



最初にお読みください



CentreCOM® 8424XL/8424TXリリースノート

この度は、CentreCOM 8424XL/8424TX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 ソフトウェアバージョン 2.6.1 pl01(2.6.1-01)

2 本バージョンで追加された機能


ソフトウェアバージョン2.6.1から2.6.1 pl01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 syslog ファシリティー設定機能

 **「コマンドリファレンス」 / 「運用・管理」 / 「ログ」**


CREATE LOG OUTPUT/SET LOG OUTPUT コマンドに FACILITY パラメーターが追加され、ログの出力先が syslog サーバーの場合に、任意のログファシリティー値を指定できるようになりました。

2.2 SNMP v2c 対応

 **「コマンドリファレンス」 / 「運用・管理」 / 「SNMP」**


ネットワーク管理プロトコル SNMP (Simple Network Management Protocol) のバージョン 2c (SNMPv2c) に対応しました。

2.3 ポートステータス一覧表示機能追加

 **「コマンドリファレンス」 / 「スイッチング」 / 「ポート」**

- SHOW SWITCH PORT コマンドに SUMMARY パラメーターが追加され、ポートステータスが一覧形式で表示されるようになりました。
- SHOW SWITCH PORT コマンドに SECURITY パラメーターが追加され、ポートセキュリティの設定および現在の状態が一覧形式で表示されるようになりました。
- SHOW SWITCH PORT COUNTER コマンドに DETAIL/SUMMARY パラメーターが追加されました。DETAIL 指定時は、これまでと同じ詳細なカウンター情報が表示されますが、SUMMARY を指定した場合は、ポートごとのカウンター情報が一覧形式で表示されるようになりました。

2.4 RRP Snooping


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

ESRP/VRPP および同等機能を持つ製品の下位に本製品を配置し、高速な冗長性を実現するためのRRP Snooping 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


ソフトウェアバージョン 2.6.1 から 2.6.1 pl01 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。

3.1 ポートセキュリティーについて

 **参照**「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 LEARN パラメーターに 0(ゼロ)を指定した場合、バージョン 2.6.1 までは、ポートセキュリティーが解除されていましたが、バージョン 2.6.1 pl01 では、ポートセキュリティーは有効のまま、解除されなくなりました。LEARN パラメーターに 0 を指定すると、MAC アドレスの学習機能を停止(ポートロック)します。
ポートセキュリティーを解除する場合は、LEARN パラメーターに NONE を指定してください。
- SET SWITCH PORT コマンドの INTRUSIONACTION パラメーターに TRAPCONTINUE/LOGCONTINUE が指定できるようになりました。TRAP/LOG を指定した場合は、未学習の送信元 MAC アドレスを持つ不正フレームを受信すると、SNMP トラップの送信 / ログの記録を行いますが、その後と同じ未学習の送信元 MAC アドレスを持つ不正フレームを受信してもトラップの送信 / ログの記録を行いません。TRAPCONTINUE/LOGCONTINUE を指定すると、トラップ送信済み / ログ記録済みの不正フレームを受信しても、再度、トラップの送信 / ログの記録を行います。

3.2 スタティックエントリー自動登録機能について

 **参照**「コマンドリファレンス」 / 「フォーディングデータベース」

- スタティックエントリー自動登録機能で指定できるマッチ条件が、1 ポートあたり 8 件から 32 件に拡張されました。

4 本バージョンで修正された項目

ソフトウェアバージョン 2.6.1 から 2.6.1 pl01 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 ポートセキュリティーの Limited モード (SET SWITCH PORT コマンドで RELEARN パラメーターを OFF) とスタティックエントリーの自動登録機能を併用している場合に、設定を保存して再起動すると、該当ポートのポートセキュリティーが正しく動作しないことがありましたが、これを修正しました。

