GVT-274046-001-00 7.0

QX-S5600G 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-S5600G 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-S5600G シリーズ Ethernet スイッチ インスタレーションマニュアル	GVT-060636-001-00 2.0	システムのインストールについて説明しています。
QX-S5600G シリーズ Ethernet スイッチ オペレーションマニュアル	GVT-070104-001-00 1.25	機能の設定について説明しています。
QX-S5600G シリーズ Ethernet スイッチ コマンドマニュアル	GVT-070107-001-00 1.25	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（７版）

改版履歴

版数	日付	内容
1.0	2026/1/6	初版発行
2.0	2026/1/19	#10931、#13376、#13488、#13735、#14289、#15848 を追加
3.0	2026/1/26	#15052、#17267、#17318、#17689、#17867 を追加
4.0	2026/2/24	管理番号 #10301 を #10561 へ訂正、#16909 を追加
5.0	2026/3/31	#15621、#16840、#18178、#19346、#19603、#20212 を追加
6.0	2026/4/23	#17228、#17933 を追加
7.0	2026/5/25	#18398 を追加

目次

1章 QX-S5600G シリーズ Ethernet スイッチ インスタレーションマニュアル

3 章-スイッチの設置

3.7.5. DC 電源ケーブルの作成

■管理情報

区分	管理番号
変更	#17228

■内容

変更前）

🕮 メモ：

DC 電源ケーブルは単線タイプを別途用意してください。

DC 電源コード作成方法手順を以下に示します。

DC コネクタは以下の 2 パーツで構成されます。パーツ B の方向には特に注意が必要です。 図 3-25 を参照し、コネクタの向きを確認した上で、接続ミスがないよう作業を行ってください。

変更後）

🕮 メモ：

QX-S5628GT-4X2Q および QX-S5648GT-4X2Q を利用時に DC 電源を使用する場合、DC 電源ケーブルは単線タイプを別途用意してください。

DC 電源コード作成方法手順を以下に示します。

DC コネクタは以下の 2 パーツで構成されます。パーツ B の方向には特に注意が必要です。 図 3-25 を参照し、コネクタの向きを確認した上で、接続ミスがないよう作業を行ってください。

11-付録 C ポートと LED

11.3.1 システムステータス LED

■管理情報

区分	管理番号
変更	#18398

■内容

変更前）

表 11-13 システムステータス LED の説明

LED 表記	状態	説明
SYS	緑点灯	装置は正常に動作しています。（電源ON）
	緑 点 滅 (1Hz)	システムがパワーオンによる自己診断をしています。
	赤点灯	自己診断に失敗したか、他のシステム障害があります。
	消灯	本製品は停止しています（電源OFF）

変更後）

表 11-13 システムステータス LED の説明

LED 表記	状態	説明
SYS	緑点灯	装置は正常に動作しています。（電源ON）
	緑 点 滅 (1Hz)	システムがパワーオンによる自己診断をしています。 あるいはAuto Config機能が動作中です。
	赤点灯	自己診断に失敗したか、他のシステム障害があります。
	消灯	本製品は停止しています（電源OFF）

2章 QX-S5600G 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

1.1.10. MAD メカニズム

I. LACP MAD

■管理情報

区分	管理番号
変更	#10931

■内容

変更前）

・ すべてのリンクはダイナミックリンクアグリゲーショングループを形成する必要があります。

変更後）

・ すべてのリンクは単一のダイナミックリンクアグリゲーショングループを形成する必要があります。

03-アクセス

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	#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。

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。

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。

17.8.6. M-LAG MAD DOWN 状態永続化の有効化

■管理情報

区分	管理番号
変更	#15621

■内容

変更前)

> 🕮 メモ：
>
> m-lag mad persistent コマンドのみ、Ver7.4.37 含む以降のバージョンからサポートしています。 ただし、UNIVERGE Network Operation Engine Overlay Network Extension での使用 は未サポートです。

変更後）

> 🕮 メモ：
>
> Ver7.4.37 含む以降のバージョンからサポートしています。 ただし、UNIVERGE Network Operation Engine Overlay Network Extension での使用は未サポートです。

