



613-000710 Rev.H 080523



最初にお読みください

CentreCOM® 9424T/SP-E・9424Ts/XP-E リリースノート

この度は、CentreCOM 9424T/SP-E・9424Ts/XP-E をご購入いただき、誠にありがとうございました。

このリリースノートは、取扱説明書と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 2.4.1J

2 本バージョンで追加された機能

ファームウェアバージョン 2.3.1J から 2.4.1J へのバージョンアップにおいて、以下の機能が追加されました。各機能の詳細については、「CentreCOM 9424T/SP-E、9424Ts/XP-E コマンドリファレンス 2.4 (613-000699 Rev.C)」をご覧ください。

2.1 ループガード (受信レート検出)

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

パケットの受信レートがポートごとに設定された上限値を上回った場合に、該当ポートに対してリンクダウンやブロードキャストパケットの受信停止といったアクションをさせることで、ループの発生を防止するループガード (受信レート検出) に対応しました。

ENABLE SWITCH PORT STORMDETECTION コマンドで機能を有効にし、SET SWITCH PORT STORMDETECTION コマンドでパラメーターの設定を行います。

2.2 コンボポートのメディア選択

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

コンボポートに対して、以下の 3 種類のモードでメディアの指定ができるようになりました。

- ・ SFP (光ファイバー) または 10/100/1000BASE-T 自動認識 (両方リンク可能な状態のときには SFP 優先)
- ・ SFP (光ファイバー) 固定
- ・ 10/100/1000BASE-T 固定


SET SWITCH PORT コマンドの COMBO パラメーターで設定します。

2.3 Web 認証

 **参照** 「コマンドリファレンス」 / 「スイッチング」 / 「ポート認証」

Supplicant の Web ブラウザーを使用して、HTTP/HTTPS プロトコルによる機器の認証を行う Web 認証に対応しました。

2.4 PKI

 「コマンドリファレンス」 / 「スイッチング」 / 「PKI」

PKI (Public Key Infrastructure) に対応しました。本機能は Web 認証で HTTPS プロトコルを使用する場合に必要となります。


2.5 ポート認証機能拡張

 「コマンドリファレンス」 / 「スイッチング」 / 「ポート認証」

ポート認証関連機能を以下のとおり拡張しました。

- 1つのポートに対して複数の認証メカニズム (802.1X/MAC アドレスベース /Web) を設定できるようになりました。
- Multi-Supplicant モード時に、ポートに接続できる Supplicant の最大数が指定できるようになりました。最大 320 までの指定が可能です。
- 本製品の Authenticator ポートに HUBなどを介して Supplicant が接続されている環境で、HUB 配下の Supplicant の移動によって接続先の Authenticator ポートが変更された場合、移動先の Authenticator ポートで再認証を行わなくても認証許可状態を引き継ぐことができるようになりました (ただし、ポートの変更は同一スイッチ内のポート間のみで可能)。
- Supplicant が所属する VLAN をユーザー単位で動的に割り当てることができるようになりました (マルチプルダイナミック VLAN)。
- ゲスト VLAN への所属をポート単位ではなくユーザー単位で行えるようになりました。

2.6 ルーティング制御

 「コマンドリファレンス」 / 「バーチャル LAN」

ルーティングをさせない VLAN を作成できるようになりました。本機能を設定すると、該当の VLAN から他の VLAN への通信が遮断されます (ただし、他の VLAN から本機能を設定した VLAN への通信は可能)。

CREATE VLAN コマンドで L2ONLY パラメーターを指定して VLAN を作成します。

2.7 VRRP VLAN インターフェース / ポート監視

 「コマンドリファレンス」 / 「VRRP」

VRRP において、VLAN インターフェース / ポートの監視機能に対応しました、これにより、VLAN インターフェースまたはポートのリンクアップ・ダウンによるマスタールーターとバックアップルーターの切り替えが可能になります。

ADD VRRP MONITOREDINTERFACE コマンドで VLAN インターフェースを監視対象として設定します。

ポート監視機能の ON/OFF は CREATE VRRP コマンドの PORTMONITORING パラメーターで設定します。

2.8 DHCP サーバー


 「コマンドリファレンス」 / 「DHCP サーバー」

クライアントに対して動的に IP 設定パラメーターを提供する DHCP サーバー機能に対応しました。

3 本バージョンで仕様変更された機能

ファームウェアバージョン 2.3.1J から 2.4.1J 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。各機能の詳細については、「CentreCOM 9424T/SP-E、9424Ts/XP-E コマンドリファレンス 2.4 (613-000699 Rev.C)」をご覧ください。

