



最初にお読みください

---

---

---

---

---

# CentreCOM® 8724SL/8748SL リリースノート

---

この度は、CentreCOM 8724SL/8748SL（以下、CentreCOM を省略）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（J613-M0019-00 Rev.A）とコマンドリファレンス（J613-M0019-01 Rev.F）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 2.9.1-02

---

### 2 重要：2.6.1 pl12 以前からバージョンアップするときの注意事項

---

ソフトウェアバージョン 2.6.1 pl12 以前から 2.9.1-02 にバージョンアップすると、最初の再起動時に「設定なし」の状態では起動する場合があります。

このようなときは、バージョンアップ後にコンソールからログインし、SET CONFIG コマンドで起動時設定ファイルを指定しなおした後、本製品を再起動してください。例えば、バージョンアップ前に mynet.cfg という設定ファイルを使用していた場合は、次のようにします。

```
SET CONFIG=mynet.cfg
```

```
RESTART SWITCH
```

また、リモートからバージョンアップを行うときは、バージョンアップ後アクセス不能に陥ることを避けるため、次の手順にしたがってバージョンアップを行ってください。

1. バージョン 2.6.1 pl12 以前で動作している本製品にログインします。
2. 次のコマンドを実行し、Boot configuration file: に表示されるファイル名をメモします。

```
SHOW CONFIG
```

3. 次のコマンドを実行し、現在の設定を boot.cfg に保存します。boot.cfg は、「設定なし」で起動したときに自動実行される特殊なファイルです。

```
CREATE CONFIG=boot.cfg
```

4. ログアウトします。
5. 「バージョンアップ手順書」の指示にしたがって、2.9.1-02 にバージョンアップします。
6. バージョン 2.9.1-02 で動作している本製品にログインします。
7. 次のコマンドを実行します。xxxx には手順 2 でメモしたファイル名を指定します。

```
SET CONFIG=xxxx
```

8. 手順 3 で作成した boot.cfg を削除します。

```
DELETE FILE=boot.cfg
```


9. 以上です。


### 3 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 2.7.6-05 から 2.9.1-02 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。

#### 3.1 ポートランキング /LACP とオーバーラップ STP の併用


 [「コマンドリファレンス」](#) / [「スイッチング」](#) / [「ポート」](#)

 [「コマンドリファレンス」](#) / [「スイッチング」](#) / [「LACP \(IEEE 802.3ad\)」](#)

 [「コマンドリファレンス」](#) / [「スイッチング」](#) / [「スパンニングツリー \(STP/RSTP\)」](#)


ポートランキングとオーバーラップ STP、LACP とオーバーラップ STP の併用が可能になりました。

#### 3.2 マルチプル VLAN (Private VLAN) : 複数アップリンクポートのサポート

 [「コマンドリファレンス」](#) / [「スイッチング」](#) / [「バーチャル LAN」](#)

1 つのマルチプル VLAN (Private VLAN) に対して、アップリンクポートを複数設定できるようになりました。

#### 3.3 OSPF : AS 外部経路取り込み時の詳細設定

 [「コマンドリファレンス」](#) / [「IP」](#) / [「経路制御 \(OSPF\)」](#)


AS 境界ルーター (ASBR) において、AS 外部経路を取り込むときに、取り込む経路の数に上限を設けたり、メトリック、メトリックタイプ、経路タグなどを任意に設定したりできるようになりました。設定は機能拡張された ADD OSPF REDISTRIBUTE コマンドで行います。

### 4 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 2.7.6-05 から 2.9.1-02 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。

#### 4.1 DHCP Snooping : スタティックエントリーの追加・削除

 [「コマンドリファレンス」](#) / [「スイッチング」](#) / [「DHCP Snooping」](#)

- ADD DHCP Snooping BINDING コマンドでスタティックエントリーを追加するとき、MAC アドレスを省略できるようになりました。なお、MAC アドレスを省略する場合は、DHCP Snooping のオプション機能である ARP セキュリティを有効化しないでください (デフォルトは無効)。
- DELETE DHCP Snooping BINDING コマンドでスタティックエントリーを削除するとき、前バージョンまでは MAC アドレスを指定していましたが、本バージョンでは IP アドレスを指定する方式に仕様変更されました。


#### 4.2 OSPF : ASBR の動作仕様変更

 [「コマンドリファレンス」](#) / [「IP」](#) / [「経路制御 \(OSPF\)」](#)

前バージョンまで、SET OSPF コマンドで ASEXTERNAL=ON を指定すると (ASBR として動作させるための設定)、スタティック経路と非 OSPF インターフェースに接続されたネット


ワークの経路情報が AS 外部経路として自動的に取り込まれていましたが、本バージョンでは非 OSPF インターフェースの直結経路はデフォルトで取り込まれなくなりました。非 OSPF インターフェースの直結経路を AS 外部経路として取り込むには、機能拡張された ADD OSPF REDISTRIBUTE コマンドを PROTOCOL=INTERFACE として実行してください。

#### 4.3 OSPF : SET OSPF コマンドから ADD OSPF REDISTRIBUTE コマンドへの自動変換

 **「コマンドリファレンス」 / 「IP」 / 「経路制御 (OSPF)」**

本バージョンより、SET OSPF コマンドの STATICEXPORT=YES、RIP=IMPORT/BOTH、BGPIMPORT=ON は、それぞれ ADD OSPF REDISTRIBUTE コマンドの PROTOCOL=STATIC、PROTOCOL=RIP、PROTOCOL=BGP に自動変換されます。また、SET OSPF コマンドの BGPLIMIT パラメーターと ADD OSPF REDISTRIBUTE PROTOCOL=BGP の LIMIT パラメーターは、一方を変更すると他方にも反映されます。

