



トラブルシューティング

この章では、Cisco IOS ソフトウェアに関連する、Catalyst 3550 スイッチにおけるソフトウェアの問題を特定し、解決する方法について説明します。問題を特定して解決する際には、問題の性質に応じて、CLI (コマンドライン インターフェイス)、デバイス マネージャ、または Network Assistant を使用できます。



(注) この章で使用されるコマンドの構文および使用方法の詳細については、このリリースのコマンドリファレンス、および『Cisco IOS Command Summary for Cisco IOS』Release 12.1 を参照してください。

この章で説明する内容は、次のとおりです。

- [回復手順 \(p.37-2\)](#)
- [自動ネゴシエーションの不一致の防止 \(p.37-13\)](#)
- [GBIC モジュールのセキュリティと識別 \(p.37-13\)](#)
- [接続問題の診断 \(p.37-14\)](#)
- [PoE スイッチ ポートのトラブルシューティング \(p.37-19\)](#)
- [debug コマンドの使用 \(p.37-20\)](#)
- [show forward コマンドの使用例 \(p.37-23\)](#)
- [クラッシュ情報ファイル \(p.37-24\)](#)



(注) ACL (アクセス制御リスト) を適用したあとでパケットのパフォーマンスに問題が生じた場合、または Ternary Content Addressable Memory (TCAM) 容量に関するメッセージを受信した場合は、「[ACL リソースの利用率および設定問題の表示](#)」(p.28-47) を参照してください。

回復手順

これらの回復手順を実行するには、スイッチを直接操作する必要があります。

- [ソフトウェア障害からの回復 \(p.37-2\)](#)
- [パスワードを忘れた場合の回復 \(p.37-3\)](#)
- [コマンドスイッチ障害からの回復 \(p.37-8\)](#)
- [メンバー接続の回復 \(p.37-12\)](#)

ソフトウェア障害からの回復

アップグレード時にスイッチソフトウェアで障害が発生する状況としては、スイッチに誤ったファイルをダウンロードした場合、およびイメージファイルを削除した場合が考えられます。いずれの場合にも、スイッチは Power-on Self-Test (POST; 電源投入時セルフテスト) をパスしなくなり、接続できなくなります。

次の手順では XMODEM プロトコルを使用し、イメージファイルが壊れた状況、またはイメージファイルを間違えた状況からの回復を図ります。XMODEM プロトコルをサポートするソフトウェアパッケージは多いため、使用するエミュレーションソフトウェアによって、この手順が異なる場合もあります。

ソフトウェア障害から回復するには、次の手順を実行します。

ステップ 1 XMODEM プロトコルをサポートする端末エミュレーションソフトウェアを備えた PC を、スイッチのコンソールポートに接続します。

ステップ 2 エミュレーションソフトウェアの回線速度を 9600 ボーに設定します。

ステップ 3 スwitchの電源コードを取り外します。

ステップ 4 **Mode** ボタンを押しながら、電源コードを再度スイッチに接続します。

ポート 1X 上部の LED が消灯してから 1 ~ 2 秒後に、**Mode** ボタンを離します。ソフトウェアに関する数行分の情報と指示が表示されます。

```
The system has been interrupted prior to initializing the flash file system. The
following commands will initialize the flash file system, and finish loading the
operating system software#
```

```
flash_init
load_helper
boot
```

ステップ 5 フラッシュファイルシステムを初期化します。

```
switch# flash_init
```

ステップ 6 コンソールポートの速度を 9600 以外に設定していた場合は、その設定していた速度にリセットされています。エミュレーションソフトウェアの回線速度をスイッチのコンソールポートに合わせて変更します。

ステップ 7 ヘルパー ファイルをロードします。

```
switch# load_helper
```

ステップ 8 XMODEM プロトコルを使用し、ファイル転送を開始します。

```
switch# copy xmodem: flash:image_filename.bin
```

ステップ 9 XMODEM 要求が表示されたら、端末エミュレーション ソフトウェアの適切なコマンドを使用して転送を開始し、ソフトウェア イメージをフラッシュ メモリにコピーします。

パスワードを忘れた場合の回復

エンド ユーザが物理的にスイッチにアクセスする際、電源投入時にブート プロセスを中断して新しいパスワードを入力することで、失われたパスワードを回復できます。これは、Catalyst 3550 のデフォルト設定です。



(注)

Catalyst 3550 ファスト イーサネット スイッチでは、エンドユーザがデフォルト設定に戻すことに同意するだけでパスワードをリセットできます。この方法で、システム管理者はこの機能の一部をディセーブルにできます。Catalyst 3550 ファスト イーサネット スイッチでパスワードをリセットしようとしているユーザがいて、パスワード回復がディセーブルになっている場合は、回復プロセスの間、ステータス メッセージにその旨が表示されます。

スイッチのパスワードを忘れた場合、次の手順を実行します。

ステップ 1 端末エミュレーションソフトウェアが稼働している端末またはPCをスイッチのコンソールポートに接続します。

ステップ 2 エミュレーションソフトウェアの回線速度を 9600 ボーに設定します。

ステップ 3 スイッチの電源コードを取り外します。

ステップ 4 電源コードを再度スイッチに接続し、15 秒以内にポート 1X 上部のシステム LED が緑色に点滅している間に **Mode** ボタンを押します。システム LED がオレンジに変わってすぐに緑に点灯したままになるまで **Mode** ボタンを押し続け、そのあと **Mode** ボタンを離します。

ソフトウェアに関する数行分の情報と指示が表示され、パスワード回復手順がディセーブルになっていないかどうか通知されます。

- 次のような開始のメッセージが表示された場合

```
The system has been interrupted prior to initializing the flash file system.The following commands will initialize the flash file system
```

「パスワード回復がイネーブルになっている場合のパスワード回復」(p.37-4)に進み、その手順を実行します。

- 次のような開始のメッセージが表示された場合

The password-recovery mechanism has been triggered, but is currently disabled.

