



最初にお読みください



CentreCOM® x200シリーズ リリースノート

この度は、CentreCOM x200 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。最初は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 5.4.4-4.12

2 重要：注意事項

2.1 ファームウェアバージョンアップ時の注意事項

タイムゾーンの設定が入っている状態で 5.4.3 以前から、5.4.4 以降のファームウェアへバージョンアップした場合、バージョンアップ後にタイムゾーンの設定を反映させるため、再度システムの再起動が必要となります。

2.2 AMF におけるファームウェアバージョンの混在について

参照 [コマンドリファレンス] / [運用・管理] / [システム]

AMF メンバーとして x210/x200 シリーズを使用する場合、AMF マスターと x210/x200 のファームウェアバージョンは次表◎または○の組み合わせでご使用ください。

		x210/x200 シリーズ		
		5.4.4-0.x	5.4.4-1.x	5.4.4-2.x/3.x/4.x
AMF マスター	5.4.4-0.x	○	◎	◎
	5.4.4-1.x	×	◎	◎
	5.4.4-2.x/3.x/4.x	◎	◎	◎

◎ = 利用可能 (マスターにメンバープロダクト拡張ライセンスは不要です)

○ = 利用可能 (マスターにメンバープロダクト拡張ライセンスが必要です)

× = 利用不可 (x210/x200 シリーズが AMF ネットワークに参加できません)

* AMF マスターが 5.4.4-2.x で x210/x200 シリーズが 5.4.4-0.x のとき、x210/x200 のオートリカバリーを実行すると x210/x200 のコンソールに「An AMF-ALL license must exist on the ATMF Master for this node's recovery」のようなログメッセージが出力されますが、これは表示上の問題でオートリカバリーの動作には影響ありません。

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 5.4.4-3.10 から 5.4.4-4.12 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 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]

MAC アドレススラッシングプロテクションにおいて、アクション実行時のログメッセージに、MAC アドレス、ポート情報、VLAN 情報が付与されるようになりました。

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 **5.4.4-3.10** から **5.4.4-4.12** 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 OpenSSL 脆弱性 (CVE-2015-1788, CVE-2015-1790 ~ 1793, CVE-2015-4000) への対策を行いました。
- 4.2 SFP モジュール (AT-SPBD10-A/B, AT-SPBD20-A/B) を装着し起動すると、まれにこの SFP のメディアタイプが Unknown と間違って表示されていましたが、これを修正しました。
- 4.3 NTP クライアント機能使用時、NTP によってシステム時刻が西暦 2000 年よりも前に変更されると、その後 show log コマンドを実行してもログが表示されなくなることがありましたが、これを修正しました。
- 4.4 ミラーポートに設定されているインターフェースを含む範囲指定で QoS ポリシーマップを設定すると、異常終了する場合がありますでしたが、これを修正しました。
- 4.5 switchport port-security aging コマンドの設定にかかわらず、パケットの MAC アドレスがつねにダイナミックエントリーとして FDB に登録されていましたが、これを修正しました。
- 4.6 HTTPS にて Web 認証を使用した際、不正な通信を行うと機器が再起動してしまうことがありましたが、これを修正しました。
- 4.7 vlan classifier activate コマンドが適応されているポートがリンクアップしている状態で、no vlan classifier activate を実行した場合、筐体宛て通信ができなくなることがありましたが、これを修正しました。
- 4.8 5.4.4-1.1 以降のファームウェアでは DHCP クライアント機能を使用できませんでしたが、これを修正しました。
- 4.9 マルチキャスト MAC アドレスを持つホストを ARP 登録した際、フラッディングしないにもかかわらず show arp 上は flood と表示されていましたが、これを修正しました。
- 4.10 atmf working-set コマンドにて、複数回連続して任意のグループとローカルノードを行き来すると、各ワーキングセット実行時の内部接続が切断されず、指定したワーキングセットプロンプトに移動できなくなっていました。これを修正しました。
- 4.11 AMF と EPSR の併用時、EPSR リングのダウン、アップが発生した場合に AMF の Blocking ポートの位置が変化することがありましたが、これを修正しました。
- 4.12 プロセス間の同期メッセージが原因で、ごくまれに AMF 関連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。
- 4.13 HTTP リクエストに Host パラメーターが含まれない場合、関連プロセスが再起動する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 **5.4.4-4.12** には、以下の制限事項があります。

5.1 システム

 **「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
- show ecofriendly コマンドの表示には、ecofriendly led コマンドの設定状態しか反映されません（筐体上の MODE LED 表示切替ボタンによるエコ LED 機能のオン・オフは反映されません）。
- 検索ドメインリスト (ip domain-list) 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エントリーを使用しません。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。
- ライセンスを無効化すると、不要なエラーメッセージがログに出力されます。ライセンス自体は正常に削除されます。
- 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。

5.2 コマンドラインインターフェース (CLI)

 **「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、"%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

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


ファイル名には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 クライアント

 **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 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 に所属するポートを持つ 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。