#### 4.4 IGMP Snooping : 高速脱退機能 (Fast Leave) の設定コマンド変更

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

IGMP Snooping 高速脱退 (Fast Leave) 機能の設定コマンドが以下のとおり変更されました。対象 VLAN の指定が必須になったことと、コマンドリファレンス上の見出し名が「SET IGMPSPNOOPING FASTLEAVE」から「SET IGMPSPNOOPING VLAN FASTLEAVE」に変更されている点にご注意ください。

##### 旧コマンド

```
SET IGMPSPNOOPING FASTLEAVE={ON|OFF|YES|NO|TRUE|FALSE}  
[INTERFACE=vlan-if]
```

##### 新コマンド

```
SET IGMPSPNOOPING VLAN={vlanname|1..4094|ALL}  
FASTLEAVE={ON|OFF|YES|NO|TRUE|FALSE}
```

なお、本バージョンでは従来のコマンドも受け付けますが、設定保存時には新コマンドに自動変換されます。

## 5 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 2.7.6-05 から 2.9.1-02 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。

- 5.1 SHOW LOG RECEIVE コマンドの RECEIVE パラメーターに値を指定しても、項目の絞り込みが行われませんでした。これを修正しました。また、MASK パラメーターを指定するとエラーになっていましたが、これを修正しました。
- 5.2 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ていましたが、これを修正しました。
- 5.3 CREATE LOG OUTPUT コマンドでログ出力先を定義しようとすると、「Internal Error: Failed to create output definition.」というエラーメッセージが表示され、出力先を定義できないことがありましたが、これを修正しました。

- 5.4 CREATE TRIGGER MODULE コマンドにおいて、「?」や「TAB」キーによる入力候補の表示が正しく機能しないことがありましたが、これを修正しました。
- 5.5 トランクグループに所属するポートを、DISABLE SWITCH PORT コマンドの LINK パラメーターの指定で物理的にリンクダウンさせた後で、ENABLE SWITCH PORT コマンドでリンクアップさせると、ポートランキングが正常に動作しなくなりましたが、これを修正しました。
- 5.6 SHOW SWITCH PORT コマンドの表示において、「Broadcast rate limit」、「Multicast rate limit」、「DLF rate limit」各欄の表示が「xxxx/s」（xxxx は数値）のようになっていましたが、これを「xxxx fps」（Frames Per Second）に修正しました。
- 5.7 ポートランキングと 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 値が更新されていましたが、これを修正しました。  
（「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）
- 5.8 トランクグループ内のポートがリンクダウンしたとき、一時的に通信が途絶えることがありましたが、これを修正しました。
- 5.9 スパニングツリープロトコル（STP）有効時に Topology Change が発生すると、すべてのポートから ARP エントリーが削除されていましたが、これを修正しました。
- 5.10 マルチプルスパニングツリープロトコル（MSTP）有効時に CIST リージョナルルートとして動作しているとき、BPDU 内の CIST Internal Root Pathcost フィールドに 0 ではなく External Pathcost の値をセットして送信していましたが、これを修正しました。
- 5.11 ファイアウォールが有効化されているコンピューターに対して FINGER コマンドを実行するとレポートすることがありましたが、これを修正しました。
- 5.12 SET PING の後に「?」キーを入力しても、次の入力候補キーワードが表示されませんでした。これを修正しました。
- 5.13 PING コマンドの PATTERN パラメーターに 16 進数を 9 桁以上入力してもエラーにならず、また、9 桁以上入力した場合は末尾の 8 桁がデータパターンとして使用されていましたが、これを修正しました。
- 5.14 OSPF において、DD パケットの Interface MTU フィールドに常時 0 をセットしていましたが、これを修正しました。
- 5.15 同一内容のタイプ 5 LSA またはタイプ 7 LSA を複数受信したとき、ルーター ID が最大の LSA だけでなく、すべての LSA の情報を受け入れていましたが、これを修正しました。
- 5.16 OSPF において、ABR として動作しており、なおかつ、バックボーンエリアの経路を集約している場合、通過エリアに対するタイプ 3 LSA でもバックボーンエリアの経路を集約して通知していましたが、これを修正しました。

- 5.17 バックアップ DR として動作している OSPF インターフェースのルーター優先度 (SET OSPF INTERFACE コマンドの PRIORITY パラメーター) を 0 に変更しても、該当インターフェースが非 DR/ 非バックアップ DR に移行しませんでした、これを修正しました。
- 5.18 ASBR として動作している場合、IP ルートフィルタを用いて非 OSPF インターフェースの経路情報を配布しないよう設定すると、LSAge=3600 のタイプ 5 LSA を 1 秒間隔で送信してしまい、結果的に OSPF の隣接関係を確立できなくなることがありましたが、これを修正しました。
- 5.19 BGP 使用時、INROUTEMAP を用いて、受信した UPDATE に Well-known コミュニティを付加した場合、本来再通知してはならないピアにも UPDATE を送信することがありましたが、これを修正しました。
- 5.20 BGP 経路で学習したデフォルト経路に対し、経路選択時の優先度 (preference) が正しく設定されていませんでしたが、これを修正しました。
- 5.21 ADD BGP IMPORT コマンドを実行し、特定のソース (起源) を持つ経路情報を BGP に取り込むよう設定していても、IP 経路表の更新が BGP の経路表に動的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。
- 5.22 SHOW BGP ROUTE コマンドの出力において、集約経路および集約経路に内包された個々の経路には最適経路を示す「>」記号が付加されませんでしたが、これを修正しました。
- 5.23 経路情報を E-BGP ピアに再通知するとき、ルートマップによって設定された MED 属性を付加したまま UPDATE メッセージを送信することがありましたが、これを修正しました。
- 5.24 SET BGP PEER コマンドにおいて、「LOCAL=NONE」の指定がエラーになっていましたが、これを修正しました。
- 5.25 DISABLE BGP DEFAULTORIGINATE コマンドを実行しても、すでに通知していたデフォルト経路の取り消しをピアに通知しませんでした、これを修正しました。
- 5.26 VLAN インターフェースに IP アドレスを設定したとき、ARP キャッシュに IP アドレス 255.255.255.255 のエントリーが登録されることがありましたが、これを修正しました。
- 5.27 不正な ARP パケットを受信しても、SHOW IP COUNTER=ARP の arpRxDiscPkts カウンターがカウントされませんでした、これを修正しました。
- 5.28 Gratuitous ARP パケットの受信時、受信インターフェースと異なるネットワークの IP アドレスであっても、そのアドレスを ARP キャッシュに登録していましたが、これを修正しました。