3.1 MAC アドレスベース認証ポートのモード変更


 「コマンドリファレンス」 / 「スイッチング」 / 「ポート認証」

MAC アドレスベース認証では、Multi-Suppliant モード (MODE=MULTI) のみをサポートするように仕様変更しました。

ファームウェアバージョン 2.4.1J で、バージョン 2.3.1J 以前の Single-Suppliant モード (MODE=SINGLE) と同様の動作をさせるには、SET PORTAUTH PORT または SET PORTACCESS PORT コマンドで MODE=MULTI、SUPPLIMIT=1 を指定してください (SUPPLIMIT は、接続可能な Suppliant の最大数を設定するパラメーター)。

また、設定ファイルに MODE=SINGLE が記述されている場合も、バージョン 2.4.1J 以降のファームウェアでは MODE=MULTI、SUPPLIMIT=1 として動作します。

3.2 SHOW PORTACCESS/PORTAUTH コマンドの表示内容

 「コマンドリファレンス」 / 「スイッチング」 / 「ポート認証」

Suppliant の所属 VLAN をポート単位ではなく、ユーザー (Suppliant) 単位で設定できるようになったため、SHOW PORTACCESS/PORTAUTH コマンドの表示形態も変更されました。詳細はコマンドリファレンスを参照してください。

4 本バージョンで修正された項目

ファームウェアバージョン 2.3.1J から 2.4.1J 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 本製品に対して複数のクライアントから Telnet セッションの確立・切断を繰り返し行っているとき、SHOW FILE コマンド、CREATE CONFIG コマンドがエラーで実行できない場合がありますでしたが、これを修正しました。
- 4.2 本体宛での Telnet など TCP 通信において、再送が発生した場合、メモリーが解放されませんでしたでしたが、これを修正しました。
- 4.3 (9424Ts/XP-E のみ) SHOW SYSTEM コマンドで表示される System Up Time の時間と SNMP マネージャー上に表示される SystemTable の時間が一致していませんでしたが、これを修正しました。
- 4.4 Telnet 経由でコマンドを実行中に Telnet セッションを強制切断すると、マネージメントの送受信バッファが解放されないことがありましたが、これを修正しました。
- 4.5 Telnet 経由でコマンドを実行中にクライアントの接続ポートからケーブルを抜くと、マネージメントの送受信バッファが解放されないことがありましたが、これを修正しました。

- 4.6 SHOW SWITCH COUNTER で表示される「Frames 1519-1522 Bytes」が正しくカウントアップされるように修正しました。
- 4.7 (9424Ts/XP-E のみ) SET SWITCH MULTICASTMODE コマンドに B を指定して EAP パケット透過を有効にしても、VID=0 のタグ付きパケットが転送されませんでした。これを修正しました。
- 4.8 トランクグループからポートを削除した後、該当ポートに対して SET SWITCH PORT コマンドで複数のパラメーターを指定した設定を行うと、コンソールがハングアップすることがありましたが、これを修正しました。
- 4.9 CREATE QOS FLOWGROUP コマンドの PRIORITY オプションと、CREATE QOS POLICY コマンドの MOVEPRIORITYTOTOS オプションが同時に設定されていると、どちらの機能も正しく動作しませんでした。これを修正しました。
- 4.10 ポート認証と IGMP Snooping 併用時、IGMP パケットに対してポート認証が正しく動作しませんでした。これを修正しました。
- 4.11 ポート認証が成功し、ポートがダイナミック VLAN の所属になったとき、Supplicant からの該当 VLAN (の IP アドレス) 宛ての Ping に対して応答しませんでした。これを修正しました。
- 4.12 MAC ベース認証において、本製品からの 1 回目の Access-Request に対して RADIUS サーバーから応答がなく、Access-Request パケットが再送された場合、RADIUS サーバーから応答があっても認証が成功しませんでした。これを修正しました。
- 4.13 MAC アドレスベース認証の Authenticator ポートがリンクダウンすると、SNMP 用のメモリーが減少することがありましたが、これを修正しました。
- 4.14 本製品に HUB などを通して接続された端末を移動することで、本製品の接続ポートがリンクダウンをとまわずに変更された場合、ARP の登録が更新されず、本製品宛ての通信やルーティングができなくなっていました。これを修正しました。
- 4.15 ポート認証において、認証サーバーリストから削除された RADIUS サーバー宛てに Access-Request パケットが送信されていましたが、これを修正しました。
- 4.16 本製品の Authenticator ポートから EAP-Request (MD5) が再送信される場合のパケットフォーマットが正しくありませんでしたが、これを修正しました。
- 4.17 SET PORTAUTH PORT または SET PORTACCESS PORT コマンドの QUIETPERIOD パラメーターにハイフン (-) が指定できていましたが、これをできないように修正しました。
- 4.18 SHOW CONFIG コマンドの DYNAMIC パラメーターに PORTAUTH を指定できませんでしたが、これを修正しました。
- 4.19 ダイナミック VLAN によって Authenticator ポートの所属 VLAN を動的にアサインしようとしたとき、該当の Authenticator ポートに隣接するポートがタグ付きポートとして

