



CentreCOM® x230シリーズ リリースノート

この度は、CentreCOM x230 シリーズをお買いあげいただき、誠にありがとうございます。このリリースノートは、取扱説明書、コマンドリファレンスの補足や、ご使用前にご理解いただきたい注意点など、お客様に最新の情報をお知らせするものです。最初にこのリリースノートをよくお読みになり、本製品を正しくご使用ください。

1 ファームウェアバージョン 5.4.4-3.8

2 本バージョンで追加・拡張された機能

ファームウェアバージョン 5.4.4-3.6 から 5.4.4-3.8 へのバージョンアップにおいて、以下の機能が追加・拡張されました。

2.1 ip igmp trusted コマンド

 **参照** 「コマンドリファレンス」 / 「IP マルチキャスト」 / 「IGMP Snooping」

ip igmp trusted コマンドが追加されました。対象スイッチポートにおいて、選択したパラメーターのパケットを IGMP Snooping で処理するように設定します。no 形式で実行した場合は、選択したパラメーターのパケットを IGMP Snooping で処理せずに破棄します。

ip igmp trusted コマンド

書式

```
[no] ip igmp trusted {all|query|report|routermode}
```

パラメーター

all:	すべての IGMP パケットと ip igmp snooping routermode コマンドで指定されているパケット
query:	IGMP Query
report:	IGMP Membership Report
routermode:	ip igmp snooping routermode コマンドで指定されているパケット

2.2 match dscp コマンド

 **参照** 「コマンドリファレンス」 / 「トラフィック制御」 / 「Quality of Service」

match dscp コマンドと match ip-precedence コマンドはこれまで IPv4 パケットにのみ対応していましたが、本バージョンより IPv6 パケットにもマッチするようになりました。IPv6 パケットにおいて、match dscp は Traffic Class フィールドの先頭 6 ビット、match ip-precedence は Traffic Class フィールドの先頭 3 ビットにマッチします。

3 本バージョンで仕様変更された機能

ファームウェアバージョン **5.4.4-3.6** から **5.4.4-3.8** へのバージョンアップにおいて、以下の機能が仕様変更されました。

3.1 ログの仕様変更

 **「コマンドリファレンス」 / 「運用・管理」 / 「ログ」**

ポートセキュリティの不正パケット受信時に表示されるログに、不正な MAC アドレスが表示されるようになりました。

3.2 ポートセキュリティの仕様変更

 **「コマンドリファレンス」 / 「インターフェース」 / 「スイッチポート」**

ポートセキュリティが有効なポートで受信したパケットの送信元 MAC アドレスが FDB に手動登録されている場合、FDB に登録されているポートと受信したポートが異なっていても不正パケットとして扱わない仕様でしたが、本バージョンより、受信したパケットの送信元 MAC アドレスが FDB に手動登録されていても、FDB に登録されているポートと受信したポートが異なる場合は不正パケットとして扱うよう仕様変更しました。

4 本バージョンで修正された項目

ファームウェアバージョン **5.4.4-3.6** から **5.4.4-3.8** へのバージョンアップにおいて、以下の項目が修正されました。

- 4.1 glibc に関する脆弱性 (CVE-2015-0235) への対策を行いました。
- 4.2 OpenSSL 脆弱性 (CVE-2014-3569 ~ 3572, CVE-2014-8275, CVE-2015-0204 ~ 0206) への対策を行いました。
- 4.3 MAC ベース認証を使用しているポートでループによるストームが発生した後、ループを解除した際に Supplicant が接続されている別ポート上で連続的にトラフィックを受信し続けていると、認証解除と認証処理が繰り返されることがありましたが、これを修正しました。
- 4.4 まれに、VLAN に関連する内部処理の異常が原因で通信停止や AMF 離脱などが発生することがありましたが、これを修正しました。
- 4.5 MSTP/RSTP のトポロジーチェンジ発生時に、BPDU のブリッジ ID が対向スイッチの値になることがありましたが、これを修正しました。
- 4.6 clear mac address-table コマンドの dynamic オプションでダイナミックエントリーを削除しようとする関連プロセスが再起動していましたが、これを修正しました。
- 4.7 DHCP Snooping 機能の ARP セキュリティが有効な VLAN で、不正ではない ARP パケットが正常に登録されないことがありましたが、これを修正しました。
- 4.8 マルチキャストパケットを受信中に、IGMP Report パケットとマルチキャストの UDP パケットを受信し続けていると nsm プロセスが異常終了することがありましたが、これを修正しました。

