



CentreCOM® x510シリーズ リリースノート

この度は、CentreCOM x510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 5.4.3-1.4

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 **5.4.3-0.1** から **5.4.3-1.4** 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 AT-x510-28GPX/AT-x510-52GPX

ファームウェアバージョン **5.4.3-0.1** 以降より、PoE 給電機能に対応した新機種「AT-x510-28GPX」、「AT-x510-52GPX」をサポートします。

2.2 フィーチャーライセンス AT-x510-FL01

本バージョンより、CentreCOM x510 シリーズ用プレミアムライセンス「AT-x510-FL01」をサポートします。

2.3 ダブルタグ 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」


ダブルタグ VLAN (VLAN スタッキング) をサポートしました。ご使用にはフィーチャーライセンスが必要です。

2.4 UDLD

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

対向機器との間でフレームの到達性を監視し、フレームの送信、もしくは受信が正しく行えない単方向のリンク状態を検出したとき、当該ポートをリンクダウンする UDLD (UniDirectional Link Detection) 機能をサポートしました。ご使用にはフィーチャーライセンスが必要です。


2.5 EPSR マスター


 **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」


リング構成の Ethernet ネットワークのループ防止・冗長化を管理、制御する EPSR マスター機能をサポートしました。ご使用にはフィーチャーライセンスが必要です。

2.6 IPv4/v6 経路制御プロトコル

 [「コマンドリファレンス」 / 「IP ルーティング」 / 「経路制御 \(RIP\)」](#)


 [「コマンドリファレンス」 / 「IP ルーティング」 / 「経路制御 \(OSPF\)」](#)

 [「コマンドリファレンス」 / 「IPv6 ルーティング」 / 「経路制御 \(RIPng\)」](#)

 [「コマンドリファレンス」 / 「IPv6 ルーティング」 / 「経路制御 \(OSPFv3\)」](#)

IPv4/v6 の各種経路制御プロトコルをサポートしました。IPv4 ルーティングはRIPv1/v2、OSPFに、IPv6 ルーティングはRIPng、OSPFv3に、新たに対応します。ご使用にはフィーチャーライセンスが必要です。

2.7 6to4 トンネリング

 [「コマンドリファレンス」 / 「IPv6 ルーティング」 / 「IPv6 インターフェース」](#)

IPv4 ネットワーク経由でIPv6の通信を可能にする6to4 トンネリングをサポートしました。ご使用にはフィーチャーライセンスが必要です。

2.8 platform stop-unreg-mc-flooding コマンド

 [「コマンドリファレンス」 / 「IP マルチキャスト」 / 「一般設定」](#)

platform stop-unreg-mc-flooding コマンドが追加されました。
L2 マルチキャスト環境でIGMP機能を使用してマルチキャスト通信を行っているとき、最初にグループに参加するとき、または、最後のホストがグループを脱退するとき、そのグループのIPマルチキャストパケットが一瞬フラッディングしますが、このコマンドを有効にすることで、フラッディングを抑制します。

2.9 PIM

 [「コマンドリファレンス」 / 「IP マルチキャスト」 / 「PIM」](#)

 [「コマンドリファレンス」 / 「IPv6 マルチキャスト」 / 「PIM」](#)

IPv4/v6 マルチキャスト経路制御プロトコルPIM (Protocol Independent Multicast) をサポートしました。IPv4 マルチキャストルーティングはPIM-DM (Dense Mode)、PIM-SM (Sparse Mode)、およびその拡張仕様であるPIM-SSM (Source Specific Multicast) を、IPv6 マルチキャストルーティングはPIM-SMv6に対応します。ご使用にはフィーチャーライセンスが必要です。

2.10 PIM-DM to SM Translation

 [「コマンドリファレンス」 / 「IP マルチキャスト」 / 「PIM」](#)

PIM-DMの下流インターフェースにある経路を、PIM-SMの下流インターフェースの経路に変換する機能をサポートしました。ご使用にはフィーチャーライセンスが必要です。


2.11 スタティック IPv4/v6 マルチキャストルーティング

 [「コマンドリファレンス」](#) / [「IP マルチキャスト」](#) / [「一般設定」](#)

 [「コマンドリファレンス」](#) / [「IPv6 マルチキャスト」](#) / [「一般設定」](#)

手動経路設定による IPv4/v6 マルチキャストルーティングをサポートしました。

2.12 ハードウェアアクセスリスト

 [「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 MAC アクセスリストの設定を行う `access-list(hardware mac)` コマンドに `vlan`、`inner-vlan` パラメーターが追加されました。

