NEC

GVT-274042-001-00 6.0

QX-S3400F/S4100G/S4500G 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-S3400F/S4100G/S4500G 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-S3400F/S4100G/S4500G シリーズ Ethernet スイッチ インスタレーションマニュアル	GVT-089507-001-00 1.8	システムのインストールについて説明しています。
QX-S3400F/S4100G/S4500G シリーズ Ethernet スイッチ オペレーションマニュアル	GVT-089510-001-00 1.14	機能の設定について説明しています。
QX-S3400F/S4100G/S4500G シリーズ Ethernet スイッチコマンドマニュアル	GVT-089512-001-00 1.12	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４月（６版）

改版履歴

版数	日付	内容
1.0	2026/1/6	新規作成
2.0	2026/1/20	#15154、#13376、#13634、#15848 を追加
3.0	2026/2/6	誤記修正。#17241、#17267、#17829 を追加
4.0	2026/3/18	#16909、#18926 を追加
5.0	2026/3/31	#19603、#20083 を追加
6.0	2026/4/23	誤記修正。#16840 を追加

目次

1章 QX-S3400F/S4100G/S4500G シリーズ Ethernet スイッチ インスタレーションマニュアル

追加および変更はありません。

２章 QX-S3400F/S4100G/S4500G シリーズ Ethernet スイッチ オペレーションマニュアル

01-はじめに

1.4.5 コマンドエイリアスの設定と使用方法

II. 設定手順

■管理情報

区分	管理番号
変更	#15154

■内容

変更前）

以下にコマンドエイリアスの設定を以下に示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2.コマンドエイリアスを有効にする	**command-alias enable**	デフォルト：有効
3.コマンドエイリアスを設定する	**alias** *alias command*	デフォルト：設定なし システム定義のコマンドエイリアスは表 1-3 を参照してください。
4.（オプション設定項目） コマンドエイリアスで定義されたコマンドを表示する	**display alias [alias]**	すべての view で実行可能です。

変更後）

以下にコマンドエイリアスの設定を以下に示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2.コマンドエイリアスを設定する	**alias** *alias command*	デフォルト：設定なし システム定義のコマンドエイリアスは表 1-3 を参照してください。
3.（オプション設定項目） コマンドエイリアスで定義されたコマンドを表示する	**display alias [alias]**	すべての view で実行可能です。

