GVT-273553-001-00 6.0

QX-S5800X シリーズ Ethernet スイッチ
マニュアル訂正資料

本資料について

この資料は、以下に示す QX-S5800X シリーズ Ethernet スイッチに関するマニュアルからの変更内容を記載しています。

マニュアル	マニュアル番号	内容
QX-S5800X シリーズ Ethernet スイッチ インスタレーションマニュアル	GVT-088696-001-00 1.6	システムのインストールについて説明しています。
QX-S5800X シリーズ Ethernet スイッチ オペレーションマニュアル	GVT-088697-001-00 1.10	機能の設定について説明しています。
QX-S5800X シリーズ Ethernet スイッチ コマンドマニュアル	GVT-088698-001-00 1.7	機能に関するコマンドについて説明しています。

発行

２０２６年５月（６版）

改版履歴

版数	日付	内容
1.0	2026/1/14	初版発行
2.0	2026/1/19	#10697、#10886、#13735、#14289、#15848 を追加
3.0	2026/1/26	#17318、#17267 を追加
4.0	2026/2/24	#16909 を追加
5.0	2026/3/31	#16840、#19346、#19603、#20212 を追加
6.0	2026/5/25	#17933 を追加

目次

1章 QX-S5800X シリーズ Ethernet スイッチ インスタレーションマニュアル

5 章 IRF スタックの設定

5.3 IRF スタックの基本的な設定

■管理情報

区分	管理番号
追加	#11724

■内容

変更前）

・基本的な IRF スタックの設定を確認するため、display irf configuration コマンドを実行してください。

変更後）

・基本的な IRF スタックの設定を確認するため、display irf configuration コマンドを実行してください。

・system view の設定はすべての IRF スタックメンバで同じ設定にすることを推奨します（slot 指定コマンドを除く）。

・switch-mode コマンドおよび max-ecmp-num コマンドは、すべての IRF スタックメンバで同じ設定にしてください。異なる場合は IRF スタックを構築できません。

8.13 IRF スタックの設定(IRF スタック構成時)

■管理情報

区分	管理番号
追加	#11724

■内容

変更前)

オプション設定の項目は、未設定ではデフォルト値が使用されます。お客様、または SE 部門から情報が入手できない場合など、もともとデフォルト値を利用している場合は、改めて設定する必要はありません。

変更後)

オプション設定の項目は、未設定ではデフォルト値が使用されます。お客様、または SE 部門から情報が入手できない場合など、もともとデフォルト値を利用している場合は、改めて設定する必要はありません。

メモ

IRF を構築する際は以下に注意をしてください。

・system view の設定はすべての IRF スタックメンバで同じ設定にすることを推奨します(slot 指定コマンドを除く)。

・switch-mode コマンドおよび max-ecmp-num コマンドは、すべての IRF スタックメンバで同じ設定にしてください。異なる場合は IRF スタックを構築できません。

2章 QX-S5800X シリーズ Ethernet スイッチ オペレーションマニュアル

02-IRF スタック

1.5 IRF スタックユニットの設定

■管理情報

区分	管理番号
追加	#11724

■内容

変更前）

1.5.　IRF スタックユニットの設定

変更後）

1.5.　IRF スタックユニットの設定

⚠ 重要

IRF を構築する際は以下に注意をしてください。

・system view の設定はすべての IRF スタックメンバで同じ設定にすることを推奨します (slot 指定コマンドを除く)。

・switch-mode コマンドおよび max-ecmp-num コマンドは、すべての IRF スタックメンバで同じ設定にしてください。異なる場合は IRF スタックを構築できません。

1.6.3 BFD MAD の設定

Ⅰ. 制限とガイドライン

■管理情報

区分	管理番号
変更	#10301

■内容

変更前）

VLAN インタフェースで BFD MAD を設定するとき、以下の制限とガイドラインに従ってください。

カテゴリ	制限とガイドライン
BFD MAD VLAN	・VLAN インタフェース 1 で、BFD MAD を有効にすることはできません。 ・中継装置を使用する場合、以下の作業を行ってください。 ・IRF スタックユニットと中継装置で BFD MAD の VLAN と VLAN インタフェースを作成してください。 ・IRF スタックユニットと中継装置で BFD MAD の VLAN に BFD MAD のポートを関連付けてください。 ・IRF スタックユニットで BFD MAD VLAN の VLAN インタフェースを作成してください。 ・ネットワークの IRF スタックユニットは異なる BFD MAD の VLAN を使用してください。 ・正しいトラフィックの転送を行うため、BFD MAD VLAN は BFD MAD リンクのポートのみを使用してください。もし BFD MAD リンクのポートでない場合、BFD MAD VLAN からのポートを取り除いてください。 port trunk permit vlan all コマ ンドですべての VLAN にポートが割り当てられている場合、 BFD MAD VLAN からポートを除外するため、undo port trunk permit コマンドを使用してください。

変更後）

VLAN インタフェースで BFD MAD を設定するとき、以下の制限とガイドラインに従ってください。

カテゴリ	制限とガイドライン
BFD MAD VLAN	・VLAN インタフェース 1 で、BFD MAD を有効にすることはできません。 ・中継装置を使用する場合、以下の作業を行ってください。 ・IRF スタックユニットと中継装置で BFD MAD の VLAN と VLAN インタフェースを作成してください。 ・IRF スタックユニットと中継装置で BFD MAD の VLAN に BFD MAD のポートを関連付けてください。 ・IRF スタックユニットで BFD MAD VLAN の VLAN インタフェースを作成してください。 ・ネットワークの IRF スタックユニットは異なる BFD MAD の VLAN を使用してください。 ・正しいトラフィックの転送を行うため、BFD MAD VLAN は BFD MAD リンクのポートのみを使用してください。もし BFD MAD リンクのポートでない場合、BFD MAD VLAN からのポートを取り除いてください。port trunk permit vlan all コマ ンドですべての VLAN にポートが割り当てられている場合、 BFD MAD VLAN からポートを除外するため、undo port trunk permit コマンドを使用してください。

03-アクセス

8.30.7 BPDU ドロップ機能の有効化

Ⅱ. 制限とガイドライン

■管理情報

区分	管理番号
追加	#10301

■内容

この問題を回避するため、ポートで BPDU ドロップ機能を有効にします。BPDU ドロップ機能が有効になったポートでは、BPDU の受信を行わず、BPDU 攻撃による影響を受けません。

