CentreCOM 9100/8500 シリーズ リリースノート

ファームウェア バージョン 4.1.10

このたびは CentreCOM 9100/8500 シリーズ（以下、「C9100/8500」または「本製品」と略記）をお買い上げいただき、誠にありがとうございます。本リリースノートは、本製品に付属する他のドキュメント類を補足・訂正するものです。ご使用前に必ずご一読ください。

目次

1. 必要動作環境

ファームウェア バージョン 4.1.10 を使用するには、32MB のメモリが必要です。C9108 と C8518 の初期モデルには実装メモリ 16MB のものがありますが、これらの筐体で本バージョンをご利用いただくにはメモリのアップグレードが必要となります。以前のバージョンからファームウェアをアップグレードする場合は、最初に下記の要領でメモリ容量を確認してください。メモリのアップグレードサービスについては、販売代理店または弊社営業部までご相談ください。

メモリ容量を調べるには、show memory コマンドを使います。「Total DRAM Size」（図の二重下線部）に「16777216(16MB)」と表示される場合、または、「current free」と「current alloc」の bytes 値（図の一重下線部）の合計が「16000000」に満たない場合はメモリのアップグレードが必要となります(表示内容はバージョンによって若干異なります。図はV2.1.10での例です)。

```
* C8500:3 # show memory

System Memory Information
-------------------------
Total DRAM Size: 33554432 (32MB)

 status   bytes    blocks   avg block  max block
 ------ --------- -------- ---------- ----------
current
   free  20749088        3    6916362  20665632
  alloc   7488928      242      30945         -
・・・・・・(以下省略)
```


PN J613-M6673-02 Rev.C 990914
FN RelNo-4.1.10.fm

2. 本バージョンで追加 / 強化された機能

本バージョンでは、以下の機能が追加または強化されました。詳細については、かっこ内に記載した「CentreCOM 9100/8500 シリーズ ユーザーガイド ファームウェア V4.1」（J613-M6673-00 Rev.B）の該当箇所をご参照ください。

- **ERRP** ― 複数の C9100/8500 を連携させることによりデフォルトゲートウェイ（ルータ）の多重化を実現します（第 13 章「ERRP」）。
- **アクセスポリシー** ― ダイナミックルーティングプロトコルによる経路情報のやりとりに対してフィルタをかけることができます（第 14 章「アクセスポリシー」）。
- **IPX ルーティング** ― IPX パケットのスタティックおよびダイナミック（RIP/SAP）ルーティングが可能になりました（第 12 章「IPX ルーティング」）。
- **PIM-DM** ― IP マルチキャストルーティングプロトコルに PIM-DM が追加されました（第 11 章「IP マルチキャストルーティング」）。
- **サブネット内QoS(ISQ)** ― ルーティングを必要としない同一サブネット内のIPトラフィックに対しても IP QoS を適用できるようになりました（8-9 ページ「サブネット内 QoS（ISQ）」）。
- **VLAN アグリゲーション** ― サブ VLAN 間でデフォルトゲートウェイアドレスを共用し、IP アドレススペースを有効活用します（5-14 ページ「VLAN アグリゲーション機能」）。
- **OSPF 機能強化** ― IR（内部ルータ）、ABR（エリア境界ルータ）に加え、ASBR（AS 境界ルータ）としての使用が可能になりました。また、準スタブエリア（NSSA）のサポートが追加されました（第 10 章「ルーティングプロトコル」）。
- **L2 モデル（C8525/8550）サポート機能強化** ― 本バージョンから、L2 モデルでも基本的な IP ルーティング機能（スタティックおよび RIP）を使用できるようになりました。ただし、OSPF、DVMRP、PIM-DM、IPX ルーティング等を使用するには別売の L3 キーが必要です（第 1 章「本製品の概要」）。
- **UDP フォワーディング** ― 特定 L4 ポート宛ての UDP ブロードキャストパケットを、あらかじめ指定した IP アドレスまたは VLAN に転送します。既存の DHCP/BOOTP リレー機能よりもきめの細かいコントロールが可能です（9-11 ページ「UDP フォワーディング」）。
- **RADIUS クライアント** ― RADIUS 認証サーバを利用したユーザアカウントの一元管理が可能になりました（3-24 ページ「RADIUS クライアント」）。
- **DNS クライアント** ― 一部のコマンドで、ホスト・ドメイン名による指定ができるようになりました（3-19 ページ「DNS クライアントの設定」）。
- **SNTP クライアント** ― NTP サーバを利用してシステムクロックを自動調整する機能が追加されました（3-21 ページ「SNTP クライアントの設定」）。
- **ログ機能強化** ― CLI からの設定変更をログに記録する機能が追加されました（15-10 ページ「設定変更ログ機能」）。
- **CLI 機能強化** ― CLI でコマンド出力の一時停止をオン / オフできるようになりました（3-5 ページ「ページャー機能」）。

3. 本バージョンで制限が解除された項目

本バージョンでは、前バージョン（2.1.10）における制限事項のうち、下記の項目が制限解除されました（かっこ内は「リリースノート バージョン 2.1.10」（J613-M6673-02 Rev.B）の該当項目を示します）。

