
IP8800/S2340 ソフトウェアマニュアル

訂正資料

Ver.2.7 以降対応版

■はじめに

このマニュアルは、以下に示す IP8800/S2340 ソフトウェアマニュアルからの変更内容を記載しています。

マニュアル名	マニュアル番号	発行
IP8800/S2340 ソフトウェアマニュアル コンフィグレーションガイド Vol.1 (Ver.2.7 対応)	IP88S23-S001-80	2024 年 12 月
IP8800/S2340 ソフトウェアマニュアル コンフィグレーションガイド Vol.2 (Ver.2.7 対応)	IP88S23-S002-80	2024 年 12 月
IP8800/S2340 ソフトウェアマニュアル コンフィグレーションコマンドレファレンス (Ver.2.7 対応)	IP88S23-S003-80	2024 年 12 月
IP8800/S2340 ソフトウェアマニュアル 運用コマンドレファレンス (Ver.2.7 対応)	IP88S23-S004-80	2024 年 12 月
IP8800/S2340 ソフトウェアマニュアル メッセージ・ログレファレンス (Ver.2.7 対応)	IP88S23-S005-80	2024 年 12 月
IP8800/S2340 ソフトウェアマニュアル MIB レファレンス (Ver.2.7 対応)	IP88S23-S006-80	2024 年 12 月

■商標一覧

Cisco は、米国 Cisco Systems, Inc. の米国および他の国々における登録商標です。
Ethernet は、富士フイルムビジネスイノベーション株式会社の登録商標です。
GSRP は、アラクサラネットワークス株式会社の登録商標です。
Microsoft は、米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。
OpenSSL は、米国およびその他の国における米国 OpenSSL Software Foundation の登録商標です。
Python は、Python Software Foundation の登録商標です。
RSA および RC4 は、米国およびその他の国における米国 EMC Corporation の登録商標です。
sFlow は、米国およびその他の国における米国 InMon Corp. の登録商標です。
ssh は、SSH Communications Security, Inc. の登録商標です。
UNIX は、The Open Group の米国ならびに他の国における登録商標です。
Windows は、米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。
イーサネットは、富士フイルムビジネスイノベーション株式会社の登録商標です。
そのほかの記載の会社名、製品名は、それぞれの会社の商標もしくは登録商標です。

■マニュアルはよく読み、保管してください。

製品を使用する前に、安全上の説明をよく読み、十分理解してください。
このマニュアルは、いつでも参照できるよう、手近な所に保管してください。

■ご注意

このマニュアルの内容については、改良のため、予告なく変更する場合があります。

■発行

2026 年 1 月 (初版) 855-040096-230-A 1N

■著作権

Copyright(C) NEC Corporation 2026. All rights reserved.

目次

第 1 編 コンフィグレーションガイド Vol.1	4
第 2 編 コンフィグレーションガイド Vol.2	11
第 3 編 コンフィグレーションコマンドレファレンス	24
第 4 編 運用コマンドレファレンス	32
第 5 編 メッセージ・ログレファレンス	38
第 6 編 MIB レファレンス	40

15 ソフトウェアの管理

15.1 ソフトウェアのアップデートの解説

15.1.2 アップデートの準備

削除

(2) 内蔵フラッシュメモリ容量を確保する方法 [Ver1.0 以降]

(2) 内蔵フラッシュメモリ容量を確保する方法

内蔵フラッシュメモリ容量が不足している場合は、次に示す方法で未使用容量を確保してください。

- ・ /usr/var/core/配下のファイルを運用コマンド rm で削除する。
- ・ ~~運用コマンド erase protocol dump を実行する。~~
- ・ 運用コマンド squeeze を実行する。
- ・ ユーザ領域に保存しているユーザファイルを削減する。

24 VLAN

24.7 MAC VLAN の解説

24.7.4 MAC ポートの VLAN 設定

変更

[Ver2.8 以降]

MAC ポートに VLAN を設定する場合、コンフィグレーションコマンド `switchport mac vlan` による設定と、レイヤ 2 認証機能による動的な設定ができます。

また、同じ MAC ポートでコンフィグレーションコマンド `switchport mac vlan` による VLAN 設定と、レイヤ 2 認証機能により動的な VLAN 設定を共存させる使い方ができます。同じ MAC ポートに共存させる場合は、コンフィグレーションコマンド `no switchport mac auto-vlan` を設定しないでください。

