613-001901 Rev.A 140114

Allied Telesis

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、ご使用の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 5.3.4A-3.9

2 重要：注意事項

2.1 ファームウェアバージョン 5.3.4A-1.2 リリース前に IPv6 ライセンスを購入された方へ

ファームウェアバージョン **5.3.4A-1.2** リリース前に IPv6 ライセンスを有効化した機器で UDLD/SNMP の IPv6 対応機能を使用する場合は、IPv6 ライセンスのライセンスパスワードを更新する必要がありますので、弊社サポートセンターまたは保守契約締結時にご案内差し上げております「窓口のご案内」記載の窓口までご連絡ください。

3 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 **5.3.4A-3.8** から **5.3.4A-3.9** 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。

3.1 SNMP

参照 「コマンドリファレンス」/「運用・管理」/「SNMP」

不正なコミュニティー名もしくは不正なパスワードの SNMP マネージャーからアクセスした時に、Log（不正アクセス端末の IPaddress を含む）が出力されるように仕様拡張されました。

4 本バージョンで修正された機能

ファームウェアバージョン **5.3.4A-3.8** から **5.3.4A-3.9** 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 認証ポートが直接サプリカントのリンクアップ / ダウンを検知しない環境において、一度 Web 認証に失敗した後にサプリカントが DHCP にて IP アドレスの再取得を実施すると、再度 Web 認証を実施した際に認証画面が表示されませんでしたが、これを修正しました。

4.2 LDF 検出による検出時動作がいずれかのスイッチポートで発生すると、本体宛てのパケットが破棄され、Ping に応答しなくな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 **5.3.4A-3.9** 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」**

○ show tech-support コマンド実行時に不正なエラーメッセージが表示されます。これは表示だけの問題で、ファイルへの出力は正常に行われます。

○ インターフェースで受信可能な最大パケットサイズを 1518 バイト以上に設定した場合、1518 バイト以上のブロードキャストパケット、マルチキャストパケット、ジャンボフレームを受信すると、"BAD PACKET SIZE" というエラーが受信パケット数分出力されます。

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（CLI）」**

DHCP Snooping が無効な状態で、clear ip dhcp snooping statistics または clear arp security statistics コマンドを実行すると、その後 enable コマンドが正しく動作しません。現象発生後、特権モードに移行するにはログアウトし、再ログインする必要があります。

5.3 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」**

security-password forced-change コマンドで、パスワード有効期限が過ぎた次のログイン時に、パスワード変更を求める表示が出るように設定しても、スタートアップコンフィグが存在しない場合、新パスワードを入力しても拒否されログインできません。security-password forced-change コマンドを設定した場合、設定を保存し、スタートアップコンフィグを指定してください。

5.4 ログ

参照 **「コマンドリファレンス」/「運用・管理」/ 「ログ」**

○ email ログ送信時、メールヘッダーに From フィールド（送信元メールアドレス）を付けません。mail コマンドで手動送信したメールには From フィールドを付けます。

○ 保存するメッセージの最大量が log size コマンドで設定した値と異なります。

○ ポートセキュリティーで、指定されたアクションを実行し、ポートが無効化した場合に出力されるログレベルが 6:informational のため、初期設定のログレベルではログが出力されません。ログを出力させたい場合は、ログレベルを変更してください。

5.5 トリガー

参照 **「コマンドリファレンス」/「運用・管理」/ 「トリガー」**

定時トリガー（type time）を設定時、設定したトリガーの開始時刻とシステム時刻との差が少ないとトリガーが動作しません。トリガーの開始時刻とシステム時刻の差が 40 秒以上になるように設定してください。

5.6 SNMP

参照「コマンドリファレンス」/「運用・管理」/「SNMP」

○ 本製品で SNMPv3 を使用して、SNMP マネージャーとして SwimView を接続した環境において、本製品を再起動すると、SwimView との接続ができなくなります。
なお、SNMP マネージャーとして Swim Manager を接続した場合は、本現象は発生しません。また、SwimView を接続した場合でも、SNMPv1 または SNMPv2c を使用する場合は、本現象は発生しません。

○ Ether-Like.mib、dot3StatsTable の値が一部 CLI 上の値と一致しない場合があります。dot3StatsTable には主にポートカウンター情報のオブジェクトがあります。
ポートカウンター情報は CLI の show platform port counters コマンドで確認してください。

○ 「no rmon collection stats」で RMON 統計情報エントリーを削除するときは、関連する RMON アラーム設定を先に削除してください。逆の順序で削除すると RMON 関連プロセスが異常終了します。

○ 「no snmp-server ipv6」で IPv6 の SNMP エージェントを無効にし、再度有効にすると、IPv4 と IPv6 の SNMP が併用できなくなります。IPv4、IPv6 ともに有効にしてから、設定を保存、再起動することにより併用が可能になります。