- 5.29 IPv6 の Ping (ICMPv6 Echo Request) に対して Echo Reply を送信するとき、IPv6 ヘッダーの Hop limit フィールドに、受信した Echo Request の Hop limit 値をセットしていましたが、これを修正しました。
- 5.30 IPv6 インターフェースにおいてリンクローカルアドレスの重複を検出しても、該当インターフェースが使用不可にならず、同インターフェースに設定されたグローバルアドレスでは通信が可能でしたが、これを修正しました。
- 5.31 リンクダウンしているインターフェースにリンクローカルアドレスを設定した場合、SHOW IPV6 INTERFACE で表示されるインターフェースの状態が「tentative」ではなく「preferred」になっていましたが、これを修正しました。
- 5.32 IPv6 アドレスが設定されているインターフェースに対して、IPv4 のマルチホーミング設定を行い、設定を保存した上でシステムを再起動すると、エラーが発生していましたが、これを修正しました。
- 5.33 RIPng においてトリガーアップデートが動作しませんでしたでしたが、これを修正しました。
- 5.34 IPv6 の Neighbour をスタティック登録していても、他のポートから NA パケットを受信すると Neighbour キャッシュのポート番号が書き換えられていましたが、これを修正しました。
- 5.35 ルーター通知 (RA) パケットの送信を無効に設定しても、Lifetime フィールドが 0 のルーター通知 (RA) パケットが送信されませんでしたでしたが、これを修正しました。
- 5.36 IPv6 インターフェースのリンクローカルアドレスを変更しても、変更前のアドレスで Lifetime フィールドが 0 のルーター通知 (RA) パケットが送信されませんでしたでしたが、これを修正しました。
- 5.37 ルーター通知 (RA) において、SET IPV6 PREFIX コマンドでパラメーターに ONLINK=NO を指定して実行すると、プレフィックス情報オプションの L フラグだけでなく、A フラグ (AUTONOMOUS パラメーター) もオフになっていましたが、これを修正しました。
- 5.38 (PIM-SM) PIM-SM 関連のログと SNMP トラップを有効にしても (SET PIM LOG コマンド)、PIM インターフェース削除時のログとトラップが生成されませんでしたでしたが、これを修正しました。
- 5.39 (PIM-SM) PIM インターフェースでメンバーからの IGMP Leave メッセージを受信しても、該当インターフェースが下流インターフェースのエントリーから削除されないため、マルチキャストパケットがフラディングされていましたが、これを修正しました。
- 5.40 (PIM-SM) DR でないインターフェースにおいて、マルチキャストグループが登録されている状態で IGMP Report を受信すると、PIM Join メッセージを送信していましたが、これを修正しました。
- 5.41 IGMP の統計カウンター outQuery の値が正しくありませんでしたが、これを修正しました。


- 5.42 ポートランキングと IGMP Snooping を併用しており、なおかつ、IGMP を無効に設定しているとき、マスターポートで Leave メッセージを受信すると、該当マルチキャストグループからトランクポートが削除されていましたが、これを修正しました。  
〔「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〕
- 5.43 PIM6-SM において、本製品が BSR として動作している場合、C-RP の情報がタイムアウトしても、該当 C-RP が担当していたマルチキャストグループの情報を保持し続けていましたが、これを修正しました。
- 5.44 PIM6-SM において、Assert メッセージの送信間隔が規格値の 180 秒ではなく 190 秒になっていましたが、これを修正しました。
- 5.45 PIM6-SM において、Register Probe Time (SET PIM6 コマンドの PROBTIME) を変更すると、同タイマー満了後、Register パケットを送信しなくなり、結果としてマルチキャストデータも送信されなくなっていました。これを修正しました。
- 5.46 IPX インターフェースの構成ポートがすべてリンクダウンしても、SHOW IPX CIRCUIT コマンドの表示項目 Link State に反映されませんでした。これを修正しました。
- 5.47 Smurf AMP 攻撃を検知しても、SHOW FIREWALL POLICY コマンドの COUNTER オプションで表示されるカウンターがカウントされませんでした。これを修正しました。
- 5.48 ファイアウォール NAT を使用している環境で、PUBLIC 側から PRIVATE 側へ traceroute を実行すると、PUBLIC インターフェースからの返答パケットに対しても NAT 変換が行われることがありましたが、これを修正しました。
- 5.49 アクセスリストが登録されている状態でファイアウォールポリシーを削除するとリポートしていましたが、これを修正しました。
- 5.50 ファイアウォール使用時、PUBLIC 側のクライアントから本製品の PUBLIC インターフェースに Telnet 接続すると、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。

