J613-M0019-04 Rev.Y 140711

Allied Telesis

CentreCOM® 8700SL シリーズ リリースノート

この度は、CentreCOM 8700SL シリーズ（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、613-000900 Rev.A）とコマンドリファレンス（J613-M0019-01 Rev.P）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　ソフトウェアバージョン　2.9.2-14

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 **2.9.2-14** 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、**2.9.2-14** にバージョンアップします。
6. バージョン **2.9.2-14** 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　重要：ハードウェアリビジョンに関する注意（8724SL V2 のみ）

ハードウェアリビジョン D1 以降の 8724SL V2 にソフトウェアをダウンロードする場合は、**2.9.1-16** 以降をご使用ください。

ハードウェアリビジョンは、8724SL V2 の底面に貼付されているシリアル番号シール（バーコード）に記載されています。

（例）

4　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 2.9.2-07 から 2.9.2-14 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。

4.1　IPv6 over IPv4/6to4 トンネルインターフェースにおける MSS クランプ機能

参照「コマンドリファレンス」/「IPv6」/「IPv6 インターフェース」

IPv6 over IPv4 および 6to4 トンネルインターフェースにおいて、IPv6 上の TCP Syn パケットを監視し、TCP ヘッダー内の MSS オプションの値が 1220 を超える場合、同オプションの値を 1220 に書き換える MSS クランプ機能をサポートしました。本機能はつねに有効であり、無効にはできません。また、MSS の値は 1220 固定です。

なお、本機能では、IPv6 パケットが IPv4 パケットにカプセル化される時点で、IPv6 パケット内 TCP Syn パケットの MSS オプション値を書き換えます。IPv6 パケットのカプセル化を解除するときは、書き換えを行いません。

5　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 2.9.2-07 から 2.9.2-14 へのバージョンアップにおいて、以下の仕様変更が行われました。

5.1　ログメッセージタイプの名称変更

参照「コマンドリファレンス」/「運用・管理」/「ログ」

DNS 関連のログメッセージタイプの名称が、IPDNS から DNS に変更になりました。
本仕様変更にともない、以前のバージョンの設定で以下のコマンドの MODULE パラメーターに IPDNS を指定している場合は、DNS へ変更してください。

○　以前のバージョンでの設定（変更前）
ADD LOG OUTPUT [MODULE=IPDNS]
SET LOG OUTPUT FILTER [MODULE=IPDNS]
SHOW LOG [MODULE=IPDNS]

○　本バージョンでの設定（変更後）
ADD LOG OUTPUT [MODULE=DNS]
SET LOG OUTPUT FILTER [MODULE=DNS]
SHOW LOG [MODULE=DNS]

5.2 SHOW INTERFACE COUNTERS の表示変更

参照「コマンドリファレンス」/「運用・管理」/「SNMP」

本バージョンより、下記のコマンドで 64 ビットの MIB カウンター ifHCInOctets と ifHCOutOctets が表示されるようになっていますが、これらのカウンターは未サポートです。

- SHOW INTERFACE（COUNTERS オプション指定時）

また、MIB オブジェクト ifHCInOctets と ifHCOutOctets も同様に未サポートとなります。

5.3 SHOW IP DNS / SHOW IP DNS CACHE コマンドの表示変更

参照「コマンドリファレンス」/「IP」/「名前解決」

該当コマンドの表示項目が一部変更になりました。

○ SHOW IP DNS コマンド

```
Manager > show ip dns

DNS Server Configuration
------------------------------------------------------------------------------
Domain                        Int/Status    Server Addr Preference          Requests
 Primary (v4)                             Primary (v6)
 Secondary (v4)                           Secondary (v6)
------------------------------------------------------------------------------
ANY*                          ppp0/Up       Prefer IPV4                          3
 200.100.10.1                             Not set
 200.100.10.2                             Not set
------------------------------------------------------------------------------

Cache:
  Maximum entries ................... 30
  Current entries ................... 2 (592 bytes)
  Timeout (minutes) ................. 10
  Cache hits ........................ 1

Global configuration:
  IP RR Type query preference ....... IPv4
```

以下は変更／追加された項目です。

Primary (v4)	プライマリー DNS サーバーアドレス。未設定の場合は 0.0.0.0 と表示される。サーバーアドレスを動的に取得しているときは、該当インターフェースがダウンだとアドレスは未設定状態となる
Secondary (v4)	セカンダリー DNS サーバーアドレス。未設定の場合は 0.0.0.0 と表示される
Primary (v6)	未サポート
Secondary (v6)	未サポート
Server Addr Preference	未サポート (Prefer IPV4 のみ表示)
Global configuration セクション	DNS の全体設定が表示される
IP RR Type query preference	未サポート (IPv4 のみ表示)

○ SHOW IP DNS CACHE コマンド

表示項目名の「IP Address」が「IPv4 Address」へ変更されました。

5.4 DHCPv4 サーバーの仕様変更

参照「コマンドリファレンス」/「DHCP サーバー」

DHCPv4 サーバー機能において、DHCP クライアントに配布した IP アドレスが重複していた場合、DHCP クライアントが送信する DHCP DECLINE メッセージを受信しても同じ IP アドレスを再配布することがありましたが、異なる IP アドレスを再配布するように仕様変更しました。

6 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 **2.9.2-07** から **2.9.2-14** 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。

6.1 起動時にトリガースクリプトが実行される際、スクリプトファイルのファイル名（ベース名）が 9 文字以上だと該当スクリプトを正常に実行できない場合がありましたが、これを修正しました。

6.2 スイッチポートの DESCRIPTION を削除した際に、SHOW INTERFACE COUNTERS で表示されるスイッチポートのインターフェース名がデフォルトの表示に戻りませんでしたが、これを修正しました。

