AX2630S ソフトウェアマニュアル

訂正資料

Ver.2.0 以降対応版

AlaxalA

■はじめに

このマニュアルは，以下に示す AX2630S 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
AX2630S 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.2.0 対応）	AX26S-S001	2022 年 3 月
AX2630S 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.2.0 対応）	AX26S-S002	2022 年 3 月
AX2630S 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.2.0 対応）	AX26S-S003	2022 年 3 月
AX2630S ソフトウェアマニュアル 運用コマンドレファレンス（Ver.2.0 対応）	AX26S-S004	2022 年 3 月
AX2630S 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.2.0 対応）	AX26S-S005	2022 年 3 月
AX2630S ソフトウェアマニュアル MIB レファレンス（Ver.2.0 対応）	AX26S-S006	2022 年 3 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。
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

２０２２年６月　（第２版）　ＳＯＦＴ－ＡＭ－２６８８＿Ｒ１

■著作権

変更内容

■第 2 版の変更内容

表　変更内容

対象マニュアル名	追加・変更内容
コンフィグレーションガイド Vol.1	29　Ring Protocol とスパニングツリーの併用 29.1.2 動作仕様 30　IGMP snooping/MLD snooping の解説 30.3.1 MAC アドレスの学習 30.3.3 マルチキャストルータとの接続 30.3.4 クエリア機能 30.5 IGMP snooping/MLD snooping 使用時の注意事項
コンフィグレーションガイド Vol.2	1　フィルタ 1.1.7 フィルタ使用時の注意事項 7　IEEE802.1X の設定と運用 7.1.8 IEEE802.1X 認証状態の変更 8　Web 認証の解説 8.6 認証エラーメッセージ 12　マルチステップ認証 12.1.8 マルチステップ認証使用時の注意事項
コンフィグレーションコマンドレファレンス	17　VLAN vlan 19　Ring Protocol forwarding-shift-time 29　Web 認証 web-authentication ip address
運用コマンドレファレンス	32　IEEE802.1X clear dot1x statistics show web-authentication logging restart web-authentication 33　Web 認証 show web-authentication logging restart web-authentication 44　応答メッセージ 44.1.32　マルチステップ認証

なお，単なる誤字・脱字などはお断りなく訂正しました。

目次

29　Ring Protocol とスパニングツリーの併用

29.1 解説

29.1.2 動作仕様

変更

(6) リングポート以外のポートの一時的なブロッキングについて

変更前

Ring Protocol とスパニングツリーを併用する装置で，次に示すイベントが発生した場合，リングポート以外のスパニングツリーが動作しているポートを一時的にブロッキング状態にします。

・装置起動（装置再起動も含む）

・コンフィグレーションファイルのランニングコンフィグレーションへの反映

・restart vlan コマンド

・restart spanning-tree コマンド

スパニングツリーが仮想リンク経由の制御フレームを送受信できるようになる前にアクセスネットワーク内だけでトポロジを構築した場合，それだけではループ構成とならないためどのポートもブロッキングされません。したがって，このままでは，リングネットワークとアクセスネットワークにわたるループ構成となります。このため，本機能で一時的にブロッキングしてループを防止します。本機能は PortFast 機能を設定しているポートでも動作します。本機能でのブロッキングは，次のどちらかで行われます。

・イベント発生から 20 秒間

・イベント発生から 20 秒以内に仮想リンク経由で制御フレームを受信した場合は受信から 6 秒間

変更後

Ring Protocol とスパニングツリーを併用する装置で，次に示すイベントが発生した場合，リングポート以外のスパニングツリーが動作しているポートを一時的にブロッキング状態にします。

・装置起動（装置再起動も含む）

・コンフィグレーションファイルのランニングコンフィグレーションへの反映

・restart vlan コマンド

・restart spanning-tree コマンド

スパニングツリーが仮想リンク経由の制御フレームを送受信できるようになる前にアクセスネットワーク内だけでトポロジを構築した場合，それだけではループ構成とならないためどのポートもブロッキングされません。したがって，このままでは，リングネットワークとアクセスネットワークにわたるループ構成となります。このため，本機能で一時的にブロッキングしてループを防止します。本機能は PortFast 機能を設定しているポートでも動作します。本機能でのブロッキングは，使用しているスパニングツリー種別と状態により以下となります。

・PVST+/STP の場合，Rapid PVST+/Rapid STP/MSTP で本装置がルートブリッジの場合

イベント発生から 30 秒間

・Rapid PVST+/Rapid STP/MSTP で本装置が指定ブリッジの場合

イベント発生後，仮想リンク経由で BPDU 受信してから 4 秒間

30　IGMP snooping/MLD snooping の解説

30.3 IGMP snooping

30.3.1 MAC アドレスの学習

変更

(2) エントリの削除［Ver.2.1 以降］

変更前

注

Group Membership Interval は，Robustness Variable（RV）×Query Interval（QI）＋Query Response Interval（QRI）で算出します。

RV，QI，QRI の値を次に示します。

・他装置が代表クエリアで IGMPv3 で運用している場合

RV，QI=受信した Query メッセージから取得

QRI=10 秒

・自装置が代表クエリアで IGMPv3 で運用している場合，または IGMPv2 で運用している場合

RV=2

QI=コンフィグレーションコマンド ip igmp snooping query-interval で指定した時間

QRI=10 秒

変更後

注

Group Membership Interval は，Robustness Variable（RV）×Query Interval（QI）＋Query Response Interval（QRI）で算出します。

