613-001467 Rev.J 130520

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 5.4.3-0.1

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 **5.4.3-0.1** 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 findme コマンド

参照 「コマンドリファレンス」/「運用・管理」/「システム」

機器のポート LED を一定期間（デフォルト 60 秒間）点滅させる findme コマンドが追加されました。このコマンドは、ラック内で機器の位置を確認したいときなどに便利です。

3.2 boot config-file コマンドの backup オプション

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」

起動時コンフィグ（スタートアップコンフィグ）の実体ファイルを指定する boot config-file コマンドに、バックアップ用のコンフィグファイルを指定する backup オプションが追加されました。

3.3 Syslog メッセージのバッファ設定コマンドの追加

参照 「コマンドリファレンス」/「運用・管理」/「ログ」

ログを Syslog サーバーに送る前に一時的にバッファする log host startup-delay コマンドを追加しました。ログ送信までの時間はオプションの delay パラメーターで、バッファするログメッセージ数はオプションの message コマンドで設定できます。

3.4 MAC アドレススラッシングプロテクショントラップ

参照「コマンドリファレンス」/「運用・管理」/「SNMP」

MAC アドレススラッシングを検出した際、SNMP マネージャーに TRAP を送信する MAC アドレススラッシングプロテクショントラップをサポートしました。
これにともない、snmp-server enable trap コマンドで指定できる通知メッセージ種別に thrash-limit が追加されました。

3.5 リンクトラップ送信タイミングの設定コマンドの追加

参照「コマンドリファレンス」/「運用・管理」/「SNMP」

対象インターフェースのリンクステータスが変化した時に送信する SNMP トラップの送信タイミングを設定する snmp trap link-status trap-delay コマンドを追加しました。

3.6 NTP の IP インターフェース設定

参照「コマンドリファレンス」/「運用・管理」/「NTP」

NTP の通信を行うインターフェースを指定する機能をサポートしました。インターフェースは ntp source コマンドで設定します。

3.7 mirror interface コマンドの none オプション

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」

mirror interface コマンドに none オプションが追加されました。
前バージョンまでは、ハードウェアパケットフィルターや QoS ポリシーマップの copy-to-mirror アクションを使用してミラーリングを行う場合に、mirror interface コマンドでダミーのポートを指定する必要がありましたが、本バージョンからは「mirror interface none」と指定すればよくなります。

3.8 Web 認証：ブロッキングモード

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」

L2 スイッチである本製品において、上位 L3 スイッチによるルーティングを介さずに、Web 認証とダイナミック VLAN の併用を可能にするブロッキングモードをサポートしました。

3.9 スパニングツリープロトコルの情報表示コマンド

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」

show spanning-tree brief コマンドと show spanning-tree statistics コマンドが追加されました。

3.10 DHCP Snooping のオプションコマンド追加

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

DHCP Snooping の動作オプションを変更、確認する下記のコマンドが追加されました。詳細はコマンドリファレンスをご覧ください。

- ip dhcp snooping agent-option circuit-id vlantriplet
- ip dhcp snooping agent-option remote-id
- ip dhcp snooping verify mac-address
- show ip dhcp snooping agent-option

3.11 ARP のマルチキャスト MAC アドレス対応

参照「コマンドリファレンス」/「IP ルーティング」/「ARP」

マルチキャスト MAC アドレスを含んだ ARP パケットを受信可能にする arp-mac-disparity コマンドをサポートしました。
これにより、Microsoft Network Load Balancing（MS-NLB）などのマルチキャスト MAC アドレスを用いて動作するサービスに対応します。

3.12 IGMP Snooping の機能拡張

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

○ IGMP Snooping において、グループメンバーが存在しないマルチキャストトラフィックはすべてのポートにフラッディングされていましたが、フラッディングしないよう機能拡張しました。

○ show ip igmp snooping mrouter interface コマンドにおいて、インターフェース名の指定（interface IFRANGE）を省略できるようになりました。インターフェース名の省略時は、すべての VLAN インターフェースが表示対象になります。

3.13 MLD Snooping の機能拡張

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

MLD Snooping において、グループメンバーが存在しないマルチキャストトラフィックはすべてのポートにフラッディングされていましたが、フラッディングしないよう機能拡張しました。

3.14 DHCP サーバーのオプションコマンド

参照「コマンドリファレンス」/「IP 付加機能」/「DHCP サーバー」

IP アドレス使用状況確認機能の動作を制御する下記のコマンドが追加されました。

- probe enable
- probe packets
- probe timeout
- probe type

4　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 **5.3.4A-3.8** から **5.4.3-0.1** 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。