なお、同一 QoS クラスマップ内では、ハードウェアアクセスリスト (`match access-group` コマンドで指定) の `vlan`、`inner-vlan` と、クラスマップの `match vlan`、`match inner-vlan` 節を混在させず、どちらか一方だけをお使いください。

3 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 **5.4.3.0.1** から **5.4.3-1.4** 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。

- 3.1 VCS と 802.1X 認証を併用する構成において、VCS スレープ上に接続された Supplicant が認証に失敗していましたが、これを修正しました。
- 3.2 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したが、これを修正しました。
- 3.3 一度 NTP サーバーと同期した後、NTP サーバーとの通信が切断されても、`show ntp associations` コマンドおよび `show ntp status` コマンドの表示結果では NTP サーバーと同期しているように表示されていましたが、正しい状態を表示するよう修正しました。
- 3.4 `show loop-protection` コマンドで表示される Last LDF Rx の時刻が正しくありませんでしたが、これを修正しました。
- 3.5 ポートセキュリティによって学習された MAC アドレスをエージアウトするよう設定した場合、FDB と `show port-security interface` コマンドの「Total MAC Addresses」の値が一致しないことがありましたが、これを修正しました。
- 3.6 LDF フレームの Length フィールドに誤った値が設定されていましたが、これを修正しました。
- 3.7 802.1X 認証において EAPOL バージョンを 2 (IEEE 802.1X-2004 準拠モード) に設定した場合、一度 Supplicant が認証に失敗し、Auth-fail VLAN に割り当てられると、その後 Supplicant が EAPOL-Start パケットを送信しても認証を開始しませんでした。これを修正しました。


- 3.8 Web 認証による認証が成功する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。
- 3.9 転送有効 (enable) に設定された VLAN と無効 (disabled) に設定された VLAN が混在する設定において、switchport trunk allowed vlan コマンドに all パラメータを指定して、全ての VLAN ID のタグ付きパケットを送受信するよう設定しようとする、転送が有効に設定された VLAN 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。
- 3.10 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) からポートを削除した場合に、DHCP Snooping の DHCP リースの最大数が正しく更新されませんでした。これを修正しました。
- 3.11 RSTP のトポロジーチェンジが発生している最中、IP ユニキャストパケットを受信すると、パケットの転送が遅くなることがありましたが、これを修正しました。
- 3.12 IP 経路 (スタティック、ダイナミックとも) の登録時に、VCS 管理用サブネットと重複していると誤判定されてエラーとなり、該当経路が経路表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。
- 3.13 ポリシーベースルーティングで設定したネクストホップの経路が検出できない場合、新しい経路としてデフォルト経路が正しく選択されていませんでしたが、デフォルト経路を新しい経路として使用するよう修正しました。
- 3.14 VRRP とプロキシ ARP の両方を有効にしている VLAN インターフェースにおいて、マスタールーターにバーチャル IP アドレスを設定されていない場合、接続機器からの ARP Request に対して、バーチャル MAC アドレスではなく受信インターフェースの実際の MAC アドレスで応答してしまうことがありましたが、これを修正しました。
- 3.15 IPv6 使用時、仕様上の最大値まで IPv6 ホストエントリを登録できませんでしたが、これを修正しました。
- 3.16 IPv6 インターフェースがリンクダウンした状態からリンクアップするとき、2 回目以降のリンクアップからは DAD (Duplicate-Address-Detection) が行われていませんでしたが、リンクアップ時に毎回実行するよう修正しました。
- 3.17 スタティックに設定されたルーターポートで IGMP Query メッセージを受信すると、受信から 260 秒後に登録が解除されていましたが、これを修正しました。
- 3.18 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。
- 3.19 IGMP Snooping とエンハンストプライベート VLAN を併用する場合、マルチキャストパケットが無関係なポートに転送されてしまうことがありましたが、これを修正しました。
- 3.20 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でした。これを修正しました。