この機能を使用することで、装置は以下の BPDU パケットをドロップします。

・EOAM

・GVRP

・LACP

・LLDP

・PVST

・STP（STP、RSTP、MSTP を含みます）

9.3 ループ検出の有効化

■管理情報

区分	管理番号
変更	#15848

■内容

変更前）

9.3.1. 制限とガイドライン

ループ検出を有効にするときは、次の制限事項とガイドラインに従ってください。

ループ検出はグローバルあるいは指定されたポートで有効にすることができます。ポートが VLAN で検出フレームを受信すると、ループの検出が有効かどうかに関係なく、そのポートでループ保護アクションが起動されます。

変更後）

9.3.1. 制限とガイドライン

ループ検出を有効にするときは、次の制限事項とガイドラインに従ってください。

- ループ検出はグローバルあるいはポート単位で有効にすることができます。指定のポートのみループ検出を有効化する場合は、グローバルの設定を無効に設定してください。
- ループ検出はポートで有効化されている VLAN の検出フレームを受信すると、受信したポートのループ検出が有効かどうかに関係なく、そのポートで指定したループ保護アクションが動作します。
- リンクアグリゲーションポート単位にループ検出を有効化する場合は、リンクアグリゲーショングループの論理ポート（aggregate interface view）にループ検出の設定をする必要があります。メンバポートに設定しても動作しません。

14.2. 制限とガイドライン

■管理情報

区分	管理番号
変更	#16909

■内容

変更前）

VLAN タグをパケットに追加するには、VLAN マッピングと QinQ の両方を設定できます。 VLAN マッピングは、設定の重複が発生した場合に有効になります。 QinQ の詳細については、セクション 3 アクセス オペレーションマニュアルの"QinQ"を参照してください。
パケットに VLAN タグを追加または置換するには、VLAN マッピングと QoS ポリシーの両方を設定できます。 QoS ポリシーは、設定の重複が発生した場合に有効になります。QoS ポリシーの詳細はセクション 8 ACL and QoS オペレーションマニュアルの"QoS ポリシー"を参照してください。

変更後）

VLAN タグをパケットに追加するには、VLAN マッピングと QinQ の両方を設定できます。 VLAN マッピングは、設定の重複が発生した場合に有効になります。 QinQ の詳細については、オペレーションマニュアルのセクション 3 アクセス "QinQ"を参照してください。
パケットに VLAN タグを追加または置換するには、VLAN マッピングと QoS ポリシーの両方を設定できます。 QoS ポリシーは、設定の重複が発生した場合に有効になります。QoS ポリシーの詳細はオペレーションマニュアルのセクション 8 ACL and QoS "QoS ポリシー"を参照してください。
VLAN マッピングを適用したインタフェースを経由し､かつ VLAN マッピング対象の VLAN インタフェースを経由する L3 通信は未サポートです。
VLAN マッピング対象の VLAN に VLAN インタフェースを作成および IP アドレスを設定する場合は、L3 通信の経路（送受信インタフェース）には VLAN マッピングを適用しないでください。

14.2. 制限とガイドライン

■管理情報

区分	管理番号
変更	#16840

■内容

変更前）

VLAN タグをパケットに追加するには、VLAN マッピングと QinQ の両方を設定できます。 VLAN マッピングは、設定の重複が発生した場合に有効になります。 QinQ の詳細については、セクション 3 アクセス オペレーションマニュアルの"QinQ"を参照してください。
パケットに VLAN タグを追加または置換するには、VLAN マッピングと QoS ポリシーの両方を設定できます。 QoS ポリシーは、設定の重複が発生した場合に有効になります。QoS ポリシーの詳細はセクション 8 ACL and QoS オペレーションマニュアルの"QoS ポリシー"を参照してください。

変更後）

VLAN タグをパケットに追加するには、VLAN マッピングと QinQ の両方を設定できます。 VLAN マッピングは、設定の重複が発生した場合に有効になります。 QinQ の詳細については、セクション 3 アクセス オペレーションマニュアルの"QinQ"を参照してください。
パケットに VLAN タグを追加または置換するには、VLAN マッピングと QoS ポリシーの両方を設定できます。 QoS ポリシーは、設定の重複が発生した場合に有効になります。QoS ポリシーの詳細はセクション 8 ACL and QoS オペレーションマニュアルの"QoS ポリシー"を参照してください。

DHCP スヌーピングとの併用はできません。

15 章 LLDP

■管理情報

区分	管理番号
追加	#17933

■内容

15.13. MAC アドレス借用の設定

15.13.1. 受信した管理アドレス TLV の ARP または ND エントリの生成の有効化

I. 受信した管理アドレス TLV の ARP または ND エントリの生成

この機能により、装置はインタフェースで管理アドレス TLV を含む LLDP フレームを受信した後に ARP または ND エントリを生成できます。ARP または ND エントリは、アドバタイズされた管理アドレスをフレームの送信元アドレスにマッピングします。

インタフェースで ARP エントリと ND エントリの両方の生成を有効にできます。

管理アドレス TLV に IPv4 アドレスが含まれている場合、装置は ARP エントリを生成します。管理アドレス TLV に IPv6 アドレスが含まれている場合、装置は ND エントリを生成します。

Layer 2 Ethernet interface view では、この機能によりレイヤ 2 Ethernet インタフェースが、生成されたエントリの出力インタフェースに設定されます。エントリが属する VLAN は、この機能で指定された VLAN です。次のいずれかの状況では、装置は ARP または ND エントリを生成できません。

・指定された VLAN または対応する VLAN インタフェースが存在しません。

・VLAN ID が属する VLAN インタフェースが物理的にダウンしています。

Layer 3 Ethernet interface view では、vlan vlan-id を指定するかどうかに関係なく、レイヤ 3 Ethernet インタフェースが出力インタフェースとして記録されます。

I. 制限とガイドライン

この機能は、次の要件を満たすように LLDP フレームの送信元 MAC アドレスを設定する機能を使用して設定する必要があります。

・装置は、LLDP フレームの送信元 MAC アドレスとして、出力インタフェースの MAC アドレスではなく VLAN インタフェースの MAC アドレスを使用します。