6.3 （8748SL のみ）MAC アドレスベース認証において、意図しないタイミングで認証タイムアウトが発生し、認証のやり直しが発生することがありましたが、これを修正しました。

6.4 DHCP Snooping の ARP セキュリティーが有効の場合、Trusted ポートで STP の状態が Blocking になっていても、ARP パケットを破棄せず、ループが発生していましたが、これを修正しました。

6.5 DHCP Snooping の Trusted ポートで、STP の状態が Blocking になっていても、DHCP Discover を破棄せず、ループが発生していましたが、これを修正しました。

6.6 OSPF が設定された IP インターフェースを通じてパケットを送信中に、同 IP インターフェースを削除すると機器が再起動していましたが、これを修正しました。

6.7 DVMRP を使用したマルチキャストルーティング環境において、同一 VLAN に複数のホストが存在するとき、ホストが接続されているポートの 1 つがリンクダウンすると、他のポートに接続されたホストへのマルチキャストトラフィックも一時的に停止することがありましたが、これを修正しました。

6.8 PUBLIC 側からの TCP SYN パケットに対する代理応答機能（TCP セットアッププロキシー）を使用し、PRIVATE 側に位置する HTTP サーバーを PUBLIC 側に公開する場合、アクセスが集中すると PUBLIC から HTTP サーバーにアクセスできなくなることがありましたが、これを修正しました。

6.9 FTP クライアントが FTP アクティブモードを使用したとき、送信した FTP 制御コマンドに対して FTP サーバー側からエラー応答された場合、ファイアウォールが誤ってデー

タコネクションを削除することがあり、その場合 FTP データが破棄されていましたが、これを修正しました。

6.10 ファイアウォール有効時、フラグメントされたマルチキャストパケットを受信してもルーティングしませんでしたが、これを修正しました。

6.11 2 つのファイアウォールポリシーにおいて、複数の VLAN と 1 つの WAN インターフェースとの間で ENAT を使用している場合、片方のポリシーに設定されている外部から内部への通信を許可するルールが動作しないことがありましたが、これを修正しました。

7 本バージョンでの制限事項

ソフトウェアバージョン **2.9.2-14** には、以下の制限事項があります。

7.1 RADIUS

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。

7.2 ZMODEM によるファイル受信

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」**

ZMODEM によるファイル受信中（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。

7.3 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。

○ スクリプトの実行結果を Syslog サーバーに転送すると、20 行分しか送信されません。

7.4 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。

7.5 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。

○ 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。

7.6 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。

7.7 SET ASYN 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」

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）。

7.8 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。

7.9 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、受信した BPDU に 4 Byte のデータを付加して転送します。

7.10 ポートカウンター

参照「コマンドリファレンス」/「スイッチング」/「ポート」

inHdrErrors カウンターは、ヘッダーのチェックサムが誤ったパケットを複数受信した場合でも 1 しかカウントアップされません。

7.11 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」

○ コマンドの入力順によっては、トランクグループ内にタグなしポートとタグ付きポートの両方を所属させてもエラーになりません。これを回避するため、トランクグループの作成は (1) メンバーポートのタグ設定、(2) トランクグループの作成、の順に行ってください。

○ トランキングポート上で LDF 検出を有効にすると、パケットがすべてのトランキングポートから送出されます。

7.12 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。

7.13 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」
参照「コマンドリファレンス」/「スイッチング」/「ポート認証」

LDF 検出機能と 802.1X 認証を併用するときは、デフォルトの Single-Supplicant モードを使ってください。Multi-Supplicant モードは使えません。
（MAC ベース認証には Single-Supplicant モード、Multi-Supplicant モードの区別がないため、本制限は適用されません）

7.14 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。

7.15 バーチャル LAN

参照「コマンドリファレンス」/「スイッチング」/「バーチャル LAN」

○ Protected VLAN の所属ポートをミラーリングのソース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。

○ マルチプル VLAN（Private VLAN）において、プライベートポート配下の端末から本製品への Telnet 接続が可能になっています。

7.16 スパニングツリープロトコル（STP/RSTP）

参照「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）」

○ 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。

○ 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関わらず Topology Change が発生します。

7.17 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」

○ 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。

7.18 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 EMPORT=False を指定すると、IMPORT=True、EMPORT=True の設定で動作します。False で動作させたい場合は、IMPORT、EMPORT 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）。

○ 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。

7.19 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 SERVERTIMEOUT 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 SERVERTIMEOUT より大きく設定した場合は、SERVERTIMEOUT 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 Supplicant 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 の 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 Supplicant の MAC アドレスをゲスト VLAN 上で学習しません。

○ 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。

7.20 DHCP Snooping

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

(8748SL のみ) DHCP Snooping 使用時、接続可能クライアント数 (SET DHCPSNOOPING PORT コマンドの MAXLEASES パラメーター) は、システム全体で 500 以下になるよう設定してください (DHCP Snooping 機能で登録できるクライアントの数は、システム全体で最大 500 クライアントです。20 ページの「8.22 DHCP Snooping」もご参照ください)。

7.21 IP 統計情報

参照「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。

7.22 ディレクティドブロードキャストパケット

参照「コマンドリファレンス」/「IP」

特定 VLAN に対するディレクティ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) 宛てのディレクティ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ドブロードキャストパケットを転送できなくなります。

7.23 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)

参照「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。

7.24 Gratuitous ARP

参照「コマンドリファレンス」/「IP」/「IP インターフェース」

IP インターフェースの設定（ADD/SET IP INTERFACE コマンド）で Gratuitous ARP を受け入れないようにしても、Gratuitous ARP Request パケット受信時には ARP キャッシュを更新します。