- `upload configuration` コマンドで、Proxy ARP エントリと IP QoS の設定情報が正しくアップロードされるようになりました（2 ページ「設定アップロード時の注意点」）。
- Rx ポートだけでなく、Tx ポート切断時にもリダンダントポートが切り替わるようになりました（3 ページ「リダンダントポートの切り替わり条件」）。
- `show ports info` コマンドで、GBIC-LX ポートの Port Type と 10/100M ポートの Actual Mode が正しく表示されるようになりました（3 ページ「show ports info コマンド」）。
- `upload/show configuration` コマンドで、スマートリダンダンシー機能の設定情報が正しくアップロード / 表示されるようになりました。また、`show ports info` コマンドで、リダンダントポートに関する情報が正しく表示されるようになりました（5 ページ「スマートリダンダンシー機能とリダンダントポート」）。
- Internet Explorer 4.0 上で 30 文字を超える STPD 名が正しく表示されるようになりました（5 ページ「IE4.0 で長い STPD 名が表示されない」）。
- Web インタフェース上でログを表示させるとブラウザがハングしたような状態になる問題が解消されました（5 ページ「ログ表示中にブラウザがハングしたように見える」）。
- ロードシェアリングと STP を併用できるようになりました（6 ページ「ロードシェアリング」）。
- `config igmp <query_interval> <query_response_interval> <last_member_query_interval>` コマンドで、IGMP タイマーを変更できるようになりました（10 ページ「IGMP タイマー」）。
- STP イネーブル時にコールドスタートトラップが送信されない問題を修正しました（11 ページ「コールドスタートトラップと STP」）。
- 特定の条件下で SNMP マネージャから C9100/8500 の SNMP エージェントにアクセスできない問題を修正しました（11 ページ「SNMP マネージャとデフォルトゲートウェイ」）。

4. 使用できない機能

4.1 XMODEM によるファームウェアのダウンロード

本バージョンでは、XMODEM プロトコルによるコンソールポート経由でのファームウェアのダウンロード（`download image xmodem` コマンド）ができません。コンソールポート経由でファームウェアをダウンロードする必要があるときは、16 ページの「BootROM 機能」を参照してください。

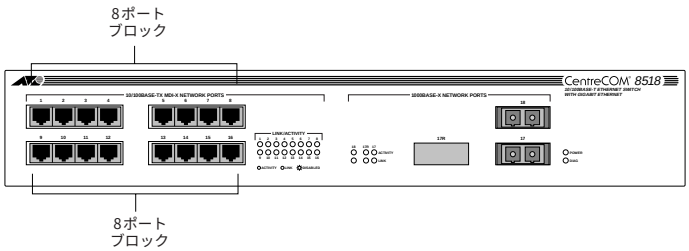
5. ユーザーガイドの訂正

「CentreCOM 9100/8500 シリーズ ユーザーガイド ファームウェア V4.1」(J613-M6673-00 Rev.B) に誤記がありました。ここに訂正し深くお詫びいたします。

5.1 C8518 における ERRP ポートの組み合わせ（ユーザーガイド P13-5、図 13-1）

ユーザーガイド 13-5 ページの図 13-1（「C8518 における ERRP ポートの組み合わせ」）を下記のとおり訂正します。C8518 では、上段の 8 ポート（ポート 1 ～ 8）と下段の 8 ポート（ポート 9 ～ 16）でそれぞれ ERRP のポートブロックを形成します。

図 13-1：C8518 における ERRP ポートの組み合わせ



5.2 sysName は 32 文字以内（ユーザーガイド P3-18 ～、表 3-8）

ユーザーガイドには sysName の最大文字数が 255 文字と記載されていますが、これは 32 文字の誤りです（本バージョンから文字数が変更されました）。

6. 使用上の注意と既知の問題点

このセクションでは、本製品を使用する際の注意事項および制限事項について説明します。

6.1 セキュリティ

6.1.1 サービス不能攻撃への対処法

送信元 IP アドレスを偽造した ICMP パケットや UDP パケットを利用してターゲットおよび中継ネットワーク上のサービスを妨害するサービス不能攻撃（'smurf' や 'fraggle' など）を防ぐには、次のコマンドを使って IP ブロードキャストパケットの転送をディセーブルにしてください。

```
disable ipforwarding broadcast vlan <name>
```

smurf では ICMP エコー要求（ping）パケットが、fraggle では echo（7/udp）や chargen（19/udp）が利用されます。これらの攻撃については、下記の URL 等を参考にしてください。

```
http://users.quadrunner.com/chuegen/smurf.txt
```

6.1.2 Telnet および Web アクセス

Telnet アクセスと Web アクセスはデフォルトでイネーブルになっています。セキュリティを重視する場合は、これらのサービスをディセーブルにするか、RADIUS サーバによるログイン認証を検討してください。

6.1.3 SNMP アクセス

SNMP アクセスはデフォルトでイネーブルになっています。また、Read-only コミュニティ名として「public」が、Read-write コミュニティ名として「private」が設定されています。セキュリティを重視する場合は、SNMP アクセスをディセーブルにするか、ネットワークマネージャの IP アドレスをアクセスリストに登録して、SNMP アクセスを許可するホストを制限してください。また、デフォルトのコミュニティ名を必ず変更するようにしてください。ネットワークマネージャをアクセスリストに登録するには、次のコマンドを使います。

```
config snmp add <ipaddress> {<mask>}
```