4.1　ユーザー権限レベルの細分化

参照「コマンドリファレンス」/「運用・管理」/「ユーザー認証」

ユーザーの権限レベルが 1 ～ 14、15 の 2 レベルから、1 ～ 6、7 ～ 14、15 の 3 レベルに細分化されました。

前バージョンまで

1 ～ 14	特権 EXEC モードへの移行権限を持たない（非特権 EXEC モードコマンドのみ実行可能）
15	特権 EXEC モードへの移行権限を持つ（すべてのコマンドを実行可能）

本バージョンから

1 ～ 6	特権 EXEC モードへの移行権限を持たない（非特権 EXEC モードコマンドのみ実行可能）
7 ～ 14	特権 EXEC モードへの移行権限を持たない（非特権 EXEC モードコマンドとすべての show コマンドのみ実行可能）
15	特権 EXEC モードへの移行権限を持つ（すべてのコマンドを実行可能）

4.2　リンクダウン / リンクアップ時のログレベル

参照「コマンドリファレンス」/「運用・管理」/「ログ」

VLAN またはポートインターフェースでリンクダウン / リンクアップが起きた際に出力されるログのログレベルが「notice/5」になりました。

4.3　VLAN インターフェースの ifIndex 値変更

参照「コマンドリファレンス」/「運用・管理」/「SNMP」

VLAN インターフェースのインターフェースインデックス（ifIndex）が次のとおり変更されました。

前バージョンまで
　200 + X（X は VLAN ID）

本バージョンから
　300 + X（X は VLAN ID）

4.4　DHCP Snooping テーブルのポートあたりエントリー数

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

DHCP Snooping テーブル（バインディングデータベース）に登録できるポートあたりの最大エントリー数が 118 から 115 に変更されました。これにともない、ip dhcp snooping max-bindings コマンドの書式も次のように変更されています。

前バージョンまで
　ip dhcp snooping max-bindings <0-118>

本バージョンから
　ip dhcp snooping max-bindings <0-115>

4.5 ハードウェアパケットフィルター登録数

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」

ハードウェアパケットフィルター登録数のサポートリミットが 122 から 118 に変更されました（28 ページの「サポートリミット一覧」を参照）。

4.6 CPU 宛て ARP Request パケットの優先制御

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

前バージョンまで、CPU 宛て ARP Request はキュー 0 で処理されていましたが、本バージョンからはキュー 1 で処理されるようになりました。

4.7 storm-downtime コマンドの初期値

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

QoS ストームプロテクション機能における、受信レート超過時の動作継続時間（自動回復までの時間）を設定する storm-downtime コマンドの初期値が、「設定なし（自動回復しない）」から「10 秒」に変更されました。

5 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 **5.4.3-0.1** 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。

5.1 複数の DNS サーバーを設定した際、show hosts コマンドで表示されるアドレスが「0.0.0.1」となっていましたが、これを修正しました。

5.2 起動中に Ctrl+C を入力すると再起動することがありましたが、これを修正しました。

5.3 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ていましたが、これを修正しました。

5.4 boot system コマンド、boot config-file コマンドでファイル名、および、フォルダー名にスペースが入っていてもエラーメッセージが表示されませんでしたが、これを修正しました。

5.5 Linux Kernel の脆弱性（CVE-2010-3432）への対策を行いました。

5.6 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ていましたが、これを修正しました。

5.7 内蔵ファンや内部の温度に異常が発生した場合、メモリーを大量に消費してしまうことがありましたが、これを修正しました。

5.8 NFS ポート（2049/tcp）がすべての IP インターフェースでリスニング状態になっていましたが、これを修正しました。

5.9 ランニングコンフィグ保存時に「no ip domain-lookup」（DNS 問い合わせ機能の無効化）の設定が保存されませんでしたが、これを修正しました。

5.10 ポリシーマップの追加 / 削除を繰り返すと、メモリーリークが発生していましたが、これを修正しました。

5.11 Telnet または SSH を用いてログインする際、パスワードが IMI に保存されたまま解放されない場合がありましたが、これを修正しました。

5.12 本来コンフィグモードで実行すべき do コマンドを非特権 EXEC モードや特権 EXEC モードで実行しようとしたとき、認識できないキーワードの先頭を指し示す「^」マークの位置が正しく表示されないことがありましたが、これを修正しました。