7.25 ADD IP ROUTE コマンド

参照「コマンドリファレンス」/「IP」/「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。

7.26 RIP

参照「コマンドリファレンス」/「IP」/「経路制御（RIP)」

ADD/SET IP RIP コマンドの DEMAND パラメーターを YES にした後で再び NO（デフォルト）に戻すと、RIP 経路がタイムアウトしなくなります。

7.27 OSPF

参照「コマンドリファレンス」/「IP」/「経路制御（OSPF)」

- ○ 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（DEFROUTE=OFF が機能しません)。
- ○ ADD/SET OSPF REDISTRIBUTE コマンドで SUBNET=OFF を指定しても、クラスフル、クラスレス両方の経路を取り込みます（SUBNET=OFF が機能しません)。
- ○ 本バージョンでは OSPF の仮想リンクを使用できません。仮想リンクを使用する場合は、バージョン 2.9.1-21 以前のファームウェアをご使用ください。

7.28 DNS キャッシュ

参照「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。

7.29 DNS リレー

参照「コマンドリファレンス」/「IP」/「DNS リレー」

DNS リレーと DNS キャッシュの併用時、あるドメインの IPv6 アドレス（AAAA レコード）が DNS キャッシュに登録されている状態で、DNS クライアントから該当ドメインの IPv4 アドレス（A レコード）に対する問い合わせを受けた場合、キャッシュ済みの IPv6 アドレスを返答してしまいます。またこれとは逆に、あるドメインの IPv4 アドレス（A レコード）がキャッシュされている状態で、該当ドメインの IPv6 アドレス（AAAA レコード）を要求された場合、キャッシュ済みの IPv4 アドレスを返答してしまいます。この事象を回避するには DNS キャッシュ機能を無効化してください。

7.30 DHCP/BOOTP リレー

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

DHCP/BOOTP リレーエージェント機能使用時に、本製品に特定の OS を使用した PC を直接接続して PC を起動すると、DHCP サーバーからの IP アドレスの取得に失敗します。

○ 以下の OS を用いたときには IP アドレスの取得に失敗します。ただし、PC 起動後に IP アドレスを再取得した場合はアドレスの取得が可能です。
- Windows 98
- Windows Vista
- Linux
- Mac OS X

○ 以下の OS を用いたときには IP アドレスは取得可能です。
- Windows 2000
- Windows XP

○ 本現象は PC を直接接続した場合に発生し、HUB やスイッチを経由して接続した場合は発生しません。

○ 本現象は DHCP/BOOTP リレーをおこなうインターフェースに PC を 1 台のみ接続した場合に発生し、複数台の PC を接続した場合は発生しません。

7.31 UDP ブロードキャストヘルパー

参照「コマンドリファレンス」/「IP」/「UDP ブロードキャストヘルパー」

フラグメント化されている UDP ブロードキャストパケットは転送されません。

7.32 IPv6 インターフェース

参照「コマンドリファレンス」/「IPv6」/「IPv6 インターフェース」

○ 6to4 トンネルは、本製品 1 台につき 1 個だけをサポートします。

○ 6to4 トンネルコマンドを保存し、再起動するとエラーメッセージが出力されます。（動作に問題はありません。）

7.33 DVMRP

参照「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ディングされません。

7.34 PIM

参照「コマンドリファレンス」/「IP マルチキャスト」/「PIM」

○ （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）すべてのポートがリンクダウンしている状態で ADD PIM BSRCANDIDATE コマンドを実行すると、警告メッセージが表示されます。

○ （PIM-SM）PIM-SM 使用時、まれに意図しないタイミングでマルチキャスト経路の再登録が発生することがあります。

7.35 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。

○ DISABLE IP IGMP ALLGROUP コマンドで All Group へ所属することを禁止したポートで、IGMP ALL group Query パケットまたは制御用マルチキャストグループアドレス宛てパケットを受信した場合、SHOW IGMPSNOOPING コマンドの All Groups 欄内で「#」が付与された状態で表示されるのが正しい動作ですが、該当ポートは表示されません。

7.36 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 IGMPSNOOPING 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 内にフラッディングされません。

7.37 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。

7.38 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。

○ 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（エンハンスト、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。

○ 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。

○ 本製品自身が送信するパケットにスタティック NAT（1 対 1 のアドレス変換）を適用する場合は、インターフェース NAT のスタティック NAT（NAT=STANDARD）ではなく、ルール NAT のスタンダード NAT（NATTYPE=STANDARD）を使用してください。インターフェース NAT のスタティック NAT では意図したとおりに NAT が行われないことがあります。

8 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。

8.1 8724SL の最大消費電力

参照「取扱説明書」132 ページ

取扱説明書には 8724SL の最大消費電力が「51W」と記載されていますが、正しくは「50W」です。

8.2 フィーチャーライセンスの品番について

参照「コマンドリファレンス」

コマンドリファレンスに記載されているフィーチャーライセンスの品番は次のように読みかえてください。

AT-FL-02	→	AT-FL-02 または AT-FL-02-B
AT-FL-03	→	AT-FL-03 または AT-FL-03-B
AT-FL-08	→	AT-FL-08 または AT-FL-08-B
AT-FL-13	→	AT-FL-13 または AT-FL-13-B

品番末尾の「-B」の有無による機能的な差異はありませんが、「-B」なしのライセンスは販売を終了しているため、新規ご購入時は「-B」付きのライセンスをお買い求めください。

8.3 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。セキュリティーを重視する場合は、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。

