



## 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 スイッチの問題点を特定し、解決する方法について説明します。2975 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 を使用して、問題を特定し解決できます。

特に明記しないかぎり、スイッチという用語はスタンドアロン スイッチおよびスイッチ スタックを意味します。

LED の説明など、トラブルシューティングの詳細については、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。



(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、このリリースのコマンド リファレンス、および『*Cisco IOS Commands Master List*』 Release 12.2 を参照してください。このドキュメントは、Cisco.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References] から入手できます。

この章で説明する内容は、次のとおりです。

- 「ソフトウェアで障害が発生した場合の回復」 (P.36-2)
- 「パスワードを忘れた場合の回復」 (P.36-3)
- 「スイッチ スタック問題の回避」 (P.36-8)
- 「コマンド スイッチで障害が発生した場合の回復」 (P.36-9)
- 「クラスタ メンバー スイッチとの接続の回復」 (P.36-12)



(注)

回復手順を実行するには、スイッチを直接操作しなければなりません。

- 「自動ネゴシエーションの不一致の防止」 (P.36-12)
- 「PoE スイッチ ポートのトラブルシューティング」 (P.36-13)
- 「SFP モジュールのセキュリティと識別」 (P.36-13)
- 「SFP モジュール ステータスのモニタ」 (P.36-14)
- 「ping の使用」 (P.36-14)
- 「レイヤ 2 traceroute の使用」 (P.36-16)
- 「IP traceroute の使用」 (P.36-17)
- 「TDR の使用」 (P.36-19)
- 「debug コマンドの使用」 (P.36-20)

- 「show platform forward コマンドの使用」(P.36-22)
- 「crashinfo ファイルの使用」(P.36-23)

## ソフトウェアで障害が発生した場合の回復

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 Power-On Self-Test (POST; 電源投入時セルフテスト) 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た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。

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なければなりません。

**ステップ 1** PC 上で、Cisco.com から tar 形式のソフトウェア イメージファイル (image\_filename.tar) をダウンロードします。

Cisco IOS イメージは、tar ファイルのディレクトリ内に bin ファイルとして格納されます。Cisco.com 上のソフトウェア イメージファイルの検索方法については、リリース ノートを参照してください。

**ステップ 2** tar ファイルから bin ファイルを抽出します。

- Windows を使用している場合は、tar ファイルの読み取り機能を備えた zip プログラムを使用します。zip プログラムを使用して bin ファイルを特定し、抽出します。
- UNIX を使用している場合は、次の手順に従ってください。

1. **tar -tvf <image\_filename.tar>** UNIX コマンドを使用して、tar ファイルの内容を表示します。

```
unix-1% tar -tvf image_filename.tar
```

2. **tar -xvf <image\_filename.tar> <image\_filename.bin>** UNIX コマンドを使用して、bin ファイルを特定し、抽出します。

```
unix-1% tar -xvf image_filename.tar image_filename.bin
x c2975-lanbase-mz.122-46.EX/c2975-lanbase-mz.122-46.EX.bin, 2928176 bytes, 5720
tape blocks
```

3. **ls -l <image\_filename.bin>** UNIX コマンドを使用して、bin ファイルが抽出されたことを確認します。

```
unix-1% ls -l image_filename.bin
-rw-r--r--  1 bobas      2928176 Apr 21 12:01
c2975-lanbase-mz.122-46.EX/c2975-lanbase-mz.122-46.EX.bin
```

**ステップ 3** 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 4** 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 5** スwitchの電源コードを取り外します。

**ステップ 6** **Mode** ボタンを押しながら、電源コードを再びスイッチに接続します。

ポート 1 の上の LED が消灯してから 1 ~ 2 秒後に、**Mode** ボタンを離します。ソフトウェアについての情報および指示が数行表示されます。

```
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 7** 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 8** 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 9** 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 10** XMODEM プロトコルを使用して、ファイル転送を開始します。

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

**ステップ 11** 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。

**ステップ 12** 新規にダウンロードされた Cisco IOS イメージを起動します。

