



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した Catalyst 3550 の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。問題の性質に応じて、コマンドライン インターフェイス (CLI)、デバイス マネージャ、または Network Assistant を使用して、問題を特定し解決できます。



(注)

この章で使用するコマンドの構文および使用方法の詳細については、このリリースに対応するコマンド 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。

この章の内容は、次のとおりです。

- 「回復手順の使用」 (P.37-1)
- 「自動ネゴシエーションの不一致の防止」 (P.37-10)
- 「GBIC モジュールのセキュリティと識別」 (P.37-11)
- 「接続性の問題の診断」 (P.37-11)
- 「PoE スイッチ ポートのトラブルシューティング」 (P.37-16)
- 「debug コマンドの使用」 (P.37-17)
- 「show forward コマンドの使用」 (P.37-19)
- 「crashinfo ファイルの使用」 (P.37-21)



(注)

ACL を適用後、パケットのパフォーマンスの問題が発生しているか、TCAM 容量に関するメッセージを受信している場合は、「ACL リソース使用量と設定上の問題の表示」 (P.28-45) を参照してください。

回復手順の使用

ここで紹介する回復手順を実行するには、スイッチを直接操作してください。

- 「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.37-2)
- 「コマンド スイッチで障害が発生した場合の回復」 (P.37-6)
- 「メンバ スイッチとの接続の回復」 (P.37-10)

ソフトウェア障害からの回復

スイッチ ソフトウェアが破損する状況としては、アップグレードを行った場合、スイッチに誤ったファイルをダウンロードした場合、イメージファイルを削除した場合などが考えられます。いずれの場合にも、スイッチは電源投入時自己診断テスト (POST) に失敗し、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て、破損したイメージ ファイルまたは間違っイメージ ファイルを回復します。XMODEM プロトコルをサポートするソフトウェア パッケージは多数あり、使用するエミュレーション ソフトウェアによって、この手順は異なります。

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 の上の LED が消灯してから 1 ~ 2 秒後に、Mode ボタンを放します。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、9600 にリセットされます。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 ファイルがある場合にはロードします。
- ```
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 ソフトウェアに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

スイッチを直接操作できるエンド ユーザは、スイッチの電源投入時に起動プロセスを中断して新しいパスワードを入力することにより、パスワードを紛失した状態から回復できます。これは、Catalyst 3550 スwitch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、システム管理者はデフォルト設定に戻す場合に限りエンドユーザによるパスワードのリセットを許可することによって、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 スイッチのパスワードをリセットしようとするエンドユーザであり、パスワード回復がディセーブルになっている場合、リカバリ処理中にステータスメッセージにこの情報が表示されます。

スイッチ パスワードを忘れるか紛失した場合は、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** 電源コードをスイッチに再接続してから 15 秒以内に、Mode ボタンを押します。このときポート 1X の上のシステム LED はグリーンに点滅しています。システム LED が一瞬オレンジに点灯してからグリーンになるまで Mode ボタンを押したままにしてください。グリーンになったら Mode ボタンを離します。

ソフトウェアについての情報および指示が数行表示され、パスワード回復手順がディセーブルであるかどうかが表示されます。

- 次の内容で始まる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の場合のパスワード回復」(P.37-3) に進んで、その手順に従います。

- 次の内容で始まる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.37-5) に進んで、その手順に従います。

パスワード回復がイネーブルの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の場合は、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、9600 にリセットされます。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 ファイルがある場合にはロードします。
- ```
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 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
```
- セットアップ 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、特権 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 を押して応答します。
- これで、コンフィギュレーション ファイルがリロードされ、パスワードを変更できます。
- 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。数字で始めることができます。大文字と小文字が区別され、スペースを使用できますが、先行スペースは無視されます。
- ステップ 12** 特権 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状態になることがあります。この状態になっているインターフェイスを調べるには、**show running-config** 特権 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 コマンドを入力して、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の場合、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 (仮想 LAN) コンフィギュレーション ファイルがあるかどうかを確認してください。

- **n** (no) を入力すると、**Mode** ボタンを押さなかった場合と同様に、通常のブートプロセスが継続されます。ブートローダ プロンプトにはアクセスできません。したがって、新しいパスワードを入力できません。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るときに、パスワードをリセットできます。

パスワード回復メカニズムがディセーブルの場合は、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 ファイルがある場合にはロードします。
- ```
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 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
```

セットアップ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、特権 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。数字で始めることができます。大文字と小文字が区別され、スペースを使用できますが、先行スペースは無視されます。

ステップ 8 特権 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状態になることがあります。この状態になっているインターフェイスを調べるには、**show running-config** 特権 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 コマンドを入力して、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。システム管理者によって、バックアップスイッチと VLAN コンフィギュレーション ファイルが使用可能に設定されている場合は、これらを使用します。

コマンドスイッチで障害が発生した場合の回復

ここでは、コマンドスイッチで障害が発生した場合の回復手順について説明します。ホットスタンバイ ルータ プロトコル (HSRP) を使用すると、冗長コマンドスイッチグループを設定できます。詳細については、第 5 章「スイッチのクラスタ化」、第 32 章「HSRP の設定」、および Cisco.com から入手できる『*Getting Started with Cisco Network Assistant*』を参照してください。



(注) HSRP は、クラスタを冗長構成にする場合に適しています。

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、メンバスイッチとの管理接続が失われるので、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は影響を受けません。また、メンバスイッチも通

常どおりにパケットを転送します。メンバスイッチは、ポートを介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できます。

コマンド対応メンバスイッチまたは他のスイッチに IP アドレスを割り当て、コマンドスイッチのパスワードを書き留め、メンバスイッチと交換用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により、コマンドスイッチ障害に備えます。ここでは、故障したコマンドスイッチを交換する 2 つの解決方法について説明します。

- 故障したコマンドスイッチをクラスタメンバと交換する場合
- 故障したコマンドスイッチを他のスイッチと交換する場合

コマンド対応スイッチについては、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と交換する場合

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対応メンバ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 メンバスイッチからコマンドスイッチを外し、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代わりに新しいメンバスイッチを取り付け、コマンドスイッチとクラスタメンバ間の接続を復元します。

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ール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、特権 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 クラスタからメンバスイッチを削除します。

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

ステップ 8 特権 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て、スイッチの IP 情報を設定します。IP アドレス情報およびパスワードを入力するように要求されます。特権 EXEC モードから **setup** と入力し、Return 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スイッチによって異なります。

