



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 2.3.0J

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 2.0.0J から 2.3.0J 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 2.3 (613-000699 Rev.B)」をご覧ください。

2.1 9424Ts/XP-E の機能追加

9424Ts/XP-E で以下の機能をサポートしました。


- ・ ハードウェアパケットフィルター (アクセスコントロールリスト)
- ・ QoS/ ポリシーベース QoS
- ・ 攻撃検出
- ・ IGMP Snooping
- ・ MLD Snooping

2.2 EPSR Snooping

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

リング構成の Ethernet ネットワークに特化したレイヤー 2 のループ防止・冗長化機能、イーサネットリングプロテクション (EPSR = Ethernet Protected Switched Ring) の Snooping 機能に対応しました。EPSR ドメインにおいて制御メッセージを監視し、リング障害の発生・回復時には FDB クリアを実施します。

2.3 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」


- 802.1X Authenticator ポートにおいて、認証方式 EAP-TLS、EAP-TTLS、EAP-PEAP に対応しました (EAP-TLS、EAP-TTLS、EAP-PEAP を使用する Supplicant を認証できるようにしました)。
- Single Authentication (Single-Supplicant モード) 時に、Authenticator ポートでゲスト VLAN を指定できるようになりました。SET PORTAUTH PORT または SET PORTACCESS PORT コマンドの GUESTVLAN パラメーターで指定します。

2.4 DHCP/BOOTP リレー

 「コマンドリファレンス」 / 「IP」 / 「DHCP/BOOTP リレー」

受信した DHCP/BOOTP パケットを別セグメントの DHCP/BOOTP サーバーに転送する DHCP/BOOTP リレーエージェント機能に対応しました。

2.5 VRRP


 「コマンドリファレンス」 / 「VRRP」

複数のルーター（レイヤー 3 スイッチ）をグループ化し、あたかも 1 台のルーターであるかのように見せかけることで、IP ネットワークに冗長性を与えるプロトコル、VRRP（Virtual Router Redundancy Protocol）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 2.0.0J から 2.3.0J 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 2.3（613-000699 Rev.B）」をご覧ください。

3.1 SET SWITCH MULTICASTMODE コマンド

 「コマンドリファレンス」 / 「スイッチング」

SET SWITCH MULTICASTMODE コマンドのデフォルト値が 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）から、A（BPDU/EAP パケットをすべて破棄する）に変更されました。

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 2.0.0J から 2.3.0J 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 本製品の電源をオンにしてから起動が完了するまでの間に、電源ケーブルを抜く、またはリセットボタンを押すと、SHOW SYSTEM コマンドで表示される MAC Address や Serial Number が不正な値になる場合がありましたが、これを修正しました。
- 4.2 SHOW SWITCH FDB コマンドまたは SHOW CONFIG コマンドで DYNAMIC パラメーターを指定して実行すると、エラーで表示がされない場合がありましたが、これを修正しました。
- 4.3 HTTP サーバー（サポート対象外）がデフォルトで有効になっているため、TCP ポート 80 番がオープンしていましたが、デフォルトで無効になるよう修正しました。
- 4.4 SHOW CFLASH コマンドの表示項目「Number of directories」に、カレントディレクトリーにあるサブディレクトリーの数ではなく、カレントディレクトリーにあるファイルの数（= Number of files と同義）が表示されていましたが、これを修正しました。
- 4.5 本製品起動時に生成される「system: System initialization complete」のログメッセージが、syslog サーバーに出力されませんでした。これを修正しました。