- 4.9 show mls qos interface storm-status コマンド実行時、複数のインターフェースを指定した場合、再起動することがありましたが、これを修正しました。
- 4.10 atmf working-set コマンドの実行後に atmf reboot-rolling コマンドでファームウェアを更新した場合、一部の AMF ノードで正常にファームウェアを更新できないことがありましたが、これを修正しました。

5 本バージョンでの制限事項

ファームウェアバージョン **5.4.4-3.8** には、以下の制限事項があります。

5.1 システム

 **参照** 「コマンドリファレンス」 / 「運用・管理」 / 「システム」

- システム起動時に下記のコンソールメッセージやログメッセージが出力されることがありますが、動作には影響ありません。
 - ・ コンソールメッセージ
stop: Unable to stop job: Did not receive a reply. Possible causes include: the remote application did not send a reply, the message bus security policy blocked the reply, the reply timeout expired, or the network connection was broken.
xx:xx:xx awplus init: getty (ttyS0) main process (XXXX) terminated with status 1
 - ・ ログメッセージ
daemon.warning awplus init: network/getty_console (ttyS0) main process (XXXX) terminated with status 1
- ドメインリストを設定する場合、最初にトップレベルドメインだけのものを設定すると、同一トップレベルドメインを持つ他のドメインリストを使用しません。その結果、ホスト名を指定した Ping に失敗することがあります。
- タイムゾーンの設定を変更したとき (clock timezone コマンド実行後) は、設定を保存しシステムを再起動してください。
- show license コマンドにおいて、Base License の提供機能として「RADIUS-100」と「VRRP」が表示されますが、x230 シリーズではこれらの機能をサポートしていません。

5.2 コマンドラインインターフェース (CLI)

 **参照** 「コマンドリファレンス」 / 「運用・管理」 / 「コマンドラインインターフェース」

- edit コマンドを使用すると、コンソールターミナルのサイズが自動で変更されてしまいます。
- コマンドラインインターフェース (CLI) の操作中に Ctrl/C や Ctrl/Z を入力して反応がなくなった場合は、もう一度 Ctrl/C を入力するか、Ctrl/D を入力してください。
- enable コマンド (非特権 EXEC モード) のパスワード入力に連続して失敗した場合、エラーメッセージに続いて表示されるプロンプトの先頭に「enable-local 15」という不要な文字列が表示されます。
- 非特権 EXEC モードで show log permanent コマンドを実行した場合、「%Permanent logging is not available on this device」のようなログが出力され、実行できません。

5.3 ファイル操作

 **参照**「コマンドリファレンス」 / 「運用・管理」 / 「ファイル操作」

ファイル名にスペースは使用できません。

5.4 コンフィグレーション

 **参照**「コマンドリファレンス」 / 「運用・管理」 / 「コンフィグレーション」

boot config-file コマンドにおいて、コンフィグファイルを相対パスで指定した場合、show boot コマンドや show system コマンドにおいても相対パスで表示されます。その場合でも起動時コンフィグとして正常に動作しますが、atmf provision node clone コマンドにおける複製元ノードでは、起動時コンフィグを相対パスで指定せず、絶対パスで指定してください。

5.5 ユーザー認証

 **参照**「コマンドリファレンス」 / 「運用・管理」 / 「ユーザー認証」

- TACACS+ サーバーを利用したコマンドアカウントिंग (aaa accounting commands) 有効時、end コマンドのログは TACACS+ サーバーに送信されません。
- TACACS+ サーバーを利用した CLI ログインのアカウントिंगにおいて、SSH 経由でログインしたユーザーのログアウト時に Stop メッセージを送信しません。
- スクリプトで実行されたコマンドは TACACS+ サーバーへは送信されません。

5.6 radius-server host コマンド

 **参照**「コマンドリファレンス」 / 「運用・管理」 / 「RADIUSクライアント」

radius-server host コマンドの retransmit パラメーター、または、radius-server retransmit コマンドで 0 を指定しても、初期値の 3 回再送を行います。

