



J613-M0005-12 Rev.K 100302



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す。このリリースノートは、取扱説明書（J613-M0005-10 Rev.B）とコマンドリファレンス（J613-M0005-13 Rev.K）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 2.7.9-01

## 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 2.7.7-01 から 2.7.9-01 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 省電力モード

 **参照** 「コマンドリファレンス」 / 「スイッチング」

リンクしていないスイッチポートへの電力供給を制限し、消費電力を抑える省電力モードに対応しました。

省電力モードを有効にするには、ENABLE SWITCH POWERSAVE コマンドを使います（本機能の設定は、スイッチポート別ではなく、装置全体に対して機能します）。

### 2.2 ループガード（LDF 検出）

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

ループガード機能として LDF 検出機能をサポートしました。本機能は、一定時間毎に特殊な試験フレーム（LDF）を送出し、接続機器を介して同じ LDF が同じ筐体に戻って来た場合に、関連するポートを無効化したり、ログに記録したりする機能です。

詳細は、コマンドリファレンス「スイッチング / 概要」の「ループガード」をご覧ください。

### 2.3 検疫ソリューション対応

マイクロソフト社「Windows Server 2008」標準の NAP（ネットワークアクセス保護）に対応しました。

### 2.4 ポート認証：認証ポート間の Supplicant 移動

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

ポート認証使用時、認証ポートに 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（認証ポートをリンクダウンさせずに）移動できるようになりました。あるポートで認証をパスした Supplicant が別の認証ポートに移動すると、移動前のポートから該当 Supplicant の認証情報が削除され、移動先のポートで新たに認証を受けることになります。

---

## 2.5 MLDv2 Snooping

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

VLAN 環境において不要な IPv6 マルチキャストトラフィックをフィルタリングする MLD Snooping のバージョン 2 (MLDv2 Snooping) に対応しました。

詳細は、コマンドリファレンス「MLD Snooping」をご覧ください。

---

## 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 **2.7.7-01** から **2.7.9-01** 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 フラッシュメモリー上のファイルシステムに存在するファイルの名前を変更すると、複数のファイルが消失することがありましたが、これを修正しました。
- 3.2 バージョン 2.6.2 以前のファームウェアから、バージョン 2.7.3-06 以降のファームウェアにバージョンアップをすると、バージョン 2.6.2 以前に作成した長い名前 (28.3 形式) のファイルが、バージョンアップ後に短い名前 (8.3 形式) で表示されるようになっていましたが、バージョン 2.7.9-01 へのバージョンアップ後には、長い名前が表示されるよう修正しました。
- 3.3 SET CONFIG コマンドの実行に失敗したとき、表示されるエラーメッセージが文字化けすることがありましたが、これを修正しました。
- 3.4 SHOW SYSTEM コマンドおよび SHOW LOG コマンドの実行結果に、「No patches found」の警告メッセージが表示されないよう修正しました。
- 3.5 パケットの受信時にポートでリンクダウンが発生すると、受信したパケットの格納領域を初期化する処理が行われますが、ごくまれに初期化が一定時間内に完了せず、本製品がリポートする場合がありますでしたが、これを修正しました。
- 3.6 DISABLE SWITCH PORT (LINK=ENABLE) コマンドで無効に設定されているポートにおいて、MLD/IGMP の制御パケットを受信すると、本製品がリポートすることがありましたが、これを修正しました。
- 3.7 SET SWITCH PORT コマンドの LEARN パラメーターの指定によるポートセキュリティ設定時、RESET SWITCH FDB コマンドを実行しても、設定ファイルと FDB からポートセキュリティ (learn) のエントリーが削除されませんでしたでしたが、これを修正しました。
- 3.8 ポートセキュリティ有効時、いったん INTRUSIONACTION の対象となった MAC アドレスを、ADD SWITCH FILTER コマンドでポートセキュリティの learn エントリーとして FDB に登録しなおしても、SHOW SWITCH PORT INTRUSION コマンドやログメッセージで、INTRUSIONACTION の対象 MAC アドレスとして表示されていましたが、これを修正しました。
- 3.9 マルチプル VLAN において、すでにアップリンクポートが存在する VLAN に対して、ADD VLAN PORT コマンドで別のポートをアップリンクとして追加することができませんでしたでしたが、これを修正しました。