動的に VLAN が設定できるレイヤ 2 認証機能と認証モードを次の表に示します。

24.8 MAC VLAN のコマンドガイド

24.8.1 コマンド一覧

追加

表 24-12 コンフィグレーションコマンド一覧 [Ver2.8 以降]

表 24-12 コンフィグレーションコマンド一覧

コマンド名		説明
mac-address		MAC VLAN で VLAN に所属する端末の MAC アドレスをコンフィグレーションによって設定します。
switchport auto-vlan	mac	no switchport mac auto-vlan コマンドで、認証機能による認証後 VLAN が switchport mac vlan コマンドで指定された VLAN と一致するときだけ通信できるようにします。
switchport mac		MAC ポートの VLAN を設定します。
switchport mode		ポートの種類（MAC、トランク）を設定します。
switchport trunk		トランクポートの VLAN を設定します。
vlan		mac-based パラメータを指定して MAC VLAN を作成します。

24.8.3 MAC ポートのネイティブ VLAN の設定

変更

[設定のポイント] [Ver2.8 以降]

[設定のポイント]

MAC ポートで MAC VLAN に登録した MAC アドレスに一致しない Untagged フレームを扱いたい場合、そのフレームを扱う VLAN としてネイティブ VLAN を設定します。ネイティブ VLAN はポート VLAN と MAC VLAN が設定できます。

ネイティブ VLAN の VLAN ID を switchport mac native vlan コマンドで指定すると、MAC ポート上で登録した MAC アドレスに一致しない Untagged フレームを扱う VLAN となります。ネイティブ VLAN は、コンフィグレーションで明示して指定しない場合は VLAN 1（デフォルト VLAN）です。

ネイティブ VLAN に state suspend コマンドが設定されていた場合は、登録した MAC アドレスに一致しないフレームが中継されません。

26 スパニングツリー

26.1 スパニングツリーの解説

26.1.2 スパニングツリーの種類

追加

表 26-2 スパニングツリーの組み合わせと適用範囲 [Ver1.0 以降]

表 26-2 スパニングツリーの組み合わせと適用範囲

ツリー構築条件	トポロジー計算結果の適用範囲
PVST+単独	<p>PVST+が動作している VLAN には VLAN ごとのスパニングツリーを適用します。そのほかの VLAN はスパニングツリーを適用しません。</p> <p>本装置では、デフォルトでポート VLAN 上で PVST+が動作します。</p> <p>スパニングツリーを使用しない場合は、意図しないトポロジー変更で通信への影響が生じないように、コンフィグレーションコマンド <code>spanning-tree disable</code> を設定しておくことをお勧めします。</p>
シングルスパニングツリー単独	<p>全 VLAN にシングルスパニングツリーを適用します。</p> <p>PVST+をすべて停止した構成です。</p>
PVST+とシングルスパニングツリーの組み合わせ	<p>PVST+が動作している VLAN には VLAN ごとのスパニングツリーを適用します。そのほかの VLAN にはシングルスパニングツリーを適用します。</p>
マルチプルスパニングツリー単独	<p>全 VLAN にマルチプルスパニングツリーを適用します。</p>

5 レイヤ2 認証

5.1 概要

5.1.3 MAC VLAN の動的 VLAN 設定とレイヤ 2 認証

削除

[Ver2.8 以降]

なお、コンフィグレーションコマンド `switchport mac vlan` が設定されている認証対象の MAC ポートでは、コンフィグレーションコマンドで設定された認証後 VLAN 以外の VLAN 切り替えはできません。さらに、認証対象の MAC ポートに動的に VLAN が設定されている状態で、コンフィグレーションコマンド `switchport mac vlan` が設定された場合、該当ポートに動的に設定された VLAN を認証後 VLAN とした認証端末はすべて認証が解除されます。

5.2 レイヤ2 認証と他機能との共存について

5.2.1 レイヤ2 認証と他機能との共存

変更

表 5-5 他機能との共存仕様 [Ver2.8 以降]