```
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ければ、**enable** と入力し、**Return** を押してください。セットアッププログラムを開始するには、**setup** と入力し、**Return** を押してください。

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。

ホスト名を入力するように要求された場合、コマンドスイッチ上で指定できるホスト名の文字数は 28 文字、メンバスイッチ上では 31 文字に制限されていることに注意してください。どのスイッチでも、ホスト名の最終文字として **-n** (**n** は数字) を使用しないでください。

Telnet (仮想端末) パスワードを入力するように要求された場合、パスワードには 1 ~ 25 文字の英数字を使用でき、大文字と小文字が区別され、スペースを使用できますが、先行スペースは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** パスワードを入力するように要求された場合、故障したコマンドスイッチのパスワードを再び入力してください。

ステップ 13 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** を押します (要求された場合)。

ステップ 14 クラスタに名前を指定し、**Return** を押します (要求された場合)。

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

ステップ 15 初期設定が表示されたら、アドレスが正しいことを確認してください。

ステップ 16 表示された情報が正しい場合は、**Y** を入力し、**Return** を押します。

情報に誤りがある場合には、**N** を入力し、**Return** 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、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 メニューから、[Add to Cluster] を選択し、クラスタへ追加する候補スイッチの一覧を表示します。

故障したコマンドスイッチを他のスイッチと交換する場合

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対応スイッチと交換する場合、次の手順に従ってください。

ステップ 1 メンバスイッチからコマンドスイッチを外し、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代わりに新しいスイッチを取り付け、コマンドスイッチとクラスタメンバ間の接続を復元します。

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。ポートの詳しい使用方法については、スイッチのハードウェア インストール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、特権 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て、スイッチの IP 情報を設定します。