- 3.21 予約済み IPv6 マルチキャストアドレス (FF0X::) を含む不正な MLD Query を受信した際、MLD Query を破棄せずにフラッディングしていましたが、これを修正しました。
- 3.22 remark new-cos コマンドの internal オプションが正しく機能していませんでしたが、これを修正しました。
- 3.23 DHCP のリース時間の最小値は 20 秒にもかかわらず、20 秒未満を設定しようとした時のエラーメッセージとして「Lease must be at least one minute」と表示されていましたが、これを修正しました。
- 3.24 DHCP リレーエージェント機能において、DHCP パケットの転送先に IPv4 アドレスを指定している場合、DHCP リレーエージェント機能の設定を変更しようとした際、関連プロセス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。
- 3.25 通信中に AMF メンバーを再起動すると、再起動した機器の show atmf node コマンド、show atmf working-set コマンドの結果が正しくありませんでしたが、これを修正しました。
- 3.26 AMF、VCS、EPSR を併用した構成で、AMF メンバーを再起動すると、その配下のメンバーが AMF ネットワークに再参加しないことがありましたが、これを修正しました。

4 本バージョンでの制限事項


ファームウェアバージョン **5.4.3-1.4** には、以下の制限事項があります。

4.1 システム

 **「コマンドリファレンス」 / 「運用・管理」 / 「システム」**


- 次の通常起動時にロードされる通常用ファームウェアのイメージファイルが USB メモリー上にある状態で VCS のスタックメンバーに加入し、そのファームウェアが VCS マスターのものと異なると、次の緊急起動時にロードされるバックアップ用ファームウェアのイメージファイルが、USB メモリーではなくフラッシュメモリーにあるものとして指定されてしまいます。
- 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。
- 本製品は SD カードには対応していませんが、USB オートブート時に、SD カードに関するエラーメッセージがログに出力されます。これは表示のみの問題であり、動作には影響しません。
 - ・ daemon.err awplus automount[2577]: failed to mount /mnt/card

4.2 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。

4.3 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、リポートすることがあります。
- USB メモリーに空き容量がない状態で、create autoboot コマンドを実行するとエラーメッセージが表示され、その後別の USB メモリーを使用しようとする、正しくディレクトリーが読み取れません。エラーメッセージ出力後に別の USB メモリーを使う際は、一度本体を再起動してから使用してください。同一の USB メモリーを使用するには問題ありません。
- cd コマンドにて USB メモリーを利用中、USB メモリーを抜くと、その後再度 USB メモリーを挿しても認識されません。USB メモリーを抜く前には必ず、cd flash で USB メモリーの利用を中止してください。
- USB メモリーを取り外した時のメッセージが Enter キーを入力するまで表示されません。

4.4 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。
- tacacs-server timeout コマンドで設定できるタイムアウト値の最大は 190 秒です。
- ユーザー認証に TACACS+ を使用するとき、同時に使用できる仮想端末ポート (VTY) の数は 20 までとなります。また内部のユーザー認証データベースを使用するときは、同時に使用できる仮想端末ポート (VTY) の数は 33 までとなります。
- TACACS+ 認証を使用して VCS マスターにログイン後、他のスタックメンバーにリモートログインしている最中に、ほかの TACACS+ セッションが同じユーザー名、パスワードでログインすると、以下のメッセージが出力されます。
 - ・ You don't exist, go away!

4.5 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」


ローカル RADIUS サーバーに登録していない RADIUS クライアント (NAS) から、RADIUS Access-Request パケットを受信した場合、show radius local-server statistics コマンドで表示される Unknown NAS のカウンターがカウントアップしません。

4.6 RADIUS サーバー

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

- USB メモリーを利用してローカル CA の証明書をダウンロードする際、USB メモリーにすでに同じ名前のローカル CA の証明書が入っていた場合、Overwrite usb:/rootca.cer? (y/n) と確認のメッセージが表示されますが、Y も N も入力できず、上書きできません。USB メモリーに入っているファイルを削除するか、ファイル名を変更してダウンロードを行ってください。
- 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。

4.7 ログ

 **「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。
- MSTP 有効時、多数のインターフェースが同時にアップまたはダウンし、ログメッセージが大量に発生した場合、すべてのログメッセージが Syslog サーバーに転送されない場合があります。
- ターミナルモニターを有効にした後、VCS のバックアップメンバーにリモートログインを行いながら USB メモリーを抜き差しすると、ターミナルモニターのログが正しく表示されません。
- 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、default log buffered コマンドを実行すると、ログが出力されなくなります。
- 以下のログがコンソールに表示されないことがあります。
 - ・ Configuration update completed for portxxx
 - ・ Member x (xxxx.xxxx.xxxx) has become the Active Master
- 不揮発性メモリー (NVS) に出力するログメッセージのメッセージフィルターを追加した後、default log コマンドを使用して不揮発性メモリーのログ出力を初期値に戻しても、作成されたメッセージフィルターが削除されません。メッセージフィルターは、log(filter) コマンドを no 形式で実行するか、本体を再起動すると削除されます。
- (AT-x510-28GPX/AT-x510-52GPX のみ) 起動時において、電源ユニットに関するログが不自然なタイミングで表示されます。また、2つの電源ユニットがどちらも正しく動作しているにもかかわらず、一方についてのログしか表示されない場合があります。