## 6 本バージョンでの制限事項

---

ソフトウェアバージョン **2.9.1-02** には、以下の制限事項があります。

### 6.1 RADIUS

 **「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。

---


## 6.2 アップロード

 **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。

---


## 6.3 ログ

 **参照** 「コマンドリファレンス」 / 「運用・管理」 / 「ログ」

CREATE LOG OUTPUT コマンドの QUEUEONLY、MAXQUEUESEVERITY パラメーターが機能しません。

---

## 6.4 SNMP

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


- dot3StatsCarrierSenseErrors の値が取得できません。
- topologyChange トラップと newRoot トラップが送信されません。
- 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。
- プライベート MIB の instRelMajor、instRelMinor、instRelInterim の値を取得できません。
- プライベート MIB の atrMacBasedAuthPaeState において、本来と異なる値を持つものがあります。
  - ・ authenticated(5) になるべき MIB の値が、authenticating(6) になります。
  - ・ held(7) になるべき MIB の値が、aborting(6) になります。
  - ・ SET PORTAUTH PORT コマンドで「SET PORTAUTH=MACBASED PORT=5 CONTROL=AUTHORISED;UNAUTHORISED」を設定しても、MIB の値が forceAuth(8) または forceUnauth(9) にならず、initialise(1) になります。
- プライベート MIB の atrMacBasedAuthControlledPortStatus において、本来と異なる値を持つものがあります。
  - ・ 認証を行っていないにもかかわらず MIB の値が unauthorised(2) にならず、authorised(1) になります。
  - ・ SET PORTAUTH PORT コマンドで「SET PORTAUTH=MACBASED PORT=xx CONTROL=AUTHORISED;UNAUTHORISED」を設定しても、MIB の値が forceAuth(10) または forceUnauth(12) にならず、never(1) になります。
- プライベート MIB の restart の値を Get Next Request では取得できません。Get Request ならば取得できます。



- GBIC スロットの ifJackType (ポート形状を示す変数。MAU MIB) のデフォルト値が正しくありません。このため、GBIC が未装着にもかかわらず、SNMP マネージャー上では 1000BASE-T の GBIC が装着されているように見えることがあります。この現象は、8724SL ではポート 25 のみ、8748SL ではポート 49 と 50 の両方で発生します。なお、本現象は GBIC をいったん装着してから抜くことで解消します。また、起動時に GBIC が装着されていた場合は、起動後に GBIC を抜いても本現象は発生しません。

---

## 6.5 NTP

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

- SET NTP UTCOFFSET=NONE を実行した後、設定を保存して再起動すると、起動時に「Invalid zone or time for UTC offset.」というエラーメッセージが表示されます。タイムゾーンをデフォルト値に戻す場合は、SET NTP UTCOFFSET=UTC (または GMT) のように指定してください。
- 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。

---


## 6.6 TELNET コマンド

 **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。

---


## 6.7 BPDU フォワーディング

 **参照** 「コマンドリファレンス」 / 「スイッチング」

BPDU フォワーディング有効時、転送された BPDU のサイズが 68 Byte になります。

---


## 6.8 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」

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 (Private 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。

---


## 6.9 ポートセキュリティー

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

ポートセキュリティーがオンのポートで受信したパケットの VLAN ID が、ポートの所属 VLAN と一致しない場合でも、アドレスを FDB に登録します。

---


## 6.10 LACP (IEEE802.3ad)

 [「コマンドリファレンス」](#) / [「スイッチング」](#) / [「LACP \(IEEE802.3ad\)」](#)

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。

---


## 6.11 バーチャル LAN

 [「コマンドリファレンス」](#) / [「スイッチング」](#) / [「バーチャル LAN」](#)

Protected VLAN のポートをミラーリングポートに設定すると、Protected VLAN のポート間で通信ができてしまいます。

---


## 6.12 スパニングツリープロトコル (STP/RSTP)

 [「コマンドリファレンス」](#) / [「スイッチング」](#) / [「スパニングツリー \(STP/RSTP\)」](#)

- Rapid モードのスパニングツリープロトコル (RSTP) 有効時、Topology change が起きた後、FDB が正常に登録されないことがあります。通信の動作に影響はありません。
- スパニングツリープロトコル (STP) 有効時、スイッチポートがリンクダウンしても STP のポート状態が Forwarding のまま変化しません。このため、スパニングツリーの再構成にかかる時間が最大エージタイム (MaxAge) の分だけ長くなります。

---


## 6.13 マルチプルスパニングツリープロトコル (MSTP)

 [「コマンドリファレンス」](#) / [「スイッチング」](#) / [「マルチプルスパニングツリープロトコル」](#)

- DISABLE MSTP MSTI PORT コマンドを実行してマルチプルスパニングツリープロトコル (MSTP) を無効にしたポートでは、MAC アドレスの学習が行われません。BPDU を送信する必要がないポートでは、DISABLE MSTP MSTI PORT コマンドを使用するのではなく、SET MSTP CIST PORT コマンドの EDGEPORT パラメーターに YES を指定してエッジポートに設定してください。
- マルチプ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 PRPOTOCOLVERSION 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。

---

## 6.14 フォワーディングデータベース


 [「コマンドリファレンス」](#) / [「スイッチング」](#) / [「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。

- フィルタリング対象の MAC アドレスを持つ機器が、PORT パラメーターで指定したのとは異なるポートに接続されている場合、本製品から該当 MAC アドレスに宛てたパケットに対して、ACTION=DISCARD のスタティックエントリー（スイッチフィルター）が正しく機能しません。

---


## 6.15 ハードウェア IP フィルター

 **参照** 「コマンドリファレンス」 / 「スイッチング」 / 「ハードウェア IP フィルター」

- 8748SL では、ポート 25 ~ 48 とポート 49 で受信したパケットに対して、ハードウェア IP フィルターの SENDNONUNICASTTOPORT、SENDEPORT アクションが機能しません。
- 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ームタイプ Ethernet 2 の IPX パケットにもマッチしてしまいます。
- ADD SWITCH L3FILTER MATCH コマンドで IMPORT=False、または EXPORT=False を指定すると、IMPORT=True、EXPORT=True の設定で動作しません。False で動作させたい場合は、IMPORT、EXPORT パラメーターを指定しないでください（デフォルトで False の設定になります）。