```
switch:boot flash:image_filename.bin
```

**ステップ 13** `archive download-sw` イネーブル EXEC コマンドを使用して、スイッチまたはスイッチ スタックにソフトウェア イメージをダウンロードします。

**ステップ 14** `reload` イネーブル EXEC コマンドを使用してスイッチを再起動し、新しいソフトウェア イメージが適切に動作していることを確認します。

**ステップ 15** スイッチから、`flash:image_filename.bin` ファイルを削除します。

## パスワードを忘れた場合の回復

スイッチのデフォルト設定では、スイッチを直接操作するエンド ユーザが、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。



(注)

これらのスイッチでは、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。パスワード回復がディセーブルになっている場合に、エンド ユーザがパスワードをリセットしようとする、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。

ここでは、スイッチのパスワードを忘れた場合の回復手順について説明します。

- 「パスワード回復がイネーブルになっている場合の手順」(P.36-4)
- 「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.36-6)

パスワードの回復をイネーブルまたはディセーブルにするは、**service password-recovery** グローバル コンフィギュレーション コマンドを使用します。**service password-recovery** または **no service password-recovery** コマンドをスタック マスターに入力すると、スタック全体にコマンドが伝播され、スタック内のすべてのスイッチに適用されます。

スイッチのパスワードを忘れた場合には、次の手順に従ってください。

- 
- ステップ 1** 端末エミュレーション ソフトウェアが稼動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。スイッチ スタックに対してパスワードを回復する場合は、スタック マスターのコンソール 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** スタンドアロン スイッチまたはスイッチ スタック全体の電源を切断します。
- ステップ 4** 電源コードをスタンドアロン スイッチまたはスタック マスターに再接続してから 15 秒以内に、**Mode** ボタンを押します。このときシステム LED はグリーンに点滅しています。システム LED がアンバー (一瞬) 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を示されます。

- 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になっている場合の手順」(P.36-4) 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.36-6) に進んで、その手順に従います。

- ステップ 5** パスワードが回復したら、スタンドアロンスイッチまたはスタック マスターをリロードします。

```
Switch> reload
slot <stack-master-member-number>
Proceed with reload?[confirm] y
```

- ステップ 6** スイッチ スタックの残りのメンバーの電源をオンにします。
- 

## パスワード回復がイネーブルになっている場合の手順

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
```

- 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:
```

スイッチのファイル システムが表示されます。

```
Directory of flash:
 13 drwx      192  Mar 01 1993 22:30:48 c2975-lanbase-mz.122-46.EX
 11 -rwx      5825  Mar 01 1993 22:31:59 config.text
 18 -rwx      720   Mar 01 1993 02:21:30 vlan.dat
```

```
16128000 bytes total (10003456 bytes free)
```

**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、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
```



**(注)** 接続されたすべてのスタック メンバーの電源をオンにし、完全に初期化されるまで待機してから、ステップ 9 に進んでください。このステップに従わなかった場合は、スイッチの設定によっては設定を失う可能性もあります。

**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。

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** 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 14** スイッチ スタックをリロードします。

```
Switch# reload
```

## 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 (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、通常の起動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。

**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:
```

スイッチのファイル システムが表示されます。

```
Directory of flash:
```

```
13 drwx          192  Mar 01 1993 22:30:48 c2975-lanbase-mz.122-46.EX.0
```

```
16128000 bytes total (10003456 bytes free)
```

**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、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。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** イネーブル EXEC モードに戻ります。

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

