J613-M0109-11 Rev.N 110630

Allied Telesis

CentreCOM® 9424T/SP　リリースノート

この度は、CentreCOM 9424T/SP をお買いあげいただき、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　2.3.5J

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 2.3.3J から 2.3.5J 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。

2.1　ポートトランキング

参照 「コマンドリファレンス」/「スイッチング」/「ポート」

トランクポートに接続された機器の MAC アドレスを、SNMP 経由で取得できるようになりました。

3　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 2.3.3J から 2.3.5J 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　SHOW DEBUG コマンドまたは SHOW CONFIG コマンドを INFO オプション指定で実行すると、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。

3.2　本製品を起動してから 4 日間経過すると、本製品から送出される SNMP トラップの System UP Time の値が 0（ゼロ）に戻っていましたが、これを修正しました。

3.3　同じ IP アドレスを異なる MAC アドレスの端末で使用すると、SNMP 用の ARP テーブルが更新されないため、SHOW IP ARP コマンドで表示される値と ipNetToMediaTable の値に不一致が発生していましたが、これを修正しました。

3.4　SNMP 設定が無効の状態でリンクアップ・ダウンが発生すると、まれに CPU 使用率が上昇し、本製品宛ての通信に影響を与えることがありましたが、これを修正しました。

3.5　Rapid STP 有効時、エッジポートに設定されたポートでリンクアップ・ダウンが発生すると、トポロジーチェンジのログ、トラップが生成されていましたが、これを修正しました。

3.6 Multiple STP において、1 つの MST インスタンスに対して多数の VLAN を関連付ける設定を行うと、一部の VID が設定ファイルに正常に反映されないことがありましたが、これを修正しました。

3.7 802.1X 認証で EAP-Request の再送が発生した場合、最後の再送パケットに対して Supplicant から EAP-Response を受信しても、RADIUS サーバーに Access-Request が送信されず、認証に失敗していましたが、これを修正しました。

3.8 802.1X 認証に失敗した後、再度認証を行おうとすると本製品がリブートしたり、認証ができなくなったりすることがありましたが、これを修正しました。

3.9 Sender Protocol Address フィールドが 0.0.0.0 の ARP パケットを受信すると、誤った内容が ARP キャッシュに登録される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 2.3.5J には、以下の制限事項があります。

4.1 MSTP とポートトランキングの併用

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

4.2 ポート認証と攻撃検出機能の併用

ポート認証と攻撃検出機能は併用できません。

4.3 IGMP Snooping とポートセキュリティーの併用

IGMP Snooping とポートセキュリティーは併用できません。

4.4 SNMP

参照 「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。

4.5 バーチャル LAN

参照 「コマンドリファレンス」/「バーチャル LAN」

ゲスト VLAN を設定している VLAN に、DESTROY VLAN コマンドを実行すると、VLAN が削除されてしまいます。

4.6 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」/「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。

4.7 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 で表示されます。
表示上の問題であり動作には問題ありません。

4.8 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ーの指定）をしないようにしてください。

○ 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。

4.9 QoS

参照「コマンドリファレンス」/「QoS」/「QoS」

SET QOS SCHEDULING コマンドに WRR（ラウンドロビン）、WEIGHTS パラメーターの Q7 に 0（ゼロ）を指定して、キュー 7 が最優先（STRICT）になる設定をした場合、ユーザープライオリティー値 7 を持つフラッディングパケットが最優先で転送されません。

4.10 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」/「ハードウェアパケットフィルター」

○ レガシーモードでは、エントリーを複数作成する場合に、アクションに許可（permit）が指定されているエントリーが最後（最も大きい番号）になるように設定する必要がありますが、新動作モード（エンハンスモード）ではこの制限は解除されます。

○ レガシーモードでは、アクションに許可（permit）を指定したエントリーに、アクションを破棄（deny）に指定したエントリーよりも大きなエントリー番号を設定しても、許可（permit）を指定したエントリーが正しく処理されない場合がありますが、新動作モード（エンハンスモード）ではこの制限は解除されます。