5.7 RADIUS サーバー

 **参照**「コマンドリファレンス」 / 「運用・管理」 / 「RADIUSサーバー」

- server auth-port コマンドによりローカル RADIUS サーバーの認証用 UDP ポート番号を 63998 以上に設定しようとする、関連プロセスが再起動するログが出力されます。また、上記の UDP ポート番号を使用してポート認証を行うことができません。
- ローカル RADIUS サーバーに登録するユーザー名の長さは 63 文字までにしてください。
- サポートリミット以上のユーザー情報が記載されている CSV ファイルを読み込んだとき、ローカル RADIUS サーバーには 1 件も登録されないにも関わらず、「Successful operation」と表示されます。

5.8 ログ

 **参照**「コマンドリファレンス」 / 「運用・管理」 / 「ログ」

- no log buffered コマンドを入力してランタイムメモリー (RAM) へのログ出力を一度無効にした後、default log buffered コマンドを実行しても、ログ出力が再開しません。その場合は「log buffered」を実行することにより再開できます。
- 複数の VLAN に所属する SFP モジュールをホットスワップすると、次のようなログが表示されます。

```
user.warning awplus NSM[XXXX]: 601 log messages were dropped - exceeded  
the log rate limit
```

これは短時間に大量のログメッセージが生成されたため一部のログ出力を抑制したことを示すものです。ログを抑制せずに出力させたい場合は、log-rate-limit nsm コマンドで単位時間あたりのログ出力上限設定を変更してください。

5.9 トリガー

 **「コマンドリファレンス」 / 「運用・管理」 / 「トリガー」**

トリガー設定時、script コマンドで指定したスクリプトファイルが存在しない場合、コンソールに出力されるメッセージ内のスクリプトファイルのパスが誤っています。

誤：

```
% Script /flash/script-3.scp does not exist. Please ensure it is created before
```

正：

```
% Script flash:/script-3.scp does not exist. Please ensure it is created before
```

また、スクリプトファイルが存在しないにもかかわらず前述のコマンドは入力できてしまうため、コンフィグに反映され、show trigger コマンドのスクリプト情報にもこのスクリプトファイルが表示されます。

5.10 SNMP

 **「コマンドリファレンス」 / 「運用・管理」 / 「SNMP」**

- snmp-server enable trap コマンドは、省略せずに入力してください。省略した場合、実行できない、または、コンソールの表示が乱れることがあります。
- IP-MIB は未サポートです。
- VLAN 名を SNMP の dot1qVlanStaticName から設定する場合は、31 文字以内で設定してください。

5.11 sFlow

 **「コマンドリファレンス」 / 「運用・管理」 / 「sFlow」**

sflow collector コマンドで UDP ポートを変更したのち、UDP ポートを初期値に戻す場合は、「no sflow collector」ではなく「sflow collector port 6343」を実行してください。

5.12 NTP

 **「コマンドリファレンス」 / 「運用・管理」 / 「NTP」**

- 初期設定時など、NTP を設定していない状態で show ntp status コマンドを入力すると、NTP サーバーと同期していることを示す以下のようなメッセージが表示されます。
Clock is synchronized, stratum 0, actual frequency is 0.000PPM, precision is 2
- NTPv4 を使用している場合、ntp master コマンドによる NTP 階層レベル (Stratum) の設定と NTP サーバーによる時刻の取得を併用すると、NTP サーバーによって自動決定される階層レベルが優先されます。
- NTP による時刻の同期を設定している場合、時刻の手動変更は未サポートとなります。

- ntp master コマンドで <1-15> パラメーターを省略した場合、NTP 階層レベル (Stratum) は 6 になるべきですが、実際は 12 になります。この問題を回避するため、同コマンドでは NTP 階層レベルを明示的に指定してください。

5.13 端末設定

 **「コマンドリファレンス」 / 「運用・管理」 / 「端末設定」**

仮想端末ポート (Telnet/SSH クライアントが接続する仮想的な通信ポート) がすべて使用されているとき、write memory など一部のコマンドが実行できなくなります。

5.14 Telnet

 **「コマンドリファレンス」 / 「運用・管理」 / 「Telnet」**

本製品から他の機器に Telnet で接続しているとき、次のようなメッセージが表示されます。

```
No entry for terminal type "network";  
using vt100 terminal settings.
```