○ LACP を使用しトランクグループを作成した際、対向機器の SNMP マネージャーで linkDown トラップを受信できない場合があります。送信先ホストの設定をする際、通知メッセージの形式で informs を指定すると informs パケットが受信できます。

○ fallingAlarm トラップが正しい OID で送信されません。

○ rmon alarm コマンドでサンプル値としきい値の比較方法に absolute を指定しているとき、risingAlarm トラップと fallingAlarm トラップが送信されません。

○ LAG インターフェースに SNMP のブリッジ MIB のポート番号が割り当てられていません。

5.7 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 sflow の UDP ポートを設定したとき、コンフィグに反映されず、保存、再起動で初期設定に戻ってしまいます。再起動した場合は、再度設定してください。SNMP マネージャーから設定した場合も同様です。

○ SNMP マネージャーから下記の Object を 1 以外に設定しても、sFlow サンプリング、sFlow カウンターは有効になりません。SNMP から有効にする場合は、下記のように設定してください。
- フローサンプリング
  sFlowFsReceiver : 1
  かつ
  sFlowFsPacketSamplinkgRate : 0 以外
  に設定
- カウンターサンプリング
  sFlowCpReceiver : 1

かつ
sFLowCpInterval : 0 以外
に設定

5.8 端末設定

参照「コマンドリファレンス」/「運用・管理」/「端末設定」

コンソールターミナルおよび仮想端末における 1 画面当たり表示行数は、実際のコンソールターミナルや仮想端末に表示できる行数より小さい値に設定してください。

5.9 SSH サーバー

参照「コマンドリファレンス」/「運用・管理」/「Secure Shell」

○ SSH サーバーのリスニング TCP ポート番号を 23 に設定しないてください。23 に設定すると不正なログが大量に出力されます。

○ ssh server allow-users コマンド、ssh server deny-users コマンドの設定数は、それぞれ 256 件以内にしてください。設定数がそれぞれ 256 件を超えると SSH サーバーにアクセスできなくなります。

5.10 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」

○ コンボポート、SFP ポートにおいて、polarity コマンドで mdi または、mdix 設定するとエラーになります。

○ 通信速度が 1000Mbps の SFP ポートで通信速度を 100Mbps に設定すると、設定をオートネゴシエーションに戻してもリンクダウンしたままになります。通信速度を 1000Mbps、デュプレックスモードを Full Duplex に設定する、または SFP モジュールを抜き差しすることで通信が復旧します。

5.11 ポートセキュリティー

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」

○ ポートセキュリティーにおいて、不正パケット受信時のアクションとして shutdown（DISABLE）が実行されたときに、show port-security interface コマンドで表示される Port Status が ENABLED のままになります。

○ ポートセキュリティーにおいて、不正パケット受信時のアクションが実行されてポートがロックされたあと、ポートセキュリティーを無効にしても、show port-security interface コマンドで表示される Lock Status が LOCKED のままになります。

○ ポートセキュリティーにおいて、不正パケット受信時のアクションとして shutdown（DISABLE）が実行されたあと、clear mac address-table コマンドでスタティックエントリーを削除すると、show port-security interface コマンドで表示される Lock Status が LOCKED から UNLOCKED に変わり、ポートがリンクダウンしたままになります。
ポートのロックを解除するには、switchport port-security コマンドを no 形式で実行してください。

○　ジャンボフレームとポートセキュリティーは併用できません。

○　ポートセキュリティーによって学習された MAC アドレスをエージアウトしないよう設定し、ポートセキュリティーの不正パケット受信時の動作を指定している場合、ポートセキュリティーを無効にしてもスタティック MAC アドレスがコンフィグに残ったままになります。コンフィグに残ってしまったスタティック MAC アドレスは、no mac address-table static または、clear mac address-table コマンドで削除してください。

○　ポートセキュリティーにおいて、不正パケット受信時の動作を shutdown に設定している状態で、ポートセキュリティーを無効にすると、ログが正しく出力されず、show interface status コマンドでインターフェースのステータスが正しく表示されません。shutdown コマンドでインターフェースを無効にし、その後有効にすることで正しく表示されます。

○　ポートセキュリティーと UDLD は併用できません。

5.12 MAC アドレススラッシング検出

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」

○　MAC アドレススラッシング検出時の動作に vlan-disable を指定したとき、検出後の動作継続時間内に、該当 VLAN に対して switchport enable vlan コマンドを実行しても、手動で動作を解除できず、VLAN を有効にできません。

○　MAC アドレススラッシングプロテクションが、設定した検出しきい値どおりに動作しないことがあります。複数の MAC アドレスが同時に移動した場合、しきい値に関係なく MAC アドレススラッシングプロテクションが機能します。

○　MAC アドレススラッシング検出時の動作に learn-disable アクションを設定しているとき、MAC アドレススラッシング検出後、MAC アドレスの学習が停止されないことがあります。

