

QX-S5100G シリーズ Ethernet スイッチ マニュアル訂正資料

All Rights Reserved

事前に NEC の書面による許可なく、本マニュアルをいかなる形式または方法で複製または配布することを禁止します。

商標

本マニュアルに記載されているその他の商標は、各社が保有します。

注意

本マニュアルの内容は、予告なく変更されることがあります。本マニュアルのすべての記述、情報、および推奨事項は、明示的か暗黙的にかかわらず、いかなる種類の保証の対象になりません。

本資料について

この資料は、以下に示す QX-S5100G 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-S5100G シリーズ Ethernet スイッチ インストールマニュアル	GVT-159428-001-00 1.2	システムのインストール について説明していま す。
QX-S5100G シリーズ Ethernet スイッチ オペレーションマニュアル	GVT-159429-001-00 1.6	機能の設定について説明 しています。
QX-S5100G シリーズ Ethernet スイッチ コマンドマニュアル	GVT-159430-001-00 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4月（7版）

改版履歴

版数	日付	内容
1.0	2026/1/6	新規作成
2.0	2026/1/16	#13376、#13634、#14289、#15154、#15848 を追加
3.0	2026/1/30	#17267、#17318 を追加
4.0	2026/2/16	#16909、#18282 を追加
5.0	2026/3/2	#19603 を追加
6.0	2026/3/20	#20212 を追加
7.0	2026/4/16	#16840、#17228 を追加

目次

1章 QX-S5100G シリーズ Ethernet スイッチ インスタレーションマニュアル.....	6
3章-装置の設置.....	7
3.1.5 DC 電源ケーブルの作成.....	7
2章 QX-S5100G シリーズ Ethernet スイッチ オペレーションマニュアル.....	8
01-はじめに.....	9
1.4.5 コマンドエイリアスの設定と使用方法.....	9
03-アクセス.....	10
9.3 ループ検出の有効化.....	10
14章 VLAN マッピング.....	11
14.2 VLAN マッピング設定作業リスト.....	12
04-IP サービス.....	13
10章 DHCP スヌーピング.....	13
05-ルーティングプロトコル.....	14
7.7.9 デフォルトルートへの再配信の設定.....	14
8.4.2 インタフェース PBR のポリシーの設定.....	15
07-ACL and QoS.....	16
5.1.2 トラフィックポリシング.....	16
09-セキュリティ.....	17
4.1. 概要.....	17
4.8 MAC アドレス認証タイマの設定.....	18
3章 QX-S5100G シリーズ Ethernet スイッチ コマンドマニュアル.....	19
03-アクセス.....	20
4.1.1 display mac-address.....	20
9.1.2 loopback-detection action.....	21
9.1.3 loopback-detection enable.....	22
14.1.2 vlan mapping.....	23
03-アクセス.....	24
20.1.1 http-redirect https-port.....	24
09-セキュリティ.....	25
1.3.9 primary authentication (RADIUS scheme view).....	25
10-高可用性.....	26
4.1.5 display rrpp verbose.....	26
4.1.7 protected-vlan.....	28
11-システム管理.....	29
1.1.3 ping.....	29
1.1.4 ping ipv6.....	30
1.1.5 tracert.....	31
1.1.6 tracert ipv6.....	32
3.1.18 ntp-service unicast-peer.....	33
3.1.19 ntp-service unicast-server.....	34

1 章 QX-S5100G 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-装置の設置

3.1.5 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 3-23 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)

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 3-23 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。

2章 QX-S5100G 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	—
2.コマンドエイリアスを有効にする	command-alias enable	デフォルト：無効
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	—
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。

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)

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。

14 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-S5100G シリーズは、下記インタフェースでの VLAN マッピングをサポートしていません。

- ・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-S5100G シリーズは、下記インタフェースでの VLAN マッピングをサポートしていません。

- ・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。

14.2 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、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 8 ACL and QoS "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 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。

04-IP サービス

10 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)