---

## 6.16 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-Suppllicant 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。
- RADIUS サーバーによってダイナミック VLAN を割り当てられた Suppllicant がリンクダウン、ログオフなどで存在しなくなった場合、プライベート MIB である AuthPreAuthVlan、AuthPostAuthVlan が不正な値を返します。
- 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 Suppllicant の MAC アドレスをゲスト VLAN 上で学習しません。
- Authenticator ポート、MAC ベース認証ポートにおいて、Suppllicant の再認証を有効にし (REAUTHENABLED =TRUE)、再認証間隔 (REAUTHPERIOD) を短い値 (10 秒程度) に設定しているとき、RADIUS サーバーから Suppllicant に向けて短い間隔で Ping 通信が行われるとレポートすることがあります。
- MAC ベース認証において再認証に失敗しても、プライベート MIB の atrMacBasedAuthUnauthenticated トラップが送信されません。

- MAC ベース認証ポートにおいて、認証済み Supplicant が ARP 解決を実行した場合、直後の IP パケット 1 個が本製品によって破棄されます。
- MAC ベース認証ポートにおいて、認証済み Supplicant からの NBT (NetBIOS over TCP/IP) 通信ができなくなることがまれにあります。そのようなときは、Supplicant 側で通信を再試行してください。

---


## 6.17 IP 統計情報

 **【コマンドリファレンス】 / 【IP】**

ファイアウォール有効時、SHOW IP INTERFACE COUNTER コマンドで表示される受信パケットカウンター (ifInPkts, ifInBcastPkts, ifInUcastPkts, ifInDiscards) に、実際の受信パケット数の 2 倍の値が表示されます。

---


## 6.18 ディレクティッドブロードキャストパケット

 **【コマンドリファレンス】 / 【IP】**

特定 VLAN に対するディレクティッドブロードキャスト転送をオンにしている場合、ブロードキャスト MAC アドレス (FF-FF-FF-FF- FF-FF) 宛でのディレクティッドブロードキャストパケットを (別 VLAN で) 受信すると、それ以降、本体 MAC アドレス宛てに送信された通常のディレクティッドブロードキャストパケットを転送できなくなります。

---

## 6.19 TRACE、SET TRACE コマンド

 **【コマンドリファレンス】 / 【IP】**

- SET TRACE コマンドにおいて、MINTTL (最少ホップ数) に MAXTTL (最大ホップ数) より大きい値を指定してもエラーになりません。
- TRACE コマンドにおいて、パラメーター指定が正しくないときに表示が文字化けします。

---


## 6.20 ローカル IP インターフェース (ループバックインターフェース)

 **【コマンドリファレンス】 / 【IP】 / 【IP インターフェース】**

ローカル IP インターフェース (ループバックインターフェース) にブロードキャストアドレスを指定してもエラーになりません。ローカル IP インターフェースに IP アドレスを割り当てるときは、割り当てようとしている IP アドレスがご使用のネットワークにおいて利用可能なものであるかどうかを確認してください。

---

## 6.21 ADD IP ROUTE コマンド

 **【コマンドリファレンス】 / 【経路制御】**

ADD IP ROUTE コマンドで METRIC1 パラメーターに値を指定し、METRIC2 パラメーターには値を指定しない場合、METRIC2 パラメーターに省略時の 1 が設定されず、METRIC1 パラメーターで指定した値が設定されます。

---


## 6.22 SHOW IP ROUTE コマンド

 **「コマンドリファレンス」 / 「IP」 / 「経路制御」**

経路タグ値が大きい場合、SHOW IP ROUTE コマンドの表示において、Tag 欄の値が Metrics 欄の値と連結してしまい、1 つの大きな値のように表示されることがあります。

---

## 6.23 OSPF

 **「コマンドリファレンス」 / 「IP」 / 「経路制御 (OSPF)」**

- SET OSPF コマンドで DEFROUTE=ON を指定した場合、IP の経路表にデフォルト経路がなくても、デフォルトルートの AS 外部 LSA を生成します。
- SET OSPF コマンドで DEFROUTE=OFF を指定しても、デフォルトルートの AS 外部 LSA を生成します。
- 準スタブエリア (NSSA) の ASBR として動作している場合、タイプ 7 LSA の Forwarding Address を正しく選択できず、該当経路宛での通信ができなくなることがあります。
- PURGE OSPF コマンドを実行しても、ADD OSPF REDISTRIBUTE コマンドによる設定内容は消去されません。これらを削除するには、DELETE OSPF REDISTRIBUTE コマンドを使ってください。
- 本製品を準スタブエリア (NSSA) のエリア境界ルーター (ABR) として動作させると、リポートすることがあります。

---

## 6.24 BGP-4

 **「コマンドリファレンス」 / 「IP」 / 「経路制御 (BGP-4)」**

自動ソフトリセットを有効にしても、SET BGP PEER コマンドの DEFAULTORIGINATE パラメーターの設定変更が自動的に反映されません。

---

## 6.25 DNS サーバーアドレスの動的取得

 **「コマンドリファレンス」 / 「IP」 / 「名前解決」**

ADD IP DNS コマンドの INTERFACE パラメーターで、DNS サーバーアドレスを DHCP で動的に取得するよう設定していないにもかかわらず、DNS サーバーアドレスが動的に取得されます。

---


## 6.26 DNS キャッシュ

 **「コマンドリファレンス」 / 「IP」 / 「名前解決」**

DNS キャッシュ機能のキャッシュサイズを 1 に設定した場合、最初のキャッシュエントリーがエージングも上書きもされずに残り続けます。キャッシュサイズを 1 に設定しないでください。

---


## 6.27 RIPng

 **「コマンドリファレンス」 / 「IPv6」 / 「経路制御 (RIPng)」**

RIPng を無効にしても、タイムアウトで完全に削除されるまで RIPng 由来の経路を使用しつづけます。

---

## 6.28 ルーター通知 (RA)

 **「コマンドリファレンス」 / 「IPv6」 / 「近隣探索」**

IPv6 インターフェースがダウンしても、Lifetime フィールドが 0 のルーター通知 (RA) パケットが送信されません。

---

## 6.29 DVMRP

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

- DVMRP インターフェースを削除し、再度追加した場合、該当インターフェース上の DVMRP 経路がホールドダウン状態のままとなります。
- DVMRP が有効で、IGMP Snooping が無効のとき、マルチキャストデータがフラッシングされません。