- 3.10 ユーザー定義の STP ドメインが無効の状態では、DELETE VLAN PORT、DELETE STP VLAN、PURGE STP コマンドを順に実行すると、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 本バージョンでの制限事項

---

ファームウェアバージョン 2.7.9-01 には、以下の制限事項があります。

---

### 4.1 ファイルシステム

 **参照** 「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使用時、コンパクトフラッシュの空き容量がない状態で新しく設定スクリプトをコンパクトフラッシュに作成しようとする、「Operation Successful」と表示されることがあります。なお、この状態でコンパクトフラッシュの内容を SHOW FILE コマンドまたは PC で確認すると、作成したファイルが存在するようには見えますが、ファイルには何も記録されません。

---

### 4.2 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」

- 複数の IP インターフェース (IP アドレス) を設定している場合、RADIUS Access-Request パケットの始点 IP アドレスと NAS-IP-Address の値が異なることがあります。両者を一致させたい場合は、RADIUS サーバーの指定時 (ADD RADIUS SERVER コマンドの実行時) に、LOCAL パラメーターでローカル IP インターフェースを指定してください。
  - RADIUS サーバーを複数登録している場合、最初に登録した RADIUS サーバーに対してのみ、SET RADIUS コマンドの RETRANSMITCOUNT パラメーターが正しく動作しません。最初の RADIUS サーバーへの再送回数のみ、RETRANSMITCOUNT の指定値よりも 1 回少なくなります。
- 

### 4.3 アップロード・ダウンロード

 **参照** 「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 によるアップロード時 (UPLOAD METHOD=TFTP)、IPv6 アドレスの指定ができません。
  - ZMODEM によるファイル受信 (LOAD METHOD=ZMODEM) にターミナルソフト側で送信をキャンセルすると、コマンドプロンプトに復帰しないことがあります。ターミナルソフトが Windows 付属のハイパーターミナルの場合、本現象は起こりません。
- 

### 4.4 ログ

 **参照** 「コマンドリファレンス」/「運用・管理」/「ログ」

DESTINATION=NVS のログ出力先定義に対し、SET LOG OUTPUT コマンドで MESSAGES パラメーター (保存件数) を変更すると、すでに NVS 上に保存されていたメッセージがすべて消去されます。

---

## 4.5 スクリプト

 **参照** 「コマンドリファレンス」 / 「運用・管理」 / 「スクリプト」

スクリプトで IF THEN ELSE 文を使用する際、比較対象文字列の長さが 32 文字以上の場合、スクリプトが正しく動作しません。31 文字以下の長さの比較対象文字列を使用してください。

---


## 4.6 SNMP

 **参照** 「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。
- イーサネット MIB の dot3StatsFrameTooLongs が正しくカウントアップされません。
- 既に作成されているユーザーグループに対して SET SNMP GROUP コマンドで SECURITYLEVEL を変更することはできません。
- SNMP マネージャーと通信しているトランクポートのケーブルを抜くと、リンクダウントラップが送出されない場合があります。

---

## 4.7 NTP

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

本製品の IP アドレスを変更しても、SHOW NTP コマンドの「Host Address」欄（NTP モジュールの使用している IP アドレス）が更新されません。これは表示だけの問題で動作には影響ありません。

---

## 4.8 非同期ポート

 **参照** 「コマンドリファレンス」 / 「運用・管理」 / 「非同期ポート」

- SET ASYN コマンドの PROMPT パラメーターでコマンドプロンプトの文字列を変更した後、「SHOW CONFIG DYNAMIC」を実行すると、プロンプト文字列がデフォルト設定に戻ります（SET ASYN コマンドの設定自体はダイナミックコンフィグ中に残っています）。
- 非同期ポート端末の画面あたりの行数をデフォルトの 21 またはそれ以上に設定した場合、SHOW IP ARP コマンドの結果が設定した値 +20 行分表示されます。