5.13 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、それ以降ログアウトするまで、非特権 EXEC モードで enable コマンドを実行しても特権 EXEC モードに移行できなくなっていましたが、これを修正しました。

5.14 CLI や SNMP の各種ファイル操作機能において、名前に「*」や「\」を含むファイルやディレクトリーを作成できていましたが、これらの文字を含むファイルやディレクトリーを作成できないように修正しました。

5.15 ファイルが存在しているディレクトリーを delete force recursive で削除することができませんでしたが、これを修正しました。

5.16 フラッシュメモリー上に多数のディレクトリーや階層を作成した状態で本製品をリブートするとログインできなくなっていましたが、これを修正しました。

5.17 SCP（Secure CoPy）経由でリモートサーバーにファイルをコピーする場合、コピー先のファイル名が正しくない名前になることがありましたが、これを修正しました。

5.18 フラッシュメモリーの空き容量が少ない状態で、フラッシュメモリーへの書き込みとファイル削除を頻繁に実行すると、まれにフラッシュメモリーへの書き込み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。

5.19 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、新パスワードの入力が拒否されログインできませんでしたが、これを修正しました。

5.20 show radius コマンドにおいて、Auth Status と Acct Status が正しく表示されませんでしたが、これを修正しました。

5.21 RADIUS サーバーを使用したユーザーのログインに失敗することがありましたが、これを修正しました。

5.22 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）を付けませんでしたが、これを修正しました。

5.23 ランニングコンフィグをファイルにコピーするとき、ログが正しく記録されませんでしたが、これを修正しました。

5.24 設定やポートのリンク状態にかかわらず、Syslog モジュールがメモリーリークを起こすことがありましたが、これを修正しました。

5.25 インターフェーストリガーに日付指定をしても、トリガーが起動されませんでしたが、これを修正しました。

5.26 起動時に、LLDP パケットの送信に失敗したという誤ったログが表示されていましたが、これを修正しました。

5.27 SNMP 経由でコンフィグファイルを作成するときに、ファイル名として使えない文字を使用してもエラーになりませんでしたが、これを修正しました。

5.28 Routing Information MIB の取得に失敗することがありましたが、これを修正しました。

5.29 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したが、これを修正しました。

5.30 AT-LOG-MIB の logIndex のオブジェクトのエージェントが返す Syntax が MIB 定義ファイルで定義されている Syntax と異なっていましたが、これを修正しました。

5.31 AT-FILEv2 MIB を用いて SNMP 経由でファイルやディレクトリーのコピー、移動、削除を行う際、ファイルパスにスペースが含まれていると処理に失敗していましたが、これを修正しました。

5.32 「no rmon collection stats」で RMON 統計情報エントリーを削除するときに、関連する RMON アラーム設定を先に削除しないと RMON 関連プロセスが異常終了していましたが、これを修正しました。

5.33 不要な UDP/TCP ポートがオープンしていましたが、これを修正しました。

5.34 「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 が併用できなくなっていましたが、これを修正しました。

5.35 SNMP の AT-SETUP mib にて backupCnfgPath を何も文字を入れないまま SET を実行すると、SNMP モジュールが正常に動作しないことがありましたが、これを修正しました。

5.36 LAG インターフェースが SNMP のブリッジ MIB のポート番号に割り当てられていませんでしたが、これを修正しました。

5.37 AT-LOG-MIB（プライベート MIB）に対し、logIndex=4294967295 の SNMP Get-Next 要求を受信すると誤った値を返していましたが、これを修正しました。

5.38 SNMP 経由で ipForwarding（1.3.6.1.2.1.4.1）オブジェクトに forwarding(1) をセットすると、IP パケット転送が有効になっていましたが、これを修正しました。

5.39 プライベート MIB の atPortInfoTranceiverTable を取得できませんでしたが、これを修正しました。

5.40 SNMP 経由で取得する ifInDiscards の値がつねに 0 になっていましたが、これを修正しました。

5.41 プライベート MIB の licenseNewInstallStatus を取得できませんでしたが、これを修正しました。

5.42 AT-Filev2-MIB（プライベート MIB）の atFilev2Table を取得できませんでしたが、新しい atFilev2FileViewer から同様の情報を取得できるようにしました。

5.43 sFlow 有効時にログメッセージが大量に出力され、本体宛通信が停止する場合がありましたが、これを修正しました。

5.44 show ntp associations コマンドを実行した後、その出力結果に続いて改行されずに新しいコマンドプロンプトが表示されていましたが、これを修正しました。

