
AX2340S ソフトウェアマニュアル

訂正資料

Ver.2.1 対応版

■はじめに

このマニュアルは、以下に示す AX2340S 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
AX2340S 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.2.1 対応)	AX23S-S001-20	2022 年 5 月
AX2340S 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.2.1 対応)	AX23S-S002-20	2022 年 5 月
AX2340S 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リファレンス (Ver.2.1 対応)	AX23S-S003-20	2022 年 5 月
AX2340S ソフトウェアマニュアル 運用コマンドリファレンス (Ver.2.1 対応)	AX23S-S004-20	2022 年 5 月
AX2340S ソフトウェアマニュアル メッセージ・ログリファレンス (Ver.2.1 対応)	AX23S-S005-20	2022 年 5 月
AX2340S ソフトウェアマニュアル MIB リファレンス (Ver.2.1 対応)	AX23S-S006-20	2022 年 5 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 (初版) SOFT-AM-2687

■著作権

All Rights Reserved, Copyright (C), 2021, 2022, ALAXALA Networks, Corp.

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	15
第 3 編 コンフィグレーションコマンドレファレンス	15
第 4 編 運用コマンドレファレンス	25
第 5 編 メッセージ・ログレファレンス	27
第 6 編 MIB レファレンス	28

27 Ring Protocol の解説

27.1 Ring Protocol の概要

27.1.3 サポート仕様

変更

表 27-1 Ring Protocol でサポートする項目・仕様

変更前

表 27-1 Ring Protocol でサポートする項目・仕様

項目		内容
省略		
ノード	マスタノード	×
	トランジットノード	○
	共有ノード	×
省略		

(凡例) ○ : サポート × : 未サポート

変更後

表 27-1 Ring Protocol でサポートする項目・仕様

項目		内容
省略		
ノード	マスタノード	×
	トランジットノード	○
	共有ノード	×※
省略		

(凡例) ○ : サポート × : 未サポート

注※マルチリング構成における共有リンク内ノード（非終端ノード）であれば共有ノードですがトランジットノードと同じ動作が可能です。

29 IGMP snooping/MLD snooping の解説

29.3 IGMP snooping

29.3.1 MAC アドレスの学習

変更

(2) エントリの削除

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

29.3.3 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

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 29-4 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	$\text{Robustness Variable}^{**1} \times \text{Query Interval}^{**2} + \text{Query Response Interval}^{**3} / 2 + X^{**4}$
IGMPv2 General Query メッセージ	
IGMPv3 General Query メッセージ ^{**5}	$\text{Robustness Variable} \times \text{Query Interval} + \text{Query Response Interval} / 2 + X^{**4}$
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 29-4 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

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トルータポートは、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ン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トルータポートは、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。
 - ポートまたはチャンネルグループを 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ン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。
 - ポートをチャン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ン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ンネルグループがスパン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

29.3.4 IGMP クエリア機能

変更

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)

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

追加

(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、IGMP 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。

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

8.6 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。

12 マルチステップ認証

12.1 解説

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。

第3編 コンフィグレーションコマンドレファレンス

追加および変更はありません。

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).	<p>[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。</p> <p>[対処] ありません。</p>	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.	<p>[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。</p> <p>[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。</p>	ユーザ名 IP アドレス
54	NORMAL	LOGIN	Force login succeeded.	<p>[意味] 強制認証に成功しました。</p> <p>[対処] ありません。</p>	MAC アドレス ユーザ名 IP アドレス VLAN ID ポート番号
:	:	:	:	:	:

追加および変更はありません。

追加および変更はありません。