RV，QI，QRI の値を次に示します。

・他装置が代表クエリアで IGMPv3 で運用している場合

RV，QI，QRI=最後に受信した Query メッセージから取得

・自装置が代表クエリアで IGMPv3 で運用している場合，または IGMPv2 で運用している場合

RV=2

QI=コンフィグレーションコマンド ip igmp snooping query-interval で指定した時間

QRI= QI が 11 秒以上の場合は 10 秒，QI が 10 秒以下の場合は(QI – 1)秒

30.3.3 マルチキャストルータとの接続

変更

(2) マルチキャストルータポートの自動学習［Ver.2.1 以降］

変更前

(b) マルチキャストルータポートの保持時間

自動設定したマルチキャストルータポートの保持時間は，監視対象により異なります。
マルチキャストルータポートの保持時間を次の表に示します。

表 30-4　マルチキャストルータの保持時間

監視対象パケット	保持時間
IGMPv1 Membership Query メッセージ	Robustness Variable※1×Query Interval※2 + Query Response Interval※3 /2+X※4
IGMPv2 General Query メッセージ	
IGMPv3 General Query メッセージ※5	Robustness Variable×Query Interval+ Query Response Interval/2+X※4
IPv4 PIM-Hello メッセージ	受信した PIM-Hello メッセージの Holdtime オプションの値。Holdtime オプションが存在しない場合は 105 秒。

注※1

Robustness Variable は 2 固定。

注※2

デフォルト値は 125 秒。コンフィグレーションコマンド ip igmp snooping query-interval を設定した場合は，該当コマンドで指定した値。

注※3

デフォルト値は 10 秒。Query Interval が 10 秒以下の場合は，Query Interval の値。

注※4

コンフィグレーションコマンド ip igmp snooping mrouter discovery extension で指定した時間。

注※5

IGMPv3 Query メッセージの場合，Robustness Variable，Query Interval は，受信した Query メッセージから取得。Query Response Interval は 10 秒固定。

変更後

(b) マルチキャストルータポートの保持時間

自動設定したマルチキャストルータポートの保持時間は，監視対象により異なります。保持時間内に再度自動設定済のポートから監視対象パケットを受信した場合，該当する自動設定マルチキャストルータポートの保持時間を更新します。

マルチキャストルータポートの保持時間を次の表に示します。

表 30-4 マルチキャストルータポートの保持時間

監視対象パケット	保持時間
IGMPv1 Membership Query メッセージ	Robustness Variable※1×Query Interval※2 + Query Response Interval※3 /2+X※4
IGMPv2 General Query メッセージ	
IGMPv3 General Query メッセージ※5	Robustness Variable×Query Interval+ Query Response Interval/2+X※4
IPv4 PIM-Hello メッセージ	受信した PIM-Hello メッセージの Holdtime オプションの値※6。Holdtime オプションが存在しない場合は 105 秒。

注※1

Robustness Variable は 2 固定。

注※2

デフォルト値は 125 秒。コンフィグレーションコマンド ip igmp snooping query-interval を設定した場合は，該当コマンドで指定した値。

注※3

デフォルト値は 10 秒。Query Interval が 10 秒以下の場合は，Query Interval – 1 秒。

注※4

コンフィグレーションコマンド ip igmp snooping mrouter discovery extension で指定した時間。すでに学習した状態で値を変更した場合，保持時間を更新するときに変更後の値で反映する。

注※5

IGMPv3 Query メッセージの場合，Robustness Variable，Query Interval，Query Response Interval は，最後に受信した Query メッセージから取得。0.1 秒単位の部分は 1 秒単位に切り上げ。

注※6

PIM-Hello メッセージの Holdtime が 0 の場合は検知しません。また，すでに PIM 監視により自動設定している VLAN の該当ポートで Holdtime が 0 の PIM-Hello メッセージを受信した場合，保持時間は更新せずに PIM 監視により自動設定した当該マルチキャストルータポートは削除します。

変更
(2) マルチキャストルータポートの自動学習［Ver.2.1 以降］

変更前

(c) マルチキャストルータポートの削除

自動設定したマルチキャスルータルータポートは，保持時間中に該当ポートまたはチャネルグループで再度マルチキャストルータを検知しなければ，保持時間満了となり，自動的に削除します。

保持時間満了以外で自動設定したマルチキャストルータポートを削除する条件と削除対象を次に示します。

・運用コマンド clear igmp-snooping all を実行した場合

すべての VLAN の自動設定したすべてのマルチキャストルータポートを削除します。

・運用コマンド clear igmp-snooping mrouter を実行した場合

該当 VLAN の自動設定したすべてのマルチキャストルータポートを削除します。

・VLAN で IGMP snooping を無効にした場合

該当 VLAN の自動設定したすべてのマルチキャストルータポートを削除します。

・コンフィグレーションコマンド ip igmp snooping mrouter discovery igmp を削除した場合

該当 VLAN の IGMP 監視で自動設定したすべてのマルチキャストルータポートを削除します。

・コンフィグレーションコマンド ip igmp snooping mrouter discovery pim を削除した場合

該当 VLAN の PIM 監視で自動設定したすべてのマルチキャストルータポートを削除します。

・ポートまたはチャネルグループを VLAN から削除した場合

すべての VLAN の該当ポートまたは該当チャネルグループで自動設定したマルチキャストルータポートを削除します。

・ポートをチャネルグループに追加した際に，該当ポートをマルチキャストルータポートに自動設定している場合

すべての VLAN の該当ポートで自動設定したマルチキャストルータポートを削除します。

また，次に示す場合は削除しません。

・該当ポートまたはチャネルグループがリンクダウンした場合

・該当ポートまたはチャネルグループがスパニングツリーなどで Blocking 状態になった場合

変更後

(c) マルチキャストルータポートの削除

自動設定したマルチキャスルータルータポートは，保持時間中に該当ポートまたはチャネルグループで再度マルチキャストルータを検知しなければ，保持時間満了となり，自動的に削除します。