「パスワード回復がディセーブルになっている場合の手順」(p.37-6)に進み、その手順を実行します。

パスワード回復がイネーブルになっている場合のパスワード回復

パスワード回復メカニズムがイネーブルになっている場合は、次のメッセージが表示されます。

The system has been interrupted prior to initializing the flash file system. The following commands will initialize the flash file system, and finish loading the operating system software:

```
flash_init
load_helper
boot
```

パスワード回復がイネーブルになっている場合、次の手順を実行します。

ステップ 1 フラッシュ ファイル システムを初期化します。

```
switch# flash_init
```

ステップ 2 コンソール ポートの速度を 9600 以外に設定していた場合は、その設定していた速度にリセットされています。エミュレーション ソフトウェアの回線速度をスイッチのコンソール ポートに合わせて変更します。

ステップ 3 ヘルパー ファイルをロードします。

```
switch# load_helper
```

ステップ 4 フラッシュ メモリの内容を表示します。

```
switch# dir flash:
```

スイッチのファイル システムがディレクトリに表示されます。

ステップ 5 コンフィギュレーション ファイルの名前を config.text.old に変更します。

このファイルには、パスワード定義が収められています。

```
switch# rename flash:config.text flash:config.text.old
```

ステップ 6 システムを起動します。

```
switch# boot
```

setup プログラムを起動するように求められます。プロンプトに N を入力します。

```
Continue with the configuration dialog? [yes/no]: N
```

ステップ 7 スイッチ プロンプトで、イネーブル EXEC モードを開始します。

```
Switch> enable
```

ステップ 8 コンフィギュレーション ファイルを元の名前に戻します。

```
Switch# rename flash:config.text.old flash:config.text
```

ステップ 9 コンフィギュレーション ファイルをメモリにコピーします。

```
Switch# copy flash:config.text system:running-config  
Source filename [config.text]?  
Destination filename [running-config]?
```

確認を求めるプロンプトに、Return キーを押して応答します。

コンフィギュレーション ファイルがリロードされ、パスワードの変更が可能となります。

ステップ 10 グローバル コンフィギュレーション モードを開始します。

```
Switch# configure terminal
```

ステップ 11 パスワードを変更します。

```
Switch (config)# enable secret password
```

シークレット パスワードは 1 ~ 25 文字の英数字です。先頭の文字は数字でもよく、大文字と小文字は区別されます。スペースも使用できますが、先頭のスペースは無視されます。

ステップ 12 イネーブル EXEC モードに戻ります。

```
Switch (config)# exit  
Switch#
```

ステップ 13 実行コンフィギュレーションをスタートアップ コンフィギュレーション ファイルに書き込みます。

```
Switch# copy running-config startup-config
```

新しいパスワードがスタートアップ コンフィギュレーションに組み込まれました。



(注) 上記の手順を実行すると、スイッチの仮想インターフェイスがシャットダウン ステートになることがあります。このステートになっているインターフェイスを調べるには、**show running-config** イネーブル EXEC コマンドを入力します。インターフェイスを再びイネーブルにするには、**interface vlan *vlan-id*** グローバル コンフィギュレーション コマンドを入力し、シャットダウン インターフェイスの VLAN ID を指定します。スイッチがインターフェイス コンフィギュレーション モードの状態では、**no shutdown** コマンドを入力します。

パスワード回復がディセーブルになっている場合の手順

パスワード回復メカニズムがディセーブルになっている場合は、次のメッセージが表示されます。

```
The password-recovery mechanism has been triggered, but
is currently disabled. Access to the boot loader prompt
through the password-recovery mechanism is disallowed at
this point. However, if you agree to let the system be
reset back to the default system configuration, access
to the boot loader prompt can still be allowed.
```

```
Would you like to reset the system back to the default configuration (y/n)?
```



注意

スイッチをデフォルト設定に戻すと、既存の設定がすべて失われます。システム管理者に問い合わせ、バックアップスイッチと VLAN コンフィギュレーション ファイルの有無を確認することを推奨します。

- **n** (no) を入力すると、**Mode** ボタンが押されていない場合と同様に、通常の起動プロセスが継続されます。ブート ロードер プロンプトにアクセスできないため、新しいパスワードの入力はできません。次のメッセージが表示されます。

```
Press Enter to continue.....
```

- **y** (yes) を入力すると、フラッシュメモリ内のコンフィギュレーション ファイルおよび VLAN データベース ファイルが削除されます。デフォルト設定がロードされたら、パスワードをリセットできます。

パスワード回復がディセーブルになっている場合、次の手順を実行します。

ステップ 1 パスワード回復手順の継続を選択すると、既存の設定が失われます。

```
Would you like to reset the system back to the default configuration (y/n)? Y
```

ステップ 2 ヘルパー ファイルをロードします。

```
Switch# load_helper
```

ステップ 3 フラッシュメモリの内容を表示します。

```
switch# dir flash:
```

スイッチのファイルシステムがディレクトリに表示されます。

ステップ 4 システムを起動します。

```
Switch# boot
```

setup プログラムを起動するように求められます。パスワード回復手順を継続するには、プロンプトに **N** を入力します。

```
Continue with the configuration dialog? [yes/no]: N
```

ステップ 5 スイッチ プロンプトで、イネーブル EXEC モードを開始します。

```
Switch> enable
```

ステップ 6 グローバル コンフィギュレーション モードを開始します。

```
Switch# configure terminal
```

ステップ 7 パスワードを変更します。

```
Switch (config)# enable secret password
```

シークレット パスワードは 1 ~ 25 文字の英数字です。先頭の文字は数字でもよく、大文字と小文字は区別されます。スペースも使用できますが、先頭のスペースは無視されます。

ステップ 8 イネーブル EXEC モードに戻ります。

```
Switch (config)# exit  
Switch#
```

ステップ 9 実行コンフィギュレーションをスタートアップ コンフィギュレーション ファイルに書き込みます。

```
Switch# copy running-config startup-config
```

新しいパスワードがスタートアップ コンフィギュレーションに組み込まれました。



(注) 上記の手順を実行すると、スイッチの仮想インターフェイスがシャットダウン ステートになることがあります。このステートになっているインターフェイスを調べるには、**show running-config** イネーブル EXEC コマンドを入力します。インターフェイスを再びイネーブルにするには、**interface vlan *vlan-id*** グローバル コンフィギュレーション コマンドを入力し、シャットダウン インターフェイスの VLAN ID を指定します。スイッチがインターフェイス コンフィギュレーション モードの状態では、**no shutdown** コマンドを入力します。

ステップ 10 ここでスイッチを再設定する必要があります。バックアップ スイッチと VLAN コンフィギュレーション ファイルがシステム管理者によって利用できるようになっている場合は、それらを利用します。

コマンド スイッチ障害からの回復

ここでは、コマンド スイッチ障害から回復する手順について説明します。冗長コマンド スイッチ グループを設定するには、Hot Standby Router Protocol (HSRP) を使用します。詳細については、第 5 章「スイッチのクラスタ設定」、第 32 章「HSRP の設定」、Cisco.com の『*Getting Started with Cisco Network Assistant*』を参照してください。



(注) HSRP は、クラスタに冗長性を持たせる方法として適しています。

スタンバイ コマンド スイッチが未設定で、かつコマンド スイッチで電源故障などの障害が発生した場合には、メンバー スイッチとの管理接続が失われるため、新しいコマンド スイッチに交換する必要があります。ただし、接続されているスイッチ間の接続能力は影響を受けません。また、メンバー スイッチも通常どおりにパケットを伝送します。メンバー スイッチは、ポートを通してスタンドアロンのスイッチとして管理できます。また、IP アドレスが与えられている場合は、他の管理インターフェイスを使用して管理もできます。