10 章 DHCP スヌーピング

10.1 概要

DHCP スヌーピング (DHCP snooping) は、DHCP サーバと DHCP クライアント間でやりとりされる DHCP メッセージを監視して動的な IP ソースフィルタリングを行う機能です。本機能を利用することで、DHCP サーバを用いたネットワーク環境において、正当な DHCP クライアントにだけ IP 通信を許可することができる DHCP セキュリティ機能です。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)

10 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。

10.1 概要

DHCP スヌーピング (DHCP snooping) は、DHCP サーバと DHCP クライアント間でやりとりされる DHCP メッセージを監視して動的な IP ソースフィルタリングを行う機能です。本機能を利用することで、DHCP サーバを用いたネットワーク環境において、正当な DHCP クライアントにだけ IP 通信を許可することができる DHCP セキュリティ機能です。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。

05-ルーティングプロトコル

7.7.9 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。

8.4.2. 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。

07-ACL and QoS

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せん。

- ・ 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せん。

- ・ 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。

09-セキュリティ

4.1. 概要

■管理情報

区分	管理番号
変更	#20212

■内容

変更前)

📖 メモ：

認証に失敗した MAC アドレスがスタティック MAC アドレスまたは任意のセキュリティ認証をパスした MAC アドレスである場合、装置はその MAC アドレスをサイレントアドレスとして記憶しません。

変更後)

📖 メモ：

認証に失敗した MAC アドレスがスタティック MAC アドレスまたは任意のセキュリティ認証をパスした MAC アドレスである場合、装置はその MAC アドレスをサイレントアドレスとして記憶しません。

QX-S5100G 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。

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 アドレスエイ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。

3章 QX-S5100G シリーズ Ethernet スイッチ コマンドマニュアル

03-アクセス

4.1.1 display mac-address

表 4-1 コマンド出力

■管理情報

区分	管理番号
変更	#12836

■内容

変更前)

フィールド	説明
Aging	エントリがエージングアウト可能かどうかを示します。 <ul style="list-style-type: none"> ● Y-エントリはエージングアウト可能です。 ● N-エントリはエージングアウトできません。

変更後)

フィールド	説明
Aging	エントリがエージングアウト可能かどうかを示します。 <ul style="list-style-type: none"> ● Y-エントリはエージングアウト可能です。 ● N-エントリはエージングアウトできません。但し MAC 認証によるエントリは例外です。

9.1.2 loopback-detection action

説明

■管理情報

区分	管理番号
変更	#12847

■内容

変更前)

loopback-detection action コマンドはポートのループ保護のアクションを設定します。

undo loopback-detection action コマンドはデフォルトに戻します。

変更後)

loopback-detection action コマンドはポートのループ保護のアクションを設定します。

undo loopback-detection action コマンドは無効に設定します。

アクションをデフォルト値に戻すときは**loopback-detection action block** コマンドを実行してください。

9.1.3 loopback-detection enable

説明

■管理情報

区分	管理番号
変更	#12847

■内容

変更前)

loopback-detection enable コマンドはポートでループ検出を有効にします。

undo loopback-detection enable コマンドはポートでループ検出を無効にします。

グローバルでループ検出を有効にする場合、**loopback-detection global enable** コマンドを使用します。

変更後)

loopback-detection enable コマンドはポートでループ検出を有効にします。

undo loopback-detection enable コマンドはポートでループ検出を無効にします。

有効VLANをデフォルト値に戻すときは、**undo loopback-detection enable vlan all** コマンド実行後に **loopback-detection enable vlan 1** コマンドを実行してください。

グローバルでループ検出を有効にする場合、**loopback-detection global enable** コマンドを使用します。

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。

03-アクセス

20.1.1 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。**

09-セキュリティ

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: 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。

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。

10-高可用性

4.1.5 display rrpp verbose

例

■管理情報

区分	管理番号
変更	#18282

■内容

変更前)