○　MAC アドレススラッシングプロテクション設定時、ループを検出したすべてのポートが、設定した動作を行います。

○　MAC アドレススラッシング検出時の動作に port-disable または link-down を指定したとき、検出後の動作継続時間内に、該当ポートに対して shutdown コマンドでインターフェースを無効化すると、以下のような状態になります。

port-disable 設定時：リンクダウンしますが、show interface コマンドで Link is UP と表示されます。
link-down 設定時：リンクダウンしていたポートがリンクアップしてしまいます。

5.13 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」

○　MSTP を設定後、LDF 検出機能を有効にし、MSTP を無効にするか MST インスタンスに関連付けられた VLAN を削除すると、LDF が送出されなくなります。
LDF の送出を再開させるには、システムを再起動してください。

ただし、MST インスタンスを作成せずに MSTP を有効にしただけの場合は、現象は発生しません。また、RSTP では本現象は発生しません。

○ LDF 検出によってループを検出しているとき、FDB の MAC アドレスエントリーがエージアウトしても削除されません。

○ LDF 送信間隔（loop-protection コマンドの ldf-interval パラメーター）を最小値の 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）。

○ LDF 検出機能により、ループを検出した VLAN のポートが無効化されている場合、switchport enable vlan コマンドを VID を指定せずに実行しても、無効化されている VLAN のポートは有効になりません。LDF 検出機能により無効化されている VLAN のポートを有効にするには、switchport enable vlan コマンドを VID を指定して実行してください。

○ 本来、LDF 機能はアクセスリストのエントリーに空きがない場合には使用できませんが、アクセスリストのエントリーに空きがない場合でも、loop-protection loop-detect コマンドを 1 回入力し、エラーメッセージが表示された後に、再度同じコマンドを入力すると、コマンドが実行されてしまいます。また、loop-protection loop-detect コマンドを 1 回入力し、エラーメッセージが表示された後に、当該のポートからアクセスリストのエントリーを削除すると、アクセスリストの登録数と最大数が正しく表示されなくなります。

5.14 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」**

○ フローコントロール（802.3x PAUSE の受信）を有効にすると、スイッチポートのデュプレックスがオートネゴシエーション以外の固定設定であっても、フローコントロールが動作します。

○ SFP モジュールを装着した状態でシステムを再起動すると、ifOutDiscards カウンターがカウントアップします。本現象は AT-MG8T 装着時には発生しません。

○ egress-rate-limit コマンドでポートに送信レートの上限値を設定すると、上限値が設定されていないポートでも、送信レートが制限されることがあります。本現象は約 700Byte 以上のブロードキャスト、マルチキャストパケット送信時に発生します。

5.15 パケットストームプロテクション

参照 **「コマンドリファレンス」/「運用・管理」/「スイッチポート」**

リンク速度の異なるポートが混在する環境において、高速なポートにパケットストームプロテクションの設定を行った場合、高速なポートから低速なポートへの転送レートは、パケットストームプロテクションの設定値よりも低くなります。

5.16 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」

○ ポート認証と LACP を同一ポートで併用することはできません。認証ポートでは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）で設定するようにしてください。

○ 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）とパケットストームプロテクションを併用するときは、グループ内のスイッチポートに対してパケットストームプロテクションを設定するようにしてください。スタティックチャンネルグループに対して設定すると、パケットストームプロテクションが正しく動作しません。

○ 複数の Telnet セッションで 1 セッションがポートインターフェースモードに入り、別のセッションが VLAN インターフェースモードに入っているとき、ポートインターフェースモードの switchport 以降に入力できるコマンド（static-channel-group 等）を実行するとエラーになります。

○ ゲスト VLAN に所属している Supplicant がスタティックチャンネルグループに所属している状態でスタティックチャンネルグループの設定を削除すると、認証の設定が消えているにもかかわらず、スタティックチャンネルグループに所属していたポートがゲスト VLAN に所属したままになります。ゲスト VLAN の設定を削除してから、スタティックチャンネルグループの設定を削除してください。

○ スタティックチャンネルグループの対向機器の先に SNMP マネージャーが接続されている場合、スタティックチャンネルグループのメンバーポートをリンクアップした際、対向機器のリンクアップトラップが SNMP マネージャーに送信されないことがあります。

○ トランクグループ（saX, poX）に対して egress-rate-limit コマンドを実行した場合、送信レート上限値はトランクグループ全体に対してではなく、メンバーポート単位で適用されます。またこのとき、ランニングコンフィグ上でもトランクグループではなくメンバーポートに対する設定に変換されます（CLI からメンバーポートに対して同コマンドを実行するとエラーになりますが、スタートアップコンフィグから読み込んだときはエラーになりません）。

○ LACP チャンネルグループ（poX）のネイティブ VLAN を初期値（vlan1）から変更している場合、その状態からネイティブ VLAN なしに設定変更するときは、必ず次の手順にしたがってください。

