NEC

GVT-274041-001-00 4.0

QX-S1100G シリーズ Ethernet スイッチ
マニュアル訂正資料

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、明示的か暗黙的かにかかわらず、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-S1100G 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-S1100G シリーズ Ethernet スイッチ インスタレーションマニュアル	GVT-125430-001-00 1.5	システムのインストールについて説明しています。
QX-S1100G シリーズ Ethernet スイッチ オペレーションマニュアル	GVT-125431-001-00 1.9	機能の設定について説明しています。
QX-S1100G シリーズ Ethernet スイッチ コマンドマニュアル	GVT-125432-001-00 1.8	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（４版）

改版履歴

版数	日付	内容
1.0	2026/1/5	新規作成
2.0	2026/1/20	#13376、#13634、#15848 の追加
3.0	2026/2/6	#17251 の追加
4.0	2026/4/23	#17880 の追加

目次

1章 QX-S1100G 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-S1100G シリーズ Ethernet スイッチ オペレーションマニュアル

02-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。

06-ACL and QoS

1.1.3 走査順

■管理情報

区分	管理番号
変更	#17880

■内容

変更前）

インバースマスク（inverse mask）と呼ばれるワイルドカードマスクは、10 進数表示のドット表示で表される 32 ビットバイナリです。ネットマスクの 0 は“一致する（do care）”ビットと表現され、1 は“無視する（don’t care）”ビットと表現されます。サブネットマスクの 0 と 1 を反転したものとは異なります。IP アドレスが“do care”ビットである場合、一致させ、“無視する（don’t care）”ビットである場合、無視されます。ワイルドマスクが 0.255.255.255、ネットマスクが 192.168.1.1 の場合、最初の 0 は”一致する（do care）"ビットで、２番目以降が“無視する（don’t care）”ビットであるため、192.0.0.0 のネットワークに一致する ACL となります。ワイルドカードマスクの 0 と 1 は非連続にすることができます。たとえば 0.255.0.255 は有効なワイルドマスクです。

変更後）

インバースマスク（inverse mask）と呼ばれるワイルドカードマスクは、10 進数表示のドット表示で表される 32 ビットバイナリです。ネットマスクの 0 は“一致する（do care）”ビットと表現され、1 は“無視する（don’t care）”ビットと表現されます。サブネットマスクの 0 と 1 を反転したものとは異なります。IP アドレスが“do care”ビットである場合、一致させ、“無視する（don’t care）”ビットである場合、無視されます。ワイルドマスクが 0.255.255.255、ネットマスクが 192.168.1.1 の場合、最初の 0 は”一致する（do care）"ビットで、２番目以降が“無視する（don’t care）”ビットであるため、192.0.0.0 のネットワークに一致する ACL となります。ワイルドカードマスクの 0 と 1 は非連続にすることができます。たとえば 0.255.0.255 は有効なワイルドマスクです.

メモ：

・標準 IPv4 ACL、拡張 IPv4 ACL のマスク値は、インバースマスクとなります。
0 は "一致する(do care)" ビット、1 は "無視する(don’t care)" ビットとなります。

・標準 IPv6 ACL、拡張 IPv6 ACL、L2 ACL のマスク値は、インバースマスクではありません。
1 は "一致する(do care)" ビット、0 は "無視する(don’t care)" ビットとなります。

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。

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。

09-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。

3章 QX-S1100G シリーズ Ethernet スイッチ コマンドマニュアル

02-アクセス

1.1.11 ifmonitor crc-error

デフォルト

■管理情報

区分	管理番号
変更	#13251

■内容

変更前）

上限しきい値は 1000 です。下限しきい値は 100 です。統計情報収集および比較間隔は 10 秒です。

変更後）

上限しきい値は 1000 です。下限しきい値は 100 です。統計情報収集および比較間隔は 30 秒です。

1.1.12 ifmonitor input-error

デフォルト

■管理情報

区分	管理番号
変更	#13251

■内容

変更前）

上限しきい値は 1000 です。下限しきい値は 100 です。統計情報収集および比較間隔は 10 秒です。

変更後）

上限しきい値は 1000 です。下限しきい値は 100 です。統計情報収集および比較間隔は 30 秒です。

1.1.13 ifmonitor output-error

デフォルト

■管理情報

区分	管理番号
変更	#13251

■内容

変更前）

上限しきい値は 1000 です。下限しきい値は 100 です。統計情報収集および比較間隔は 10 秒です。

変更後）

上限しきい値は 1000 です。下限しきい値は 100 です。統計情報収集および比較間隔は 30 秒です。

06-ACL and QoS

1.1.11 packet-filter

説明

■管理情報

区分	管理番号
変更	#10704

■内容

変更前）
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）
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。

07-セキュリティ

3.1.10 mac-authentication parallel-with-dot1x

I. 説明

■管理情報

区分	管理番号
変更	#17251

■内容

変更前）

undo mac-authentication parallel-with-dot1x コマンドはデフォルトに戻します。

変更後）

undo mac-authentication parallel-with-dot1x コマンドはポートで MAC アドレス認証と 802.1X 認証の並列処理を無効にします。

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 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。

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: プライマリ RADIUS 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: 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。

3.1.12 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。