---

## 6.30 PIM

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

- (PIM-DM/PIM-SM) マルチキャストデータの通信負荷が高いと、PIM パケットを処理できず、マルチキャスト通信が途絶えることがあります。これを選けるには、次のようなハードウェア IP フィルターを設定し、PIM パケットを優先的に処理させるようにしてください。


```
ADD SWITCH L3FILTER MATCH=DIP DCLASS=HOST
```

```
ADD SWITCH L3FILTER=1 ENTRY DIP=224.0.0.13 PRIO=5 AC=SEND
```

- (PIM-DM) Prune 中に上流ルーターの Generation ID が変更されても Prune メッセージを再送せず、結果として、次の Prune メッセージを送信するタイミングまで不要なマルチキャストトラフィックを受信してしまいます。
- (PIM-SM) (S,G) null Register メッセージのパケットフォーマットが正しくありません。ただし、動作には影響ありません。
- (PIM-SM) すべてのポートがリンクダウンしている状態で ADD PIM BSR CANDIDATE コマンドを実行すると、警告メッセージが表示されます。

---


## 6.31 IGMP

 **「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。

---


## 6.32 IGMP Snooping

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

- SET IGMP Snooping ROUTERMODE コマンドでパラメーターに NONE を指定しても、224.0.0.1 および 224.0.0.2 からのマルチキャストパケットを受信した場合には All Group を作成します。All Group を作成しない場合は、DISABLE IP IGMP ALLGROUP コマンドを使用してください。
- DVMRP または PIM を有効にしているとき、IGMP Snooping を無効に設定しても、マルチキャストトラフィックの受信インターフェース (VLAN) においては、該当トラフィックが VLAN 内にフラディングされません。

---

## 6.33 MVR

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

(8748SL のみ) 「1 ~ 24、50」と「25 ~ 48、49」のポートグループをまたぐ構成で複数の VLAN を作成し、MVR を利用したマルチキャスト通信を行っているとき、片方のポートグループで IGMP Leave メッセージを受信すると、もう片方のポートグループでもマルチキャスト通信が停止します。

---

## 6.34 PIM6-SM

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

- Join/Prune Interval (SET PIM6 コマンドの JPINTERVAL) の設定を変更しても、Join/Prune Holdtime が変更されません。
- C-BSR (ブートストラップルーター候補) において、BSR 優先度を何度も変更すると、BSR の選出が正しく行われなくなることがあります。このようなときは本製品を再起動してください。
- マルチキャストデータを送受信しているとき、SHOW PIM6 コマンドに ROUTE オプションを付けて実行するとレポートすることがあります。

---

## 6.35 ファイアウォール

 **参照** 「コマンドリファレンス」 / 「ファイアウォール」

- PUBLIC 側で受信したパケットを破棄した場合、SHOW FIREWALL POLICY コマンドの COUNTER オプションで表示される Total Packets Received カウンターが 2 ずつカウントされます。
- ファイアウォールポリシーにアクセスリストを登録する場合、IP アドレスリストよりルール番号の大きい MAC アドレスリストは有効になりません。MAC アドレスリストのルール番号は IP アドレスリストのルール番号よりも小さくなるように設定してください。
- ADD FIREWALL POLICY コマンドでダイナミック ENAT の PUBLIC インターフェースに IP と LIST を指定したルールを設定した場合、エラーメッセージが表示されます。

その場合は、ADD FIREWALL POLICY コマンドで MAC アドレスリストを追加し、SET FIREWALL POLICY コマンドで IP アドレスを設定してください。

- PUBLIC 側から PRIVATE 側に対して FTP 通信を行った場合、SHOW FIREWALL SESSION コマンドで不要なセッションが表示されることがあります。これは表示だけの問題であり、動作には影響ありません。
- PUBLIC 側インターフェースにルール NAT（エンハンスド、リバース、ダブルのいずれか）を設定した場合、PUBLIC 側から PRIVATE 側への FTP 通信が正常に行えないことがあります。
- 攻撃検出機能によって攻撃を検出したとき、検出されたパケットが許可されているにも関わらず、SHOW FIREWALL EVENT コマンドの出力では Deny Event（拒否イベント）に表示されます。
- SHOW FIREWALL EVENT コマンドで表示されるイベント情報は、内部テーブルがいっぱいになると古い情報から削除されます。このとき、攻撃開始のイベント情報が削除されてしまうと、攻撃の終了を検出しても、攻撃終了のイベントを通知しなくなります。
- ファイアウォール有効時、TCP コネクションキュー内に確立したセッションが残ってしまいます。
- ファイアウォール有効時、RTSP パケット（ポート番号：554）を許可するようルールを設定しても、パケットが転送されません。これを回避するには、RTSP のポート番号を変更してください。
- ファイアウォール NAT を使用している環境で、PUBLIC 側から PRIVATE 側へ traceroute を実行すると、PRIVATE 側から返信される ICMP メッセージ（Time-to-live exceeded）内のオリジナルヘッダーに PRIVATE 側アドレスが未変換のまま残ります。

---

## 6.36 VRRP

### 参照 「コマンドリファレンス」 / 「VRRP」

ブリエンプトモード OFF かつ優先度 231 以上でバックアップルーターとして動作している場合、マスタールーターがダウンしてもマスターに移行しません。このような場合は、バックアップルーター側で VRRP を再起動してください（DISABLE VRRP → ENABLE VRRP の順に実行）。




## 7 取扱説明書・コマンドリファレンスの補足・誤記訂正

---


取扱説明書とコマンドリファレンスの補足事項です。

### 7.1 HTTP サーバー（サポート対象外）

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


本製品はデフォルトで HTTP サーバー（サポート対象外）が有効になっているため、IP 有効時は TCP ポート 80 番がオープンしています。セキュリティを重視する場合は、DISABLE HTTP SERVER コマンドを実行して、HTTP サーバーを無効にしてください。