保持時間満了以外で自動設定したマルチキャストルータポートを削除する条件と削除対象を次に示します。

・運用コマンド clear igmp-snooping all を実行した場合

すべての VLAN の自動設定したすべてのマルチキャストルータポートを削除します。

・運用コマンド clear igmp-snooping mrouter を実行した場合

該当 VLAN の自動設定したすべてのマルチキャストルータポートを削除します。

・運用コマンド restart snooping で IGMP snooping/MLD snooping プログラムを再起動した場合

すべての VLAN の自動設定したすべてのマルチキャストルータポートを削除します。

・コンフィグレーションにより IGMP snooping を無効にした場合

該当 VLAN の自動設定したすべてのマルチキャストルータポートを削除します。

・コンフィグレーションコマンド ip igmp snooping mrouter discovery igmp を削除した場合

該当 VLAN の IGMP 監視で自動設定したすべてのマルチキャストルータポートを削除します。

・コンフィグレーションコマンド ip igmp snooping mrouter discovery pim を削除した場合

該当 VLAN の PIM 監視で自動設定したすべてのマルチキャストルータポートを削除します。

・ポートまたはチャネルグループを VLAN から削除した場合

当該 VLAN の当該ポートまたは当該チャネルグループで自動設定したマルチキャストルータポートを削除します。

・ポートをチャネルグループに追加した際に，当該ポートをマルチキャストルータポートに自動設定している場合

該当する VLAN の当該ポートで自動設定したマルチキャストルータポートを削除します。

・PIM 監視で自動設定した状態で Holdtime が 0 秒の PIM-Hello メッセージを受信した場合

PIM 監視で自動設定している該当マルチキャストルータポートを削除します。

また，次に示す場合は削除しません。

・該当ポートまたはチャネルグループがリンクダウンした場合

・該当ポートまたはチャネルグループがスパニングツリーなどで Blocking 状態になった場合

・該当 VLAN が Down 状態または Disable 状態になった場合

30.3.4 IGMP クエリア機能

変更

［Ver.2.1 以降］

変更前

注

IGMPv2 で運用する場合，該当する VLAN では Query Interval を統一してください。

変更後

注

IGMPv2 で運用する場合，該当する VLAN では Query Interval を統一してください。また，代表クエリアの Query インターバルを 10 秒以下とする場合、以下の条件を満たすネットワーク設計をしてください。

・本装置の配下に接続する IPv4 マルチキャスト受信者の同時接続数÷Query インターバル(秒)＝100 以下

変更前

注

Other Querier Present Interval は，Robustness Variable（RV）×Query Interval（QI）＋Query Response Interval（QRI）/2 で算出します。

RV，QI，QRI の値を次に示します。

・他装置が代表クエリアで IGMPv3 で運用している場合

RV，QI=受信した Query メッセージから取得

QRI=10 秒

・本装置が代表クエリアで IGMPv3 で運用している場合，または IGMPv2 で運用している場合

RV=2

QI=コンフィグレーションコマンド ip igmp snooping query-interval で指定した時間

QRI= 10 秒

本装置で送信する IGMP Query のバージョンは， IGMPv2 をデフォルト値としています。装置起動以降，IGMP Query のバージョンは，代表クエリアの IGMP バージョンに従います。

変更後

注

Other Querier Present Interval は，Robustness Variable（RV）×Query Interval（QI）＋Query Response Interval（QRI）/2 で算出します。0.1 秒単位の部分は 1 秒単位に切り上げます。

RV，QI，QRI の値を次に示します。

・他装置が代表クエリアで IGMPv3 で運用している場合

RV，QI，QRI=最後に受信した Query メッセージから取得。

・他装置が代表クエリアで IGMPv2 で運用している場合

RV=2

QI=コンフィグレーションコマンド ip igmp snooping query-interval で指定した時間(デフォルトは 125 秒)

QRI=QI が 11 秒以上の場合は 10 秒，QI が 10 秒以下の場合は QI - 1 秒

本装置で送信する IGMP Query のバージョンは， IGMPv2 をデフォルト値としています。装置起動以降，IGMP Query のバージョンは，代表クエリアの IGMP バージョンに従います。本装置が送信する Membership Query メッセージに設定する値は以下です。

・IGMPv1/IGMPv2

Max Resp Code=本装置の QI※が 11 秒以上の場合は 100，QI が 10 秒以下の場合は(QI – 1)秒×10，但し QI が 1 秒の場合は 9

・IGMPv3

Max Resp Code=本装置の QI※が 11 秒以上の場合は 100，QI が 10 秒以下の場合は(QI – 1)秒×10，

但し QI が 1 秒の場合は 9
　QRV=2
QQIC=本装置の QI，128 以上の場合は浮動小数点演算で端数は切り上げ
※本装置の QI=コンフィグレーションコマンド ip igmp snooping query-interval で指定した時間(デフォルトは 125 秒)