5.15 Secure Shell

 **「コマンドリファレンス」 / 「運用・管理」 / 「Secure Shell」**

- SSH サーバーにおけるセッションタイムアウト (アイドル時タイムアウト) は、ssh server session-timeout コマンドで設定した値の 2 倍で動作します。
- 本製品の SSH サーバーに対して、次に示すような非対話式 SSH 接続 (コマンド実行) をしないでください。
※ 本製品の IP アドレスを 192.168.10.1 と仮定しています。
clientHost> ssh manager@192.168.10.1 "show system"

5.16 インターフェース

 **「コマンドリファレンス」 / 「インターフェース」**

- SFP ポートでは、polarity コマンドでのインターフェースの極性の固定設定は未サポートです。
- SFP ポートで Copper SFP (AT-MG8T) を使用する際、Polarity Auto でリンクアップしたときの表示が必ず MDI と表示されてしまいます。

5.17 ポートミラーリング

 **「コマンドリファレンス」 / 「インターフェース」 / 「スイッチポート」**

複数ポートにインターフェースモードのコマンドを発行するときは、interface コマンドで対象ポートを指定するときに、通常ポートとして使用できないミラーポートを含めないようにしてください。ミラーポートを含めた場合、一部のポートに設定が反映されなかったり、エラーメッセージが重複して表示されたりすることがあります。

5.18 ループガード

 **参照** 「コマンドリファレンス」 / 「インターフェース」 / 「スイッチポート」

- LDF 送信間隔 (loop-protection コマンドの ldf-interval パラメーター) を 1 秒に設定する場合、ループ検出時の動作持続時間 (loop-protection timeout コマンド) は 2 秒以上に設定してください (初期値は 7 秒)。

- MAC アドレススラッシングプロテクションにおいて、vlan-disable、link-down アクション実行時のログメッセージに誤りがありますので、下記のとおり読み替えてください。

[vlan-disable の場合]

誤 : Thrash: Loop Protection has disabled "port" on ifindex XXXX vlan X

正 : Thrash: Loop Protection has disabled "VLAN" on ifindex XXXX vlan X

[link-down の場合]

誤 : Thrash: Loop Protection has disabled "port" on ifindex XXXX

正 : Thrash: Loop Protection has disabled "port-link" on ifindex XXXX

- LDF 検出機能が vlan-disable となっている VLAN の所属ポートで、switchport enable vlan コマンドを実行しないでください。
- LDF 検出の port-disable アクションによってポートがシャットダウン状態になっていても、show interface コマンドの administrative state 欄には err-disabled ではなく UP と表示されます。またこのとき、MIB の ifAdminStatus も UP になります。LDF 検出のポート状態を確認するには、show loop-protection コマンドを使ってください

5.19 リンクアグリゲーション

 **参照** 「コマンドリファレンス」 / 「インターフェース」 / 「リンクアグリゲーション」

- スタティックチャンネルグループ (手動設定のトランクグループ) において、shutdown コマンドによって無効にしていたポートに対して no shutdown コマンドを入力しても、ポートが有効にならないことがあります。この場合は、再度 shutdown コマンド、no shutdown コマンドを入力してください。
- スタティックチャンネルグループのインターフェースを shutdown コマンドにより無効に設定した後、リンクアップしているポートをそのスタティックチャンネルグループに追加すると、該当するインターフェースが再び有効になります。
- show interface コマンドで表示される poX インターフェース (LACP チャンネルグループ) の input packets 欄と output packets 欄の値には、リンクダウンしているメンバーポートの値が含まれません。LACP チャンネルグループ全体の正確な値を確認するには、poX インターフェースではなく各メンバーポートのカウンターを参照してください。