・ネイバ装置は、正しい ARP または ND エントリを生成できます。

III. 設定手順

操作	コマンド	補足
1.system view に移行する	**system-view**	ー
2.Layer 2 または Layer 3 Ethernet interface view に移行する	**interface** interface-type interface-number	ー
3.インタフェースで受信した管理アドレス TLV の ARP または ND エントリの生成を有効にする	・Layer 2 Ethernet interface view: **lldp management-address** { **arp-learning** | **nd-learning** } **vlan** vlan-id ・Layer 3 Ethernet interface view: **lldp management-address** { **arp-learning** | **nd-learning** } [**vlan** vlan-id]	**デフォルト：無効** Layer 2 Ethernet interface view で、vlan vlan-id は生成された ARP または ND エントリが属する VLAN ID を指定します。ARP または ND エントリが相互に上書きしないようにするために、異なるレイヤ 2 Ethernet インタフェースに同じ VLAN ID を指定しないでください。 インタフェースで ARP エントリと ND エントリの両方の生成を有効にできます。

04-IP サービス

■管理情報

区分	管理番号
追加	#17933

■内容

5 章 ARP direct route advertisement

5.1. ARP direct route advertisement

5.1.1. ARP direct route advertisement のメカニズム

この機能は、パケット転送とルートアドバタイズメントの ARP エントリに基づいてダイレクトルートを生成します。

5.1.2. レイヤ 3 アクセスネットワークにおけるアプリケーション

図 5-1 に示すように、この機能はアドバタイズするルーティングプロトコルのために、Server A へのダイレクトルートと Server B へのホストルートを生成します。
したがって、各装置はネットワーク内のサーバに送信されるトラフィックだけを転送するため、帯域幅が節約されます

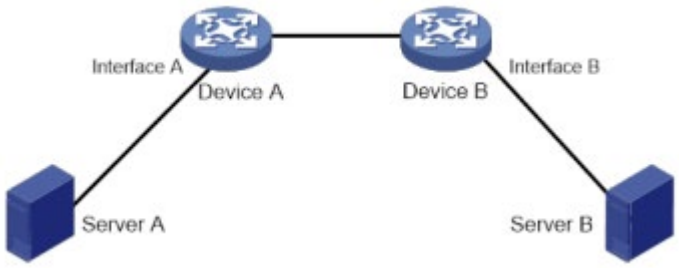


図 5-1 レイヤ 3 アクセスネットワーク内のアプリケーション

5.2. ARP direct route advertisement の有効化

操作	コマンド	補足
1.system view に移行する	**system-view**	ー
2.interface view に移行する	**Interface** interface-type interface-number	ー
3. ARP ダイレクトルートアドバタイズメントを有効にする	**arp route-direct advertise** [**preference** preference-value | **tag** tag-value] *	デフォルト：無効

5 章 IP アドレス

■管理情報

区分	管理番号
追加	#17933

■内容

5.3. IP アンナンバードの設定

他のインタフェースから IP アドレスを借用するようにインタフェースを設定できます。

これを IP アンナンバードと呼び、IP アドレスを借用しているインタフェースを IP アンナンバードインタフェースと呼びます。

IP アンナンバードを使用すると、使用可能な IP アドレスが不十分な場合や、インタフェースがごくたまにしか使用されない場合に、IP アドレスを保存できます。

I. 制限とガイドライン

・ループバックインタフェースは他のインタフェースの IP アドレスを借用できませんが、他のインタフェースはループバックインタフェースの IP アドレスを借用できます。

・インタフェースは、アンナンバードインタフェースから IP アドレスを借りることはできません。

・複数のインタフェースが同じアンナンバード IP アドレスを使用できます。

・インタフェースに手動で設定された IP アドレスが複数ある場合は、手動で設定されたプライマリ IP アドレスだけを借用できます。

・IP アンナンバードが設定されているインタフェースでは、ダイナミックルーティングプロトコルを有効にできません。インタフェースが他の装置と通信できるようにするには、インタフェース上のピア装置へのスタティックルートを設定します。

II. 前提条件

IP アドレスを借用するインタフェースに IP アドレスを設定します。

インタフェースに手動で IP アドレスを割り当てるか、BOOTP、または DHCP を介して IP アドレスを取得するようにインタフェースを設定できます。

III. 設定手順

操作	コマンド	補足
1.system view に移行する	**system-view**	ー
2.interface view に移行する	**Interface** interface-type interface-number	ー
3.指定したインタフェー スの IP アドレスを借用するインタフェースを指定する	**ip address unnumbered interface** interface-type interface-number	デフォルト：設定なし

10.2 制限とガイドライン

■管理情報

区分	管理番号
変更	#16840

■内容

変更前）

・レイヤ 2 Ethernet インタフェース、アグリゲートインタフェース、レイヤ 3 Ethernet インタフェースは、トラステッドポートとして指定できます。アグリゲートインタフェースの詳細は、セクション 3 アクセス オペレーションマニュアルの”リンクアグリゲーション”を参照してください。

変更後）

・レイヤ 2 Ethernet インタフェース、アグリゲートインタフェース、レイヤ 3 Ethernet インタフェースは、トラステッドポートとして指定できます。アグリゲートインタフェースの詳細は、セクション 3 アクセス オペレーションマニュアルの”リンクアグリゲーション”を参照してください。

・VLAN マッピングとの併用はできません。

05-ルーティングプロトコル

5.7.9 デフォルトルートの再配信の設定

II. 設定手順

■管理情報

区分	管理番号
変更	#14289

■内容

変更前）

操作	コマンド	補足
3. デフォルトルートを再配信するように設定する	**default-route-advertise** [[[**always** | **permit-calculate-other**] | **cost** *cost* | **route-policy** *route-policy-name* | **type** *type*] * | **summary cost** *cost*]	デフォルト：再配信されません。 このコマンドは VPN のみ設定可能です。 PE ルータは CE ルータに Type-3 LSA でデフォルトルートを配信します。

変更後）

操作	コマンド	補足
3. デフォルトルートを再配信するように設定する	**default-route-advertise** [[[**always** | **permit-calculate-other**] | **cost** *cost* | **route-policy** *route-policy-name* | **type** *type*] * | **summary cost** *cost*]	デフォルト：再配信されません。 このコマンドは Type-5 LSA（summary cost 指定時は Type-3 LSA）のデフォルトルートを再配信します。