4.8 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。

4.9 SNMP

「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。
- VCS 構成のシャーンに GetNext Request を送信すると、SNMP が 「no such object」と応答することがあります。
- SNMP MIB で、ifHCInUcastPkts と ifHCOOutUcastPkts 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、関連プロセスが異常終了し、本製品がリブートします。


4.10 sFlow

「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 が有効なインターフェースで VLAN タグがついたパケットを受信したとき、ingress 方向のサンプリング情報に VLAN タグ情報が付与されません。


- 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。

4.11 NTP

 **「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。
- NTP を使用していると、以下のログが出力されますが、動作には問題ありません。
 - ・ frequency error 501 PPM exceeds tolerance 500 PPM
- NTP を設定していないときでも、NTP カウンターがカウントアップします。
- 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, precision 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。

4.12 端末設定

 **「コマンドリファレンス」 / 「運用・管理」 / 「端末設定」**

- clear line console コマンドを実行すると、他の VCS メンバー上のコンソールで接続しているユーザーのセッションも切断されます。
- 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。

4.13 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.

4.14 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」

- 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。
- IPv6 アドレスを持つインターフェースに show interface コマンドを入力した際の結果に、実際のホップリミットの値が表示されません。
- 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。


4.15 フローコントロール

 **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」

SFP モジュールの対向機器がフローコントロールを有効にしている場合、本製品のフローコントロールを無効に設定していても、フローコントロールが動作してしまいます。


フローコントロールの初期設定は機器によって異なりますので、SFP スロットを使用して接続する際には、あらかじめ設定をご確認ください。

4.16 ポートセキュリティ

 **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は併用できません。
- ポートセキュリティ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。

4.17 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。

4.18 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」

- QoS と LDF 検出を同一ポートで併用した場合、LDF が CPU に到達しないようなアクセスリストを設定してしまうと、LDF パケットを受信してもループを検出できません。
- 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。
- 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)。
- 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。
- 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。

4.19 リンクアグリゲーション (IEEE 802.3ad)

 **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) 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
- 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。
- LACP ポート上にエンハンストプライベート VLAN のセカンダリーポートを設定することは未サポートとなります。


4.20 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。
- VCS とリンクアグリゲーション併用時、トランクポートで認証を行った後、Supplicant 宛てのパケットを VCS のスレーブで受信すると不必要なログメッセージが出力されます。

- ローミング認証有効時、同時に多数の Supplicant のポート移動を行うと、再認証が発生する場合があります。
- スタティックチャンネルグループ内にゲスト VLAN に所属している Supplicant がいると、そのトランクポートのコンフィグに switchport access vlan の設定が追加されてしまいます。チャンネルグループを削除しても switchport access vlan の設定は残るので、先に switchport access vlan の設定を削除してからチャンネルグループを削除してください。
- 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、認証成功後にリダイレクトされた Web ページの表示に失敗することがあります。その場合は Web ページを再読み込みしてください。
- 64 文字のユーザー名でポート認証を行うと、認証に失敗します。
- 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。
- 802.1X 認証において EAPOL パケット (EAP Request/Identity) を最大再送回数まで送信してしまうと、その後 Supplicant の抜き差しを行い EAPOL-Start パケットを受信しても、EAP-Request 送信間隔 (Tx Period、初期値 30 秒) が経過するまで EAPOL パケットを送信しません。


4.21 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」

- PoE に対応した機器と PoE に対応していない機器が混在した VCS 環境において、power-inline enable コマンドを入力すると、PoE に対応していない機器に対するエラーメッセージが表示されますが、一部の非 PoE ポートの分しか表示されません。