---


## 4.9 ターミナルサービス

 **参照** 「コマンドリファレンス」 / 「運用・管理」 / 「ターミナルサービス」

TELNET コマンドの実行時に DNS サーバーへの問い合わせが行われた場合、DNS サーバーからの応答に IPv6 アドレスが含まれていると、TELNET コマンドが反応しなくなります。

---

## 4.10 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」

- ポートトランキングと IGMP Snooping の併用時、マスターポートがリンクダウンすると SHOW IGMPSPNOOPING コマンドで表示される Entry timeout 値が更新されます。これは表示だけの問題であり、動作には影響ありません。  
（「マスターポート」はトランクグループ内で最初にリンクアップしたポートを示します）

- CREATE SWITCH TRUNK コマンドの PORT パラメーターでトランクポートを指定した場合、指定ポートがマルチプル VLAN (Protected Port VLAN) の同一グループ所属であるかのチェックが行われません。これを回避するため、マルチプル VLAN とポート トランキングを併用するときは、先にトランクグループを作成してから、トランクグループをマルチプル VLAN に割り当ててください。
- 通常、トランクグループに属するポートは、同一 VLAN の所属で、同一のタグ設定 (タグ付き・タグなし) にする必要がありますが、ポートをトランクグループに登録後、SET VLAN PORT コマンドによりポートごとのタグ付きまたはタグなしの変更を行うと、「Operation Successful」と表示され、変更が適用されます。VLAN のタグ付き・タグなしを変更する場合は、トランクグループに所属するすべてのポートについて同じ設定を行ってください。
- マルチプル VLAN (Protected Port VLAN) のアップリンクポートに設定したポートとクライアントポートに設定したポートを、同じトランクグループに所属させることができてしまいます。アップリンクポートとクライアントポートは同一のトランクグループに所属させないでください。
- 同じポートにポートトランキングとポートセキュリティを併用した場合、ポートセキュリティにより登録した MAC アドレスがトランクグループに移動しません。
- ポートトランキングとスパニングツリープロトコルを併用した場合、古い番号のポートがマスターポートになる場合があります。

---

#### 4.11 LACP (IEEE 802.3ad)

 **参照** 「コマンドリファレンス」 / 「スイッチング」 / 「LACP (IEEE 802.3ad)」

- LACP によって自動生成されたトランクグループのメンバーポートに対して CREATE SWITCH TRUNK コマンドを実行すると、通信ができなくなります。
- トランクグループ内のポートがリンクダウンすると、トランクグループ内の他のポートもリンクダウンするため通信が一時的に途絶えることがあります。
- LACP とポートセキュリティを併用すると、LACP によるトランクポートの生成は行われません。

---

#### 4.12 バーチャル LAN

 **参照** 「コマンドリファレンス」 / 「バーチャル LAN」

通信中のポートを新しい VLAN に割り当てると、新旧の VID で登録された MAC アドレスが FDB に共存してしまい、VLAN を越えてユニキャストメッセージが通信されてしまう場合があります。この現象を回避するには、RESET SWITCH FDB コマンド、リンクダウン、エージングタイマーの発動によって FDB の MAC アドレスを削除するか、ポートが通信を行っていない状態で VLAN の割り当てを行ってください。

---

#### 4.13 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」 / 「スパニングツリープロトコル」

ポートトランキング (または LACP) とスパニングツリープロトコル (STP/RSTP) を併用する場合、トランクグループのマスターポートがリンクダウンすると、トランクグループ内の他のポートが正常にリンクしているにもかかわらず Topology Change が発生します。

---

#### 4.14 マルチブル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」 / 「スパニングツリープロトコル」 / 「Multiple STP」

- マルチブルスパニングツリープロトコル (MSTP) を有効にすると、ミラーポートから  
も BPDU を送信します。
- SET MSTP コマンドの PROTOCOLVERSION パラメーターに RSTP を指定するとループ  
が発生します。本製品の配下に RSTP 動作中のスイッチが存在している場合でも、  
PROTOCOLVERSION には RSTP を指定せず、デフォルト値の MSTP でご使用くださ  
い。
- マルチブルスパニングツリープロトコル (MSTP) を有効にすると、ランタイムコンフィ  
グから DELETE VLAN コマンドの設定が削除されます。これを回避するには、再起動ト  
リガーを使用して起動直後に同コマンドを実行させてください。