- 4.2 SET LOG OUTPUT コマンドで、出力先に PERMANENT を指定して、保存するメッセージの最大数を変更し、設定を保存して再起動すると、再起動前のログ情報が消えてしまうことがありましたが、これを修正しました。
- 4.3 ハードウェア IP フィルターで、IPOINT オプションを指定しない場合、10/100M ポートで最大 252 個まで (IGMP Snooping および MLD Snooping 無効時は 254 個) フィルターエントリを作成できるはずが、125 個以上作成できないことがありましたが、これを修正しました。
- 4.4 Protected Ports VLAN から、DELETE VLAN PORT コマンドでクライアントポートを削除すると、削除したポート以外のポートとアップリンクポート間の通信ができないことがありましたが、これを修正しました。
- 4.5 SET SWITCH PORT コマンドの INGRESSLIMIT パラメーターで、受信レート上限値を設定したポートに、ADD SWITCH L3FILTER ENTRY コマンドで入力ポート (IPOINT) のみを指定したハードウェア IP フィルターを設定すると、受信レートの制限が有効にならないことがありましたが、これを修正しました。
- 4.6 スパニングツリープロトコルで、最大エージタイムのタイマー稼働中に、Configuration BPDU (Hello パケット) を受信した際のタイマー更新処理に誤りがあり、正しく動作しないことがありましたが、これを修正しました。
- 4.7 スパニングツリープロトコルで、RAPID モードのときに、本製品がルートブリッジになっても、New Root トラップが発行されないことがありましたが、これを修正しました。
- 4.8 ポートセキュリティの Dynamic Limited モード設定時 (SET SWITCH PORT コマンドで RELEARN パラメーターを ON)、学習可能な送信元 MAC アドレスの最大数に達して学習機能を停止した状態 (ポートロック状態) で、SET SWITCH PORT コマンドの INTRUSIONACTION パラメーターを TRAP から LOG、または LOG から TRAP に変更すると、学習済みの通信可能な MAC アドレスが、不正 MAC アドレスとして扱われることがありましたが、これを修正しました。
- 4.9 ポートセキュリティ機能有効時、SET SWITCH PORT コマンドの INTRUSIONACTION パラメーターに DISABLE を設定しても、学習可能な送信元 MAC アドレスの最大数を超えて、未学習の送信元 MAC アドレスを持つフレームを受信した場合に、SNMP トラップを送信しないことがありましたが、これを修正しました。

5 本バージョンでの制限事項

ソフトウェアバージョン 2.6.1 pl01 には、以下の制限事項があります。

5.1 ログについて

「コマンドリファレンス」 / 「運用・管理」 / 「ログ」

ADD LOG OUTPUT/SET LOG OUTPUT コマンドで、MODULE=SWITCH と指定すると、設定が正しく反映されないため syslog サーバーへの出力ができません。スイッチングモジュールを指定する場合は、モジュール名ではなく、MODULE=87 とモジュール ID を指定してください。

5.2 トリガーについて

「コマンドリファレンス」 / 「運用・管理」 / 「トリガー」

- CREATE TRIGGER REBOOT コマンドに RESTART または ALL を指定した場合、RESTART REBOOT コマンド実行による再起動と、RESTART SWITCH コマンド実行による再起動で、syslog サーバーに転送される情報が異なります。
- CREATE TRIGGER コマンドの REPEAT パラメーターに回数を指定した後、設定を保存すると、設定ファイル上の REPEAT パラメーターの値が入力時とは異なる場合があります。
また、CREATE TRIGGER コマンドの REPEAT パラメーターに回数を指定し、トリガーが指定回数実行された後で設定を保存し、SET CONFIG コマンドで起動時設定ファイルとして再起動すると、REPEAT の設定値が不正な値と判断され、トリガーの設定が反映されません。

5.3 SNMP について

「コマンドリファレンス」 / 「運用・管理」 / 「SNMP」

イーサネット MIB の dot3StatsCarrierSenseErrors の値が取得できません。

5.4 ポートセキュリティーについて

「コマンドリファレンス」 / 「スイッチング」 / 「ポート」

パケット受信中のポートに対して、SET SWITCH PORT コマンドで RELEARN パラメーターを OFF から ON (Dynamic Limited モード有効) に変更すると、FDB に送信元 MAC アドレスが登録されず、すべてのパケットが破棄されます。
運用中に、RELEARN パラメーターを変更しないでください。