5.8 トリガー

 **参照** 「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。

5.9 SNMP

 **参照** 「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。

5.10 sFlow

 **参照** 「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。

5.11 NTP

 **参照** 「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。

5.12 端末設定

 **参照** 「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。

5.13 Telnet

 **参照** 「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.


5.14 Secure Shell

 **参照** 「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"
```

5.15 インターフェース

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


- AT-x200-GE-52T の 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。
- AT-x200-GE-52T の 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。
- 多数の VLAN が所属しているインターフェースを shutdown コマンドでダウンさせた場合に "i/o error on routing socket No buffer space available - disabling" のようなログが出力されることがありますが、通信に影響はありません。
- IPv6 アドレスを設定している VLAN を、メンバーポートが存在する状態のまま no vlan で削除すると、関連プロセスが異常終了することがあります。

5.16 スイッチポート

 **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」


1518 オクテットより長いパケットを受信しても show platform port counters コマンドの OversizePkts 値がカウントされません。

5.17 ポートミラーリング

 **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」

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」

- 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 アクシオ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 検出機能のアクションが 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。
- LDF 検出機能でループを検知し、検出時の動作が行われているとき、当該ポートが所属する VLAN を変更しないでください。VLAN を変更した場合、検出時の動作に問題はありませんが、show loop-protection コマンドによる表示が旧 VLAN と新 VLAN の両方表示されます。

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。
- バージョン **5.4.3-2.5** より前のファームウェアにおいて、一度でも Web 認証サーバー（HTTPS）用の独自 SSL 証明書をインストール（copy xxxxx web-auth-https-file）したことがある場合、独自証明書を削除して、Web 認証サーバーにシステム付属の証明書を使わせるには、次の手順を実行してください。

1. 独自にインストールした SSL 証明書を削除する。
awplus# erase web-auth-https-file
 2. システムを再起動する（※ 未保存の設定がある場合は再起動前に保存してください）。
awplus# reboot
- 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。
 - 802.1X 認証が有効化されたポートがリンクアップする際、誤って以下のログが出力されますが、動作に影響はありません。
Interface portx.x.x: set STP state to BLOCKING
 - 約 20 端末ほどの Supplicant が Web 認証に失敗すると、その後 Web 認証が動作しなくなります。
 - 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 VLAN

参照「コマンドリファレンス」 / 「L2 スイッチング」 / 「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。
- 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トポート・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。
- インターフェースにプライベート VLAN の設定をしたままプライベート VLAN を削除することはできません。プライベート VLAN を削除する場合は次の手順で VLAN を削除するようにしてください。

1. インターフェースに対して `switchport mode private-vlan` コマンドを `no` 形式で実行して VLAN の設定を解除する。

5.22 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。

5.23 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。
- EPSR スーパールーブリベンション構成において、優先順位の低いリングの一部が切れている状態かつ、Common Link が切れている状態で、その Common Link を持つ機器が、再起動をすると、優先順位の低いリングへの接続ポートがリンクアップしているにも関わらず、ポートのステータスがブロックになっているため、通信ができません。正しく配線されていることを確認してから起動するようにしてください。

5.24 ARP

 **参照** 「コマンドリファレンス」 / 「IP」 / 「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。
- 2000pps を超える速度で ARP Request を受信すると、それに対する応答ができない場合があります。

5.25 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。

5.26 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います。

5.27 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 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
- 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出してしまいます。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。

5.28 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GRESS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
```

- ハードウェア IP アクセスリストにおいて、アクションが copy-to-mirror または send-to-mirror のアクセスリストがポートに適用されているとき、mirror interface を別のポートに再設定する際は、以下の手順で行ってください。
 1. 設定済みのポートからアクセスリストの設定を解除 (no access-group)
 2. 設定済みのポートからミラーポートの設定を解除 (no mirror interface)
 3. 移行したいポートへミラーポートを再設定 (mirror interface none)
 4. 移行したいポートへアクセスリストの設定 (access-group)

5.29 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 「|」 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。

5.30 DHCP サーバー

 **参照** 「コマンドリファレンス」 / 「IP 付加機能」 / 「DHCP サーバー」

- 同じ DHCP クライアントから 2 回目の割り当て要求があった場合、割り当て中の IP アドレスは show ip dhcp binding コマンドの実行結果で表示される IP アドレス割り当て状況に残ったままになります。リースしているアドレスの使用期間が満了すると、当該の IP アドレスは割り当て状況一覧から消去されます。
- show ip dhcp binding コマンドで DHCP クライアントへの IP アドレス割り当て状況を確認するとき、いくつかの DHCP プールに関する情報が表示されないことがあります。

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)」

- 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。
- AMF マスターが AMF メンバーよりも後に 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、全ての 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ことがあります。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 フィチャーライセンス AT-x200-GE-FL02 と AT-x200-GE-FL03

ファームウェアバージョン **5.3.4A-3.4** より、AT-x200-GE-28T/52T 共通の IPv6 ライセンス「AT-x200-GE-FL02」とアプリケーションライセンス「AT-x200-GE-FL03」をサポートしました。既存の IPv6 ライセンス「AT-x200-GE-28T-IPv6」と「AT-x200-GE-52T-IPv6」はファームウェアバージョン **5.3.4A-3.4** 以降でも引き続き使用できます。

6.2 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。

6.3 ループガード (LDF 検出)

 **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」

ファームウェアバージョン **5.4.3.0.1** のリリースノート (Rev.J) には、「LACP と LDF 検出は併用できません」とありますが、LACP と LDF 検出は問題なく併用できます。

7 サポートリミット一覧

パフォーマンス	
VLAN 登録数	256
MAC アドレス (FDB) 登録数	8K
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)	16 ※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	118 ※2※3
認証端末数	
認証端末数 (ポートあたり)	320
認証端末数 (装置あたり)	480
マルチプルダイナミック VLAN (ポートあたり)	40
マルチプルダイナミック VLAN (装置あたり)	120
ローカル RADIUS サーバー	
ユーザー登録数	-
RADIUS クライアント (NAS) 登録数	-
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グループは 8 グループ、LACP は 8 グループ設定可能。合わせて 16 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します。

※3 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。

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「AT-x200-GE-28T/AT-x200-GE-52T 取扱説明書」(613-001396 Rev.B)、コマンドリファレンス「CentreCOM x200 シリーズ コマンドリファレンス」(613-001463 Rev.J) 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/>