6.1.4 ユーザアカウントデータベース

出荷時には、管理者レベルの *admin* と一般ユーザレベルの *user* がユーザアカウントデータベースに登録されています。これらのアカウントにはパスワードが設定されていません。必ずパスワードを設定してからご使用ください。また、セキュリティを重視する場合は、RADIUS 認証サーバの使用を検討してください。なお、ユーザアカウントデータベースには、最低 1 つ管理者レベルのアカウントが必要です。

6.2 コマンドラインインタフェース（CLI）

6.2.1 設定保存について

電源オフ後や再起動後も設定が消えないようにするには、設定変更後に `save` コマンドを実行する必要があります。`save` コマンドの詳細については、『CentreCOM 9100 / 8500 シリーズ ユーザーガイド』の第 16 章をご覧ください。

6.2.2 show diagnostics コマンド

`show diagnostics` コマンドは、コールドスタート時に実行される電源投入時テスト（POST）の結果を表示するものです。ウォームブート後（`reboot` コマンドで再起動した後）に `show diagnostics` コマンドを実行しても、何も表示されません。

6.2.3 Telnet セッションタイムアウト時の動作

`idletimeouts`によってTelnetセッションがタイムアウトすると、次のTelnetセッション確立時にコンソールポートに接続したターミナルでセッションが一時的にハングした状態になります。当該 Telnet セッションを終了すれば、コンソールセッションは正常に戻ります。また、これ以降は新たに Telnet セッションを開始しても問題は起きません。

6.2.4 create/config account コマンドの encrypted オプション

`create account`および`config account`コマンドの`encypted`オプションは、設定ファイルのアップロード / ダウンロード時にパスワードが平文のまま送られることを避けるためのものです（本製品が使用）。ユーザが使用するものではありませんのでご注意ください。

6.2.5 ping コマンド実行中のエラーメッセージについて

リモートホストからの応答がない場合、ping コマンドはデフォルトの 4 パケット送信後にいったん統計情報を表示しますが、それ以降もエコーパケットの送信を続けます。これを中断するには、「Return」キーを押してください。中断後、あらためて完全な統計情報が表示されます。

ping がリダイレクトされた場合、最後のパケットは正常に受信しても Lost と表示されます。

ping 実行中に Echo Reply 以外の ICMP メッセージ（IRDP、Time To Live expired、destination unreachable など）を受信すると、コンソール画面にエラーメッセージが表示されますが、このエラーメッセージは無視してかまいません。

6.2.6 設定ファイル読み込み時のエラーメッセージ

設定ファイルの読み込み中に表示されるエラーメッセージは無視してかまいません。

6.2.7 CLI から他ホストへの Telnet 時にコンソールがロックする

コマンドラインインタフェースから他ホストへの Telnet 接続時、リモートホストが反応しないとコンソールがハングした状態になります。この場合は、「Ctrl」＋「]」キーを押して、ロックした Telnet セッションを強制終了させてください。

6.2.8 show config コマンドの出力

`show config` コマンドでは、ページャー機能が働かず、すべての情報が一度に出力されます。これは、ターミナルソフトで出力をログにキャプチャ保存することを想定しているためです。

6.2.9 端末設定

ご使用のアプリケーションの端末設定メニューでVT-100が選択されていることを確認してください。また、画面の自動更新時に正しい表示が行われるよう、画面を最大化してください。

6.3 ポート関連

6.3.1 ギガビットポートのオートネゴシエーションをオフにする

対向機器が 802.3z 準拠のオートネゴシエーションに対応していない場合は、ギガビットポートのオートネゴシエーションをオフにする必要があります。オートネゴシエーションをオフにするときは、次のように通信モード（full / half）を明示的に指定しなくてはなりません。

```
config ports 25 auto off duplex full
```

6.3.2 フロー制御

フロー制御はギガビットポートでのみサポートされています。フロー制御のイネーブル / ディセーブルは、オートネゴシエーションのオン / オフと連動しています。フロー制御の設定を確認するには、`show ports configuration` コマンドを使います。

6.3.3 スマートリダンダンシー機能（C9108 を除く）

リダンダントギガビットポートを使ってデュアルホーム接続している場合、スマートリダンダンシー機能をディセーブルに設定すると、起動時にプライマリ / セカンダリのどちらのポートがアクティブになるかを予測できません（先に初期化が完了したポートがアクティブになります）。この動作が都合悪いときは、次のコマンドを実行してスマートリダンダンシー機能をイネーブルにしてください（デフォルトはイネーブル）。

```
enable smartredundancy <portlist>
```

スマートリダンダンシーがイネーブルのときは、つねにプライマリポートが優先的に使用されます。つまり、プライマリポートがリンクアップしているときは、つねにプライマリポートがアクティブになり、リダンダントポートは待機状態になります。