7.4.2. インタフェース PBR のポリシーの設定

制限とガイドライン

■管理情報

区分	管理番号
変更	#17318

■内容

変更前）

指定されるポリシーはすでに作成されている必要があります。インタフェースには 1 つのポリシーのみ適用することができます。新しいポリシーを適用する前にインタフェースから現在のポリシーを削除してください。

複数のインタフェースにポリシーを適用することができます。

変更後）

指定されるポリシーはすでに作成されている必要があります。インタフェースには 1 つのポリシーのみ適用することができます。新しいポリシーを適用する前にインタフェースから現在のポリシーを削除してください。

複数のインタフェースで同じポリシーを適用することができます。

08-ACL and QoS

4.1. 概要

■管理情報

区分	管理番号
変更	#19346-1

■内容

変更前）

プライオリティマッピングはプライオリティマッピングテーブルに実装され、以下のプライオリティを決定します。

- 802.1p プライオリティ
- DSCP
- EXP
- IP プレシーデンス
- ローカルプレシーデンス
- ドロッププライオリティ

変更後）

プライオリティマッピングはプライオリティマッピングテーブルに実装され、以下のプライオリティを決定します。

- 802.1p プライオリティ
- DSCP
- IP プレシーデンス
- ローカルプレシーデンス

4.1.1. プライオリティ

■管理情報

区分	管理番号
変更	#19346-2

■内容

変更前）

パケットに含まれているプライオリティは、802.1p プライオリティ、DSCP プレシーデンス、IP プレシーデンス、EXP があります。パケットに含まれるプライオリティは、他の装置でも使用されるため、ネットワークに影響します。プライオリティの詳細はセクション 8 *ACL and QoS* オペレーションマニュアルの *"付録"* を参照してください。

ローカルに割り当てられたプライオリティは装置内でのみ使用されます。プライオリティはローカルプレシーデンス、ドロッププライオリティがあります。

- ローカルプレシーデンス－スケジューリング用に使用されます。ローカルプレシーデンスの値は出力キューに対応します。ローカルプレシーデンスの値が高いパケットが高い出力キューに割り当てられます。
- ドロッププライオリティ－パケットの廃棄を行うために使用します。ドロッププライオリティの値が高いパケットを優先的に廃棄します。
- ユーザプライオリティ－装置が自動で転送するパスに従いパケットのプライオリティフィールドから優先度を決定します。パケットのスケジューリングプライオリティと転送プライオリティを決定します。ユーザプライオリティは以下のアイテムを示します。
  - レイヤ 2 パケットの 802.1p プライオリティ
  - レイヤ 3 パケットの IP プレシーデンス

QX-S5800X シリーズはローカルプレシーデンス、ドロッププライオリティのみサポートします。

変更後）

パケットに含まれているプライオリティは、802.1p プライオリティ、DSCP プレシーデンス、IP プレシーデンスがあります。パケットに含まれるプライオリティは、他の装置でも使用されるため、ネットワークに影響します。プライオリティの詳細はオペレーションマニュアルのセクション 8 *ACL and QoS* ”*付録*”を参照してください。

- ユーザプライオリティ－転送するパスに従い装置が自動でパケットのプライオリティフィールドから優先度を決定します。パケットのスケジューリングプライオリティと転送プライオリティを決定します。ユーザプライオリティは以下のアイテムを示します。
  - レイヤ 2 パケットの 802.1p プライオリティ
  - レイヤ 3 パケットの IP プレシーデンス、DSCP

ローカルに割り当てられたプライオリティは装置内でのみ使用されます。プライオリティはローカルプレシーデンスがあります。

- ローカルプレシーデンス－スケジューリング用に使用されます。ローカルプレシーデンスの値は出力キューに対応します。ローカルプレシーデンスの値が高いパケットが高い出力キューに割り当てられます。