表 5-5 他機能との共存仕様

レイヤ 2 認証	機能名		共存仕様
IEEE802.1X	:		
	VLAN	ポート VLAN	固定 VLAN モードで使用できます。
		プロトコル VLAN	装置で同時に使用できません。
		MAC VLAN	ダイナミック VLAN モードで使用できます。 コンフィグレーションコマンド <code>mac-address</code> で設定した MAC アドレスも認証の対象となります。
	VLAN 拡張 機能	VLAN トンネリング	装置で同時に使用できません。
		EAPOL フォワーディング	装置で同時に使用できません。
	スパニングツリー		使用できますが、認証ポートには <code>PortFast</code> と <code>BPDU</code> フィルタを設定して、スパニングツリーを動作させないでください。
	:		
Web 認証	:		
	VLAN	ポート VLAN	固定 VLAN モードで使用できます。
		プロトコル VLAN	装置で同時に使用できません。
		MAC VLAN	ダイナミック VLAN モードで使用できます。 コンフィグレーションコマンド <code>mac-address</code> で設定した MAC アドレスも認証の対象となります。
	VLAN 拡張 機能	VLAN トンネリング	装置で同時に使用できません。
		EAPOL フォワーディング	共存できます。
	スパニングツリー		使用できますが、認証ポートには <code>PortFast</code> と <code>BPDU</code> フィルタを設定して、スパニングツリーを動作させないでください。
:			
MAC 認証	:		
	VLAN	ポート VLAN	固定 VLAN モードで使用できます。
		プロトコル VLAN	装置で同時に使用できません。
		MAC VLAN	ダイナミック VLAN モードで使用できます。 コンフィグレーションコマンド <code>mac-address</code> で設定した MAC アドレスも認証の対象となります。

レイヤ2 認証	機能名		共存仕様
	VLAN 拡張 機能	VLAN トンネリング	装置で同時に使用できません。
		EAPOL フォワーディング	共存できます。
	スパニングツリー		使用できますが、認証ポートには PortFast と BPDU フィルタを設定して、スパニングツリーを動作させないでください。
			:

5.3 レイヤ 2 認証共通の機能

追加

[Ver2.8 以降]

レイヤ 2 認証共通の機能について説明します。

- ・ 認証前端末の通信許可
- ・ 認証数制限
- ・ 強制認証
- ・ 認証済み端末のポート間移動および認証対象外ポートへ移動時の認証解除
- ・ RADIUS サーバ通信の `dead interval` 機能
- ・ MAC ポートに `dot1q` 設定時の動作
- ・ リンクダウン時の認証解除の抑止
- ・ ダイナミック ACL/QoS
- ・ RADIUS 認証方式のダイナミック VLAN モードにおける認証後 VLAN の決定
- ・ 動的 VLAN 設定とコンフィグレーションコマンドの併用
- ・ MAC VLAN のネイティブ VLAN 設定

5.3.4 認証済み端末のポート間移動および認証対象外ポートへ移動時の認証解除

変更

[Ver2.8 以降]

レイヤ 2 認証で認証された端末をほかのポートに移動した場合、ポートの状態や認証状態がどのように変わるか説明します。

認証済み端末のポート間移動には次の図に示す四つのケースがあります。

：

なお、MAC VLAN を使用した場合、次のようにケース 1 とケース 2 を判定します。

ケース 1：

移動先の認証対象ポートで、次の条件をすべて満たしている場合は、同一の VLAN への移動と見なします。

- ・ コンフィグレーションコマンド `no switchport mac auto-vlan`、または `switchport mac vlan` の設定が以下のどれかにあてはまる
 - ・ コンフィグレーションコマンド `no switchport mac auto-vlan` を設定していない
 - ・ コンフィグレーションコマンド `no switchport mac auto-vlan` を設定しているが、コンフィグレーションコマンド `switchport mac vlan` を設定していない
 - ・ コンフィグレーションコマンド `no switchport mac auto-vlan` を設定しているが、コンフィグレーション

ンコマンド `switchport mac vlan` で同じ VLAN ID を設定している

- ・コンフィグレーションコマンド `switchport mac native vlan` で同じ VLAN ID を設定している
- ・Web 認証と MAC 認証で、コンフィグレーションコマンド `switchport mac dot1q vlan` を設定していない、または同じ VLAN ID を設定している

ケース 2 :

移動先の認証対象ポートで、上記の条件をひとつでも満たさない場合は、異なる VLAN への移動と見なします。

変更

表 5-13 Web 認証でのポート間移動時の動作（固定 VLAN モード）[Ver2.1 以降]

表 5-15 MAC 認証でのポート間移動時の動作（固定 VLAN モード）[Ver2.1 以降]

表 5-16 MAC 認証でのポート間移動時の動作（ダイナミック VLAN モード）[Ver2.1 以降]