1. 該当 LACP チャンネルグループのネイティブ VLAN を初期値の vlan1 に戻します。
（インターフェース名 po1 は一例です。適宜変更してください）

```
awplus(config)# interface po1
awplus(config-if)# no switchport trunk native vlan
```

2. ネイティブ VLAN の設定をなしに変更します。

```
awplus(config-if)# switchport trunk native vlan none
```

ネイティブ VLAN の設定を初期値に戻さずに手順 2 だけを実行した場合、その後で以前ネイティブ VLAN に設定されていた VLAN を削除（no vlan）すると、該当 LACP チャンネルグループ経由の通信ができなくなります。

○ 非特権 EXEC モードで show static-channel-group コマンドを「show sta」という省略形で実行すると、同コマンドだけでなく show startup-config コマンドの出力も表示されます。

5.17 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」

○ 複数の Supplicant が同時に Web 認証を行った場合、いずれかの Supplicant の認証に失敗し、認証画面が崩れた状態で表示される（User name 欄だけが表示される）ことがあります。そのような場合は、Web ブラウザーで「再読込」を実行してください。

○ Web 認証と Auth-fail VLAN 併用時、認証失敗した Supplicant が Auth-fail VLAN の所属になったとき、Supplicant の Web 認証画面に認証失敗のメッセージが表示されず、「Authenticated」と表示されます。これは表示だけの問題で動作には影響しません。

○ Web 認証の Ping ポーリング機能を有効にし、auth-web-server ping-poll failcount コマンドで Supplicant がいなくなったと判断する Ping 無応答の回数を 1 に設定すると、Supplicant が Ping に応答しているにもかかわらず、認証が解除されます。failcount には 2 以上の値を指定するようにしてください。

○ 802.1X 認証または MAC ベース認証と MSTP を同一筐体内で併用し、かつ認証ポートでゲスト VLAN を使用した場合、認証成功時と認証解除時に不正なエラーメッセージが表示されます。これは表示だけの問題で動作には影響しません。

○ auth supplicant-mac コマンドで特定の MAC アドレスを持つ Supplicant 固有のパラメーターが設定されている場合、該当 Supplicant の認証にタイムアウトしていったん本製品から EAP-Failure が送信されると、その後 Supplicant から EAPOL-Start を受信しても、EAP-Request ではなく EAP-Failure を返すため、認証を開始できなくなります。

○ Web 認証において、auth max-supplicant コマンドで設定された最大数まで Supplicant が認証されている状態にもかかわらず、新たな Supplicant から Web 認証サーバーへのアクセスが可能です。この際、認証画面には HTTP 403 エラーが表示されます。

○ Web 認証のインターセプトモードが設定されているとき、no auth-web-server mode promiscuous コマンドの実行で、インターセプトモードの設定が無効になります。

○ 同一ポート上で 802.1X 認証、MAC ベース認証、Web 認証を併用した場合、または MAC ベース認証と Web 認証を併用した場合に、Web 認証用 DHCP サーバー機能を使用すると、認証前の Supplicant が Web 認証用 DHCP サーバーから IP アドレスを取得できません。このような場合は、Web 認証用 DHCP サーバー機能ではなく、通常の DHCP サーバー機能を使用してください。

○ LACP とポート認証を同一ポートで併用したとき、LACP ポートがリンクアップすると認証情報に対向機器の情報が載る場合があります。Single-host モードのポートでは該当情報が消えるまで (約 30 秒)Supplicant は認証を行うことができません。ホストモードを Single-host モード以外に設定することで回避できます。

○ auth-web-server dhcp ipaddress コマンドが、no auth-web-server ipaddress によりランニングコンフィグから削除されてしまいます。また、auth-web-server ipaddress コマンドが no auth-web-server dhcp ipaddress によりランニングコンフィグから削除されてしまいます。設定したコマンドの no 形式で削除してください。

○ 本製品と Supplicant の間に EAP 透過スイッチをはさんだ状態で 802.1X 認証を使用すると、認証ポートを抜き差しした後すぐに行われる再認証が失敗します。また、その状態で Supplicant から EAP-logoff メッセージを送信し、再び認証を行うと認証関連プロセスが異常終了します。EAP 透過スイッチと接続する場合、EAPOL のバージョン 2 を使用することで回避できます。

○ EAP 透過機能で forward（受信した EAPOL パケットを VLAN に関係なくすべてのポートに転送する）に設定した場合、ポートミラーリングのソースポートからコピーされた EAPOL パケットとは別にミラーポートへ EAPOL パケットが転送されます。