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

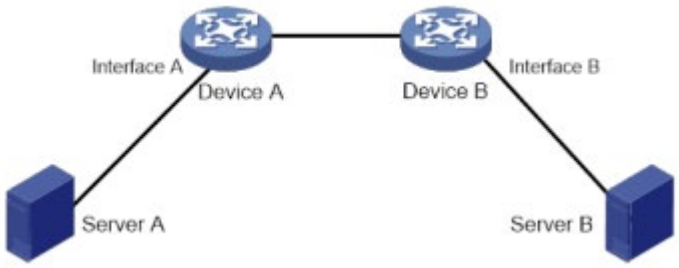


図 5-1 レイヤ 3 アクセスネットワーク内のアプリケーション

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

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）

・VXLAN ネットワークでは Ethernet サービスインスタンスは、Ethernet サービスインスタンスが存在するレイヤ 2 Ethernet インタフェースの DHCP snooping の設定（トラステッドポートの設定を除きます）を使用します。Ethernet サービスインスタンスの詳細はセクション 12 VXLAN オペレーションマニュアルの “VXLAN” を参照してください。

変更後）

・VXLAN ネットワークでは Ethernet サービスインスタンスは、Ethernet サービスインスタンスが存在するレイヤ 2 Ethernet インタフェースの DHCP snooping の設定（トラステッドポートの設定を除きます）を使用します。Ethernet サービスインスタンスの詳細はセクション 12 VXLAN オペレーションマニュアルの “VXLAN” 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。

7.3.3. ノードのアクション設定

II. パケット転送を指示するためのアクションの設定

■管理情報

区分	管理番号
変更	#13488

■内容

変更前）

操作	コマンド	補足
3. ネクストホップを設定する	**apply next-hop** [**vpn-instance** *vpn-instance-name*] { *ip-address* [**direct**] [**track** *track-entry-number*] }&<1-2>	デフォルト：ネクストホップは指定されません。 バックアップあるいはロードバランスに、このステップを複数実行することで最大 8 つのネクストホップを設定することができます。

変更後）

操作	コマンド	補足
3. ネクストホップを設定する	**apply next-hop** [**vpn-instance** *vpn-instance-name*] { *ip-address* [**direct**] [**track** *track-entry-number*] }&<1-8>	デフォルト：ネクストホップは指定されません。 バックアップのために、このステップを複数実行することで最大 8 つのネクストホップを設定することができます。