02-IRF スタック

1.9.1. 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

6.1.6 スタティックモードのリンクアグリゲーションの動作

Ⅱ. 各メンバポートのアグリゲーションステートの設定

■管理情報

区分	管理番号
変更	#17829

■内容

変更前）

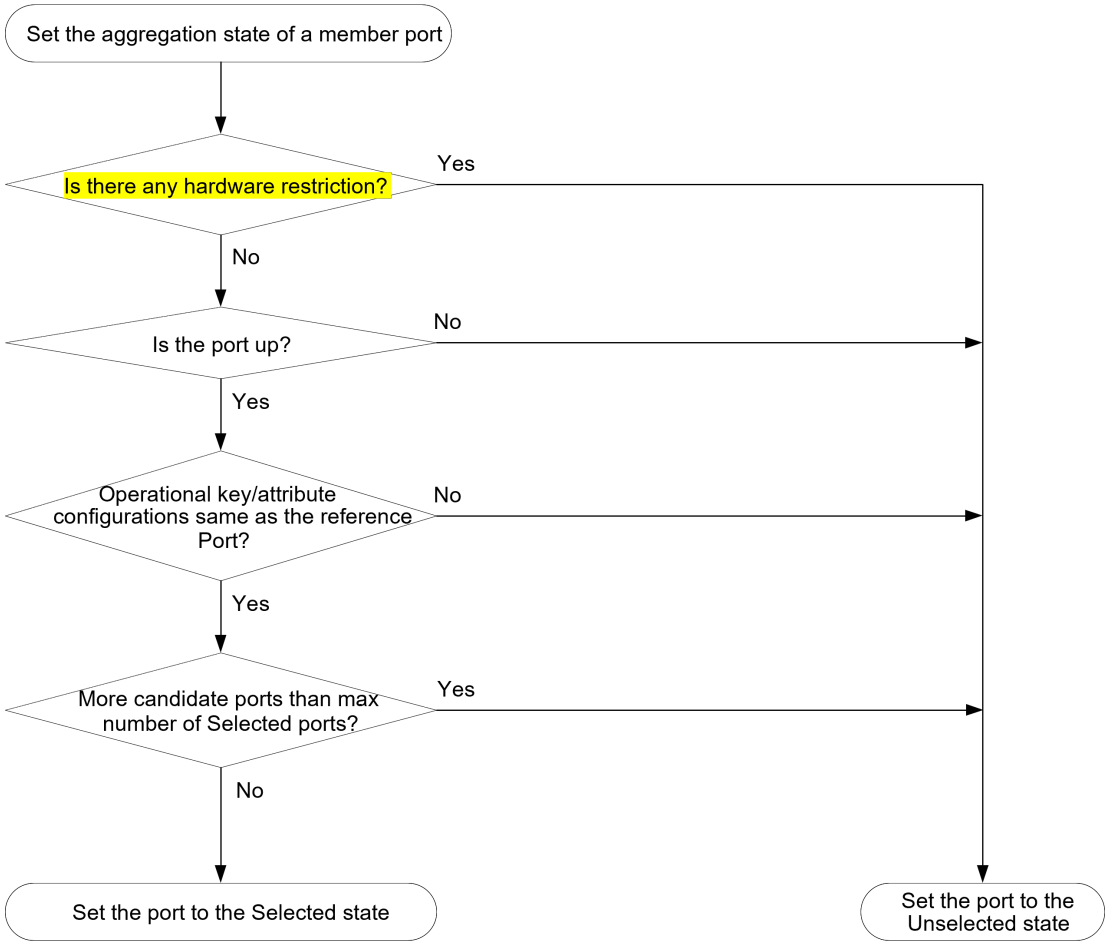

図 6-2 スタティックアグリゲーショングループのアグリゲーションステートの設定

変更後）

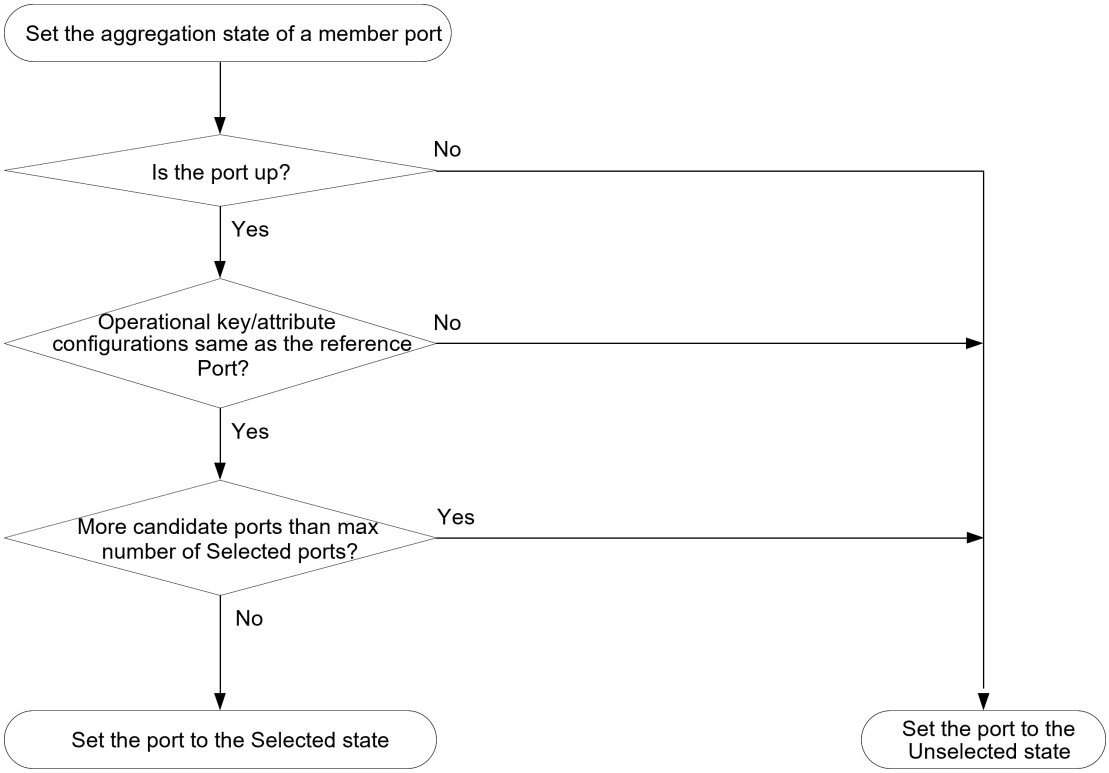

図 6-2 スタティックアグリゲーショングループのアグリゲーションステートの設定

6.1.8 ダイナミックリンクアグリゲーションの動作

Ⅱ. メンバポートのアグリゲーションステートの設定

■管理情報

区分	管理番号
変更	#17829

■内容

変更前）

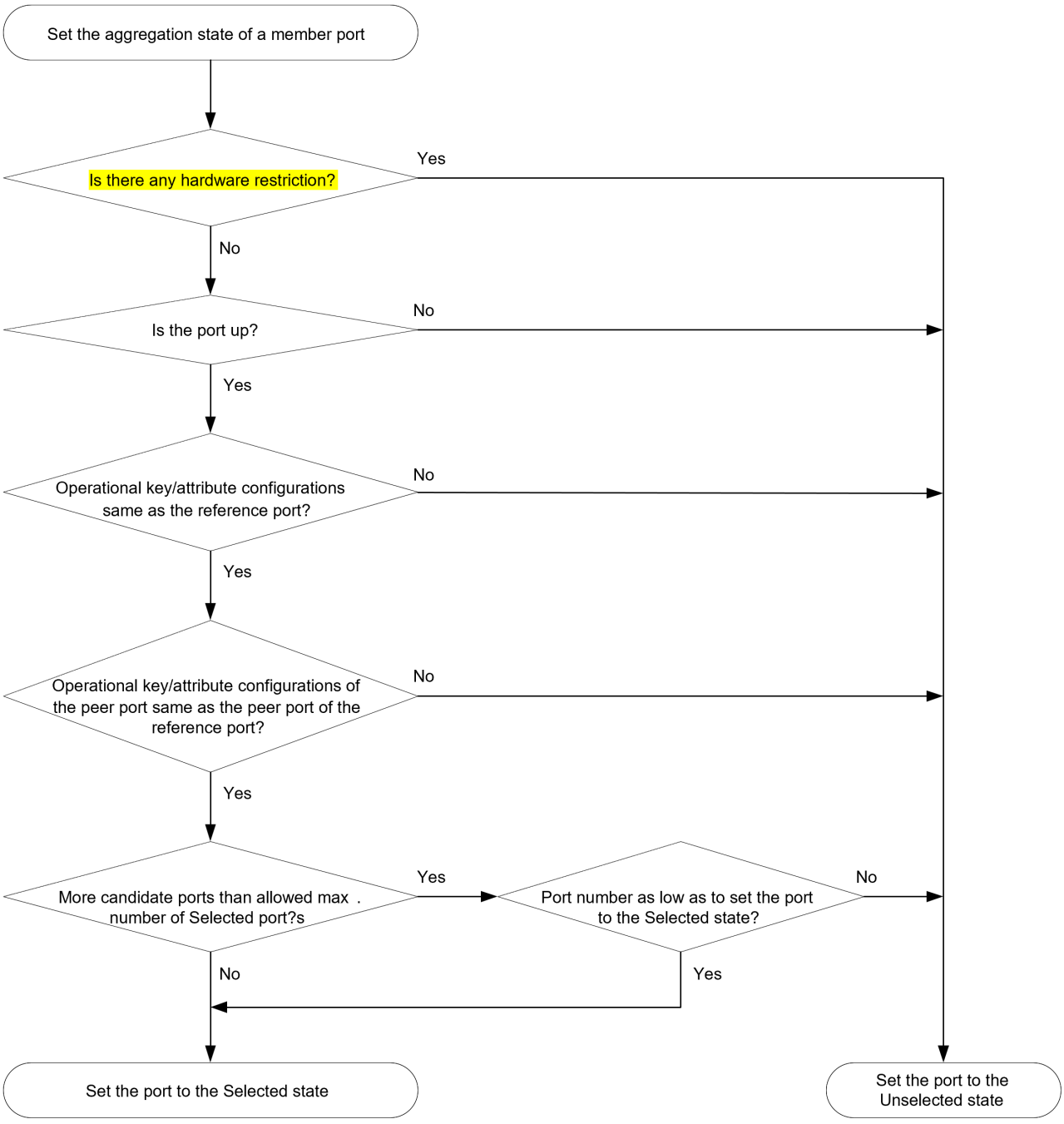

図 6-3 ダイナミックアグリゲーショングループのアグリゲーションステートの設定

変更後）

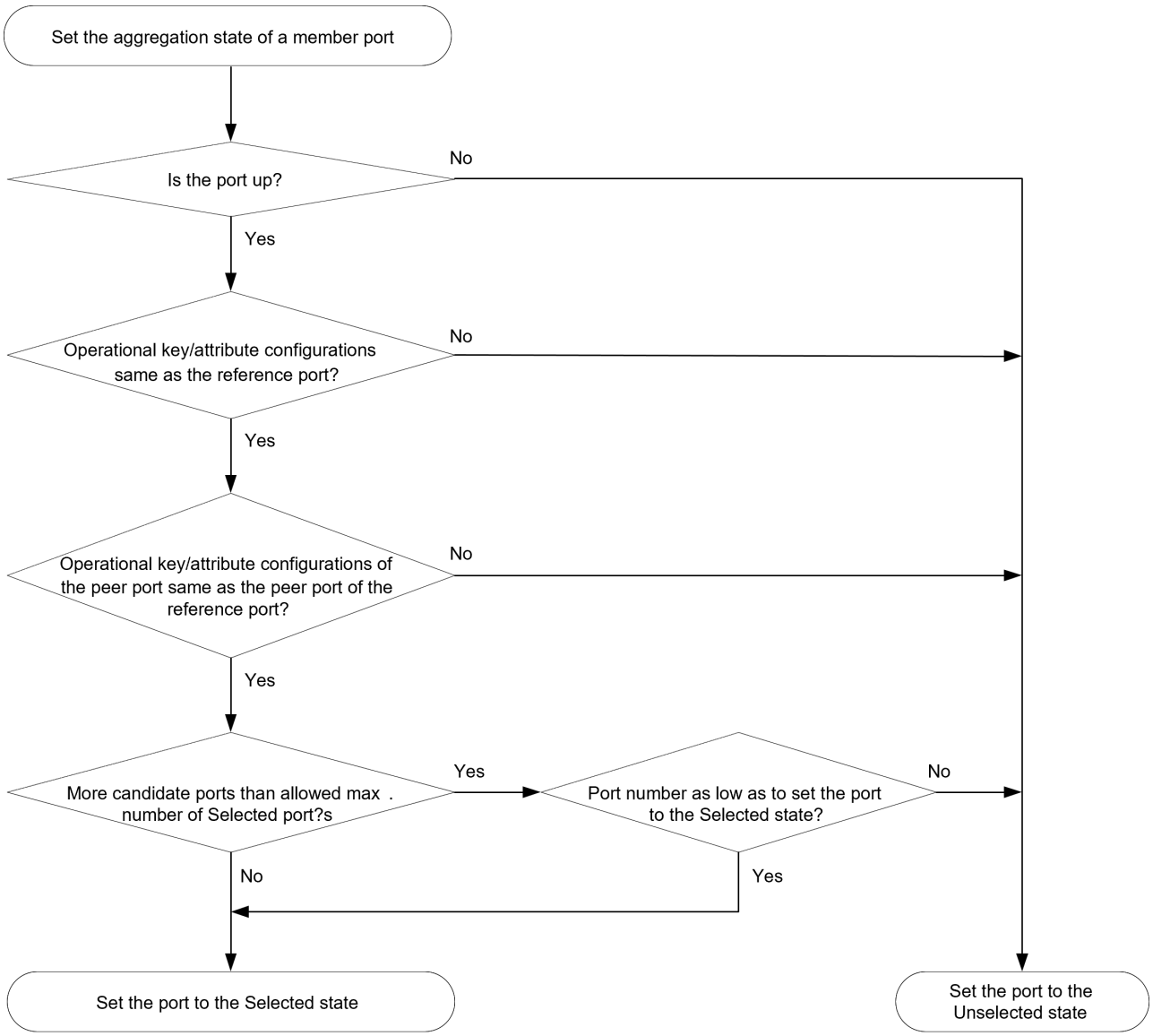

図 6-3 ダイナミックアグリゲーショングループのアグリゲーションステートの設定

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）

