



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、VCS設定 / 運用マニュアルの補足や、ご使用前にご理解いただきたい注意点など、お客様に最新の情報をお知らせするものです。最初にこのリリースノートをよくお読みになり、本製品を正しくご使用ください。

1 ファームウェアバージョン 5.4.2A-0.1

2 本バージョンでの制限事項

ファームウェアバージョン **5.4.2A-0.1** には、以下の制限事項があります。

2.1 システム

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

- ip domain-name コマンドでドメインを設定してなくても、ホスト名を使った Ping や Trace を実行できますが、その際、デフォルトドメインは DNS リクエストパケットに追加されません。ホスト名で Ping や Trace を実行する際は必ずドメインを指定してください。
- 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に指定され、show boot コマンドで表示されるパス表記が正しく表示されません。
- 起動直後に下記のログが出力される場合がありますが、動作には問題ありません。
 - ・ init: network/getty_console (ttyS0) main process (3874) terminated with status 255
- フラッシュメモリーの空き容量が 8MByte 以下の場合、NSM のレポートによる Core files が正しく保存されません。Core files を正しく保存するには 10MByte 以上の空き容量を空けて運用するようにしてください。

2.2 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」

- 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。

2.3 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、新パスワードの入力が拒否されログインできません。security-password forced-change コマンドの実行後は、設定内容をスタートアップコンフィグに保存してください。
- 特権パスワードを設定している場合、権限レベル 1～6 のユーザーも同一の特権パスワードで特権モードに移行できます。
- 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。
- ユーザー認証で TACACS+ サーバーを使用するときは、アカウントिंग機能を無効にしてください。
- 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 22 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。

2.4 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。

2.5 RADIUS サーバー

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

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、rwrite 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。

2.6 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。
- USB が挿入されていない状態で、show file system コマンドを実行すると以下のログが表示されます。
 - ・ 2000 Jan 1 11:46:07 daemon.notice awplus automount[19836]: >>
mount: mounting /dev/sda on /mnt/usb failed: No such device or address
 - ・ 2000 Jan 1 11:46:07 daemon.err awplus automount[19836]:
mount(generic): failed to mount /dev/sda (type vfat) on /mnt/usb
 - ・ 2000 Jan 1 11:46:07 daemon.err awplus automount[19836]: failed to
mount /mnt/usb
- 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。

2.7 SNMP

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

- dot1dStpPortState (ブリッジ MIB) において、ブロッキングポートの状態が blocking(2) ではなく disable(1) になっています。
- dot1dStpPortPathCost (ブリッジ MIB) の値が正しくありません。
- dot1dUserPriorityRegenTable への Get-Next 要求に対して間違ったオブジェクトを返します。
- SNMP マネージャーから OID 1.3.6.1.2.1.3.1.1.2 を Get できるのは、本体に ARP エントリーが 1000 個未満の場合に限ります。
- MIB-II の以下のオブジェクトは未サポートです。
 - ・ -currSoftSaveToFile
 - ・ -nextBootPath
 - ・ -backupPath
 - ・ -bootCnfgPath
 - ・ -backupCnfgPath

2.8 sFlow

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

- 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
sFlowFsPacketSamplingRate : 0 以外
に設定。

カウンタサンプリング
sFlowCpReceiver : 1
かつ
sFlowCpInterval : 0 以外
に設定。

- 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。

2.9 NTP

 **参照**「コマンドリファレンス」 / 「運用・管理」 / 「NTP」

- show ntp associations で、同期していないサーバーを同期していると、不正確な情報を表示することがあります。
- 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。

2.10 端末設定

 **参照**「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。

2.11 SSH 公開鍵認証

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

VCS 構成において、SSH のユーザー公開鍵を登録しても VCS グループ内で同期されず、VCS メンバーにユーザー公開鍵が登録されません。このため、SSH 公開鍵認証を用いて筐体へログインしている環境でマスターフェイルオーバーが発生すると、パスワードプロンプトが表示され、SSH 公開鍵認証を行うことができません。本問題が発生すると認証済みユーザー公開鍵リストに登録されているリモート SSH ユーザーの公開鍵情報が消去されます。remote-login コマンドを用いて VCS メンバーそれぞれに、手動でリモート SSH ユーザーの公開鍵を登録することで本問題を回避することができます。