- 4.6 (9424Ts/XP-E のみ) プライベート MIB の以下のエントリーに対して Get Bulk Request を受けると、正しく値を返さない場合がありますでしたが、これを修正しました。
atiStkSwSysInfoGroup 配下
 - atiStkSwTemperatureInfoEntry
 - atiStkSwFanInfoEntry
- 4.7 プライベート MIB の atiStkSwSysTemperatureLimitValue が正しい値を返すよう修正しました。
- 4.8 プライベート MIB の atiStkSwSysProductInfoTable 内 atiStkSwSysRPSPresent が正しい値を返すよう修正しました。
- 4.9 RRP Snooping 使用時、マスターからスレーブへの切り替えが発生すると本製品の FDB がクリアされますが、この際、切り替え前のマスター接続ポート以外のポートの MAC アドレスが削除される場合がありますでしたが、これを修正しました。
- 4.10 (9424Ts/XP-E のみ) SET SWITCH PORT コマンドの PORT パラメーターに ALL、MDIMODE パラメーターに MDI または MDIX を指定して実行すると、「ERROR: Failed to configure port 25」というエラーメッセージが表示されていましたが、表示されないよう修正しました。
- 4.11 (9424Ts/XP-E のみ) XFP ポートがタグなしポートの場合でも、本製品 (CPU) 発の packets にタグが付与されて送信されていましたが、これを修正しました。
- 4.12 ルーティング後の packets がトランクポートに転送されたとき、アルゴリズムに従った分散が行われずに送られていましたが、これを修正しました (ただし、アルゴリズムに IP アドレスを指定した場合のみ)。
- 4.13 802.1X 認証と MAC ベース認証併用時、SHOW PORTAUTH または SHOW PORTACCESS コマンドで表示される「Number of Suppliants」の値が正しくありませんでしたが、これを修正しました。
- 4.14 MAC ベース認証有効時、RADIUS サーバーを複数台登録しても、優先順位 2 以降のサーバーに対して正常な認証を行うことができませんでしたが、これを修正しました。
- 4.15 RADIUS Access-Request packets に含まれる Calling-Station-Id/Called-Station-Id の MAC アドレスが、「-」を用いて表されるよう修正しました。
- 4.16 本製品を DHCP クライアントとして動作させた場合に、DHCP クライアントのリース時間経過後に送信される DHCP Discover の送信間隔が、60 秒を超えた後は 60 秒間隔で送信されるよう修正しました。
- 4.17 (9424Ts/XP-E のみ) TTL=1 の packets を受信しても、ICMP Time Exceeded メッセージが送信されませんが、これを修正しました。
- 4.18 RIP 有効時、ARP request を受信中にポートのリンクアップ・リンクダウンを繰り返すと、本製品がハングアップする場合がありますでしたが、これを修正しました。

以下の項目は、ファームウェアバージョン 2.0.0J のリリースノートに記載されていませんでしたが、実際には 2.0.0J で修正済みでした。

4.19 SNMP 有効時、SNMP マネージャーからのアクセスによってメモリーコラプションが発生し、本製品がハングアップする場合がありますでしたが、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 2.3.0J には、以下の制限事項があります。

5.1 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を同一ポートで併用できません。

5.2 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。

5.3 ポートランキングと RRP Snooping の併用

ポートランキングと RRP Snooping は併用できません。

5.4 SHOW FILE コマンドと CREATE CONFIG コマンド

 **「コマンドリファレンス」 / 「運用・管理」**

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。

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。
- マネージメントアクセスコントロールが有効の場合、本製品で ARP が解決されずに正しくルーティングできないことがあります。ルーティング機能使用時に、本製品（CPU）宛ての packets をフィルタリングする場合は、ハードウェアパケットフィルターを使用してください。

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 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。
- 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。

5.9 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。

5.10 SHOW SWITCH COUNTER コマンド

 「コマンドリファレンス」 / 「スイッチング」


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ません。

5.11 EAP パケットのフラッディング仕様

 「コマンドリファレンス」 / 「スイッチング」

- SET SWITCH MULTICASTMODE コマンドでマルチキャストフレームのフラッディング仕様が設定可能ですが、EAP パケットについては、設定にかかわらず常に D (BPDU/EAP パケットを、VLAN 内に転送する。タグ付きポートを含む。ただし、BPDU/EAP パケットにタグが付けられることはない) で動作します。
- SET SWITCH MULTICASTMODE コマンドに D (BPDU/EAP パケットを、VLAN 内に転送する。タグ付きポートを含む。ただし、BPDU/EAP パケットにタグが付けられることはない) が指定されている場合、タグ付きポートで受信する EAP パケットにはタグが付与されています。


5.12 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」

- 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。


- トランクグループからポートを 1 ポート削除すると、残りのトランクポートでリンクダウン・アップが発生します。
- 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出されます。
- 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。

5.13 ポートセキュリティ

 **「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。

5.14 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」**


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。

5.15 バーチャル LAN

 **「コマンドリファレンス」 / 「バーチャル LAN」**


IP アドレスが割り当てられた VLAN を削除する場合は、DELETE IP INTERFACE コマンドで IP アドレスを削除してから、DESTROY VLAN コマンドを実行するようにしてください。IP アドレスが割り当てられた VLAN を指定して DESTROY VLAN コマンドを実行してもエラーで設定はできませんが、その後に本製品に Telnet 接続をして、CREATE VLAN コマンドを実行すると本製品がハングアップする場合があります。