- 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。


4.22 バーチャル LAN

 **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。
- 大量に VLAN を作成後、switchport trunk allowed vlan コマンドを except オプション付きで指定しトランクポートの設定を行うと、再起動することがあります。switchport trunk allowed vlan コマンドを except オプション付きで指定するときには、VLAN 数を 700 以内にしてください。または、except オプションではなく、add または、all オプションを設定してください。
- 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。
- ダブルタグ VLAN のプロバイダーポートをミラーリングした場合、platform vlan-stacking-tpid コマンドの設定にかかわらず、TPID は常に 8100 となります。


- 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。
- コンフィグに何も設定されていない状態のとき、AMF の管理用 VLAN の初期設定として使用される vlan4091、vlan4092 を作成し、通常の VLAN としてポートに設定することができますが、スイッチングしません。
- VLAN ID 4094 をデータ VLAN として利用している場合、VLAN テーブル MIB (OID:1.3.6.1.2.1.17.7.1.4.2.1.3.0.4094) は利用できません。

4.23 GVRP

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


学習する VLAN 情報が多い場合、GVRP を設定しているポートをダウンさせ、その後すぐにアップさせると、正常に VLAN 情報が学習できなくなります。GVRP を利用する際の最大 VLAN 数は、100 です。

4.24 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。
- VCS と PIM-SM を併用している時、リポートローリングを行うと 20 秒程度のマルチキャストトラフィックの通信断が発生します。

4.25 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 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。
- EPSR と GVRP の併用は未サポートになります。

4.26 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。


- ip dhcp snooping agent-option allow-untrusted コマンドを実行し、リレーエージェント情報オプション（オプションコード 82）を含む DHCP パケットの Untrusted ポートでの受信を有効（破棄しない）に設定しても、リレーエージェント情報オプションを含む DHCP パケットが破棄されます。

4.27 IP ルーティング

 **「コマンドリファレンス」 / 「IP ルーティング」**


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。

4.28 経路制御

 **「コマンドリファレンス」 / 「IP ルーティング」 / 「経路制御」**


maximum-paths コマンドを設定して、コストパスの最大値を変更しても有効になりません。

4.29 OSPF

 **「コマンドリファレンス」 / 「IP ルーティング」 / 「経路制御 (OSPF)」**

- 2つのルーターの各々に同じ送信先アドレスとネクストホップを持つスタティックルートを設定し、External LSA の Forwarding address が Non-Zero になる設定をしたとき、優先度の低い（router ID の低い値を持つ）ルーターがグレースフルリスタートをさせると、優先度の低いルーターからの External LSA を登録してしまいます。不正な AS External LSA の情報を元にルート情報が作成されますが、経路は登録されているので通信は可能です。
- VRRP が動作する機器は、OSPF のエリア境界ルーター（ABR）に設定することはできません。
ABR でグレースフルリスタートが発生した後、隣接関係をダウンさせると、隣接関係を保持していたサブネットのサマリー LSA が削除されます。
- OSPF において、代表ルーター（DR）として動作している時に clear ip ospf process コマンドを入力すると、隣接ルーターが DR に変更されます。


4.30 IPv6 ルーティング

 **「コマンドリファレンス」 / 「IPv6 ルーティング」**

- IPv6 アドレスを設定する際、不正なインターフェース ID が指定されてもエラーになりません。
- 6to4 のトンネリングが確立している状態で DSCP 値をダイナミックに変更すると、その後トンネリングの確立に失敗します。DSCP 値を変更する場合は、変更後の設定を保存後、機器を再起動してください。
- 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。


- IPv6において、インターフェース経路（直接経路）が2重に登録されることがあります。
- IPv6において、VLAN が削除されたとき、リンクローカルアドレスがIPv6 転送表から消えません。

4.31 IPv6 インターフェース

 **参照** 「コマンドリファレンス」 / 「IPv6 ルーティング」 / 「IPv6 インターフェース」

6to4 トンネリングパケットの外側ヘッダーに TTL 値を指定すると、トラフィックが流れなくなります。

4.32 OSPFv3

 **参照** 「コマンドリファレンス」 / 「IPv6 ルーティング」 / 「経路制御 (OSPFv3)」

- 動作中の機器に OSPFv3 の設定をした場合、OSPFv3 が動作する VLAN インターフェースが一度リンクアップしないと、show ipv6 ospf interface コマンドで、OSPFv3 インターフェースの情報が表示されません。設定後は、機器を再起動するか、VLAN インターフェースの所属ポートをリンクアップさせてください。
- OSPFv3 使用時、passive-interface コマンドで指定するパッシブインターフェースには、実在するインターフェースのみを指定してください。
- OSPFv3 Authentication の設定を変更した場合は、設定を保存後、再起動してください。
- OSPFv3 が動作中に VCS フェイルオーバーが発生した場合、IPv6 ユニキャストトラフィックの回復に時間がかかることがまれにあります。
- 本製品を OSPFv3 のエリア境界ルーターとして使用する場合は、VCS 構成は使用できません。