5.20 ポート認証

 **参照** 「コマンドリファレンス」 / 「インターフェース」 / 「ポート認証」

- 802.1X 認証において、認証を 3 台以上の RADIUS サーバーにて行う場合、はじめの 2 台の RADIUS サーバーにて認証に失敗した際、Authenticator から 3 台目の RADIUS サーバーに Access-Request が送信されません。
- 認証済みポートが認証を解除されても、マルチキャストトラフィックが該当ポートに転送され続ける場合があります。
- 認証ポートが MAC 認証、Web 認証を併用しており、かつ直接 Supplicant の Linkup/Down を検知しない環境にて、一度 Web 認証に失敗した後、Supplicant が DHCP の再取得を実施すると、その後 MAC 認証が実施されません。
- 802.1X 認証と Web 認証の 2 ステップ認証機能利用時に、ローカル RADIUS サーバーは使用できません。また、802.1X 認証と Web 認証の 2 ステップ認証でローカル RADIUS サーバー以外の RADIUS サーバーを使用するときは、認証スイッチと RADIUS サーバーとの間で使用する認証方式を、802.1X 認証と Web 認証でそれぞれ別の方式に設定してください。
- auth-mac password コマンドの password 名に「encrypted」を設定することはできません。
- インターフェース上で、dot1x port-control コマンドを設定する前に dot1x control-direction コマンドを設定しないでください。設定すると「no dot1x control-direction」を実行しても、dot1x control-direction コマンドを削除することができなくなります。その場合は、「no dot1x port-control」を実行してください。
- auth-web method コマンドで認証方式を変更した場合は、対象ポートをいったんリンクダウンさせ、その後リンクアップさせてください。
- Web 認証とゲスト VLAN は併用できません。
- Web 認証サーバーのセッションキープ機能有効時、Web 認証端末が認証画面にアクセスしてから認証に成功するまでの間に、端末上のバックグラウンドプログラム等が自発的な HTTP 通信を試みた場合、認証成功後に意図したページへリダイレクトされないことがあります。

5.21 Power over Ethernet

 **参照** 「コマンドリファレンス」 / 「インターフェース」 / 「Power over Ethernet」

- power-inline enable コマンドを no 形式で実行し、PoE 給電機能を無効に設定すると、本来、show power-inline コマンドの Oper の表示が「Disabled」と表示されるべきですが、受電機器が接続されたポートでは「Off」と表示されます。
- PoE 電源の電力使用量が最大供給電力を上回った場合、show power-inline interface detail コマンドの Detection Status は「Denied」と表示されるべきですが、「Off」と表示されてしまいます。同様に、ポートの出力電力が上限値を上回った場合、「Fault」と表示されるべきですが、「Off」と表示されてしまいます。

- ポートの出力電力が上限値を上回った状態で数分間放置すると、実際に接続している受電機器の電力クラスと異なる電力クラスが表示される、または「n/a」と表示されることがあります。また、これに伴って Max も実際とは異なる値が表示されます。ポートの出力電力が上限値未満に戻ると、表示も回復します。
- ポートの出力電力が上限値を上回った状態のとき、show power-inline の Oper の表示が、実際の「Fault（ポートの出力電力が上限値を上回ったために給電を停止している）」ではなく「Denied（PoE 電源の電力使用量が最大供給電力を上回ったために給電を停止している）」となることがあります。
- show power-inline コマンドにおいて、クラス 4 受電機器が接続されたポートの出力上限値の表示が 30000 (mW) となるべきところ、15400 (mW) として表示されることがあります。ただし、給電自体は問題なく、30000 (mW) まで供給されます。

5.22 バーチャル LAN

参照「コマンドリファレンス」/「インターフェース」/「バーチャル LAN」

- プライベート VLAN からプライマリー VLAN を削除する場合は、事前にプライマリー VLAN、セカンダリー VLAN とともに、プライベート VLAN の関連付けを解除してください。その後、プライマリー VLAN のみを削除、再作成し、改めてプライベート VLAN とプライマリー VLAN、セカンダリー VLAN の関連付けを行ってください。
- エンハンスドプライベート VLAN を設定したポートからプライベート VLAN 用ポートとしての設定を削除すると、該当のポートでパケットが転送できなくなります。プライベート VLAN 用ポートとしての設定を削除した後は、本製品を再起動してください。
- プライベート VLAN 設定時に一度設定したホストポートは、その後設定を削除しても、show vlan private-vlan の表示に反映されず、ホストポートとして表示されたままになります。
- プライベート VLAN でセカンダリー VLAN を削除したとき、private-vlan association コマンドの設定を削除することができなくなります。セカンダリー VLAN を削除する場合は、事前に private-vlan association コマンドの設定を削除してください。
- タグ付きのトランクポートにポート認証が設定されている際、認証の設定を維持したままポートトランキングの設定を削除し、ネイティブ VLAN の設定を行う場合は、一度タグなし VLAN に設定を変更してから再度ポートトランキングを設定し、ネイティブ VLAN の設定変更を行ってください。
- マルチプル VLAN（プライベート VLAN）を CLI から設定した場合、コマンドの入力順序によってはプロミスキャスポート・ホストポート間の通信ができなくなる場合があります。その場合は、設定を保存してから再起動してください。
- 1 ポートに適用する VLAN クラシファイアグループは 2 グループまでに行ってください。
- 同じ VLAN クラシファイアグループ内に複数のルールを定義した場合、設定順ではなく番号順に反映されます。
- IP サブネット VLAN が正しく動作せず、パケットが正しい VLAN に転送されません。