8.4 ADD USER コマンド、SET USER コマンド

参照「コマンドリファレンス」/「運用・管理」/「ユーザー認証データベース」

コマンドリファレンスに記載されている ADD USER コマンド、SET USER コマンドの USER パラメーター、PASSWORD パラメーターに使用可能な文字を下記のとおり補足・訂正します。

[USER パラメーター]
誤：
login-name: ログイン名（1 ～ 64 文字。英数字のみ使用可能。大文字小文字を区別しない。空白不可）

正：
login-name: ログイン名（1 ～ 64 文字。大文字小文字を区別しない。空白不可。入力可能文字：!#$%&'()*+,-./0123456789:;<=>@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~）

[PASSWORD パラメーター]
誤：
password: パスワード（1 ～ 32 文字。任意の印刷可能文字を使用可能。大文字小文字を区別する。空白を含む場合はダブルクォートで囲む）

正：
password: パスワード（1 ～ 32 文字。大文字小文字を区別する。空白を使用する場合、全体をダブルクォーテーション (") で囲む。入力可能文字：!#$%&'()*+,-./0123456789:;<=>@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~）

8.5 弊社 CentreNET SwimRadius（Ver.1.1 pl 0 以前）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」

本製品自身（コマンドラインインターフェース）へのログイン認証に弊社 CentreNET SwimRadius の **Ver.1.1 pl 0 以前**を使用する場合は、以下の点にご注意ください。

なお、**Ver.1.1 pl 1 以降**の SwimRadius は、ユーザーごとに Service-Type 属性の有無と値を設定できるようになっているため、下記の制限はありません。

○ **Ver.1.1 pl 0 以前**の SwimRadius は、Telnet で接続してきたユーザーの認証要求に対して Access-Accept（認証成功）を返すとき、Service-Type 属性を付加しますが、同属性の値としてはつねに Administrative(6) をセットするため、**Ver.1.1 pl 0 以前**の SwimRadius によって認証された Telnet ユーザーは、つねに Security Officer レベルでログインすることとなります。

○ **Ver.1.1 pl 0 以前**の SwimRadius は、コンソールポート経由で接続してきたユーザーの認証要求に対して Access-Accept（認証成功）を返すときに Service-Type 属性を付加しません。本製品は Service-Type 属性のない Access-Accept を受信した場合は該当ユーザーのログインを許可しないため、コンソールポート経由のログイン認証を **Ver.1.1 pl 0 以前**の SwimRadius で行うことはできません。

8.6 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。

8.7 CREATE LOG OUTPUT コマンド、SET LOG OUTPUT コマンド

参照「コマンドリファレンス」/「運用・管理」/「ログ」

コマンドリファレンスに記載されている CREATE LOG OUTPUT コマンド、SET LOG OUTPUT コマンドのパラメーター説明を下記のとおり補足・訂正します。CREATE LOG OUTPUT コマンドの QUEUEONLY、MAXQUEUESEVERITY パラメーターは機能しません。

［MAXQUEUESEVERITY パラメーター ］
誤：
QUEUEONLY パラメーターに YES を指定した（キューがいっぱいになるまでログを出力しない）ときに、すぐに出力せずにキューに入れる最大のログレベルを指定する。QUEUEONLY が YES のときは、MAXQUEUESEVERITY よりも低いログレベルのメッセージは、キューの長さが MESSAGES パラメーターの値に達するまでキューイングされる。一方、MAXQUEUESEVERITY 以上のログレベルを持つメッセージが生成されたときは、ただちにキューがフラッシュ（処理）される。OUTPUT パラメーターに TEMPORARY を指定しているときは、本パラメーターは指定できない。デフォルトは 7、すなわちキューがいっぱいにならないうちに処理されるのは、最高のログレベルを持つメッセージが来たときだけとなる。

正：
QUEUEONLY パラメーターに YES を指定した（キューがいっぱいになるまでログを出力しない）ときに、すぐに出力せずにキューに入れる最大のログレベルを指定する。QUEUEONLY が YES のときは、MAXQUEUESEVERITY よりも低いログレベルのメッセージは、キューの長さが MESSAGES パラメーターの値に達するまでキューイングされる。一方、MAXQUEUESEVERITY 以上のログレベルを持つメッセージが生成されたときは、ただちにキューがフラッシュ（処理）される。DESTINATION パラメーターに SYSLOG を指定しているとき、および、OUTPUT パラメーターに TEMPORARY を指定しているときは、本パラメーターは指定できない。デフォルトは 7、すなわちキューがいっぱいにならないうちに処理されるのは、最高のログレベルを持つメッセージが来たときだけとなる。

［MESSAGES パラメーター ］
誤：
DESTINATION が NVS か MEMORY のときは、保存するメッセージの最大数。最大値に達したときは、古いメッセージから順番に削除される。DESTINATION が EMAIL の

場合は、一度に送信されるメッセージの数。DESTINATION が MEMORY のときのデフォルトは 200、EMAIL のときは 100。NVS のときは 20。

正：
DESTINATION が SYSLOG の場合は、キューの長さ。DESTINATION が NVS か MEMORY のときは、保存するメッセージの最大数。最大値に達したときは、古いメッセージから順番に削除される。DESTINATION が EMAIL の場合は、一度に送信されるメッセージの数。DESTINATION が SYSLOG のときのデフォルトは 20、MEMORY のときのデフォルトは 200、EMAIL のときは 100。NVS のときは 20。

[QUEUEONLY パラメーター]
誤：
キューがいっぱいになるまでメッセージを処理しないかどうか。OUTPUT に TEMPORARY を指定した場合は、本パラメーターは指定できない。デフォルトは NO。