### 7.2 弊社 CentreNET SwimRadius 使用時の注意

 **参照** 「コマンドリファレンス」 / 「運用・管理」 / 「認証サーバー」

RADIUS サーバーとして弊社 CentreNET SwimRadius を使用する場合、本製品自身へのログイン認証（ユーザー認証）には SwimRadius を利用しないでください（SwimRadius は、ポート認証機能に特化した RADIUS サーバーです）。

### 7.3 DESTINATION=ROUTER のログ出力先定義

 **参照** 「コマンドリファレンス」 / 「運用・管理」 / 「ログ」

DESTINATION=ROUTER のログ出力先定義を使用するときは、ログの送信側と受信側で同一ファームウェア（ファイル名とバージョンが同じもの）を使用してください。それ以外の構成はサポート対象外とさせていただきますのでご注意ください。

### 7.4 送信元アドレスがマルチキャストアドレスのフレーム

受信した Ethernet フレームの送信元アドレスがマルチキャストアドレスだった場合、このフレームは転送されずに破棄されます。

### 7.5 スイッチポートの統計カウンター（8748SL のみ）

8748SL では、ポートグループ「1～24、50」と「25～48、49」をまたぐパケットは、SHOW SWITCH PORT COUNTER コマンドで表示される ifOutUcastPkts、ifOutErrors、DropEvents カウンターにカウントされません。

### 7.6 1000Mbps ポートのフラッシングレート

リンクしている 10/100Mbps ポートの数によって、拡張モジュールの 1000Mbps ポートのブロードキャスト、マルチキャストの転送率が下がる場合があります。


### 7.7 ポート帯域制限機能の受信レート上限値と TCP 通信のスループット

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

スイッチポートに受信レート上限値（INGRESSLIMIT）を設定している場合、同ポートを経由した TCP の通信では、TCP データのスループットが設定した上限値よりも低くなります（低下の度合いは通信状況に依存します）。これは TCP プロトコルの特性として、帯域制限機能によって破棄されたパケットの再送処理などが発生するためです。また、TCP 以外においても、同様の再送処理を行うプロトコルではこの現象が発生する可能性があります。

---


## 7.8 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」 / 「スイッチング」 / 「フォワーディングデータベース」

1 回目のエージアウトでは、すべてのダイナミックエントリーがフォワーディングデータベースから削除されない場合があります。ただし、2 回目以降のエージアウトではすべてのダイナミックエントリーが削除されます。

---


## 7.9 ハードウェア IP フィルター

 **参照** 「コマンドリファレンス」 / 「スイッチング」 / 「ハードウェア IP フィルター」

- IPv6 ルーティングを有効にしている場合、ルーティング対象の IPv6 パケットに対して、EtherType = 0x86DD (IPv6) の条件を持つハードウェア IP フィルターエントリーがマッチしません。ルーティング対象の IPv6 パケットをフィルタリングするには、IPv6 フィルターを使用してください。ルーティング対象でない (スイッチングされる) IPv6 パケットには、前述のハードウェア IP フィルターがマッチします。
- IPX ルーティングを有効にしている場合、ルーティング対象の IPX パケットに対しては、SENDMIRROR 以外のアクションが機能しません。また、SENDMIRROR アクションと EPORT パラメーターは併用できません。ルーティング対象の IPX パケットをフィルタリングするには、IPX トラフィックフィルターを使用してください。なお、ルーティング対象でない (スイッチングされる) IPX パケットには、すべてのアクションが機能します (ただし、IP パケットを前提としている MOVETOSTOPRIO、SETTOS、MOVEPRIOTOTOS、SETIPDSCP アクションは使用不可)。

---

## 7.10 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 (802.1X 認証、MAC ベース認証) を有効にしたポートでは、ポートトラッキング、スパンニングツリープロトコル、ポートセキュリティーを使用できません。また、802.1X 認証の Authenticator ポートと MAC ベース認証ポートをタグ付きに設定することはできません。


---


## 7.11 IP マルチキャストのハードウェア処理


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

スイッチ間をタグ付きポートで接続している場合、タグ付きポートを通過する IP マルチキャストパケットは、最初に ADD IP INTERFACE コマンドを実行した VLAN の VID を持つものだけがハードウェア処理の対象となり、他の VID を持つパケットはソフトウェア処理となります。ソフトウェア処理される場合のパフォーマンスは「ワイヤースピード ÷ VLAN 数」となります。タグ VLAN 環境で IP マルチキャストを使用するときは、タグ付きポートに割り当てる VLAN 数を 3 つまでにすることをおすすめします。

## 7.12 IGMP Snooping/MLD Snooping 無効時のポート帯域制限 (INGRESSLIMIT) 設定

 [「コマンドリファレンス」](#) / [「スイッチング」](#) / [「ポート」](#)

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

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

IGMP Snooping や MLD Snooping を無効に設定しているときは（デフォルトは有効）、スイッチポートの受信レート上限値（INGRESSLIMIT）を 1000Kbps 未満に設定しないでください。1000Kbps 未満に設定すると、該当ポートで受信したマルチキャストパケットが他のポートにフラッディングされなくなります。

## 8 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。

- 以下の機能別キーワードを含む全コマンド

ENABLE の後に [?] キーを押すと表示される機能別キーワードです。

ACC, APPLTALK, BRI, CLASSIFIER, ETH, FRAMERELAY, GARP, GRE, GUI, IPSEC, ISAKMP, ISDN, L2TP, LAPB, LAPD, LDAP, LOADBALANCER, LB, LPD, MIOX, PKI, PRI, Q931, RSVP, SA, SERVICE, SSL, STAR, STARTUP, STT, SYN, TPAD, TACACS, VLANRELAY, X25C, X25T, TDM, DS3, VOIP