7.4.2. インタフェース PBR のポリシーの設定

II. 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-S5600G 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

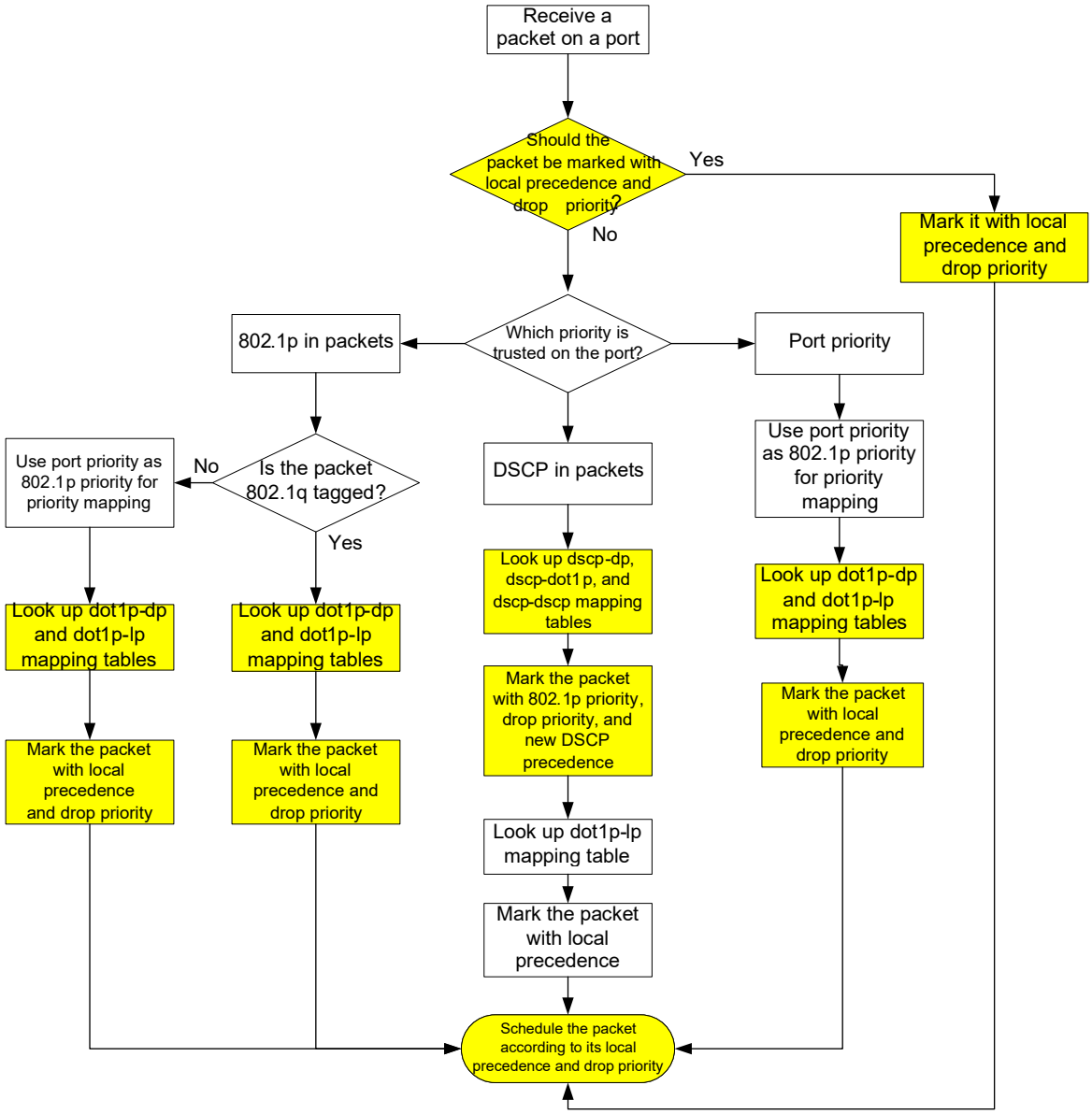
区分	管理番号
変更	#19346-3

■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

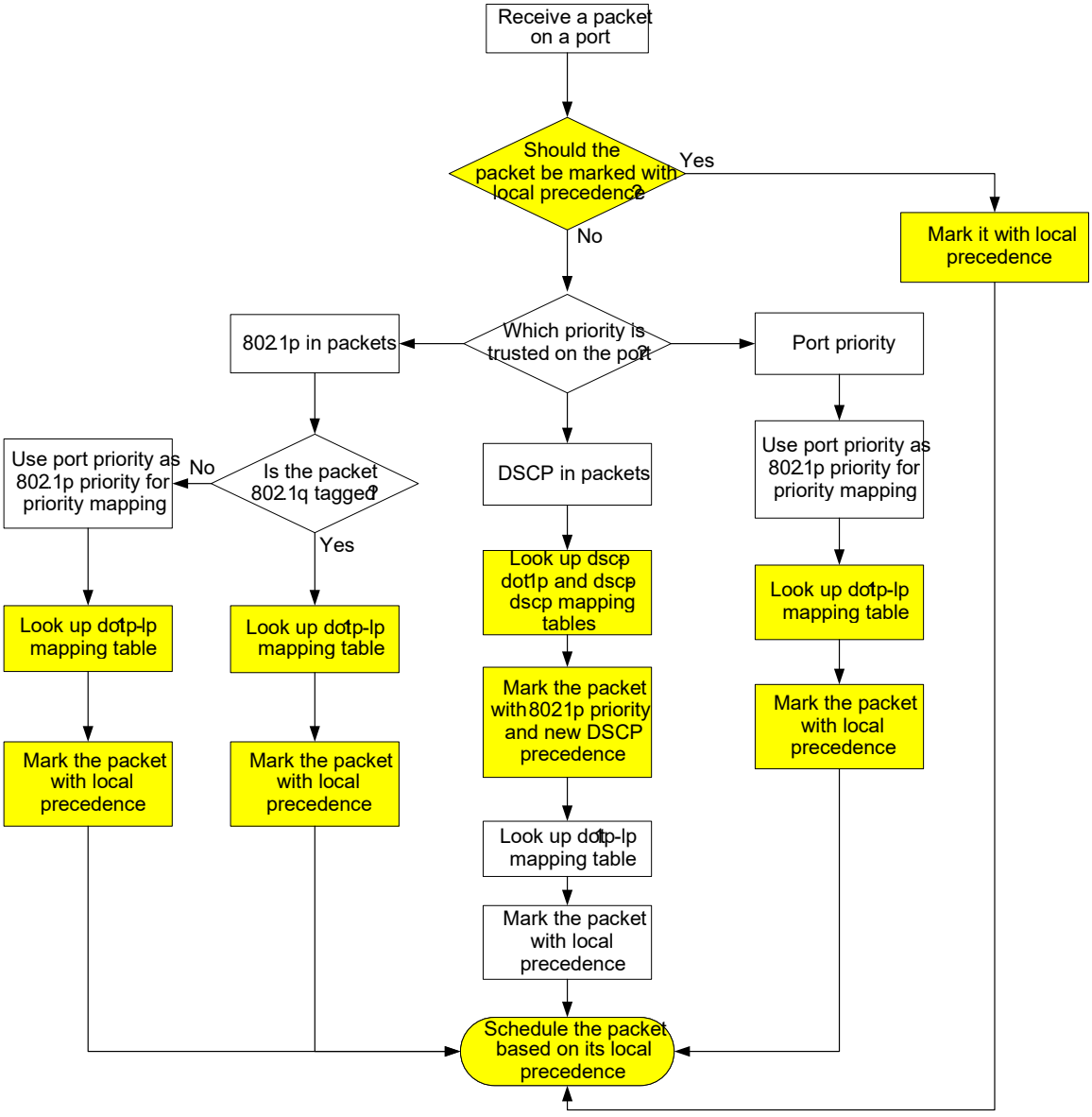


詳細は、セクション 8 *ACL and QoS オペレーションマニュアルの"プライオリティマーキング"*を参照してください。

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 }**

12.2.1. 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 12-2 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	3	0
4	4	0
5	5	0
6	6	0
7	7	0

表 12-3 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 12-4 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 12-5 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 12-2 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 12-3 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 12-4 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-S5600G 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。

10-高可用性

4.1.6 プロトコルと標準

■管理情報

区分	管理番号
削除	#17689

■内容

変更後）

“4.1.6 プロトコルと標準”節の全体を削除

3章 QX-S5600G シリーズ Ethernet スイッチ コマンドマニュアル

01-Fundamentals

10.1.18 display power

Table 10-6 Command output

■管理情報

区分	管理番号
変更	#13735

■内容

変更前）

Field	Description
Current(A)	Output current of the power supply, in amperes. If this field is not supported, two hyphens (--) are displayed.