5.23 UDLD

 **参照** 「コマンドリファレンス」 / 「L2 スイッチング」 / 「UDLD」

UDLD が Unidirectional を検出した場合、show interface コマンドの administrative state 欄には err-disabled と表示されますが、このとき標準 MIB の ifAdminStatus は UP を示しません。

5.24 イーサネットリングプロテクション (EPSR)

 **参照** 「コマンドリファレンス」 / 「L2 スイッチング」 / 「イーサネットリングプロテクション」

EPSR 内のリンクダウンが発生した機器が、マスターからのリンクダウンパケットを受け取っても FDB 情報をクリアしない場合があります。また、リンクダウンが発生した機器は本来であれば FDB の全クリアする必要がありますが、該当ポートの FDB はリンクダウンによってクリアされるため、通信に影響はありません。

5.25 ARP

 **参照** 「コマンドリファレンス」 / 「LIP ルーティング」 / 「ARP」

- マルチキャスト MAC アドレスをもつスタティック ARP エントリーを作成した後、それを削除してから arp-mac-disparity コマンドを有効にして、同一のエントリーをダイナミックに再学習させる場合は、設定後にコンフィグを保存して再起動してください。
- 同一 MAC アドレスに対して複数の ARP エントリー（異なる IP アドレス）を登録している場合、そのうちの 1 つを削除すると、残りの ARP エントリーに対応する FDB エントリーも削除されます。その場合は、手動でスタティックな FDB エントリーを登録してください。

5.26 IPv6

 **参照** 「コマンドリファレンス」 / 「IPv6」

- 自身の IPv6 アドレス宛に ping を実行するとエラーメッセージが表示されます。
- フラグメントされた IPv6 Echo Request は利用できません。利用した場合 Duplicate パケットは正しく再構築されませんのでご注意ください。

5.27 IGMP Snooping

 **参照** 「コマンドリファレンス」 / 「IP マルチキャスト」 / 「IGMP Snooping」

- マルチキャストグループをスタティックに登録している状態で、同じマルチキャストグループをダイナミックに学習すると、その後スタティック登録したグループを削除しても、show ip igmp groups コマンドと show ip igmp snooping statistics interface コマンドの表示からは該当グループが削除されません。これは表示だけの問題で動作には影響ありません。
- IGMP Snooping が有効な状態で、一旦無効にし、再度有効にした場合、その後に受信する IGMP Report を全ポートにフラディングします。

IGMP Snooping を再度有効にした後、clear ip igmp group コマンドを実行して全てのエントリーを消去することで回避できます。

- Include リスト（送信元指定）付きのグループレコードが登録されている状態で、あるポートに接続された唯一のメンバーからグループ脱退要求を受信すると、そのポートには該当グループのマルチキャストトラフィックが転送されなくなりますが、他のポートで同じグループへの参加要求を受信すると、脱退要求によって転送のとまっていたポートでもマルチキャストの転送が再開されてしまいます（この転送は、脱退要求を受信したポートの Port Member list タイマーが満了するまで続きます）。
- ダイナミック登録されたルーターポートを改めてスタティックに設定した場合、ダイナミック登録されてから一定時間が経過すると設定が削除されます。また、一定時間が経過するまでの間、コンフィグ上にはスタティック設定が表示されますが、ip igmp snooping mrouter interface コマンドを no 形式で実行しても、コンフィグから削除することができません。
ルーターポートをスタティックに設定する場合は、該当のポートがダイナミック登録されていないことを確認してください。
- 未認識の IGMP メッセージタイプを持つ IGMP パケットは破棄されます。
- 不正な IP チェックサムを持つ IGMP Query を受信しても破棄しません。そのため、当該の IGMP Query を受信したインターフェースはルーターポートとして登録されてしまいます。