正：
キューがいっぱいになるまでメッセージを処理しないかどうか。OUTPUT に TEMPORARY を指定した場合は、本パラメーターは指定できない。DESTINATION に SYSLOG を指定した場合本パラメーターは動作しない。デフォルトは NO。

8.8 SET 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」**

コマンドリファレンスに記載されている SET TELNET コマンドの MAXSESSIONS パラメーターの設定値とパラメーター説明を下記のとおり補足・訂正します。

[MAXSESSIONS パラメーター]
誤：
[MAXSESSIONS=0..30]
同時確立可能な Telnet セッションの最大数。セッション数が最大に達すると、それ以降のセッション確立要求は拒否される。0 を指定すると Telnet 接続が不可となる。なお、コマンド入力時点で確立されているセッション数（SHOW TELNET コマンドの「Telnet Current Sessions」欄）よりも小さい値に設定することはできない。デフォルトは 30。

正：
[MAXSESSIONS=1..32]
MAXSESSIONS: 同時接続可能な Telnet セッション数。ここで設定した値のセッション数になると、次に張ろうとするセッションが破棄される。また、設定する際に確立されているセッション数以下の値は設定できない。デフォルトは 32。

8.9 SHOW 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」**

コマンドリファレンスに記載されている SHOW TELNET コマンドの入力・出力・画面例を下記のとおり補足・訂正します。

[入力・出力・画面例]

誤：

```
Manager > show telnet
TELNET Module Configuration
-----------------------------------------
Telnet Server .................. Enabled
Telnet Server Listen Port ...... 23
Telnet Terminal Type ........... UNKNOWN
Telnet Insert Null's ........... Off
Telnet Com Port Control ........ Disabled
Telnet Current Sessions ........ 0
Telnet Session Limit ........... 30
Telnet Idle Timeout ............ Off
-----------------------------------------
```

正：

```
Manager > show telnet
TELNET Module Configuration
-----------------------------------------
Telnet Server .................. Enabled
Telnet Server Listen Port ...... 23
Telnet Terminal Type ........... UNKNOWN
Telnet Insert Null's ........... Off
Telnet Com Port Control ........ Disabled
Telnet Current Sessions ........ 0
Telnet Session Limit ........... 32
Telnet Idle Timeout ............ Off
-----------------------------------------
```

8.10 送信元アドレスがマルチキャスト MAC アドレスの Ethernet フレーム

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

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 MAC 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。
ただし、ENABLE IP MACDISPARITY コマンドを実行した上で、マルチキャスト MAC アドレスのスタティック ARP エントリーを登録すれば、このマルチキャスト MAC アドレスを送信元とする Ethernet フレームを転送させることが可能です。

8.11 スイッチポートの統計カウンター（8748SL のみ）

参照「コマンドリファレンス」/「スイッチング」/「ポート」

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。

8.12 1000Mbps ポートのフラッディングレート

参照「コマンドリファレンス」/「スイッチング」/「ポート」

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。

8.13 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。

8.14 ポート帯域制限機能の受信レート上限値とハードウェア IP フィルター

参照「コマンドリファレンス」/「スイッチング」/「ポート」

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」

ポート帯域制限機能の受信レート上限値（INGRESSLIMIT）とハードウェア IP フィルターを併用している場合、ハードウェア IP フィルターの NODROP エントリーにマッチしたパケットに対して、受信レート上限値が適用されないことがあります。これを回避するには、EDIT コマンドで設定ファイルを開き、受信レート上限値の設定コマンド（SET SWITCH PORT=x INGRESSLIMIT=x）がハードウェア IP フィルター設定コマンドの後にくるよう編集するか、あるいは、次のような再起動トリガーを定義して、起動時に受信レート上限値の設定が自動的に再入力されるようにしてください。

再起動トリガーの設定例

```
ENABLE TRIGGER
CREATE TRIGGER=1 REBOOT=ALL SCRIPT=INGRESS.SCP
```

トリガースクリプト INGRESS.SCP の例

```
SET SWITCH PORT=1 INGRESSLIMIT=1000
```

8.15 ダイナミック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」

ダイナミックポートセキュリティー使用時（RELEARN=ON）、スイッチポートがロックされた後に、ADD SWITCH FILTER コマンドでスタティックエントリーを追加するとき、ENTRY パラメーターを省略するとエントリー番号が 0 から始まらず、結果的に設定保存後の再起動時にエラーが発生することがあります。これを回避するため、スイッチポートのロック後にスタティックエントリーを追加するときは、ENTRY パラメーターに 0 から始まる番号を指定してください。

8.16 LDF 検出

参照「コマンドリファレンス」/「スイッチング」/「ポート」

配下の HUB やスイッチにて輻輳などにより LDF が消失した場合、ループを検出できない場合があります。

8.17 マルチプルスパニングツリープロトコル（MSTP）

参照「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。

8.18 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。

8.19 QoS

参照「コマンドリファレンス」/「スイッチング」/「QoS」

本体より送出される制御パケットは、すべて「キュー番号 : 3」を使用します。「キュー番号 : 3」はデフォルトのユーザープライオリティーが「6、7」となっていますが本体より送出される制御パケットは、ユーザープライオリティーを変更しても、常に「キュー番号 : 3」を使用し、優先的に送出されます。本体発の制御パケットはユーザープライオリティーの変更ができません。

8.20 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）。

8.21 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、ポートトランキング、スパ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。

8.22 DHCP Snooping

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

○ コマンドリファレンスに記載されている SHOW DHCPSNOOPING DATABASE コマンドの表示項目説明を下記のとおり補足・訂正します。

〔Entries with client lease but no listeners セクション〕
誤：
CLASSIFR モジュールとの連携がうまくいかなかったなどの理由で現在無効となっているクライアントの登録情報が表示される