Voltage(V)	Output voltage of the power supply, in volts. If this field is not supported, two hyphens (--) are displayed.
Power(W)	Output power of the power supply, in watts. If this field is not supported, two hyphens (--) are displayed.

変更後）

Field	Description
Current(A)	Output current of the power supply, in amperes. This field is not supported.
Voltage(V)	Output voltage of the power supply, in volts. This field is not supported.
Power(W)	Output power of the power supply, in watts. This field is not supported.

02-IRF

1.1.16 mad bfd enable

説明

■管理情報

区分	管理番号
変更	#10561

■内容

変更前）

When you configure BFD MAD on a VLAN interface, follow these guidelines:

Category	Restrictions and guidelines
BFD MAD VLAN	・Do not enable BFD MAD on VLAN-interface 1. ・If you are using an intermediate device, perform the following tasks: ・On both the IRF fabric and the intermediate device, create a VLAN for BFD MAD. ・On both the IRF fabric and the intermediate device, assign the ports of BFD MAD links to the BFD MAD VLAN. ・On the IRF fabric, create a VLAN interface for the BFD MAD VLAN. ・Make sure the IRF fabrics on the network use different BFD MAD VLANs. ・Make sure the BFD MAD VLAN contains only ports on the BFD MAD links. Exclude a port from the BFD MAD VLAN if the port is not on the BFD MAD link. For example, if you have assigned the port to all VLANs by using the **port trunk permit vlan all** command, use the **undo port trunk permit** command to exclude the port from the BFD MAD VLAN.