5.28 MLD Snooping

 **参照**「コマンドリファレンス」 / 「IPv6 マルチキャスト」 / 「MLD Snooping」

- clear ipv6 mld コマンド実行時に「% No such Group-Rec found」というエラーメッセージが表示されることがありますが、コマンドの動作には問題ありません。
- MLD Snooping の Report 抑制機能が有効なとき（初期設定は有効）、ルーターポートで受信した MLDv1 Report または Done メッセージを受信ポートから再送してしまいます。これを回避するには、「no ipv6 mld snooping report-suppression」で Report 抑制機能を無効化してください。
- MLD メッセージを受信する環境では MLD Snooping を有効にしてください。MLD snooping が無効に設定されたインターフェースで MLD メッセージを受信すると次のようなログが出力されます。

NSM[1414]: [MLD-DECODE] Socket Read: No MLD-IF for interface port6.0.49

5.29 アクセスリスト

 **参照**「コマンドリファレンス」 / 「トラフィック制御」 / 「アクセスリスト」

- ハードウェアアクセスリストをサポートリミットまで使用する設定を行った場合は、設定をスタートアップコンフィグに保存し、いったん再起動してください。

- ARP や IGMP など CPU で処理されるパケットに対してイングレスフィルタが正しく動作しません。
ARP に関しては、以下の設定でフィルタすることが可能です。

```
mls qos enable
access-list 4000 deny any any vlan 100
class-map class1
match access-group 4000
policy-map policy1
class default
class class1
interface port2.0.24
service-policy input policy1
```

5.30 Quality of Service

 **参照** 「コマンドリファレンス」 / 「トラフィック制御」 / 「Quality of Service」

- match dscp コマンドの設定を削除する際、no match dscp と入力するとエラーとなります。no match ip-dscp コマンドを入力することで、設定を削除できます。
- wrr-queue disable queue コマンドを設定している状態で no mls qos コマンドにより QoS 自体を無効にする場合は、先に no wrr-queue disable queue コマンドを実行してください。
- QoS の送信スケジューリング方式 (PQ、WRR) が混在するポートを手動設定のトランクグループ (スタティックチャンネルグループ) に設定した場合、ポート間の送信スケジューリングが正しく同期されません。トランクグループを設定した場合は、個々のポートに同じ送信スケジューリング方式を設定しなおしてください。
- クラスマップに追加するアクセスリストの名前は 20 文字以内にしてください。
- ポリシーマップ名に「|」(縦棒) を使用しないでください。
- 受信レート検出 (QoS ストームプロテクション) 機能の storm-action コマンドの初期値に portdisable が設定されています。
- QoS ストームプロテクションの linkdown アクションを解除するときは、switchport enable vlan コマンドではなく「no shutdown」を使ってください。
- QoS ストームプロテクションの portdisable アクションによってポートがシャットダウン状態になっていても、show interface コマンドの administrative state 欄には err-disabled ではなく UP と表示されます。またこのとき、MIB の ifAdminStatus も UP になります。

5.31 アライドテレシスマネージメントフレームワーク (AMF)

 **参照** 「コマンドリファレンス」 / 「アライドテレシスマネージメントフレームワーク」

- AMF リンクとして使用しているスタティックチャンネルグループの設定や構成を変更する場合は、次に示す手順 A・B のいずれかにしたってください。

[手順 A]

1. 該当スタティックチャンネルグループに対して shutdown を実行する。
2. 設定や構成を変更する。
3. 該当スタティックチャンネルグループに対して no shutdown を実行する。

[手順 B]