コマンド スイッチとして動作するメンバー スイッチ、または他のスイッチに IP アドレスを割り当ててコマンド スイッチのパスワードを書き留め、メンバー スイッチと交換コマンド スイッチ間の冗長接続が得られるようにクラスタを配置することで、コマンド スイッチ障害に備えることができます。ここでは、故障したコマンド スイッチの交換方法を 2 通り紹介します。

- 故障したコマンド スイッチをクラスタ メンバーに交換する方法
- 故障したコマンド スイッチを別のスイッチに交換する方法

コマンド スイッチとして動作するスイッチの詳細については、リリース ノートを参照してください。

故障したコマンド スイッチをクラスタ メンバーに交換する場合

故障したコマンド スイッチを同じクラスタ内の (コマンド スイッチとして動作する) スイッチに交換するには、次の手順に従ってください。

- ステップ 1 コマンド スイッチとメンバー スイッチの接続を解除し、クラスタからコマンド スイッチを物理的に取り外します。
- ステップ 2 故障したコマンド スイッチの位置にメンバー スイッチを追加し、同じようにクラスタ メンバーと接続します。
- ステップ 3 新しいコマンド スイッチで CLI セッションを開始します。

CLI にはポートを使用してアクセスできます。また、スイッチに IP アドレスが割り当てられている場合は、Telnet を使用してアクセスできます。ポートの詳細な使用方法については、スイッチのハードウェア インストレーション ガイドを参照してください。

- ステップ 4 スイッチ プロンプトで、イネーブル EXEC モードを開始します。

```
Switch> enable
Switch#
```

- ステップ 5 故障したコマンド スイッチのパスワードを入力します。

ステップ 6 グローバル コンフィギュレーション モードを開始します。

```
Switch# configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.
```

ステップ 7 メンバー スイッチをクラスタから削除します。

```
Switch(config)# no cluster commander-address
```

ステップ 8 イネーブル EXEC モードに戻ります。

```
Switch(config)# end  
Switch#
```

ステップ 9 セットアップ プログラムを使用し、スイッチの IP 情報を設定します。このプログラムを実行すると、IP アドレス情報およびパスワードの入力を求めるプロンプトが表示されます。イネーブル EXEC モードで **setup** を入力し、**Return** キーを押します。

```
Switch# setup  
--- System Configuration Dialog ---  
Continue with configuration dialog? [yes/no]: y  
  
At any point you may enter a question mark '?' for help.  
Use ctrl-c to abort configuration dialog at any prompt.  
Default settings are in square brackets '['].  
  
Basic management setup configures only enough connectivity  
for management of the system, extended setup will ask you  
to configure each interface on the system  
  
Would you like to enter basic management setup? [yes/no]:
```

ステップ 10 最初のプロンプトに **Y** を入力します。

セットアップ プログラムのプロンプトは、コマンド スイッチとして選択したメンバー スイッチによって変わります。

```
Continue with configuration dialog? [yes/no]: y
```

または

```
Configuring global parameters:
```

このプロンプトが表示されない場合は **enable** を入力し、**Return** キーを押します。セットアップ プログラムを開始する場合は **setup** を入力し、**Return** キーを押します。

ステップ 11 セットアップ プログラムの質問に応答します。

ホスト名の入力を求めるプロンプトが表示された場合、コマンド スイッチではホスト名が 28 文字、メンバー スイッチでは 31 文字に制限されていることに注意してください。いずれのスイッチでも、ホスト名の最後の文字に $-n$ (n は数字) を使用しないでください。

Telnet (仮想端末) パスワードの入力を求めるプロンプトが表示された場合は、1 ~ 25 文字の英数字が入力できること、大文字と小文字が区別されること、スペースが使用できること、先頭のスペースが無視されることに注意してください。

- ステップ 12 **enable secret** および **enable** パスワードの入力を求めるプロンプトが表示された場合は、故障したコマンドスイッチのパスワードを再入力します。
- ステップ 13 プロンプトが表示されたら、スイッチをクラスタ コマンド スイッチとしてイネーブルにすることを確認し、**Return** キーを押します。
- ステップ 14 プロンプトが表示されたら、クラスタに名前を割り当て、**Return** キーを押します。
- クラスタ名には 1 ~ 31 文字で、英数字、ダッシュ、または下線を使用できます。
- ステップ 15 最初のコンフィギュレーションが表示されたら、アドレスが正しいことを確認します。
- ステップ 16 表示された情報が正しい場合はプロンプトに **Y** を入力し、**Return** キーを押します。
- 情報に誤りがある場合は **N** を入力し、**Return** キーを押して、ステップ 9 からやり直します。
- ステップ 17 ブラウザを起動して、新しいコマンドスイッチの IP アドレスを入力します。
- ステップ 18 クラスタに追加する候補スイッチのリストを表示するには、Cluster メニューから **Add to Cluster** を選択します。
-

故障したコマンドスイッチを他のスイッチに交換する場合

故障したコマンドスイッチを、クラスタに組み込まれていない、コマンドスイッチとして動作するスイッチに交換するには、次の手順に従ってください。

- ステップ 1 コマンドスイッチとメンバースイッチの接続を解除し、クラスタからコマンドスイッチを物理的に取り外します。
- ステップ 2 故障したコマンドスイッチの位置に新しいスイッチを追加し、同じようにクラスタメンバーと接続します。
- ステップ 3 新しいコマンドスイッチで CLI セッションを開始します。
- CLI にはポートを使用してアクセスできます。また、スイッチに IP アドレスが割り当てられている場合は、Telnet を使用してアクセスできます。ポートの詳細な使用方法については、スイッチのハードウェア インストレーション ガイドを参照してください。
- ステップ 4 スイッチ プロンプトで、イネーブル EXEC モードを開始します。
- ```
Switch> enable
Switch#
```
- ステップ 5 故障したコマンドスイッチのパスワードを入力します。

ステップ 6 セットアッププログラムを使用し、スイッチの IP 情報を設定します。

このプログラムを実行すると、IP アドレス情報およびパスワードの入力を求めるプロンプトが表示されます。イネーブル EXEC モードで **setup** を入力し、**Return** キーを押します。

```
Switch# setup
 --- System Configuration Dialog ---
Continue with configuration dialog? [yes/no]: y

At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '['].

Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system

Would you like to enter basic management setup? [yes/no]:
```