4.1.4. プライオリティのマッピング手順

■管理情報

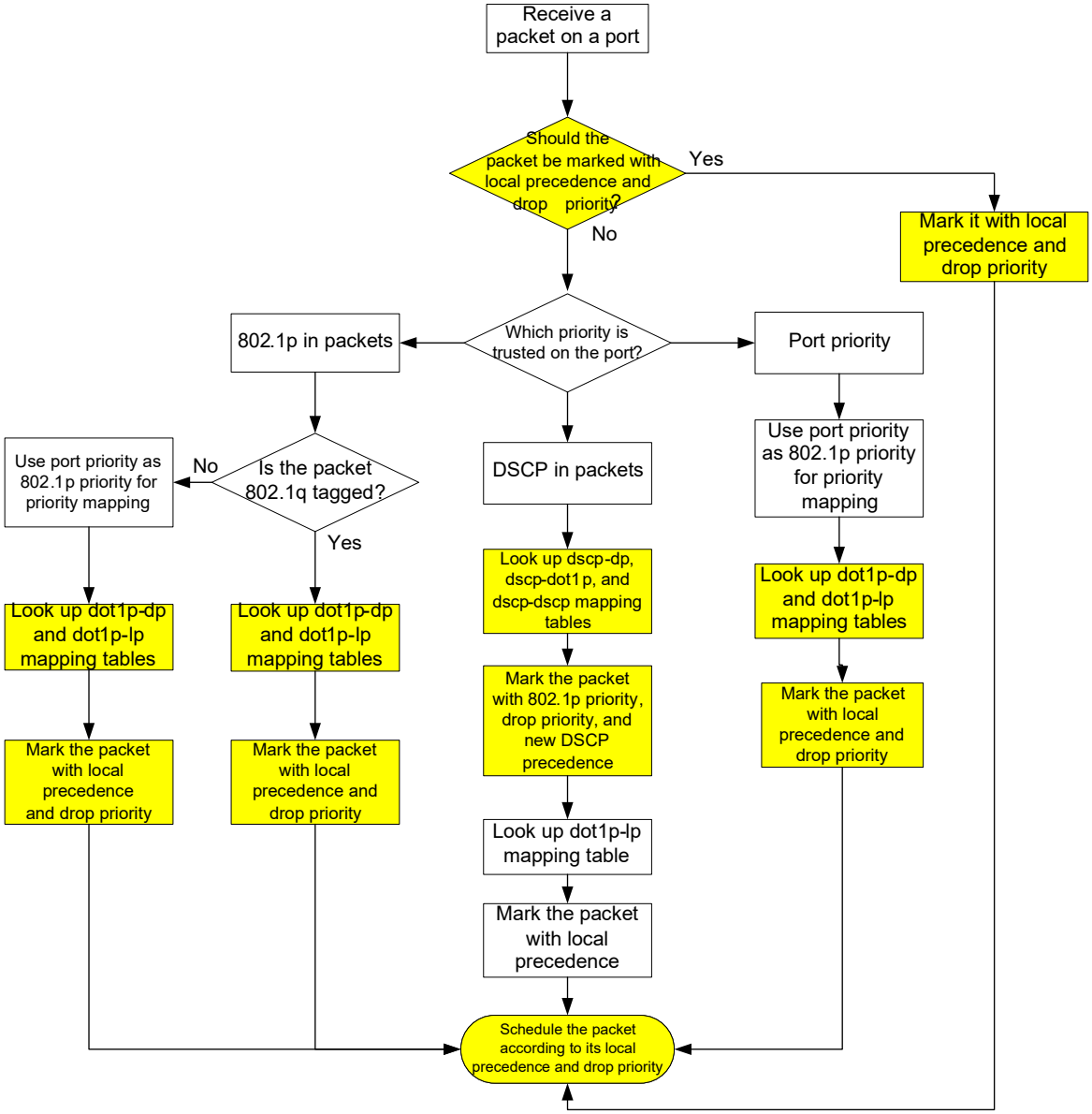
区分	管理番号
変更	#19346-3

■内容

変更前）

ポートでイーサネットパケットを受信した際、スイッチはパケットのプライオリティのスケジューリング（ローカルプレシーデンス、ドロッププレシーデンス）をマーキングします。プレシーデンスは、図 4-1 のように受信したポートのプライオリティトラステッドモードとパケットの 802.1Q タギング状態に従って行われます。

図 4-1 イーサネットパケットのプライオリティマッピング手順

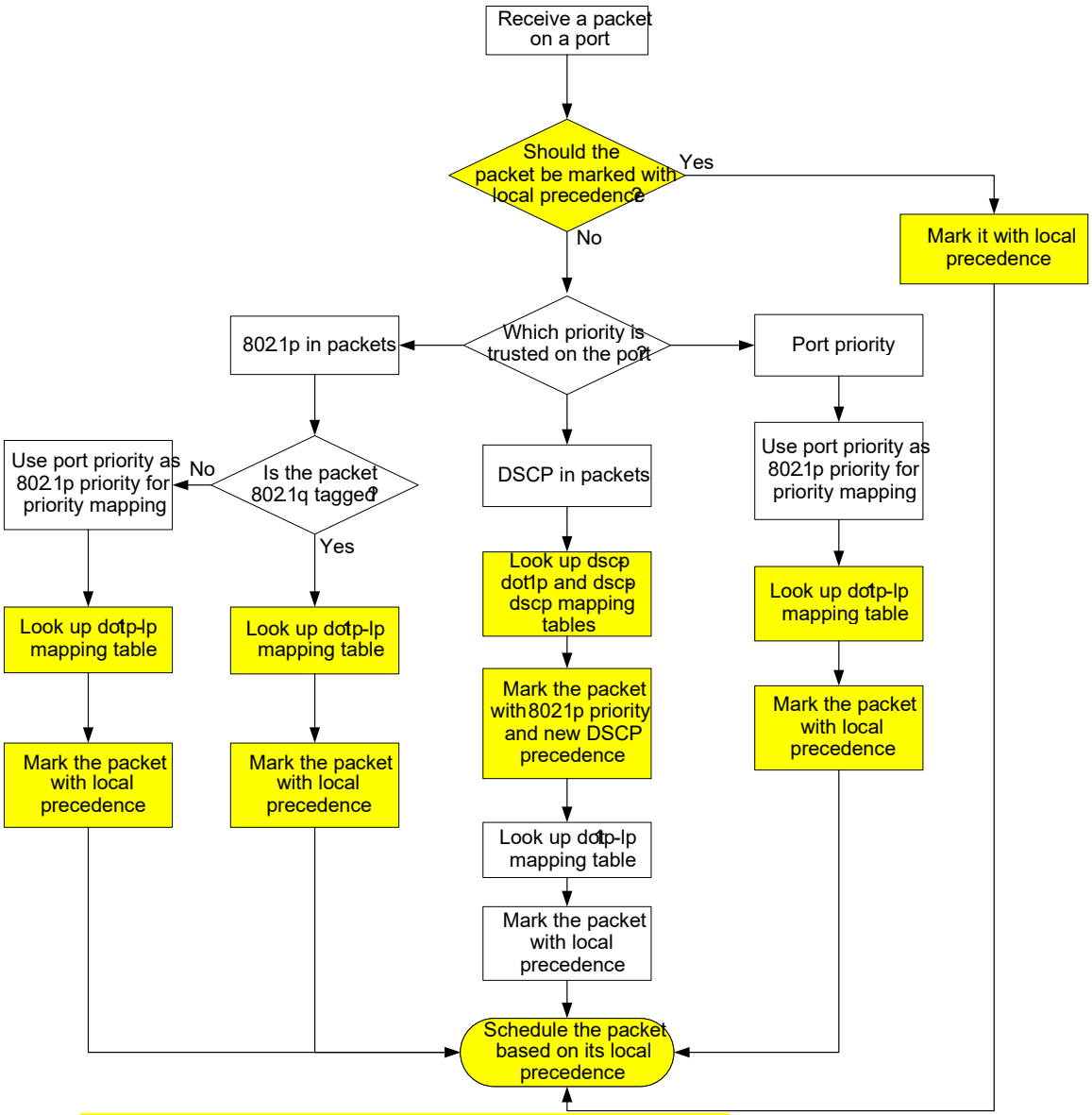


詳細は、セクション 8 *ACL and QoS オペレーションマニュアルの"プライオリティマーキング"*を参照してください。

変更後）

ポートでイーサネットパケットを受信した際、スイッチはパケットのプライオリティのスケジューリング（ローカルプレシーデンス）をマーキングします。プレシーデンスは、図 4-1 のように受信したポートのプライオリティトラステッドモードとパケットの 802.1Q タギング状態に従って行われます