5.16 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。

5.17 ラピッドスパニングツリー

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

5.18 クラシファイア

 **「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。

5.19 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 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。
- (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ら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。
- (9424T/SP-E のみ) 9424T/SP-E では、ルーティング後のパケットは常にユーザープライオリティー 7 で扱われます（L2 スイッチングされたパケットはユーザープライオリティー 0 で扱われます）。このため、意図的にプライオリティー 7 に設定されたパケットとルーティング後のパケットが同一プライオリティーで扱われることとなります。優先させたいパケットがある場合、優先させたくない（優先順位の低い）パケットに対してプライオリティーを下げる設定を行うようにしてください。

5.20 ハードウェアパケットフィルター (9424T/SP-E のみ)

 **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」

ハードウェアパケットフィルターではアクションに許可 (permit) が指定されているエントリーが最優先で処理される仕様ですが、エントリーが複数作成されていると、エントリー番号の大きいエントリーが優先的に処理される場合があります。
エントリーを複数作成する場合は、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）になるように設定してください。

5.21 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。
- ポート認証で、Single-Suppllicant 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。
サブリカント対象の 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。
- 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。
- 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。
- 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。
- 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。

5.22 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。

5.23 IP インターフェース

「コマンドリファレンス」 / 「IP」 / 「IP インターフェース」


- ダウンした IP インターフェース宛ての Ping に対して応答する場合があります。ただし、デフォルトゲートウェイの ARP 解決がなされていると本現象は発生しません。
- 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 接続が可能です。リンクアップしているインターフェースに対しては、Telnet 接続できません。

5.24 RIP

「コマンドリファレンス」 / 「IP」 / 「経路制御 (RIP)」

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 で通知されず、通信の復旧に約 180 秒かかります。

5.25 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。
- 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。

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 2.3 (613-000699 Rev.B)」の補足事項です。

6.1 エンハnstスタッキング

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

- SNMPv3 を使用して、エンハnst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nst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。

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」


- リンクダウンをとみ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。
- 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

 「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 ポートミラーリング

 「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。

6.8 ポリシーベース QoS

 「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。

6.9 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。
- SET PORTAUTH PORT または SET PORTACCESS PORT コマンドの TYPE/ROLE パラメーターに NONE を指定すると、指定ポートの設定をデフォルトに戻すことができますが、このとき、PORTAUTH/PORTACCESS パラメーターに認証メカニズム (802.1X または MACBASED) を指定する必要はありません。MAC ベース認証の設定であっても、MACBASED の指定をせずにコマンドを入力してください (指定すると、エラーになりコマンドが実行されません)。

6.10 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。
- 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。