---

#### 4.15 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」

エラーパケットを受信したときも、送信元 MAC アドレスをフォワーディングデータベース  
(FDB) に登録します。

---

#### 4.16 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」

- フレームタイプ 802.3 raw の IPX パケットにマッチさせるため、DSAP / SSAP =  
0xFFFF の条件を持つフィルターエントリーを作成した場合、このエントリーはフレ  
ムタイプ Ethernet 2 の IPX パケットにもマッチしてしまいます。
- フレームフォーマットとして 802.2 LLC を指定したハードウェア IP フィルターに対し、  
ADD SWITCH L3FILTER ENTRY コマンドで TYPE=0000 のエントリーを作成しよう  
とするとエラーになります。また、このとき表示されるエラーメッセージが適切であり  
ません。

---

#### 4.17 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 Multi-Supplicant モードの Authenticator ポートでは、Port Status が  
authorised でも IGMP Query パケットがフラッディングされません。
- ENABLE/SET PORTAUTH PORT コマンドの SERVETIMEOUT パラメーターが  
正しく動作しません。これは、SET RADIUS コマンドの TIMEOUT パラメーターと  
RETRANSMITCOUNT パラメーターの設定が優先されているためです。SET RADIUS  
コマンドで TIMEOUT × (RETRANSMITCOUNT + 1) の値を SERVETIMEOUT より  
大きく設定した場合は、SERVETIMEOUT の設定が正しく機能します。
- ポートの 802.1X 認証機能をいったん無効にしてから再度有効にすると、Authenticator  
は Supplicant の MAC アドレスをゲスト VLAN 上で学習しません。
- 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。

- ゲスト VLAN 使用時、認証成功時に出力される SNMP トラップおよびログの AuthPreAuthVLAN (未認証時の所属 VLAN) に、ゲスト VLAN の VID ではなく、本来の所属 VLAN の VID がセットされます。
- 802.1X Multi-Supplicant モードの Authenticator ポート、または MAC ベース認証ポートに対して、SET PORTAUTH PORT コマンドで CONTROL パラメーターを AUTO (デフォルト) 以外に設定すると、ポート認証に関する SNMP トラップの出力が有効に設定されていても、該当ポートで SNMP トラップ / ログメッセージが出力されません。

---

## 4.18 IP

 **参照** 「コマンドリファレンス」 / 「IP」

本バージョンでは、PURGE PING TOTALLY コマンドは未対応となっております。

---

## 4.19 IP インターフェース

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

- DHCP クライアント機能を有効から無効に変更しても (IP アドレスを固定設定しても)、該当インターフェースから DHCP サーバー宛での要求パケットが送信され続けることがあります。
- ADD/SET IP INTERFACE コマンドで他の VLAN と重複するネットワークアドレス (IP アドレス / ネットマスク) を指定しても、エラーになりません。重複したアドレスを設定しないよう注意してください。

---

## 4.20 ARP

 **参照** 「コマンドリファレンス」 / 「IP」 / 「ARP」

スタティック ARP エントリが登録されている IP インターフェースが、いったんダウンし、再度アップすると、FDB にスタティック登録されていた該当 MAC アドレスが削除されます。

---

## 4.21 ICMPv6

 **参照** 「コマンドリファレンス」 / 「IPv6」 / 「IPv6 インターフェース」

ICMPv6 Packet Too Big メッセージを受信した際、そのメッセージによって通知された MTU の値がメモリー上の設定に動的に反映されます。

---

## 4.22 IGMP

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

- Last Member Query Interval タイマーの起動中に Report メッセージを受信しても、同タイマーが更新されず、Group-specific Membership Query を再送信してしまいます。
- IGMP 設定時、StartUp Query Count は本来 Robustness Variable と同じ値になるはずですが、Robustness Variable-1 となっています。