表 5-13 Web 認証でのポート間移動時の動作（固定 VLAN モード）

ケース	移動先ポート	VLAN	認証状態	移動後の通信可否
1	認証対象ポート	同一 VLAN	移動先ポートで認証状態を継続	通信可
:	:	:	:	:

表 5-15 MAC 認証でのポート間移動時の動作（固定 VLAN モード）

ケース	移動先ポート	VLAN	認証状態	移動後の通信可否
1	認証対象ポート	同一 VLAN	移動先ポートで認証状態を継続	通信可
:	:	:	:	:

表 5-16 MAC 認証でのポート間移動時の動作（ダイナミック VLAN モード）

ケース	移動先ポート	VLAN	認証状態	移動後の通信可否
1	認証対象ポート	同一 VLAN	移動先ポートで認証状態を継続	通信可
:	:	:	:	:

追加

[ポート移動時の注意] [Ver2.8 以降]

(4) マルチステップ認証でのポート間移動の動作

:

[ポート移動時の注意]

- 1 認証ポート間で認証済み端末のポート移動をする場合は、移動前のポートと移動先のポートで、レイ

ヤ 2 認証と VLAN のコンフィグレーションの設定を合わせてください。次に示すケースでは、ポート間移動ができません。

- MAC ポートの VLAN に所属している認証済みの端末が、同一 VLAN で、かつ MAC ポート以外の認証ポートに移動した場合、移動前のポートでの認証状態は解除されません。
- 移動前ポートでダイナミック VLAN モードの認証済み端末が所属する VLAN と、移動先ポートでコンフィグレーションコマンド `switchport mac dot1q vlan` に設定している VLAN が同一の場合、移動前ポートの認証状態は解除されません。
- 異なるレイヤ 2 認証の認証ポート、または認証対象外ポートへポートを移動した場合（例えば、IEEE802.1X のポートから MAC 認証のポートへポートを移動した場合）、移動前のポートでの認証状態が解除されないことがあります。
- 移動先のポートが IEEE802.1X のシングルモードまたはマルチモードの認証対象ポートの場合、ポート移動を検知できず、移動前のポートでの認証状態が解除されないことがあります。
- マルチステップ認証ポートとシングル認証の認証ポートでポートを移動した場合（例えば、マルチステップ認証ポートから MAC 認証のポート（固定 VLAN モード）へポートを移動した場合）、移動元のポートでの認証状態が解除されないことがあります。
- 固定 VLAN モード、ダイナミック VLAN モードによらず、スパニングツリーを設定した装置では、認証ポート間のポート移動を検知できず、移動前ポートでの認証状態は解除されません。
- コンフィグレーションコマンド `no switchport mac auto-vlan` を設定している認証ポートへポート移動した場合、移動前ポートでの認証状態は解除されません。

上記のどの場合でも、移動元のポートに認証状態が残り、移動先のポートで該当端末の通信はできないため、次のどれかの運用コマンドを使用して、該当端末を認証解除する必要があります。

- IEEE802.1X : `clear dot1x auth-state` コマンド
- MAC 認証 : `clear mac-authentication auth-state` コマンド
- Web 認証 : `clear web-authentication auth-state` コマンド

5.3.9-1 動的 VLAN 設定とコンフィグレーションコマンドの併用について

追加

5.3.9-1 動的 VLAN 設定とコンフィグレーションコマンドの併用について [Ver2.8 以降]

レイヤ 2 認証（ダイナミック VLAN モード）では、認証成功時に RADIUS 認証方式やローカル認証方式により、指定する VLAN（認証後 VLAN）へ端末の通信を切り替えます。認証後 VLAN は、レイヤ 2 認証に成功したタイミングで行う動的 VLAN 設定と、コンフィグレーションコマンド `switchport mac vlan` で設定する 2 種類の方法があります。

本装置では同一の MAC ポートで、ある端末は認証後に動的 VLAN へ切り替え、別の端末は認証後にコンフィグレーションコマンド `switchport mac vlan` で設定した VLAN へ切り替えるといったことができます。

コンフィグレーションコマンド `switchport mac vlan` で設定した VLAN は、認証済み端末がいないときでも、該当の VLAN で他のポートから認証ポートへの通信ができます。

なお、コンフィグレーションコマンド `switchport mac vlan` を設定した MAC ポートで、コンフィグレーションコマンド `no switchport mac auto-vlan` を設定することで、動的 VLAN 設定によるレイヤ 2 認証を不可とすることもできます。以下に設定の組み合わせと、そのときのレイヤ 2 認証の可否を示します。