5.45 SSH サーバーのリスニング TCP ポート番号を 23 に設定すると不正なログが大量に出力されていましたが、これを修正しました。

5.46 本製品が SCP/SFTP 対応の SSH サーバーとして動作しているとき、他装置の SCP/SFTP クライアントと本製品の間で SCP/SFTP によるファイル転送ができませんでしたが、これを修正しました。

5.47 RADIUS サーバーを用いユーザー認証を行っている場合、筐体の再起動後、最初の SSH ログインに失敗していましたが、これを修正しました。

5.48 PC など他の装置から、SCP または SFTP クライアントソフトウェアを使って本製品のファイルをリモートコピーすると、ファイル転送は問題なく行われるものの、クライアントソフトウェア側で「sh: a: unknown operand」のようなメッセージが表示されることがありましたが、これを修正しました。

5.49 SSH にて公開鍵認証のみを許可にしている場合でも、クライアントから Challenge-Response（KeyBoard-Interactive）認証でアクセスすると、パスワードによって接続できていましたが、これを修正しました。

5.50 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でしたが、これを修正しました。

5.51 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 のままになっていましたが、これを修正しました。

5.52 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 のままになっていましたが、これを修正しました。

5.53 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、設定と異なるリンク状態になることがありましたが、これを修正しました。

5.54 SFP モジュールの障害を通知するログメッセージにポート番号が含まれていませんでしたが、これを修正しました。

5.55 ポートミラーリングにおいて、ミラーリングするトラフィックの向きを transmit から receive に変更した後でミラーポートの設定を解除すると、その後別のミラーポートを設定したときにポートミラーリングが正しく動作しないことがありましたが、これを修正しました。

5.56 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）を 2 秒以上に設定する必要がありましたが、この制限が解除されました。

5.57 ポートセキュリティー機能において、学習済みアドレスのエージング（switchport port-security aging）を有効にしていても、FDB にはスタティックエントリーとして登録されていましたが、ダイナミックエントリーとして登録するよう修正しました。

5.58 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。

5.59 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際、スタティックチャンネルグループに対してパケットストームプロテクションを設定すると正しく動作しませんでしたが、これを修正しました。

5.60 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したが、これを修正しました。

5.61 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っていましたが、これを修正しました。

5.62 LACP チャンネルグループの情報を詳細表示した際、ポート番号の表示が順番に表示されないことがありましたが、これを修正しました。

5.63 トランクポートで認証を使用し、ダイナミック VLAN で VLAN を割り当てられた Supplicant の認証がトランクポートのリンクアップで解除された場合、ゲスト VLAN 上で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。

5.64 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場合は所定の手順を踏む必要がありましたが、この制限を解除しました。

5.65 複数の Supplicant が同時に Web 認証を行った場合、いずれかの Supplicant の認証に失敗することがあります。このような場合、再度入力画面を表示しますが、この入力画面表示が崩れて正しく表示されない場合がありましたが、これを修正しました。

5.66 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、認証が解除されていましたが、これを修正しました。

5.67 802.1X 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ていましたが、これを修正しました。

5.68 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っていましたが、これを修正しました。

5.69 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したが、これを修正しました。

5.70 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っていましたが、これを修正しました。

5.71 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でしたが、これを修正しました。

5.72 OpenSSL 脆弱性（CVE-2010-4180）への対策を行いました。

5.73 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したが、これを修正しました。

5.74 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、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いましたが、これを修正しました。

5.75 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ていましたが、これを修正しました。

5.76 認証ポートと非認証ポート間で繰り返しローミングが発生した場合、認証ポート上で Supplicant の認証状態と FDB が一致せず、通信が遮断されることがありましたが、これを修正しました。

5.77 Auth-fail VLAN 使用時に 802.1X 認証と MAC ベース認証を併用、または、802.1X 認証、MAC ベース認証、Web 認証を併用する構成で、一度認証に成功した Supplicant が通信を終了し、再度認証を行うと認証が正しく行われませんでしたが、これを修正しました。

5.78 ポート認証において、2 回目の認証より、EAPOL パケット（EAP Request/Identity）の再送回数が auth supplicant-mac コマンドで設定した値と異なる場合がありましたが、これを修正しました。