IP アドレス情報およびパスワードを入力するように要求されます。特権 EXEC モードから **setup** と入力し、**Return** 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異なります。

```
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ければ、**enable** と入力し、**Return** を押してください。セットアッププログラムを開始するには、**setup** と入力し、**Return** を押してください。

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。

ホスト名を入力するように要求された場合、コマンドスイッチ上で指定できるホスト名の文字数は 28 文字に制限されていることに注意してください。どのスイッチでも、ホスト名の最終文字として **-n** (**n** は数字) を使用しないでください。

Telnet (仮想端末) パスワードを入力するように要求された場合、パスワードには 1 ~ 25 文字の英数字を使用でき、大文字と小文字が区別され、スペースを使用できますが、先行スペースは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** パスワードを入力するように要求された場合、故障したコマンドスイッチのパスワードを再び入力してください。

ステップ 10 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** を押します (要求された場合)。

ステップ 11 クラスタに名前を指定し、**Return** を押します (要求された場合)。

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

- ステップ 12** 初期設定が表示されたら、アドレスが正しいことを確認してください。
- ステップ 13** 表示された情報が正しい場合は、**Y** を入力し、**Return** を押します。
情報に誤りがある場合には、**N** を入力し、**Return** 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、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 メニューから、[Add to Cluster] を選択し、クラスタへ追加する候補スイッチの一覧を表示します。

メンバスイッチとの接続の回復

構成によっては、コマンドスイッチとメンバスイッチ間の接続を維持できない場合があります。メンバに対する管理接続を維持できなくなった場合で、かつ、メンバスイッチが正常にパケットを転送している場合は、次の矛盾がないかどうかを確認してください。

- メンバスイッチ (Catalyst 3550、Catalyst 3500 XL、Catalyst 2955、2950、2940、2900 XL、2820、および 1900) は、ネットワーク ポートとして定義されたポートを介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、および Catalyst 1900 メンバスイッチは、同じ管理 VLAN に所属するポートを介してコマンドスイッチに接続する必要があります。
- セキュアポートを介してコマンドスイッチに接続するメンバスイッチ (Catalyst 3550、Catalyst 3500 XL、Catalyst 2950、Catalyst 2940、Catalyst 2900 XL、Catalyst 2820、および 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 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 モジュールポートを除く 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。このプロトコルは設定を適切に調整しないことがあり、その場合はパフォーマンスが低下します。不一致は次の条件で発生します。

- 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で設定された速度またはデュプレックスのパラメータと異なっている場合。
- ポートを自動ネゴシエーションに設定したが、接続先ポートは自動ネゴシエーションを使用しない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引き出し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。

- 速度とデュプレックスの両方について、両方のポートで自動ネゴシエーションを実行させます。
- 接続の両側でポートの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) 接続先装置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設定を一致させます。速度パラメータは、接続先の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

Cisco Course Wave Division Multiplexer (CWDM) ギガビット インターフェイス コンバータ (GBIC) モジュールには、シリアル EEPROM があり、これには、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、および冗長巡回検査 (CRC) が格納されています。スイッチに CWDM GBIC モジュールを装着すると、スイッチ ソフトウェアは、EEPROM を読み取ってシリアル番号、ベンダー名、およびベンダー ID を確認し、セキュリティ コードおよび CRC を再計算します。シリアル番号、ベンダー名、ベンダー ID、セキュリティ コード、または CRC が無効な場合、スイッチはインターフェイスを `errdisable` ステートにします。



(注)

他社の CWDM GBIC モジュールを使用している場合、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に交換します。

シスコの GBIC モジュールを装着したら、`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 ステータスを確認し、`errdisable` ステートから回復する時間間隔を入力します。この時間間隔が経過すると、スイッチは `errdisable` ステートからインターフェイスを復帰させ、操作を再試行します。`errdisable recovery` コマンドの詳細については、このリリースに対応するコマンド リファレンスを参照してください。

接続性の問題の診断