表 5-25-1 動的 VLAN 設定と `switchport mac vlan` コマンドの VLAN におけるレイヤ 2 認証可否

no switchport mac auto-vlan 設定	switchport mac vlan 設定	レイヤ 2 認証可否	
		動的 VLAN 設定による VLAN	switchport mac vlan を設定している VLAN
設定あり	設定あり	不可	可
	設定なし	可	—
設定なし	設定あり	可	可
	設定なし	可	—

（凡例）可:レイヤ 2 認証可能 不可:レイヤ 2 認証不可 —:対象外

5.3.9-2 MAC ポートのネイティブ VLAN 設定

追加

5.3.9-2 MAC ポートのネイティブ VLAN 設定 [Ver2.8 以降]

コンフィグレーションコマンド `switchport mac native vlan` で MAC ポートに設定する VLAN には、ポート VLAN または MAC VLAN を指定することができますが、どちらの VLAN を指定しても、ネイティブ VLAN の動作に違いはありません。

なお、ネイティブ VLAN に MAC VLAN を設定した場合、当該 MAC ポートでは、指定した VLAN を MAC VLAN としては扱わず、ネイティブ VLAN として扱います。

5.4 レイヤ 2 認証使用時の注意事項

5.4.1 本装置の設定および状態変更時の注意

追加

(6) MAC ポートのコンフィグレーション変更での注意 [Ver2.8 以降]

(6) MAC ポートのコンフィグレーション変更での注意

証端末が接続されている MAC ポートに対して、以下のコンフィグレーションを変更した場合、該当ポートの端末を認証解除します。

なお、認証端末を接続している状態でコンフィグレーションを変更すると、コンフィグレーション変更中の端末の認証動作に影響を与えるおそれがあります。そのため、該当ポートに対してコンフィグレーションコマンド `shutdown` を実行して、運用コマンド `clear dot1x auth-state`, `clear web-authentication auth-state`, または `clear mac-authentication auth-state` で端末の認証状態を解除して認証端末が接続されていない状態にしたあと、約 60 秒の間隔をおいてからコンフィグレーションを変更してください。コンフィグレーションを変更したあと、該当ポートに対してコンフィグレーションコマンド `no shutdown` を実行してください。

- `switchport mac auto-vlan` コマンド
- `switchport mac vlan` コマンド
- `switchport mac native vlan` コマンド
- `switchport mac dot1q vlan` コマンド

6 IEEE802.1X の解説

6.1 IEEE802.1X の概要

6.1.1 サポート機能

変更

表 6-4 認証で使用する属性名（その3 Access-Accept）[Ver1.0 以降]

表 6-4 認証で使用する属性名（その3 Access-Accept）

属性名	Type 値	説明
Service-Type	6	提供するサービスタイプ。 Framed(2)固定。
:	:	:
Message-Authenticator	80	RADIUS/EAP パケットを保護するために使用する。
Tunnel-Private-Group-ID	81	VLAN を識別する文字列。Accept 時は、認証済みの Supplicant に割り当てる VLAN を意味する。ダイナミック VLAN モードだけ意味を持つ。 次に示す文字列が対応する。 (1)VLAN ID を示す文字列 (2)"VLAN"+VLAN ID を示す文字列 (3)コンフィグレーションコマンド name で指定した VLAN 名称を示す文字列 文字列にスペースを含んではいけない（含めた場合 VLAN 割り当ては失敗する）。 （設定例） VLAN10 の場合 (1)の場合 "10" (2)の場合 "VLAN10" (3)の場合 "business-office"
Acct-Interim-Interval	85	Interim パケット送信間隔(秒)。 60 以上を設定すると Interim パケットが送信される(60 未満では送信しない)。 この値を設定する場合、600 以上にすることを推奨する。600 未満にした場合ネットワークのトラフィックが増大するため注意が必要である。

9 Web 認証の設定と運用

9.3 SSL 証明書の準備

9.3.2 サーバ証明書と鍵の作成

追加

- (4) サーバ証明書を作成する [Ver2.1 以降]
- (5) 装置にインストールするための秘密鍵を生成する [Ver2.1 以降]

(4) サーバ証明書を作成する

-days オプションを使用して、有効期限を 365 日と設定したサーバ証明書 (server.crt) を作成する例を次の図に示します。認証局へサーバ証明書を依頼する場合はサーバ証明書の作成は不要です。