2.12 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」 / 「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。

2.13 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」

- 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ー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。
- PAUSE フレームをミラーリングできません。

2.14 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」

- 10Mbps でリンクアップしているポートでは、ループガード (LDF 検出) と MAC アドレススラッシングプロテクションの link-down アクションが正しく動作しません。
- 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 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。
- 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。発生時刻を確認するには、log(filter) コマンドでメッセージのレベルを informational に設定し、show log コマンドを実行します。

2.15 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」

ポートセキュリティにおいて、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。

2.16 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。

2.17 リンクアグリゲーション (ポートトランキング)

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」

トランクグループのインターフェースを shutdown コマンドで無効にした後、ポートのインターフェースに no shutdown を実行すると、show interface コマンドで表示されるステータスが DOWN のままになります。トランクグループのインターフェースを無効にした後、有効にしたい場合は、トランクグループのインターフェースに no shutdown を実行してください。

2.18 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」

- 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。
- 802.1X 認証とゲスト VLAN 併用時に、再認証間隔が経過し認証が解除されているにも関わらず認証ポートがすぐにゲスト VLAN に戻らないことがあります。
- Web 認証でプロミスクラスモード設定時、Supplicant が認証に成功すると、不要なログが出力されることがあります。
- 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。
- Authenticator、RADIUS サーバー間の認証方式を eap-md5 にした場合、3Supplicant 以上が同時に認証できない場合があります。認証に失敗した場合は、再認証を行ってください。
- 802.1X 認証のサブリカントがログオフしても、ステータスが Connecting になりません。
- 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。

2.19 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」

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。

2.20 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時、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後、再び同一ポートに追加しようとする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。

2.21 エンハンストプライベート 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」

エンハンストプライベート VLAN 構成時、プロミスクキャストポートとセカンダリーポートを同時に削除すると、running-config コマンドで secondary group 0 と表示され、アイソレート VLAN 内で通信できてしまいます。

2.22 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。

2.23 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」

- show spanning-tree mst コマンドではすべての MST インスタンスが表示されず、ポートが所属している VLAN のみ表示されます。すべての MST インスタンスを表示したい場合は、show running-config コマンドを実行してください。
- 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後、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。
- 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。
- 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。

2.24 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」

運用中の EPSR ドメインをいったん無効化し、設定を変更して再度有効化したときは、設定を保存してシステムを再起動してください。

2.25 フォワーディングデータベース

 **参照** 「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」

マスター切り替え発生後、show mac address-table を実行すると、マスター切り替えを起こした機器のポートが CPU ではなく、sa1 と表示されます。

2.26 スタティック MAC アドレスの登録

 **参照** 「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」

mac address-table static コマンドの vlan パラメーターを省略した場合、指定したスタティック MAC アドレスはデフォルト VLAN (vlan1) の所属となります。意図しない設定になることを避けるため、同コマンドを実行するときは必ず vlan パラメーターを指定してください。

2.27 IP ルーティング

 **参照** 「コマンドリファレンス」 / 「IP ルーティング」

IP インターフェースがダウンして、同インターフェースに接続されたネットワークへの直結経路がなくなった場合、別のインターフェースを経由するデフォルト経路が存在していても、該当ネットワーク宛での本体発パケット (ping コマンドで送信する ICMP パケットなど) をデフォルトゲートウェイに送りません。ただし、該当ネットワーク宛での具体的な (0.0.0.0/0 でない) 迂回経路が存在している場合は、その経路を用いて正しく送信します。また、本体発でない端末間のルーティングパケットでは本現象は発生しません。

2.28 DHCP クライアント

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

- show dhcp lease コマンドの表示内容には、現在使用している情報だけでなく、過去に DHCP サーバーから取得した情報も含まれています。
- DHCP クライアントとして動作している場合、IP アドレスを取得するタイミングで以下のようなログが出力されます。
IMISH[xxxxx]: [SCRIPT] x x x x