---

## 4.23 IGMP Snooping

 **参照** 「コマンドリファレンス」 / 「IP」

IGMP Snooping 使用時、複数のメンバーが存在するマルチキャストグループから 1 つのメンバーが脱退すると、SHOW IGMP Snooping コマンドで表示される Entry timeout が更新されます。

## 5 取扱説明書・コマンドリファレンスの補足・誤記訂正

---

取扱説明書、および「CentreCOM 8424XL/8424TX コマンドリファレンス 2.7 (Rev.K)」の補足事項と誤記訂正です。

### 5.1 スタンドキット「AT-STND-J01」（CentreCOM 8424TX のみ対象）

 **参照** 「取扱説明書」17 ページ

取扱説明書に記載がありませんが、CentreCOM 8424TXはスタンドキット「AT-STND-J01」に対応しています。

### 5.2 ポート帯域制限（送信レート）

 **参照** 「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。

### 5.3 スイッチング

 **参照** 「コマンドリファレンス」/「スイッチング」

- 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。
- 予約済マルチキャストパケットの処理で、送信元アドレスが、01-80-C2-00-00-00 ~ 01-80-C2-00-00-10 および 01-80-C2-00-00-20 ~ 01-80-C2-00-00-2F のパケットはフィルタリングされます。それ以外のパケットは、フラディングされます。

### 5.4 ループガード（LDF 検出）

 **参照** 「コマンドリファレンス」/「スイッチング」/「ポート」

複数のポート間でブロードキャストパケットによるループが発生すると、ループ発生から検出までに時間がかかる場合があります。

SET SWITCH LOOPDETECTION コマンドの INTERVAL パラメーターで、LDF の送信間隔を最小値（= 1 秒）に近い値に設定することを推奨します。

### 5.5 ICMP

 **参照** 「コマンドリファレンス」/「IP」

VLAN A、B を作成し、それぞれの VLAN に別ネットワークのアドレスを指定（VLAN A に 192.168.1.10、VLAN B に 192.168.1.20 指定、VLAN 内にルーターが存在）した場合に、VLAN A に所属する端末 C から VLAN B 宛に ICMP Request を送信すると、VLAN A と B は異なるネットワークに所属するにも関わらず、ルーターを介さずに、VLAN A から ICMP Reply が送信されます。またこの場合に、VLAN B から A への通信にハードウェアパケットフィルタを設定していても、この ICMP Reply はフィルタの条件にマッチしません。

これは、ICMP Reply を送信する際に、送信先アドレスを IP アドレスのみで検索し、そのアドレスの所属するインターフェースを送信元としているためです。



## 6 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。

```
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
ADD USER [MTU] [NETMASK] [CBNUMBER] [IPXNETWORK] [APPLENETWORK]
[APPLEZONE] [CALLINGNUMBE]
SET USER [MASK] [MTU] [NETMASK] [CBNUMBER] [IPXNETWORK]
[APPLENETWORK] [APPLEZONE] [CALLINGNUMBE] [TACRETRIES] [TACTIMEOUT]
ENABLE MAIL DEBUG
DISABLE MAIL DEBUG
RESET MAIL
SET MAIL SMTPSERVER=ipaddr
CREATE LOG OUTPUT [LOCAL]
SET ASYN [ENABLE] [TIMEOUT] [IDLETIMEOUT] [SHELLSERVER]
[TENTIMERVALU]
SET TTY IDLETIMEOUT

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}] [IGMPACTION={DENY;REPLACE}]
[IGMPFILTER={NONE;filter-id}] [IGMPMAXGROUP={NONE;1..65535}]
[VLANSTATUSTRAP={ON;OFF}] [THRASHLIMIT={5..65536;NONE}]
[THRASHREFILL=4..65536]
SET SWITCH PORT SPEED={1000MHALF;1000MFAUTO;1000MHAUTO}
ACTIVATE SWITCH PORT AUTONEGOTIATE
ENABLE PORTAUTH DEBUG={ALL;PACKET;STATE} PORT={port-list;ALL}
DISABLE PORTAUTH DEBUG={ALL;PACKET;STATE} PORT={port-list;ALL}
ENABLE RADIUS DEBUG
DISABLE RADIUS DEBUG
SHOW RADIUS DEBUG
```