ステップ 7 最初のプロンプトに **Y** を入力します。

セットアッププログラムのプロンプトは、コマンド スイッチとして選択したスイッチによって変わります。

```
Continue with configuration dialog? [yes/no]: y
```

または

```
Configuring global parameters:
```

このプロンプトが表示されない場合は **enable** を入力し、**Return** キーを押します。セットアッププログラムを開始する場合は **setup** を入力し、**Return** キーを押します。

ステップ 8 セットアッププログラムの質問に応答します。

ホスト名の入力を求めるプロンプトが表示された場合は、コマンド スイッチでは、ホスト名が 28 文字に制限されていることに注意してください。いずれのスイッチでも、ホスト名の最後の文字に  $-n$  ( $n$  は数字) を使用しないでください。

Telnet (仮想端末) パスワードの入力を求めるプロンプトが表示された場合は、1 ~ 25 文字の英数字が入力できること、大文字と小文字が区別されること、スペースが使用できること、先頭のスペースが無視されることに注意してください。

ステップ 9 **enable secret** および **enable** パスワードの入力を求めるプロンプトが表示された場合は、故障したコマンド スイッチのパスワードを再入力します。

ステップ 10 プロンプトが表示されたら、スイッチをクラスタ コマンド スイッチとしてイネーブルにすることを確認し、**Return** キーを押します。

ステップ 11 プロンプトが表示されたら、クラスタに名前を割り当て、**Return** キーを押します。

クラスタ名には 1 ~ 31 文字で、英数字、ダッシュ、または下線を使用できます。

ステップ 12 最初のコンフィギュレーションが表示されたら、アドレスが正しいことを確認します。

ステップ 13 表示された情報が正しい場合はプロンプトに Y を入力し、**Return** キーを押します。

情報に誤りがある場合は N を入力し、**Return** キーを押して、ステップ 9 からやり直します。

ステップ 14 ブラウザを起動して、新しいコマンドスイッチの IP アドレスを入力します。

ステップ 15 クラスタに追加する候補スイッチのリストを表示するには、Cluster メニューから **Add to Cluster** を選択します。

---

## メンバー接続の回復

構成によっては、コマンドスイッチとメンバースイッチ間の管理接続が維持できない場合もあります。メンバーに対する管理アクセスを維持できなくなってもメンバースイッチが通常どおりパケットを伝送している場合は、次に示す矛盾がないかどうかを確認してください。

- メンバースイッチ ( Catalyst 3550、Catalyst 3500 XL、Catalyst 2955、Catalyst 2950、Catalyst 2940、Catalyst 2900 XL、Catalyst 2820、Catalyst 1900 ) は、ネットワークポートとして定義されたポートを経由して、コマンドスイッチに接続できません。
- Catalyst 3500 XL、Catalyst 2900 XL、Catalyst 2820、Catalyst 1900 メンバースイッチを、同じ管理 VLAN に属するポートを経由して、コマンドスイッチに接続する必要があります。
- セキュアポートを経由して、コマンドスイッチに接続されたメンバースイッチ ( Catalyst 3550、Catalyst 3500 XL、Catalyst 2950、Catalyst 2940、Catalyst 2900 XL、Catalyst 2820、Catalyst 1900 ) は、セキュリティ違反が原因でポートがディセーブルになった場合、接続不能になることがあります。

## 自動ネゴシエーションの不一致の防止

IEEE (米国電気電子学会) 802.3ab 自動ネゴシエーション プロトコルは、スイッチの速度 (GBIC [ギガビット インターフェイス コンバータ] ポートを除く 10 Mbps、100 Mbps、1000 Mbps) およびデュプレックス (半二重または全二重) に関する設定を管理します。このプロトコルでは、状況によって設定の不一致が生じ、その結果パフォーマンスの低下を招くことがあります。設定の不一致は、次の状況下で発生します。

- 手動で設定した速度またはデュプレックスのパラメータが、接続ポート上で手動設定された速度またはデュプレックスの設定と異なっている場合
- ポートが自動ネゴシエーションに設定され、接続先ポートが自動ネゴシエーションではなく全二重に設定されている場合

スイッチのパフォーマンスを最大限に高めてリンクを確保するには、次のいずれかの注意事項に従って、デュプレックスおよび速度の設定を変更してください。

- 両側のポートが、速度とデュプレックスの両方について自動ネゴシエーションを行うようにします。
- 接続の両端のポートに、速度とデュプレックスのパラメータを手動で設定します。



(注) リモート デバイスが自動ネゴシエーションを実行しない場合は、2 つのポートのデュプレックス値が一致するように設定してください。速度パラメータは、接続先ポートが自動ネゴシエーションを実行しない場合でも自動調整が可能です。

## GBIC モジュールのセキュリティと識別

シスコの Coarse Wave Division Multiplexer (CWDM; 低密度波長分割多重化) GBIC モジュールに搭載されているシリアル Electrically Erasable Programmable Read-Only Memory (EEPROM; 電氣的消去再書き込み可能 ROM) には、モジュールのシリアル番号、ベンダーの名前と ID、固有のセキュリティ コード、Cyclic Redundancy Check (CRC; 巡回冗長検査) が格納されています。CWDM GBIC モジュールがスイッチに搭載されると、スイッチのソフトウェアが EEPROM を読み取り、シリアル番号とベンダーの名前、ベンダー ID をチェックして、セキュリティ コードと CRC を再計算します。シリアル番号、ベンダーの名前またはベンダー ID、セキュリティ コード、CRC のどれかが無効である場合、スイッチはそのインターフェイスをエラー ディセーブル ステートにします。



(注) シスコ製品以外の CWDM GBIC モジュールを使用している場合はスイッチから GBIC モジュールを取り外し、シスコのモジュールと交換してください。

シスコの GBIC モジュールを取り付けたあと、`errdisable recovery cause gbic-invalid` グローバル コンフィギュレーション コマンドを使用してポートのステータスを検証し、エラー ディセーブル ステートから回復するためのタイム インターバルを開始します。タイム インターバルが経過すると、スイッチはそのインターフェイスをエラー ディセーブル ステートから復帰させ、再起動します。`errdisable recovery` コマンドの詳細については、このリリースのコマンド リファレンスを参照してください。

## 接続問題の診断

ここでは、接続問題のトラブルシューティング方法について説明します。

- ping の使用 ( p.37-14 )
- IP traceroute の使用 ( p.37-15 )
- レイヤ 2 traceroute の使用 ( p.37-17 )

### ping の使用

ここでは、次の情報について説明します。

- ping の概要 ( p.37-14 )
- ping の実行 ( p.37-14 )

### ping の概要

このスイッチは、リモート ホストへの接続テストに使用できる IP packet internet groper ( ping ) をサポートしています。ping は、アドレスにエコー要求パケットを送信し、応答を待ちます。ping によって、次のいずれかの応答が返されます。