表 4-4 コマンド出力

フィールド	説明
Ring state	RRPP リング状態です。 <ul style="list-style-type: none"> ● Completed—リングが正常です。 ● Failed—リングが閉じていません。 マスタノードとして動作する装置でリングが有効でない、あるいは装置がリングのマスタノードでない場合、ハイフン (-) が表示されます。

変更後)

表 4-4 コマンド出力

フィールド	説明
Ring state	RRPP リング状態です。 <ul style="list-style-type: none"> ● マスターノードでの可能な状態： <ul style="list-style-type: none"> ○ Completed—リングが正常です。 ○ Failed—リングが閉じていません。 ○ Unknown—RRPP ドメインが無効です。 ● トランジットノードまたはエッジノードでの可能な状態： <ul style="list-style-type: none"> ○ LinkUp—ノード上の全てのポートがアップしています。 ○ LinkDown—ノード上の少なくとも1つのポートがダウンしています。 ○ PreForward—ノード上のポートがブロックされています。 ○ Unknown—RRPP ドメインが無効です。 ● アシスタントエッジノードでの可能な状態： <ul style="list-style-type: none"> ○ LinkUp—ノード上の全てのポートがアップしています。 ○ LinkDown—ノード上の少なくとも1つのポートがダウンしています。 ○ PreForward—ノード上のポートがブロックされています。 ○ LinkUpNotify—LinkUp 状態で Edge-Hello パケットを受信しません。 ○ LinkDnNotify—LinkDown 状態で Edge-Hello パケットを受信しません。

	<ul style="list-style-type: none">○ PreForwardNotify—直接接続されたエッジノードのポートがアップする、または PreForward 状態でアシスタントエッジノードが Edge-Hello パケットを受信しません。○ Unknown—RRPP ドメインが無効です。
--	--

4.1.7 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。

11-システム管理

1.1.3 ping

■管理情報

区分	管理番号
変更	#12833

■内容

変更前)

Syntax

```
ping [ ip ] [ -a source-ip | -c count | -f | -h ttl | -i interface-type interface-number | -m interval | -n | -p pad | -q | -r | -s packet-size | -t timeout | -tos tos | -v ] * host
```

パラメータ

-v: ICMP 以外のエコー応答を表示します。指定しない場合、システムは ICMP 以外のエコー応答を表示しません。

host: 宛先の IP アドレスあるいはホスト名を指定します。ホスト名の設定範囲は 1~253 文字です。大文字、小文字を区別しません。英字、数字、ハイフン (-)、アンダーライン (_)、ドット (.) を含むことができます。

変更後)

Syntax

```
ping [ ip ] [ -a source-ip | -c count | -f | -h ttl | -i interface-type interface-number | -m interval | -n | -p pad | -q | -r | -s packet-size | -t timeout | -tos tos | -v -vpn-instance vpn-instance-name ] * host
```

パラメータ

-v: ICMP 以外のエコー応答を表示します。指定しない場合、システムは ICMP 以外のエコー応答を表示しません。

-vpn-instance vpn-instance-name: 宛先が属する VPN インスタンスを指定します。大文字小文字を区別し、設定範囲は 1~31 文字です。宛先がパブリックネットワークの場合、このオプションは指定しません。

host: 宛先の IP アドレスあるいはホスト名を指定します。ホスト名の設定範囲は 1~253 文字です。大文字、小文字を区別しません。英字、数字、ハイフン (-)、アンダーライン (_)、ドット (.) を含むことができます。

1.1.4 ping ipv6

■管理情報

区分	管理番号
変更	#12833

■内容

変更前)

Syntax

```
ping ipv6 [ -a source-ipv6 | -c count | -i interface-type interface-number | -m interval | -q | -s packet-size | -t timeout | -v ] * host
```

パラメータ

-v: ICMPv6 エコー応答の詳細情報を表示します。(dst フィールドと idx フィールドを含みます) 指定しない場合、システムは ICMPv6 エコー応答の概要情報のみを表示します。(dst フィールドと idx フィールドを含みません)