以下の要件が満たされている場合、ポートでループ検出が無効であったとしてもポートのループ保護アクションは開始することができます。

- 装置でループ検出がグローバルで有効、あるいはほかのすべてのポートで有効です。
- ポートはすべての VLAN のループ検出フレームを受信します。

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。

13 章 VLAN マッピング

■管理情報

区分	管理番号
変更	#16840

■内容

変更前）

⚠ **重要：**

QX-S3400F シリーズ、QX-S4100G シリーズ、QX-S4508GT-4G-I は、下記インタフェースでの VLAN マッピングをサポートしておりません。

・リンクアグリゲーションインタフェース
・ハイブリッドポートの untagged VLAN
・トランクポートの untagged VLAN
・アクセスポート

変更後）

⚠ **重要：**

QX-S3400F シリーズ、QX-S4100G シリーズ、QX-S4508GT-4G-I は、下記インタフェースでの VLAN マッピングをサポートしておりません。

・リンクアグリゲーションインタフェース
・ハイブリッドポートの untagged VLAN
・トランクポートの untagged VLAN
・アクセスポート

DHCP スヌーピングとの併用はできません。

13.2 VLAN マッピング設定作業リスト

■管理情報

区分	管理番号
変更	#16909

■内容

変更前）

VLAN マッピングを設定するとき、以下の制限とガイドラインに従ってください。

- パケットに VLAN タグをつけることで QinQ が有効なポートで VLAN マッピングと QinQ の両方を設定することができます。設定の重複がある場合、VLAN マッピングが適用されます。QinQ 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"QinQ"を参照してください。
- パケットの VLAN タグを追加あるいは置き換える場合、VLAN マッピングと QoS ポリシーの両方を設定することができます。設定の重複がある場合、VLAN マッピングが適用されます。QoS ポリシーの詳細はセクション 7 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 マッピングを設定するとき、以下の制限とガイドラインに従ってください。

- パケットに VLAN タグをつけることで QinQ が有効なポートで VLAN マッピングと QinQ の両方を設定することができます。設定の重複がある場合、VLAN マッピングが適用されます。QinQ の詳細は、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。
- パケットの VLAN タグを追加あるいは置き換える場合、VLAN マッピングと QoS ポリシーの両方を設定することができます。設定の重複がある場合、VLAN マッピングが適用されます。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 7 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。

04-IP サービス

8 章 DHCP スヌーピング

■管理情報

区分	管理番号
変更	#16840

■内容

変更前）

8 章 DHCP スヌーピング

8.1 概要

DHCP スヌーピング（DHCP snooping）は DHCP クライアントとサーバ、あるいは DHCP クライアントとリレーエージェント間で動作し、許可された DHCP サーバから IP アドレスを取得できるようにします。セキュリティの目的から DHCP クライアントの IP アドレスと MAC アドレスバインディング（DHCP snooping エントリと呼ばれます）を記録します。

変更後）

8 章 DHCP スヌーピング

⚠ **重要：**

VLAN マッピングとの併用はできません。

8.1 概要

DHCP スヌーピング（DHCP snooping）は DHCP クライアントとサーバ、あるいは DHCP クライアントとリレーエージェント間で動作し、許可された DHCP サーバから IP アドレスを取得できるようにします。セキュリティの目的から DHCP クライアントの IP アドレスと MAC アドレスバインディング（DHCP snooping エントリと呼ばれます）を記録します。