- 正常な応答 正常な応答 ( *hostname* は維持されます ) は、ネットワーク トラフィックによって異なりますが、1 ~ 10 秒以内に発生します。
- 宛先が応答しない ホストが応答しない場合は、*no-answer* メッセージが返されます。
- 不明ホスト ホストが存在しない場合は、*unknown host* メッセージが返されます。
- 宛先に到達不能 指定されたネットワークにデフォルト ゲートウェイが到達できない場合は、*destination-unreachable* メッセージが返されます。
- ネットワークまたはホストに到達不能 ホストまたはネットワークのルーティング テーブルにエントリがない場合は、*network or host unreachable* メッセージが返されます。

### ping の実行

別の IP サブネットワーク内のホストに ping を実行する場合は、ネットワークへのスタティック ルートを定義するか、またはこれらのサブネット間でルーティングされるように IP ルーティングを設定する必要があります。詳細については、第 31 章「IP ユニキャスト ルーティングの設定」を参照してください。

IP ルーティングは、デフォルトではすべてのスイッチでディセーブルです。IP ルーティングをイネーブルにする場合、または設定する必要がある場合は、第 31 章「IP ユニキャスト ルーティングの設定」を参照してください。

ネットワーク上の別のデバイスに対してスイッチから ping を実行するには、イネーブル EXEC モードで次の手順を実行します。

| コマンド                                    | 説明                                                      |
|-----------------------------------------|---------------------------------------------------------|
| <code>ping [ip] {host   address}</code> | IP を通して、またはホスト名やネットワーク アドレスを指定して、リモート ホストに ping を実行します。 |

 (注)

ping コマンドに他のプロトコル キーワードを指定することもできますが、このリリースではサポートされていません。

次に、IP ホストに ping を実行する例を示します。

```
Switch# ping 172.20.52.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echoes to 172.20.52.3, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
Switch#
```

表 37-1 に、表示される ping 文字出力の説明を示します。

表 37-1 ping 出力表示文字

| 文字 | 説明                                                           |
|----|--------------------------------------------------------------|
| !  | 応答が受信されました。                                                  |
| .  | 応答待機中にネットワーク サーバがタイムアウトしました。                                 |
| U  | 宛先到達不能エラー Protocol Data Unit (PDU; プロトコル データ ユニット) が受信されました。 |
| C  | 輻輳に遭遇したパケットが受信されました。                                         |
| I  | ユーザがテストを中断しました。                                              |
| ?  | パケット タイプが不明です。                                               |
| &  | パケットのライフタイムを超過しました。                                          |

ping セッションを終了するには、エスケープシーケンス (デフォルトは Ctrl-^ X) を入力します。デフォルトのエスケープシーケンスを入力するには、Ctrl、Shift、および 6 キーを同時に押してから離し、X キーを押します。

## IP traceroute の使用

ここでは、次の情報について説明します。

- [IP traceroute の概要 \(p.37-15\)](#)
- [IP traceroute の実行 \(p.37-16\)](#)

### IP traceroute の概要

IP traceroute を使用すると、パケットがネットワーク内を通過するパスをホップ単位で識別できます。コマンド出力には、宛先へ向かうトラフィックが途中で通過するルータなど、すべてのネットワーク レイヤ (レイヤ 3) デバイスが表示されます。

ご使用のスイッチは、traceroute イネーブル EXEC コマンドの送信元または宛先として指定可能で、traceroute コマンドの出力にホップとして表示される場合も、表示されない場合もあります。スイッチが traceroute の宛先である場合は、traceroute 出力の最終宛先として表示されます。同じ VLAN 内のポート間でパケットのブリッジングのみを行っている中間スイッチは、traceroute 出力に表示されません。ただし、中間スイッチが特定のパケットをルーティングしているマルチレイヤ スイッチである場合は、traceroute 出力にホップとして表示されます。

traceroute イネーブル EXEC コマンドは、IP ヘッダー内の Time To Live (TTL) フィールドを使用し、ルータおよびサーバが特定のリターン メッセージを生成するようにします。traceroute を開始するには、TTL フィールドが 1 に設定された宛先ホストに UDP データグラムを送信します。ルータは、TTL 値が 1 または 0 のデータグラムを見つけるとそのデータグラムを廃棄し、Internet Control Message Protocol (ICMP) TTL 超過メッセージを送信側に返します。traceroute は、ICMP TTL 超過メッセージの送信元アドレス フィールドを調べ、最初のホップのアドレスを判断します。

ネクスト ホップを識別する場合は、TTL 値が 2 である UDP パケットを送信します。最初のルータは TTL フィールドを 1 減らし、データグラムを次のルータに送信します。2 番目のルータは TTL 値が 1 になったデータグラムを受信し、これを破棄して送信元に TTL 超過メッセージを返します。このプロセスは、データグラムが宛先ホストに到達するまで(または最大 TTL に到達するまで)、TTL 値を増分しながら継続されます。

データグラムがいつ宛先に到達するかを判別するため、tracert はデータグラム内の UDP 宛先ポート番号を、宛先ホストであまり使用されないような大きな値に設定します。ホストは、自身宛のデータグラムを受信し、ローカルに使用されない宛先ポート番号がそのデータグラム内に含まれていると、送信元に ICMP ポート到達不能エラーを送信します。ポート到達不能エラー以外のエラーはすべて中間ホップで発生します。したがって、ポート到達不能エラーが戻ってきた場合は、宛先からこのエラーが送信されたと判断できます。

## IP tracert の実行

ネットワーク内をパケットが通過するパスをトレースするには、イネーブル EXEC モードで次の手順を実行します。

| コマンド                         | 説明                                   |
|------------------------------|--------------------------------------|
| <code>tracert ip host</code> | IP を使用し、ネットワーク内をパケットが通過するパスをトレースします。 |



(注) `tracert` イネーブル EXEC コマンドに他のプロトコル キーワードの指定もできますが、このリリースではサポートされていません。

次に、IP ホストに `tracert` を実行する例を示します。

```
Switch# tracert ip 171.9.15.10

Type escape sequence to abort.
Tracing the route to 171.69.115.10

 0 172.2.52.1 0 msec 0 msec 4 msec
 1 172.2.1.203 12 msec 8 msec 0 msec
 2 171.9.16.6 4 msec 0 msec 0 msec
 3 171.9.4.5 0 msec 4 msec 0 msec
 4 171.9.121.34 0 msec 4 msec 4 msec
 5 171.9.15.9 120 msec 132 msec 128 msec
 6 171.9.15.10 132 msec 128 msec 128 msec
Switch#
```