30.5 IGMP snooping/MLD snooping 使用時の注意事項

追加

［Ver.2.1 以降］

(9) IGMP Query メッセージの送信間隔

・IGMPv2 で運用している場合，他装置を含む該当 VLAN 内では，IGzMP Query メッセージの送信間隔を同じ値に設定してください。

・Query メッセージの送信間隔を 10 秒より小さくすると，マルチキャストグループ受信者から送信される Report メッセージのバースト率が上がるため，本装置で Report メッセージを取りこぼす可能性があります。このため、Query メッセージの送信間隔は，応答される Report メッセージの総数×1/10 が，100 以下となるように設定してください。

1　フィルタ

1.1 解説

1.1.7 フィルタ使用時の注意事項

変更

（3）拡張ヘッダのある IPv6 パケットに対するフィルタ

（3）拡張ヘッダのある IPv6 パケットに対するフィルタ

受信側において，IPv6 拡張ヘッダが 1 段の Hop-by-Hop Options 以外の IPv6 パケットに対して，TCP/UDP ヘッダ・ICMP ヘッダをフロー検出条件としたフィルタはできません。該当パケットに対してフィルタを実施する場合は，フロー検出条件に MAC ヘッダ，IPv6 ヘッダを指定してください。

送信側において，IPv6 拡張ヘッダのある IPv6 パケットに対して，TCP/UDP ヘッダ・ICMP ヘッダをフロー検出条件としたフィルタはできません。該当パケットに対してフィルタを実施する場合は，フロー検出条件に MAC ヘッダ，IPv6 ヘッダを指定してください。

5　レイヤ 2 認証

5.4 レイヤ 2 認証使用時の注意事項

5.4.2 RADIUS サーバ使用時の注意

追加

（3）IPv6 アドレスの RADIUS サーバ指定の注意事項

（3）IPv6 アドレスの RADIUS サーバ指定の注意事項

IPv6 アドレスの RADIUS サーバを使用する場合，リンクローカルアドレスの RADIUS サーバは使用しないでください。レイヤ 2 認証では，リンクローカルアドレスの RADIUS サーバと通信できません。

7　IEEE802.1X の設定と運用

7.1 コマンドガイド

7.1.8 IEEE802.1X 認証状態の変更

削除

（1）認証状態の初期化

認証状態の初期化を行うには, clear dot1x auth-state コマンドを使用します。ポート番号, ~~VLAN ID,~~ 端末の MAC アドレスのどれかを指定できます。何も指定しなかった場合は，すべての認証状態を初期化します。

（2）強制的な再認証

強制的に再認証を行うには，reauthenticate dot1x コマンドを使用します。ポート番号，~~VLAN ID,~~ 端末の MAC アドレスのどれかを指定できます。指定がない場合は，すべての認証済み端末に対して再認証を行います。

8　Web 認証の解説

8.3 認証機能

8.3.4 認証ネットワークからのログアウト

追加

（4）認証済み端末の無通信監視によるログアウト

（4）認証済み端末の無通信監視によるログアウト

認証済み端末に対し，MAC アドレステーブルを周期的に監視し，端末からのアクセスがあるかをチェックしています。該当する端末からのアクセスがない状態が続いた場合に，強制的に Web 認証の認証状態を解除します。この場合には，端末にログアウト完了画面を表示しません。

ただし，回線の瞬断などの影響で認証が解除されてしまうことを防ぐために，MAC アドレステーブルのエージング時間経過後約 10 分間（60 秒周期で監視），該当する MAC アドレスを持つ端末からのアクセスがない状態が続いた場合に，認証状態を解除します。

なお，この機能はコンフィグレーションコマンド no web-authentication auto-logout で無効にできます。

（アクセスがない状態が続いた場合でも強制的にログアウトしない設定が可能）。

変更

（6）認証済み端末からの特殊パケット受信によるログアウト

（6）認証済み端末からの特殊パケット受信によるログアウト

認証済み端末から送信された特殊パケットを受信した場合，該当する端末の認証を解除します。この場合には，端末にログアウト完了画面を表示しません。特殊パケットの条件を次に示します。

認証済み端末から Web 認証専用 IP アドレス宛に送出された ping パケットコンフィグレーションコマンド web-authentication logout ping tos-windows で設定された TOS 値を持っているパケットコンフィグレーションコマンド web-authentication logout ping ttl で設定された TTL 値を持っているパケット

8.6 認証エラーメッセージ

追加

表 8-6　認証エラーメッセージとエラー発生理由対応表

表 8-6　認証エラーメッセージとエラー発生理由対応表

エラーメッセージ内容	エラー番号	エラー発生理由
You cannot login by this machine.	33	RADIUS に設定されている認証後 VLAN が，Web 認証で定義された VLAN ではありません。 または，VLAN インタフェースに設定されていません
	34	RADIUS 認証方式で，認証済み端末から再ログインを行った際に RADIUS サーバから認証許可以外（アクセス拒否またはアクセスチャレンジ）を受信しました
	:	:
	90	マルチステップ認証ユーザ認証許可オプション設定時，Web 認証が許可されていなかったため認証できませんでした
	92	マルチステップ認証のユーザ認証として Web 認証の認証中に，端末認証の認証状態が解除されたため，認証できませんでした

変更

エラー番号ごとの対処方法

変更前

エラー番号ごとの対処方法

・1x～2x：正しいユーザ ID とパスワードで再度ログイン操作を行ってください。

・3x：RADIUS の設定を見直してください。

・4x：Web 認証のコンフィグレーション，および内蔵 Web 認証 DB の設定を見直してください。

・5x：再度ログイン操作を行ってください。再び本メッセージが表示される場合は，運用コマンド restart web-authentication で Web 認証を再起動してください。