5.79 Web 認証サーバーにおいてセッションキープ機能が有効な場合、リダイレクトされる URL の末尾に不要な文字が付与されることがありましたが、これを修正しました。

5.80 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でしたが、これを修正しました。

5.81 IPv6 が有効になっていないときでも DAD（Duplicate-Address-Detection）Neighbour Solicitation パケットを送信していましたが、これを修正しました。

5.82 アイソレート VLAN に接続された端末から、筐体のプライマリー VLAN に設定された IP アドレス宛ての通信ができてしまっていましたが、これを修正しました。

5.83 VLAN インターフェースの作成、削除を繰り返した際にメモリーリークが発生していましたが、これを修正しました。

5.84 IP サブネット VLAN において、設定済みの VLAN クラシファイアグループとルール番号を再度指定すると、重複して設定できていましたが、これを修正しました。

5.85 MST インスタンスのブリッジプライオリティーを複数回変更すると、ポートステータスが正しく設定されない場合がありましたが、これを修正しました。

5.86 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でしたが、これを修正しました。

5.87 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でしたが、これを修正しました。

5.88 STP 有効時、パケットストームが発生することがありましたが、これを修正しました。

5.89 EPSR 関連プロセスが異常終了すると、エンハンストリカバリー機能の設定が解除されていましたが、これを修正しました。

5.90 コマンドリファレンスに掲載されていない epsr mode master コマンドを入力すると、本製品ではサポートされていない EPSR マスター機能が有効になっていましたが、これを修正しました。

5.91 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ていましたが、これを修正しました。

5.92 RRP Snooping を無効から有効に変更したときに FDB のクリアが行われないため、タイミングによってマスタールーターの切り替え検出に時間がかかることがありましたが、RRP Snooping 有効時にバーチャルルーターの MAC アドレスのみ FDB からクリアすることでこれを修正しました。

5.93 VLAN 数のサポートリミット（256）を超えた場合にシステムがリブートすることがありましたが、これを修正しました。

5.94 ping コマンドの size パラメーターを用いて、出力インターフェースの MTU よりも大きいパケットを送信しようとすると同コマンドが失敗していましたが、これを修正しました。

5.95 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でしたが、これを修正しました。

5.96 Gratuitous ARP パケットによって学習済みの ARP エントリーが更新された場合、更新後数秒間該当 IP アドレスと本製品間の IP 通信ができなくなっていましたが、これを修正しました。

5.97 clear arp-cache コマンドで ARP エントリーを削除した後、削除したホストから ARP Reply を受信すると ARP キャッシュに登録していましたが、これを修正しました。

5.98 ダイナミック ARP エントリーをスタティック登録すると、登録直後はスタティック ARP エントリーとして登録されますが、しばらくするとエラーログが出力され、スタティック ARP エントリーが削除されることがありましたが、これを修正しました。

5.99 まれに、接続端末との ARP 解決に失敗し、その後 ARP テーブルへの登録ができないことがありましたが、これを修正しました。

5.100 起動時に ICMPv6 パケットを送信していましたが、これを修正しました。

5.101 VLAN を 29 個以上作成すると、29、59、89 番目のローカルの IPv6 アドレスが正しく設定されませんでしたが、これを修正しました。

5.102 MLD Snooping 有効時（初期設定で有効）、本製品と同じ仮アドレスを持つ IPv6 ホストから重複検出用の NS（近隣要請）を受信しても、NA（近隣通知）で応答しないことがありましたが、これを修正しました。

5.103 IPv6 の通信が正しく行えないことがありましたが、これを修正しました。

5.104 無効状態のインターフェースに ipv6 nd suppress-ra コマンドを実行すると、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。

5.105 受信した IGMP パケットを CPU 宛てキュー 1 ではなくキュー 0 で処理していましたが、これを修正しました。

5.106 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でしたが、これを修正しました。

5.107 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でしたが、これを修正しました。

5.108 IGMP Snooping を無効に設定すると、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。

5.109 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でしたが、これを修正しました。

5.110 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でしたが、これを修正しました。

5.111 IGMP Snooping 機能と IGMP Snooping Querier 機能を同時に動かしているとき、Leave メッセージを受け取ってもグループメンバーが離脱しませんでしたが、これを修正しました。

5.112 グローバルコンフィグモードで IGMP Snooping を無効にした状態で、インターフェースモードで IGMP Snooping を有効にし、その後、再度グローバルモードで IGMP Snooping を有効にした場合、IGMP Snooping が有効になりませんでしたが、これを修正しました。