図 4-1 イーサネットパケットのプライオリティマッピング手順



詳細は、オペレーションマニュアルのセクション 8 *ACL and QoS* "*プライオリティマーキング*"を参照してください。

4.3. プライオリティマッピングの設定

■管理情報

区分	管理番号
変更	#19346-4

■内容

変更前）

操作	コマンド	補足
2. priority map view に移行する	**qos map-table** { **dot1p-dp** | **dot1p-lp** | **dscp-dot1p** | **dscp-dp** | **dscp-dscp** | **exp-dp** }	—
3. プライオリティマッピングを設定する	**import** *import-value-list* **export** *export-value*	デフォルト：デフォルトのプライオリティマップ 詳細は、セクション 8 *ACL and QoS オペレーションマニュアルの"付録"* を参照してください。 新規に設定した値は、既存の設定に上書きします。

変更後）

操作	コマンド	補足
2. priority map view に移行する	**qos map-table** { **dot1p-lp** | **dscp-dot1p** | **dscp-dscp** }	—
3. プライオリティマッピングを設定する	**import** *import-value-list* **export** *export-value*	デフォルト：デフォルトのプライオリティマップ 詳細は、オペレーションマニュアルのセクション 8 *ACL and QoS"付録"* を参照してください。 新規に設定した値は、既存の設定に上書きします。

4.6. プライオリティマッピングの表示と維持

■管理情報

区分	管理番号
変更	#19346-5

■内容

変更前）

すべての view で display コマンドを実行できます。

操作	コマンド
プライオリティマッピング の設定を表示する	**display qos map-table** { **dot1p-dp** | **dot1p-lp** | **dscp-dot1p** | **dscp-dp** | **dscp-dscp** | **exp-dp** }

変更後）

すべての view で display コマンドを実行できます。

操作	コマンド
プライオリティマッピング の設定を表示する	**display qos map-table** { **dot1p-lp** | **dscp-dot1p** | **dscp-dscp** }

14.2.1. プライオリティマップ

■管理情報

区分	管理番号
変更	#19346-6

■内容

変更前）

デフォルトの dot1p-exp、dscp-dscp プライオリティマップでは、入力した値と出力の値が同一と なります。

表 14-2 デフォルトの dot1p-lp、dot1p-dp プライオリティマップ

プライオリティの入力値	dot1p-lp マッピング	dot1p-dp マッピング
dot1p	lp	dp
0	2	0
1	0	0
2	1	0
	3	0
4	4	0
5	5	0
6	6	0
7	7	0

表 14-3 デフォルトの dscp-dp、dscp-dot1p プライオリティマップ

プライオリティの入力値	dscp-dp マッピング	dscp-dot1p マッピング
dscp	dp	dot1p
0 to 7	0	0
8 to 15	0	1
16 to 23	0	2
24 to 31	0	3
32 to 39	0	4
40 to 47	0	5
48 to 55	0	6
56 to 63	0	7

表 14-4 デフォルトの exp-dp プライオリティマップ

プライオリティの入力値	exp-dp マッピング
EXP 値	dp
0	0
1	0
2	0
3	0
4	0
5	0
6	0
7	0

表 14-5 Default port priority-local priority map デフォルトのポートプライオリティーローカルプライオリティマッピング

Port priority	ローカルプレシーデンス
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7

変更後）

デフォルトの dscp-dscp プライオリティマップでは、入力した値と出力の値が同一と なります。

表 14-2 デフォルトの dot1p-lp プライオリティマップ

プライオリティの入力値	**dot1p-lp マッピング**
dot1p	lp
0	2
1	0
2	1
	3
4	4
5	5
6	6
7	7

表 14-3 デフォルトの dscp-dot1p プライオリティマップ

プライオリティの入力値	**dscp-dot1p マッピング**
dscp	dot1p
0 to 7	0
8 to 15	1
16 to 23	2
24 to 31	3
32 to 39	4
40 to 47	5
48 to 55	6
56 to 63	7

表 14-4 デフォルトのポートプライオリティーローカルプライオリティマッピング

Port priority	**ローカルプレシーデンス**
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7

09-セキュリティ

4.1. 概要

■管理情報

区分	管理番号
追加	#20212

■内容

🕮 メモ：

QX-S5800X シリーズの MAC アドレス認証は CHAP での認証に対応していません。

15.9 ARP スキャンの設定

■管理情報

区分	管理番号
追加	#10697

■内容

15.9.1. ARP スキャンの設定

通常、ARP スキャンは、安定した小規模なネットワークで使用されます。

ARP スキャンは、アドレス範囲内の装置の ARP エントリを自動的に作成します。装置は以下の手順で ARP スキャンを実行します。

・アドレス範囲内の各 IP アドレスに ARP 要求を送信します。

・受信した ARP 応答から MAC アドレスを取得します。

・ダイナミック ARP エントリを作成します。

スキャン範囲に IP アドレスが多い場合は、ARP パケットの送信レートを設定できます。この設定により、ARP トラフィックのバーストが原因で CPU 使用率が高くなり、ネットワーク負荷が高くなるのを回避できます。

15.9.2. 制限とガイドライン

ARP テーブルに存在する IP アドレスはスキャンされません。

ARP スキャンには時間がかかります。実行中のスキャンを停止するには、Ctrl+C を押します。ダイナミック ARP エントリは、スキャンが終了する前に受信した ARP 応答に基づいて作成されます。

スタティック ARP エントリの合計数の制限により、ダイナミック ARP からの変換に失敗する場合があります。

ダイナミック ARP から変換されたスタティック ARP エントリを削除するには、undo arp ip-address コマンドを使用します。reset arp all コマンドを使用してすべての ARP エントリを削除することも、reset arp static コマンドを使用してすべてのスタティック ARP エントリを削除することもできます。

15.9.3. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. interface view に移行する	**interface** *interface-type interface-number*	—
2. ARP スキャンを開始する	**arp scan** [*start-ip-address* **to** *end-ip-address*] [**send-rate** { **ppm** *ppm* | *pps* }]	—

10-高可用性

4.3. RRPP の設定作業リスト

■管理情報

区分	管理番号
追加	#10886

■内容

注意

RRPP とループ検知機能を併用する場合は、RRPP リングを構成する各ノードのプライマリポートとセカンダリポートでループ保護アクションを設定しないで下さい。プライマリポートとセカンダリポートでループ保護アクションを設定すると、RRPP のノード上のどこかでループが発生したとき、ループ検知の保護アクションにより RRPP の Hello パケットが途切れて、マスタノードのセカンダリポートのブロックが解除されます。それにより、ループ検知の保護アクションが発生したノードのもう一方の RRPP ポートでも保護アクションが動作して自動復旧できなくなります。

