、以下の VLAN マッピングルールを設定しています。

- ルール 10、受信パケットの送信元 IP アドレスが 10.1.1.100/32 の場合、VLAN 10 で受信
- ルール 20、受信パケットの送信元 IP アドレスが 10.1.1.200/32 の場合、VLAN 20 で受信

ポート 1/0/4 はトランクポートに設定し、VLAN 10、20、30 を登録しています。

図 4-14 VLAN マッピングプロファイルを使用する場合の構成例



1. VLAN 10、20、30 を作成します。

```
sw1# configure terminal
sw1(config)# vlan 10,20,30
sw1(config-vlan)# exit
sw1(config)#
```

2. 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 10、20、30］を割り当てます。

```
sw1(config)# interface port 1/0/4
sw1(config-if-port)# switchport mode trunk
sw1(config-if-port)# switchport trunk allowed vlan 10,20,30
sw1(config-if-port)# exit
sw1(config)#
```

3. ポート 1/0/3 をトンネルポートとして設定し、タグなし VLAN として［VLAN 10、20］を割り当てます。また、アクセス VLAN として［VLAN 30］を割り当てます。

```
sw1(config)# interface port 1/0/3
sw1(config-if-port)# switchport mode dot1q-tunnel
sw1(config-if-port)# switchport hybrid allowed vlan untagged 10,20
sw1(config-if-port)# switchport access vlan 30
sw1(config-if-port)# exit
sw1(config)#
```

4. VLAN マッピングプロファイル 1 をプロファイルタイプ ip で作成します。

```
sw1(config)# vlan mapping profile 1 type ip
sw1(config-vlan-map)#
```

5. VLAN マッピングプロファイル 1 で、以下の VLAN マッピングルールを設定します。

ルール 10、受信パケットの送信元 IP アドレスが 10.1.1.100/32 の場合、VLAN 10 で受信

ルール 20、受信パケットの送信元 IP アドレスが 10.1.1.200/32 の場合、VLAN 20 で受信

```
sw1(config-vlan-map)# rule 10 match src-ip 10.1.1.100/32 dot1q-tunnel outer-vid
10
sw1(config-vlan-map)# rule 20 match src-ip 10.1.1.200/32 dot1q-tunnel outer-vid
20
sw1(config-vlan-map)# exit
sw1(config)#
```

6. ポート 1/0/3 に VLAN マッピングプロファイル 1 を適用します。

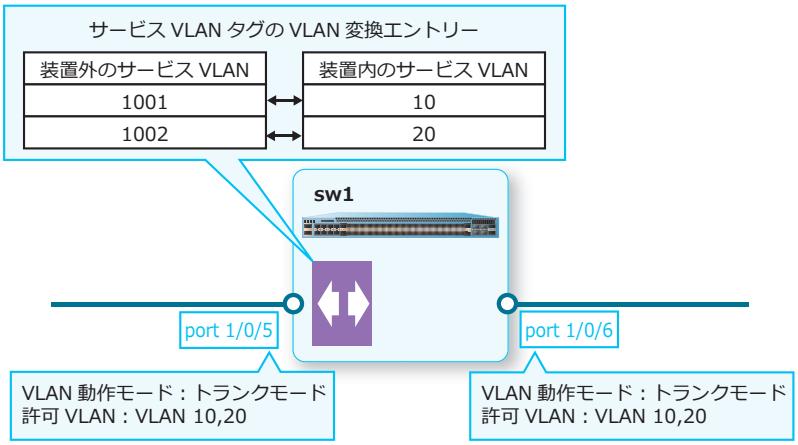
```
sw1(config)# interface port 1/0/3
sw1(config-if-port)# switchport vlan mapping profile 1
sw1(config-if-port)# end
sw1#
```

4.4.4 VLAN 変換の構成例と設定例

サービス VLAN タグの VLAN 変換を使用して、双方向の VLAN 変換を実施する構成例と設定例を示します。この設定例では、ポート 1/0/5 と 1/0/6 をトランクポートに設定し、VLAN 10、20 を登録しています。また、ポート 1/0/5 で以下の VLAN 変換エントリーを設定しています。

- 装置外のサービス VLAN 1001 と、装置内のサービス VLAN 10 を双方向に VLAN 変換
- 装置外のサービス VLAN 1002 と、装置内のサービス VLAN 20 を双方向に VLAN 変換

図 4-15 VLAN 変換の構成例



1. VLAN 10、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 1/0/5 と 1/0/6 をトランクポートとして設定し、トランクポートに［VLAN 10、20］を割り当てます。

```
sw1(config)# interface range port 1/0/5-6
sw1(config-if-port-range)# switchport mode trunk
sw1(config-if-port-range)# switchport trunk allowed vlan 10,20
sw1(config-if-port-range)# exit
sw1(config)#
```

3. ポート 1/0/5 で以下の VLAN 変換エントリーを設定します。

装置外のサービス VLAN 1001 と、装置内のサービス VLAN 10 を双方向に VLAN 変換

装置外のサービス VLAN 1002 と、装置内のサービス VLAN 20 を双方向に VLAN 変換

```
sw1(config)# interface port 1/0/5
sw1(config-if-port)# switchport vlan mapping original-vlan 1001 resultant-vlan
10
sw1(config-if-port)# switchport vlan mapping original-vlan 1002 resultant-vlan
20
sw1(config-if-port)# end
sw1#
```

5. スパニングツリー

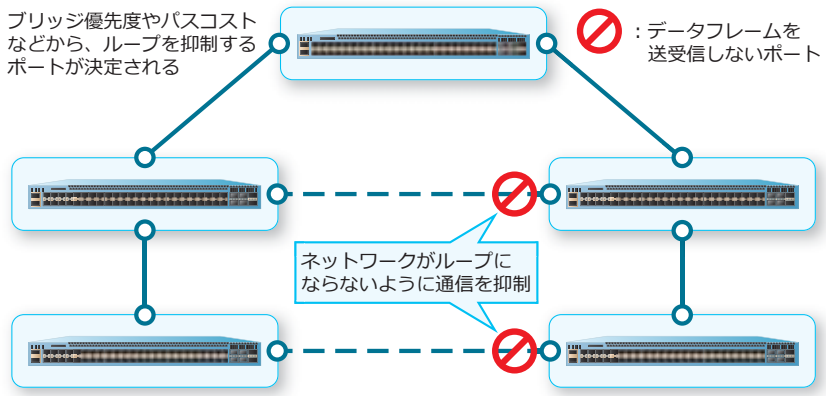
スパニングツリーの機能、状態の確認方法、および構成例と設定例について説明します。

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 スパニングツリーの機能説明

スパニングツリーは、レイヤー 2 ネットワークを冗長化するための機能です。ネットワークを物理的なループ構成で接続した場合に、ループになることを抑制して冗長化します。

図 5-1 スパニングツリーの概要



CAUTION: STP/RSTP/MSTP/RPVST+ 機能と ERPS 機能は、同一装置で併用できません。

CAUTION: STP/RSTP/MSTP/RPVST+ 機能と MMRP-Plus 機能は、装置併用をサポートした機種／バージョン以外では、同一装置で併用できません。

NOTE: NP7000 の 1.12.01 以降、NP5000 の 1.12.01 以降、NP3000 の 1.11.03 以降、NP2100 の 1.13.01 以降、NP2500 の 1.13.01 以降では、STP/RSTP/MSTP/RPVST+ 機能と MMRP-Plus 機能との装置併用をサポートしました。なお、同一インターフェース（物理ポートまたはポートチャネル）では引き続き併用不可です。

CAUTION: STP/RSTP/MSTP/RPVST+ 機能は、同一インターフェースでループ検知機能（loop-detection action notify-only 設定時を除く）、ポートリダンダント機能、VLAN 変換機能と併用できません。

CAUTION: PVST+ は未サポートです。また、RPVST+ 機能を使用して PVST+ と相互接続することは未サポートです。

5.1.1 スパニングツリーの計算

スパニングツリーを有効化すると、装置に設定したブリッジ優先度などを使用して、ルートブリッジやポートの役割が自動的に決定されます。

装置全体のスパニングツリーを有効化するには、**`spanning-tree global state`** コマンドを使用します。インターフェースごとにスパニングツリーを有効化するには、**`spanning-tree state`** コマンドを使用します。RPVST+ を使用する際、指定した VLAN のスパニングツリーを有効化するには、**`spanning-tree vlan`** コマンドを使用します。

CAUTION: 他のレイヤー 2、およびレイヤー 3 機能（スタック機能を含む）によって、CPU が過負荷となった場合、RPVST+ パケットの処理が遅れることがあります。これにより、トラフィックの損失やネットワークトポロジーの変更が発生する場合があります。

スパニングツリープロトコルの設定

スパニングツリーでは、以下の 4 種類の**スパニングツリープロトコル**に対応しています。

- **MSTP（マルチプルスパニングツリープロトコル）**
  VLAN ごとにグループ分けし、グループごとにスパニングツリーを計算するプロトコルです。
- **RSTP（ラピッドスパニングツリープロトコル）**
  対向のポート同士で直接ポートの役割を決定するプロトコルです。IEEE 802.1w で標準化されています。STP よりもスパニングツリーを短時間で計算できます。

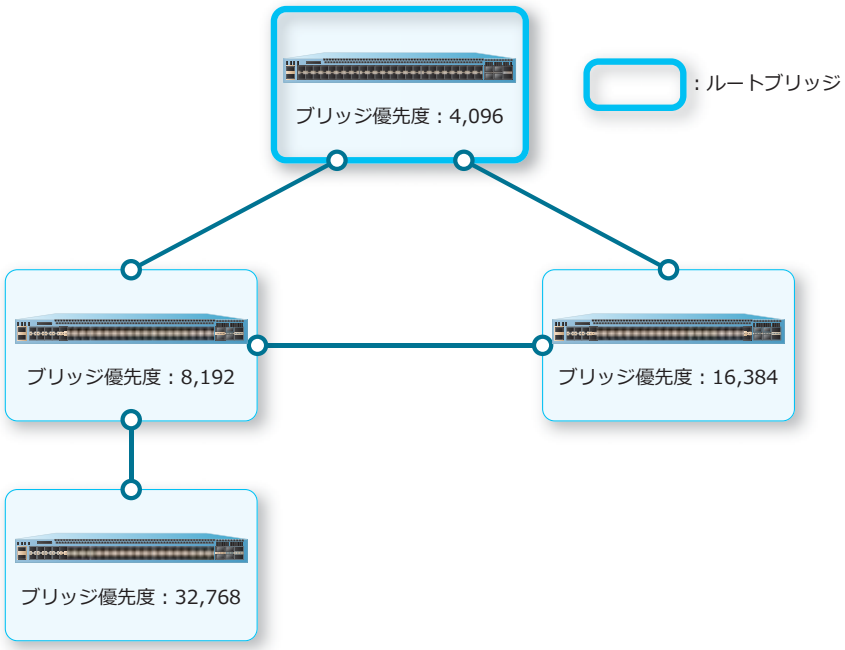
  NOTE: RSTP は、ポイントツーポイントリンクのみで利用できます。シェアードリンクの場合は、STP が利用されます。
- **STP（スパニングツリープロトコル）**
  IEEE 802.1D で標準化されているプロトコルです。
- **RPVST+（VLAN 単位のラピッドスパニングツリープロトコル）**
  RSTP と同じ方式で、VLAN ごとにスパニングツリーを提供するプロトコルです。

スパニングツリープロトコルは、**`spanning-tree mode`** コマンドで設定します。

ルートブリッジの選択

ブリッジ優先度が最も小さいブリッジが、**ルートブリッジ**に選択されます。

図 5-2 ルートブリッジの選択



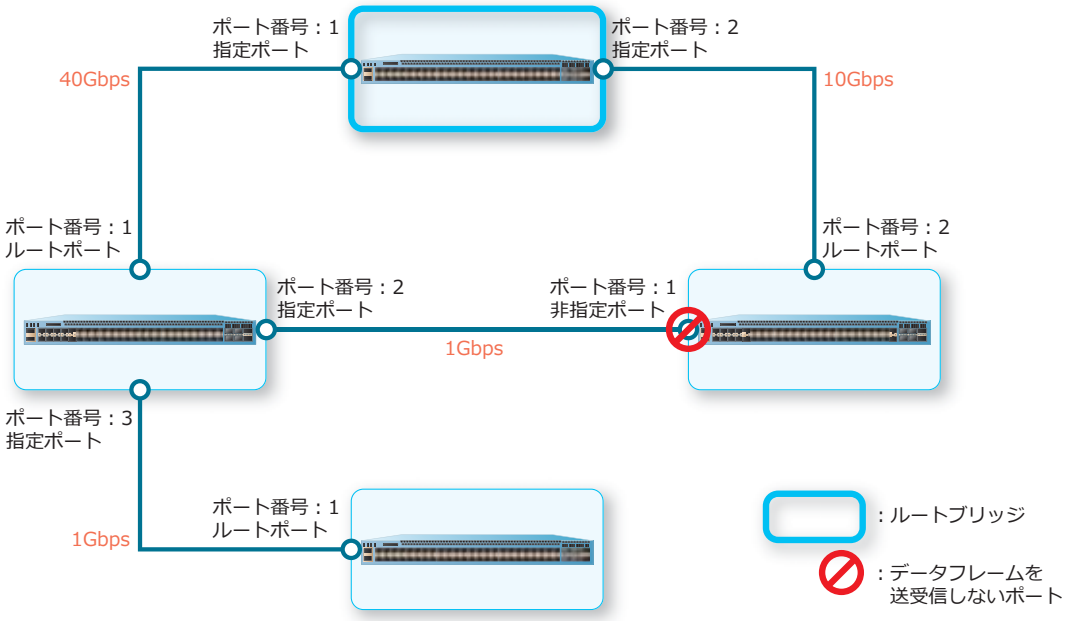
ブリッジ優先度は、**`spanning-tree priority`** コマンドで設定します。RPVST+ を使用する際、指定した VLAN のブリッジ優先度を設定するには、**`spanning-tree vlan priority`** コマンドを使用します。

ポートの役割の決定

ルートブリッジの選択後、**パスコスト**、**ポート優先度**、ポート番号を基に、ポートごとに適切な役割が自動的に決定されます。スパニングツリープロトコル種別によって違いはありますが、主なポートの役割を以下に示します。

- **ルートポート**
  通信可能なポートです。ブリッジごとに 1 ポート存在し、ルートブリッジに最も近いポートです。
- **指定ポート**
  通信可能なポートです。リンクごとに 1 ポート存在し、ルートブリッジに最も近いポートです。
- **非指定ポート**
  データフレームがブロックされ、通信できないポートです。BPDU は送受信できます。
- **代替ポート**
  ルートポートの代替ポートです。データフレームがブロックされ、通信できないポートです。BPDU は送受信できます。
- **バックアップポート**
  指定ポートの代替ポートです。データフレームがブロックされ、通信できないポートです。BPDU は送受信できます。

図 5-3 ポートの役割



NOTE: パスコスト、ポート優先度、およびポート番号は、いずれも小さい値のポートが優先的に利用されます。たとえばパスコストの場合は、インターフェースの速度が速いほど小さくなります。

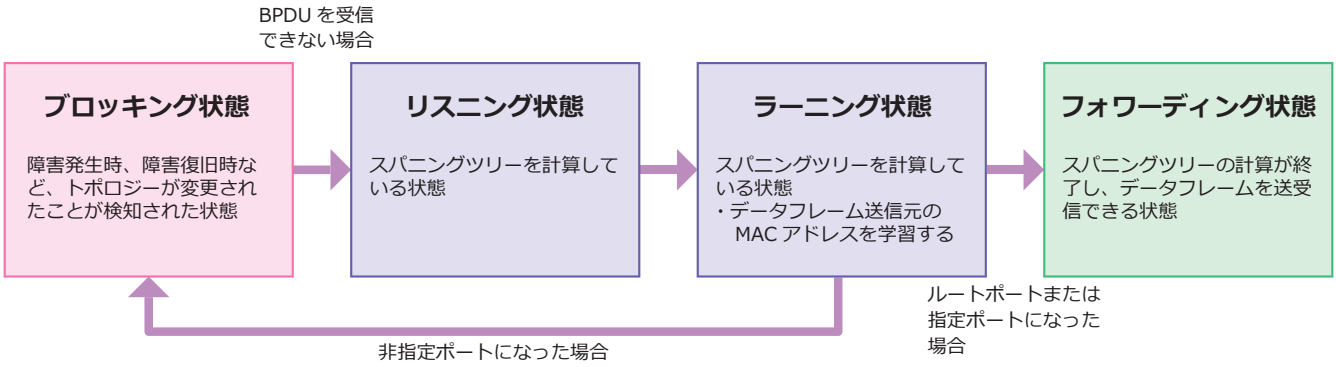
パスコストは、**`spanning-tree cost`** コマンドで設定します。RPVST+ を使用する際、指定した VLAN のパスコストを設定するには、**`spanning-tree vlan cost`** コマンドを使用します。

ポート優先度は、**`spanning-tree port-priority`** コマンドで設定します。RPVST+ を使用する際、指定した VLAN のポート優先度を設定するには、**`spanning-tree vlan port-priority`** コマンドを使用します。

5.1.2 スパニングツリーの状態遷移

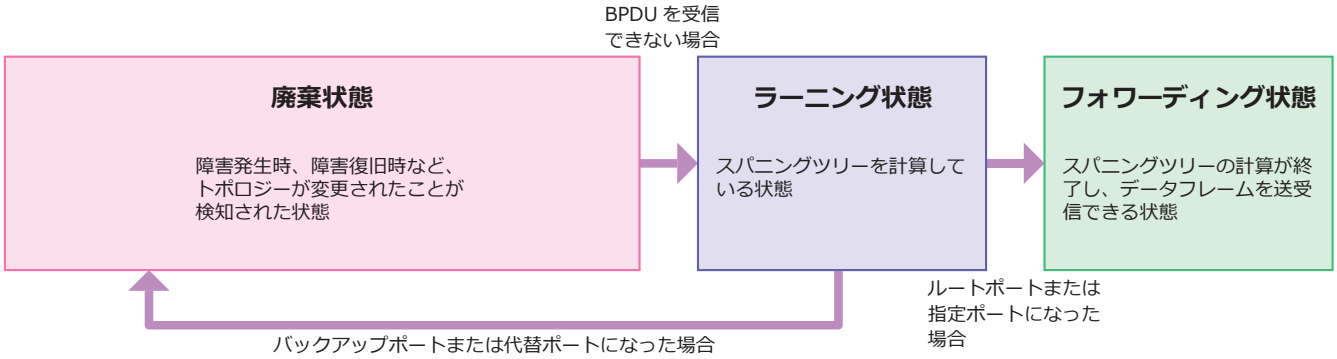
STP では、4 つの状態が定義されています。

図 5-4 STP の状態遷移



また、RSTP では、ブロッキング状態とリスニング状態の代わりに、破棄状態が定義されています。

図 5-5 RSTP の状態遷移



BPDU

スパニングツリーでは、BPDU（Bridge Protocol Data Unit）と呼ばれる制御フレームが利用されます。一定時間、BPDU を受信できないと、障害が発生したと認識されます。

BPDU に関して、以下の項目を設定できます。() 内は使用するコマンドです。

- BPDU のマルチキャスト宛先 MAC アドレス（**`spanning-tree nni-bpdu-address`** コマンド）
- BPDU のハードウェア転送の有効化（**`forward-bpdu global enable`** コマンド）

  NOTE: BPDU のハードウェア転送は、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 1.10.01 以降でサポートしています。

  NOTE: スパニングツリープロトコルが有効の場合は、BPDU のハードウェア転送を有効にできません。

  NOTE: BPDU のハードウェア転送を使用する場合は、**`spanning-tree mode`** コマンドはデフォルト設定のままで使用してください。また、BPDU のソフトウェア転送も無効（デフォルト設定）のままで使用してください。

- BPDU のソフトウェア転送の有効化（**`spanning-tree forward-bpdu`** コマンド）

  NOTE: 装置としてソフトウェア転送可能な BPDU の最大レートは 64Kbps です。

トポロジー変更通知（TCN）のフィルタリング機能の設定

トポロジー変更通知（TCN）は、ブリッジからルートブリッジに送信される BPDU です。トポロジーの変更が発生すると、トポロジー変更通知（TCN）がフラッディングされます。フィルタリング機能を有効化すると、インターフェースで受信したトポロジー変更通知（TCN）を、他のインターフェースへ伝達しなくなります。

トポロジー変更通知（TCN）のフィルタリング機能を有効化するには、**spanning-tree tcnfilter** コマンドを使用します。

5.1.3 スパニングツリータイマー

スパニングツリーでは、以下のタイマーが用意されています。

- **ハロータイム**

  装置が BPDU を定期的に送信する間隔です。2 秒に設定した場合は、2 秒に 1 回 BPDU が送信されます。

- **フォワードタイム**

  リスニング状態からラーニング状態へ移行する際、およびラーニング状態からフォワーディング状態に移行する際に待機する時間です。

- **最大エージタイム**

  障害が発生したと判断されるまでの時間です。BPDU が受信できないまま最大エージタイムが経過すると、障害が発生したと判断され、スパニングツリーの再計算が行われます。

- **転送保留カウント**

  送信する BPDU の上限の数（バーストサイズ）を設定できます。

ハロータイム、フォワードタイム、最大エージタイムは、**spanning-tree (timers)** コマンドで設定します。転送保留カウントは、**spanning-tree tx-hold-count** コマンドで設定します。RPVST+ を使用する際、指定した VLAN のハロータイム、フォワードタイム、最大エージタイムを設定するには、**spanning-tree vlan (timers)** コマンドを使用します。

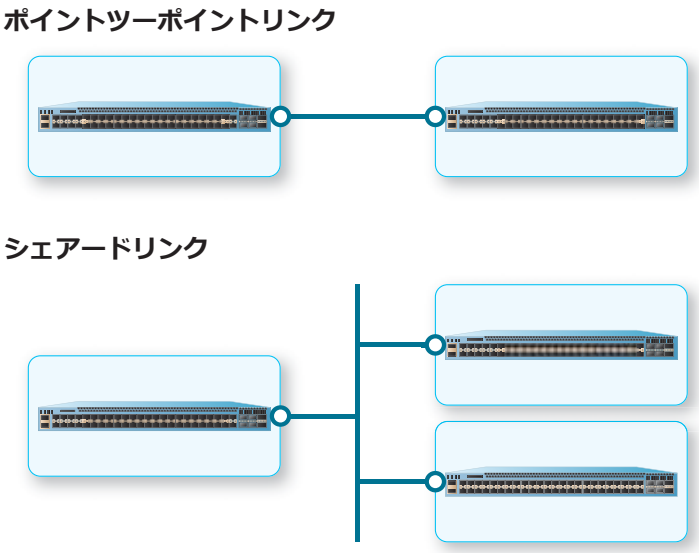
5.1.4 ポートのリンクタイプの設定

ポートの対向に、装置が直接接続されているか、ハブなどを使用して複数の装置が接続されているかを設定します。

リンクタイプには、以下の 2 種類があります。

- **ポイントツーポイントリンク**
  対向に装置が直接接続されているリンクです。
- **シェアードリンク**
  ハブなどを使用して、対向に複数の装置が接続されているリンクです。

図 5-6 ポートのリンクタイプ



ポートのリンクタイプは、**`spanning-tree link-type`** コマンドで設定します。

5.1.5 Port Fast モードの設定

Port Fast モードをエッジポートに設定すると、パソコンなど BPDU を送信しない機器を接続した場合に、リンクアップ後の転送遅延時間を待つことなく、すぐにフォワーディング状態に遷移させることができます。

Port Fast モードは、**`spanning-tree portfast`** コマンドで設定します。

5.1.6 ルートガードの設定

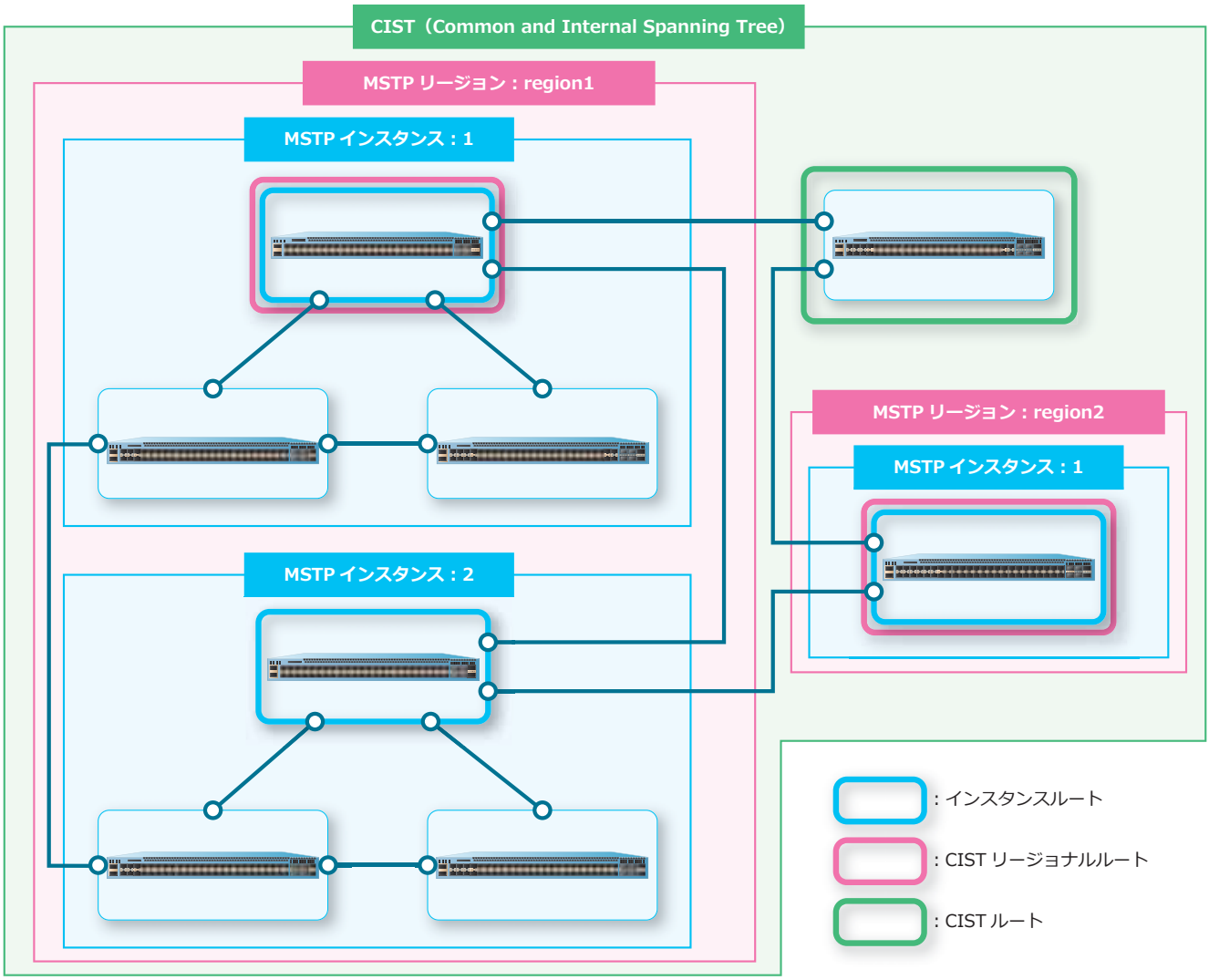
ルートブリッジのルートガードを有効化すると、優先度が高い BPDU を受信しても、ルートポートの再計算を行いません。

ルートガードは、**`spanning-tree guard root`** コマンドで有効化します。

5.1.7 MSTP の設定

MSTP（Multiple Spanning Tree Protocol）を使用すると、グループごとにスパニングツリーの再計算を行うため、影響のないグループは再計算されず、再計算に関する処理負荷を抑えることができます。

図 5-7 MSTP の概要



MSTP のグループには、以下の 3 種類があります。

- **MSTP インスタンス**

  MSTP における最小のスパニングツリーを構成するグループです。MSTP インスタンスに VLAN を割り当てることで、複数の VLAN を 1 つのグループとして扱うことができます。MSTP インスタンスのルートブリッジを**インスタンスルート**と呼びます。

- **MSTP リージョン**

  同じ設定を共有する MSTP インスタンスのグループです。MSTP インスタンスを 1 つのブリッジとみなして、スパニングツリーを構成します。MSTP リージョンのルートブリッジを **CIST リージョナルルート**と呼びます。

- **CIST（Common and Internal Spanning Tree）**

  MSTP リージョン外の装置も含めた全装置のグループです。MSTP リージョンを 1 つのブリッジとみなして、スパニングツリーを構成します。CIST のルートブリッジを **CIST ルート**と呼びます。

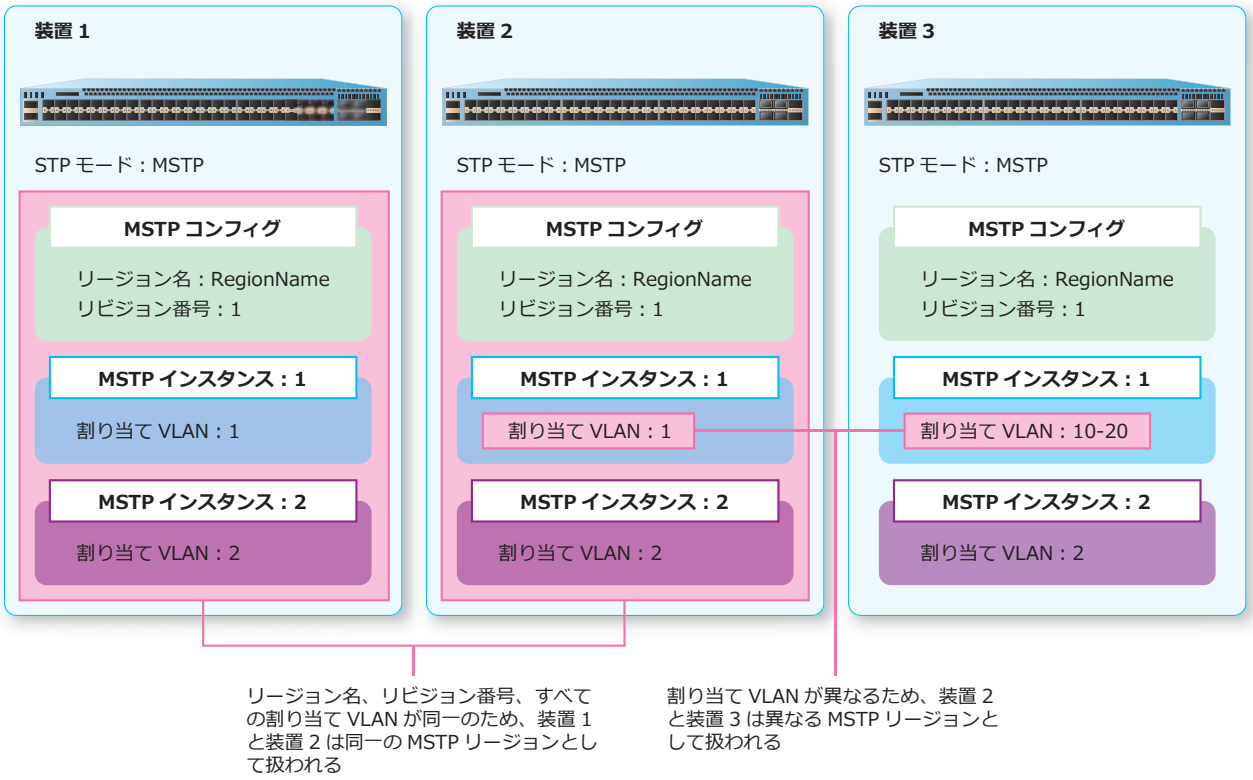
  NOTE: 1 つの装置が、インスタンスルート、CIST リージョナルルート、および CIST ルートを兼ねる場合もあります。

MSTP リージョンの区別

各装置に設定された以下の情報が一致した装置が、同一の MSTP リージョンに属すると判定されます。MSTP リージョンを区別するための設定は、**spanning-tree mst configuration** コマンドを使用して、MSTP コンフィグレーションモードに遷移して行います。() 内は使用するコマンドです。

- リージョン名（**name** コマンド）
- リビジョン番号（**revision** コマンド）
- MSTP インスタンスと VLAN の関連付け情報（**instance** コマンド）

図 5-8 MSTP リージョンの区別



MSTP インスタンスによるスパニングツリーの計算

MSTP では、MSTP インスタンスを 1 つのブリッジとみなし、MSTP インスタンスに設定されたブリッジ優先度やポート優先度などを使用して、CIST リージョナルルートやポートの役割が決定されます。

MSTP インスタンス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。

- ブリッジ優先度（**spanning-tree mst priority** コマンド）
- パスコストおよびポート優先度（**spanning-tree mst** コマンド）

5.2 スパニングツリーの状態確認

スパニングツリーの状態を表示して確認する方法を説明します。

5.2.1 インターフェース関連の設定の表示

show spanning-tree configuration interface コマンドで、スパニングツリープロトコルのインターフェース関連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 spanning-tree configuration interface port 1/0/1

Port1/0/1 ...(1)
 Spanning tree state : Enabled ...(2)
 Port path cost: 0 ...(3)
 Port priority: 128 ...(4)
 Port Identifier:  128.1 ...(5)
 Link type: auto ...(6)
 Port fast: auto ...(7)
 Hello time: 2 seconds ...(8)
 Guard root: Disabled ...(9)
 TCN filter : Disabled ...(10)
 Bpdu forward: Disabled ...(11)
```

各項目の説明は、以下のとおりです。

表 5-1 show spanning-tree configuration interface コマンドの表示項目

項番	説明
(1)	ポート番号またはポートチャネル番号を表示します。
(2)	ポートのスパニングツリープロトコルの有効 (Enabled) ／無効 (Disabled) を表示します。
(3)	ポートのパスコストを表示します。
(4)	ポート優先度を表示します。
(5)	ポート ID（ポート優先度＋ポート番号（ifindex））を表示します。
(6)	ポートのリンクタイプの設定を表示します。デフォルトの自動判別設定の場合、全二重ポートはポイントツーポイントリンク、半二重ポートはシェアードリンクと判別されます。 • auto：自動判別設定 • p2p：手動設定（ポイントツーポイントリンク） • shared：手動設定（シェアードリンク）
(7)	Port Fast モードの設定を表示します。 • auto：ネットワークポート • edge：エッジポート • none-edge：無効ポート
(8)	MSTP で使用するポートごとのハロータイムを表示します。動作モードが MSTP の場合のみ表示されます。
(9)	ルートガードの有効 (Enabled) ／無効 (Disabled) を表示します。
(10)	トポロジー変更通知（TCN）のフィルタリング機能の有効 (Enabled) ／無効 (Disabled) を表示します。

項番	説明
(11)	BPDU のソフトウェア転送の有効 (Enabled) ／無効 (Disabled) を表示します。

5.2.2 STP、RSTP の動作状況の表示

show spanning-tree コマンドで、STP、RSTP の動作状況を確認できます。

RSTP が有効な場合の表示例を以下に示します。

```
# show spanning-tree

 Spanning Tree: Enabled ...(1)
 Protocol Mode: RSTP ...(2)
 Tx-hold-count: 6 ...(3)
 NNI BPDU Address: dot1d(01-80-C2-00-00-00) ...(4)
 Root ID Priority: 4096 ...(5)
         Address: 00-40-66-45-A0-0C ...(6)
         (7)                (8)              (9)
         Hello Time: 2 sec, Max Age: 20 sec, Forward Delay: 15 sec
 Bridge  ID Priority: 4096  (priority 4096  sys-id-ext 0) ...(10)
         Address: 00-40-66-A8-C9-A5 ...(11)
         (12)               (13)             (14)
         Hello Time: 2 sec, Max Age: 20 sec, Forward Delay: 15 sec,
 Topology Changes Count: 1 ...(15)
                                                  (20)      (21)
 (16)           (17)        (18)        (19)      Priority Link    (22)
 Interface      Role        State       Cost      .Port#   Type    Edge
 ---------      ----        -----       ----      -------  -----   ----
 Port1/0/2      root        forwarding  2000      128.2    p2p     non-edge
 Port1/0/8      designated  forwarding  20000     128.8    p2p     edge
 Port1/0/17     designated  forwarding  20000     128.17   p2p     edge
```

各項目の説明は、以下のとおりです。

表 5-2 show spanning-tree コマンドの表示項目

項番	説明
(1)	STP または RSTP の有効 (Enabled) ／無効 (Disabled) を表示します。
(2)	スパニングツリープロトコルを表示します。 • RSTP：ラピッドスパニングツリープロトコル • STP compatible：スパニングツリープロトコル
(3)	転送保留カウント値を表示します。
(4)	BPDU の宛先 MAC アドレスを表示します。
(5)	ルートブリッジの優先度を表示します。
(6)	ルートブリッジの MAC アドレスを表示します。
(7)	ルートブリッジのハロータイムを表示します。
(8)	ルートブリッジの最大エージタイムを表示します。
(9)	ルートブリッジのフォワードディレイタイムを表示します。
(10)	自装置の優先度を表示します。

項番	説明
(11)	自装置の MAC アドレスを表示します。
(12)	自装置のハロータイムを表示します。
(13)	自装置の最大エージタイムを表示します。
(14)	自装置のフォワードディレイタイムを表示します。
(15)	スパニングツリープロトコルのトポロジーが変更された回数を表示します。
(16)	ポート番号またはポートチャネル番号を表示します。
(17)	ポートの役割を表示します。 • root：ルートポート • designated：指定ポート • alternate：代替ポート • backup：バックアップポート • disabled：無効ポート
(18)	ポートのステータスを表示します。 • forwarding：フォワーディング状態 • blocking：ブロッキング状態（ディスカーディング状態） • learning：ラーニング状態 • disabled：無効状態
(19)	ポートのパスコストを表示します。
(20)	ポート ID（ポート優先度＋ポート番号（ifindex））を表示します。
(21)	ポートのリンクタイプの動作状況（p2p：ポイントツーポイントリンク／ shared：シェアードリンク）を表示します。
(22)	Port Fast モードの動作状況（edge：エッジポート／ non-edge：無効ポート）を表示します。

5.2.3 MSTP の設定の表示

show spanning-tree mst configuration コマンドで、MSTP の設定を確認できます。

MSTP インスタンスに割り当てられた VLAN の表示

show spanning-tree mst configuration コマンドで MSTP インスタンスに割り当てられた VLAN を確認できます。

表示例を以下に示します。

```
# show spanning-tree mst configuration

 Name      : TEST ...(1)
 (2)           (3)
 Revision : 1,Instances configured: 2
 (4)          (5)
 Instance     Vlans
 --------     ------------------------------------------------------------------
      0       1-9,20-4094
      1       10-19
```

各項目の説明は、以下のとおりです。

表 5-3 show spanning-tree mst configuration コマンドの表示項目

項番	説明
(1)	リージョン名を表示します。
(2)	リビジョン番号を表示します。
(3)	MSTP インスタンス数を表示します。
(4)	MSTP インスタンス番号を表示します。
(5)	MSTP インスタンスに割り当てられている VLAN を表示します。

MSTP リージョンの MD5 ダイジェストの表示

show spanning-tree mst configuration digest コマンドで MSTP リージョンの MD5 ダイジェストを確認できます。

表示例を以下に示します。

```
# show spanning-tree mst configuration digest

 Name     : TEST ...(1)
 (2)          (3)
 Revision : 1,Instances configured: 2
 Digest   : 8D0D3583ABF2D8F6F4CD1141B77F53D7 ...(4)
```

各項目の説明は、以下のとおりです。

表 5-4 show spanning-tree mst configuration digest コマンドの表示項目

項番	説明
(1)	リージョン名を表示します。
(2)	リビジョン番号を表示します。
(3)	MSTP インスタンス数を表示します。
(4)	MSTP リージョンの MD5 ダイジェストを表示します。

5.2.4 MSTP の動作状況の表示

MSTP の動作状況を確認できます。

MSTP の動作状況の表示

show spanning-tree mst コマンドで MSTP の動作状況を確認できます。instance パラメーターを指定した場合は、指定したインスタンスの動作状況だけを確認できます。

表示例を以下に示します。

```
# show spanning-tree mst
 (1)                    (2)
 Spanning tree: Enabled,protocol: MSTP
 NNI BPDU Address: dot1d(01-80-C2-00-00-00) ...(3)
 Number of MST instances: 2 ...(4)
     (5)     (6)
 >>>>MST00  vlans mapped : 1-9,20-4094
 (7)                                (8)
 Bridge Address: 00-40-66-A8-CC-36, Priority: 32768 (32768 sysid 0)
 (9)                                          (10)
 Designated Root Address: 00-40-66-B4-96-B5, Priority: 4096 (4096 sysid 0)
 CIST  External Root Cost : 0 ...(11)
 (12)                                            (13)
 Regional Root Bridge Address: 00-40-66-B4-96-B5, Priority: 4096 (4096 sysid 0)
 CIST  Internal Root Cost : 20000 ...(14)
 (15)                                        (16)
 Designated Bridge Address: 00-40-66-B4-96-B5, Priority: 4096 (4096 sysid 0)
 Topology Changes Count: 4 ...(17)
 (18)             (19)        (20)        (21)       (22)      (23)    (24)
                                                     Priority Link
 Interface        Role        State       Cost       .Port#    Type    Edge
 ---------------- ----------- ----------- ---------- --------- ------ --------
 Port1/0/1        designated  forwarding  20000      128.1     p2p     edge
 Port1/0/2        designated  forwarding  20000      128.2     p2p     edge
 Port1/0/12       root        forwarding  20000      128.12    p2p     non-edge

 >>>>MST01  vlans mapped : 10-19
 Bridge Address: 00-40-66-A8-CC-36, Priority: 32769 (32768 sysid 1)
 (25)                                       (26)
 Regional Root Address: 00-40-66-B4-96-B5, Priority: 8193 (8192 sysid 1)
 MSTI  Internal Root Cost : 20000 ...(27)
 Designated Bridge Address: 00-40-66-B4-96-B5, Priority: 8193 (8192 sysid 1)
 Topology Changes Count: 4

                                                     Priority Link
 Interface        Role        State       Cost       .Port#    Type    Edge
 ---------------- ----------- ----------- ---------- --------- ------ --------
 Port1/0/1        designated  forwarding  20000      128.1     p2p     edge
 Port1/0/2        disabled    disabled    20000      128.2     p2p     edge
 Port1/0/12       root        forwarding  20000      128.12    p2p     non-edge
```

各項目の説明は、以下のとおりです。

表 5-5 show spanning-tree mst コマンドの表示項目

項番	説明
(1)	MSTP の有効 (Enabled) ／無効 (Disabled) を表示します。
(2)	スパニングツリープロトコルを表示します。
(3)	BPDU の宛先 MAC アドレスを表示します。

項番	説明
(4)	MSTP インスタンス数を表示します。
(5)	MSTP インスタンス番号を表示します。
(6)	MSTP インスタンスに割り当てられている VLAN を表示します。
(7)	自装置の MAC アドレスを表示します。
(8)	自装置の優先度（ブリッジ優先度、sysid：MSTP インスタンス番号）を表示します。
(9)	CIST ルートの MAC アドレスを表示します。
(10)	CIST ルートの優先度（ブリッジ優先度、sysid：MSTP インスタンス番号）を表示します。
(11)	CIST 外部ルートパスコストを表示します。
(12)	CIST リージョナルルートの MAC アドレスを表示します。
(13)	CIST リージョナルルートの優先度（ブリッジ優先度、sysid：MSTP インスタンス番号）を表示します。
(14)	CIST 内部ルートパスコストを表示します。
(15)	ルートポートで受信した BPDU の送信元装置の MAC アドレスを表示します。自装置がルートブリッジの場合は自装置の MAC アドレスを表示します。
(16)	ルートポートで受信した BPDU の送信元装置の優先度（ブリッジ優先度、sysid：MSTP インスタンス番号）を表示します。自装置がルートブリッジの場合は自装置の優先度を表示します。
(17)	スパニングツリープロトコルのトポロジーが変更された回数を表示します。
(18)	ポート番号またはポートチャネル番号を表示します。
(19)	ポートの役割を表示します。 • root：ルートポート • designated：指定ポート • alternate：代替ポート • backup：バックアップポート • disabled：無効ポート • master：MSTI マスターポート
(20)	ポートのステータスを表示します。 • forwarding：フォワーディング状態 • blocking：ブロッキング状態（ディスカーディング状態） • learning：ラーニング状態 • disabled：無効状態
(21)	ポートのパスコストを表示します。
(22)	ポート ID（ポート優先度＋ポート番号（ifindex））を表示します。
(23)	ポートのリンクタイプの動作状況（p2p：ポイントツーポイントリンク／ shared：シェアードリンク）を表示します。
(24)	Port Fast モードの動作状況（edge：エッジポート／ non-edge：無効ポート）を表示します。

項番	説明
(25)	MSTI リージョナルルートの MAC アドレスを表示します。
(26)	MSTI リージョナルルートの優先度（ブリッジ優先度、sysid：MSTP インスタンス番号）を表示します。
(27)	MSTI リージョナルルートまでのパスコストを表示します。

インターフェースの MSTP 詳細情報の表示

show spanning-tree mst interface detail コマンドでインターフェースの MSTP 詳細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 spanning-tree mst interface port 1/0/12 detail

Port1/0/12 ...(1)
 (2)                          (3)
 Configured link type: auto, operation status: point-to-point
 (4)                                 (5)
 Configured fast-forwarding: auto, operation status: non-edge
 Bpdu statistic counter: sent: 29, received: 408 ...(6)
     (7)                 (8)
 >>>>MST instance: 00,  vlans mapped : 1-9,20-4094
 Port state: forwarding ...(9)
 Port role: root ...(10)
             (11)             (12)            (13)
 Port info : port ID 128.12, priority: 128, cost: 20000
 (14)                                      (15)
 Designated root address: 00-40-66-B4-96-B5, priority: 4096
 (16)                                    (17)
 Regional Root address: 00-40-66-B4-96-B5, priority: 4096
 (18)                                         (19)             (20)
 Designated bridge address: 00-40-66-B4-96-B5, priority: 4096, port id: 128.49

 >>>>MST instance: 01,  vlans mapped : 10-19
 Port state: forwarding
 Port role: root
 Port info : port ID 128.12, priority: 128, cost: 20000
 (21)                                      (22)
 Designated root address: 00-40-66-B4-96-B5, priority: 8193
 (23)                                         (24)             (25)
 Designated bridge address: 00-40-66-B4-96-B5, priority: 8193, port id: 128.49
```

各項目の説明は、以下のとおりです。

表 5-6 show spanning-tree mst interface detail コマンドの表示項目

項番	説明
(1)	ポート番号またはポートチャネル番号を表示します。
(2)	ポートのリンクタイプの設定を表示します。デフォルトの自動判別設定の場合、全二重ポートはポイントツーポイントリンク、半二重ポートはシェアードリンクと判別されます。 • auto：自動判別設定 • p2p：手動設定（ポイントツーポイントリンク） • shared：手動設定（シェアードリンク）

項番	説明
(3)	ポートのリンクタイプの動作状況（p2p：ポイントツーポイントリンク／ shared：シェアードリンク）を表示します。
(4)	Port Fast モードの設定を表示します。 • auto：ネットワークポート • edge：エッジポート • non-edge：無効ポート
(5)	Port Fast モードの動作状況（edge：エッジポート／ non-edge：無効ポート）を表示します。
(6)	BPDU の送受信数を表示します。
(7)	MSTP インスタンス番号を表示します。
(8)	MSTP インスタンスに割り当てられている VLAN を表示します。
(9)	ポートのステータスを表示します。 • forwarding：フォワーディング状態 • blocking：ブロッキング状態（ディスカーディング状態） • learning：ラーニング状態 • disabled：無効状態
(10)	ポートの役割を表示します。 • root：ルートポート • designated：指定ポート • alternate：代替ポート • backup：バックアップポート • disabled：無効ポート • master：MSTI マスターポート
(11)	ポート ID（ポート優先度＋ポート番号（ifindex））を表示します。
(12)	ポート優先度を表示します。
(13)	ポートのパスコストを表示します。
(14)	CIST ルートの MAC アドレスを表示します。
(15)	CIST ルートの優先度を表示します。
(16)	CIST リージョナルルートの MAC アドレスを表示します。
(17)	CIST リージョナルルートの優先度を表示します。
(18)	対象リンクで CIST リージョナルルートに最も近い装置の MAC アドレスを表示します。
(19)	対象リンクで CIST リージョナルルートに最も近い装置の優先度を表示します。
(20)	対象リンクで CIST リージョナルルートに最も近い装置のポート ID（ポート優先度＋ポート番号（ifindex））を表示します。
(21)	MSTI リージョナルルートの MAC アドレスを表示します。
(22)	MSTI リージョナルルートの優先度を表示します。
(23)	対象リンクで MSTI リージョナルルートに最も近い装置の MAC アドレスを表示します。

項番	説明
(24)	対象リンクで MSTI リージョナルルートに最も近い装置の優先度を表示します。
(25)	対象リンクで MSTI リージョナルルートに最も近い装置のポート ID（ポート優先度＋ポート番号(ifindex)）を表示します。

5.2.5 RPVST+ の動作状況の表示

RPVST+ の動作状況を確認できます。

RPVST+ の動作状況の表示

show spanning-tree vlan コマンドで RPVST+ の動作状況を確認できます。VLAN ID を指定した場合は、指定した VLAN の動作状況だけを確認できます。

VLAN 10 を指定した場合の表示例を以下に示します。

```
# show spanning-tree vlan 10

VLAN10 ...(1)
 Spanning tree enabled protocol RPVST+ ...(2)
 Root ID Priority: 32778 ...(3)
         Address: 00-40-66-01-02-03 ...(4)
         This bridge is the root. ...(5)
         (6)                (7)               (8)
         Hello Time: 2 sec, Max Age: 20 sec, Forward Delay: 15 sec
 Bridge ID Priority: 32778 (priority 32768  sys-id-ext 10) ...(9)
         Address: 00-40-66-01-02-03 ...(10)
         (11)               (12)              (13)
         Hello Time: 2 sec, Max Age: 20 sec, Forward Delay: 15 sec
 Topology Changes Count: 1 ...(14)
 (15)            (16)       (17)       (18)      (19)     (20)    (21)
                                                Priority Link
 Interface       Role       State      Cost      .Port#   Type    Edge
 --------------- ---------- ---------- --------- -------- ------ --------
 Port1/0/1       designated forwarding 20000     128.1    p2p    non-edge
 Port1/0/2       designated forwarding 20000     128.2    p2p    non-edge
```

各項目の説明は、以下のとおりです。

表 5-7 show spanning-tree vlan コマンドの表示項目

項番	説明
(1)	VLAN ID を表示します。
(2)	有効になっているスパニングツリープロトコルを表示します。
(3)	ルートブリッジの優先度を表示します。
(4)	ルートブリッジの MAC アドレスを表示します。
(5)	自装置がルートブリッジの場合に表示されます。
(6)	ルートブリッジのハロータイムを表示します。
(7)	ルートブリッジの最大エージタイムを表示します。
(8)	ルートブリッジのフォワードディレイタイムを表示します。

項番	説明
(9)	自装置の優先度（対象 VLAN のブリッジ優先度と VLAN ID）を表示します。
(10)	自装置の MAC アドレスを表示します。
(11)	自装置のハロータイムを表示します。
(12)	自装置の最大エージタイムを表示します。
(13)	自装置のフォワードディレイタイムを表示します。
(14)	RPVST+ のトポロジーが変更された回数を表示します。
(15)	ポート番号またはポートチャネル番号を表示します。
(16)	ポートの役割を表示します。 • root：ルートポート • designated：指定ポート • alternate：代替ポート • backup：バックアップポート • disabled：無効ポート
(17)	ポートのステータスを表示します。 • forwarding：フォワーディング状態 • blocking：ブロッキング状態（ディスカーディング状態） • learning：ラーニング状態 • disabled：無効状態
(18)	ポートのパスコストを表示します。
(19)	ポート ID（ポート優先度＋ポート番号（ifindex））を表示します。
(20)	ポートのリンクタイプの動作状況（p2p：ポイントツーポイントリンク／ shared：シェアードリンク）を表示します。
(21)	Port Fast モードの動作状況（edge：エッジポート／ non-edge：無効ポート）を表示します。

インターフェースの RPVST+ 詳細情報の表示

show spanning-tree vlan interface コマンドで、指定した VLAN のインターフェースの RPVST+ 詳細情報を確認できます。

VLAN 10 のポート 1/0/1 を指定した場合の表示例を以下に示します。

```
# show spanning-tree vlan 10 interface port 1/0/1
(1)           (2)
Port1/0/1  of VLAN10
 (3)                    (4)
 Port role: designated, Port state: learning
 (5)                    (6)                  (7)
 Port path cost: 20000, Port priority: 128, Port Identifier: 128.1
 (8)                                      (9)
 Designated root bridge priority: 32768, address: 00-40-66-01-02-03
 (10)                                (11)
 Designated bridge priority: 32768, address: 00-40-66-01-02-03
 (12)                        (13)
 Designated port id: 128.1, designated path cost: 0
 (14)                         (15)
 Configured link type: auto, operation status: p2p
 (16)                                (17)
 Configured fast-forwarding: auto, operation status: non-edge
 BPDU: sent: 33, received: 0 ...(18)
```

各項目の説明は、以下のとおりです。

表 5-8 show spanning-tree vlan interface コマンドの表示項目

項番	説明
(1)	ポート番号またはポートチャネル番号を表示します。
(2)	VLAN ID を表示します。
(3)	ポートの役割を表示します。 • root：ルートポート • designated：指定ポート • alternate：代替ポート • backup：バックアップポート • disabled：無効ポート
(4)	ポートのステータスを表示します。 • forwarding：フォワーディング状態 • blocking：ブロッキング状態（ディスカーディング状態） • learning：ラーニング状態 • disabled：無効状態
(5)	ポートのパスコストを表示します。
(6)	ポート優先度を表示します。
(7)	ポート ID（ポート優先度＋ポート番号（ifindex））を表示します。
(8)	ルートブリッジの優先度を表示します。
(9)	ルートブリッジの MAC アドレスを表示します。
(10)	対象リンクでルートブリッジに最も近い装置の優先度を表示します。

項番	説明
(11)	対象リンクでルートブリッジに最も近い装置の MAC アドレスを表示します。
(12)	対象リンクでルートブリッジに最も近い装置のポート ID（ポート優先度＋ポート番号（ifindex））を表示します。
(13)	対象リンクでルートブリッジに最も近い装置からルートブリッジまでのパスコストを表示します。
(14)	ポートのリンクタイプの設定を表示します。デフォルトの自動判別設定の場合、全二重ポートはポイントツーポイントリンク、半二重ポートはシェアードリンクと判別されます。 • auto：自動判別設定 • point-to-point：手動設定（ポイントツーポイントリンク） • shared：手動設定（シェアードリンク）
(15)	ポートのリンクタイプの動作状況（p2p：ポイントツーポイントリンク／ shared：シェアードリンク）を表示します。
(16)	Port Fast モードの設定を表示します。 • auto：ネットワークポート • edge：エッジポート • non-edge：無効ポート
(17)	Port Fast モードの動作状況（edge：エッジポート／ non-edge：無効ポート）を表示します。
(18)	BPDU の送受信数を表示します。

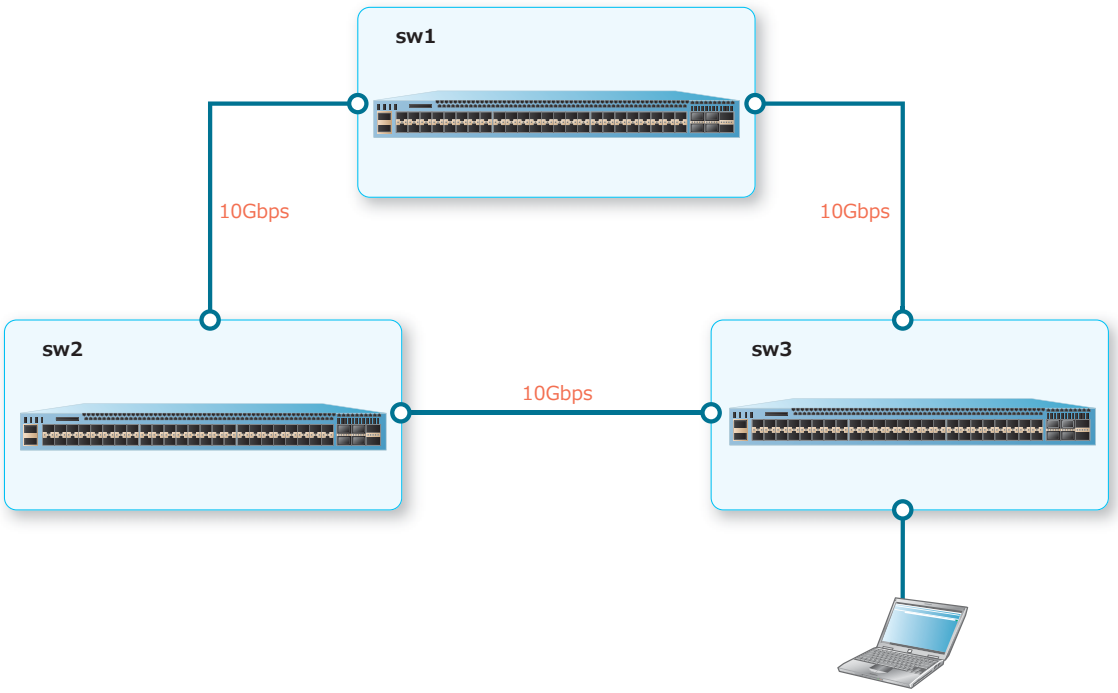
5.3 スパニングツリーの構成例と設定例

スパニングツリーを利用する場合の構成例と設定例を示します。

5.3.1 RSTP の構成例と設定例

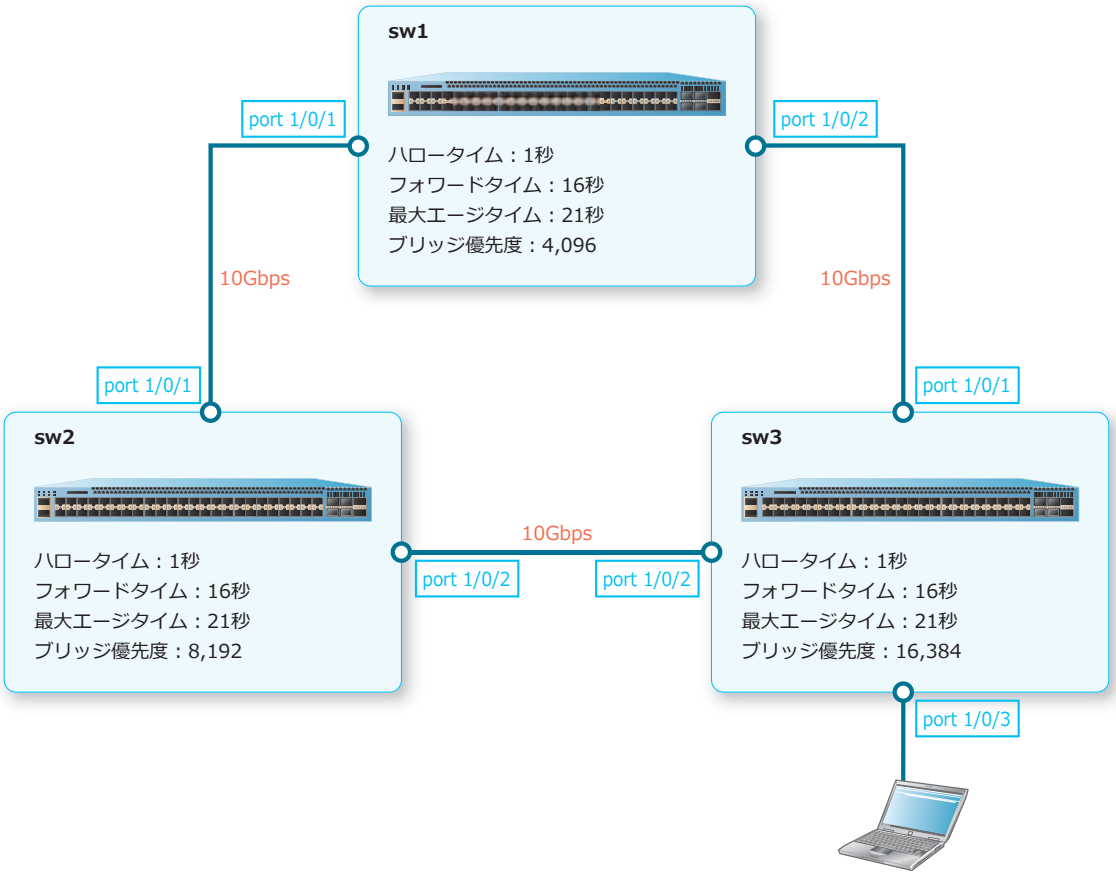
3 台の装置をリングトポロジーで接続し、RSTP を使用してスパニングツリーを有効化する場合の構成例と設定例を示します。

図 5-9 RSTP の構成例



5.3.1.1 RSTP：sw1 の設定例

図 5-10 RSTP：sw1 の設定例



1. ハロータイムを［1 秒］に、フォワードタイムを［16 秒］に、最大エージタイムを［21 秒］に設定します。

```
sw1# configure terminal
sw1(config)# spanning-tree hello-time 1
sw1(config)# spanning-tree forward-time 16
sw1(config)# spanning-tree max-age 21
sw1(config)#
```

2. ブリッジ優先度を［4,096］に設定します。

```
sw1(config)# spanning-tree priority 4096
sw1(config)#
```

3. ポート 1/0/1 からポート 1/0/2 のスパニングツリーを有効化します。

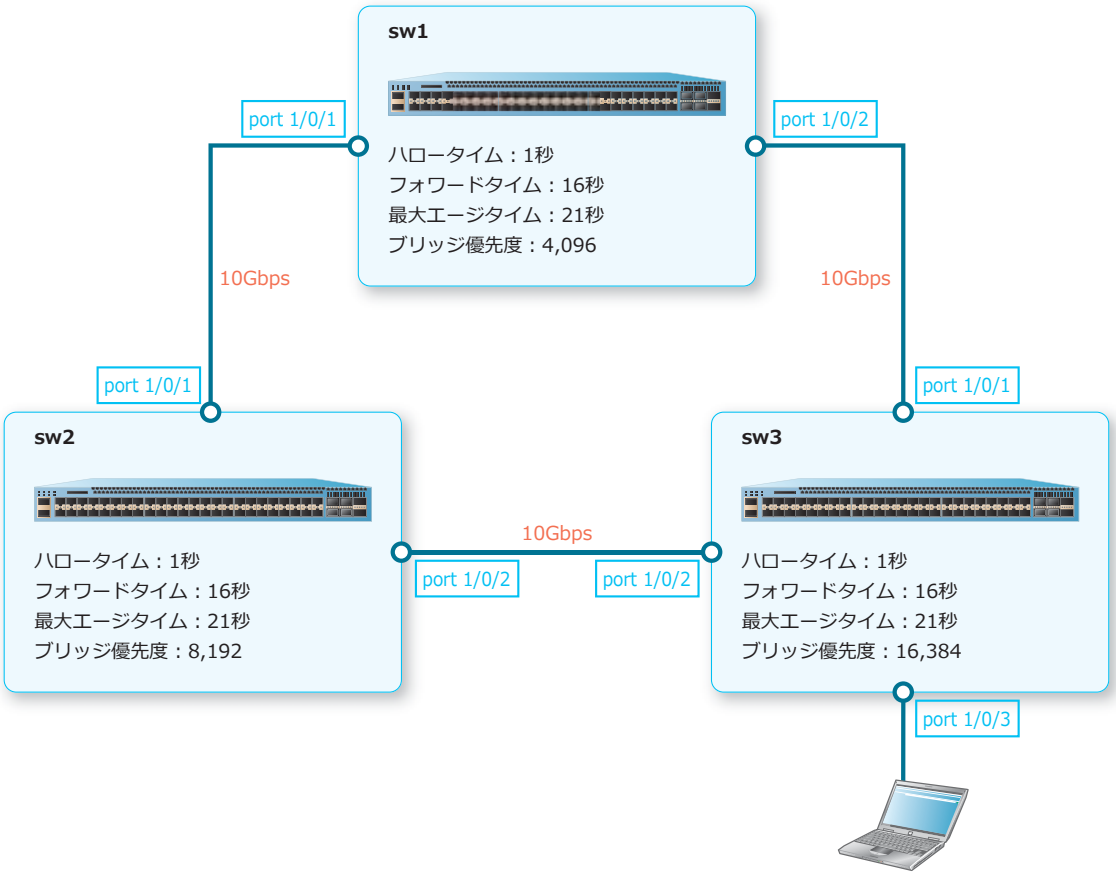
```
sw1(config)# interface range port 1/0/1-2
sw1(config-if-port-range)# spanning-tree state enable
sw1(config-if-port-range)# exit
sw1(config)#
```

4. 装置のスパニングツリーを有効化します。

```
sw1(config)# spanning-tree global state enable
sw1(config)# end
sw1#
```

5.3.1.2 RSTP：sw2 の設定例

図 5-11 RSTP：sw2 の設定例



1. ハロータイムを［1 秒］に、フォワードタイムを［16 秒］に、最大エージタイムを［21 秒］に設定します。

```
sw2# configure terminal
sw2(config)# spanning-tree hello-time 1
sw2(config)# spanning-tree forward-time 16
sw2(config)# spanning-tree max-age 21
sw2(config)#
```

2. ブリッジ優先度を［8,192］に設定します。

```
sw2(config)# spanning-tree priority 8192
sw2(config)#
```

3. ポート 1/0/1 からポート 1/0/2 のスパニングツリーを有効化します。

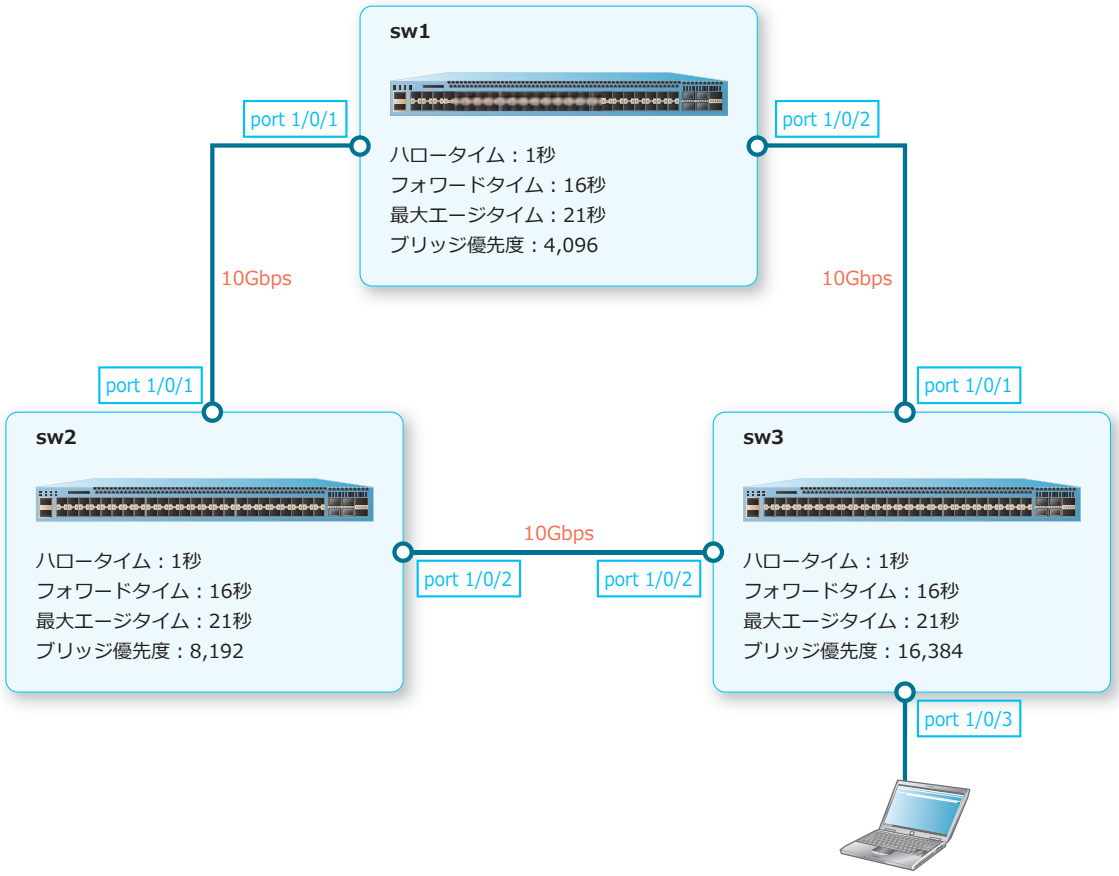
```
sw2(config)# interface range port 1/0/1-2
sw2(config-if-port-range)# spanning-tree state enable
sw2(config-if-port-range)# exit
sw2(config)#
```

4. 装置のスパニングツリーを有効化します。

```
sw2(config)# spanning-tree global state enable
sw2(config)# end
sw2#
```

5.3.1.3 RSTP：sw3 の設定例

図 5-12 RSTP：sw3 の設定例



1. ハロータイムを［1 秒］に、フォワードタイムを［16 秒］に、最大エージタイムを［21 秒］に設定します。

```
sw3# configure terminal
sw3(config)# spanning-tree hello-time 1
sw3(config)# spanning-tree forward-time 16
sw3(config)# spanning-tree max-age 21
sw3(config)#
```

2. ブリッジ優先度を［16,384］に設定します。

```
sw3(config)# spanning-tree priority 16384
sw3(config)#
```

3. ポート 1/0/1 からポート 1/0/2 のスパニングツリーを有効化します。

```
sw3(config)# interface range port 1/0/1-2
sw3(config-if-port-range)# spanning-tree state enable
sw3(config-if-port-range)# exit
sw3(config)#
```

4. ポート 1/0/3 をエッジポートに設定します。

```
sw3(config)# interface port 1/0/3
sw3(config-if-port)# spanning-tree portfast edge
sw3(config-if-port)# exit
sw3(config)#
```

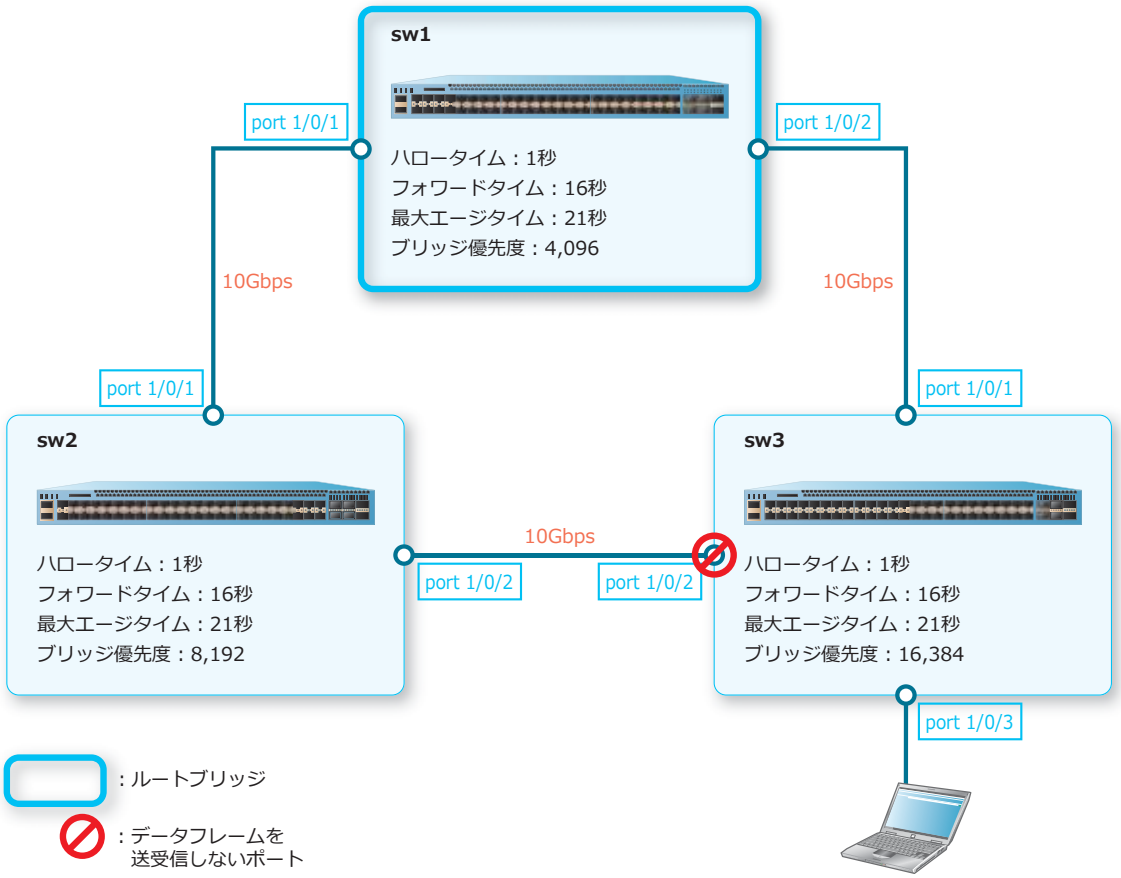
5. 装置のスパニングツリーを有効化します。

```
sw3(config)# spanning-tree global state enable
sw3(config)# end
sw3#
```

5.3.1.4 RSTP を使用した場合の設定結果例

設定例のとおりに設定すると、ルートブリッジと代替ポートは以下のように選択されます。

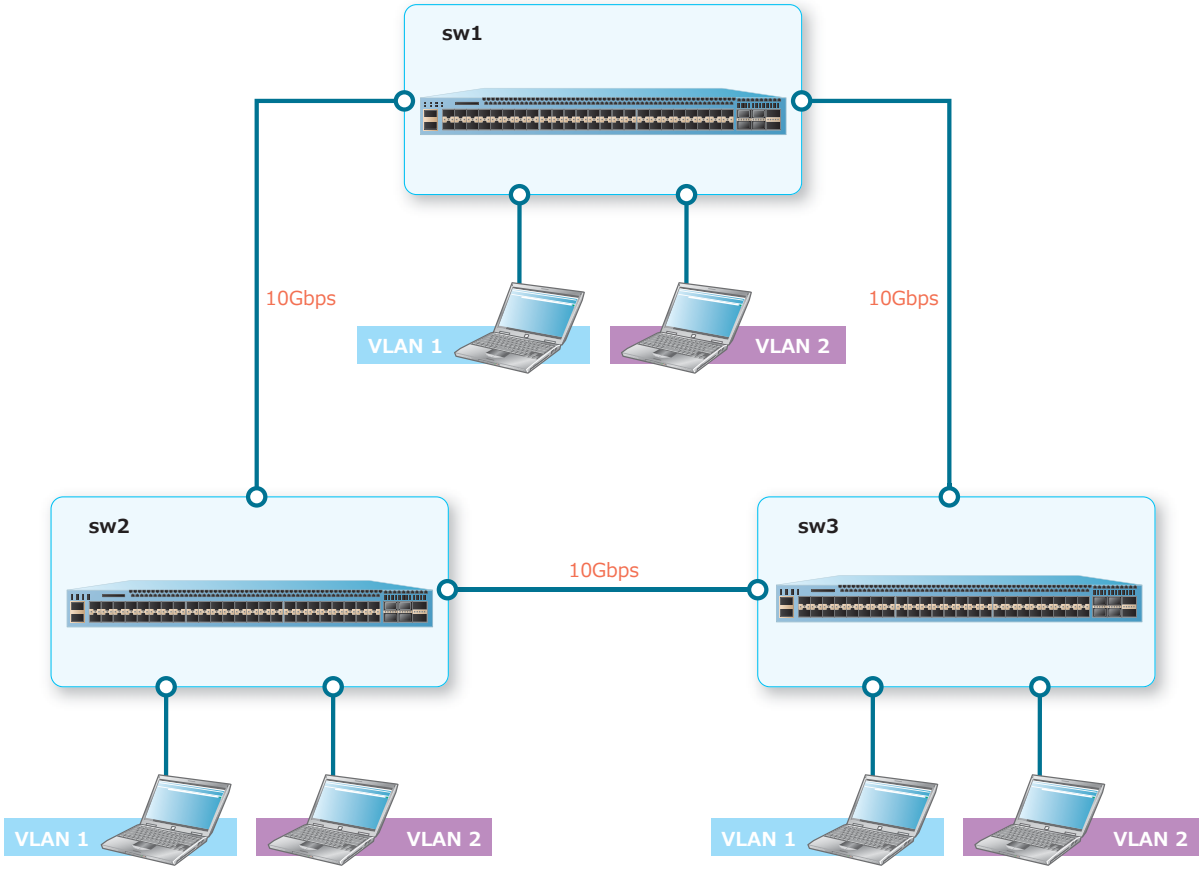
図 5-13 RSTP を使用した場合の設定結果例



5.3.2 MSTP の構成例と設定例

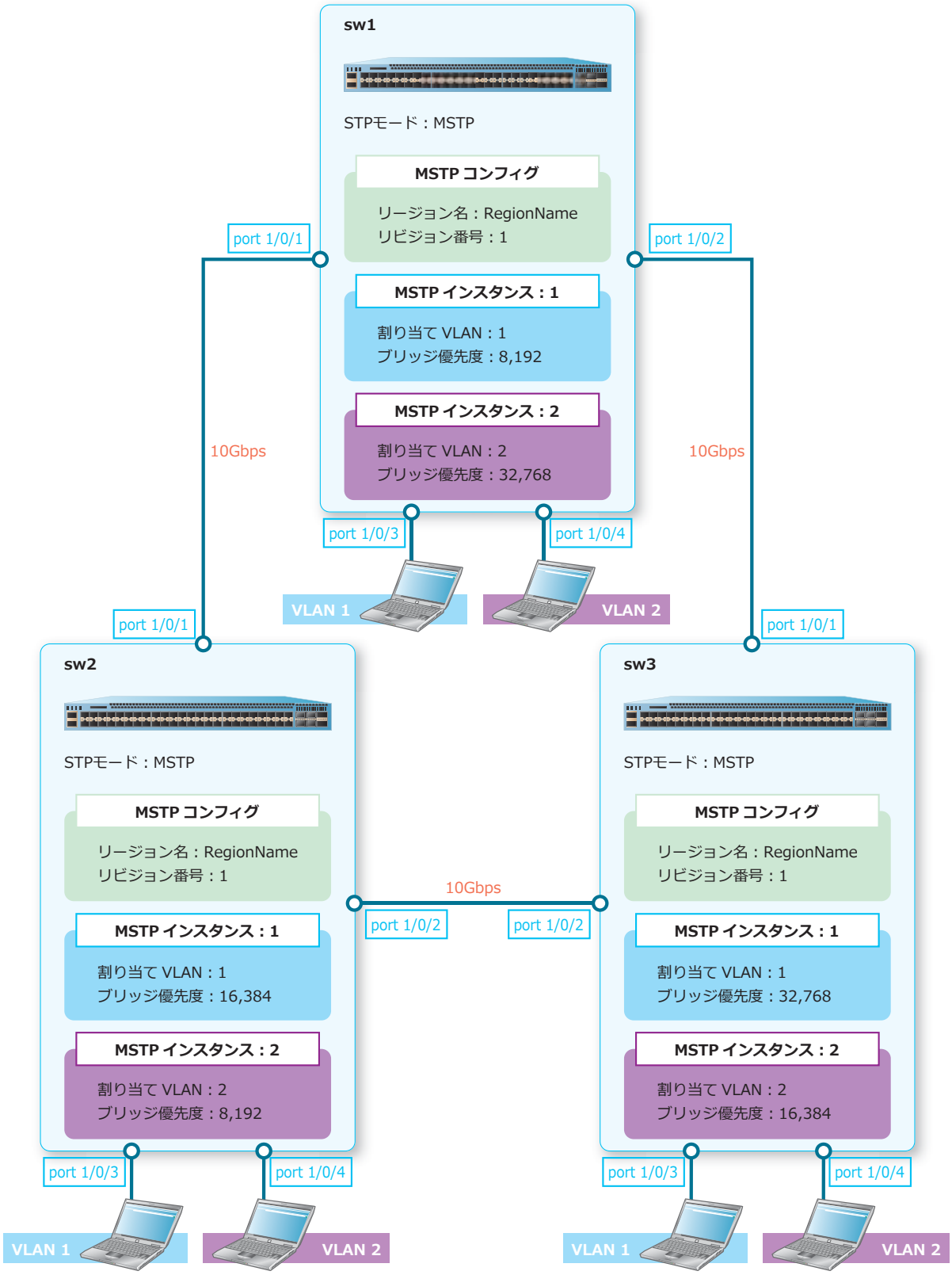
3 台の装置をリングトポロジーで接続し、MSTP を使用してスパニングツリーを有効化する場合の構成例と設定例を示します。

図 5-14 MSTP の構成例



5.3.2.1 MSTP：sw1 の設定例

図 5-15 MSTP：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 からポート 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 1 および VLAN 2］を割り当てます。

```
sw1(config)# interface range port 1/0/1-2
sw1(config-if-port-range)# switchport mode trunk
sw1(config-if-port-range)# switchport trunk allowed vlan 1,2
sw1(config-if-port-range)# exit
```

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 2］を割り当てます。

```
sw1(config)# interface port 1/0/4
sw1(config-if-port)# switchport access vlan 2
sw1(config-if-port)# exit
sw1(config)#
```

4. スパニングツリープロトコルを MSTP に設定します。

```
sw1(config)# spanning-tree mode mstp
sw1(config)#
```

5. ポート 1/0/1 からポート 1/0/2 のスパニングツリーを有効化します。

```
sw1(config)# interface range port 1/0/1-2
sw1(config-if-port-range)# spanning-tree state enable
sw1(config-if-port-range)# exit
sw1(config)#
```

6. MSTP インスタンス［1］に［VLAN 1］、MSTP インスタンス［2］に［VLAN 2］を割り当てます。

```
sw1(config)# spanning-tree mst configuration
sw1(config-mst)# instance 1 vlans 1
sw1(config-mst)# instance 2 vlans 2
sw1(config-mst)#
```

7. MSTP のリージョン名を［RegionName］に、リビジョン番号を［1］に設定します。

```
sw1(config-mst)# name RegionName
sw1(config-mst)# revision 1
sw1(config-mst)# exit
sw1(config)#
```

8. MSTP インスタンス［1］のブリッジ優先度を［8,192］に設定します。

```
sw1(config)# spanning-tree mst 1 priority 8192
sw1(config)#
```

9. ポート 1/0/3 からポート 1/0/4 をエッジポートに設定します。

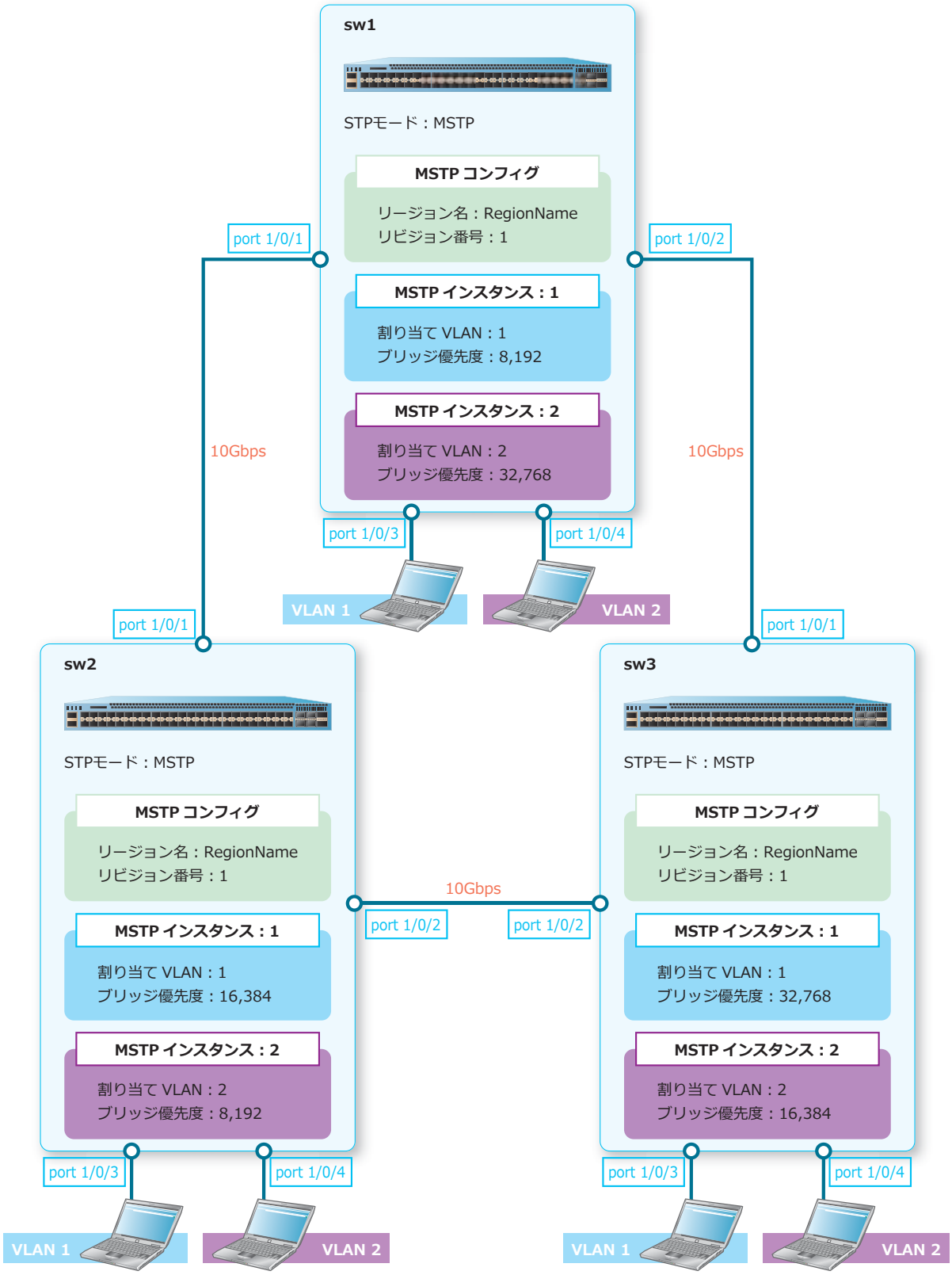
```
sw1(config)# interface range port 1/0/3-4
sw1(config-if-port-range)# spanning-tree portfast edge
sw1(config-if-port-range)# exit
sw1(config)#
```

10. 装置のスパニングツリーを有効化します。

```
sw1(config)# spanning-tree global state enable
sw1(config)# end
sw1#
```

5.3.2.2 MSTP：sw2 の設定例

図 5-16 MSTP：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 からポート 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 1 および VLAN 2］を割り当てます。

```
sw2(config)# interface range port 1/0/1-2
sw2(config-if-port-range)# switchport mode trunk
sw2(config-if-port-range)# switchport trunk allowed vlan 1,2
sw2(config-if-port-range)# exit
```

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 2］を割り当てます。

```
sw2(config)# interface port 1/0/4
sw2(config-if-port)# switchport access vlan 2
sw2(config-if-port)# exit
sw2(config)#
```

4. スパニングツリープロトコルを MSTP に設定します。

```
sw2(config)# spanning-tree mode mstp
sw2(config)#
```

5. ポート 1/0/1 からポート 1/0/2 のスパニングツリーを有効化します。

```
sw2(config)# interface range port 1/0/1-2
sw2(config-if-port-range)# spanning-tree state enable
sw2(config-if-port-range)# exit
sw2(config)#
```

6. MSTP インスタンス［1］に［VLAN 1］、MSTP インスタンス［2］に［VLAN 2］を割り当てます。

```
sw2(config)# spanning-tree mst configuration
sw2(config-mst)# instance 1 vlans 1
sw2(config-mst)# instance 2 vlans 2
sw2(config-mst)#
```

7. MSTP のリージョン名を［RegionName］に、リビジョン番号を［1］に設定します。

```
sw2(config-mst)# name RegionName
sw2(config-mst)# revision 1
sw2(config-mst)# exit
sw2(config)#
```

8. MSTP インスタンス［1］のブリッジ優先度を［16,384］に、MSTP インスタンス［2］のブリッジ優先度を［8,192］に設定します。

```
sw2(config)# spanning-tree mst 1 priority 16384
sw2(config)# spanning-tree mst 2 priority 8192
sw2(config)#
```

9. ポート 1/0/3 からポート 1/0/4 をエッジポートに設定します。

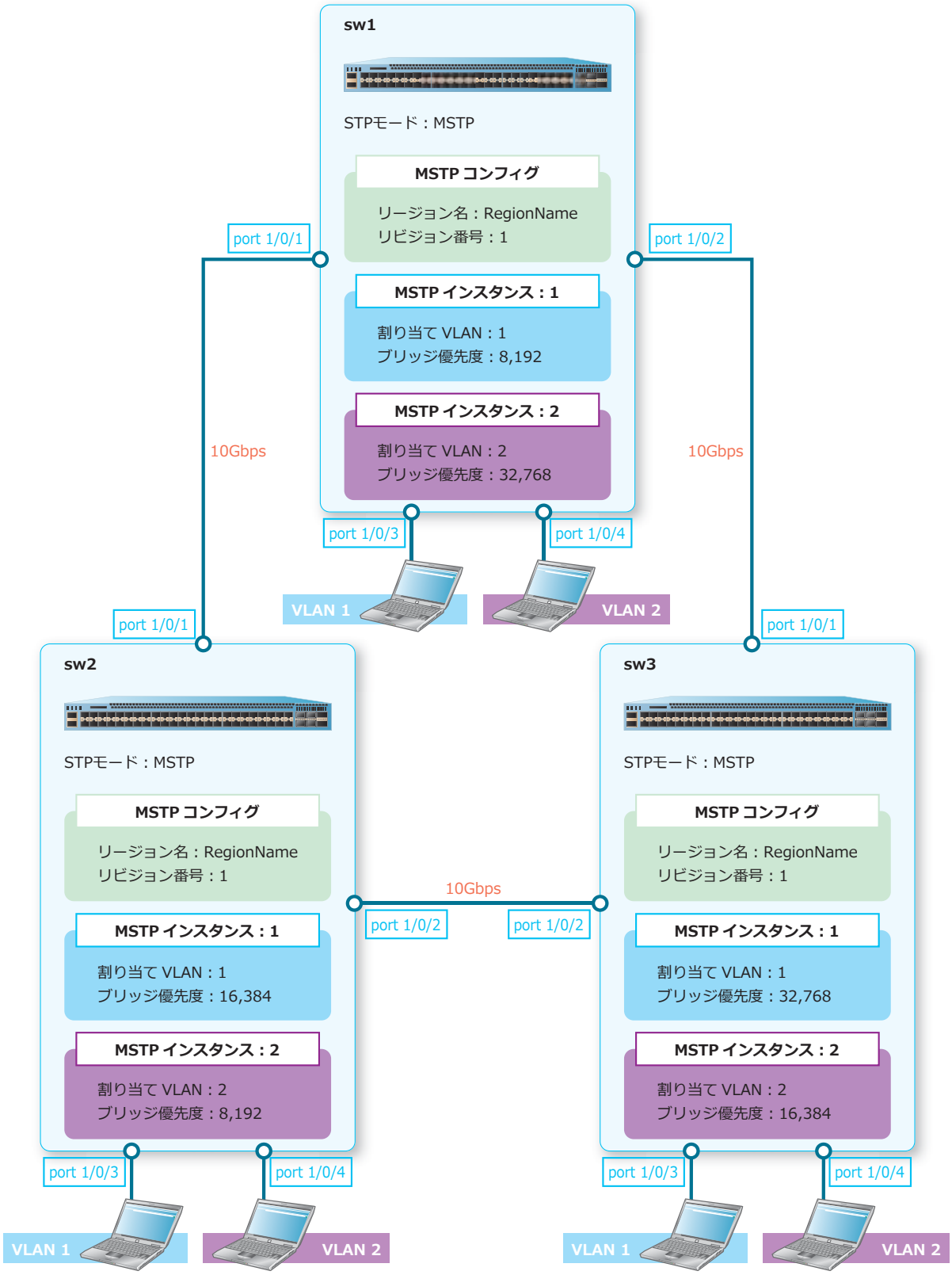
```
sw2(config)# interface range port 1/0/3-4
sw2(config-if-port-range)# spanning-tree portfast edge
sw2(config-if-port-range)# exit
sw2(config)#
```

10. 装置のスパニングツリーを有効化します。

```
sw2(config)# spanning-tree global state enable
sw2(config)# end
sw2#
```

5.3.2.3 MSTP：sw3 の設定例

図 5-17 MSTP：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 からポート 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 1 および VLAN 2］を割り当てます。

```
sw3(config)# interface range port 1/0/1-2
sw3(config-if-port-range)# switchport mode trunk
sw3(config-if-port-range)# switchport trunk allowed vlan 1,2
sw3(config-if-port-range)# exit
```

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 2］を割り当てます。

```
sw3(config)# interface port 1/0/4
sw3(config-if-port)# switchport access vlan 2
sw3(config-if-port)# exit
sw3(config)#
```

4. スパニングツリープロトコルを MSTP に設定します。

```
sw3(config)# spanning-tree mode mstp
sw3(config)#
```

5. ポート 1/0/1 からポート 1/0/2 のスパニングツリーを有効化します。

```
sw3(config)# interface range port 1/0/1-2
sw3(config-if-port-range)# spanning-tree state enable
sw3(config-if-port-range)# exit
sw3(config)#
```

6. MSTP インスタンス［1］に［VLAN 1］、MSTP インスタンス［2］に［VLAN 2］を割り当てます。

```
sw3(config)# spanning-tree mst configuration
sw3(config-mst)# instance 1 vlans 1
sw3(config-mst)# instance 2 vlans 2
sw3(config-mst)#
```

7. MSTP のリージョン名を［RegionName］に、リビジョン番号を［1］に設定します。

```
sw3(config-mst)# name RegionName
sw3(config-mst)# revision 1
sw3(config-mst)# exit
sw3(config)#
```

8. MSTP インスタンス［2］のブリッジ優先度を［16,384］に設定します。

```
sw3(config)# spanning-tree mst 2 priority 16384
sw3(config)#
```

9. ポート 1/0/3 からポート 1/0/4 をエッジポートに設定します。

```
sw3(config)# interface range port 1/0/3-4
sw3(config-if-port-range)# spanning-tree portfast edge
sw3(config-if-port-range)# exit
sw3(config)#
```

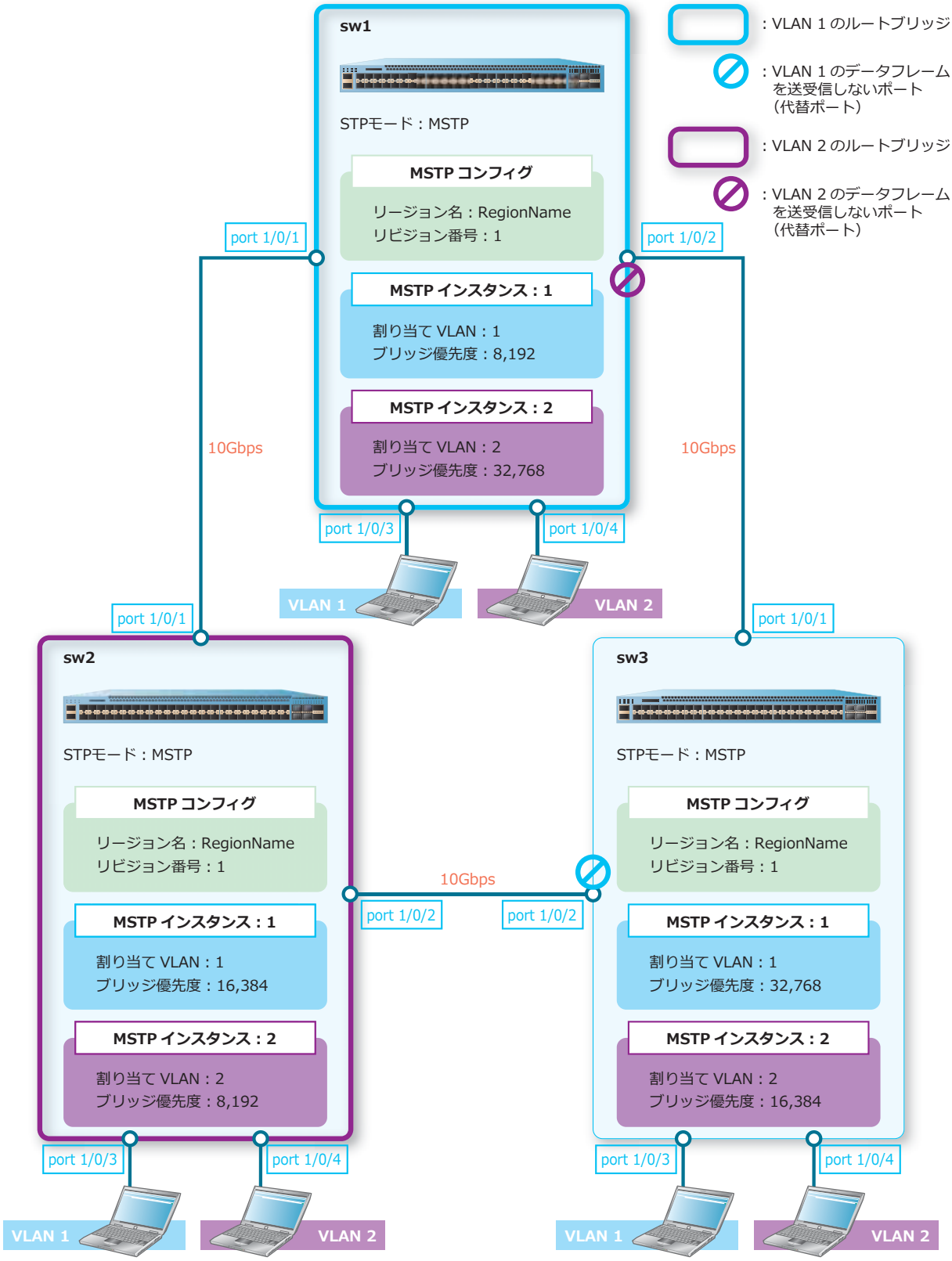
10. 装置のスパニングツリーを有効化します。

```
sw3(config)# spanning-tree global state enable
sw3(config)# end
sw3#
```

5.3.2.4 MSTP を使用した場合の設定結果例

MSTP では、MSTP インスタンスごとにルートブリッジや代替ポートが異なります。設定例のとおりに設定すると、ルートブリッジと代替ポートは以下のように選択されます。