正：
DHCP サーバーからの DHCP ACK パケットが DHCP クライアントに転送されたが、該当する Listener（CLASSIFIER）が存在しない、もしくは CLASSIFIER モジュールに何らかの問題が発生したためそれが利用できない場合に、クライアントの登録情報が表示される

〔Entries with no client lease and no listeners セクション〕
誤：
DHCP メッセージに問題があったなどの理由で現在無効となっているクライアントの登録情報が表示される

正：
DHCP メッセージに問題があったなどの理由で、DHCP サーバーからの DHCP ACK パケットが DHCP クライアントに転送されなかった場合に、クライアントの登録情報が表示される

○ DHCP Snooping 機能で登録できるクライアントの数は次のとおりです。

8724SL はポート 1 ～ 8、9 ～ 16、17 ～ 24、25、26 の 5 つ、8748SL はポート 1 ～ 8、9 ～ 16、17 ～ 24、15 ～ 32、33 ～ 41、42 ～ 48、49、50 の 8 つのブロックごとに、それぞれ最大 100 クライアントまで登録できます。システム全体では、最大 500 クライアントまで登録できます。

なお、本機能はハードウェア IP フィルター（L3 フィルター）と記憶領域を共有しているため、本機能の使用によってハードウェア IP フィルターの設定可能数が増減します。

DHCP Snooping を有効にすると、ハードウェア IP フィルターのマッチ条件（フィルター）を 2 個消費します。また、オプション機能の ARP セキュリティーを使用すると、さらに 1 個消費します（合計 3 個）。作成可能なマッチ条件はシステム全体で 14 個ですので、ご注意ください。

8.23 ICMP TTL Exceeded メッセージの送出インターフェース

参照「コマンドリファレンス」/「IP」

ICMP TTL Exceeded メッセージは、（他のインターフェース上に最適経路が存在していても）TTL=1 の IP パケットを受信したインターフェースから送出されます。

8.24 ICMP Echo Request パケット

参照「コマンドリファレンス」/「IP」

本体宛 ICMPv4/v6 Echo Request パケットの ICMP チェックサムフィールド値が「0xffff」である場合、同フィールドの値が「0x0000」であると見なしてチェックサムを検証します。

8.25 SET OSPF コマンド

参照「コマンドリファレンス」/「IP」/「経路制御（OSPF)」

SET OSPF コマンドの RIP パラメーターに EXPORT か BOTH を指定し、OSPF の経路情報を RIP 経路に取り込む設定をした場合、元となる OSPF 経路のメトリック値によって RIP で通知される経路のメトリック値は次のようになります。

- OSPF メトリック値が 8 未満の場合：RIP でもそのまま通知
- OSPF メトリック値が 8 以上の場合：RIP ではメトリック値を 8 に固定して通知

8.26 ADD BGP PEER コマンド、SET BGP PEER コマンド

参照「コマンドリファレンス」/「IP」/「経路制御（BGP-4)」

コマンドリファレンスに記載されている ADD BGP PEER コマンド、SET BGP PEER コマンドの REMOTEAS パラメーターの設定値を下記のとおり訂正します。

［REMOTEAS パラメーター］
誤：
REMOTEAS=1..65534

正：
REMOTEAS=1..65535

8.27 SET IP AUTONOMOUS コマンド

参照「コマンドリファレンス」/「IP」/「経路制御（BGP-4)」

コマンドリファレンスに記載されている SET IP AUTONOMOUS コマンドの AUTONOMOUS パラメーターの設定値を下記のとおり訂正します。

［AUTONOMOUS パラメーター］
誤：
AUTONOMOUS=1..65534

正：
AUTONOMOUS=1..65535

8.28 DNS キャッシュ

参照「コマンドリファレンス」/「IP」/「名前解決」

コマンドリファレンスに記載されている名前解決概要の DNS キャッシュを下記のとおり補足・訂正します。

〔DNS キャッシュ〕
誤：
■キャッシュエントリーの有効期限は SET IP DNS CACHE コマンドの TIMEOUT パラメーターで設定します。有効範囲は 1 ～ 60 分。デフォルトは 30 分です。
SET IP DNS CACHE TIMEOUT=15

正：
■キャッシュエントリーの最大有効期限は SET IP DNS CACHE コマンドの TIMEOUT パラメーターで設定します。有効範囲は 1 ～ 60 分。デフォルトは 30 分です。
SET IP DNS CACHE TIMEOUT=15

Note-DNS サーバーからの応答に含まれる有効期限が本パラメーターで設定した値よりも大きかった場合に本設定の時間が適用されます。

8.29 SET IP DNS CACHE コマンド

参照「コマンドリファレンス」/「IP」/「名前解決」

コマンドリファレンスに記載されている SET IP DNS CACHE コマンドのコマンド説明と TIMEOUT パラメーターの説明を下記のとおり訂正します。

〔コマンド説明〕
誤：
DNS キャッシュに保持するエントリーの最大数と、キャッシュエントリーの有効期限を変更する。

正：
DNS キャッシュに保持するエントリーの最大数と、キャッシュエントリーの最大有効期限を変更する。

〔TIMEOUT パラメーター〕
誤：
DNS キャッシュエントリーの有効期限。キャッシュに登録後、有効期限内に更新されなかったエントリーは削除される。デフォルトは 30 分。

正：
DNS キャッシュエントリーの最大有効期限。DNS サーバーからの応答に含まれる有効期限が本パラメーターで設定した値よりも大きかった場合に適用される。キャッシュに登録後、有効期限が経過するとエントリーは削除される。デフォルトは 30 分。