・6x～7x：運用コマンド restart web-authentication で Web 認証を再起動してください。

・8x：再度ログアウト操作を行ってください。

変更後

エラー番号ごとの対処方法

・1x～2x：正しいユーザ ID とパスワードで再度ログイン操作を行ってください。

・3x，83，90：RADIUS の設定を見直してください。

・4x：Web 認証のコンフィグレーション，および内蔵 Web 認証 DB の設定を見直してく

ださい。

・51：端末の IP アドレスを見直して，再度ログイン操作を行ってください。

・52～54，85，91：再度ログイン操作を行ってください。再び本メッセージが表示される場合は，運用コマンド restart web-authentication で Web 認証を再起動してください。

・6x～7x：運用コマンド restart web-authentication で Web 認証を再起動してください。

・80～82：再度ログアウト操作を行ってください。

・92：再度ログイン操作を行ってください。再び本メッセージが表示される場合は，端末認証のコンフィグレーションを見直してください。

8.7 Web 認証画面入れ替え機能

削除

Web 認証で使用するログイン画面やログアウト画面など，Web ブラウザに表示する画面情報（以降，Web 認証画面と呼びます）は，運用コマンドで入れ替えることができます。その運用コマンドで指定したディレクトリ配下に，次に示す画面のファイルがあった場合，該当する Web 認証画面と置き換えます。また，次に示すファイル以外に gif ファイルなどの画像ファイルも同時に登録できます。ただし，登録時には各ファイルのサイズチェックだけを行い，ファイルの内容はチェックしませんので，必ず動作確認を行ってから HTML ファイルや画像ファイルを登録してください。

入れ替えることができる画面を次に示します。

［入れ替え可能な画面］

・ログイン画面

・ログアウト画面

・ログイン成功画面

・ログイン失敗画面

・ログアウト完了画面

・ログアウト失敗画面

~~・Reply-Message 表示画面~~

なお，登録した Web 認証画面は運用コマンドで削除できます。削除したあとは，デフォルトの Web 認証画面に戻ります。

9　Web 認証の設定と運用

9.2 Web 認証画面作成手引き

削除

HTML 上には，JavaScript のようにクライアント端末上だけで動作する言語は使用可能ですが，サーバへアクセスするような言語は使用できません。また，perl などの CGI も指定しないでください。

ただし，ログイン画面，ログアウト画面~~，および Reply-Message 表示画面~~では，Web 認証とのインタフェース用の記述が必要です。ログイン画面については「9.2.1　ログイン画面（login.html）」を，ログアウト画面については「9.2.2　ログアウト画面（logout.html）」を参照してください。

9.2.4 Web 認証固有タグ

削除

表 9-6　特殊タグ一覧

設定可能な画面と Web 認証固有タグの組み合わせを次の表に示します。

表 9-6　特殊タグ一覧

タグ表記	画面に表示する内容	ログイン画面	ログアウト画面	ログイン成功画面	ログイン失敗画面	ログアウト完了画面	ログアウト失敗画面	~~Reply-Message 表示画面~~
<!-- Login_Time -->	ログイン時刻※1	－	－	○	－	－	－	~~－~~
<!-- Logout_Time -->	ログアウト時刻※2	－	－	○	－	○	－	~~－~~
<!-- After_Vlan -->	認証後 VLAN ID※3	－	－	○	－	－	－	~~－~~
<!-- Error_Message -->	エラーメッセージ※4	－	－	－	○	－	○	~~－~~
<!-- Redirect_URL -->	なし	－	－	－※5	－	－	－	~~－~~
<!-- Session_Code -->	なし	－	－	－	－	－	－	~~－~~※6
~~<!-- Reply_Message -->~~	~~RADIUS サーバから受信した Access-Challenge の Reply-Message~~	~~－~~	~~－~~	~~－~~	~~－~~	~~－~~	~~－~~	~~○~~

（凡例）○：画面上に表示する　－：画面上空欄となる

注※1　ログインが成功した時刻。

注※2　表示画面によって意味が異なります。

ログイン成功画面：自動ログアウトする時刻。

ログアウト完了画面：ログアウト動作が完了した時刻。

注※3　ログイン成功後，ユーザが通信を行う VLAN ID。

注※4　ログインまたはログアウトが失敗した場合のエラー要因。

注※5　画面上に表示しませんが，認証成功後のジャンプ先 URL を保持します。

~~注※6　画面上に表示しませんが，ユーザ ID と State 値を保持します。~~

設定例については，「7.4.5　応答画面サンプル」を参照してください。

10　MAC 認証の解説

10.3 認証機能

10.3.3 認証解除方式

変更

（4）認証済み端末の無通信監視によるログアウト

変更前

（4）認証済み端末の無通信監視によるログアウト

認証済み端末に対し，MAC アドレステーブルを周期的に監視することで，端末からのアクセスがあるかをチェックしています。該当する端末からのアクセスがない状態が続いた場合に，強制的に MAC 認証の認証状態を解除し，認証前の VLAN ID に収容を変更します。ただし，回線の瞬断などの影響で認証が解除されてしまうことを防ぐために，端末からのアクセスが無くなってから約 60 分間，該当する MAC アドレスを持つ端末からのアクセスがない状態が続いた場合に，認証状態を解除します。なお，この時間はコンフィグレーションコマンド mac-authentication auto-logout で変更できます。