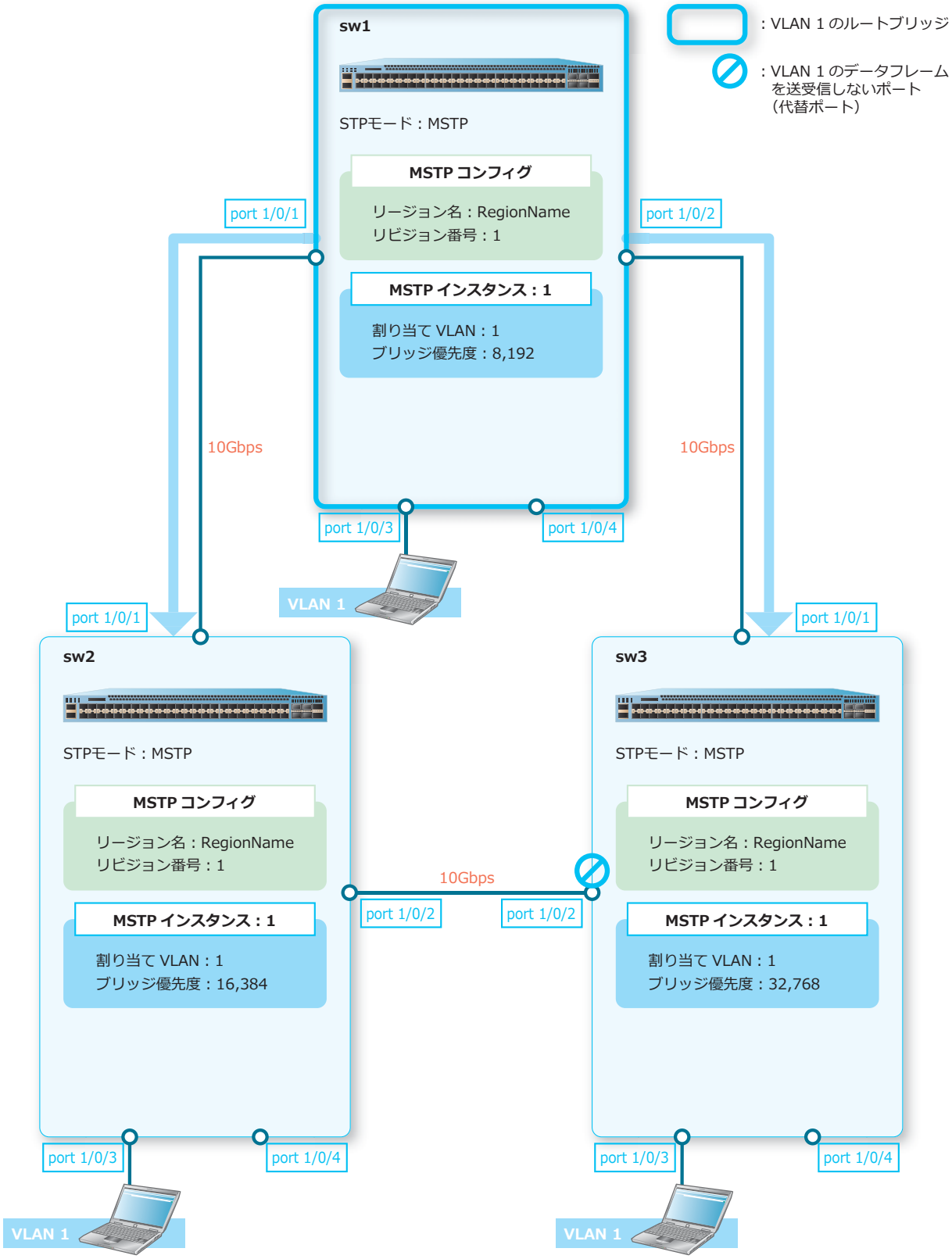
図 5-18 MSTP を使用した場合の設定結果例



MSTP インスタンス 1 の場合

MSTP インスタンス 1 のルートブリッジは sw1、代替ポートは sw3 のポート 1/0/2 です。ルートブリッジからは、下図のようにデータフレームが送信されます。

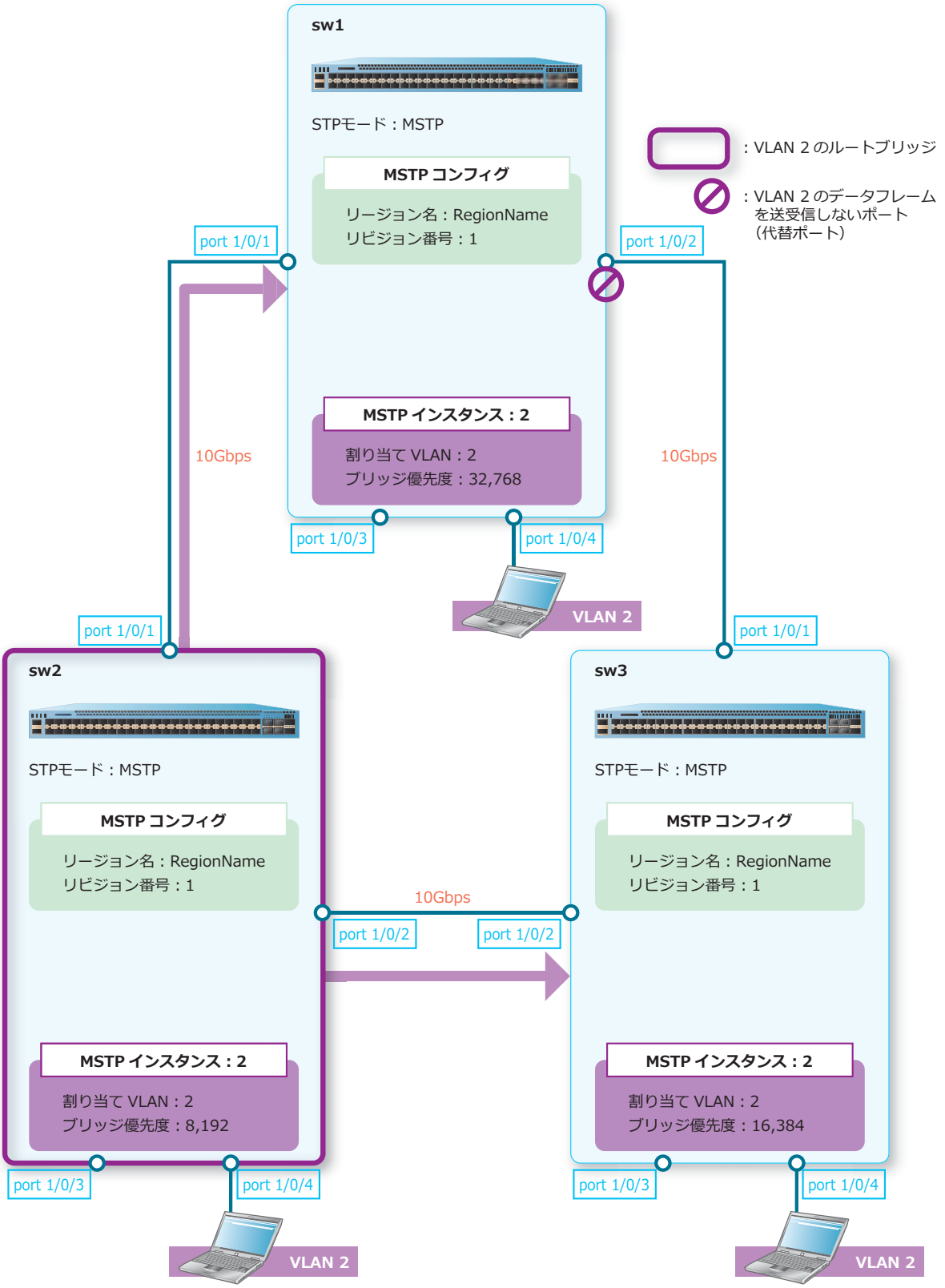
図 5-19 MSTP を使用した場合の設定結果例（MSTP インスタンス 1）



MSTP インスタンス 2 の場合

MSTP インスタンス 2 のルートブリッジは sw2、代替ポートは sw1 のポート 1/0/2 です。ルートブリッジからは、下図のようにデータフレームが送信されます。

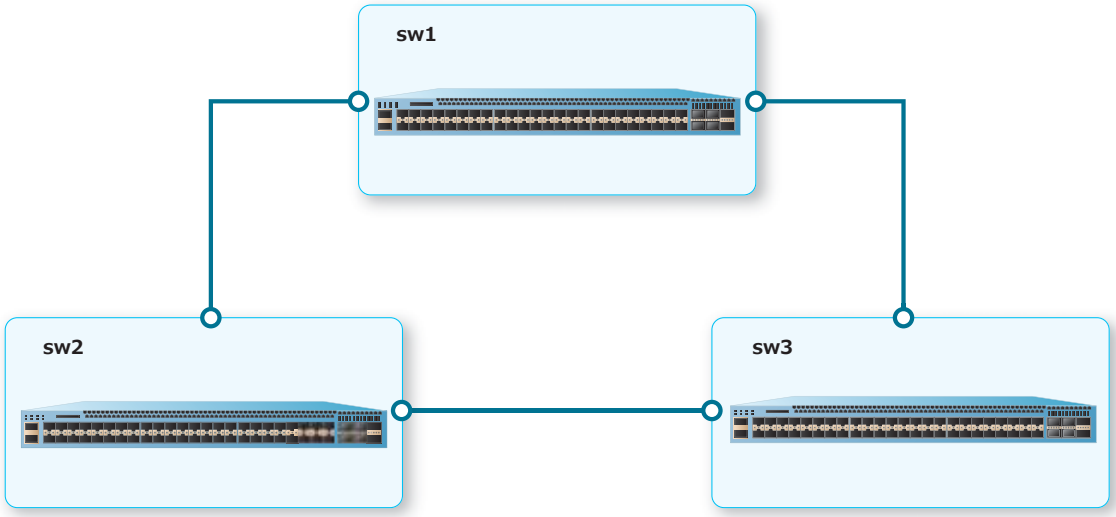
図 5-20 MSTP を使用した場合の設定結果例（MSTP インスタンス 2）



5.3.3 RPVST+ の構成例と設定例

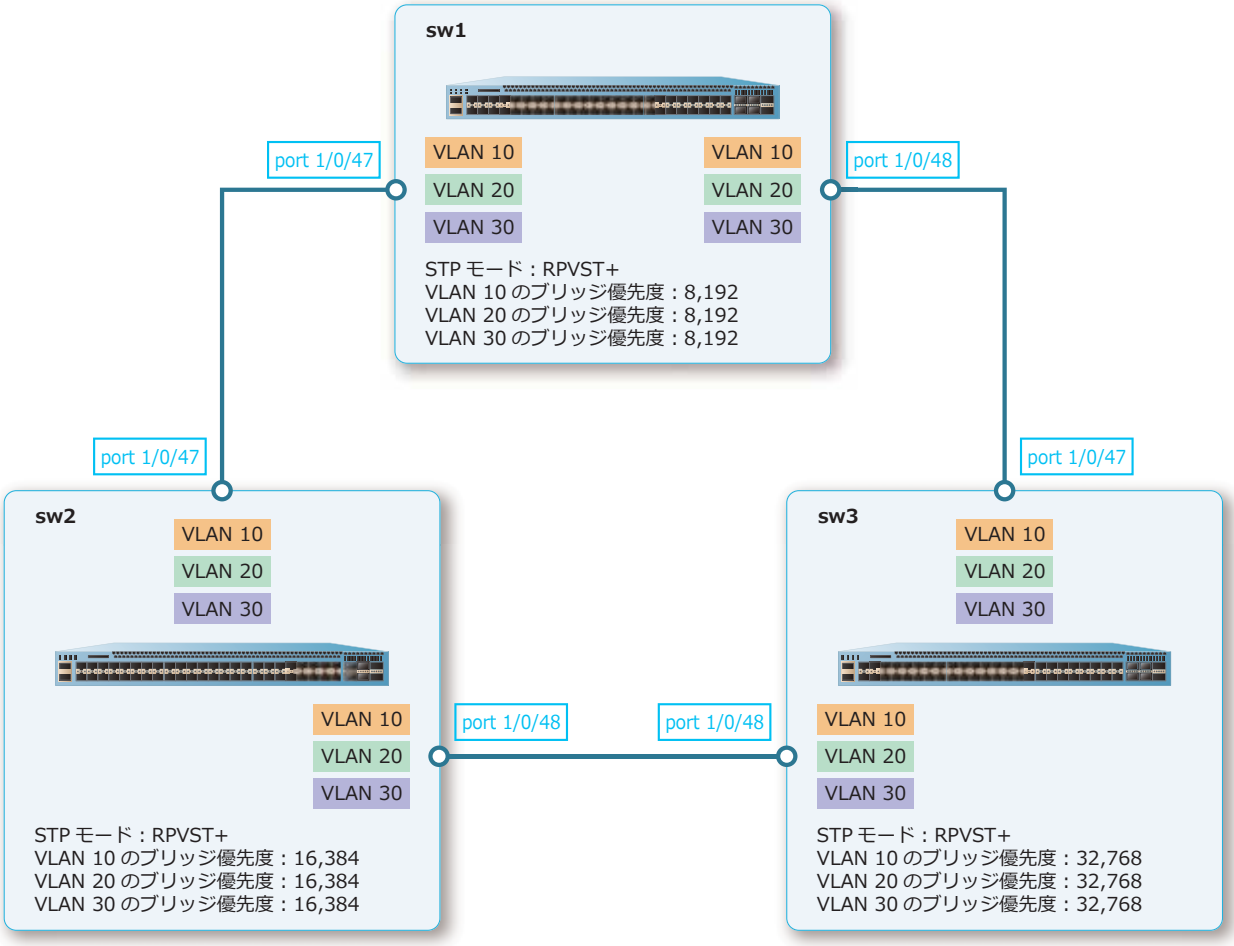
3 台の装置をリングトポロジーで接続し、RPVST+ を使用してスパニングツリーを有効化する場合の構成例と設定例を示します。

図 5-21 RPVST+ の構成例



5.3.3.1 RPVST+：sw1 の設定例

図 5-22 RPVST+：sw1 の設定例



1. VLAN 10、VLAN 20、および VLAN 30 を作成します。

```
sw1# configure terminal
sw1(config)# vlan 10,20,30
sw1(config-vlan)# exit
sw1(config)#
```

2. ポート 1/0/47 およびポート 1/0/48 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 20、および VLAN 30］を割り当てます。

```
sw1(config)# interface port 1/0/47
sw1(config-if-port)# switchport mode trunk
sw1(config-if-port)# switchport trunk allowed vlan 10,20,30
sw1(config-if-port)# exit
sw1(config)# interface port 1/0/48
sw1(config-if-port)# switchport mode trunk
sw1(config-if-port)# switchport trunk allowed vlan 10,20,30
sw1(config-if-port)# exit
sw1(config)#
```

3. スパニングツリープロトコルを RPVST+ に設定します。

```
sw1(config)# spanning-tree mode rpvst+
sw1(config)#
```

4. VLAN 10、VLAN 20、および VLAN 30 をスパニングツリー VLAN として指定し、ブリッジ優先度を［8,192］に設定します。

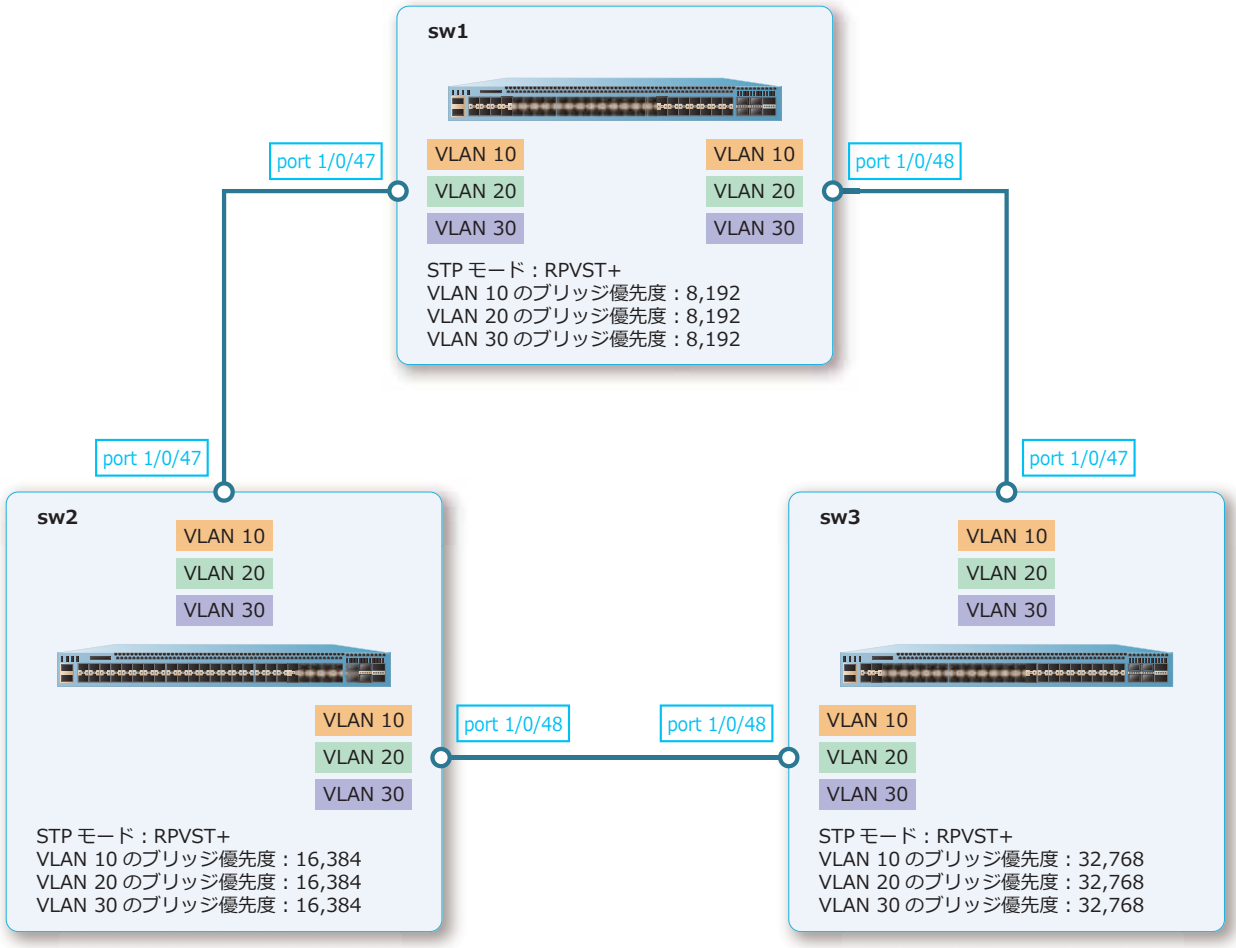
```
sw1(config)# spanning-tree vlan 10
sw1(config)# spanning-tree vlan 10 priority 8192
sw1(config)# spanning-tree vlan 20
sw1(config)# spanning-tree vlan 20 priority 8192
sw1(config)# spanning-tree vlan 30
sw1(config)# spanning-tree vlan 30 priority 8192
sw1(config)#
```

5. 装置のスパニングツリーを有効化します。

```
sw1(config)# spanning-tree global state enable
sw1(config)# end
sw1#
```

5.3.3.2 RPVST+：sw2 の設定例

図 5-23 RPVST+：sw2 の設定例



1. VLAN 10、VLAN 20、および VLAN 30 を作成します。

```
sw2# configure terminal
sw2(config)# vlan 10,20,30
sw2(config-vlan)# exit
sw2(config)#
```

2. ポート 1/0/47 およびポート 1/0/48 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 20、および VLAN 30］を割り当てます。

```
sw2(config)# interface port 1/0/47
sw2(config-if-port)# switchport mode trunk
sw2(config-if-port)# switchport trunk allowed vlan 10,20,30
sw2(config-if-port)# exit
sw2(config)# interface port 1/0/48
sw2(config-if-port)# switchport mode trunk
sw2(config-if-port)# switchport trunk allowed vlan 10,20,30
sw2(config-if-port)# exit
sw2(config)#
```

3. スパニングツリープロトコルを RPVST+ に設定します。

```
sw2(config)# spanning-tree mode rpvst+
sw2(config)#
```

4. VLAN 10、VLAN 20、および VLAN 30 をスパニングツリー VLAN として指定し、ブリッジ優先度を［16,384］に設定します。

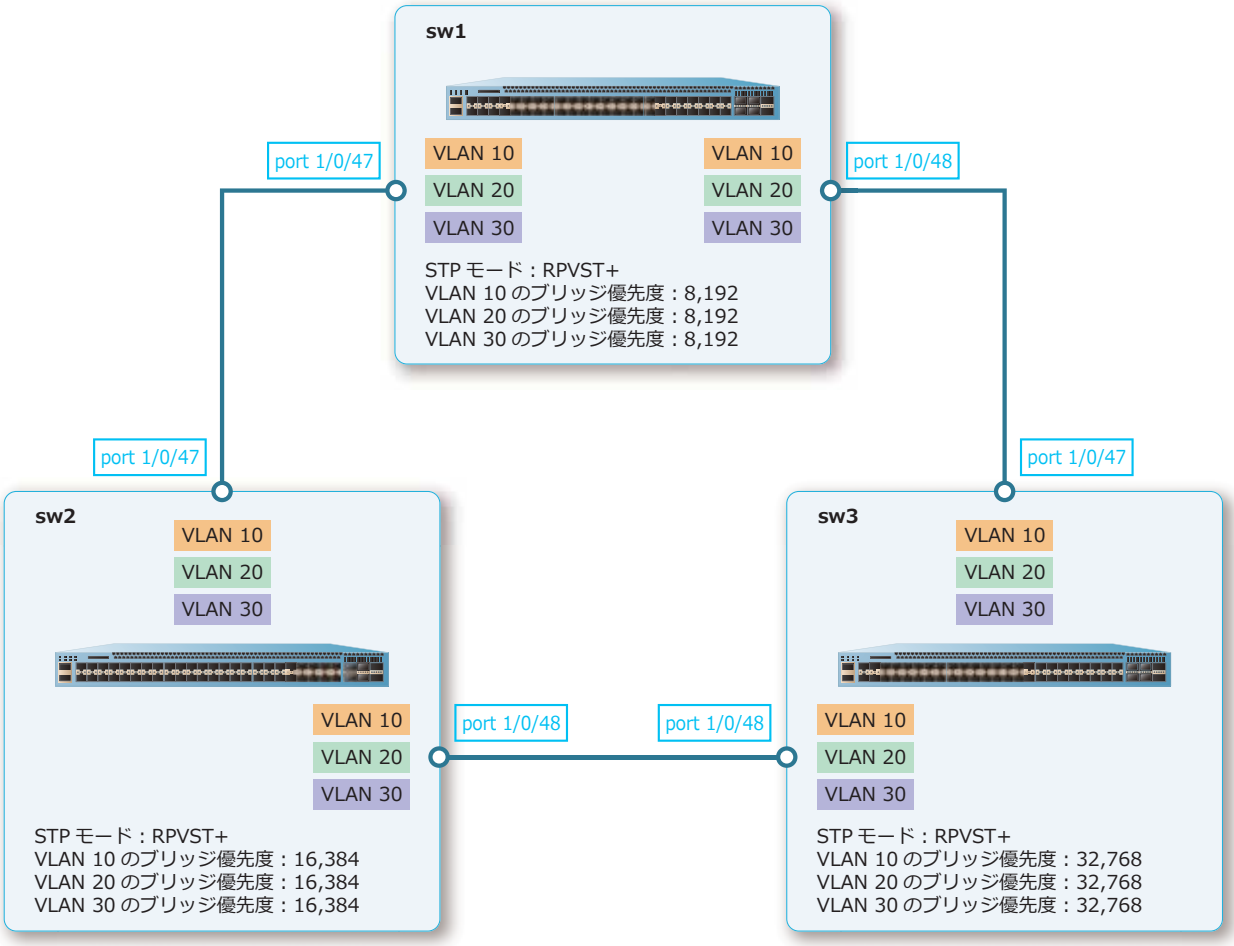
```
sw2(config)# spanning-tree vlan 10
sw2(config)# spanning-tree vlan 10 priority 16384
sw2(config)# spanning-tree vlan 20
sw2(config)# spanning-tree vlan 20 priority 16384
sw2(config)# spanning-tree vlan 30
sw2(config)# spanning-tree vlan 30 priority 16384
sw2(config)#
```

5. 装置のスパニングツリーを有効化します。

```
sw2(config)# spanning-tree global state enable
sw2(config)# end
sw2#
```

5.3.3.3 RPVST+：sw3 の設定例

図 5-24 RPVST+：sw3 の設定例



1. VLAN 10、VLAN 20、および VLAN 30 を作成します。

```
sw3# configure terminal
sw3(config)# vlan 10,20,30
sw3(config-vlan)# exit
sw3(config)#
```

2. ポート 1/0/47 およびポート 1/0/48 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 20、および VLAN 30］を割り当てます。

```
sw3(config)# interface port 1/0/47
sw3(config-if-port)# switchport mode trunk
sw3(config-if-port)# switchport trunk allowed vlan 10,20,30
sw3(config-if-port)# exit
sw3(config)# interface port 1/0/48
sw3(config-if-port)# switchport mode trunk
sw3(config-if-port)# switchport trunk allowed vlan 10,20,30
sw3(config-if-port)# exit
sw3(config)#
```

3. スパニングツリープロトコルを RPVST+ に設定します。

```
sw3(config)# spanning-tree mode rpvst+
sw3(config)#
```

4. VLAN 10、VLAN 20、および VLAN 30 をスパニングツリー VLAN として指定します。

```
sw3(config)# spanning-tree vlan 10
sw3(config)# spanning-tree vlan 20
sw3(config)# spanning-tree vlan 30
sw3(config)#
```

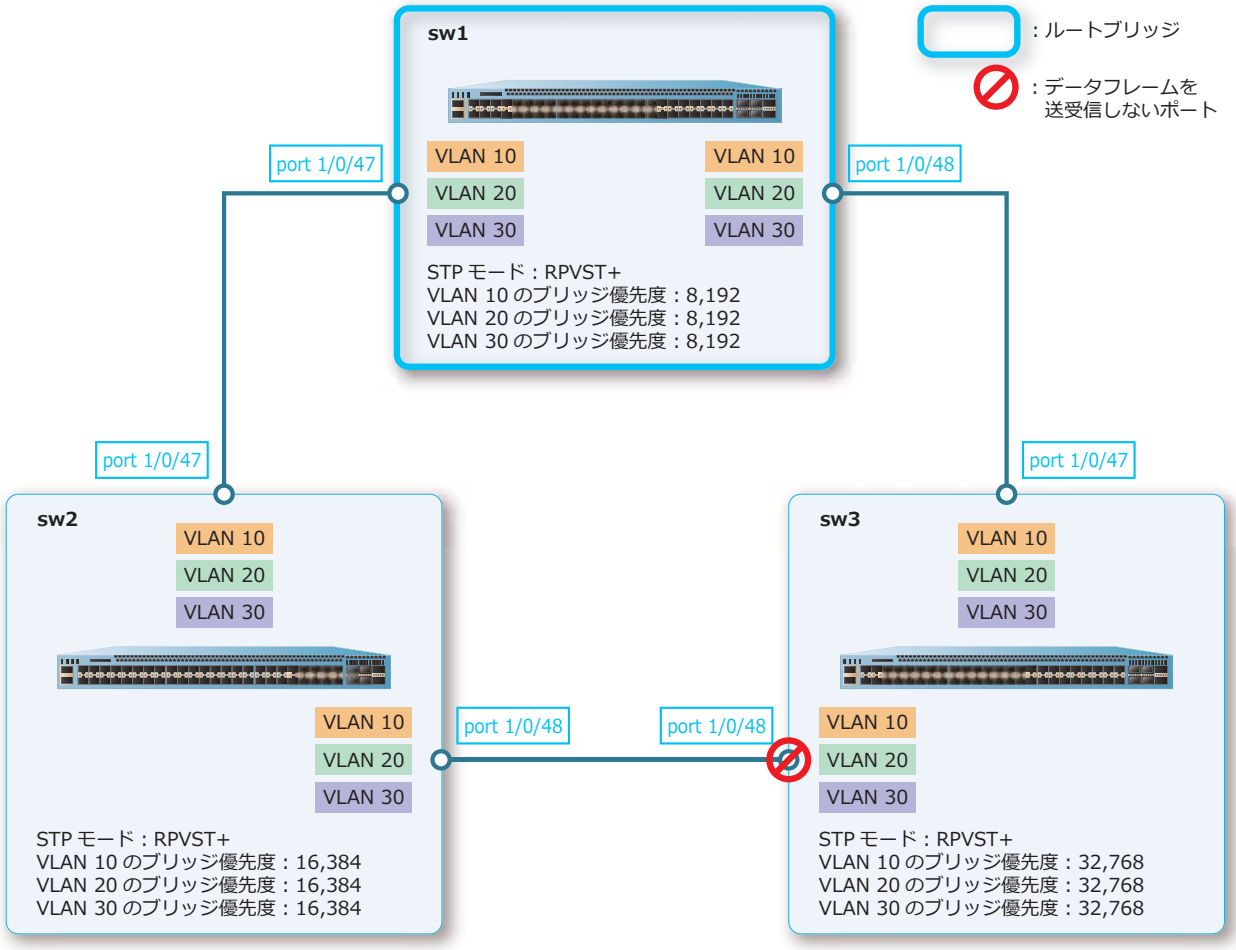
5. 装置のスパニングツリーを有効化します。

```
sw3(config)# spanning-tree global state enable
sw3(config)# end
sw3#
```

5.3.3.4 RPVST+ を使用した場合の設定結果例

RPVST+ では、VLAN ごとにルートブリッジや代替ポートが異なります。設定例のとおりに設定すると、ルートブリッジと代替ポートは以下のように選択されます。

図 5-25 RPVST+ を使用した場合の設定結果例



6. ループ検知

ループ検知の機能、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。

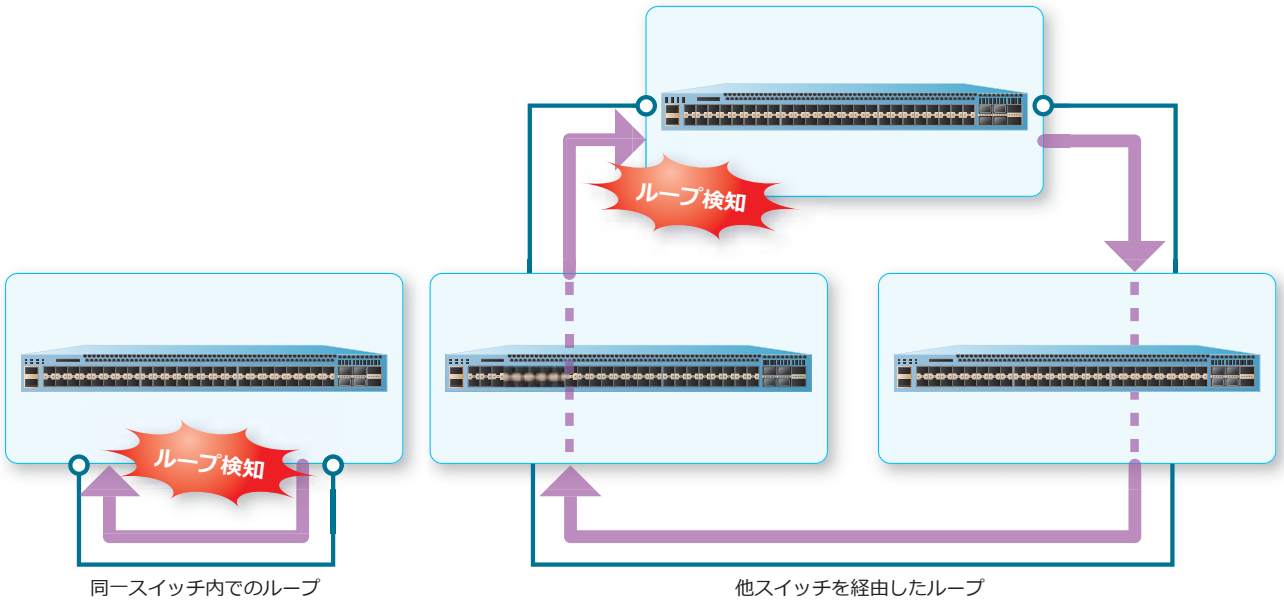
REF: コマンドの詳細については、『コマンドリファレンス』を参照してください。

6.1 ループ検知の機能説明

ループ検知を有効にすると、定期的に**ループ検知フレーム**を送信します。自装置が送信したループ検知フレームを受信した場合にループ障害が発生したと判断し、対象のポートまたは VLAN での通信を抑制して、ループ状態を解消します。さらに、ログや SNMP トラップでループ障害を検知したことを通知します。

CAUTION: ループ検知機能（loop-detection action notify-only 設定時を除く）は、同一インターフェースで STP/RSTP/MSTP/RPVST+ 機能、ERPS 機能、MMRP-Plus 機能、ポートリダンダント機能と併用できません。

図 6-1 ループ検知例

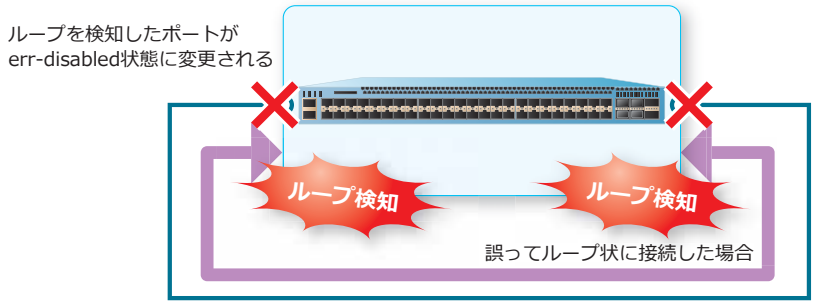


ループ検知の動作モードには、以下の 2 種類があります。

- **ポートベースモード**

  ポートベースモードでは、ポートをループ検知対象とします。

図 6-2 ポートベースモードでループを検知した場合

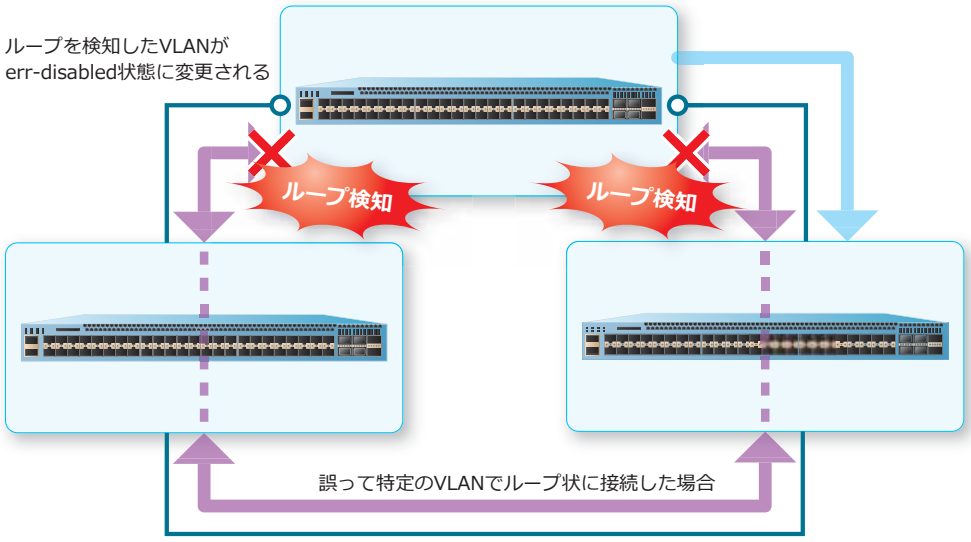


NOTE: ループ検知無効ポートで同一装置から送信されたループ検知フレームを受信した場合でも、ループが検知されます。その場合、ループ検知フレームを送信したポートが err-disabled 状態に変更されます。

- **VLAN ベースモード**

  VLAN ベースモードでは、ポートに割り当てられた VLAN のみをループ検知対象とします。

図 6-3 VLAN ベースモードでループを検知した場合



NOTE: ループ検知無効ポートで同一装置から送信されたループ検知フレームを受信した場合でも、ループが検知されます。その場合、ループ検知フレームを送信したポートの対象 VLAN が err-disabled 状態に変更されます。

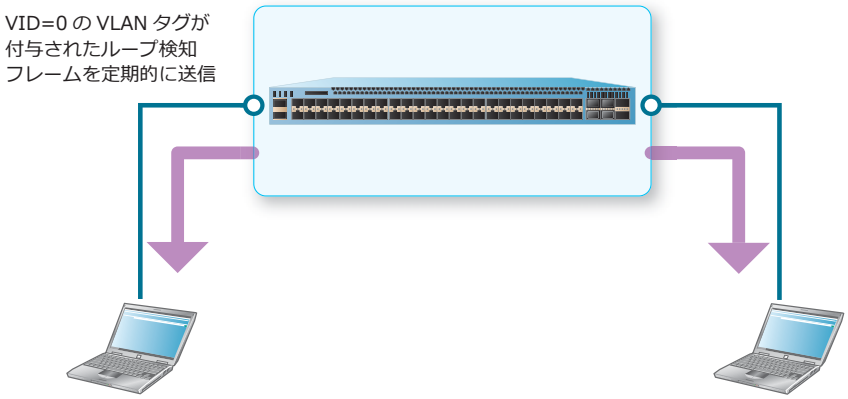
装置全体でループ検知機能を有効化するには、**`loop-detection global enable`** コマンドを使用します。インターフェースごとのループ検知機能を有効化するには、**`loop-detection enable`** コマンドを使用します。ループ検知の動作モードを設定するには、**`loop-detection mode`** コマンドを使用します。ループ検知フレームの送信間隔を設定するには、**`loop-detection interval`** コマンドを使用します。

NOTE: トランクポートで使用する場合は VLAN ベースモードで使用することを推奨します。ポートベースモードで使用する場合は、VID=0 のタグ付き形式のループ検知フレームが送信されることに注意してください。

6.1.1 ポートベースモードの動作

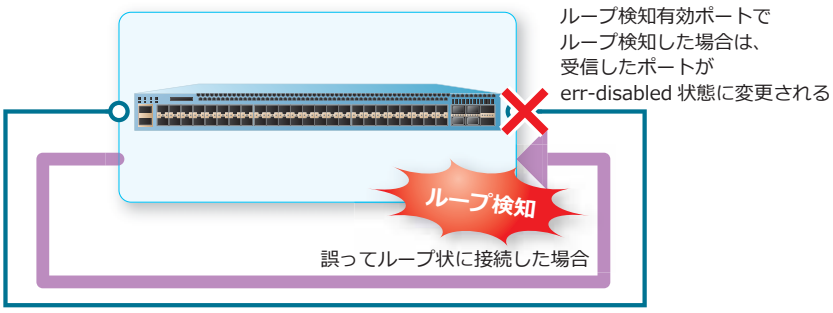
ポートベースモードでは、ループ検知を有効にしたポートから、VID=0 のタグ付き形式のループ検知フレームが定期的に送信されます。

図 6-4 ポートベースモードでのループ検知フレームの送信



誤ってループ状に接続した場合は、自装置が送信したループ検知フレームを受信することになります。ループ検知有効ポートで受信した場合は、その受信ポートが err-disabled 状態に変更されます。ループ検知無効ポートで受信した場合は、そのループ検知フレームを送信したポートが err-disabled 状態に変更されます。

図 6-5 ポートベースモードでループを検知した場合



NOTE: ポートチャネルでループ検知（ポートベースモード）を有効にしていてループを検知した場合は、そのポートチャネルのすべてのメンバーポートが err-disabled 状態に変更されます。

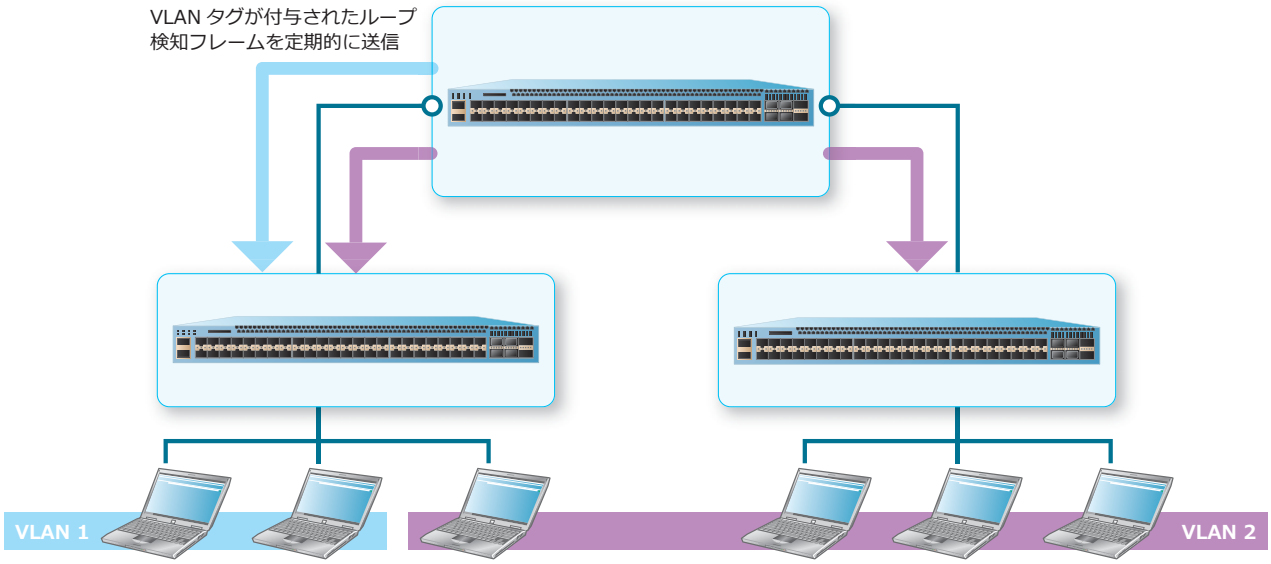
NOTE: ループ検知の動作モードがポートベースモードの場合、err-disabled 状態に変更されたポートのリンク状態は、**`show interfaces`** コマンドでは "link status is down (error disabled: Loop Detection)" と表示されます。また、**`show interfaces status`** コマンドの Status 項目では "err-disabled" と表示されます。

なお、ポートベースモードの場合は、対象ポートがトランクポートでも VID=0 のタグ付き形式のループ検知フレームを送信します。一般的には VID=0 のタグ付きフレームはプライオリティータグフレームとして扱われ、タグなしフレームを受信可能な設定のポートで受信できます。そのため、ポートベースモードのトランクポートで使用する場合は、そのポートの対向スイッチなどではタグなしフレームを受信して中継できるようにしてください。

6.1.2 VLAN ベースモードの動作

VLAN ベースモードでは、ループ検知を有効にしたポートから、ループ検知機能を有効にしている VLAN すべてに対して、VLAN タグが付与されたループ検知フレームが定期的に送信されます。ポートにタグなし VLAN が所属する場合は、VID=0 のタグ付き形式のループ検知フレームも送信されます。

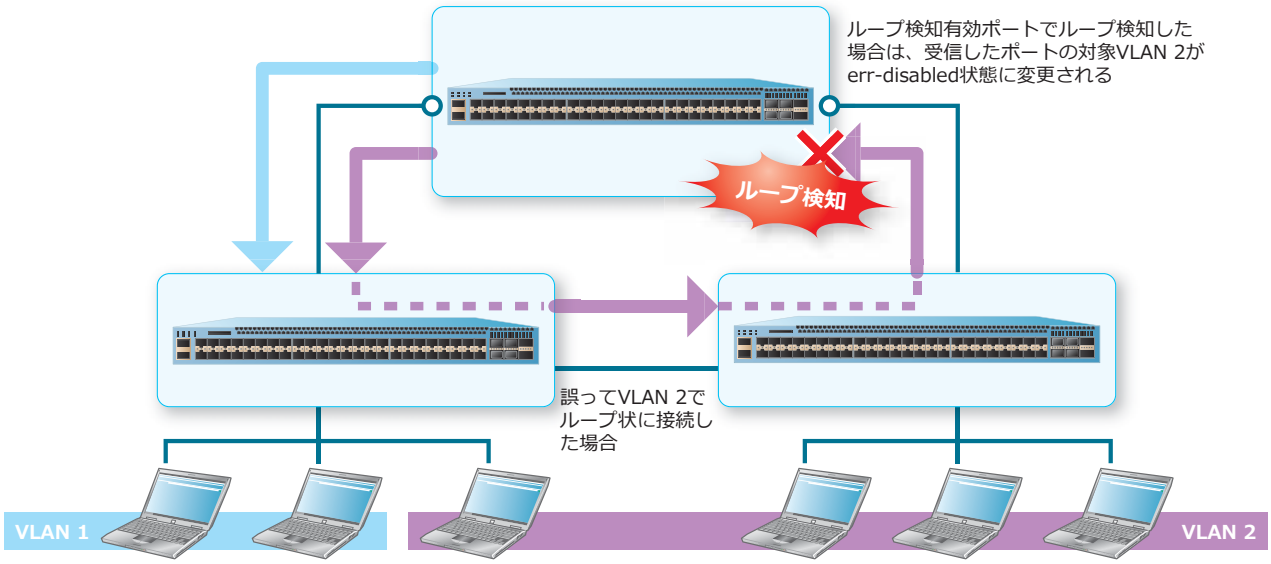
図 6-6 VLAN ベースモードでのループ検知フレームの送信



誤って特定の VLAN でループ状に接続した場合は、自装置が送信したループ検知フレームを対象 VLAN で受信することになります。ループ検知有効ポートで受信した場合は、その受信ポートの対象 VLAN が err-disabled 状態に変更されます。ループ検知無効ポートで受信した場合は、そのループ検知フレームを送信したポートの対象 VLAN が err-disabled 状態に変更されます。

下図の場合、ループ検知フレームを受信したポートの VLAN 2 は通信が抑制された状態（err-disabled 状態）に変更されますが、それ以外の VLAN では通信可能です。

図 6-7 VLAN ベースモードでループを検知した場合



NOTE: VLAN ベースモードに設定している場合、ループ検知フレームは 1 秒間に最大 80 個ずつ有効にした VLAN の数だけ送信されます。

NOTE: 装置全体でループ検知できる VLAN の最大数は 100 個です。最大数まで検知した状態では、新たに別の VLAN でループが発生しても検知できません。検知状態の VLAN 数が最大数より少なくなれば、新たに別の VLAN でも検知可能です。

NOTE: ポートチャネルでループ検知（VLAN ベースモード）を有効にしていてループを検知した場合は、そのポートチャネルのすべてのメンバーポートで対象 VLAN が err-disabled 状態に変更されます。

NOTE: ループ検知の動作モードが VLAN ベースモードの場合、err-disabled 状態に変更された VLAN は **`show loop-detection`** コマンドで確認します。なお、ポートベースモードの場合とは異なり、**`show interfaces`** コマンドや **`show interfaces status`** コマンドの表示は変わりません。

なお、VLAN ベースモードでは送信するループ検知フレーム内部の情報フィールドに対象 VLAN の情報も含まれており、ループ検知フレームを受信した際にその情報も参照しています。そのため、たとえばある VLAN のアクセスポートから送信したループ検知フレームを別の VLAN のアクセスポートで受信しても、ループ検知フレームの VLAN 情報と受信ポートの VLAN が異なるため、VLAN ベースモードではループ検知できないことに注意してください。

6.1.3 ループ検知フレームのフレーム形式

ループ検知フレームのフレーム形式は以下のとおりです。

表 6-1 ループ検知フレームのフレーム形式

フィールド	内容	バイト数
DA	CF-00-00-00-00-00	6 バイト
SA	装置の MAC アドレス	6 バイト
TPID・優先度・CFI・VID	VLAN 情報（IEEE 802.1Q タグ） TPID：0x8100 優先度：7 or 6 CFI：0 VID：ループ検知フレームの VLAN ID	4 バイト
イーサタイプ	0x9000	2 バイト
データ部	送信ポート番号、VLAN ID、装置 MAC アドレスなど	-

NOTE: NP7000 の 1.11.03 以降、NP5000 の 1.12.01 以降、NP4000 の 1.03.04 以降、NP3000 の 1.11.03 以降、NP2100 の 1.13.01 以降、NP2500 の 1.13.01 以降では、ループ検知フレームの VLAN タグの優先度は 6 に変更されています。それより前のバージョンや NP2000 では、優先度は 7 です。

6.1.4 インターフェースの復旧

err-disabled 状態に変更されたポート／ VLAN を復旧するには、以下の 2 つの方法があります。

自動復旧設定

errdisable recovery cause loop-detection コマンドを使用して、ループ検知機能によって err-disabled 状態に変更されたポート／ VLAN の自動復旧を有効にできます。自動復旧設定を有効にすると、err-disabled 状態に変更されたポート／ VLAN は、指定した時間の経過後に自動的に復旧します。以下に自動復旧の設定例を示します。

```
(config)# errdisable recovery cause loop-detection interval 300
```

> ***NOTE:*** 指定した時間が経過して自動的に復旧しても、ループが解消されていない場合は再度ループを検知することに注意してください。

コマンドによる手動復旧手順

err-disabled 状態に変更されたポートに対して **shutdown** コマンドを実行した後、**no shutdown** コマンドを実行することで、手動でポート／ VLAN を復旧できます。VLAN ベースモードで使用していてこの復旧方法を実施する際は、対象ポートがリンクダウン／リンクアップするため、対象ポートに所属するすべての VLAN に影響があることに注意してください。以下にコマンド実行例を示します。

```
(config)# interface port 1/0/1
(config-if-port)# shutdown
(config-if-port)# no shutdown
```

6.1.5 ループ検知フレームの Untag 形式変更オプション

以下のループ検知フレームは、デフォルトでは VID=0 のタグ付きフレーム形式で送信しますが、ループ検知フレームの Untag 形式変更オプションを有効にすると、タグなしフレーム形式に変更できます。

- ポートベースモードの場合に送信するループ検知フレーム
- VLAN ベースモードで、タグなし形式のフレームを送信する設定のポート（アクセスポート、トランクポートのネイティブ VLAN など）から送信するループ検知フレーム

> ***NOTE:*** ループ検知フレームの Untag 形式変更オプションは、NP7000 の 1.10.01 以降、NP5000 の 1.09.01 以降、NP3000 の 1.12.01 以降、NP2100 の 1.14.01 以降、NP2500 の 1.12.01 以降でサポートしています。

ループ検知フレームの Untag 形式変更オプションを有効にするには、**loop-detection frame-type untagged** コマンドを使用します。

6.1.6 notify-only オプション

notify-only オプションは、ループ検知による閉塞動作（ポート／ VLAN を err-disabled 状態に変更する動作）は行わずに、ログ／ SNMP トラップの出力だけを行う場合に設定します。同一インターフェースで STP/RSTP/MSTP/RPVST+ 機能、ERPS 機能、MMRP-Plus 機能、ポートリダンダント機能と併用する場合は、notify-only オプションを設定してください。

notify-only オプションを設定したインターフェースでループを検知すると、**loop-detection interval** コマンドで設定した間隔（デフォルト設定は 10 秒）でログ／ SNMP トラップが出力されます。

notify-only オプションを設定するには、**loop-detection action notify-only** コマンドを使用します。

6.1.7 no-check-src オプション

no-check-src オプションを設定すると、ループ検知フレームの送信元 MAC アドレスが自身の装置 MAC アドレスではなく他の装置の MAC アドレスの場合でも、ループを検知します。no-check-src オプションを設定することにより、ループは発生しないが、装置を跨いで好ましくない接続ミスをしてしまった場合などでも、検知することができるようになります。

no-check-src オプションを設定するには、**`loop-detection no-check-src`** コマンドを使用します。

> ***NOTE:*** no-check-src オプションを設定したインターフェースでは、ApresiaLight シリーズ（GM/FM/GS）が送信するループ検知フレームを受信した場合にも、ループを検知します。なお、ApresiaLightGC シリーズが送信するループ検知フレームの場合は、受信してもループ検知はしません。

6.2 ループ検知の状態確認

ループ検知の状態を表示して確認する方法を説明します。

6.2.1 ループ検知の設定と状態の表示

show loop-detection コマンドでループ検知の設定と状態を確認できます。

> ***NOTE:*** Frame Type 項目は、**loop-detection frame-type untagged** コマンドをサポートしている機種でのみ表示されます。

表示例を以下に示します。

```
# show loop-detection

 Loop Detection       : Enabled ...(1)
 Detection Mode       : port-based ...(2)
 Enabled VLAN         : all VLANs ...(3)
 Interval             : 10 seconds ...(4)
 Frame Type           : Priority Tag ...(5)
 (6)              (7)        (8)          (9)       (10)                  (11)
 Interface        noChkSrc   Action       State     Result                Time Left
 ---------------  --------   -----------  --------  ------------------    ----------
 Port1/0/1        Disabled   shutdown     Enabled   Normal                -
 Port1/0/2        Disabled   notify-only  Enabled   Normal                -
 Port1/0/3        Enabled    shutdown     Enabled   Normal                -
 Port1/0/4        Disabled   shutdown     Disabled  Normal                -
 Port1/0/5        Disabled   shutdown     Disabled  Normal                -
 Port1/0/6        Disabled   shutdown     Disabled  Normal                -
～～省略～～
```

各項目の説明は、以下のとおりです。

表 6-2 show loop-detection コマンドの表示項目

項番	説明
(1)	ループ検知機能のグローバル設定の有効 (Enabled) ／無効 (Disabled) を表示します。
(2)	ループ検知の動作モードを表示します。 • port-based：ポートベースモード • vlan-based：VLAN ベースモード
(3)	VLAN ベースモードでループ検知が有効な VLAN を表示します。**loop-detection vlan** コマンドがデフォルト設定で、すべての VLAN でループ検知が有効な場合は all VLANs と表示されます。
(4)	ループ検知フレームの送信間隔を表示します。
(5)	ループ検知フレームの形式を表示します。 • Priority Tag：デフォルト設定時 • Untagged：**loop-detection frame-type untagged** コマンド設定時
(6)	ポート番号またはポートチャネル番号を表示します。
(7)	no-check-src オプションの有効 (Enabled) ／無効 (Disabled) を表示します。

項番	説明
(8)	ループを検知した場合の動作を表示します。 • shutdown：ループを検知したインターフェース、または VLAN を閉塞する • notify-only：ループを検知しても閉塞は行わず、ログ／ SNMP トラップの通知のみ行う
(9)	インターフェースごとのループ検知機能の有効 (Enabled) ／無効 (Disabled) を表示します。
(10)	ループ検知状態を表示します。 • Normal：ループを検知していない状態 • Loop：ループを検知した状態（ポートベースモード） • Loop on VLAN XX：VLAN XX でループを検知した状態（VLAN ベースモード）
(11)	ループを検知した場合の動作が shutdown（デフォルト設定）の場合は、err-disabled 状態に変更されたポート／ VLAN が自動復旧されるまでの残り時間（秒）を表示します。 ループを検知した場合の動作が notify-only の場合は、ループ検知表示が自動復旧されるまでの残り時間（秒）を表示します。 • XX：自動復旧されるまでの残り時間（秒） • infinite：自動復旧設定が無効で、ループを検知した状態 • -：ループを検知していない状態

6.2.2 ループ検知の状態の表示

`show loop-detection status` コマンドでループ検知の状態を確認できます。

> ***NOTE:*** 本コマンドは、NP7000 の 1.10.01 以降、NP5000 の 1.09.01 以降、NP3000 の 1.12.01 以降、NP2100 の 1.14.01 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 loop-detection status
(1)               (2)    (3)       (4)          (5)          (6)
Interface         VLAN   Result    Time Left    Receive      Last Detection Time
---------------   ----   -------   ----------   ----------   -------------------
Port1/0/1         10     Loop      infinite               -   2022-09-02 09:47:12
Port1/0/2         20     Loop      infinite             232   2022-09-02 09:52:24
                  30     Loop      infinite             242   2022-09-02 09:53:24
Port-channel1     All    Normal    -                      0   -
```

各項目の説明は、以下のとおりです。

表 6-3 `show loop-detection status` コマンドの表示項目

項番	説明
(1)	ループ検知機能が有効なポート番号またはポートチャネル番号を表示します。
(2)	VLAN ベースモードで、ループを検知した VLAN を表示します。 • XX：ループを検知した VLAN ID • All：ループを検知した VLAN が存在しない状態
(3)	ループ検知状態を表示します。 • Normal：ループを検知していない状態 • Loop：ループを検知した状態

項番	説明
(4)	ループを検知した場合の動作が shutdown（デフォルト設定）の場合は、err-disabled 状態に変更されたポート／ VLAN が自動復旧されるまでの残り時間（秒）を表示します。 ループを検知した場合の動作が notify-only の場合は、ループ検知表示が自動復旧されるまでの残り時間（秒）を表示します。 • XX：自動復旧されるまでの残り時間（秒） • infinite：自動復旧設定が無効で、ループを検知した状態 • -：ループを検知していない状態
(5)	ログ／ SNMP トラップの通知のみを行う設定（loop-detection action notify-only）の場合に、CPU で受信したループ検知フレームの累積受信数を表示します。「ループを検知した日時」が更新された場合、累積受信数のカウントも一度クリアされます。
(6)	最も直近にループを検知した日時を表示します。ログ／ SNMP トラップの通知のみを行う設定（loop-detection action notify-only）では、定期的（loop-detection interval）にループ検知状態が継続しているかが確認されます。継続している場合は、「ループを検知した日時」が更新されます。

6.2.3 自動復旧設定の表示

show errdisable recovery コマンドで、自動復旧設定を確認できます。

表示例を以下に示します。

```
# show errdisable recovery
(1)                                  (2)           (3)
ErrDisable Cause                     State         Interval
-----------------------------------  ------------  -------------
Storm Control                        enabled       300 seconds
Loop Detection                       enabled       300 seconds
ULD                                  disabled      300 seconds

Interfaces that will be recovered at the next timeout:
(4)          (1)                                   (5)
Interface    Errdisable Cause                      Time left(sec)
---------    -----------------------------------   --------------
Port1/0/1    Loop Detection                        229
```

各項目の説明は、以下のとおりです。

表 6-4 show errdisable recovery コマンドの表示項目

項番	説明
(1)	検知の要因となった機能を表示します。 • Loop Detection：ループ検知機能 • Storm Control：ストームコントロール機能 • ULD：単方向リンク検出機能
(2)	自動復旧設定の有効 (enabled) ／無効 (disabled) を表示します。
(3)	ポートが自動的に復旧されるまでの時間設定を表示します。

項番	説明
(4)	err-disabled 状態に変更されたポートを表示します。 対象がループ検知機能で VLAN ベースモードの場合は、ポートおよびフレームの送受信が停止された VLAN を表示します。 対象がループ検知機能でループを検知した場合の動作が notify-only の場合は、ループ検知状態のポートを表示します。
(5)	err-disabled 状態に変更されたポートが自動復旧されるまでの残り時間を表示します。 対象がループ検知機能でループを検知した場合の動作が notify-only の場合は、ループ検知状態のポートが自動復旧されるまでの残り時間を表示します。

6.2.4 ブザーの状態の表示

show alarm buzzer コマンドで、ブザーの設定と状態を確認できます。

CAUTION: NP7000、NP5000、および NP4000 では、ブザーを使用できません。

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 6-5 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。

項番	説明
(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。
(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

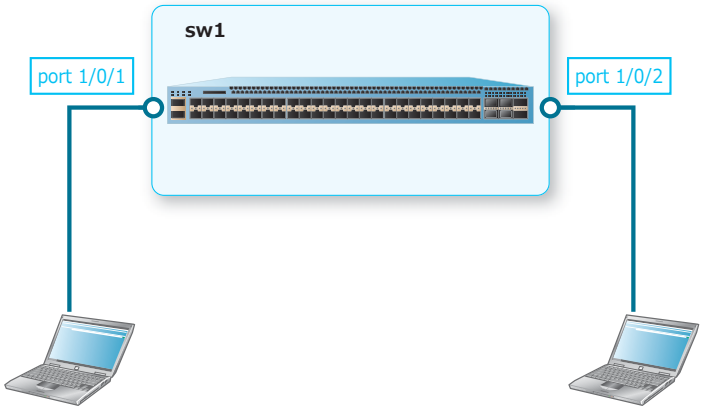
6.3 ループ検知の構成例と設定例

ループ検知を利用する場合の構成例と設定例を示します。

6.3.1 ポートベースモードのループ検知を使用する場合

装置の 2 つのポートに対して、ポートベースモードのループ検知機能を有効にする場合の構成例と設定例を示します。

図 6-8 ポートベースモードのループ検知を使用する場合の構成例



1. 装置のループ検知機能を有効にします。

```
sw1# configure terminal
sw1(config)# loop-detection global enable
sw1(config)#
```

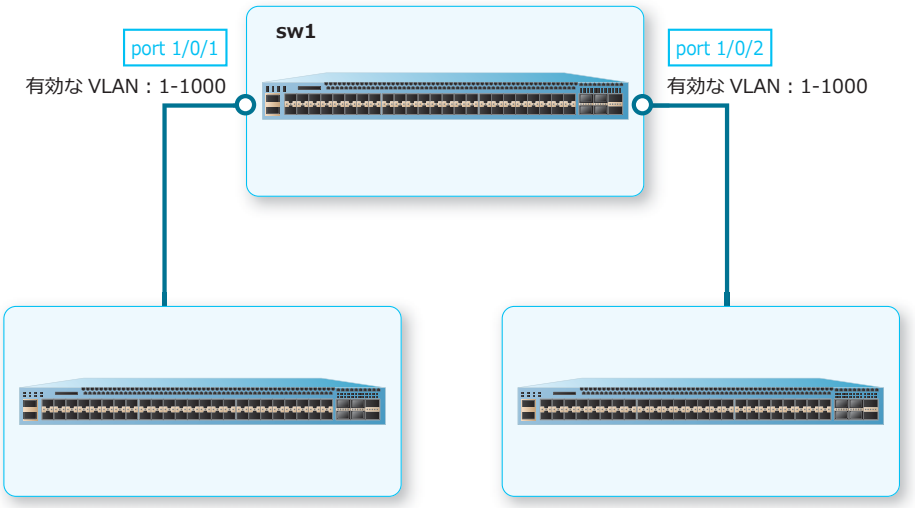
2. ポート 1/0/1 およびポート 1/0/2 で、ループ検知機能を有効にします。

```
sw1(config)# interface range port 1/0/1,1/0/2
sw1(config-if-port-range)# loop-detection enable
sw1(config-if-port-range)# end
sw1#
```

6.3.2 VLAN ベースモードのループ検知を使用する場合

装置を 3 台設置し、2 つのポートを VLAN 1 から VLAN 1000 のタグ付きメンバーとして設定し、VLAN ベースモードのループ検知機能を有効にする場合の構成例と設定例を示します。

図 6-9 VLAN ベースモードのループ検知を使用する場合の構成例



1. VLAN 2 から VLAN 1000 を作成します。

```
sw1# configure terminal
sw1(config)# vlan 2-1000
sw1(config-vlan)# exit
sw1(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 1 から VLAN 1000］を割り当てます。

```
sw1(config)# interface range port 1/0/1,1/0/2
sw1(config-if-port-range)# switchport mode trunk
sw1(config-if-port-range)# switchport trunk allowed vlan 1-1000
sw1(config-if-port-range)# exit
sw1(config)#
```

3. 装置のループ検知機能を有効にします。

```
sw1(config)# loop-detection global enable
sw1(config)#
```

4. ループ検知機能の動作モードを VLAN ベースモードに設定し、［VLAN 1 から VLAN 1000］のループ検知を有効にします。

```
sw1(config)# loop-detection mode vlan-based
sw1(config)# loop-detection vlan 1-1000
sw1(config)#
```

5. ポート 1/0/1 およびポート 1/0/2 で、ループ検知機能を有効にします。

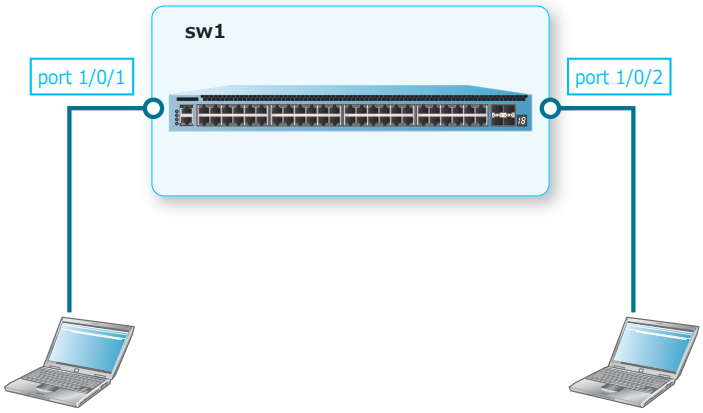
```
sw1(config)# interface range port 1/0/1,1/0/2
sw1(config-if-port-range)# loop-detection enable
sw1(config-if-port-range)# end
sw1#
```

6.3.3 ループを検知した際にブザーで通知する場合

装置の 2 つのポートに対して、ポートベースモードのループ検知機能を有効にし、ループを検知した際にブザーで通知する場合の構成例と設定例を示します。

CAUTION: NP7000、NP5000、および NP4000 では、ブザーを使用できません。

図 6-10 ループを検知した際にブザーで通知する場合の構成例



1. 装置のループ検知機能を有効にします。

```
sw1# configure terminal
sw1(config)# loop-detection global enable
sw1(config)#
```

2. ポート 1/0/1 およびポート 1/0/2 で、ループ検知機能を有効にします。

```
sw1(config)# interface range port 1/0/1,1/0/2
sw1(config-if-port-range)# loop-detection enable
sw1(config-if-port-range)# exit
sw1(config)#
```

3. ブザーのグローバル設定を有効にします。

```
sw1(config)# alarm buzzer global enable
sw1(config)#
```

4. ポート 1/0/1 およびポート 1/0/2 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。

cause パラメーターを指定しない場合は、ループ検知機能による通知のみ有効になります。

```
sw1(config)# interface range port 1/0/1,1/0/2
sw1(config-if-port-range)# alarm buzzer state enable
sw1(config-if-port-range)# end
sw1#
```

7. ストームコントロール

ストームコントロールの機能、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 ストームコントロールの機能説明

ストームコントロールは、設定したしきい値を超えるトラフィックを受信すると**ストーム**が発生したと判断し、帯域制限や対象ポートのシャットダウン（err-disabled 状態に変更）によってストームの影響を低減するための機能です。

図 7-1 ストームコントロールの動作例（1）

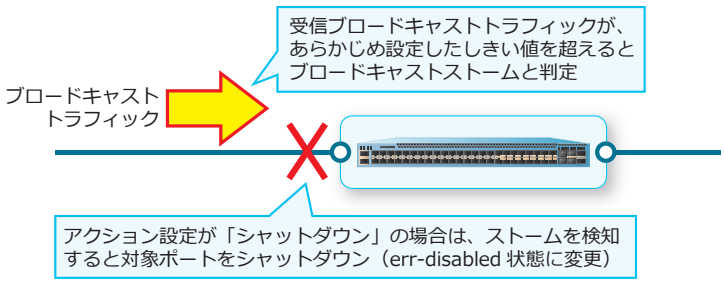
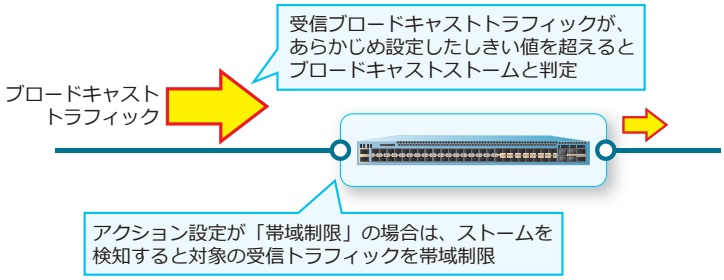


図 7-2 ストームコントロールの動作例（2）



NOTE: ストームコントロール機能で 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: Storm Control)" 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。

7.1.1 ストームコントロールの対象トラフィック

装置でストームを検知できるトラフィックは、以下の 3 種類です。

- ブロードキャスト
- マルチキャスト
- Unknown ユニキャスト

7.1.2 ストームコントロールの設定

ストームコントロールを利用するために、ポートごとに以下の情報を設定します。（）内は使用するコマンドです。

- **トラフィックの種類ごとの上限値（`storm-control`）**

  ストームと判定されるトラフィックの流量を設定します。上限値を上回ると、ストームと判定されます。トラフィックの流量の単位は、パケット数（pps）、Kbps、ポートの総帯域幅に対する受信トラフィックの割合（パーセンテージ）のいずれか 1 つを選択できます。

- **トラフィックの種類ごとの下限値（`storm-control`）**

  ストームが終了したと判定されるトラフィックの流量を設定します。下限値を下回ると、ストームが終了したと判定されます。

  NOTE: 下限値の設定を省略した場合は、上限値の 80% の値が設定されます。

- **アクション（`storm-control action`）**

  ストームと判定された場合の処理を設定します。

  CAUTION: しきい値を Kbps またはパーセンテージで指定した場合は、アクションに shutdown は指定できません。

  CAUTION: しきい値を Kbps またはパーセンテージで指定した場合は、ストームの検知／解消を示すログは出力されません。

  CAUTION: マルチキャストのストーム検知では、アクションが drop 設定の場合、宛先 IPv4 アドレスが予約 IPv4 マルチキャストアドレス（224.0.0.0 ～ 224.0.0.255）のパケットを、**`show storm-control`** コマンドやログ出力では multicast パラメーターの対象として扱いますが、帯域制限動作だけは broadcast パラメーターの対象として扱われる仕様制限があります。

  CAUTION: ユニキャストのストーム検知では、アクションが drop または none 設定の場合、ストームの検知／解消を示すログは出力されません。

  CAUTION: ユニキャストのストーム検知では、アクションが shutdown 設定の場合は、Unknown ユニキャストだけでなく宛先学習済みユニキャストも対象になる仕様制限があります。ユニキャスト（Unknown ユニキャストと宛先学習済みユニキャスト）が上限値を超えると、シャットダウン（err-disabled 状態に変更）されます。

また、ストームコントロールを利用するために、装置ごとに以下の情報を設定できます。（）内は使用するコマンドです。

- **検知ポーリング間隔（`storm-control polling interval`）**

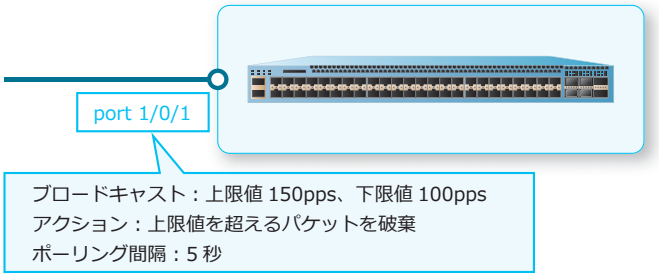
  ストームの発生を判定する時間間隔を設定します。

  NOTE: ストーム検知のチェックは、検知ポーリング間隔で設定した時間ごとに判定されます。そのため、たとえば検知ポーリング間隔を 600 秒に設定した場合は、実際にストームが発生したタイミングとストーム検知／解消タイミングは、最大 600 秒ずれる可能性があります。

- **シャットダウンするまでのリトライ回数（`storm-control polling retries`）**

  ストームと判定された際にポートをシャットダウン（err-disabled 状態に変更）する設定にした場合は、ストームと判定された回数がリトライ回数を超えたときにポートをシャットダウン（err-disabled 状態に変更）します。

図 7-3 ストームコントロールの設定例



この例では、ポート 1/0/1 にブロードキャストパケットが 1 秒間に 150 パケットを超えて届くと、ストームと判定されます。ストームと判定されてから 5 秒間は、ポート 1/0/1 に届くブロードキャストパケットのうち、上限値（1 秒間に 150 パケット）を超えるパケットが破棄されます。

次に、ポート 1/0/1 に届くブロードキャストパケットが減少し、1 秒間に 100 パケットを下回ると、ストームが終了したと判定されます。それ以降は、ポート 1/0/1 に届くすべてのブロードキャストパケットが受信されます。

7.1.3 インターフェースの復旧

上限値を超えたときにポートをシャットダウン（err-disabled 状態に変更）する設定の場合、err-disabled 状態に変更されたポートを復旧するには、以下の 2 つの方法があります。

自動復旧設定

`errdisable recovery cause storm-control` コマンドを使用して、ストームコントロール機能によって err-disabled 状態に変更されたポートの自動復旧を有効にできます。自動復旧設定を有効にすると、err-disabled 状態に変更されたポートは、指定した時間の経過後に自動的に復旧します。以下に自動復旧の設定例を示します。

```
(config)# errdisable recovery cause storm-control interval 300
```

コマンドによる手動復旧手順

err-disabled 状態に変更されたポートに対して **`shutdown`** コマンドを実行した後、**`no shutdown`** コマンドを実行することで、手動でポートを復旧できます。以下にコマンド実行例を示します。

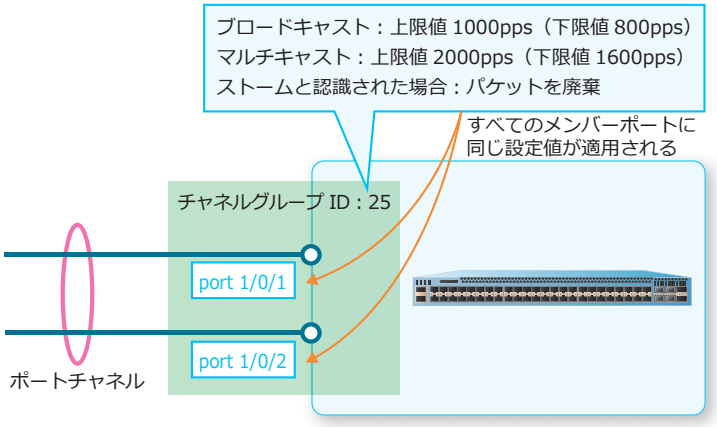
```
(config)# interface port 1/0/1
(config-if-port)# shutdown
(config-if-port)# no shutdown
```

7.1.4 ポートチャネルでのストームコントロール

ポートチャネルで設定した内容（上限値、下限値、アクション）は、そのポートチャネルのすべてのメンバーポートに同じ内容で適用されます。なお、ストームコントロールの動作はメンバーポートごとに動作します。

NOTE: ポートチャネルでのストームコントロールは、NP7000 の 1.03.03 以降、NP5000 の 1.03.03 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 1.10.01 以降でサポートしています。

図 7-4 ポートチャネルでのストームコントロールの設定例



7.2 ストームコントロールの状態確認

ストームコントロールの状態を表示して確認する方法を説明します。

7.2.1 ストームコントロールの状態の表示

show storm-control コマンドで、ストームコントロールの状態を確認できます。

CAUTION: しきい値を kbps またはパーセンテージで設定していて、かつ受信パケットのサイズが 64 バイト以外の場合は、Current 項目と State 項目を正常に表示できない制限があります。

CAUTION: ユニキャストのストームコントロールでは、Unknown ユニキャストと宛先学習済みユニキャストの両方が Current 項目でカウントされます。アクションが drop 設定の場合、State 項目は Current 項目が上限値を超えると Dropped と表示されるため、実際には Unknown ユニキャストが上限値に達しておらず破棄されていなくても、State 項目が Dropped と表示されることがあります。

ブロードキャストストームに対するストームコントロールの状態の表示

show storm-control broadcast コマンドで、ブロードキャストに対するストームコントロールの状態を確認できます。

ポート 1/0/1 からポート 1/0/6 を指定した場合の表示例を以下に示します。

```
# show storm-control interface range port 1/0/1-1/0/6 broadcast
 (1)          (2)       (3)                    (4)           (5)
 Interface    Action    Threshold              Current       State
 ------------------------------------------------------------------------
 Port1/0/1     Drop      500/300 pps            200 pps       Forwarding
 Port1/0/2     Drop      80/64 %                20 %          Forwarding
 Port1/0/3     Drop      80/64 %                70 %          Dropped
 Port1/0/4     Shutdown  500/300 pps            200 pps       Forwarding
 Port1/0/5     None      60000/50000 kbps       2000 kbps     Forwarding
 Port1/0/6     None       -                      -            Inactive

Total Entries: 6
```

各項目の説明は、以下のとおりです。

表 7-1 show storm-control broadcast 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)	アクションを表示します。 • Shutdown：ポートをシャットダウン（err-disabled 状態に変更）する • Drop：上限値を超えるパケットを破棄する • None：処理しない
(3)	しきい値の上限値／下限値、および単位を表示します。単位は以下を意味します。 • pps：packets per second、1 秒あたりの受信パケット数 • kbps：kilobit per second、1 秒あたりの受信キロビット数 • %：ポートの総帯域幅に対する、受信トラフィックのパーセンテージ
(4)	対象トラフィックの現在の受信量を表示します。

項番	説明
(5)	アクションの状況を表示します。 • Forwarding：転送（受信量に問題がないためストームコントロールが実行されていない） • Dropped：上限値を超えるパケットを破棄 • Link Down：物理的なリンクダウン • Error Disabled：ストームコントロールによるシャットダウン（err-disabled 状態） • Inactive：ストームコントロール無効

すべてのストームコントロールの状態の表示

ポート 1/0/1 からポート 1/0/2 のすべてのストームコントロールの状態を確認する場合の表示例を以下に示します。

```
# show storm-control interface range port 1/0/1-2
 (1)                                  (2)
 Polling Interval  : 5 sec            Shutdown Retries    : 3 times
 (3)        (4)       (5)       (6)                  (7)          (8)
 Interface  Storm     Action    Threshold            Current      State
 ------------------------------------------------------------------------------
 Port1/0/1  Broadcast Drop      80/64 %              50%          Forwarding
 Port1/0/1  Multicast Drop      80/64 %              50%          Forwarding
 Port1/0/1  Unicast   Drop      80/64 %              50%          Forwarding
 Port1/0/2  Broadcast Shutdown 500/300 pps          -            Error Disabled
 Port1/0/2  Multicast Shutdown 500/300 pps          -            Error Disabled
 Port1/0/2  Unicast   Shutdown 500/300 pps          -            Error Disabled

 Total Entries: 6
```

各項目の説明は、以下のとおりです。

表 7-2 `show storm-control` コマンドの表示項目

項番	説明
(1)	ポーリング間隔を表示します。
(2)	シャットダウン（err-disabled 状態に変更）するまでのリトライ回数を表示します。
(3)	ポート番号を表示します。
(4)	監視するトラフィックの種類を表示します。
(5)	アクションを表示します。 • Shutdown：ポートをシャットダウン（err-disabled 状態に変更）する • Drop：上限値を超えるパケットを破棄する • None：処理しない
(6)	しきい値の上限値／下限値、および単位を表示します。単位は以下を意味します。 • pps：packets per second、1 秒あたりの受信パケット数 • kbps：kilobit per second、1 秒あたりの受信キロビット数 • %：ポートの総帯域幅に対する、受信トラフィックのパーセンテージ
(7)	対象トラフィックの現在の受信量を表示します。

項番	説明
(8)	アクションの状況を表示します。 • Forwarding：転送（受信量に問題がないためストームコントロールが実行されていない） • Dropped：上限値を超えるパケットを破棄 • Link Down：物理的なリンクダウン • Error Disabled：ストームコントロールによるシャットダウン（err-disabled 状態） • Inactive：ストームコントロール無効

ポートチャネルでのストームコントロールの状態の表示

ポートチャネル 25（メンバーポートはポート 1/0/1 とポート 1/0/2）でのストームコントロールの状態を確認する場合の表示例を以下に示します。

> ***NOTE:*** ポートチャネルでのストームコントロールは、NP7000 の 1.03.03 以降、NP5000 の 1.03.03 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 1.10.01 以降でサポートしています。

```
# show storm-control interface port-channel 25
 (1)                                  (2)
 Polling Interval  : 5 sec            Shutdown Retries    : 3 times
 (3)         (4)        (5)       (6)                    (7)           (8)
 Interface   Storm      Action    Threshold              Current       State
 ------------------------------------------------------------------------------
 Group-25    Broadcast  Drop      1000/800 pps           -             -
 Group-25    Multicast  Drop      2000/1600 pps          -             -
 Group-25    Unicast    Drop      -                      -             -
 ------------------------------------------------------------------------------
 Port1/0/1   Broadcast  Drop      1000/800 pps           0 pps         Forwarding
 Port1/0/1   Multicast  Drop      2000/1600 pps          0 pps         Forwarding
 Port1/0/1   Unicast    Drop      -                      -             Inactive
 Port1/0/2   Broadcast  Drop      1000/800 pps           0 pps         Forwarding
 Port1/0/2   Multicast  Drop      2000/1600 pps          0 pps         Forwarding
 Port1/0/2   Unicast    Drop      -                      -             Inactive

 Total Entries: 6
```

各項目の説明は、以下のとおりです。

表 7-3 ポートチャネル指定の `show storm-control` コマンドの表示項目

項番	説明
(1)	ポーリング間隔を表示します。
(2)	シャットダウン（err-disabled 状態に変更）するまでのリトライ回数を表示します。
(3)	上段には指定したポートチャネル番号を、下段にはそのポートチャネルのメンバーポートを表示します。
(4)	監視するトラフィックの種類を表示します。
(5)	アクションを表示します。 • Shutdown：ポートをシャットダウン（err-disabled 状態に変更）する • Drop：上限値を超えるパケットを破棄する • None：処理しない

項番	説明
(6)	しきい値の上限値／下限値、および単位を表示します。単位は以下を意味します。 • pps：packets per second、1 秒あたりの受信パケット数 • kbps：kilobit per second、1 秒あたりの受信キロビット数 • %：ポートの総帯域幅に対する、受信トラフィックのパーセンテージ
(7)	対象トラフィックの現在の受信量を表示します。
(8)	アクションの状況を表示します。 • Forwarding：転送（受信量に問題がないためストームコントロールが実行されていない） • Dropped：上限値を超えるパケットを破棄 • Link Down：物理的なリンクダウン • Error Disabled：ストームコントロールによるシャットダウン（err-disabled 状態） • Inactive：ストームコントロール無効

7.2.2 自動復旧設定の表示

show errdisable recovery コマンドで、自動復旧設定を確認できます。

表示例を以下に示します。

```
# show errdisable recovery
(1)                                  (2)           (3)
ErrDisable Cause                     State         Interval
-----------------------------------  ------------  -------------
Storm Control                        enabled       120 seconds
Loop Detection                       disabled      300 seconds
ULD                                  disabled      300 seconds

Interfaces that will be recovered at the next timeout:
(4)          (1)                                   (5)
Interface    Errdisable Cause                      Time left(sec)
---------    -----------------------------------   --------------
Port1/0/2    Storm Control                         104
```

各項目の説明は、以下のとおりです。

表 7-4 show errdisable recovery コマンドの表示項目

項番	説明
(1)	検知の要因となった機能を表示します。 • Loop Detection：ループ検知機能 • Storm Control：ストームコントロール機能 • ULD：単方向リンク検出機能
(2)	自動復旧設定の有効 (enabled) ／無効 (disabled) を表示します。
(3)	ポートが自動的に復旧されるまでの時間設定を表示します。
(4)	err-disabled 状態に変更されたポートを表示します。
(5)	err-disabled 状態に変更されたポートが自動復旧されるまでの残り時間を表示します。

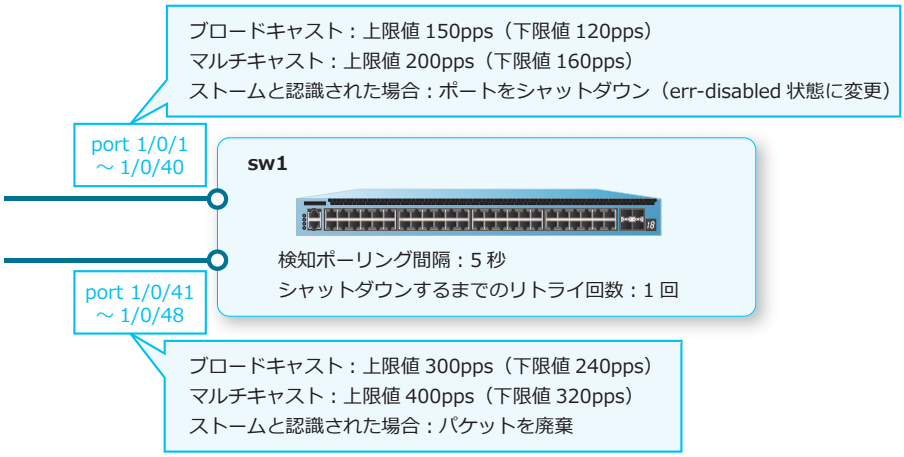
7.3 ストームコントロールの構成例と設定例

ストームコントロールを利用する場合の構成例と設定例を示します。

7.3.1 ストームコントロールの設定例

ポート 1/0/1 からポート 1/0/40、およびポート 1/0/41 からポート 1/0/48 に対して、異なるストームコントロールを設定する場合の構成例と設定例を示します。

図 7-5 ストームコントロールの構成例



NOTE: 下限値の設定を省略した場合は、上限値の 80% の値が設定されます。

1. ポート 1/0/1 からポート 1/0/40 のストームコントロールを以下のように設定します。

ストームコントロール：ブロードキャスト［上限値 150pps］、マルチキャスト［上限値 200pps］、ストームと認識された場合［ポートをシャットダウン（err-disabled 状態に変更）］

```
sw1# configure terminal
sw1(config)# interface range port 1/0/1-40
sw1(config-if-port-range)# storm-control broadcast level pps 150
sw1(config-if-port-range)# storm-control multicast level pps 200
sw1(config-if-port-range)# storm-control action shutdown
sw1(config-if-port-range)# exit
sw1(config)#
```

2. ポート 1/0/41 からポート 1/0/48 のストームコントロールを以下のように設定します。

ストームコントロール：ブロードキャスト［上限値 300pps］、マルチキャスト［上限値 400pps］、ストームと認識された場合［上限値を超えるパケットを破棄］

```
sw1(config)# interface range port 1/0/41-48
sw1(config-if-port-range)# storm-control broadcast level pps 300
sw1(config-if-port-range)# storm-control multicast level pps 400
sw1(config-if-port-range)# storm-control action drop
sw1(config-if-port-range)# exit
sw1(config)#
```

3. 検知ポーリング間隔を［5 秒］に、シャットダウンするまでのリトライ回数を［1 回］に設定します。

```
sw1(config)# storm-control polling interval 5
sw1(config)# storm-control polling retries 1
sw1(config)#
```

4. ストームを検知してシャットダウン（err-disabled 状態に変更）されたポートを自動復旧する機能を、復旧間隔を［5 秒］に設定して有効化します。

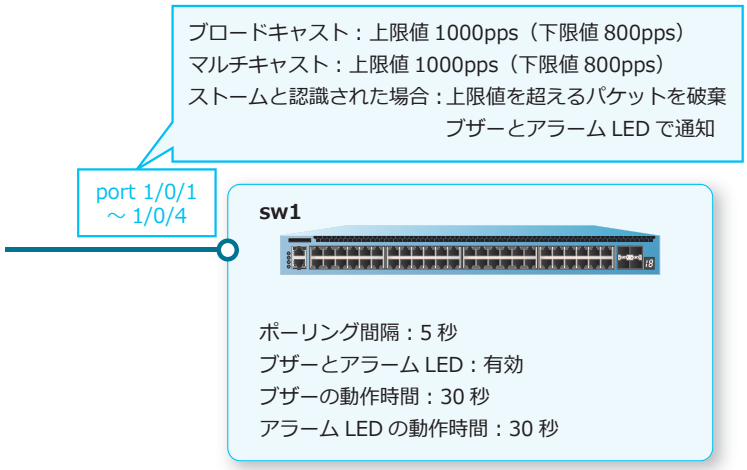
```
sw1(config)# errdisable recovery cause storm-control interval 5
sw1(config)# end
sw1#
```

7.3.2 ストームを検知した際にブザーとアラーム LED で通知する場合

ポート 1/0/1 からポート 1/0/4 に対してストームコントロールを設定し、ストームを検知した際にブザーとアラーム LED で通知する場合の構成例と設定例を示します。

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。NP4000 では、ブザーによる障害通知を使用できません。

図 7-6 ストームを検知した際にブザーとアラーム LED で通知する場合の構成例



NOTE: 下限値の設定を省略した場合は、上限値の 80% の値が設定されます。

1. ポート 1/0/1 からポート 1/0/4 のストームコントロールを以下のように設定します。

ストームコントロール：ブロードキャスト［上限値 1000pps］、マルチキャスト［上限値 1000pps］、ストームと認識された場合［上限値を超えるパケットを破棄］

```
sw1# configure terminal
sw1(config)# interface range port 1/0/1-4
sw1(config-if-port-range)# storm-control broadcast level pps 1000
sw1(config-if-port-range)# storm-control multicast level pps 1000
sw1(config-if-port-range)# exit
sw1(config)#
```

2. ポーリング間隔を［5 秒］に設定します。

```
sw1(config)# storm-control polling interval 5
```

3. ブザーとアラーム LED のグローバル設定を有効にします。また、それぞれの動作時間を 30 秒に設定します。

```
sw1(config)# alarm buzzer global enable
sw1(config)# alarm warn-led global enable
sw1(config)# alarm buzzer duration 30
sw1(config)# alarm warn-led duration 30
```