先の IPv6 アドレスあるいはホスト名を指定します。ホスト名の設定範囲は 1~253 文字です。大文字、小文字を区別しません。英字、数字、ハイフン (-)、アンダーライン (_)、ドット (.) を含むことができます。

変更後)

Syntax

```
ping ipv6 [ -a source-ipv6 | -c count | -i interface-type interface-number | -m interval | -q | -s packet-size | -t timeout | -v | -vpn-instance vpn-instance-name ] * host
```

パラメータ

-v: ICMPv6 エコー応答の詳細情報を表示します。(dst フィールドと idx フィールドを含みます) 指定しない場合、システムは ICMPv6 エコー応答の概要情報のみを表示します。(dst フィールドと idx フィールドを含みません)

-vpn-instance vpn-instance-name: 宛先が属する VPN インスタンスを指定します。大文字小文字を区別し、設定範囲は 1~31 文字です。宛先がパブリックネットワークの場合、このオプションは指定しません。

host: 宛先の IPv6 アドレスあるいはホスト名を指定します。ホスト名の設定範囲は 1~253 文字です。大文字、小文字を区別しません。英字、数字、ハイフン (-)、アンダーライン (_)、ドット (.) を含むことができます。

1.1.5 tracert

■管理情報

区分	管理番号
変更	#12833

■内容

変更前)

Syntax

```
tracert [ -a source-ip | -f first-ttl | -m max-ttl | -p port | -q packet-number | -w timeout ] * host
```

パラメータ

-q packet-number: ホップごとに送信されるプローブパケット数を指定します。設定範囲は 1~65535 です。デフォルトは 3 です。

-w timeout: プローブパケットの応答パケットのタイムアウト時間を指定します。設定範囲は 1~65535 ミリ秒です。デフォルトは 5000 ミリ秒です。

変更後)

Syntax

```
tracert [ -a source-ip | -f first-ttl | -m max-ttl | -p port | -q packet-number | -vpn-instance vpn-instance-name | -w timeout ] * host
```

パラメータ

-q packet-number: ホップごとに送信されるプローブパケット数を指定します。設定範囲は 1~65535 です。デフォルトは 3 です。

-vpn-instance vpn-instance-name: 宛先が属する VPN インスタンスを指定します。大文字小文字を区別し、設定範囲は 1~31 文字です。宛先がパブリックネットワークの場合、このオプションは指定しません。

-w timeout: プローブパケットの応答パケットのタイムアウト時間を指定します。設定範囲は 1~65535 ミリ秒です。デフォルトは 5000 ミリ秒です。

1.1.6 tracer ipv6

■管理情報

区分	管理番号
変更	#12833

■内容

変更前)

Syntax

```
tracer ipv6 [ -f first-hop | -m max-hops | -p port | -q packet-number | -w timeout ] * host
```

パラメータ

-q packet-number: ホップごとに送信されるプローブパケット数を指定します。設定範囲は 1~65535 です。デフォルトは 3 です。

-w timeout: プローブパケットの応答パケットのタイムアウト時間を指定します。設定範囲は 1~65535 ミリ秒です。デフォルトは 5000 ミリ秒です。

変更後)

Syntax

```
tracer ipv6 [ -f first-hop | -m max-hops | -p port | -q packet-number | -vpn-instance vpn-instance-name | -w timeout ] * host
```

パラメータ

-q packet-number: ホップごとに送信されるプローブパケット数を指定します。設定範囲は 1~65535 です。デフォルトは 3 です。

-vpn-instance vpn-instance-name: 宛先が属する VPN インスタンスを指定します。大文字小文字を区別し、設定範囲は 1~31 文字です。宛先がパブリックネットワークの場合、このオプションは指定しません。

-w timeout: プローブパケットの応答パケットのタイムアウト時間を指定します。設定範囲は 1~65535 ミリ秒です。デフォルトは 5000 ミリ秒です。