2.29 等コストマルチパス (ECMP) ルーティング

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

ECMP は未サポートです。

2.30 VRRP

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

priority コマンドでバーチャルルーターの優先度を設定しても、優先度に従ったマスター選出が行われない場合があります。マスタールーターとなるはずの機器が、バックアップルーターになった場合、バックアップとなったインターフェースで通信ができなくなります。

2.31 IPv6 ルーティング

 **参照** 「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。

2.32 6to4

 **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 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。
- 6to4 のトンネリングパケットを送出するために必要な IPv4 経路が存在しない状態で、出力インターフェースが 6to4 トンネルインターフェースになる IPv6 パケットを受信すると、コンソール上に次のようなメッセージが表示されます。
ATL Virtual Device tunnel100 Error-Loop

2.33 IGMP

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

IGMPv3 にて Source を含んだ ChangeToExclude の Report でグループを登録した後に同一 Source を含んだ ChangeToInclude の Report を受信した場合に限り、clear ip igmp コマンドで該当グループを削除できなくなります。インターフェースのリンクをすべてダウンさせるか、IGMP を Disable にすることで削除されます。

2.34 IGMP Snooping

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

- 「no igmp」を実行して IGMP Querier 機能を無効化すると、IGMP Snooping のルーターポート設定 (ip igmp snooping mrouter interface コマンド) も削除されます。IGMP Snooping のルーターポートをスタティックに設定している場合、「no igmp」を実行したらルーターポートを設定しなおしてください。
- 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、受信後 260 秒後に登録が解除されます。
- マルチキャストグループが最大まで登録されていると、ルーターポートが登録されません。ルーターポートを先に登録してください。

2.35 MLD Snooping

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

- IPv6 リンクローカルアドレスを有効にしていないインターフェースにおいて、MLD Snooping 有効かつ Report 抑制機能有効時、:: をソースアドレスにもつ MLD listener report と Listener Done を送信してしまいます。
- MLD Snooping のスタティックグループ設定時に source パラメーター (送信者の IPv6 アドレス) を指定すると、同一 VLAN 上に設定された他のスタティックグループ宛でのトラフィックが転送されなくなります。
- IPv6 UDP マルチキャストを受信中に MLD Snooping を Disable にしてもマルチキャストパケットをフラッディングしません。

- Multicast Address Specific Query パケットはフラッディングされます。
- 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ます。

2.36 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。

2.37 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」

- VCS 構成でトランクグループに設定したポリシーマップが、VCS メンバーを取り外したとき、ポリシーマップを削除後、再度設定するとエラーが表示され、設定できません。
- 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。
- `wrr-queue disable queues` コマンドは未サポートです。

2.38 攻撃検出

 **参照** 「コマンドリファレンス」 / 「IP 付加機能」 / 「攻撃検出」

`dos teardrop` コマンドは未サポートです。

2.39 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」

- `show ip dhcp pool` コマンドにおいて、動的 IP アドレスの合計数 (Dynamic addresses の Total 欄) が正しく表示されないことがあります。
- DHCP Release メッセージを受信しても、`show ip dhcp pool` コマンドでは対象アドレスが Leased (リース中) にカウントされたままとなります。また、`show ip dhcp binding` コマンドでも対象アドレスが表示されたままとなります。ただし、DHCP クライアントからアドレス割り当ての要求を受けた場合は、表示上リース中でも実際に使用されていないことが確認されたアドレスは割り当ての対象となります。
- DHCP Release メッセージを受信しても、リポート時などに参照する NVS 上のバックアップファイルが更新されません (IP アドレスをリースするタイミングでは更新されません)。そのため、リポートや VCS のマスター切り替えが発生した後、解放済みの IP アドレスをリース中と認識してしまうことがあります。
- DHCP クライアントから DHCP release パケットを受信しても、`show ip dhcp binding` コマンドでクライアント情報が表示されます。実際はこのアドレスは割り当ての対象となるので、動作上の問題はありません。

2.40 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」](#)

複数の Ping ボーリングを設定していると、clear ping-poll all で Ping ボーリングのカウンターが初期化されません。1 つ目の Ping ボーリングを設定した際に、clear ping-poll all を実行しカウンターが消去されることを確認すれば、その後 2 つ以上を設定してもコマンドは正しく動作します。