07-ACL and QoS

1.7.1 パケットフィルタリングのためのインタフェースへの ACL の適用

■管理情報

区分	管理番号
変更	#10704

■内容

変更前）

操作	コマンド	補足
3. パケットをフィルタするために ACL をインタフェースに適用する	packet-filter [ipv6 | mac] { acl-number | name acl-name } { inbound | outbound } [hardware-count]	デフォルト：設定なし インタフェースに同一方向の設定は最大 3 つまで設定できます。標準 ACL、拡張 ACL、L2 ACL それぞれ 1 つずつ設定することができます。 インタフェースで送信されるパケットをフィルタすることはできません。 VLAN インタフェースでフィルタリングを設定した場合、別の VLAN インタフェースに転送される場合にのみフィルタされます。

重要：

1 つのポートに同じ方向で、IPv4 フィルタと IPv6 フィルタを設定することはできません。inbound/outbound に分けて異なる方向での設定は可能です。

5.1.2 トラフィックポリシング

■管理情報

区分	管理番号
変更	#11171

■内容

変更前）

一般的なトラフィックポリシングのアプリケーションは、ネットワークの特定のトラフィックを監視し、トラフィックを妥当な範囲内で制限します。別のアプリケーションは、ネットワークリソースが積極的に使用しないようにするため、余剰トラフィックの調整を行います。たとえば、HTTP パケットの帯域幅を全体の 50%未満に制限することができます。セッションのトラフィックが制限を超過すると、トラフィックポリシングはパケットの廃棄やパケットの IP プレシーデンスをリセットすることができます。図 5-1 にインタフェースの出力トラフィックのポリシングの例を示します。

トラフィックポリシングは、ISP（Internet Service Provider）のネットワークのトラフィックの制限などに広く使用されます。トラフィックポリシングはトラフィックを分類し、検証結果にもとづいて、トラフィックを事前に定義されたトラフィック動作で処理します。トラフィック動作には以下があります。

・ 適合トラフィックを転送します。
・ 余剰トラフィックを破棄します。
・ 検証結果が適合である場合、リマークしたプレシーデンスに従ってパケットを転送します。

変更後）

一般的なトラフィックポリシングのアプリケーションは、ネットワークの特定のトラフィックを監視し、トラフィックを妥当な範囲内で制限します。別のアプリケーションは、ネットワークリソースが積極的に使用しないようにするため、余剰トラフィックの調整を行います。たとえば、HTTP パケットの帯域幅を全体の 50%未満に制限することができます。セッションのトラフィックが制限を超過すると、トラフィックポリシングはパケットの廃棄やパケットの DSCP をリセットすることができます。図 5-1 にインタフェースの出力トラフィックのポリシングの例を示します。

トラフィックポリシングは、ISP（Internet Service Provider）のネットワークのトラフィックの制限などに広く使用されます。トラフィックポリシングはトラフィックを分類し、検証結果にもとづいて、トラフィックを事前に定義されたトラフィック動作で処理します。トラフィック動作には以下があります。

・ 適合トラフィックを転送します。
・ 余剰トラフィックを破棄します。
・ 検証結果が適合である場合、リマークした DSCP に従ってパケットを転送します。

変更後）

操作	コマンド	補足
3. パケットをフィルタするために ACL をインタフェースに適用する	packet-filter [ipv6 | mac] { acl-number | name acl-name } { inbound | outbound } [hardware-count]	デフォルト：設定なし インタフェースに同一方向の設定は最大 3 つまで設定できます。標準 IPv4 ACL、標準 IPv6 ACL、L2 ACL それぞれ 1 つずつ設定することができます。 インタフェースで送信されるパケットをフィルタすることはできません。 VLAN インタフェースでフィルタリングを設定した場合、別の VLAN インタフェースに転送される場合にのみフィルタされます。