4. ポート 1/0/1 からポート 1/0/4 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 1/0/1-4
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#
```

8. アクセスリスト

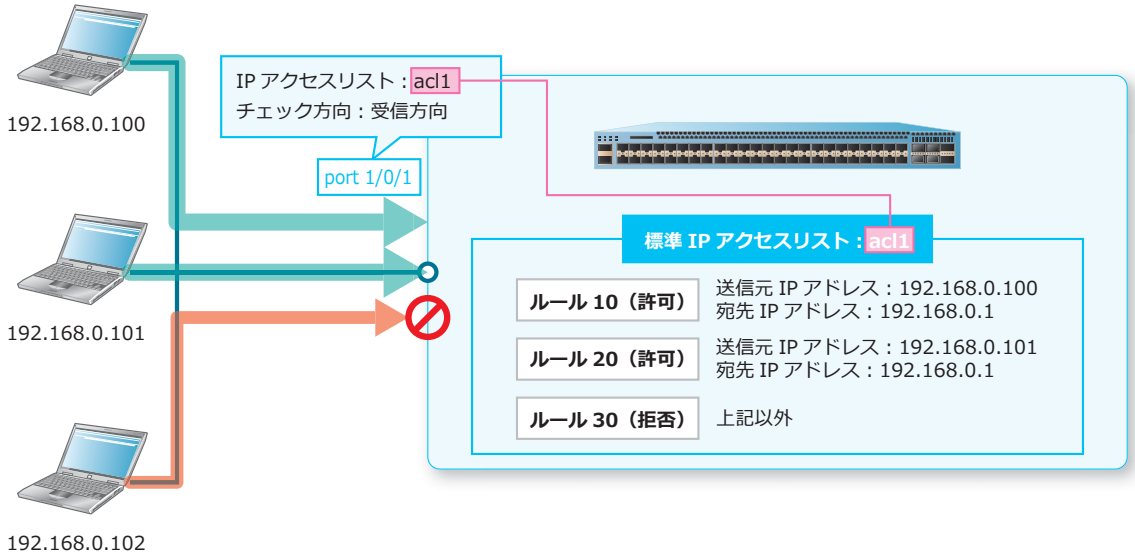
アクセスリストの機能、状態の確認方法、および構成例と設定例について説明します。

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。

8.1 アクセスリストの機能説明

アクセスリストは、あらかじめ設定した抽出条件に一致した通信のみを許可または拒否するための機能です。送信元 IP アドレスや宛先 IP アドレスなどを抽出条件として設定できます。

図 8-1 アクセスリストの概要



8.1.1 アクセスリストの作成およびインターフェースへの適用

アクセスリストを適用したインターフェースでは、抽出条件に一致したトラフィックに対してアクション（permit または deny）が実行されます。それぞれのアクションは以下のように動作します。

- permit：抽出条件に一致したトラフィックを許可して中継
- deny：抽出条件に一致したトラフィックを拒否して破棄

NOTE: 本章で説明する「パケットフィルター機能として使用するアクセスリスト」の場合、どのルールにも一致しないパケットは処理対象外になり、そのまま中継されます。アクセスリスト設定を「IP アドレスを指定するフォーマット」として利用している他機能のコマンドではそれぞれ動作が異なるため、それらの動作に関しては、『コマンドリファレンス』でそれぞれのコマンドを参照してください。

装置では、以下のアクセスリストを作成できます。各アクセスリストは、チェック対象になるパケット種別や設定できる抽出条件が異なります。

CAUTION: インターフェースに適用したアクセスリストを異なるアクセスリストで上書きした場合、一時的に当該ルールが無効となります。そのため、アクセスリストの設定変更時には、インターフェースへの適用が完了するまでの間、当該ルールが適用されません。

NOTE: 同一名称または同一番号のアクセスリストを、複数の送信ポートに適用することはできません。

- **標準 IP アクセスリスト**

  標準 IP アクセスリストは IPv4 パケットのみがチェック対象になります。設定できる抽出条件は以下のとおりです。

  - 送信元 IP アドレス
  - 宛先 IP アドレス
  - クラス ID（NP4000、NP2100、NP2000、および NP2500）

  標準 IP アクセスリストは、**ip access-list** コマンドで作成し、**ip access-group** コマンドでインターフェースに適用します。

- **拡張 IP アクセスリスト**

  拡張 IP アクセスリストは IPv4 パケットのみがチェック対象になります。設定できる抽出条件は以下のとおりです。

  - IP プロトコル番号
  - 送信元 IP アドレス
  - 送信元 L4 ポート番号（TCP または UDP プロトコル指定時）
  - 宛先 IP アドレス
  - 宛先 L4 ポート番号（TCP または UDP プロトコル指定時）
  - TCP フラグ（TCP プロトコル指定時）
  - ICMP メッセージ（ICMP プロトコル指定時）
  - フラグメント（任意の IP プロトコル番号指定時）
  - 優先度（precedence、ToS、DSCP）
  - クラス ID（NP4000、NP2100、NP2000、および NP2500）

  拡張 IP アクセスリストは、**ip access-list extended** コマンドで作成し、**ip access-group** コマンドでインターフェースに適用します。

- **標準 IPv6 アクセスリスト**

  標準 IPv6 アクセスリストは IPv6 パケットのみがチェック対象になります。設定できる抽出条件は以下のとおりです。

  - 送信元 IPv6 アドレス
  - 宛先 IPv6 アドレス
  - クラス ID

  標準 IPv6 アクセスリストは、**ipv6 access-list** コマンドで作成し、**ipv6 access-group** コマンドでインターフェースに適用します。

- **拡張 IPv6 アクセスリスト**

  拡張 IPv6 アクセスリストは IPv6 パケットのみがチェック対象になります。設定できる抽出条件は以下のとおりです。

  - IP プロトコル番号
  - 送信元 IPv6 アドレス
  - 送信元 L4 ポート番号（TCP または UDP プロトコル指定時）
  - 宛先 IPv6 アドレス
  - 宛先 L4 ポート番号（TCP または UDP プロトコル指定時）
  - TCP フラグ（TCP プロトコル指定時）
  - ICMP メッセージ（ICMP プロトコル指定時）
  - フラグメント（任意の IP プロトコル番号指定時）
  - 優先度（DSCP）、またはトラフィッククラス

- フローラベル
- ホップリミット
- クラス ID

拡張 IPv6 アクセスリストは、**ipv6 access-list extended** コマンドで作成し、**ipv6 access-group** コマンドでインターフェースに適用します。

NOTE: トラフィッククラスおよびホップリミットは、NP2100 の 1.09.05/1.10.01 以降、NP2000 の 1.09.05 以降、NP2500 の 1.10.01 以降でサポートしています。

• 拡張エキスパートアクセスリスト

拡張エキスパートアクセスリストは IPv4 パケットのみがチェック対象になります。設定できる抽出条件は以下のとおりです。

- IP プロトコル番号
- 送信元 IP アドレス
- 送信元 L4 ポート番号（TCP または UDP プロトコル指定時）
- 送信元 MAC アドレス
- 宛先 IP アドレス
- 宛先 L4 ポート番号（TCP または UDP プロトコル指定時）
- 宛先 MAC アドレス
- TCP フラグ（TCP プロトコル指定時）
- ICMP メッセージ（ICMP プロトコル指定時）
- フラグメント（任意の IP プロトコル番号指定時）
- 優先度（CoS、precedence、ToS、DSCP）
- VLAN
- クラス ID

拡張エキスパートアクセスリストは、**expert access-list extended** コマンドで作成し、**expert access-group** コマンドでインターフェースに適用します。

• 拡張 MAC アクセスリスト

拡張 MAC アクセスリストは非 IP パケットのみがチェック対象になります。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 パケットもチェック対象になります。設定できる抽出条件は以下のとおりです。

- 送信元 MAC アドレス
- 宛先 MAC アドレス
- イーサタイプ
- 優先度（CoS）
- VLAN
- クラス ID

拡張 MAC アクセスリストは、**mac access-list extended** コマンドで作成し、**mac access-group** コマンドでインターフェースに適用します。また、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するには、**mac access-list enable ip-packets** コマンドを使用します。

NOTE: 拡張 MAC アクセスリストの IP パケット対象化機能は、NP7000 の 1.07.01 以降、NP5000 の 1.07.01 以降、NP4000 の 1.03.01 以降、NP3000 の 1.11.03 以降、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。

• ARP アクセスリスト

ARP アクセスリストは ARP パケットのみがチェック対象になります。設定できる抽出条件は以下のとおりです。

• ARP ヘッダーの Sender IP address フィールド

• 送信元 MAC アドレス

ARP アクセスリストは、**`arp access-list`** コマンドで作成し、**`arp access-group`** コマンドでインターフェースに適用します。

NOTE: ARP アクセスリストは Ingress グループでのみ使用できます。

NOTE: ARP アクセスリストは、NP2100 の 1.09.05/1.10.01 以降、NP2000 の 1.09.05 以降、NP2500 の 1.10.01 以降でサポートしています。

各アクセスリストのチェック対象になるパケット種別を以下に示します。

表 8-1 各アクセスリストでチェック対象になるパケット種別

アクセスリストの種類	チェック対象になるパケット種別
標準 IP アクセスリスト	IPv4 パケット
拡張 IP アクセスリスト	IPv4 パケット
標準 IPv6 アクセスリスト	IPv6 パケット
拡張 IPv6 アクセスリスト	IPv6 パケット
拡張エキスパートアクセスリスト	IPv4 パケット
拡張 MAC アクセスリスト	非 IP パケット *1
ARP アクセスリスト	ARP パケット

*1：デフォルト設定では非 IP パケットのみがチェック対象になります。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。

各アクセスリストで設定できる抽出条件を以下に示します。

表 8-2 各アクセスリストで設定できる抽出条件

	標準 IP アクセスリスト	拡張 IP アクセスリスト	標準 IPv6 アクセスリスト	拡張 IPv6 アクセスリスト	拡張エキスパートアクセスリスト	拡張 MAC アクセスリスト
プロトコル	-	○	-	○	○	-
送信元 IP アドレス	○	○	-	-	○	-
送信元 IPv6 アドレス	-	-	○	○	-	-
送信元 MAC アドレス	-	-	-	-	○	○
送信元 L4 ポート番号	-	○	-	○	○	-
宛先 IP アドレス	○	○	-	-	○	-

	標準 IP アクセスリスト	拡張 IP アクセスリスト	標準 IPv6 アクセスリスト	拡張 IPv6 アクセスリスト	拡張エキスパートアクセスリスト	拡張 MAC アクセスリスト
宛先 IPv6 アドレス	-	-	○	○	-	-
宛先 MAC アドレス	-	-	-	-	○	○
宛先 L4 ポート番号	-	○	-	○	○	-
TCP フラグ	-	○	-	○	○	-
ICMP メッセージ	-	○	-	○	○	-
フラグメント	-	○	-	○	○	-
優先度（precedence）	-	○	-	-	○	-
優先度（ToS）	-	○	-	-	○	-
優先度（DSCP）	-	○	-	○	○	-
トラフィッククラス *2	-	-	-	○	-	-
フローラベル	-	-	-	○	-	-
ホップリミット *2	-	-	-	○	-	-
優先度（CoS）	-	-	-	-	○	○
VLAN	-	-	-	-	○	○
イーサタイプ	-	-	-	-	-	○
クラス ID*3	○ *1	○ *1	○	○	○	○

*1：NP4000、NP2100、NP2000、および NP2500 で使用できます。

*2：NP2100 の 1.09.05/1.10.01 以降、NP2000 の 1.09.05 以降、NP2500 の 1.10.01 以降でサポートしています。

*3：受信方向のアクセスリストでのみ使用できます。

ワイルドカードビットによる指定

送信元 IP アドレスや宛先 IP アドレスなど、一部の条件ではワイルドカードビットを使用できます。

（例 1）送信元 IP アドレスを 192.168.1.0、ワイルドカードビットを 0.0.0.255 に設定すると、192.168.1.XXX（XXX の部分は任意）という条件を設定できます。

（例 2）宛先 MAC アドレスを 00:AA:BB:CC:00:00、ワイルドカードビットを 00:00:00:00:FF:FF に設定すると、00:AA:BB:CC:XX:XX（XX:XX の部分は任意）という条件を設定できます。

NOTE: 拡張 MAC アクセスリストのイーサタイプ条件のマスク指定は、ワイルドカードビットとは指定方法が異なります。イーサタイプを 0x5500、マスクを 0xff00 に設定すると、0x55XX（XX の部分は任意）という条件を設定できます。

シーケンス番号

アクセスリスト内のルールの評価順序は、シーケンス番号で設定します。シーケンス番号が小さいルールから順に評価されます。シーケンス番号は、**permit** コマンドまたは **deny** コマンドでルールを登録する際に設定できます。

シーケンス番号を指定せずにルールを作成した場合、シーケンス番号は自動的に割り当てられます。シーケンス番号が自動的に割り当てられる場合は、開始値（デフォルト設定では 10）から増分値（デフォルト設定では 10）でインクリメントした番号のうち、まだ使用されていない最も小さい番号が割り当てられます。開始値と増分値を変更し、設定済みルールのシーケンス番号を一括変更するには、**access-list resequence** コマンドを使用します。

備考情報

アクセスリストには、アクセスリストの用途などを備考情報として登録できます。備考情報は、**list-remark** コマンドで登録できます。

8.1.2 CPU アクセスリスト

CPU アクセスリストは、適用したインターフェースで抽出条件に一致した受信トラフィックのうち、CPU 宛てに中継されるトラフィックに対してアクション（no-action または cpu-deny）が実行されます。それぞれのアクションは以下のように動作します。

- no-action：CPU 宛てに中継されるトラフィックに対して何もしないアクション
- cpu-deny：CPU 宛て中継を拒否するアクション

NOTE: CPU アクセスリストは、NP7000 の 1.10.02 以降、NP5000 の 1.10.01 以降でサポートしています。

装置では、以下の CPU アクセスリストを作成できます。各 CPU アクセスリストは、チェック対象となるパケット種別や、設定できる抽出条件が異なります。

CAUTION: インターフェースに適用した CPU アクセスリストを異なる CPU アクセスリストで上書きした場合、一時的に当該ルールが無効となります。そのため、CPU アクセスリストの設定変更時には、インターフェースへの適用が完了するまでの間、当該ルールが適用されません。

• 標準 IP CPU アクセスリスト

標準 IP CPU アクセスリストは、IPv4 パケットのみがチェック対象になります。また、設定できる抽出条件は以下のとおりです。

- 送信元 IP アドレス
- 宛先 IP アドレス

標準 IP CPU アクセスリストは、**ip-cpu access-list** コマンドで作成し、**ip-cpu access-group** コマンドでインターフェースに適用します。

• 拡張 IP CPU アクセスリスト

拡張 IP CPU アクセスリストは、IPv4 パケットのみがチェック対象になります。また、設定できる抽出条件は以下のとおりです。

- IP プロトコル番号
- 送信元 IP アドレス
- 送信元 L4 ポート番号（TCP または UDP プロトコル指定時）
- 宛先 IP アドレス

- 宛先 L4 ポート番号（TCP または UDP プロトコル指定時）
- TCP フラグ（TCP プロトコル指定時）
- ICMP メッセージ（ICMP プロトコル指定時）
- フラグメント（任意の IP プロトコル番号指定時）
- 優先度（precedence、ToS、DSCP）

拡張 IP CPU アクセスリストは、**ip-cpu access-list extended** コマンドで作成し、**ip-cpu access-group** コマンドでインターフェースに適用します。

• 標準 IPv6 CPU アクセスリスト

標準 IPv6 CPU アクセスリストは、IPv6 パケットのみがチェック対象になります。また、設定できる抽出条件は以下のとおりです。

- 送信元 IPv6 アドレス
- 宛先 IPv6 アドレス
- クラス ID

標準 IPv6 CPU アクセスリストは、**ipv6-cpu access-list** コマンドで作成し、**ipv6-cpu access-group** コマンドでインターフェースに適用します。

• 拡張 IPv6 CPU アクセスリスト

拡張 IPv6 CPU アクセスリストは、IPv6 パケットのみがチェック対象になります。また、設定できる抽出条件は以下のとおりです。

- IP プロトコル番号
- 送信元 IPv6 アドレス
- 送信元 L4 ポート番号（TCP または UDP プロトコル指定時）
- 宛先 IPv6 アドレス
- 宛先 L4 ポート番号（TCP または UDP プロトコル指定時）
- TCP フラグ（TCP プロトコル指定時）
- ICMP メッセージ（ICMP プロトコル指定時）
- フラグメント（任意の IP プロトコル番号指定時）
- 優先度（DSCP）
- フローラベル
- クラス ID

拡張 IPv6 CPU アクセスリストは、**ipv6-cpu access-list extended** コマンドで作成し、**ipv6-cpu access-group** コマンドでインターフェースに適用します。

• 拡張エキスパート CPU アクセスリスト

拡張エキスパート CPU アクセスリストは、IPv4 パケットのみがチェック対象になります。また、設定できる抽出条件は以下のとおりです。

- IP プロトコル番号
- 送信元 IP アドレス
- 送信元 L4 ポート番号（TCP または UDP プロトコル指定時）
- 送信元 MAC アドレス
- 宛先 IP アドレス
- 宛先 L4 ポート番号（TCP または UDP プロトコル指定時）
- 宛先 MAC アドレス
- TCP フラグ（TCP プロトコル指定時）
- ICMP メッセージ（ICMP プロトコル指定時）
- フラグメント（任意の IP プロトコル番号指定時）

- 優先度（CoS、precedence、ToS、DSCP）
- VLAN
- クラス ID

拡張エキスパート CPU アクセスリストは、**expert-cpu access-list extended** コマンドで作成し、**expert-cpu access-group** コマンドでインターフェースに適用します。

- **拡張 MAC CPU アクセスリスト**

  拡張 MAC CPU アクセスリストは、非 IP パケットのみがチェック対象になります。また、設定できる抽出条件は以下のとおりです。

  - 送信元 MAC アドレス
  - 宛先 MAC アドレス
  - イーサタイプ
  - 優先度（CoS）
  - VLAN
  - クラス ID

  拡張 MAC CPU アクセスリストは、**mac-cpu access-list extended** コマンドで作成し、**mac-cpu access-group** コマンドでインターフェースに適用します。

8.1.3 アクセスリストのリソース

アクセスリストで許可ルールまたは拒否ルールを設定すると、**リソース**と呼ばれる領域を使用します。アクセスリストを設定する際は、リソースの仕様を考慮する必要があります。

8.1.3.1 グループとリソース（NP7000）

NP7000 には、Ingress グループと Egress グループが用意されています。Ingress グループと Egress グループの使用例は下図のとおりです。

図 8-2 Ingress グループの使用例

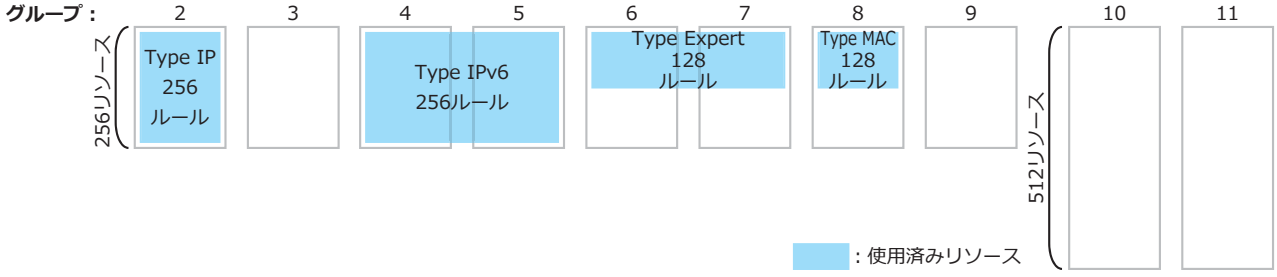
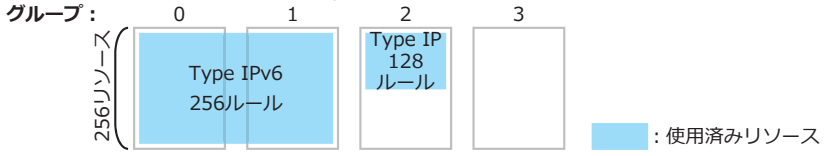


図 8-3 Egress グループの使用例



使用可能なリソース数

NP7000 のアクセスリストのリソース数を下表に示します。グループごとに使用できるリソース数が異なります。

表 8-3 NP7000 のアクセスリストのリソース

	Ingress	Egress
グループ数	10（グループ 2 から 11）	4（グループ 0 から 3）
グループごとに使用できるリソース数	グループ 2 から 9：256 リソース グループ 10 から 11：512 リソース	256 リソース

NOTE: Ingress グループのグループ 0 から 1 は使用できません。

アクセスリストの Type と使用するグループ数

アクセスリストの種類によって、アクセスリストの Type が決定されます。また、アクセスリストの Type により、1 ルールごとに使用するグループ数が異なります。

表 8-4 NP7000 のアクセスリストの Type と使用するグループ数

アクセスリストの種類	アクセスリストの Type	1 ルールごとに使用するグループ数（Ingress）	1 ルールごとに使用するグループ数（Egress）
標準 IP アクセスリスト 拡張 IP アクセスリスト	IP	1 グループ	1 グループ
標準 IPv6 アクセスリスト 拡張 IPv6 アクセスリスト	IPv6	2 グループ *1	2 グループ *2
拡張エキスパートアクセスリスト	Expert	2 グループ *1	2 グループ *2
拡張 MAC アクセスリスト	MAC	1 グループ	1 グループ
標準 IP CPU アクセスリスト 拡張 IP CPU アクセスリスト	IP-CPU	1 グループ	-
標準 IPv6 CPU アクセスリスト 拡張 IPv6 CPU アクセスリスト	IPv6-CPU	2 グループ *1	-
拡張エキスパート CPU アクセスリスト	Expert-CPU	2 グループ *1	-
拡張 MAC CPU アクセスリスト	MAC-CPU	1 グループ	-

*1：連続した 2 グループで 1 リソースずつ使用されます。連続した 2 グループの使用パターンは、グループ（2, 3）（4, 5）（6, 7）（8, 9）（10, 11）です。

*2：連続した 2 グループで 1 リソースずつ使用されます。連続した 2 グループの使用パターンは、（0, 1）（2, 3）です。

NOTE: アクセスリストの Type が異なるルールは、同じグループに同時に設定できません。

設定可能な最大ルール数

1 種類の Type のアクセスリストのみを設定した場合の、設定可能な最大ルール数を示します。

表 8-5 NP7000 に 1 種類の Type のアクセスリストのみを設定した場合の最大ルール数

Type	Ingress	Egress
IP MAC	グループ 2,3,4,5,6,7,8,9（各 256 ルール）＋グループ 10,11（各 512 ルール）＝ 3,072	グループ 0,1,2,3（各 256 ルール）＝ 1,024
IPv6 Expert	グループ 2 と 3, グループ 4 と 5, グループ 6 と 7, グループ 8 と 9（各 256 ルール）＋グループ 10 と 11（512 ルール）＝ 1,536	グループ 0 と 1, グループ 2 と 3（各 256 ルール）＝ 512

NOTE: スタック構成の場合でも、設定可能な最大ルール数は変わりません。

8.1.3.2 グループとリソース（NP5000）

NP5000 には、Ingress グループと Egress グループが用意されています。Ingress グループと Egress グループの使用例は下図のとおりです。

図 8-4 Ingress グループの使用例

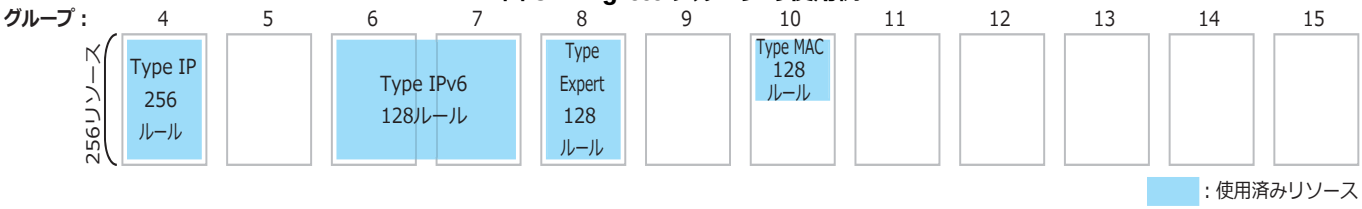
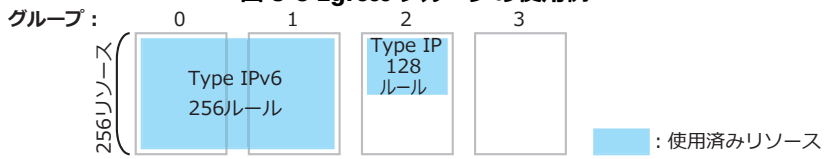


図 8-5 Egress グループの使用例



使用可能なリソース数

NP5000 のアクセスリストのリソース数を下表に示します。

表 8-6 NP5000 のアクセスリストのリソース

	Ingress	Egress
グループ数	12（グループ 4 から 15）	4（グループ 0 から 3）
グループごとに使用できるリソース数	256 リソース	256 リソース

NOTE: Ingress グループのグループ 0 から 3 は使用できません。

アクセスリストの Type と使用するグループ数

アクセスリストの種類によって、アクセスリストの Type が決定されます。また、アクセスリストの Type により、1 ルールごとに使用するグループ数およびリソース数が異なります。

表 8-7 NP5000 のアクセスリストの Type と使用するグループ数

アクセスリストの種類	アクセスリストの Type	1 ルールごとに使用するグループ数（Ingress）	1 ルールごとに使用するグループ数（Egress）
標準 IP アクセスリスト 拡張 IP アクセスリスト	IP	1 グループ	1 グループ
標準 IPv6 アクセスリスト 拡張 IPv6 アクセスリスト	IPv6	2 グループ *1	2 グループ *2
拡張エキスパートアクセスリスト	Expert	1 グループ *3	2 グループ *2
拡張 MAC アクセスリスト	MAC	1 グループ	1 グループ
標準 IP CPU アクセスリスト 拡張 IP CPU アクセスリスト	IP-CPU	1 グループ	-
標準 IPv6 CPU アクセスリスト 拡張 IPv6 CPU アクセスリスト	IPv6-CPU	2 グループ *1	-
拡張エキスパート CPU アクセスリスト	Expert-CPU	1 グループ *3	-
拡張 MAC CPU アクセスリスト	MAC-CPU	1 グループ	-

*1：連続した 2 グループで 2 リソースずつ（合計 4 リソース）使用されます。連続した 2 グループの使用パターンは、グループ（4, 5）（6, 7）（8, 9）（10, 11）（12, 13）（14, 15）です。

*2：連続した 2 グループで 1 リソースずつ使用されます。連続した 2 グループの使用パターンは、グループ（0, 1）（2, 3）です。

*3：グループごとに 2 リソースずつ使用されます。

NOTE: アクセスリストの Type が異なるルールは、同じグループに同時に設定できません。

設定可能な最大ルール数

1 種類の Type のアクセスリストのみを設定した場合の、設定可能な最大ルール数を示します。

表 8-8 NP5000 に 1 種類の Type のアクセスリストのみを設定した場合の最大ルール数

Type	Ingress	Egress
IP MAC	グループ 4,5,6,7,8,9,10,11,12,13,14,15（各 256 ルール）= 3,072	グループ 0,1,2,3（各 256 ルール）= 1,024
IPv6	グループ 4 と 5, グループ 6 と 7, グループ 8 と 9, グループ 10 と 11, グループ 12 と 13, グループ 14 と 15（各 128 ルール）= 768	グループ 0 と 1, グループ 2 と 3（各 256 ルール）= 512
Expert	グループ 4,5,6,7,8,9,10,11,12,13,14,15（各 128 ルール）= 1,536	グループ 0 と 1, グループ 2 と 3（各 256 ルール）= 512

NOTE: スタック構成の場合でも、設定可能な最大ルール数は変わりません。

8.1.3.3 グループとリソース（NP4000）

NP4000 には、Ingress グループと Egress グループが用意されています。Ingress グループと Egress グループの使用例は下図のとおりです。

図 8-6 Ingress グループの使用例

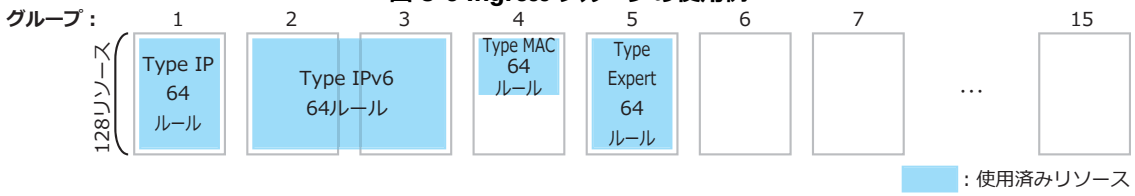
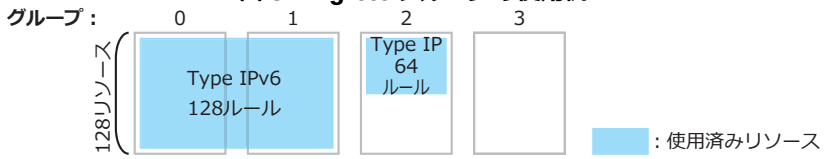


図 8-7 Egress グループの使用例



使用可能なリソース数

NP4000 のアクセスリストのリソース数を下表に示します。

表 8-9 NP4000 のアクセスリストのリソース

	Ingress	Egress
グループ数	15（グループ 1 から 15）	4（グループ 0 から 3）
グループごとに使用できるリソース数	128 リソース	128 リソース

NOTE: Ingress グループのグループ 0 は使用できません。

アクセスリストの Type と使用するグループ数

アクセスリストの種類によって、アクセスリストの Type が決定されます。また、アクセスリストの Type により、1 ルールごとに使用するグループ数およびリソース数が異なります。

表 8-10 NP4000 のアクセスリストの Type と使用するグループ数

アクセスリストの種類	アクセスリストの Type	1 ルールごとに使用するグループ数（Ingress）	1 ルールごとに使用するグループ数（Egress）
標準 IP アクセスリスト 拡張 IP アクセスリスト	IP	1 グループ *1	1 グループ
標準 IPv6 アクセスリスト 拡張 IPv6 アクセスリスト	IPv6	2 グループ *2	2 グループ *3
拡張エキスパートアクセスリスト	Expert	1 グループ *1	2 グループ *3
拡張 MAC アクセスリスト	MAC	1 グループ	1 グループ

*1：グループごとに 2 リソースずつ使用されます。

*2：連続した 2 グループで 2 リソースずつ（合計 4 リソース）使用されます。連続した 2 グループの使用パターンは、グループ（2, 3）（4, 5）（6, 7）（8, 9）（10, 11）（12, 13）（14, 15）です。

*3：連続した 2 グループで 1 リソースずつ使用されます。連続した 2 グループの使用パターンは、グループ（0, 1）（2, 3）です。

NOTE: アクセスリストの Type が異なるルールは、同じグループに同時に設定できません。

設定可能な最大ルール数

1 種類の Type のアクセスリストのみを設定した場合の、設定可能な最大ルール数を示します。

表 8-11 NP4000 に 1 種類の Type のアクセスリストのみを設定した場合の最大ルール数

Type	Ingress	Egress
IP	グループ 1,2,3,4,5,6,7,8,9,10,11,12,13, 14,15（各 64 ルール） = 960	グループ 0,1,2,3（各 128 ルール） = 512
IPv6	グループ 2 と 3, グループ 4 と 5, グループ 6 と 7, グループ 8 と 9, グループ 10 と 11, グループ 12 と 13, グループ 14 と 15（各 64 ルール） = 448	グループ 0 と 1, グループ 2 と 3（各 128 ルール） = 256
Expert	グループ 1,2,3,4,5,6,7,8,9,10,11,12,13, 14,15（各 64 ルール） = 960	グループ 0 と 1, グループ 2 と 3（各 128 ルール） = 256
MAC	グループ 1,2,3,4,5,6,7,8,9,10,11,12,13, 14,15（各 128 ルール） = 1,920	グループ 0,1,2,3（各 128 ルール） = 512

NOTE: スタック構成の場合でも、設定可能な最大ルール数は変わりません。

8.1.3.4 グループとリソース（NP3000）

NP3000 には、Ingress グループと Egress グループが用意されています。Ingress グループと Egress グループの使用例は下図のとおりです。

図 8-8 Ingress グループの使用例

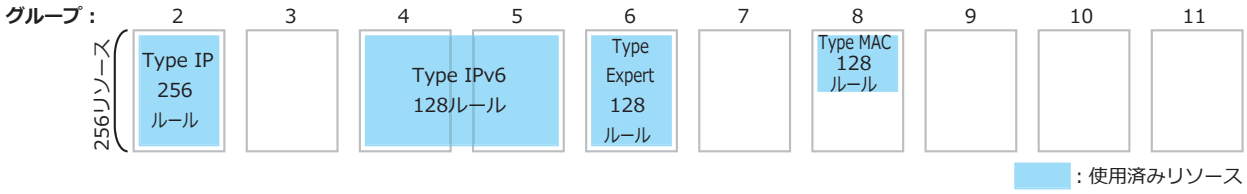
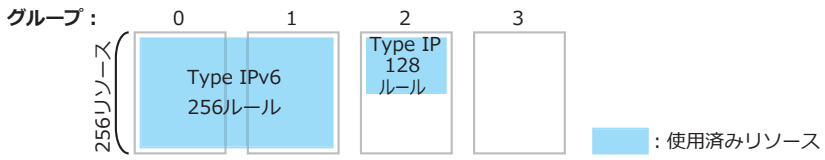


図 8-9 Egress グループの使用例



使用可能なリソース数

NP3000 のアクセスリストのリソース数を下表に示します。

表 8-12 NP3000 のアクセスリストのリソース

	Ingress	Egress
グループ数	10（グループ 2 から 11）	4（グループ 0 から 3）
グループごとに使用できるリソース数	256 リソース	256 リソース

NOTE: Ingress グループのグループ 0 から 1 は使用できません。

アクセスリストの Type と使用するグループ数

アクセスリストの種類によって、アクセスリストの Type が決定されます。また、アクセスリストの Type により、1 ルールごとに使用するグループ数およびリソース数が異なります。

表 8-13 NP3000 のアクセスリストの Type と使用するグループ数

アクセスリストの種類	アクセスリストの Type	1 ルールごとに使用するグループ数（Ingress）	1 ルールごとに使用するグループ数（Egress）
標準 IP アクセスリスト 拡張 IP アクセスリスト	IP	1 グループ	1 グループ
標準 IPv6 アクセスリスト 拡張 IPv6 アクセスリスト	IPv6	2 グループ *1	2 グループ *2
拡張エキスパートアクセスリスト	Expert	1 グループ *3	2 グループ *2
拡張 MAC アクセスリスト	MAC	1 グループ	1 グループ

*1：連続した 2 グループで 2 リソースずつ（合計 4 リソース）使用されます。連続した 2 グループの使用パターンは、グループ（2, 3）（4, 5）（6, 7）（8, 9）（10, 11）です。

*2：連続した 2 グループで 1 リソースずつ使用されます。連続した 2 グループの使用パターンは、グループ（0, 1）（2, 3）です。

*3：グループごとに 2 リソースずつ使用されます。

NOTE: アクセスリストの Type が異なるルールは、同じグループに同時に設定できません。

設定可能な最大ルール数

1 種類の Type のアクセスリストのみを設定した場合の、設定可能な最大ルール数を示します。

表 8-14 NP3000 に 1 種類の Type のアクセスリストのみを設定した場合の最大ルール数

Type	Ingress	Egress
IP MAC	グループ 2,3,4,5,6,7,8,9,10,11（各 256 ルール）＝ 2,560	グループ 0,1,2,3（各 256 ルール）＝ 1,024
IPv6	グループ 2 と 3, グループ 4 と 5, グループ 6 と 7, グループ 8 と 9, グループ 10 と 11（各 128 ルール）＝ 640	グループ 0 と 1, グループ 2 と 3（各 256 ルール）＝ 512
Expert	グループ 2,3,4,5,6,7,8,9,10,11（各 128 ルール）＝ 1,280	グループ 0 と 1, グループ 2 と 3（各 256 ルール）＝ 512

NOTE: スタック構成の場合でも、設定可能な最大ルール数は変わりません。

8.1.3.5 グループとリソース（NP2100）

NP2100 には、Ingress グループと Egress グループが用意されています。Ingress グループと Egress グループの使用例は下図のとおりです。

図 8-10 Ingress グループの使用例

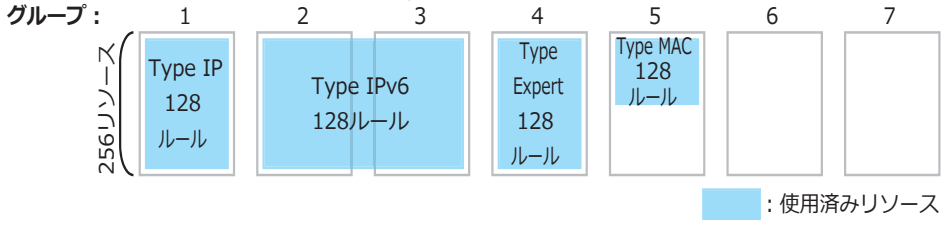
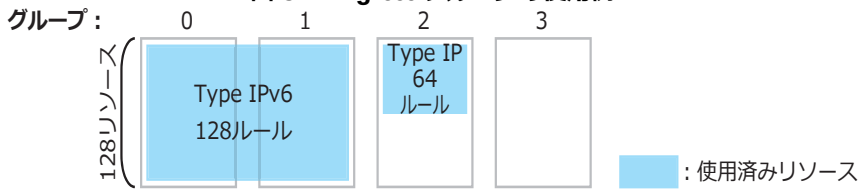


図 8-11 Egress グループの使用例



使用可能なリソース数

NP2100 のアクセスリストのリソース数を下表に示します。

表 8-15 NP2100 のアクセスリストのリソース

	Ingress	Egress
グループ数	7（グループ 1 から 7）	4（グループ 0 から 3）
グループごとに使用できるリソース数	256 リソース	128 リソース

NOTE: Ingress グループのグループ 0 は使用できません。

アクセスリストの Type と使用するグループ数

アクセスリストの種類によって、アクセスリストの Type が決定されます。また、アクセスリストの Type により、1 ルールごとに使用するグループ数およびリソース数が異なります。

表 8-16 NP2100 のアクセスリストの Type と使用するグループ数

アクセスリストの種類	アクセスリストの Type	1 ルールごとに使用するグループ数（Ingress）	1 ルールごとに使用するグループ数（Egress）
標準 IP アクセスリスト 拡張 IP アクセスリスト	IP	1 グループ *1	1 グループ
標準 IPv6 アクセスリスト 拡張 IPv6 アクセスリスト	IPv6	2 グループ *2	2 グループ *3
拡張エキスパートアクセスリスト	Expert	1 グループ *1	2 グループ *3
拡張 MAC アクセスリスト	MAC	1 グループ	1 グループ
ARP アクセスリスト	ARP	1 グループ *1	-

*1：グループごとに 2 リソースずつ使用されます。

*2：連続した 2 グループで 2 リソースずつ（合計 4 リソース）使用されます。連続した 2 グループの使用パターンは、グループ（2, 3）（4, 5）（6, 7）です。

*3：連続した 2 グループで 1 リソースずつ使用されます。連続した 2 グループの使用パターンは、グループ（0, 1）（2, 3）です。

NOTE: アクセスリストの Type が異なるルールは、同じグループに同時に設定できません。

設定可能な最大ルール数

1 種類の Type のアクセスリストのみを設定した場合の、設定可能な最大ルール数を示します。

表 8-17 NP2100 に 1 種類の Type のアクセスリストのみを設定した場合の最大ルール数

Type	Ingress	Egress
IP	グループ 1,2,3,4,5,6,7（各 128 ルール）= 896	グループ 0,1,2,3（各 128 ルール）= 512
IPv6	グループ 2 と 3, グループ 4 と 5, グループ 6 と 7（各 128 ルール）= 384	グループ 0 と 1, グループ 2 と 3（各 128 ルール）= 256
Expert	グループ 1,2,3,4,5,6,7（各 128 ルール）= 896	グループ 0 と 1, グループ 2 と 3（各 128 ルール）= 256
MAC	グループ 1,2,3,4,5,6,7（各 256 ルール）= 1,792	グループ 0,1,2,3（各 128 ルール）= 512
ARP	グループ 1,2,3,4,5,6,7（各 128 ルール）= 896	-

NOTE: スタック構成の場合でも、設定可能な最大ルール数は変わりません。

8.1.3.6 グループとリソース（NP2000）

NP2000 には、Ingress グループと Egress グループが用意されています。Ingress グループと Egress グループの使用例は下図のとおりです。

図 8-12 Ingress グループの使用例

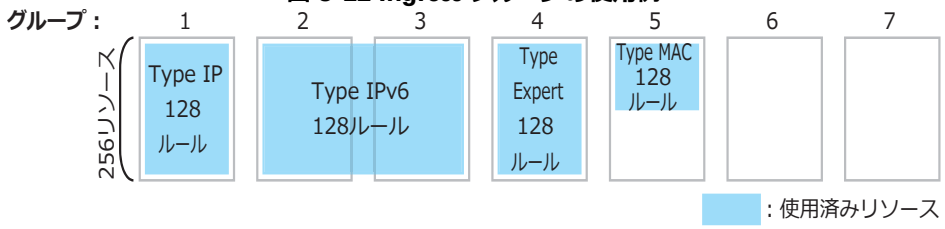
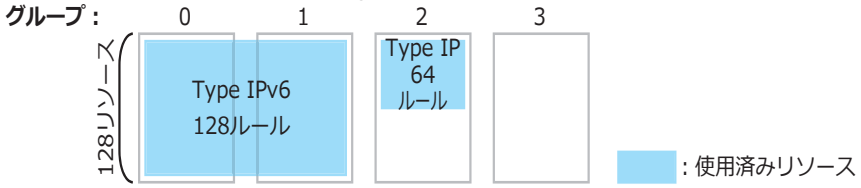


図 8-13 Egress グループの使用例



使用可能なリソース数

NP2000 のアクセスリストのリソース数を下表に示します。

表 8-18 NP2000 のアクセスリストのリソース

	Ingress	Egress
グループ数	7（グループ 1 から 7）	4（グループ 0 から 3）
グループごとに使用できるリソース数	256 リソース	128 リソース

NOTE: Ingress グループのグループ 0 は使用できません。

アクセスリストの Type と使用するグループ数

アクセスリストの種類によって、アクセスリストの Type が決定されます。また、アクセスリストの Type により、1 ルールごとに使用するグループ数およびリソース数が異なります。

表 8-19 NP2000 のアクセスリストの Type と使用するグループ数

アクセスリストの種類	アクセスリストの Type	1 ルールごとに使用するグループ数（Ingress）	1 ルールごとに使用するグループ数（Egress）
標準 IP アクセスリスト 拡張 IP アクセスリスト	IP	1 グループ *1	1 グループ
標準 IPv6 アクセスリスト 拡張 IPv6 アクセスリスト	IPv6	2 グループ *2	2 グループ *3
拡張エキスパートアクセスリスト	Expert	1 グループ *1	2 グループ *3
拡張 MAC アクセスリスト	MAC	1 グループ	1 グループ
ARP アクセスリスト	ARP	1 グループ *1	-

*1：グループごとに 2 リソースずつ使用されます。

*2：連続した 2 グループで 2 リソースずつ（合計 4 リソース）使用されます。連続した 2 グループの使用パターンは、グループ（2, 3）（4, 5）（6, 7）です。

*3：連続した 2 グループで 1 リソースずつ使用されます。連続した 2 グループの使用パターンは、グループ（0, 1）（2, 3）です。

NOTE: アクセスリストの Type が異なるルールは、同じグループに同時に設定できません。

設定可能な最大ルール数

1 種類の Type のアクセスリストのみを設定した場合の、設定可能な最大ルール数を示します。

表 8-20 NP2000 に 1 種類の Type のアクセスリストのみを設定した場合の最大ルール数

Type	Ingress	Egress
IP	グループ 1,2,3,4,5,6,7（各 128 ルール）= 896	グループ 0,1,2,3（各 128 ルール）= 512
IPv6	グループ 2 と 3, グループ 4 と 5, グループ 6 と 7（各 128 ルール）= 384	グループ 0 と 1, グループ 2 と 3（各 128 ルール）= 256
Expert	グループ 1,2,3,4,5,6,7（各 128 ルール）= 896	グループ 0 と 1, グループ 2 と 3（各 128 ルール）= 256
MAC	グループ 1,2,3,4,5,6,7（各 256 ルール）= 1,792	グループ 0,1,2,3（各 128 ルール）= 512
ARP	グループ 1,2,3,4,5,6,7（各 128 ルール）= 896	-

NOTE: スタック構成の場合でも、設定可能な最大ルール数は変わりません。

8.1.3.7 グループとリソース（NP2500）

NP2500 には、Ingress グループと Egress グループが用意されています。Ingress グループと Egress グループの使用例は下図のとおりです。

図 8-14 Ingress グループの使用例

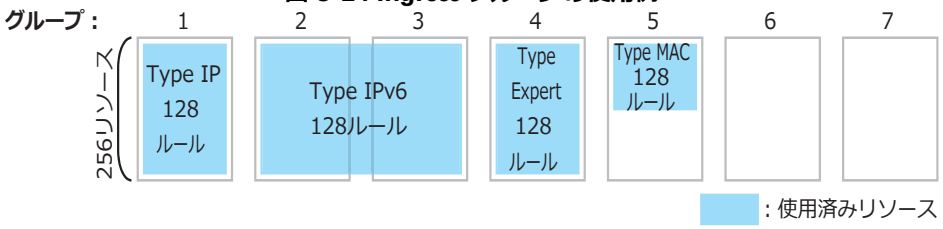
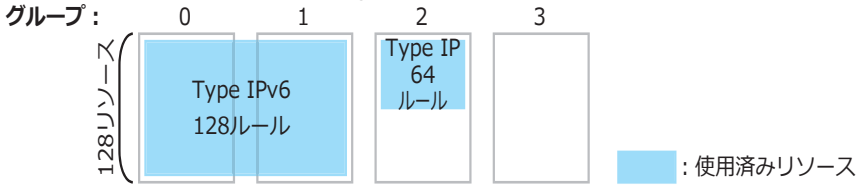


図 8-15 Egress グループの使用例



使用可能なリソース数

NP2500 のアクセスリストのリソース数を下表に示します。

表 8-21 NP2500 のアクセスリストのリソース

	Ingress	Egress
グループ数	7（グループ 1 から 7）	4（グループ 0 から 3）
グループごとに使用できるリソース数	256 リソース	128 リソース

NOTE: Ingress グループのグループ 0 は使用できません。

アクセスリストの Type と使用するグループ数

アクセスリストの種類によって、アクセスリストの Type が決定されます。また、アクセスリストの Type により、1 ルールごとに使用するグループ数およびリソース数が異なります。

表 8-22 NP2500 のアクセスリストの Type と使用するグループ数

アクセスリストの種類	アクセスリストの Type	1 ルールごとに使用するグループ数（Ingress）	1 ルールごとに使用するグループ数（Egress）
標準 IP アクセスリスト 拡張 IP アクセスリスト	IP	1 グループ *1	1 グループ
標準 IPv6 アクセスリスト 拡張 IPv6 アクセスリスト	IPv6	2 グループ *2	2 グループ *3
拡張エキスパートアクセスリスト	Expert	1 グループ *1	2 グループ *3
拡張 MAC アクセスリスト	MAC	1 グループ	1 グループ
ARP アクセスリスト	ARP	1 グループ *1	-

*1：グループごとに 2 リソースずつ使用されます。

*2：連続した 2 グループで 2 リソースずつ（合計 4 リソース）使用されます。連続した 2 グループの使用パターンは、グループ（2, 3）（4, 5）（6, 7）です。

*3：連続した 2 グループで 1 リソースずつ使用されます。連続した 2 グループの使用パターンは、グループ（0, 1）（2, 3）です。

NOTE: アクセスリストの Type が異なるルールは、同じグループに同時に設定できません。

設定可能な最大ルール数

1 種類の Type のアクセスリストのみを設定した場合の、設定可能な最大ルール数を示します。

表 8-23 NP2500 に 1 種類の Type のアクセスリストのみを設定した場合の最大ルール数

Type	Ingress	Egress
IP	グループ 1,2,3,4,5,6,7（各 128 ルール）= 896	グループ 0,1,2,3（各 128 ルール）= 512
IPv6	グループ 2 と 3, グループ 4 と 5, グループ 6 と 7（各 128 ルール）= 384	グループ 0 と 1, グループ 2 と 3（各 128 ルール）= 256
Expert	グループ 1,2,3,4,5,6,7（各 128 ルール）= 896	グループ 0 と 1, グループ 2 と 3（各 128 ルール）= 256
MAC	グループ 1,2,3,4,5,6,7（各 256 ルール）= 1,792	グループ 0,1,2,3（各 128 ルール）= 512
ARP	グループ 1,2,3,4,5,6,7（各 128 ルール）= 896	-

NOTE: スタック構成の場合でも、設定可能な最大ルール数は変わりません。

8.1.4 アクセスリストのリソースを使用する機能

以下の機能を有効にする際、アクセスリストのリソースを使用します。

表 8-24 アクセスリストのリソースを使用する機能

機能	使用するグループ（Ingress）数
AccessDefender	5 グループ以上 *1
ループ検知	1 グループ *2 AccessDefender 制御用の 1 グループ、ループ検知、およびポートリダンダントで使用するグループは、同じグループを共有します。
CFM（IEEE 802.1ag）	1 グループ
MMRP-Plus	1 グループ
ポートリダンダントの FDB フラッシュフレーム送信、受信機能	1 グループ *2 AccessDefender 制御用の 1 グループ、ループ検知、およびポートリダンダントで使用するグループは、同じグループを共有します。
IGMP スヌーピングの **ip igmp snooping unregistered-filter** コマンド	1 グループ
MLD スヌーピングの **ipv6 mld snooping unregistered-filter** コマンド	1 グループ
ポリシーマップ *3	使用するアクセスリスト種別や設定量によります。
ポリシーベースルーティング	使用するアクセスリスト種別や設定量によります。
ユニキャストリバースパス転送（URPF）で access-group オプション、または ipv6-access-group オプションを使用する場合	使用するアクセスリスト種別や設定量によります。
その他、アクセスリストを使用する機能	使用するアクセスリスト種別や設定量によります。

*1：最大認証クライアント数により使用するグループ数が変わります。詳細については、「第 6 編 AccessDefender」の「アクセスリストグループと最大認証クライアント数」を参照してください。

*2：**show access-list resource** コマンドでは、AccessDefenderIII & Loop Detection と表示されます。

*3：ポリシーマップを input 側に適用した場合は、アクセスリストの Ingress グループのリソースを使用します。ポリシーマップを output 側に適用した場合は、アクセスリストの Egress グループのリソースを使用します。

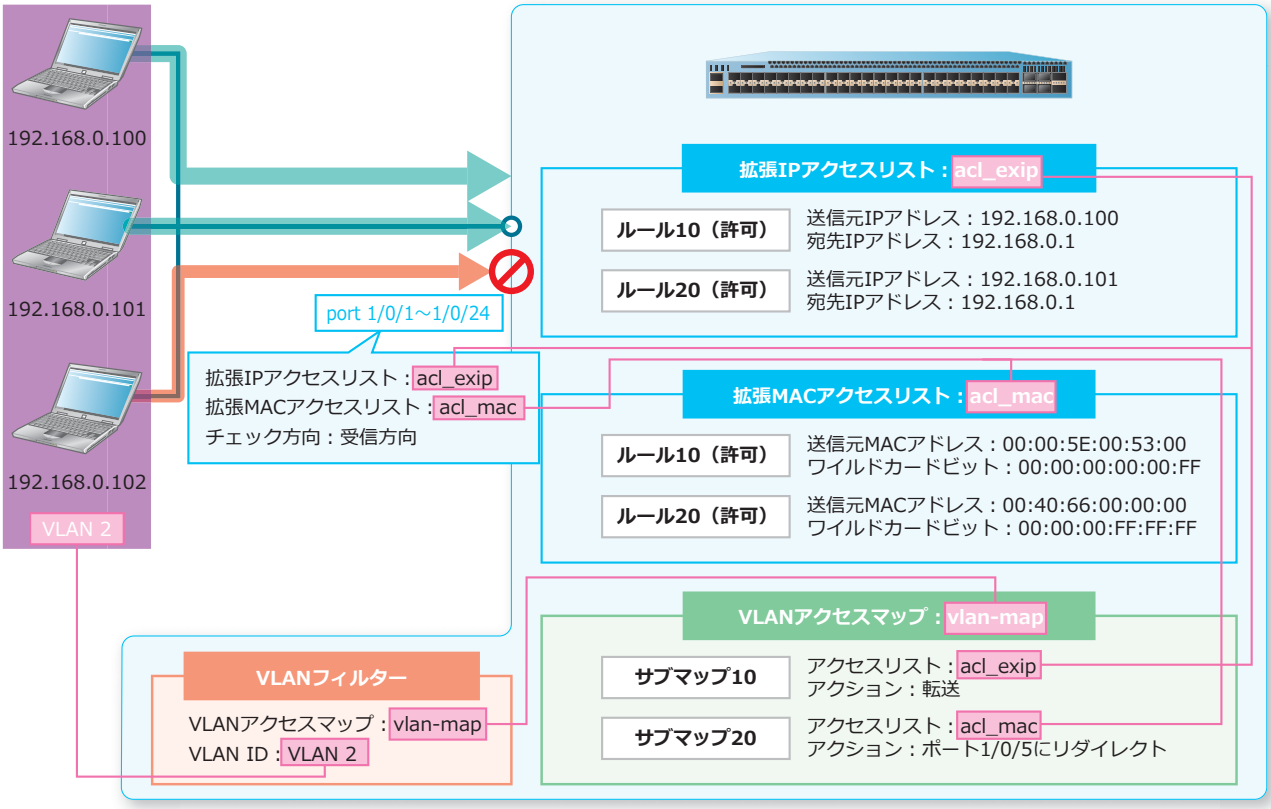
8.1.5 アクセスリストハードウェアカウンター

アクセスリストハードウェアカウンターを有効にすると、アクセスリストに登録したルールに一致したパケット数をカウントできます。アクセスリストハードウェアカウンターは、**acl-hardware-counter** コマンドで有効化します。また、アクセスリストハードウェアカウンターをクリアするには、**clear acl-hardware-counter** コマンドを使用します。

8.1.6 VLAN に対するアクセスコントロールの適用

特定の VLAN の受信パケットに対してアクセスコントロールを実施する場合、VLAN アクセスマップを使用することもできます。アクセスリストに対してアクションを設定したものを**サブマップ**と呼び、1 つ以上のサブマップをリストにまとめたものを **VLAN アクセスマップ**と呼びます。また、VLAN アクセスマップを VLAN に割り当てるための設定を **VLAN フィルター**と呼びます。

図 8-16 VLAN に対するアクセスコントロールの適用



VLAN に対してアクセスコントロールを適用する際に必要な設定は以下のとおりです。（）内は使用するコマンドです。

- VLAN アクセスマップおよびサブマップの作成（**`vlan access-map`** コマンド）

  NOTE: サブマップのシーケンス番号を指定しない場合は、開始値 10 から増分値 10 でインクリメントした番号のうち、まだ使用されていない最も小さい番号が自動的に割り当てられます。

- サブマップへのアクセスリストの関連付け（**`match ip address`** コマンド、**`match ipv6 address`** コマンド、**`match mac address`** コマンド）

  NOTE: VLAN アクセスマップの対象にする条件は、サブマップに関連付けるアクセスリストにおいて、permit ルールで設定します。

  NOTE: 拡張エキスパートアクセスリスト、および CPU アクセスリストは、サブマップに関連付けられません。

  NOTE: NP7000 および NP5000 において、フィルタリング対象のエントリー数は装置全体で最大 3,072 個ですが、設定可能なエントリー数は使用するアクセスリストの種別、設定順序、および当該サブマップを **`vlan filter`** コマンドで適用した VLAN の組み合わせによって変化します。

NOTE: NP4000 において、フィルタリング対象のエントリー数は装置全体で最大 1,920 個ですが、設定可能なエントリー数は使用するアクセスリストの種別、設定順序、および当該サブマップを **vlan filter** コマンドで適用した VLAN の組み合わせによって変化します。

NOTE: NP3000 において、フィルタリング対象のエントリー数は装置全体で最大 2,560 個ですが、設定可能なエントリー数は使用するアクセスリストの種別、設定順序、および当該サブマップを **vlan filter** コマンドで適用した VLAN の組み合わせによって変化します。

NOTE: NP2100、NP2000、および NP2500 において、フィルタリング対象のエントリー数は装置全体で最大 1,792 個ですが、設定可能なエントリー数は使用するアクセスリストの種別、設定順序、および当該サブマップを **vlan filter** コマンドで適用した VLAN の組み合わせによって変化します。

- サブマップへのアクションの設定（**action** コマンド）
- VLAN フィルターの作成（**vlan filter** コマンド）

CAUTION: 適用する VLAN アクセスマップのエントリー数や、適用対象の VLAN 数が多いほど、設定反映時間が長くなります。

NOTE: NP7000 の 1.08.01 以降、NP5000 の 1.07.01 以降、NP4000 の 1.02.04 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 1.10.01 以降では、**vlan filter** コマンド実行時に VLAN フィルターの設定が完了するまでに 5 秒以上を要する場合は、CLI に進捗状況（%）が表示されます。

8.1.7 アクセスリストの優先順位

アクセスリストの場合

1 つのアクセスリストにおいては、小さいシーケンス番号のルールから順番にチェックされ、マッチした場合には以降のシーケンス番号はチェックしないという、First Match 規則で動作します。

同一ポートに複数種別のアクセスリストを設定している場合は、以下のように 1 つのパケットが複数種別のアクセスリストにマッチする可能性があります。

- 「標準または拡張 IP アクセスリスト」、「拡張エキスパートアクセスリスト」、および「IP パケット対象化機能を有効にした拡張 MAC アクセスリスト」を同一ポートに設定している場合は、任意の IPv4 パケットが複数のアクセスリストにマッチする可能性があります。
- 「標準または拡張 IPv6 アクセスリスト」および「IP パケット対象化機能を有効にした拡張 MAC アクセスリスト」を同一ポートに設定している場合は、任意の IPv6 パケットが複数のアクセスリストにマッチする可能性があります。
- 「ARP アクセスリスト」および「拡張 MAC アクセスリスト」を同一ポートに設定している場合は、任意の ARP パケットが複数のアクセスリストにマッチする可能性があります。

この場合、アクセスリストの優先順位に従って、最も優先順位の高いアクセスリストのアクションが採用されます。アクセスリストの優先順位を以下に示します。

図 8-17 アクセスリストの優先順位（Ingress グループの場合）

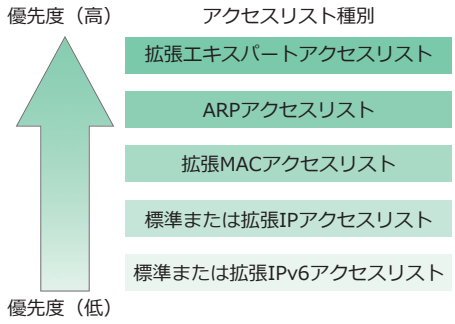
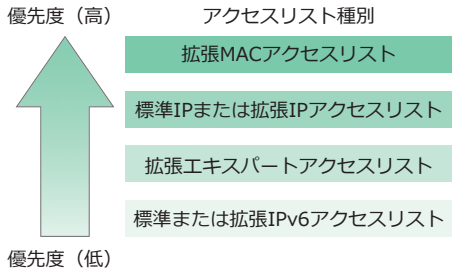


図 8-18 アクセスリストの優先順位（Egress グループの場合）



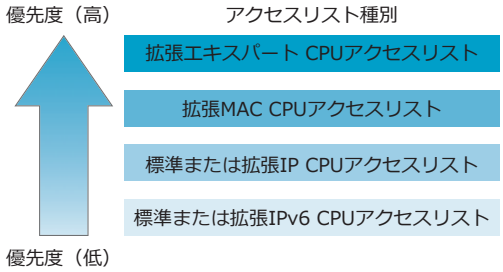
NOTE: アクセスリストの優先順位は、**`show access-list resource reserved-priority`** コマンドで確認できます。

NOTE: アクセスリストハードウェアカウンターを有効にしている場合は、アクションが採用されなくても、マッチしたすべてのアクセスリストでカウントします。

CPU アクセスリストの場合

CPU アクセスリストも通常のアクセスリストと同様に、小さいシーケンス番号のルールから順番にチェックされます。CPU アクセスリストの優先順位を以下に示します。

図 8-19 CPU アクセスリストの優先順位



VLAN アクセスマップの場合

1 つの VLAN アクセスマップにおいて、割り当てられたすべてのサブマップの種別（**`match`** コマンドで関連付けたアクセスリストの種別）が 1 種類の場合は、小さいシーケンス番号のサブマップから順番にチェックされ、マッチした場合には以降のシーケンス番号はチェックしないという、First Match 規則で動作します。

1 つの VLAN アクセスマップにおいて、割り当てられたサブマップの種別（**`match`** コマンドで関連付けたアクセスリストの種別）が複数の場合は、以下のように 1 つのパケットが複数種別のサブマップにマッチする可能性があります。

- 「標準または拡張 IP アクセスリスト」を関連付けたサブマップ、および「IP パケット対象化機能を有効にした拡張 MAC アクセスリスト」を関連付けたサブマップの両方を設定している場合は、任意の IPv4 パケットが両方のサブマップにマッチする可能性があります。

- 「標準または拡張 IPv6 アクセスリスト」を関連付けたサブマップ、および「IP パケット対象化機能を有効にした拡張 MAC アクセスリスト」を関連付けたサブマップの両方を設定している場合は、任意の IPv6 パケットが両方のサブマップにマッチする可能性があります。
- 「ARP アクセスリスト」を関連付けたサブマップ、および「拡張 MAC アクセスリスト」を関連付けたサブマップの両方を設定している場合は、任意の ARP パケットが両方のサブマップにマッチする可能性があります。

この場合、アクセスリストの優先順位に従って、1 番優先順位の高いアクセスリストを関連付けたサブマップのアクションが採用されます。

> ***NOTE:*** 複数のサブマップにマッチした場合の候補となるアクションが「forward」と「redirect」の場合は、アクセスリストの優先順位に関係なく「redirect」が採用されます。

アクセスリストと VLAN アクセスマップを併用している場合

受信したパケットがアクセスリストと VLAN アクセスマップ（サブマップに関連付けたアクセスリストが同一種別）の両方にマッチする場合は、アクセスリストが優先されます。

受信したパケットがアクセスリストと VLAN アクセスマップ（サブマップに関連付けたアクセスリストが異なる種別）の両方にマッチする場合は、アクセスリストの優先順位に従って、最も優先順位の高いアクセスリストに紐付いているアクションが採用されます。

8.2 アクセスリストの状態確認

アクセスリストの状態を表示して確認する方法を説明します。

8.2.1 ポートに適用したアクセスリストの表示

show access-group コマンドで、ポートに適用したアクセスリストを確認できます。

表示例を以下に示します。

```
# show access-group

Port1/0/1: ...(1)
  (2)                           (3)
  Inbound ip access-list     : simple-ip-acl(ID: 1998)
  Inbound mac access-list    : simple-mac-acl(ID: 7998)
```

各項目の説明は、以下のとおりです。

表 8-25 show access-group 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)	アクセスリストの種類を表示します。 • Inbound ip access-list：受信方向に適用した IP アクセスリスト • Inbound arp access-list：受信方向に適用した ARP アクセスリスト • Inbound ipv6 access-list：受信方向に適用した IPv6 アクセスリスト • Inbound expert access-list：受信方向に適用した拡張エキスパートアクセスリスト • Inbound mac access-list：受信方向に適用した拡張 MAC アクセスリスト • Outbound ip access-list：送信方向に適用した IP アクセスリスト • Outbound ipv6 access-list：送信方向に適用した IPv6 アクセスリスト • Outbound expert access-list：送信方向に適用した拡張エキスパートアクセスリスト • Outbound mac access-list：送信方向に適用した拡張 MAC アクセスリスト • Inbound ip-cpu access-list：適用した IP CPU アクセスリスト • Inbound ipv6-cpu access-list：適用した IPv6 CPU アクセスリスト • Inbound expert-cpu access-list：適用した拡張エキスパート CPU アクセスリスト • Inbound mac-cpu access-list：適用した拡張 MAC CPU アクセスリスト
(3)	アクセスリスト名およびアクセスリスト番号を表示します。

8.2.2 アクセスリストの設定の表示

アクセスリストの設定を確認できます。

すべてのアクセスリストの一覧表示

show access-list コマンドで、すべてのアクセスリストの一覧を確認できます。

表示例を以下に示します。

```
# show access-list
(1)                                          (2)
Access-List-Name                             Type
-------------------------------------------  ---------------
rd-ip-acl(ID: 1998)                          ip acl
simple-ip-acl(ID: 3998)                      ip ext-acl
simple-rd-acl(ID: 3999)                      ip ext-acl
rd-mac-acl(ID: 6998)                         mac ext-acl
ip6-acl(ID: 14999)                           ipv6 ext-acl

Total Entries: 5
```

各項目の説明は、以下のとおりです。

表 8-26 show access-list コマンドの表示項目

項番	説明
(1)	アクセスリスト名およびアクセスリスト番号を表示します。
(2)	アクセスリストの種類を表示します。 • ip acl：標準 IP アクセスリスト • ip ext-acl：拡張 IP アクセスリスト • arp acl：ARP アクセスリスト • ipv6 acl：標準 IPv6 アクセスリスト • ipv6 ext-acl：拡張 IPv6 アクセスリスト • expert ext-acl：拡張エキスパートアクセスリスト • mac ext-acl：拡張 MAC アクセスリスト • ip-cpu acl：標準 IP CPU アクセスリスト • ip-cpu ext-acl：拡張 IP CPU アクセスリスト • ipv6-cpu acl：標準 IPv6 CPU アクセスリスト • ipv6-cpu ext-acl：拡張 IPv6 CPU アクセスリスト • expert-cpu ext-acl：拡張エキスパート CPU アクセスリスト • mac-cpu ext-acl：拡張 MAC CPU アクセスリスト

アクセスリストの設定の表示

アクセスリストを指定して **show access-list** コマンドを実行すると、指定したアクセスリストの設定を確認できます。

IP アクセスリスト「simple-ip-acl」を指定した場合の表示例を以下に示します。

```
# show access-list ip simple-ip-acl

Extended IP access list simple-ip-acl(ID: 3994) ...(1)
    (2)                                          (3)              (4)
    10 permit tcp any 10.20.0.0 0.0.255.255  (Ing: 0 packets  Egr: 0 packets)
    20 permit tcp any host 10.100.1.2  (Ing: 0 packets  Egr: 0 packets)
    30 permit icmp any any  (Ing: 0 packets  Egr: 0 packets)

    Counter enable on following port(s): ...(5)
    Ingress port(s): Port1/0/5-1/0/8
    Egress port(s): Port1/0/3
```

各項目の説明は、以下のとおりです。

表 8-27 show access-list ip <NAME> コマンドの表示項目

項番	説明
(1)	アクセスリスト名およびアクセスリスト番号を表示します。
(2)	各ルールのシーケンス番号、アクション、抽出条件を表示します。
(3)	アクセスリストハードウェアカウンターの受信パケット数を表示します。アクセスリストハードウェアカウンターが無効の場合は表示されません。
(4)	アクセスリストハードウェアカウンターの送信パケット数を表示します。アクセスリストハードウェアカウンターが無効の場合は表示されません。
(5)	アクセスリストハードウェアカウンターが有効化されているポート番号を表示します。アクセスリストハードウェアカウンターが無効の場合は表示されません。

8.2.3 VLAN アクセスマップの設定の表示

show vlan access-map コマンドで、VLAN アクセスマップの設定を確認できます。

表示例を以下に示します。

```
# show vlan access-map

VLAN access-map vlan-map 10 ...(1)
  match ip access list: stp_ip1(ID: 1888) ...(2)
  action: forward ...(3)
  Counter enable on VLAN(s): 1-2 ...(4)
  match count: 0 packets ...(5)
VLAN access-map vlan-map 20
  match mac access list: ext_mac(ID: 6995)
  action: redirect port 1/0/5
  Counter enable on VLAN(s): 1-2
  match count: 0 packets
```

各項目の説明は、以下のとおりです。

表 8-28 `show vlan access-map` コマンドの表示項目

項番	説明
(1)	サブマップの情報（VLAN アクセスマップ名およびシーケンス番号）を表示します。
(2)	サブマップに関連付けられたアクセスリスト名およびアクセスリスト番号を表示します。 • match ip access list：IP アクセスリスト指定（**`match ip address`** コマンド） • match arp address：ARP アクセスリスト指定（**`match arp address`** コマンド） • match ipv6 access list：IPv6 アクセスリスト指定（**`match ipv6 address`** コマンド） • match mac access list：拡張 MAC アクセスリスト指定（**`match mac address`** コマンド）
(3)	サブマップと一致したパケットに対するアクションを表示します。
(4)	アクセスリストハードウェアカウンターが有効化されている VLAN を表示します。
(5)	アクセスリストハードウェアカウンターの受信パケット数を表示します。

8.2.4 VLAN フィルターの設定の表示

`show vlan filter` コマンドで VLAN フィルターの設定を確認できます。

表示例を以下に示します。

```
# show vlan filter

VLAN Map aa ...(1)
  Configured on VLANs: 5-127,221-333 ...(2)
VLAN Map bb
  Configured on VLANs: 1111-1222
```

各項目の説明は、以下のとおりです。

表 8-29 `show vlan filter` コマンドの表示項目

項番	説明
(1)	VLAN アクセスマップ名を表示します。
(2)	対象の VLAN アクセスマップを適用している VLAN を表示します。

8.2.5 アクセスリストのリソース情報の表示

アクセスリストのリソースに関する情報を表示できます。

アクセスリストのリソースを使用している機能の表示

show access-list resource reserved-group コマンドで、アクセスリストのリソースを使用している機能を確認できます。

表示例を以下に示します。

```
# show access-list resource reserved-group

Ingress ACL
 (1)             (2)
 Group           Function
-------------    ---------------------
 1/2             Access-list (Expert)
 1/3             Access-list (Expert)
 1/4             Access-list (IPv4)
 1/5             Access-list (MAC)
 1/6             Access-list (IPv6)
 1/7             Access-list (IPv6)
 1/8             -
 1/9             -
 1/10            -
 1/11            -

Egress ACL
 (3)             (4)
 Group           Function
-------------    ---------------------
 1/0             Access-list (Expert)
 1/1             Access-list (Expert)
 1/2             Access-list (IPv6)
 1/3             Access-list (IPv6)
```

各項目の説明は、以下のとおりです。

表 8-30 show access-list resource reserved-group コマンドの表示項目

項番	説明
(1)	アクセスリストの Ingress グループ ID を表示します。

項番	説明
(2)	Ingress グループを利用している機能を表示します。 • Access-list (Expert-CPU)：拡張エキスパート CPU アクセスリストを使用している機能 • Access-list (MAC-CPU)：拡張 MAC CPU アクセスリストを使用している機能 • Access-list (IPv4-CPU)：IP CPU アクセスリストを使用している機能 • Access-list (IPv6-CPU)：IPv6 CPU アクセスリストを使用している機能 • Access-list (Expert)：拡張エキスパートアクセスリストを使用している機能 • Access-list (ARP)：ARP アクセスリストを使用している機能 • Access-list (MAC)：拡張 MAC アクセスリストを使用している機能 • Access-list (IPv4)：IP アクセスリストを使用している機能 • Access-list (IPv6)：IPv6 アクセスリストを使用している機能 • CFM：CFM（Connectivity Fault Management） • MMRP (reserve)：MMRP-Plus（予約状態） • MMRP：MMRP-Plus • AccessDefenderI：AccessDefender 制御用 • AccessDefenderII：AccessDefender 制御用 • AccessDefenderIII & Loop Detection：AccessDefender 制御用、ループ検知、およびポートリダンダントの一部コマンド • AccessDefender (reserve)：AccessDefender クライアント用（予約状態） • AccessDefender (Client)：AccessDefender クライアント用（使用中） • AccessDefender (Clientv6)：AccessDefender クライアント用（IPv6 認証用、使用中） • IGMP snooping：IGMP スヌーピングの unregistered-filter 用 • MLD snooping：MLD スヌーピングの unregistered-filter 用 • IPV4_PROUTE：IPv4 ポリシーベースルーティング • IPV6_PROUTE：IPv6 ポリシーベースルーティング • IPV4_URPF：ユニキャストリバースパス転送（URPF）
(3)	アクセスリストの Egress グループ ID を表示します。
(4)	Egress グループを利用している機能を表示します。 • Access-list (Expert)：拡張エキスパートアクセスリストを使用している機能 • Access-list (MAC)：拡張 MAC アクセスリストを使用している機能 • Access-list (IPv4)：IP アクセスリストを使用している機能 • Access-list (IPv6)：IPv6 アクセスリストを使用している機能

アクセスリストのリソースの優先順位の表示

show access-list resource reserved-priority コマンドで、アクセスリストのリソースの優先順位を確認できます。

表示例を以下に示します。

```
# show access-list resource reserved-priority

Ingress ACL
 (1)             (2)
 Priority        Function
-------------    ---------------------
 1               Access-list (Expert)
 1               Access-list (Expert)
 3               Access-list (MAC)
 4               Access-list (IPv4)
 5               Access-list (IPv6)
 5               Access-list (IPv6)
 7               -
 8               -
 9               -
 10              -

Egress ACL
 (3)             (4)
 Priority        Function
-------------    ---------------------
 1               Access-list (Expert)
 1               Access-list (Expert)
 3               Access-list (IPv6)
 3               Access-list (IPv6)
```

各項目の説明は、以下のとおりです。

表 8-31 show access-list resource reserved-priority コマンドの表示項目

項番	説明
(1)	アクセスリストの Ingress グループの優先度を表示します。

項番	説明
(2)	Ingress グループを利用している機能を表示します。 • Access-list (Expert-CPU)：拡張エキスパート CPU アクセスリストを使用している機能 • Access-list (MAC-CPU)：拡張 MAC CPU アクセスリストを使用している機能 • Access-list (IPv4-CPU)：IP CPU アクセスリストを使用している機能 • Access-list (IPv6-CPU)：IPv6 CPU アクセスリストを使用している機能 • Access-list (Expert)：拡張エキスパートアクセスリストを使用している機能 • Access-list (ARP)：ARP アクセスリストを使用している機能 • Access-list (MAC)：拡張 MAC アクセスリストを使用している機能 • Access-list (IPv4)：IP アクセスリストを使用している機能 • Access-list (IPv6)：IPv6 アクセスリストを使用している機能 • CFM：CFM（Connectivity Fault Management） • MMRP：MMRP-Plus • AccessDefenderI：AccessDefender 制御用 • AccessDefenderII：AccessDefender 制御用 • AccessDefenderIII & Loop Detection：AccessDefender 制御用、ループ検知、およびポートリダンダントの一部コマンド • AccessDefender (Client)：AccessDefender クライアント用 • AccessDefender (Clientv6)：AccessDefender クライアント用（IPv6 認証用） • IGMP snooping：IGMP スヌーピングの unregistered-filter 用 • MLD snooping：MLD スヌーピングの unregistered-filter 用 • IPV4_PROUTE：IPv4 ポリシーベースルーティング • IPV6_PROUTE：IPv6 ポリシーベースルーティング • IPV4_URPF：ユニキャストリバースパス転送（URPF）
(3)	アクセスリストの Egress グループの優先度を表示します。
(4)	Egress グループを利用している機能を表示します。 • Access-list (Expert)：拡張エキスパートアクセスリストを使用している機能 • Access-list (MAC)：拡張 MAC アクセスリストを使用している機能 • Access-list (IPv4)：IP アクセスリストを使用している機能 • Access-list (IPv6)：IPv6 アクセスリストを使用している機能

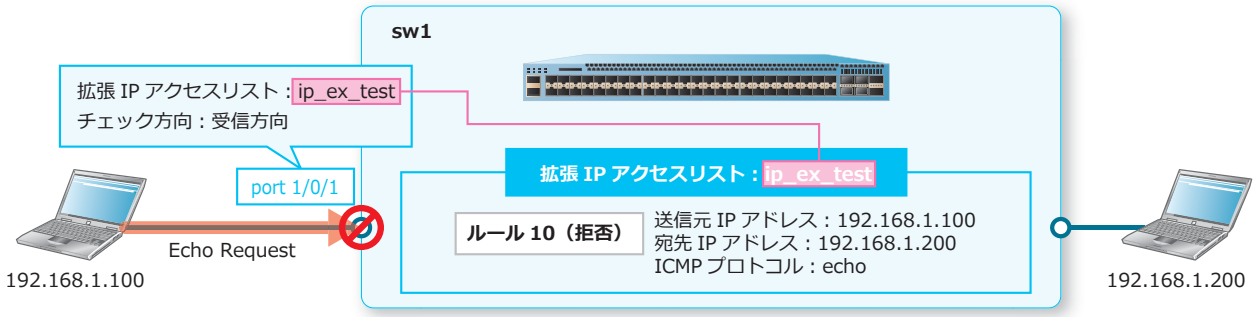
8.3 アクセスリストの構成例と設定例

アクセスリストを利用する場合の構成例と設定例を示します。

8.3.1 特定の ICMP Echo Request を破棄する場合

ポート 1/0/1 で受信した IPv4 パケットにおいて、192.168.1.100 から 192.168.1.200 へ送信された ICMP メッセージ「Echo Request」を破棄する場合の構成例と設定例を示します。

図 8-20 特定の ICMP Echo Request を破棄する場合の構成例



1. 拡張 IP アクセスリスト［ip_ex_test］を作成します。

```
sw1# configure terminal
sw1(config)# ip access-list extended ip_ex_test
sw1(config-ip-ext-acl)#
```

2. パケットの中継を拒否して破棄する以下のルールを設定します。

ルール 10（拒否）：ICMP プロトコル、送信元 IP アドレス［192.168.1.100］、宛先 IP アドレス［192.168.1.200］、ICMP メッセージ［echo］

```
sw1(config-ip-ext-acl)# deny icmp host 192.168.1.100 host 192.168.1.200 echo
sw1(config-ip-ext-acl)# exit
sw1(config)#
```

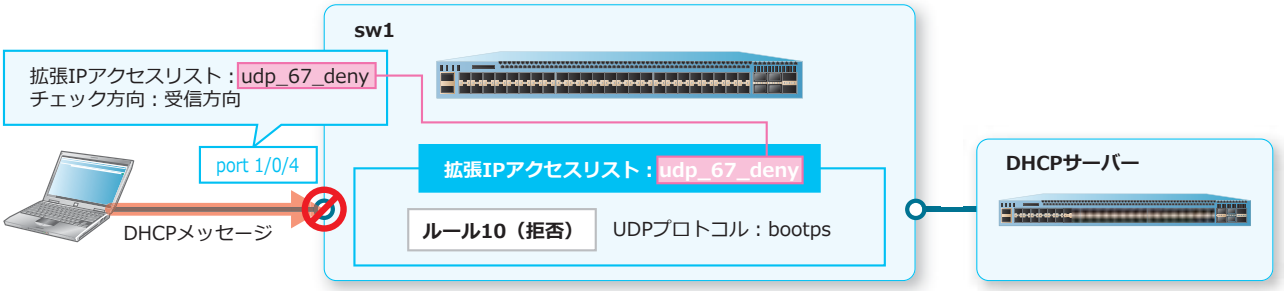
3. 設定した拡張 IP アクセスリストを、ポート 1/0/1 に受信方向で適用します。

```
sw1(config)# interface port 1/0/1
sw1(config-if-port)# ip access-group ip_ex_test in
sw1(config-if-port)# end
sw1#
```

8.3.2 DHCP サーバー宛ての DHCP パケットを破棄する場合

ポート 1/0/4 で受信した IPv4 パケットにおいて、DHCP サーバー宛ての DHCP パケット（UDP プロトコル、宛先 L4 ポート番号 bootps(67)）を破棄する場合の構成例と設定例を示します。

図 8-21 DHCP サーバー宛ての DHCP パケットを破棄する場合の構成例



1. 拡張 IP アクセスリスト［udp_67_deny］を作成します。

```
sw1# configure terminal
sw1(config)# ip access-list extended udp_67_deny
sw1(config-ip-ext-acl)#
```

2. パケットの中継を拒否して破棄する以下のルールを設定します。

ルール 10（拒否）：UDP プロトコル、宛先 L4 ポート番号［bootps(67)］

```
sw1(config-ip-ext-acl)# deny udp any any eq bootps
sw1(config-ip-ext-acl)# exit
sw1(config)#
```

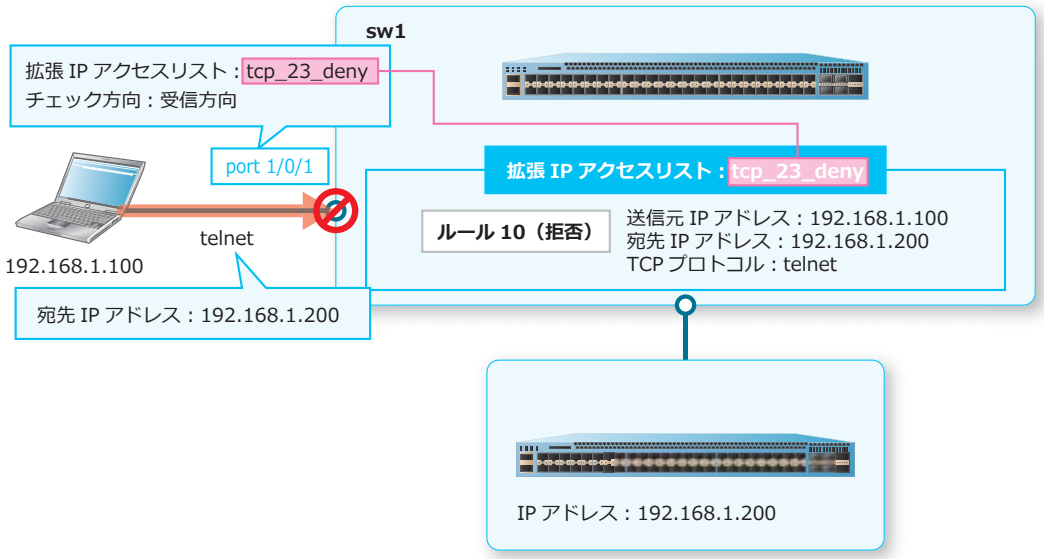
3. 設定した拡張 IP アクセスリストを、ポート 1/0/4 に受信方向で適用します。

```
sw1(config)# interface port 1/0/4
sw1(config-if-port)# ip access-group udp_67_deny in
sw1(config-if-port)# end
sw1#
```

8.3.3 特定の telnet パケットを破棄する場合

ポート 1/0/1 で受信した IPv4 パケットにおいて、192.168.1.100 から 192.168.1.200 へ送信された telnet パケット（TCP プロトコル、宛先 L4 ポート番号 telnet(23)）を破棄する場合の構成例と設定例を示します。

図 8-22 特定の telnet パケットを破棄する場合の構成例



1. 拡張 IP アクセスリスト［tcp_23_deny］を作成します。

```
sw1# configure terminal
sw1(config)# ip access-list extended tcp_23_deny
sw1(config-ip-ext-acl)#
```

2. パケットの中継を拒否して破棄する以下のルールを設定します。

ルール 10（拒否）：TCP プロトコル、送信元 IP アドレス［192.168.1.100］、宛先 IP アドレス［192.168.1.200］、宛先 L4 ポート番号［telnet(23)］

```
sw1(config-ip-ext-acl)# deny tcp host 192.168.1.100 host 192.168.1.200 eq telnet
sw1(config-ip-ext-acl)# exit
sw1(config)#
```

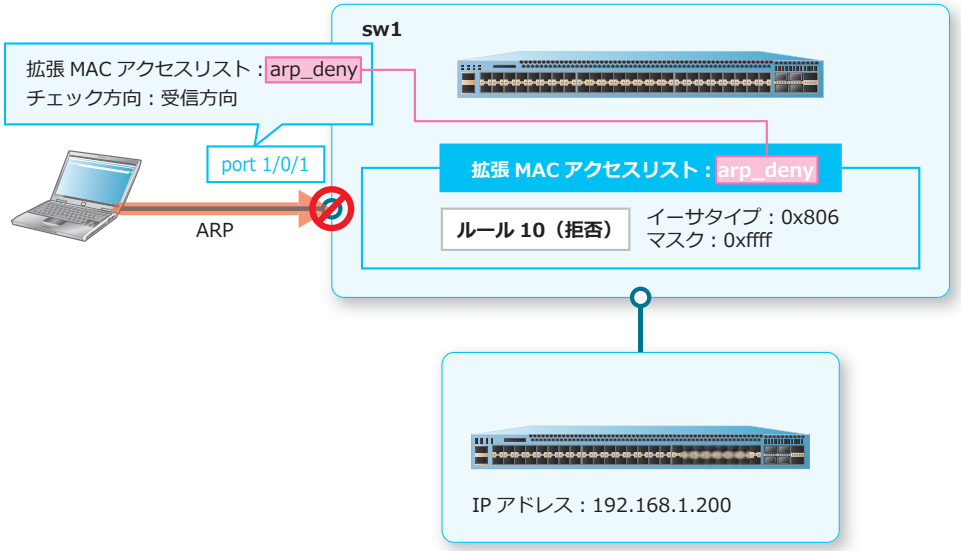
3. 設定した拡張 IP アクセスリストを、ポート 1/0/1 に受信方向で適用します。

```
sw1(config)# interface port 1/0/1
sw1(config-if-port)# ip access-group tcp_23_deny in
sw1(config-if-port)# end
sw1#
```

8.3.4 中継する ARP パケットを破棄する場合

ポート 1/0/1 で受信した非 IP パケットにおいて、中継する ARP パケットを破棄する場合の構成例と設定例を示します。

図 8-23 中継する ARP パケットを破棄する場合の構成例



1. 拡張 MAC アクセスリスト［arp_deny］を作成します。

```
sw1# configure terminal
sw1(config)# mac access-list extended arp_deny
sw1(config-mac-ext-acl)#
```

2. パケットの中継を拒否して破棄する以下のルールを設定します。

ルール 10（拒否）：イーサタイプ［0x806］、マスク［0xffff］

```
sw1(config-mac-ext-acl)# deny any any ethernet-type 0x806 0xffff
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 arp_deny in
sw1(config-if-port)# end
sw1#
```

8.3.5 CPU アクセスリストの設定例

ポート 1/0/1 ～ポート 1/0/3 で受信した IPv4 パケットにおいて、192.0.2.100 と 192.0.2.150 から送信された ICMP パケットのうち、CPU 宛てに中継されるトラフィックに対して、CPU 宛て中継を拒否する場合の設定例を示します。

- 拡張 IP CPU アクセスリスト［Example-DENY-ICMP］
- 送信元 IP アドレス［192.0.2.100］からの ICMP パケットの CPU 宛て中継を拒否
- 送信元 IP アドレス［192.0.2.150］からの ICMP パケットの CPU 宛て中継を拒否
- CPU アクセスリストを適用するポートは、ポート 1/0/1 からポート 1/0/3

1. 拡張 IP CPU アクセスリスト［Example-DENY-ICMP］を作成し、以下のルールを設定します。

ルール 10（cpu-deny）：ICMP プロトコル、送信元 IP アドレス［192.0.2.100］

ルール 20（cpu-deny）：ICMP プロトコル、送信元 IP アドレス［192.0.2.150］

```
sw1# configure terminal
sw1(config)# ip-cpu access-list extended Example-DENY-ICMP
sw1(config-ip-cpu-ext-acl)# 10 cpu-deny icmp host 192.0.2.100 any
sw1(config-ip-cpu-ext-acl)# 20 cpu-deny icmp host 192.0.2.150 any
sw1(config-ip-cpu-ext-acl)# exit
sw1(config)#
```

2. 設定した拡張 IP CPU アクセスリストをポート 1/0/1 からポート 1/0/3 に適用します。

```
sw1(config)# interface range port 1/0/1-3
sw1(config-if-port-range)# ip-cpu access-group Example-DENY-ICMP

The remaining applicable IP-CPU related access entries are 3070
sw1(config-if-port-range)# end
sw1#
```

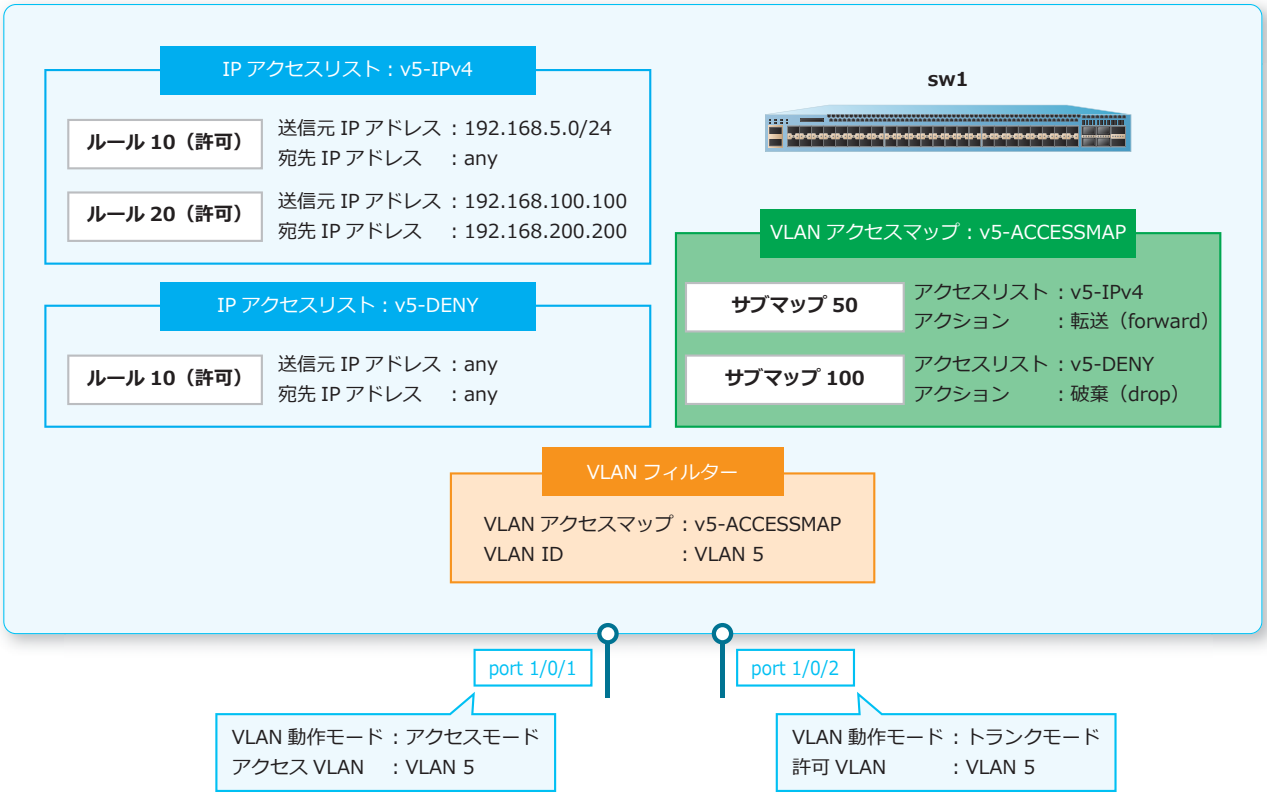
3. 実施後のアクセスリスト関連の設定を以下に抜粋します。

```
# ACL

ip-cpu access-list extended Example-DENY-ICMP 18999
 10 cpu-deny icmp host 192.0.2.100 any
 20 cpu-deny icmp host 192.0.2.150 any
interface port 1/0/1
 ip-cpu access-group Example-DENY-ICMP
interface port 1/0/2
 ip-cpu access-group Example-DENY-ICMP
interface port 1/0/3
 ip-cpu access-group Example-DENY-ICMP
```

8.3.6 VLAN アクセスマップの設定例

VLAN 5（ポート 1/0/1、ポート 1/0/2）で受信した IPv4 パケットにおいて、「192.168.5.0/24 から送信された IPv4 パケット」、および「192.168.100.100 から 192.168.200.200 へ送信された IPv4 パケット」のみを許可して、それ以外の IPv4 パケットを破棄する場合の構成例と設定例を示します。

図 8-24 VLAN アクセスマップの構成例



1. VLAN 5 を作成します。

```
sw1# configure terminal
sw1(config)# vlan 5
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 5］を割り当てます。

```
sw1(config)# interface port 1/0/1
sw1(config-if-port)# switchport access vlan 5
sw1(config-if-port)# exit
sw1(config)#
```

3. 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 5］を割り当てます。

```
sw1(config)# interface port1/0/2
sw1(config-if-port)# switchport mode trunk
sw1(config-if-port)# switchport trunk allowed vlan 5
sw1(config-if-port)# exit
sw1(config)#
```

4. IP アクセスリスト［v5-IPv4］を作成します。VLAN アクセスマップのフィルタリング対象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［192.168.5.0 0.0.0.255］、宛先 IP アドレス［any］

ルール 20（許可）：送信元 IP アドレス［192.168.100.100］、宛先 IP アドレス［192.168.200.200］

```
sw1(config)# ip access-list v5-IPv4
sw1(config-ip-acl)# 10 permit 192.168.5.0 0.0.0.255 any
sw1(config-ip-acl)# 20 permit host 192.168.100.100 host 192.168.200.200
sw1(config-ip-acl)# exit
sw1(config)#
```

5. IP アクセスリスト［v5-DENY］を作成します。VLAN アクセスマップのフィルタリング対象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［any］、宛先 IP アドレス［any］

```
sw1(config)# ip access-list v5-DENY
sw1(config-ip-acl)# 10 permit any any
sw1(config-ip-acl)# exit
sw1(config)#
```

6. VLAN アクセスマップ［v5-ACCESSMAP］のサブマップを以下のように設定します。

サブマップ 50：アクセスリスト［v5-IPv4］、アクション［forward］

サブマップ 100：アクセスリスト［v5-DENY］、アクション［drop］

```
sw1(config)# vlan access-map v5-ACCESSMAP 50
sw1(config-access-map)# match ip address v5-IPv4
sw1(config-access-map)# action forward
sw1(config-access-map)# exit
sw1(config)#
sw1(config)# vlan access-map v5-ACCESSMAP 100
sw1(config-access-map)# match ip address v5-DENY
sw1(config-access-map)# action drop
sw1(config-access-map)# exit
sw1(config)#
```

7. VLAN 5 に VLAN アクセスマップ［v5-ACCESSMAP］を適用します。

```
sw1(config)# vlan filter v5-ACCESSMAP vlan-list 5
sw1(config)# end
sw1#
```

9. トラフィックセグメンテーション（中継パス制限）

トラフィックセグメンテーションの機能、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。

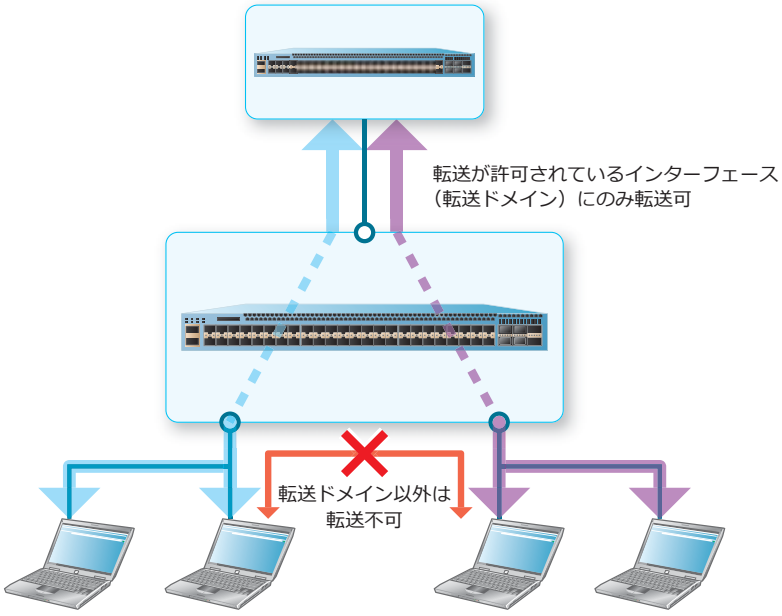
REF: コマンドの詳細については、『コマンドリファレンス』を参照してください。

9.1 トラフィックセグメンテーション（中継パス制限）の機能説明

トラフィックセグメンテーションは、1 つのインターフェースから、他のインターフェースのグループへのトラフィックの流れを制限する機能です。転送が許可されているインターフェースのことを、インターフェースの**転送ドメイン**と呼びます。

転送ドメインを設定するには、`traffic-segmentation forward` コマンドを使用します。

図 9-1 トラフィックセグメンテーションの概要



CAUTION: レイヤー 3 中継するトラフィックは、トラフィックセグメンテーション（中継パス制限）による転送先インターフェース制限の対象外で、トラフィックセグメンテーション（中継パス制限）の設定にかかわらずレイヤー 3 中継されます。

NOTE: 転送を許可する宛先インターフェースとしてポートチャネルを指定する場合は、そのポートチャネルのすべてのメンバーポートを指定してください。

転送が許可されるインターフェース

インターフェースの転送ドメインの設定の有無により、転送が許可されるインターフェースが異なります。

表 9-1 転送が許可されるインターフェース

インターフェースの転送ドメイン	概要
設定なし	すべてのインターフェースへの転送が許可されます。
設定あり	転送ドメインとして登録したインターフェースへの転送のみが許可されます。 それ以外のインターフェースへの転送は制限されます。

9.2 トラフィックセグメンテーション（中継パス制限）の状態確認

show traffic-segmentation forward コマンドで、転送ドメインの設定を確認できます。

表示例を以下に示します。

```
# show traffic-segmentation forward
(1)                (2)
Interface          Forwarding Domain
---------------    ------------------------------------------------------------
Port1/0/1          Port1/0/2-1/0/5,1/0/11-1/0/12
Port-channel40     Port1/0/6-1/0/12

Total Entries: 2
```

各項目の説明は、以下のとおりです。

表 9-2 show traffic-segmentation forward コマンドの表示項目

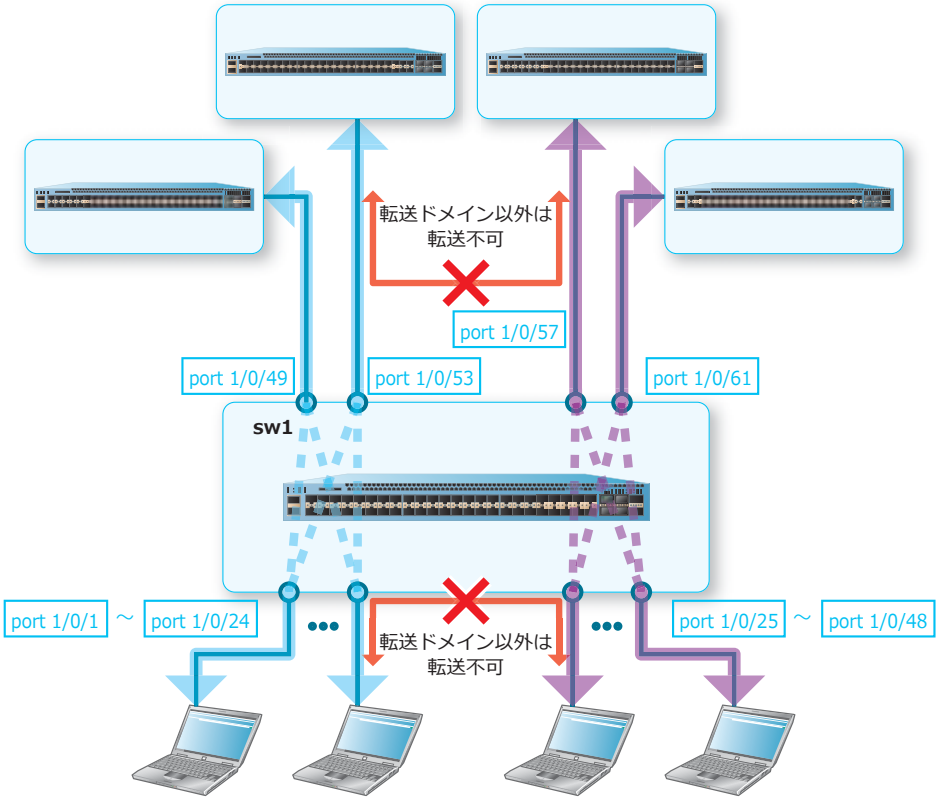
項番	説明
(1)	ポート番号またはポートチャネル番号を表示します。
(2)	受信したフレームの転送を許可するインターフェース（転送ドメイン）を表示します。

9.3 トラフィックセグメンテーション（中継パス制限）の構成例と設定例

以下のように転送先を制限する、トラフィックセグメンテーションの構成例と設定例を示します。

- ポート 1/0/1 からポート 1/0/24、ポート 1/0/49、およびポート 1/0/53 で受信したトラフィックを、「ポート 1/0/1 からポート 1/0/24、ポート 1/0/49、およびポート 1/0/53」にのみ転送を許可する
- ポート 1/0/25 からポート 1/0/48、ポート 1/0/57、およびポート 1/0/61 で受信したトラフィックを、「ポート 1/0/25 からポート 1/0/48、ポート 1/0/57、およびポート 1/0/61」にのみ転送を許可する

図 9-2 トラフィックセグメンテーションの構成例



1. ポート 1/0/1 からポート 1/0/24、ポート 1/0/49、およびポート 1/0/53 において、受信したフレームの転送を許可するインターフェースを［ポート 1/0/1 からポート 1/0/24、ポート 1/0/49、およびポート 1/0/53］に設定します。

```
sw1# configure terminal
sw1(config)# interface range port 1/0/1-24,1/0/49,1/0/53
sw1(config-if-port-range)# traffic-segmentation forward interface range port
1/0/1-24,1/0/49,1/0/53
sw1(config-if-port-range)# exit
sw1(config)#
```

2. ポート 1/0/25 からポート 1/0/48、ポート 1/0/57、およびポート 1/0/61 において、受信したフレームの転送を許可するインターフェースを［ポート 1/0/25 からポート 1/0/48、ポート 1/0/57、およびポート 1/0/61］に設定します。

```
sw1(config)# interface range port 1/0/25-48,1/0/57,1/0/61
sw1(config-if-port-range)# traffic-segmentation forward interface range port
1/0/25-48,1/0/57,1/0/61
sw1(config-if-port-range)# end
sw1#
```

10. リングプロテクション（ERPS）

リングプロテクション（ERPS）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 ERPS の機能説明

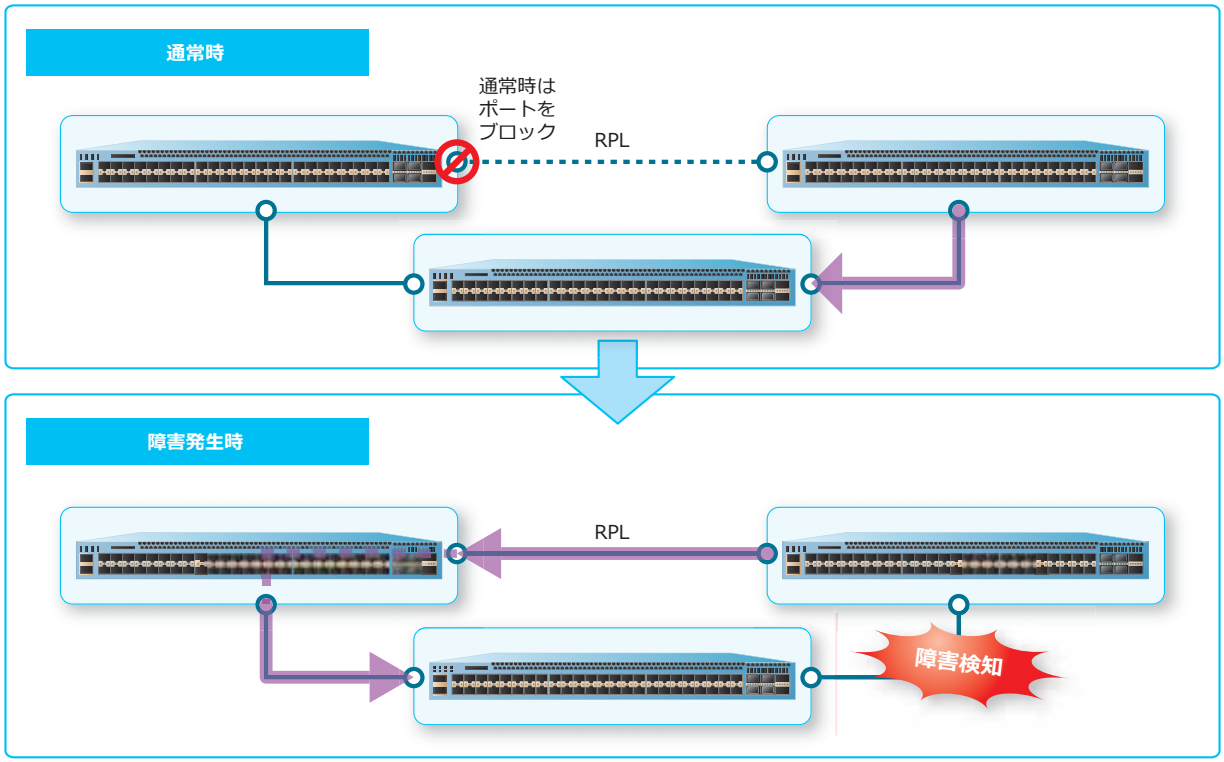
リングプロテクション（以後、ERPS）は、リングトポロジー構成のレイヤー 2 冗長プロトコルです。装置は、ITU-T G.8032 ERPS（Ethernet Ring Protection Switching）に準拠しています。

ERPS では、リング内の 1 つのリンクを **RPL**（Ring Protection Link）として設定します。通常時は、ループを回避するために RPL はパケット転送用リンクとして使用されません。ネットワーク上で障害を検知したときは、RPL を使用してパケットを転送します。

CAUTION: ERPS 機能は、同一装置で STP/RSTP/MSTP/RPVST+ 機能、MMRP-Plus 機能と併用できません。

CAUTION: ERPS 機能は、同一インターフェースでループ検知機能（loop-detection action notify-only 設定時を除く）、ポートリダンダント機能と併用できません。

図 10-1 ERPS の概要



G.8032 物理リング

ERPS 機能では **G.8032 物理リング**（以後、**リング**）を構成するために物理的なリングを作成し、リングポートおよび ERP インスタンスを設定します。なお、リングは、**ethernet ring g8032** コマンドで作成します。

NOTE: 作成可能なリングの最大数は 14 個です。

• リングポート

リングで使用するポートを装置ごとに 2 つずつ設定します。リングポートは、**port0** コマンドおよび **port1** コマンドで設定します。

• ERP インスタンス

リングで保護する VLAN などの情報をまとめるために ERP インスタンスを作成し、以下の項目を設定します。（）内は使用するコマンドです。なお、ERP インスタンスは、**instance** コマンドで作成し、**activate** コマンドで有効化します。

- トラフィックを保護する VLAN（**inclusion-list vlan-ids** コマンド）
- VLAN を保護する際に RPL として使用するリンク（**rpl** コマンド）
- R-APS メッセージを送受信するための VLAN（**r-aps channel-vlan** コマンド）
- ERP インスタンスのリング MEL 値（管理レベル）（**level** コマンド）
- ERP インスタンスの説明（**description** コマンド）
- 各種タイマーを設定するプロファイル（**ethernet ring g8032 profile** コマンドで作成、**profile** コマンドで ERP インスタンスに登録）

NOTE: ERP インスタンスは 1 リングに 1 個までのサポートとなります。

NOTE: CFM 機能と併用する場合は、リング MEL 値（管理レベル）を CFM のドメインレベルより高く設定してください。

G.8032 プロファイル

G.8032 プロファイル（以後、**プロファイル**）は、以下のタイマーを設定するために作成します。プロファイルは、**ethernet ring g8032 profile** コマンドで作成し、**profile** コマンドで ERP インスタンスに登録します。各種タイマーは、**timer** コマンドで作成します。

NOTE: 作成可能なプロファイルの最大数は 8 個です。

• ガードタイマー

さまざまな R-APS メッセージを連続して受信したときに、連続した状態変化を発生させないために設定します。500 ミリ秒に設定した場合は、初めの R-APS メッセージを受信してから 500 ミリ秒間は、その他の状態変更メッセージが無視されます。

• ホールドオフタイマー

障害を検知してから、RPL が有効になるまでの時間を設定します。断続的に障害が検知されるネットワークの場合に設定すると、ERPS 機能による状態変化を回避できます。5 秒に設定した場合は、障害を検知してから 5 秒後に RPL が有効になります。

• WTR タイマー

切り戻し機能を有効にした場合に、切り戻しを保留にする時間を設定します。切り戻し機能は、障害が発生したリンクが復旧してから、RPL の使用を終了して通常の状態に自動的に戻す機能です。5 分に設定した場合は、リンクが復旧してから 5 分間は、通常の状態に自動的に戻ることはありません。切り戻し機能は、**revertive** コマンドを使用して有効／無効を設定できます。

10.1.1 R-APS メッセージ

R-APS メッセージは、ERPS 機能における状態の変化を装置に通知するためのメッセージです。ネットワーク上で障害を検知したときや、障害が発生したリンクが復旧したときに、送信されます。

R-APS メッセージを送受信するための VLAN を、**R-APS チャネル VLAN** と呼びます。

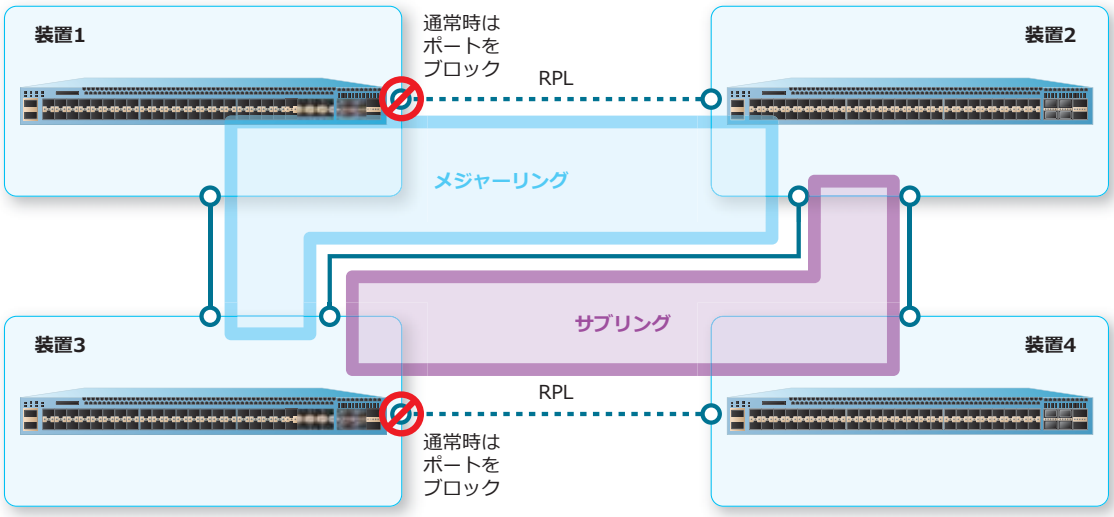
10.1.2 サブリング

装置を 2 つのリングトポロジーで接続した場合、一方のリングを**メジャーリング**、他方を**サブリング**と呼びます。サブリングは、メジャーリングを構成する 2 つのノードとその間のリンクを含みます。下図の場合は装置 1 ～ 3 で構成するリングをメジャーリング、装置 2 ～ 4 で構成するリングをサブリングと呼びます。

NOTE: メジャーリングとサブリングが共用するリンクを接続するポートは、メジャーリングのリングポートとして設定してください。なお、リングポートとして設定したポートは、サブリングのリングポートとしては設定できません。

NOTE: メジャーリングとサブリングが共用するリンクにおいて障害が検知された場合は、メジャーリングの RPL が転送用リンクとして使用されます。

図 10-2 サブリングの概要



サブリングは、**sub-ring** コマンドで設定します。また、サブリングのトポロジーが変更された場合に、メジャーリングにトポロジー変更通知（TCN）を伝達するには、**tcn-propagation** コマンドを使用します。

10.2 ERPS の状態確認

ERPS の状態を表示して確認する方法を説明します。

10.2.1 ERPS の概要情報の表示

show ethernet ring g8032 brief コマンドで、ERPS の概要情報を確認できます。

表示例を以下に示します。

```
# show ethernet ring g8032 brief

ERPS Version : G.8032v1 ...(1)
(2)                              (3)      (4)          (5)
Ring                             InstID   Status       Port-State
-----                            ----     -----        -------
RING1                            1        Idle         p0:Port1/0/5,Blocking(RPL)
                                                       p1:Port1/0/9,Forwarding
SUB-RING5                        2        Idle         p0:Port1/0/3,Forwarding
                                                       p1:-,Forwarding
Total Entries: 2
```