2.41 バーチャルシャーシスタック (VCS)

 [「VCS 設定 / 運用マニュアル」](#)

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

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

 [「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」](#)

- VCS メンバー起動時に生成される vcstackStkPortLinkUp トラップと vcstackStkPortLinkDown トラップの送信順序が正しくないことがあります。
- VCS 構成時、スレープに接続したコンソールターミナルでは、ラインモードの length コマンドが正しく動作しないことがあります。
- VCS 構成、かつホストモードが Multi-host の時に、Active Master と Backup Member での認証状態が Authenticated と示されることがあります。これは表示だけの問題であり、動作には影響ありません。
- VCS 構成において、デフォルトコンフィグ (スタートアップコンフィグの設定なし) で再起動すると、以下のようなエラーメッセージが表示されますが、動作に影響はありません。
 - ・ daemon.err awplus rpc.statd[1425]: unable to register (stat d, 1, tcp)
- VCS グループをまたぐトランクポートにアクセスリストを設定した際、片側の筐体のみプロファイルサイズが上限に達すると、show platform classifier statistics utilization brief コマンドで表示されるプロファイルサイズの表示が誤った表示となります。本問題は再起動するまで誤った内容が表示され続けます。
- IPv6 機能と VCS は併用できません。
- VCS マスターにログインしている状態からスレープにリモートログインし、スレープ上で、show users コマンドを実行しても、VCS マスターのコンソールログインの情報が表示されないことがあります。一度、コンソールからログアウトすると正しく表示されるようになります。
- VCS 構成時、起動時に以下のエラーメッセージが出力されますが、動作に問題はありません。
 - ・ user.crit x900 HSL[1122]: Internal error: VCS sync timeout for lock-step operation
 - ・ user.err x900 HSL[1122]: No VCS sync response from member-1

3 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、VCS 設定 / 運用マニュアル）の補足事項および誤記訂正です。

3.1 NTP

 **参照** 「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。

3.2 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」

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、宛て先 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。

3.3 フォワーディングデータベース

 **参照** 「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 アドレス宛て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。

3.4 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」

コマンドリファレンスには記載されておりませんが、本製品はマルチキャスト 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ています。これは 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するためのもので、コマンド仕様は下記のとおりです。

arp-mac-disparity コマンド

モード

インターフェースモード

書式

[no] arp-mac-disparity

解説

マルチキャスト MAC アドレスの ARP エントリー（例：IP=192.168.10.2 / MAC=01-00-5e-28-0a-02）を登録可能にする。
デフォルトは登録不可。

注意・補足事項

本コマンドの設定により、ユニキャスト IP アドレスとマルチキャスト MAC アドレスの関連付けをした ARP エントリーがダイナミックに生成可能となるが、該当 ARP エントリーに登録された IP アドレス宛てのトラフィックは対応するポートにのみ送られる。

4 サポートリミット一覧

パフォーマンス	
VLAN 登録数	単体：4094 ※ 1 VCS：2000 ※ 2
MAC アドレス (FDB) 登録数	単体：16K VCS：4K ※ 3
IPv4 ホスト (ARP) 登録数	単体：2K VCS：768 ※ 4
IPv4 ルート登録数	1K ※ 5
リンクアグリゲーション	
グループ数 (筐体あたり)	128 ※ 6
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 ※ 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	-

※ 表中では、K=1024

- ※ 1 VCS 機能の有効 / 無効にかかわらず VCS 管理用に VLAN が一つ使用されます (デフォルトは VID 4094)。
- ※ 2 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。
- ※ 3 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。
- ※ 4 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。
- ※ 5 インターフェース経路およびスタティック経路を合わせた登録数です。
- ※ 6 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。
- ※ 7 アクセスリストのエントリー数を示します。
- ※ 8 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。

5 未サポート機能 (コマンド)

最新のコマンドリファレンス、VCS 設定 / 運用マニュアル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。

6 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.A)、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.A)、「CentreCOM x510 シリーズ VCS 設定 / 運用マニュアル」(613-001766 Rev.A) 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/>