変更後）

When you configure BFD MAD on a VLAN interface, follow these guidelines:

Category	Restrictions and guidelines
BFD MAD VLAN	・Do not enable BFD MAD on VLAN-interface 1. ・If you are using an intermediate device, perform the following tasks: ・On both the IRF fabric and the intermediate device, create a VLAN for BFD MAD. ・On both the IRF fabric and the intermediate device, assign the ports of BFD MAD links to the BFD MAD VLAN. ・On the IRF fabric, create a VLAN interface for the BFD MAD VLAN. ・Make sure the IRF fabrics on the network use different BFD MAD VLANs. ・Make sure the BFD MAD VLAN contains only ports on the BFD MAD links. Exclude a port from the BFD MAD VLAN if the port is not on the BFD MAD link. For example, if you have assigned the port to all VLANs by using the **port trunk permit vlan all** command, use the **undo port trunk permit** command to exclude the port from the BFD MAD VLAN.

1.1.17. mad enable

Usage guidelines

■管理情報

区分	管理番号
変更	#10931

■内容

変更前）
You must set up a dynamic link aggregation group that spans all IRF member devices between the IRF fabric and the intermediate device.

変更後）
You must configure all IRF stack member devices to participate in a single dynamic link aggregation group when connected to the intermediate device.

03-Layer 2 - LAN Switching

10.1.10. vlan

I. Usage guidelines

■管理情報

区分	管理番号
変更	#17867

■内容

変更前)

You cannot create or delete the system default VLAN (VLAN 1) or reserved VLANs.

Before you delete a dynamic VLAN or a VLAN locked by an application, you must first remove the configuration from the VLAN.

The maximum number of VLANs supported on the QX-S5600G Series Ethernet Switch is 1024.

変更後)

You cannot create or delete the system default VLAN (VLAN 1) or reserved VLANs.

Before you delete a dynamic VLAN or a VLAN locked by an application, you must first remove the configuration from the VLAN.

14.1.2 vlan mapping

Usage guidelines

■管理情報

区分	管理番号
変更	#16909

■内容

変更前)

The MTU of an interface is 1500 bytes by default. After a VLAN tag is added to a packet, the packet length is added by 4 bytes. As a best practice, set the MTU to a minimum of 1504 bytes for ports on the forwarding path of the packet on the service provider network.

変更後)

The MTU of an interface is 1500 bytes by default. After a VLAN tag is added to a packet, the packet length is added by 4 bytes. As a best practice, set the MTU to a minimum of 1504 bytes for ports on the forwarding path of the packet on the service provider network.
VLAN mapping is supported only for Layer 2 switching and is not supported for Layer 3 routing.
If you create a VLAN interface for the original VLAN and set an IP address, do not configure VLAN mapping on the interface that sends and receives the Layer 3 routing traffic.

17.1.18 m-lag mad restore

■管理情報

区分	管理番号
追加	#15621

■内容

NOTE:

It is not supported for use with the UNIVERGE Network Operation Engine Overlay Network Extension.

Use **m-lag mad restore** to bring up the interfaces in M-LAG MAD DOWN state.

Syntax

m-lag mad restore

Views

System view

Predefined user roles

network-admin

Usage guidelines

Execute this command only when both the peer link and the keepalive link are down.

You can bring up the interfaces in M-LAG MAD DOWN state on the secondary M-LAG member device for it to forward traffic if the following conditions exist:

· The primary M-LAG member device fails while the peer link is down.

· M-LAG MAD DOWN state persists on the secondary M-LAG member device.