所属している VLAN をアサインさせようとする、認証に失敗していましたが、これを修正しました。

- 4.20 MAC アドレスベース認証使用時、本製品の Authenticator ポートに HUB などを介して接続されている Supplicant をいったん HUB から外し、再度接続すると認証ができなくなりましたが、これを修正しました。
- 4.21 同一 ROUTE、同一 NEXTHOP で MASK のみ異なるスタティック経路がルーティングテーブルに追加登録される時、エラーが出力されないように修正しました。また、複数登録された場合、先に設定されていたスタティック経路を削除すると、正しく通信ができなくなる場合がありますでしたが、これを修正しました。
- 4.22 IP ヘッダーの終点 IP アドレスに IP マルチキャストアドレス、IP ペイロードに TCP ヘッダーを持った本製品 MAC アドレス宛てのパケットを受信すると、本製品がクラッシュしていましたが、これを修正しました。
- 4.23 IP インターフェースを複数設定し、そのうちの 1 つがリンクダウンしている状態で、別のインターフェースでデフォルトゲートウェイの ARP 解決がなされると、該当インターフェース宛ての Ping に応答しませんでしたでしたが、応答するように修正しました。
- 4.24 ローカルインターフェースとして設定されておらず、リンクダウンしているインターフェースに対して Telnet 接続が可能でしたが、これを修正しました。
- 4.25 RIP 有効時、経路情報に登録されている IP インターフェースがダウンしたとき、隣接ルーターに経路情報がメトリック 16 で通知されませんでしたでしたが、これを修正しました。
- 4.26 RIP 有効時、Address Family Identifier に 0、Metric に 16 がセットされた RIP パケットが Response で送信されていましたが、Request で送信されるように修正しました。
- 4.27 (9424Ts/XP-E のみ) 大量の ARP Request を受信し続けている状態で、本製品を起動すると起動後に ARP 解決ができない場合がありますでしたが、これを修正しました。
- 4.28 Gratuitous ARP Reply パケット受信時に、ARP キャッシュにエントリが登録されませんでしたでしたが、これを修正しました。
- 4.29 ネクストホップの ARP 解決のために ARP パケットを送信する際、送信処理のタイミングによっては本製品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。
- 4.30 VRRP のバックアップルーターとして動作しているときに、ブロードキャストパケットやバックアップルーター宛てのユニキャストパケットを高レートで受信し続けると、マスターに移行することがありましたが、これを修正しました。
- 4.31 VRRP 使用時、ルーターの状態が INITIAL (初期状態) から BACKUP (バックアップ)、または BACKUP から INITIAL に移行するとき、不正なログメッセージが出力されていましたが、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 2.4.1J には、以下の制限事項があります。

5.1 MSTP とポートランキングの併用

マルチブラスパニングツリープロトコル (MSTP) とポートランキングは併用できません。

5.2 ポート認証 (802.1X 認証 / MAC アドレスベース認証) と攻撃検出機能の併用

ポート認証 (802.1X 認証 / MAC アドレスベース認証) と攻撃検出機能は併用できません。

5.3 802.1X 認証とスパニングツリーの併用

ポート認証の 802.1X 認証とスパニングツリーは併用できません。

5.4 IGMP Snooping とポートセキュリティの併用


IGMP Snooping とポートセキュリティは併用できません。

5.5 マネージメントアクセスコントロール

 「コマンドリファレンス」 / 「運用・管理」 / 「マネージメントアクセスコントロール」


エントリーがない状態でマネージメントアクセスコントロールを有効にした場合は、ARP パケットの受信も許可しなくなる (ARP Request に応答しない) 仕様ですが、一度エントリーを追加して削除するという操作によってエントリーがない状態にした場合は、ARP パケットの受信が許可されるようになります。

5.6 攻撃検出

 「コマンドリファレンス」 / 「運用・管理」 / 「攻撃検出」

SYN Flood Attack、Smurf Attack、IP Options Attack のいずれかの不正パケット検出直後に、SET DOS SYNFLOOD、SET DOS SMURF、SET DOS IPOPTION コマンドの STATE パラメーターで有効・無効設定を変更すると、不正パケットを受信していないにもかかわらず、攻撃検出のメッセージが画面に表示されます。本現象は、検出した不正パケットと STATE パラメーター変更コマンドの組み合わせが同じ場合にのみ発生します。