ここでは、接続性の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.37-11)
- 「IP traceroute の使用」(P.37-13)
- 「レイヤ 2 traceroute の使用」(P.37-14)

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.37-11)
- 「ping の実行」(P.37-12)

ping の概要

スイッチは IP の ping をサポートしており、これを使ってリモート ホストへの接続をテストできます。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 は次のいずれかの応答を返します。

- 正常な応答：正常な応答 (*hostname* が存在する) は、ネットワーク トラフィックにもよりますが、1 ~ 10 秒以内で発生します。
- 宛先の応答なし：ホストが応答しない場合、*no-answer* メッセージが返ってきます。
- ホスト不明：ホストが存在しない場合、*unknown host* メッセージが返ってきます。
- 宛先に到達不能：デフォルト ゲートウェイが指定されたネットワークに到達できない場合、*destination-unreachable* メッセージが返ってきます。

- ネットワークまたはホストに到達不能：ルート テーブルにホストまたはネットワークに関するエントリがない場合、*network or host unreachable* メッセージが返ってきます。

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になります。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。

スイッチからネットワーク上の別のデバイスに ping を実行するには、特権 EXEC モードで次のコマンドを使用します。

コマンド	目的
<code>ping [ip] {host address}</code>	IP 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へ ping を実行します。



(注)

ping コマンドでは、他のプロトコル キーワードも使用可能ですが、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 で、ping の文字出力について説明します。

表 37-1 ping の出力表示文字

文字	説明
!	感嘆符 1 個につき 1 回の応答を受信したことを示します。
.	ピリオド 1 個につき応答待ちの間にネットワーク サーバのタイムアウトが 1 回発生したことを示します。
U	宛先到達不能エラー PDU を受信したことを示します。
C	輻輳に遭遇したパケットを受信したことを示します。
I	ユーザによりテストが中断されたことを示します。
?	パケット タイプが不明です。
&	パケットの存続時間を超過したことを示します。

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放し、**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.37-13)
- 「IP traceroute の実行」(P.37-13)

IP traceroute の概要

IP traceroute を使用すると、ネットワーク上でパケットが通過するパスをホップバイホップで識別できます。このコマンドを実行すると、トラフィックが宛先に到達するまでに通過するルータなどのすべてのネットワーク層（レイヤ 3）デバイスが表示されます。

スイッチは、**traceroute** 特権 EXEC コマンドの送信元または宛先として指定できます。また、スイッチは **traceroute** コマンドの出力でホップとして表示される場合があります。スイッチを **traceroute** の宛先とすると、スイッチは、**traceroute** の出力で最終の宛先として表示されます。中間スイッチが同じ VLAN 内でポート間のパケットのブリッジングだけを行う場合、**traceroute** の出力に中間スイッチは表示されません。ただし、中間スイッチが、特定の packets をルーティングするマルチレイヤスイッチの場合、中間スイッチは **traceroute** の出力にホップとして表示されます。

traceroute 特権 EXEC コマンドは、IP ヘッダーの存続可能時間（TTL）フィールドを使用して、ルータおよびサーバで特定のリターンメッセージが生成されるようにします。**traceroute** の実行は、ユーザデータグラム プロトコル（UDP）データグラムを、TTL フィールドが 1 に設定されている宛先ホストへ送信することから始まります。ルータは 1 または 0 の TTL 値を発見すると、データグラムをドロップして、送信元にインターネット制御メッセージ プロトコル（ICMP）**time-to-live-exceeded** メッセージを送り返します。**traceroute** は、ICMP **time-to-live-exceeded** メッセージの送信元アドレスフィールドを調べて、最初のホップのアドレスを判別します。

ネクスト ホップを識別するために、**traceroute** は TTL 値が 2 の UDP パケットを送信します。1 番目のルータは、TTL フィールドの値から 1 を差し引いて次のルータにデータグラムを送信します。2 番目のルータは、TTL 値が 1 であることを確認すると、このデータグラムを廃棄し、**time-to-live-exceeded** メッセージを送信元へ返します。このように、データグラムが宛先ホストに到達するまで（または TTL の最大値に達するまで）TTL の値は増分され、処理が続けられます。

データグラムが宛先に到達したことを判別するために、**traceroute** は、データグラムの UDP の宛先ポート番号を宛先ホストが使用しないような非常に大きい値に設定します。ホストが、ローカルで使用されない宛先ポート番号を持つ自分自身宛のデータグラムを受信すると、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すべてのエラーは、中間ホップから送信されるため、ポート到達不能エラーを受信することは、このメッセージが宛先から送信されたことを意味します。

IP traceroute の実行

パケットがネットワークを通過するパスを追跡するには、特権 EXEC モードで次の手順を実行します。

コマンド	目的
traceroute ip host	IP を使用して、パケットがネットワークを通過するパスを追跡します。



(注) **traceroute** 特権 EXEC コマンドでは、他のプロトコル キーワードも使用可能ですが、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 **traceroute** を実行する例を示します。