図 9-24 サーバ証明書の作成

```
unix# openssl x509 -in server.pem -out server.crt -req -signkey server.key -days 365
Signature ok
subject=/C=JP/ST=TOKYO/L=MINATOKU/O=NEC/OU=AX/CN=www.example.com/emailAddress=admin@example.com
Getting Private key
Enter pass phrase for server.key: *****
```

1. サーバ用のパスワードを入力します。

<-1

(5) 装置にインストールするための秘密鍵を生成する

装置にインストールするための秘密鍵 (serverinstall.key) を生成する例を次の図に示します。この秘密鍵は、サーバ証明書などを本装置へインストールするために必要です。

図 9-25 秘密鍵の生成

```
unix# openssl rsa -in server.key -out serverinstall.key
Enter pass phrase for server.key: *****
writing RSA key
```

1. サーバ用のパスワードを入力します。

<-1

第3編 コンフィグレーションコマンドレファレンス

12 SNMP

snmp-server host

変更

[注意事項] [Ver1.0 以降]

[注意事項]

1. `version` に 3 を設定していて、`snmp-server user` コマンドで設定されていないセキュリティユーザ名を本コマンドに設定した場合、本コマンドに設定したセキュリティユーザの情報は無効となりますので、ご注意ください。
2. `version` に 3 を設定していて、`<string>`で指定したセキュリティユーザのセキュリティレベルより高いセキュリティレベルを設定した場合は無効となります。
3. `poe` は、PoE 機能をサポートするモデルでだけ有効になります。

17 VLAN

switchport mac

変更

[パラメータ] [Ver2.8 以降]

[パラメータ]

native vlan <vlan id>

送信元 mac が未登録のフレームを受信する VLAN を設定します。設定した VLAN でフレームを送信することもできます。指定できる VLAN はポート VLAN または MAC VLAN です。

1. 本パラメータ省略時の初期値

省略できません

2. 値の設定範囲

「パラメータに指定できる値」を参照してください。

dot1q vlan <vlan id list>

本パラメータで設定した VLAN リストのフレームを Tagged フレームで送信します。また、本パラメータで設定した Tagged フレームを中継できます。設定した VLAN 以外の VLAN で Tagged フレームを受信した場合は廃棄します。

~~vlan パラメータで設定した VLAN は指定できません。~~

1. 本パラメータ省略時の初期値

省略できません

2. 値の設定範囲

<vlan id list>の指定方法、また、値の設定範囲については「パラメータに指定できる値」を参照してください。

dot1q vlan add <vlan id list>

このポートで Tagged フレームが中継可能な VLAN を VLAN リストに追加します。~~vlan パラメータで設定した VLAN は指定できません。~~

1. 本パラメータ省略時の初期値

省略できません

2. 値の設定範囲

<vlan id list>の指定方法、また、値の設定範囲については「パラメータに指定できる値」を参照してください。

追加

[注意事項] [Ver2.8 以降]

1. `no switchport mac auto-vlan` コマンド設定時は、有効な MAC VLAN が一つも設定されていない場合だけ、認証機能による認証後 VLAN に指定された MAC VLAN で通信できます。
2. `no switchport mac auto-vlan` コマンド設定時は、有効な MAC VLAN が設定された場合、認証機能による認証後 VLAN に指定された MAC VLAN は、設定された MAC VLAN と一致するときだけ通信できます。このため、有効な MAC VLAN が一つも設定されていない状態で、認証済みとしていた端末が存在している場合、有効な MAC VLAN を設定すると、端末の認証は解除されます。

switchport mac auto-vlan

追加

switchport mac auto-vlan コマンドを新規追加 [Ver2.8 以降]

no switchport mac auto-vlan コマンドで、認証機能による認証後 VLAN が switchport mac vlan コマンドで指定された VLAN と一致するときだけ通信できるようにします。

[入力形式]

情報の設定

```
no switchport mac auto-vlan
```

情報の削除

```
switchport mac auto-vlan
```

[入力モード]

(config-if)

イーサネットインタフェース、ポートチャネルインタフェース

[パラメータ]

なし

[コマンド省略時の動作]

認証機能による認証後 VLAN と switchport mac vlan コマンドで指定された VLAN との突合せをしません。

[通信への影響]

なし

[設定値の反映契機]

設定値変更後、すぐに運用に反映されます。

[注意事項]