各項目の説明は、以下のとおりです。

表 10-1 show ethernet ring g8032 brief コマンドの表示項目

項番	説明
(1)	リングプロテクション（ERPS）の対応バージョンを表示します。
(2)	リング名を表示します。
(3)	ERP インスタンスのインスタンス ID を表示します。
(4)	リングノードの状態を表示します。 • Deactivated：非アクティブ状態 • Idle：標準状態（RPL ポートが閉塞状態） • Protection：リング上で障害が発生して切り替わっている状態（RPL ポートが開放状態）
(5)	リングポート（port0、port1）の状態を表示します。PRL ポートの場合は状態の後に (RPL) と表示されます。 • Forwarding：中継可能な状態 • Blocking：中継を抑止している状態（リンクアップ時） • SF blocked：対象リングポートがダウン状態

10.2.2 ERPS の詳細情報の表示

show ethernet ring g8032 status コマンドで、ERPS の詳細情報を確認できます。

表示例を以下に示します。

```
# show ethernet ring g8032 status

 ERPS Version: G.8032v1 ...(1)
 ----------------------------
 Ethernet Ring RING1 ...(2)
 Admin Port0: Port1/0/5 ...(3)
 Admin Port1: Port1/0/9 ...(3)
 ----------------------------
 Instance  : 1 ...(4)
 Instance Status: Idle ...(5)
 (6)                   (7)
 R-APS Channel : 4001,Protected VLANs:10,20
 Port0: Port1/0/5, Blocking ...(8)
 Port1: Port1/0/9, Forwarding ...(8)
 Profile: TEST ...(9)
 Description : TEST-RING-1 ...(10)
 Guard Timer: 500 milliseconds ...(11)
 Hold-off Timer: 0 milliseconds ...(12)
 WTR Timer: 5 minutes ...(13)
 Revertive ...(14)
 MEL: 1 ...(15)
 RPL Role: Owner ...(16)
 RPL Port: Port0 ...(17)
 (18)                    (19)
 Sub Ring Instance : 2, TC Propagation State: Enabled

 ----------------------------
 Ethernet Ring SUB-RING5 ...(2)
 Admin Port0: Port1/0/3 ...(3)
 Admin Port1: virtual_channel ...(3)
 ----------------------------
 Instance  : 2 ...(4)
 Instance Status: Idle ...(5)
 (6)                   (7)
 R-APS Channel : 4005,Protected VLANs:10,20
 Port0: Port1/0/3, Forwarding ...(8)
 Port1: virtual_channel, Forwarding ...(8)
 Profile: TEST ...(9)
 Description : TEST-SUB-RING-5 ...(10)
 Guard Timer: 500 milliseconds ...(11)
 Hold-off Timer: 0 milliseconds ...(12)
 WTR Timer: 5 minutes ...(13)
 Revertive ...(14)
 MEL: 1 ...(15)
 RPL Role: None ...(16)
 RPL Port: - ...(17)
 Sub Ring Instance: none ...(18)
```

各項目の説明は、以下のとおりです。

表 10-2 show ethernet ring g8032 status コマンドの表示項目

項番	説明
(1)	リングプロテクション（ERPS）の対応バージョンを表示します。
(2)	リング名を表示します。

項番	説明
(3)	リングポート（port0、port1）として使用するポート番号またはポートチャネル番号を表示します。 port1 を none 指定で設定した場合は virtual_channel と表示されます。
(4)	ERP インスタンスのインスタンス ID を表示します。
(5)	リングノードの状態を表示します。 • Deactivated：非アクティブ状態 • Idle：標準状態（RPL ポートが閉塞状態） • Protection：リング上で障害が発生して切り替わっている状態（RPL ポートが開放状態）
(6)	R-APS メッセージを送受信する R-APS チャネル VLAN を表示します。
(7)	保護している VLAN を表示します。
(8)	リングポート（port0、port1）の状態を表示します。 • Forwarding：中継可能な状態 • Blocking：中継を抑止している状態（リンクアップ時） • SF blocked：対象リングポートがダウン状態
(9)	関連付けられたプロファイル名を表示します。
(10)	対象 ERP インスタンスの説明を表示します。
(11)	ガードタイマーのタイマー値を表示します。
(12)	ホールドオフタイマーのタイマー値を表示します。
(13)	WTR タイマーのタイマー値を表示します。
(14)	切り戻し機能の有効 (Revertive) ／無効 (Non-revertive) を表示します。
(15)	対象 ERP インスタンスのリング MEL 値（管理レベル）を表示します。
(16)	RPL オーナーの場合は Owner と表示されます。それ以外の場合は None と表示されます。
(17)	RPL ポートとして設定されているリングポートを表示します。
(18)	サブリングを設定している場合に、サブリングの ERP インスタンスを表示します。サブリングを設定していない場合は none と表示されます。
(19)	サブリングを設定している場合に、トポロジー変更通知の有効 (Enabled) ／無効 (Disabled) を表示します。

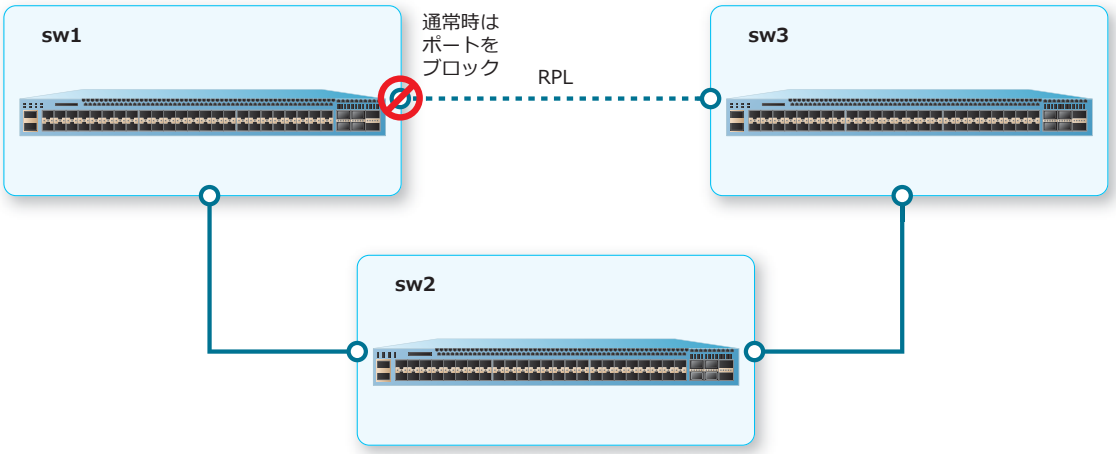
10.3 ERPS の構成例と設定例

ERPS を利用する場合の構成例と設定例を示します。

10.3.1 メジャーリングのみの場合

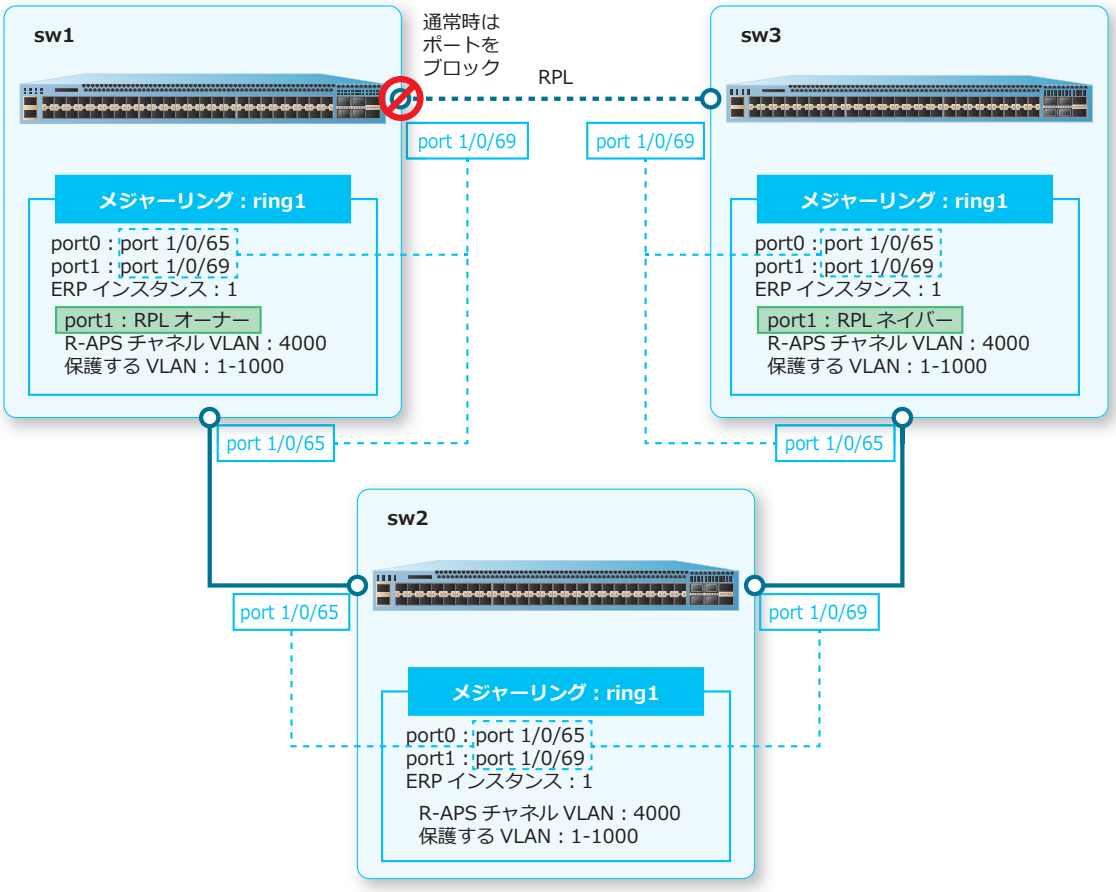
3 台の装置をリングトポロジーで接続し、ERP インスタンスを有効化する場合の構成例と設定例を示します。

図 10-3 メジャーリングのみの場合の構成例



10.3.1.1 RPL オーナーの設定例（sw1）

図 10-4 RPL オーナーの設定例（sw1）



1. VLAN 1 から VLAN 1000、および VLAN 4000 を作成します。

```
sw1# configure terminal
sw1(config)# vlan 1-1000,4000
sw1(config-vlan)# exit
sw1(config)#
```

2. ポート 1/0/65 およびポート 1/0/69 をトランクポートとして設定し、トランクポートにすべての VLAN を割り当てます。

```
sw1(config)# interface range port 1/0/65,1/0/69
sw1(config-if-port-range)# switchport mode trunk
sw1(config-if-port-range)# exit
sw1(config)#
```

3. リング［ring1］を作成し、port0 を［ポート 1/0/65］に、port1 を［ポート 1/0/69］に設定します。

```
sw1(config)# ethernet ring g8032 ring1
sw1(config-erps-ring)# port0 interface port 1/0/65
sw1(config-erps-ring)# port1 interface port 1/0/69
sw1(config-erps-ring)#
```

4. リング［ring1］に ERP インスタンス［1］を作成し、ERPS インスタンス設定モードに遷移します。

```
sw1(config-erps-ring)# instance 1
sw1(config-erps-ring-instance)#
```

5. sw1 を RPL オーナーとして、port1 を RPL ポートに設定します。

```
sw1(config-erps-ring-instance)# rpl port1 owner
sw1(config-erps-ring-instance)#
```

6. R-APS チャネル VLAN を［VLAN 4000］に、保護する VLAN を［VLAN 1 から VLAN 1000］に設定します。

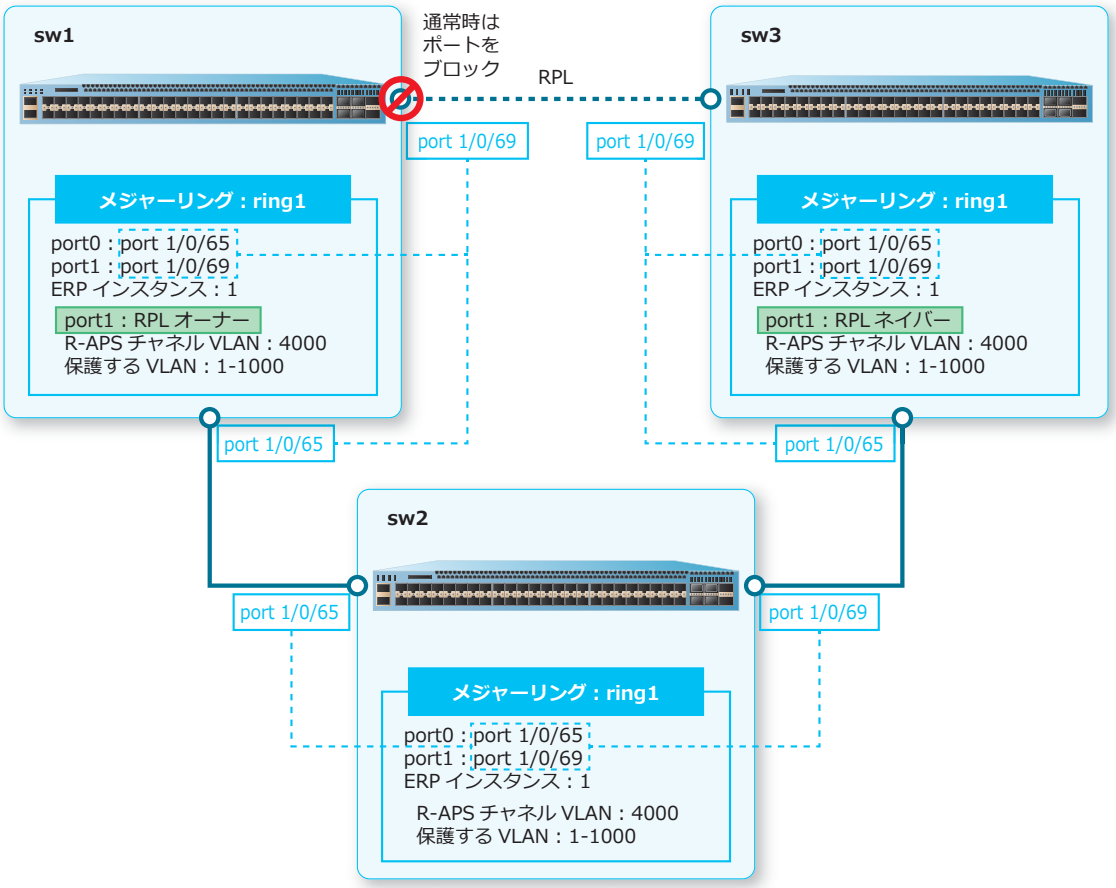
```
sw1(config-erps-ring-instance)# r-aps channel-vlan 4000
sw1(config-erps-ring-instance)# inclusion-list vlan-ids 1-1000
sw1(config-erps-ring-instance)#
```

7. ERP インスタンス［1］を有効化します。

```
sw1(config-erps-ring-instance)# activate
sw1(config-erps-ring-instance)# end
sw1#
```

10.3.1.2 リングを構成する装置の設定例（sw2）

図 10-5 リングを構成する装置の設定例（sw2）



1. VLAN 1 から VLAN 1000、および VLAN 4000 を作成します。

```
sw2# configure terminal
sw2(config)# vlan 1-1000,4000
sw2(config-vlan)# exit
sw2(config)#
```

2. ポート 1/0/65 およびポート 1/0/69 をトランクポートとして設定し、トランクポートにすべての VLAN を割り当てます。

```
sw2(config)# interface range port 1/0/65,1/0/69
sw2(config-if-port-range)# switchport mode trunk
sw2(config-if-port-range)# exit
sw2(config)#
```

3. リング［ring1］を作成し、port0 を［ポート 1/0/65］に、port1 を［ポート 1/0/69］に設定します。

```
sw2(config)# ethernet ring g8032 ring1
sw2(config-erps-ring)# port0 interface port 1/0/65
sw2(config-erps-ring)# port1 interface port 1/0/69
sw2(config-erps-ring)#
```

4. リング［ring1］に ERP インスタンス［1］を作成し、ERPS インスタンス設定モードに遷移します。

```
sw2(config-erps-ring)# instance 1
sw2(config-erps-ring-instance)#
```

5. R-APS チャネル VLAN を［VLAN 4000］に、保護する VLAN を［VLAN 1 から VLAN 1000］に設定します。

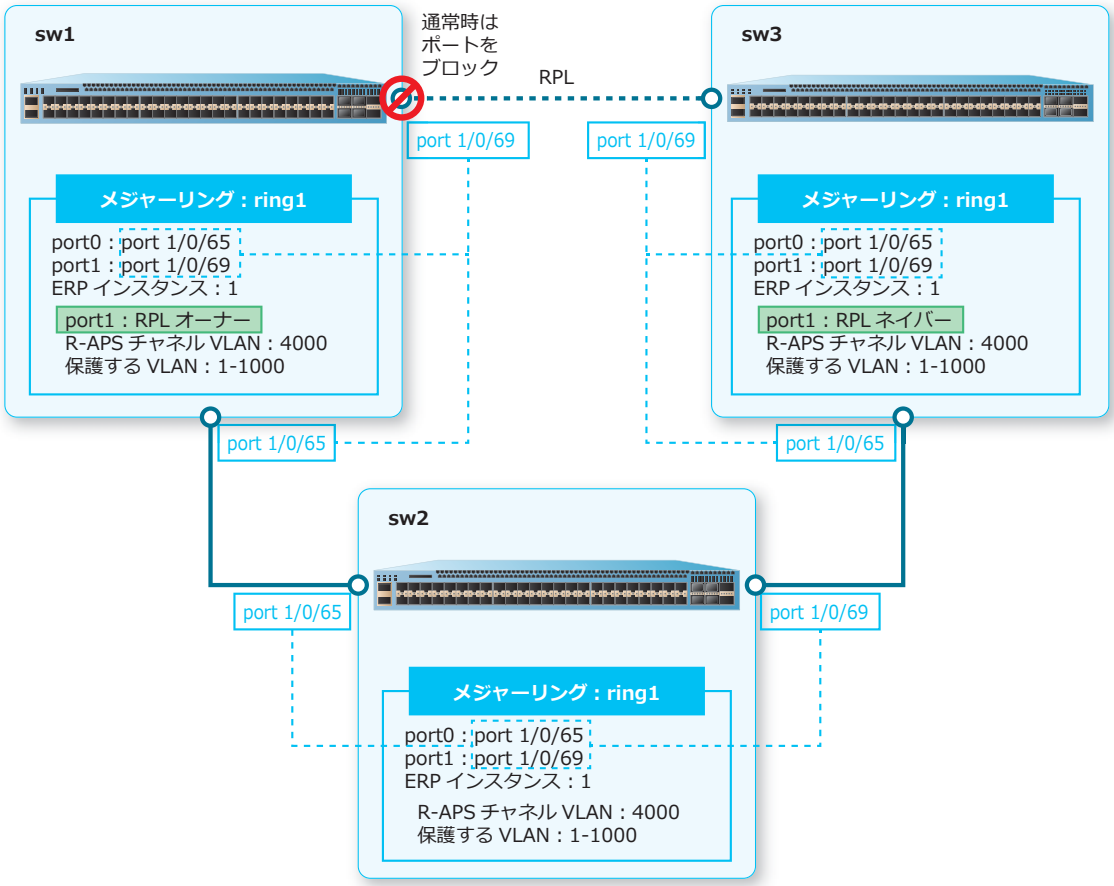
```
sw2(config-erps-ring-instance)# r-aps channel-vlan 4000
sw2(config-erps-ring-instance)# inclusion-list vlan-ids 1-1000
sw2(config-erps-ring-instance)#
```

6. ERP インスタンス［1］を有効化します。

```
sw2(config-erps-ring-instance)# activate
sw2(config-erps-ring-instance)# end
sw2#
```

10.3.1.3 RPL ネイバーの設定例（sw3）

図 10-6 RPL ネイバーの設定例（sw3）



1. VLAN 1 から VLAN 1000、および VLAN 4000 を作成します。

```
sw3# configure terminal
sw3(config)# vlan 1-1000,4000
sw3(config-vlan)# exit
sw3(config)#
```

2. ポート 1/0/65 およびポート 1/0/69 をトランクポートとして設定し、トランクポートにすべての VLAN を割り当てます。

```
sw3(config)# interface range port 1/0/65,1/0/69
sw3(config-if-port-range)# switchport mode trunk
sw3(config-if-port-range)# exit
sw3(config)#
```

3. リング［ring1］を作成し、port0 を［ポート 1/0/65］に、port1 を［ポート 1/0/69］を設定します。

```
sw3(config)# ethernet ring g8032 ring1
sw3(config-erps-ring)# port0 interface port 1/0/65
sw3(config-erps-ring)# port1 interface port 1/0/69
sw3(config-erps-ring)#
```

4. リング［ring1］に ERP インスタンス［1］を作成し、ERPS インスタンス設定モードに遷移します。

```
sw3(config-erps-ring)# instance 1
sw3(config-erps-ring-instance)#
```

5. sw3 を RPL ネイバーとして、port1 を RPL ポートに設定します。

```
sw3(config-erps-ring-instance)# rpl port1
sw3(config-erps-ring-instance)#
```

6. R-APS チャネル VLAN を［VLAN 4000］に、保護する VLAN を［VLAN 1 から VLAN 1000］に設定します。

```
sw3(config-erps-ring-instance)# r-aps channel-vlan 4000
sw3(config-erps-ring-instance)# inclusion-list vlan-ids 1-1000
sw3(config-erps-ring-instance)#
```

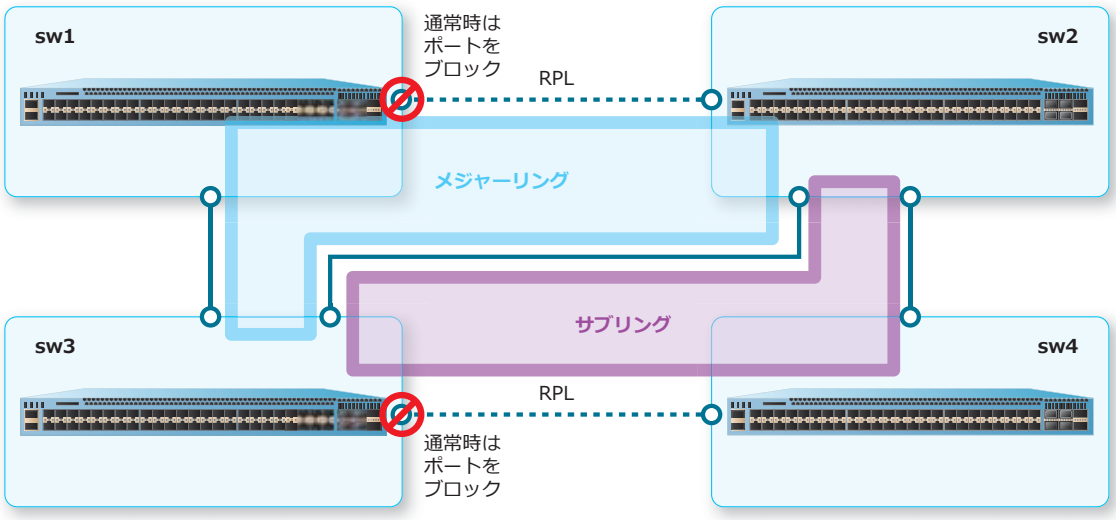
7. ERP インスタンス［1］を有効化します。

```
sw3(config-erps-ring-instance)# activate
sw3(config-erps-ring-instance)# end
sw3#
```

10.3.2 サブリングを作成する場合

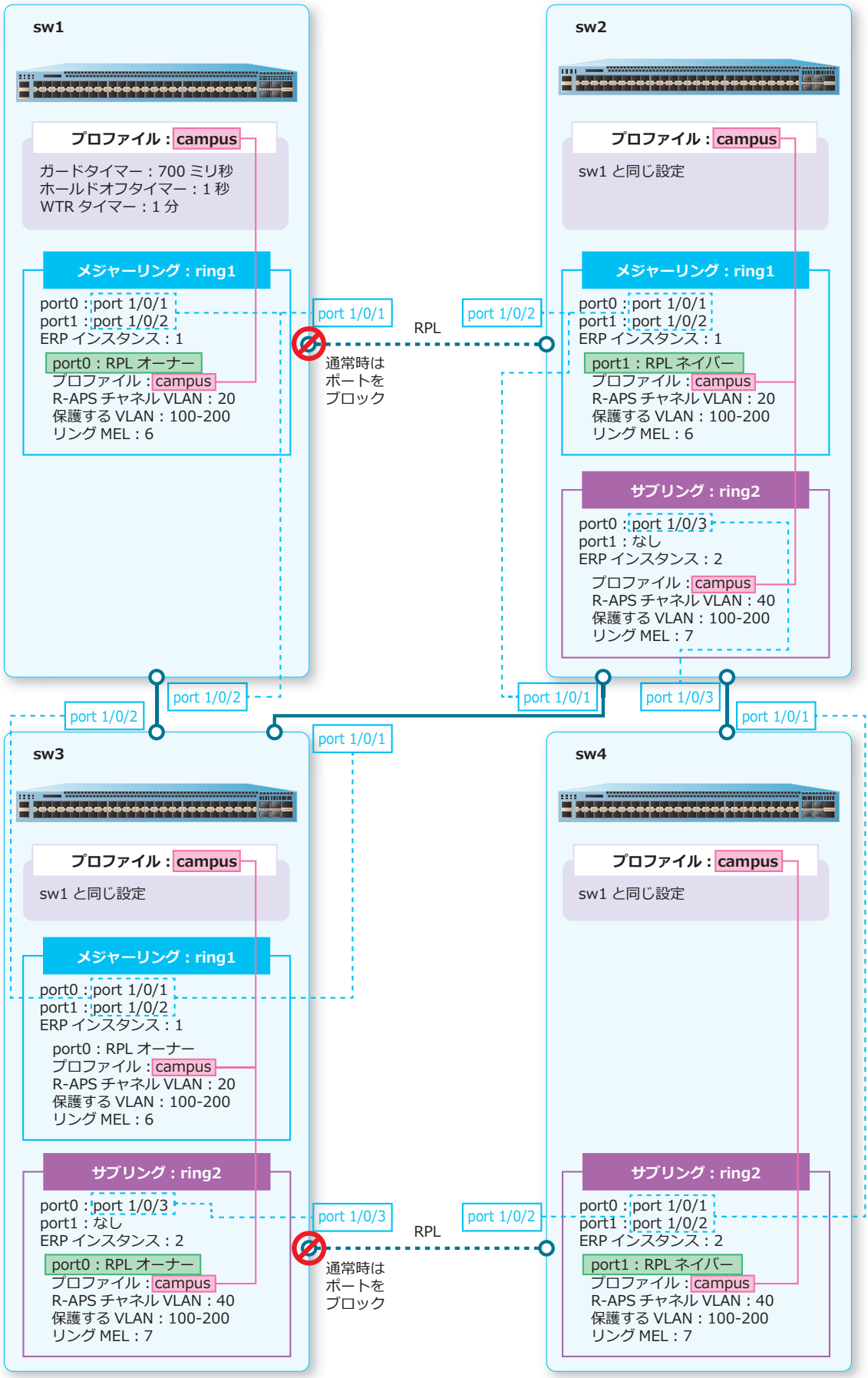
4 台の装置を 2 つのリングトポロジーで接続し、2 つの ERP インスタンスを有効化する場合の構成例と設定例を示します。2 つのリングトポロジーで接続する場合、一方のリングをメジャーリング、他方をサブリングと呼びます。サブリングは、メジャーリングを構成する 2 つのノードとその間のリンクを含みます。メジャーリングとサブリングが共用するリンクにおいて障害が検知された場合は、メジャーリングの RPL が転送用リンクとして使用されます。

図 10-7 サブリングを作成する場合の構成例



10.3.2.1 メジャーリングの RPL オーナーの設定例（sw1）

図 10-8 メジャーリングの RPL オーナーの設定例（sw1）



1. VLAN 20、および VLAN 100 から VLAN 200 を作成します。

```
sw1# configure terminal
sw1(config)# vlan 20,100-200
sw1(config-vlan)# exit
sw1(config)#
```

2. ポート 1/0/1 からポート 1/0/2 をトランクポートとして設定し、トランクポートにすべての VLAN を割り当てます。

```
sw1(config)# interface range port 1/0/1-2
sw1(config-if-port-range)# switchport mode trunk
sw1(config-if-port-range)# exit
sw1(config)#
```

3. プロファイル［campus］を作成し、ガードタイマーを［700 ミリ秒］に、ホールドオフタイマーを［1 秒］に、WTR タイマーを［1 分］に設定します。

```
sw1(config)# ethernet ring g8032 profile campus
sw1(config-erps-ring-profile)# timer guard 700
sw1(config-erps-ring-profile)# timer hold-off 1
sw1(config-erps-ring-profile)# timer wtr 1
sw1(config-erps-ring-profile)# exit
sw1(config)#
```

4. リング［ring1］を作成し、port0 を［ポート 1/0/1］に、port1 を［ポート 1/0/2］に設定します。

```
sw1(config)# ethernet ring g8032 ring1
sw1(config-erps-ring)# port0 interface port 1/0/1
sw1(config-erps-ring)# port1 interface port 1/0/2
sw1(config-erps-ring)#
```

5. リング［ring1］に ERP インスタンス［1］を作成し、ERPS インスタンス設定モードに遷移します。

```
sw1(config-erps-ring)# instance 1
sw1(config-erps-ring-instance)#
```

6. sw1 を RPL オーナーとして、port0 を RPL ポートに設定します。

```
sw1(config-erps-ring-instance)# rpl port0 owner
sw1(config-erps-ring-instance)#
```

7. ERP インスタンス［1］にプロファイル［campus］を関連付け、R-APS チャネル VLAN を［VLAN 20］に、保護する VLAN を［VLAN 100 から VLAN 200］に設定します。

```
sw1(config-erps-ring-instance)# profile campus
sw1(config-erps-ring-instance)# r-aps channel-vlan 20
sw1(config-erps-ring-instance)# inclusion-list vlan-ids 100-200
sw1(config-erps-ring-instance)#
```

8. リング MEL 値（管理レベル）を［6］に設定します。

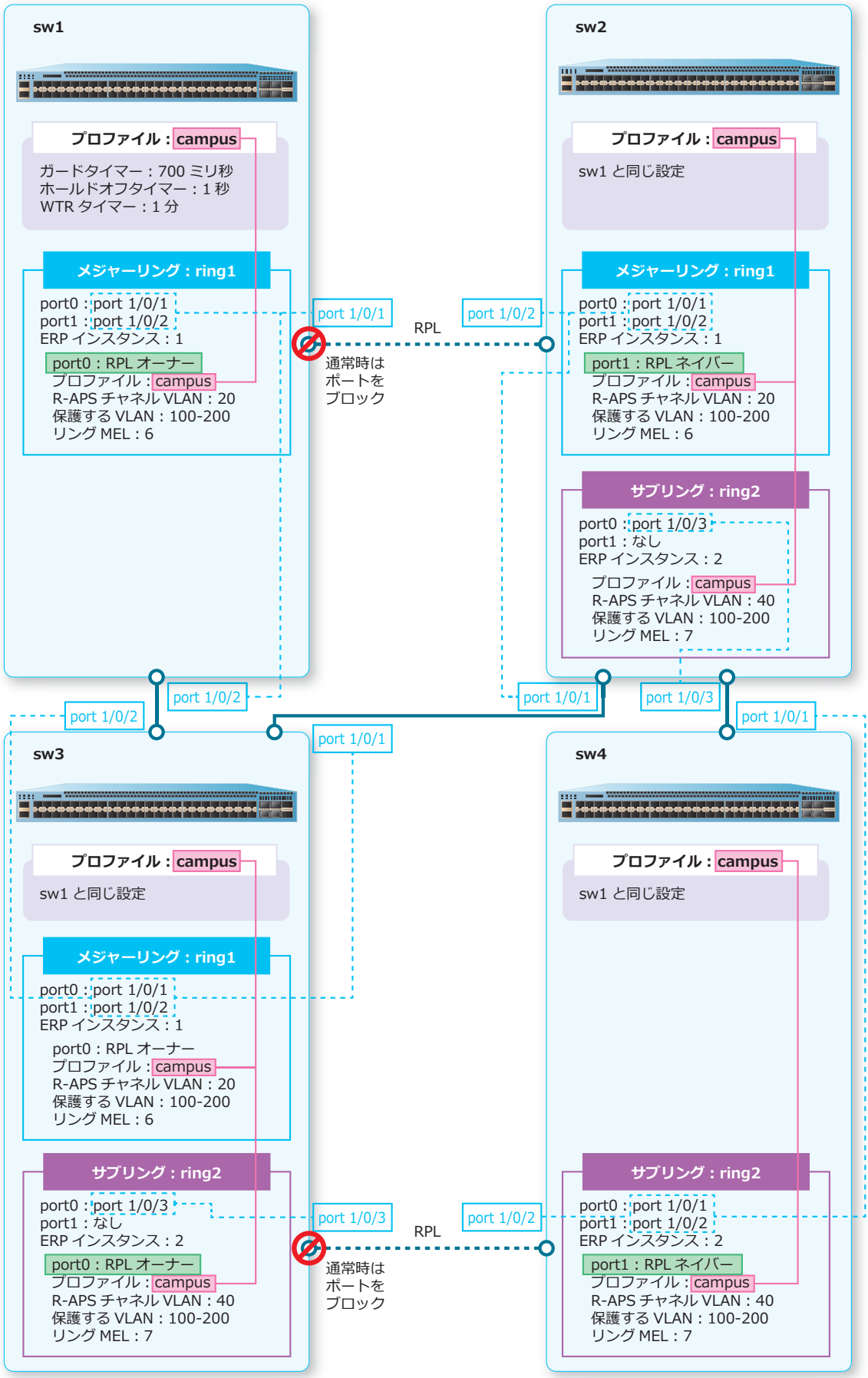
```
sw1(config-erps-ring-instance)# level 6
sw1(config-erps-ring-instance)#
```

9. ERP インスタンス［1］を有効化します。

```
sw1(config-erps-ring-instance)# activate
sw1(config-erps-ring-instance)# end
sw1#
```

10.3.2.2 メジャーリングの RPL ネイバーの設定例（sw2）

図 10-9 メジャーリングの RPL ネイバーの設定例（sw2）



1. VLAN 20、VLAN 40、および VLAN 100 から VLAN 200 を作成します。

```
sw2# configure terminal
sw2(config)# vlan 20,40,100-200
sw2(config-vlan)# exit
sw2(config)#
```

2. ポート 1/0/1 からポート 1/0/3 をトランクポートとして設定し、トランクポートにすべての VLAN を割り当てます。

```
sw2(config)# interface range port 1/0/1-3
sw2(config-if-port-range)# switchport mode trunk
sw2(config-if-port-range)# exit
sw2(config)#
```

3. プロファイル［campus］を作成し、ガードタイマーを［700 ミリ秒］に、ホールドオフタイマーを［1 秒］に、WTR タイマーを［1 分］に設定します。

```
sw2(config)# ethernet ring g8032 profile campus
sw2(config-erps-ring-profile)# timer guard 700
sw2(config-erps-ring-profile)# timer hold-off 1
sw2(config-erps-ring-profile)# timer wtr 1
sw2(config-erps-ring-profile)# exit
sw2(config)#
```

4. リング［ring1］を作成し、port0 を［ポート 1/0/1］に、port1 を［ポート 1/0/2］に設定します。

```
sw2(config)# ethernet ring g8032 ring1
sw2(config-erps-ring)# port0 interface port 1/0/1
sw2(config-erps-ring)# port1 interface port 1/0/2
sw2(config-erps-ring)#
```

5. リング［ring1］に ERP インスタンス［1］を作成し、ERPS インスタンス設定モードに遷移します。

```
sw2(config-erps-ring)# instance 1
sw2(config-erps-ring-instance)#
```

6. sw2 を RPL ネイバーとして、port1 を RPL ポートに設定します。

```
sw2(config-erps-ring-instance)# rpl port1
sw2(config-erps-ring-instance)#
```

7. ERP インスタンス［1］にプロファイル［campus］を関連付け、R-APS チャネル VLAN を［VLAN 20］に、保護する VLAN を［VLAN 100 から VLAN 200］に設定します。

```
sw2(config-erps-ring-instance)# profile campus
sw2(config-erps-ring-instance)# r-aps channel-vlan 20
sw2(config-erps-ring-instance)# inclusion-list vlan-ids 100-200
sw2(config-erps-ring-instance)#
```

8. リング MEL 値（管理レベル）を［6］に設定します。

```
sw2(config-erps-ring-instance)# level 6
sw2(config-erps-ring-instance)#
```

9. ERP インスタンス［1］を有効化します。

```
sw2(config-erps-ring-instance)# activate
sw2(config-erps-ring-instance)# exit
sw2(config-erps-ring)# exit
sw2(config)#
```

10. リング［ring2］を作成し、port0 を［ポート 1/0/3］に、port1 を［なし］に設定します。

```
sw2(config)# ethernet ring g8032 ring2
sw2(config-erps-ring)# port0 interface port 1/0/3
sw2(config-erps-ring)# port1 none
sw2(config-erps-ring)#
```

11. リング［ring2］に ERP インスタンス［2］を作成し、ERPS インスタンス設定モードに遷移します。

```
sw2(config-erps-ring)# instance 2
sw2(config-erps-ring-instance)#
```

12. ERP インスタンス［2］にプロファイル［campus］を関連付け、R-APS チャネル VLAN を［VLAN 40］に、保護する VLAN を［VLAN 100 から VLAN 200］に設定します。

```
sw2(config-erps-ring-instance)# profile campus
sw2(config-erps-ring-instance)# r-aps channel-vlan 40
sw2(config-erps-ring-instance)# inclusion-list vlan-ids 100-200
sw2(config-erps-ring-instance)#
```

13. リング MEL 値（管理レベル）を［7］に設定し、一度 ERP インスタンス［2］の設定を終了します。

```
sw2(config-erps-ring-instance)# level 7
sw2(config-erps-ring-instance)# exit
sw2(config-erps-ring)# exit
sw2(config)#
```

14. リング［ring1］にリング［ring2］をサブリングとして設定します。

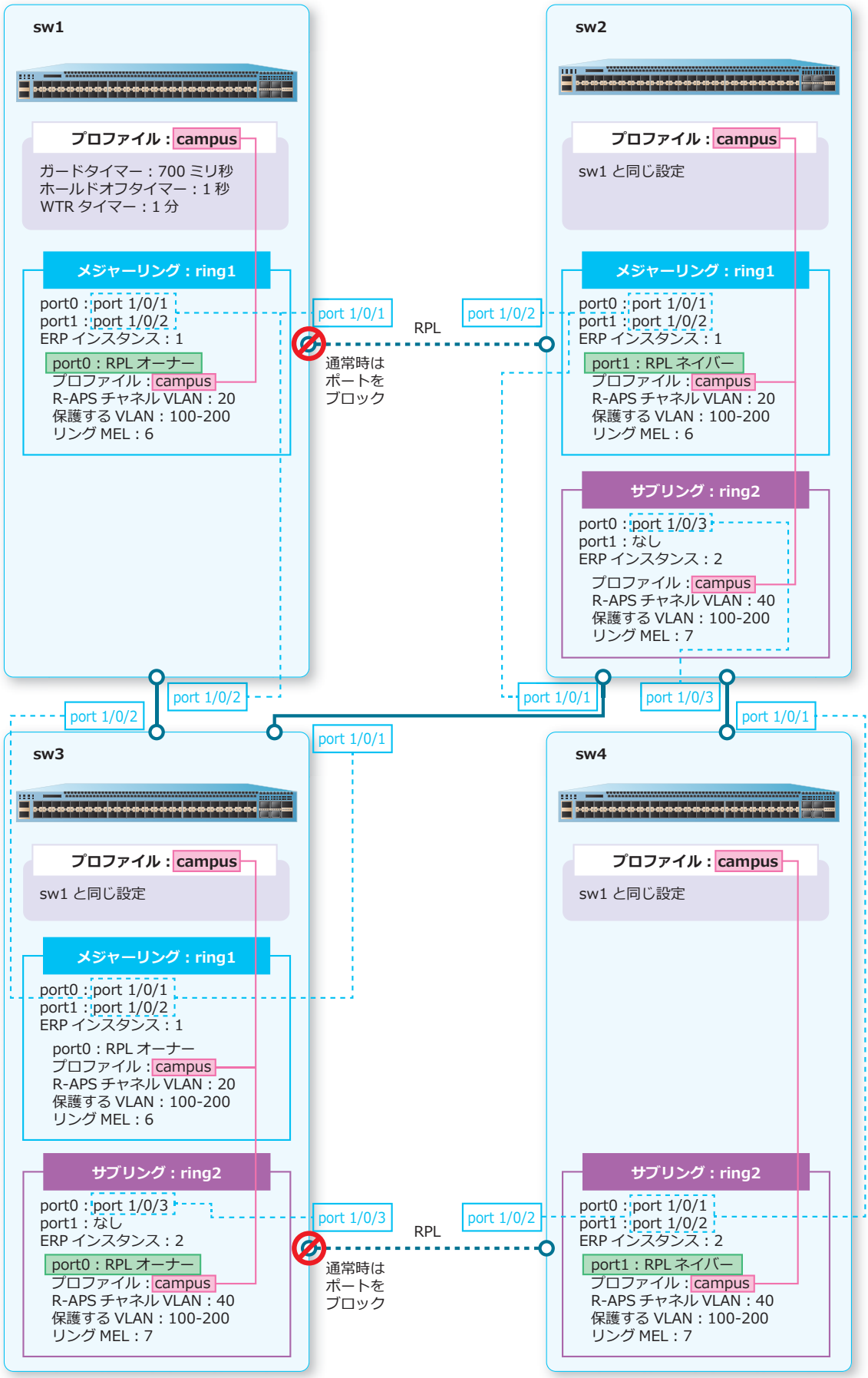
```
sw2(config)# ethernet ring g8032 ring1
sw2(config-erps-ring)# sub-ring ring2
sw2(config-erps-ring)# exit
sw2(config)#
```

15. ERP インスタンス［2］を有効化します。

```
sw2(config)# ethernet ring g8032 ring2
sw2(config-erps-ring)# instance 2
sw2(config-erps-ring-instance)# activate
sw2(config-erps-ring-instance)# end
sw2#
```

10.3.2.3 サブリングの RPL オーナーの設定例（sw3）

図 10-10 サブリングの RPL オーナーの設定例（sw3）



1. VLAN 20、VLAN 40、および VLAN 100 から VLAN 200 を作成します。

```
sw3# configure terminal
sw3(config)# vlan 20,40,100-200
sw3(config-vlan)# exit
sw3(config)#
```

2. ポート 1/0/1 からポート 1/0/3 をトランクポートとして設定し、トランクポートにすべての VLAN を割り当てます。

```
sw3(config)# interface range port 1/0/1-3
sw3(config-if-port-range)# switchport mode trunk
sw3(config-if-port-range)# exit
sw3(config)#
```

3. プロファイル［campus］を作成し、ガードタイマーを［700 ミリ秒］に、ホールドオフタイマーを［1 秒］に、WTR タイマーを［1 分］に設定します。

```
sw3(config)# ethernet ring g8032 profile campus
sw3(config-erps-ring-profile)# timer guard 700
sw3(config-erps-ring-profile)# timer hold-off 1
sw3(config-erps-ring-profile)# timer wtr 1
sw3(config-erps-ring-profile)# exit
sw3(config)#
```

4. リング［ring1］を作成し、port0 を［ポート 1/0/1］に、port1 を［ポート 1/0/2］に設定します。

```
sw3(config)# ethernet ring g8032 ring1
sw3(config-erps-ring)# port0 interface port 1/0/1
sw3(config-erps-ring)# port1 interface port 1/0/2
sw3(config-erps-ring)#
```

5. リング［ring1］に ERP インスタンス［1］を作成し、ERPS インスタンス設定モードに遷移します。

```
sw3(config-erps-ring)# instance 1
sw3(config-erps-ring-instance)#
```

6. ERP インスタンス［1］にプロファイル［campus］を関連付け、R-APS チャネル VLAN を［VLAN 20］に、保護する VLAN を［VLAN 100 から VLAN 200］に設定します。

```
sw3(config-erps-ring-instance)# profile campus
sw3(config-erps-ring-instance)# r-aps channel-vlan 20
sw3(config-erps-ring-instance)# inclusion-list vlan-ids 100-200
sw3(config-erps-ring-instance)#
```

7. リング MEL 値（管理レベル）を［6］に設定します。

```
sw3(config-erps-ring-instance)# level 6
sw3(config-erps-ring-instance)#
```

8. ERP インスタンス［1］を有効化します。

```
sw3(config-erps-ring-instance)# activate
sw3(config-erps-ring-instance)# exit
sw3(config-erps-ring)#
```

9. リング［ring2］を作成し、port0 を［ポート 1/0/3］に、port1 を［なし］に設定します。

```
sw3(config)# ethernet ring g8032 ring2
sw3(config-erps-ring)# port0 interface port 1/0/3
sw3(config-erps-ring)# port1 none
sw3(config-erps-ring)#
```

10. リング［ring2］に ERP インスタンス［2］を作成し、ERPS インスタンス設定モードに遷移します。

```
sw3(config-erps-ring)# instance 2
sw3(config-erps-ring-instance)#
```

11. sw3 を RPL オーナーとして、port0 を RPL ポートに設定します。

```
sw3(config-erps-ring-instance)# rpl port0 owner
sw3(config-erps-ring-instance)#
```

12. ERP インスタンス［2］にプロファイル［campus］を関連付け、R-APS チャネル VLAN を［VLAN 40］に、保護する VLAN を［VLAN 100 から VLAN 200］に設定します。

```
sw3(config-erps-ring-instance)# profile campus
sw3(config-erps-ring-instance)# r-aps channel-vlan 40
sw3(config-erps-ring-instance)# inclusion-list vlan-ids 100-200
sw3(config-erps-ring-instance)#
```

13. リング MEL 値（管理レベル）を［7］に設定し、一度 ERP インスタンス［2］の設定を終了します。

```
sw3(config-erps-ring-instance)# level 7
sw3(config-erps-ring-instance)# exit
sw3(config-erps-ring)# exit
sw3(config)#
```

14. リング［ring1］にリング［ring2］をサブリングとして設定します。

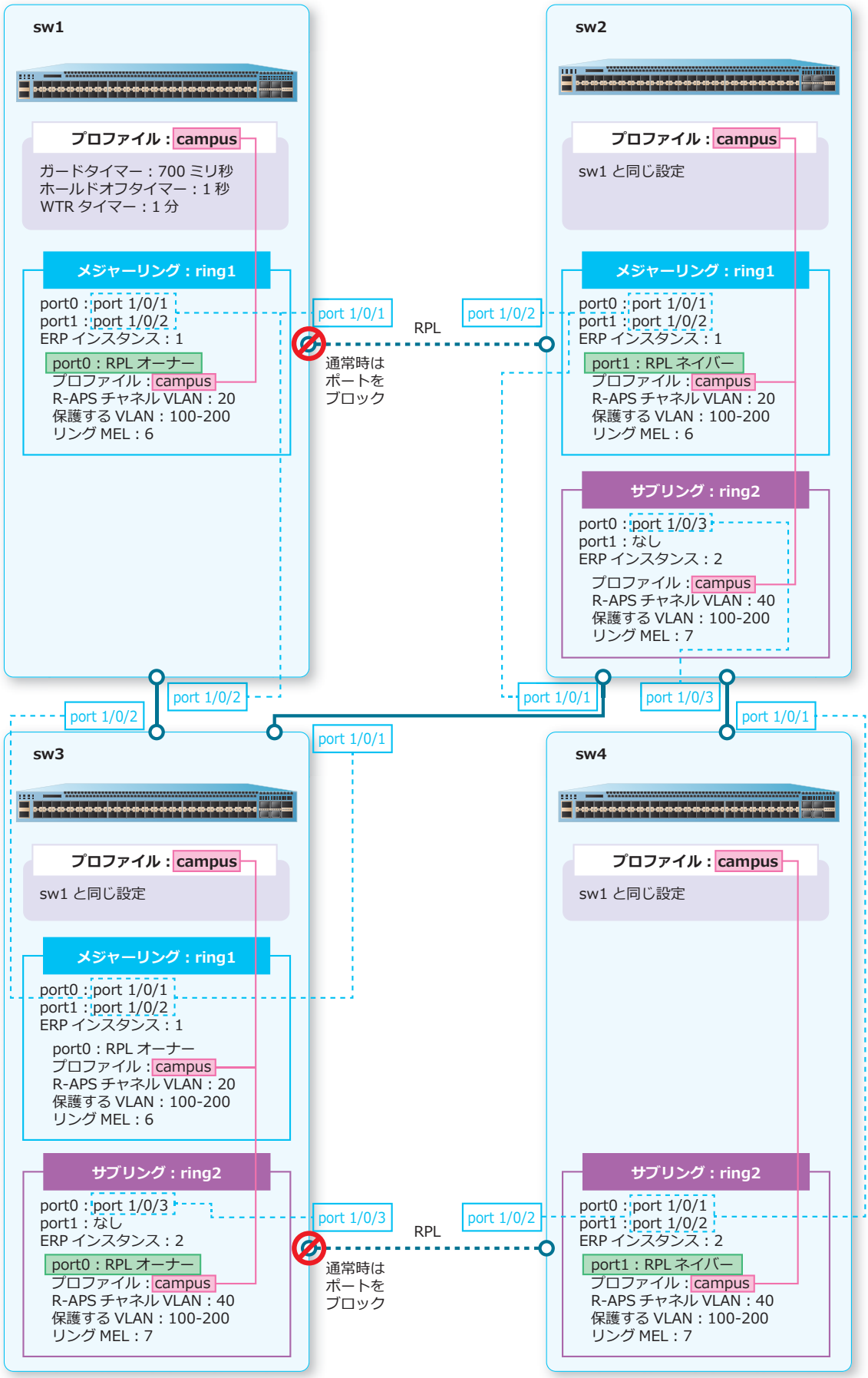
```
sw3(config)# ethernet ring g8032 ring1
sw3(config-erps-ring)# sub-ring ring2
sw3(config-erps-ring)# exit
sw3(config)#
```

15. ERP インスタンス［2］を有効化します。

```
sw3(config)# ethernet ring g8032 ring2
sw3(config-erps-ring)# instance 2
sw3(config-erps-ring-instance)# activate
sw3(config-erps-ring-instance)# end
sw3#
```

10.3.2.4 サブリングの RPL ネイバーの設定例（sw4）

図 10-11 サブリングの RPL ネイバーの設定例（sw4）



1. VLAN 40、および VLAN 100 から VLAN 200 を作成します。

```
sw4# configure terminal
sw4(config)# vlan 40,100-200
sw4(config-vlan)# exit
sw4(config)#
```

2. ポート 1/0/1 からポート 1/0/2 をトランクポートとして設定し、トランクポートにすべての VLAN を割り当てます。

```
sw4(config)# interface range port 1/0/1-2
sw4(config-if-port-range)# switchport mode trunk
sw4(config-if-port-range)# exit
sw4(config)#
```

3. プロファイル［campus］を作成し、ガードタイマーを［700 ミリ秒］に、ホールドオフタイマーを［1 秒］に、WTR タイマーを［1 分］に設定します。

```
sw4(config)# ethernet ring g8032 profile campus
sw4(config-erps-ring-profile)# timer guard 700
sw4(config-erps-ring-profile)# timer hold-off 1
sw4(config-erps-ring-profile)# timer wtr 1
sw4(config-erps-ring-profile)# exit
sw4(config)#
```

4. リング［ring2］を作成し、port0 を［ポート 1/0/1］に、port1 を［ポート 1/0/2］に設定します。

```
sw4(config)# ethernet ring g8032 ring2
sw4(config-erps-ring)# port0 interface port 1/0/1
sw4(config-erps-ring)# port1 interface port 1/0/2
sw4(config-erps-ring)#
```

5. リング［ring2］に ERP インスタンス［2］を作成し、ERPS インスタンス設定モードに遷移します。

```
sw4(config-erps-ring)# instance 2
sw4(config-erps-ring-instance)#
```

6. sw4 を RPL ネイバーとして、port1 を RPL ポートに設定します。

```
sw4(config-erps-ring-instance)# rpl port1
sw4(config-erps-ring-instance)#
```

7. ERP インスタンス［2］にプロファイル［campus］を関連付け、R-APS チャネル VLAN を［VLAN 40］に、保護する VLAN を［VLAN 100 から VLAN 200］に設定します。

```
sw4(config-erps-ring-instance)# profile campus
sw4(config-erps-ring-instance)# r-aps channel-vlan 40
sw4(config-erps-ring-instance)# inclusion-list vlan-ids 100-200
sw4(config-erps-ring-instance)#
```

8. リング MEL 値（管理レベル）を［7］に設定します。

```
sw4(config-erps-ring-instance)# level 7
sw4(config-erps-ring-instance)#
```

9. ERP インスタンス［2］を有効化します。

```
sw4(config-erps-ring-instance)# activate
sw4(config-erps-ring-instance)# end
sw4#
```

11. QoS

QoS 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。

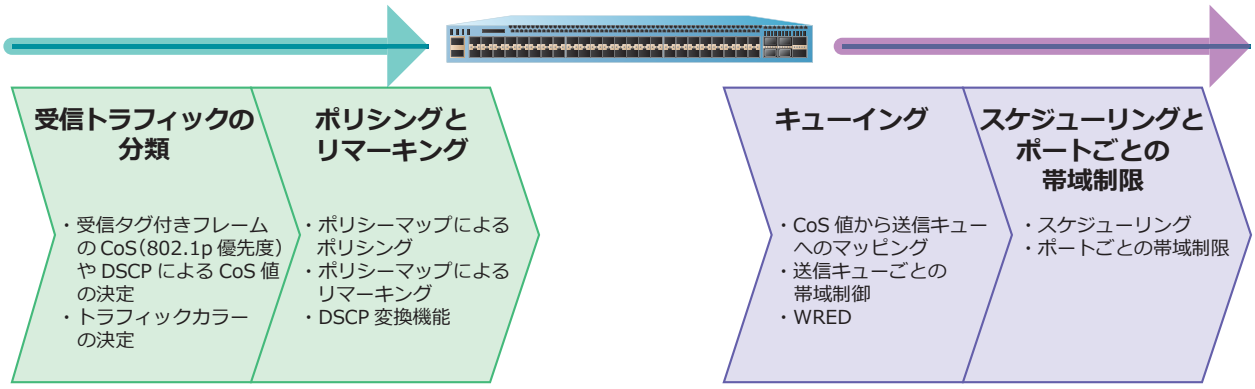
11.1 QoS の機能説明

QoS（Quality of Service）は、ネットワーク上を流れるパケットに優先順位を設定して、通信品質を確保する機能です。たとえば、パケットロスで通信品質が劣化してしまう IP 電話などの通信を、優先して処理できます。

本装置では、以下の順序で QoS 制御を行います。

1. 受信トラフィックの分類
2. ポリシングとリマーキング
3. キューイング
4. スケジューリングとポートごとの帯域制限

図 11-1 QoS の概要



NOTE: ポリシーマップによるポリシングと一部のリマーキング機能は、送信側でも設定できます。

NOTE: ポートごとの帯域制限機能は、受信側でも設定できます。

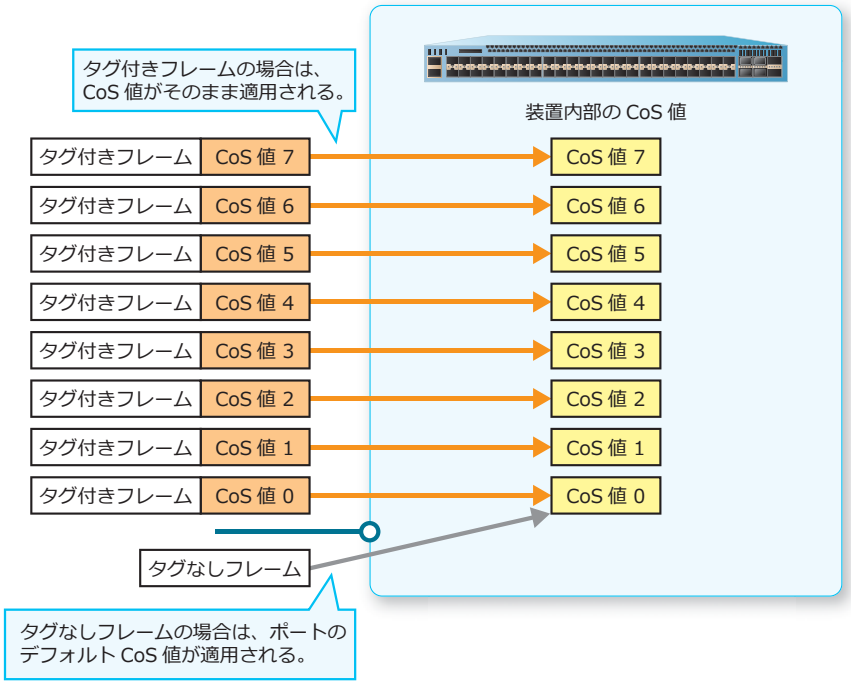
11.1.1 受信トラフィックの分類

受信したトラフィックは、装置内部では CoS 値により分類されます。この CoS 値は、タグ付きフレームの CoS（802.1p 優先度）と同じもので、装置からタグ付きフレームとして送信される場合は、この CoS 値が反映されます。

受信トラフィックの分類は、受信トラフィックの分類設定によって動作が異なります。受信トラフィックの分類設定がデフォルトの「受信トラフィックの CoS を信頼するモード」の場合は、以下のように分類されます。

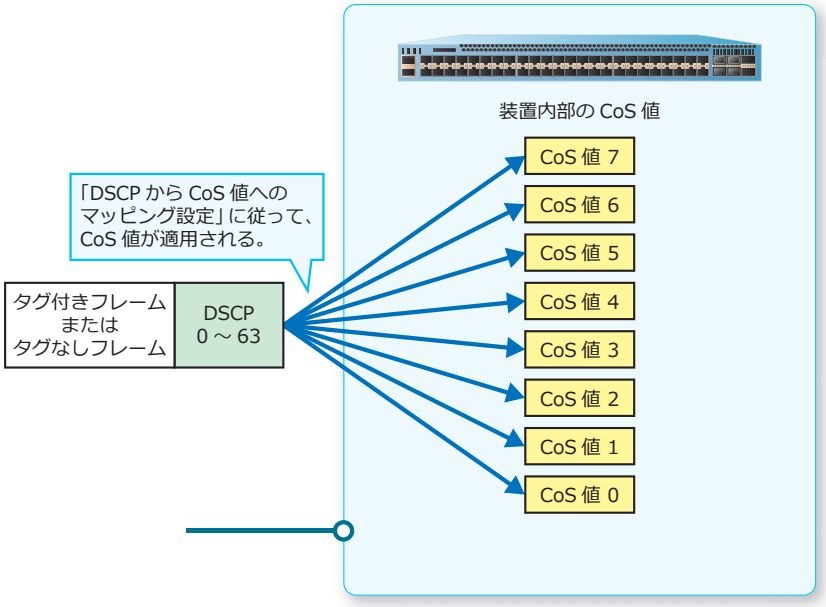
- 受信トラフィックがタグなしフレームの場合：
  ポートのデフォルト CoS 値が適用される。
- 受信トラフィックがタグ付きフレームの場合：
  受信したタグ付きフレームの CoS（802.1p 優先度）がそのまま適用される。

図 11-2 「受信トラフィックの CoS を信頼するモード」の場合の分類



受信トラフィックの分類設定が「受信トラフィックの DSCP を信頼するモード」の場合は、「DSCP から CoS 値へのマッピング設定」に従って CoS 値が適用されます。

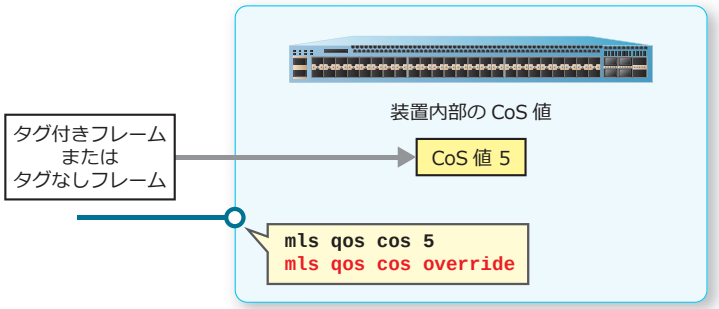
図 11-3 「受信トラフィックの DSCP を信頼するモード」の場合の分類



受信トラフィックの分類設定を変更するには、**`mls qos trust`** コマンドを使用します。ポートのデフォルト CoS 値を変更するには、**`mls qos cos`** コマンドを使用します。「DSCP から CoS 値へのマッピング設定」を変更するには、**`mls qos map dscp-cos`** コマンドを使用します。

なお、**mls qos cos override** コマンドを設定した場合は、受信トラフィックの分類設定にかかわらず、ポートのデフォルト CoS 値が適用されます。

図 11-4 mls qos cos override コマンドの設定例



REF: 受信ポートがトンネルポートの場合は、受信設定コマンドによって適用される CoS 値が変わります。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。

11.1.1.1 ポリシーマップによる CoS 値のリマーキング

ポリシーマップを使用して CoS 値を変更できます。詳細については、「ポリシーマップ」を参照してください。

11.1.1.2 受信時のトラフィック初期カラーの決定

受信したトラフィックは、3 種類のトラフィックカラー（グリーン、イエロー、レッド）に分類されます。デフォルト設定ではすべてグリーンに分類されます。

受信トラフィックの分類設定がデフォルトの「受信トラフィックの CoS を信頼するモード」の場合は、「CoS からトラフィック初期カラーへのマッピング設定」に従って決定されます。受信トラフィックの分類設定が「受信トラフィックの DSCP を信頼するモード」の場合は、「DSCP からトラフィック初期カラーへのマッピング設定」に従って決定されます。

「CoS からトラフィック初期カラーへのマッピング設定」を変更するには、**mls qos map cos-color** コマンドを使用します。「DSCP からトラフィック初期カラーへのマッピング設定」を変更するには、**mls qos map dscp-color** コマンドを使用します。

11.1.2 ポリシーマップ

ポリシーマップは、「トラフィックの分類」「ポリシング」「リマーキング」をまとめた機能です。ポリシーマップは受信側ポート、送信側ポートの両方で使用できます。

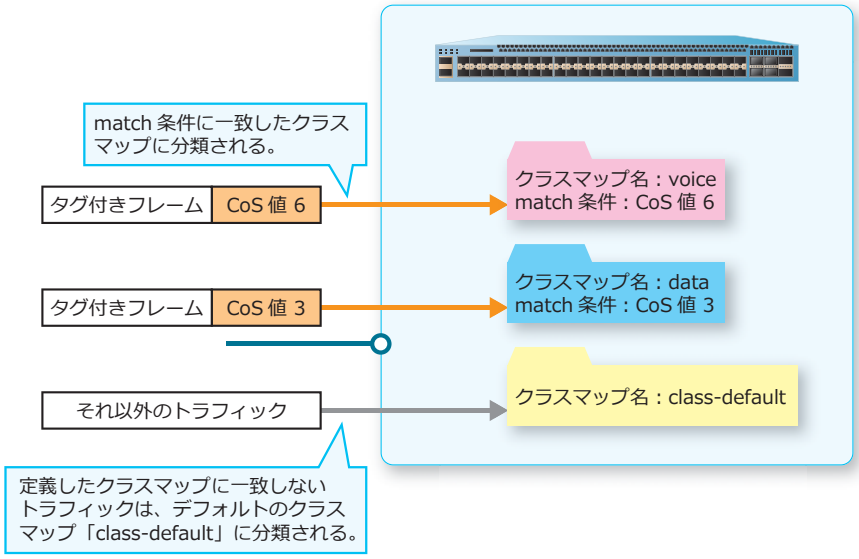
CAUTION: ポリシーマップの一部のリマーキング機能は、送信側では使用できません。

ポリシーマップでの「トラフィックの分類」

ポリシーマップではクラスマップによってトラフィックを分類します。クラスマップでは、分類するための一致条件を設定します。分類するための一致条件には以下を指定できます。

- アクセスリスト
- CoS 値
- DSCP
- precedence 値
- プロトコル
- VLAN ID

図 11-5 ポリシーマップでの「トラフィックの分類」の例



ポリシーマップでの「ポリシング」

ポリシーマップでは、クラスマップごとにポリサーを適用できます。また、集約ポリサーを利用することにより、複数のクラスマップに対して同じポリサーを適用することもできます。詳細については、「ポリシング」を参照してください。

ポリシーマップでの「リマーキング」

ポリシーマップでは、クラスマップごとに以下のアクションを設定できます。

- CoS 値の変更
- DSCP の変更
- precedence 値の変更（受信側ポート適用時のみ）
- cos-queue（送信キューへのマッピング）（受信側ポート適用時のみ）

CAUTION: スタック構成において、cos-queue アクションによる送信キューへのマッピングは、スタック装置を跨がない（受信ポートと同一装置のポートから送信する）トラフィックに対しては動作しますが、スタック装置を跨ぐ（受信ポートと異なるメンバー装置のポートから送信する）トラフィックに対しては動作しません。そのため、該当トラフィックがスタック装置を跨ぐ場合は、cos-queue アクションではなく CoS 値の変更アクション（**set cos** コマンド）を使用することを推奨します。

CAUTION: ApresiaNP2100-48T4X、ApresiaNP2100-48T4X-PoE、ApresiaNP2000-48T4X、および ApresiaNP2000-48T4X-PoE では、特定のポートを跨ぐ通信（「ポート 1 ～ 24、49 ～ 50 で受信して、ポート 25 ～ 48、51 ～ 52 から送信するトラフィック」、またはその逆）に対しては、cos-queue アクションによる送信キューへのマッピングは動作しません。そのため、該当トラフィックが条件にマッチする場合は、cos-queue アクションではなく CoS 値の変更アクション（**set cos** コマンド）を使用することを推奨します。

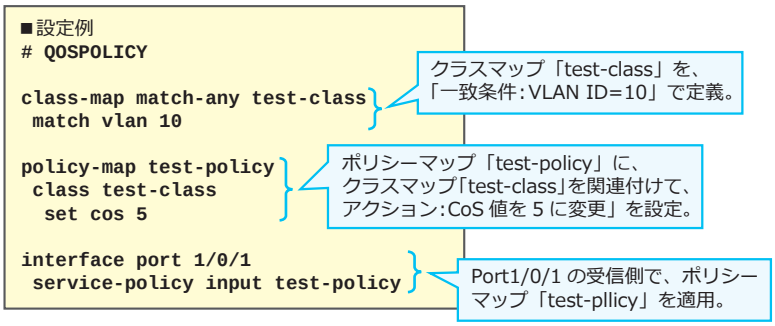
ポリシーマップの設定コマンド

クラスマップを定義するには、**class-map** コマンドを使用します。クラスマップで一致条件を設定するには、**match** コマンドを使用します。

ポリシーマップを定義するには、**policy-map** コマンドを使用します。ポリシーマップにクラスマップを関連付けるには、**class** コマンドを使用します。関連付けたクラスマップでリマーキングを設定するには、**set** コマンドを使用します。ポリシーマップを物理ポートに適用するには、**service-policy** コマンドを使用します。

ポリシーマップに関連付けたクラスマップでポリシングを設定するには、**police** コマンド、**police cir** コマンド、**police aggregate** コマンドを使用します。集約ポリサーを定義するには、**mls qos aggregate-policer** コマンドを使用します。

図 11-6 ポリシーマップの設定コマンドの例



11.1.3 ポリシング

ポリシーマップでは、クラスマップごとにポリサーを適用できます。ポリサーは対象トラフィックを計測し、通信量に基づいて 3 種類のトラフィックカラー（グリーン、イエロー、レッド）に分類します。分類されたトラフィックごとに送信を許可したり破棄することにより、トラフィックの帯域制限を行います。

ポリサーの種類

ポリサーは、平均レートを使用する 1 レートポリサーと、保証帯域（CIR）および最大帯域（PIR）を使用する 2 レートポリサーを利用できます。また、各ポリサーでは、ポリサーに入力される前のトラフィック初期カラーを利用しないカラーブラインドモードと、トラフィックの初期カラーを利用するカラーアウェアモードを選択できます。

表 11-1 利用可能なポリサーの種類と動作モード

利用可能レート	トラフィック初期カラーの利用	ポリサーの種類・動作モード
平均レート（バーストサイズ）	利用しない	1 レート 2 カラーポリサー・カラーブラインドモード
平均レート（バーストサイズ、最大バーストサイズ）	利用しない	1 レート 3 カラーポリサー・カラーブラインドモード
平均レート（バーストサイズ、最大バーストサイズ）	利用する	1 レート 3 カラーポリサー・カラーアウェアモード
保証帯域（CIR）および最大帯域（PIR）	利用しない	2 レート 3 カラーポリサー・カラーブラインドモード
保証帯域（CIR）および最大帯域（PIR）	利用する	2 レート 3 カラーポリサー・カラーアウェアモード

カラーブラインドモードとカラーアウェアモード

カラーブラインドモードは、ポリサーに入力される前のトラフィック初期カラーを利用しないモードです。対象ポリサーでの帯域計測結果のみで、トラフィックが分類されます。

カラーアウェアモードは、ポリサーに入力される前のトラフィック初期カラーを利用するモードです。カラーアウェアモードでは、最終的に分類されるトラフィックカラーが初期カラーよりもよくなることはありません。

- 初期カラーがグリーンの場合は、対象ポリサーでの帯域計測の結果、最終的にグリーン、イエロー、レッドのいずれかに分類される。
- 初期カラーがイエローの場合は、対象ポリサーでの帯域計測の結果、最終的にイエロー、レッドのいずれかに分類される。
- 初期カラーがレッドの場合は、対象ポリサーでの帯域計測後も、レッドに分類される。

ポリサーのアクション

ポリサーで分類したトラフィックごとに、以下のアクションを設定できます。

- 対象トラフィックを破棄
- 対象トラフィックを何も変更せずに送信
- 対象トラフィックの CoS 値を変更して送信
- 対象トラフィックの DSCP を変更して送信

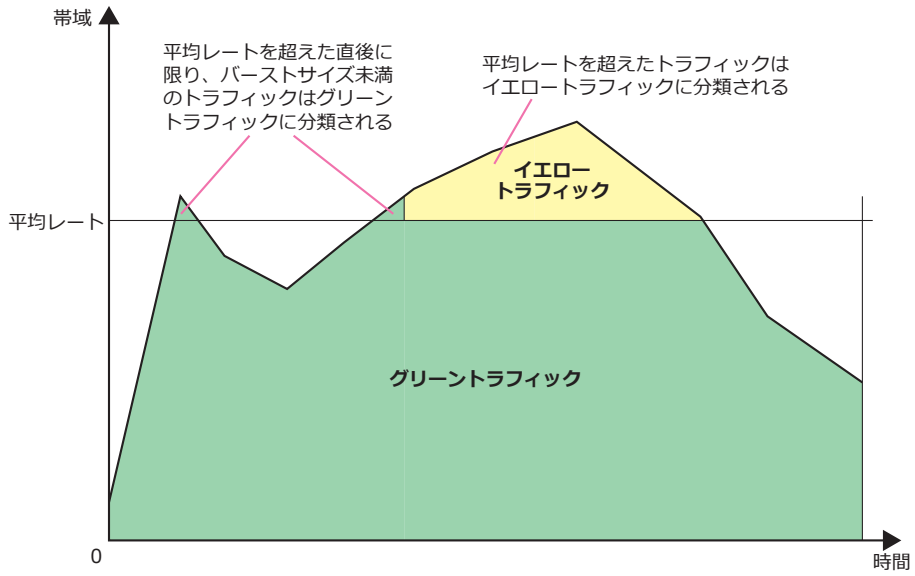
11.1.3.1 1 レート 2 カラーポリサー

1 レート 2 カラーポリサーは、平均レート（バーストサイズ）を設定し、トラフィックを 2 段階（グリーン、イエロー）に分類します。

• 平均レート（バーストサイズ）

グリーントラフィックとイエロートラフィックの境界を定義します。

図 11-7 1 レート 2 カラーポリサーの概要



1 レート 2 カラーポリサーは、`police` コマンドで以下を設定します。

- 平均レート（バーストサイズ）
- グリーントラフィックに対するアクション、イエロートラフィックに対するアクション

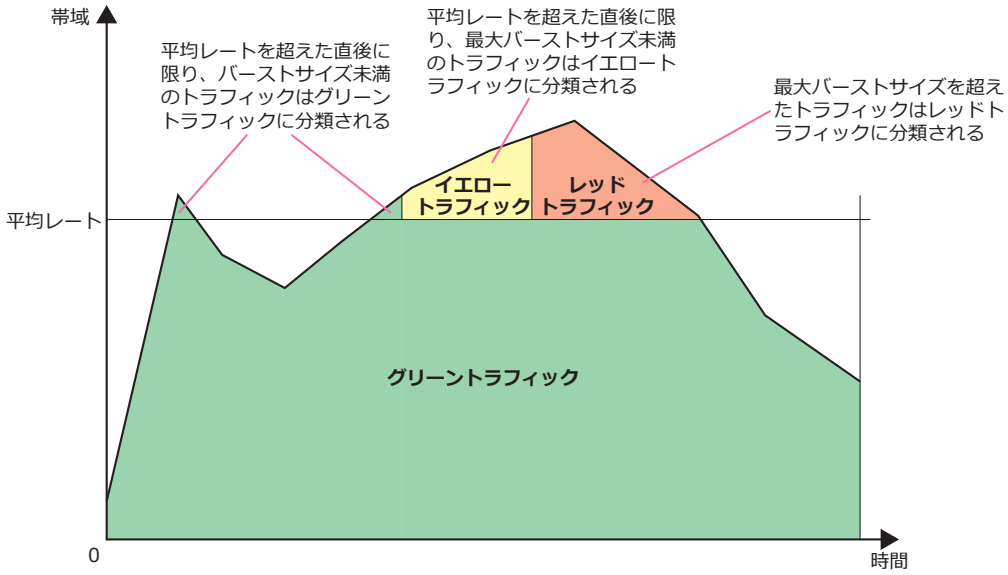
NOTE: 1 レート 2 カラーポリサーは、カラーブラインドモードでのみ動作します。カラーアウェアモードでは動作しません。

11.1.3.2 1 レート 3 カラーポリサー

1 レート 3 カラーポリサーは、平均レート（バーストサイズ、最大バーストサイズ）を設定し、トラフィックを 3 段階（グリーン、イエロー、レッド）に分類します。

- **平均レート（バーストサイズ）**
  グリーントラフィックとイエロートラフィックの境界を定義します。
- **最大バーストサイズ**
  イエロートラフィックとレッドトラフィックの境界を定義します。

図 11-8 1 レート 3 カラーポリサーの概要



1 レート 3 カラーポリサーは、`police` コマンドで以下を設定します。

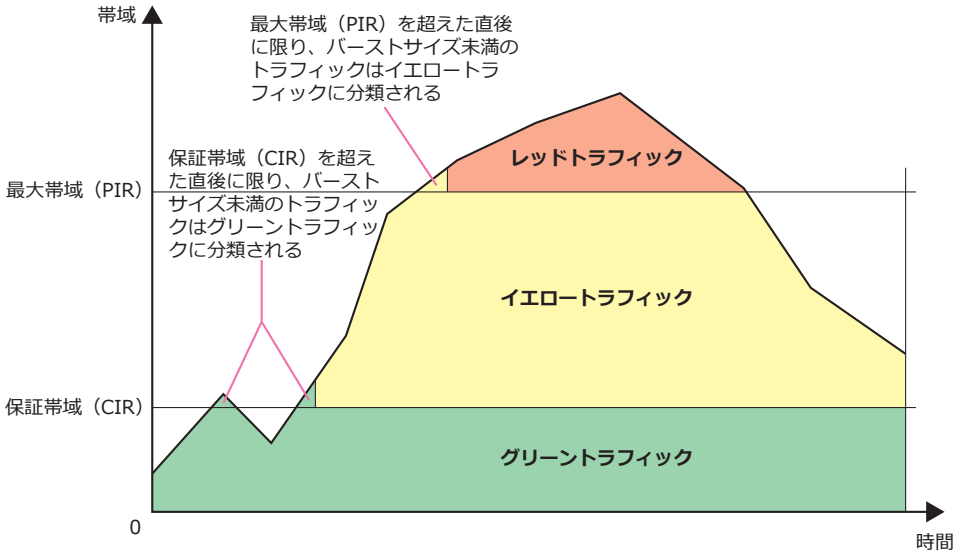
- 平均レート（バーストサイズ、最大バーストサイズ）
- グリーントラフィックに対するアクション、イエロートラフィックに対するアクション、レッドトラフィックに対するアクション
- カラーブラインドモード（デフォルト設定）にするか、カラーアウェアモードにするかの設定

11.1.3.3 2 レート 3 カラーポリサー

2 レート 3 カラーポリサーは、保証帯域（CIR）および最大帯域（PIR）の 2 つのレートを設定し、トラフィックを 3 段階（グリーン、イエロー、レッド）に分類します。

- **保証帯域（CIR）**
  グリーントラフィックとイエロートラフィックの境界を定義します。
- **最大帯域（PIR）**
  イエロートラフィックとレッドトラフィックの境界を定義します。

図 11-9 2 レート 3 カラーポリサーの概要



2 レート 3 カラーポリサーは、`police` コマンドで以下を設定します。

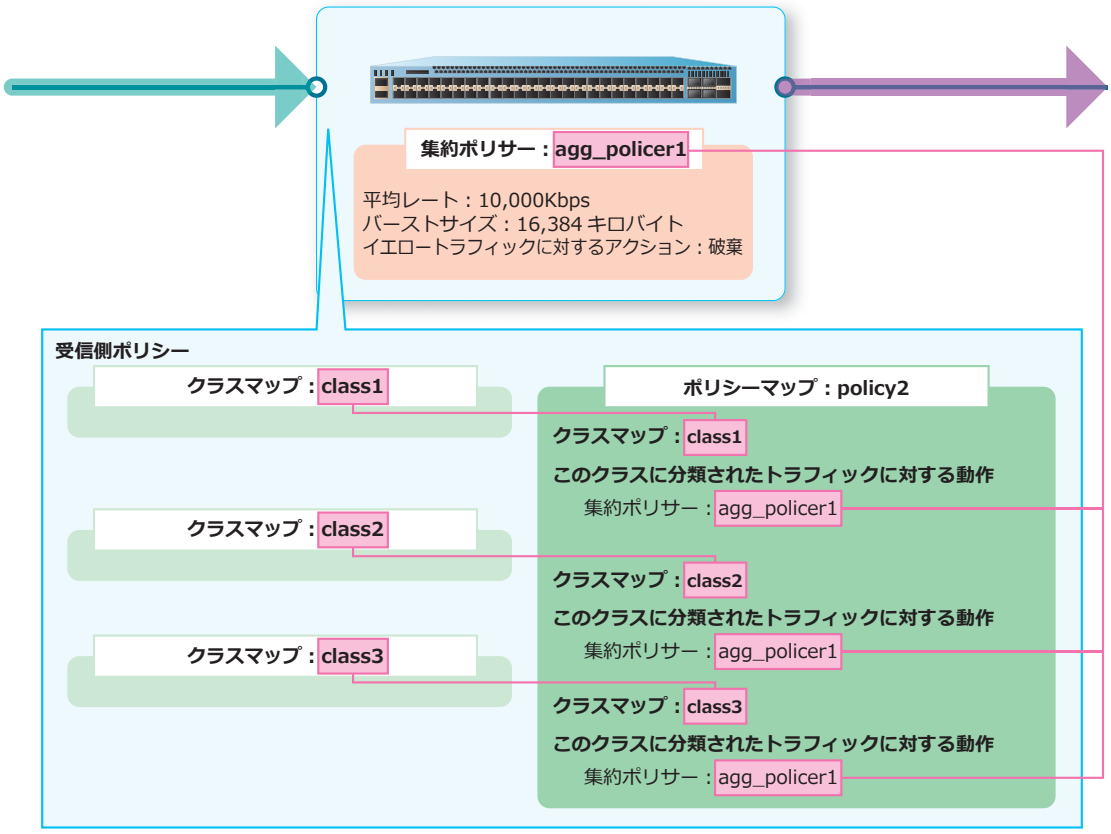
- 保証帯域（CIR）（バーストサイズ）
- 最大帯域（PIR）（バーストサイズ）
- グリーントラフィックに対するアクション、イエロートラフィックに対するアクション、レッドトラフィックに対するアクション
- カラーブラインドモード（デフォルト設定）にするか、カラーアウェアモードにするかの設定

11.1.3.4 集約ポリサー

ポリシーマップでは、集約ポリサーを利用することにより、複数のクラスマップに対して同じポリサーを適用できます。

集約ポリサーにおいても、1 レート 2 カラーポリサー、1 レート 3 カラーポリサー、および 2 レート 3 カラーポリサーを利用できます。

図 11-10 集約ポリサーの概要



集約ポリサーは、**`mls qos aggregate-policer`** コマンドで設定します。

11.1.4 DSCP 変換機能

DSCP 変換機能では、DSCP の値を「DSCP 変換マップ」に従って変換します。DSCP 変換機能を使用する場合は、受信トラフィックの分類設定を「受信トラフィックの DSCP を信頼するモード」に設定します。

「DSCP 変換機能」と「受信側ポリシーマップによる DSCP の変更」の両方を設定している場合は、ポリシーマップの一致条件にマッチしたトラフィックに対しては「ポリシーマップによる DSCP の変更」が適用されます。それ以外のトラフィックに対しては「DSCP 変換機能」が適用されます。

DSCP 変換機能を設定しても、以下は変換前の DSCP を基に動作します。

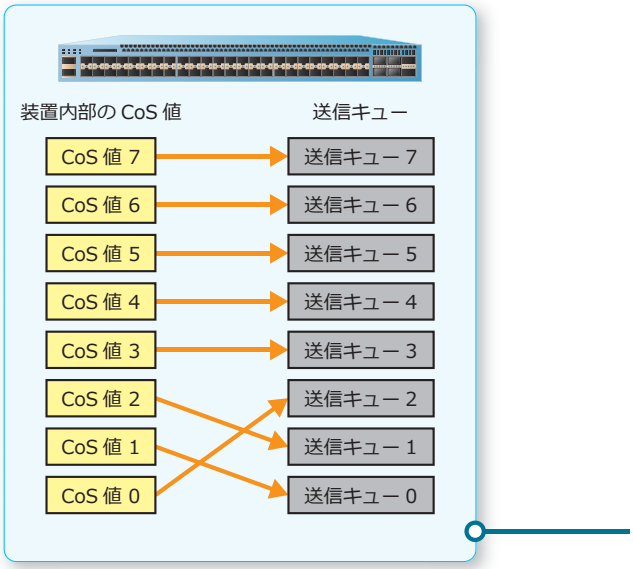
- DSCP から CoS 値へのマッピング設定（**`mls qos map dscp-cos`**）
- DSCP からトラフィック初期カラーへのマッピング設定（**`mls qos map dscp-color`**）
- 受信側ポリシーマップの一致条件

DSCP 変換マップを定義するには、**`mls qos map dscp-mutation`** コマンドを使用します。DSCP 変換マップを適用するには、**`mls qos dscp-mutation`** コマンドを使用します。

11.1.5 CoS 値から送信キューへのマッピング

送信トラフィックをキューイングする送信キューは、CoS 値に基づいて決定されます。デフォルト設定の「CoS 値から送信キューへのマッピング設定」を以下に示します。

図 11-11 CoS 値から送信キューへのマッピング設定（デフォルト）



「CoS 値から送信キューへのマッピング設定」を変更するには、**`priority-queue cos-map`** コマンドを使用します。

11.1.6 送信キューごとの帯域制御

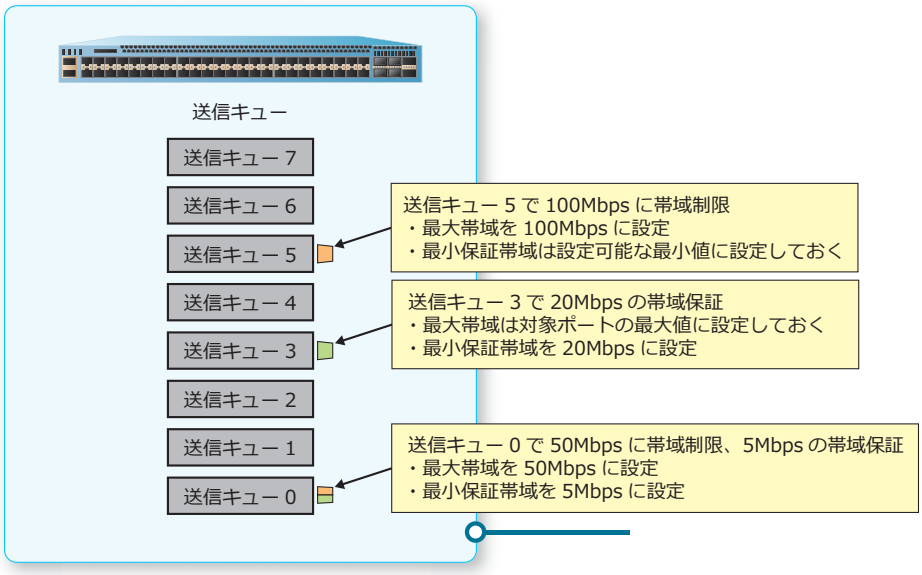
送信キューごとに、最大帯域（Max Bandwidth）と最小保証帯域（Min Bandwidth）を設定できます。

最大帯域（Max Bandwidth）を設定した送信キューでは、そのキューから送信するトラフィックが指定した最大帯域に制限されます。

最小保証帯域（Min Bandwidth）を設定した送信キューでは、対象ポートが輻輳状態でも、そのキューから送信するトラフィックが指定した最小帯域分は破棄されずに送信されます。

NOTE: 使用する場合は、最大帯域と最小保証帯域の両方を設定する必要があります。

図 11-12 送信キューごとの帯域制御の例



送信キューごとの帯域制御を設定するには、**`queue rate-limit`** コマンドを使用します。

11.1.7 WRED

WRED を有効にすると、キューイングする際に輻輳の可能性を検知し、優先順位が低いトラフィックを重点的に廃棄することで、輻輳を抑えます。また、優先順位が高いトラフィックを廃棄されにくく設定することで、輻輳を抑えながらサービス品質をある程度維持できます。

WRED を有効にするには、**`random-detect`** コマンドを使用します。

WRED の動作を変更する場合に利用する設定は以下のとおりです。() 内は使用するコマンドです。

- WRED の最小しきい値、最大しきい値、および最大廃棄率（**`random-detect profile`** コマンド）
- 平均キューサイズの計算に使用される WRED 指数の加重係数（**`random-detect exponential-weight`** コマンド）

CAUTION: NP2100、NP2000、および NP2500 では、WRED を使用できません。

11.1.7.1 ECN による WRED の拡張

ECN（Explicit Congestion Notification）を有効化すると、輻輳が発生したときに、トラフィックに ECN マーク（ECT ビットおよび CE ビット）を付与して、送信者（ルーターやエンドホスト）に対して輻輳が発生していることを通知します。

ECN に対応した送信者（ルーターやエンドホスト）は、通知された ECN マークによって、装置において輻輳が発生していることを検知すると、送信するトラフィックを抑えることで輻輳を回避できます。

ECN は、キューごとに有効化できます。ECN を有効化するには、**`random-detect ecn`** コマンドを使用します。

CAUTION: NP2100、NP2000、および NP2500 では、WRED を使用できません。

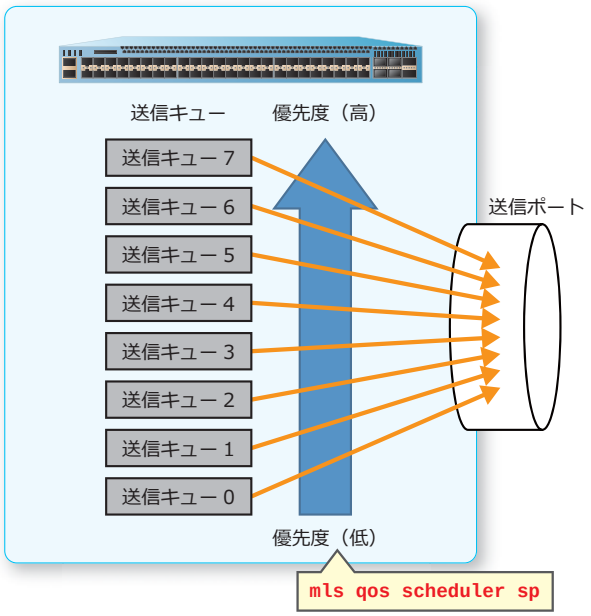
11.1.8 スケジューリング

送信ポートごとにスケジューリングアルゴリズムを設定できます。デフォルト設定では、全ポート WRR（Weighted Round Robin）スケジューリングに設定されています。スケジューリングアルゴリズムは以下を指定できます。

- Strict Priority Queuing
- Round Robin スケジューリング
- WRR（Weighted Round Robin）スケジューリング
- WDRR（Weighted Deficit Round Robin）スケジューリング

NOTE: WRR スケジューリングまたは WDRR スケジューリングにおいて、重みが 0 に設定されている送信キューは Strict Priority Queuing で動作します。

図 11-13 Strict Priority Queuing に設定した場合の例



スケジューリングアルゴリズムを設定するには、**`mls qos scheduler`** コマンドを使用します。WRR スケジューリングの重みを設定するには、**`wrr-queue bandwidth`** コマンドを使用します。WDRR スケジューリングの重みを設定するには、**`wdrr-queue bandwidth`** コマンドを使用します。

11.1.9 ポートごとの帯域制限

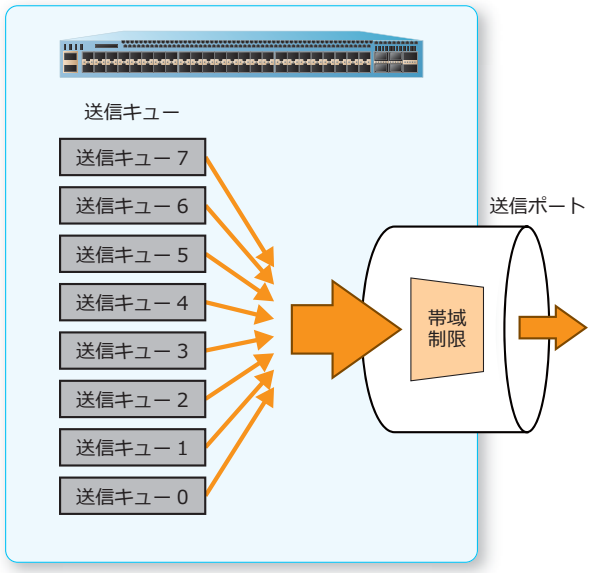
ポートごとの帯域制限は、受信ポートまたは送信ポートごとに設定できます。

CAUTION: 運用中にバーストサイズの設定を大きい値から小さい値に変更すると、トラフィック状況によっては一時的にパケットの中継が停止します。そのため、バーストサイズの設定を大きい値から小さい値に変更する場合は、一度 **`no rate-limit`** コマンドで削除してから、再度設定してください。

NOTE: NP7000 の受信ポートごとの帯域制限では、IFG（Inter Frame Gap）と Preamble/SFD を含めて帯域計測を行います。送信ポートごとの帯域制限では、IFG（Inter Frame Gap）と Preamble/SFD を含めずに帯域計測を行います。

NOTE: NP5000、NP4000、NP3000、NP2100、NP2000、および NP2500 の受信ポートごとの帯域制限と送信ポートごとの帯域制限では、IFG（Inter Frame Gap）と Preamble/SFD を含めずに帯域計測を行います。

図 11-14 送信ポートの帯域制限の例



受信ポートごとの帯域制限を設定するには、**`rate-limit input`** コマンドを使用します。送信ポートごとの帯域制限を設定するには、**`rate-limit output`** コマンドを使用します。

11.2 QoS の状態確認

QoS の状態を表示して確認する方法を説明します。

11.2.1 受信トラフィックの分類機能の表示

受信トラフィックの分類機能の設定を確認する方法を説明します。

11.2.1.1 受信トラフィックの分類設定の表示

show mls qos interface trust コマンドで、受信トラフィックの分類設定を確認できます。

ポート 1/0/2 からポート 1/0/5 を指定した場合の表示例を以下に示します。

```
# show mls qos interface port 1/0/2-1/0/5 trust
 (1)            (2)
 Interface      Trust State
 ------------   ------------
 Port1/0/2      trust CoS
 Port1/0/3      trust CoS
 Port1/0/4      trust CoS
 Port1/0/5      trust CoS
```

各項目の説明は、以下のとおりです。

表 11-2 show mls qos interface trust 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)	受信トラフィックの分類設定を表示します。 • trust CoS：受信トラフィックの CoS を信頼するモード • trust DSCP：受信トラフィックの DSCP を信頼するモード

11.2.1.2 ポートのデフォルト CoS 値の表示

show mls qos interface cos コマンドで、ポートのデフォルト CoS 値を確認できます。

ポート 1/0/2 からポート 1/0/5 を指定した場合の表示例を以下に示します。

```
# show mls qos interface port 1/0/2-5 cos
 (1)            (2)    (3)
 Interface      CoS    Override
 ------------   ----   ---------
 Port1/0/2      0      No
 Port1/0/3      0      No
 Port1/0/4      0      No
 Port1/0/5      0      No
```

各項目の説明は、以下のとおりです。

表 11-3 show mls qos interface cos 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。

項番	説明
(2)	デフォルトの CoS 値を表示します。
(3)	受信トラフィックの CoS を、デフォルトの CoS 値で書き換える設定を表示します。 • Yes：デフォルトの CoS 値で書き換える • No：デフォルトの CoS 値で書き換えない

11.2.1.3 DSCP から CoS 値へのマッピング設定の表示

show mls qos interface map dscp-cos コマンドで、DSCP から CoS 値へのマッピング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 mls qos interface port 1/0/1 map dscp-cos

Port1/0/1 ...(1)
        0  1  2  3  4  5  6  7  8  9 ...(2)
   ---------------------------------
   00   00 00 00 00 00 00 00 00 01 01
   10   01 01 01 01 01 01 02 02 02 02
   20   02 02 02 02 03 03 03 03 03 03
   30   03 03 04 04 04 04 04 04 04 04
   40   05 05 05 05 05 05 05 05 06 06
   50   06 06 06 06 06 06 07 07 07 07
   60   07 07 07 07
```

各項目の説明は、以下のとおりです。

表 11-4 show mls qos interface map dscp-cos 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)	DSCP から CoS 値へのマッピング設定を表形式で表示します。表の縦軸は DSCP の 10 の位を、横軸は DSCP の 1 の位を表します。交差する点に表示されている数値が、マッピングする CoS 値を表します。

11.2.1.4 CoS からトラフィック初期カラーへのマッピング設定の表示

show mls qos interface map cos-color コマンドで、CoS からトラフィック初期カラーへのマッピング設定を確認できます。

ポート 1/0/3 からポート 1/0/4 を指定した場合の表示例を以下に示します。

```
# show mls qos interface port 1/0/3-4 map cos-color

Port1/0/3 ...(1)
  CoS 0-2,5,7 are mapped to green ...(2)
  CoS 3-4 are mapped to yellow ...(3)
  CoS 6 are mapped to red ...(4)
Port1/0/4
  CoS 0-7 are mapped to green
```

各項目の説明は、以下のとおりです。

表 11-5 show mls qos interface map cos-color 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)	グリーントラフィックに分類される CoS を表示します。
(3)	イエロートラフィックに分類される CoS を表示します。
(4)	レッドトラフィックに分類される CoS を表示します。

11.2.1.5 DSCP からトラフィック初期カラーへのマッピング設定の表示

show mls qos interface map dscp-color コマンドで、DSCP からトラフィック初期カラーへのマッピング設定を確認できます。

ポート 1/0/1 からポート 1/0/2 を指定した場合の表示例を以下に示します。

```
# show mls qos interface port 1/0/1-2 map dscp-color

Port1/0/1 ...(1)
  DSCP 0-7 are mapped to green ...(2)
  DSCP 41-63 are mapped to yellow ...(3)
  DSCP 8-40 are mapped to red ...(4)
Port1/0/2
  DSCP 0-63 are mapped to green
```

各項目の説明は、以下のとおりです。

表 11-6 show mls qos interface map dscp-color 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)	グリーントラフィックに分類される DSCP を表示します。
(3)	イエロートラフィックに分類される DSCP を表示します。
(4)	レッドトラフィックに分類される DSCP を表示します。

11.2.2 ポリシーマップ機能の表示

ポリシーマップ機能の設定を確認する方法を説明します。

11.2.2.1 クラスマップの表示

show class-map コマンドで、クラスマップを確認できます。

表示例を以下に示します。

```
# show class-map

 Class Map match-any c2 ...(1)
  Match protocol ip ...(2)

 Class Map match-any c3
  Match access-group acl_home_user

 Class Map match-any class-default
  Match any
```

各項目の説明は、以下のとおりです。

表 11-7 show class-map コマンドの表示項目

項番	説明
(1)	クラスマップ内の複数の match ステートメントを評価する方法、およびクラスマップ名を表示します。 • match-all：論理 AND に基づく評価 • match-any：論理 OR に基づく評価
(2)	クラスマップの一致条件を表示します。

11.2.2.2 ポリシーマップの表示

show policy-map コマンドで、ポリシーマップを確認できます。

ポリシーマップ名指定のポリシーマップの表示

ポリシーマップ「policy1」を確認する場合の表示例を以下に示します。

```
# show policy-map policy1

 Policy Map policy1 ...(1)
  Class Map example001 ...(2)
   police cir 500 bc 10 pir 1000 be 10 conform-action transmit exceed-action set-dscp-tr
ansmit 2 violate-action drop ...(3)
```

各項目の説明は、以下のとおりです。

表 11-8 show policy-map コマンドの表示項目

項番	説明
(1)	ポリシーマップ名を表示します。
(2)	ポリシーマップに割り当てられたクラスマップ名を表示します。
(3)	対象のクラスマップに一致したトラフィックに対して行う操作内容（ポリシング、マーキング）を表示します。

ポート指定のポリシーマップの表示

ポート 1/0/1 に適用したポリシーマップを確認する場合の表示例を以下に示します。

```
# show policy-map interface port 1/0/1

 Policy Map: policy1 : input ...(1)
  Class Map example001 ...(2)
   police cir 500 bc 10 pir 1000 be 10 conform-action transmit exceed-action set-dscp-tr
ansmit 2 violate-action drop ...(3)
```

各項目の説明は、以下のとおりです。

表 11-9 show policy-map interface コマンドの表示項目

項番	説明
(1)	ポリシーマップ名およびポリシーマップの動作対象となるトラフィックの方向（受信／送信）を表示します。
(2)	ポリシーマップに割り当てられたクラスマップ名を表示します。
(3)	対象のクラスマップに一致したトラフィックに対して行う操作内容（ポリシング、マーキング）を表示します。

11.2.2.3 集約ポリサーの表示

show mls qos aggregate-policer コマンドで、集約ポリサーを確認できます。

表示例を以下に示します。

```
# show mls qos aggregate-policer

mls qos aggregate-policer agg_policer5 cir 500 bc 10 pir 1000 be 10 conform-action transm
it exceed-action set-dscp-transmit 2 violate-action drop ...(1)
```

各項目の説明は、以下のとおりです。

表 11-10 show mls qos aggregate-policer コマンドの表示項目

項番	説明
(1)	集約ポリサーの設定を表示します。

11.2.3 DSCP 変換機能の表示

DSCP 変換機能の設定を確認する方法を説明します。

11.2.3.1 DSCP 変換マップの表示

show mls qos map dscp-mutation コマンドで、DSCP 変換マップを確認できます。

表示例を以下に示します。

```
# show mls qos map dscp-mutation

DSCP Mutation: mutemap1 ...(1)
Attaching interface: ...(2)
   Port1/0/1

        0  1  2  3  4  5  6  7  8  9 ...(3)
   --------------------------------
   00   00 01 02 03 04 05 06 07 08 09
   10   10 11 12 13 14 15 16 17 18 19
   20   20 21 22 23 24 25 26 27 28 29
   30   30 31 32 33 34 35 36 37 38 39
   40   40 41 42 43 44 45 46 47 48 49
   50   50 51 52 53 54 55 56 57 58 59
   60   60 61 62 63
```

各項目の説明は、以下のとおりです。

表 11-11 show mls qos map dscp-mutation コマンドの表示項目

項番	説明
(1)	DSCP 変換マップ名を表示します。
(2)	DSCP 変換マップが適用されている受信ポート番号を表示します。
(3)	DSCP 変換マップを表形式で表示します。表の縦軸は DSCP の 10 の位を、横軸は DSCP の 1 の位を表します。交差する点に表示されている数値が、変換後 DSCP を表します。

11.2.3.2 ポートに適用した DSCP 変換マップの表示

show mls qos interface dscp-mutation コマンドで、ポートに適用した DSCP 変換マップを確認できます。

ポート 1/0/1 からポート 1/0/2 を指定した場合の表示例を以下に示します。