○ アカウンティング機能（aaa accounting xxx コマンド）で複数の RADIUS サーバーを使用する場合は、無応答のサーバーに対する要求送信抑制期間を初期値（0 分）以外に設定してください（radius-server deadtime コマンドまたはサーバーグループモードの deadtime コマンドで設定）。抑制期間が初期値（0 分）のままアカウンティング機能を使用した場合、サーバーリストの先頭に記述された RADIUS サーバーにしかアカウンティング要求が送信されません。

○ Web 認証サーバーで HTTPS（SSL）を有効化している環境において、独自の SSL サーバー証明書をインストールすると、その後 erase web-auth-https-file コマンドを実行しても独自証明書が正しく削除されず、最後にインストールしていた独自証明書が使い続けられます。

○ 認証ポートが MAC 認証、Web 認証を併用しており、かつ直接サプリカントの Linkup/Down を検知しない環境にて、一度 Web 認証に失敗した後、サプリカントが 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。

○ プロミスキャスモードと Web 認証用 DHCP サーバーを併用し、認証前と認証後の IP アドレスが変わる、かつ VLANID は変わらない構成では、Web 認証用 Ping-Polling は使用できません。

5.18 VLAN クラシファイア

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」

○ VLAN クラシファイアルールにマッチしないパケットにおいて、その送信元 IP アドレスが VLAN インターフェースに設定されているアドレスと同一ネットワークアドレスのパケットの場合、ポート本来の VLAN に転送されません。VLAN インターフェースに設定されているアドレスと異なるネットワークアドレスのパケットの場合は、ポート本来の VLAN に転送されます。

○ 一つのルールで構成される VLAN クラシファイアグループと、そのルールを含む複数のルールで構成されるグループが、それぞれ異なるスイッチポート上に設定されているとき、一つのルールで構成されるグループをポート上から削除したあと、再び同一ポートに追加しようとするとエラーメッセージがコンソールに出力され、グループをポートに設定することができず、HSL エラーログも出力されます。
一つのルールで構成される VLAN クラシファイアグループを削除するより前に、そのルールを含む複数のルールで構成されるグループを他のポート上から削除してください。その後、一つのルールで構成されるグループを削除することで、そのグループを同一ポートに設定しなおすことができます。

5.19 プライベート 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 のアイソレート VLAN に設定したポートをプライマリー VLAN に変更した場合、ランニングコンフィグは正しく表示されますが、正常に動作しません。アイソレート VLAN に設定したポートをプライマリー VLAN に変更する場合、アイソレート VLAN の設定を削除し、プライマリー VLAN の設定を行ってください。

5.20 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」

vlan コマンドは数値とカンマ、ハイフンだけを受け付ける仕様ですが、指定値にこれら以外の文字が含まれていてもエラーになりません。このとき、意図した VLAN が作成されなかったり（例：「10,20」のつもりで「10.20」と誤入力すると「10」しか作成されない）、意図したのとは異なる VLAN が作成されたりする（例：「1001」のつもりで「100q」と誤入力すると「100」が作成される）場合がありますのでご注意ください。

5.21 スパニングツリープロトコル

参照「コマンドリファレンス」/「L2 スイッチング」/「スパニングツリープロトコル」

○ BPDU ガード機能の動作中に、グローバルコンフィグモードにて spanning-tree portfast bpdu-guard コマンドを no 形式で実行してリンクアップしたあと、再度 spanning-tree portfast bpdu-guard コマンドを実行すると、BPDU ガード機能が動作しません。

ケーブルを抜き差しすることで、再度 BPDU ガード機能が動作します。

また、インターフェースモードにて spanning-tree portfast bpdu-guard コマンドを実行する場合は、本現象は発生しません。

○ 動作モードの設定（spanning-tree mode コマンド）が RSTP のとき、no spanning-tree force-version コマンドを使用して明示的なバージョン指定を削除することができません。no 形式を用いずに適切なバージョンを指定して設定しなおしてください。

○ ターミナルモニター実行中 spanning-tree enable コマンドを no 形式で実行すると不正なエラーメッセージが表示されます。これは表示だけの問題で動作には影響しません。

○ spanning-tree priority コマンドを no 形式で実行してもポートプライオリティーが初期値に戻りません。初期値に戻す場合は、spanning-tree priority コマンドでポートプライオリティーを 128 に変更してください。

5.22 EPSR

参照「コマンドリファレンス」/「L2 スイッチング」/「EPSR」

○ EPSR と MAC アドレススラッシングプロテクション併用時、EPSR のトポロジーチェンジにより、ループが検出される場合があります。EPSR とループガードを併用する場合は LDF 検出機能を使用してください。

○ EPSR（トランジットノード）の設定を有効から無効に変更しても、コントロール VLAN 上で受信した EPSR Healthcheck メッセージを同一 VLAN 内のすべてのポートに転送せず、EPSR 有効時の下流側ポートにだけ転送する動作を続けます。このようなときは、コントロール VLAN から所属ポートを削除し、再度追加してください。