5.5 ポートミラーリングについて

「コマンドリファレンス」 / 「スイッチング」 / 「ポート」

システム再起動後にソースポートをタグ付きに設定した場合、同ポートでタグなしパケットを受信すると、タグ付きでミラーポートから出力されます。

5.6 802.1X 認証について

参照「コマンドリファレンス」 / 「スイッチング」 / 「802.1X 認証」

- 802.1X 認証機能が無効のまま、SET PORTAUTH PORT SUPPLICANTMAC コマンドで CONTROL パラメーターの設定を変更しても、現在の設定に反映されません。
- Windows 2000 Server (IAS) を RADIUS サーバーとして使用している場合、本製品の Supplicant ポートは認証されません。
- システム起動直後、ケーブルを接続していない Authenticator ポートに対して SHOW PORTAUTH PORT コマンドを実行すると、Authenticator PAE State が INITIALISE であるにもかかわらず、Port Status が authorised と表示されます。
- Authenticator ポートから IGMP Query メッセージが送信されません。その場合には、IGMP Snooping を無効に設定してください。
- RESET PORTAUTH PORT MULTIMIB コマンドを使用しても未認証の supplicant 情報はリセットされません。
- SNMP マネージャーで、dot1xAuthAuthControlledPortControl の情報を変更 (Set) した後、設定を保存すると、設定の変更が設定ファイルに反映されません。Authenticator ポートの状態を手動で変更する場合は、SET PORTAUTH PORT コマンドの CONTROL パラメーターで指定してください。
- クライアントが RADIUS サーバーに送る Access-request (認証要求) に含まれる NAS-Port のアトリビュートの値は、「物理ポートの番号-1」になります。

5.7 RRP Snooping について

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

RRP Snooping 有効時、マスターポートになっているポートで 802.1X 認証機能を有効にすると、マスターポートのステータスが残ってしまいます。ただし、動作上の問題はなく、SHOW RRPSNOOPING コマンドでは表示されません。802.1X 認証機能を無効にしたとき、有効前のマスターポートのステータスが表示される場合があります。


5.8 スパニングツリープロトコルについて

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 モード (SET STP コマンドの MODE パラメーターで設定) のときに、SET STP コマンドを DEFAULT オプション付きで実行すると、DISABLE STP PORT コマンドで STP を無効にしていたポートで通信ができなくなります。DISABLE STP PORT コマンドで STP を無効にしたポートがある場合は、SET STP コマンドの DEFAULT オプションを使用しないでください。


- RAPID モード (SET STP コマンドの MODE パラメーターで設定) で新規作成した STP ドメインの所属 VLAN にタグ付きポートを割り当てると、DISABLE STP PORT コマンドの設定が削除されます。STP ドメインの所属 VLAN にタグ付きポートを割り当てるときは、DISABLE STP PORT コマンドで STP を無効にしたポートがないかどうかを確認してください。
- RAPID モード (SET STP コマンドの MODE パラメーターで設定) のときに、DISABLE STP PORT コマンドで STP を無効にしていたポートに、SET STP コマンドで RSTPTYPE パラメーターを変更しても、現在の設定に反映されません。
- RAPID モードで STP ドメインを複数作成した場合には、CREATE CONFIG コマンドで設定を保存するのではなく、SHOW CONFIG コマンドで DYNAMIC オプションを指定して現在の設定内容を表示し、その内容を EDIT コマンドで設定ファイルに貼り付けてください。CREATE CONFIG コマンドで設定を保存すると、正しく動作しないことがあります。
- STANDARD モードと RAPID モードの両方の STP ドメインに属するポートにおいて、SET STP PORT コマンドで PATHCOST パラメーターを変更すると、エラーメッセージが表示されます。ただし、動作上の問題はなく、現在の設定にも正しく反映されます。エラーメッセージを表示させないようにするには、SET STP PORT コマンドで、STP ドメインとポートの両方を指定してください。
- STANDARD モード (SET STP コマンドの MODE パラメーターで設定) のときに、ENABLE STP コマンドを実行すると、DISABLE STP PORT コマンドの設定が削除されます。