```
# show mls qos interface port 1/0/1-2 dscp-mutation
 (1)          (2)
 Interface    DSCP Mutation Map
 ----------   ------------------
 Port1/0/1    Mutate Map TEST-MAP1
 Port1/0/2    Mutate Map
```

各項目の説明は、以下のとおりです。

表 11-12 show mls qos interface dscp-mutation 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)	DSCP 変換マップ名を表示します。"Mutate Map" の後に設定した DSCP 変換マップ名が表示されます。

11.2.4 CoS 値から送信キューへのマッピング設定の表示

show mls qos queueing コマンドで、CoS 値から送信キューへのマッピング設定を確認できます。

表示例を以下に示します。

```
# show mls qos queueing

 CoS-queue map:
   (1)   (2)
   CoS   QID
   ---   ---
    0     2
    1     0
    2     1
    3     3
    4     4
    5     5
    6     6
    7     7
```

各項目の説明は、以下のとおりです。

表 11-13 show mls qos queueing コマンドの表示項目

項番	説明
(1)	CoS 値を表示します。
(2)	送信キュー番号を表示します。

11.2.5 送信キューごとの帯域制御設定の表示

show mls qos interface queue-rate-limit コマンドで、送信キューごとの帯域制御設定を確認できます。

ポート 1/0/1 からポート 1/0/2 を指定した場合の表示例を以下に示します。

```
# show mls qos interface port 1/0/1-2 queue-rate-limit

Port1/0/1 ...(1)
 (2)   (3)                  (4)
 QID   Min Bandwidth        Max Bandwidth
 ----  -------------------  -------------------
 0     1000 kbps            2000 kbps
 1     No Limit             No Limit
 2     No Limit             No Limit
 3     10%(100000 kbps)     20%(200000 kbps)
 4     No Limit             No Limit
 5     No Limit             No Limit
 6     No Limit             No Limit
 7     No Limit             No Limit
Port1/0/2
 QID   Min Bandwidth        Max Bandwidth
 ----  -------------------  ------------------
 0     1000 kbps            2000 kbps
 1     No Limit             No Limit
 2     No Limit             No Limit
 3     10%                  20%
 4     No Limit             No Limit
 5     No Limit             No Limit
 6     No Limit             No Limit
 7     No Limit             No Limit
```

各項目の説明は、以下のとおりです。

表 11-14 show mls qos interface queue-rate-limit 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)	送信キューの ID を表示します。
(3)	最小保証帯域（kbps）を表示します。 **queue rate-limit** コマンドで最小保証帯域をパーセント指定で設定した場合は、「リンクアップポート：パーセント設定値と実際の設定値（kbps）を表示」、「リンクダウンポート：パーセント設定値のみ表示」となります。
(4)	最大帯域（kbps）を表示します。 **queue rate-limit** コマンドで最大帯域をパーセント指定で設定した場合は、「リンクアップポート：パーセント設定値と実際の設定値（kbps）を表示」、「リンクダウンポート：パーセント設定値のみ表示」となります。

11.2.6 WRED 機能の表示

WRED 機能の設定や WRED ドロップカウンターを確認する方法を説明します。

CAUTION: NP2100、NP2000、および NP2500 では、WRED は使用できません。

11.2.6.1 WRED プロファイル設定の表示

`show random-detect profile` コマンドで、WRED プロファイル設定を確認できます。

WRED プロファイル 1 を指定した場合の表示例を以下に示します。

```
# show random-detect profile 1


 WRED Profile 1 ...(1)
 (2)               (3)             (4)             (5)
 Packet Type       Min-Threshold   Max-Threshold   Max-Drop-Rate
 ---------------   -------------   -------------   -------------
 TCP-GREEN         20              80              0
 TCP-YELLOW        20              80              0
 TCP-RED           20              80              0
 NON-TCP-GREEN     20              80              0
 NON-TCP-YELLOW    20              80              0
 NON-TCP-RED       20              80              0
```

各項目の説明は、以下のとおりです。

表 11-15 `show random-detect profile` コマンドの表示項目

項番	説明
(1)	WRED プロファイル ID を表示します。
(2)	パケットタイプを表示します。
(3)	WRED の最小しきい値（キューサイズ：セル単位）を表示します。
(4)	WRED の最大しきい値（キューサイズ：セル単位）を表示します。
(5)	平均キューサイズが最大しきい値に達したときの最大廃棄率を指定します。 0-10（0%-10%）、11（25%）、12（50%）、13（75%）、14（100%）

11.2.6.2 ポートの WRED 設定の表示

show queueing random-detect コマンドで、ポートの WRED 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 queueing random-detect interface port 1/0/1

 Current WRED configuration:

   Port1/0/1 ...(1)
   (2)  (3)          (4)                   (5)      (6)
   CoS  WRED State   Exp-weight-constant   Profile  ECN State
   ---  ----------   -------------------   -------  ---------
   0    Disabled     9                     1        Disabled
   1    Disabled     9                     1        Disabled
   2    Disabled     9                     1        Disabled
   3    Disabled     9                     1        Disabled
   4    Disabled     9                     1        Disabled
   5    Disabled     9                     1        Disabled
   6    Disabled     9                     1        Disabled
   7    Disabled     9                     1        Disabled
```

各項目の説明は、以下のとおりです。

表 11-16 show queueing random-detect 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)	CoS キューを表示します。
(3)	WRED 機能の有効 (Enabled) ／無効 (Disabled) を表示します。
(4)	加重係数を表示します。
(5)	WRED プロファイル ID を表示します。
(6)	明示的輻輳通知（ECN）の有効 (Enabled) ／無効 (Disabled) を表示します。

11.2.6.3 WRED ドロップカウンターの表示

show random-detect drop-counter コマンドで、WRED ドロップカウンターを確認できます。また、WRED ドロップカウンターをクリアするには、**clear random-detect drop-counter** コマンドを使用します。

> ***CAUTION:*** NP3000 では、ポートごとの WRED 廃棄パケット数のみ確認できます。トラフィッククラーごとの WRED 廃棄パケット数は確認できません。

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 random-detect drop-counter interface port 1/0/1

 Current WRED Drop Counter:
 (1)        (2)                  (3)                  (4)
 Interface  Green                Yellow               Red
 ---------- -------------------- -------------------- --------------------
 Port1/0/1  0                    0                    0
```

各項目の説明は、以下のとおりです。

表 11-17 show random-detect drop-counter 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)	グリーントラフィックの WRED 廃棄パケット数を表示します。
(3)	イエロートラフィックの WRED 廃棄パケット数を表示します。
(4)	レッドトラフィックの WRED 廃棄パケット数を表示します。

11.2.7 スケジューリング機能の表示

スケジューリング機能の設定を確認する方法を説明します。

11.2.7.1 スケジューリングアルゴリズム設定の表示

show mls qos interface scheduler コマンドで、スケジューリングアルゴリズム設定を確認できます。

ポート 1/0/1 からポート 1/0/2 を指定した場合の表示例を以下に示します。

```
# show mls qos interface port 1/0/1-1/0/2 scheduler
 (1)          (2)
 Interface    Scheduler Method
 ----------   ------------------
 Port1/0/1    sp
 Port1/0/2    wrr
```

各項目の説明は、以下のとおりです。

表 11-18 `show mls qos interface scheduler` 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)	スケジューリングアルゴリズムを表示します。 • sp：Strict Priority Queuing • rr：Round Robin スケジューリング • wrr：WRR（Weighted Round Robin）スケジューリング • wdrr：WDRR（Weighted Deficit Round Robin）スケジューリング

11.2.7.2 WRR と WDRR の重み設定の表示

`show mls qos queueing interface` コマンドで、WRR と WDRR の重み設定を確認できます。

ポート 1/0/3 を指定した場合の表示例を以下に示します。

```
# show mls qos queueing interface port 1/0/3

Interface: Port1/0/3 ...(1)
 wrr bandwidth weights: ...(2)
   QID  Weights
   ---  -------
    0      1
    1      1
    2      1
    3      1
    4      1
    5      1
    6      1
    7      1
 wdrr bandwidth weights: ...(3)
   QID  Quantum
   ---  -------
    0      1
    1      1
    2      1
    3      1
    4      1
    5      1
    6      1
    7      1
```

各項目の説明は、以下のとおりです。

表 11-19 `show mls qos queueing 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)	WRR スケジューリングの重みを表示します。
(3)	WDRR スケジューリングの重みを表示します。

11.2.8 ポートごとの帯域制限設定の表示

show mls qos interface rate-limit コマンドで、ポートごとの帯域制限設定を確認できます。

ポート 1/0/1 からポート 1/0/4 を指定した場合の表示例を以下に示します。

```
# show mls qos interface port 1/0/1-4 rate-limit
 (1)        (2)                 (3)                 (4)           (5)
 Interface  Rx Rate             TX Rate             Rx Burst      Tx Burst
 ---------- ------------------- ------------------- ------------- -------------
 Port1/0/1  1000 kbps           No Limit            64 kbyte      No Limit
 Port1/0/2  No Limit            2000 kbps           No Limit      2000 kbyte
 Port1/0/3  10%(10000 kbps)     20%(20000 kbps)     64 kbyte      64 kbyte
 Port1/0/4  2%                  2000 kbps           64 kbyte      64 kbyte
```

各項目の説明は、以下のとおりです。

表 11-20 show mls qos interface rate-limit 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)	受信帯域制限機能の帯域制限値（kbps）を表示します。 **rate-limit input** コマンドで帯域制限値をパーセント指定で設定した場合は、「リンクアップポート：パーセント設定値と実際の設定値（kbps）を表示」、「リンクダウンポート：パーセント設定値のみ表示」となります。
(3)	送信帯域制限機能の帯域制限値（kbps）を表示します。 **rate-limit output** コマンドで帯域制限値をパーセント指定で設定した場合は、「リンクアップポート：パーセント設定値と実際の設定値（kbps）を表示」、「リンクダウンポート：パーセント設定値のみ表示」となります。
(4)	受信帯域制限機能のバーストサイズ（kbyte）を表示します。
(5)	送信帯域制限機能のバーストサイズ（kbyte）を表示します。

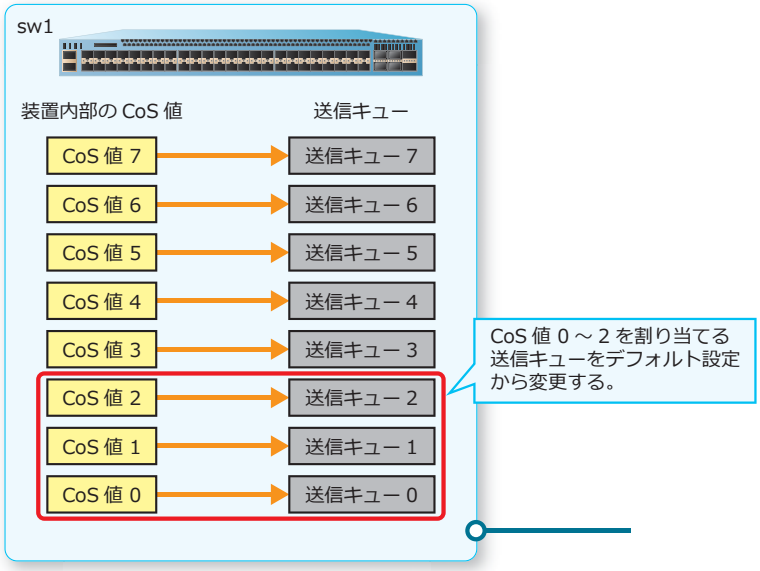
11.3 QoS の構成例と設定例

QoS を利用する場合の構成例と設定例を示します。

11.3.1 CoS 値から送信キューへのマッピングを昇順に変更する場合

CoS 値から送信キューへのマッピングを昇順に変更する場合の構成例と設定例を示します。

図 11-15 CoS 値から送信キューへのマッピングを昇順に変更する場合の構成例



1. 実施前の「CoS 値から送信キューへのマッピング設定」を確認します。

```
sw1# show mls qos queueing

 CoS-queue map:
   CoS    QID
   ---    ---
    0      2
    1      0
    2      1
    3      3
    4      4
    5      5
    6      6
    7      7
```

2. CoS 値から送信キューへのマッピングを昇順に変更するために、以下のように設定します。なお、デフォルト設定の場合は省略しています。

・送信キュー 0 に、CoS 値 =0 を関連付ける

・送信キュー 1 に、CoS 値 =1 を関連付ける

・送信キュー 2 に、CoS 値 =2 を関連付ける

```
sw1# configure terminal
sw1(config)# priority-queue cos-map 0 0
sw1(config)# priority-queue cos-map 1 1
sw1(config)# priority-queue cos-map 2 2
sw1(config)# end
sw1#
```

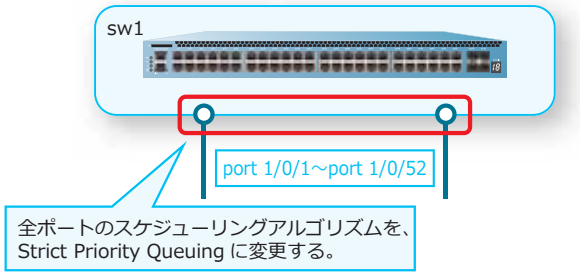
3. 実施後の「CoS 値から送信キューへのマッピング設定」を確認します。

```
sw1# show mls qos queueing

 CoS-queue map:
   CoS    QID
   ---    ---
    0      0
    1      1
    2      2
    3      3
    4      4
    5      5
    6      6
    7      7
```

11.3.2 Strict Priority Queuing に変更する場合

ApresiaNP2000-48T4X の全ポート（1/0/1-52）のスケジューリングアルゴリズムを、Strict Priority Queuing に変更する場合の設定例を示します。

図 11-16 Strict Priority Queuing に変更する場合の構成例



1. 実施前のスケジューリング設定を確認します。

```
sw1# show mls qos interface scheduler

 Interface      Scheduler Method
 ------------   -----------------
 Port1/0/1      wrr
 Port1/0/2      wrr
 Port1/0/3      wrr
～～省略～～
 Port1/0/50     wrr
 Port1/0/51     wrr
 Port1/0/52     wrr
```

2. 全ポート（1/0/1-52）で、スケジューリングアルゴリズムを Strict Priority Queuing に設定します。

```
sw1# configure terminal
sw1(config)# interface range port 1/0/1-52
sw1(config-if-port-range)# mls qos scheduler sp
sw1(config-if-port-range)# end
sw1#
```

3. 実施後のスケジューリング設定を確認します。

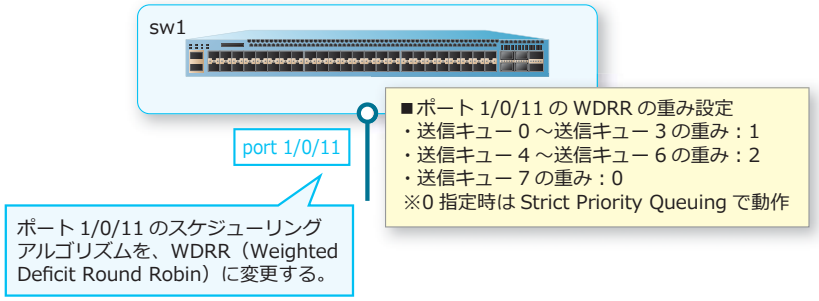
```
sw1# show mls qos interface scheduler

 Interface      Scheduler Method
 ------------   -----------------
 Port1/0/1      sp
 Port1/0/2      sp
 Port1/0/3      sp
～～省略～～
 Port1/0/50     sp
 Port1/0/51     sp
 Port1/0/52     sp
```

11.3.3 WDRR（Weighted Deficit Round Robin）に変更する場合

ポート 1/0/11 のスケジューリングアルゴリズムを、WDRR（Weighted Deficit Round Robin）に変更する場合の構成例と設定例を示します。なお、重みは以下になるように設定します。

- 送信キュー 0 ～送信キュー 3 の重み：1
- 送信キュー 4 ～送信キュー 6 の重み：2
- 送信キュー 7 の重み：0
  ※0 指定時は Strict Priority Queuing で動作

図 11-17 WDRR（Weighted Deficit Round Robin）に変更する場合の構成例



1. 実施前のポート 1/0/11 のスケジューリング設定と、WDRR の重み設定を確認します。

```
sw1# show mls qos interface port 1/0/11 scheduler

 Interface     Scheduler Method
 ------------  -----------------
 Port1/0/11    wrr

sw1# show mls qos queueing interface port 1/0/11

Interface: Port1/0/11
 wrr bandwidth weights:
   QID  Weights
   ---  -------
    0     1
    1     1
    2     1
    3     1
    4     1
    5     1
    6     1
    7     1
 wdrr bandwidth weights:
   QID  Quantum
   ---  -------
    0     1
    1     1
    2     1
    3     1
    4     1
    5     1
    6     1
    7     1
```

2. ポート 1/0/11 で、スケジューリングアルゴリズムを WDRR（Weighted Deficit Round Robin）に設定します。また、WDRR の重みを［送信キュー 0 ～送信キュー 3 の重み：1］［送信キュー 4 ～送信キュー 6 の重み：2］［送信キュー 7 の重み：0 ※Strict Priority Queuing］に設定します。

```
sw1# configure terminal
sw1(config)# interface port 1/0/11
sw1(config-if-port)# mls qos scheduler wdrr
sw1(config-if-port)# wdrr-queue bandwidth 1 1 1 1 2 2 2 0
sw1(config-if-port)# end
sw1#
```

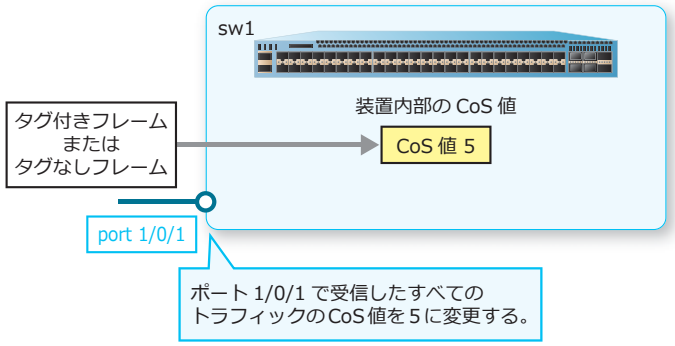
3. 実施後のポート 1/0/11 のスケジューリング設定と、WDRR の重み設定を確認します。

```
sw1# show mls qos interface port 1/0/11 scheduler

 Interface      Scheduler Method
 ------------   -----------------
 Port1/0/11     wdrr

sw1# show mls qos queueing interface port 1/0/11

Interface: Port1/0/11
 wrr bandwidth weights:
   QID  Weights
   ---  -------
    0      1
    1      1
    2      1
    3      1
    4      1
    5      1
    6      1
    7      1
 wdrr bandwidth weights:
   QID  Quantum
   ---  -------
    0      1
    1      1
    2      1
    3      1
    4      2
    5      2
    6      2
    7      0
```

11.3.4 受信したすべてのトラフィックの CoS 値を変更する場合

ポート 1/0/1 で受信したすべてのトラフィック（タグ付きフレーム、タグなしフレーム）の CoS 値を 5 に変更する場合の構成例と設定例を示します。

図 11-18 受信したすべてのトラフィックの CoS 値を変更する場合の構成例



1. 実施前のポート 1/0/1 のデフォルト CoS 値を確認します。

```
sw1# show mls qos interface port 1/0/1 cos

 Interface      CoS    Override
 ------------   ----   ---------
 Port1/0/1      0      No
```

2. ポート 1/0/1 で、デフォルト CoS 値を［5］に設定します。また、すべてのトラフィック（タグ付きフレーム、タグなしフレーム）を対象にするために override オプションも設定します。

```
sw1# configure terminal
sw1(config)# interface port 1/0/1
sw1(config-if-port)# mls qos cos 5
sw1(config-if-port)# mls qos cos override
sw1(config-if-port)# end
sw1#
```

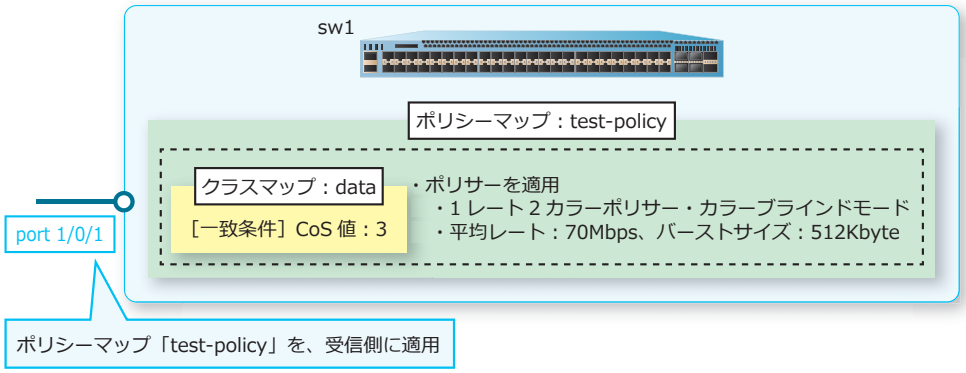
3. 実施後のポート 1/0/1 のデフォルト CoS 値を確認します。

```
sw1# show mls qos interface port 1/0/1 cos

 Interface      CoS    Override
 ------------   ----   ---------
 Port1/0/1      5      Yes
```

11.3.5 ポリシーマップによるポリシングの設定例

ポート 1/0/1 で受信した「CoS 値：3」のトラフィックに対して、受信側でポリシングを適用する場合の構成例と設定例を示します。

図 11-19 ポリシーマップによるポリシングの構成例



1. クラスマップ［data］を作成し、一致条件を［CoS 値：3］に設定します。

```
sw1# configure terminal
sw1(config)# class-map data
sw1(config-cmap)# match cos 3
sw1(config-cmap)# exit
sw1(config)#
```

2. ポリシーマップ［test-policy］を作成します。

```
sw1(config)# policy-map test-policy
sw1(config-pmap)#
```

3. ポリシーマップにクラスマップ［data］を関連付け、［data］に分類されたトラフィックに対して［1 レート 2 カラーポリサー・カラーブラインドモード］を適用します。ポリサーは、平均レート［70Mbps］、バーストサイズ［512Kbyte］、イエロートラフィックに対するアクション［破棄］と設定します。

```
sw1(config-pmap)# class data
sw1(config-pmap-c)# police 70000 512 exceed-action drop
sw1(config-pmap-c)# exit
sw1(config-pmap)# exit
sw1(config)#
```

4. ポート 1/0/1 の受信側に、ポリシーマップ［test-policy］を適用します。

```
sw1(config)# interface port 1/0/1
sw1(config-if-port)# service-policy input test-policy
sw1(config-if-port)# end
sw1#
```

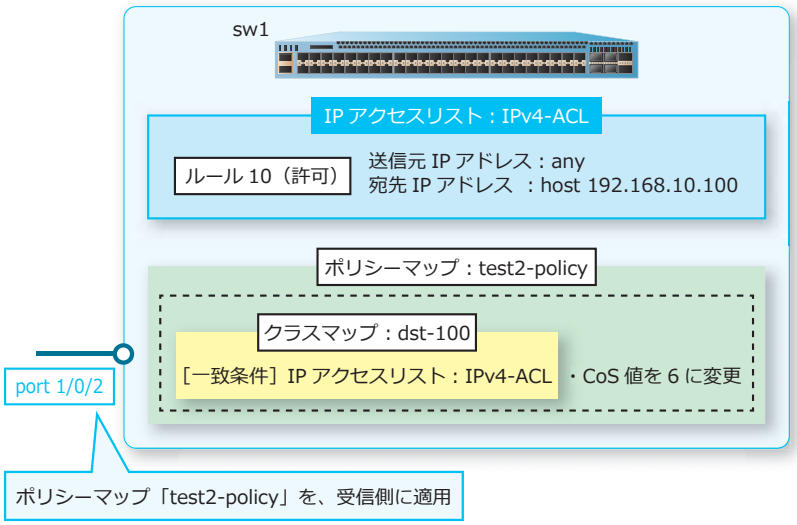
5. 実施後に、ポート 1/0/1 に適用したポリシーマップと、クラスマップ「data」を確認します。

```
sw1# show policy-map interface port 1/0/1

 Policy Map: test-policy : input
  Class Map data
   police 70000 512 conform-action transmit exceed-action drop

sw1# show class-map data

 Class Map match-any data
  Match 802.1P 3
```

11.3.6 ポリシーマップによるリマーキングの設定例

ポート 1/0/2 で受信した「192.168.10.100 宛てのトラフィック」に対して、受信側で CoS 値を 6 に変更する場合の構成例と設定を示します。

図 11-20 ポリシーマップによるリマーキングの構成例



1. IP アクセスリスト［IPv4-ACL］を作成します。クラスマップ「dst-100」の対象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［any］、宛先 IP アドレス［host 192.168.10.100］

```
sw1# configure terminal
sw1(config)# ip access-list IPv4-ACL
sw1(config-ip-acl)# 10 permit any host 192.168.10.100
sw1(config-ip-acl)# exit
sw1(config)#
```

2. クラスマップ［dst-100］を作成し、一致条件を［IP アクセスリスト：IPv4-ACL］に設定します。

```
sw1(config)# class-map dst-100
sw1(config-cmap)# match access-group name IPv4-ACL
sw1(config-cmap)# exit
sw1(config)#
```

3. ポリシーマップ［test2-policy］を作成します。

```
sw1(config)# policy-map test2-policy
sw1(config-pmap)#
```

4. ポリシーマップにクラスマップ［dst-100］を関連付け、［dst-100］に分類されたトラフィックに対して CoS 値を［6］に変更するアクションを適用します。

```
sw1(config-pmap)# class dst-100
sw1(config-pmap-c)# set cos 6
sw1(config-pmap-c)# exit
sw1(config-pmap)# exit
sw1(config)#
```

5. ポート 1/0/2 の受信側に、ポリシーマップ［test2-policy］を適用します。

```
sw1(config)# interface port 1/0/2
sw1(config-if-port)# service-policy input test2-policy
sw1(config-if-port)# end
sw1#
```

6. 実施後に、ポート 1/0/2 に適用したポリシーマップと、クラスマップ「dst-100」、および IP アクセスリスト「IPv4-ACL」を確認します。

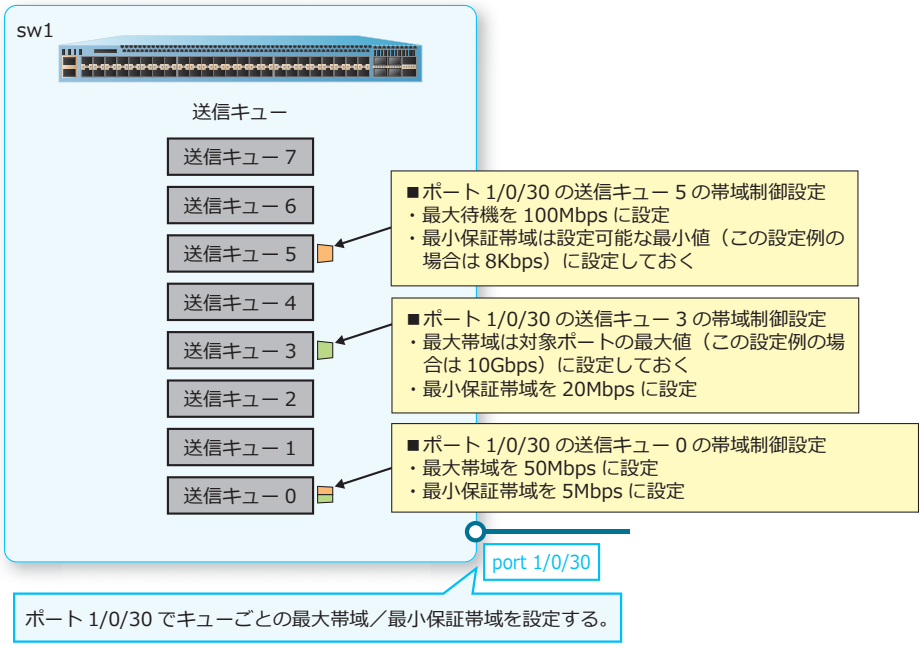
```
sw1# show policy-map interface port 1/0/2

 Policy Map: test2-policy : input
  Class Map dst-100
   set 802.1P 6

sw1# show class-map dst-100

 Class Map match-any dst-100
  Match access-group IPv4-ACL

sw1# show access-list ip IPv4-ACL

Standard IP access list IPv4-ACL(ID: 1999)
    10 permit any host 192.168.10.100
```

11.3.7 送信キューの最大帯域／最小保証帯域の設定例

ApresiaNP7000-48X6L のポート 1/0/30（10Gbps 想定）の送信キューで、以下のように最大帯域／最小保証帯域を使用する場合の構成例と設定例を示します。

- 送信キュー 5 で 100Mbps に帯域制限（最小保証帯域は設定可能な最小値に設定しておく）
- 送信キュー 3 で 20Mbps の帯域保証（最大帯域は対象ポートの最大値に設定しておく）
- 送信キュー 0 で 50Mbps に帯域制限、5Mbps の帯域保証

図 11-21 送信キューの最大帯域／最小保証帯域の構成例



1. 実施前のポート 1/0/30 のキューごとの帯域制御設定を確認します。

```
sw1# show mls qos interface port 1/0/30 queue-rate-limit

Port1/0/30
 QID    Min Bandwidth          Max Bandwidth
 ----   --------------------   --------------------
 0      No Limit               No Limit
 1      No Limit               No Limit
 2      No Limit               No Limit
 3      No Limit               No Limit
 4      No Limit               No Limit
 5      No Limit               No Limit
 6      No Limit               No Limit
 7      No Limit               No Limit
```

2. ポート 1/0/30 の送信キュー 5 で、最大帯域を［100Mbps］に設定します。最小保証帯域は NP7000 の設定可能な最小値（8Kbps）に設定しておきます。

```
sw1# configure terminal
sw1(config)# interface port 1/0/30
sw1(config-if-port)# queue 5 rate-limit 8 100000
sw1(config-if-port)#
```

3. ポート 1/0/30 の送信キュー 3 で、最小保証帯域を［20Mbps］に設定します。最大帯域は対象ポートの最大値（10Gbps 想定）に設定しておきます。

```
sw1(config-if-port)# queue 3 rate-limit 20000 10000000
sw1(config-if-port)#
```

4. ポート 1/0/30 の送信キュー 0 で、最小保証帯域を［5Mbps］に、最大帯域を［50Mbps］に設定します。

```
sw1(config-if-port)# queue 0 rate-limit 5000 50000
sw1(config-if-port)# end
sw1#
```

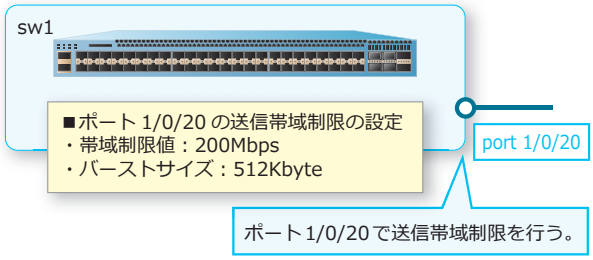
5. 実施後のポート 1/0/30 のキューごとの帯域制御設定を確認します。

```
sw1# show mls qos interface port 1/0/30 queue-rate-limit

Port1/0/30
 QID   Min Bandwidth        Max Bandwidth
 ----  -------------------  -------------------
 0     5000 kbps            50000 kbps
 1     No Limit             No Limit
 2     No Limit             No Limit
 3     20000 kbps           10000000 kbps
 4     No Limit             No Limit
 5     8 kbps               100000 kbps
 6     No Limit             No Limit
 7     No Limit             No Limit
```

11.3.8 送信ポートの帯域制限の設定例

ポート 1/0/20 で、送信帯域制限を「帯域制限値：200Mbps」「バーストサイズ：512Kbyte」で設定する場合の構成例と設定例を示します。

図 11-22 送信ポートの帯域制限の構成例



1. 実施前のポート 1/0/20 の帯域制限設定を確認します。

```
sw1# show mls qos interface port 1/0/20 rate-limit

 Interface  Rx Rate              TX Rate              Rx Burst      Tx Burst
 ---------- -------------------- -------------------- ------------- -------------
 Port1/0/20 No Limit             No Limit             No Limit      No Limit
```

2. ポート 1/0/20 で、送信帯域制限を［帯域制限値：200Mbps］［バーストサイズ：512Kbyte］に設定します。

```
sw1# configure terminal
sw1(config)# interface port 1/0/20
sw1(config-if-port)# rate-limit output 200000 512
sw1(config-if-port)# end
sw1#
```

3. 実施後のポート 1/0/20 の帯域制限設定を確認します。

```
sw1# show mls qos interface port 1/0/20 rate-limit

 Interface  Rx Rate              TX Rate              Rx Burst      Tx Burst
 ---------- -------------------- -------------------- ------------- -------------
 Port1/0/20 No Limit             200000 kbps          No Limit      512 kbyte
```

12. マルチキャストフィルター

マルチキャストフィルタリングモードの機能、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。

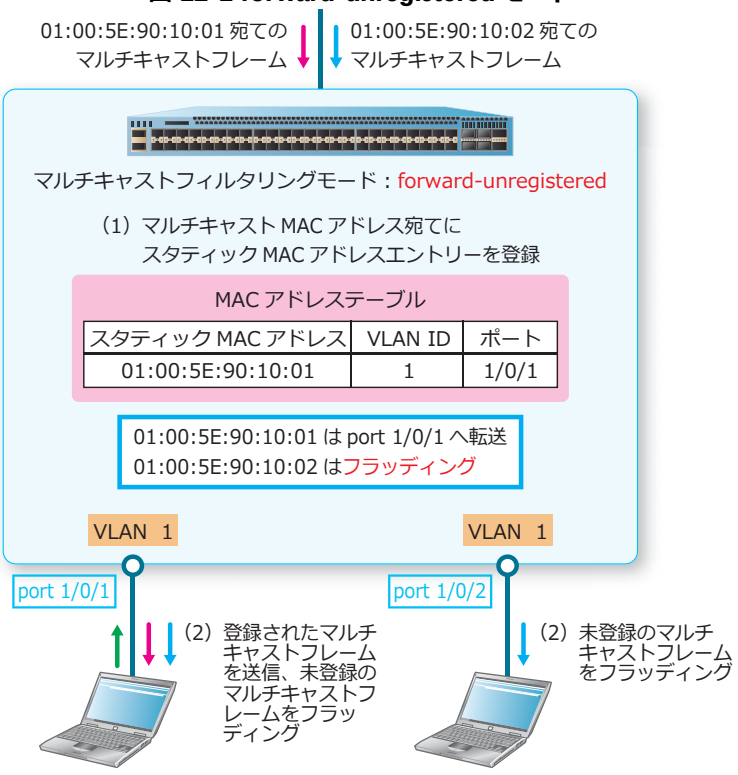
12.1 マルチキャストフィルタリングモードの機能説明

VLAN ごとにマルチキャストフレームの中継処理方法を設定できます。設定を変更するには、**`multicast filtering-mode`** コマンドを使用します。

デフォルト設定での動作（forward-unregistered モード）

デフォルトの forward-unregistered モードの場合は、スタティックに設定したマルチキャスト MAC アドレス宛てのマルチキャストフレームを登録されたポートのみに転送し、未登録のマルチキャストフレームをフラッディングします。IGMP スヌーピング／ MLD スヌーピング使用時には、テーブル上限を超えて登録できなかったマルチキャストパケットもフラッディングされます。

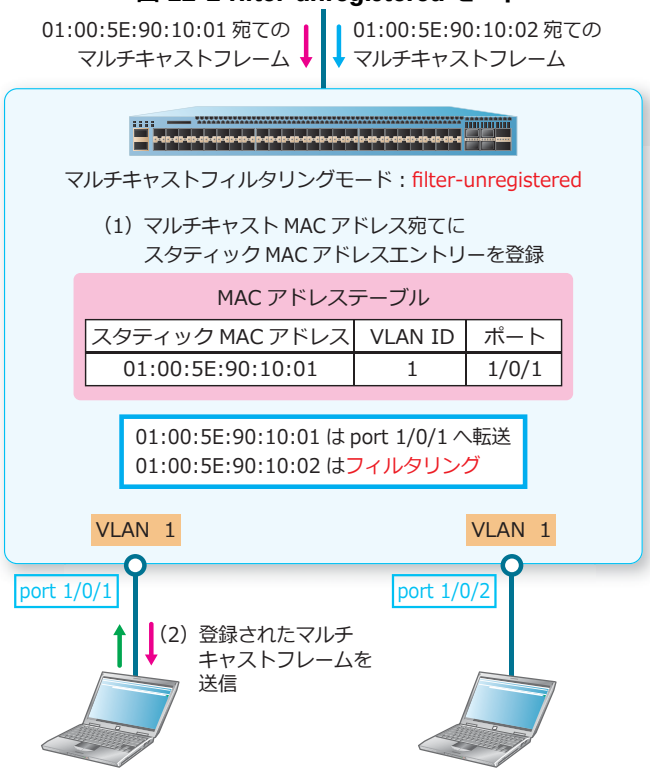
図 12-1 forward-unregistered モード



マルチキャストフレームのフィルタリング（filter-unregistered モード）

filter-unregistered モードの場合は、スタティックに設定したマルチキャスト MAC アドレス宛てのマルチキャストフレームを登録されたポートのみに転送し、未登録のマルチキャストフレームをフィルタリングできます。IGMP スヌーピング／ MLD スヌーピング使用時には、テーブル上限を超えて登録できなかったマルチキャストパケットもフィルタリングされます。

図 12-2 filter-unregistered モード



マルチキャストフレームのフラッディング（forward-all モード）

forward-all モードの場合は、マルチキャスト MAC アドレス宛てのスタティック MAC アドレスエントリーの設定にかかわらず、すべてのマルチキャストフレームを同一 VLAN のすべてのポートにフラッディングします。IGMP スヌーピング／ MLD スヌーピング使用時には、テーブルの登録の有無にかかわらず、マルチキャストパケットを同一 VLAN のすべてのポートにフラッディングします。

12.2 マルチキャストフィルタリングモードの状態確認

マルチキャストフィルタリングモードの状態を表示して確認する方法を説明します。

12.2.1 マルチキャストフィルタリングモードの表示

show multicast filtering-mode コマンドで、マルチキャストフィルタリングモードを確認できます。

表示例を以下に示します。

```
# show multicast filtering-mode
(1)                              (2)
Interface                        Layer 2 Multicast Filtering Mode
-------------------------------  -------------------------------
default                          forward-unregistered
VLAN0002                         forward-unregistered

Total Entries: 2
```

各項目の説明は、以下のとおりです。

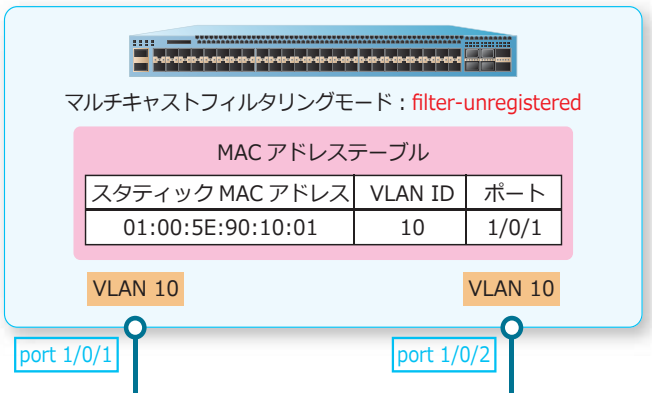
表 12-1 show multicast filtering-mode コマンドの表示項目

項番	説明
(1)	VLAN 名を表示します。
(2)	マルチキャストフィルタリングモードを表示します。 • forward-all：すべてのマルチキャストフレームをフラッディング • forward-unregistered：登録済みのマルチキャストフレームは登録されたポートのみに転送し、未登録のマルチキャストフレームはフラッディング • filter-unregistered：登録済みのマルチキャストフレームは登録されたポートのみに転送し、未登録のマルチキャストフレームはフィルタリング

12.3 マルチキャストフィルタリングモードの構成例と設定例

VLAN 10 で、マルチキャストフィルタリングモードを filter-unregistered モードにする場合の構成例と設定例を示します。この設定例では、マルチキャストアドレス宛てのスタティック MAC アドレスエントリーも設定しています。

図 12-3 マルチキャストフィルタリングモードの構成例



1. VLAN 10 を作成します。

```
# configure terminal
(config)# vlan 10
(config-vlan)# exit
(config)#
```

2. ポート 1/0/1 およびポート 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 10］を割り当てます。

```
(config)# interface range port 1/0/1-2
(config-if-port-range)# switchport mode access
(config-if-port-range)# switchport access vlan 10
(config-if-port-range)# exit
(config)#
```

3. VLAN 10 で、マルチキャストフィルタリングモードを［filter-unregistered］に設定します。

```
(config)# vlan 10
(config-vlan)# multicast filtering-mode filter-unregistered
(config-vlan)# exit
(config)#
```

4. スタティック MAC アドレスエントリー［01:00:5E:90:10:01］［VLAN 10］［転送先ポート 1/0/1］を設定します。

```
(config)# mac-address-table static 0100.5e90.1001 vlan 10 interface port 1/0/1
(config)# end
#
```

5. 実施後のマルチキャストフィルタリングモードと、スタティック MAC アドレスエントリーを確認します。

```
# show multicast filtering-mode vlan 10

Interface                        Layer 2 Multicast Filtering Mode
-------------------------------  --------------------------------
VLAN0010                         filter-unregistered

Total Entries: 1

# show mac-address-table static vlan 10

VLAN  MAC Address        Type        Ports
----  -----------------  ----------  -------------------------
  10  01-00-5E-90-10-01  Static      Port1/0/1

Total Entries: 1

#
```

13. IGMP スヌーピング／ MLD スヌーピング

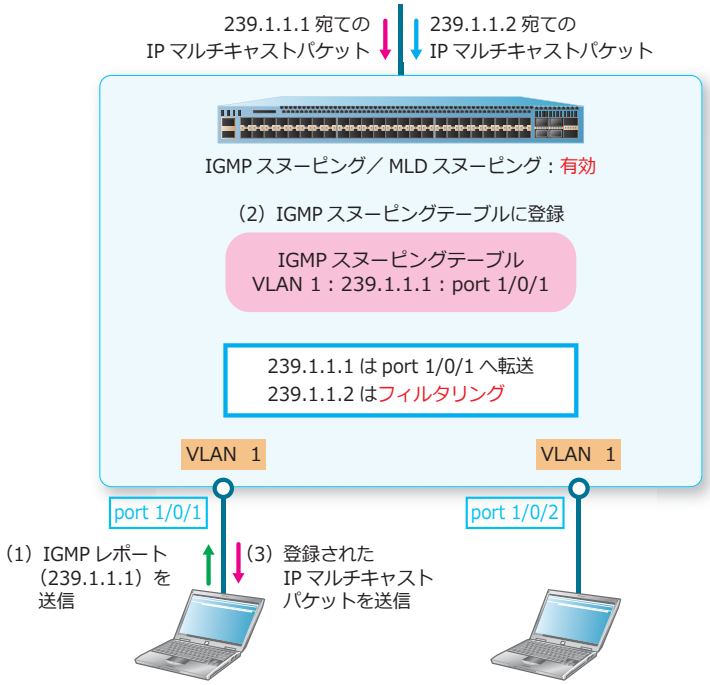
IGMP スヌーピング／ MLD スヌーピングの機能、状態の確認方法、および構成例と設定例について説明します。

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 IGMP スヌーピング／ MLD スヌーピングの機能説明

IGMP スヌーピング／ MLD スヌーピングを有効化すると、IP マルチキャストのレイヤー 2 中継はフィルタリングされます。装置はホストから送られてくる参加要求（IGMP レポート／ MLD レポート）を受信すると、IP マルチキャストを転送する宛先ポートを登録します。これにより、IGMP スヌーピングテーブル／ MLD スヌーピングテーブルに登録された IP マルチキャストは、登録された宛先ポートのみに転送されます。

図 13-1 IGMP スヌーピング／ MLD スヌーピングの概要



IGMP スヌーピングを有効にするには、VLAN および装置全体に対して **`ip igmp snooping`** コマンドを使用します。MLD スヌーピングを有効にするには、VLAN および装置全体に対して **`ipv6 mld snooping`** コマンドを使用します。

また、IGMP スヌーピングテーブルに登録されたエントリーを削除するには、**`clear ip igmp snooping groups`** コマンドを使用します。MLD スヌーピングテーブルに登録されたエントリーを削除するには、**`clear ipv6 mld snooping groups`** コマンドを使用します。

NOTE: NP7000、NP5000、NP4000、および NP3000 では、IGMP スヌーピング／ MLD スヌーピングは IP アドレスベースで処理されます。

NOTE: NP2100、NP2000、および NP2500 では、IGMP スヌーピング／ MLD スヌーピングは MAC アドレスベースで処理されます。そのため、同一 MAC アドレスになる IP マルチキャストの中継動作は同じになります。

13.1.1 IP マルチキャストの中継動作

IGMP スヌーピング／ MLD スヌーピングでは、登録状況に応じて IP マルチキャストの中継動作が異なります。登録状況ごとの中継動作を以下に示します。

(1) IGMP スヌーピングエントリー／ MLD スヌーピングエントリーとして登録済み

ホストからの参加要求を受信して、IGMP スヌーピングテーブル／ MLD スヌーピングテーブルに宛先ポートが登録されたエントリー宛ての IP マルチキャストは、登録された宛先ポートとマルチキャストルーターポートにのみ転送されます。それ以外のポートには転送されません。IGMP スヌーピングテーブルに登録済みのエントリーは、**show ip igmp snooping groups** コマンドで確認可能です。MLD スヌーピングテーブルに登録済みのエントリーは、**show ipv6 mld snooping groups** コマンドで確認可能です。

IGMP スヌーピングテーブル／ MLD スヌーピングテーブルに登録されたエントリーは、ハードウェア中継するためのマルチキャスト転送キャッシュにも登録されます。IPv4 マルチキャスト転送キャッシュを確認するには、**show ip mroute forwarding-cache** コマンドを使用します。IPv6 マルチキャスト転送キャッシュを確認するには、**show ipv6 mroute forwarding-cache** コマンドを使用します。

> ***REF:*** IPv4 マルチキャスト転送キャッシュについては、「第 5 編 レイヤー 3」の「IPv4 マルチキャスト転送キャッシュの表示」を参照してください。
>
> ***REF:*** IPv6 マルチキャスト転送キャッシュについては、「第 5 編 レイヤー 3」の「IPv6 マルチキャスト転送キャッシュの表示」を参照してください。

(2) 宛先が未知でマルチキャスト転送キャッシュに登録済み

ホストからの参加要求は受信していないが、IP マルチキャストを受信して IPv4 マルチキャスト転送キャッシュ／ IPv6 マルチキャスト転送キャッシュに登録済みの IP マルチキャストは、マルチキャストルーターポートにのみ転送されます。それ以外のポートには転送されません。

NP7000、NP5000、NP4000、および NP3000 の場合、このケースの IP マルチキャストは IGMP スヌーピングテーブル／ MLD スヌーピングテーブルには登録されませんが、マルチキャスト転送キャッシュにはリソースの範囲内で上限まで登録されます。上限を超えて登録されなかった IP マルチキャストが「(3) 未登録の IP マルチキャスト」になります。

NP2100、NP2000、および NP2500 の場合、このケースの IP マルチキャストはマルチキャスト転送キャッシュだけでなく、「宛先が未知の IP マルチキャスト」として IGMP スヌーピングテーブル／ MLD スヌーピングテーブルにも登録されます。「宛先が未知の IP マルチキャスト」の上限を超えて登録されなかった IP マルチキャストが「(3) 未登録の IP マルチキャスト」になります。なお、「宛先が未知の IP マルチキャスト」を学習する機能はデフォルト設定では有効ですが、無効にすることもできます。

(3) 未登録の IP マルチキャスト

IGMP スヌーピングテーブル／ MLD スヌーピングテーブルに未登録の IP マルチキャスト、および IPv4 マルチキャスト転送キャッシュ／ IPv6 マルチキャスト転送キャッシュに未登録の IP マルチキャストは、すべてのポートに転送されます。

「(3) 未登録の IP マルチキャスト」の転送は、フィルタリングできます。IGMP スヌーピングでフィルタリングするには、**ip igmp snooping unregistered-filter** コマンドでフィルタリングする宛先インターフェースを指定して設定します。MLD スヌーピングでフィルタリングするには、**ipv6 mld snooping unregistered-filter** コマンドでフィルタリングする宛先インターフェースを指定して設定します。

> ***NOTE:*** **ip igmp snooping unregistered-filter** コマンド、および **ipv6 mld snooping unregistered-filter** コマンドは、NP7000 の 1.10.02 以降、NP5000 の 1.11.01 以降、NP3000 の 1.10.01 以降、NP2100 の 1.12.01 以降、NP2500 の 1.12.01 以降でサポートしています。
>
> ***NOTE:*** **ip igmp snooping unregistered-filter** コマンド、および **ipv6 mld snooping unregistered-filter** コマンドを使用する場合、**multicast filtering-mode** コマンドはデフォルト設定（forward-unregistered モード）のまま使用してください。また、同一ポート／同一ポートチャネルで「宛先不明マルチキャストフレームを対象にした Egress フィルタリング（**egress-filtering umc** コマンド）」との併用は未サポートです。
>
> ***NOTE:*** **ip igmp snooping unregistered-filter** コマンドを使用する場合、アクセスリストのリソース（Ingress）を 1 グループ占有します。
>
> ***NOTE:*** **ipv6 mld snooping unregistered-filter** コマンドを使用する場合、アクセスリストのリソース（Ingress）を 1 グループ占有します。
>
> ***NOTE:*** **ip igmp snooping unregistered-filter** コマンド、および **ipv6 mld snooping unregistered-filter** コマンドをサポートしていない機種やバージョンの場合、「(3) 未登録の IP マルチキャスト」の転送をフィルタリングする方法としては、「対象 VLAN で **multicast filtering-mode** コマンドを filter-unregistered モードに設定する方法」や、「宛先不明マルチキャストフレームを対象にした Egress フィルタリング（**egress-filtering umc** コマンド）を利用する方法」があります。それぞれの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。

13.1.1.1 宛先が未知の IP マルチキャスト関連の設定

NP2100、NP2000、および NP2500 では、ホストからの参加要求を受信していない状態で IP マルチキャストを受信した場合は、対象の IP マルチキャストはマルチキャスト転送キャッシュだけでなく、「宛先が未知の IP マルチキャスト」として IGMP スヌーピングテーブル／ MLD スヌーピングテーブルにも登録されます。「宛先が未知の IP マルチキャスト」はマルチキャストルーターポートにのみ転送され、それ以外のポートには転送されません。

宛先が未知の IP マルチキャスト関連の設定を以下に示します。

- **「宛先が未知の IP マルチキャスト」を学習する機能の有効／無効**

  デフォルト設定では有効に設定されています。設定を変更するには、**ip igmp snooping unknown-data learn** コマンド、または **ipv6 mld snooping unknown-data learn** コマンドを使用します。

- **「宛先が未知の IP マルチキャスト」の有効期限**

  デフォルト設定では有効期限なしに設定されています。設定を変更するには、**ip igmp snooping unknown-data expiry-time** コマンド、または **ipv6 mld snooping unknown-data expiry-time** コマンドを使用します。

- **「宛先が未知の IP マルチキャスト」の登録上限数**

  デフォルト設定では 128 個に設定されています。設定を変更するには、**ip igmp snooping unknown-data limit** コマンド、または **ipv6 mld snooping unknown-data limit** コマンドを使用します。

IGMP スヌーピングテーブルに登録された「宛先が未知の IP マルチキャスト」だけを対象にして削除するには、**clear ip igmp snooping unknown-data** コマンドを使用します。MLD スヌーピングテーブルに登録された「宛先が未知の IP マルチキャスト」だけを対象にして削除するには、**clear ipv6 mld snooping unknown-data** コマンドを使用します。

13.1.2 マルチキャストルーターポート

IGMP スヌーピング／ MLD スヌーピングを有効にすると、クエリーの受信ポートや PIM 制御パケットの受信ポートを、マルチキャストルーターポートとして動的に学習します。

マルチキャストルーターポートは、スタティックに設定することもできます。IGMP スヌーピングでマルチキャストルーターポートをスタティックに設定するには、**ip igmp snooping mrouter** コマンドを使用します。MLD スヌーピングでマルチキャストルーターポートをスタティックに設定するには、**ipv6 mld snooping mrouter** コマンドを使用します。

また、動的に学習してマルチキャストルーターポートになることを禁止する設定も可能です。IGMP スヌーピングでマルチキャストルーターポートになることを禁止するインターフェースを設定するには、**ip igmp snooping mrouter forbidden** コマンドを使用します。MLD スヌーピングでマルチキャストルーターポートになることを禁止するインターフェースを設定するには、**ipv6 mld snooping mrouter forbidden** コマンドを使用します。

13.1.3 参加要求を許可する最小バージョンの設定

ホストから送られてくる参加要求（IGMP レポート／ MLD レポート）を許可する最小バージョンを設定できます。

IGMP スヌーピングでホストからの参加要求（Membership Report）を許可する IGMP の最小バージョンを設定すると、以下のように動作します。最小バージョンを設定するには、**ip igmp snooping minimum-version** コマンドを使用します。

- デフォルト設定では、すべてのバージョンの参加要求を許可
- 最小バージョンを 2 に設定すると、IGMP バージョン 1 の参加要求を拒否
- 最小バージョンを 3 に設定すると、IGMP バージョン 1 および IGMP バージョン 2 の参加要求を拒否

MLD スヌーピングでホストからの参加要求（Multicast Listener Report）を許可する MLD の最小バージョンを設定すると、以下のように動作します。最小バージョンを設定するには、**ipv6 mld snooping minimum-version** コマンドを使用します。

- デフォルト設定では、すべてのバージョンの参加要求を許可
- 最小バージョンを 2 に設定すると、MLD バージョン 1 の参加要求を拒否

13.1.4 高速離脱機能

高速離脱機能が有効な場合は、ホストからの離脱要求を受信すると、即座に対象の IGMP スヌーピングエントリー／ MLD スヌーピングエントリーを削除します。

> ***NOTE:*** 高速離脱機能は、ポートにホストが 1 台だけ接続されている場合に効果があります。ハブを介して複数のホストを接続している場合は、高速離脱機能を有効にしないでください。

IGMP スヌーピングで高速離脱機能を有効にするには、**ip igmp snooping fast-leave** コマンドを使用します。group-list オプションで高速離脱の対象にするマルチキャストグループを定義した IP アクセスリストを指定することもできます。

MLD スヌーピングで高速離脱機能を有効にするには、**ipv6 mld snooping fast-leave** コマンドを使用します。group-list オプションで高速離脱の対象にするマルチキャストグループを定義した IPv6 アクセスリストを指定することもできます。

13.1.5 スタティックエントリーの設定

IGMP スヌーピングエントリー／ MLD スヌーピングエントリーは、スタティックに設定することもできます。

IGMP スヌーピングでスタティックエントリーを設定するには、**ip igmp snooping static-group** コマンドを使用します。MLD スヌーピングでスタティックエントリーを設定するには、**ipv6 mld snooping static-group** コマンドを使用します。

13.1.6 クエリア関連の設定

IGMP スヌーピング／ MLD スヌーピングでは、本装置をクエリアとして動作させることができます。

> ***NOTE:*** IGMP スヌーピングのクエリアを有効にするには、対象 VLAN の VLAN インターフェースを作成し、IPv4 アドレスを設定してください。

> ***NOTE:*** MLD スヌーピングのクエリアを有効にするには、対象 VLAN の VLAN インターフェースを作成し、IPv6 アドレスを設定してください。

IGMP スヌーピングのクエリアに関連する設定を、以下に示します。各コマンドの詳細は『コマンドリファレンス』を参照してください。

表 13-1 IGMP スヌーピングのクエリア機能に関する設定

設定内容	デフォルト設定	設定コマンド
クエリアの有効／無効	無効	**ip igmp snooping querier** コマンド
クエリアのバージョン	IGMP バージョン 3	**ip igmp snooping query-version** コマンド
定期的に送信する Membership Query の送信間隔	125 秒	**ip igmp snooping query-interval** コマンド
Membership Query で通知される最大応答時間	10 秒	**ip igmp snooping query-max-response-time** コマンド
ロバストネス変数	2	**ip igmp snooping robustness-variable** コマンド
Group-Specific Query の送信間隔	1 秒	**ip igmp snooping last-member-query-interval** コマンド

MLD スヌーピングのクエリアに関連する設定を、以下に示します。各コマンドの詳細は『コマンドリファレンス』を参照してください。

表 13-2 MLD スヌーピングのクエリア機能に関する設定

設定内容	デフォルト設定	設定コマンド
クエリアの有効／無効	無効	**ipv6 mld snooping querier** コマンド
クエリアのバージョン	MLD バージョン 2	**ipv6 mld snooping query-version** コマンド
定期的に送信する Multicast Listener Query の送信間隔	125 秒	**ipv6 mld snooping query-interval** コマンド
Multicast Listener Query で通知される最大応答時間	10 秒	**ipv6 mld snooping query-max-response-time** コマンド
ロバストネス変数	2	**ipv6 mld snooping robustness-variable** コマンド
Multicast Address Specific Query の送信間隔	1 秒	**ipv6 mld snooping last-listener-query-interval** コマンド

13.1.7 レポート抑制機能

レポート抑制機能を有効にすると、指定した期間はホストから送信される重複したレポート（同一 IP マルチキャストへの参加要求や離脱要求）を抑制し、1 つのレポートだけを中継します。

IGMP スヌーピングのレポート抑制機能は、IGMPv1 と IGMPv2 に対してのみ動作します。IGMP スヌーピングのレポート抑制機能を有効にするには、**ip igmp snooping report-suppression** コマンドを使用します。重複したレポートを抑制する期間を設定するには、**ip igmp snooping suppression-time** コマンドを使用します。

MLD スヌーピングのレポート抑制機能は、MLDv1 に対してのみ動作します。MLD スヌーピングのレポート抑制機能を有効にするには、**ipv6 mld snooping report-suppression** コマンドを使用します。重複したレポートを抑制する期間を設定するには、**ipv6 mld snooping suppression-time** コマンドを使用します。

13.1.8 プロキシレポーティング機能

プロキシレポーティング機能を有効にすると、ルーター（クエリア）からのクエリーに対する代理応答や、ホストからのレポートなどの代理送信を行います。

IGMP スヌーピングのプロキシレポーティング機能を有効にするには、**ip igmp snooping proxy-reporting** コマンドを使用します。MLD スヌーピングのプロキシレポーティング機能を有効にするには、**ipv6 mld snooping proxy-reporting** コマンドを使用します。

13.2 IGMP スヌーピング／ MLD スヌーピングの状態確認

IGMP スヌーピング／ MLD スヌーピ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 IGMP スヌーピングの状態確認

IGMP スヌーピングの状態を表示して確認する方法を説明します。

13.2.1.1 IGMP スヌーピングの設定の表示

`show ip igmp snooping` コマンドで、IGMP スヌーピングの設定を確認できます。

> ***NOTE:*** Unregistered-filter interfaces 項目は、IGMP スヌーピングの **`ip igmp snooping unregistered-filter`** コマンドをサポートしている機種でのみ表示されます。

表示例を以下に示します。

```
# show ip igmp snooping

IGMP snooping global state        : Enabled ...(1)
Dynamic mrouter aging time        : 300 seconds ...(2)
Unregistered-filter interfaces    : 1/0/1-1/0/20 ...(3)
                                    1/0/23-1/0/24
                                    port-channel7

VLAN #10 configuration ...(4)
    IGMP snooping state               : Enabled ...(5)
    Minimum version                   : v1 ...(6)
    Fast leave                        : Enabled (host-based) ...(7)
    Report suppression                : Disabled ...(8)
    Suppression time                  : 10 seconds ...(9)
    Querier state                     : Enabled (Non-active) ...(10)
    Query version                     : v3 ...(11)
    Query interval                    : 125 seconds ...(12)
    Max response time                 : 10 seconds ...(13)
    Robustness value                  : 2 ...(14)
    Last member query interval        : 1 seconds ...(15)
    Proxy reporting                   : Disabled (Source 0.0.0.0) ...(16)
    Ignore topology change            : Disabled ...(17)

Total Entries: 1
```

各項目の説明は、以下のとおりです。

表 13-3 `show ip igmp snooping` コマンドの表示項目

項番	説明
(1)	IGMP スヌーピング機能のグローバル設定の有効 (Enabled) ／無効 (Disabled) を表示します。
(2)	学習したマルチキャストルーターポートのエージングタイムの設定値を表示します。
(3)	IGMP スヌーピングの unregistered-filter を設定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。
(4)	VLAN ID を表示します。
(5)	VLAN ごとの IGMP スヌーピング機能の有効 (Enabled) ／無効 (Disabled) を表示します。

項番	説明
(6)	レシーバーからの参加要求（Membership Report）を許可する IGMP の最小バージョンを表示します。 • v1：最小バージョンの制限なし（デフォルト設定） • v2：IGMPv1 ホストの参加を制限し、IGMPv2/v3 ホストのみ許可 • v3：IGMPv1/v2 ホストの参加を制限し、IGMPv3 ホストのみ許可
(7)	IGMP スヌーピングの高速離脱機能の有効 (Enabled) ／無効 (Disabled) を表示します。group-list オプションを指定して有効にした場合は、対象の IP アクセスリスト名も表示されます。
(8)	IGMP スヌーピングのレポート抑制機能の有効 (Enabled) ／無効 (Disabled) を表示します。
(9)	IGMP スヌーピングのレポート抑制機能の抑制期間を表示します。
(10)	IGMP スヌーピングのクエリアの有効／無効を表示します。 • Enabled（Active）: IGMP スヌーピングのクエリアが有効で、アクティブ状態 • Enabled（Non-active）: IGMP スヌーピングのクエリアが有効で、非アクティブ状態 • Disabled : IGMP スヌーピングのクエリアが無効
(11)	IGMP スヌーピングのクエリアで使用する IGMP のバージョンを表示します。
(12)	IGMP スヌーピングのクエリアが定期的に送信する Membership Query の送信間隔を表示します。
(13)	IGMP スヌーピングのクエリアが送信する Membership Query で通知される最大応答時間を表示します。
(14)	IGMP スヌーピングのロバストネス変数を表示します。
(15)	IGMP スヌーピングのクエリアの、Group-Specific Query または Group-and-Source-Specific Query の送信間隔を表示します。
(16)	IGMP スヌーピングのプロキシレポーティング機能の有効 (Enabled) ／無効 (Disabled) を表示します。source オプションを指定して有効にした場合は、指定した送信元 IPv4 アドレスも表示されます。
(17)	スパニングツリープロトコルに起因するクエリー送信禁止の有効 (Enabled) ／無効 (Disabled) を表示します。

13.2.1.2 マルチキャストルーターポート情報の表示

show ip igmp snooping mrouter コマンドで、IGMP スヌーピングのマルチキャストルーターポート情報を確認できます。

表示例を以下に示します。

```
# show ip igmp snooping mrouter
(1)     (2)
VLAN    Ports
-----   -----------------------------
10      1/0/8,port-channel5 (static)
        1/0/1-1/0/2 (forbidden)
        1/0/12 (dynamic)

Total Entries: 1
```

各項目の説明は、以下のとおりです。

表 13-4 `show ip igmp snooping mrouter` コマンドの表示項目

項番	説明
(1)	VLAN ID を表示します。
(2)	ポート番号またはポートチャネル番号を表示します。 • (dynamic)：学習したマルチキャストルーターポート • (static)：スタティックに設定したマルチキャストルーターポート • (forbidden)：マルチキャストルーターポートになることを禁止したポート

13.2.1.3 IGMP スヌーピングエントリーの表示

`show ip igmp snooping groups` コマンドで、IGMP スヌーピ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 igmp snooping groups

IGMP Snooping Connected Group Membership:
(1)       (2)               (3)               (4) (5)        (6)
VLAN ID  Group address     Source address    FM  Exp(sec)   Interface
-------  ---------------   ---------------   --  --------   ---------
10       233.252.0.1              *          EX  226        1/0/4

Total Entries: 1
```

各項目の説明は、以下のとおりです。

表 13-5 `show ip igmp snooping groups` コマンドの表示項目

項番	説明
(1)	VLAN ID を表示します。
(2)	IPv4 マルチキャストグループアドレスを表示します。
(3)	送信元 IPv4 アドレスを表示します。 なお、NP2100、NP2000、および NP2500 では、IGMP スヌーピングは MAC アドレスベースで処理されるため、送信元フィルタリングは動作しません。
(4)	フィルターモード（IN：INCLUDE モード／ EX：EXCLUDE モード）を表示します。
(5)	IGMP スヌーピングエントリーが削除されるまでの残り時間（秒）を表示します。
(6)	ポート番号またはポートチャネル番号を表示します。

13.2.1.4 スタティック IGMP スヌーピングエントリーの表示

show ip igmp snooping static-group コマンドで、スタティック IGMP スヌーピ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 igmp snooping static-group
(1)      (2)              (3)
VLAN ID  Group address    Interface
-------  ---------------  ------------------------
10       233.252.0.100    1/0/4,port-channel2

Total Entries: 1
```

各項目の説明は、以下のとおりです。

表 13-6 show ip igmp snooping static-group コマンドの表示項目

項番	説明
(1)	VLAN ID を表示します。
(2)	IPv4 マルチキャストグループアドレスを表示します。
(3)	ポート番号またはポートチャネル番号を表示します。

13.2.1.5 IGMP スヌーピング統計情報の表示

show ip igmp snooping statistics コマンドで、IGMP スヌーピング統計情報を確認できます。

ポート 1/0/2 を指定した場合の表示例を以下に示します。

```
# show ip igmp snooping statistics interface port 1/0/2

Interface Port1/0/2 ...(1)
  IGMPv1 Rx: Report 0, Query 0 ...(2)
  IGMPv2 Rx: Report 0, Query 0, Leave 0 ...(3)
  IGMPv3 Rx: Report 0, Query 0 ...(4)
  IGMPv1 Tx: Report 0, Query 0 ...(5)
  IGMPv2 Tx: Report 0, Query 0, Leave 0 ...(6)
  IGMPv3 Tx: Report 0, Query 5 ...(7)

Total Entries: 1
```

各項目の説明は、以下のとおりです。

表 13-7 show ip igmp snooping statistics コマンドの表示項目

項番	説明
(1)	ポート番号またはポートチャネル番号を表示します。
(2)	対象インターフェースで受信した IGMPv1 の Report, Query の数を表示します。
(3)	対象インターフェースで受信した IGMPv2 の Report, Query, Leave の数を表示します。
(4)	対象インターフェースで受信した IGMPv3 の Report, Query の数を表示します。
(5)	対象インターフェースから送信した IGMPv1 の Report, Query の数を表示します。

項番	説明
(6)	対象インターフェースから送信した IGMPv2 の Report, Query, Leave の数を表示します。
(7)	対象インターフェースから送信した IGMPv3 の Report, Query の数を表示します。

13.2.2 MLD スヌーピングの状態確認

MLD スヌーピングの状態を表示して確認する方法を説明します。

13.2.2.1 MLD スヌーピングの設定の表示

show ipv6 mld snooping コマンドで、MLD スヌーピングの設定を確認できます。

> ***NOTE:*** Unregistered-filter interfaces 項目は、MLD スヌーピングの **ipv6 mld snooping unregistered-filter** コマンドをサポートしている機種でのみ表示されます。

表示例を以下に示します。

```
# show ipv6 mld snooping

MLD snooping global state: Enabled ...(1)
Unregistered-filter interfaces    : 1/0/1-1/0/20 ...(2)
                                    1/0/23-1/0/24
                                    port-channel7

VLAN #10 configuration ...(3)
    MLD snooping state            : Enabled ...(4)
    Minimum version               : v1 ...(5)
    Fast leave                    : Enabled (host-based) ...(6)
    Report suppression            : Disabled ...(7)
    Suppression time              : 10 seconds ...(8)
    Proxy reporting               : Disabled (Source ::) ...(9)
    Mrouter port learning         : Enabled ...(10)
    Querier state                 : Enabled (Non-active) ...(11)
    Query version                 : v2 ...(12)
    Query interval                : 125 seconds ...(13)
    Max response time             : 10 seconds ...(14)
    Robustness value              : 2 ...(15)
    Last listener query interval : 1 seconds ...(16)
    Ignore topology change        : Disabled ...(17)

Total Entries: 1
```

各項目の説明は、以下のとおりです。

表 13-8 show ipv6 mld snooping コマンドの表示項目

項番	説明
(1)	MLD スヌーピング機能のグローバル設定の有効 (Enabled) ／無効 (Disabled) を表示します。
(2)	MLD スヌーピングの unregistered-filter を設定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。
(3)	VLAN ID を表示します。
(4)	VLAN ごとの MLD スヌーピング機能の有効 (Enabled) ／無効 (Disabled) を表示します。

項番	説明
(5)	リスナーからの参加要求（Multicast Listener Report）を許可する MLD の最小バージョンを表示します。 • v1：最小バージョンの制限なし（デフォルト設定） • v2：MLDv1 ホストの参加を制限し、MLDv2 ホストのみ許可
(6)	MLD スヌーピングの高速離脱機能の有効 (Enabled) ／無効 (Disabled) を表示します。group-list オプションを指定して有効にした場合は、対象の IPv6 アクセスリスト名も表示されます。
(7)	MLD スヌーピングのレポート抑制機能の有効 (Enabled) ／無効 (Disabled) を表示します。
(8)	MLD スヌーピングのレポート抑制機能の抑制期間を表示します。
(9)	MLD スヌーピングのプロキシレポーティング機能の有効 (Enabled) ／無効 (Disabled) を表示します。source オプションを指定して有効にした場合は、指定した送信元 IPv6 アドレスも表示されます。
(10)	マルチキャストルーターポートの自動学習の有効 (Enabled) ／無効 (Disabled) を表示します。
(11)	MLD スヌーピングのクエリアの有効／無効を表示します。 • Enabled（Active）：MLD スヌーピングのクエリアが有効で、アクティブ状態 • Enabled（Non-active）：MLD スヌーピングのクエリアが有効で、非アクティブ状態 • Disabled：MLD スヌーピングのクエリアが無効
(12)	MLD スヌーピングのクエリアで使用する MLD のバージョンを表示します。
(13)	MLD スヌーピングのクエリアが定期的に送信する Multicast Listener Query の送信間隔を表示します。
(14)	MLD スヌーピングのクエリアが送信する Multicast Listener Query で通知される最大応答時間を表示します。
(15)	MLD スヌーピングのロバストネス変数を表示します。
(16)	MLD スヌーピングのクエリアの、Multicast Address Specific Query または Multicast Address and Source Specific Query の送信間隔を表示します。
(17)	スパニングツリープロトコルに起因するクエリー送信禁止の有効 (Enabled) ／無効 (Disabled) を表示します。

13.2.2.2 マルチキャストルーターポート情報の表示

show ipv6 mld snooping mrouter コマンドで、MLD スヌーピングのマルチキャストルーターポート情報を確認できます。

表示例を以下に示します。

```
# show ipv6 mld snooping mrouter
(1)     (2)
VLAN    Ports
-----   ----------------------------
10      1/0/8,port-channel5 (static)
        1/0/1-1/0/2 (forbidden)
        1/0/12 (dynamic)

Total Entries: 1
```

各項目の説明は、以下のとおりです。

表 13-9 `show ipv6 mld snooping mrouter` コマンドの表示項目

項番	説明
(1)	VLAN ID を表示します。
(2)	ポート番号またはポートチャネル番号を表示します。 • (dynamic)：学習したマルチキャストルーターポート • (static)：スタティックに設定したマルチキャストルーターポート • (forbidden)：マルチキャストルーターポートになることを禁止したポート

13.2.2.3 MLD スヌーピングエントリーの表示

`show ipv6 mld snooping groups` コマンドで、MLD スヌーピ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 mld snooping groups

MLD Snooping Connected Group Membership:
(1)     (2)                   (3)                   (4)(5)       (6)
VLAN ID Group address         Source address        FM Exp(sec) Interface
------- --------------------- --------------------- -- -------- ---------
10      ff05::db8:0:1                 *             EX 213      1/0/4

Total Entries: 1
```

各項目の説明は、以下のとおりです。

表 13-10 `show ipv6 mld snooping groups` コマンドの表示項目

項番	説明
(1)	VLAN ID を表示します。
(2)	IPv6 マルチキャストグループアドレスを表示します。
(3)	送信元 IPv6 アドレスを表示します。 なお、NP2100、NP2000、および NP2500 では、MLD スヌーピングは MAC アドレスベースで処理されるため、送信元フィルタリングは動作しません。
(4)	フィルターモード（IN：INCLUDE モード／ EX：EXCLUDE モード）を表示します。
(5)	MLD スヌーピングエントリーが削除されるまでの残り時間（秒）を表示します。
(6)	ポート番号またはポートチャネル番号を表示します。

13.2.2.4 スタティック MLD スヌーピングエントリーの表示

show ipv6 mld snooping static-group コマンドで、スタティック MLD スヌーピ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 mld snooping static-group
(1)      (2)                                    (3)
VLAN ID  Group address                          Interface
-------  ---------------                        ------------------------
10       ff05::db8:0:5555                       1/0/4,port-channel2

Total Entries: 1
```

各項目の説明は、以下のとおりです。

表 13-11 show ipv6 mld snooping static-group コマンドの表示項目

項番	説明
(1)	VLAN ID を表示します。
(2)	IPv6 マルチキャストグループアドレスを表示します。
(3)	ポート番号またはポートチャネル番号を表示します。

13.2.2.5 MLD スヌーピング統計情報の表示

show ipv6 mld snooping statistics コマンドで、MLD スヌーピング統計情報を確認できます。

ポート 1/0/2 を指定した場合の表示例を以下に示します。

```
# show ipv6 mld snooping statistics interface port 1/0/2

Interface Port1/0/2 ...(1)
  Rx: v1Report 0, v2Report 0, Query 0, v1Done 0 ...(2)
  Tx: v1Report 0, v2Report 0, Query 138, v1Done 0 ...(3)

Total Entries: 1
```

各項目の説明は、以下のとおりです。

表 13-12 show ipv6 mld snooping statistics コマンドの表示項目

項番	説明
(1)	ポート番号またはポートチャネル番号を表示します。
(2)	対象インターフェースで受信した MLDv1 Report, MLDv2 Report, Query, MLDv1 Done の数を表示します。
(3)	対象インターフェースから送信した MLDv1 Report, MLDv2 Report, Query, MLDv1 Done の数を表示します。

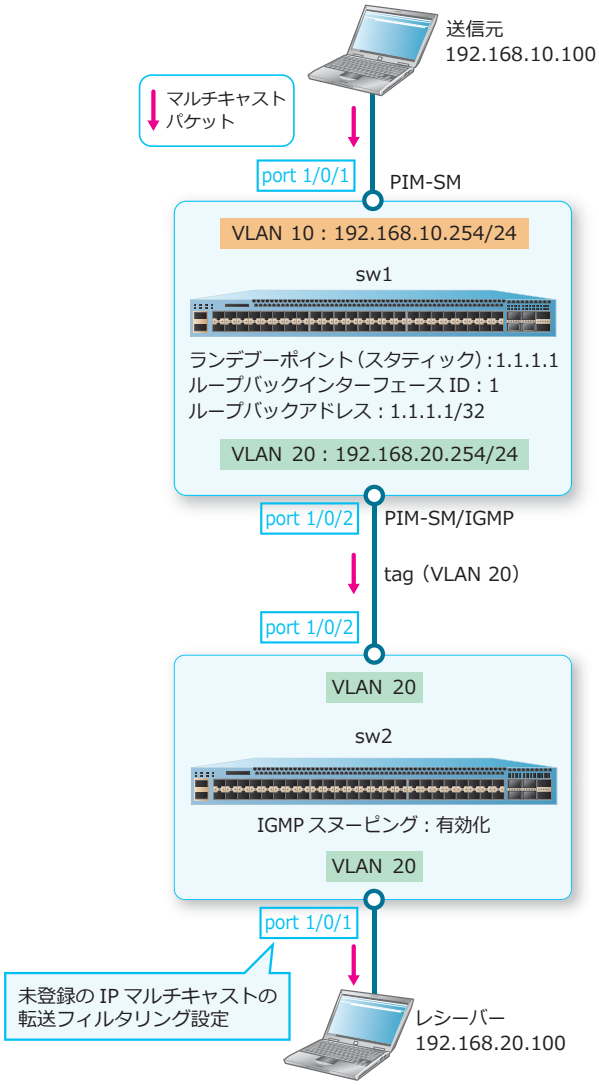
13.3 IGMP スヌーピング／ MLD スヌーピングの構成例と設定例

IGMP スヌーピング／ MLD スヌーピングの構成例と設定例を示します。

13.3.1 IGMP スヌーピングの設定例

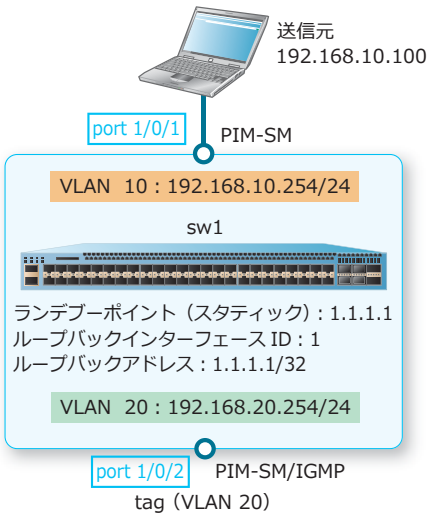
L2 スイッチ（sw2）の VLAN 20 で、IGMP スヌーピングを使用する場合の構成例と設定例を示します。sw2 では、ポート 1/0/1 からの未登録の IP マルチキャストの転送をフィルタリングするために、**`ip igmp snooping unregistered-filter`** コマンドを使用します。また、この設定例では、マルチキャストルーター（sw1）も設定しています。

図 13-2 IGMP スヌーピングの構成例



13.3.1.1 マルチキャストルーターの設定例（sw1）

図 13-3 マルチキャストルーターの設定例（sw1）



1. VLAN 10 および VLAN 20 を作成します。

```
sw1# configure terminal
sw1(config)# vlan 10
sw1(config-vlan)# exit
sw1(config)# vlan 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 をトランクポートとして設定し、トランクポートに［VLAN 20］を割り当てます。

```
sw1(config)# interface port 1/0/1
sw1(config-if-port)# switchport access vlan 10
sw1(config)# interface port 1/0/2
sw1(config-if-port)# switchport mode trunk
sw1(config-if-port)# switchport trunk allowed 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、PIM-SM と IGMP を有効化します。

```
sw1(config)# interface vlan 10
sw1(config-if-vlan)# ip address 192.168.10.254/24
sw1(config-if-vlan)# ip pim sparse-mode
sw1(config-if-vlan)# ip igmp enable
sw1(config-if-vlan)#
sw1(config)# interface vlan 20
sw1(config-if-vlan)# ip address 192.168.20.254/24
sw1(config-if-vlan)# ip pim sparse-mode
sw1(config-if-vlan)# ip igmp enable
sw1(config-if-vlan)# exit
sw1(config)#
```

4. ループバックインターフェース ID を［1］に、ループバックアドレスを［1.1.1.1/32］に設定し、PIM-SM を有効化します。

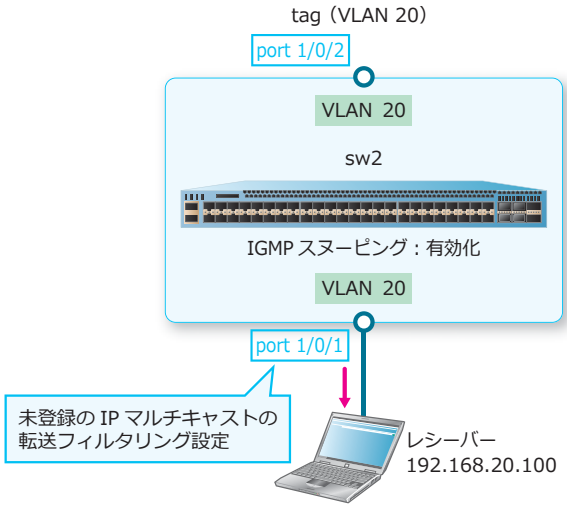
```
sw1(config)# interface loopback 1
sw1(config-if-loopback)# ip address 1.1.1.1/32
sw1(config-if-loopback)# ip pim sparse-mode
sw1(config-if-loopback)# exit
sw1(config)#
```

5. ランデブーポイント（スタティック）の IP アドレスを［1.1.1.1］に設定します。また、マルチキャストルーティングを有効化します。

```
sw1(config)# ip pim rp-address 1.1.1.1
sw1(config)# ip multicast-routing
sw1(config)# end
sw1#
```

13.3.1.2 IGMP スヌーピングの設定例（sw2）

図 13-4 IGMP スヌーピングの設定例（sw2）



1. VLAN 20 を作成します。

```
sw2# configure terminal
sw2(config)# vlan 20
sw2(config-vlan)# exit
sw2(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 20］を割り当てます。また、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 20］を割り当てます。

```
sw2(config)# interface port 1/0/1
sw2(config-if-port)# switchport access vlan 20
sw2(config)# interface port 1/0/2
sw2(config-if-port)# switchport mode trunk
sw2(config-if-port)# switchport trunk allowed vlan 20
sw2(config-if-port)# exit
sw2(config)#
```

3. 装置全体の IGMP スヌーピング設定を有効にします。

```
sw2(config)# ip igmp snooping
sw2(config)#
```

4. VLAN 20 で、VLAN ごとの IGMP スヌーピング設定を有効にします。

```
sw2(config)# vlan 20
sw2(config-vlan)# ip igmp snooping
sw2(config-vlan)# exit
sw2(config)#
```

5. ポート 1/0/1 を指定して、未登録の IP マルチキャストの転送フィルタリングを設定します。

```
sw2(config)# ip igmp snooping unregistered-filter interface port 1/0/1
sw2(config)# end
sw2#
```

6. 実施後の IGMP スヌーピング関連の設定を以下に抜粋します。

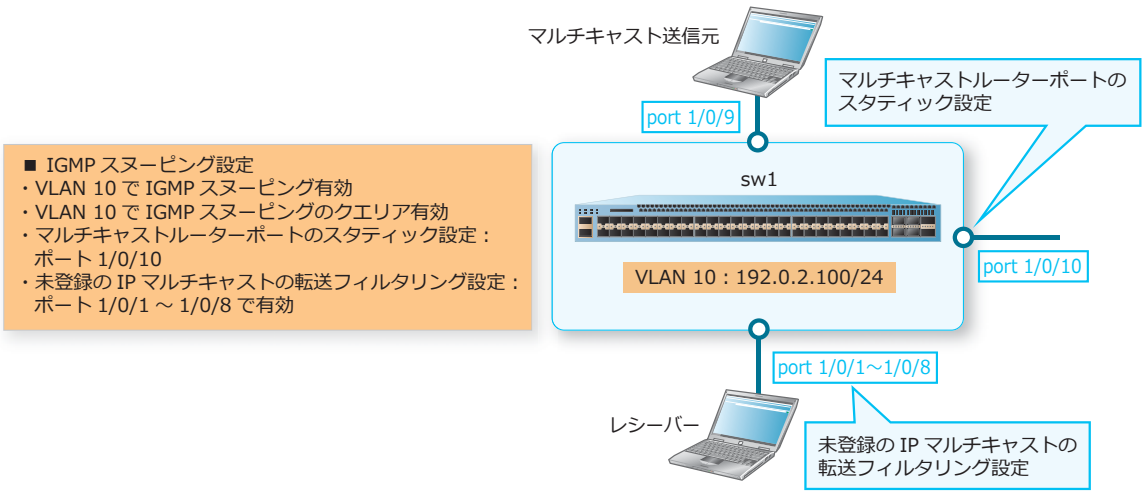
```
# IGMP-SNOOPING

ip igmp snooping
ip igmp snooping unregistered-filter interface port 1/0/1
vlan 20
 ip igmp snooping
```

13.3.2 IGMP スヌーピングの設定例（自装置でクエリア有効時）

IGMP スヌーピングを使用する場合の構成例と設定例を示します。この例では、自装置でクエリアを有効にしています。

- VLAN 10 で IGMP スヌーピングを有効化
- VLAN 10 で IGMP スヌーピングのクエリア機能を有効化
- ポート 1/0/10 をマルチキャストルーターポートに設定
- **ip igmp snooping unregistered-filter** コマンドを使用して、ポート 1/0/1 ～ 1/0/8 への未登録の IP マルチキャストの転送をフィルタリング

図 13-5 IGMP スヌーピングの設定例（自装置でクエリア有効時）



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 からポート 1/0/10 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 range port 1/0/1-10
sw1(config-if-port-range)# switchport access vlan 10
sw1(config-if-port-range)# exit
sw1(config)#
```

3. VLAN 10 の IP アドレスを［192.0.2.100/24］に設定します。

```
sw1(config)# interface vlan 10
sw1(config-if-vlan)# ip address 192.0.2.100/24
sw1(config-if-vlan)# exit
sw1(config)#
```

4. 装置全体の IGMP スヌーピング設定を有効にします。

```
sw1(config)# ip igmp snooping
sw1(config)#
```

5. VLAN 10 で、VLAN ごとの IGMP スヌーピング設定を有効にします。

```
sw1(config)# vlan 10
sw1(config-vlan)# ip igmp snooping
sw1(config-vlan)#
```

6. VLAN 10 で、IGMP スヌーピングのクエリア機能を有効にします。

```
sw1(config-vlan)# ip igmp snooping querier
sw1(config-vlan)#
```

7. VLAN 10 で、ポート 1/0/10 をマルチキャストルーターポートに設定します。

```
sw1(config-vlan)# ip igmp snooping mrouter interface port 1/0/10
sw1(config-vlan)# exit
sw1(config)#
```

8. ポート 1/0/1 からポート 1/0/8 を指定して、未登録の IP マルチキャストの転送フィルタリングを設定します。

```
sw1(config)# ip igmp snooping unregistered-filter interface port 1/0/1-1/0/8
sw1(config)# end
sw1#
```

9. 実施後の IGMP スヌーピング関連の設定を以下に抜粋します。

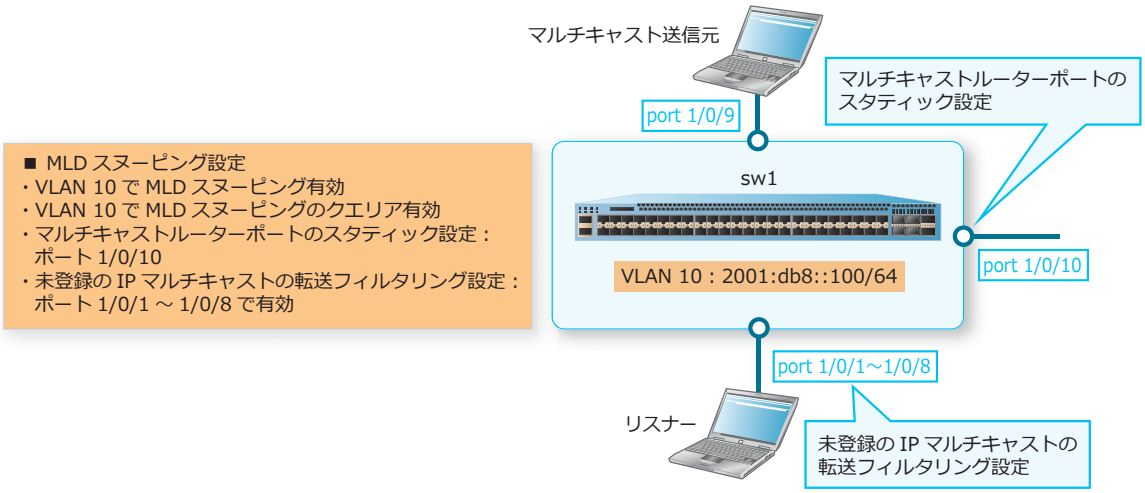
```
# IGMP-SNOOPING

ip igmp snooping
ip igmp snooping unregistered-filter interface port 1/0/1-1/0/8
vlan 10
 ip igmp snooping
 ip igmp snooping mrouter interface port 1/0/10
 ip igmp snooping querier
```

13.3.3 MLD スヌーピングの設定例（自装置でクエリア有効時）

MLD スヌーピングを使用する場合の構成例と設定例を示します。この例では、自装置でクエリアを有効にしています。

- VLAN 10 で MLD スヌーピングを有効化
- VLAN 10 で MLD スヌーピングのクエリア機能を有効化
- ポート 1/0/10 をマルチキャストルーターポートに設定
- **`ipv6 mld snooping unregistered-filter`** コマンドを使用して、ポート 1/0/1 ～ 1/0/8 への未登録の IP マルチキャストの転送をフィルタリング

図 13-6 MLD スヌーピングの設定例（自装置でクエリア有効時）



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 からポート 1/0/10 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 range port 1/0/1-10
sw1(config-if-port-range)# switchport access vlan 10
sw1(config-if-port-range)# exit
sw1(config)#
```

3. VLAN 10 の IPv6 アドレスを［2001:db8::100/64］に設定します。

```
sw1(config)# interface vlan 10
sw1(config-if-vlan)# ipv6 address 2001:db8::100/64
sw1(config-if-vlan)# exit
sw1(config)#
```

4. 装置全体の MLD スヌーピング設定を有効にします。

```
sw1(config)# ipv6 mld snooping
sw1(config)#
```

5. VLAN 10 で、VLAN ごとの MLD スヌーピング設定を有効にします。

```
sw1(config)# vlan 10
sw1(config-vlan)# ipv6 mld snooping
sw1(config-vlan)#
```

6. VLAN 10 で、MLD スヌーピングのクエリア機能を有効にします。

```
sw1(config-vlan)# ipv6 mld snooping querier
sw1(config-vlan)#
```

7. VLAN 10 で、ポート 1/0/10 をマルチキャストルーターポートに設定します。

```
sw1(config-vlan)# ipv6 mld snooping mrouter interface port 1/0/10
sw1(config-vlan)# exit
sw1(config)#
```

8. ポート 1/0/1 からポート 1/0/8 を指定して、未登録の IP マルチキャストの転送フィルタリングを設定します。

```
sw1(config)# ipv6 mld snooping unregistered-filter interface port 1/0/1-1/0/8
sw1(config)# end
sw1#
```

9. 実施後の MLD スヌーピング関連の設定を以下に抜粋します。

```
# MLD-SNOOPING

ipv6 mld snooping
ipv6 mld snooping unregistered-filter interface port 1/0/1-1/0/8
vlan 10
 ipv6 mld snooping
 ipv6 mld snooping querier
 ipv6 mld snooping mrouter interface port 1/0/10
```

14. MMRP-Plus

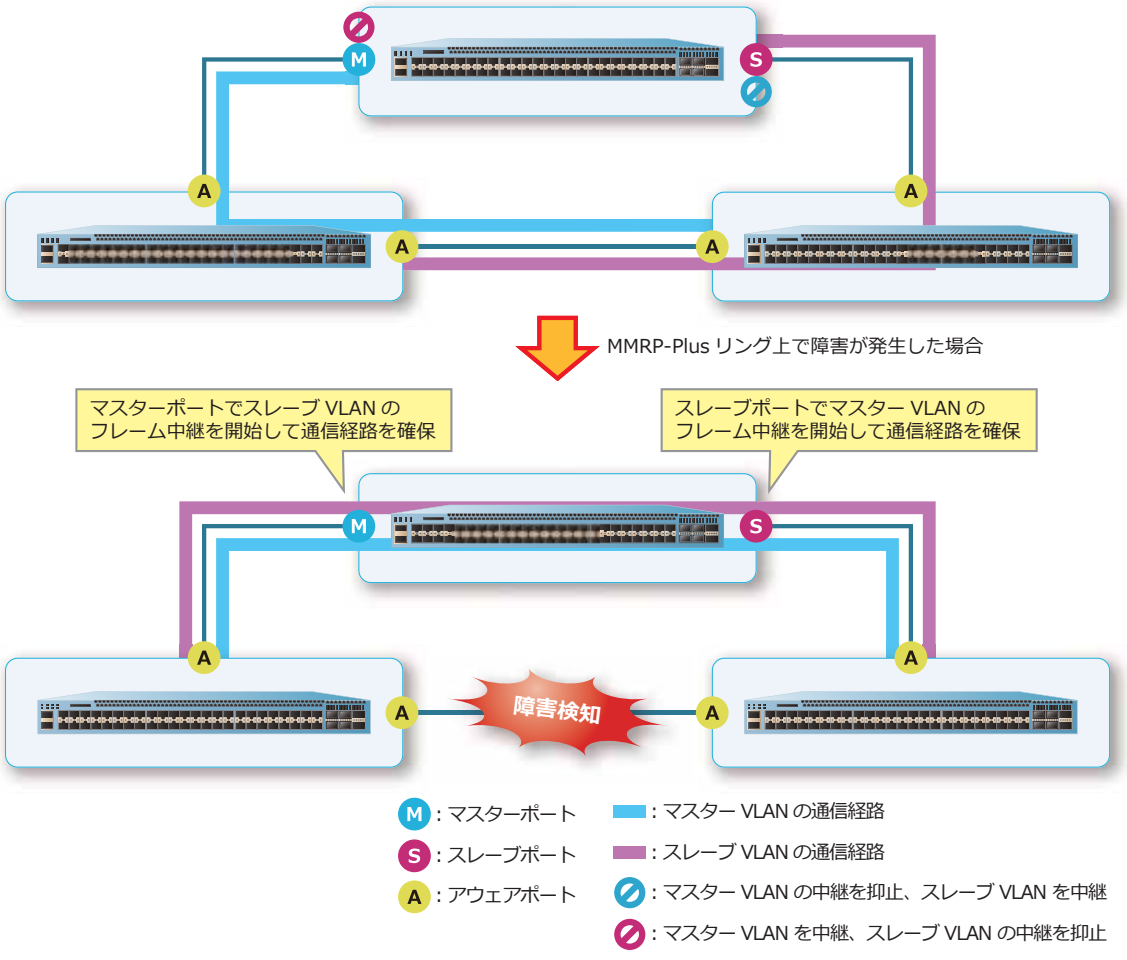
MMRP-Plus の機能、状態の確認方法、および構成例と設定例について説明します。

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。

14.1 MMRP-Plus の機能説明

MMRP-Plus（Multi Master Ring Protocol Plus）は、リング型構成のレイヤー 2 冗長プロトコルです。MMRP-Plus では、**リングポート（マスターポート**、**スレーブポート**、および**アウェアポート**）を設定します。正常時は、マスターポートではマスター VLAN のフレームを中継し、スレーブ VLAN のフレーム中継を抑止します。スレーブポートではスレーブ VLAN のフレームを中継し、マスター VLAN のフレーム中継を抑止します。MMRP-Plus リング（以後、リング）上で障害を検知すると、マスターポートおよびスレーブポートでブロックされていたフレームの中継が開始され、通信経路が切り替わります。

図 14-1 MMRP-Plus の概要



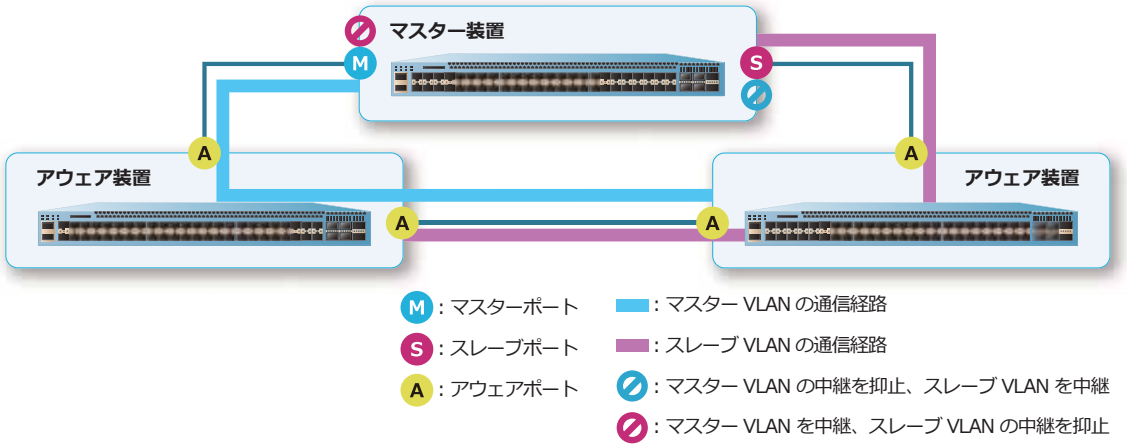
装置全体で MMRP-Plus を有効化するには、**`mmrp-plus enable`** コマンドを使用します。

14.1.1 MMRP-Plus の基本設定

MMRP-Plus は、1 台の**マスター装置**と複数台の**アウェア装置**から構成されます。このような構成を**シングルマスター構成**と呼びます。

マスター装置にはマスターポートとスレーブポートの 2 個のリングポートを設定し、アウェア装置には 2 個のアウェアポートを設定します。リングポートには、物理ポートまたはポートチャネルを設定できます。

図 14-2 シングルマスター構成



マスター装置にマスターポートとスレーブポートを設定するには、**`mmrp-plus ring ring-master`** コマンドを使用します。アウェア装置にアウェアポートを設定するには、**`mmrp-plus ring aware`** コマンドを使用します。

> ***NOTE:*** NP7000、NP5000、NP3000、NP2100、NP2000、および NP2500 では、リングポートは装置ごとに最大 50 個まで設定できます。スタック構成を組んでいても、リングポート数は装置 1 台分の値となります。

> ***NOTE:*** NP4000 では、リングポートは装置ごとに最大 24 個まで設定できます。スタック構成を組んでいても、リングポート数は装置 1 台分の値となります。

> ***NOTE:*** MMRP-Plus 制御フレームの送出・中継を他のユーザートラフィックよりも優先させるために、MMRP-Plus のリングポートでは制御フレームを中継する送信キュー（デフォルト設定では送信キュー 7）が Strict Priority Queuing でスケジューリングされるように設定してください。なお、一部の機種（ApresiaNP5000 シリーズ、ApresiaNP4000 シリーズ）では、対象ポートが輻輳状態の場合に mls qos scheduler 設定を正常に変更できない制限があるため、mls qos scheduler 設定を変更する際は、対象ポートを shutdown 設定で閉塞した状態にしてください。

> ***NOTE:*** 従来の AEOS 製品（Ver7、8）と MMRP-Plus のリングを構成することが可能です。AEOS 製品と MMRP-Plus のリング構成を組む場合には、事前に十分な検証を行ってください。

14.1.1.1 リング名

MMRP-Plus のリング名を設定するには、**`mmrp-plus ring name`** コマンドを使用します。

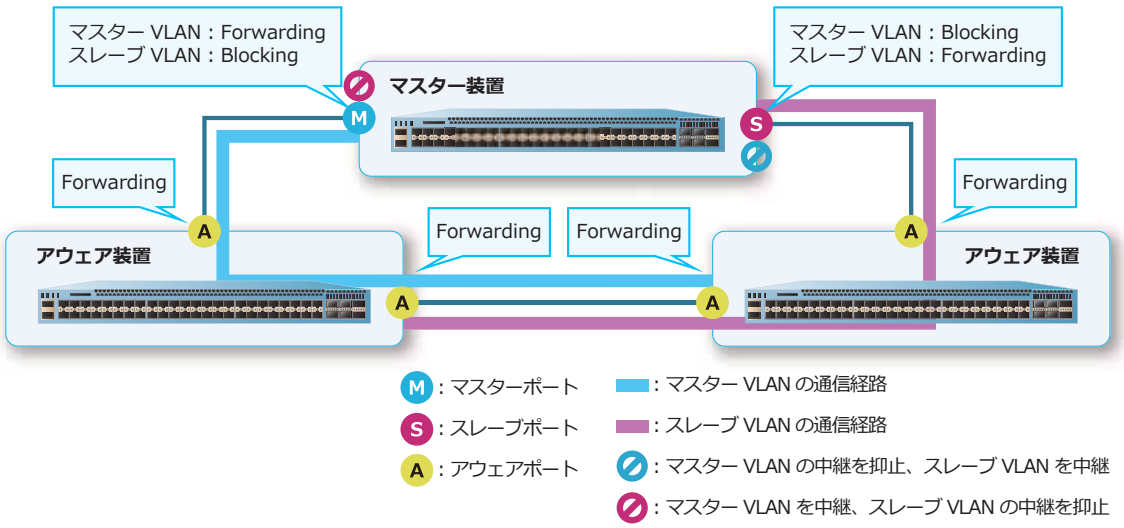
14.1.1.2 リングポートのステータス

リングポートのステータスには、Blocking 状態、Forwarding 状態、Down 状態、FailureUp 状態、および Listening 状態が定義されています。なお、アウェアポートは Blocking 状態にはなりません。