4.33 近隣探索

 **参照** 「コマンドリファレンス」 / 「IPv6 ルーティング」 / 「近隣探索」

イベントログ上に「Neighbor discovery has timed out on link eth1->5」のログメッセージが不要に表示されることがあります。これは表示上の問題であり通信には影響はありません。


4.34 IGMP

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

- 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。
- show ip igmp groups コマンドの表示結果に、IGMP を有効に設定していない VLAN が表示されることがあります。これは show ip igmp groups コマンドの表示だけの問題であり、動作に影響はありません。

- IGMP プロキシシーにおいて、下流インターフェースに指定している VLAN を無効にしても、上流インターフェースにグループ情報が残り続けます。
- 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での 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。
- マルチキャストグループをスタティックに登録した後、登録したインターフェースにスタティックに登録してあるものと同じマルチキャストグループの参加、離脱が発生すると、マルチキャストグループがコンフィグから削除しても消せなくなります。
この場合は、マルチキャストグループにメンバーが参加した状態で `ip igmp static-group` コマンドを `no` 形式で実行するか、IGMP 機能を一旦無効にし、再度有効にすると、マルチキャストグループは正常に削除されます。


4.35 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。
- 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。
- IGMP Snooping を使用している際、スタティック登録のマルチキャストグループ宛に、ポートに直接接続されたグループメンバーからの Leave メッセージを受信すると、そのポートにはマルチキャストパケットは転送されなくなりますが、他のポートのグループメンバーから同じグループ宛に Join メッセージを受信すると、Leave メッセージによって転送のとまっていたポートにもマルチキャストが再び転送されてしまいます。
- 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、受信ポートが所属するすべての 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。


- 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。
- 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。

4.36 PIM

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


- PIMv6 使用時、PIMv6 インターフェースが最大まで設定されているとき、それらの VLAN の一つを削除しても、新たに VLAN インターフェースに PIMv6 を設定することができません。
VLAN インターフェースから PIMv6 の設定を削除してから、VLAN を削除してください。
- VRRPv3 と PIM-SMv6 は併用できません。

4.37 MLD

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

- MLDv2 において、グループエントリーがスタティック登録されている状態で、同じグループがダイナミックに登録され、待機時間が経過した時、ダイナミック登録されたエントリーとともに、スタティック登録されたエントリーもコンフィグから削除されます。
- `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 パケットの Max Query Response Time フィールドの値が、本製品の設定の 1 / 100 の数値で送出されます。MLD をお使いの際は、`ipv6 mld query-max-response-time` コマンドでなるべく大きい値（最大値は 240）を設定してください。

4.38 MLD 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 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。
- 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。


4.39 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。

4.40 ハードウェアパケットフィルタ

 **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」

- IGMP パケットはハードウェアパケットフィルタでフィルタリングできません。
- トランクポート上で OSPF の Hello パケットをフィルタリングできません。

4.41 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」

- ポリシーベースルーティングのネクストホップの最大登録数は 127 件です。
- QoS の match eth-format protocol コマンドで AppleTalk パケットを制御できません。
- 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 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。

4.42 攻撃検出

 **「コマンドリファレンス」 / 「トラフィック制御」 / 「攻撃検出」**

dos teardrop コマンドは未サポートです。

4.43 DNS リレー

 **「コマンドリファレンス」 / 「IP 付加機能」 / 「DNS リレー」**

DNS のキャッシュサイズまたはタイムアウトの設定を変更すると、IPv6 DNS キャッシュエントリが削除されます。

4.44 DHCP サーバー

 **「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。

4.45 DHCPv6 サーバー

 **「コマンドリファレンス」 / 「IP 付加機能」 / 「DHCPv6 サーバー」**

DHCPv6 サーバー機能において、動的に割り当てるアドレスの最終有効時間が infinite (無期限) の場合、IPv6 アドレスを配布しても、show コマンドに反映されません。


4.46 Ping ボーリング

 **「コマンドリファレンス」 / 「IP 付加機能」 / 「Ping ボーリング」**

Ping ボ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

4.47 アライドテレシスマネージメントフレームワーク (AMF)