6.3.4 ロードシェアリング使用時の注意

ロードシェアリング構成時は、対向するロードシェアリングポート間にリピータなどをはさまず、C9100 / 8500 同士を直接接続してください。

6.4 ポートミラーリング

6.4.1 VLAN ミラーリングとロードシェアリング

VLAN ミラーリング（またはポート / VLAN ミラーリング）とロードシェアリングを同時に使用することはできません。このようなミラーリングの設定を行うと、ロードシェアリンググループではマスターポートしか使用されなくなり、障害発生時のリンク切り替えが正常に動作しなくなります。また、マスターポートがダウンした場合、ロードシェアリンググループを通過するトラフィックがミラーポートにコピーされなくなります。上記のミラーリングエントリを削除すると、この問題は解消します。

6.4.2 IP マルチキャストトラフィックのミラーリング

IGMP スヌーピングの働きによって、マルチキャストトラフィックがミラーポートにコピーされなくなる場合があります。このようなときは、ミラーポートに対して `restart` コマンドを実行するか、ミラーポートのケーブルを抜き差しすると、`IGMP host_timeout` パラメータ（デフォルト 260 秒）に設定された時間の経過後に、マルチキャストトラフィックのミラーリングが再開されます。

6.4.3 MAC ミラーリング

本バージョンでは、MAC アドレスベースのポートミラーリングが正しく機能しません。

6.4.4 ポートミラーリング使用時のパフォーマンス

ラインレートで動作中のギガビットポートに対してミラーリングを行うと、トラフィックのスループットが約 30％低下します。

6.4.5 ポートミラーリングと 802.1Q タグ

ミラーリング使用時、タグ付きポートから送出されるトラフィックはミラーポートにタグなしの状態でコピーされます。受信したトラフィックについては、ミラーポートへのコピー時にもタグの有無が正しく反映されます。

6.4.6 ミラーポートリンクステータス変化時のフラッディング

ミラーリング使用時にミラーポートのリンクステータスが変化すると、FDB からミラー対象のポートや VLAN に関するエントリがいったん削除されます。このため、ミラーポートからアナライザを取り外したり取り付けたりすると、一時的にフラッディングが発生しますが、これは仕様です。

6.5 VLAN/ スイッチング

6.5.1 デフォルト / スタティックルート

削除したVLAN内に設定されていたデフォルトルートやスタティックルートは無効になりますが、ルートエントリ自体は残ります。これらルートの削除は手動で行う必要があります。

複数のデフォルトルートを設定した場合は、最小メトリックのルートが使用されます。最小メトリックのルートが複数存在する場合は、そのうちのいずれかが選択されます。

6.5.2 ARP エージングタイマー

ARP エントリのタイムアウトは分単位で設定します。デフォルトは 20 分です。設定コマンドは次のとおりです。

```
config iparp timeout <minutes>
```

6.5.3 プロトコル "IP" の変更

定義済みのプロトコル "IP" に変更を加えるときは、キーワード `protocol` を省略できません。「`config ip add ...`」ではエラーになります。「`config protocol ip add ...`」のように完全な構文で表記してください。

6.5.4 LLC=0xFFFF のプロトコルフィルタ

LLC 値に 0xffff を指定したプロトコルフィルタを VLAN に割り当てないでください。これを行うと、すべてのトラフィックがこの VLAN に割り当てられ、プロトコルフィルタを持たない VLAN が正常に動作しなくなります。もし上記の設定を行い、これを保存をしてしまったときは、`unconfig switch all` コマンドを使って設定をリセットしてください。

6.5.5 GVRP とロードシェアリング

GVRP とロードシェアリングを同時に使用することはできません。

6.5.6 GVRP 送信統計

GVRP の送信パケット統計では、実際に送信された数よりもつねに多く表示されます。

6.6 VLAN アグリゲーション

6.6.1 クライアントを別のサブ VLAN に移動した場合

VLAN アグリゲーション使用時に、クライアントホストをあるサブ VLAN から別のサブ VLAN に移動すると、スーパー VLAN 経由の通信ができなくなることがあります。その場合は、クライアントかスイッチの ARP キャッシュをいったんクリアしてください。

6.6.2 スタティック ARP エントリ

スーパーVLAN やサブ VLAN 内のホストに対応するスタティック ARP エントリを作成することはできません。

6.6.3 VLAN アグリゲーションと QoS

サブ VLAN には IP アドレスを割り当てられないため、VLAN アグリゲーションと ISQ（サブネット内 QoS）の併用はできません。

6.7 スパニングツリープロトコル（STP）

6.7.1 STP と ERRP

スパニングツリープロトコルと ERRP を同時に使用することはできません。

6.7.2 enable ignore-stp コマンド

`enable ignore-stp` コマンドを実行したときは、必ず本製品を再起動してください。

6.8 Quality of Service（QoS）

6.8.1 帯域幅設定の実効値

QoS プロファイルの帯域幅設定（最大 / 最小）では、0 ～ 100% の任意の値を設定できますが、内部的には次に示す値のどれかに丸めて処理されます。

0, 1, 2, 3, 4, 5, 10, 20, 30, 40, 50, 60, 70, 80, 100

6.8.2 最小帯域幅の合計値は 90%以内に

QoS プロファイルの最小帯域幅を設定するときは、各プロファイルの最小帯域幅の合計が 90% を超えないように設定することをおすすめします。もし 90% を超えるような設定を行うと、ポートの帯域を超えるトラフィックが断続的に発生した場合に、プライオリティの低いトラフィックがまったく送信されなくなる可能性があります。