3.1.18 ntp-service unicast-peer

■管理情報

区分	管理番号
変更	#12833

■内容

変更前)

Syntax

```
ntp-service unicast-peer { peer-name | ip-address } [ authentication-keyid keyid | maxpoll maxpoll-interval | minpoll minpoll-interval | priority | source interface-type interface-number | version number ] *
undo ntp-service unicast-peer { peer-name | ip-address }
```

パラメータ

ip-address: シンメトリック-パッシブピアの IP アドレスを指定します。ブロードキャストアドレス、マルチキャストアドレス、ローカルクロックの IP アドレスでなくユニキャストアドレスにする必要があります。

authentication-keyid keyid: NTP メッセージをピアに送信するために使用するキーの ID を指定します。設定範囲は 1~4294967295 です。指定しない場合、ローカル装置とピアは互いに認証しません。

変更後)

Syntax

```
ntp-service unicast-peer { peer-name | ip-address } [ vpn-instance vpn-instance-name ]
[ authentication-keyid keyid | maxpoll maxpoll-interval | minpoll minpoll-interval | priority | source interface-type interface-number | version number ] *
undo ntp-service unicast-peer { peer-name | ip-address } [ vpn-instance vpn-instance-name ]
```

パラメータ

ip-address: シンメトリック-パッシブピアの IP アドレスを指定します。ブロードキャストアドレス、マルチキャストアドレス、ローカルクロックの IP アドレスでなくユニキャストアドレスにする必要があります。

vpn-instance vpn-instance-name: シンメトリック-パッシブピアが属する VPN インスタンスを指定します。大文字小文字を区別し、設定範囲は 1~31 文字です。シンメトリック-パッシブピアがパブリックネットワークの場合、このオプションは指定しません。

authentication-keyid keyid: NTP メッセージをピアに送信するために使用するキーの ID を指定します。設定範囲は 1~4294967295 です。指定しない場合、ローカル装置とピアは互いに認証しません。

3.1.19 ntp-service unicast-server

■管理情報

区分	管理番号
変更	#12833

■内容

変更前)

Syntax

```
ntp-service unicast-server { server-name | ip-address } [ authentication-keyid keyid | maxpoll maxpoll-interval | minpoll minpoll-interval | priority | source interface-type interface-number | version number ] *
```

```
undo ntp-service unicast-server { server-name | ip-address }
```

パラメータ

ip-address: NTPサーバのIPアドレスを指定します。ブロードキャストアドレス、マルチキャストアドレス、ローカルルックのIPアドレスでなくユニキャストアドレスにする必要があります。

authentication-keyid keyid: NTP メッセージを NTP サーバに送信するために使用するキーの ID を指定します。設定範囲は 1~4294967295 です。指定しない場合、ローカル装置と NTP サーバは互いに認証しません。

変更後)

Syntax

```
ntp-service unicast-server { server-name | ip-address } [ vpn-instance vpn-instance-name ] [ authentication-keyid keyid | maxpoll maxpoll-interval | minpoll minpoll-interval | priority | source interface-type interface-number | version number ] *
```

```
undo ntp-service unicast-server { server-name | ip-address } [ vpn-instance vpn-instance-name ]
```

パラメータ

ip-address: NTPサーバのIPアドレスを指定します。ブロードキャストアドレス、マルチキャストアドレス、ローカルルックのIPアドレスでなくユニキャストアドレスにする必要があります。

vpn-instance vpn-instance-name: NTPサーバが属するVPNインスタンスを指定します。大文字小文字を区別し、設定範囲は1~31文字です。NTPサーバがパブリックネットワークの場合、このオプションは指定しません。

authentication-keyid keyid: NTP メッセージを NTP サーバに送信するために使用するキーの ID を指定します。設定範囲は 1~4294967295 です。指定しない場合、ローカル装置と NTP サーバは互いに認証しません。