5.9 スタティックエントリーについて

 **「コマンドリファレンス」 / 「フォワーディングデータベース」**

本製品宛通信時、スタティックエントリーを登録したポート以外でも通信が可能になります。

5.10 ハードウェア IP フィルターについて

 **「コマンドリファレンス」 / 「ハードウェア IP フィルター」**

PROTOCOL=IGMP を指定しても、IGMP メッセージがフィルタリングされません。

5.11 経路制御について

 **「コマンドリファレンス」 / 「IP」 / 「経路制御(スタティック)」**

ADD IP ROUTE コマンドの NEXTHOP パラメーターに自インターフェースアドレスを指定すると、IP ルーティングテーブルに登録されてしまいます。その場合、登録したネットワーク宛での通信ができませんので指定しないでください。

5.12 IGMP について

「コマンドリファレンス」 / 「IP マルチキャスト」 / 「IGMP」

- Last Query Interval Timer (retransmit timer) が起動中に Leave Group メッセージを受信すると、Last Query Interval Timer が更新されます。
- Last Query Interval Timer (retransmit timer) が起動中に Membership Report メッセージを受信しても、Refresh Timer は更新されますが、Last Query Interval Timer が停止しないため、Group Specific Query を送信します。
- NONQUERIER が Leave Group メッセージを受信すると RT (Refresh Timer) を更新しません。

5.13 IGMP Snooping について

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

1つのポートに同一グループの複数メンバーが登録されている場合、そのうち1つのホストからの Leave Group メッセージを受信すると、他のホストがいるにもかかわらずグループから削除されます。

5.14 DHCP サーバー機能について

「コマンドリファレンス」 / 「DHCP サーバー」

- DHCP クライアントが DHCP Discover を送信した際に、DHCP サーバーが割り当てようとしている IP アドレスを、ICMP には応答せず ARP のみに応答する別のホストがすでに使用していると、DHCP Discover を送信した DHCP クライアントが、DHCP Offer を受信することができません (IP アドレスを取得することができません)。
- DHCP サーバー機能使用時、DELETE IP INTERFACE コマンドを実行すると、同コマンドを実行したのとは別の VLAN において、DHCP クライアントが IP アドレスを取得できなくなる場合があります。このようなときは、RESET IP コマンドを実行してください。
- DHCP サーバー機能使用時、リレーエージェント経由で受信したリース延長要求に対し、DHCPNAK メッセージを返送するため、DHCP クライアントと DHCP サーバーが別セグメントに所属し、クライアントからの延長要求を受信した際に、DHCP サーバーは正しく応答できません。
- SHOW DHCP CLIENT コマンドで表示される DHCP レンジ内の IP アドレスのテーブルには Client ID が表示されていなくても、内部で保持している DHCP テーブルにクライアントの割り当てが残っている場合、ADD DHCP RANGE コマンドで、IP アドレスを特定の MAC アドレスに関連付け (静的割り当て) ようとするとエラーメッセージが表示され、静的割り当てが行えないことがあります。このようなときは、DESTROY DHCP RANGE コマンドを実行してください。


5.15 ファームウェアインストーラーによるソフトウェアのバージョンアップについて

本製品のソフトウェアをバージョンアップする場合には、必ず、本製品からログアウトしてください。本製品にログインしたままで、セットアップツールを使用して本製品のソフトウェアをバージョンアップしようとしても、エラーメッセージが表示されて、バージョンアップを実行することができません。

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CD-ROMに収録されている「CentreCOM 8424XL/8424TX コマンドリファレンス 2.6 (Rev.C)」の補足事項です。


6.1 ポート帯域制限(送信レート)の設定について

 **「コマンドリファレンス」 / 「スイッチング」 / 「ポート」**

 **「取扱説明書」 45 ページ**


バージョン 2.6.1 で、SET SWITCH PORT コマンドの EGRESSLIMIT パラメーターで、ポート帯域制限の送信レートの設定を変更した場合、設定を有効にするために本製品を再起動する必要がなくなりました。

6.2 ポートミラーリングについて

 **「コマンドリファレンス」 / 「スイッチング」 / 「ポート」**

タグ付きの packets がタグなしのソースポートから入力されると、ミラーポートからはタグなしの状態ですべて出力されます。

6.3 DHCP サーバー機能について

 **「コマンドリファレンス」 / 「DHCP サーバー」**

DHCP クライアントからのオプション 57 (Maximum DHCP Message Size) メッセージを受けられません。

6.4 フラッディングレートについて

10/100Mbps ポートが 24 ポートリンクした状態で、拡張モジュールの 1000Mbps ポート (ポート 25) からフラッディングパケットを送信すると、1000Mbps ポート (ポート 26) から送信されるパケットの転送率が下がる場合があります。