6.8.3 IPQoS コマンドの書式について

IPQoS でレイヤー 4 の送信元ポートを指定する場合は、必ず送信元 IP アドレスとペアで指定してください。送信元 IP アドレスによるフィルタリングが必要ない場合は、ワイルドカード（0.0.0.0/0）を指定します。次に例を示します。

- 宛先 IP アドレス：192.x.x.x（192.0.0.0/8）
- 宛先レイヤー 4 ポート：無制限（指定なし）
- 送信元 IP アドレス：無制限（0.0.0.0/0：省略できないのでワイルドカードを指定）
- 送信元レイヤー 4 ポート：80/UDP
- QoS プロファイル：*qp3*

```
config ipqos add udp 192.0.0.0/8 0.0.0.0/0 l4-srcport 80 qp3
```

6.8.4 マルチキャストルーティングプロトコル使用時の注意

マルチキャストルーティングプロトコル使用時に次のような IPQoS プロファイルを設定したとします。

```
config ipqos add udp 225.1.2.3/32 192.1.2.3/32 qp3
```

この場合、送信元 IP アドレス（ここでは 192.1.2.3/32）に適用される実際のマスク長は、ルーティングプロトコル経由で得られたマルチキャストルートによって決まります。たとえば、この例では、送信元 IP アドレスの実際のマスク長が 24 ビットになることもあり得ます。その場合、ホスト 192.1.2.4 がマルチキャストグループ 225.1.2.3 に対して最初にパケットを送信したとすると、それ以降同サブネット（192.1.2.0/24）から 225.1.2.3 へのトラフィックには、すべてデフォルトの QoS プロファイル *qp1* が適用されます（上記設定の *qp3* ではありません）。これを防ぐには、マルチキャストルートのマスク長と一致した設定を行ってください。上記の例では、次のように設定を変更してください。

```
config ipqos add udp 225.1.2.3/32 192.1.2.0/24 qp3
```

6.8.5 QoS モニタ（show ports qosmonitor コマンド）の表示

Egress モードで宛先 IP アドレスに QoS プロファイルを割り当てていると、QoS モニタ（`show ports qosmonitor` コマンド）において、キュー番号（Q0 ～ Q3）とトラフィックの関係が正しく表示されないことがあります。ただし、これは表示だけの問題であり、QoS は設定どおりに動作します。IP QoS の設定を確認するには、`show ipqos` コマンドを使用してください。

6.9 IP ルーティング

6.9.1 UDP フォワーディングと DHCP/BOOTP リレー

DHCP/BOOTP リレーと UDP フォワーディングを同時に使用しないでください。DHCP/BOOTP パケットの転送先が一カ所だけなら、DHCP/BOOTP リレーを使用してください。複数の DHCP サーバを使い分けたいような場合は、UDP フォワーディングを使用してください。

6.9.2 IP ルーティングには 2 つの VLAN が必要

本製品を IP ルータとして動作させるには、IP アドレス割り当て済みの VLAN が最低 2 つ必要です。IP VLAN が 1 つしかなくても、IP ルーティングや RIP 等をイネーブルにすることはできますが、その場合 IP ルータとしては機能しません。

6.9.3 IGMP、IGMP スヌーピングと IP ユニキャスト / マルチキャストルーティング

IP ユニキャストルーティングやマルチキャストルーティングの使用時は、IGMP と IGMP スヌーピングをイネーブルにしてください。IGMP と IGMP スヌーピングはデフォルトでイネーブルになっています。IGMP および IGMP スヌーピングの設定は、`show ipconfig` コマンドで確認できます。

6.9.4 IP ルートシェアリング

IP ルートシェアリングは、同一メトリックのルートが複数存在する場合に、トラフィックをこれら複数の経路に分散して送信する機能です。この機能を使用するには、`enable iproute sharing` コマンドを実行し、通常どおりスタティックルートやダイナミックルーティングの設定を行います。ルートシェアリングでは、最大 5 つの経路が同時に使用されます。なお、RIP や DVMRP のルーティングテーブルには、特定宛先へのルートが 1 つしか登録されないので、通常 IP ルートシェアリングは行われません。ただし、OSPF やスタティックルートを RIP ドメイン内に広告する設定（RIP Export）を行っている場合は、この限りではありません。

IP ルートシェアリングは限られた帯域を有効利用するための機能ですが、トラブル発生時のトラフィック監視作業が困難になるため、その点を考慮した上でご使用ください。

6.9.5 ルートプライオリティの変更

ルートプライオリティを変更したときは、必ず本製品を再起動してください。

6.10 IP マルチネット

6.10.1 マルチネットの制限事項

IP マルチネット機能には下記の制限がありますのでご注意ください。

- マルチネット VLAN にはタグ付きポートを割り当てないでください。
- マルチネット VLAN では IP マルチキャストルーティング機能を使用できません。
- マルチネットと RIP/OSPF を同時に使用しないでください。