重要：

1 つのポートに同じ方向で、同じ IP プロトコルバージョンの標準 ACL と拡張 ACL を設定することはできません。

inbound/outbound に分けて異なる方向での設定は可能です。

08-セキュリティ

4.8 MAC アドレス認証タイマの設定

■管理情報

区分	管理番号
変更	#13376

■内容

変更前）

MAC アドレス認証では以下のタイマを使用します。

- **Offline detect timer**－ユーザがアイドル状態であることを検出するために、装置がユーザからのトラフィックを待つ期間を設定します。装置はタイマが終了するとユーザをログオフし、ユーザのアカウントの停止を要求します。このタイマは、MAC 認証オフライン検出機能が有効な場合にのみ効果があります。
  オフライン検出タイマを設定した後、mac-address timer コマンドを用いて MAC アドレスエージングタイマに同じ値を設定します。この操作をすることで、オフライン検出タイマ内でオフラインとなった MAC 認証ユーザが MAC アドレスのエントリが終了することを避けられます。

変更後）

MAC アドレス認証では以下のタイマを使用します。

- **Offline detect timer**－ユーザがアイドル状態であることを検出するために、装置がユーザからのトラフィックを待つ期間を設定します。装置はタイマが終了するとユーザをログオフし、ユーザのアカウントの停止を要求します。このタイマは、MAC 認証オフライン検出機能が有効な場合にのみ効果があります。

09-高可用性

9.1.3 サポートアプリケーションモジュール

■管理情報

区分	管理番号
変更	#17241

■内容

変更前）

以下のアプリケーションモジュールが Track モジュールに関連づけることができます。

- VRRP
- スタティックルーティング
- PBR
- EAA
- ERPS

変更後）

- VRRP
- スタティックルーティング

9.4 Track 設定作業リスト

■管理情報

区分	管理番号
変更	#17241

■内容

変更前）

作業リスト
(必須設定項目) Trackモジュールと検出モジュールの関連づけ • TrackとNQAの関連づけ • TrackとBFDの関連づけ • TrackとPoEの関連づけ
(必須設定項目) Trackモジュールとアプリケーションモジュールの関連づけ: • TrackとVRRPの関連づけ • Trackとスタティックルーティングの関連づけ • TrackとPBRの関連づけ

変更後）

作業リスト
(必須設定項目) Trackモジュールと検出モジュールの関連づけ • TrackとNQAの関連づけ • TrackとBFDの関連づけ • TrackとPoEの関連づけ
(必須設定項目) Trackモジュールとアプリケーションモジュールの関連づけ: • TrackとVRRPの関連づけ • Trackとスタティックルーティングの関連づけ

9.6.4 Track と PBR の関連づけ

■管理情報

区分	管理番号
削除	#17241

変更後）

9.6.4 Track と PBR の関連付けの節全体を削除

3章 QX-S3400F/S4100G/S4500G シリーズ Ethernet スイッチ コマンドマニュアル

01-はじめに

9.1.14 display fan

表 9-4 コマンド出力

■管理情報

区分	管理番号
変更	#20083

■内容

変更前）

フィールド	説明
Slot 1	IRFスタック装置のIDです。
Fan 1	内蔵ファンの番号です。
State	ファンの稼働状態を示します。 **Absent**–ファンスロットにファンがありません。 **Normal**–ファンが正常に動作しています。 **Fault**–ファンに問題があります。

変更後）

フィールド	説明
Slot 1	IRFスタック装置のIDです。
Fan 1	内蔵ファンの番号です。
State	ファンの稼働状態を示します。 **Absent**–ファンスロットにファンがありません。 **Normal**–ファンが正常に動作しています。 **Fault**–ファンに問題があります。 **Fan-less**–ファンレスモデルのためファンはありません。

02-IRF スタック

1.1.17. mad enable

説明

■管理情報

区分	管理番号
変更	#10931

■内容

変更前）

IRF スタックユニットと中継装置間ですべての IRF スタックメンバ装置に接続するダイナミックリンクアグリゲーショングループを設定する必要があります。

変更後）

IRF スタックユニットと中継装置間ですべての IRF スタックメンバ装置に接続するため、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設定する必要があります。

03-アクセス

13.1.2 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

16.1.1. 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 コマンドでは、HTTPS リダイレクトする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 コマンドでは、HTTPS リダイレクトする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。