8.30 Ping ポーリング

参照「コマンドリファレンス」/「IP」/「Ping ポーリング」

コマンドリファレンスに記載されている ADD PING POLL コマンド、DELETE PING POLL コマンド、DISABLE PING POLL コマンド、DISABLE PING POLL DEBUG コマンド、

ENABLE PING POLL コマンド、ENABLE PING POLL DEBUG コマンド、RESET PING POLL コマンド、SET PING POLL コマンド、SHOW PING POLL コマンドの POLL パラメーターの設定値を下記のとおり訂正します。

〔POLL パラメーター〕
誤：
poll-id: Ping ポーリング ID（1 ～ 100）
正：
poll-id: Ping ポーリング ID（1 ～ 250）

8.31 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。

8.32 ルーター通知（RA）

参照「コマンドリファレンス」/「IPv6」/「近隣探索」

システム再起動により IPv6 インターフェースがダウンした場合は、Lifetime=0 のルーター通知（RA）パケットを送信しません。

8.33 PIM

参照「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。これを避けるには、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=SENDC
```

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

参照「コマンドリファレンス」/「スイッチング」/「ポート」

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

参照「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。

8.35 SHOW IGMPSNOOPING コマンド

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

SHOW IGMPSNOOPING コマンドで COUNTERS オプションを指定するときは、次の書式にしがたい VLAN オプションを同時に指定してください。
（VLAN は COUNTERS よりも前に指定する必要があります）