```
Switch#
```



(注) 接続されたすべてのスタック メンバーの電源をオンにし、完全に初期化されるまで待機してから、ステップ 9 に進んでください。

**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。

## スイッチ スタック問題の回避



(注)

- スイッチ スタックに追加または削除するスイッチの電源が切断されていることを確認します。スイッチ スタックの電源に関するすべての考慮事項については、ハードウェア インストール ガイドの「Switch Installation」の章を参照してください。
- スタック メンバーを追加または削除したあとで、スイッチ スタックがすべての帯域幅 (32 Gb/s) で動作していることを確認します。スタック モード LED が点灯するまで、スタック メンバーの Mode ボタンを押します。スイッチ上の最後の 2 つのポート LED は、グリーンに点灯します。スイッチ モデルに応じて、最後の 2 つのポートは 10/100/1000 ポートまたは Small Form-factor Pluggable (SFP) モジュール ポートになります。最後の 2 つのポート LED のいずれか、または両方がグリーンに点灯しない場合は、スタックがすべての帯域幅で動作していません。
- スイッチ スタックを管理する場合は、CLI セッションを 1 つだけ使用することを推奨します。スタック マスターに複数の CLI セッションを使用する場合は、慎重に行ってください。特定のセッションで入力したコマンドは、他のセッションに表示されません。したがって、コマンドを入力したセッションを識別できなくなることがあります。
- スタック内のスイッチの位置に従ってスタック メンバー番号を手動で割り当てると、離れた位置からのスイッチ スタックのトラブルシューティングが容易になります。ただし、あとでスイッチを追加、削除、再編成する場合は、手動で割り当てられた番号を思い出す必要があります。スタック メンバー番号を手動で割り当てするには、**switch current-stack-member-number renumber new-stack-member-number** グローバル コンフィギュレーション コマンドを使用します。スタック メンバー番号の詳細については、「[メンバー番号](#)」(P.6-5) を参照してください。

スタック メンバーを同一モデルと交換した場合、新しいスイッチは交換前のスイッチとまったく同じ設定で動作します。また、新しいスイッチでは、交換前のスイッチと同じメンバー番号が使用されます。

電源がオンの状態のスタック メンバーを取り外すと、スイッチ スタックがそれぞれ同じ設定を持つ複数のスイッチ スタックに分割 (パーティション化) されます。スイッチ スタックを分割状態のまま使用する場合は、新規に作成されたスイッチ スタックの IP アドレスを変更します。パーティション化されたスイッチ スタックを元に戻す手順は、次のとおりです。

1. 新規に作成されたスイッチ スタックの電源を切断します。
2. 新しいスイッチ スタックを、StackWise ポートを介して元のスイッチ スタックに再度接続します。
3. スイッチの電源をオンにします。

スイッチ スタックおよびスタック メンバーのモニタに使用できるコマンドについては、「[スタック情報の表示](#)」(P.6-23) を参照してください。



## 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。Hot Standby Router Protocol (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。詳細は、第 5 章「スイッチのクラスタ化」を参照してください。Cisco.com から入手できる『*Getting Started with Cisco Network Assistant*』も参照してください。



(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、メンバー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、メンバースイッチも通常どおりにパケットを転送します。メンバースイッチは、コンソール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、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と交換する場合」(P.36-9)
- 「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」(P.36-11)

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。

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ーと交換する場合

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ー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との接続を切断し、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ー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ー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 にはコンソール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。コンソール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、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** クラスタからメンバースイッチを削除します。