7 未サポートコマンド(機能)

以下のコマンド(機能)はサポート対象外ですので、あらかじめご了承ください。
太字はコマンド名、細字は該当コマンドのパラメーター名です。

SHOW EXCEPTION
SHOW DEBUG [STACK]
SHOW BUFFER [SCAN] [QUEUEPOINTERS]


```
SHOW FLASH FFS
CLEAR FLASH TOTALLY
DELETE NVS BLOCK [INDEX]
CLEAR NVS TOTALLY
SHOW FFILE VERIFY
SHOW FFILE [DEBUG]
PURGE FILE TRANSLATIONTABLE
CLEAR CFLASH
SHOW CFLASH COUNTERS
SHOW CFLASH TEST
SHOW CFLASH REGISTER
SHOW CFLASH SECTOR
SHOW CFLASH FAT
SHOW CFLASH IDENTITY
ENABLE CFLASH DEBUG
DISABLE CFLASH DEBUG
ENABLE CFLASH TEST END [START]
DISABLE CFLASH TEST
ENABLE RADIUS DEBUG
DISABLE RADIUS DEBUG
SHOW RADIUS DEBUG
ENABLE MAIL DEBUG
DISABLE MAIL DEBUG
RESET MAIL
SET MAIL SMTPSERVER=ipaddr

ENABLE SWITCH DEBUG
DISABLE SWITCH DEBUG
SHOW SWITCH DEBUG
ENABLE SWITCH BIST
SHOW SWITCH BIST
SHOW SWITCH MEMORY
SET SWITCH SOCK
SHOW SWITCH SOCK
SET SWITCH PHY
SHOW SWITCH PHY
SHOW SWITCH SWTABLE
SET SWITCH PORT [MODE={MASTER;SLAVE}]
SET SWITCH PORT [SPEED=
{1000MFULL;1000MHALF;1000MFAUTO;1000MHAUTO}]
ACTIVATE SWITCH PORT AUTONEGOTIATE
ENABLE PORTAUTH DEBUG PORT
DISABLE PORTAUTH DEBUG PORT
```

ENABLE VLAN DEBUG
DISABLE VLAN DEBUG
SHOW VLAN DEBUG

ENABLE STP DEBUG [PORT]
DISABLE STP DEBUG [PORT]
SHOW STP DEBUG
SHOW STP PORT RSTPSTATE

ENABLE SWITCH L3FILTER SWFILTBYPASS
DISABLE SWITCH L3FILTER SWFILTBYPASS

SHOW IP CACHE
SHOW IP CASSI
ENABLE IP DEBUG
DISABLE IP DEBUG
SHOW IP DEBUG
SHOW PING DEBUG
PURGE PING TOTALLY
SHOW TRACE DEBUG
SET IP FLOW
SHOW IP FLOW
ENABLE TCP DEBUG
DISABLE TCP DEBUG
ENABLE IP ICMPREPLYMSG
DISABLE IP ICMPREPLYMSG
SHOW IP ICMPREPLYMSG
ADD IP INTERFACE IPADDRESS [FRAGMENT]
SET IP INTERFACE IPADDRESS [FRAGMENT]
ENABLE IP ROUTE DEBUG
DISABLE IP ROUTE DEBUG
SHOW IP ROUTE DUMP
ENABLE PING POLL DEBUG
DISABLE PING POLL DEBUG

ENABLE IP IGMP DEBUG
DISABLE IP IGMP DEBUG
SHOW IP IGMP DEBUG

ENABLE MLDSNOOPING DEBUG
DISABLE MLDSNOOPING DEBUG

ENABLE DHCP [BOOTP] [DEBUG]
DISABLE DHCP [BOOTP] [DEBUG]

ENABLE TEST INTERFACE
DISABLE TEST INTERFACE
SHOW TEST [INTERFACE]
RESET TEST INTERFACE
SHOW PKT
SET PKT
START PKT
STOP PKT
MODIFY
DUMP