5.113 IGMP Snooping において、高負荷のマルチキャストトラフィックを受信している状態で IGMP のグループ参加（Join）要求を受信した場合に該当グループを登録しないことがありましたが、これを修正しました。

5.114 本製品がサポートするマルチキャストグループアドレス登録数は最大 256 件ですが、ip igmp static-group コマンドでは 256 件を超えてもエラーになりませんでしたが、これを修正しました。

5.115 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したが、これを修正しました。

5.116 IGMPv3 グループアドレスがタイムアウト後も削除されずに残ることがありましたが、これを修正しました。

5.117 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いましたが、これを修正しました。

5.118 IGMP Snooping Report 抑制機能が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したが、これを修正しました。

5.119 グローバルコンフィグモードで no ipv6 mld snooping が設定されている場合、インターフェースモードで no ipv6 mld snooping を設定しても、コンフィグには反映されませんでしたが、これを修正しました。

5.120 DHCPv6 でメッセージ種別が Solicit のパケットを受信すると MLD Snooping のルーターポートとして登録されていましたが、これを修正しました。

5.121 show ipv6 mld snooping mrouter、show ipv6 mld snooping statistics interface コマンドにおいて、所属ポートが 1 ポートしかない VLAN の登録情報が表示されませんでしたが、これを修正しました。

5.122 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 になっていましたが、これを修正しました。

5.123 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でしたが、これを修正しました。

5.124 トランクグループからポートを削除し、そのポートを新規のトランクグループに追加した後、アクセスリストをトランクグループに追加すると、エラーが表示され、アクセスリストを追加することができませんでしたが、これを修正しました。

5.125 TCP パケットに対するハードウェア IP アクセスリストをいずれかのポートに適用したまま設定を変更した場合、エラーメッセージが表示されず、設定も直ちに反映されませんでしたが、正しくエラーとして処理されるよう修正しました。

5.126 「show ipv6 access-list ?」を入力しても後続のキーワードやパラメーターに関するヘルプが表示されませんでしたが、これを修正しました。

5.127 MLD Snooping 無効化コマンド（no ipv6 mld snooping）を含む設定で起動した場合、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 になっていましたが、これを修正しました。

5.128 Web 認証またはポリシーベース QoS の使用時、show platform classifier statistics utilization brief コマンドの表示が不正になることがありましたが、これを修正しました。

5.129 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でしたが、これを修正しました。

5.130 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 1 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でしたが、これを修正しました。

5.131 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したが（linkdown 指定時と同じ動作になります）、これを修正しました。

5.132 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でしたが、これを修正しました。

5.133 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」として反映されていましたが、これを修正しました。

5.134 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っていましたが、これを修正しました。

5.135 1 つのクラスマップに複数のハードウェアアクセスリストを適用させたとき、show mls qos interface policer-counters コマンドで表示されるカウンターのカウントアップの対象となるハードウェアアクセスリストは、シーケンス番号が最若番の ACL エントリーのみで、2 番目以降の ACL エントリーに対してはカウントアップしませんでしたが、これを修正しました。

5.136 QoS ストームプロテクション機能において、受信レートが実際の値より高く検出されていましたが、これを修正しました。

5.137 show mls qos interface storm-status コマンドにおいて、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したが、これを修正しました。

5.138 対象トラフィッククラスにシングルレートまたは、ツインレートの個別ポリサーを適用する際、設定したとおりに動作しませんでしたが、これを修正しました。

5.139 police single-rate コマンドの MINBURST と MAXBURST を省略して action に policed-dscp-transmit を指定すると、エラーメッセージが表示されていましたが、これを修正しました。

5.140 メータリングのアクションに drop-red を指定したとき、show mls qos interface policer-counters コマンドで表示される Aggregate Bytes の値に Red 帯域に分類されたバイト数が含まれていませんでしたが、これを修正しました。

5.141 Ping of Death 攻撃を検出の対象として設定した場合に、ポートがシャットダウンされませんでしたが、これを修正しました。

5.142 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っていましたが、これを修正しました。

5.143 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したが、これを修正しました。

5.144 DHCP サーバー機能で複数の DHCP レンジ（動的 IP アドレス範囲）を設定している場合、DHCP クライアントがレンジ間を移動すると、DHCP クライアントの仕様によっては移動後のレンジで IP アドレスを取得できないことがありましたが、これを修正しました。