```
イネーブル Switch(config)# no cluster commander-address
```

**ステップ 8** 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。イネーブル EXEC モードから **setup** と入力し、**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** キーを押してください。セットアッププログラムを開始するには、**setup** と入力し、**Return** キーを押してください。

**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、メンバー 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** キーを押します (要求された場合)。

**ステップ 14** クラスタに名前を指定し、**Return** キーを押します (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** キーを押します。

情報に誤りがある場合には、**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、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** 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ー間の接続を復元します。

**ステップ 2** 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 にはコンソール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。コンソール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 3** 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 4** 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 5** 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。イネーブル EXEC モードから **setup** と入力し、**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 6** 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** キーを押してください。セットアッププログラムを開始するには、**setup** と入力し、**Return** キーを押してください。

**ステップ 7** 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 8** **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 9** 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 (要求された場合)。
- ステップ 10** クラスタに名前を指定し、**Return** キーを押します (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 11** 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 12** 表示された情報が正しい場合は、**Y** を入力し、**Return** キーを押します。  
情報に誤りがある場合には、**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 13** 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 14** 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。

## クラスタ メンバー 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ー スイッチ間の接続を維持できない場合があります。メンバーに対する管理接続を維持できなくなった場合で、かつ、メンバー 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。

- メンバー スイッチ (Catalyst 3750、Catalyst 3560、Catalyst 3550、Catalyst 3500 XL、Catalyst 2970、Catalyst 2960、Catalyst 2950、Catalyst 2900 XL、Catalyst 2820、および Catalyst 1900 スイッチ) 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 メンバー 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ー スイッチ (Catalyst 3750、Catalyst 3560、Catalyst 3550、Catalyst 2970、Catalyst 2960、Catalyst 2950、Catalyst 3500 XL、Catalyst 2900 XL、Catalyst 2820、および Catalyst 1900 スイッチ) 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 プロトコルは速度 (10 Mb/s、100 Mb/s、および Small Form-Factor Pluggable [SFP] モジュール ポート以外の 1000 Mb/s) およびデュプレックス (半二重または全二重) に関するスイッチの設定を管理します。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。
- ポートが自動ネゴシエーション モードに設定されており、接続ポートが自動ネゴシエーションを指定せずに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、両端のポートに自動ネゴシエーションを実行させます。
- 接続の両端で、ポートの速度およびデュプレックス パラメータを手動設定します。



(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設定が一致するように設定します。速度パラメータは、接続ポートが自動ネゴシエーションを行わない場合でも、自動調整が可能です。

## PoE スイッチ ポートのトラブルシューティング

ここでは、Power over Ethernet (PoE) ポートのトラブルシューティングについて説明します。

### 電力喪失によるポートの障害

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装置 (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。errdisable 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 コマンドを入力してから、**no shutdown** インターフェイス コマンドを入力します。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あと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 リファレンスに記載されている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** 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

### 不正リンクアップによるポート障害

シスコ受電装置をポートに接続し、**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、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 errdisable ステートから修正するには、**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装置を接続しないでください。

## SFP モジュールのセキュリティと識別

シスコの SFP モジュールは、モジュールのシリアル番号、ベンダー名とベンダー ID、一意のセキュリティ コード、および Cyclic Redundancy Check (CRC; 巡回冗長検査) が格納されたシリアル Electrically Erasable Programmable Read-Only Memory (EEPROM; 電氣的消去再書き込み可能 ROM) を備えています。スイッチに SFP 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、ソフトウェアは、セキュリティ エラー メッセージを生成し、インターフェイスを `errdisable` ステートにします。



(注)

セキュリティ エラー メッセージは、`GBIC_SECURITY` ファシリティを参照します。スイッチは、SFP モジュールをサポートしていますが、`GBIC` (ギガビット インターフェイス コンバータ) モジュールはサポートしていません。エラー メッセージテキストは、`GBIC` インターフェイスおよびモジュールを参照しますが、セキュリティ メッセージは、実際は SFP モジュールおよびモジュール インターフェイスを参照します。エラー メッセージの詳細については、このリリースに対応するシステム メッセージ ガイドを参照してください。

他社の SFP モジュールを使用している場合、スイッチから SFP 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 SFP 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。

モジュールがシスコ製 SFP モジュールとして識別されたにもかかわらず、システムがベンダー データ情報を読み取ってその情報が正確かどうかを確認できないと、SFP モジュール エラー メッセージが生成されます。この場合、SFP モジュールを取り外して再び装着してください。それでも障害が発生する場合は、SFP モジュールが不良品である可能性があります。

## SFP モジュール ステータスのモニタ

`show interfaces transceiver` イネーブル EXEC コマンドを使用すると、SFP モジュールの物理または動作ステータスを確認できます。このコマンドは、温度や特定のインターフェイス上の SFP モジュールの現状などの動作ステータスと、アラーム ステータスを表示します。また、このコマンドを使用して SFP モジュールの速度およびデュプレックス設定も確認できます。詳細については、このリリースのコマンド リファレン스에記載された「`show interfaces transceiver`」コマンドの説明を参照してください。

## 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.36-15)
- 「[ping の実行](#)」(P.36-15)

## 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

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、イネーブル EXEC モードで次のコマンドを使用します。

コマンド	目的