なお，この機能はコンフィグレーションコマンド no mac-authentication auto-logout で無効にできます。（アクセスがない状態が続いた場合でも強制的にログアウトしない設定が可能）。

変更後

（4）認証済み端末の無通信監視によるログアウト

認証済み端末に対し，MAC アドレステーブルを周期的に監視することで，端末からのアクセスがあるかをチェックしています。該当する端末からのアクセスがない状態が続いた場合に，強制的に MAC 認証の認証状態を解除し，認証前の VLAN ID に収容を変更します。ただし，回線の瞬断などの影響で認証が解除されてしまうことを防ぐために，端末からのアクセスが無くなってから約 60 分間（60 秒周期で監視），該当する MAC アドレスを持つ端末からのアクセスがない状態が続いた場合に，認証状態を解除します。なお，この時間はコンフィグレーションコマンド mac-authentication auto-logout で 1 秒単位の時間を設定できますが，設定した時間を満たす回数を 60 秒周期で監視する動作となります。

なお，この機能はコンフィグレーションコマンド no mac-authentication auto-logout で無効にできます。（アクセスがない状態が続いた場合でも強制的にログアウトしない設定が可能）。

12　マルチステップ認証

12.1 解説

12.1.2 サポート機能

追加

表 12-1　マルチステップ認証のオプション

表 12-1　マルチステップ認証のオプション

端末認証	ユーザ認証	オプション種別（コンフィグレーション※）	動作概要
MAC 認証	IEEE802.1X 認証または Web 認証	基本マルチステップ認証（パラメータなし）	端末認証成功時だけ，ユーザ認証ができます。
		ユーザ認証許可オプション（permissive パラメータ）	端末認証に失敗しても，ユーザ認証ができます。
IEEE802.1X 認証または MAC 認証	Web 認証	端末認証 dot1x オプション（dot1x パラメータ）	端末認証成功時だけ，ユーザ認証ができます。

注※

ポート単位に指定できます。

12.1.8 マルチステップ認証使用時の注意事項

追加

(2) マルチステップ認証の認証数制限について

コンフィグレーションコマンド authentication max-user で設定した認証数制限はユーザ認証の認証数に対して適用します。

2　運用端末接続

ftp-server

追加

リモート運用端末から ftp プロトコルを使用したアクセスを許可するために使用します。なお，本装置へログインを許可または拒否するリモート運用端末の IPv4 アドレスまたは IPv6 アドレスを指定する場合は，config-line モードで telnet アクセスと共通のアクセスリストを指定してください。

追加

［注意事項］

1. config-line モードでアクセスリストを指定している場合，ftp で本装置へログインを許可または拒否するリモート運用端末の IPv4 アドレスまたは IPv6 アドレスも同じアクセスリストに従って制限されます。

17　VLAN

vlan

削除

表 17–1　マルチコマンドモードでのコマンド可否［Ver.2.1 以降］

表 17–1　マルチコマンドモードでのコマンド可否

項番	コマンド	マルチコマンドモード可否
1	state {suspend | active}	○
2	name	×
3	protocol	○
4	mac-address	×
~~5~~	vlan-mac	○

削除

表 17–3　デフォルト VLAN のパラメータの扱い［Ver.2.1 以降］

表 17–3　デフォルト VLAN のパラメータの扱い

項番	コマンド	パラメータ	ユーザの設定可否	デフォルト VLAN 特有の動作
1	state {suspend | active}	－	○	－
2	name	<string>	○	－
3	protocol	<protocol name>	×	－
4	mac-address	<mac>	×	－
~~5~~	~~vlan-mac~~	~~－~~	~~○~~	~~－~~

19　Ring Protocol

forwarding-shift-time

削除
［Ver.2.1 以降］

トランジットノードの場合，フラッシュ制御フレームの受信待ちを行う保護時間を設定します。

保護時間が経過すると，フラッシュ制御フレームを受信していない場合でも，リングポートがブロッキング状態からフォワーディング状態に遷移します。

~~マスタノードの場合，セカンダリポートのポートアップを検出したときに，フォワーディング状態に遷移するまでの保護時間を設定します。~~

削除
［Ver.2.1 以降］

［パラメータ］

{<seconds> | infinity}

トランジットノードの場合，フラッシュ制御フレーム受信までの保護時間を秒単位で指定します。

「infinity」を指定した場合は保護時間が無限となり，フラッシュ制御フレームを受信するまでは，トランジットノードのリングポートはフォワーディング状態になりません。

~~マスタノードの場合，セカンダリポートをフォワーディング状態に変更するまでの保護時間を秒単位で指定します。~~

「infinity」を指定した場合は保護時間が無限となり，セカンダリポートのポートアップを検出してもフォワーディング状態になりません。

削除
［Ver.2.1 以降］

［コマンド省略時の動作］

トランジットノードの場合，フラッシュ制御フレームの受信待ち保護時間は 10 秒となります。

~~マスタノードの場合，セカンダリポートの保護時間は 10 秒となります。~~

削除
［Ver.2.1 以降］

［注意事項］

1.マスタノードでのヘルスチェックフレームの送信間隔が，トランジットノードでのフラッシュ制御フレームの受信待ちの保護時間よりも大きい場合，マスタノードが復旧を検出するよりも先にトランジットノードのリングポートがフォワーディング状態になります。そのため，一時的にループが発生するおそれがあります。