07-ACL and QoS

1.1.11 packet-filter

■管理情報

区分	管理番号
変更	#10704

■内容

変更前）

重要：

1 つのポートに同じ方向で、IPv4 フィルタと IPv6 フィルタを設定することはできません。
inbound/outbound に分けて異なる方向での設定は可能です。

説明
インタフェースの同一方向に対して、最大 3 つの ACL（1 つの標準 IPv4 ACL、1 つの標準 IPv4 ACL、1 つの L2 ACL）を適用することができます。

変更後）

重要：

1 つのポートに同じ方向で、同じ IP プロトコルバージョンの標準 ACL と拡張 ACL を設定することはできません。
inbound/outbound に分けて異なる方向での設定は可能です。

説明
インタフェースの同一方向に対して、最大 3 つの ACL（1 つの標準 IPv4 ACL、1 つの標準 IPv6 ACL、1 つの L2 ACL）を適用することができます。

08-セキュリティ

■管理情報

区分	管理番号
その他	#18926

■内容

しおりの構成として、「08-セキュリティ」の中に「09-高可用性」、「10-システム管理」が入っていますが、正しくは「08-セキュリティ」、「09-高可用性」、「10-システム管理」は同じ階層となります。

1.3.9 primary authentication (RADIUS scheme view)

パラメータ

■管理情報

区分	管理番号
変更	#13634

■内容

変更前）

port-number: プライマリ RADIUS 認証サーバのサービスポート番号を UDP ポート番号で指定します。設定範囲は 1～65535 です。デフォルトは 1812 です。

key: セキュアなプライマリ RADIUS アカウンティングサーバの通信を行うために共有キーを設定します。

cipher: 暗号テキストを指定します。

変更後）

port-number: プライマリ RADIUS 認証サーバのサービスポート番号を UDP ポート番号で指定します。設定範囲は 1～65535 です。デフォルトは 1812 です。

key: プライマリ RADIUS 認証サーバとのセキュア通信のための共有鍵を指定します。

cipher: 暗号テキストを指定します。

1.3.20 secondary authentication（RADIUS scheme view）

パラメータ

■管理情報

区分	管理番号
変更	#13634

■内容

変更前）

port-number: セカンダリ RADIUS 認証サーバのサービスポート番号を UDP ポート番号で指定します。設定範囲は 1～65535 です。デフォルトは 1812 です。

key: セキュアなプライマリ RADIUS アカウンティングサーバの通信を行うために共有キーを設定します。

cipher: 暗号テキストを指定します。

変更後）

port-number: セカンダリ RADIUS 認証サーバのサービスポート番号を UDP ポート番号で指定します。設定範囲は 1～65535 です。デフォルトは 1812 です。

key: セカンダリ RADIUS 認証サーバとのセキュア通信のための共有鍵を指定します。

cipher: 暗号テキストを指定します。

3.1.11 mac-authentication timer (system view)

説明

■管理情報

区分	管理番号
変更	#13376

■内容

変更前）

MAC アドレス認証ユーザは以下のタイマを使用します。

- **Offline detect timer**—ユーザがアイドル状態であることを検出するために、装置がユーザからのトラフィックを待つ期間を設定します。ユーザの接続が期間内でアイドル状態になっている場合、装置はユーザをログアウトし、ユーザのアカウントを停止します。このタイマは MAC アドレス認証のオフライン状態の検出機能が有効である場合のみ有効です。
  Offline detect timer を設定したのち、コマンドで MAC アドレスエージングタイマに、Offline detect timer と同一の値を設定してください。これによって Offline detect timer の期間内に許可されたユーザの MAC アドレスエントリが終了してしまわないように防止します。

変更後）

MAC アドレス認証ユーザは以下のタイマを使用します。

- **Offline detect timer**—ユーザがアイドル状態であることを検出するために、装置がユーザからのトラフィックを待つ期間を設定します。ユーザの接続が期間内でアイドル状態になっている場合、装置はユーザをログアウトし、ユーザのアカウントを停止します。このタイマは MAC アドレス認証のオフライン状態の検出機能が有効である場合のみ有効です。

09-高可用性

3.1.7 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 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 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。