ping ip <i>host</i>   <i>address</i>	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 36-1 で、ping の文字出力について説明します。

表 36-1 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。

表 36-1 ping の出力表示文字 (続き)

文字	説明
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 (デフォルトでは **Ctrl-^ X**) を入力してください。Ctrl キー、Shift キー、および 6 キーを同時に押してから離し、そのあと 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.36-16)
- 「使用時の注意事項」(P.36-16)
- 「物理パスの表示」(P.36-17)

## 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 はユニキャスト送信元および宛先 MAC (メディアアクセス制御) アドレスだけをサポートします。パス内にあるスイッチの MAC アドレステーブルを使用してパスを識別します。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だけを識別できます。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。

## 使用時の注意事項

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 が適切に動作するために、CDP をディセーブルにしないでください。レイヤ 2 traceroute をサポートするスイッチの一覧については、「使用時の注意事項」(P.36-16) を参照してください。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な場合、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。CDP をイネーブルにする場合の詳細については、第 23 章「CDP の設定」を参照してください。
- スイッチは、ping イネーブル 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はないスイッチに、**traceroute mac** または **traceroute mac ip** イネーブル 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 パスだけを表示します。異なる VLAN にある送信元および宛先 MAC アドレスを指定する場合、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または宛先 MAC アドレスを指定する場合、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。
- 送信元または宛先 MAC アドレスが複数の VLAN に属している場合、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 が指定されない場合、パスは識別されず、エラー メッセージが表示されます。
- 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 アドレスを指定する場合、スイッチは Address Resolution Protocol (ARP) を使用して、IP アドレスを対応する MAC アドレスおよび VLAN ID に関連付けます。
  - ARP エントリが指定した IP アドレスにある場合、スイッチは関連する 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 クエリーを送信して IP アドレスを解決しようとします。IP アドレスが解決されない場合、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 ネイバが 1 つのポート上で検出されると、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 上ではサポートされません。

## 物理パスの表示

次のいずれかのイネーブル 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、このリリースに対応するコマンドリファレンスを参照してください。

## 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.36-17)
- 「IP traceroute の実行」(P.36-18)

## 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単位で識別できます。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 レイヤ (レイヤ 3) デバイスが表示されます。

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** イネーブル EXEC コマンドは、IP ヘッダーの Time To Live (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、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。ルータが TTL 値が 1 または 0 であることを検出すると、データグラムを廃棄し、Internet Control Message Protocol (ICMP) time-to-live-exceeded メッセージを送信元に送信します。**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学習するために、**traceroute** は、データグラムの UDP 宛先ポート番号を、宛先ホストが使用する可能性のない大きな値に設定します。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を除く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という事は、このメッセージが宛先ポートから送信されたことを意味します。

## IP traceroute の実行

ネットワーク上でパケットが通過するパスを追跡するには、イネーブル EXEC モードで次の手順を実行します。

コマンド	目的
<b>traceroute ip host</b>	ネットワーク上でパケットが通過するパスを追跡します。



**(注)** **traceroute** イネーブル 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#

ディスプレイには、送信される 3 つのプロープごとに、ホップ カウント、ルータの IP アドレス、およびラウンドトリップ タイム（ミリ秒単位）が表示されます。

表 36-2 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	ソース クエンチ
U	ポートが到達不能です。

実行中の追跡を終了するには、エスケープ シーケンス（デフォルトでは **Ctrl-^ X**）を入力してください。**Ctrl** キー、**Shift** キー、および **6** キーを同時に押してから離し、そのあと **X** キーを押します。

## TDR の使用

ここでは、次の情報について説明します。

- 「TDR の概要」(P.36-19)
- 「TDR の実行および結果の表示」(P.36-20)

## TDR の概要

Time Domain Reflector (TDR) 機能を使用してケーブル配線の問題を診断して解決できます。TDR 稼動時、ローカル デバイスはケーブルを介して信号を送信して、最初に送信した信号と反射された信号を比べます。

TDR は 10/100/1000 の銅線イーサネット ポート上でだけサポートされます。SFP モジュール ポート上ではサポートされません。

TDR は次のケーブル障害を検出します。

- ツイストペア ケーブルの導線のオープン、損傷、切断：導線がリモート デバイスからの導線に接続されていない状態。
- ツイストペア ケーブルの導線のショート：導線が互いに接触している状態、またはリモート デバイスからの導線に接触している状態。たとえば、ツイスト ペア ケーブルの一方の導線が、もう一方の導線にはんだ付けされている場合、ツイストペア ケーブルのショートが発生します。

ツイストペアの導線の一方がオープンになっている場合、TDR はオープンになっている導線の長さを検出できます。

次の状況で TDR を使用して、ケーブル障害を診断および解決してください。

- スイッチの交換
- 配線クローゼットの設定
- リンクが確立できない、または適切に動作していない場合における、2つのデバイス間の接続のトラブルシューティング

## TDR の実行および結果の表示

インターフェイス上で TDR を実行する場合は、スタック マスターまたはスタック メンバーで実行できます。

TDR を実行する場合、**test cable-diagnostics tdr interface interface-id** イネーブル EXEC コマンドを実行します。

TDR の結果を表示するには、**show cable-diagnostics tdr interface interface-id** イネーブル EXEC コマンドを実行します。出力フィールドの説明に関しては、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。

## 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の問題を診断し、解決する方法について説明します。

- 「特定機能に関するデバッグのイネーブル化」(P.36-20)
- 「システム全体診断のイネーブル化」(P.36-21)
- 「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.36-21)



注意

デバッグ出力には、CPU プロセスで高いプライオリティが与えられるので、システムが使用不能になる可能性があります。したがって、**debug** コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカル サポート担当者とともにトラブルシューティングを行う場合に限定してください。**debug** コマンドは、ネットワークトラフィックが少なく、ユーザも少ないときに使用するのが最良です。このような時間にデバッグを実行すると、**debug** コマンドの処理の負担によってシステム使用が影響を受ける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

デバッグをイネーブルにすると、スタック マスターでだけデバッグがイネーブルになります。スタック メンバーでのデバッグをイネーブルにするには、**session switch-number** イネーブル EXEC コマンドを使用して、スタック メンバーからセッションを開始する必要があります。そのあと、スタック メンバーのコマンドラインプロンプトに **debug** を入力します。

**debug** コマンドはすべてイネーブル 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、Switched Port Analyzer (SPAN; スイッチド ポート アナライザ) 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 span-session
```