保護時間を設定する場合，マスタノードでのヘルスチェックの送信間隔を十分に考慮した値を設定してください。

~~2.マスタノードでのヘルスチェックフレームの送信間隔が，マスタノードでのフォワーディング状態に遷移するまでの保護時間よりも大きい場合，マスタノードが復旧を検出するよりも先にセカンダリポートがフォワーディング状態になります。そのため，一時的にループが発生するおそれがあります。~~

~~保護時間を設定する場合，マスタノードでのヘルスチェックの送信間隔を十分に考慮した値を設定してください。~~

26　フロー検出モード/フロー動作

flow detection mode

変更

［コマンド省略時の動作］

変更前

なし

変更後

フロー検出モードは，layer2-1 で動作します。

31　Web 認証

web-authentication ip address

変更

［設定の反映契機］

変更前

［設定の反映契機］

設定値変更後，運用コマンド restart web-authentication web-server による Web サーバの再起動後に反映されます。

変更後

［設定の反映契機］

設定値変更後，運用コマンド restart web-authentication による Web 認証プログラムの再起動後に反映されます。

25　Ring Protocol

show axrp

変更

［注意事項］

変更前

統計情報は，上限値でカウンタ更新を停止します。

変更後

なし

32　IEEE802.1X

show dot1x logging

追加

表 32-6　動作ログメッセージ一覧

表 32-6　動作ログメッセージ一覧

番号	ログ識別	ログ種別	メッセージ表記	意味・対処	付加情報
33	NOTICE	LOGIN	Login failed. ; Failed to assign VLAN. (Reason: No Tunnel-Type Attribute.)	［意味］ Tunnel-Type 属性がないため，認証後 VLAN の割り当てに失敗しました。 ［対処］ RADIUS サーバが送信する Accept パケット内に Tunnel-Type 属性を設定してください。	MAC アドレス ポート番号
34	NOTICE	LOGIN	Login failed. ; Failed to assign VLAN. (Reason: Tunnel-Type Attribute is not VLAN(13).)	［意味］ Tunnel-Type 属性の値が VLAN(13)でないため，認証後 VLAN の割り当てに失敗しました。 ［対処］ RADIUS サーバが送信する Accept パケット内の Tunnel-Type 属性を VLAN(13)に設定してください。	MAC アドレス ポート番号
35	NOTICE	LOGIN	Login failed. ; Failed to assign VLAN. (Reason: No Tunnel-Medium-Type Attribute.)	［意味］ Tunnel-Medium-Type 属性がないため，認証後 VLAN の割り当てに失敗しました。 ［対処］ RADIUS サーバが送信する Accept パケット内に Tunnel-Medium-Type 属性を設定してください。	MAC アドレス ポート番号
36	NOTICE	LOGIN	Login failed. ; Failed to assign VLAN. (Reason: Tunnel-Medium-Type Attribute is not IEEE802(6).)	［意味］ Tunnel-Medium-Type 属性の値が IEEE802(6)でないため，認証後 VLAN の割り当てに失敗しました。 ［対処］ RADIUS サーバが送信する Accept パケット内の Tunnel-Medium-Type 属性を IEEE802(6)に設定してください。	MAC アドレス ポート番号
37	NOTICE	LOGIN	Login failed. ; Failed to assign VLAN. (Reason: No Tunnel-Private-Group-ID Attribute.)	［意味］ Tunnel-Private-Group-ID 属性がないため，認証後 VLAN の割り当てに失敗しました。 ［対処］ RADIUS サーバが送信する Accept パケット内に Tunnel-Private-Group-ID 属性を設定してください。	MAC アドレス ポート番号
38	NOTICE	LOGIN	Login failed. ; Failed to assign VLAN. (Reason: Invalid Tunnel-Private-Gr	［意味］ Tunnel-Private-Group-ID 属性に不正な値が設定されているため，認証後 VLAN の割り当てに失敗しました。	MAC アドレス ポート番号

番号	ログ識別	ログ種別	メッセージ表記	意味・対処	付加情報
			oup-ID Attribute.)	［対処］ RADIUS サーバが送信する Accept パケット内の Tunnel-Private-Group-ID 属性に設定する内容を確認してください。	
39	NOTICE	LOGIN	Login failed. ; Failed to assign VLAN. (Reason: The VLAN ID is out of range.)	［意味］ VLAN ID が範囲外のため，認証後 VLAN の割り当てに失敗しました。 ［対処］ RADIUS サーバが送信する Accept パケット内の Tunnel-Private-Group-ID 属性に設定する VLAN ID の範囲を確認してください。	MAC アドレス ポート番号 VLAN ID
40	NOTICE	LOGIN	Login failed. ; Failed to assign VLAN. (Reason: The Port doesn't belong to VLAN.)	［意味］ 認証ポートが VLAN ID に属していないため，認証後 VLAN の割り当てに失敗しました。 ［対処］ RADIUS サーバが送信する Accept パケット内の Tunnel-Private-Group-ID 属性に設定する VLAN ID が，コンフィグレーションコマンド switchport mac の vlan パラメータで認証ポートに設定した VLAN ID に含まれていることを確認してください。	MAC アドレス ポート番号 VLAN ID
42	NOTICE	LOGIN	Login failed. ; Failed to assign VLAN. (Reason: The VLAN status is disabled.)	［意味］ VLAN が disable 状態のため，認証後 VLAN の割り当てに失敗しました。 ［対処］ 割り当てる VLAN の状態をコンフィグレーションコマンド state で active に設定してください。	MAC アドレス ポート番号 VLAN ID
46	NOTICE	LOGIN	Login failed. ; Failed to authenticate the supplicant because it could not be registered to MAC VLAN.(code=x)	［意味］ MAC VLAN への Supplicant 登録が失敗したため，認証に失敗しました。 ［対処］ ほかの認証との認証合計数が装置の収容条件や設定した最大認証端末数を上回っている場合は，下回った時点で，再度認証操作をしてください。 また，ほかの認証で認証していないことを確認してください。	MAC アドレス ポート番号 VLAN ID