```
Switch# traceroute 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#
```

ホップ カウント、ルータの IP アドレス、および送信される 3 つのプロープそれぞれのラウンドトリップ時間（ミリ秒）が表示されます。

表 37-2 **traceroute** の出力表示文字

文字	説明
*	プローブがタイムアウトになりました。
?	パケット タイプが不明です。
A	管理上、到達不能です。通常、この出力は、アクセス リストがトラフィックをブロックしていることを表しています。
H	ホストが到達不能です。
N	ネットワークが到達不能です。
P	プロトコルが到達不能です。
Q	発信元。
U	ポートが到達不能です。

進行中の追跡を終了するには、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放し、**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.37-15)
- 「使用上のガイドライン」 (P.37-15)
- 「物理パスの表示」 (P.37-16)

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識別できます。レイヤ 2 Traceroute は、ユニキャストの送信元および宛先 MAC アドレスだけをサポートします。パス内のスイッチが保持する 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 をサポートしないデバイスをパスで検出すると、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てしまいます。

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まで、または宛先デバイスから宛先ホストまでのパスは識別できません。

使用上のガイドライン

レイヤ 2 traceroute の使用上の注意事項を次に示します。

- Cisco Discovery Protocol (CDP) がネットワーク上のすべてのデバイスでイネーブルでなければなりません。レイヤ 2 traceroute を適切に機能させるためには、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 に対して透過的な場合、スイッチはこれらのデバイスを通過するパスを識別できません。



(注) CDP をイネーブルにする場合の詳細については第 22 章「CDP の設定」を参照してください。

- スイッチは、**ping** 特権 EXEC コマンドを使用して接続をテストする場合に他のスイッチから到達できます。物理パス内のすべてのスイッチは、他のスイッチから到達可能でなければなりません。
- パス内で識別可能な最大ホップ数は 10 です。
- 送信元デバイスから宛先デバイスの物理パス内にないスイッチに、**traceroute mac** または **traceroute mac ip** 特権 EXEC コマンドを実行できます。パス内のすべてのスイッチは、このスイッチから到達可能でなければなりません。
- 指定した送信元および宛先 MAC アドレスが同一 VLAN に属する場合、**traceroute mac** コマンド出力はレイヤ 2 パスのみを表示します。指定した送信元および宛先 MAC アドレスが、それぞれ異なる VLAN に属している場合は、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または宛先 MAC アドレスを指定すると、パスは識別されず、エラー メッセージが表示されます。
- 送信元または宛先 MAC アドレスが複数の VLAN に属する場合は、送信元および宛先 MAC アドレスの両方が属している VLAN を指定する必要があります。VLAN を指定しないと、パスは識別されず、エラー メッセージが表示されます。
- 指定した送信元および宛先 MAC アドレスが同一サブネットに属する場合、**traceroute mac ip** コマンド出力はレイヤ 2 パスを表示します。IP アドレスを指定した場合、スイッチはアドレス解決プロトコル (ARP) を使用し、IP アドレスとそれに対応する MAC アドレスおよび VLAN ID を関連付けます。
 - 指定の IP アドレスの ARP のエントリが存在している場合、スイッチは関連付けられた MAC アドレスを使用し、物理パスを識別します。
 - ARP のエントリが存在しない場合、スイッチは ARP クエリーを送信し、IP アドレスを解決しようと試みます。IP アドレスが解決されない場合は、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介して 1 つのポートに接続されている場合（たとえば複数の CDP ネイバーがポートで検出された場合）、レイヤ 2 `traceroute` 機能はサポートされません。複数の CDP ネイバーが 1 つのポートで検出された場合、レイヤ 2 パスは特定されず、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 ではサポートされません。

物理パスの表示

次のいずれかの特権 EXEC コマンドを使用して、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表示できます。

- `traceroute mac [interface interface-id] {source-mac-address} [interface interface-id] {destination-mac-address} [vlan vlan-id] [detail]`
- `traceroute 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障害」(P.37-16)
- 「偽のリンク アップによりポートが使用不可になる」(P.37-16)

電力消失によるポートの障害

Power over Ethernet (PoE) スイッチ ポートに接続され、AC 電源から電力が供給されている受電デバイス (Cisco IP Phone 7910 など) に AC 電源から電力が供給されない場合、そのデバイスは `errdisable` ステートになることがあります。エラー ディセーブル状態から回復するためには、`shutdown` インターフェイス コンフィギュレーション コマンドを入力し、次に `no shutdown` インターフェイス コマンドを入力してください。スイッチで自動回復を設定し、`errdisable` ステートから回復することもできます。`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、指定した期間が経過した後自動的にインターフェイスを `errdisable` ステートから復帰させます。

このリリースのコマンド リファレン스에記載されている次のコマンドを使用すると、PoE ポート ステータスをモニタできます。

- `show controllers power inline` 特権 EXEC コマンド
- `show power inline` 特権 EXEC コマンド
- `debug ilpower` 特権 EXEC コマンド

偽のリンク アップによりポートが使用不可になる

シスコ受電デバイスをポートに接続し、`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は、ポートで不正リンク アップが発生し、ポートが `errdisable` ステートになることがあります。ポートを `error-disabled` 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 コマンドを入力します。

`power inline never` コマンドで設定したポートにシスコ受電デバイス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。

- 「特定機能に関するデバッグのイネーブル化」(P.37-17)
- 「システム全体診断のイネーブル化」(P.37-18)
- 「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.37-18)
- 「`debug auto qos` コマンドの使用」(P.37-19)



注意

デバッグ出力は CPU プロセスで高プライオリティが割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、`debug` コマンドは、絞り込まれた問題のトラブルシューティングか、シスコのテクニカルサポート スタッフとのトラブルシューティングセッション中に限定的に使用してください。ネットワーク トラフィック量やユーザ数が少ない期間に `debug` コマンドを使用することをお勧めします。デバッグをこのような時間帯に行うと、`debug` コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。



(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` コマンドはすべて特権 EXEC モードで実行します。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、特権 EXEC モードで次のコマンドを入力します。