- 以下のコマンド（パラメーター）

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。

**COPY**  
**DUMP**  
**START PKT**  
**STOP PKT**  
**SET PKT**  
**SHOW SYSTEM TEMPERATURE**  
**TRACE** [ADDRONLY]  
**PING** [APPLEADDR ; OSIADDRESS] [SAPPLEADDRESS ; SOSIADDRESS]  
**SET PING** [APPLEADDR ; OSIADDRESS] [SAPPLEADDRESS ; SOSIADDRESS]  
**PURGE PING TOTALLY**  
**SHOW SWITCH SOCK**  
**SHOW SWITCH MEMORY**  
**SHOW SWITCH SWTABLE**  
**SET SWITCH SOCK**  
**SET SWITCH PORT** [MULTICASTMODE] [SPEED={10MHAUTO ; 10MFAUTO ; 100MHAUTO ; 100MFAUTO ; 1000MHAUTO ; 1000MFAUTO ; 1000MHALF}]  
**ENABLE/DISABLE SWITCH BIST**  
**CREATE/DESTROY IP POOL**  
**SHOW IP POOL**  
**ADD/DELETE IP ROUTE FILTER** [PROTOCOL={STATIC ; INTERFACE}]  
**ADD/DELETE/SET IP FILTER PRIORITY**  
**ADD/DELETE IP EGP**  
**ENABLE/DISABLE IP EGP**

SHOW IP EGP  
ADD/SET IP RIP [NEXTHOP]  
ADD/DELETE IP SA  
SHOW IP SA  
SET IP ARP [DLC] [CIRCUIT]  
SET IP RIP NEWIPADDRESS  
SET IP FLOW  
SHOW IP FLOW  
SHOW IP CACHE  
SHOW IP ROUTE [CACHE]  
SHOW IP ROUTE TEMPLATE  
SHOW IP ROUTE MULTICAST  
ENABLE/DISABLE IP FOFILTER  
ENABLE/DISABLE IP MULTICASTSWITCHING  
ENABLE/DISABLE IP SRCROUTE  
ADD/DELETE/SET IP ROUTE BLACKHOLE  
ADD/DELETE DVMRP [DLC]  
ADD/DELETE DVMRP INTERFACE [DLC]  
SET DVMRP [DLC]  
SET DVMRP INTERFACE [DLC]  
ADD/DELETE IPV6 FILTER [PRIORITY]  
ADD/DELETE IPV6 INTERFACE [PRIORITYFILTER]  
SET IPV6 FILTER [PRIORITY]  
SET IPV6 INTERFACE [PRIORITYFILTER]  
ENABLE/DISABLE IPV6 FLOW  
ADD/SET IPV6 INTERFACE [TYPE=ANYCAST]  
CREATE FIREWALL POLICY DYNAMIC  
ADD/DELETE FIREWALL POLICY DYNAMIC  
ADD/DELETE FIREWALL POLICY PROXY  
ADD/DELETE FIREWALL POLICY SPAMSOURCES  
ADD/DELETE FIREWALL POLICY HTTPFILTER  
SET FIREWALL POLICY SMTPDOMAIN  
SET FIREWALL POLICY ATTACK  
ENABLE/DISABLE FIREWALL POLICY SMTPRELAY  
ENABLE/DISABLE FIREWALL POLICY HTTPCOOKIES  
CREATE QOS  
ADD/DELETE QOS  
SET QOS PORT  
SET QOS POLICY  
SET QOS TRAFFICCLASS  
SET QOS FLOWGROUP  
SHOW QOS POLICY  
SHOW QOS TRAFFICCLASS  
SHOW QOS FLOWGROUP  
CREATE/DESTROY PPP [AUTHMODE] [BAPMODE] [CBMODE] [CBDELAY]  
[COPY] [DEBUGMAXBYTES] [DESCRIPTION] [FRAGMENT]  
[FRAGOVERHEAD] [LOGIN] [MAXLINKS] [MRU] [NULLFRAGTIMER]  
[NUMBER] [TYPE]

ADD/DELETE PPP [AUTHENTICATION] [CBDELAY] [CBMODE] [CBNUMBER]  
[CBOPERATION] [COMPALGORITHM] [COMPRESSION] [CONFIGURE]  
[MODEM] [NUMBER] [PREDCHECK] [RESTART] [STACHECK] [TERMINATE]  
[TYPE]  
ADD/DELETE/SET PPP ACSERVICE  
ADD/DELETE/SET PPP TEMPLATE  
ENABLE/DISABLE PPP TEMPLATE  
ADD/DELETE PPP MAXSESSIONS  
ADD/DELETE PPP ACRADIUS  
ADD/DELETE PPP VLAN  
ENABLE/DISABLE PPP ACCESSCONCENTRATOR  
ACTIVATE PPP RXPKT  
ADD/DELETE/SET PIM INTERFACE [SRCAPABLE]  
SHOW PIM [STATEREFRESH]  
ADD/SET PIM BSRCANDIDATE [HASHMASKLENGTH]  
SET BOOTP MAXHOPS  
ENABLE/DISABLE DHCP [BOOTP]  
ENABLE/DISABLE BGP DAMPING  
CREATE/SET BGP DAMPING PARAMETERSET  
ADD IP ROUTEMAP [MATCH TAG]  
CREATE/SET VRRP ADVERTISEMENT  
ADD/SET IP RIP REDISTRIBUTE [ROUTEMAP] [LIMIT] [METRIC] [SUBNET]  
ADD/SET OSPF REDISTRIBUTE [ROUTEMAP]  
ENABLE/DISABLE DHCP Snooping STRICTUNICAST  
ADD/DELETE IGMP Snooping VLAN ROUTERPORT  
SET IGMP Snooping VLAN QUERY SOLICIT

## 9 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（J613-M0019-01 Rev.F）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。

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