 **「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 クロスリンク、EPSR、VCS を使用した構成で、VCS メンバーがダウンし、復旧した際、復旧した VCS メンバーに接続されている AMF ノードが認識されません。EPSR リング内では、AMF Node Depth 値が異なる AMF ノード同士は AMF リンクで接続してください。
- VCS 構成において、スタックリンクに障害が発生し VCS メンバーが Disabled Master 状態になると、スタックリンクとレジリエンスリンク以外のポートは無効化されますが、EPSR を併用している場合、show atmf nodes コマンドの結果には、Disabled

Master 状態となり無効化されたポートに接続された AMF ノードが表示されてしまいます。

EP SR リング内では、AMF マスターからの距離（ホップ数）の異なる AMF ノード同士は、AMF クロスリンクではなく AMF リンクで接続してください。

4.48 パーチャルシャーシスタック (VCS)


「コマンドリファレンス」 / 「パーチャルシャーシスタック」

- VCS バックアップメンバーが再加入中にコンフィグを変更すると、再加入したバックアップメンバーにコンフィグが反映されないことがあります。バックアップメンバーが加入中に設定の変更はしないでください。
- まれに VCS マスター切り替え後の新マスターが、設定されているプライオリティ値に従わずに選定されることがあります。
- VCS スレープを交換する際、マスターとスタックケーブルで接続して電源をオンした後、通常、スタック ID を変更し、AMF を有効に設定するため、2 回の再起動が必要になりますが、AMF ネットワークに所属後、コンフィグの同期に時間がかかり、コンフィグの同期後に以下のようなエラーメッセージが表示され、もう一度再起動を要求されます。
 - ・ Post startup check found the following errors:
 - ・ Processes not ready:
 - ・ authd bgpd epsrd irdpd lacpd mstpd ospf6d ospfd pdmd pim6d pimd ripd ripngd rmond sflowd vrrpd
 - ・ Timed out after 300 seconds
 - ・ Bootup failed, rebooting in 3 seconds.
 - ・ Do you wish to cancel the reboot? (y) :
- LDF が検出され link-down アクションが実行されている間にループを解消し、VCS マスター切り替えが発生すると、LDF 検出時アクションが実行されたポートが設定時間経過後も復旧しません。
該当のポートにて shutdown コマンドを no 形式で実行すると、リンクが復旧します。
- VCS と EP SR を併用する場合、reboot rolling コマンドを実行した際に約 1 分程度の通信断が発生する場合があります。
- VCS グループの再起動やマスター切り替えが発生すると、スレープのコンフィグから egress-rate-limit コマンドの設定が消えることがあります。
- 同一ネットワーク上に複数の VCS グループが存在する場合は、パーチャル MAC アドレスの下位 12 ビットとして使用されるパーチャルシャーシ ID を、該当する VCS グループ間で重複しないように設定してください。パーチャルシャーシ ID の設定は、stack virtual-chassis-id コマンドで行います。また、VCS グループのパーチャルシャーシ ID は、show stack コマンドを detail オプション付きで実行したときに表示される「Virtual Chassis ID」欄で確認できます。

5 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。

5.1 CentreCOM x510 シリーズの定格入力電流

 「取扱説明書」(Rev.B) 71 ページ

取扱説明書 (Rev.B) 71 ページ「本製品の仕様」の表において、AT-x510-28GTX/AT-x510-52GTX/AT-x510-28GPX/AT-x510-52GPX の定格入力電流の記載に誤りがありましたので、下記のとおり訂正いたします。

誤：

—	AT-x510-28GTX	AT-x510-52GTX	AT-x510-28GPX	AT-x510-52GPX
電源部				
定格入力電流	1.1A	1.1A	6.5A	6.8A
最大入力電流 (実測値)	0.97A	0.96A	5.9A	6.1A
平均消費電力	41W (最大52W)*4	69W (最大86W)*4	260W (最大530W)*4	270W (最大550W)*4
平均発熱量	150kJ/h (最大190kJ/h)*4	240kJ/h (最大310kJ/h)*4	940kJ/h (最大1900kJ/h)*4	990kJ/h (最大2000kJ/h)*4