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。

- モニタするトラフィック タイプを生成するようにスイッチが正しく設定されてい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である間にモニタすべきタイプのトラフィックを生成しないことがあります。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。

SPAN のデバッグをディセーブルにする場合は、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 span-session
```

また、イネーブル 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 span-session
```

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
```

## 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、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** イネーブル 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** 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。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のが便利です。

## 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、コンソール 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。

出力先に指定できるのは、コンソール、仮想端末、内部バッファ、および Syslog サーバが稼働している UNIX ホストです。Syslog フォーマットは、4.3 Berkeley Standard Distribution (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ることが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。

スタックメンバーによって生成されたシステムエラーメッセージは、スタックマスターによってすべてのスタックメンバーに表示されます。Syslog はスタックマスターに置かれます。



(注) スタックマスターに障害が発生しても Syslog が失われないように、Syslog をフラッシュメモリに保存してください。

システムメッセージロギングの詳細については、第 28 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。

## show platform forward コマンドの使用

**show platform forward** イネーブル 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がシステムを介して送信された場合、転送結果に関して、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ポートマップ、ビットマップ、および出力側の情報が表示されます。



(注) **show platform 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スイッチコマンドリファレンスを参照してください。

このコマンドで出力される情報のほとんどは、主に、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使用するテクニカルサポート担当者に役立つものです。ただし、パケット転送情報はトラブルシューティングにも役立ちます。

次に、VLAN 5 のポート 1 に入るパケットが、不明な MAC アドレスにアドレス指定されている場合の **show platform forward** コマンドの出力例を示します。パケットは VLAN 5 内のその他のすべてのポートに対してフラグディングされなければなりません。

```
Switch# show platform forward gigabitethernet1/0/1 vlan 5 1.1.1 2.2.2 ip 13.1.1.1 13.2.2.2
udp 10 20
```

```
Global Port Number:24, Asic Number:5
Src Real Vlan Id:5, Mapped Vlan Id:5
```

```
Ingress:
  Lookup                Key-Used                Index-Hit  A-Data
InptACL  40_0D020202_0D010101-00_40000014_000A0000    01FFA  03000000
L2Local  80_00050002_00020002-00_00000000_00000000    00C71  0000002B
Station Descriptor:02340000, DestIndex:0239, RewriteIndex:F005
```

```
=====
Egress:Asic 2, switch 1
Output Packets:
```

```
-----
Packet 1
  Lookup                Key-Used                Index-Hit  A-Data
OutptACL 50_0D020202_0D010101-00_40000014_000A0000    01FFE  03000000
```