3章 QX-S5800X シリーズ Ethernet スイッチ コマンドマニュアル

01-はじめに

10.1.19 display power

表 10-6 コマンド出力

■管理情報

区分	管理番号
変更	#13735

■内容

変更前）

フィールド	説明
Current(A)	電源ユニットの出力電流（アンペア単位）です。 このフィールドがサポートされていない場合は、2 つのハイフン(--)が表示されます。
Voltage(V)	電源ユニットの出力電圧（ボルト単位）です。 このフィールドがサポートされていない場合は、2つのハイフン(--)が表示されます。
Power(W)	電源ユニットの出力電力（ワット単位）です。 このフィールドがサポートされていない場合は、2つのハイフン(--)が表示されます。

変更後）

フィールド	説明
Current(A)	電源ユニットの出力電流（アンペア単位）です。 このフィールドは未サポートです。
Voltage(V)	電源ユニットの出力電圧（ボルト単位）です。 このフィールドは未サポートです。
Power(W)	電源ユニットの出力電力（ワット単位）です。 このフィールドは未サポートです。

02-IRF スタック

1.1.19 mad bfd enable

説明

■管理情報

区分	管理番号
変更	#10301

■内容

変更前）

VLAN インタフェースで BFD MAD を設定するとき、以下のガイドラインに従います。

カテゴリ	制限とガイドライン
BFD MAD VLAN	・VLAN インタフェース 1 で、BFD MAD を有効にすることはできません。 ・中継装置を使用する場合、次の作業を行います。 ■IRF スタック装置と中継装置で BFD MAD の VLAN を作成します。 ■IRF スタック装置と中継装置で BFD MAD リンクのポート BFD MAD VLAN に割り当てます。 ■IRF スタックユニットで、BFD MAD VLAN の VLAN インタフェースを作成します。 ・ネットワークの IRF スタックユニットは異なる BFD MAD VLAN を使用してください。 ・正しいトラフィックの転送を行うため、BFD MAD VLAN は BFD MAD リンクのポートのみを使用してください。もし BFD MAD リンクのポートでない場合、BFD MAD VLAN からのポートを取り除いてください。 たとえば port trunk permit vlan all コマンドですべての VLAN にポートが割り当 てられている場合、BFD MAD VLAN からポートを除外するため、undo port trunk permit コマンドを使用してください。

変更後）

VLAN インタフェースで BFD MAD を設定するとき、以下のガイドラインに従います。

カテゴリ	制限とガイドライン
BFD MAD VLAN	・VLAN インタフェース 1 で、BFD MAD を有効にすることはできません。 ・中継装置を使用する場合、次の作業を行います。 ■IRF スタック装置と中継装置で BFD MAD の VLAN を作成します。 ■IRF スタック装置と中継装置で BFD MAD リンクのポート BFD MAD VLAN に割り当てます。 ■IRF スタックユニットで、BFD MAD VLAN の VLAN インタフェースを作成します。 ■ネットワークの IRF スタックユニットは異なる BFD MAD VLAN を使用してください。 ・正しいトラフィックの転送を行うため、BFD MAD VLAN は BFD MAD リンクのポートのみを使用してください。もし BFD MAD リンクのポートでない場合、BFD MAD VLAN からのポートを取り除いてください。たとえば port trunk permit vlan all コマンドですべての VLAN にポートが割り当 てられている場合、BFD MAD VLAN からポートを除外するため、undo port trunk permit コマンドを使用してください。

03-アクセス

8.1.2 BPDU bpdu-drop any

Ⅱ. 説明

■管理情報

区分	管理番号
追加	#10301

■内容

bpdu-drop any コマンドはポートで BPDU ドロップ機能を有効にします。

undo bpdu-drop any コマンドは BPDU ドロップ機能を無効にします。

この機能を使用することで、装置は以下の BPDU パケットをドロップします。

・EOAM

・GVRP

・LACP

・LLDP

・PVST

・STP（STP、RSTP、MSTP を含みます）

14.1.2 vlan mapping

説明

■管理情報

区分	管理番号
変更	#16909

■内容

変更前）

インタフェースの MTU はデフォルトで 1500 バイトです。パケットに VLAN タグを追加したのち、パケット長は 4 バイト追加されます。one-to-two VLAN マッピングを設定するとき、サービスプロバイダ側ネットワークのインタフェースの MTU を少なくとも 1504 バイトに設定することを推奨します。

変更後）

インタフェースの MTU はデフォルトで 1500 バイトです。パケットに VLAN タグを追加したのち、パケット長は 4 バイト追加されます。one-to-two VLAN マッピングを設定するとき、サービスプロバイダ側ネットワークのインタフェースの MTU を少なくとも 1504 バイトに設定することを推奨します。
VLAN マッピングを適用したインタフェースを経由し、かつ VLAN マッピング対象の VLAN インタフェースを経由する L3 通信は未サポートです。
VLAN マッピング対象の VLAN に VLAN インタフェースを作成および IP アドレスを設定する場合は、L3 通信の経路（送受信インタフェース）には VLAN マッピングを適用しないでください。

04-IP サービス

21.1.1 http-redirect https-port

説明

■管理情報

区分	管理番号
変更	#19603

■内容

変更前）

http-redirect https-port コマンドは HTTPS リダイレクトの待機ポート番号を指定します。

undo http-redirect https-port コマンドで、設定を削除します。

変更後）

http-redirect https-port コマンドは HTTPS リダイレクトの待機ポート番号を指定します。

undo http-redirect https-port コマンドで、6654 ポートにリダイレクトします。

08-ACL and QoS

3.1.1. display qos map-table

■管理情報

区分	管理番号
変更	#19346-1

■内容

変更前）

Syntax

display qos map-table [dot1p-dp | dot1p-lp | dscp-dot1p | dscp-dp | dscp-dscp]

パラメータ

装置は表 3-1 に示すプライオリティマッピングを適用します。

表 3-1 プライオリティマッピング

プライオリティマッピング	説明
dot1p-dp	802.1p-drop プライオリティマッピングです。
dot1p-exp	802.1p-EXP プライオリティマッピングです。
dot1p-lp	802.1p-local プライオリティマッピングです。
dscp-dot1p	DSCP-802.1p プライオリティマッピングです。
dscp-dp	DSCP-drop プライオリティマッピングです。
dscp-dscp	DSCP-DSCP プライオリティマッピングです。
exp-dot1p	EXP-802.1p プライオリティマッピングです。
exp-dp	EXP-drop プライオリティマッピングです。