clear dot1x statistics

追加

［注意事項］

・本コマンドを実行すると，show dot1x コマンドの Last EAPOL（最後に受信した EAPOL の送信元 MAC アドレス）もクリアされます。

33　Web 認証

show web-authentication logging

追加

表 33-6 動作ログメッセージ一覧

表 33-6　動作ログメッセージ一覧

番号	ログ識別	ログ種別	メッセージ表記	意味・対処	付加情報
:	:	:	:	:	:
50	NORMAL	LOGOUT	Force logout ; Authentic mode had changed (static vlan -> dynamic vlan).	［意味］ 固定 VLAN モードからダイナミック VLAN モードに認証方式が切り替わったため，全ユーザの認証を解除しました。 ［対処］ ありません。	MAC アドレス ユーザ名 IP アドレス VLAN ID ポート番号
51	NOTICE	LOGIN	Login failed ; IP address is not right.	［意味］ 固定 VLAN モードまたはダイナミック VLAN モード時，Web 認証専用 IP アドレス以外の IP アドレスでログイン操作が行われました。または，認証端末の IP アドレスから VLAN，MAC アドレス，及びポートの特定に失敗しました。 ［対処］ Web 認証専用 IP アドレスでログイン操作をしてください。または，認証端末の IP アドレスを確認して下さい。	ユーザ名 IP アドレス
54	NORMAL	LOGIN	Force login succeeded.	［意味］ 強制認証に成功しました。 ［対処］ ありません。	MAC アドレス ユーザ名 IP アドレス VLAN ID ポート番号
:	:	:	:	:	:

set web-authentication html-files

削除

［パラメータ］

<directory>

登録用の画面，メッセージおよび Web ブラウザのお気に入りに表示するアイコンを格納したディレクトリを指定します。

なお，登録用の画面，メッセージおよび Web ブラウザのお気に入りに表示するアイコンは，次の条件に従ってディレクトリに格納しておく必要があります。

・/config/wa/htdocs 以外のディレクトリに格納してください。

・ディレクトリ内にサブディレクトリを作成しないでください。

・ディレクトリ内に必ず「login.html」を格納してください。

・登録用の画面，メッセージ，およびアイコンのファイル名は，次のとおり指定してください。

ログイン画面：「login.html」

~~Reply-Message 表示画面：「loginProcess.html」~~

ログイン成功画面：「loginOK.html」

ログイン失敗画面：「loginNG.html」

ログアウト画面：「logout.html」

ログアウト成功画面：「logoutOK.html」

ログアウト失敗画面：「logoutNG.html」

認証エラーメッセージ：「webauth.msg」

Web ブラウザのお気に入りに表示するアイコン：「favicon.ico」

その他のファイル（gif など）を格納する場合，ファイル名は任意です。

削除

［実行例］

Web 認証の画面，メッセージおよびアイコンの登録の実行例を次に示します（登録用の画面，メッセージおよびアイコンをディレクトリ「k-html」に格納した場合）

```
# ls -l k-html
-rwxr-xr-x    operator    users    1108 Dec    6 09:59 login.html
~~-rwxr-xr-x    operator    users    1263 Dec    6 09:59 loginProcess.html~~
-rwxr-xr-x    operator    users    1302 Dec    6 09:59 loginNG.html
-rwxr-xr-x    operator    users    1300 Dec    6 09:59 loginOK.html
-rwxr-xr-x    operator    users     843 Dec    6 09:59 logout.html
-rwxr-xr-x    operator    users     869 Dec    6 09:59 logoutNG.html
-rwxr-xr-x    operator    users     992 Dec    6 09:59 logoutOK.html
-rwxr-xr-x    operator    users     109 Dec    6 09:59 webauth.msg
```

```
-rwxr-xr-x    operator    users      199 Dec    6 09:59 favicon.ico
-rwxr-xr-x    operator    users 20045 Dec    6 09:59 aaa.gif

# set web-authentication html-files k-html
Would you wish to install new html-files ? (y/n):y
executing…
Install complete.
```

restart web-authentication

削除

［パラメータ］

core-file

再起動時に Web 認証のコアファイル~~と Web サーバのコアファイル~~を出力します。

削除

［注意事項］

コアファイルの格納ディレクトリおよび名称は，次のとおりになります。

格納ディレクトリ：/usr/var/core/

Web 認証のコアファイル：wad.core

~~Web サーバのコアファイル：httpd.core~~

指定ファイルがすでに存在する場合は無条件に上書きするので，必要ならば，ファイルをあらかじめバックアップしておいてください。

44　応答メッセージ

44.1.32 マルチステップ認証

追加

表 44-32　マルチステップ認証の操作の応答メッセージ

表 44-32　マルチステップ認証の応答メッセージ

メッセージ	内容
Connection failed to 802.1X program.	IEEE802.1X プログラムへの接続が失敗しました。コマンドを再実行してください。頻発する場合は，restart dot1x コマンドで IEEE802.1X を再起動してください。

第5編　メッセージ・ログレファレンス

追加および変更はありません。

第6編　MIB レファレンス

追加および変更はありません。