- **Blocking 状態および Forwarding 状態**

  リングポートで通信が行われている状態です。

図 14-3 Blocking 状態および Forwarding 状態



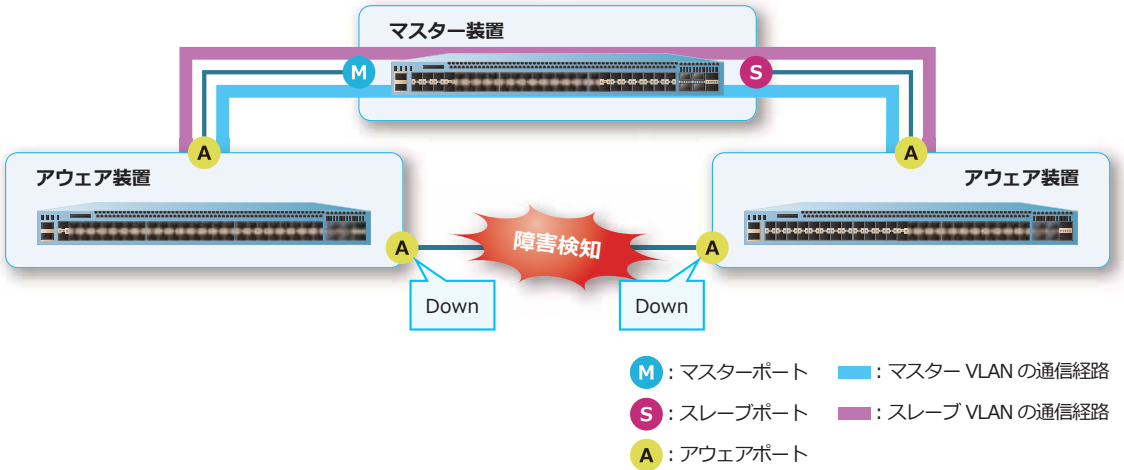
マスターポートが Blocking 状態のときは、マスター VLAN を中継し、スレーブ VLAN の中継を抑止します。スレーブポートが Blocking 状態のときは、スレーブ VLAN を中継し、マスター VLAN の中継を抑止します。

リングポートが Forwarding 状態のときは、マスター VLAN およびスレーブ VLAN を中継します。

- **Down 状態**

  障害を検知し、通信不可の状態です。

図 14-4 Down 状態



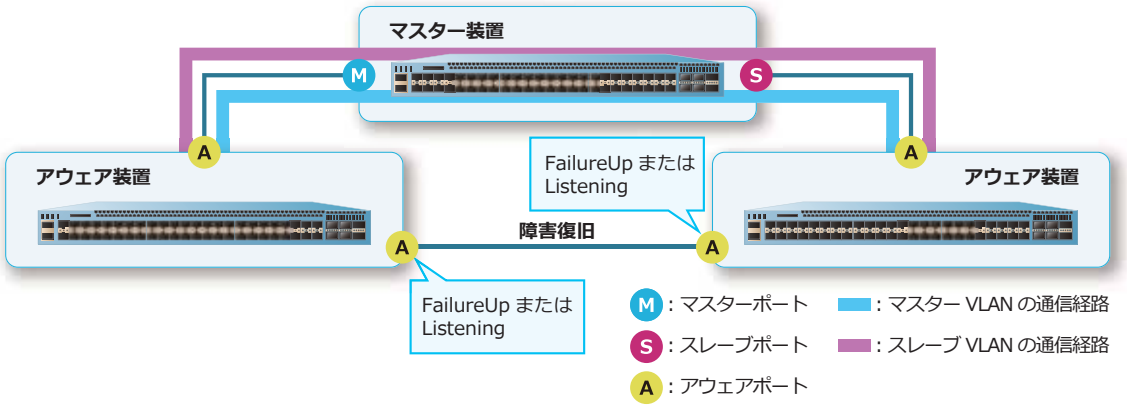
通信不可とは、以下の状態を示します。

- リングポートが物理ポートで構成されている場合：その物理ポートがリンクダウン、または LLDP による疑似リンクダウンになった状態
- リングポートがポートチャネルで構成されている場合：ポートチャネルを構成するすべてのメンバーポートが通信不可になった状態

- **FailureUp 状態および Listening 状態**

  障害が復旧してから、リングが正常状態に戻るまでの状態です。

図 14-5 FailureUp 状態および Listening 状態



FailureUp 状態は、リングポートを構成する物理ポートまたはポートチャネルはアップしているが、リングポートとしては通信不可の状態で、指定した時間が経過するまでリング復旧処理を待機するための状態です。指定した時間が経過すると、FailureUp 状態から Listening 状態に遷移します。

Listening 状態は、リング復旧処理途中の状態で、ユーザートラフィックは中継不可ですが、ハローフレームなどの MMRP-Plus 制御フレームのみ中継可能な状態です。

リンクダウン障害が復旧した後の切り戻り方法を設定するには、**`mmrp-plus ring revertive`** コマンドを使用します。設定によって以下のように動作します。

- 切り戻りタイマー値が 0（デフォルト設定）の場合は、リンクダウン障害が復旧するとすぐに Listening 状態へ遷移してリング復旧処理が開始されます。この場合は、FailureUp 状態には遷移しません。
- 切り戻りタイマー値が 0 以外に設定されている場合は、リンクダウン障害が復旧すると FailureUp 状態に遷移します。その後、切り戻りタイマー値の経過後に Listening 状態へ遷移し、リング復旧処理が開始されます。
- 手動切り戻り設定（disable パラメーター指定）の場合は、リンクダウン障害が復旧すると FailureUp 状態に遷移します。**`clear mmrp-plus failure ring`** コマンドを実行すると Listening 状態へ遷移し、リング復旧処理が開始されます。

NOTE: 手動切り戻り設定は、MMRP-Plus リングの切り戻しを計画的に実施できるメリットがあります。

NOTE: MMRP-Plus とレイヤー 3 機能を併用する場合、切り戻り方法はデフォルト設定（自動切り戻り有効で切り戻りタイマー値：0 秒）で使用することを推奨します。

14.1.1.3 MMRP-Plus 制御用 VLAN

ハローフレームなどの MMRP-Plus 制御フレームは、指定した VLAN ID のタグ付きフレームとして送信されます。そのため、リングポートはトランクポートとして設定し、指定した VLAN ID を割り当ててください。

MMRP-Plus 制御フレームを送受信する VLAN（MMRP-Plus 制御用 VLAN）を設定するには、**`mmrp-plus ring vid`** コマンドを使用します。MMRP-Plus 制御用 VLAN は「MMRP-Plus 制御フレームを送受信する専用 VLAN」としてリングごとに用意し、ユーザー VLAN と分けることを推奨します。

MMRP-Plus 制御フレーム

MMRP-Plus 制御フレームは、以下のとおりです。

• ハローフレーム

HelloB1：Blocking 状態のスレーブポートが送出するハローフレーム

HelloB2：Blocking 状態のマスターポートが送出するハローフレーム

HelloF1：Forwarding 状態のスレーブポートから送出するハローフレーム

HelloF2：Forwarding 状態のマスターポートから送出するハローフレーム

• ハローフレーム以外の MMRP-Plus 制御フレーム

リングの状態が変わった際に送出されます。

FDB Flush：MMRP-Plus の状態遷移に伴い、トラフィックの経路が変わった場合にマスターポートおよびスレーブポートが送出する FDB フラッシュ要求フレーム

Link Down：リングポートダウン時にアウェアポートが送出するリンクダウン通知フレーム

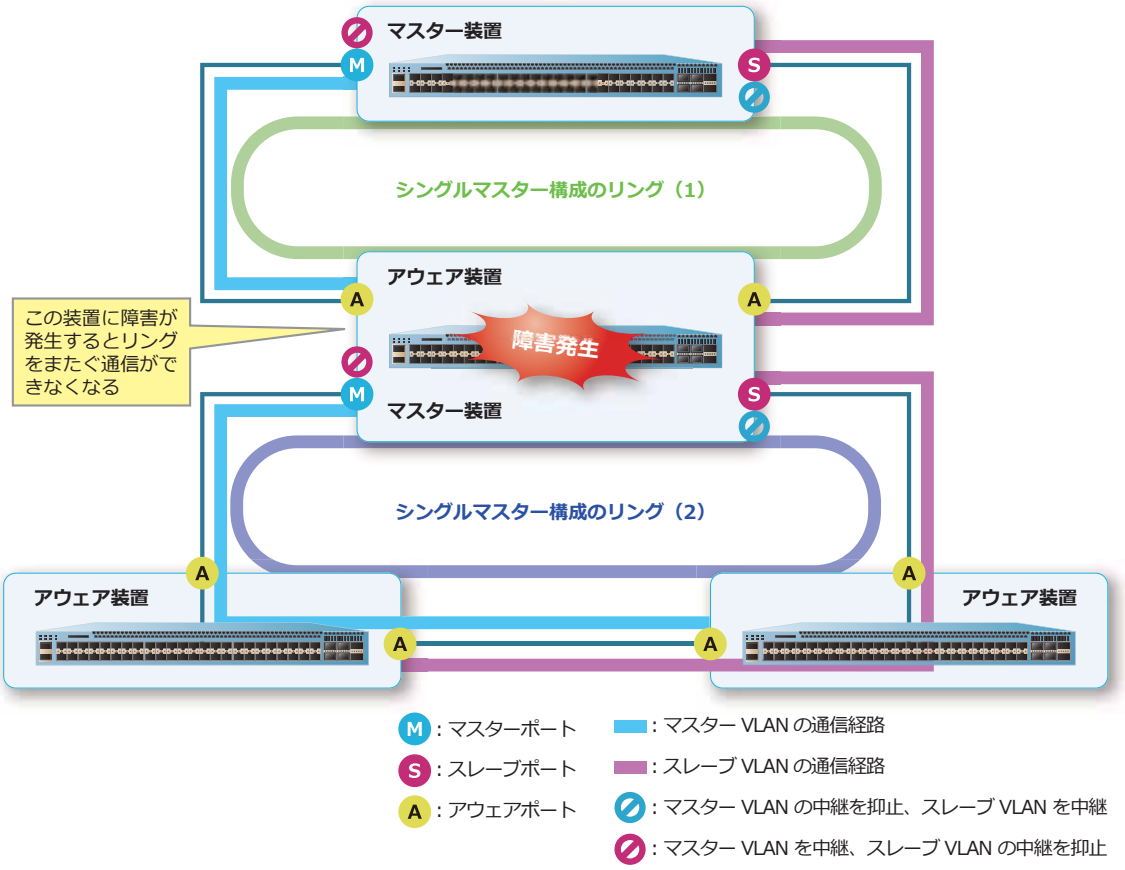
Link Up：アップリンクポートがリンクアップした際にマスターポートおよびスレーブポートが送出するリンクアップ通知フレーム

Blocking：マスターポートおよびスレーブポートが Blocking 状態に移行した際にマスターポートおよびスレーブポートが送出する通知フレーム

14.1.2 分散マスター構成

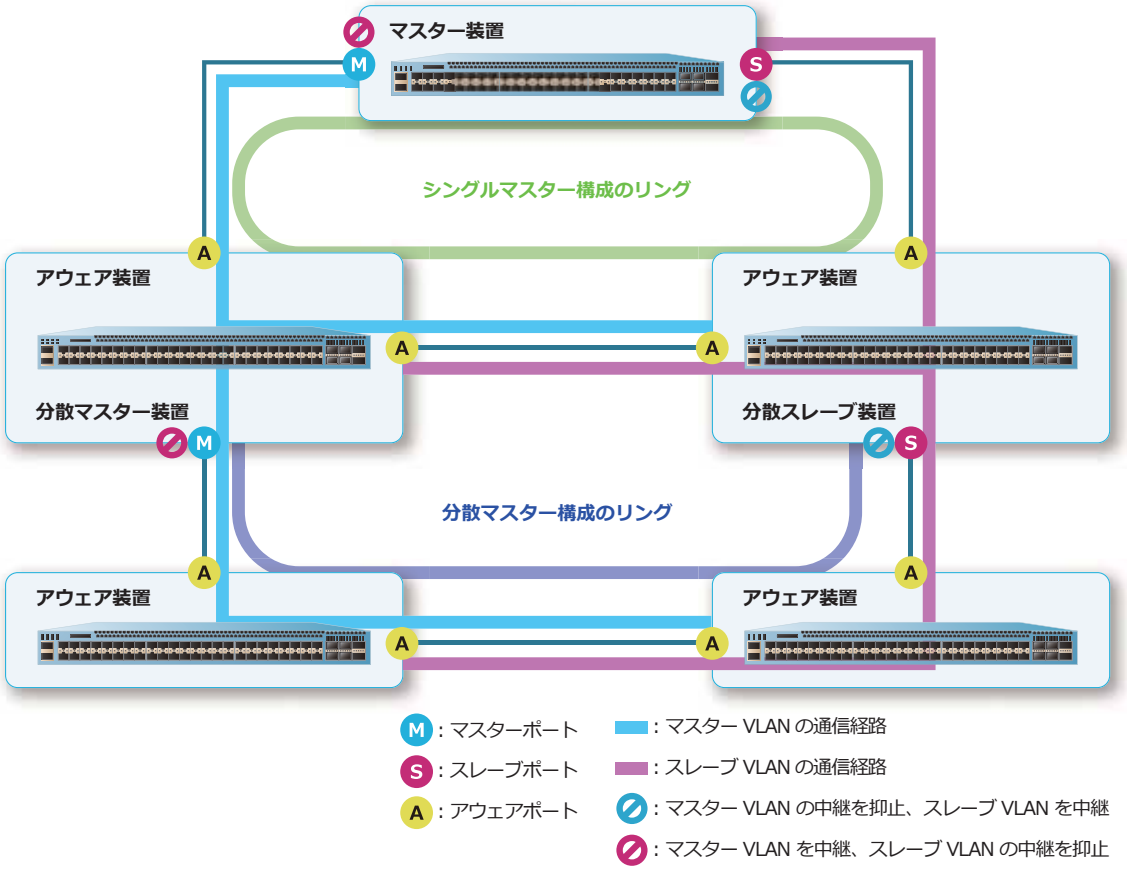
複数のリングを接続してネットワークを拡張する際、異なるリングを接続するポイントを 1 台の装置にすると、その装置に障害が発生した場合にリングをまたぐ通信ができなくなってしまいます。

図 14-6 シングルマスター構成の多段接続の例



そこで、複数のリングの接続を 2 台の装置（**分散マスター装置**および**分散スレーブ装置**）に分散することで、一方の装置に障害が発生しても、異なるリングをまたぐ通信が停止しないようにします。このような構成を**分散マスター構成**と呼びます。分散マスター構成の場合は、分散マスター装置にマスターポートを、分散スレーブ装置にスレーブポートを設定します。

図 14-7 分散マスター構成



分散マスター装置にマスターポートを設定するには、**`mmrp-plus ring divided-master`** コマンドを使用します。分散スレーブ装置にスレーブポートを設定するには、**`mmrp-plus ring divided-slave`** コマンドを使用します。

分散マスター構成では、リング経路以外の通信経路を確保するために分散マスター装置と分散スレーブ装置の間を接続する必要がありますが、基本的にはこの経路には他の装置を配置しないで分散マスター装置と分散スレーブ装置を直接接続することを推奨します。他の装置を接続している場合、その装置は分散マスター構成のリングとは関係のない装置となるため、分散マスター構成のリングの切り替わり／切り戻り時の FDB テーブル消去の対象になりません。これは、片方向通信の場合の切り替わり／切り戻り時間が長くなる原因になります。

14.1.3 VLAN 分散

MMRP-Plus では、マスターポートまたはスレーブポートでフレーム中継を抑止してループ構成になることを防いでいますが、VLAN ごとに抑止するポートを分散させることにより、MMRP-Plus の VLAN 分散を可能にしています。

それぞれの VLAN は、マスター VLAN またはスレーブ VLAN のいずれかに所属します。マスター VLAN は「正常時にはマスターポートでフレーム中継され、スレーブポートで抑止される」と動作します。スレーブ VLAN は「正常時にはスレーブポートでフレーム中継され、マスターポートで抑止される」と動作します。

マスター VLAN ／スレーブ VLAN を定義する VLAN グループを設定するには、**`mmrp-plus vlangroup slave-vid`** コマンドを使用します。リングに VLAN グループを適用するには、**`mmrp-plus ring vlangroup`** コマンドを使用します。デフォルト設定では、すべての VLAN がマスター VLAN に所属する設定になっています。

> ***NOTE:*** 分散マスター構成で VLAN 分散を使用する場合は、分散マスター装置と分散スレーブ装置を同一の VLAN 分散設定にしてください。

> ***NOTE:*** 稼働中の MMRP-Plus リングで VLAN グループの設定（mmrp-plus vlangroup slave-vid）を変更する場合は、リング内の任意の経路がリンクダウンしている状態で変更してください。リング内の経路がすべてリンクアップしている状態で変更を行うと、VLAN 分散設定が不一致になるタイミングなどにループが発生する原因になります。

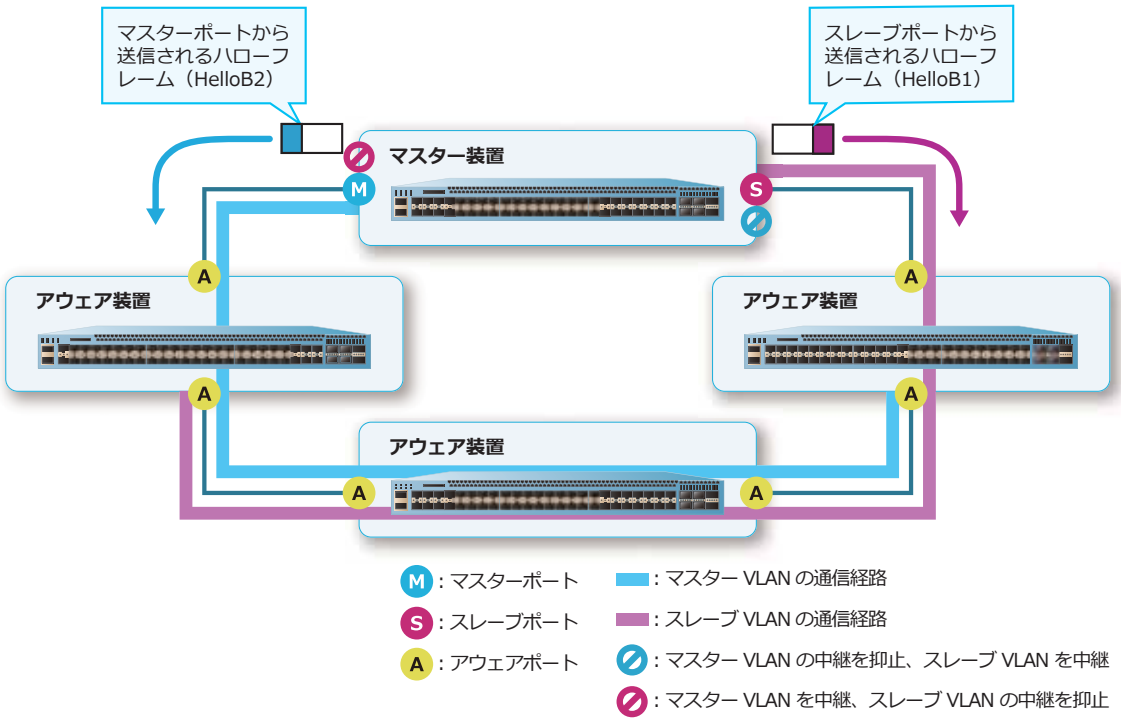
14.1.4 MMRP-Plus の動作例

リングに障害が発生した場合の動作、および復旧した場合の動作を説明します。

14.1.4.1 正常時

正常時は、マスターポートではマスター VLAN のフレームを中継し、スレーブ VLAN のフレーム中継を抑止します。スレーブポートではスレーブ VLAN のフレームを中継し、マスター VLAN のフレーム中継を抑止します。マスターポート／スレーブポートのそれぞれからハローフレームを送信し、リングの健全性を確認します。

図 14-8 正常時の通信経路の例



正常時のリングポートの状態およびコネクション状態は、以下のとおりです。

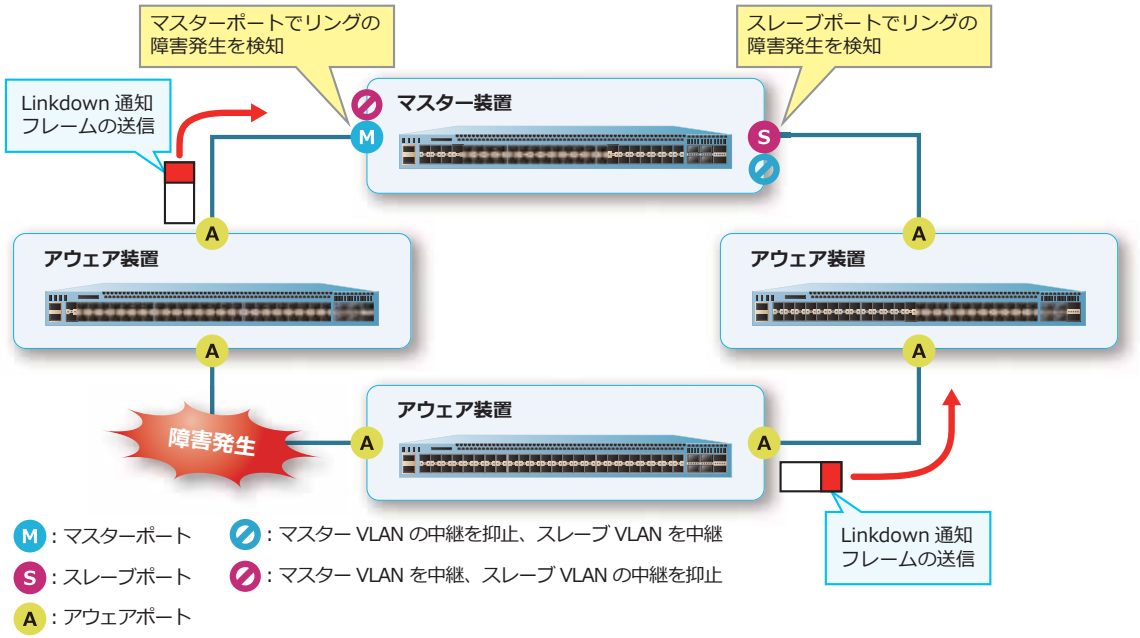
表 14-1 正常時のリングポート／コネクションの状態

リングポート	MMRP-Plus 状態	マスター VLAN 状態	スレーブ VLAN 状態	コネクション状態
マスターポート	Blocking	Forwarding	Blocking	Normal
スレーブポート	Blocking	Blocking	Forwarding	Normal
アウェアポート	Forwarding	Forwarding	Forwarding	Normal

14.1.4.2 リンクダウン障害発生時

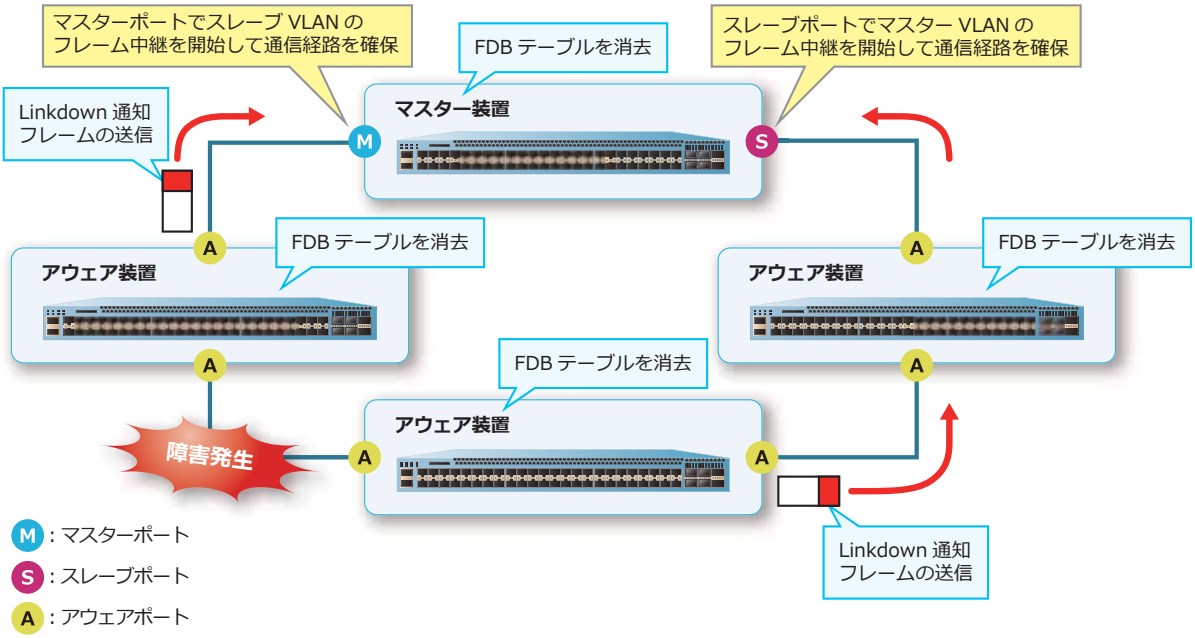
リンクダウン障害発生時は、リンクダウンしたリングポートは Down 状態へ遷移します。一方のアウェアポートが Down 状態に遷移したアウェア装置は、もう一方のアウェアポートから Linkdown 通知フレームを送信します。マスターポートおよびスレーブポートは Linkdown 通知フレームを受信することで、リング上でリンクダウンを伴う障害が発生したこと検知します。

図 14-9 リンクダウン障害発生時の動作例（1）



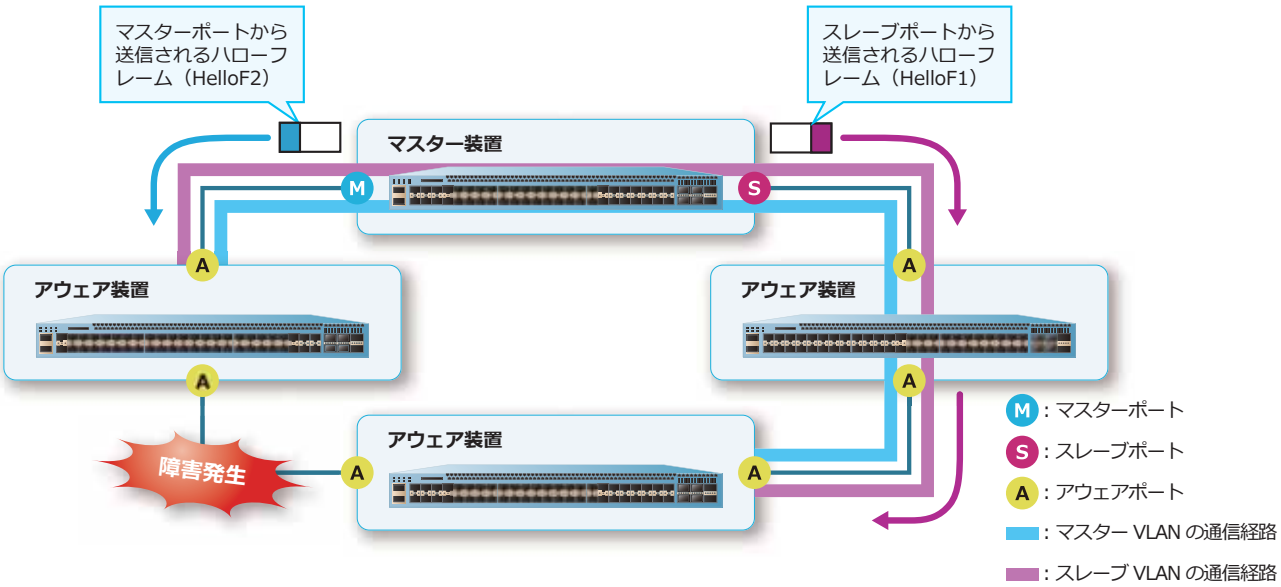
リング上の障害を検知すると、マスターポートおよびスレーブポートでブロックされていたフレームの中継が開始され、通信経路が切り替わります。その際に、通信が復旧するまでの時間を短縮するために、リング上の各装置の FDB テーブルを消去します。障害発生時に FDB テーブルを消去するポートを限定するには、**`mmrp-plus ring fdb-flush port`** コマンドを使用します。

図 14-10 リンクダウン障害発生時の動作例（2）



切り替わり後のリングの動作例は以下のとおりです。

図 14-11 リンクダウン障害による切り替わり後の通信経路の例



リンクダウン障害が発生して切り替わった後のリングポートの状態およびコネクション状態は、以下のとおりです。

表 14-2 リンクダウン障害による切り替わり後のリングポート／コネクションの状態

リングポート	MMRP-Plus 状態	マスター VLAN 状態	スレーブ VLAN 状態	コネクション状態
マスターポート	Forwarding	Forwarding	Forwarding	Broken
スレーブポート	Forwarding	Forwarding	Forwarding	Broken

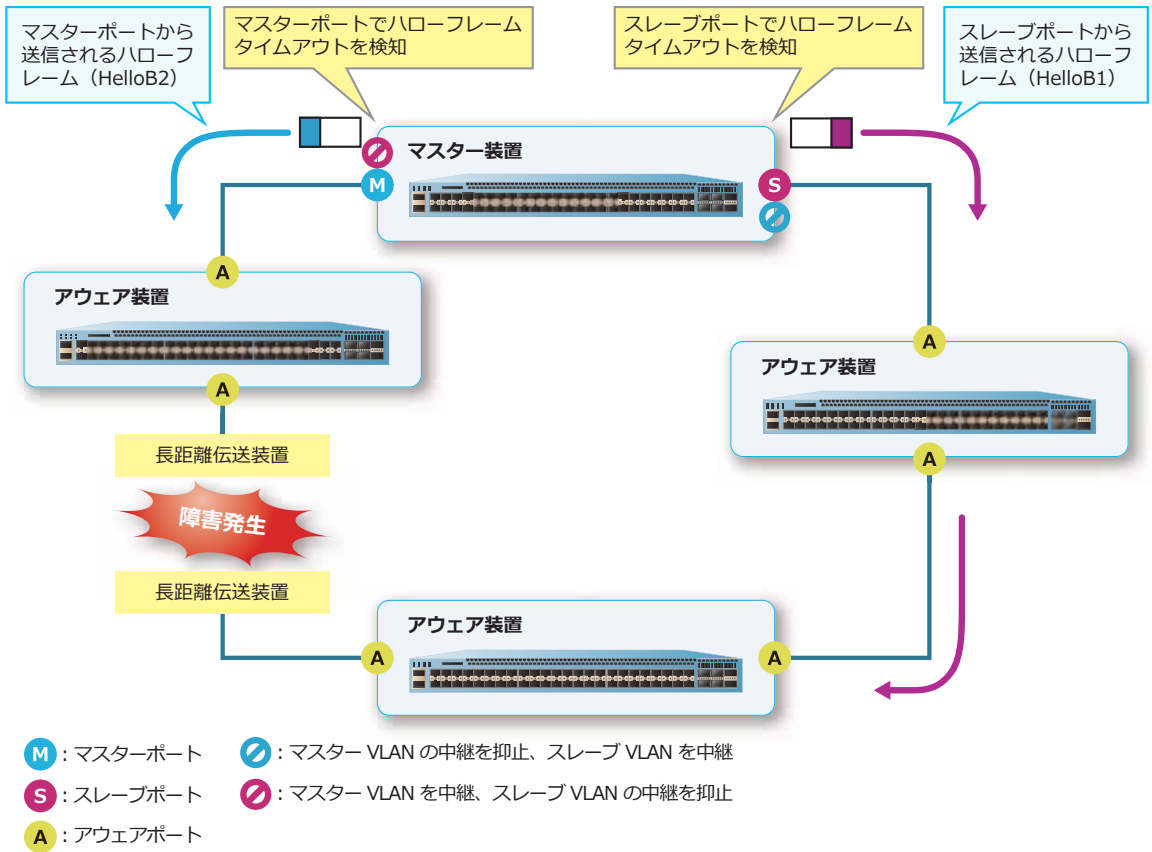
リングポート	MMRP-Plus 状態	マスター VLAN 状態	スレーブ VLAN 状態	コネクション状態
アウェアポート	Forwarding	Forwarding	Forwarding	Normal または Broken*1
リンクダウン障害が発生したアウェアポート	Down	Down	Down	Broken

*1：障害が発生していないリンク側は Normal、障害が発生しているリンク側は Broken

14.1.4.3 ハローフレームタイムアウトによる障害検知時

リンクダウンを伴わない障害が発生した場合は、ハローフレームタイムアウトにより障害を検知します。たとえば、リングの一部に長距離伝送装置が接続されていて、長距離伝送装置間で障害が発生した場合が該当します。この場合、リングポートはリンクダウンせず、Linkdown 通知フレームは送信されません。

図 14-12 ハローフレームタイムアウト障害発生時の動作例



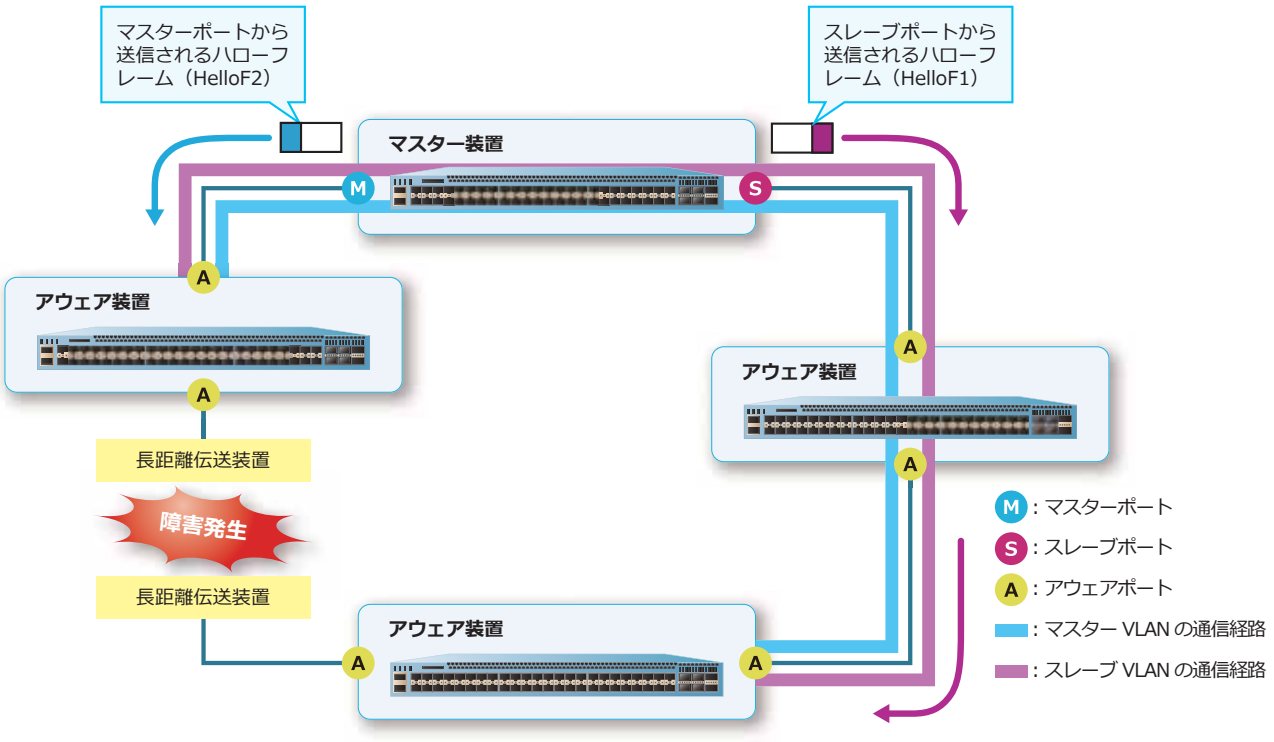
ハローフレームの受信タイムアウト時間を設定するには、**`mmrp-plus ring hello-timeout`** コマンドを使用します。

> ***NOTE:*** 装置の CPU 負荷が高い場合に、ハローフレームタイムアウト時間を小さくすると、MMRP-Plus の状態が不安定になる恐れがあります。

ハローフレームタイムアウトでリング上の障害を検知すると、マスターポートおよびスレーブポートでブロックされていたフレームの中継が開始され、通信経路が切り替わります。その際に、通信が復旧するまでの時間を短縮するために、リング上の各装置の FDB テーブルを消去します。障害発生時に FDB テーブルを消去するポートを限定するには、**`mmrp-plus ring fdb-flush port`** コマンドを使用します。

切り替わり後のリングの動作例は以下のとおりです。

図 14-13 ハローフレームタイムアウトによる切り替わり後の通信経路の例



ハローフレームタイムアウトにより切り替わった後のリングポートの状態およびコネクション状態は、以下のとおりです。

表 14-3 ハローフレームタイムアウトによる切り替わり後のリングポート／コネクションの状態

リングポート	MMRP-Plus 状態	マスター VLAN 状態	スレーブ VLAN 状態	コネクション状態
マスターポート	Forwarding	Forwarding	Forwarding	Broken
スレーブポート	Forwarding	Forwarding	Forwarding	Broken
アウェアポート	Forwarding	Forwarding	Forwarding	Normal または Broken*1

*1：障害が発生していないリンク側は Normal、障害が発生しているリンク側は Broken

14.1.4.4 障害復旧時

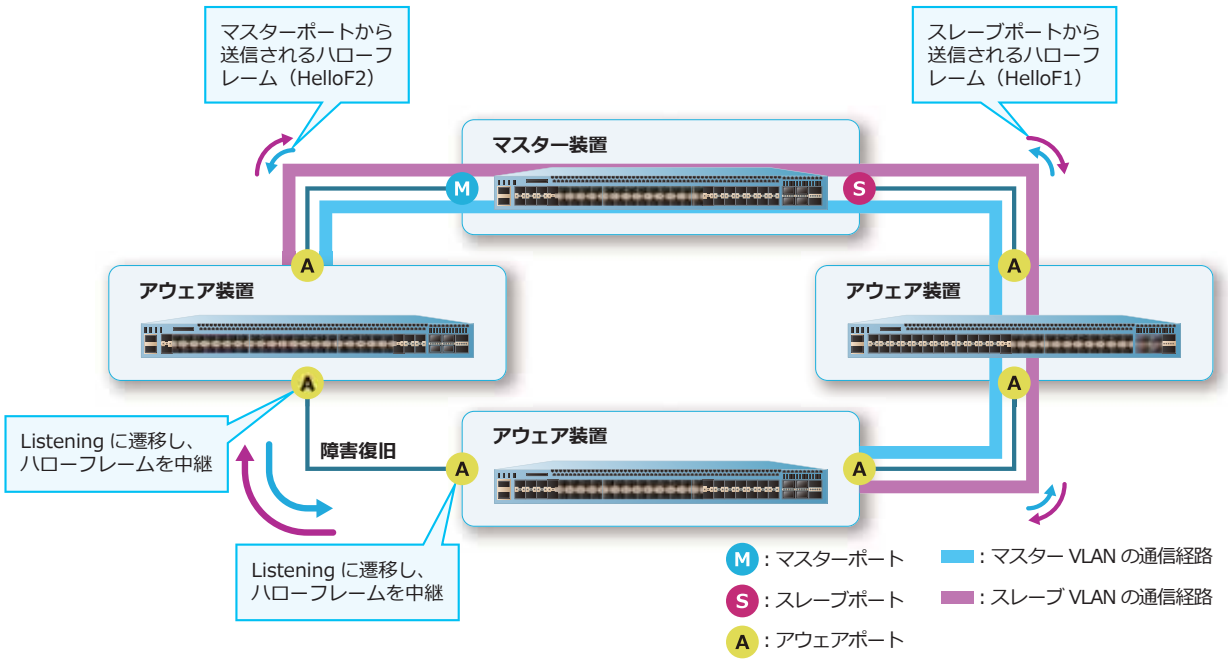
障害復旧時の動作を、リンクダウン障害が復旧した場合を例に説明します。

リンクダウンしていたリングポートがリンクアップすると、切り戻り方法の設定に従って動作します。

- 切り戻りタイマー値が 0（デフォルト設定）の場合は、リンクダウン障害が復旧するとすぐに Listening 状態へ遷移してリング復旧処理が開始されます。この場合は、FailureUp 状態には遷移しません。
- 切り戻りタイマー値が 0 以外に設定されている場合は、リンクダウン障害が復旧すると FailureUp 状態に遷移します。その後、切り戻りタイマー値の経過後に Listening 状態へ遷移し、リング復旧処理が開始されます。
- 手動切り戻り設定（disable パラメーター指定）の場合は、リンクダウン障害が復旧すると FailureUp 状態に遷移します。**`clear mmrp-plus failure ring`** コマンドを実行すると Listening 状態へ遷移し、リング復旧処理が開始されます。

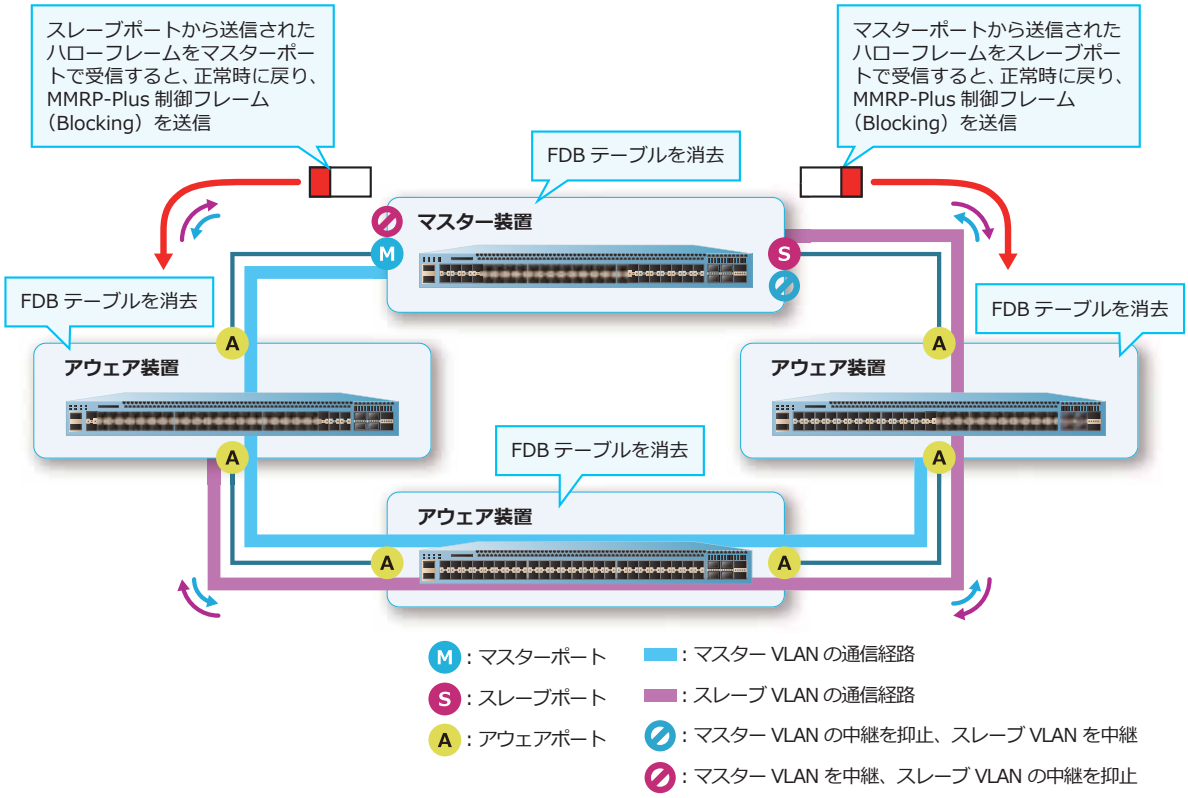
リンクダウン障害が復旧したアウェアポートが Listening 状態になると、ハローフレームなどの MMRP-Plus 制御フレームの中継が可能になります。その結果、マスターポート／スレーブポートでハローフレームを受信できるようになり、リング上の障害が復旧したと判断できるようになります。

図 14-14 障害復旧時の動作例（1）



リング上の障害が復旧したと判断されるとマスターポート／スレーブポートは正常時の状態に復旧し、正常時に戻ったことを通知するための MMRP-Plus 制御フレームを送信します。Listening 状態のアウェアポートがマスターポート／スレーブポートからの MMRP-Plus 制御フレーム（Blocking）を両方とも受信すると、正常時の状態に復旧します。その際に、通信が復旧するまでの時間を短縮するために、リング上の各装置の FDB テーブルを消去します。

図 14-15 障害復旧時の動作例（2）



リスニングタイムアウト時間

マスターポートまたはスレーブポートを設定した装置の負荷が大きいために、通常どおり復旧動作が行われているにもかかわらずリスニングタイムアウトを検知する場合があります。その場合は、リスニングタイムアウト時間を大きく設定して、タイムアウトを回避します。リスニングタイムアウト時間を設定するには、**`mmrp-plus ring listening-timer`** コマンドを使用します。

14.1.5 アップリンクポート連携機能

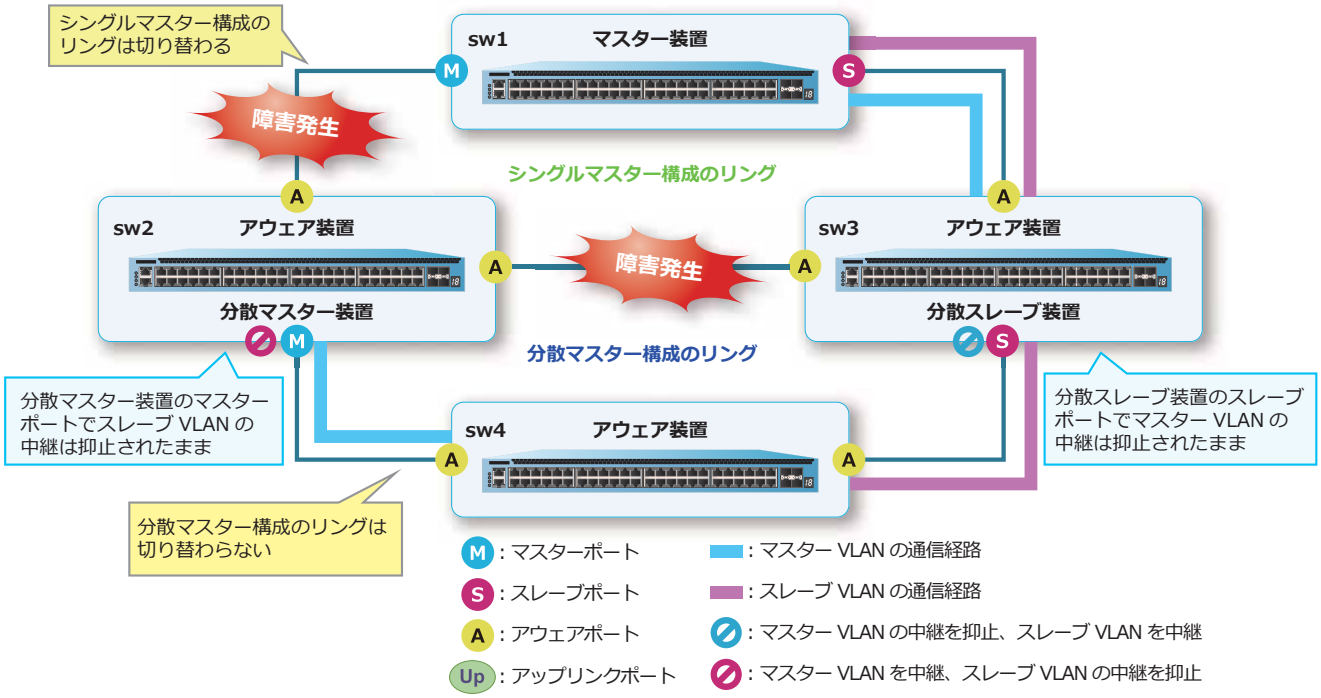
アップリンクポート連携機能は、分散マスター構成の分散マスター装置／分散スレーブ装置で使用できるオプション機能で、アウェア装置やシングルマスター構成のマスター装置では使用できません。この機能は、アップリンクポートに設定したすべてのポートがリンクダウンした場合に、当該 MMRP-Plus を強制的に切り替えます。また、アップリンクポートに設定したポートのうち 1 ポートでもリンクアップした場合は、当該 MMRP-Plus を切り戻します。

> ***CAUTION:*** アップリンクポート連携機能とポートリスタート機能は、同一リングで併用できません。また、ポートリダンダント機能とは同一インターフェースで併用できません。

> ***NOTE:*** アップリンクポート連携機能は、NP7000 の 1.06.01 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 1.07.01 以降、NP2500 の 1.08.02 以降でサポートしています。

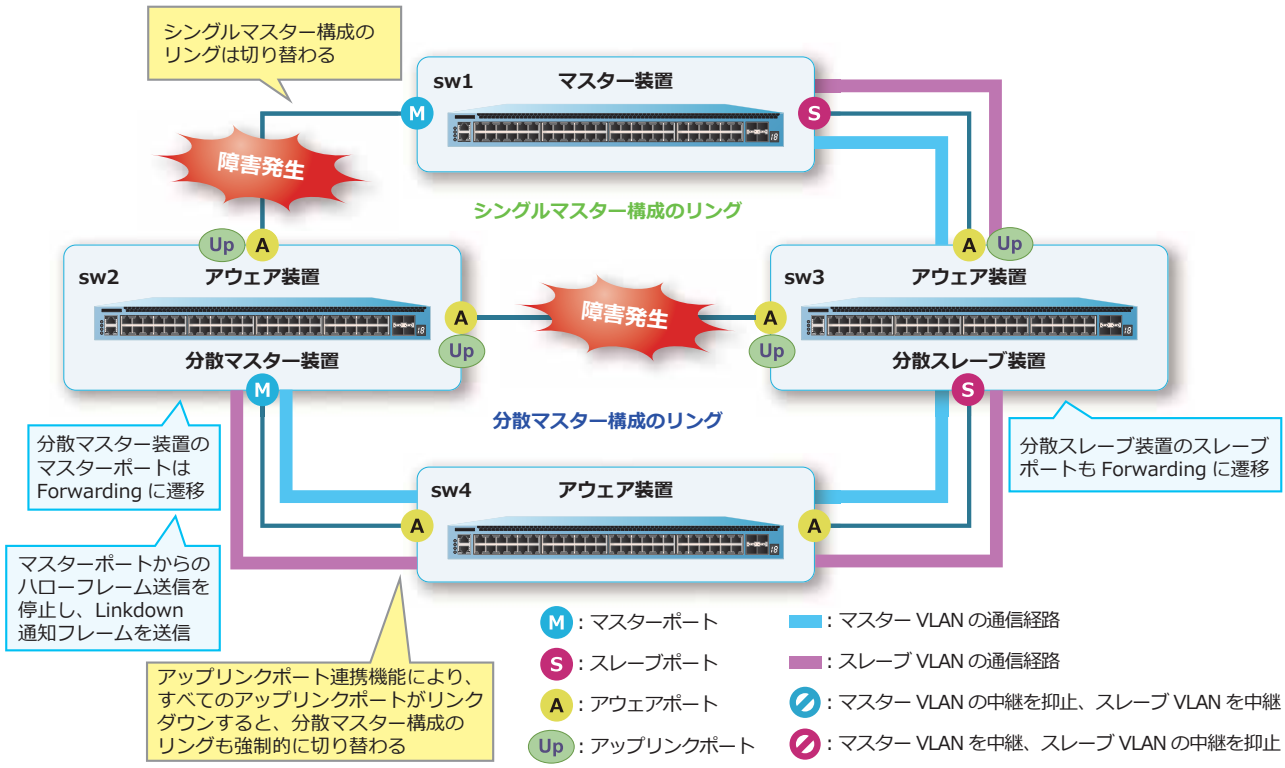
例のような構成で、シングルマスター構成のリングの 2 カ所がリンクダウンする二重障害が発生した場合、シングルマスター構成のリングは切り替わりますが、分散マスター構成のリングは切り替わりません。その結果、「sw1,sw3 ～ sw2,sw4 の間のマスター VLAN の通信」「sw2 ～ sw1,sw3,sw4 の間のスレーブ VLAN の通信」はできなくなります。

図 14-16 二重障害発生時の通信不可経路の例



アップリンクポート連携機能を使用すると、そのような状況になることを回避できます。例のようにアップリンクポートが設定されている場合、すべてのアップリンクポートがリンクダウンした分散マスター装置では、アップリンクポート連携機能が動作してマスターポートは Forwarding 状態に遷移します。同時に、マスターポートからのハローフレーム送信を停止し、Linkdown 通知フレームを送信して分散マスター構成のリングを強制的に切り替えます。これにより、すべてのスイッチ間でマスター VLAN とスレーブ VLAN の通信が可能になります。

図 14-17 アップリンクポート連携機能の動作例



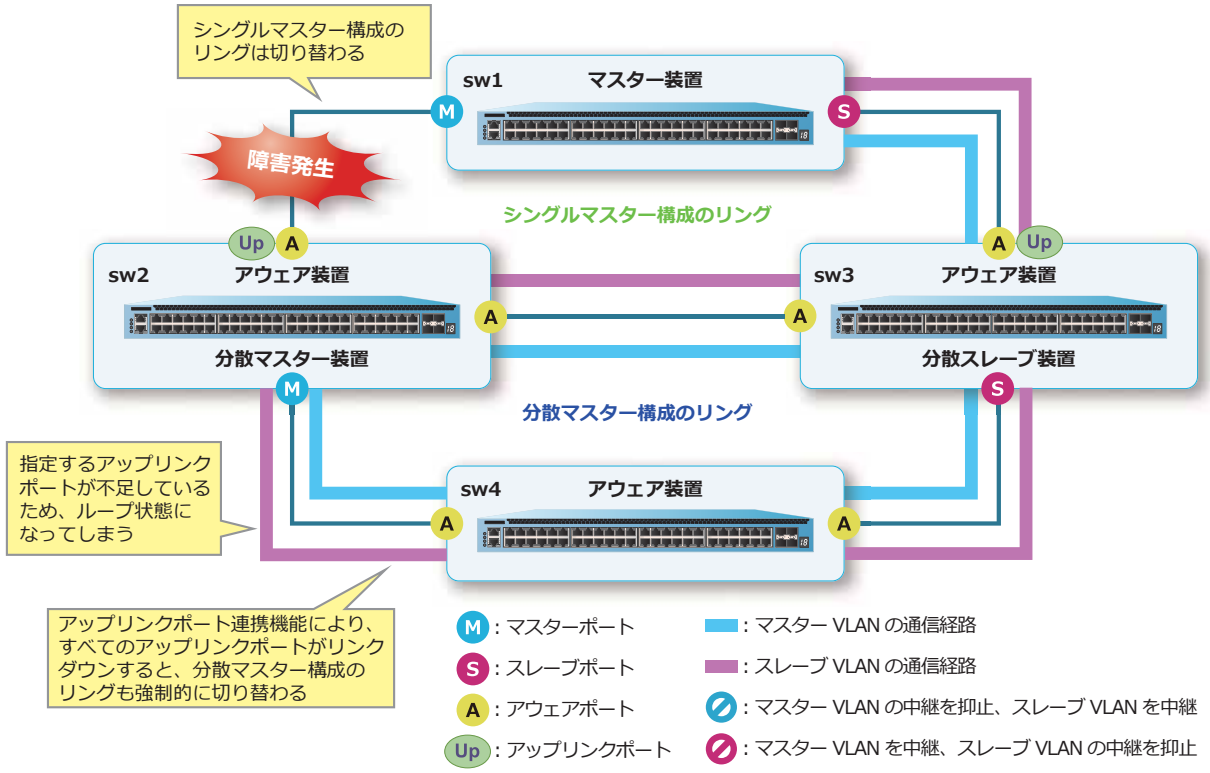
分散スレーブ装置の場合も同様に動作します。すべてのアップリンクポートがリンクダウンした分散スレーブ装置では、アップリンクポート連携機能が動作してスレーブポートは Forwarding 状態に遷移します。同時に、スレーブポートからのハローフレーム送信を停止し、Linkdown 通知フレームを送信して分散マスター構成のリングを強制的に切り替えます。

アップリンクポート連携機能を設定するには、**`mmrp-plus ring uplink port`** コマンドを使用します。

> ***NOTE:*** **`mmrp-plus ring uplink port`** コマンドは既存の設定を上書きするため、設定時はすべての対象ポートを指定して実行してください。また、ポートチャネルを対象にする場合は、そのポートチャネルのすべてのメンバーポートを指定してください。

ネットワーク構成によっては、指定するアップリンクポートが不足している場合に、アップリンクポート連携機能動作時にループ状態になることがあります。例の構成のように片方のアウェアポートだけをアップリンクポートとして設定した場合は、そのポートがリンクダウンすると、シングルマスター構成のリングだけでなく、アップリンクポート連携機能によって分散マスター構成のリングも切り替わります。その結果、ループ状態になってしまいます。このような状況にならないように、アップリンクポート連携機能を使用する際は十分に事前検討した上で使用してください。

図 14-18 アップリンクポート設定不足時のループ発生例



14.1.6 ポートリスタート機能

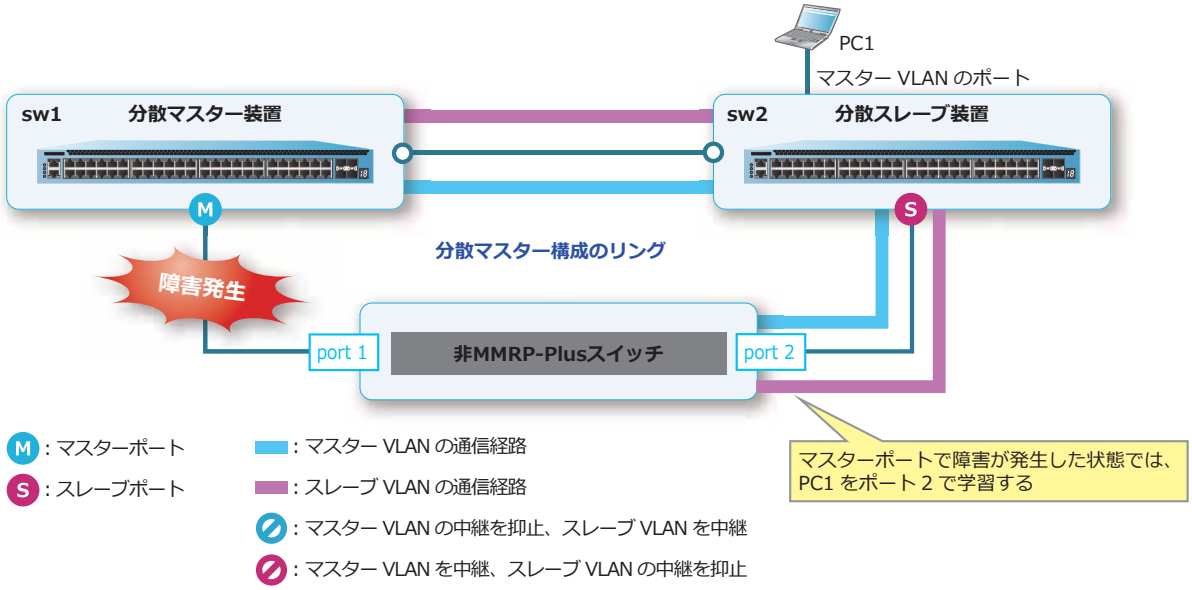
ポートリスタート機能は、分散マスター構成の分散マスター装置／分散スレーブ装置、またはシングルマスター構成のマスター装置で使用できるオプション機能で、アウェア装置では使用できません。この機能は、非 MMRP-Plus スイッチ（MMRP-Plus が動作しない他社スイッチなど）を接続する場合に有効なオプション機能です。基本的には「1 台の非 MMRP-Plus スイッチを、分散マスタースイッチと分散スレーブスイッチに直接接続して収容する」構成で使用します。

> ***CAUTION:*** ポートリスタート機能とアップリンクポート連携機能は、同一リングで併用できません。また、ポートリスタート機能を有効にしたリングポートでは、LLDP 疑似リンクダウン機能は併用できません。

> ***NOTE:*** ポートリスタート機能は、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 1.07.01 以降、NP2500 の 1.08.02 以降でサポートしています。

例のような構成で、マスターポートのリンクダウン障害が発生した場合は、マスター VLAN は分散スレーブ装置を経由して通信することになります。そのため、非 MMRP-Plus スイッチではマスター VLAN の PC1 をポート 2 で学習します。

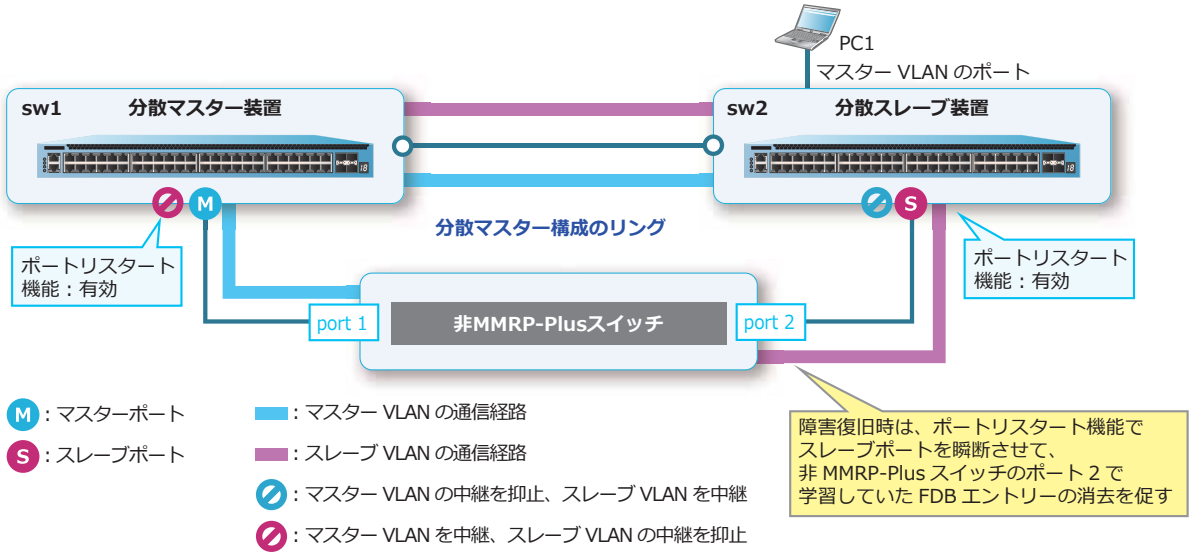
図 14-19 ポートリスタート機能の動作例（1）



この状態からマスターポートがリンクアップして障害が復旧した場合は、マスター VLAN は分散マスター装置を経由して通信することになります。しかし、非 MMRP-Plus スイッチでは復旧時に FDB フラッシュはされないため、PC1 をポート 2 で学習したままになります。そのため、PC1 をポート 1 で再学習するか、またはエージング時間が経過して FDB エントリーが消去されるまでは、非 MMRP-Plus スイッチでは PC1 宛てのトラフィックを通信できないポート宛てに中継することになります。

ポートリスタート機能を使用すると、そのような状況になることを回避できます。例のようにポートリスタート機能を有効にしていると、マスターポートの障害復旧時にはスレーブポートを瞬断させます。スレーブポートの障害復旧時にはマスターポートを瞬断させます。これにより、非 MMRP-Plus スイッチの FDB エントリーの消去を促します。

図 14-20 ポートリスタート機能の動作例（2）



ポートリスタート機能を設定するには、**`mmrp-plus ring port-restart enable`** コマンドを使用します。

14.1.7 別リングへの FDB フラッシュフレーム送信機能

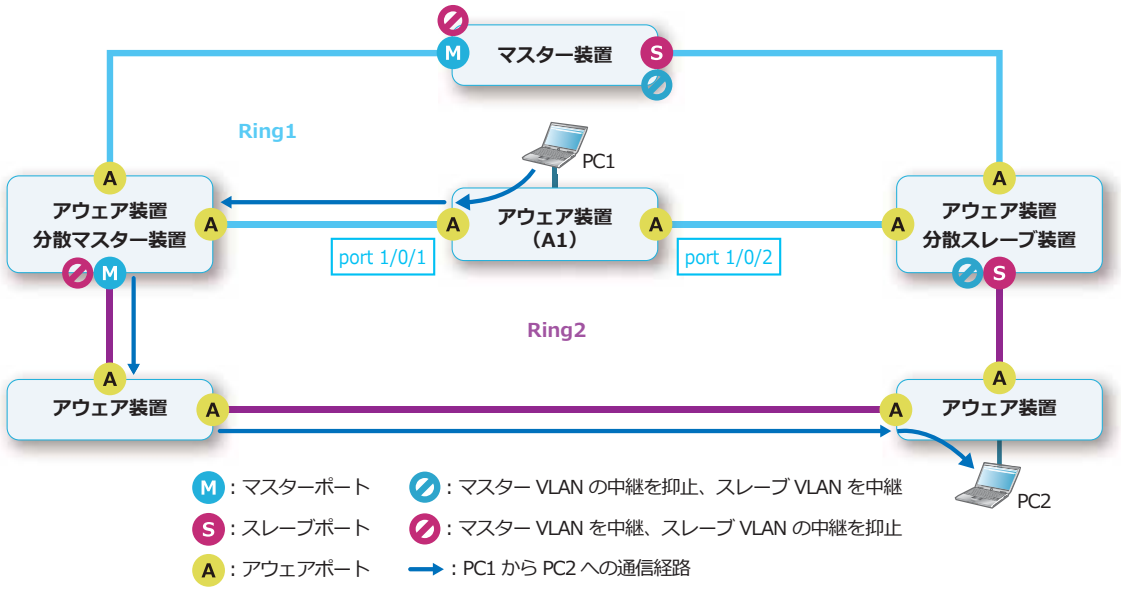
別リングへの FDB フラッシュフレーム送信機能は、分散マスター構成の分散マスター装置／分散スレーブ装置で使用できるオプション機能で、アウェア装置やシングルマスター構成のマスター装置では使用できません。この機能は、以下の条件をすべて満たす構成の場合に有効なオプション機能です。

- 分散マスター構成で、分散マスター装置と分散スレーブ装置が別リングにも接続されている。
- 分散マスター装置と分散スレーブ装置の間に別リングのアウェア装置が接続されている。
- 分散マスター構成のリングの切り替わり／切り戻り時に、その別リングのアウェア装置で中継方向が変更される通信が存在する。

NOTE: シングルマスター構成の場合や、分散マスター装置と分散スレーブ装置が直接接続されている場合は、本機能を設定する必要はありません。

例のような構成（対象はマスター VLAN とします）の場合、正常時はマスター装置／分散スレーブ装置のスレーブポートでフレーム中継が抑止されているため、PC1 と PC2 間の通信経路は図のようになります。そのため、アウェア装置 A1 では PC2 をポート 1/0/1 で学習します。

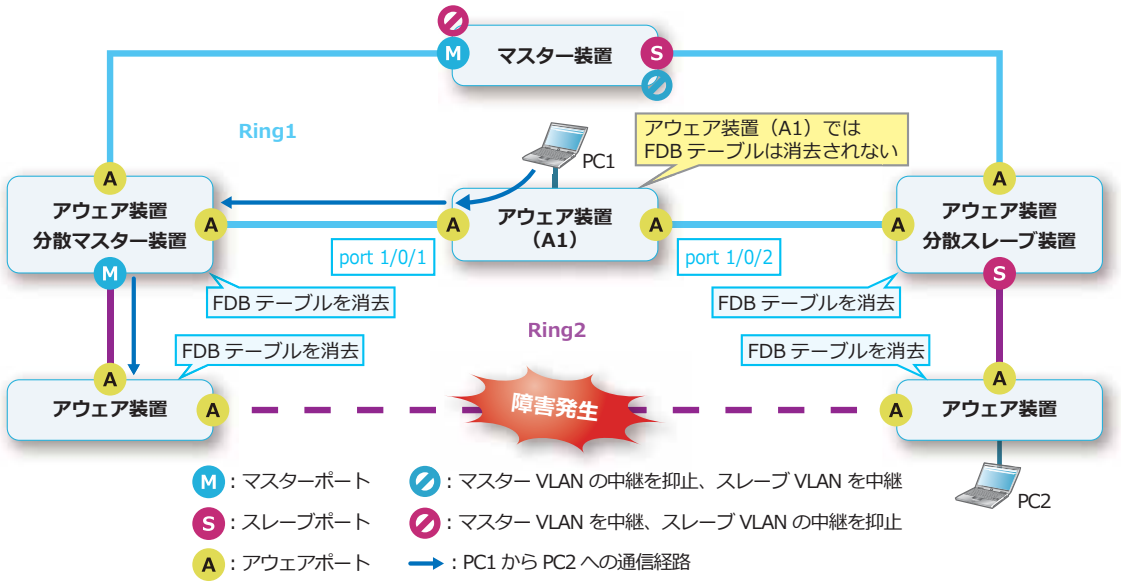
図 14-21 別リングへの FDB フラッシュフレーム送信機能の動作例（1）



この例において、PC1 から PC2 への通信経路上の Ring2 で障害が発生した場合を想定します。

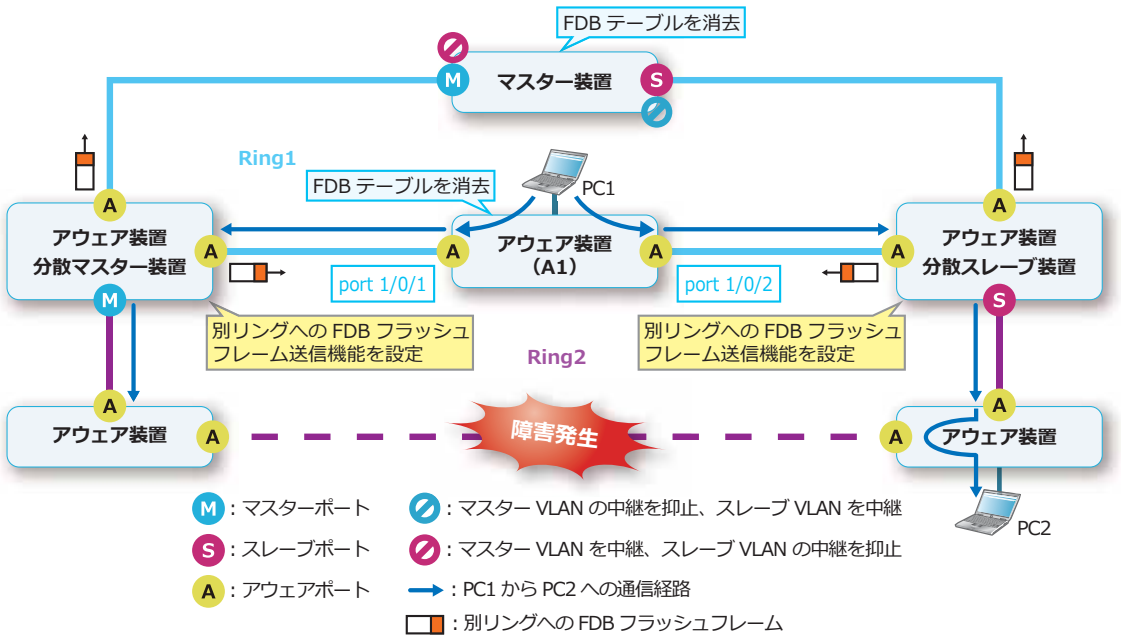
分散マスター構成の Ring2 で障害が発生した場合、通常は Ring2 の装置で FDB テーブルが消去され、別リングの装置では FDB テーブルは消去されません。そのため、アウェア装置 A1 では PC2 をポート 1/0/2 で再学習するか、またはエージング時間が経過して FDB エントリーが消去されるまでは、PC2 宛てのトラフィックを通信できないポートに中継することになります。

図 14-22 別リングへの FDB フラッシュフレーム送信機能の動作例（2）



このような状況で PC1 から PC2 への通信が復旧するまでの時間を短縮するには、別リングへの FDB フラッシュフレーム送信機能を使用します。Ring2 の分散マスター装置／分散スレーブ装置で FDB フラッシュフレーム送信機能を設定していると、設定した別リングのリングポートからも FDB フラッシュフレームを送信するようになります。その結果、アウェア装置 A1 でも FDB テーブルが消去されて、PC1 から PC2 への通信が復旧するまでの時間の短縮が期待できます。

図 14-23 別リングへの FDB フラッシュフレーム送信機能の動作例（3）



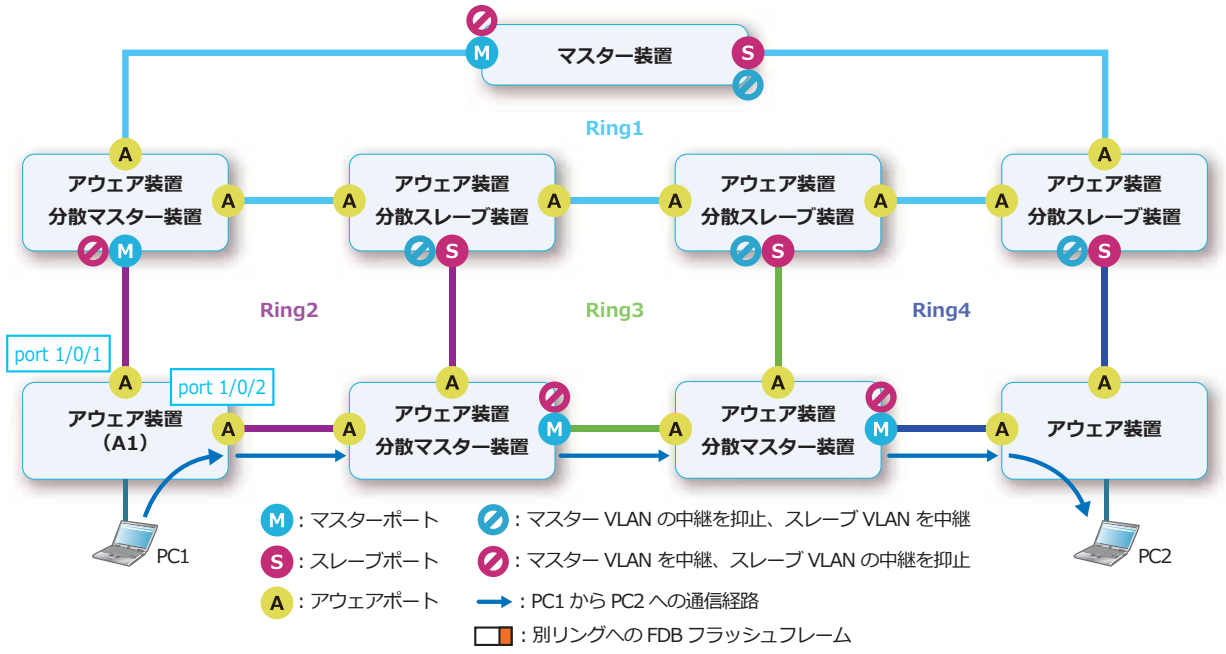
FDB フラッシュフレームを送信する別リングのリングポートを設定するには、**`mmrp-plus ring transmit-fdb-flush port`** コマンドを使用します。

14.1.8 FDB フラッシュフレーム中継機能

FDB フラッシュフレーム中継機能は、分散マスター構成の分散マスター装置／分散スレーブ装置で使用できるオプション機能で、アウェア装置やシングルマスター構成のマスター装置では使用できません。

例のような構成（対象はマスター VLAN とします）の場合、正常時はマスター装置／分散スレーブ装置のスレーブポートでフレーム中継が抑止されているため、PC1 と PC2 間の通信経路は図のようになります。そのため、アウェア装置 A1 では PC2 をポート 1/0/2 で学習します。

図 14-24 FDB フラッシュフレーム中継機能の動作例（1）

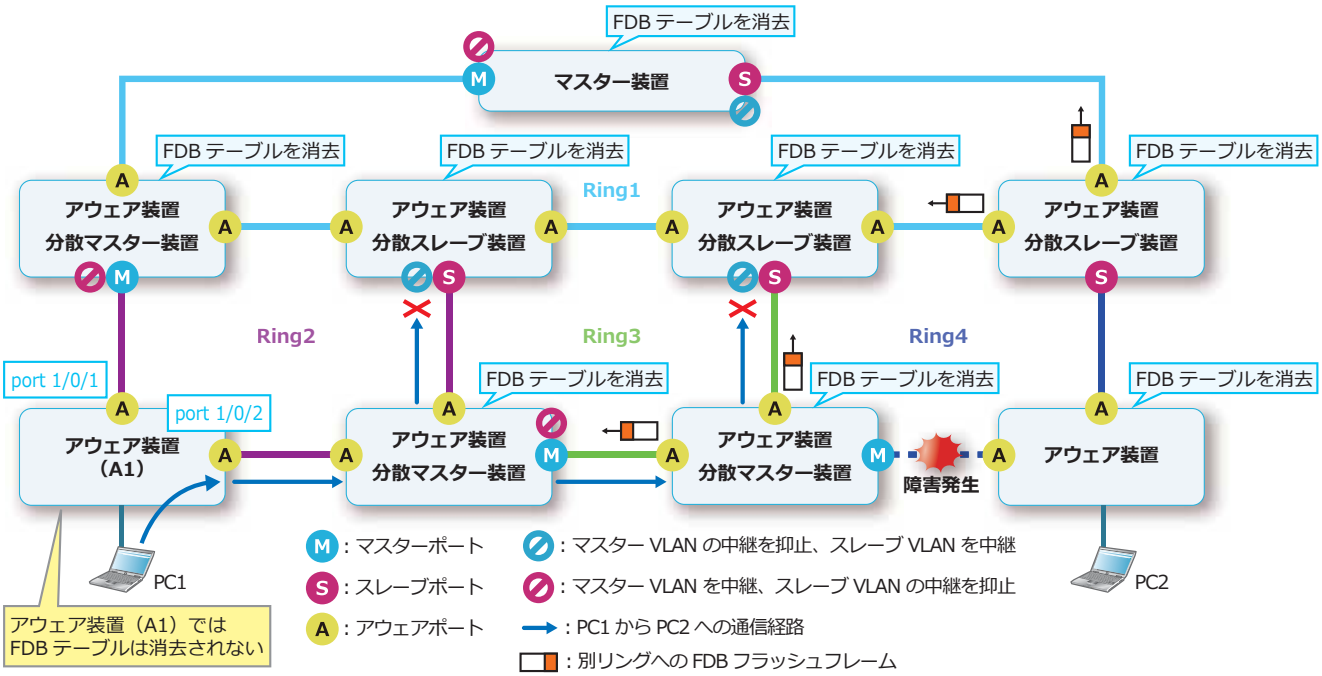


この例において、PC1 から PC2 への通信経路上の Ring4 で障害が発生した場合を想定します。

Ring4 で障害が発生した場合、通常は Ring4 の装置で FDB テーブルが消去されます。Ring4 の分散マスター装置／分散スレーブ装置で「別リングへの FDB フラッシュフレーム送信機能」を設定していると、Ring4 の切り替わり／切り戻り時に Ring1 と Ring3 にも FDB フラッシュフレームを送信し、Ring1 と Ring3 の装置も FDB テーブルを消去できます。

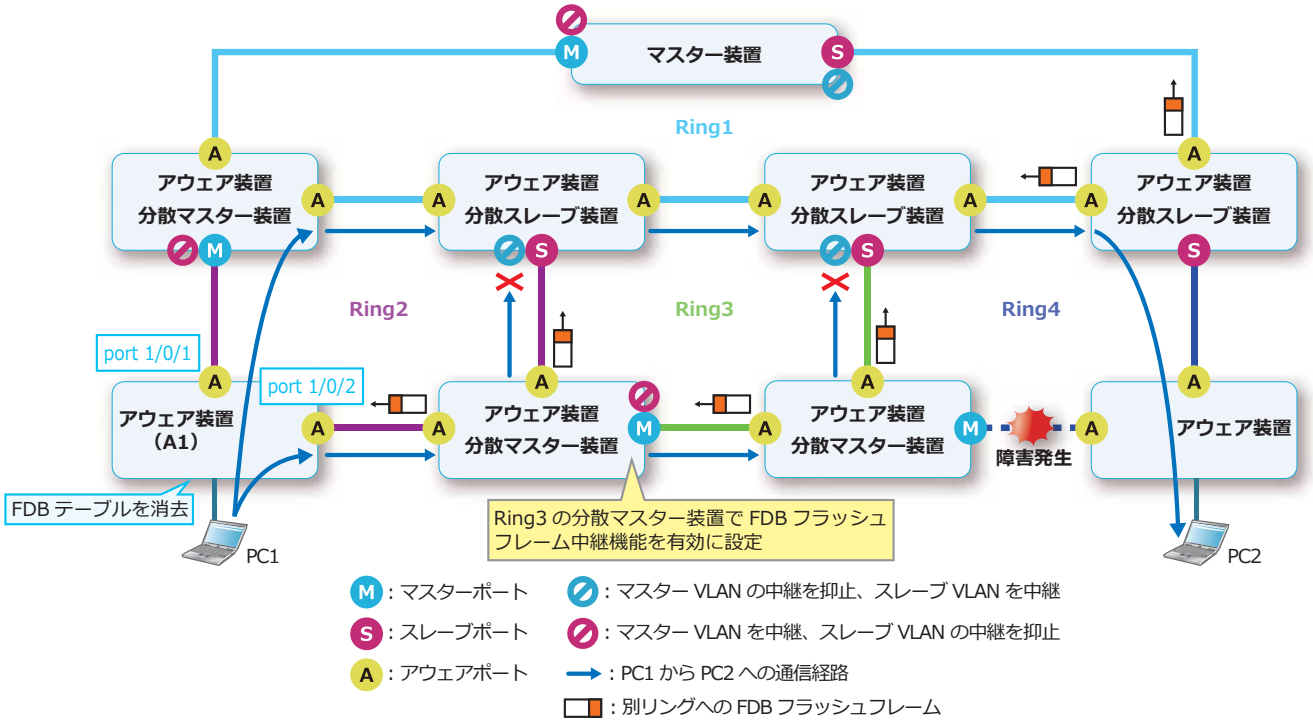
しかしながら、Ring2 には FDB フラッシュフレームが届かないため、アウェア装置 A1 では FDB テーブルは消去されません。その結果、PC2 をポート 1/0/1 で再学習するか、またはエージング時間が経過して FDB エントリーが消去されるまでは、アウェア装置 A1 では PC2 宛てのトラフィックを通信できないポートに中継することになります。

図 14-25 FDB フラッシュフレーム中継機能の動作例（2）



このような状況で PC1 から PC2 への通信が復旧するまでの時間を短縮するには、FDB フラッシュフレーム中継機能を使用します。Ring3 の分散マスター装置で FDB フラッシュフレーム中継機能を有効にしていると、Ring4 から送信されてきた FDB フラッシュフレームを Ring2 に中継できるようになります。その結果、アウェア装置 A1 でも FDB テーブルが消去されて、PC1 から PC2 への通信が復旧するまでの時間の短縮が期待できます。

図 14-26 FDB フラッシュフレーム中継機能の動作例（3）



FDB フラッシュフレーム中継機能を有効にするには、**`mmrp-plus ring transmit-fdb-flush retransmit enable`** コマンドを使用します。分散マスター装置のマスターポート／分散スレーブ装置のスレーブポートで受信した FDB フラッシュフレームの中継先ポートは、**`mmrp-plus ring transmit-fdb-flush port`** コマンドで指定します。

> ***NOTE:*** 複数のリングで FDB フラッシュフレーム中継機能を使用する場合は、FDB フラッシュフレームの中継がループしないよう、ネットワーク設計を十分に検討して使用してください。

14.1.9 FDB フラッシュ対象ポート（fdb-flush port）

ApresiaNP シリーズでは、MMRP-Plus リングの障害発生／復旧時には装置全体の FDB エントリーを消去しますが、FDB エントリーを消去する対象ポートを設定することもできます。

MMRP-Plus リングの障害発生／復旧時に FDB エントリーを消去する対象ポートを設定するには、**`mmrp-plus ring fdb-flush port`** コマンドを使用します。

> ***NOTE:*** 本コマンドを設定する場合は、対象 MMRP-Plus リングのリングポートを含めて設定してください。
>
> ***NOTE:*** ポートチャネルを対象にする場合は、そのポートチャネルのすべてのメンバーポートを指定してください。
>
> ***NOTE:*** 本コマンドは既存の設定を上書きするため、設定時はすべての対象ポートを指定して実行してください。

本コマンドの設定によって、MMRP-Plus リングの障害発生および復旧時の FDB エントリーと ARP キャッシュエントリーの消去動作が変わります。デフォルト設定時と、本コマンドを MMRP-Plus ポートを含めて設定した場合の、それぞれのエントリーの消去対象になるポートを以下に示します。

表 14-4 mmrp-plus ring fdb-flush port 設定と対象ポート

設定	FDB エントリーの消去対象ポート	ARP キャッシュエントリーの消去対象ポート
デフォルト設定時	MMRP-Plus ポートを含むすべてのポート	MMRP-Plus ポートのみ
MMRP-Plus ポートを含めてポート指定時	MMRP-Plus ポートを含む指定ポート	MMRP-Plus ポートと指定ポート

14.1.10 MAC アドレス学習停止時間（fdb-flush timer）

片方向通信の場合は、切り替わり／切り戻り時に新しい経路をすぐに再学習できません。そこで MMRP-Plus では、切り替わり／切り戻り時に装置の FDB テーブルを消去することで、片方向通信の場合でも高速な切り替えを実現しています。

ただし、リング上に他社製スイッチが混在している場合は、切り戻り時にリングがループ状態になり、誤った方向に MAC アドレスを学習してしまう可能性があります。これを防止するため、FDB テーブルを消去する際にいったん MAC アドレスの学習を停止し、MAC アドレス学習停止時間（FDB フラッシュタイマー）が経過した後、学習を再開する仕組みになっています。

MAC アドレス学習停止時間を設定するには、**`mmrp-plus ring fdb-flush timer`** コマンドを使用します。

> ***NOTE:*** レイヤー 3 機能と MMRP-Plus を併用する場合、MAC アドレス学習停止時間を 0 秒に設定することを推奨します。

14.1.11 MMRP-Plus DFM 機能

MMRP-Plus DFM（Double Fault Monitor）機能は、分散マスター構成のリングでのみ使用できるオプション機能で、シングルマスター構成のリングでは使用できません。分散マスター構成のリング内で二重障害が発生した場合に、通信経路をあらかじめ設定していた迂回路に切り替えることにより通信断を回避するオプション機能です。

CAUTION: MMRP-Plus DFM 機能はスタック構成の装置での使用はサポートしていません。

NOTE: MMRP-Plus DFM 機能を使用するリングでは、そのリング内のすべての MMRP-Plus 装置で MMRP-Plus DFM 機能を有効にする必要があります。

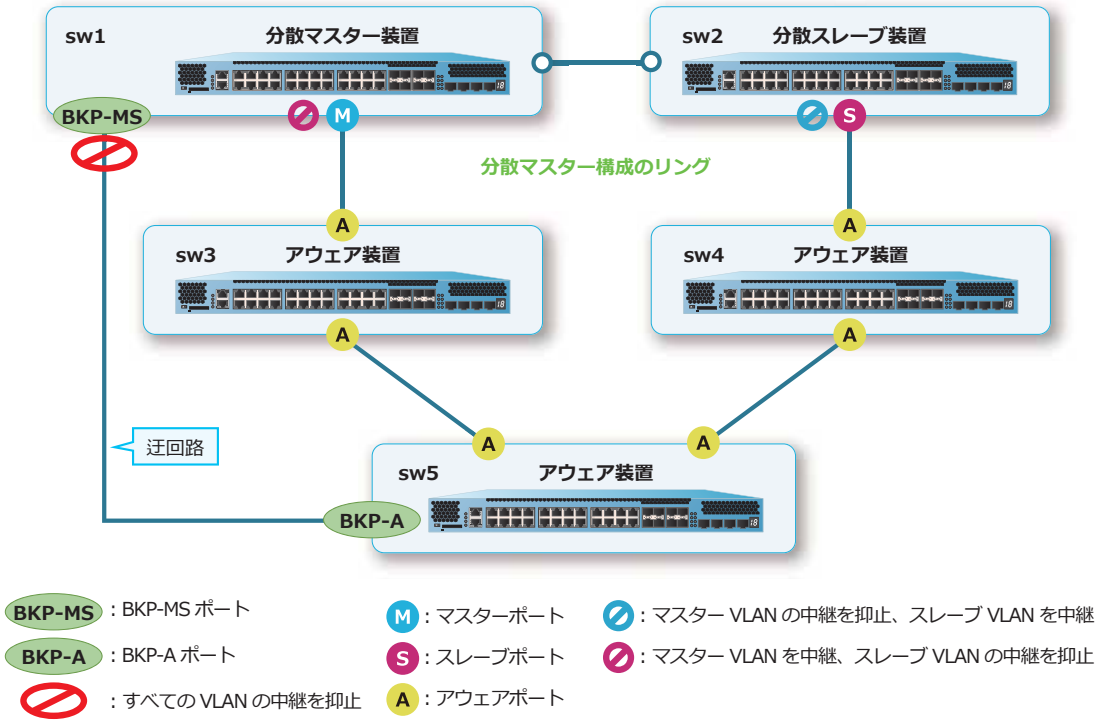
NOTE: MMRP-Plus DFM 機能を使用する装置で設定可能なリング数は最大 15 個です。

NOTE: MMRP-Plus DFM 機能は、NP3000 の 1.11.01 以降でサポートしています。

14.1.11.1 MMRP-Plus DFM 機能の基本設定

MMRP-Plus DFM 機能では、「分散マスター装置とアウェア装置間」または「分散スレーブ装置とアウェア装置間」に迂回路を設定します。分散マスター装置または分散スレーブ装置に設定した迂回路接続ポートは BKP-MS ポートと呼びます。アウェア装置に設定した迂回路接続ポートは BKP-A ポートと呼びます。「分散マスター装置とアウェア装置間」に迂回路を設定した場合の構成例を以下に示します。

図 14-27 MMRP-Plus DFM 機能の構成例



迂回路は 1 つの MMRP-Plus リングにつき 1 経路まで接続できます。また、各装置は 1 つの MMRP-Plus リングに対して 1 個の物理ポートを迂回路接続ポートとして設定できます。複数の物理ポートやポートチャネルを迂回路接続ポートとして設定することはできません。

BKP-MS ポートと BKP-A ポートの間の迂回路には、レイヤー 2 スイッチのような MAC アドレスを学習して中継先を判断する装置を接続しないようにしてください。そのような装置を接続していると、迂回路への切り替わり／切り戻り時に、その装置で MAC アドレスを再学習するまでユニキャストトラフィックが中継されない可能性があります。

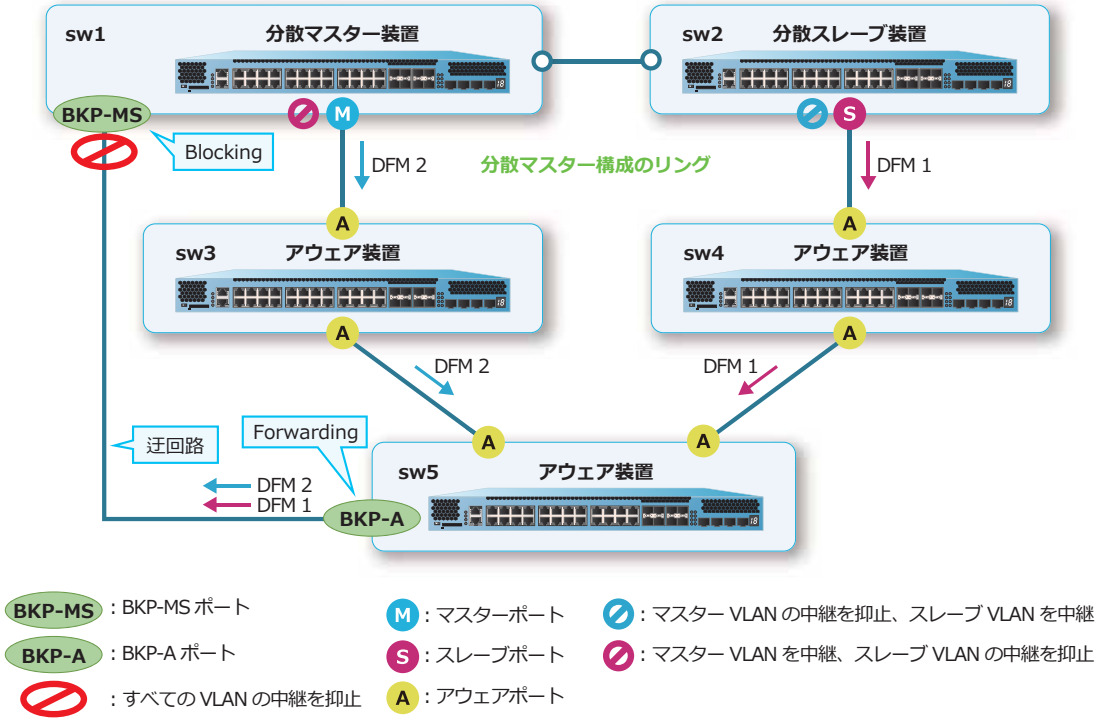
MMRP-Plus DFM 機能を有効にするには、**`mmrp-plus ring double-fault-monitor enable`** コマンドを使用します。また、迂回路接続ポートを設定するには、**`mmrp-plus ring backup-path`** コマンドを使用します。

NOTE: 別リングのリングポートや、すでに別リングの迂回路接続ポートとして設定されている物理ポートを迂回路接続ポートとして設定することはできません。

14.1.11.2 MMRP-Plus DFM 機能の動作例

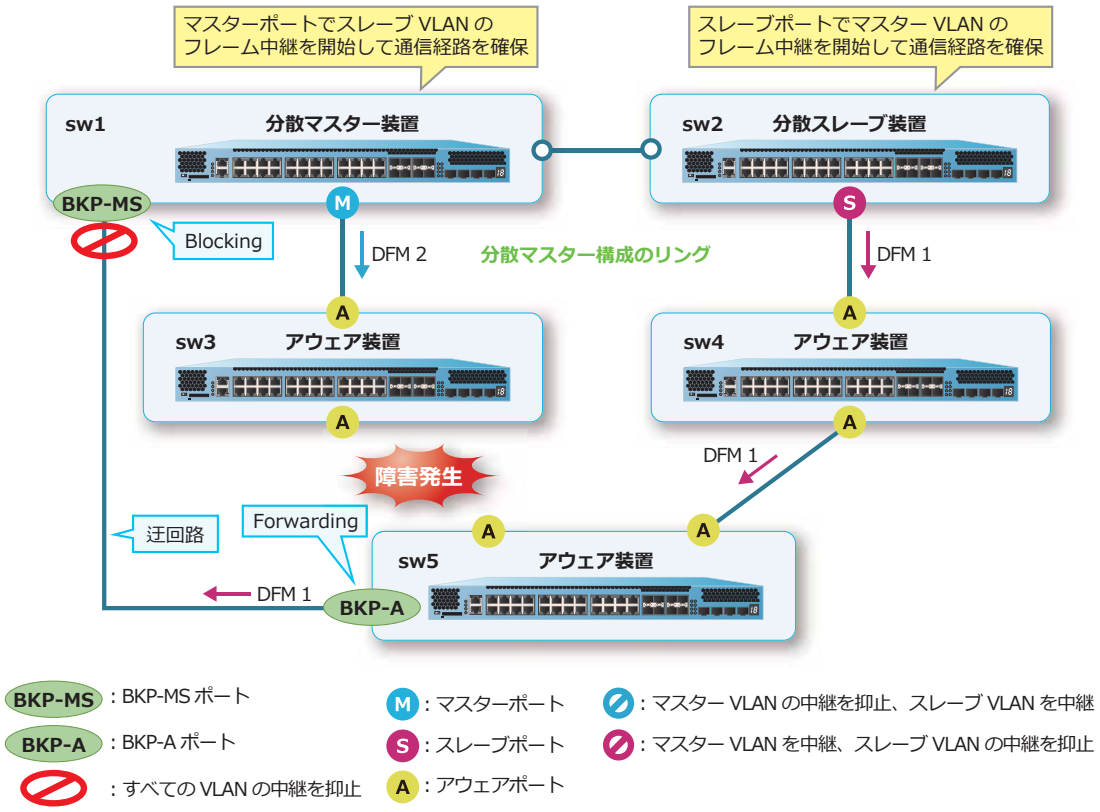
MMRP-Plus DFM 機能を有効にした分散マスター構成のリングでは、分散マスター装置と分散スレーブ装置がハローフレームとは別に MMRP-Plus DFM 機能用の制御フレーム（DFM フレーム）をリング内に定期的に送信します。迂回路に接続されたアウェア装置では、アウェアポートで受信した DFM フレームを迂回路接続ポート（BKP-A ポート）に中継します。その結果、正常時には BKP-MS ポートで分散マスター装置または分散スレーブ装置が送信した DFM フレームを受信することになります。
BKP-MS ポートは、両方または片方の DFM フレームを受信し続けている間は、すべての VLAN の中継を抑止します。

図 14-28 MMRP-Plus DFM 機能の正常時の動作例



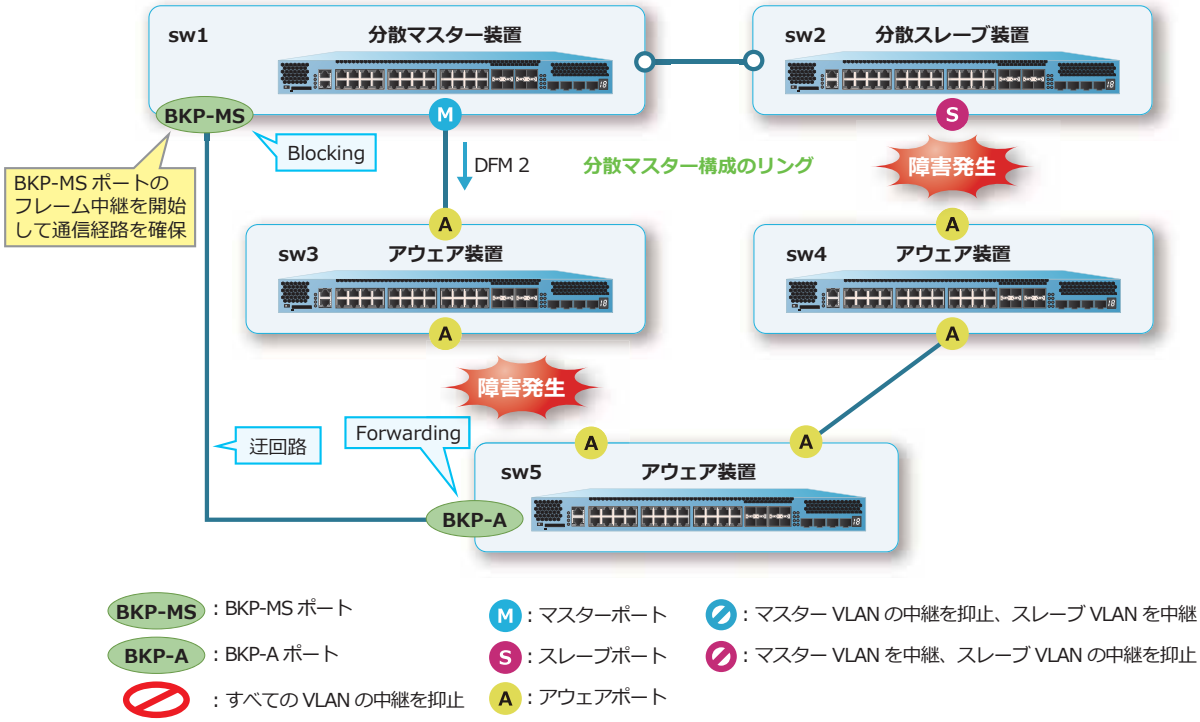
この構成例において、sw3 ～ sw5 の間でリンクダウン障害が発生した場合は、マスターポートおよびスレーブポートでブロックされていたフレームの中継が開始され、通信経路が切り替わります。これは通常の MMRP-Plus の切り替わり動作です。この時点ではまだ、BKP-MS ポートで分散スレーブ装置が送信した DFM フレームを受信しているため、BKP-MS ポートはすべての VLAN の中継を抑止したままです。