```
Switch# debug etherchannel
```

スイッチは `no` 形式のコマンドが入力されるまで、出力を生成し続けます。

`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、次の状況が考えられます。

- 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` コマンドを使用して、設定を確認します。
- 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特定の間は、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。デバッグする機能によっては、TCP/IP の `ping` コマンドなどを使用すると、ネットワーク トラフィックを生成できます。

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

```
Switch# no debug etherchannel
```

また、特権 EXEC モードで `undebug` 形式のコマンドを入力することもできます。

```
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、特権 EXEC モードで次のコマンドを入力します。

```
Switch# show debugging
```

システム全体診断のイネーブル化

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

```
Switch# debug all
```



注意

デバッグ出力は他のネットワーク トラフィックより優先され、**debug all** 特権 EXEC コマンドは他の **debug** コマンドより出力が大量になるので、スイッチのパフォーマンスが極度に低下したり、場合によっては使用不能になったりすることがあります。状況にかかわらず、特定性の高い **debug** コマンドを使用するのが原則です。

no debug all 特権 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。いずれかの **debug** コマンドが誤ってイネーブルのままにならないようにするには、**no debug all** コマンドを使用すると便利です。

デバッグおよびエラー メッセージ出力のリダイレクト

ネットワーク サーバはデフォルトで、**debug** コマンドおよびシステム エラー メッセージの出力をコンソールに送信します。このデフォルトの設定を使用する場合は、ポートに接続する代わりに、仮想端末接続によってデバッグ出力をモニタできます。

指定できる宛先として、コンソール、仮想端末、内部バッファ、および **syslog** サーバを実行している UNIX ホストがあります。**Syslog** フォーマットは、4.3 BSD UNIX およびそのバリエーションと互換性があります。



(注)

デバッグの出力先がシステムのオーバーヘッドに影響を与えないように注意してください。コンソールでメッセージ ロギングを行うと、オーバーヘッドが非常に大きくなりますが、仮想端末でメッセージ ロギングを行うと、オーバーヘッドが小さくなります。**Syslog** サーバでメッセージ ロギングを行うと、オーバーヘッドはさらに小さくなり、内部バッファであれば最小限ですみます。

システム メッセージ ロギングの詳細については、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

Automatic QoS (Auto-QoS) がイネーブルのときに自動的に生成される Quality of Service (QoS) コマンドを表示するには、**debug auto qos** 特権 EXEC コマンドを使用します。