変更後）

Syntax

display qos map-table [dot1p-lp | dscp-dot1p | dscp-dscp]

パラメータ

装置は表 3-1 に示すプライオリティマッピングを適用します。

表 3-1 プライオリティマッピング

プライオリティマッピング	説明
dot1p-lp	802.1p-local プライオリティマッピングです。
dscp-dot1p	DSCP-802.1p プライオリティマッピングです。
dscp-dscp	DSCP-DSCP プライオリティマッピングです。

3.1.3. qos map-table

Syntax

■管理情報

区分	管理番号
変更	#19346-2

■内容

変更前）

qos map-table { dot1p-dp | dot1p-lp | dscp-dot1p | dscp-dp | dscp-dscp }

変更後）

qos map-table { dot1p-lp | dscp-dot1p | dscp-dscp }

09-セキュリティ

14.7. ARP スキャンおよび固定 ARP 設定コマンド

■管理情報

区分	管理番号
追加	#10697

■内容

14.7.1. arp scan

Syntax

arp scan [*start-ip-address to end-ip-address*] [**send-rate** { **ppm** *ppm* | *pps* }]

View

Layer 3 Ethernet interface view
VLAN interface view

定義済みユーザロール

network-admin

パラメータ

start-ip-address: スキャン範囲の開始 IP アドレスを指定します。
end-ip-address: スキャン範囲の終了 IP アドレスを指定します。終了 IP アドレスは、開始 IP アドレス以上である必要があります。
send-rate: 装置が ARP スキャンの ARP 要求を送信するレートを指定します。
ppm *ppm*: ARP パケット送信レートをパケット/分 (ppm) で指定します。ppm の設定範囲は 10～600 で、10 の倍数である必要があります。
pps: ARP パケット送信レートをパケット/秒 (pps)で指定します。pps の設定範囲は 10~1000 で、10 の倍数である必要があります。

説明

arp scan コマンドはアドレス範囲内で ARP スキャンをトリガします。
ARP スキャンは、指定されたアドレス範囲内の装置の ARP エントリを自動的に作成します。既存の ARP エントリ内にすでに存在する IP アドレスはスキャンされません。
インタフェースのプライマリ IP アドレスとセカンダリ IP アドレスがアドレス範囲内にある場合、ARP 要求内の送信元 IP アドレスは、最小ネットワークセグメントのアドレスになります。
アドレス範囲が指定されていない場合、装置はインタフェースのプライマリ IP アドレスが存在するサブネット上の装置の ARP エントリを学習します。ARP 要求内の送信元 IP アドレスは、インタフェースのプライマリ IP アドレスです。
開始 IP アドレスと終了 IP アドレスは、インタフェースのプライマリ IP アドレスまたはセカンダリ IP アドレスと同じサブネット上にある必要があります。
ARP スキャンには時間がかかります。実行中のスキャンを停止するには、Ctrl+C を押します。ダイナミック ARP エントリは、スキャンが終了する前に受信した ARP 応答に基づいて作成されます。
スキャン範囲に IP アドレスが多い場合は、ARP パケットの送信レートを設定できます。この設定により、ARP トラフィックのバーストが原因で CPU 使用率が高くなり、ネットワーク負荷が高くなるのを回避できます。
送信レートを大きな値に設定すると、装置のパフォーマンスを確保するために、指定されたレートよりも低いレートが使用される場合があります。
ARP パケット送信レートを設定しない場合、装置は指定されたスキャン範囲内のすべての IP アドレスに ARP 要求を同時に送信します。

例
VLAN インタフェース 2 のプライマリ IP アドレスが存在するネットワーク上のネイバをスキャンするために、装置を設定します。
<Switch> system-view
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] arp scan
アドレス範囲内のネイバをスキャンする装置を設定します。
<Switch> system-view
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] arp scan 1.1.1.1 to 1.1.1.20
VLAN インタフェース 2 上のアドレス範囲内のネイバをスキャンする装置を設定し、ARP パケットの送信レートを 10 pps に設定します。
<Switch> system-view
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] arp scan 1.1.1.1 to 1.1.1.20 send-rate 10

10-高可用性

4.1.7 fast-detection enable

■管理情報

区分	管理番号
変更	#11751

■内容

変更前）

メモ：

このコマンドは、UNIVERGE Network Operation Engine Overlay Network Extension 使用時のみサポートしています。

Syntax

fast-detection enable

undo fast-detection enable

変更後）

Syntax

fast-detection enable

undo fast-detection enable

4.1.8 fast-timer

■管理情報

区分	管理番号
変更	#11751

■内容

変更前）

メモ：

このコマンドは、UNIVERGE Network Operation Engine Overlay Network Extension 使用時のみサポートしています。

Syntax

fast-timer hello-timer hello-value fail-timer fail-value

undo fast-timer

変更後）

Syntax

fast-timer hello-timer hello-value fail-timer fail-value

undo fast-timer

4.1.9 protected-vlan

説明

■管理情報

区分	管理番号
変更	#17267

■内容

変更前）

protected-vlan コマンドは RRPP ドメインのプロテクト VLAN を設定します。

undo protected-vlan コマンドは RRPP ドメインからプロテクト VLAN を削除します。

プロテクト VLAN のリングを設定する前後に、RRPP ドメインで設定したプロテクト VLAN を削除、あるいは修正することができます。しかしドメインで設定されたすべてのプロテクト VLAN の設定を削除することはできません。VLAN ドメイン用に構成されています。

VLAN インスタンスのマッピングを変更するとき、RRPP ドメインのプロテクト VLAN も変更します。

変更後）

protected-vlan コマンドは RRPP ドメインのプロテクト VLAN を設定します。

undo protected-vlan コマンドは RRPP ドメインからプロテクト VLAN を削除します。

装置のスパニングツリーの動作モードが PVST モード の場合、MSTI の ID の値は 0 だけです。

プロテクト VLAN のリングを設定する前後に、RRPP ドメインで設定したプロテクト VLAN を削除、あるいは修正することができます。しかしドメインで設定されたすべてのプロテクト VLAN の設定を削除することはできません。VLAN ドメイン用に構成されています。

VLAN インスタンスのマッピングを変更するとき、RRPP ドメインのプロテクト VLAN も変更します。