

QX-S4200G 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-S4200G シリーズ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-S4200G シリーズ Ethernet スイッチ インストールマニュアル	GVT-243239-001-00 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-S4200G シリーズ Ethernet スイッチ オペレーションマニュアル	GVT-243240-001-00 1.1	機能の設定について説明 しています。
QX-S4200G シリーズ Ethernet スイッチ コマンドマニュアル	GVT-243241-001-00 1.0	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9月（5版）

改版履歴

版数	日付	内容
1.0	1/14	新規作成
2.0	1/26	#13376、#13634 の追加
3.0	2/16	#16909 の追加
4.0	3/18	#19603 の追加
5.0	9/28	・ #20290 の追加 ・ #11731 の追加 ・ 3 章「QX-S1100G シリーズ Ethernet スイッチ コマンドマニュアル」について、セキュリティの章の番号誤記修正

目次

1 章 QX-S4200G シリーズ Ethernet スイッチ インスタレーションマニュアル	6
2 章 QX-S4200G シリーズ Ethernet スイッチ オペレーションマニュアル	8
03-アクセス	9
9.3 ループ検出の有効化	9
14.2 制限とガイドライン	10
08-セキュリティ	11
4.8 MAC アドレス 認証タイマの設定	11
09-高可用性	12
5.3.2 Smart Link グループのプロテクト VLAN の設定	12
3 章 QX-S4200G シリーズ Ethernet スイッチ コマンドマニュアル	14
04-IP サービス	15
20.1.1 http-redirect https-port	15
03-アクセス	16
14.1.2 vlan mapping	16
08-セキュリティ	17
1.3.9 primary authentication (RADIUS scheme view)	17
1.3.20 secondary authentication (RADIUS scheme view)	18
3.1.12 mac-authentication timer (system view)	19
09-装置管理	20
9.1.22 display transceiver diagnosis	20

1 章 QX-S4200G シリーズ Ethernet スイッチ インストールMANUAL

追加および変更はありません。

2 章 QX-S4200G シリーズ Ethernet スイッチ オペレーションマニュアル

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。

14.2 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 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 タグを追加するには、VLAN マッピングと QinQ の両方を設定することができます。設定の競合が発生した場合は、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することができます。設定の競合が発生した場合は、QoS ポリシーが適用されます。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 タグを追加するには、VLAN マッピングと QinQ の両方を設定することができます。設定の競合が発生した場合は、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することができます。設定の競合が発生した場合は、QoS ポリシーが適用されます。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。

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

5.3.2 Smart Link グループのプロテクト VLAN の設定

■管理情報

区分	管理番号
変更	#20290

■内容

変更前)



重要：

pvst mode を設定している装置で Smart Link を使用する場合は、以下の通りに **protected-vlan reference-instance** コマンドを指定してください。**reference-instance** の値が正しく指定されていない場合は、Smart Link の STANDBY ポートがパケットを転送します。

- ・ **stp global enable** コマンド設定なし

protected-vlan reference-instance 0 コマンドを設定します。

- ・ **stp global enable** コマンド設定あり

Smart Link の対象となる vlan の ID が 145 以上の場合は **protected-vlan reference-instance 0** を設定します。それ以外の vlan の場合は、該当する vlan と同じ ID を instance に設定します。たとえば、VLAN 100 を使用する場合は **protected-vlan reference-instance 100** を設定します。

変更後)

**重要：**

pvst mode を設定している装置で Smart Link を使用する場合は、以下の通りに **protected-vlan reference-instance** コマンドを指定してください。**reference-instance** の値が正しく指定されていない場合は、Smart Link の STANDBY ポートがパケットを転送します。

- ・ **stp global enable** コマンド設定なし

protected-vlan reference-instance 0 コマンドを設定します。

- ・ **stp global enable** コマンド設定あり

VLAN の個数が 128 個までは、VLAN ID=インスタンス ID でマッピングされます。129 個目以降の VLAN は全て、インスタンス 0 にマッピングされます。

例) **vlan 1, 3, 5, 200** を定義している場合、以下のように自動的にマッピングされます。

Instance	VLANs Mapped
0	2, 4, 6 to 199, 201 to 4094
(未定義の VLAN、または、129 個目以降の VLAN は 0 にマッピングされる)	
1	1
3	3
5	5
200	200

注) **display stp region-configuration** は、MSTP モード時しか利用できず、PVST モード時は、実際の MSTI マッピング状態を確認できません。

Smart Link の対象となる vlan の ID が、VLAN ID=インスタンス ID でマッピングされた vlan の場合は、**protected-vlan reference-instance** に該当する vlan と同じ ID を instance に設定します。Smart Link の対象となる vlan の ID が、インスタンス 0 にマッピングされている場合は、**protected-vlan reference-instance 0** を設定します。

たとえば、VLAN 100 を使用する場合は、**protected-vlan reference-instance 100** を設定します。しかし、VLAN 200 を使用する場合は、定義された VLAN の数により、vlan と同じ ID または 0 のどちらを指定すべきか判断する必要があります。

3 章 QX-S4200G シリーズ Ethernet スイッチ コマンドマニュアル

04-IP サービス

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。**

03-アクセス

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。

08-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。

09-装置管理

9.1.22 display transceiver diagnosis

■管理情報

区分	管理番号
削除	#11731

■内容

変更後)

“9.1.22 display transceiver diagnosis” 節の全体を削除