5.23 DHCP Snooping

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

○ DHCP Snooping 有効時、ループガードの LDF 検出によって port-disable の動作が継続しているポートでは、DHCP メッセージがフィルタリングされずに通過します。

○ snmp-server enable trap コマンドで DHCP Snooping 関連のトラップを有効に設定しているとき、ip dhcp snooping violation コマンドでトラップを設定しようとすると、「SNMP trap for DHCP Snooping is disabled」というメッセージが表示され、トラップの設定が有効になりません。トラップを設定する場合は、ip dhcp snooping violation コマンド、snmp-server enable trap コマンドの順に入力してください。また、上記のエラーメッセージが表示された場合は、再度 snmp-server enable trap コマンドを入力することで、トラップの設定が有効になります。

5.24 RRP Snooping

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

RRP Snooping を無効から有効に変更したときに FDB のクリアが行われません。そのため、有効化前にバーチャルルーターの MAC アドレスを学習していた場合、該当アドレスがエージアウトするまでマスターポートが認識されず、結果としてマスタールーターの切り替えを検出できない場合があります。これを回避するには、次のいずれかを実施してください。

- RRP Snooping の有効化後に手動で FDB をクリアする
- RRP Snooping の有効化後にマスターポートのケーブルを抜き差しする
- RRP Snooping を有効化後にマスターポートのケーブルを接続する
- RRP Snooping の有効化後にマスターポートを shutdown し、その後 no shutdown する

5.25 IP インターフェース

参照「コマンドリファレンス」/「IP」/「IP インターフェース」

ip address dhcp コマンドを、client-id パラメーターを付けて VLAN インターフェースに設定した後、再起動を行うと、設定が反映されません。VLAN インターフェースには、hostname パラメーターのみを指定してください。client-id パラメーターを使用する場合は、リブートトリガーにより起動後に再設定を行うようにしてください。

5.26 スタティック ARP エントリー

参照「コマンドリファレンス」/「IP」/「ARP」

VLAN に IP アドレスを設定し、スタティック ARP エントリーを登録すると、IP アドレス変更前のスタティック ARP エントリーが show arp コマンドを実行しても表示されません。show running-config コマンドで表示されない ARP エントリーを確認し、ARP キャッシュから削除、再度登録することで表示されるようになります。

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」

○ ip igmp static-group コマンドで source パラメーターを指定しても、指定した送信元 IP アドレス以外からのマルチキャストパケットも指定したポートにだけ送信してしまいます。

○ レコードタイプが MODE_IS_EXCLUDE で送信元リストが指定されている IGMPv3 Report メッセージを受信してもグループ参加と認識できません。送信元リストが空の MODE_IS_EXCLUDE は正しく認識されます。

○ レコードタイプが BLOCK_OLD_SOURCES の IGMPv3 Report メッセージをルーターポートに転送しません。

○ IGMPv2 ホストと IGMPv3 ホストが同一 VLAN 上に混在している場合、IGMPv2 ホストが先にグループに参加していると、レコードタイプが CHANGE_TO_EXCLUDE の IGMPv3 Report メッセージを受信してもグループ参加と認識できません。マルチキャストルーターからの General Query メッセージに対して、IGMPv3 ホストがレコードタイプ MODE_IS_EXCLUDE の Report メッセージを返した場合は正しく認識します。

○ IGMP Snooping をいったん無効にし、再度有効にする場合は、システムを再起動してください。

○ IGMP Snooping の Report 抑制機能が無効の場合（no ip igmp snooping report-suppression）、Leave メッセージを受信すると、ルーターポートへ 2 パケット転送されます。

○ IGMP Snooping の IGMP Querier 機能を有効にした場合（ip igmp snooping querier）、ホストから Leave メッセージを受信しても Specific Query メッセージを送信しません。

○ IGMP Snooping の IGMP Querier 機能を有効にした場合、他の装置からの Query メッセージを受信しても、Query メッセージ送信が停止されません。

○ IGMP Snooping の IGMP Querier 機能を有効にした状態で IP アドレスを変更すると、変更後正しい IP アドレスで Query を送信しません。IP アドレスを変更する場合は、IGMP Querier 機能を無効にし、変更後、再度有効にしてください。

○ グローバルコンフィグモードの ip igmp snooping コマンド、インターフェースモードの ip igmp snooping コマンドのどちらか一方のみが実行されている状態では、不要なパケットが複製され出力されます。

○ IGMP Snooping の設定を無効で起動した場合、有効に変更しても、IGMP パケットが正しく転送されません。IGMP Snooping を無効から有効に設定変更した場合は、設定を保存し再起動してください。

○ 空の Exclude リストを持つグループレコードが存在している状態で、同グループに対する Exclude リスト追加要求（BLOCK_OLD_SOURCES）を受信すると、それ以降該当グループがタイムアウトしたり、脱退メッセージ（CHANGE_TO_INCLUDE{}）を受信したりしても、該当グループが正しく削除されません。