5.145 default-router コマンドで、デフォルトゲートウェイアドレスとして正しくない値（255.255.255.255 など）を入力した際のエラーメッセージの内容が誤っていましたが、これを修正しました。

5.146 Ping ポーリング設定が 13 個以上存在していると、show counter ping-poll コマンドの結果が正しく表示されませんでしたが、これを修正しました。

5.147 複数の Ping ポーリングを設定していると、clear ping-poll all で Ping ポーリングのカウンターが初期化されませんでしたが、これを修正しました。

6 本バージョンでの制限事項

ファームウェアバージョン **5.4.3-0.1** には、以下の制限事項があります。

6.1 システム

参照 **「コマンドリファレンス」/「運用・管理」/「システム」**

○ ダイナミックコンフィグ上で、no ip name-server、no ip domain-lookup を設定しても DNS 問い合わせ機能が無効になりません。

○ 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

6.2 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。

6.3 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」

○ ZMODEM を使用して、ファイルサイズ 3 MByte 以上のファイルを転送すると、リブートすることがあります。

○ メモリー消費の大きい設定をしている場合（例：DHCP サーバーを使用している、VLAN を多数設定している、など）、ファームウェアイメージファイルのようにサイズの大きいファイルをダウンロードすると、「Total Free Memory is now Low xxx」のようなメッセージが表示されたり、debug-low-memory-*.tgz（* には可変の文字列が入ります）という名前のデバッグ用ファイルが出力されたりすることがありますが、動作上影響はありません。

6.4 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」

アクセスが許可されていないホスト / ユーザーから SSH でログインしようとした場合、コンソール上にデバッグメッセージが表示されます。

6.5 ログ

参照「コマンドリファレンス」/「運用・管理」/「ログ」

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。

6.6 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。

6.7 SNMP

参照「コマンドリファレンス」/「運用・管理」/「SNMP」

○ 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。

○ SNMP MIB で、ifHCInUcastPkts と ifHCOutUcastPkts の値が正しくありません。それぞれ、ユニキャストパケットの受信数と送信数を示すはずですが、ブロードキャスト / マルチキャストパケットもカウントされてしまいます。

○ 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。

○ 一定以上の文字数の名前を持つファイルが保存された状態で、SNMP MIB の atFilev2FileViewerName を get しようとすると、関連プロセスが異常終了し、本製品がリブートします。

6.8 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。

○ sFlow MIB の sFlowFsReceiver と sFlowCpReceiver の値を変更後、初期値に戻すためには sFlow を無効にする必要があります。

6.9 NTP

参照「コマンドリファレンス」/「運用・管理」/「NTP」

○ 実際には NTP サーバーと時刻同期が取れていない状態でも、show ntp associations コマンド上では同期済みと表示される場合があります。

○ すでに NTP サーバーが設定されている状態で、別のサーバーに設定を変更した場合、一度設定を削除した後、新規に設定を追加してください。削除せずに変更した場合、正しく同期しない場合があります。

○ 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, presicion is 2

○ show ntp association detail コマンドの org time および xmt time の表示が、NTP による同期の有無にかかわらず、「06:28:16.000 UTC Thu Feb 7 2036」を示します。これは表示だけの問題で、システムの時計の動作には影響しません。

○ 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 ピアまたは NTP サーバーのアドレスにドメイン名を指定した場合、コンソールの反応が数分の間停止したり、ドメイン名が正常に解決され、時刻を同期できているにもかかわらず、「Warning: Host xxx cannot be resolved」メッセージが表示されたりすることがあります。

6.10 端末の 1 画面当たり表示行数

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。

6.11 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.

6.12 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。

○ show interface コマンドで表示される dropped カウンターがカウントされません。show platform port counters コマンドの ifInDiscards カウンターで確認してください。

○ 1 つのインターフェースに設定可能な IPv6 アドレスは 16 アドレスまでです。

6.13 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」

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。

6.14 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 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。

6.15 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」

○ 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。

6.16 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」

○ LACP と LDF 検出は併用できません。

○ 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。

6.17 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。

6.18 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」/「インターフェース」/「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。

6.19 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」

○ 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）。

○ 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。

○ マルチキャストパケットの受信中に LACP チャンネルグループのメンバーポートをリンクダウンさせると次のようなログメッセージが出力されますが、動作には影響ありません。

2012 Nov 2 02:22:47 user.err x210-1 HSL[572]: HSL: ERROR: Can't find multicast FDB entry : Port port1.0.3 mac (0100.5e00.0002) VID 20