6.10.2 マルチネットと DHCP/BOOTP リレー

ダミープロトコルを割り当てられた VLAN では、DHCP/BOOTP リレー機能を利用できません。同機能は IP プロトコル VLAN でのみ利用可能です。

6.10.3 マルチネット VLAN 内ホストの IP 設定

マルチネット VLAN に所属するホストのデフォルトゲートウェイや IP アドレス設定が間違っていると、本製品のパフォーマンスを低下させるおそれがありますのでご注意ください。

6.11 RIP

6.11.1 デフォルト設定の変更

本バージョンでは、次のデフォルト設定値が変更になりました。

- `enable rip export static` ― イネーブル → ディセーブル
- `enable rip aggregation` ― イネーブル →ディセーブル

6.11.2 RIP V2 Authentication

RIP バージョン 2 の Authentication 機能はサポートしておりません。

6.12 OSPF

6.12.1 ルータ ID の設定

OSPF を実行しているスイッチのルータ ID は、自動（デフォルト）ではなく手動で設定することをおすすめします。自動設定では、ルータインタフェースの IP アドレスのうちもっとも大きいものがルータ ID として使用されますが、この場合、OSPF のディセーブル / イネーブル等を行うとルータ ID が変わる場合があり、規模が大きいネットワーク環境では、変更前の古いルータ ID でリンクステートデータベースが使われ続ける可能性があります。

ルータ ID の固定設定を行うには、`config ospf routerid <routerid>` コマンドを使います。`<routerid>` には 10 進ドット表記の IP アドレスを指定します。ルータ ID は他のスイッチと重複しないように設定しなくてはなりません。

6.12.2 OSPF VLAN はデフォルトでバックボーンエリアに所属

特に設定を行わない限り、VLAN は自動的にバックボーンエリア（0.0.0.0）の所属となります。システムによってはこれが通信不良の原因になることがあり得ますので、そのような場合は、`config ospf vlan <name> area <areaid>` コマンドを使って、VLAN の所属エリアを変更してください。エリアの作成には `create ospf area <areaid>` コマンドを使います。

6.12.3 推奨設定最大値

OSPF の設定を行うときは、以下の範囲内で行うことをおすすめします。

- 1 つの OSPF エリア内のルータは 40 個まで
- エリア内、エリア間、エリア外ルートの合計数は約 2000 個まで。

6.13 IP マルチキャストルーティング

6.13.1 Cisco 社製品とのインターオペラビリティ

Cisco 社製品と相互運用する場合は、Cisco 側機器で PIM 2.0 対応の IOS（バージョン 11.3 以上）を使用してください。また、DVMRP ではなく PIM-DM をご使用ください。

6.13.2 PIM-DM とルートシェアリング

本バージョンでは、PIM-DM でのルートシェアリングは未サポートです。

6.14 IPX ルーティング

6.14.1 IPX ルーティングではロードシェアリング不可

IPX ルーティング使用時は、IPX VLAN にロードシェアリングポートを含めることができません。

6.14.2 IPX ルート / サービスエントリ数

本バージョンにおける IPX/RIP および IPX/SAP エントリの上限は約 2000 個です。また、スタティックなルートエントリおよびサービスエントリはそれぞれ 64 個までとなります。

6.14.3 IPX タイマーのチューニング

大規模な IPX ネットワークでは、IPX/RIP および IPX/SAP パケットの送信間隔を長くする（たとえば、デフォルトの 60 秒から 120 秒へ）ことで、CPU への負荷を軽減させることができます。

```
config ipxrip vlan [<name> | all] update-interval <time>
{hold-multiplier <number>}

config ipxsap vlan [<name> | all] update-interval <time>
{hold-multiplier <number>}
```

ルート情報の更新間隔を長くするには、`hold-multiplier` の値を大きくする方法もあります。ルートエントリのタイムアウト時間は、`update-interval` × `hold-multiplier` で求められます。`hold-multiplier` のデフォルト値は 3 ですので、これをより大きな値にすれば、タイムアウトを長くすることができます。

6.14.4 IPX ルーティングのパフォーマンス

ユーザーガイドにもあるとおり、IPX ルーティングはソフトウェアによって処理されます。そのため、環境にもよりますが、通常はワイヤスピード以下のパフォーマンスとなります。IPX パケットのスイッチングはワイヤスピードで行われます。

6.15 ERRP

6.15.1 ERRP 設定コマンドのキーワードは「ESRP」

ERRP 設定コマンドのキーワードは、ERRP ではなく「**ESRP**」です。間違えやすいのでご注意ください。

6.15.2 ERRP VLAN 作成上の注意

ギガビットポート上に、ERRP を使用する VLAN と ERRP を使用しない VLAN を重ねて設定しないでください。10/100M ポートでは、本リリースノート「ユーザーガイドの訂正」および、ユーザーガイド記載の構成ルールにしたがってください。

6.15.3 ERRP VLAN には他のルータを置かない

ERRP VLAN 内に ERRP を使用しない他のルータ（RIP や OSPF を使用しているもの）を配置しないでください。ERRP は、デフォルトルートを 1 つしか持てないクライアントに対してレイヤー 3/2 レベルの冗長性を提供するものです。VLAN 内に ERRP 非対応のルータがあると、切り替え時に RIP や OSPF との干渉が起こる可能性があります。