ENABLE DHCP Snooping DEBUG  
DISABLE DHCP Snooping DEBUG  
RESET DHCP Snooping Counter  
SHOW DHCP Snooping Filter All

ENABLE VLAN DEBUG  
DISABLE VLAN DEBUG  
SHOW VLAN DEBUG

ENABLE STP DEBUG [PORT]  
DISABLE STP DEBUG [PORT]  
SHOW STP DEBUG  
SHOW STP[={stp-name | ALL}] PORT={port-list;ALL} RSTPSTATE

DISABLE MSTP PORT  
ENABLE MSTP PORT

ENABLE SWITCH L3 Filter SW Filter Bypass  
DISABLE SWITCH L3 Filter SW Filter Bypass

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] [ARPCHECKTIMEOUT]  
SHOW IP FLOW  
ENABLE TCP DEBUG  
DISABLE TCP DEBUG  
ENABLE IP ICMP Reply Message={ALL;NETUNREACH;HOSTUNREACH;REDIRECT}  
DISABLE IP ICMP Reply Message={ALL;NETUNREACH;HOSTUNREACH;REDIRECT}  
SHOW IP ICMP Reply Message  
ENABLE IP [SPOOF CHECK]  
DISABLE IP [SPOOF CHECK]  
ADD IP INTERFACE IP Address Fragment  
SET IP INTERFACE IP Address Fragment  
ENABLE IP ROUTE DEBUG  
DISABLE IP ROUTE DEBUG  
SHOW IP ROUTE DUMP  
SET IP DNS Cache  
SHOW IP DNS Cache  
ENABLE IP ARP [AGE POLL]  
DISABLE IP ARP [AGE POLL]  
SET IP ARP Wait Timeout  
SET IP ARP Refresh

ENABLE PING POLL=1..100 DEBUG  
DISABLE PING POLL=1..100 DEBU

ENABLE IP IGMP DEBUG  
DISABLE IP IGMP DEBUG  
SHOW IP IGMP DEBUG  
CREATE IP IGMP DESTINATION  
ADD IP IGMP DESTINATION  
DELETE IP IGMP DESTINATION  
DESTROY IP IGMP DESTINATION  
ENABLE IP IGMP ALLGROUP  
DISABLE IP IGMP ALLGROUP  
ADD IGMP FILTER  
CREATE IGMP FILTER  
DELETE IGMP FILTER  
DESTROY IGMP FILTER  
SET IGMP FILTER  
SHOW IGMP FILTER  
ADD IGMP SNOOPING ROUTERADDRESS  
DELETE IGMP SNOOPING ROUTERADDRESS  
SET IGMP SNOOPING ROUTERMODE  
SHOW IGMP SNOOPING ROUTERADDRESS  
SET IGMP SNOOPING ROUTERMODE FASTLEAVE

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

LOAD [SERVER=ip6add]  
UPLOAD [SERVER=ip6add]  
SET LOADER [SERVER=ip6add]  
ADD USER RSO IP=ip6add  
DELETE USER RSO IP=ip6add  
ADD PING POLL IPADDRESS=ip6add  
SET PING POLL [IPADDRESS=ip6add]

ENABLE MLDSNOOPING DEBUG  
DISABLE MLDSNOOPING DEBUG  
SET MLDSNOOPING VLAN={vlanname;1..4094;ALL} FASTLEAVE={ON;OFF;SINGLE;  
MULTIPLE}

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

SHOW DEBUG [STACK]  
MODIFY  
DUMP

## 7 コマンドリファレンスについて

---

最新のコマンドリファレンス「CentreCOM 8424XL/8424TX コマンドリファレンス 2.7 (Rev.K)」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、お手持ちのコマンドリファレンス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。

※パーツナンバー「J613-M0005-13 Rev.K」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/>**