○ スタティックマルチキャストグループが登録されている状態で、該当のマルチキャストグループと同じグループアドレス宛ての Join メッセージを他のポートから受信すると、その後 Leave メッセージを受信しても、そのポートには該当マルチキャストグループ宛のマルチキャストパケットが転送されるようになります。

○ IGMP Snooping を無効に設定していても、IGMP Query に応答して Report を送信することがあります。これを回避するには、次のいずれかを実施してください。
- システム全体で IGMP Snooping を無効にする際は、グローバルコンフィグモード・インターフェースモードの両方で無効にしてください。
- 特定のインターフェースで IGMP Snooping を無効にする際は、そのインターフェース上で IGMP Report 抑制機能も無効にしてください。

○ IGMP バージョン 3 使用時は、IGMP Snooping Report 抑制機能を無効化しないでください。無効に設定されていると、グループメンバーからの IGMP Report メッセージのバージョンが 3 であった場合、マルチキャストトラフィックが転送されなくなることがあります。

○ 複数ポートの IGMPv3 ホストから ALLOW_NEW_SOURCES レポートによる同一グループの登録があった後、いずれかのホストから該当グループの MODE_IS_INCLUDE レポートを受信すると、show ip igmp snooping statistics interface コマンドの Port member list の表示において、MODE_IS_INCLUDE を受信していないポートのタイマーも更新されます。これは表示だけの問題であり、MODE_IS_INCLUDE を受信していないポートは、最初に ALLOW_NEW_SOURCES で登録したときのタイマーが満了すると削除されます。

○ 本来 IGMPv1/IGMPv2 だけを対象とするはずの IGMP Snooping の Report 抑制機能が、IGMPv3 の Report メッセージに対しても動作してしまいます。

○ VLAN ID のみ異なる、未登録の IP マルチキャストトラフィックをタグ付きポートで受信すると、該当マルチキャストトラフィックは、登録済みの VLAN を除く他のすべての VLAN でフラッディングされます。ただし、各 VLAN で該当マルチキャストグループのメンバーが登録されると、IGMP Snooping が正常に動作するようになり、フラッディングは行われなくなります。

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」

○ グローバルコンフィグモードの ipv6 mld snooping コマンド、インターフェースモードの ipv6 mld snooping コマンドのどちらか一方のみが実行されている状態では、不要なパケットが複製され出力されます。

○ MLD Snooping の設定を無効で起動した場合、有効に変更しても、MLD パケットが正しく転送されません。MLD Snooping を無効から有効に設定変更した場合は、設定を保存し再起動してください。

○ MLD Snooping をいったん無効にし、再度有効にする場合は、システムを再起動してください。

○ 複数の VLAN インターフェースが指定されたインターフェースモードで、以下の MLD Snooping のコマンドを実行しても、最初に指定した VLAN インターフェースでのみコマンドが実行されます。
- ipv6 mld access-group
- ipv6 mld limit
- ipv6 mld snooping
- ipv6 mld snooping fast-leave
- ipv6 mld snooping mrouter interface
- ipv6 mld snooping report-suppression

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」

○ グローバルコンフィグモードで IGMP Snooping を無効にすると、show platform classifier statistics utilization brief コマンドで表示される ACL（ハードウェアアクセスリストによる内部領域の消費量）が -1 になります。これは表示だけの問題で動作には影響しません。

○ ハードウェアアクセスリストを作成するときに、終点ポート番号を範囲で指定した場合、範囲の上限値が始点ポート番号に指定した値よりも小さいとエラーで設定ができません。
例）始点ポート番号：80、終点ポート番号：1 ～ 60 を許可
access-list 3001 permit udp any eq 80 any range 1 60

このような場合は、アクセスリストを 2 個に分けて作成することで、設定が可能になります（61 ～ 80 を破棄する設定を追加します）。
access-list 3000 deny udp any eq 80 any range 61 80
access-list 3001 permit udp any eq 80 any range 1 80

5.30 ハードウェアパケットフィルター

参照 「コマンドリファレンス」/「トラフィック制御」/「ハードウェアパケットフィルター」

access-group コマンドでスイッチポートに適用した状態のままハードウェア MAC アクセスリストの内容を変更することはできません。ハードウェア MAC アクセスリストの内容を変更する場合は、no access-group でポートへの適用を解除してから内容を変更し、再度 access-group コマンドを実行してポートに適用しなおしてください。

5.31 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」

○ QoS ポリシーマップが適用されたスイッチポートに対して、適用を解除する設定を行っても、該当インスタンスにおいて QoS が使用するシステム内部領域が一つ消費されたままになり、すべての領域が解放されません。
すべての領域を解放するには、システムを再起動してください。