図 14-29 単体のリング障害発生時の動作例



単体のリング障害が発生している状態から、さらに sw2 ～ sw4 の間でリンクダウン障害が発生した場合は、リング内で二重障害が発生したことになります。BKP-MS ポートでは両方の DFM フレームを受信しない状態になるため DFM フレームの受信タイムアウトを検知して、ブロックしていたフレームの中継を開始します。これにより通信経路が迂回路に切り替わります。

図 14-30 リング内で二重障害発生時の動作例



DFM フレームの受信タイムアウト時間を設定するには、**`mmrp-plus ring dfm-timeout`** コマンドを使用します。デフォルト設定は 1 秒です。

リング内で二重障害が発生している状態からいずれか一方の障害が復旧した場合、BKP-MS ポートでは DFM フレームの受信を検知して、すべての VLAN の中継を抑止する状態に切り戻ります。障害が復旧したリングポートが Listening 状態（リスニングタイムアウト時間のデフォルト設定は 10 秒）の間に、先に BKP-MS ポートが Blocking 状態に切り戻ることを想定しており、それにより復旧時にループ状態になることを回避しています。

なお、このような仕組みで復旧するため、二重障害時に迂回路に切り替わっていた通信は、「BKP-MS ポートが正常状態（通信を抑止）に復旧」してから「障害が復旧したリングポートがリスニングタイムアウト（デフォルト設定は 10 秒）して正常状態（通信可能）に復旧」するまでの間は通信断になることに注意してください。

14.1.11.3迂回路の正常性監視

MMRP-Plus DFM 機能では、迂回路の正常性を監視する機能も備えています。リング内二重障害が発生して BKP-MS ポートで DFM フレームの受信タイムアウトを検知した際の動作は、迂回路の状態によって以下のように異なります。

- 迂回路が正常と判断されている状態では、DFM フレームの受信タイムアウトを検知すると BKP-MS ポートは切り替わって、すべての VLAN の中継を開始する（Forwarding に遷移）。
- 迂回路が異常と判断されている状態では、DFM フレームの受信タイムアウトを検知しても BKP-MS ポートは切り替わらずに、すべての VLAN の中継を抑止し続ける（Blocking 状態を維持）。

迂回路の正常性監視は以下のように動作します。

- BKP-MS ポートは「BKP Check 1」制御フレームを定期的に送信し、「BKP Check 2」制御フレームの受信を監視する。
- BKP-A ポートでは「BKP Check 1」制御フレームの受信を監視し、「BKP Check 1」制御フレームの受信が正常ならば「BKP Check 2」制御フレームを送信する。
- BKP-MS ポートでは「BKP Check 2」制御フレームの受信タイムアウトを検知すると、迂回路に異常があると判断する。迂回路が異常な場合は、BKP-MS ポートを通信可能には変更しない。

BKP Check フレームの受信タイムアウト時間を設定するには、**`mmrp-plus ring bkp-check-timeout`** コマンドを使用します。デフォルト設定は 1 秒です。

14.1.12他社製スイッチが混在する場合

MMRP-Plus を使用する際は、リング上のすべての装置を MMRP-Plus 対応装置にすることを推奨します。リング上に他社製スイッチが混在している場合は、以下のような問題があります。

- 他社製スイッチ間にリンクダウン障害が発生しても、Linkdown 通知フレームによる高速な切り替えはできません。ハローフレームタイムアウトによりリング上の障害を検知します。
- 他社製スイッチ間のリンクダウン障害が復旧する際には、ループ状態を経由します。ループ状態は、リンクダウン障害が復旧した時点から、マスターポートおよびスレーブポートが Blocking 状態へ遷移し、リングが正常状態に戻るまで継続されます。

  NOTE: リング上のすべての装置で MMRP-Plus が動作している場合は、リンクダウン障害復旧時にリングポートは Listening 状態を経由するため、ループ状態にはなりません。

- 他社製スイッチでは、MMRP-Plus の切り替わり／切り戻り時に FDB テーブルが消去されません。そのため、他社製スイッチを経由する通信の切り替わり／切り戻り時間が長くなることがあります。

14.1.13 MMRP-Plus の制限事項および注意事項

- MMRP-Plus 機能と STP/RSTP/MSTP/RPVST+ 機能は、装置併用をサポートした機種／バージョン以外では、同一装置で併用できません。
- NP7000 の 1.12.01 以降、NP5000 の 1.12.01 以降、NP3000 の 1.11.03 以降、NP2100 の 1.13.01 以降、NP2500 の 1.13.01 以降では、MMRP-Plus 機能と STP/RSTP/MSTP/RPVST+ 機能との装置併用をサポートしました。なお、同一インターフェース（物理ポートまたはポートチャネル）では引き続き併用不可です。
- MMRP-Plus 機能と ERPS 機能は、同一装置で併用できません。
- MMRP-Plus のリングポートでは、ループ検知機能（loop-detection action notify-only 設定時を除く）、CFM 機能を有効にすることは未サポートです。
- スタック構成の装置をシングルマスター構成のマスター装置として使用する場合、スタック跨ぎのポートチャネルをマスターポートまたはスレーブポートとして使用することはできません。
- スタック構成の装置を分散マスター装置として使用する場合、スタック跨ぎのポートチャネルを分散マスターポートとして使用することはできません。
- スタック構成の装置を分散スレーブ装置として使用する場合、スタック跨ぎのポートチャネルを分散スレーブポートとして使用することはできません。
- MMRP-Plus リングポートの FailureUp 状態は切り戻り途中の通信不可な状態ですが、物理ポートはリンクアップしているため、レイヤー 3 機能の VLAN インターフェースとしてはリンクアップしているポートとして扱われます。これにより、同一装置で MMRP-Plus とレイヤー 3 機能を併用している場合に、ネットワーク構成によっては余分な通信不可時間が増えることも考えられます。そのため、MMRP-Plus とレイヤー 3 機能を併用する場合、切り戻り方法（**`mmrp-plus ring revertive`** コマンド）はデフォルト設定（自動切り戻り有効、切り戻りタイマー値：0）で使用することを推奨します。
- NP5000 で 40G ポートを MMRP-Plus のリングポートに使用する場合、切り替わりには最大 1 秒程度要する場合があります。

14.2 MMRP-Plus の状態確認

MMRP-Plus の状態を表示して確認する方法を説明します。

14.2.1 MMRP-Plus の設定の表示

show mmrp-plus configuration コマンドで、MMRP-Plus の設定を確認できます。

表示例を以下に示します。

```
# show mmrp-plus configuration

MMRP-Plus Switch Configuration
        Status          : Enable ...(1)
        Hello interval  : 100ms ...(2)
        Polling rate    : 1000ms ...(3)

MMRP-Plus Ring Configuration:
 RM: Ring Master, RA: Ring Aware, DM: Divided Master, DS: Divided Slave
 Vid : Hello VID
 Fdb : FDB Flush Timer
 Pr  : Port Restart (O: enable -: disable)
 Vg  : VLAN Group
 Re  : Revertive setting
 Ht  : Hello Timeout Timer
 Lis : Listening Timer
 P   : Port-Channel                                          (11)
(4)  (5)       (6)  (7)         (7)           (8)    (9) (10)  (12)     (13)   (14)
ID   Name      Type Pt1         Pt2         | Vid    Fdb  Pr Vg Re       Ht     Lis
-----------------------------------------+-------------------------------------
1    R01-A     RA   1/0/1       1/0/2       | 4011   1    -  -  0        1      10
2    R01-1-M   RM   1/0/5(M)    1/0/6(S)    | 4012   1    -  1  60       1      10
3    TEST03    DM   P5                      | 4013   1    O  -  disable  1      10
4    Ring004   DS               1/0/24      | 4014   1    -  2  0        1      10
```

各項目の説明は、以下のとおりです。

表 14-5 show mmrp-plus configuration コマンドの表示項目

項番	説明
(1)	MMRP-Plus の有効 (Enable) ／無効 (Disable) を表示します。
(2)	MMRP-Plus のハローフレームの送信間隔を表示します。
(3)	MMRP-Plus のハローフレームのポーリングレートを表示します。
(4)	MMRP-Plus のリング ID を表示します。
(5)	MMRP-Plus のリング名を表示します。リング名が 8 文字以上の場合は、先頭の 7 文字までが表示されます。
(6)	MMRP-Plus のリングの動作モードを表示します。 • RM：シングルマスター • RA：アウェア • DM：分散マスター • DS：分散スレーブ

項番	説明
(7)	ポート番号またはポートチャネル番号を表示します。番号の前に「P」が表示されている場合はポートチャネル番号です。 シングルマスター構成では、マスターポートに (M)、スレーブポートに (S) が付与されて表示されます。
(8)	MMRP-Plus 制御フレームの VLAN ID を表示します。
(9)	FDB フラッシュタイマーを表示します。
(10)	ポートリスタート機能の有効 (O) ／無効 (-) を表示します。
(11)	関連付けられた VLAN グループ番号を表示します。
(12)	切り戻りタイマーを表示します。disable パラメーター指定時は disable と表示されます。
(13)	ハローフレームの受信タイムアウト時間を表示します。
(14)	リスニングタイマーを表示します。

14.2.2 MMRP-Plus のリングごとの設定の表示

show mmrp-plus configuration ring コマンドで、リングごとの設定を確認できます。

リング ID 1 のマスター装置の設定を確認する場合の表示例を以下に示します。

```
# show mmrp-plus configuration ring 1

================================================================================
Ring ID             : 1 ...(1)
Ring name           : TEST-RING1 ...(2)
Type                : Ring Master ...(3)
Master Port         : 1/0/1 ...(4)
Slave Port          : 1/0/2 ...(4)
VLAN ID             : 4001 ...(5)
VLAN Group          : 2 ...(6)
  Master VID        : 1-19,21-29,31-39,41-4094 ...(7)
  Slave VID         : 20,30,40 ...(8)
Listening Time      : 10 s ...(9)
FDB Flush
  Timer             : 1 s ...(10)
  Port              : - ...(11)
Hello-timeout       : 1 s ...(12)
Revertive           : 0 s ...(13)
Port-Restart        : Disable ...(14)
  Forcedown Time    : 500 ms ...(15)
  Link Up Wait      : 10000 ms ...(16)
```

各項目の説明は、以下のとおりです。

表 14-6 show mmrp-plus configuration ring コマンドの表示項目（マスター装置）

項番	説明
(1)	MMRP-Plus のリング ID を表示します。
(2)	MMRP-Plus のリング名を表示します。

項番	説明
(3)	MMRP-Plus のリングの動作モードを表示します。 • Ring Master：シングルマスター • Ring Aware：アウェア • Divided Master：分散マスター • Divided Slave：分散スレーブ
(4)	リングポートを表示します。リングポート種別により項目名称が以下のように変更されます。ポートチャネルの場合はポートチャネル番号とメンバーポートのポート番号が表示されます。 • マスターポート（物理ポート）：Master Port • スレーブポート（物理ポート）：Slave Port • アウェアポート（物理ポート）：Aware Port • マスターポート（ポートチャネル）：Master Port-Channel • スレーブポート（ポートチャネル）：Slave Port-Channel • アウェアポート（ポートチャネル）：Aware Port-Channel
(5)	MMRP-Plus 制御フレームの VLAN ID を表示します。
(6)	関連付けられた VLAN グループ番号を表示します。未指定時は Default と表示されます。
(7)	マスター VLAN を表示します。
(8)	スレーブ VLAN を表示します。
(9)	リスニングタイマーを表示します。
(10)	FDB フラッシュタイマーを表示します。
(11)	リングが切り替わる際に FDB エントリーを消去するポート番号を表示します。
(12)	ハローフレームの受信タイムアウト時間を表示します。
(13)	切り戻りタイマーを表示します。disable パラメーター指定時は Disable と表示されます。
(14)	ポートリスタート機能の有効 (Enable) ／無効 (Disable) を表示します。
(15)	ポートリスタート機能のリンク瞬断時間を表示します。
(16)	ポートリスタート機能のリンク保護時間を表示します。

リング ID 2 のアウェア装置の設定を確認する場合の表示例を以下に示します。

```
# show mmrp-plus configuration ring 2

================================================================================
Ring ID             : 2 ...(1)
Ring name           : TEST-RING2 ...(2)
Type                : Ring Aware ...(3)
Aware Port          : 1/0/3 ...(4)
Aware Port          : 1/0/4 ...(4)
VLAN ID             : 4002 ...(5)
Listening Time      : 10 s ...(6)
FDB Flush
  Timer             : 1 s ...(7)
  Port              : - ...(8)
Hello-timeout       : 1 s ...(9)
Revertive           : 0 s ...(10)
```

各項目の説明は、以下のとおりです。

表 14-7 `show mmrp-plus configuration ring` コマンドの表示項目（アウェア装置）

項番	説明
(1)	MMRP-Plus のリング ID を表示します。
(2)	MMRP-Plus のリング名を表示します。
(3)	MMRP-Plus のリングの動作モードを表示します。 • Ring Master：シングルマスター • Ring Aware：アウェア • Divided Master：分散マスター • Divided Slave：分散スレーブ
(4)	リングポートを表示します。リングポート種別により項目名称が以下のように変更されます。ポートチャネルの場合はポートチャネル番号とメンバーポートのポート番号が表示されます。 • マスターポート (物理ポート) : Master Port • スレーブポート (物理ポート) : Slave Port • アウェアポート (物理ポート) : Aware Port • マスターポート (ポートチャネル) : Master Port-Channel • スレーブポート (ポートチャネル) : Slave Port-Channel • アウェアポート (ポートチャネル) : Aware Port-Channel
(5)	MMRP-Plus 制御フレームの VLAN ID を表示します。
(6)	リスニングタイマーを表示します。
(7)	FDB フラッシュタイマーを表示します。
(8)	リングが切り替わる際に FDB エントリーを消去するポート番号を表示します。
(9)	ハローフレームの受信タイムアウト時間を表示します。
(10)	切り戻りタイマーを表示します。disable パラメーター指定時は Disable と表示されます。

リング ID 3 の分散マスター装置の設定を確認する場合の表示例を以下に示します。

```
# show mmrp-plus configuration ring 3

================================================================================
Ring ID             : 3 ...(1)
Ring name           : TEST-RING3 ...(2)
Type                : Divided Master ...(3)
Master Port         : 1/0/5 ...(4)
VLAN ID             : 4003 ...(5)
VLAN Group          : 2 ...(6)
  Master VID        : 1-19,21-29,31-39,41-4094 ...(7)
  Slave VID         : 20,30,40 ...(8)
Listening Time      : 10 s ...(9)
FDB Flush
  Timer             : 1 s ...(10)
  Port              : - ...(11)
Hello-timeout       : 1 s ...(12)
Revertive           : 0 s ...(13)
Port-Restart        : Disable ...(14)
  Forcedown Time    : 500 ms ...(15)
  Link Up Wait      : 10000 ms ...(16)
FDBFlush Transmit
  Port              : - ...(17)
  Retransmit        : Disable ...(18)
Uplink
  Port              : 1/0/9-1/0/10 ...(19)
```

各項目の説明は、以下のとおりです。

表 14-8 `show mmrp-plus configuration ring` コマンドの表示項目（分散マスター装置）

項番	説明
(1)	MMRP-Plus のリング ID を表示します。
(2)	MMRP-Plus のリング名を表示します。
(3)	MMRP-Plus のリングの動作モードを表示します。 • Ring Master：シングルマスター • Ring Aware：アウェア • Divided Master：分散マスター • Divided Slave：分散スレーブ
(4)	リングポートを表示します。リングポート種別により項目名称が以下のように変更されます。ポートチャネルの場合はポートチャネル番号とメンバーポートのポート番号が表示されます。 • マスターポート (物理ポート) : Master Port • スレーブポート (物理ポート) : Slave Port • アウェアポート (物理ポート) : Aware Port • マスターポート (ポートチャネル) : Master Port-Channel • スレーブポート (ポートチャネル) : Slave Port-Channel • アウェアポート (ポートチャネル) : Aware Port-Channel
(5)	MMRP-Plus 制御フレームの VLAN ID を表示します。
(6)	関連付けられた VLAN グループ番号を表示します。未指定時は Default と表示されます。
(7)	マスター VLAN を表示します。
(8)	スレーブ VLAN を表示します。

項番	説明
(9)	リスニングタイマーを表示します。
(10)	FDB フラッシュタイマーを表示します。
(11)	リングが切り替わる際に FDB エントリーを消去するポート番号を表示します。
(12)	ハローフレームの受信タイムアウト時間を表示します。
(13)	切り戻りタイマーを表示します。disable パラメーター指定時は Disable と表示されます。
(14)	ポートリスタート機能の有効 (Enable) ／無効 (Disable) を表示します。
(15)	ポートリスタート機能のリンク瞬断時間を表示します。
(16)	ポートリスタート機能のリンク保護時間を表示します。
(17)	FDB フラッシュフレーム送信機能で指定した送信ポートを表示します。
(18)	FDB フラッシュフレーム中継機能の有効 (Enable) ／無効 (Disable) を表示します。
(19)	アップリンクポート連携機能で指定したアップリンクポートを表示します。

14.2.3 MMRP-Plus の VLAN グループの表示

show mmrp-plus vlangroup コマンドで、VLAN グループのマスター VLAN、およびスレーブ VLAN を確認できます。

表示例を以下に示します。

```
# show mmrp-plus vlangroup 8

VLAN Group Configuration: Group 8 ...(1)
  Master VID    : 1-4094 ...(2)
  Slave VID     : - ...(3)
```

各項目の説明は、以下のとおりです。

表 14-9 show mmrp-plus vlangroup コマンドの表示項目

項番	説明
(1)	VLAN グループ番号を表示します。
(2)	マスター VLAN を表示します。
(3)	スレーブ VLAN を表示します。

14.2.4 MMRP-Plus の動作状態の表示

show mmrp-plus status コマンドで、MMRP-Plus の動作状態を確認できます。

表示例を以下に示します。

```
# show mmrp-plus status

VLAN group   : Default ...(1)
  Master VLAN : 1-4094 ...(2)
  Slave VLAN  : - ...(3)
-------------------------------------------------------------------------------
 (4)         (5)    (6)            (7)              (8)              (9)
 Pt.         Ring   MMRP           Master VLAN      Slave VLAN       Ring name
 /Pt-C.      ID     Port Mode      Port Status      Port Status
-------------------------------------------------------------------------------
 1/0/1       1      Ring Aware     Forwarding       Forwarding       0123456789
 1/0/2       1      Ring Aware     Forwarding       Forwarding       0123456789
 1/0/5       3      Ring Master    Down             Down             r3
 1/0/6       3      Ring Slave     Down             Down             r3
 1/0/4       4      Div Master     Down             Down

VLAN group   : 2
  Master VLAN : 2-8,11-4094
  Slave VLAN  : 1,9-10
-------------------------------------------------------------------------------
 Pt.         Ring   MMRP           Master VLAN      Slave VLAN       Ring name
 /Pt-C.      ID     Port Mode      Port Status      Port Status
-------------------------------------------------------------------------------
 1/0/3       2      Div Slave      Down             Down
 P1          5      Div Slave      Down             Down
```

各項目の説明は、以下のとおりです。

表 14-10 show mmrp-plus status コマンドの表示項目

項番	説明
(1)	VLAN グループ番号を表示します。未指定時は Default と表示されます。
(2)	マスター VLAN を表示します。
(3)	スレーブ VLAN を表示します。
(4)	ポート番号またはポートチャネル番号を表示します。番号の前に「P」が表示されている場合はポートチャネル番号です。
(5)	MMRP-Plus のリング ID を表示します。
(6)	リングポートの動作モードを表示します。 • Ring Master：マスターポート • Ring Slave：スレーブポート • Ring Aware：アウェアポート • Div Master：分散マスターポート • Div Slave：分散スレーブポート

項番	説明
(7)	対象リングポートのマスター VLAN に対する状態を表示します。 • Blocking：ユーザーフレームの中継を抑止している状態 • Forwarding：ユーザーフレームを中継している状態 • Down：障害発生中ですべての通信不可 • FailureUp：リング復旧待機状態（すべての通信不可） • Listening：リング復旧中（MMRP-Plus 制御フレームのみ通信可能）
(8)	対象リングポートのスレーブ VLAN に対する状態を表示します。各状態の説明は (7) と同じです。
(9)	MMRP-Plus のリング名を表示します。リング名が 11 文字以上の場合は、先頭の 10 文字までが表示されます。

14.2.5 MMRP-Plus のポートごとの動作状態の表示

show mmrp-plus status port コマンドで、MMRP-Plus のポートごとの動作状態を確認できます。

リングポート 1/0/1 を指定した場合の表示例を以下に示します。

```
# show mmrp-plus status port 1/0/1

================================================================================
Port 1/0/1 ...(1)
  Ring ID           : 1 ...(2)
  Ring Name         : Ring1 ...(3)
  Port Mode         : Ring Master ...(4)
  VLAN Group        : Default ...(5)
    Master VLAN     : 1-4094 ...(6)
    Slave VLAN      : - ...(7)
  Link Status       : 1G/F ...(8)
  MMRP-Plus Status  : Blocking ...(9)
    Master VLAN     : Forwarding ...(10)
    Slave VLAN      : Blocking ...(11)
  Connection        : Normal ...(12)
--------------------------------------------------------------------
   (13)             (14)                    (15)
  Frame Type       Receive Frame Count     Transmit Frame Count
--------------------------------------------------------------------
  HelloB1                          135                        -
  HelloB2                            0                      136
  HelloF1                            0                        -
  HelloF2                            0                        0
  FDB Flush                          0                        0
  Link Down                          0                        0
  Link Up                            0                        0
  Blocking                           2                        2
  Forwarding                         0                        0
```

各項目の説明は、以下のとおりです。

表 14-11 show mmrp-plus status port コマンドの表示項目

項番	説明
(1)	ポート番号またはポートチャネル番号を表示します。ポートチャネルの場合は、ポートチャネル番号とメンバーポートのポート番号が表示されます。
(2)	MMRP-Plus のリング ID を表示します。

項番	説明
(3)	MMRP-Plus のリング名を表示します。
(4)	リングポートの動作モードを表示します。 • Ring Master：マスターポート • Ring Slave：スレーブポート • Ring Aware Default：デフォルト状態のアウェアポート • Ring Aware Master：スレーブポート方向に接続されたアウェアポート • Ring Aware Slave：マスターポート方向に接続されたアウェアポート • Divided Master：分散マスターポート • Divided Slave：分散スレーブポート
(5)	VLAN グループ番号を表示します。未指定時は Default と表示されます。
(6)	マスター VLAN を表示します。
(7)	スレーブ VLAN を表示します。
(8)	ポートのリンク状態を表示します。
(9)	リングポートの MMRP-Plus 状態を表示します。 【マスターポート、スレーブポート、分散マスターポート、分散スレーブポートの場合】 • Blocking：リング正常時 • Forwarding：リング障害時 【アウェアポートの場合】 • Forwarding：リング正常時、リング障害時 【共通】 • Down：対象リングポートがダウン状態 • FailureUp：対象リングポートがダウン状態から復旧して、リング復旧待機状態 • Listening：リング復旧中（MMRP-Plus 制御フレームのみ通信可能）
(10)	対象リングポートのマスター VLAN に対する状態を表示します。 • Blocking：ユーザーフレームの中継を抑止している状態 • Forwarding：ユーザーフレームを中継している状態 • Down：障害発生中ですべての通信不可 • FailureUp：リング復旧待機状態（すべての通信不可） • Listening：リング復旧中（MMRP-Plus 制御フレームのみ通信可能）
(11)	対象リングポートのスレーブ VLAN に対する状態を表示します。各状態の説明は (10) と同じです。
(12)	リングの接続状態を表示します。 • Normal：正常状態（MMRP-Plus ハローフレーム受信中） • Broken：障害発生中（MMRP-Plus ハローフレーム未受信） • Abnormal：異常状態（正常時とは反対方向の MMRP-Plus ハローフレーム受信）

項番	説明
(13)	MMRP-Plus 制御フレームの種別を表示します。 • HelloB1：Blocking 状態のスレーブが送信する MMRP-Plus ハローフレーム • HelloB2：Blocking 状態のマスターが送信する MMRP-Plus ハローフレーム • HelloF1：Forwarding 状態のスレーブが送信する MMRP-Plus ハローフレーム • HelloF2：Forwarding 状態のマスターが送信する MMRP-Plus ハローフレーム • FDB Flush：FDB エントリーのクリア要求を示す制御フレーム • Link Down：リンクダウン検知を示す制御フレーム • Link Up：リンクアップ検知を示す制御フレーム • Blocking：Blocking 状態へ遷移時のマスター／スレーブが送信する制御フレーム
(14)	受信した MMRP-Plus 制御フレーム数を表示します。
(15)	送信した MMRP-Plus 制御フレーム数を表示します。

14.2.6 MMRP-Plus のリングごとの動作状態の表示

show mmrp-plus status ring コマンドで、MMRP-Plus のリングごとの動作状態を確認できます。

リング ID 1 を指定した場合の表示例を以下に示します。

```
# show mmrp-plus status ring 1

================================================================================
Port 1/0/1 ...(1)
  Ring ID           : 1 ...(2)
  Ring Name         : 01234567890123456789012345678912 ...(3)
  Port Mode         : Ring Aware Slave ...(4)
  VLAN Group        : Default ...(5)
    Master VLAN     : 1-4094 ...(6)
    Slave VLAN      : - ...(7)
  Link Status       : 1G/F ...(8)
  MMRP-Plus Status  : Forwarding ...(9)
    Master VLAN     : Forwarding ...(10)
    Slave VLAN      : Forwarding ...(11)
  Connection        : Normal ...(12)
--------------------------------------------------------------------
  (13)              (14)                      (15)
  Frame Type        Receive Frame Count       Transmit Frame Count
--------------------------------------------------------------------
  HelloB1                             0                          -
  HelloB2                           338                          -
  HelloF1                             0                          -
  HelloF2                            10                          -
  FDB Flush                           0                          0
  Link Down                           0                          0
  Link Up                             0                          0
  Blocking                            3                          0
  Forwarding                          0                          0
================================================================================
Port 1/0/2
  Ring ID           : 1
  Ring Name         : 01234567890123456789012345678912
  Port Mode         : Ring Aware Master
  VLAN Group        : Default
    Master VLAN     : 1-4094
    Slave VLAN      : -
  Link Status       : 1G/F
  MMRP-Plus Status  : Forwarding
    Master VLAN     : Forwarding
    Slave VLAN      : Forwarding
  Connection        : Normal
--------------------------------------------------------------------
  Frame Type        Receive Frame Count       Transmit Frame Count
--------------------------------------------------------------------
  HelloB1                           339                          -
  HelloB2                             0                          -
  HelloF1                            10                          -
  HelloF2                             0                          -
  FDB Flush                           0                          0
  Link Down                           0                          0
  Link Up                             0                          0
  Blocking                            3                          0
  Forwarding                          0                          0
```

各項目の説明は、以下のとおりです。

表 14-12 `show mmrp-plus status ring` コマンドの表示項目

項番	説明
(1)	ポート番号またはポートチャネル番号を表示します。ポートチャネルの場合は、ポートチャネル番号とメンバーポートのポート番号が表示されます。
(2)	MMRP-Plus のリング ID を表示します。
(3)	MMRP-Plus のリング名を表示します。
(4)	リングポートの動作モードを表示します。 • Ring Master：マスターポート • Ring Slave：スレーブポート • Ring Aware Default：デフォルト状態のアウェアポート • Ring Aware Master：スレーブポート方向に接続されたアウェアポート • Ring Aware Slave：マスターポート方向に接続されたアウェアポート • Divided Master：分散マスターポート • Divided Slave：分散スレーブポート
(5)	VLAN グループ番号を表示します。未指定時は Default と表示されます。
(6)	マスター VLAN を表示します。
(7)	スレーブ VLAN を表示します。
(8)	ポートのリンク状態を表示します。
(9)	リングポートの MMRP-Plus 状態を表示します。 【マスターポート、スレーブポート、分散マスターポート、分散スレーブポートの場合】 • Blocking：リング正常時 • Forwarding：リング障害時 【アウェアポートの場合】 • Forwarding：リング正常時、リング障害時 【共通】 • Down：対象リングポートがダウン状態 • FailureUp：対象リングポートがダウン状態から復旧して、リング復旧待機状態 • Listening：リング復旧中（MMRP-Plus 制御フレームのみ通信可能）
(10)	対象リングポートのマスター VLAN に対する状態を表示します。 • Blocking：ユーザーフレームの中継を抑止している状態 • Forwarding：ユーザーフレームを中継している状態 • Down：障害発生中ですべての通信不可 • FailureUp：リング復旧待機状態（すべての通信不可） • Listening：リング復旧中（MMRP-Plus 制御フレームのみ通信可能）
(11)	対象リングポートのスレーブ VLAN に対する状態を表示します。各状態の説明は (10) と同じです。
(12)	リングの接続状態を表示します。 • Normal：正常状態（MMRP-Plus ハローフレーム受信中） • Broken：障害発生中（MMRP-Plus ハローフレーム未受信） • Abnormal：異常状態（正常時とは反対方向の MMRP-Plus ハローフレーム受信）

項番	説明
(13)	MMRP-Plus 制御フレームの種別を表示します。 • HelloB1：Blocking 状態のスレーブが送信する MMRP-Plus ハローフレーム • HelloB2：Blocking 状態のマスターが送信する MMRP-Plus ハローフレーム • HelloF1：Forwarding 状態のスレーブが送信する MMRP-Plus ハローフレーム • HelloF2：Forwarding 状態のマスターが送信する MMRP-Plus ハローフレーム • FDB Flush：FDB エントリーのクリア要求を示す制御フレーム • Link Down：リンクダウン検知を示す制御フレーム • Link Up：リンクアップ検知を示す制御フレーム • Blocking：Blocking 状態へ遷移時のマスター／スレーブが送信する制御フレーム
(14)	受信した MMRP-Plus 制御フレーム数を表示します。
(15)	送信した MMRP-Plus 制御フレーム数を表示します。

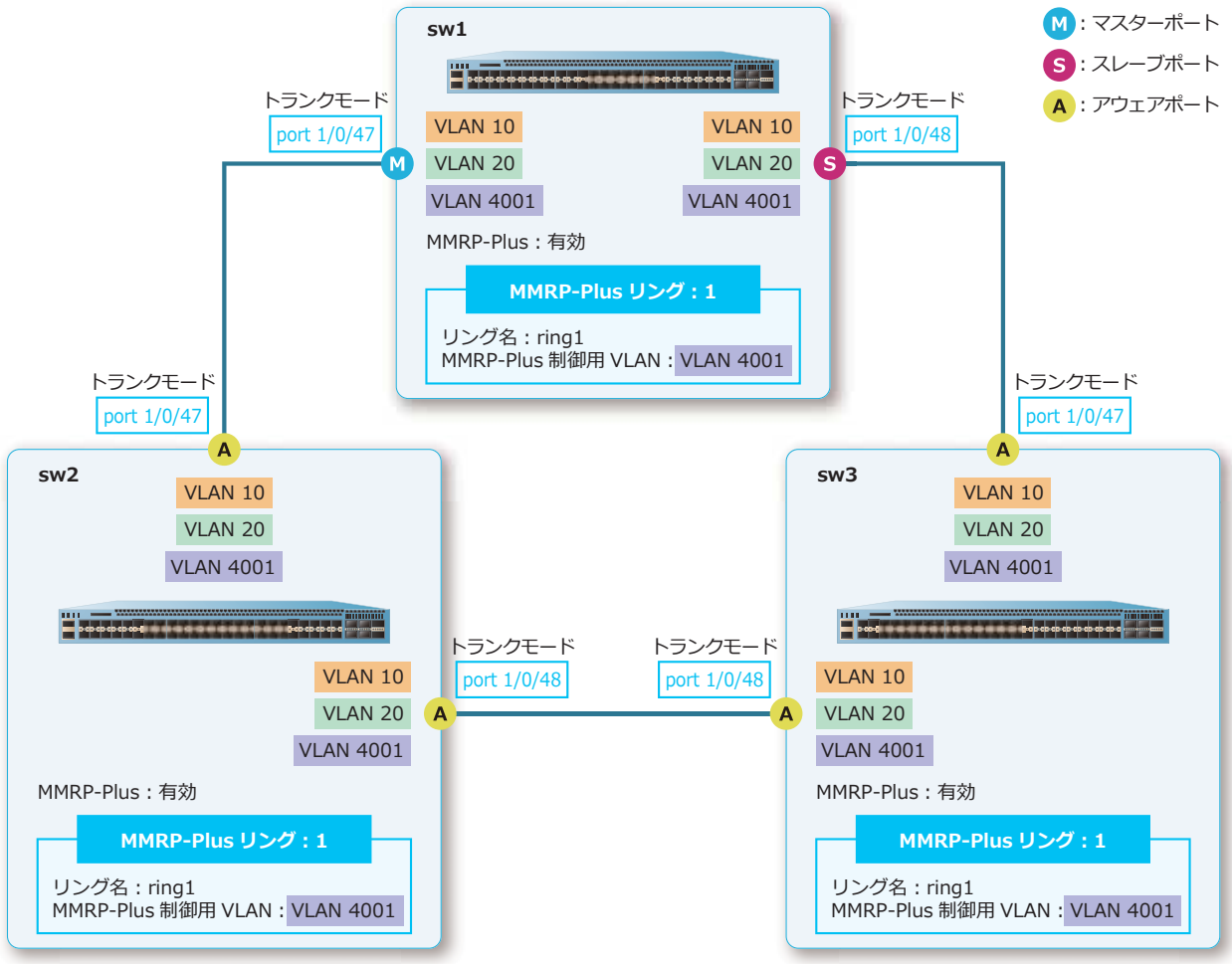
14.3 MMRP-Plus の構成例と設定例

MMRP-Plus を利用する場合の構成例と設定例を示します。

14.3.1 シングルマスター構成で VLAN 分散を使用しない場合

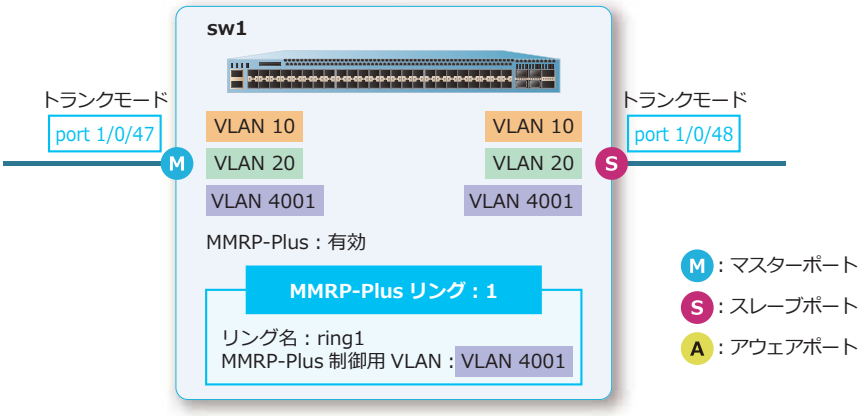
シングルマスター構成で VLAN 分散を使用しない場合の構成例と設定例を示します。なお、本設定例では sw3 の設定は省略します。

図 14-31 シングルマスター構成で VLAN 分散を使用しない場合の構成例



14.3.1.1 マスター装置の設定例（sw1）

図 14-32 マスター装置の設定例（sw1）



1. VLAN 10、VLAN 20、VLAN 4001 を作成し、設定例のように VLAN を割り当てます。

```
sw1# configure terminal
sw1(config)# vlan 10,20,4001
sw1(config-vlan)# exit
sw1(config)#
sw1(config)# interface range port 1/0/47-48
sw1(config-if-port-range)# switchport mode trunk
sw1(config-if-port-range)# switchport trunk allowed vlan 10,20,4001
sw1(config-if-port-range)# exit
sw1(config)#
```

2. リングポート（1/0/47, 1/0/48）で、スケジューリングアルゴリズムを Strict Priority Queuing に設定します。

```
sw1(config)# interface range port 1/0/47-48
sw1(config-if-port-range)# mls qos scheduler sp
sw1(config-if-port-range)# exit
sw1(config)#
```

3. リング ID［1］の MMRP-Plus リング名を［ring1］に設定します。

```
sw1(config)# mmrp-plus ring 1 name ring1
sw1(config)#
```

4. リング ID［1］の MMRP-Plus 制御用 VLAN を［VLAN 4001］に設定します。

```
sw1(config)# mmrp-plus ring 1 vid 4001
sw1(config)#
```

5. マスターポートを［ポート 1/0/47］、スレーブポートを［ポート 1/0/48］指定で、sw1 をリング ID［1］のマスター装置に設定します。

```
sw1(config)# mmrp-plus ring 1 ring-master master port 1/0/47 slave port 1/0/48
sw1(config)#
```

6. MMRP-Plus を有効化します。

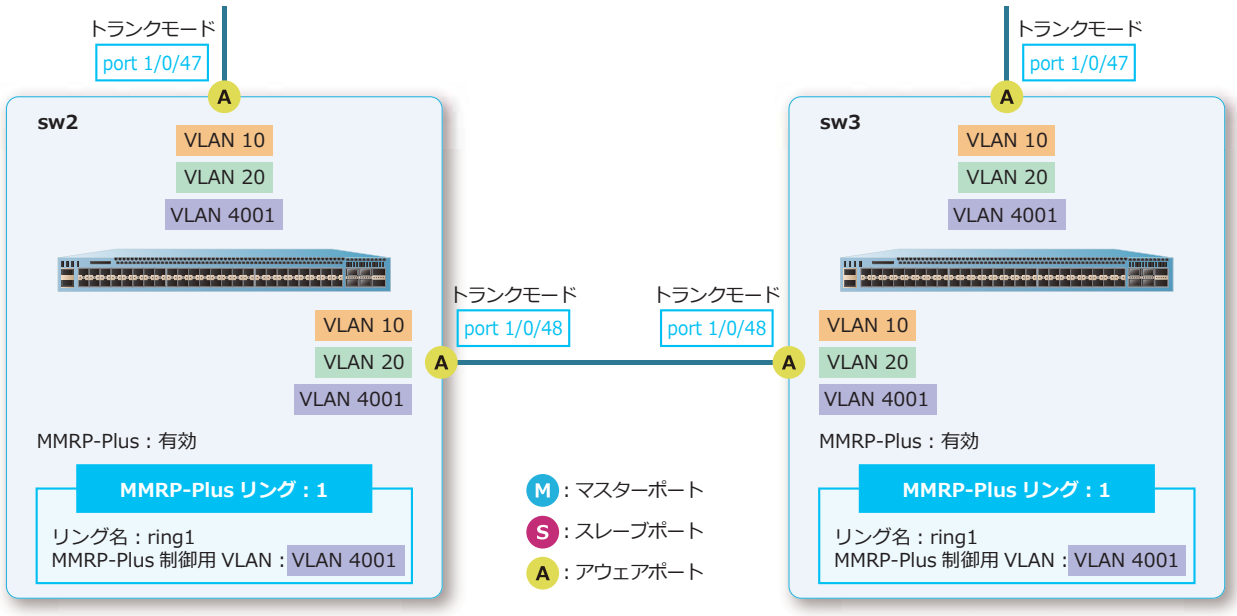
```
sw1(config)# mmrp-plus enable
sw1(config)# end
sw1#
```

7. 実施後の MMRP-Plus 関連の設定を以下に抜粋します。

```
# MMRP

mmrp-plus ring 1 name ring1
mmrp-plus ring 1 vid 4001
mmrp-plus ring 1 ring-master master port 1/0/47 slave port 1/0/48
mmrp-plus enable
```

14.3.1.2 アウェア装置の設定例（sw2、sw3）

図 14-33 アウェア装置の設定例（sw2、sw3）



1. VLAN 10、VLAN 20、VLAN 4001 を作成し、設定例のように VLAN を割り当てます。

```
sw2# configure terminal
sw2(config)# vlan 10,20,4001
sw2(config-vlan)# exit
sw2(config)#
sw2(config)# interface range port 1/0/47-48
sw2(config-if-port-range)# switchport mode trunk
sw2(config-if-port-range)# switchport trunk allowed vlan 10,20,4001
sw2(config-if-port-range)# exit
sw2(config)#
```

2. リングポート（1/0/47, 1/0/48）で、スケジューリングアルゴリズムを Strict Priority Queuing に設定します。

```
sw2(config)# interface range port 1/0/47-48
sw2(config-if-port-range)# mls qos scheduler sp
sw2(config-if-port-range)# exit
sw2(config)#
```

3. リング ID［1］の MMRP-Plus リング名を［ring1］に設定します。

```
sw2(config)# mmrp-plus ring 1 name ring1
sw2(config)#
```

4. リング ID［1］の MMRP-Plus 制御用 VLAN を［VLAN 4001］に設定します。

```
sw2(config)# mmrp-plus ring 1 vid 4001
sw2(config)#
```

5. アウェアポートを［ポート 1/0/47, ポート 1/0/48］指定で、sw2 をリング ID［1］のアウェア装置に設定します。

```
sw2(config)# mmrp-plus ring 1 aware port 1/0/47 port 1/0/48
sw2(config)#
```

6. MMRP-Plus を有効化します。

```
sw2(config)# mmrp-plus enable
sw2(config)# end
sw2#
```

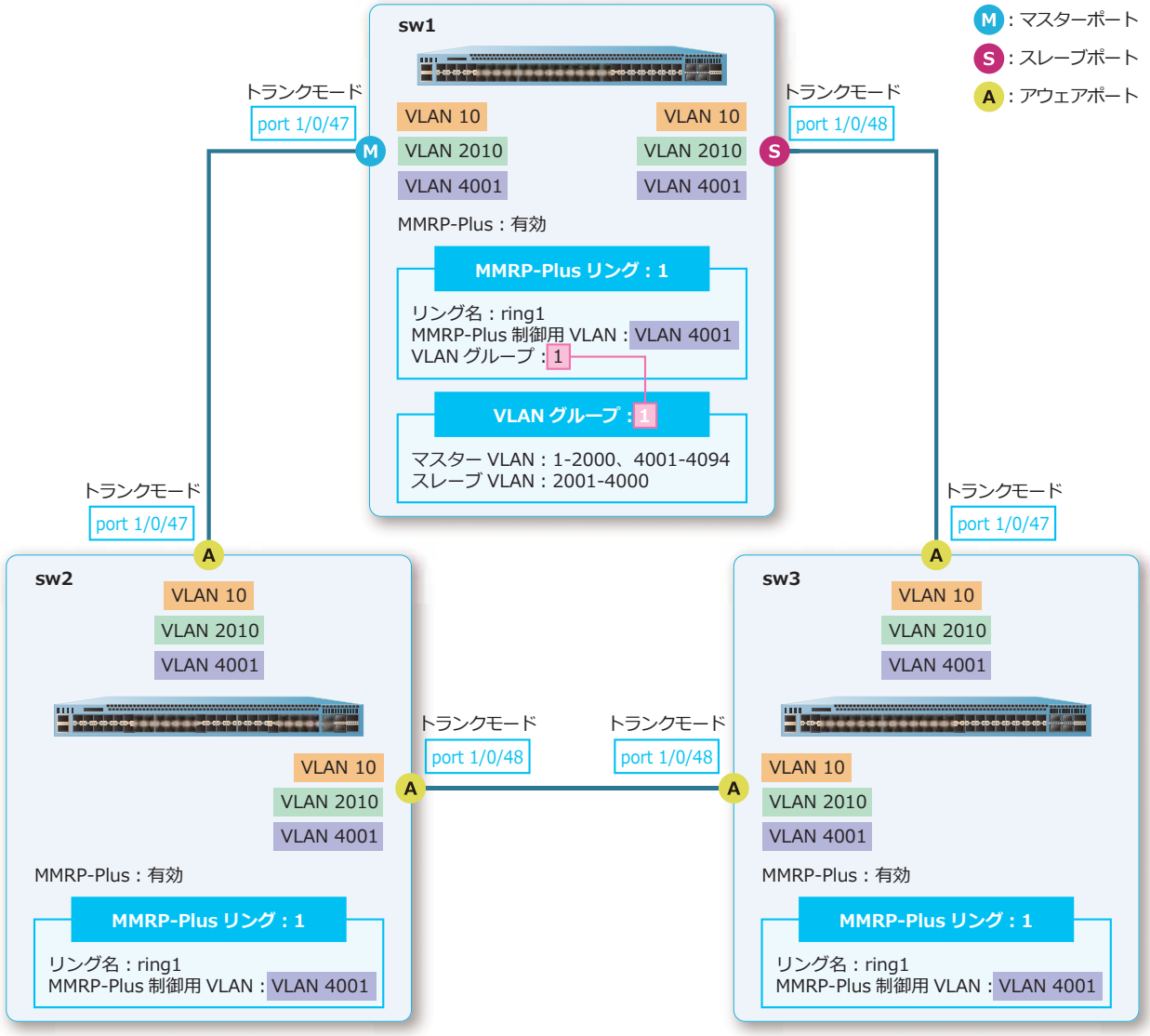
7. 実施後の MMRP-Plus 関連の設定を以下に抜粋します。

```
# MMRP

mmrp-plus ring 1 name ring1
mmrp-plus ring 1 vid 4001
mmrp-plus ring 1 aware port 1/0/47 port 1/0/48
mmrp-plus enable
```

14.3.2 シングルマスター構成で VLAN 分散を使用する場合

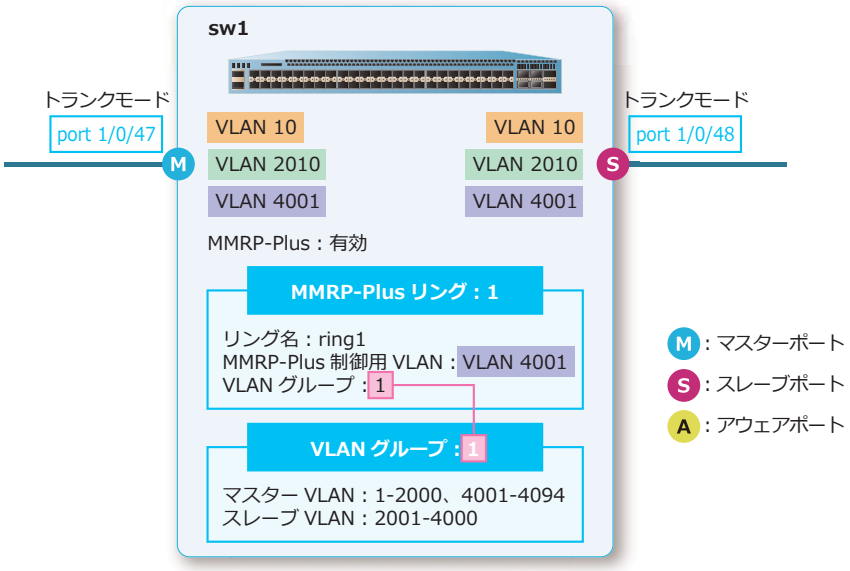
シングルマスター構成で VLAN 分散を使用する場合の構成例と設定例を示します。なお、本設定例では sw3 の設定は省略します。

図 14-34 シングルマスター構成で VLAN 分散を使用する場合の構成例



14.3.2.1 マスター装置の設定例（sw1）

図 14-35 マスター装置の設定例（sw1）



1. VLAN 10、VLAN 2010、VLAN 4001 を作成し、設定例のように VLAN を割り当てます。

```
sw1# configure terminal
sw1(config)# vlan 10,2010,4001
sw1(config-vlan)# exit
sw1(config)#
sw1(config)# interface range port 1/0/47-48
sw1(config-if-port-range)# switchport mode trunk
sw1(config-if-port-range)# switchport trunk allowed vlan 10,2010,4001
sw1(config-if-port-range)# exit
sw1(config)#
```

2. リングポート（1/0/47, 1/0/48）で、スケジューリングアルゴリズムを Strict Priority Queuing に設定します。

```
sw1(config)# interface range port 1/0/47-48
sw1(config-if-port-range)# mls qos scheduler sp
sw1(config-if-port-range)# exit
sw1(config)#
```

3. VLAN グループ［1］のスレーブ VLAN に［VLAN 2001 から VLAN 4000］を割り当てます。

```
sw1(config)# mmrp-plus vlangroup 1 slave-vid 2001-4000
sw1(config)#
```

4. リング ID［1］の MMRP-Plus リング名を［ring1］に設定します。

```
sw1(config)# mmrp-plus ring 1 name ring1
sw1(config)#
```

5. リング ID［1］の MMRP-Plus 制御用 VLAN を［VLAN 4001］に設定します。

```
sw1(config)# mmrp-plus ring 1 vid 4001
sw1(config)#
```

6. リング ID［1］に VLAN グループ［1］を割り当てます。

```
sw1(config)# mmrp-plus ring 1 vlangroup 1
sw1(config)#
```

7. マスターポートを［ポート 1/0/47］、スレーブポートを［ポート 1/0/48］指定で、sw1 をリング ID［1］のマスター装置に設定します。

```
sw1(config)# mmrp-plus ring 1 ring-master master port 1/0/47 slave port 1/0/48
sw1(config)#
```

8. MMRP-Plus を有効化します。

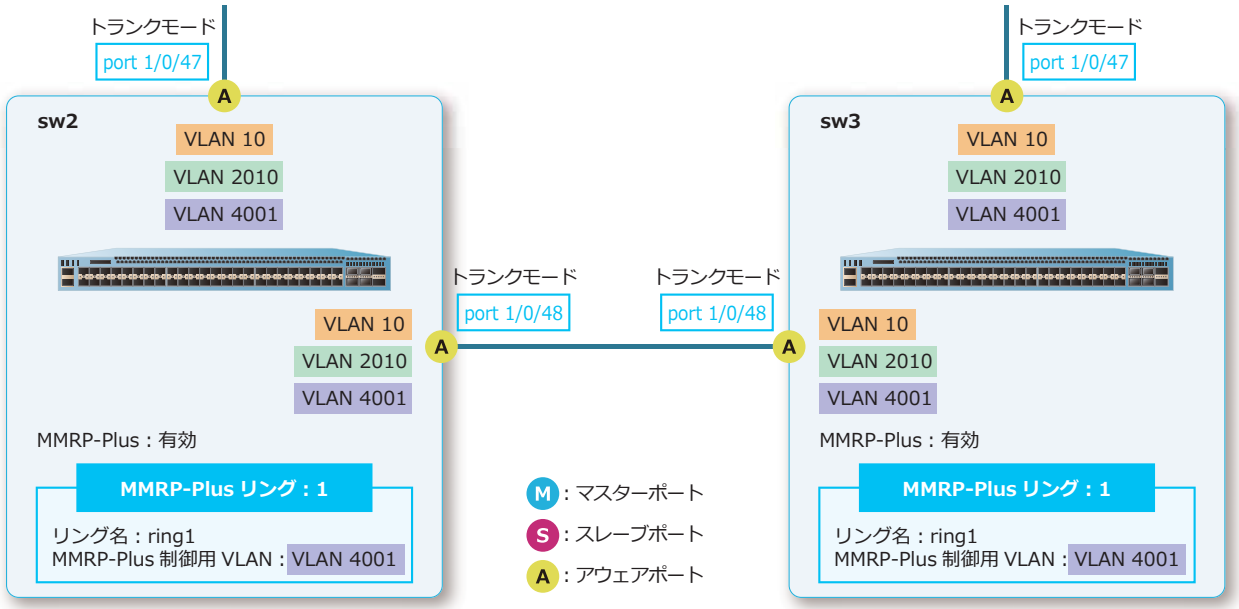
```
sw1(config)# mmrp-plus enable
sw1(config)# end
sw1#
```

9. 実施後の MMRP-Plus 関連の設定を以下に抜粋します。

```
# MMRP

mmrp-plus vlangroup 1 slave-vid 2001-4000
mmrp-plus ring 1 name ring1
mmrp-plus ring 1 vid 4001
mmrp-plus ring 1 vlangroup 1
mmrp-plus ring 1 ring-master master port 1/0/47 slave port 1/0/48
mmrp-plus enable
```

14.3.2.2 アウェア装置の設定例（sw2、sw3）

図 14-36 アウェア装置の設定例（sw2、sw3）



1. VLAN 10、VLAN 2010、VLAN 4001 を作成し、設定例のように VLAN を割り当てます。

```
sw2# configure terminal
sw2(config)# vlan 10,2010,4001
sw2(config-vlan)# exit
sw2(config)#
sw2(config)# interface range port 1/0/47-48
sw2(config-if-port-range)# switchport mode trunk
sw2(config-if-port-range)# switchport trunk allowed vlan 10,2010,4001
sw2(config-if-port-range)# exit
sw2(config)#
```

2. リングポート（1/0/47, 1/0/48）で、スケジューリングアルゴリズムを Strict Priority Queuing に設定します。

```
sw2(config)# interface range port 1/0/47-48
sw2(config-if-port-range)# mls qos scheduler sp
sw2(config-if-port-range)# exit
sw2(config)#
```

3. リング ID［1］の MMRP-Plus リング名を［ring1］に設定します。

```
sw2(config)# mmrp-plus ring 1 name ring1
sw2(config)#
```

4. リング ID［1］の MMRP-Plus 制御用 VLAN を［VLAN 4001］に設定します。

```
sw2(config)# mmrp-plus ring 1 vid 4001
sw2(config)#
```

5. アウェアポートを［ポート 1/0/47, ポート 1/0/48］指定で、sw2 をリング ID［1］のアウェア装置に設定します。

```
sw2(config)# mmrp-plus ring 1 aware port 1/0/47 port 1/0/48
sw2(config)#
```

6. MMRP-Plus を有効化します。

```
sw2(config)# mmrp-plus enable
sw2(config)# end
sw2#
```

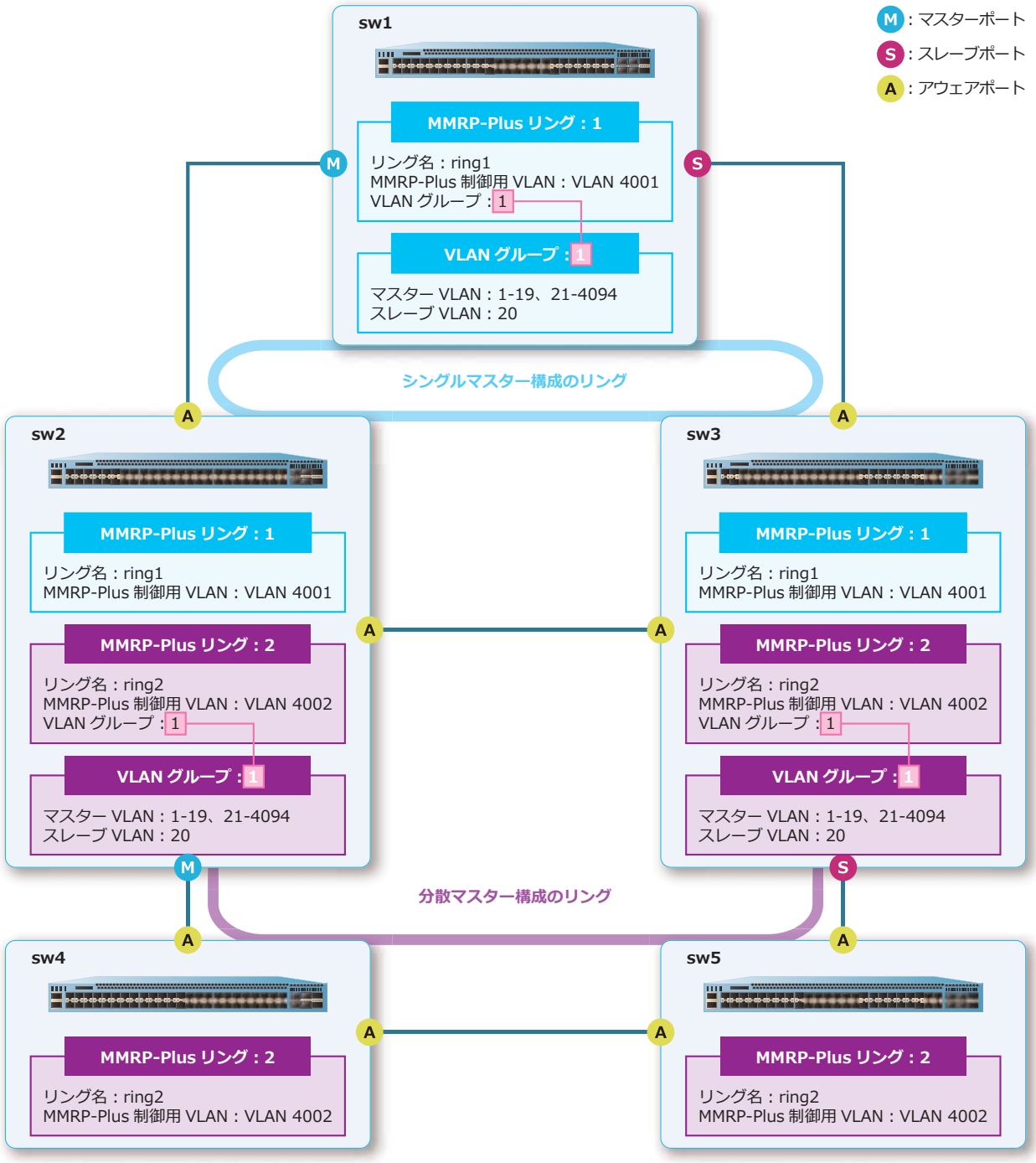
7. 実施後の MMRP-Plus 関連の設定を以下に抜粋します。

```
# MMRP

mmrp-plus ring 1 name ring1
mmrp-plus ring 1 vid 4001
mmrp-plus ring 1 aware port 1/0/47 port 1/0/48
mmrp-plus enable
```

14.3.3 分散マスター構成で VLAN 分散を使用する場合

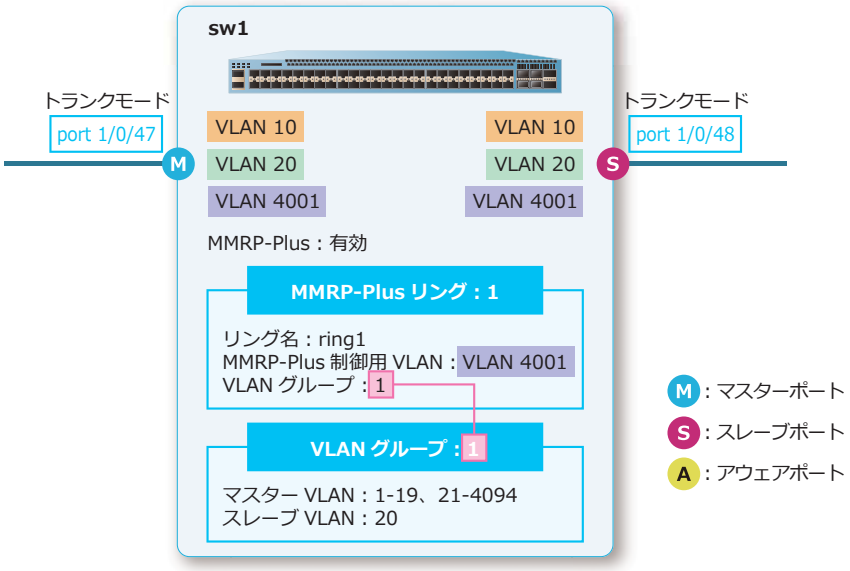
分散マスター構成で VLAN 分散を使用する場合の構成例と設定例を示します。なお、本設定例では sw5 の設定は省略します。

図 14-37 分散マスター構成で VLAN 分散を使用する場合の構成例



14.3.3.1 リング ID［1］のマスター装置の設定例（sw1）

図 14-38 リング ID［1］のマスター装置の設定例（sw1）



1. VLAN 10、VLAN 20、VLAN 4001 を作成し、設定例のように VLAN を割り当てます。

```
sw1# configure terminal
sw1(config)# vlan 10,20,4001
sw1(config-vlan)# exit
sw1(config)#
sw1(config)# interface range port 1/0/47-48
sw1(config-if-port-range)# switchport mode trunk
sw1(config-if-port-range)# switchport trunk allowed vlan 10,20,4001
sw1(config-if-port-range)# exit
sw1(config)#
```

2. リングポート（1/0/47, 1/0/48）で、スケジューリングアルゴリズムを Strict Priority Queuing に設定します。

```
sw1(config)# interface range port 1/0/47-48
sw1(config-if-port-range)# mls qos scheduler sp
sw1(config-if-port-range)# exit
sw1(config)#
```

3. VLAN グループ［1］のスレーブ VLAN に［VLAN 20］を割り当てます。

```
sw1(config)# mmrp-plus vlangroup 1 slave-vid 20
sw1(config)#
```

4. リング ID［1］の MMRP-Plus リング名を［ring1］に設定します。

```
sw1(config)# mmrp-plus ring 1 name ring1
sw1(config)#
```

5. リング ID［1］の MMRP-Plus 制御用 VLAN を［VLAN 4001］に設定します。

```
sw1(config)# mmrp-plus ring 1 vid 4001
sw1(config)#
```

6. リング ID［1］に VLAN グループ［1］を割り当てます。

```
sw1(config)# mmrp-plus ring 1 vlangroup 1
sw1(config)#
```

7. マスターポートを［ポート 1/0/47］、スレーブポートを［ポート 1/0/48］指定で、sw1 をリング ID［1］のマスター装置に設定します。

```
sw1(config)# mmrp-plus ring 1 ring-master master port 1/0/47 slave port 1/0/48
sw1(config)#
```

8. MMRP-Plus を有効化します。

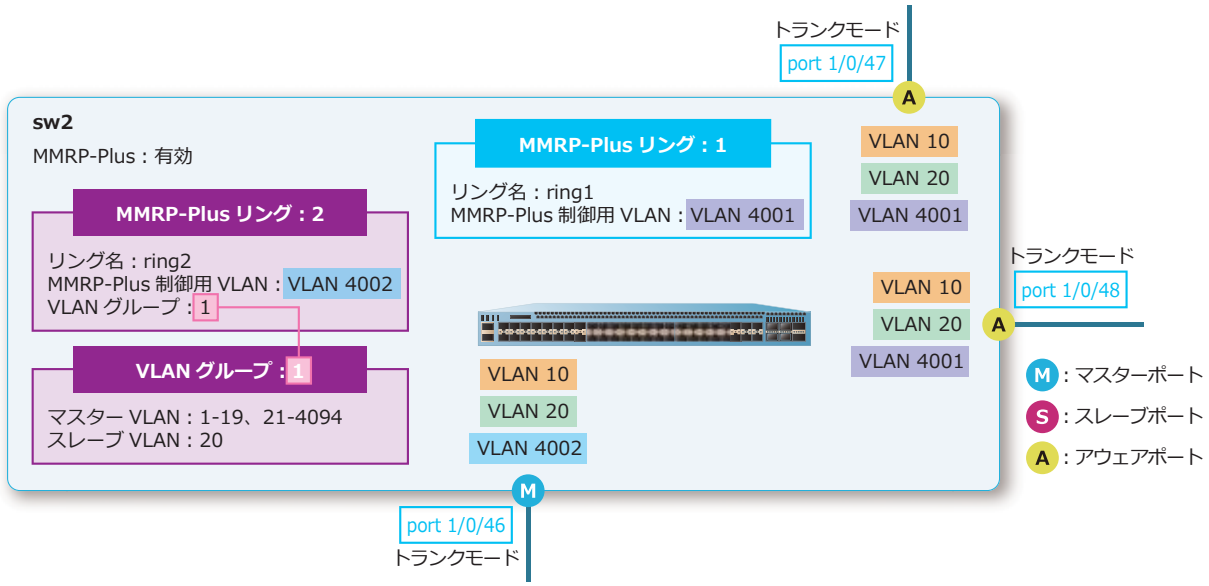
```
sw1(config)# mmrp-plus enable
sw1(config)# end
sw1#
```

9. 実施後の MMRP-Plus 関連の設定を以下に抜粋します。

```
# MMRP

mmrp-plus vlangroup 1 slave-vid 20
mmrp-plus ring 1 name ring1
mmrp-plus ring 1 vid 4001
mmrp-plus ring 1 vlangroup 1
mmrp-plus ring 1 ring-master master port 1/0/47 slave port 1/0/48
mmrp-plus enable
```

14.3.3.2 リング ID［2］の分散マスター装置の設定例（sw2）

図 14-39 リング ID［2］の分散マスター装置の設定例（sw2）



1. VLAN 10、VLAN 20、VLAN 4001、VLAN 4002 を作成し、設定例のように VLAN を割り当てます。

```
sw2# configure terminal
sw2(config)# vlan 10,20,4001,4002
sw2(config-vlan)# exit
sw2(config)#
sw2(config)# interface port 1/0/46
sw2(config-if-port)# switchport mode trunk
sw2(config-if-port)# switchport trunk allowed vlan 10,20,4002
sw2(config-if-port)# exit
sw2(config)#
sw2(config)# interface range port 1/0/47-48
sw2(config-if-port-range)# switchport mode trunk
sw2(config-if-port-range)# switchport trunk allowed vlan 10,20,4001
sw2(config-if-port-range)# exit
sw2(config)#
```

2. リングポート（1/0/46, 1/0/47, 1/0/48）で、スケジューリングアルゴリズムを Strict Priority Queuing に設定します。

```
sw2(config)# interface range port 1/0/46-48
sw2(config-if-port-range)# mls qos scheduler sp
sw2(config-if-port-range)# exit
sw2(config)#
```

3. VLAN グループ［1］のスレーブ VLAN に［VLAN 20］を割り当てます。

```
sw2(config)# mmrp-plus vlangroup 1 slave-vid 20
sw2(config)#
```

4. リング ID［1］の MMRP-Plus リング名を［ring1］に設定します。

```
sw2(config)# mmrp-plus ring 1 name ring1
sw2(config)#
```

5. リング ID［1］の MMRP-Plus 制御用 VLAN を［VLAN 4001］に設定します。

```
sw2(config)# mmrp-plus ring 1 vid 4001
sw2(config)#
```

6. アウェアポートを［ポート 1/0/47, ポート 1/0/48］指定で、sw2 をリング ID［1］のアウェア装置に設定します。

```
sw2(config)# mmrp-plus ring 1 aware port 1/0/47 port 1/0/48
sw2(config)#
```

7. リング ID［2］の MMRP-Plus リング名を［ring2］に設定します。

```
sw2(config)# mmrp-plus ring 2 name ring2
sw2(config)#
```

8. リング ID［2］の MMRP-Plus 制御用 VLAN を［VLAN 4002］に設定します。

```
sw2(config)# mmrp-plus ring 2 vid 4002
sw2(config)#
```

9. リング ID［2］に VLAN グループ［1］を割り当てます。

```
sw2(config)# mmrp-plus ring 2 vlangroup 1
sw2(config)#
```

10. 分散マスターポートを［ポート 1/0/46］指定で、sw2 をリング ID［2］の分散マスター装置に設定します。

```
sw2(config)# mmrp-plus ring 2 divided-master port 1/0/46
sw2(config)#
```

11. MMRP-Plus を有効化します。

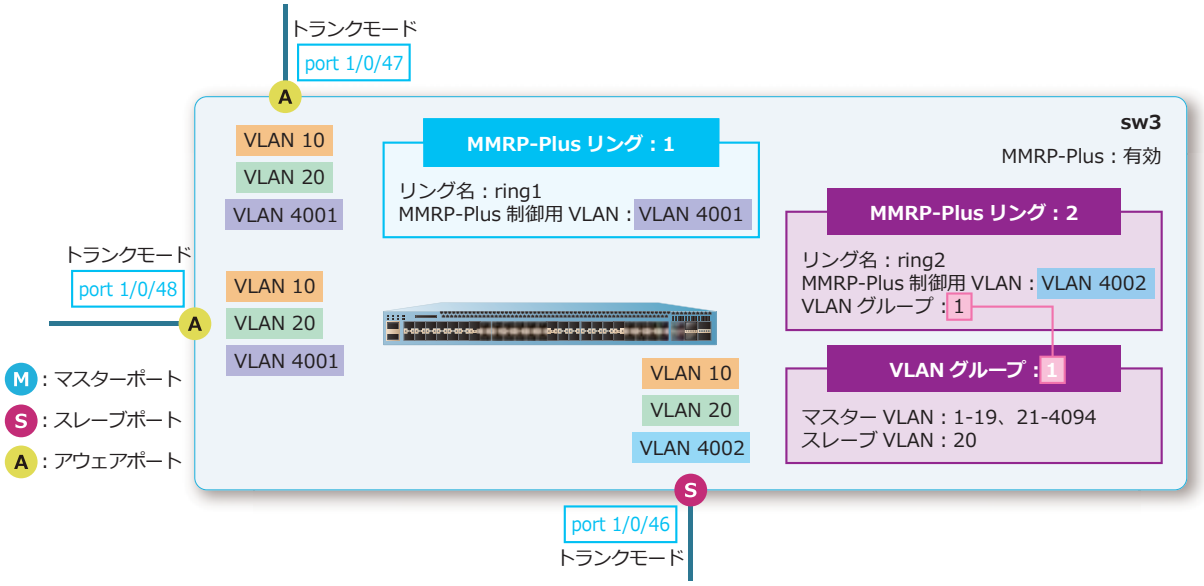
```
sw2(config)# mmrp-plus enable
sw2(config)# end
sw2#
```

12. 実施後の MMRP-Plus 関連の設定を以下に抜粋します。

```
# MMRP

mmrp-plus vlangroup 1 slave-vid 20
mmrp-plus ring 1 name ring1
mmrp-plus ring 1 vid 4001
mmrp-plus ring 1 aware port 1/0/47 port 1/0/48
mmrp-plus ring 2 name ring2
mmrp-plus ring 2 vid 4002
mmrp-plus ring 2 vlangroup 1
mmrp-plus ring 2 divided-master port 1/0/46
mmrp-plus enable
```

14.3.3.3 リング ID［2］の分散スレーブ装置の設定例（sw3）

図 14-40 リング ID［2］の分散スレーブ装置の設定例（sw3）



1. VLAN 10、VLAN 20、VLAN 4001、VLAN 4002 を作成し、設定例のように VLAN を割り当てます。

```
sw3# configure terminal
sw3(config)# vlan 10,20,4001,4002
sw3(config-vlan)# exit
sw3(config)#
sw3(config)# interface port 1/0/46
sw3(config-if-port)# switchport mode trunk
sw3(config-if-port)# switchport trunk allowed vlan 10,20,4002
sw3(config-if-port)# exit
sw3(config)#
sw3(config)# interface range port 1/0/47-48
sw3(config-if-port-range)# switchport mode trunk
sw3(config-if-port-range)# switchport trunk allowed vlan 10,20,4001
sw3(config-if-port-range)# exit
sw3(config)#
```

2. リングポート（1/0/46, 1/0/47, 1/0/48）で、スケジューリングアルゴリズムを Strict Priority Queuing に設定します。

```
sw3(config)# interface range port 1/0/46-48
sw3(config-if-port-range)# mls qos scheduler sp
sw3(config-if-port-range)# exit
sw3(config)#
```

3. VLAN グループ［1］のスレーブ VLAN に［VLAN 20］を割り当てます。

```
sw3(config)# mmrp-plus vlangroup 1 slave-vid 20
sw3(config)#
```

4. リング ID［1］の MMRP-Plus リング名を［ring1］に設定します。

```
sw3(config)# mmrp-plus ring 1 name ring1
sw3(config)#
```

5. リング ID［1］の MMRP-Plus 制御用 VLAN を［VLAN 4001］に設定します。

```
sw3(config)# mmrp-plus ring 1 vid 4001
sw3(config)#
```

6. アウェアポートを［ポート 1/0/47, ポート 1/0/48］指定で、sw3 をリング ID［1］のアウェア装置に設定します。

```
sw3(config)# mmrp-plus ring 1 aware port 1/0/47 port 1/0/48
sw3(config)#
```

7. リング ID［2］の MMRP-Plus リング名を［ring2］に設定します。

```
sw3(config)# mmrp-plus ring 2 name ring2
sw3(config)#
```

8. リング ID［2］の MMRP-Plus 制御用 VLAN を［VLAN 4002］に設定します。

```
sw3(config)# mmrp-plus ring 2 vid 4002
sw3(config)#
```

9. リング ID［2］に VLAN グループ［1］を割り当てます。

```
sw3(config)# mmrp-plus ring 2 vlangroup 1
sw3(config)#
```

10. 分散スレーブポートを［ポート 1/0/46］指定で、sw3 をリング ID［2］の分散スレーブ装置に設定します。

```
sw3(config)# mmrp-plus ring 2 divided-slave port 1/0/46
sw3(config)#
```

11. MMRP-Plus を有効化します。

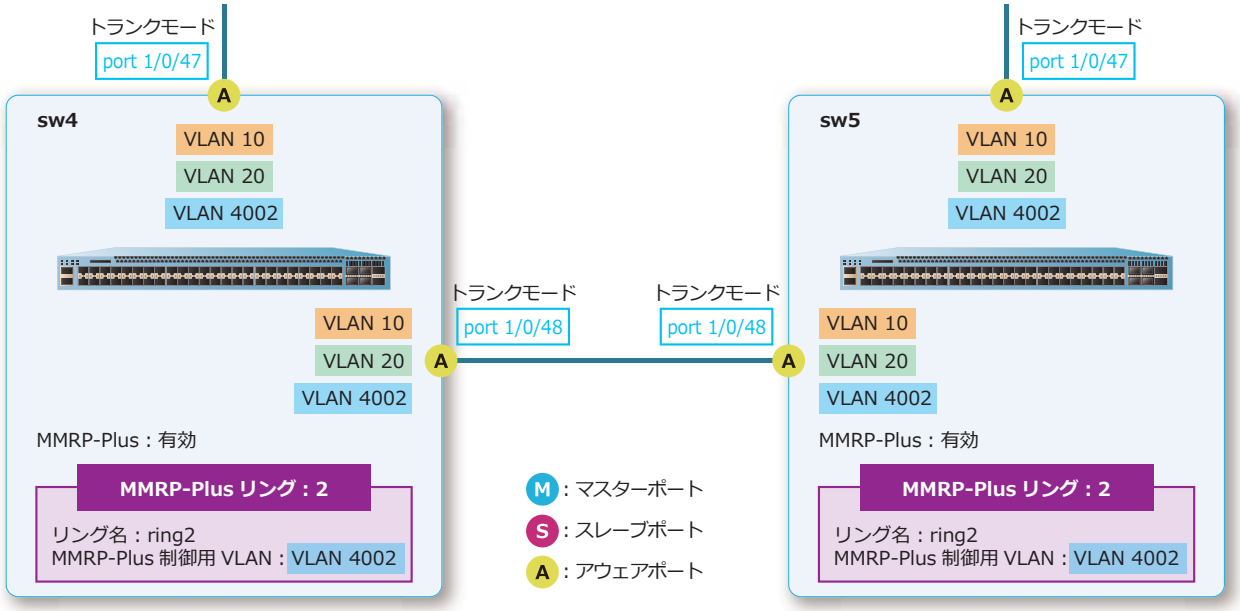
```
sw3(config)# mmrp-plus enable
sw3(config)# end
sw3#
```

12. 実施後の MMRP-Plus 関連の設定を以下に抜粋します。

```
# MMRP

mmrp-plus vlangroup 1 slave-vid 20
mmrp-plus ring 1 name ring1
mmrp-plus ring 1 vid 4001
mmrp-plus ring 1 aware port 1/0/47 port 1/0/48
mmrp-plus ring 2 name ring2
mmrp-plus ring 2 vid 4002
mmrp-plus ring 2 vlangroup 1
mmrp-plus ring 2 divided-slave port 1/0/46
mmrp-plus enable
```

14.3.3.4 リング ID［2］のアウェア装置の設定例（sw4、sw5）

図 14-41 リング ID［2］のアウェア装置の設定例（sw4、sw5）



1. VLAN 10、VLAN 20、VLAN 4002 を作成し、設定例のように VLAN を割り当てます。

```
sw4# configure terminal
sw4(config)# vlan 10,20,4002
sw4(config-vlan)# exit
sw4(config)#
sw4(config)# interface range port 1/0/47-48
sw4(config-if-port-range)# switchport mode trunk
sw4(config-if-port-range)# switchport trunk allowed vlan 10,20,4002
sw4(config-if-port-range)# exit
sw4(config)#
```

2. リングポート（1/0/47, 1/0/48）で、スケジューリングアルゴリズムを Strict Priority Queuing に設定します。

```
sw4(config)# interface range port 1/0/47-48
sw4(config-if-port-range)# mls qos scheduler sp
sw4(config-if-port-range)# exit
sw4(config)#
```

3. リング ID［2］の MMRP-Plus リング名を［ring2］に設定します。

```
sw4(config)# mmrp-plus ring 2 name ring2
sw4(config)#
```

4. リング ID［2］の MMRP-Plus 制御用 VLAN を［VLAN 4002］に設定します。

```
sw4(config)# mmrp-plus ring 2 vid 4002
sw4(config)#
```

5. アウェアポートを［ポート 1/0/47, ポート 1/0/48］指定で、sw4 をリング ID［2］のアウェア装置に設定します。

```
sw4(config)# mmrp-plus ring 2 aware port 1/0/47 port 1/0/48
sw4(config)#
```

6. MMRP-Plus を有効化します。

```
sw4(config)# mmrp-plus enable
sw4(config)# end
sw4#
```

7. 実施後の MMRP-Plus 関連の設定を以下に抜粋します。

```
# MMRP

mmrp-plus ring 2 name ring2
mmrp-plus ring 2 vid 4002
mmrp-plus ring 2 aware port 1/0/47 port 1/0/48
mmrp-plus enable
```

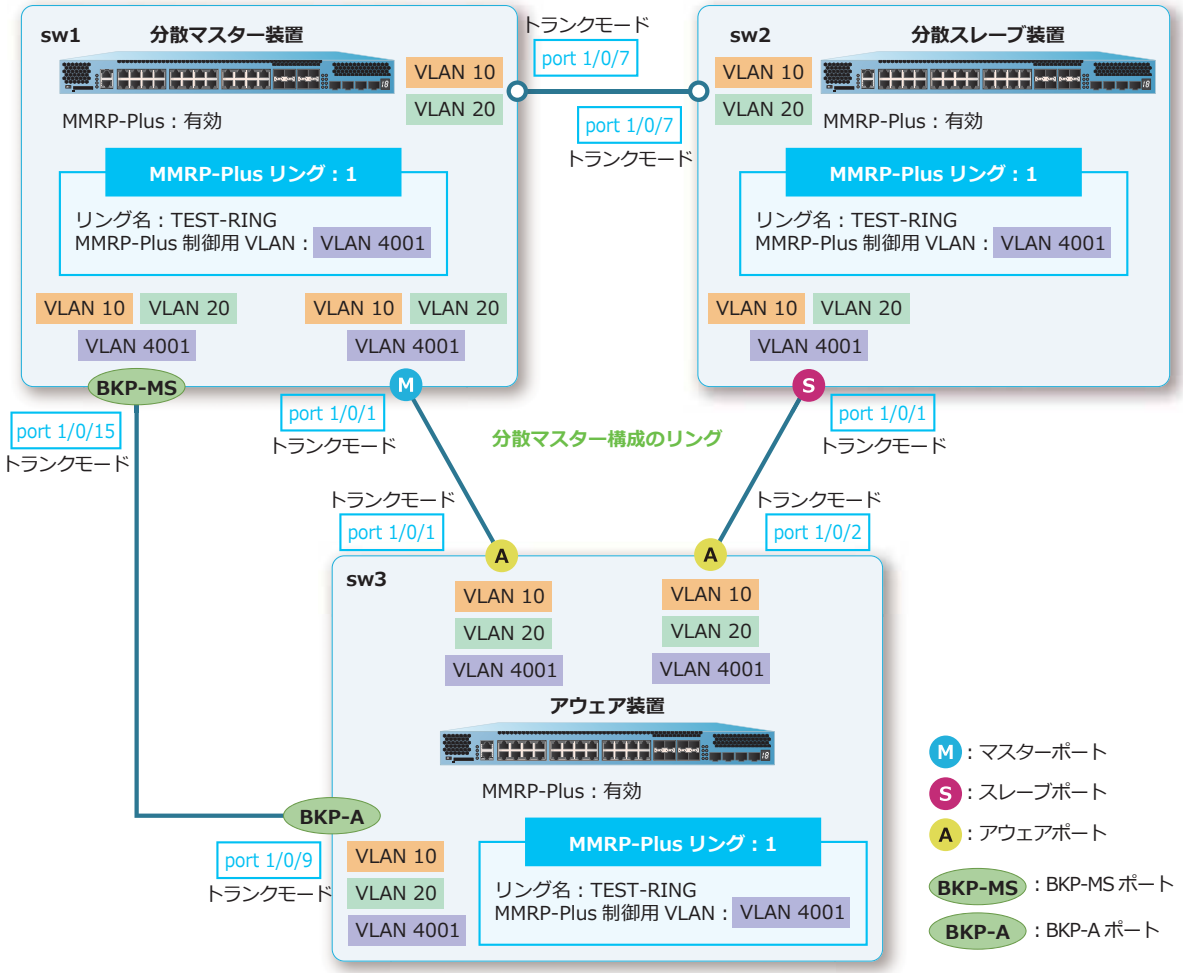
14.3.4 MMRP-Plus DFM 機能を使用する場合

分散マスター構成で MMRP-Plus DFM 機能を使用する場合の構成例と設定例を示します。

NOTE: MMRP-Plus DFM 機能は、NP3000 の 1.11.01 以降でサポートしています。

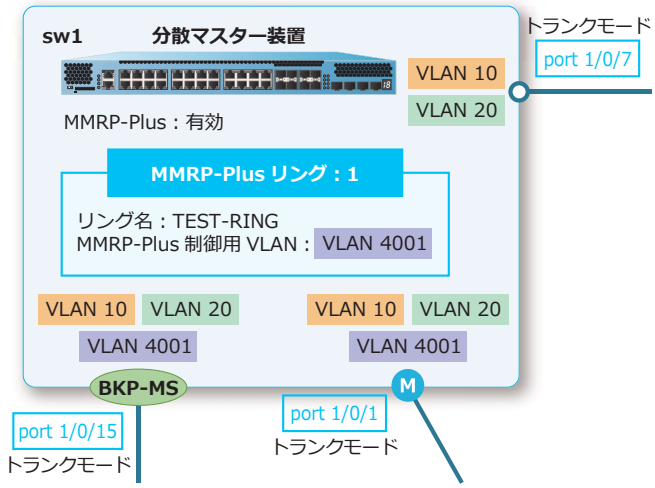
- リング ID：1
- リング名称：TEST-RING
- MMRP-Plus 制御用 VLAN：4001
- VLAN グループの割り当てなし（デフォルト設定、すべての VLAN がマスター VLAN）
- sw1 が分散マスター装置：マスターポート 1/0/1、BKP-MS ポート 1/0/15
- sw2 が分散スレーブ装置：スレーブポート 1/0/1
- sw3 がアウェア装置：アウェアポート 1/0/1,1/0/2、BKP-A ポート 1/0/9

図 14-42 分散マスター構成で MMRP-Plus DFM 機能を使用する場合の構成例



14.3.4.1 分散マスター装置の設定例（sw1）

図 14-43 分散マスター装置の設定例（sw1）



1. VLAN 10、VLAN 20、VLAN 4001 を作成し、設定例のように VLAN を割り当てます。

```
sw1# configure terminal
sw1(config)# vlan 10,20,4001
sw1(config-vlan)# exit
sw1(config)#
sw1(config)# interface range port 1/0/1,1/0/15
sw1(config-if-port-range)# switchport mode trunk
sw1(config-if-port-range)# switchport trunk allowed vlan 10,20,4001
sw1(config-if-port-range)# exit
sw1(config)#
sw1(config)# interface port 1/0/7
sw1(config-if-port)# switchport mode trunk
sw1(config-if-port)# switchport trunk allowed vlan 10,20
sw1(config-if-port)# exit
sw1(config)#
```

2. リングポート（1/0/1）と BKP-MS ポート（1/0/15）で、スケジューリングアルゴリズムを Strict Priority Queuing に設定します。

```
sw1(config)# interface range port 1/0/1,1/0/15
sw1(config-if-port-range)# mls qos scheduler sp
sw1(config-if-port-range)# exit
sw1(config)#
```

3. リング ID［1］の MMRP-Plus リング名を［TEST-RING］に設定します。

```
sw1(config)# mmrp-plus ring 1 name TEST-RING
sw1(config)#
```

4. リング ID［1］の MMRP-Plus 制御用 VLAN を［VLAN 4001］に設定します。

```
sw1(config)# mmrp-plus ring 1 vid 4001
sw1(config)#
```

5. リング ID［1］で、分散マスターポートを［ポート 1/0/1］指定で、sw1 を分散マスター装置に設定します。

```
sw1(config)# mmrp-plus ring 1 divided-master port 1/0/1
sw1(config)#
```

6. MMRP-Plus DFM 機能を有効化します。

```
sw1(config)# mmrp-plus ring 1 double-fault-monitor enable
sw1(config)#
```

7. MMRP-Plus を有効化します。

```
sw1(config)# mmrp-plus enable
sw1(config)#
```

8. MMRP-Plus DFM 機能で使用するリング ID［1］の迂回路接続ポート（BKM-MS）を［ポート 1/0/15］に設定します。

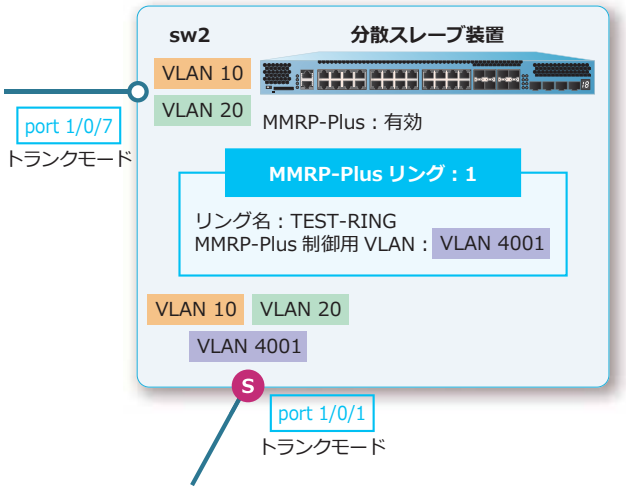
```
sw1(config)# mmrp-plus ring 1 backup-path port 1/0/15
sw1(config)# end
sw1#
```

9. 実施後の MMRP-Plus 関連の設定を以下に抜粋します。

```
# MMRP

mmrp-plus ring 1 name TEST-RING
mmrp-plus ring 1 vid 4001
mmrp-plus ring 1 double-fault-monitor enable
mmrp-plus ring 1 divided-master port 1/0/1
mmrp-plus enable
mmrp-plus ring 1 backup-path port 1/0/15
```

14.3.4.2 分散スレーブ装置の設定例（sw2）

図 14-44 分散スレーブ装置の設定例（sw2）



1. VLAN 10、VLAN 20、VLAN 4001 を作成し、設定例のように VLAN を割り当てます。

```
sw2# configure terminal
sw2(config)# vlan 10,20,4001
sw2(config-vlan)# exit
sw2(config)#
sw2(config)# interface port 1/0/1
sw2(config-if-port)# switchport mode trunk
sw2(config-if-port)# switchport trunk allowed vlan 10,20,4001
sw2(config-if-port)# exit
sw2(config)#
sw2(config)# interface port 1/0/7
sw2(config-if-port)# switchport mode trunk
sw2(config-if-port)# switchport trunk allowed vlan 10,20
sw2(config-if-port)# exit
sw2(config)#
```

2. リングポート（1/0/1）で、スケジューリングアルゴリズムを Strict Priority Queuing に設定します。

```
sw2(config)# interface port 1/0/1
sw2(config-if-port)# mls qos scheduler sp
sw2(config-if-port)# exit
sw2(config)#
```

3. リング ID［1］の MMRP-Plus リング名を［TEST-RING］に設定します。

```
sw2(config)# mmrp-plus ring 1 name TEST-RING
sw2(config)#
```

4. リング ID［1］の MMRP-Plus 制御用 VLAN を［VLAN 4001］に設定します。

```
sw2(config)# mmrp-plus ring 1 vid 4001
sw2(config)#
```

5. リング ID［1］で、分散スレーブポートを［ポート 1/0/1］指定で、sw2 を分散スレーブ装置に設定します。

```
sw2(config)# mmrp-plus ring 1 divided-slave port 1/0/1
sw2(config)#
```

6. MMRP-Plus DFM 機能を有効化します。

```
sw2(config)# mmrp-plus ring 1 double-fault-monitor enable
sw2(config)#
```

7. MMRP-Plus を有効化します。

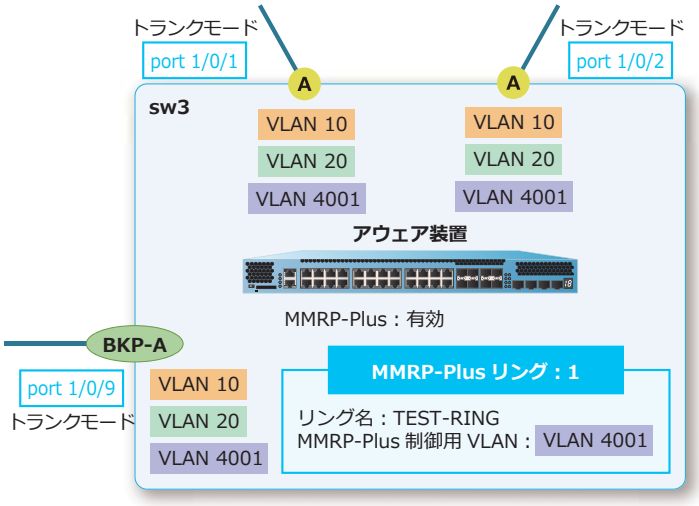
```
sw2(config)# mmrp-plus enable
sw2(config)#
```

8. 実施後の MMRP-Plus 関連の設定を以下に抜粋します。

```
# MMRP

mmrp-plus ring 1 name TEST-RING
mmrp-plus ring 1 vid 4001
mmrp-plus ring 1 double-fault-monitor enable
mmrp-plus ring 1 divided-slave port 1/0/1
mmrp-plus enable
```

14.3.4.3 アウェア装置の設定例（sw3）

図 14-45 アウェア装置の設定例（sw3）



1. VLAN 10、VLAN 20、VLAN 4001 を作成し、設定例のように VLAN を割り当てます。

```
sw3# configure terminal
sw3(config)# vlan 10,20,4001
sw3(config-vlan)# exit
sw3(config)#
sw3(config)# interface range port 1/0/1-2,1/0/9
sw3(config-if-port-range)# switchport mode trunk
sw3(config-if-port-range)# switchport trunk allowed vlan 10,20,4001
sw3(config-if-port-range)# exit
sw3(config)#
```

2. リングポート（1/0/1-2）と BKP-A ポート（1/0/9）で、スケジューリングアルゴリズムを Strict Priority Queuing に設定します。

```
sw3(config)# interface range port 1/0/1-2,1/0/9
sw3(config-if-port-range)# mls qos scheduler sp
sw3(config-if-port-range)# exit
sw3(config)#
```

3. リング ID［1］の MMRP-Plus リング名を［TEST-RING］に設定します。

```
sw3(config)# mmrp-plus ring 1 name TEST-RING
sw3(config)#
```

4. リング ID［1］の MMRP-Plus 制御用 VLAN を［VLAN 4001］に設定します。

```
sw3(config)# mmrp-plus ring 1 vid 4001
sw3(config)#
```

5. リング ID［1］で、アウェアポートを［ポート 1/0/1, ポート 1/0/2］指定で、sw3 をアウェア装置に設定します。

```
sw3(config)# mmrp-plus ring 1 aware port 1/0/1 port 1/0/2
sw3(config)#
```

6. MMRP-Plus DFM 機能を有効化します。

```
sw3(config)# mmrp-plus ring 1 double-fault-monitor enable
sw3(config)#
```

7. MMRP-Plus を有効化します。

```
sw3(config)# mmrp-plus enable
sw3(config)#
```

8. MMRP-Plus DFM 機能で使用するリング ID［1］の迂回路接続ポート（BKM-A）を［ポート 1/0/9］に設定します。

```
sw3(config)# mmrp-plus ring 1 backup-path port 1/0/9
sw3(config)# end
sw3#
```

9. 実施後の MMRP-Plus 関連の設定を以下に抜粋します。

```
# MMRP

mmrp-plus ring 1 name TEST-RING
mmrp-plus ring 1 vid 4001
mmrp-plus ring 1 double-fault-monitor enable
mmrp-plus ring 1 aware port 1/0/1 port 1/0/2
mmrp-plus enable
mmrp-plus ring 1 backup-path port 1/0/9
```

15. リンクダウン連携機能

リンクダウン連携機能、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。

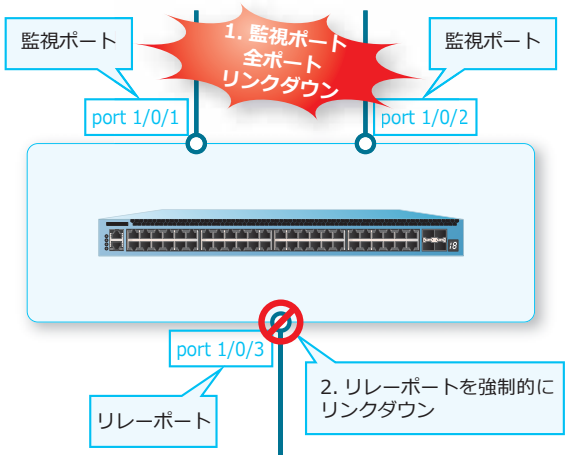
REF: コマンドの詳細については、『コマンドリファレンス』を参照してください。

15.1 リンクダウン連携機能の機能説明

リンクダウン連携機能は、監視ポートのリンク状態に追従して、リレーポートのリンク状態を変更する機能です。

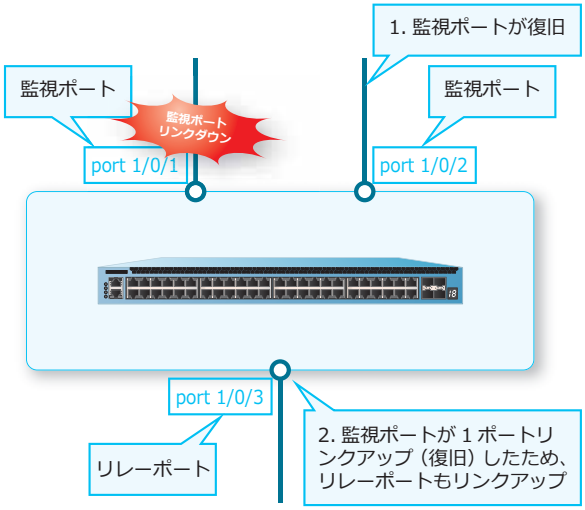
監視ポートとして設定したすべてのポートがリンクダウンすると、リレーポートとして設定したすべてのポートが強制的にリンクダウンされます。

図 15-1 監視ポート障害時の動作



監視ポートとして設定したすべてのポートがリンクダウンしている状態から 1 つ以上のポートがリンクアップすると、リレーポートとして設定したすべてのポートの強制的なリンクダウン状態が解除されてリンクアップに戻ります。

図 15-2 監視ポート復旧時の動作



任意のポートを複数のリンクダウン連携インスタンスのリレーポートとして設定することもできますが、その場合は以下のように動作します。

- そのリレーポートが所属する複数のリンクダウン連携インスタンスのいずれか 1 つで切り替わり条件（監視ポートがすべてリンクダウン）を満たすと、リレーポートが強制的にリンクダウンされます。
- そのリレーポートが所属するすべてのリンクダウン連携インスタンスで復旧条件（監視ポートが 1 つ以上リンクアップ）を満たすと、リレーポートの強制的なリンクダウン状態が解除されてリンクアップに戻ります。

15.2 リンクダウン連携機能の状態確認

リンクダウン連携機能の状態を表示して確認する方法を説明します。

15.2.1 リンクダウン連携設定およびポートのリンク状態の表示

show link-relay コマンドで、リンクダウン連携設定およびポートのリンク状態を確認できます。

表示例を以下に示します。

```
# show link-relay

Track Port T: LinkUp t: LinkDown
Relay Port R: LinkUp r: LinkDown
(1)
   C Port
       1       8 9      16 17     24 25
ID     +-------+ +-------+ +-------+ +---
1   1  TTTTT... .R....R. ........ ..
32  1  ......Rr ........ TTT..... ..
```

各項目の説明は、以下のとおりです。

表 15-1 show link-relay コマンドの表示項目

項番	説明
(1)	リンクダウン連携インスタンスごとに、リンクダウン連携設定、およびポートのリンク状態を表示します。 "C" 列はスタックのボックス ID を示します。スタックが無効な場合は 1 が表示されます。

15.2.2 監視ポートの状態の表示

show link-relay status コマンドで、リンクダウン連携インスタンスごとの監視ポートの状態を確認できます。

表示例を以下に示します。

```
# show link-relay status
(1) (2)      (3)
ID  Status   Remain Ports
--  ------   ------------
1   Up       5
2   Down     0
32  Up       3
```

各項目の説明は、以下のとおりです。

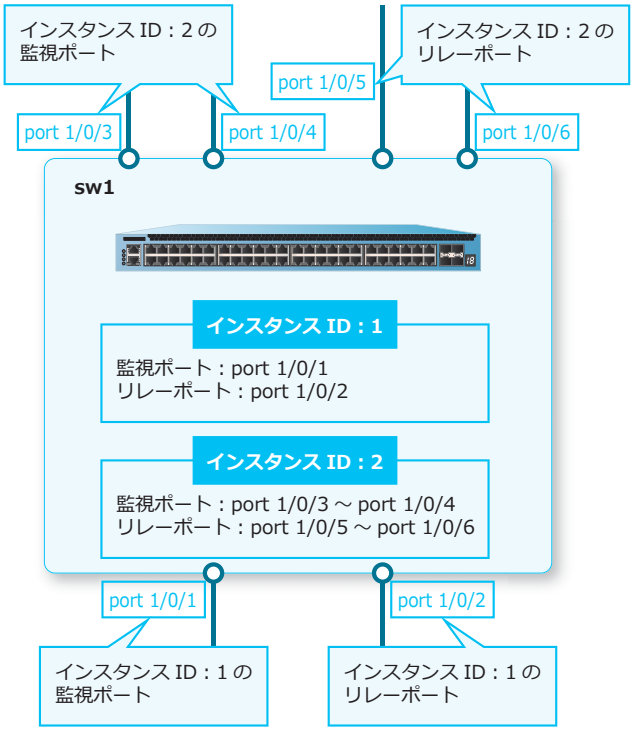
表 15-2 `show link-relay status` コマンドの表示項目

項番	説明
(1)	リンクダウン連携インスタンスを表示します。
(2)	リンクダウン連携インスタンスの状態を表示します。 • Down：すべての監視ポートがリンクダウン状態 • Up：少なくとも 1 ポート以上の監視ポートがリンクアップ状態
(3)	リンクアップ状態の監視ポートの数を表示します。

15.3 リンクダウン連携機能の構成例と設定例

リンクダウン連携機能を利用する場合の構成例と設定例を示します。

図 15-3 リンクダウン連携機能の構成例



1. リンクダウン連携インスタンス［1］で、監視ポートを［ポート 1/0/1］に、リレーポートを［ポート 1/0/2］に設定します。

```
sw1# configure terminal
sw1(config)# link-relay id 1 track-port interface port 1/0/1 relay-port
interface port 1/0/2
sw1(config)#
```

2. リンクダウン連携インスタンス［2］で、監視ポートを［ポート 1/0/3 からポート 1/0/4］に、リレーポートを［ポート 1/0/5 からポート 1/0/6］に設定します。

```
sw1(config)# link-relay id 2 track-port interface port 1/0/3-1/0/4 relay-port
interface port 1/0/5-1/0/6
sw1(config)# exit
sw1#
```