5.7 コンパクトフラッシュ

 「コマンドリファレンス」 / 「運用・管理」 / 「記憶装置とファイルシステム」

コンパクトフラッシュ上のファイルに対して、ディレクトリーを指定して以下のコマンドを実行することができません。

- ・ COPY
- ・ RENAME
- ・ DELETE
- ・ SET CFLASH DIR

5.8 TFTP サーバーを使用したアップロード・ダウンロード

 「コマンドリファレンス」 / 「運用・管理」 / 「アップロード・ダウンロード」


TFTP サーバーからダウンロードした45Byte より小さいファイルを TFTP サーバーにアップロードすると、本製品がリブートすることがあります。

5.9 ログ

 「コマンドリファレンス」 / 「運用・管理」 / 「ログ」


- (9424T/SP-E のみ) 本製品 (CPU) 宛てのパケットを高レートで受信していると、「rps: RPS not present」という不正なログが出力される場合があります。これは表示だけの問題であり、動作には影響ありません。
- ログ機能が Disabled (無効) の状態で PURGE LOG コマンドを実行するとログ機能が Enabled (有効) になります。
- Default_VLAN に IP アドレスを設定していない状態で、他の VLAN に IP アドレスを設定し IP インターフェースを作成すると、「Set Management VLAN failed」という不正なログが出力されます。これは表示だけの問題であり、動作には影響ありません。

5.10 SNMP

 「コマンドリファレンス」 / 「運用・管理」 / 「SNMP」


複数の SNMP マネージャーから同時にプライベート MIB の取得を繰り返し行っていると、本製品の SNMP エージェントが応答しなくなる場合があります。

5.11 ブロードキャストパケットのフィルタリング

 「コマンドリファレンス」 / 「スイッチング」 / 「ポート」

SET SWITCH PORT コマンドの BCASTFILTERING パラメーターで、ブロードキャストパケットのフィルタリング機能を有効に設定しても、ARP Request パケットが破棄されずに受信されます。


5.12 L/A LED (9424Ts/XP-E のみ)

 「コマンドリファレンス」 / 「スイッチング」 / 「ポート」

以下の条件下において、まれに L/A (LINK/ACTIVITY) LED が正しく動作しない場合があります。


- ・ 本製品起動直後にポート 1 に対して DISABLE SWITCH PORT コマンドを実行 (消灯しない場合がある)
- ・ XFP ポートに対して DISABLE SWITCH PORT コマンドを実行 (消灯しない場合がある)
- ・ XFP ポートに対して ENABLE SWITCH PORT コマンドを実行 (点灯しない場合がある)

5.13 XFP ポートのリンク (9424Ts/XP-E のみ)

 「コマンドリファレンス」 / 「スイッチング」 / 「ポート」

XFP ポートに対して DISABLE SWITCH PORT コマンドを実行しても、対向機器からのパケットが受信され、受信パケットのカウンターもカウントされます (スイッチングは行われません)。


5.14 コンボポートのメディア選択設定

 「コマンドリファレンス」 / 「スイッチング」 / 「ポート」

- ファームウェアバージョン 2.4.1J で、SET SWITCH PORT コマンドの COMBO パラメーターでコンボポートに対してメディア選択の設定ができるようになりましたが、設定内容を SHOW SWITCH PORT コマンドで確認することができません。
- SET SWITCH PORT コマンドの COMBO パラメーターに FIBER (SFP の光ファイバーポート) を指定するときは、あらかじめ該当ポートの通信モードを AUTONEGOTIATE または 1000MFULL に設定しておいてください。


通信モードが 10/100M のまま FIBER に設定して保存すると、再起動時に FIBER の設定がエラーではじかれます。

5.15 ポートランキング

 「コマンドリファレンス」 / 「スイッチング」 / 「ポート」


- CREATE SWITCH TRUNK コマンドの SELECT パラメーターに MAC アドレスの選択基準 (MACSRC、MACDEST、MACBOTH) が指定されていると、ルーティング後のパケットが負荷分散されずに送われます。
- ARP エントリーが登録されているポートを含めてトランクグループを作成すると、負荷分散が行われません。トランクグループ作成後、RESET IP INTERFACE コマンドで ARP エントリーを削除すると、正常に負荷分散されるようになります。

5.16 ポートセキュリティー

 「コマンドリファレンス」 / 「スイッチング」 / 「ポート」


本製品に IP アドレスが設定されているとき、ポートセキュリティーが有効なポートで、本製品の IP アドレス宛ての ARP Request を受信すると、ARP Reply がフラッディングされます。

5.17 マルチプル VLAN (Protected Ports VLAN)