Examples

Bring up the interfaces in M-LAG MAD DOWN state.

```
<Sysname> system-view
[Sysname] m-lag mad restore
To avoid network issues, make sure the primary device has failed and cannot forward traffic.
Continue? [Y/N]:y
```

Related commands

display m-lag mad verbose
m-lag mad restore

17.1.21 m-lag standalone enable

■管理情報

区分	管理番号
追加	#15621

■内容

NOTE:

It is not supported for use with the UNIVERGE Network Operation Engine Overlay Network Extension.

Use **m-lag standalone enable** to enable M-LAG standalone mode.
Use undo **m-lag standalone enable** to disable M-LAG standalone mode.

Syntax

```
m-lag standalone enable [ delay delay-time ]
undo m-lag standalone enable [ delay ]
```

Default

M-LAG standalone mode is disabled.

Views

System view

Predefined user roles

network-admin

Parameters

delay *delay-time: Sets the delay that the device must wait before changing to M-LAG standalone mode. The value range for this delay is 0 to 3600 seconds. If you do not set this parameter, the device changes to M-LAG standalone mode without delay when both the peer link and the keepalive link go down.*

Usage guidelines

Enable M-LAG standalone mode to avoid forwarding issues in the multi-active situation that might occur after both the peer link and the keepalive link are down.

M-LAG standalone mode helps avoid traffic forwarding issues in this multi-active situation by allowing only the member ports in the M-LAG interfaces on one member device to forward traffic.

An M-LAG member device does not enter M-LAG standalone mode if the M-LAG peer reboots.

If you execute this command multiple times, the most recent configuration takes effect.

As a best practice, enable M-LAG standalone mode on both primary and secondary M-LAG member devices.

To prevent member ports of M-LAG interfaces from flapping, set the M-LAG standalone mode delay to be longer than the time required for a device reboot.

In a single-level M-LAG network, before you enable M-LAG standalone mode on an M-LAG member device, make sure its LACP system priority is higher than that of the remote aggregation system. This restriction ensures that the reference port is on the remote aggregation system and prevents the interfaces attached to the M-LAG system from flapping.

An M-LAG member device changes to M-LAG standalone mode only when it detects that both the peer link and the keepalive link are down. It does not change to M-LAG standalone mode when the peer M-

LAG member device reboots. As a best practice, set the delay that the device must wait before changing to M-LAG standalone mode based on the cause of simultaneous failure of the peer link and keepalive link:

Examples

Enable M-LAG standalone mode.

```
<Sysname> system-view

[Sysname] m-lag standalone enable
```

04-Layer 3

5. 1. IP addressing commands

■管理情報

区分	管理番号
追加	#17933

■内容

5.1.4. ip address unnumbered

Use ip address unnumbered to configure the current interface as IP unnumbered to borrow an IP address from the specified interface.

Use undo ip address unnumbered to restore the default.

Syntax

ip address unnumbered interface interface-type interface-number

undo ip address unnumbered

Default

The interface does not borrow IP addresses from other interfaces.

Views

Interface view

Predefined user roles

network-admin

Parameters

interface interface-type interface-number: Specifies an interface from which the current interface can borrow an IP address.

Usage guidelines

Typically, you assign an IP address to an interface either manually or through DHCP. If the IP addresses are not enough, or the interface is used only occasionally, you can configure an interface to borrow an IP address from other interfaces. This is called IP unnumbered, and the interface borrowing the IP address is called IP unnumbered interface.

Loopback interfaces cannot borrow IP addresses of other interfaces, but other interfaces can borrow IP addresses of loopback interfaces.

Multiple interfaces can use the same unnumbered IP address. If an interface has multiple manually configured IP addresses, only the primary IP address manually configured can be borrowed.

You cannot enable a dynamic routing protocol on the interface that has no IP address configured. To enable the interface to communicate with other devices, you must configure a static route to the peer device on the interface.

Examples

Configure the interface VLAN-interface 2 to borrow the IP address of VLAN-interface 100.

<Sysname> system-view

[Sysname] interface vlan-interface 2

[Sysname-Vlan-interface2] ip address unnumbered interface vlan-interface 10

13.1.1. http-redirect https-port

Usage guidelines

■管理情報

区分	管理番号
変更	#19603

■内容

変更前）

Using undo http-redirect https-port cannot restore the default. You must use the http-redirect https-port 8443 command to reconfigure the HTTPS redirect listening port number.