○ QoS ポリシーマップのフィルタリング機能において、フレームフォーマットに 802.2 LLC を指定しても、正しくフィルタリングされません。

○ QoS ストームプロテクション機能において、対象トラフィッククラスの受信レートが設定した上限値を超過した場合の動作として、受信ポートの無効化（portdisable）を指定していても、実際には受信ポートが物理的にリンクダウンします（linkdown 指定時と同じ動作になります）。

○ QoS ストームプロテクション機能において、受信レート超過時の動作に linkdown を指定したとき、動作継続時間内に shutdown コマンドを no 形式で実行しても、手動で動作を解除できません。ポートはリンクアップしますが、storm-downtime コマンドで設定された動作の持続時間が経過するまで、QoS ストームプロテクション機能を再開できません。

○ QoS ストームプロテクション機能において、storm-action コマンドを no 形式で実行して初期値（portdisable）に戻す設定をしても、コンフィグ上には「storm-action unknown」として反映されます。実際には、初期値である portdisable として正常に動作します。

○ QoS ストームプロテクション機能において、受信レート超過時の動作に vlandisable を指定したとき、動作継続時間内に該当ポートからポリシーマップを削除すると、switchport enable vlan コマンドを no 形式で実行しても、手動で動作を解除できなくなります。

○ QoS ストームプロテクション機能では、受信レートが実際の値より高く検出されます。

○ show mls qos interface storm-status コマンドでは、QoS ストームプロテクション機能のアクションが実行されていないときでも、アクションの残り時間（Timeout Remaining）が常にカウントされています。

○ QoS の match eth-format protocol コマンドで AppleTalk パケットを制御できません。

5.32 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」

○ DHCP サーバー機能において、リース時間が 59 秒以下に設定されている状態でクライアントに IP アドレスが割り当てられると、clear ip dhcp binding コマンドで DHCP サーバーのリース情報を削除できなくなります。

○ clear ip dhcp binding コマンドで、特定の MAC アドレス、または IP アドレスを指定して DHCP クライアントのリース情報（エントリー）を削除すると、コマンドで指定したクライアントだけでなく、他のクライアントのリース情報も削除されることがあります。

6 マニュアルの補足・誤記訂正

最新マニュアル（取扱説明書、コマンドリファレンス）の補足事項および誤記訂正です。

6.1 フィーチャーライセンス 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 loop-protection コマンド

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」**

ファームウェアバージョン **5.3.4A-3.8** より、loop-protection コマンドの ldf-interval（LDF 送信間隔）の有効範囲が下記のとおり変更されています。

○ バージョン **5.3.4A-3.7** まで

```
loop-protection loop-detect [ldf-interval <5-600>]
```

○ バージョン **5.3.4A-3.8** から

```
loop-protection loop-detect [ldf-interval <1-600>]
```

6.3 ARP セキュリティーとアクセスリスト、QoS の併用

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

ARP セキュリティーを有効にしているポートでは、アクセスリスト、QoS を使用できません。

6.4 IGMP Snooping

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

IGMP Snooping の Report 抑制機能有効時には、あるポートで Leave メッセージを受信しても、他ポートに同一グループのメンバーが存在していると、Leave メッセージを受信したポートがメンバーリストから削除されず、該当グループ宛てのマルチキャストトラフィックが送信され続けます。

これは下記仕様によるものですが、「no ip igmp snooping report-suppression」で Report 抑制機能を無効化することにより回避可能です。

(1) Report 抑制機能では、Leave メッセージを受信しても、他ポートに同一グループのメンバーが存在する場合はルーターポートから Leave メッセージを送信しません。

(2) IGMP Snooping 機能では、Leave メッセージの受信後すぐにメンバーリストからポートを削除するのではなく、Leave メッセージを受信した Querier が送信する Group-specific Query に応答がないポートのみメンバーリストから削除します。

したがって、仕様 (1) によりルーターポートから Leave メッセージが送信されない場合、Querier は Leave メッセージを受信しないため Group-specific Query を送信せず、結果として Leave メッセージの受信ポートがメンバーリストから削除されません。

6.5 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」

ファームウェアバージョン **5.3.4A-3.8** より、loop-protection コマンドの ldf-interval（LDF 送信間隔）の有効範囲が下記のとおり変更されています。

○ Web 認証サーバーのインターセプトモードとセッションキープ機能を併用すると、セッションキープ機能が働かない場合があります。

○ プロミスキャス / インターセプト Web 認証使用時、端末のデフォルトゲートウェイが本製品となり、認証成功後の通信に失敗することがあります。

6.6 IGMP Snooping

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

MLD Snooping 使用時、1 つのポートに複数の MLDv1 ホストを接続している場合は、初期設定で有効になっている Report 抑制機能を「no ipv6 mld snooping reportsuppression」で無効化してください。

7　サポートリミット一覧

パフォーマンス	
VLAN 登録数	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	122 ※2※3※4
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　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。

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.D）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 Web ページで最新の情報をご覧ください。

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