出力表示には、ホップ数、ルータの IP アドレス、送信された 3 つのプロープそれぞれに対する往復時間 (ミリ秒) が示されます。

表 37-2 traceroute 出力表示文字

| 文字 | 説明                                                   |
|----|------------------------------------------------------|
| *  | プローブがタイムアウトしました。                                     |
| ?  | パケット タイプが不明です。                                       |
| A  | 管理上、到達できません。通常は、アクセス リストによってトラフィックがブロックされていることを示します。 |
| H  | ホストに到達できません。                                         |
| N  | ネットワークに到達できません。                                      |
| P  | プロトコルに到達できません。                                       |
| Q  | 送信元の抑制です。                                            |
| U  | ポートに到達できません。                                         |

進行中のトレースを終了するには、エスケープ シーケンス (デフォルトは `Ctrl-^ X`) を入力します。デフォルトのエスケープ シーケンスを入力するには、`Ctrl`、`Shift`、および `6` キーを同時に押してから離し、`X` キーを押します。

## レイヤ 2 traceroute の使用

ここでは、次の情報について説明します。

- [レイヤ 2 traceroute の概要 \(p.37-17\)](#)
- [使用上の注意事項 \(p.37-17\)](#)
- [物理パスの表示 \(p.37-18\)](#)

### レイヤ 2 traceroute の概要

レイヤ 2 traceroute 機能により、パケットが通過する送信元デバイスから宛先デバイスへの物理パスをスイッチが識別できます。レイヤ 2 traceroute は、ユニキャスト送信元および宛先 MAC (メディア アクセス制御) アドレスのみをサポートしています。パスにあるスイッチの MAC アドレステーブルを使用してパスを判別します。スイッチがレイヤ 2 traceroute に対応していないパスにあるデバイスを検出すると、スイッチはレイヤ 2 トレース キューを送信し続けてタイムアウトにします。

スイッチは、送信元デバイスから宛先デバイスへのパスのみを識別できます。パケットが通過する送信元ホストから送信元デバイスへのパス、あるいは宛先デバイスから宛先ホストへのパスは識別できません。

### 使用上の注意事項

レイヤ 2 traceroute の使用上の注意事項は次のとおりです。

- Cisco Discovery Protocol (CDP) は、ネットワークのすべてのデバイスでイネーブルになっていなければなりません。レイヤ 2 traceroute を適切に機能させるには、CDP をディセーブルにしないでください。物理パス内のデバイスが CDP に対してトランスペアレントの場合、スイッチはこれらのデバイスを通るパスを識別できません。



(注) CDP のイネーブル化の詳細については、[第 22 章「CDP の設定」](#)を参照してください。

- ping イネーブル EXEC コマンドを使用して接続をテストできる場合、スイッチは他のスイッチから到達可能です。物理パス内のすべてのスイッチは、互いに到達可能でなければなりません。
- パス内で識別される最大ホップ数は 10 です。
- 送信元デバイスから宛先デバイスへの物理パス上にないスイッチに、`tracert mac` または `tracert mac ip` イネーブル EXEC コマンドを入力できます。パス内の全スイッチは、互いに到達可能でなければなりません。
- 指定された送信元および宛先 MAC アドレスが同じ VLAN に属している場合、`tracert mac` コマンド出力は、レイヤ 2 パスのみを表示します。異なる VLAN に属する送信元および宛先 MAC アドレスを指定した場合、レイヤ 2 パスは識別されず、エラーメッセージが表示されます。
- マルチキャスト送信元 MAC アドレスまたはマルチキャスト宛先 MAC アドレスを指定した場合、パスは識別されず、エラーメッセージが表示されます。
- 複数の VLAN に属する送信元または宛先 MAC アドレスを指定した場合、送信元および宛先 MAC アドレスの両方が属する VLAN を指定しなければなりません。VLAN を指定しない場合、パスは識別されず、エラーメッセージが表示されます。
- 指定された送信元および宛先 IP アドレスが同じサブネットに属している場合、`tracert mac ip` コマンド出力は、レイヤ 2 パスを表示します。IP アドレスを指定すると、スイッチは Address Resolution Protocol (ARP; アドレス解決プロトコル) を使用して IP アドレスと対応する MAC アドレスおよび VLAN ID を対応付けます。
  - 指定した IP アドレスに対して ARP が存在する場合、スイッチは対応する MAC アドレスを使用して物理パスを識別します。
  - ARP エントリが存在しない場合、スイッチは ARP クエリを送信して IP アドレスを解釈しようとします。IP アドレスが解釈されない場合、パスは識別されず、エラーメッセージが表示されます。
- 複数のデバイスがハブを経由して 1 つのポートに接続されている場合(たとえば複数の CDP ネイバがポートで検出される場合) レイヤ 2 `tracert` 機能はサポートされません。複数の CDP ネイバがポートで検出されると、レイヤ 2 パスは識別されず、エラーメッセージが表示されます。
- この機能は、トークンリング VLAN ではサポートされていません。

## 物理パスの表示

パケットが通過する送信元デバイスから宛先デバイスへのパスは、次のイネーブル EXEC コマンドを使用して表示できます。

- `tracert mac [interface interface-id] {source-mac-address} [interface interface-id] {destination-mac-address} [vlan vlan-id] [detail]`
- `tracert mac ip {source-ip-address | source-hostname} {destination-ip-address | destination-hostname} [detail]`

詳細については、このリリースのコマンド リファレンスを参照してください。

## PoE スイッチ ポートのトラブルシューティング

ここでは、次の情報について説明します。

- [電力消失によるポートのディセーブル \(p.37-19\)](#)
- [問題のあるリンク アップによるポートのディセーブル \(p.37-19\)](#)

### 電力消失によるポートのディセーブル

Power over Ethernet ( PoE ) スイッチ ポートに接続され、AC 電源から電力供給されている受電装置 ( Cisco IP Phone 7910 等 ) への AC 電源からの電力供給が停止した場合、デバイスはエラー ディセーブル ステートになる可能性があります。エラー ディセーブル ステートから回復するには、`shutdown` インターフェイス コンフィギュレーション コマンドとそれに続く `no shutdown` インターフェイス コンフィギュレーション コマンドを使用します。スイッチに自動回復を設定してエラー ディセーブル ステートから回復することも可能です。 `errdisable recovery cause loopback` および `errdisable recovery interval seconds` グローバル コンフィギュレーション コマンドは、一定時間後に自動的に インターフェイスをエラー ディセーブル ステートから回復させます。

このリリースのコマンド リファレンスで説明されているこれらのコマンドを使用して、PoE ポート ステータスをモニタします。

- `show controllers power inline` イネーブル EXEC コマンド
- `show power inline` イネーブル EXEC コマンド
- `debug ilpower` イネーブル EXEC コマンド