変更後）

Using undo http-redirect https-port redirects to port 6654. You must use the http-redirect https-port 8443 command to reconfigure the HTTPS redirect listening port number.

05.Layer 3 - IP Routing

6.1.1. apply next-hop

■管理情報

区分	管理番号
変更	#13488

■内容

変更前）

Syntax

apply next-hop [**vpn-instance** *vpn-instance-name*] { *ip-address* [**direct**] [**track** *track-entry-number*] }&<1-2>

undo apply next-hop [[**vpn-instance** *vpn-instance-name*] *ip-address*&<1-2>]

Parameters

&<1-2>: Indicates that the argument before it can be entered up to two times.

変更後）

Syntax

apply next-hop [**vpn-instance** *vpn-instance-name*] { *ip-address* [**direct**] [**track** *track-entry-number*] }&<1-n>

undo apply next-hop [[**vpn-instance** *vpn-instance-name*] *ip-address*&<1-n>]

Parameters

&<1-n>: Indicates that the argument before it can be entered up to n times. In V7.1.6, n is 2.
From V7.2.16 and later, n is 8.

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 | exp-dp]

Parameters

The device provides the following types of priority map.

Table 3-1 Priority maps

Priority mapping	Description
dot1p-dp	802.1p-drop priority map.
dot1p-lp	802.1p-local priority map
dscp-dot1p	DSCP-802.1p priority map.
dscp-dp	DSCP-drop priority map.
dscp-dscp	DSCP-DSCP priority map.
exp-dp	EXP-drop priority map.

変更後）

Syntax

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

Parameters

The device provides the following types of priority map.

Table 3-1 Priority maps

Priority mapping	Description
dot1p-lp	802.1p-local priority map
dscp-dot1p	DSCP-802.1p priority map.
dscp-dscp	DSCP-DSCP priority map.

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 | exp-dp }

変更後）

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

09-Security

1.2.4 display local-user

■管理情報

区分	管理番号
変更	#15052

■内容

変更前）

Syntax

display local-user [class { manage | network } | idle-cut { disable | enable } | service-type { ftp | http | https | lan-access | ssh | telnet | terminal } | state { active | block } | user-name *user-name* **class { manage | network } | vlan** *vlan-id* **]**

Parameters

service-type: Specifies the local users that use a specific type of service.

ftp: FTP users.

http: HTTP users.

https: HTTPS users.

lan-access: LAN users that typically access the network through an Ethernet, such as 802.1X users.

ssh: SSH users.

telnet: Telnet users.

terminal: Terminal users that log in through console ports.

変更後）

Syntax

display local-user [class { manage | network } | idle-cut { disable | enable } | service-type { ftp | lan-access | ssh | telnet | terminal } | state { active | block } | user-name *user-name* **class { manage | network } | vlan** *vlan-id* **]**

Parameters

service-type: Specifies the local users that use a specific type of service.

ftp: FTP users.

lan-access: LAN users that typically access the network through an Ethernet, such as 802.1X users.

ssh: SSH users.

telnet: Telnet users.

terminal: Terminal users that log in through console ports.

1.2.7 local-user

■管理情報

区分	管理番号
変更	#15052

■内容

変更前）

Syntax

undo local-user { *user-name* **class { manage | network } | all [service-type { ftp | http | https | lan-access | ssh | telnet | terminal } | class { manage | network }] }**

Parameters

service-type: Specifies the local users that use a specific type of service.

ftp: FTP users.

http: HTTP users.

https: HTTPS users.

lan-access: LAN users that typically access the network through an Ethernet, such as 802.1X users.

ssh: SSH users.

telnet: Telnet users.

terminal: Terminal users that log in through console ports.

変更後）

Syntax

undo local-user { *user-name* **class { manage | network } | all [service-type { ftp | lan-access | ssh | telnet | terminal } | class { manage | network }] }**

Parameters

service-type: Specifies the local users that use a specific type of service.

ftp: FTP users.

lan-access: LAN users that typically access the network through an Ethernet, such as 802.1X users.

ssh: SSH users.

telnet: Telnet users.

terminal: Terminal users that log in through console ports.