6.15.4 EDP

ERRP 使用時は、関連するポートで EDP（Enterprise Discovery Protocol）をイネーブルにする必要があります。EDP の設定は `show edp` コマンドで確認します。デフォルトはイネーブルです。また、EDP をオン / オフするには、`[enable | disable] edp` コマンドを使います。

6.15.5 ERRP 関連のエラーメッセージ

ERRP 設定時に次のようなエラーメッセージが表示されることがあります。

```
WARNING: MAC address conflict between VLAN junk2 and VLAN Default.
```

これは、ERRP VLAN が非 ERRP VLAN とポートを共有している場合や、ERRP VLAN がポートブロックを他の VLAN と共有しているような場合です。ユーザーガイドや本リリースノートの注意事項をよく確認してください。

6.16 アクセスポリシー

6.16.1 マルチキャスト環境におけるゲートウェイフィルタ設定上の留意点

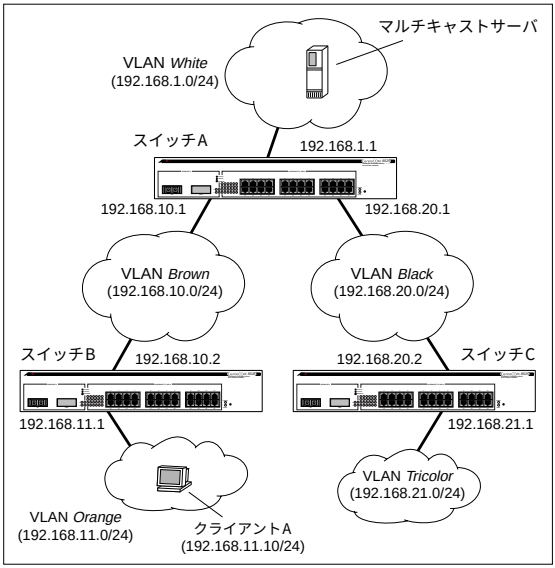
DVMRP や PIM-DM を使用している環境で、ゲートウェイフィルタ（trusted-gateway filter）によるマルチキャストトラフィックのフィルタリングを行う場合は、次の点に注意してください。

- DVMRP では、クライアントに最も近いルータでアクセスポリシーの設定を行います。
- これに対し、PIM-DM 環境では、サーバに最も近いルータでアクセスポリシーの設定を行います。

以下、具体例を示しながら解説します。

ここでは、次のような構成のネットワークを想定します。

この構成において、ダイナミックマルチキャストルーティングプロトコル（DVMRP または PIM-DM）を使用しているものとします。ゲートウェイフィルタを使用して、マルチキャストサーバの送出したマルチキャストパケットがクライアント A（192.168.11.10）に配信されないようにするには、次のような設定を行います。



- DVMRP 環境では、スイッチ B で次の設定を行います。

```
config access-profile nomulticast ipaddress
config access-profile nomulticast add ipaddress 192.168.10.1
config access-profile nomulticast mode deny
config dvmrp vlan brown trusted-gateway nomulticast
```

- PIM-DM 環境では、スイッチ A で次の設定を行います。

```
config access-profile nomulticast ipaddress
config access-profile nomulticast add ipaddress 192.168.10.2
config access-profile nomulticast mode deny
config dvmrp vlan brown trusted-gateway nomulticast
```

6.17 ログ

6.17.1 clear log コマンド

デフォルトでは、warning レベルと critical レベルのログエントリは再起動しても消去されません。また、これらのエントリは、通常の `clear log` コマンドでも消去されません。すべてのログエントリを削除するには、`clear log static` コマンドを実行します。

6.18 BootROM 機能

ここでは BootROM 機能を使って起動時にファームウェアを選択する方法、および、シリアルポート経由でファームウェアをダウンロードする方法などについて説明します。

6.18.1 BootROM 機能の起動

コンソールポートにターミナルを接続し、端末設定が正しいことを確認したら、端末のスペースキーを押しながら C9100/8500 の電源を投入します。画面に "BootROM->" プロンプトが表示されたら、スペースキーをはなしてください。ここで「h」(help) キーを押すと、次のコマンド一覧が表示されます。

```
1: Select primary image
2: Select secondary image
d: Force default configuration
s: Load from Serial Port to RAM
p: Boot PCMCIA card
f: Boot FLASH image
b: Change baud rate
h: Help
g: Boot RAM image
BootROM->
```

注意！ BootROM 機能は、ハードウェア故障以外の原因（ファームウェアが壊れた場合など）で起動時にシステム内のファームウェアを読み込めなくなった場合など、緊急時に使用する回避機能です。それ以外の目的では使用しないでください。

6.18.2 起動ファームウェアの選択方法

起動するファームウェアを選択するには、BootROM 機能の起動後に「1」(Select primary image) キーか「2」(Select secondary image) キーのどちらかを押してください。1 が primary 領域、2 が secondary 領域のファームウェアを表します。ファームウェアを選択したら、「f」(Boot FLASH image) キーを押してスイッチを起動します。