### 問題のあるリンク アップによるポートのディセーブル

シスコの受電装置がポートに接続されていて `power inline never` インターフェイス コンフィギュレーション コマンドを使用してポートを設定した場合、問題のあるリンク アップがあるとポートがエラー ディセーブル ステートになる場合があります。エラー ディセーブル ステートから回復するには、`shutdown` および `no shutdown` インターフェイス コンフィギュレーション コマンドを使用します。

`power inline never` コマンドを設定しているポートに、シスコの受電装置を接続しないでください。

## debug コマンドの使用

ここでは、**debug** コマンドを使用してインターネットワーキング問題を診断および解決する方法について説明します。具体的な内容は次のとおりです。

- 特定の機能に関するデバッグのイネーブル化 (p.37-20)
- 全システム診断のイネーブル化 (p.37-21)
- デバッグおよびエラー メッセージ出力のリダイレクト (p.37-21)
- `debug auto qos` コマンドの使用 (p.37-22)



注意

CPU プロセス内では、デバッグ出力に高いプライオリティが割り当てられているため、デバッグを行うとシステムが使用不可能になることがあります。このため、**debug** コマンドは、特定の問題のトラブルシューティングを行う場合やシスコのテクニカル サポート スタッフによるトラブルシューティング セッション中に限って使用してください。**debug** コマンドは、ネットワークトラフィック量が少ない、またはユーザ数が少ない時間帯に使用してください。これらの期間にデバッグを実行すると、**debug** コマンドの処理がもたらすオーバーヘッドの増加により、システムの利用に影響が生じる可能性が低くなります。



(注)

特定の **debug** コマンドの構文および使用方法の詳細については、このリリースのコマンド リファレンスを参照してください。

### 特定の機能に関するデバッグのイネーブル化

**debug** コマンドはすべてイネーブル EXEC モードで入力します。ほとんどの **debug** コマンドは引数を取りません。たとえば、EtherChannel に対するデバッグをイネーブルにするには、イネーブル EXEC モードで次のコマンドを入力します。

```
Switch# debug etherchannel
```

このコマンドの **no** 形式が入力されるまで、スイッチは出力の生成を続けます。

**debug** コマンドをイネーブルにしても出力が表示されない場合は、次の可能性を検討してください。

- スイッチが適切に設定されていないため、モニタ対象のトラフィック タイプが生成されない可能性があります。**show running-config** コマンドを使用し、コンフィギュレーションを確認してください。
- スイッチが正しく設定されていても、デバッグがイネーブルになっている期間に、モニタ対象のトラフィック タイプが生成されない場合もあります。デバッグを行う機能に応じて TCP/IP **ping** コマンドなどを使用し、ネットワーク トラフィックを生成します。

EtherChannel のデバッグをディセーブルにするには、イネーブル EXEC モードで次のコマンドを入力します。

```
Switch# no debug etherchannel
```

あるいは、イネーブル EXEC モードで、このコマンドの **undebug** 形式を入力します。

```
Switch# undebug etherchannel
```

各デバッグ オプションのステータスを表示するには、イネーブル EXEC モードで次のコマンドを入力します。

```
Switch# show debugging
```

## 全システム診断のイネーブル化

全システム診断をイネーブルにするには、イネーブル EXEC モードで次のコマンドを入力します。

```
Switch# debug all
```



注意

デバッグの出力は他のネットワークトラフィックよりも優先され、また、`debug all` イネーブル EXEC コマンドを実行すると他の `debug` コマンドよりも大量の出力が生成されるため、スイッチのパフォーマンスが大幅に低下したり、使用できなくなることがあります。`debug` コマンドは、なるべく対象を特定して使用してください。

`no debug all` イネーブル EXEC コマンドを使用すると、すべての診断出力がディセーブルになります。`no debug all` コマンドを使用すると、誤ってイネーブルのままとなった `debug` コマンドを、簡単にディセーブルにできます。

## デバッグおよびエラー メッセージ出力のリダイレクト

デフォルトでは、ネットワークサーバは `debug` コマンドの出力やシステム エラー メッセージをコンソールに送信します。このデフォルトを使用する場合は、ポートに接続する代わりに仮想端末接続を使用し、デバッグ出力をモニタできます。

宛先として使用できるのは、コンソール、仮想端末、内部バッファ、および Syslog サーバが動作している UNIX ホストなどです。Syslog 形式は、4.3 Berkeley Standard Distribution (BSD) UNIX および派生 OS と互換性があります。



(注)

デバッグの宛先によって、システムのオーバーヘッドが変わることに注意してください。ロギングメッセージをコンソールに送信すると、大きなオーバーヘッドが発生しますが、仮想端末に出力すれば、オーバーヘッドは小さくなります。Syslog サーバに出力すると、オーバーヘッドはさらに小さくなります。最もオーバーヘッドが小さいのは、内部バッファへの出力です。

システムメッセージのロギングに関する詳細については、[第 26 章「システムメッセージロギングの設定」](#)を参照してください。

## debug auto qos コマンドの使用

**debug auto qos** イネーブル EXEC コマンドを使用して、自動 Quality of Service (QoS; サービス品質) がイネーブルに設定されている場合に自動生成される QoS コマンドを表示できます。

QoS コマンドを表示し、QoS ドメイン内で Voice over IP (VoIP) の自動 QoS をイネーブルにするには、イネーブル EXEC モードで次の手順を実行します。

|        | コマンド                                        | 説明                                                                                                                                                                                                                                                                                  |
|--------|---------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ステップ 1 | <b>debug auto qos</b>                       | 自動 QoS 用のデバッグをイネーブルにします。デバッグがイネーブルになると、スイッチは、自動 QoS がイネーブルまたはディセーブルになる際に自動的に生成される QoS コマンドを表示しません。                                                                                                                                                                                  |
| ステップ 2 | <b>configure terminal</b>                   | グローバル コンフィギュレーション モードを開始します。                                                                                                                                                                                                                                                        |
| ステップ 3 | <b>interface interface-id</b>               | Cisco IP Phone に接続されたインターフェイスを指定して、インターフェイス コンフィギュレーション モードを開始します。また、ネットワーク内部にある別のスイッチやルータに接続されているアップリンク インターフェイスを指定します。                                                                                                                                                            |
| ステップ 4 | <b>auto qos voip {cisco-phone   trust}</b>  | 自動 QoS をイネーブルにします。<br>キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> <li><b>cisco-phone</b> インターフェイスが Cisco IP Phone に接続されている場合、着信パケットの QoS ラベルは IP Phone が検出されたときのみ信頼されます。</li> <li><b>trust</b> アップリンク インターフェイスが信頼できるスイッチまたはルータに接続されていて、入力パケット内の VoIP 分類が信頼されます。</li> </ul> |
| ステップ 5 | <b>end</b>                                  | イネーブル EXEC モードに戻ります。                                                                                                                                                                                                                                                                |
| ステップ 6 | <b>show auto qos interface interface-id</b> | 設定を確認します。<br><br>このコマンドは、最初に適用された自動 QoS 設定を表示するもので、有効になったユーザによる変更は反映されません。                                                                                                                                                                                                          |