```
SHOW IGMPSNOOPING VLAN={vlanname|1..4094|ALL} COUNTERS
```

9 サポートリミット一覧

パフォーマンス	
VLAN 登録数	255
MAC アドレス（FDB）登録数	8K
IPv4 ホスト（ARP）登録数	2K
IPv4 ルート登録数	2K※1
リンクアグリゲーション	
グループ数（筐体あたり）	6
ポート数（グループあたり）	8
ハードウェアパケットフィルター	
マッチ条件フィルター登録数	14
フィルターエントリー登録数	124
認証端末数	
認証端末数（ポートあたり）	480
認証端末数（装置あたり）	480
マルチプルダイナミック VLAN（ポートあたり）	-
マルチプルダイナミック VLAN（装置あたり）	-
ローカル RADIUS サーバー	
ユーザー登録数	-
RADIUS クライアント（NAS）登録数	-
その他	
VRF-Lite インターフェース数	-
IPv4 マルチキャストルーティングインターフェース数	32

※ 表中では、K=1024
※1 インターフェース経路、スタティック経路、ダイナミック経路など、各種経路情報を含めた登録数です。

10 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。

なお、以下の一覧に記載がなくても、最新のコマンドリファレンスに記載されていない機能、コマンドはサポート対象外ですので、あらかじめご了承ください。最新マニュアルの入手先については、次節「最新マニュアルについて」をご覧ください。

○ 以下のキーワードを含む全コマンド
ENABLE、ADD、SET、SHOW などの後に [?] キーを押すと表示される機能別キーワードです。

ACC, APPLETALK, BRI, CLASSIFIER, CLNS, DHCP6, EPSR, ETH, FRAMERELAY, GARP, GRE, GUI, HTTP, IPSEC, ISAKMP, ISDN, L2TP, LAPB, LAPD, LDAP, LLDP, LOADBALANCER, LB, LPD, MACFF, MIOX, PKI, PKT, PRI, Q931, RSVP, SA, SERVICE, SKEY, SSL, STACK, STAR, STARTUP, STREAM, STT, SYN, TACACS, TACPLUS, TEST, TPAD, 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/MODIFY
SET/START/STOP PKT
SHOW BUFFER [SCAN[=ADDRESS] [QUEUEPOINTERS]]
SHOW SYSTEM TEMPERATURE
SET SYSTEM HOSTID
SET SYSTEM TERRITORY
SET SYSTEM DISTINGUISHEDNAME
LOAD [METHOD=LDAP] [ATTRIBUTE] [BASEOBJECT]
TRACE [ADDRONLY]
PING [APPLEADDR] [OSIADDRESS] [SAPPLEADDRESS] [SOSIADDRESS]
SET PING [APPLEADDR] [OSIADDRESS] [SAPPLEADDRESS] [SOSIADDRESS]
PURGE FILE TRANSLATIONTABLE
PURGE PING TOTALLY
SET/SHOW SWITCH SOCK
SHOW SWITCH MEMORY
SHOW SWITCH SWTABLE
SET SWITCH PORT [MULTICASTMODE] [SPEED={xxxMHAUTO ¦ xxxMFAUTO ¦ 1000MHALF}]
DISABLE/ENABLE SWITCH BIST
SET VLAN VIRTACTIVATION
ADD/DELETE/SET IP FILTER [PRIORITY]
ADD/SET IP ROUTE FILTER [POLICY] [PROTOCOL={STATIC ¦ INTERFACE}]
ADD/DELETE/DISABLE/ENABLE/SET/SHOW IP EGP
ADD/DELETE/SET/SHOW IP SA
ADD/SET IP INTERFACE [VJC] [PRIORITYFILTER] [MULTICAST] [IGMPPROXY]
ADD/DELETE/SET IP ROUTE BLACKHOLE
ADD/SET IP RIP [NEXTHOP]
SET IP RIP NEWIPADDRESS

SET IP ARP [DLCI] [CIRCUIT]
CREATE/DESTROY/SHOW IP POOL
SHOW IP ROUTE [CACHE]
SHOW IP CACHE
SHOW IP ROUTE TEMPLATE
SET/SHOW IP FLOW
DISABLE/ENABLE IP FOFILTER
DISABLE/ENABLE IP MULTICASTSWITCHING
DISABLE/ENABLE IP SRCROUTE
ADD IP ROUTEMAP [MATCH TAG]
ADD IPV6 INTERFACE IPADDRESS={DHCP¦DHCPTEMP¦PD} [APPINT] [HINT] [KEY] [PRIORITYFILTER] [TYPE=ANYCAST]
SET IPV6 INTERFACE [PRIORITYFILTER]
ADD/SET IPV6 FILTER [PRIORITY]
DISABLE/ENABLE IPV6 FLOW
ADD/SET PIM6 INTERFACE [MODE=DENSE] [SRCAPABLE]
SET PIM6 [SOURCEALIVETIME] [SRINTERVAL]
SHOW PIM6 [STATEREFRESH]
ADD/DELETE/SET DVMRP [DLC]
ADD/DELETE/SET DVMRP INTERFACE [DLC]
DISABLE/ENABLE ENCO COMPSTATISTICS
SHOW ENCO CHANNEL
SHOW ENCO COUNTER={DES ¦ HMAC ¦ JOBPROCCESSING ¦ PRED ¦ STAC ¦ USER ¦ UTIL}
SHOW IPX CALLLOG
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
ADD/SET PIM INTERFACE [SRCAPABLE] [DLCI]
DELETE PIM INTERFACE [SRCAPABLE]
SHOW PIM [STATEREFRESH]
ADD/SET PIM BSRCANDIDATE [HASHMASKLENGTH]
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] [STACCHECK] [TERMINATE] [TYPE]
ADD/DELETE/SET PPP ACSERVICE
ADD/DELETE/DISABLE/ENABLE/SET PPP TEMPLATE

ADD/DELETE PPP MAXSESSIONS
ADD/DELETE PPP ACRADIUS
ADD/DELETE PPP VLAN
DISABLE/ENABLE PPP ACCESSCONCENTRATOR
ACTIVATE PPP RXPKT
SET BOOTP MAXHOPS
DISABLE/ENABLE DHCP [BOOTP]
DISABLE/ENABLE DHCPSNOOPING STRICTUNICAST
ADD/DELETE DHCPSNOOPING BINDING [ROUTER]
ADD/DELETE/ENABLE/SHOW DHCPSNOOPING XLA
DISABLE/ENABLE DHCPSNOOPING IPFILTERING
DISABLE/ENABLE DHCPSNOOPING LOG
SET DHCPSNOOPING ARPSECURITY [ACTION={NONE|DISABLE}]
ENABLE DHCPSNOOPING BLOCK={ALL|IP}
DISABLE/ENABLE BGP DAMPING
CREATE/SET BGP DAMPING PARAMETERSET
ADD/SET IP RIP REDISTRIBUTE [ROUTEMAP] [LIMIT] [METRIC] [SUBNET]
ADD/SET OSPF REDISTRIBUTE [ROUTEMAP]
ADD/SET OSPF AREA [NSSATRANSLATOR] [NSSASTABILITY]
ADD/CREATE/DELETE/DESTROY/SHOW FIREWALL POLICY DYNAMIC
ADD/DELETE FIREWALL POLICY HTTPFILTER
ADD FIREWALL POLICY INTERFACE [TRUSTPRIVATE]
ADD/DELETE FIREWALL POLICY PROXY
ADD/SET FIREWALL POLICY RULE [ENCAPSULATION]
[NATTYPE={ENAPT|NATP}] [TTL]
ADD/DELETE FIREWALL POLICY SPAMSOURCES
ADD/DELETE/SET/SHOW FIREWALL POLICY UDPPORTTIMEOUT
DISABLE/ENABLE FIREWALL POLICY HTTPCOOKIES
DISABLE/ENABLE FIREWALL POLICY SMTPRELAY
DISABLE/ENABLE/SET/SHOW FIREWALL SIPALG
RESET/SHOW FIREWALL POLICY MACCACHE
SET FIREWALL POLICY [FTPDATAPORT] [ICMPUNREACHABLETIMEOUT]
[MACCACHETIMEOUT] [RADIUSLIMIT]
SET FIREWALL POLICY SMTPDOMAIN
SHOW FIREWALL POLICY USER
ADD/DELETE/DISABLE/ENABLE/SET/SHOW FIREWALL MONITOR
ADD/DELETE/SET/SHOW FIREWALL POLICY LIMITRULE
ADD/DELETE FIREWALL POLICY NAT={ENAPT}
DISABLE/ENABLE FIREWALL SESSIONREPORT
RESET FIREWALL SIPALG AUTOCLIENTS
RESET FIREWALL SIPALG COUNTER
SET FIREWALL POLICY ATTACK
ADD/DELETE IGMPSNOOPING VLAN ROUTERPORT
SET IGMPSNOOPING VLAN QUERYSOLICIT
ENABLE/SET PORTAUTH[=8021X] [AUTOAUTHENTICATE]
DISABLE/ENABLE SWITCH LOOPDETECTION={BOTH|BCCOUNTER}
DISABLE/ENABLE SWITCH LOOPDETECTION DEBUG
SET SWITCH LOOPDETECTION=BCCOUNTER

SHOW SWITCH LOOPDETECTION=BCCOUNTER
SET/CLEAR TIMEZONE
SHOW TIME RTC

11 最新マニュアルについて

最新の取扱説明書「CentreCOM 8724SL/8748SL 取扱説明書」（J613-M0019-00 Rev.A）、「CentreCOM 8724SL V2 取扱説明書」（613-000900 Rev.A）、および、最新のコマンドリファレンス「CentreCOM 8700SL シリーズ コマンドリファレンス 2.9」（J613-M0019-01 Rev.P）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、これらの最新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、弊社ホームページで最新の情報をご覧ください。

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