```

Port      Vlan      SrcMac      DstMac      Cos  Dscp
Gi1/0/1   0005 0001.0001.0001  0002.0002.0002

-----
Packet 2
  Lookup                               Key-Used                               Index-Hit  A-Data
OutputACL 50_0D020202_0D010101-00_40000014_000A0000  01FFE  03000000

Port      Vlan      SrcMac      DstMac      Cos  Dscp
Gi1/0/2   0005 0001.0001.0001  0002.0002.0002

-----
<output truncated>
-----
Packet 10
  Lookup                               Key-Used                               Index-Hit  A-Data
OutputACL 50_0D020202_0D010101-00_40000014_000A0000  01FFE  03000000
Packet dropped due to failed DEJA_VU Check on Gi1/0/2

```

次に、VLAN 5 のポート 1 に着信するパケットを、VLAN 上の別のポートで学習済みのアドレスに送信する場合の出力例を示します。パケットは、アドレスを学習したポートから転送する必要があります。

```

Switch# show platform forward gigabitethernet1/0/1 vlan 5 1.1.1 0009.43a8.0145 ip 13.1.1.1 13.2.2.2 udp 10 20
Global Port Number:24, Asic Number:5
Src Real Vlan Id:5, Mapped Vlan Id:5

Ingress:
  Lookup                               Key-Used                               Index-Hit  A-Data
InptACL  40_0D020202_0D010101-00_40000014_000A0000  01FFA  03000000
L2Local  80_00050009_43A80145-00_00000000_00000000  00086  02010197
Station Descriptor:F0050003, DestIndex:F005, RewriteIndex:0003

=====
Egress:Asic 3, switch 1
Output Packets:

-----
Packet 1
  Lookup                               Key-Used                               Index-Hit  A-Data
OutputACL 50_0D020202_0D010101-00_40000014_000A0000  01FFE  03000000

Port      Vlan      SrcMac      DstMac      Cos  Dscp
interface-id  0005 0001.0001.0001  0009.43A8.0145

```

## crashinfo ファイルの使用

crashinfo ファイルには、シスコのテクニカル サポート担当者が Cisco IOS イメージの障害（クラッシュ）が原因で起きた問題をデバッグするときを使用する情報が保存されます。スイッチは障害発生時にその情報をコンソールに書き込みます。スイッチは次の 2 つのタイプの crashinfo ファイルを作成します。

- 基本 crashinfo ファイル：障害発生後に Cisco IOS イメージを起動すると、スイッチが自動的にこのファイルを作成します。
- 拡張 crashinfo ファイル：システムに障害が発生すると、スイッチが自動的にこのファイルを作成します。

## 基本 crashinfo ファイル

この基本ファイルに保存される情報は、障害が発生した Cisco IOS イメージの名前、バージョン、プロセッサレジスタのリスト、およびその他のスイッチ固有の情報です。**show tech-support** イネーブル 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。

基本 crashinfo ファイルはすべて、フラッシュ ファイル システムの次のディレクトリに保存されます。  
flash:/crashinfo/.

ファイル名は crashinfo\_*n* になります。*n* には一連の番号が入ります。

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。**delete** イネーブル 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** イネーブル EXEC コマンドを使用します。**more** イネーブル EXEC コマンド、**copy** イネーブル 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。

## 拡張 crashinfo ファイル

システムに障害が発生すると、スイッチが拡張 crashinfo ファイルを作成します。拡張ファイルに保存される情報は、スイッチの障害となった原因を特定するのに役立つ追加情報です。このファイルに手動でアクセスし、**more** または **copy** イネーブル EXEC コマンドを使用すると、シスコのテクニカル サポート担当者にこの情報を提供できます。

拡張 crashinfo ファイルはすべて、フラッシュ ファイル システムの次のディレクトリに保存されます。  
flash:/crashinfo\_ext/.

ファイル名は crashinfo\_ext\_*n* になります。*n* には一連の番号が入ります。

**no exception crashinfo** グローバル コンフィギュレーション コマンドを使用すると、スイッチが拡張 crashinfo ファイルを作成しないように設定できます。