1.2.10 service-type

■管理情報

区分	管理番号
変更	#15052

■内容

変更前）

Syntax

service-type { **ftp** | **lan-access** | { **http** | **https** | **ssh** | **telnet** | **terminal** } * }

undo service-type { **ftp** | **lan-access** | { **http** | **https** | **ssh** | **telnet** | **terminal** } * }

Parameters

ftp: Authorizes the user to use the FTP service. The authorized directory can be modified by using the authorization-attribute work-directory command.

http: Authorizes the user to use the HTTP service.

https: Authorizes the user to use the HTTPS service.

lan-access: Authorizes the user to use the LAN access service. The users are typically Ethernet users, for example, 802.1X users.

ssh: Authorizes the user to use the SSH service.

telnet: Authorizes the user to use the Telnet service.

terminal: Authorizes the user to use the terminal service and log in from a console port.

変更後）

Syntaxservice-type { **ftp** | **lan-access** | { **ssh** | **telnet** | **terminal** } * }

undo service-type { **ftp** | **lan-access** | { **ssh** | **telnet** | **terminal** } * }

Parameters

ftp: Authorizes the user to use the FTP service. The authorized directory can be modified by using the authorization-attribute work-directory command.

lan-access: Authorizes the user to use the LAN access service. The users are typically Ethernet users, for example, 802.1X users.

ssh: Authorizes the user to use the SSH service.

telnet: Authorizes the user to use the Telnet service.

terminal: Authorizes the user to use the terminal service and log in from a console port.

3.1.10 mac-authentication timer

Usage guidelines

■管理情報

区分	管理番号
変更	#13376

■内容

変更前）

MAC authentication uses the following timers:

- **Offline detect timer**—Sets the interval that the device waits for traffic from a user before the device regards the user as idle. The device logs off the user and requests to stop accounting for the user after the timer expires. This timer takes effect only when the MAC authentication offline detection feature is enabled.

  After you set the offline detect timer, assign the same value to the MAC address aging timer by using the mac-address timer command. This operation prevents a MAC authenticated user from being offline within the offline detect interval due to MAC address entry expiration.

変更後）

MAC authentication uses the following timers:

- **Offline detect timer**—Sets the interval that the device waits for traffic from a user before the device regards the user as idle. The device logs off the user and requests to stop accounting for the user after the timer expires. This timer takes effect only when the MAC authentication offline detection feature is enabled.

10-High Availability

4.1.9 protected-vlan

Usage guidelines

■管理情報

区分	管理番号
変更	#17267

■内容

変更前）

You can delete or modify the protected VLANs configured for an RRPP domain before and after you configure rings for the domain. However, after you configure rings for the RRPP domain, you cannot delete configurations of all the protected VLANs configured for the domain.

When the VLAN-to-instance mappings change, the protected VLANs of an RRPP domain also change.

変更後）

When the device's spanning tree operation mode is PVST mode, the MSTI ID value is only 0.

You can delete or modify the protected VLANs configured for an RRPP domain before and after you configure rings for the domain. However, after you configure rings for the RRPP domain, you cannot delete configurations of all the protected VLANs configured for the domain.

When the VLAN-to-instance mappings change, the protected VLANs of an RRPP domain also change.

8.1.3. bfd detect-multiplier

Default

■管理情報

区分	管理番号
変更	#18178

■内容

変更前）

The single-hop detection time multiplier is 5.

変更後）

Up to Software Version v7.4.37 ： The single-hop detection time multiplier is 5.

Software Version v7.4.40 or later ： The single-hop detection time multiplier is 3.

8.1.11. bfd multi-hop detect-multiplier

Default

■管理情報

区分	管理番号
変更	#18178

■内容

変更前）

The multihop detection time multiplier is 5.

変更後）

Up to Software Version v7.4.37 ： The multihop detection time multiplier is 5.

Software Version v7.4.40 or later ： The multihop detection time multiplier is 3.