自動 QoS の詳細については、「[自動 QoS の設定](#)」(p.29-17) を参照してください。

次の例は、自動 QoS がイネーブルの場合に自動生成される QoS コマンドを表示する方法を示します。

```
Switch# debug auto qos
AutoQoS debugging is on
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# auto qos voip cisco-phone
```

## show forward コマンドの使用例

show forward イネーブル EXEC コマンドの出力から、インターフェイスに入るパケットの性質に関する有意義な情報を取得できます。パケットに関して入力されたパラメータに応じて、参照テーブル結果、転送宛先の計算に使用されるマップとマスク、ビットマップ、および出力側の情報を表示します。



(注) show forward コマンドの構文および使用方法の詳細については、このリリースのコマンド リファレンスを参照してください。

次に、FastEthernet ポート 8 に対する show forward イネーブル EXEC コマンドの出力例を示します。VLAN ID、送信元および宛先 MAC アドレス、送信元と宛先 IP アドレスが示されています。

```
Switch# show forward fastethernet0/8 vlan 8 0000.1111.2222 0022.3355.9800 ip 8.8.8.10
4.4.4.33 255
signature:00000007, comparison ind:10, control info:2000941A control map:00000000
vlan:8, vlanid entry:000C0012 00000000 00000000 04620000
vlan:8, vlanid entry:000C0012 00000000 00000000 04620000

lookup key bk adata rawoff secoff sec
qos 940808080A04040421 800000000000FF0000 0 00000000 006304 004064 4
acl 940808080A04040421 800000000000FF0000 1 00000082 045408 002016 1
learn 187008000011112222 801008002233559800 0 80010003 002176 002176 0
forw 187008000011112222 801008002233559800 1 40020000 043328 010560 5

bridgeDestMap: 00000000 00000000 0000FFFF FFFFFFFC7
vlanMask: 00000000 00000000 0000FFFF FFFFFFFE7F
portMask: 00000000 00000000 00000000 00000080
sourceMask: 00000000 00000000 00000000 00000000
globalMap: 00000000 00000000 00000000 00000000
globalMask: 00000000 00000000 0002FFFF EFFFFFFC03
forwMap: 00000000 00000000 00000000 00000100

frame notifies:
src u_dat vlan fl q-map
2 00 8 00 00000000 00000000 00000000 00000100
Egress q 8
signature:00000007, comparison ind:10, control info:2000941A control map:00000000
vlan:8, vlanid entry:000C0012 00000000 00000000 04620000
FastEthernet0/9 vlan 8, dst 0022.3355.9800 src 0000.1111.2222, cos 0x0, dscp 0x0
```

これらの情報は、テクニカル サポート担当者がスイッチの Application-Specific Integrated Circuit (ASIC; 特定用途向け IC) に関する詳細情報を利用するうえで役立ちます。ただし、一般のユーザも [Egress q] セクションを参照し、出力インターフェイスに関する情報を入手できます。個別の宛先ポートごとに、出力セクションがあります。出力インターフェイス、出力 VLAN ID、および書き換えられたフレームの宛先 MAC アドレスを含む行の情報は重要です。上記の出力例から、出力インターフェイスが FastEthernet 9 ポートで、出力 VLAN が VLAN 8 であることがわかり、また書き換えられたフレームの送信元および宛先 MAC アドレスを判別することもできます。

出力インターフェイスがトランク ポートで、さまざまな VLAN 上でフレームの複数のコピーを送信する必要がある場合 (IP マルチキャスト フレームなど) 同じ出力インターフェイス名と異なる出力 VLAN が複数の行に表示されることがあります。出力のセキュリティ ACL がない場合は、出力ポートを示す行のない [Egress q] セクションが 1 つまたは複数表示されることもあります。これは、出力 ACL によってパケットが拒否されるためです。

パケットの宛先の 1 つが CPU である場合は `[Cpu q]` セクションが表示され、そのあとにキューの名前が表示されます。キューの名前は、`show controllers cpu-interface` イネーブル EXEC コマンドによって出力されるキュー名のいずれかに対応している必要があります（このコマンドを実行すると、各キューで受信されたパケット名に対する統計情報が表示されます）。

次に、`[Cpu q]` セクションの表示例を示します。

```
Cpu q:100 - routing queue
```

## クラッシュ情報ファイル

クラッシュ情報ファイルには、シスコのテクニカルサポートスタッフがソフトウェア イメージの障害（クラッシュ）の原因となる問題をデバッグするときに役立つ情報が保存されています。クラッシュ情報は障害発生時にコンソールに出力され、障害後最初のイメージ起動時にクラッシュ情報ファイルが作成されます。

ファイル内の情報には、障害が発生したソフトウェア イメージの名前やバージョン、プロセッサレジスタのダンプ、およびスタックトレースが含まれます。`show tech-support` イネーブル EXEC コマンドを使用して、この情報をシスコのテクニカルサポートスタッフに提供してください。

すべてのクラッシュ情報ファイルは、フラッシュ ファイル システム内の次のディレクトリに保管されます。

```
flash:/crashinfo/crashinfo_n (n はシーケンス番号)
```

新たに作成されるクラッシュ情報ファイルごとに、既存のシーケンス番号よりも大きなシーケンス番号が使用されるため、シーケンス番号が最大であるファイルに最新の障害が記述されます。スイッチにはリアルタイム クロックがないため、タイムスタンプの代わりにバージョン番号が使用されます。ファイル作成時に使用されるファイル名を変更することはできません。ただし、ファイルが作成されたあとに、`rename` イネーブル EXEC コマンドを使用して名前を変更することもできますが、`show stacks` または `show tech-support` イネーブル EXEC コマンドを実行しても、名前が変更されたファイルの内容は表示されません。クラッシュ情報ファイルを削除する場合は、`delete` イネーブル EXEC コマンドを使用します。

最新のクラッシュ情報ファイル（つまり、ファイル名の末尾のシーケンス番号が最大であるファイル）を表示する場合は、`show stacks` または `show tech-support` イネーブル EXEC コマンドを使用します。`more` や `copy` イネーブル EXEC コマンドなど、ファイルをコピーまたは表示するコマンドを使用し、ファイルにアクセスすることもできます。