16. ポートリダンダント

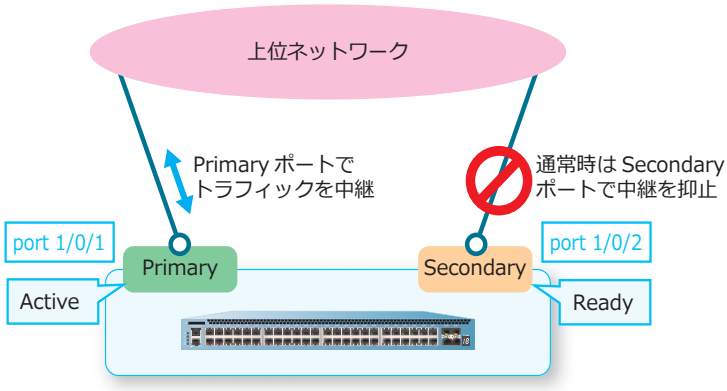
ポートリダンダントの機能、状態の確認方法、および構成例と設定例について説明します。

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 ポートリダンダントの機能説明

ポートリダンダントは、Primary ポートと Secondary ポートのペアで構成される、レイヤー 2 の冗長機能です。通常時は、Primary ポートが Active 状態でトラフィックを中継し、Secondary ポートが Ready 状態でトラフィックの中継を抑止します。

図 16-1 通常時のトラフィック中継

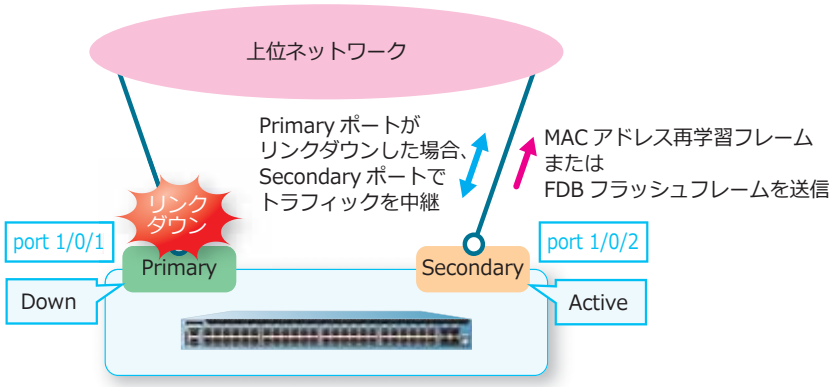


NOTE: 装置全体で設定できるリダンダントグループは、最大 32 個です。スタック構成の場合も同様です。

NOTE: Ready 状態のポートはトラフィックの中継を抑止している状態ですが、物理ポートはリンクアップしているため、レイヤー 3 機能の VLAN インターフェースとしてはリンクアップしているポートとして扱われます。

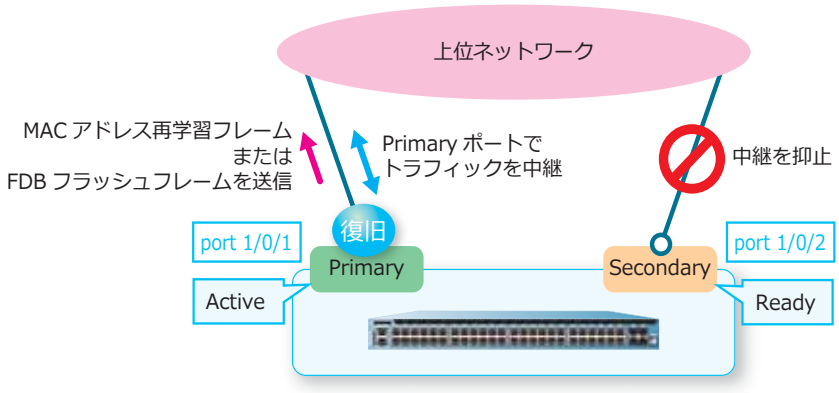
Primary ポートがリンクダウンすると、Secondary ポートが Active 状態に遷移してトラフィックを中継します。このとき、Secondary ポートから MAC アドレス再学習フレームまたは FDB フラッシュフレームを送信し、上位ネットワークの MAC アドレステーブルの更新を促します。

図 16-2 Primary ポートがリンクダウンした場合のトラフィック中継



Primary ポートがリンクアップすると、Primary ポートが Active 状態に復旧します。このとき、Primary ポートから MAC アドレス再学習フレームまたは FDB フラッシュフレームを送信し、上位ネットワークの MAC アドレステーブルの更新を促します。

図 16-3 Primary ポートが Active 状態に復旧した場合のトラフィック中継



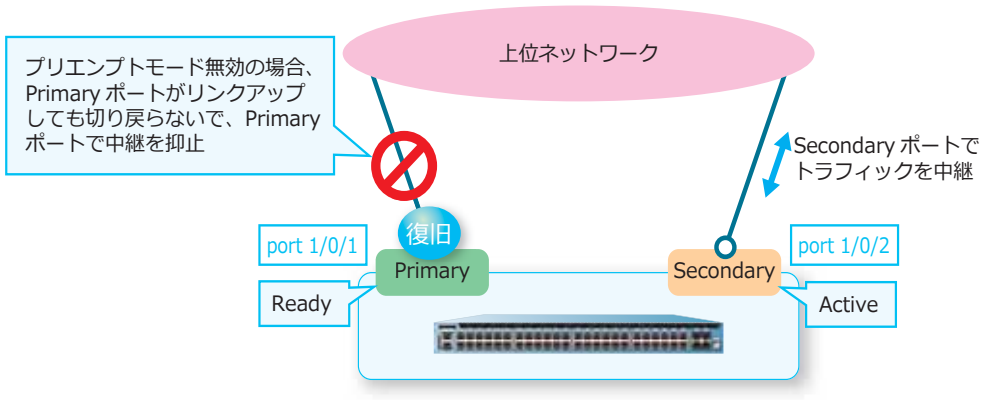
ポートリダンダントを設定するには、**`redundant group-number`** コマンドを使用します。

16.1.1 プリエンプトモードと切り戻り遅延時間の設定

NOTE: プリエンプトモードと切り戻り遅延時間の設定は、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。

デフォルト設定（プリエンプトモード有効）では、「Primary ポートがリンクアップすると、Primary ポートが Active 状態に切り戻る動作」ですが、プリエンプトモードを無効にすることにより、「Primary ポートがリンクアップしても切り戻さない動作」に変更できます。この場合、Primary ポートがリンクアップしても Secondary ポートが Active 状態のままで、リンクアップした Primary ポートが Ready 状態になります。

図 16-4 プリエンプトモード



また、プリエンプトモードが有効な場合に、切り戻り遅延時間（デフォルトは 0 秒）を設定できます。たとえば、切り戻り遅延時間を 60 秒に設定した場合、Primary ポートがリンクアップしてから 60 秒経過すると、Primary ポートが Active 状態に切り戻ります。なお、切り戻り遅延時間が経過するまでの間に Secondary ポートがリンクダウンした場合は、切り戻り遅延時間の経過を待たずに、即時 Primary ポートが Active 状態に切り戻ります。

プリエンプトモードと切り戻り遅延時間を設定するには、**`redundant group-number preempt`** コマンドを使用します。

NOTE: プリエンプトモードが無効な装置を起動した場合、Primary ポートと Secondary ポートのどちらが最初に Active 状態になるかは、それぞれのポートがリンクアップした順番によります。

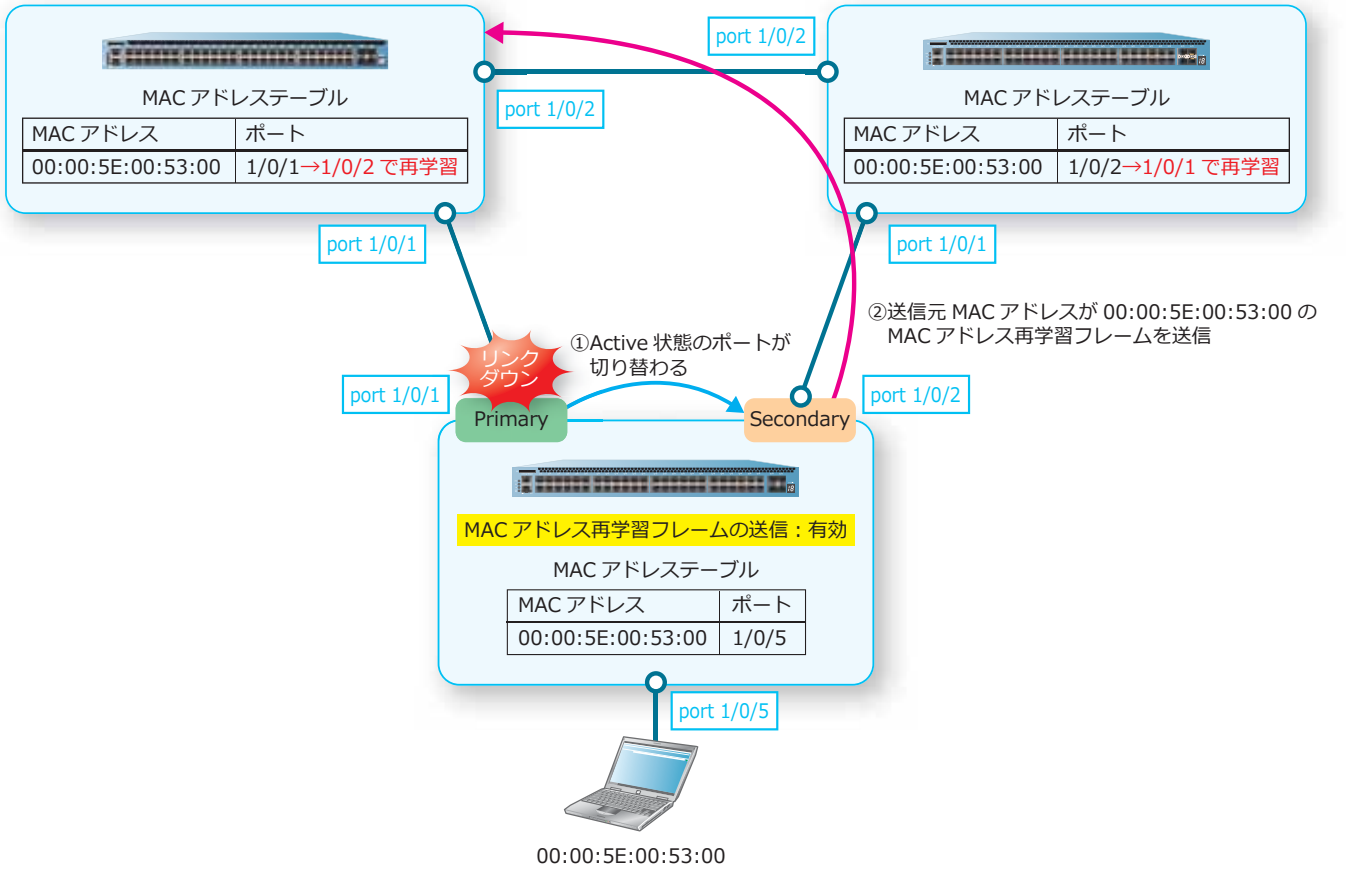
NOTE: プリエンプトモードが無効で「Primary ポートが Ready 状態、Secondary ポートが Active 状態」の場合に、**`no redundant group-number preempt`** コマンドでプリエンプトモードを有効に変更すると、Primary ポートが Active 状態に切り戻ります。

16.1.2 MAC アドレス再学習フレーム送信機能の仕様と動作

MAC アドレス再学習フレームの送信を有効にした場合、Active 状態のポートが切り替わる際に、上位スイッチの MAC アドレステーブルを更新するために、再学習が必要な MAC アドレス（Primary ポートおよび Secondary ポート以外で学習した MAC アドレスエントリー）のための、MAC アドレス再学習フレームを送信します。

MAC アドレス再学習フレームの送信元 MAC アドレスは、そのエントリー自身の MAC アドレスになります。上位スイッチの MAC アドレステーブルで再学習させることで、上位スイッチ側からの片方向トラフィックのみの場合でも、すぐに通信を復旧できます。

図 16-5 MAC アドレス再学習フレーム送信機能



MAC アドレス再学習フレームの送信を有効にするには、**`redundant mac-address-table-update`** コマンドを使用します。

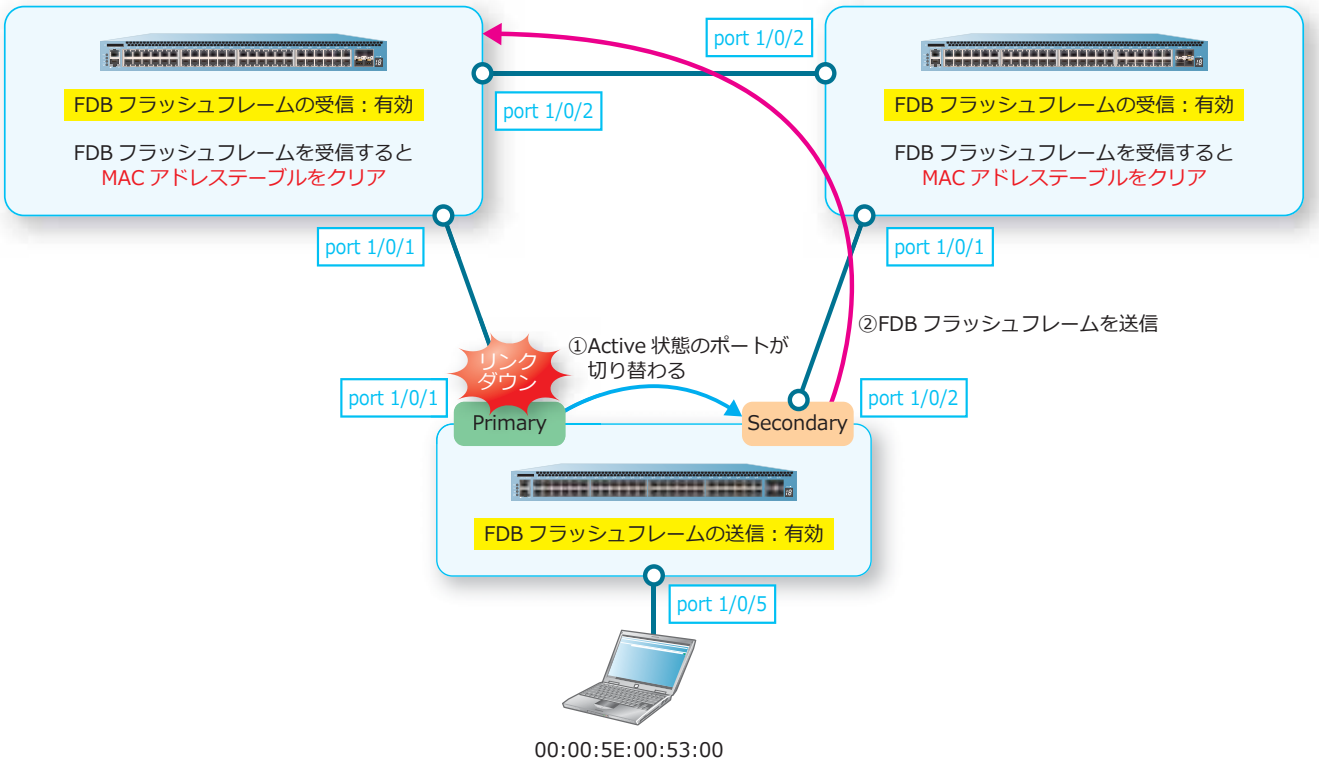
16.1.3 FDB フラッシュフレーム送信機能／ FDB フラッシュフレーム受信機能の仕様と動作

FDB フラッシュフレームの送信を有効にした場合、Active 状態のポートが切り替わる際に、FDB フラッシュフレームを送信します。このとき、FDB フラッシュフレーム受信機能を有効にしたスイッチでは、FDB フラッシュフレームを受信した場合に、装置全体の MAC アドレステーブルをクリアします。

これにより、上位スイッチ側からの片方向トラフィックしかない場合でも、FDB フラッシュフレームの受信を有効にした上位スイッチが FDB フラッシュフレームを受信して装置全体の MAC アドレステーブルをクリアすることで、すぐに通信を復旧できます。

なお、FDB フラッシュフレームであることを判断するための宛先 MAC アドレスの設定は、任意に変更できます。これにより、特定の宛先 MAC アドレスのフレームを受信した場合に、装置全体の MAC アドレステーブルをクリアすることもできます。

図 16-6 FDB フラッシュフレーム送信機能／ FDB フラッシュフレーム受信機能



FDB フラッシュフレームの送信を有効にするには、**`redundant fdb-flush send enable`** コマンドを使用します。FDB フラッシュフレームの受信を設定するには、**`redundant fdb-flush receive enable`** コマンドを使用します。FDB フラッシュフレームであることを判断する宛先 MAC アドレスを設定するには、**`redundant fdb-flush dst-mac`** コマンドを使用します。

16.2 ポートリダンダントの状態確認

ポートリダンダントの状態を表示して確認する方法を説明します。

16.2.1 ポートリダンダントの設定と動作状態の表示

show redundant コマンドで、ポートリダンダントの設定と動作状態を確認できます。

表示例を以下に示します。

```
# show redundant

 Mac-address-table-update    :Disable ...(1)
 FDB-flush send              :Enable (count 3) ...(2)
 FDB-flush receive           :Disable ...(3)
 VLAN ID                     :300 ...(4)
 Dst MAC address             :01-40-66-C0-4F-44 ...(5)
 A: Active      a: Active (port-channel)
 R: Ready       r: Ready (port-channel)
 D: Link Down   d: Link Down (port-channel)
         (7)
(6)    C Pre Port
             1       8 9      16 17    24 25    32 33    40 41    48 49
GrpNo        +-------+ +-------+ +-------+ +-------+ +-------+ +-------+ +---
  1    1 Dis AR..... ........ ........ ........ ........ ........ ....
  8    1 120 ........ ........ ....aarr ........ ........ ........ ....
```

各項目の説明は、以下のとおりです。

表 16-1 show redundant コマンドの表示項目

項番	説明
(1)	MAC アドレス再学習フレーム送信の有効 (Enable) ／無効 (Disable) を表示します。有効時には送信回数も表示します。
(2)	FDB フラッシュフレーム送信の有効 (Enable) ／無効 (Disable) を表示します。有効時には送信回数も表示します。
(3)	FDB フラッシュフレーム受信の有効 (Enabled) ／無効 (Disable) を表示します。
(4)	FDB フラッシュフレームの VLAN タグの VLAN ID を表示します。
(5)	FDB フラッシュフレームの宛先 MAC アドレスを表示します。
(6)	リダンダントグループ ID ごとに、プリエンプトモードと切り戻り遅延時間の設定、ポートリダンダントの設定、およびポートのリンク状態を表示します。 "C" 列はスタックのボックス ID を示します。スタックが無効な場合は 1 が表示されます。
(7)	プリエンプトモードと切り戻り遅延時間を表示します。 • - ：プリエンプトモード有効で切り戻り遅延時間 0 秒設定 • Dis ：プリエンプトモード無効 • 1-300 ：プリエンプトモード有効で、切り戻り遅延時間（秒）を表示

16.2.2 ポートリダンダントのインターフェース情報の表示

show redundant portbase コマンドで、ポートリダンダントのインターフェース情報を確認できます。

表示例を以下に示します。

```
# show redundant portbase
(1)              (2)       (3)      (4)
Port             Status    GrpNo    Pri/Sec
Port1/0/1        Active    1        Primary
Port1/0/2        Ready     1        Secondary
Port-channel20 Active    8        Primary
Port-channel21 Ready     8        Secondary
```

各項目の説明は、以下のとおりです。

表 16-2 show redundant portbase コマンドの表示項目

項番	説明
(1)	ポートリダンダントを設定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。
(2)	ポートリダンダントの動作状態を表示します。 • Active：トラフィックの中継が可能な状態 • Ready：トラフィックの中継を抑止している状態 • Down：対象ポート、またはポートチャネルがダウンしている状態
(3)	リダンダントグループ ID を表示します。
(4)	ポート種別を表示します。 • Primary：ポートリダンダントの Primary ポート • Secondary：ポートリダンダントの Secondary ポート

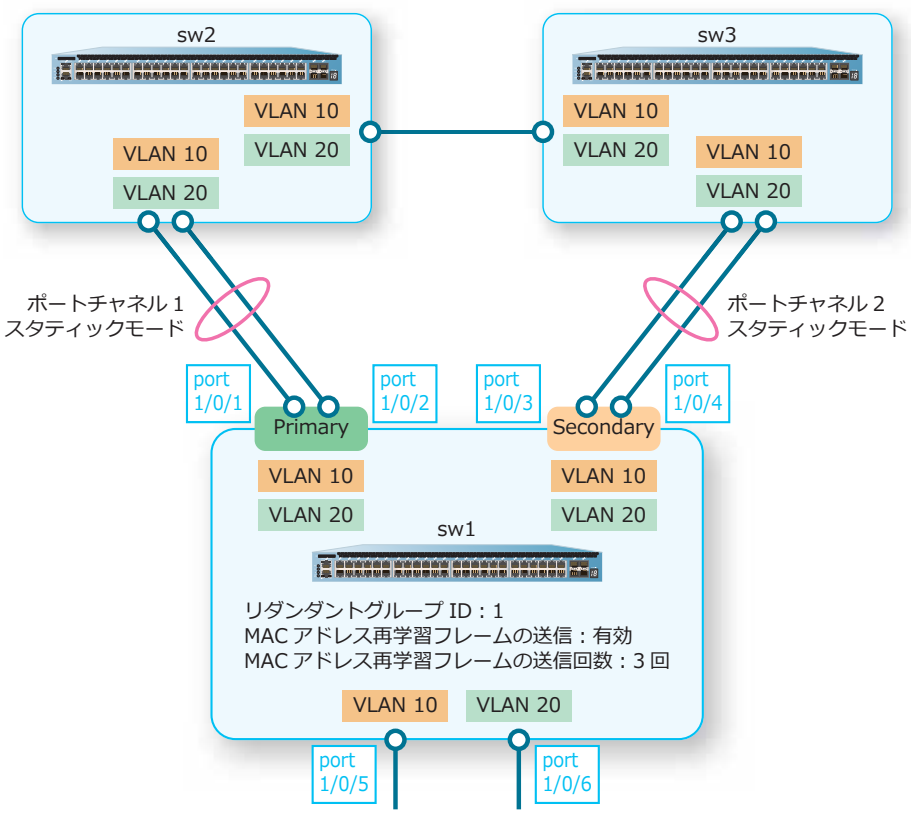
16.3 ポートリダンダントの構成例と設定例

ポートリダンダントを利用する場合の構成例と設定例を示します。

16.3.1 MAC アドレス再学習フレームを使用する場合

MACアドレス再学習フレームの送信を有効にしたポートリダンダント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、sw1 の設定例のみ示します。

図 16-7 MAC アドレス再学習フレームを使用する場合の構成例



1. VLAN 10 および 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 およびポート 1/0/2 をチャネルグループ ID［1］のメンバーポートに、スタティックモードで設定します。また、ポート 1/0/3 およびポート 1/0/4 をチャネルグループ ID［2］のメンバーポートに、スタティックモードで設定します。

```
sw1(config)# interface range port 1/0/1-2
sw1(config-if-port-range)# channel-group 1 mode on
sw1(config-if-port-range)# exit
sw1(config)# interface range port 1/0/3-4
sw1(config-if-port-range)# channel-group 2 mode on
sw1(config-if-port-range)# exit
sw1(config)#
```

3. チャネルグループ 1 およびチャネルグループ 2 をトランクポートとして設定し、トランクポートに［VLAN 10］および［VLAN 20］を割り当てます。

```
sw1(config)# interface port-channel 1
sw1(config-if-port-channel)# switchport mode trunk
sw1(config-if-port-channel)# switchport trunk allowed vlan 10,20
sw1(config-if-port-channel)# exit
sw1(config)# interface port-channel 2
sw1(config-if-port-channel)# switchport mode trunk
sw1(config-if-port-channel)# switchport trunk allowed vlan 10,20
sw1(config-if-port-channel)# exit
sw1(config)#
```

4. ポート 1/0/5 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 1/0/6 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 1/0/5
sw1(config-if-port)# switchport access vlan 10
sw1(config-if-port)# exit
sw1(config)# interface port 1/0/6
sw1(config-if-port)# switchport access vlan 20
sw1(config-if-port)# exit
sw1(config)#
```

5. リダンダントグループ ID［1］の Primary ポートにチャネルグループ 1 を、Secondary ポートにチャネルグループ 2 を割り当てます。

```
sw1(config)# interface port-channel 1
sw1(config-if-port-channel)# redundant group-number 1 primary
sw1(config-if-port-channel)# exit
sw1(config)# interface port-channel 2
sw1(config-if-port-channel)# redundant group-number 1 secondary
sw1(config-if-port-channel)# exit
sw1(config)#
```

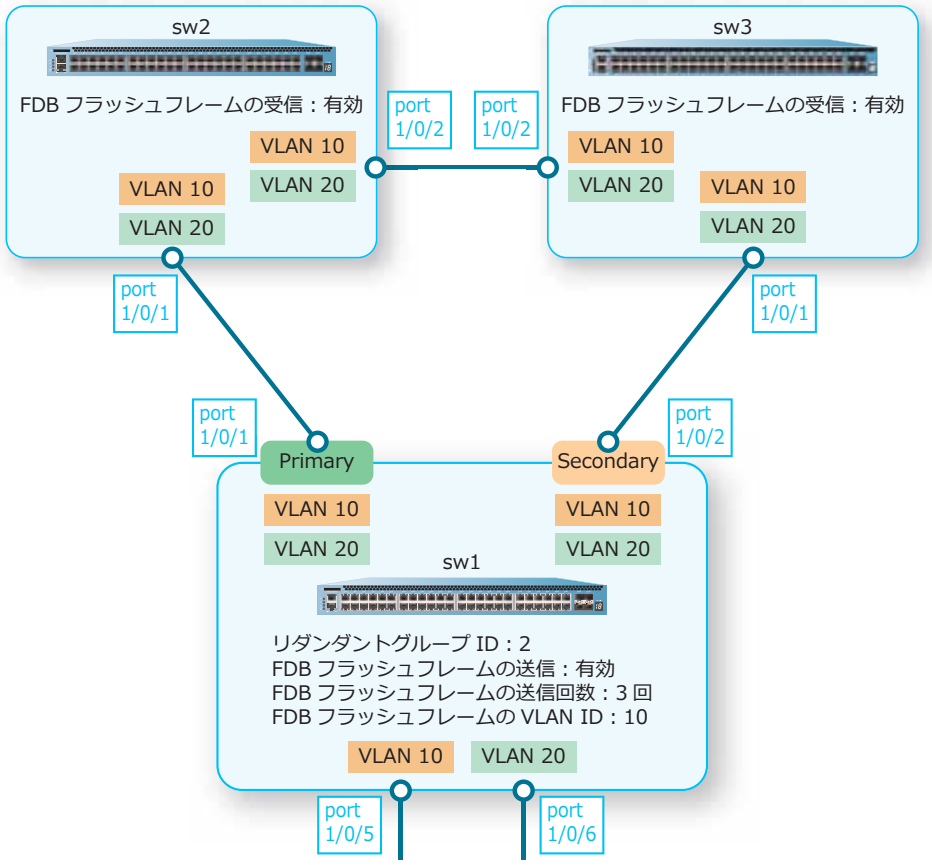
6. MAC アドレス再学習フレームの送信を、送信回数［3 回］で有効にします。

```
sw1(config)# redundant mac-address-table-update count 3
sw1(config)# end
sw1#
```

16.3.2 FDB フラッシュフレームを使用する場合

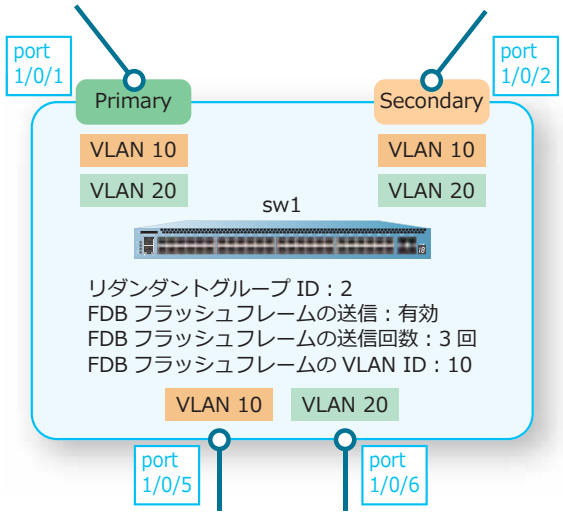
FDB フラッシュフレームの送信を有効にしたポートリダンダントを使用する場合の構成例と設定例を示します。

図 16-8 FDB フラッシュフレームを使用する場合の構成例



16.3.2.1 FDB フラッシュフレームを使用する場合：sw1 の設定例

図 16-9 FDB フラッシュフレームを使用する場合：sw1 の設定例



1. VLAN 10 および 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 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 10］および［VLAN 20］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 10,20
sw1(config-if-port)# exit
sw1(config)# interface port 1/0/2
sw1(config-if-port)# switchport mode trunk
sw1(config-if-port)# switchport trunk allowed vlan 10,20
sw1(config-if-port)# exit
sw1(config)#
```

3. ポート 1/0/5 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 1/0/6 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 1/0/5
sw1(config-if-port)# switchport access vlan 10
sw1(config-if-port)# exit
sw1(config)# interface port 1/0/6
sw1(config-if-port)# switchport access vlan 20
sw1(config-if-port)# exit
sw1(config)#
```

4. リダンダントグループ ID［2］の Primary ポートにポート 1/0/1 を、Secondary ポートにポート 1/0/2 を割り当てます。

```
sw1(config)# interface port 1/0/1
sw1(config-if-port)# redundant group-number 2 primary
sw1(config-if-port)# exit
sw1(config)# interface port 1/0/2
sw1(config-if-port)# redundant group-number 2 secondary
sw1(config-if-port)# exit
sw1(config)#
```

5. FDB フラッシュフレームの VLAN ID を［VLAN 10］に設定します。

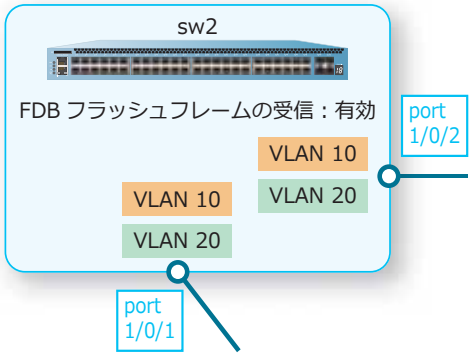
```
sw1(config)# redundant fdb-flush vid 10
sw1(config)#
```

6. FDB フラッシュフレームの送信を、送信回数［3 回］で有効にします。

```
sw1(config)# redundant fdb-flush send enable count 3
sw1(config)# end
sw1#
```

16.3.2.2 FDB フラッシュフレームを使用する場合：sw2 の設定例

図 16-10 FDB フラッシュフレームを使用する場合：sw2 の設定例



1. VLAN 10 および VLAN 20 を作成します。

```
sw2# configure terminal
sw2(config)# vlan 10,20
sw2(config-vlan)# exit
sw2(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 10］および［VLAN 20］を割り当てます。

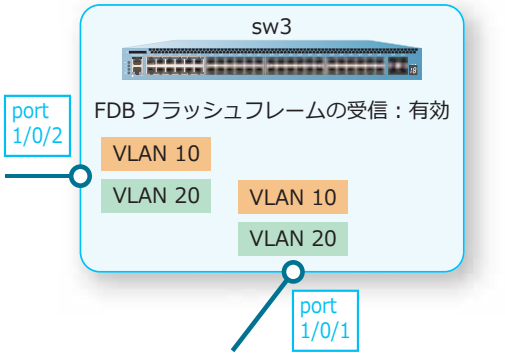
```
sw2(config)# interface port 1/0/1
sw2(config-if-port)# switchport mode trunk
sw2(config-if-port)# switchport trunk allowed vlan 10,20
sw2(config-if-port)# exit
sw2(config)# interface port 1/0/2
sw2(config-if-port)# switchport mode trunk
sw2(config-if-port)# switchport trunk allowed vlan 10,20
sw2(config-if-port)# exit
sw2(config)#
```

3. FDB フラッシュフレームの受信機能を有効にします。

```
sw2(config)# redundant fdb-flush receive enable
sw2(config)# end
sw2#
```

16.3.2.3 FDB フラッシュフレームを使用する場合：sw3 の設定例

図 16-11 FDB フラッシュフレームを使用する場合：sw3 の設定例



1. VLAN 10 および VLAN 20 を作成します。

```
sw3# configure terminal
sw3(config)# vlan 10,20
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 10］および［VLAN 20］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 10,20
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 10,20
sw3(config-if-port)# exit
sw3(config)#
```

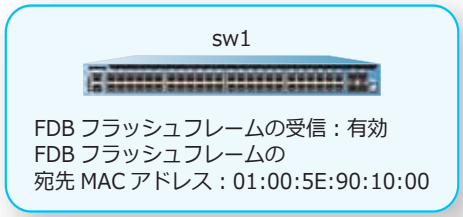
3. FDB フラッシュフレームの受信機能を有効にします。

```
sw3(config)# redundant fdb-flush receive enable
sw3(config)# end
sw3#
```

16.3.3 特定のフレーム受信で MAC アドレステーブルをクリアする場合

特定の宛先 MAC アドレスのフレーム受信によって、MAC アドレステーブルをクリアする場合の構成例と設定例を示します。

図 16-12 特定のフレーム受信で MAC アドレステーブルをクリアする場合の構成例



1. FDB フラッシュフレームの宛先 MAC アドレスを［01:00:5E:90:10:00］に設定します。

```
sw1# configure terminal
sw1(config)# redundant fdb-flush dst-mac 01:00:5e:90:10:00
sw1(config)#
```

2. FDB フラッシュフレームの受信を有効にします。

```
sw1(config)# redundant fdb-flush receive enable
sw1(config)# end
sw1#
```

17. Voice VLAN

Voice VLAN 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。

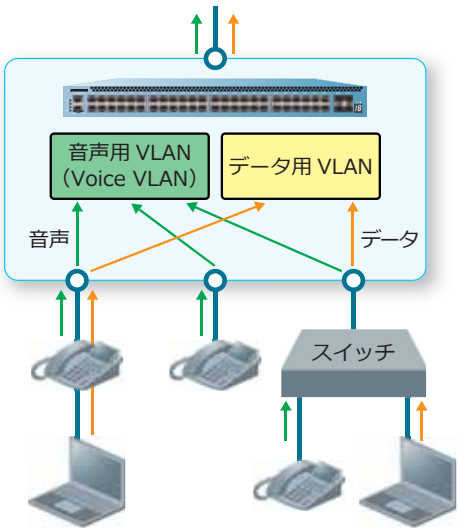
REF: コマンドの詳細については、『コマンドリファレンス』を参照してください。

17.1 Voice VLAN の機能説明

Voice VLAN は、音声トラフィックの QoS 設定を自動的に設定する機能です。IP 電話と PC を同一ポートで収容する場合などに、音声トラフィックをデータトラフィックとは別の VLAN で収容し、優先度を上げて音声トラフィックの品質を確保します。

CAUTION: NP7000、NP5000、NP4000、および NP3000 では、Voice VLAN は使用できません。

図 17-1 Voice VLAN の概要



Voice VLAN を有効にするには、**`voice vlan`** コマンドで Voice VLAN として使用する VLAN ID を指定します。また、Voice VLAN で収容した音声トラフィックに適用する QoS を設定するには、**`voice vlan qos`** コマンド、および **`voice vlan dscp`** コマンドを使用します。

インターフェースの Voice VLAN 動作モードを設定するには、**`voice vlan mode`** コマンドを使用します。インターフェースの Voice VLAN を有効にするには、**`voice vlan enable`** コマンドを使用します。

17.1.1 Voice VLAN 端末と LLDP-MED 端末

Voice VLAN に収容する端末には、以下の 2 種類のパターンがあります。

- **Voice VLAN 端末**
  IP 電話の OUI（音声トラフィックの送信元 MAC アドレス）で判定
- **LLDP-MED 端末**
  IP 電話からの LLDP-MED で判定

Voice VLAN 端末

Voice VLAN を有効にしたインターフェースで、あらかじめ登録した MAC アドレスと一致する送信元 MAC アドレスのトラフィックを受信した場合は音声トラフィックと判断し、その MAC アドレスを Voice VLAN 端末として登録します。

音声トラフィックと判断する MAC アドレスはデフォルトでいくつか登録されていますが、**voice vlan mac-address** コマンドを使用して追加することもできます。

表 17-1 音声トラフィックと判断する MAC アドレス（デフォルト）

OUI Address	Mask	Description
00:01:E3:00:00:00	FF:FF:FF:00:00:00	Siemens
00:03:6B:00:00:00	FF:FF:FF:00:00:00	Cisco
00:09:6E:00:00:00	FF:FF:FF:00:00:00	Avaya
00:0F:E2:00:00:00	FF:FF:FF:00:00:00	Huawei&3COM
00:60:B9:00:00:00	FF:FF:FF:00:00:00	NEC&Philips
00:D0:1E:00:00:00	FF:FF:FF:00:00:00	Pingtel
00:E0:75:00:00:00	FF:FF:FF:00:00:00	Veritel
00:E0:BB:00:00:00	FF:FF:FF:00:00:00	3COM

NOTE: 音声トラフィックと判断する MAC アドレスのデフォルト設定は、削除できません。

LLDP-MED 端末

Voice VLAN を有効にしたインターフェースで、IP 電話からの LLDP-MED を受信した場合は、LLDP-MED 端末として登録します。

対象インターフェースで LLDP-MED 端末を登録できるようにするには、LLDP を有効にし、**lldp med-tlv-select capabilities**コマンドと**lldp med-tlv-select network-policy**コマンドを使用して、Capabilities TLV と Network Policy TLV の通知を有効にしてください。

CAUTION: 受信する音声パケットがタグなし形式、または VID=0 のタグ付き形式の場合は、LLDP-MED とは併用しないでください。この場合は、Voice VLAN 端末として登録されるように使用してください。

17.1.2 Voice VLAN の動作モード

Voice VLAN を使用する場合は、対象インターフェースを以下のいずれかの動作モードに設定します。

- **自動モード（untag）**

  Voice VLAN 端末が登録されると、対象インターフェースに Voice VLAN がタグなしメンバーとして自動的に割り当てられるモード

- **自動モード（tag）**

  Voice VLAN 端末が登録されると、対象インターフェースに Voice VLAN がタグ付きメンバーとして割り当てられるモード

- **マニュアルモード**

  対象インターフェースに、あらかじめ手動で Voice VLAN を割り当てておくモード

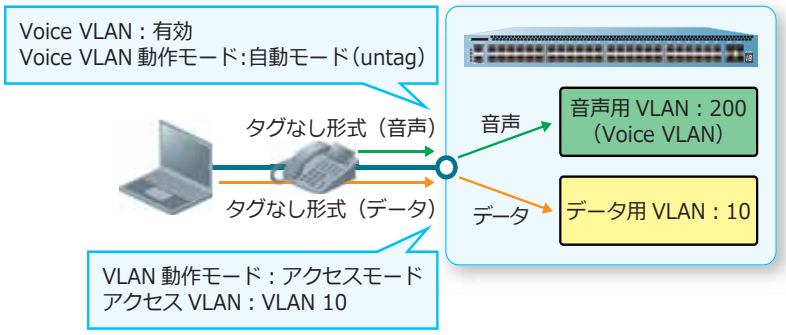
自動モード（untag）

自動モード（untag）は、アクセスポートとハイブリッドポートで使用できます。このモードでは、Voice VLAN 端末が登録されると、対象インターフェースに Voice VLAN がタグなしメンバーとして自動的に割り当てられます。そのため、音声トラフィックは「タグなし形式」を想定しています。

Voice VLAN 端末からの音声パケットが停止し、その Voice VLAN 端末の MAC アドレスが MAC アドレステーブルから削除されると、Voice VLAN 端末のエージングタイマーが開始され、エージングタイマーが満了すると対象の Voice VLAN 端末は削除されます。

同一インターフェースに登録された Voice VLAN 端末がすべて削除されると、割り当てた Voice VLAN も自動的に削除されます。

図 17-2 自動モード（untag）の使用例



自動モード（tag）

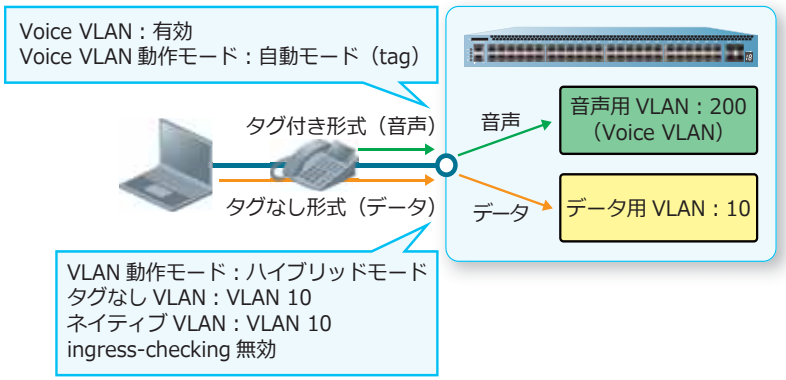
自動モード（tag）は、ハイブリッドポートで使用できます。このモードでは、Voice VLAN 端末が登録されると対象インターフェースに Voice VLAN がタグ付きメンバーとして自動的に割り当てられます。そのため、音声トラフィックは「タグ付き形式」を想定しています。

> ***CAUTION:*** 自動モード（tag）に設定する場合は、対象インターフェースの **`ingress-checking`** コマンドを無効にしてください。

Voice VLAN 端末からの音声パケットが停止し、その Voice VLAN 端末の MAC アドレスが MAC アドレステーブルから削除されると、Voice VLAN 端末のエージングタイマーが開始され、エージングタイマーが満了すると対象の Voice VLAN 端末は削除されます。

同一インターフェースに登録された Voice VLAN 端末がすべて削除されると、割り当てた Voice VLAN も自動的に削除されます。

図 17-3 自動モード（tag）の使用例



マニュアルモード

マニュアルモードは、アクセスポートとハイブリッドポートで使用できます。このモードは、あらかじめ Voice VLAN を割り当てておくモードです。Voice VLAN の自動割り当てが不要な場合、IP 電話のみ接続する場合、および IP 電話を LLDP-MED 端末として登録する場合などに使用します。

図 17-4 マニュアルモードの使用例（1/2）

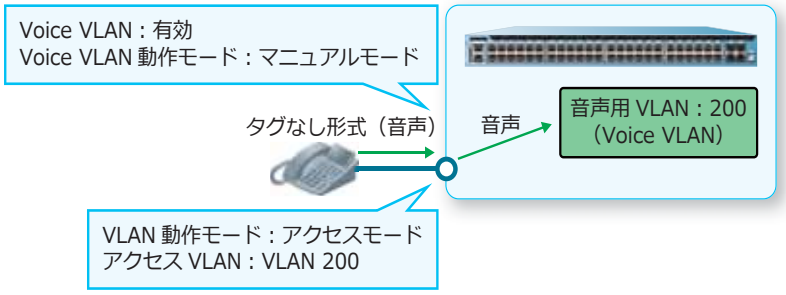
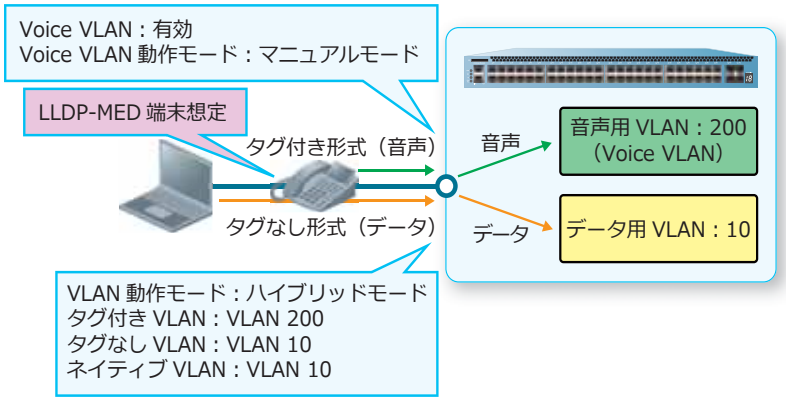


図 17-5 マニュアルモードの使用例（2/2）



17.2 Voice VLAN の状態確認

Voice VLAN の状態を表示して確認する方法を説明します。

17.2.1 Voice VLAN の設定の表示

show voice vlan コマンドで、Voice VLAN の設定を確認できます。

表示例を以下に示します。

```
# show voice vlan

 Voice VLAN ID         : 2 ...(1)
 Voice VLAN CoS        : 5 ...(2)
 Dscp                  : Disable ...(3)
 Aging Time            : 720 minutes ...(4)
 Member Ports          : 1/0/1-1/0/2,1/0/5-1/0/6,1/0/49 ...(5)
 Dynamic Member Ports  : 1/0/1-1/0/2 ...(6)

 Voice VLAN OUI        : ...(7)

 OUI Address         Mask                Description
 ------------------  ------------------  --------------
 00-01-E3-00-00-00   FF-FF-FF-00-00-00   Siemens
 00-03-6B-00-00-00   FF-FF-FF-00-00-00   Cisco
 00-09-6E-00-00-00   FF-FF-FF-00-00-00   Avaya
 00-0F-E2-00-00-00   FF-FF-FF-00-00-00   Huawei&3COM
 00-60-B9-00-00-00   FF-FF-FF-00-00-00   NEC&Philips
 00-D0-1E-00-00-00   FF-FF-FF-00-00-00   Pingtel
 00-E0-75-00-00-00   FF-FF-FF-00-00-00   Veritel
 00-E0-BB-00-00-00   FF-FF-FF-00-00-00   3COM

 Total OUI: 8
```

各項目の説明は、以下のとおりです。

表 17-2 show voice vlan コマンドの表示項目

項番	説明
(1)	Voice VLAN の VLAN ID を表示します。
(2)	Voice VLAN の CoS 値を表示します。
(3)	Voice VLAN の DSCP を表示します。未設定時は Disable と表示されます。
(4)	Voice VLAN 端末のエージングタイム設定を表示します。
(5)	Voice VLAN を有効にしたポート番号を表示します。ポートチャネルの場合は、メンバーポートのポート番号が表示されます。
(6)	動作モードが自動モード（untag, tag）の場合に、自動的に Voice VLAN に割り当てられたポート番号を表示します。ポートチャネルが自動的に割り当てられた場合は、すべてのメンバーポートのポート番号が表示されます。
(7)	Voice VLAN 端末として登録する MAC アドレスを表示します。

ポート 1/0/5 からポート 1/0/7 の、Voice VLAN の設定を確認する場合の表示例を以下に示します。

```
# show voice vlan interface port 1/0/5-7
 (1)              (2)        (3)
 Interface        State      Mode
 --------------   --------   -----------
 Port1/0/5        Enabled    Auto/Untag
 Port1/0/6        Enabled    Manual
 Port1/0/7        Disabled   Auto/Untag
```

各項目の説明は、以下のとおりです。

表 17-3 `show voice vlan` コマンドの表示項目

項番	説明
(1)	ポート番号またはポートチャネル番号を表示します。
(2)	Voice VLAN の有効 (Enabled) ／無効 (Disabled) を表示します。
(3)	Voice VLAN の動作モードを表示します。 • Auto/Untag：自動モード（untag） • Auto/Tag：自動モード（tag） • Manual：マニュアルモード

17.2.2 Voice VLAN 端末の表示

`show voice vlan device` コマンドで、Voice VLAN 端末を確認できます。

表示例を以下に示します。

```
# show voice vlan device
 (1)              (2)                  (3)                (4)
 Interface        Voice Device         Start Time         Status
 --------------   -----------------    ----------------   ------
 Port1/0/2        00-01-E3-33-33-33    2020-03-05 16:11   Active
 Port-channel5    00-01-E3-11-11-11    2020-03-05 16:10   Aging
 Port-channel5    00-01-E3-22-22-22    2020-03-05 16:10   Active

 Total Entries: 3
```

各項目の説明は、以下のとおりです。

表 17-4 `show voice vlan device` コマンドの表示項目

項番	説明
(1)	ポート番号またはポートチャネル番号を表示します。
(2)	Voice VLAN 端末の MAC アドレスを表示します。
(3)	Voice VLAN 端末が登録された日時を表示します。
(4)	Voice VLAN 端末の状態を表示します。 • Active：Voice VLAN 端末の MAC アドレスが MAC アドレステーブルに登録されている状態 • Aging：Voice VLAN 端末の MAC アドレスが MAC アドレステーブルから削除され、Voice VLAN 端末のエージングタイマーが開始している状態

17.2.3 LLDP-MED 端末の表示

show voice vlan lldp-med device コマンドで、LLDP-MED 端末を確認できます。

表示例を以下に示します。

```
# show voice vlan lldp-med device

 Index               : 1 ...(1)
 Interface           : Port1/0/2 ...(2)
 Chassis ID Subtype  : Network Address ...(3)
 Chassis ID          : 10.1.2.3 ...(4)
 Port ID Subtype     : MAC Address ...(5)
 Port ID             : 00-40-66-11-11-11 ...(6)
 Create Time         : 3/5/2020  16:25:55 ...(7)
 Remain Time         : 120 Seconds ...(8)

 Index               : 2
 Interface           : Port-channel5
 Chassis ID Subtype  : Network Address
 Chassis ID          : 20.1.1.1
 Port ID Subtype     : MAC Address
 Port ID             : 00-40-66-22-22-22
 Create Time         : 3/5/2020  16:25:56
 Remain Time         : 120 Seconds
```

各項目の説明は、以下のとおりです。

表 17-5 show voice vlan lldp-med device コマンドの表示項目

項番	説明
(1)	登録番号を表示します。
(2)	ポート番号またはポートチャネル番号を表示します。
(3)	LLDP-MED 端末から通知された、Chassis ID TLV のサブタイプを表示します。
(4)	LLDP-MED 端末から Chassis ID TLV で通知された、Chassis ID 情報を表示します。
(5)	LLDP-MED 端末から通知された、Port ID TLV のサブタイプを表示します。
(6)	LLDP-MED 端末から Port ID TLV で通知された、Port ID 情報を表示します。
(7)	登録された日時を表示します。
(8)	エージングタイムアウトまでの残り時間を表示します。

17.3 Voice VLAN の構成例と設定例

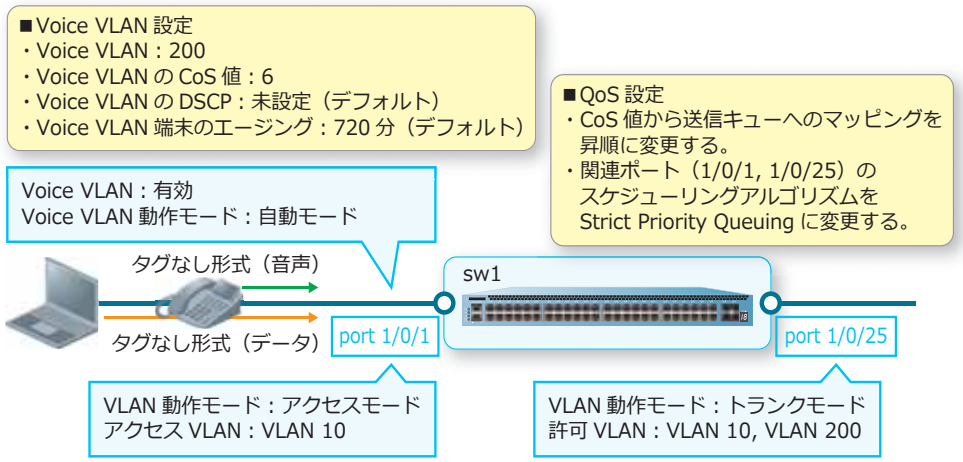
Voice VLAN を利用する場合の構成例と設定例を示します。

17.3.1 自動モード（untag）で使用する場合

自動モード（untag）で使用する場合の構成例と設定例を示します。この例では、音声トラフィックとデータトラフィックのどちらも、タグなし形式を想定しています。

- 音声トラフィックは Voice VLAN 200 で収容し、CoS 値を 6 に設定する。
- データトラフィックは VLAN 10 で収容し、CoS 値はポートのデフォルト CoS 値のままとする。
- 音声トラフィックと判断する MAC アドレスに、00:40:66:XX:XX:XX（XX は任意）を追加する。
- ポート 1/0/1 で、Voice VLAN を自動モード（untag）（デフォルト設定）で有効にする。
- CoS 値から送信キューへのマッピングを昇順に変更する。
- 関連ポート（1/0/1, 1/0/25）のスケジューリングアルゴリズムを、Strict Priority Queuing に変更する。

図 17-6 自動モード（untag）で使用する場合の構成例



1. CoS 値から送信キューへのマッピングを昇順に変更するために、以下のように設定します。なお、デフォルト設定の場合は省略しています。

・送信キュー 0 に、CoS 値 =0 を関連付ける

・送信キュー 1 に、CoS 値 =1 を関連付ける

・送信キュー 2 に、CoS 値 =2 を関連付ける

```
sw1# configure terminal
sw1(config)# priority-queue cos-map 0 0
sw1(config)# priority-queue cos-map 1 1
sw1(config)# priority-queue cos-map 2 2
sw1(config)#
```

2. 関連ポート（1/0/1, 1/0/25）で、スケジューリングアルゴリズムを Strict Priority Queuing に設定します。

```
sw1(config)# interface range port 1/0/1,1/0/25
sw1(config-if-port-range)# mls qos scheduler sp
sw1(config-if-port-range)# exit
sw1(config)#
```

3. VLAN 10、VLAN 200 を作成します。

```
sw1(config)# vlan 10,200
sw1(config-vlan)# exit
sw1(config)#
```

4. 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)#
```

5. ポート 1/0/25 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 200］を割り当てます。

```
sw1(config)# interface port 1/0/25
sw1(config-if-port)# switchport mode trunk
sw1(config-if-port)# switchport trunk allowed vlan 10,200
sw1(config-if-port)# exit
sw1(config)#
```

6. 音声トラフィックと判断する MAC アドレスとして、OUI=00:40:66:00:00:00、MASK=FF:FF:FF:00:00:00、名称 =Apresia を追加します。

```
sw1(config)# voice vlan mac-address 0040.6600.0000 ffff.ff00.0000 description
Apresia
sw1(config)#
```

7. Voice VLAN を［VLAN 200］に指定して有効にします。また、Voice VLAN の CoS 値を［6］に設定します。

```
sw1(config)# voice vlan 200
sw1(config)# voice vlan qos 6
sw1(config)#
```

8. ポート 1/0/1 で、Voice VLAN を自動モード（untag）（デフォルト設定）で有効にします。

```
sw1(config)# interface port 1/0/1
sw1(config-if-port)# voice vlan mode auto untag
sw1(config-if-port)# voice vlan enable
sw1(config-if-port)# end
sw1#
```

9. 実施後の Voice VLAN 設定を確認します。

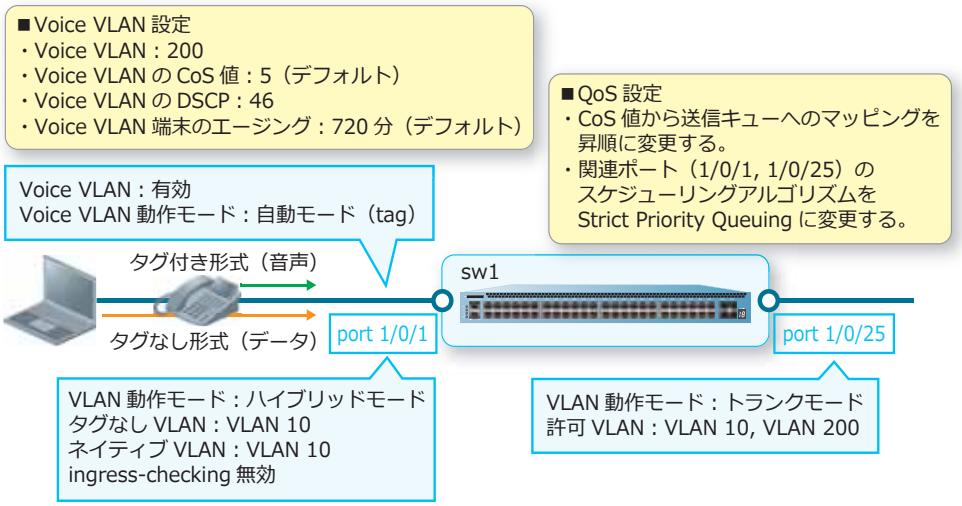
```
sw1# show voice vlan

 Voice VLAN ID         : 200
 Voice VLAN CoS        : 6
 Dscp                  : Disable
 Aging Time            : 720 minutes
 Member Ports          : 1/0/25
 Dynamic Member Ports  :

 Voice VLAN OUI        :

 OUI Address         Mask                Description
 ------------------  ------------------  --------------
 00-01-E3-00-00-00   FF-FF-FF-00-00-00   Siemens
 00-03-6B-00-00-00   FF-FF-FF-00-00-00   Cisco
 00-09-6E-00-00-00   FF-FF-FF-00-00-00   Avaya
 00-0F-E2-00-00-00   FF-FF-FF-00-00-00   Huawei&3COM
 00-40-66-00-00-00   FF-FF-FF-00-00-00   Apresia
 00-60-B9-00-00-00   FF-FF-FF-00-00-00   NEC&Philips
 00-D0-1E-00-00-00   FF-FF-FF-00-00-00   Pingtel
 00-E0-75-00-00-00   FF-FF-FF-00-00-00   Veritel
 00-E0-BB-00-00-00   FF-FF-FF-00-00-00   3COM

 Total OUI: 9
```

17.3.2 自動モード（tag）で使用する場合

自動モード（tag）で使用する場合の構成例と設定例を示します。この例では、音声トラフィックはタグ付き形式、データトラフィックはタグなし形式を想定しています。

- 音声トラフィックは Voice VLAN 200 で収容し、CoS 値を 5（デフォルト設定）、DSCP を 46 に設定する。
- データトラフィックは VLAN 10 で収容し、CoS 値はポートのデフォルト CoS 値のままとする。
- ポート 1/0/1 で、Voice VLAN を自動モード（tag）で有効にする。
- CoS 値から送信キューへのマッピングを昇順に変更する。
- 関連ポート（1/0/1, 1/0/25）のスケジューリングアルゴリズムを、Strict Priority Queuing に変更する。
- 自動モード（tag）に設定するポート 1/0/1 で、ingress-checking を無効にする。

図 17-7 自動モード（tag）で使用する場合の構成例



1. CoS 値から送信キューへのマッピングを昇順に変更するために、以下のように設定します。なお、デフォルト設定の場合は省略しています。

・送信キュー 0 に、CoS 値 =0 を関連付ける

・送信キュー 1 に、CoS 値 =1 を関連付ける

・送信キュー 2 に、CoS 値 =2 を関連付ける

```
sw1# configure terminal
sw1(config)# priority-queue cos-map 0 0
sw1(config)# priority-queue cos-map 1 1
sw1(config)# priority-queue cos-map 2 2
sw1(config)#
```

2. 関連ポート（1/0/1, 1/0/25）で、スケジューリングアルゴリズムを Strict Priority Queuing に設定します。

```
sw1(config)# interface range port 1/0/1,1/0/25
sw1(config-if-port-range)# mls qos scheduler sp
sw1(config-if-port-range)# exit
sw1(config)#
```

3. VLAN 10、VLAN 200 を作成します。

```
sw1(config)# vlan 10,200
sw1(config-vlan)# exit
sw1(config)#
```

4. ポート 1/0/1 をハイブリッドポートとして設定し、タグなし VLAN に［VLAN 10］を割り当てます。また、ネイティブ VLAN を［VLAN 10］に設定します。

```
sw1(config)# interface port 1/0/1
sw1(config-if-port)# switchport mode hybrid
sw1(config-if-port)# switchport hybrid allowed vlan untagged 10
sw1(config-if-port)# switchport hybrid native vlan 10
sw1(config-if-port)# exit
sw1(config)#
```

5. ポート 1/0/25 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 200］を割り当てます。

```
sw1(config)# interface port 1/0/25
sw1(config-if-port)# switchport mode trunk
sw1(config-if-port)# switchport trunk allowed vlan 10,200
sw1(config-if-port)# exit
sw1(config)#
```

6. Voice VLAN を［VLAN 200］に指定して有効にします。また、Voice VLAN の DSCP を［46］に設定します。

```
sw1(config)# voice vlan 200
sw1(config)# voice vlan dscp 46
sw1(config)#
```

7. ポート 1/0/1 で、Voice VLAN を自動モード（tag）で有効にします。また、ingress-checking を無効にします。

```
sw1(config)# interface port 1/0/1
sw1(config-if-port)# voice vlan mode auto tag
sw1(config-if-port)# voice vlan enable
sw1(config-if-port)# no ingress-checking
sw1(config-if-port)# end
#
```

8. 実施後の Voice VLAN 設定を確認します。

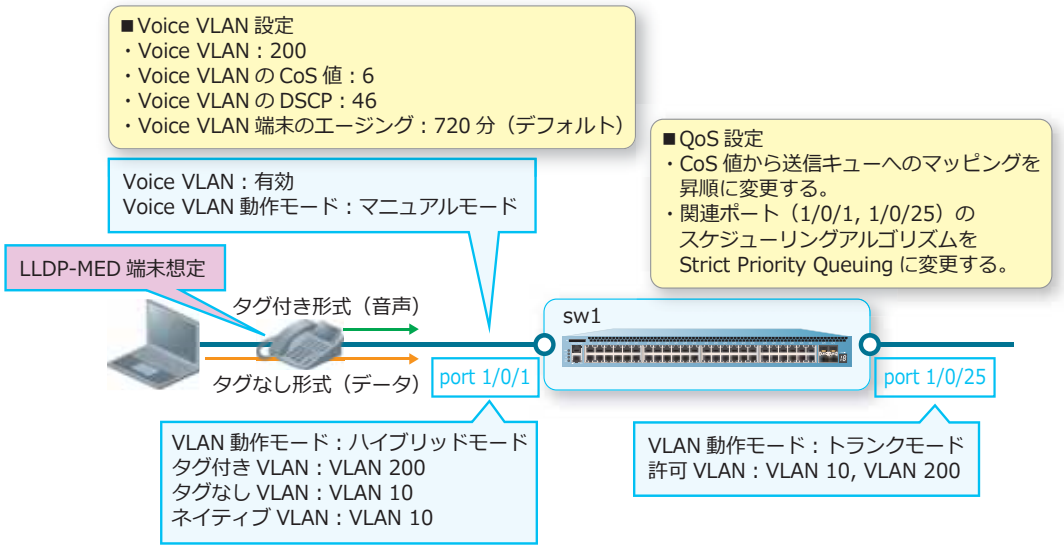
```
sw1# show voice vlan
 Voice VLAN ID         : 200
 Voice VLAN CoS        : 5
 Dscp                  : 46
 Aging Time            : 720 minutes
 Member Ports          : 1/0/25
 Dynamic Member Ports  :

 Voice VLAN OUI        :

 OUI Address         Mask                Description
 ------------------  ------------------  --------------
 00-01-E3-00-00-00   FF-FF-FF-00-00-00   Siemens
 00-03-6B-00-00-00   FF-FF-FF-00-00-00   Cisco
 00-09-6E-00-00-00   FF-FF-FF-00-00-00   Avaya
 00-0F-E2-00-00-00   FF-FF-FF-00-00-00   Huawei&3COM
 00-60-B9-00-00-00   FF-FF-FF-00-00-00   NEC&Philips
 00-D0-1E-00-00-00   FF-FF-FF-00-00-00   Pingtel
 00-E0-75-00-00-00   FF-FF-FF-00-00-00   Veritel
 00-E0-BB-00-00-00   FF-FF-FF-00-00-00   3COM

 Total OUI: 8
```

17.3.3 LLDP-MED による端末登録を使用する場合

LLDP-MED による端末登録を使用する場合の構成例と設定例を示します。この例では、音声トラフィックはタグ付き形式、データトラフィックはタグなし形式を想定しています。

- IP 電話は LLDP-MED 端末として登録することを想定する。Voice VLAN を VLAN 200、Voice VLAN の CoS 値を 6、DSCP を 46 に設定する。LLDP-MED Capabilities TLV と LLDP-MED Network Policy TLV を有効にして LLDP-MED により通知する。
- データトラフィックは VLAN 10 で収容し、CoS 値はポートのデフォルト CoS 値のままとする。
- ポート 1/0/1 で、Voice VLAN をマニュアルモードで有効にする。
- CoS 値から送信キューへのマッピングを昇順に変更する。
- 関連ポート（1/0/1, 1/0/25）のスケジューリングアルゴリズムを、Strict Priority Queuing に変更する。
- LLDPDU の送信間隔などの LLDP 関連パラメーターはデフォルト設定のままとする。

図 17-8 LLDP-MED による端末登録を使用する場合の構成例



1. CoS 値から送信キューへのマッピングを昇順に変更するために、以下のように設定します。なお、デフォルト設定の場合は省略しています。

・送信キュー 0 に、CoS 値 =0 を関連付ける

・送信キュー 1 に、CoS 値 =1 を関連付ける

・送信キュー 2 に、CoS 値 =2 を関連付ける

```
sw1# configure terminal
sw1(config)# priority-queue cos-map 0 0
sw1(config)# priority-queue cos-map 1 1
sw1(config)# priority-queue cos-map 2 2
sw1(config)#
```

2. 関連ポート（1/0/1, 1/0/25）で、スケジューリングアルゴリズムを Strict Priority Queuing に設定します。

```
sw1(config)# interface range port 1/0/1,1/0/25
sw1(config-if-port-range)# mls qos scheduler sp
sw1(config-if-port-range)# exit
sw1(config)#
```

3. VLAN 10、VLAN 200 を作成します。

```
sw1(config)# vlan 10,200
sw1(config-vlan)# exit
sw1(config)#
```

4. ポート 1/0/1 をハイブリッドポートとして設定し、タグ付き VLAN に［VLAN 200］、タグなし VLAN に［VLAN 10］を割り当てます。また、ネイティブ VLAN を［VLAN 10］に設定します。

```
sw1(config)# interface port 1/0/1
sw1(config-if-port)# switchport mode hybrid
sw1(config-if-port)# switchport hybrid allowed vlan tagged 200
sw1(config-if-port)# switchport hybrid allowed vlan untagged 10
sw1(config-if-port)# switchport hybrid native vlan 10
sw1(config-if-port)# exit
sw1(config)#
```

5. ポート 1/0/25 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 200］を割り当てます。

```
sw1(config)# interface port 1/0/25
sw1(config-if-port)# switchport mode trunk
sw1(config-if-port)# switchport trunk allowed vlan 10,200
sw1(config-if-port)# exit
sw1(config)#
```

6. LLDP を有効にします。また、ポート 1/0/1 で、LLDP-MED Capabilities TLV と LLDP-MED Network Policy TLV を有効にします。

```
sw1(config)# lldp run
sw1(config)# interface port 1/0/1
sw1(config-if-port)# lldp med-tlv-select capabilities
sw1(config-if-port)# lldp med-tlv-select network-policy
sw1(config-if-port)# exit
sw1(config)#
```

7. Voice VLAN を［VLAN 200］に指定して有効にします。また、Voice VLAN の CoS 値を［6］、DSCP を［46］に設定します。

```
sw1(config)# voice vlan 200
sw1(config)# voice vlan qos 6
sw1(config)# voice vlan dscp 46
sw1(config)#
```

8. ポート 1/0/1 で、Voice VLAN をマニュアルモードで有効にします。

```
sw1(config)# interface port 1/0/1
sw1(config-if-port)# voice vlan mode manual
sw1(config-if-port)# voice vlan enable
sw1(config-if-port)# end
sw1#
```

9. 実施後の Voice VLAN 設定を確認します。

```
sw1# show voice vlan

 Voice VLAN ID         : 200
 Voice VLAN CoS        : 6
 Dscp                  : 46
 Aging Time            : 720 minutes
 Member Ports          : 1/0/1,1/0/25
 Dynamic Member Ports  :

 Voice VLAN OUI        :

 OUI Address         Mask                Description
 ------------------  ------------------  --------------
 00-01-E3-00-00-00   FF-FF-FF-00-00-00   Siemens
 00-03-6B-00-00-00   FF-FF-FF-00-00-00   Cisco
 00-09-6E-00-00-00   FF-FF-FF-00-00-00   Avaya
 00-0F-E2-00-00-00   FF-FF-FF-00-00-00   Huawei&3COM
 00-60-B9-00-00-00   FF-FF-FF-00-00-00   NEC&Philips
 00-D0-1E-00-00-00   FF-FF-FF-00-00-00   Pingtel
 00-E0-75-00-00-00   FF-FF-FF-00-00-00   Veritel
 00-E0-BB-00-00-00   FF-FF-FF-00-00-00   3COM

 Total OUI: 8
```

18. ポートセキュリティー

ポートセキュリティーの機能、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。

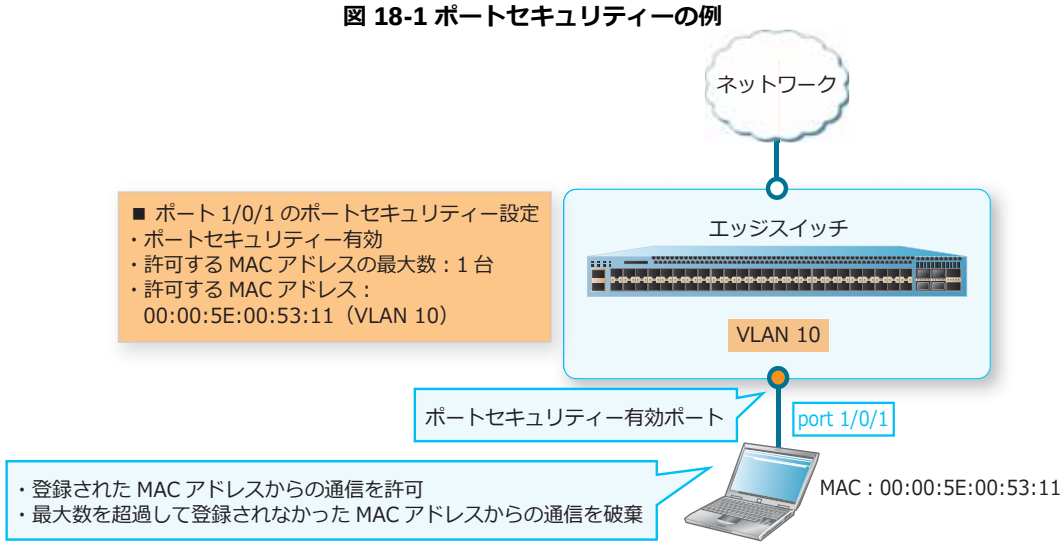
18.1 ポートセキュリティーの機能説明

ポートセキュリティーは、ネットワークの入り口であるエッジスイッチのポートにおいて、登録された MAC アドレスからの通信のみを許可し、許可しない MAC アドレス（最大数を超過して登録されなかった MAC アドレス）からの通信を破棄する機能です。

CAUTION: ポートセキュリティー機能は、AccessDefender による認証が有効なポートや、ポートチャネルのメンバーポートでは併用できません。

NOTE: ポートセキュリティーは、NP5000 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。

図 18-1 ポートセキュリティーの例



ポートセキュリティーの有効化

ポートセキュリティーは、デフォルト設定では無効です。ポートセキュリティーを有効にするには、**`switchport port-security`** コマンドを使用します。

許可する MAC アドレスの装置全体の最大数の設定

ポートセキュリティーで許可する MAC アドレスの装置全体の最大数は、デフォルト設定では未設定です。未設定時は、最大設定値の 12,288 で動作します。許可する MAC アドレスの装置全体の最大数を設定するには、**`port-security limit global`** コマンドを使用します。

許可しない MAC アドレス（最大数を超過して登録されなかった MAC アドレス）からの通信を受信した場合の動作がログ出力される設定の場合、装置全体の最大数を超過したことを検知すると、それを知らせるログが出力されます。

許可する MAC アドレスのポートごとの最大数の設定

ポートセキュリティーで許可する MAC アドレスのポートごとの最大数は、デフォルト設定では 32 です。許可する MAC アドレスのポートごとの最大数を設定するには、**switchport port-security maximum** コマンドを使用します。

許可しない MAC アドレス（最大数を超過して登録されなかった MAC アドレス）からの通信を受信した場合の動作がログ出力される設定の場合、ポートごとの最大数を超過したことを検知すると、それを知らせるログが出力されます。

許可する MAC アドレスの設定

許可する MAC アドレスは、デフォルト設定では未設定です。許可する MAC アドレスを設定するには、**switchport port-security mac-address** コマンドを使用します。

> ***NOTE:*** 許可する MAC アドレスとして、同一エントリー（同じ MAC アドレス／同じ VLAN ID）を複数ポートに登録することはできません。

許可しない MAC アドレスからの通信を受信した場合の動作設定

許可しない MAC アドレス（最大数を超過して登録されなかった MAC アドレス）からの通信を受信した場合の動作は、以下のいずれかに設定できます。動作を設定するには、**switchport port-security violation** コマンドを使用します。

- protect：許可しない MAC アドレスからの通信を破棄（デフォルト設定）
- restrict：許可しない MAC アドレスからの通信を破棄、CPU カウンターでカウント、ログ出力
- shutdown：対象ポートをシャットダウン（err-disabled 状態に変更）、ログ出力

ポートセキュリティーで手動または動的に登録されたエントリーは、**show port-security address** コマンドで確認します。

> ***NOTE:*** ポートセキュリティーで登録されたエントリーは、**show mac-address-table** コマンドでも「タイプ：Static」のエントリーとして表示されますが、スタティック MAC アドレスエントリーとは別扱いのため、**show mac-address-table static** コマンドでは表示されません。

18.1.1 許可する MAC アドレスの手動設定

許可する MAC アドレスを手動で設定するには、通常は permanent パラメーターを指定しない形式で **switchport port-security mac-address** コマンドを設定します。permanent パラメーター未指定のエントリー設定は、**clear port-security** コマンドの削除対象外です。

18.1.2 動的に登録されるエントリーの動作設定

ポートセキュリティーを有効にしたポートで、許可する MAC アドレスのポートごとの最大数まで空きがある状態では、受信した順に最大数まで許可する MAC アドレスとして動的に登録されます。

> ***NOTE:*** 許可する MAC アドレスを動的に登録させない場合は、許可する MAC アドレスのポートごとの最大数を、**switchport port-security mac-address** コマンドでスタティックに設定した許可する MAC アドレスの数に設定して使用してください。

動的に登録されるエントリーの動作モードは、以下のいずれかに設定できます。動作モードを設定するには、**switchport port-security mode** コマンドを使用します。

- delete-on-timeout：エージングタイムアウト対象にするモード
- permanent：エージングタイムアウトの対象外にするモード

delete-on-timeout モードの場合、動的に登録されたエントリーはエージングタイムアウト対象になります。エージングタイムは、デフォルト設定では 0 分（エージングタイムアウト無効）です。変更するには、**switchport port-security aging time** コマンドを使用します。また、エージングタイムのタイプは、デフォルト設定では「エントリーが登録されてからの経過時間」です。変更するには、**switchport port-security aging type** コマンドを使用します。

permanent モードの場合、動的に登録されたエントリーはエージングタイムアウトの対象外になります。動的に登録されると、running-config にもエントリー設定（permanent パラメーター指定の **switchport port-security mac-address** コマンド設定）が自動的に追加されます。この状態で設定を保存すると、次回起動時にもエントリー設定を引き継ぐことができます。

動的に登録されたエントリーを削除するには、**clear port-security** コマンドを使用します。**clear port-security** コマンドを実行すると、permanent パラメーター指定の **switchport port-security mac-address** コマンド設定も running-config から削除されます。

18.1.3 インターフェースの復旧

許可しない MAC アドレス（最大数を超過して登録されなかった MAC アドレス）からの通信を受信した場合の動作が、ポートをシャットダウン（err-disabled 状態に変更）する設定の場合、err-disabled 状態に変更されたポートを復旧するには、以下の 2 つの方法があります。

自動復旧設定

errdisable recovery cause psecure-violation コマンドを使用して、ポートセキュリティー機能によって err-disabled 状態に変更されたポートの自動復旧を有効にできます。自動復旧設定を有効にすると、err-disabled 状態に変更されたポートは、指定した時間の経過後に自動的に復旧します。以下に自動復旧の設定例を示します。

```
(config)# errdisable recovery cause psecure-violation interval 300
```

コマンドによる手動復旧手順

err-disabled 状態に変更されたポートに対して **shutdown** コマンドを実行した後、**no shutdown** コマンドを実行することで、手動でポートを復旧できます。以下にコマンド実行例を示します。

```
(config)# interface port 1/0/1
(config-if-port)# shutdown
(config-if-port)# no shutdown
```

18.2 ポートセキュリティーの状態確認

ポートセキュリティーの状態を表示して確認する方法を説明します。

18.2.1 ポートセキュリティーの情報の表示

show port-security コマンドでポートセキュリティーの情報を確認できます。

表示例を以下に示します。

```
# show port-security

D:Delete-on-Timeout    P:Permanent
(1)          (2)  (3)    (4)          (5)          (6)       (7)      (8)
Interface    Max  Curr   Violation    Violation    Security  Admin    Current
No.          No.  No.    Act.         Count        Mode      State    State
------------ ----- ----- -------- -------------------- -- -------- ------------
Port1/0/1    2     2     Shutdown -                    P  Enabled  Forwarding
Port1/0/2    1     1     Restrict 2485                 D  Enabled  Forwarding
Port1/0/3    32    1     Protect  -                    D  Enabled  Forwarding
Port1/0/4    32    0     Protect  -                    D  Disabled -
Port1/0/5    32    0     Protect  -                    D  Disabled -
～～省略～～
```

各項目の説明は、以下のとおりです。

表 18-1 show port-security 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)	ポートセキュリティー機能で許可する MAC アドレスの、ポートごとの最大数を表示します。
(3)	現時点で登録されているエントリー数を表示します。
(4)	許可しない MAC アドレス（最大数を超過して登録されなかった MAC アドレス）からの通信を受信した場合の動作を表示します。 • Protect：許可しない MAC アドレスからの通信を破棄 • Restrict：許可しない MAC アドレスからの通信を破棄、CPU カウンターでカウント、ログ出力 • Shutdown：対象ポートをシャットダウン（err-disabled 状態に変更）、ログ出力
(5)	許可しない MAC アドレスからの通信を受信した場合の動作が Restrict の場合に、CPU カウンターでカウントした許可しない MAC アドレスからのパケット数を表示します。CPU 宛てに中継されなかったパケットはカウントされません。
(6)	動的に登録されるエントリーの動作モードを表示します。 • D：動的に登録されたエントリーがエージングタイムアウトするモード • P：動的に登録されたエントリーがエージングタイムアウトしないモード
(7)	ポートセキュリティー機能の有効 (Enabled) ／無効 (Disabled) を表示します。
(8)	ポートの状態を表示します。 • Forwarding：ポートセキュリティー機能が有効な状態 • Err-disabled：シャットダウン（err-disabled 状態に変更）された状態 • -：ポートセキュリティー機能が無効な状態

18.2.2 ポートセキュリティーのエントリーの表示

show port-security address コマンドでポートセキュリティーのエントリーを確認できます。

表示例を以下に示します。

```
# show port-security address
(1)          (2)     (3)                (4)                (5)
Interface    VLAN ID MAC Address        Address Type       Remaining Time
                                                               (mins)
------------ ------- ------------------ ------------------ --------------
Port1/0/1    20      00-00-5E-00-53-11 Permanent          -    (I)
Port1/0/1    20      00-00-5E-00-53-22 Permanent          -    (I)
Port1/0/2    30      00-00-5E-00-53-AA Delete-on-Timeout 476
Port1/0/3    50      00-00-5E-00-53-BB Delete-on-Timeout 18   (I)

Total Entries: 4
```

各項目の説明は、以下のとおりです。

表 18-2 show port-security address 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)	VLAN ID を表示します。
(3)	MAC アドレスを表示します。
(4)	エントリーのタイプを表示します。 • Permanent：**switchport port-security mac-address** コマンドで設定したエントリー、または動的に登録されて自動的に設定された permanent パラメーター指定のエントリー • Delete-on-Timeout：delete-on-timeout モードのポートで動的に登録されたエントリー
(5)	エージングタイムアウトまでの残り時間を表示します。 エントリーのタイプが Permanent の場合は、残り時間は表示されません。 エージングタイムのタイプが inactivity タイプの場合、残り時間の後ろに (I) が表示されます。また、対象エントリーが無通信になったと判断する前の状態では、残り時間は表示されません。

18.2.3 自動復旧設定の表示

show errdisable recovery コマンドで、自動復旧設定を確認できます。

> ***NOTE:*** ErrDisable Cause 項目の Port Security は、ポートセキュリティーをサポートしている機種でのみ表示されます。

表示例を以下に示します。

```
# show errdisable recovery
(1)                                  (2)           (3)
ErrDisable Cause                     State         Interval
-----------------------------------  ------------  -------------
Port Security                        disabled      300 seconds
Storm Control                        enabled       300 seconds
Loop Detection                       enabled       300 seconds
ULD                                  disabled      300 seconds

Interfaces that will be recovered at the next timeout:
(4)          (1)                                  (5)
Interface    Errdisable Cause                     Time left(sec)
---------    -----------------------------------  --------------
Port1/0/1    Port Security                        52
```

各項目の説明は、以下のとおりです。

表 18-3 show errdisable recovery コマンドの表示項目

項番	説明
(1)	検知の要因となった機能を表示します。 • Loop Detection：ループ検知機能 • Storm Control：ストームコントロール機能 • ULD：単方向リンク検出機能 • Port Security：ポートセキュリティー機能
(2)	自動復旧設定の有効 (enabled) ／無効 (disabled) を表示します。
(3)	ポートが自動復旧されるまでの時間設定を表示します。
(4)	err-disabled 状態に変更されたポートを表示します。
(5)	err-disabled 状態に変更されたポートが自動復旧されるまでの残り時間を表示します。

18.3 ポートセキュリティーの構成例と設定例

ポートセキュリティーを利用する場合の構成例と設定例を示します。

18.3.1 手動で登録した MAC アドレスのみ許可する場合

手動で登録した MAC アドレスのみを許可する場合の構成例と設定例を示します。

- ポート 1/0/1 で、ポートごとの許可する MAC アドレスの最大数を 1 個に設定して、ポートセキュリティーを有効にする。また、許可する MAC アドレスとして 00:00:5E:00:53:11（VLAN 10）を登録する。
- ポート 1/0/2 で、ポートごとの許可する MAC アドレスの最大数を 2 個に設定して、ポートセキュリティーを有効にする。また、許可する MAC アドレスとして 00:00:5E:00:53:21（VLAN 20）、00:00:5E:00:53:22（VLAN 20）を登録する。
- ポート 1/0/1 とポート 1/0/2 で、許可しない MAC アドレス（最大数を超過して登録されなかった MAC アドレス）からの通信を受信した場合の動作を restrict（許可しない MAC アドレスからの通信を破棄、CPU カウンターでカウント、ログ出力）に設定する。

1. ポート 1/0/1 で以下の設定を実施して、ポートセキュリティーを有効にします。

・ポートごとの許可する MAC アドレスの最大数は 1 個

・許可する MAC アドレスは 00:00:5E:00:53:11（VLAN 10）

・許可しない MAC アドレスからの通信受信時の動作は restrict

```
sw1# configure terminal
sw1(config)# interface port 1/0/1
sw1(config-if-port)# switchport port-security maximum 1
sw1(config-if-port)# switchport port-security mac-address 00:00:5e:00:53:11
vlan 10
sw1(config-if-port)# switchport port-security violation restrict
sw1(config-if-port)# switchport port-security
sw1(config-if-port)# exit
sw1(config)#
```

2. ポート 1/0/2 で以下の設定を実施して、ポートセキュリティーを有効にします。

・ポートごとの許可する MAC アドレスの最大数は 2 個

・許可する MAC アドレスは 00:00:5E:00:53:21（VLAN 20）、00:00:5E:00:53:22（VLAN 20）

・許可しない MAC アドレスからの通信受信時の動作は restrict

```
sw1(config)# interface port 1/0/2
sw1(config-if-port)# switchport port-security maximum 2
sw1(config-if-port)# switchport port-security mac-address 00:00:5e:00:53:21
vlan 20
sw1(config-if-port)# switchport port-security mac-address 00:00:5e:00:53:22
vlan 20
sw1(config-if-port)# switchport port-security violation restrict
sw1(config-if-port)# switchport port-security
sw1(config-if-port)# end
sw1#
```

3. 実施後のポートセキュリティー設定を確認します。

```
sw1# show port-security interface range port 1/0/1-2

 D:Delete-on-Timeout P:Permanent
 Interface    Max  Curr   Violation    Violation   Security  Admin   Current
 No.          No.   No.     Act.       Count           Mode  State   State
 ------------ ----- ----- -------- -------------------- -- -------- ------------
 Port1/0/1    1     1     Restrict 0                    D  Enabled  Forwarding
 Port1/0/2    2     2     Restrict 0                    D  Enabled  Forwarding

sw1#
sw1# show port-security interface range port 1/0/1-2 address

 Interface    VLAN ID MAC Address       Address Type      Remaining Time
                                                              (mins)
 ------------ ------- ----------------- ----------------- --------------
 Port1/0/1    10      00-00-5E-00-53-11 Permanent         -
 Port1/0/2    20      00-00-5E-00-53-21 Permanent         -
 Port1/0/2    20      00-00-5E-00-53-22 Permanent         -

 Total Entries: 3

sw1#
```

4. 実施後のポートセキュリティー関連の設定を以下に抜粋します。

```
# PORT-SECURITY

interface port 1/0/1
 switchport port-security
 switchport port-security maximum 1
 switchport port-security violation restrict
 switchport port-security mac-address 00-00-5E-00-53-11 vlan 10
interface port 1/0/2
 switchport port-security
 switchport port-security maximum 2
 switchport port-security violation restrict
 switchport port-security mac-address 00-00-5E-00-53-21 vlan 20
 switchport port-security mac-address 00-00-5E-00-53-22 vlan 20
```

18.3.2 手動または動的に登録した MAC アドレスを許可する場合

手動または動的に登録した MAC アドレスを許可する場合の構成例と設定例を示します。

- ポート 1/0/1 で、ポートごとの許可する MAC アドレスの最大数を 10 個に設定して、ポートセキュリティーを有効にする。また、許可する MAC アドレスとして 00:00:5E:00:53:11（VLAN 10）を登録する。
- ポート 1/0/1 で、動的に登録される MAC アドレスの動作モードを delete-on-timeout（デフォルト設定）にする。また、エージングタイムは 60 分、エージングタイムのタイプは inactivity（無通信になったと判断されてから指定したエージングタイムが経過すると削除されるモード）に設定する。
- ポート 1/0/1 で、許可しない MAC アドレス（最大数を超過して登録されなかった MAC アドレス）からの通信を受信した場合の動作を protect（デフォルト設定、許可しない MAC アドレスからの通信を破棄）に設定する。

1. ポート 1/0/1 で以下の設定を実施して、ポートセキュリティーを有効にします。なお、デフォルト設定の場合は省略しています。

・ポートごとの許可する MAC アドレスの最大数は 10 個

・許可する MAC アドレスは 00:00:5E:00:53:11（VLAN 10）

・動的に登録されるエントリーの動作モードは delete-on-timeout（デフォルト設定）

・動的に登録されたエントリーのエージングタイムは 60 分

・動的に登録されたエントリーのエージングタイムのタイプは inactivity

・許可しない MAC アドレスからの通信受信時の動作は protect（デフォルト設定）

```
sw1# configure terminal
sw1(config)# interface port 1/0/1
sw1(config-if-port)# switchport port-security maximum 10
sw1(config-if-port)# switchport port-security mac-address 00:00:5e:00:53:11
vlan 10
sw1(config-if-port)# switchport port-security aging time 60
sw1(config-if-port)# switchport port-security aging type inactivity
sw1(config-if-port)# switchport port-security
sw1(config-if-port)# end
sw1#
```

2. 実施後のポートセキュリティー設定を確認します。

```
sw1# show port-security interface port 1/0/1

 D:Delete-on-Timeout P:Permanent
 Interface    Max  Curr   Violation    Violation   Security  Admin   Current
 No.          No.   No.     Act.       Count           Mode  State   State
 ------------ ----- ----- -------- -------------------- -- -------- ------------
 Port1/0/1    10    1     Protect  -                    D  Enabled  Forwarding

sw1#
sw1# show port-security interface port 1/0/1 address

 Interface    VLAN ID MAC Address       Address Type      Remaining Time
                                                              (mins)
 ------------ ------- ----------------- ----------------- --------------
 Port1/0/1    10      00-00-5E-00-53-11 Permanent         -    (I)

 Total Entries: 1

sw1#
```

3. 実施後のポートセキュリティー関連の設定を以下に抜粋します。

```
# PORT-SECURITY

interface port 1/0/1
 switchport port-security
 switchport port-security maximum 10
 switchport port-security aging time 60
 switchport port-security aging type inactivity
 switchport port-security mac-address 00-00-5E-00-53-11 vlan 10
```

18.3.3 MAC アドレス学習数の上限のみ設定する場合

許可する MAC アドレスは指定せずに、MAC アドレス学習数の上限のみ設定する場合の構成例と設定例を示します。

- ポートセキュリティーで許可する MAC アドレスの装置全体の最大数を 20 個に設定する。
- ポート 1/0/1 で、ポートごとの許可する MAC アドレスの最大数を 10 個に設定して、ポートセキュリティーを有効にする。
- ポート 1/0/2 で、ポートごとの許可する MAC アドレスの最大数を 15 個に設定して、ポートセキュリティーを有効にする。
- ポート 1/0/1 とポート 1/0/2 で、動的に登録される MAC アドレスの動作モードを delete-on-timeout（デフォルト設定）にする。また、エージングタイムは 480 分、エージングタイムのタイプは absolute（デフォルト設定、登録されてから指定したエージングタイムが経過すると削除されるモード）に設定する。
- ポート 1/0/1 とポート 1/0/2 で、許可しない MAC アドレス（最大数を超過して登録されなかった MAC アドレス）からの通信を受信した場合の動作を restrict（許可しない MAC アドレスからの通信を破棄、CPU カウンターでカウント、ログ出力）に設定する。

1. ポートセキュリティーで許可する MAC アドレスの装置全体の最大数を 20 個に設定します。

```
sw1# configure terminal
sw1(config)# port-security limit global 20
sw1(config)#
```

2. ポート 1/0/1 で以下の設定を実施して、ポートセキュリティーを有効にします。なお、デフォルト設定の場合は省略しています。

・ポートごとの許可する MAC アドレスの最大数は 10 個

・動的に登録されるエントリーの動作モードは delete-on-timeout（デフォルト設定）

・動的に登録されたエントリーのエージングタイムは 480 分

・動的に登録されたエントリーのエージングタイムのタイプは absolute（デフォルト設定）

・許可しない MAC アドレスからの通信受信時の動作は restrict

```
sw1(config)# interface port 1/0/1
sw1(config-if-port)# switchport port-security maximum 10
sw1(config-if-port)# switchport port-security aging time 480
sw1(config-if-port)# switchport port-security violation restrict
sw1(config-if-port)# switchport port-security
sw1(config-if-port)# exit
sw1(config)#
```

3. ポート 1/0/2 で以下の設定を実施して、ポートセキュリティーを有効にします。なお、デフォルト設定の場合は省略しています。

・ポートごとの許可する MAC アドレスの最大数は 15 個

・動的に登録されるエントリーの動作モードは delete-on-timeout（デフォルト設定）

・動的に登録されたエントリーのエージングタイムは 480 分

・動的に登録されたエントリーのエージングタイムのタイプは absolute（デフォルト設定）

・許可しない MAC アドレスからの通信受信時の動作は restrict

```
sw1(config)# interface port 1/0/2
sw1(config-if-port)# switchport port-security maximum 15
sw1(config-if-port)# switchport port-security aging time 480
sw1(config-if-port)# switchport port-security violation restrict
sw1(config-if-port)# switchport port-security
sw1(config-if-port)# end
sw1#
```

4. 実施後のポートセキュリティー設定を確認します。

```
sw1# show port-security interface range port 1/0/1-2

 D:Delete-on-Timeout P:Permanent
 Interface    Max  Curr   Violation    Violation   Security  Admin   Current
 No.          No.  No.      Act.       Count           Mode  State   State
 ------------ ----- ----- -------- -------------------- -- -------- ------------
 Port1/0/1    10    0     Restrict 0                    D  Enabled  Forwarding
 Port1/0/2    15    0     Restrict 0                    D  Enabled  Forwarding

sw1#
```

5. 実施後のポートセキュリティー関連の設定を以下に抜粋します。

```
# PORT-SECURITY

port-security limit global 20
interface port 1/0/1
 switchport port-security
 switchport port-security maximum 10
 switchport port-security violation restrict
 switchport port-security aging time 480
interface port 1/0/2
 switchport port-security
 switchport port-security maximum 15
 switchport port-security violation restrict
 switchport port-security aging time 480
```

19. Egress フィルタリング

Egress フィルタリングの機能、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。

19.1 Egress フィルタリングの機能説明

Egress フィルタリングは、指定したフレームのハードウェア中継による送信を制限（破棄）する機能で、送信ポートごとに設定できます。指定可能なフレーム種別は以下の 3 種類です。

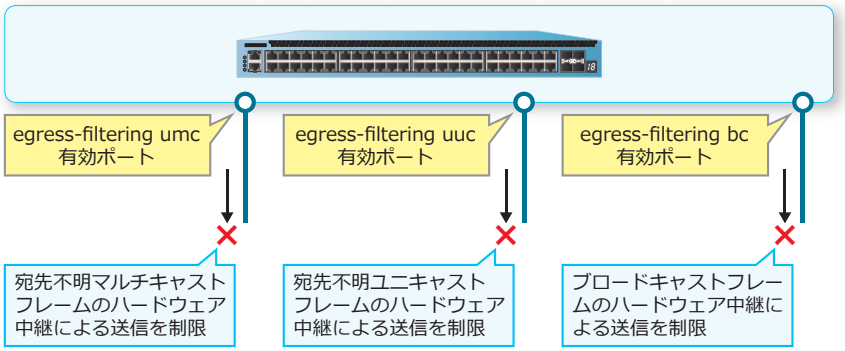
- 宛先不明マルチキャストフレーム
- 宛先不明ユニキャストフレーム
- ブロードキャストフレーム

NOTE: Egress フィルタリングは、NP7000 の 1.11.01 以降、NP5000 の 1.10.01 以降、NP2100 の 1.10.03 以降、NP2500 の 1.10.02 以降でサポートしています。

NOTE: Egress フィルタリングは MAC アドレスベースで処理されます。

NOTE: CPU から送信されるフレーム、および CPU によりソフトウェア中継されるフレームは Egress フィルタリングによる制限（破棄）の対象外です。

図 19-1 Egress フィルタリングの例



19.1.1 宛先不明マルチキャストフレームを対象にする場合

宛先不明マルチキャストフレームを指定して Egress フィルタリングを有効にするには、**egress-filtering umc** コマンドを使用します。

以下の機能で学習／設定したマルチキャストフレームは、Egress フィルタリングによる制限（破棄）の対象外です。

- IGMP スヌーピング、IGMP、PIM で学習した IPv4 マルチキャスト
- MLD スヌーピング、MLD、IPv6 PIM で学習した IPv6 マルチキャスト
- **mac-address-table static** コマンドで設定したマルチキャスト MAC アドレスエントリー

上記以外のマルチキャスト MAC アドレス宛てのフレームが対象になるため、上記に当てはまらない場合は予約 IPv4 マルチキャスト（224.0.0.0/24）、および予約 IPv6 マルチキャスト（ff02::/111, ff02::1:ff00:0/104, ff05::/111）でも対象になり、制限（破棄）されます。

ただし、IGMP スヌーピングを有効にした VLAN では、General Query（224.0.0.1 宛て）は egress-filtering umc を有効にしたポートからもソフトウェア中継で送信されます。同様に、MLD スヌーピングを有効にした VLAN では、Multicast Listener Query（ff02::1 宛て）は egress-filtering umc を有効にしたポートからもソフトウェア中継で送信されます。

> ***NOTE:*** 同一ポート／同一ポートチャネルで、**egress-filtering umc** コマンドと、「IGMP スヌーピングの **ip igmp snooping unregistered-filter** コマンド」または「MLD スヌーピングの **ipv6 mld snooping unregistered-filter** コマンド」の併用は未サポートです。

19.1.2 宛先不明ユニキャストフレームを対象にする場合

宛先不明ユニキャストフレーム（宛先 MAC アドレスが MAC アドレステーブルに登録されていないユニキャスト MAC アドレス）を指定して Egress フィルタリングを有効にするには、**egress-filtering uuc** コマンドを使用します。

19.1.3 ブロードキャストフレームを対象にする場合

ブロードキャストフレーム（宛先 MAC アドレスが FF:FF:FF:FF:FF:FF）を指定して Egress フィルタリングを有効にするには、**egress-filtering bc** コマンドを使用します。

19.2 Egress フィルタリングの状態確認

show egress-filtering コマンドで、Egress フィルタリングの設定を確認できます。

表示例を以下に示します。

```
# show egress-filtering umc

Unknown Multicast Egress Filtering: 1/0/3-1/0/4,1/0/6, port-channel5 ...(1)

# show egress-filtering uuc

Unknown Unicast Egress Filtering: 1/0/1,1/0/5 ...(2)

# show egress-filtering bc

Broadcast Egress Filtering: 1/0/1,1/0/3 ...(3)
```

各項目の説明は、以下のとおりです。

表 19-1 show egress-filtering コマンドの表示項目

項番	説明
(1)	宛先不明マルチキャストフレームの Egress フィルタリングを有効にしたポート番号およびポートチャネル番号を表示します。
(2)	宛先不明ユニキャストフレームの Egress フィルタリングを有効にしたポート番号およびポートチャネル番号を表示します。
(3)	ブロードキャストフレームの Egress フィルタリングを有効にしたポート番号およびポートチャネル番号を表示します。

19.3 Egress フィルタリングの構成例と設定例

Egress フィルタリングを使用する場合の構成例と設定例を示します。この例では以下のように設定しています。

- ポート 1/0/1、ポート 1/0/3、ポートチャネル 7（スタティックモード、メンバーポートはポート 1/0/7 と 1/0/8）で、宛先不明マルチキャストフレームを対象にした Egress フィルタリングを有効にする。
- ポート 1/0/1、ポート 1/0/2 で、宛先不明ユニキャストフレームを対象にした Egress フィルタリングを有効にする。
- ポート 1/0/9 で、ブロードキャストフレームを対象にした Egress フィルタリングを有効にする。

1. チャネルグループ ID［7］を指定して、スタティックモードでポートチャネルを設定します。

・メンバーポートはポート 1/0/7 とポート 1/0/8

```
sw1# configure terminal
sw1(config)# interface range port 1/0/7-8
sw1(config-if-port-range)# channel-group 7 mode on
sw1(config-if-port-range)# exit
sw1(config)#
```

2. ポート 1/0/1、ポート 1/0/3、ポートチャネル 7 で、宛先不明マルチキャストフレームを指定して Egress フィルタリングを有効にします。

```
sw1(config)# interface range port 1/0/1,1/0/3
sw1(config-if-port-range)# egress-filtering umc
sw1(config-if-port-range)# exit
sw1(config)# interface port-channel 7
sw1(config-if-port-channel)# egress-filtering umc
sw1(config-if-port-channel)# exit
sw1(config)#
```

3. ポート 1/0/1、ポート 1/0/2 で、宛先不明ユニキャストフレームを指定して Egress フィルタリングを有効にします。

```
sw1(config)# interface range port 1/0/1-2
sw1(config-if-port-range)# egress-filtering uuc
sw1(config-if-port-range)# exit
sw1(config)#
```

4. ポート 1/0/9 で、ブロードキャストフレームを指定して Egress フィルタリングを有効にします。

```
sw1(config)# interface port 1/0/9
sw1(config-if-port)# egress-filtering bc
sw1(config-if-port)# end
sw1#
```

5. 実施後の Egress フィルタリング設定を確認します。

```
sw1# show egress-filtering umc

Unknown Multicast Egress Filtering: 1/0/1,1/0/3, port-channel7

sw1# show egress-filtering uuc

Unknown Unicast Egress Filtering: 1/0/1-1/0/2

sw1# show egress-filtering bc

Broadcast Egress Filtering: 1/0/9

sw1#
```

6. 実施後の Egress フィルタリング関連の設定を以下に抜粋します。

```
# EGRESS-FILTERING

interface port 1/0/1
 egress-filtering umc
 egress-filtering uuc
interface port 1/0/2
 egress-filtering uuc
interface port 1/0/3
 egress-filtering umc
interface port 1/0/9
 egress-filtering bc
interface port-channel 7
 egress-filtering umc
```