 「コマンドリファレンス」 / 「バーチャル LAN」


- Protected Ports VLAN のクライアントポートとタグ付きポートは同一ポートに設定できない仕様ですが、先にクライアントポートを設定し、次に同一ポートをタグ付きポートにする設定を行うと、設定がエラーではじかれません。
- SET SWITCH MULTICASTMODE コマンドで B (BPDU/EAP パケットを、VLAN を超えて、すべてのポートに転送する) が設定されていると、マルチプル VLAN (Protected Ports VLAN) のグループを超えて BPDU/EAP パケットが同一 VLAN 内にフラッディングされます。

5.18 スパニングツリー

 「コマンドリファレンス」 / 「スパニングツリープロトコル」 / 「STP」

スパニングツリー有効時、DISABLE SWITCH PORT コマンドを実行すると、SHOW STP PORT コマンドの表示項目「State」において、該当ポートが Blocking で表示されます。表示上の問題であり動作には問題ありません。

5.19 ラピッドスパニングツリー

 **参照** 「コマンドリファレンス」 / 「スパニングツリープロトコル」 / 「Rapid STP」


- Rapid STP 有効時、DISABLE SWITCH PORT コマンドを実行すると、SHOW RSTP コマンドに PORTSTATE パラメーターを指定して表示される「Enable」において、該当ポートが Disabled で表示されません。表示上の問題であり動作には問題ありません。
- Rapid STP 有効時、トポロジーチェンジ発生時にエッジポートに設定されたポートの FDB が消去されます。

5.20 クラシファイア

 **参照** 「コマンドリファレンス」 / 「クラシファイア」


CREATE CLASSIFIER コマンドの ETHFORMAT パラメーターに 802.2-UNTAGGED を指定した場合、ハードウェアパケットフィルタによる制御が正常に動作しません。

5.21 ポリシーベース QoS

 **参照** 「コマンドリファレンス」 / 「QoS」 / 「ポリシーベース QoS」

- トラフィックが同一 QoS ポリシー内の複数のトラフィッククラスにマッチした場合、CREATE QOS TRAFFICCLASS コマンドの MAXBANDWIDTH パラメーター（最大帯域設定）が正しく動作しません。
MAXBANDWIDTH パラメーターを指定する場合は、同一 QoS ポリシー内で、複数のトラフィッククラスにマッチするような設定（IP と TCP、TCP と TCP ポートなど一方がもう一方を包括するようなフィルタの指定）をしないようにしてください。
- (9424T/SP-E のみ) CREATE QOS POLICY コマンドの REDIRECTPORT パラメーターでトラフィックの出力先ポートとして指定されたポートから送出されるパケットにタグが付与されます。ただし、REDIRECTPORT に指定されたポートと同じポートグループ（1～12のグループまたは13～24のグループ）内から転送されたパケットに限り、本現象が発生します。
- SET QOS TRAFFICCLASS コマンドの EXCEEDREMARKVALUE パラメーターに NONE を指定することができません（エラーではじかれます）。
EXCEEDREMARKVALUE パラメーターを NONE に戻す場合は、該当のトラフィッククラスを DESTROY QOS TRAFFICCLASS で一度削除し、トラフィッククラスを作成しなおしてください。

5.22 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」 / 「ハードウェアパケットフィルタ」

- (9424T/SP-E のみ) ハードウェアパケットフィルタを設定する場合には、以下の点にご注意ください。
 - ・ アクションに許可 (permit) を使用する場合は、許可 (permit) が指定されているエントリを最後（最も大きい番号）になるように設定してください。
 - ・ アクション許可 (permit) とアクション破棄 (deny) を併用する場合は、許可 (permit) と破棄 (deny) の各エントリに同じ IP マスク値（例：24 ビット）を設定しないでください。
許可 (permit) と破棄 (deny) の各エントリで同じ IP マスク値を使用する場合

は、必ず、どちらか片方のエントリーにその他のパラメーター（例：UDPなど）を指定してください。

- （9424Ts/XP-Eのみ）ハードウェアパケットフィルターではエントリー番号順ではなく、コマンドで入力した順に処理されることがあります。設定を変更する場合は、PURGE ACL コマンド実行後に、エントリー番号順に設定を行ってください。