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

	コマンド	目的
ステップ1	debug auto qos	自動 QoS 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設定された場合、スイッチは自動 QoS がイネーブルまたはディセーブルに設定されると自動的に生成される QoS コマンドを表示します。
ステップ2	configure terminal	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	interface interface-id	Cisco IP Phone に接続するインターフェイスを指定し、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。ネットワークの内部で別のスイッチまたはルータに接続する、アップリンク インターフェイスを指定することもできます。
ステップ4	auto qos voip {cisco-phone trust}	自動 QoS をイネーブルにします。 キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> • cisco-phone : 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 が検出された場合だけ信頼されます。 • trust : 信頼できるスイッチまたはルータにアップリンク インターフェイスが接続されていて、入力パケット内の VoIP 分類が信頼されます。
ステップ5	end	特権 EXEC モードに戻ります。
ステップ6	show auto qos interface interface-id	入力内容を確認します。 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、ユーザにより有効になった変更は反映されません。

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

次に、自動 QoS がイネーブルにされた場合に、自動的に生成される QoS コマンドを表示する例を示します。

```
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

show platform forward 特権 EXEC コマンドの出力からは、インターフェイスに入るパケットの性質に関して、有意義な情報がいくつか得られます。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が表示されます。



(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、このリリースに対応するコマンドリファレンスを参照してください。

次に、ファストイーサネットポート 8 に対する **show forward** 特権 EXEC コマンドの出力例を示します。ここで、VLAN ID、送信元および宛先の MAC アドレス、送信元および宛先 IP アドレスが指定されています。

```
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	80000000000000FF0000	0	00000000	006304	004064 4
acl	940808080A04040421	80000000000000FF0000	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
```

この情報の多くは、主に、スイッチの特定用途向け IC (ASIC) に関する詳細情報を利用するテクニカルサポート担当者に役立ちます。ただし、出力インターフェイスに関する情報を入手するために *Egress q* セクションを表示できます。それぞれの宛先ポートの出力セクションがあります。重要な情報は、出力インターフェイス、出力 VLAN ID、およびフレームの書き換えられた宛先 MAC アドレスの名前を含む行にあります。例では、出力インターフェイスがファストイーサネットポート 9 であり、出力 VLAN が VLAN 8 であることが表示され、フレームの書き換えられた送信元および宛先の MAC アドレスが表示されています。

出力インターフェイスが異なる VLAN でフレーム (IP マルチキャストフレームなど) の複数のコピーを送信する必要があるトランクポートの場合、複数の回線には同じ出力インターフェイス名と、異なる出力 VLAN が含まれることがあります。出力セキュリティアクセスコントロールリスト (ACL) がある場合、*Egress q* セクションの 1 つ以上に、出力ポートをリストする行が含まれない可能性があります。これは、出力 ACL がパケットを拒否した場合に発生します。

CPU がパケットの宛先の 1 つである場合は、*CPU q* セクションに続いて、キュー名が表示されます。この名前は、**show controllers cpu-interface** 特権 EXEC コマンドの出力のキュー名の 1 つに対応します。ここに、各キューで受信したパケットの数の統計情報が表示されます。

次に、*Cpu q* のセクションの表示の例を示します。

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

crashinfo ファイルの使用

crashinfo 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。スイッチで障害が発生するとコンソールにクラッシュ情報が書き込まれ、障害後にイメージを起動するとき（システム障害中ではない）にこの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** 特権 EXEC コマンドを使用することによって、この情報をシスコのテクニカル サポート 担当者に提供できます。

すべての crashinfo 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存されます。

flash:/crashinfo/crashinfo_*n* (*n* はシーケンス番号)

新しい crashinfo ファイルが作成されるたびに、前のシーケンス番号より大きいシーケンス番号が使用されるので、シーケンス番号が最大のファイルに、最新の障害が記述されています。タイムスタンプではなく、バージョン番号を使用するのは、スイッチにリアルタイム クロックが組み込まれていないからです。ファイル作成時にシステムが使用す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てから、**rename** 特権 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** 特権 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。**delete** 特権 EXEC コマンドを使用して crashinfo ファイルを削除できます。

最新の crashinfo 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** 特権 EXEC コマンドを使用します。**more** 特権 EXEC コマンド、**copy** 特権 EXEC コマンドなど、ファイルのコピーまたは表示が可能な任意のコマンドを使用して、ファイルにアクセスすることもできます。