6.11 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。

6.12 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。


6.13 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。

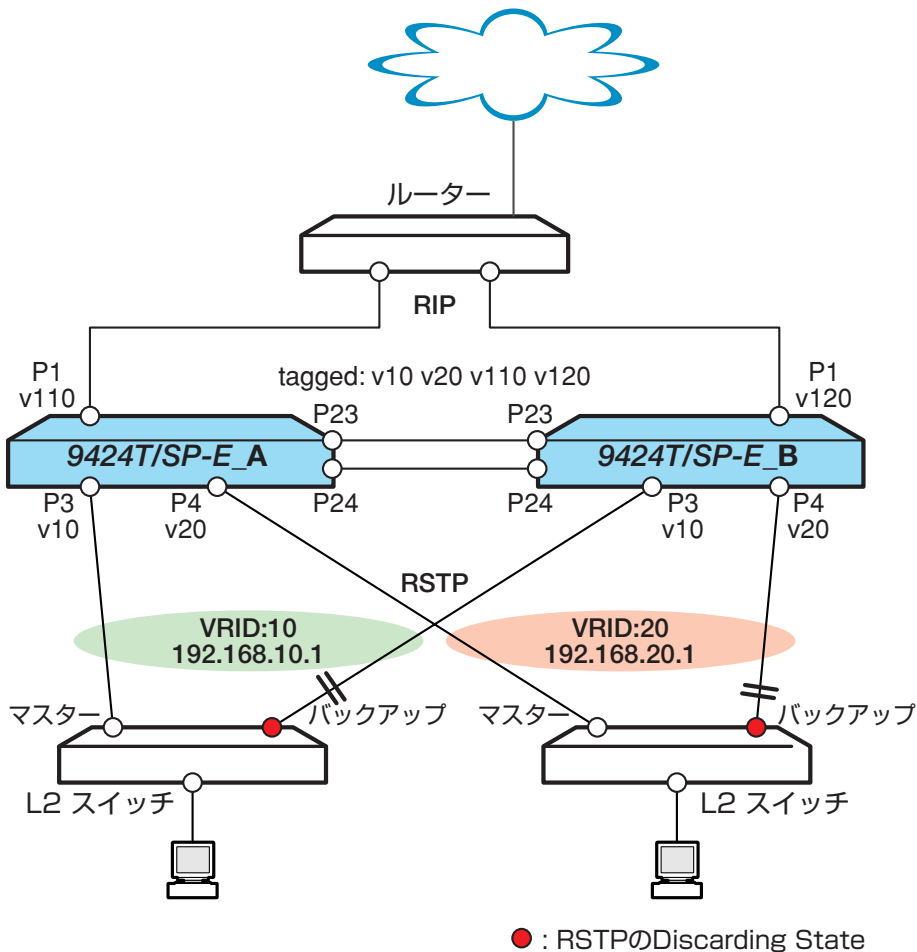
6.14 VRRP

 参照 「コマンドリファレンス」 / 「VRRP」

本製品で VRRP を使用する場合は、RSTP と併用してください。また、バーチャルルーターは 9424T/SP-E と 9424Ts/XP-E のみで構成するようにしてください。以下に推奨構成と設定例を示します。

VRRP のマスタールーターとバックアップルーターの切り替えはマスタールーターの障害発生時のみ行われます。VLAN インターフェースまたはポートのリンクアップ・ダウンによる切り替えはサポート対象外となりますので、ご了承ください。

〔構成例〕



〔設定例〕

9424T/SP-E_A

```
create switch trunk=t1 port=23-24
create vlan=v10 vid=10 taggedports=23-24 untaggedports=3
create vlan=v20 vid=20 taggedports=23-24 untaggedports=4
create vlan=v110 vid=110 taggedports=23-24 untaggedports=1-2
create vlan=v120 vid=120 taggedports=23-24
enable rstp
set rstp priority=1
add ip interface=vlan10 ipaddress=192.168.10.101 mask=255.255.255.0
add ip interface=vlan20 ipaddress=192.168.20.101 mask=255.255.255.0
add ip interface=vlan110 ipaddress=192.168.110.101 mask=255.255.255.0
add ip interface=vlan120 ipaddress=192.168.120.101 mask=255.255.255.0
add ip rip interface=vlan110 send=rip2
add ip rip interface=vlan120 send=rip2
enable vrrp
create vrrp=10 over=vlan10 ipaddress=192.168.10.1 priority=200
create vrrp=20 over=vlan20 ipaddress=192.168.20.1 priority=200
```

9424T/SP-E_B

```
create switch trunk=t1 port=23-24
create vlan=v10 vid=10 taggedports=23-24 untaggedports=3
create vlan=v20 vid=20 taggedports=23-24 untaggedports=4
create vlan=v110 vid=110 taggedports=23-24
create vlan=v120 vid=120 taggedports=23-24 untaggedports=1-2
enable rstp
set rstp priority=2
add ip interface=vlan10 ipaddress=192.168.10.102 mask=255.255.255.0
add ip interface=vlan20 ipaddress=192.168.20.102 mask=255.255.255.0
add ip interface=vlan110 ipaddress=192.168.110.102 mask=255.255.255.0
add ip interface=vlan120 ipaddress=192.168.120.102 mask=255.255.255.0
add ip rip interface=vlan110 send=rip2
add ip rip interface=vlan120 send=rip2
enable vrrp
create vrrp=10 over=vlan10 ipaddress=192.168.10.1
create vrrp=20 over=vlan20 ipaddress=192.168.20.1
```

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。

```
SET SYSTEM DISTINGUISHEDNAME
MENU
SET SWITCH CONSOLEMODE
SET AUTHENTICATION METHOD=TACACS
ADD/DELETE TACACSS SERVER
ENABLE/DISABLE/SHOW HTTP SERVER
SET SWITCH PORT
[BACKPRESSURE={YES|NO|ON|OFF|TRUE|FALSE|ENABLED|DISABLED}]
[BPLIMIT={1..7935}] [FCTRLLIMIT={1..7935}] [SPEED={1000MFULL}]
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]
CREATE/ADD/DELETE/SET/SHOW/PURGE PKI
SET/SHOW SSL

SHOW TCP
SET BOOTP RELAY MAXHOPS

CREATE/SET VRRP=vr-identifier [PORTMONITORING={ON;OFF}] [STEPVALUE]
ADD/DELETE VRRP MONITOREDINTERFACE

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 2.3 (613-000699 Rev.B)」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.B」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/>