5.23 ポート認証

参照「コマンドリファレンス」/「スイッチング」/「ポート認証」

- ポートを Authenticator ポートに設定すると、同ポートで自動的にイーグレスフィルタリングが有効になり、その設定が設定ファイルに書き込まれます。Authenticator ポートではイーグレスフィルタリングが有効になっている必要がありますので、イーグレスフィルタリングの設定は変更しないようにしてください。
- 802.1X 認証で Single-Suppliant モードの場合、EAP-Request パケットの宛先は、条件により異なります。
Suppliant 対象の MAC アドレスを FDB に学習していない場合は、マルチキャストで送信しますが、学習後は、ユニキャストで送信します。
- ポートを 802.1X Authenticator ポートに設定すると、設定ファイルにイーグレスフィルタリングを有効にする設定が自動的に書き込まれますが、802.1X 認証を無効に設定しても、イーグレスフィルタリング有効の設定が解除されません。
- ポートを 802.1X Authenticator ポートに設定すると、設定ファイルに「set switch port=xx securitymode=pacontrol」という設定（未サポートのセキュリティーモード設定）が自動的に書き込まれます。
- SET PORTAUTH PORT または SET PORTACCESS PORT コマンドの SERVETIMEOUT/SERVTIMEOUT パラメーターに 31（秒）以上の値を指定すると、タイムアウト値が 60（秒）で動作します。
- ポートがリンクダウンしているときに、SET PORTAUTH PORT または SET PORTACCESS PORT コマンドの CONTROL パラメーターを設定変更できません。
- SET PORTAUTH PORT または SET PORTACCESS PORT コマンドの MODE パラメーターに MULTI、CONTROL パラメーターに AUTHORISED を指定しているとき、SHOW PORTAUTH (PORT) または SHOW PORTACCESS (PORT) コマンドでサブリカント数が正しく表示されない場合があります。
- 802.1X Authenticator ポートまたは MAC ベース認証ポートに、ADD SWITCH FILTER コマンドによるスタティック MAC アドレスの登録が可能です。登録されたスタティック MAC アドレスで通信をすることはできません。
- ダイナミック VLAN で、認証されたポートを別の MST インスタンスに所属する VLAN に指定した場合、同一 VLAN 内でも通信ができなくなります。
- ポートに対して、最初に Suppliant/Authenticator ポートの設定を行い、次に VLAN の設定（タグなしポートとして設定）を行うと、エラーで VLAN の設定ができません。また、本製品の仕様では、Suppliant/Authenticator ポートをタグ付きに設定することはできませんが、上記手順でタグ付きの設定を行っても、エラーになりません。Suppliant/Authenticator ポートの設定を行う場合は、最初に VLAN の設定を行うようにしてください。

- 1つのポートに対して MAC アドレスベース認証と Web 認証を設定しているとき、MAC アドレスベース認証中に Web 認証を行うと認証失敗となり、ログインページに戻りますが、ログインページに「Login Failed! Could not authenticate」のエラーメッセージが表示されません。
- RADIUS サーバーに送信される Access-Request パケットの始点 IP アドレスに、パケットを送出したインターフェースの IP アドレスがセットされます。
- MAC アドレスベース認証と Web 認証では、Supplicant の MAC アドレスがエイジングにより FDB から削除されると、認証許可状態が解除されます。

5.24 PKI

「コマンドリファレンス」 / 「スイッチング」 / 「PKI」

SET SYSTEM DISTINGUISHEDNAME コマンドで「/」を使用しないでください（「/」は未サポート）。「/」は設定ファイルで「,」に変換されます。

5.25 IP

「コマンドリファレンス」 / 「IP」

サーバーとして使用される UDP または TCP ポート番号がヘッダーの終点ポートにセットされた TTL=1 のパケットを受信すると、ICMP Time Exceeded メッセージが送信されません。

5.26 ARP

「コマンドリファレンス」 / 「IP」 / 「ARP」

- 異なるネットワークから本製品（CPU）宛ての通信を連続的に行うと、ARP が解決しているにもかかわらず、ARP Request が送信される場合があります。
- ARP 解決されていない IP アドレス宛てのルーティングされた 1 パケット目の TTL の値が 2 減算されます。

5.27 IPv6 マルチキャスト

「コマンドリファレンス」 / 「IPv6 マルチキャスト」

- IPv6 マルチキャストアドレスと一致した MAC アドレスのパケットを受信すると、マルチキャストグループとして登録してしまうことがあります。
- マルチキャストルーターに接続されるポートが存在しない状態で、Multicast Listener Report を受信すると、すべてのポートに転送されます。

6 取扱説明書・コマンドリファレンスの補足・誤記訂正

同梱の取扱説明書、および「CentreCOM 9424T/SP-E、9424Ts/XP-E コマンドリファレンス 2.4 (613-000699 Rev.C)」の補足事項です。

6.1 エンハンススタッキング

「コマンドリファレンス」 / 「運用・管理」 / 「エンハンススタッキング」


- マスタースイッチからスレーブスイッチに SNMP 経由でエンハンススタッキング接続している最中に、他のスイッチから該当のマスタースイッチに Telnet や SNMP による接続を行わないでください。

- SNMPv3 を使用して、エンハンススタッキンググループのスレーブスイッチにアクセスすることはできません。
- エンハンススタッキングを使用する場合、マスタースイッチとスレーブスイッチを接続するには、下記のとおりに接続してください。
 - ・ スレーブスイッチ側は、Default_VLAN に所属するポートにマスタースイッチを接続してください。Default_VLAN 以外の VLAN に所属するポートに接続した場合は、IP インターフェースを作成して IP アドレスを設定しなければなりません。
 - ・ マスタースイッチ側は、ローカルインターフェースに設定した VLAN に所属するポートにスレーブスイッチを接続してください。