6.18.3 XMODEM によるファームウェアのダウンロード方法

BootROM 機能を起動したら、「s」(Load from Serial Port to RAM) を選択します。すると、シリアルポートからのダウンロード待ちであることが表示されますので、ご使用のターミナルソフトから XMODEM プロトコルでファイルを転送します。転送終了後に「g」(Boot RAM image) キーを押すと、読み込んだファームウェアを使って再起動します。

6.18.4 出荷時設定に戻す

本製品の設定内容を出荷時の状態に戻すには、BootROM プロンプトで「d」(Force default configuration) キーを押します。本機能はパスワードを忘れてしまった場合などに有効ですが、これまでに行った設定がすべて削除されますので、使用にあたっては充分注意してください。

6.19 Web インタフェース

6.19.1 Web サーバがビジー状態の場合

複数のユーザが同じスイッチにアクセスした場合、"Web: server busy" というエラーメッセージが表示されることがあります。その場合は、一度ログアウトしてから、再度ログインしてください。

6.19.2 Microsoft Internet Explorer 4.0 での注意

Internet Explorer 4.0 では、ユーザログイン情報がブラウザのキャッシュに残ります。これは、セキュリティ上の問題を引き起こす可能性がありますので、ログアウトするたびに、必ず IE 4.0 をいったん終了させてください。

6.19.3 GVRP VLAN の設定

Web インタフェースでは GVRP VLAN の設定を行うことができません。「Submit」ボタンを押すと画面がリフレッシュされ、次項「「Submit」ボタンを押したとき」にあるとおり CLI 上でアスタリスクが表示されるため、問題なく設定が行われたように見えますが、実際には設定変更は行われません。

6.19.4 「Submit」ボタンを押したとき

設定パラメータを変更せずに「Submit」ボタンを押した場合でも、CLI プロンプトには設定変更が保存されていないことを示すアスタリスクが表示されます。

6.19.5 デフォルト QoS プロファイルが表示されない

ユーザ定義の QoS プロファイルがない場合、port configuration 画面の QoS Profile フィールドには、デフォルト QoS プロファイルの *qp1* が表示されず、代わりに空白のセルが表示されます。

6.19.6 ログエントリの順序

ログエントリ数が最大値（999）を超えた場合、Web インタフェースではエントリの順番が正しく表示されません。順序を確認するには、各エントリのタイムスタンプをご覧ください。

6.19.7 RADIUS 認証サーバ使用時の Web アクセス

RADIUS サーバ使用時にサーバとの通信が途絶えると、Web ページが表示されるまでに非常に長い時間（数分）がかかるようになります。これは、Web サーバが RADIUS サーバとの通信断絶後もページごとに認証要求を出すためです。

6.20 SNMP/RMON

6.20.1 RMON機能のイネーブル

RMON 機能をイネーブルにするには、次のコマンドを使います。

```
[enable | disable] rmon
```

RMON の設定を確認するには、`show management` コマンドを使います。

6.20.2 トラップレシーバアドレスの指定

トラップレシーバの IP アドレスにマルチキャストやブロードキャストアドレスを指定すると、正しく動作しません。

6.20.3 SNMP トラップ送信先ポート

SNMP トラップの送信先 UDP ポートは RFC2021 に基づいており、CLI から設定を変更することはできません。

6.20.4 Bridge MIB

IEEE Bridge MIB の dot1dTpPortEntry、dot1dTpPortInDiscards、dot1dBasePortEntry は、カウントアップされません。

6.20.5 空の GBIC スロット

リダンダントポートに GBIC モジュールが装着されていない場合、ifMauTable にはリダンダントポートに該当するエントリが存在しません。また、プライマリポートに GBIC モジュールが装着されていない場合は、"unknown MAU" として認識されます。

6.20.6 プライベート MIB の AtiInputPowerVoltage

プライベート MIB の AtiInputPowerVoltage はつねに 110 ボルトのままで、実際の電圧を反映しておりません。

6.20.7 リダンダントポート切り替え時のトラップ

リダンダントポート切り替え発生時にはトラップが送信されます。ただし、トラップレシーバがリダンダントポートに接続されている場合は、トラップを受信できません。これは、トラップが切り替え前に送信されるためです。

6.20.8 認証トラップの設定

認証トラップのイネーブル / ディセーブル設定を SNMP 経由で行うことはできません。snmpEnableAuthenTrap オブジェクトへの Set は可能ですが、実際には Set した内容が有効になりません。認証トラップの設定は、CLI の `show management` コマンドで確認できます。認証トラップの設定は、CLI か Web インタフェースから行ってください。

6.20.9 RMON cRCAlignment カウンタ

10/100M ポートでは、Alignment エラーパケットを受信しても、RMON Statistics グループの cRCAlignment パケットカウンタがカウントアップされません。CRC エラーパケットを受信したときはカウントアップされます。また、ショートパケット（フレーム長 59byte 以下）やロングパケット（フレーム長 1519byte 以上）で、かつ CRC エラーがあるパケットを受信した場合は、cRCAlignment パケットカウンタがカウントアップされてしまいます。