* 4 AT-SP10LR × 4 個 使用時

正：

—	AT-x510-28GTX	AT-x510-52GTX	AT-x510-28GPX	AT-x510-52GPX
電源部				
定格入力電流 (AC電源×1個)	1.0A	1.0A	3.0A	3.0A
AC電源×1個 使用時				
最大入力電流 (実測値)	0.97A	0.96A	3.3A	3.6A
平均消費電力	41W (最大52W)*4	69W (最大86W)*4	150W (最大290W)*5	170W (最大320W)*5
平均発熱量	150kJ/h (最大190kJ/h)*4	240kJ/h (最大310kJ/h)*4	540kJ/h (最大1100kJ/h)*5	630kJ/h (最大1200kJ/h)*5
AC電源×2個 使用時				
最大入力電流 (実測値)	0.97A	0.96A	5.9A	6.1A
平均消費電力	41W (最大52W)*4	69W (最大86W)*4	260W (最大530W)*6	270W (最大550W)*6
平均発熱量	150kJ/h (最大190kJ/h)*4	240kJ/h (最大310kJ/h)*4	940kJ/h (最大1900kJ/h)*6	990kJ/h (最大2000kJ/h)*6

* 4 AT-SP10LR × 4 個 使用時


* 5 AT-SP10LR × 4 個 使用時

システム全体の PoE 負荷: 平均消費電力 / 発電量 = 93W 時、最大消費電力 / 発熱量 = 185W 時

* 6 AT-SP10LR × 4 個 使用時


システム全体の PoE 負荷: 平均消費電力 / 発電量 = 185W 時、最大消費電力 / 発熱量 = 370W 時

5.2 NTP

 [「コマンドリファレンス」](#) / [「運用・管理」](#) / [「NTP」](#)


NTP の認証が有効な NTP クライアントとして動作している場合でも、NTP の認証が有効でない NTP サーバーと時刻同期ができてしまいます。

5.3 ループガード (LDF 検出)

 [「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.B) 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。

5.4 スパニングツリープロトコル

 [「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」](#)

片方向通信中に STP でトポロジーチェンジが発生した場合、宛先 MAC アドレスがエージアウトしない場合があります。片方向通信のみの環境では、RSTP または MSTP を使用してください。

5.5 フォワーディングデータベース

 [「コマンドリファレンス」](#) / [「L2スイッチング」](#) / [「フォワーディングデータベース」](#)

登録されている MAC アドレス宛へ通信を転送している場合、エージングタイム経過後も該当アドレスが MAC テーブルから削除されません。

6 サポートリミット一覧

パフォーマンス	
VLAN 登録数	単体：4094 VCS：2000 ※ 1
MAC アドレス (FDB) 登録数	単体：16K VCS：4K ※ 2
IPv4 ホスト (ARP) 登録数	単体：2K VCS：768 ※ 3
IPv4 ルート登録数	1K ※ 4
リンクアグリゲーション	
グループ数 (筐体あたり)	128 ※ 5
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	
登録数	240 ※ 6 ※ 7 ※ 8
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
マルチプルダイナミック VLAN (ポートあたり)	1K
マルチプルダイナミック VLAN (装置あたり)	1K
ローカル RADIUS サーバー	
ユーザー登録数	100
RADIUS クライアント (NAS) 登録数	24
その他	
VRP-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	32

※ 表中では、K=1024

※ 1 VCS 構成時、VCS グループに設定する VLAN の数は 2000 個までをサポートします。

※ 2 VCS 構成時、フォワーディングデータベース (FDB) のエントリー数は 4K 個までサポートします。

※ 3 VCS 構成時、IPv4 ホスト登録数 (ARP エントリー数) は最大で 768 個までサポートします。

※ 4 インターフェース経路、スタティック経路、ダイナミック経路など、各種経路情報を含めた登録数です。

※ 5 スタティックチャンネルグループは 96 グループ、LACP は 32 グループ設定可能。合わせて 128 グループをサポートします。

※ 6 アクセスリストのエントリー数を示します。

※ 7 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。

※ 8 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。

7 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。

8 最新マニュアルについて

最新の取扱説明書「CentreCOM x510 シリーズ 取扱説明書」(613-001684 Rev.B)、コマンドリファレンス「CentreCOM x510 シリーズ コマンドリファレンス」(613-001763 Rev.C)は弊社ホームページに掲載されています。

なお、VCS の設定、運用に関する情報は、別紙「CentreCOM x510 シリーズ VCS 設定 / 運用マニュアル」に掲載しておりましたが、「CentreCOM x510 シリーズ コマンドリファレンス」(613-001763 Rev.B)以降、コマンドリファレンスに合わせて掲載しております。

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/>