6.2 本製品起動時のご注意

本製品の電源をオンにしてから起動が完了するまでの間は、電源ケーブルを抜いたり、リセットボタンを押したりしないでください。

6.3 認証サーバー

 「コマンドリファレンス」 / 「運用・管理」 / 「認証サーバー」

ADD RADIUSSERVER コマンドで認証サーバーリストに追加されたRADIUS サーバーと本製品が接続された状態で、ENABLE AUTHENTICATION コマンドにより認証が有効の場合は、RADIUS サーバーに登録したログイン名 / パスワードでしか本製品にログインすることができません。


本製品に設定されているユーザー名 / パスワードでログインする場合は、ENABLE AUTHENTICATION コマンドを実行しないでください。

6.4 SNMP

 「コマンドリファレンス」 / 「運用・管理」 / 「SNMP」

- プライベート MIB の atiStkSwSysProductInfoTable 内 atiStkSwSysDCState が正しい値を返しません。リダンダント電源装置「CentreCOM RPS3204」使用時は、SHOW SYSTEM コマンドで本製品の電源とリダンダント電源装置の電源の On/Off を確認してください。
- ブリッジ MIB の dot1dStpPort Table 内の dot1dStpPortEnable を変更しても設定は変更されません。本製品では、ポート単位でスパニングツリープロトコルの有効 / 無効を変更することはできません。
- SNMP マネージャーからシステム名を設定した場合、ログアウト / ログイン後にシステム名がプロンプトに反映されます。


6.5 フォワーディングデータベース

 「コマンドリファレンス」 / 「フォワーディングデータベース」

- リンクダウンをとまなわない端末移動があった場合、学習機能により登録された MAC アドレスがエージングするまで、通信が復旧しないことがあります。
- IP インターフェースを複数作成すると、FDB に PORT0 (ゼロ) の MAC アドレス (本製品の MAC アドレス) が複数表示されます。


- (9424T/SP-E のみ) ポートグループ 1～12 とポートグループ 13～24 グループ間で通信を行った場合、同一の MAC アドレスがどちらのポートの FDB にも表示される場合があります。
- 予約マルチキャストアドレスを、FDB にスタティックエントリーとして登録することはできません。

6.6 複数ポートから 1 ポートへの通信

 **参照** 「コマンドリファレンス」 / 「スイッチング」


- Jumbo フレームを複数ポートから 1 ポートに対して同時に送信すると、受信した 1 ポートからフレームが転送されません。
- ポートグループ 1～12 とポートグループ 13～24 間の通信において、複数ポートから 1 ポートに対して同時にパケットを送信し、パケットロスが発生した場合、送信ポートによってパケットの損失率にばらつきがあります。

6.7 ポートランキング

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


ランキンググループの最若番ポートを抜き差しすると、接続の組み合わせによって、ポートのリンクアップトラップが生成されない場合があります。

6.8 ポートミラーリング

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

ポートミラーリング機能が有効の場合、「01:80:C2:00:00:00」などの予約マルチキャストアドレスをソースポートで受信すると、ミラーポートからパケットが重複して送信されます。

6.9 MAC アドレス VLAN

 **参照** 「コマンドリファレンス」 / 「バーチャル LAN」

MAC アドレス VLAN で本製品宛での通信、およびルーティングをさせることはできません。


6.10 ポリシーベース QoS

 **参照** 「コマンドリファレンス」 / 「QoS」 / 「ポリシーベース QoS」

- CREATE QOS TRAFFICCLASS コマンドの MAXBANDWIDTH パラメーターに 0 (ゼロ) を指定すると、帯域ゼロのトラフィッククラスが作成されますが、このトラフィッククラスが割り当てられた QoS ポリシー作成直後の一定量の通信、および本製品再起動直後の一定量の通信に限り、該当ポートからのトラフィックがフィルタされません (帯域ゼロになりません)。
- (9424T/SP-E のみ) 出力ポートに QoS ポリシーを関連づけた場合、フィルターの対象となるのは学習済みのユニキャストアドレス宛でのトラフィックのみです。未学習のユニキャスト / マルチキャストアドレス、およびブロードキャスト宛でのトラフィックは対象になりません。また、学習済みのマルチキャストアドレス宛でのトラフィックも対象になりません。
- (9424Ts/XP-E のみ) 最大帯域幅 (MAXBANDWIDTH) が割り当てられたトラフィッククラスを QoS ポリシーで出力ポート (EGRESSPORT) に設定すると、