○ poX インターフェース（LACP チャンネルグループ）では、下記カウンターの値に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。
- show interface コマンドで表示される poX インターフェースの input packets 欄と output packets 欄
- ifHCInOctets
- ifHCOutOctes

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。

6.20 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」

○ 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。

○ 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。

○ dot1 control-direction コマンドの both オプションは未サポートです。

○ Supplicant の再認証間隔（reAuthPeriod）の初期値は 3600 秒ですが、2 回目の再送間隔は約 1800 秒と前回の再送間隔の約半分になります。一定間隔で再送する場合は、auth timeout reauth-period コマンドで初期値以外の値を設定してください。

○ 802.1X 認証の Supplicant がログオフしても、ステータスが Connecting になりません。

○ 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。

○ 802.1X 認証において、Auth-fail VLAN の設定を初期値のままにしていると Auth-fail VLAN へ移行できない場合があります。dot1x max-reauth-req コマンドで設定する EAPOL パケットの最大再送回数を dot1x max-auth-fail コマンドで設定する Supplicant の最大ログイン試行回数以上に設定してください。

○ Web 認証において、一度プロミスキャスモードに設定すると、その後インターセプトモードに変更しても、プロミスキャスモード設定時と同様に、動作します。インターセプトモードに設定を変更後、コンフィグを保存し、再起動した場合は、インターセプトモードとして動作します。

○ 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た場合、マルチキャストトラフィックが該当のポートにも転送され続ける場合があります。

6.21 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」

○ 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。

○ 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。

○ エンハンストプライベート 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 のプロミスキャスポートに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）を設定した場合、再起動後、ホストポートへパケットが転送されません。再起動後、プロミスキャスポートの設定を再入力すると、パケットが正常に転送されるようになります。

6.22 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」

チャンネルグループを作成後に MSTP を有効にすると、FDB に学習した MAC アドレスがケーブルがリンクダウンしてもクリアされません。チャンネルグループを作成する前に MSTP を有効にしてください。

6.23 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 の経路切り替えが発生した際、EPSR ポートから送信された一部のトラップが SNMP マネージャーに到達できない場合があります。

6.24 DHCP Snooping

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

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。

6.25 IP

参照「コマンドリファレンス」/「IP」/「IP インターフェース」

ループバックインターフェースに IP アドレスを設定した時、ループバックインターフェース宛のルートエントリーがハードウェアテーブルに登録されません。

6.26 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。

○ ライセンスなしでも IPv6 上での Ping 実行や syslog の転送が可能ですが、サポート対象外ですのでご注意ください。

6.27 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。

○ 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。

○ 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 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。

○ 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。

○ 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 を全ポートにフラッディングします。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。

○ 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。

○ 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）。

○ 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。

○ 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。

○ 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。

6.28 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。

○ 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。

○ IPv6 マルチキャストパケットの受信中に MLD Snooping を無効から有効に変更すると、MLD Snooping が有効になりません。MLD Snooping を無効から有効に変更するときは、IPv6 マルチキャストの通信が行われていない状態で実施してください。

○ 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。

○ 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。

6.29 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」

ntp access-group コマンドによって NTP サービスに対するアクセス制御の設定を行う場合、ホストを許可（permit）する形式で標準 IP アクセスリストを作成していると、エントリーにマッチするホストのみでなく、マッチしないホストも時刻の同期を行うことができてしまいます。標準 IP アクセスリストを作成する際、許可するホストを指定したあとに、すべてを拒否（deny any）するエントリーを追加してください。

6.30 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」

IGMP パケットはハードウェアパケットフィルターでフィルタリングできません。

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

○ 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 コマンドの設定を削除する場合、no mls qos コマンドよりも先に 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ル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ル方式を設定しなおしてください。

6.32 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、使用期限の切れた IP アドレスがデータベースから削除されません。なお、IP アドレスを割り当てる際には、IP アドレスが使用中かどうか確認してからクライアントに割り当てているため、動作に影響はありません。

6.33 Ping ポーリング

参照「コマンドリファレンス」/「IP 付加機能」/「Ping ポーリング」

Ping ポーリング機能を一旦無効化してから再度有効化すると、プロセス終了を示す以下のようなログが表示されますが、動作に問題はありません。
init: network/ping-poll main process (13750) killed by HUP signal

7 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。

7.1 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。

8 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。

9　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。

10　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.E）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/