4.11 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。

- ○ ポートを 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、ポート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。
- ○ 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）コマンドでサプ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。
- ○ ポート認証使用時、Authenticator ポートに HUB などを介して接続されている Supplicant を、同一スイッチ内の別のポートに（Authenticator ポートをリンクダウンさせずに）移動することはできません。
- ○ ポートに対して、最初に Supplicant/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、Supplicant/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。Supplicant/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。
- ○ MAC アドレスベース認証では、Supplicant の MAC アドレスがエージングにより FDB から削除されると、認証許可状態が解除されます。
- ○ ポートがゲスト VLAN に割り当てられているとき、ゲスト VLAN に所属する別の PC から未学習のユニキャストアドレスでは通信できません。
- ○ Authenticator ポートにゲスト VLAN を設定している状態で、DISABLE PORTAUTH コマンドを実行しても、ゲスト VLAN に割り当てられてしまいます。

4.12 IPv6 マルチキャスト

参照 「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。

5 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 コマンドリファレンス 2.3（J613-M0109-12 Rev.G)」の補足事項です。

5.1 エンハンストスタッキング

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

○ マスタースイッチからスレーブスイッチに SNMP 経由でエンハンスト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。

○ エンハンスト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。

5.2 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。

5.3 認証サーバー

参照 「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。

○ ユーザー認証において、本製品から送信される Access-Request パケットの再送回数は 3 回が仕様ですが、2 回しか送信されません。

5.4 SNMP

参照 「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。

5.5 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」/「フォワーディングデータベース」

○ リンクダウンをとも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。

○ 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。

5.6 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。

5.7 ポートトランキング

参照「コマンドリファレンス」/「スイッチング」/「ポート」

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。

5.8 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。

5.9 マルチプル VLAN（Protected Ports VLAN）

参照「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。

○ 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。

5.10 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」

○ ラピッドスパ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ーが 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。

5.11 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ーされません（帯域ゼロになりません）。

○ 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て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て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てのトラフィックも対象になりません。

5.12 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」

○ ポート認証が有効のとき、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。

○ ポート認証が有効のとき、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。

○ RADIUS サーバーへの通信不可および RADIUS サーバーからの応答が遅延したときに、Access-Request パケットの再送が行われません。

5.13 MAC ベース認証とゲスト VLAN の併用

参照「コマンドリファレンス」/「スイッチング」/「ポート認証」

コマンドリファレンスの解説編および SET PORTACCESS PORT/SET PORTAUTH PORT コマンドのパラメーターの説明に以下の記述がありますが、MAC ベース認証とゲスト VLAN の併用は実際にはサポート対象外となりますので、訂正してお詫びいたします。

- （ポート認証の解説編「ゲスト VLAN の設定例」）
  Note - 以下の例は、802.1X Supplicant を使用していますが、MAC ベース認証でも同様に動作します。
- （SET PORTACCESS PORT/SET PORTAUTH PORT コマンドの説明）
  GUESTVLAN: （802.1X Authenticator ポート、MAC ベース認証ポート）ゲスト VLAN を指定する。

5.14 MLD Snooping

参照 「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。

6 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。

SET SYSTEM DISTINGUISHEDNAME
MENU
SET SWITCH CONSOLEMODE
SET AUTHENTICATION METHOD=TACACS
ADD/DELETE TACACS SERVER
SET SWITCH PORT
[BACKPRESSURE={YES¦NO¦ON¦OFF¦TRUE¦FALSE¦ENABLED¦DISABLED}]
[BPLIMIT={1..7935}][FCTRLLIMIT={1..7935}]
SET SWITCH PORT SECURITYMODE=PACONTROL
CREATE/DESTROY/ADD/DELETE/SET/SHOW LACP
ADD SWITCH FDB MODE=LOCKED
ADD SWITCH FILTER MODE=LOCKED
ENABLE/DISABLE/SET/SHOW PURGE GARP
SET VLAN={vlanname¦1..4049}[TYPE=PORTBASED]
CREATE/ADD/DELETE/SET/SHOW/PURGE PKI
SET/SHOW SSL

7 コマンドリファレンスについて

最新の取扱説明書「CentreCOM 9424T/SP、9408LC/SP 取扱説明書（J613-M0109-10 Rev.C）」およびコマンドリファレンス「CentreCOM 9424T/SP コマンドリファレンス 2.3（J613-M0109-12 Rev.G）」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。

コマンドリファレンスのパーツナンバー「J613-M0109-12 Rev.G」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-telesis.co.jp/