1. 本コマンドを設定すると、認証済みとしていた端末が存在している場合、端末の認証は解除されます。

43 コンフィグレーション編集時のエラーメッセージ

43.1 コンフィグレーション編集時のエラーメッセージ

43.1.13 VLAN 情報

追加

表 43-13 VLAN のエラーメッセージ [Ver2.8 以降]

表 43-13 VLAN のエラーメッセージ

メッセージ	内容
Can not change mode from <value1> to <value2>.	<p>すでに VLAN 種別に<value1>が指定されているため、<value2>に変更できません。指定した VLAN 種別に変更するには、対象 VLAN を削除してから再設定してください。</p> <p><value1>, <value2> : VLAN 種別</p> <ul style="list-style-type: none"> • port-based : ポート VLAN • protocol-based : プロトコル VLAN • mac-based : MAC VLAN
:	:
Relations between vlan in dot1q configuration and native configuration are inconsistent.	switchport mac dot1q vlan と switchport mac native vlan で、同じ VLAN を指定しているため設定できません。
Relations between vlan in mac-address-table static configuration and switchport configuration are inconsistent.	mac-address-table static の vlan 指定と switchport のコンフィグレーションが不一致です。mac-address-table static で指定された vlan は、指定されたインタフェースの switchport access/switchport trunk allowed vlan で指定されていなければなりません。
Relations between vlan in native configuration and mac vlan configuration are inconsistent.	switchport mac native vlan と switchport mac vlan で、同じ VLAN を指定しているため設定できません。
Relations between vlan-tunneling and IP configuration are inconsistent.	VLAN トンネリングと IP 情報の関係が不一致です。VLAN トンネリング設定時は、IP 情報を設定できません。
:	:

21 リンクアグリゲーション

show channel-group

追加

表 21-3 リンクアグリゲーション詳細情報表示項目 [Ver1.0 以降]

表 21-3 リンクアグリゲーション詳細情報表示項目

表示項目	意味	表示詳細情報
Reason	障害要因	- : Status が"Up"
		Standby : 自チャネルグループのポートがスタンバイ状態
		CH Disabled : 自チャネルグループが Disable 状態
		Port Down : 自チャネルグループのポートが DOWN
		Duplex Half : 自チャネルグループ内ポートの Duplex モードが Half
		Port Speed Unmatch : 自チャネルグループ内の他ポートと回線速度が不一致
		Port Selecting : 自チャネルグループへのポートアグリゲーション条件チェック実施中
		:

34 Web 認証

show web-authentication logging

追加

表 34-5 動作ログメッセージ一覧 [Ver2.8 以降]

表 34-5 動作ログメッセージ一覧

番号	ログ識別	ログ種別	メッセージテキスト
			内容と対応
			付加情報
23	NOTICE	LOGIN	Login failed ; L2MacManager failed.
			L2MAC 管理プログラムから認証できない通知が届いたために、認証に失敗しました。
			[対応] 再度、ログイン操作をしてください。本メッセージが頻繁に出力される場合は、restart vlan mac-manager コマンドを実行してください。
			MAC アドレス，ユーザ名

35 MAC 認証

show mac-authentication

変更

表 35-5 MAC 認証のコンフィグレーションの表示項目 [Ver2.4 以降]

表 35-5 MAC 認証のコンフィグレーションの表示項目

表示項目	意味	表示詳細情報
Auto-logout	アクセスがない状態が続いたことを検出したときの認証解除設定	該当する MAC アドレスから, アクセスがない状態が続いたことを検出したときの認証解除機能の状態 enable : アクセスがない状態を検出したときの認証解除機能有効 disable : アクセスがない状態を検出したときの認証解除機能無効

2 イベント発生部位形式

2.8 PORT

追加

表 2-15 イベント発生部位 PORT の運用メッセージ [Ver1.0 以降]

表 2-15 イベント発生部位 PORT の運用メッセージ

メッセージ 識別子	イベント レベル	メッセージテキスト
		内容と対応
25011500	E4	Transceiver not supported.
		<p>未サポートのトランシーバを検出しました。</p> <p>なお、オプションライセンス（アップリンク 10G）を未設定のときに、SFP+/SFP 共用ポートに SFP+のトランシーバを挿入したときにも出力されます。</p> <p>[対応]</p> <p>「ハードウェア取扱説明書」のトランシーバの章を参照して、該当ポート番号でサポートしているトランシーバを挿入してください。</p>

第6編 MIB レファレンス

追加および変更はありません。