MAXBANDWIDTHが設定されていないポートのフラディングレートが、MAXBANDWIDTHと同じ値に制限されます。

6.11 ポート認証

 **「コマンドリファレンス」 / 「スイッチング」 / 「ポート認証」**


- ポート認証有効時、RADIUS サーバーを 3 台登録し、本製品からの Access-Request に対して 3 台とも応答がないと、全サーバーに対して同時に Access-Request パケットが再送されます。
- ポート認証有効時、RADIUS サーバーを 3 台登録し、優先順位 3 のサーバーでのみ認証が行われた場合、認証のたびに 3 台のサーバーに対して Access-Request パケットが送信されます。
また、優先順位 2 のサーバーでのみ認証が行われた場合は、優先順位 1 と 2 のサーバーに対して Access-Request パケットが送信されます。

6.12 PKI

 **「コマンドリファレンス」 / 「スイッチング」 / 「PKI」**


証明書のシリアル番号が -2147483649 以下、2147483648 以上の場合、SHOW PKI CERTIFICATE コマンドで表示される Serial Number の項には、xx:xx:xx:xx...の形式で表示されます。

6.13 バーチャル LAN

 **「コマンドリファレンス」 / 「バーチャル LAN」**


- MAC アドレス VLAN に MAC アドレスを追加したとき、別の VLAN から、MAC アドレス VLAN に追加した MAC アドレスを送信元 MAC アドレスとして持つ機器同士で双方向のユニキャスト通信を行うと、パケットが転送されてしまいます。
- (9424Ts/XP-E のみ) イングレスフィルタリング無効の状態では 2 つの VLAN を作成した場合に、双方のタグなしポート間で、VLAN を超えてフレームを転送してしまうことがあります。

6.14 マルチプル VLAN (Protected Ports VLAN)

 **「コマンドリファレンス」 / 「バーチャル LAN」**

複数の Protected Ports VLAN が存在し (例えば VLAN10 と VLAN20 が存在するような場合)、アップリンクポートの一部を共有している場合、VLAN10 のクライアントから VLAN20 宛てにパケットを送信すると、VLAN20 のアップリンクポートだけでなくクライアントポートにも送信されます。

6.15 ラピッドスパンニングツリー

 **「コマンドリファレンス」 / 「スパンニングツリープロトコル」 / 「Rapid STP」**

- ラピッドスパンニングツリープロトコルを有効にし、トランクグループに所属したポートがリンクアップすると、そのポートの通信速度の設定に関係なく、ポートプライオリティが 64、パスコストが 2000 に設定されます。
- ACTIVATE STP/MSTP コマンドを実行すると、設定ファイルに保存されますが、ACTIVATE RSTP コマンドを実行しても、設定ファイルには保存されません。

6.16 MLD Snooping

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

マルチキャストルーターが接続されるポートが存在しない状態で、Multicast Listener Reportを受信すると、すべてのポートに転送されます。

SET IPV6 MLDSNOOPING コマンドの ROUTERPORT パラメーターでポートを設定すれば転送されません。

7 未サポートコマンド (機能)

以下のコマンド (パラメーター) はサポート対象外ですので、あらかじめご了承ください。

```
MENU
SET SWITCH CONSOLEMODE
SET AUTHENTICATION METHOD=TACACS
ADD/DELETE TACACS SERVER
ENABLE/DISABLE/SHOW HTTP SERVER

SET SWITCH PORT
[BACKPRESSURE={YES|NO|ON|OFF|TRUE|FALSE|ENABLED|DISABLED}]
[BPLIMIT={1..7935}] [FCTRLLIMIT={1..7935}]

SET PORTAUTH PORT/SET PORTACCESS PORT
[FORCERENEWING={ENABLED|DISABLED}]
SET PORTAUTH IDTOGGLE

SET SWITCH PORT SECURITYMODE=PACONTROL

CREATE/DESTROY/ADD/DELETE/SET/SHOW LACP

ENABLE/DISABLE/SET/SHOW/PURGE GARP
SET VLAN={Vlanname|1..4094} [TYPE=PORTBASED]

PURGE/SHOW PKI
SET PKI CERTSTORELIMIT

SET/SHOW SSL

SET BOOTP RELAY MAXHOPS
```

8 コマンドリファレンスについて

コマンドリファレンス「CentreCOM 9424T/SP-E、9424Ts/XP-E コマンドリファレンス 2.4 (613-000699 Rev.C)」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、上記のコマンドリファレンスに対応した内容になっていますので、あわせてご覧ください。

コマンドリファレンスのパーツナンバー「613-000699 Rev.C」はコマンドリファレンスの全ページ (左下) に入っています。

<http://www.allied-tesesis.co.jp/>