1. 該当ノード・対向ノードの該当スタティックチャンネルグループに対して no switchport atmf-link を実行する。
 2. 設定や構成を変更する。
 3. 該当ノード・対向ノードの該当スタティックチャンネルグループに対して switchport atmf-link を実行する。
- リポートローリング機能でファームウェアバージョンを A から B に更新する場合、すでに対象ノードのフラッシュメモリー上にバージョン B のファームウェアイメージファイルが存在していると、ファームウェアの更新に失敗します。このような場合は、対象ノードから該当するファームウェアイメージファイルを削除してください。
 - AMF マスターが AMF メンバーよりも後から AMF ネットワークに参加するとき、AMF マスターのコンフィグにてその他メンバーからのワーキングセット利用やリモートログインに制限がかけてあっても、既存のメンバーに対してこれらの制限が反映されません。再度 AMF マスター上で atmf restricted-login コマンドを実行することで、すべての AMF メンバーに対して制限をかけることができます。
 - AMF クロスリンクを抜き差しすると、show atmf links statistics コマンドの表示結果にて、Discards カウンターが 8 ずつ増加します。
 - AMF 仮想リンクを使用している環境において、仮想リンクが通過する経路上の最小 MTU (経路 MTU) が 1500 バイト未満の場合 (例: PPPoE 接続のルーターを介して仮想リンクを設定している場合)、ワーキングセットプロンプトで実行したコマンドの結果が表示されずにプロンプトが返ってくる場合があります。本現象を回避するには、ルーター間で L2TP や IPsec などのトンネリング設定を行い (AMF 仮想リンクのトンネリングパケットをさらにもう一回トンネリングする)、トンネルの入り口で AMF トンネリングパケットをフラグメント化、トンネル出口で再構成することで、1500 バイトの AMF トンネリングパケットが破棄されないようにしてください。
 - オートリカバリーが成功したにもかかわらず、リカバリー後に正しく通信できない場合は、代替機の接続先が交換前と同じポートかどうかを確認してください。誤って交換前とは異なるポートに代替機を接続してしまった場合は、オートリカバリーが動作したとしても、交換前とネットワーク構成が異なるため、正しく通信できない可能性がありますのでご注意ください。
 - atmf cleanup コマンドの実行後、再起動時に HSL のエラーログが表示されますが、通信には影響はありません。
 - atmf provision node clone コマンドで新規ノードの事前設定をクローン作成する場合は、複製元ノードの起動時コンフィグ (boot config-file コマンド) が絶対パスで指定されていることを確認してください。

6 マニュアルの補足・誤記訂正

各種ドキュメントの補足事項および誤記訂正です。

6.1 サポートする SFP/SFP+ モジュールについて

本製品がサポートする SFP/SFP+ モジュールの最新情報については、弊社ホームページをご覧ください。

7 サポートリミット一覧

パフォーマンス	
VLAN 登録数	4094
MAC アドレス (FDB) 登録数	16K
IPv4 ホスト (ARP) 登録数	-
IPv4 ルート登録数	-
リンクアグリゲーション	
グループ数 (筐体あたり)	18 ※1
ポート数 (グループあたり)	8
ハードウェアパケットフィルター	
登録数	116 ※2※3※4
認証端末数	
認証端末数 (ポートあたり)	1K
認証端末数 (装置あたり)	1K
マルチブルダイナミック VLAN (ポートあたり)	1K
マルチブルダイナミック VLAN (装置あたり)	1K
ローカル RADIUS サーバー	
ユーザー登録数	3
RADIUS クライアント (NAS) 登録数	1 ※5
その他	
VRF-Lite インターフェース数	-
IPv4 マルチキャストルーティングインターフェース数	-

※ 表中では、K=1024

※1 スタティックチャンネル、LACP 合わせて 18 グループをサポートします。

※2 アクセスリストのエントリー数を示す。

※3 1 ポートにのみ設定した場合の最大数。エントリーの消費量はルール数やポート数に依存します。

※4 ユーザー設定とは別に、アクセスリストを使用する機能を有効化した場合に消費されるエントリーを含みます。

※5 radius-server local コマンドでローカル RADIUS を有効にした際に、自動登録されるローカルホスト (127.0.0.1) を含みます。

ローカルホスト以外の RADIUS クライアント (NAS) を登録したい場合は、no nas 127.0.0.1 コマンドでローカルホストを削除することで登録可能です。

8 未サポート機能 (コマンド)

最新のコマンドリファレンスに記載されていない機能、コマンドはサポート対象外ですので、あらかじめご了承ください。最新マニュアルの入手先については、次節「最新マニュアルについて」をご覧ください。

9 最新マニュアルについて

最新の取扱説明書「CentreCOM x230 シリーズ 取扱説明書」(613-001870 Rev.B)、コマンドリファレンス「CentreCOM x230 シリーズ コマンドリファレンス」(613-001990 Rev.B)は弊社ホームページに掲載されています。

本リリースノートは、これらの最新マニュアルに対応した内容になっていますので、お手持ちのマニュアルが上記のものでない場合は、弊社ホームページで最新の情報をご覧ください。

<http://www.allied-telesis.co.jp/>