CHAPTER 50

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 3750-X または 3560-X 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。問題の性質に応じて、Command-Line Interface（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 Catalyst 3750-X または 3560-X スタンドアロン スイッチおよび Catalyst 3750-X 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、このリリースに対応するコマンド リファレンスおよび『*Cisco IOS Command Summary, Release 12.2*』を参照してください。

（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。

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; 電源投入時自己診断テスト）に失敗し、接続できなくなります。

ここで紹介する手順では、破損したイメージ ファイルまたは不良なイメージ ファイルの回復に boot loader コマンドおよび TFTP を使用します。

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 ファイルに移動し、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。

```
switch% 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。

```
switch% tar -xvf image_filename.tar image_filename.bin
x image_name.bin, 3970586 bytes, 7756 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。

```
switch% ls -l image_filename.bin
-rw-r--r--   1 boba      3970586 Apr 21 12:00 image_name.bin
```

ステップ 3　PC をスイッチのイーサネット管理ポートに接続します。

ステップ 4　スイッチの電源コードを外します。

ステップ 5　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 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
```

```
boot
```

ステップ 6　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 7　イーサネット管理ポートを通じて、スイッチを TFTP サーバに接続します。

ステップ 8　TFTP を使用してファイル転送を開始します。

a. TFTP サーバの IP アドレスを指定します。

```
switch: set ip_addr ip_address/mask
```

b. デフォルト ルータを指定します。

```
switch: set default_router ip_address
```

ステップ 9　TFTP サーバからスイッチへソフトウェア イメージをコピーします。

```
switch: copy tftp://ip_address/filesystem:/source-file-url flash:image_filename.bin
```

ステップ 10　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 11　**archive download-sw** 特権 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 12　**reload** 特権 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 13　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かぎりエンド 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と、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.50-4）
- 「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.50-6）

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　次のいずれかの方法で、スイッチに端末または PC を接続します。

- 端末または端末エミュレーション ソフトウェアが稼動している 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 スタックの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。
- PC をイーサネット管理ポートに接続します。スイッチ スタックのパスワードを回復する場合は、Catalyst 3750-X スタック メンバーのイーサネット管理ポートに接続します。内部イーサネット管理ポートの詳しい使用方法については、「イーサネット管理ポートの使用」（P.13-24）およびハードウェア 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 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　Catalyst 3750-X スイッチの場合は、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。Catalyst 3560-X スイッチの場合は、スイッチの電源を切断します。

ステップ 4　スイッチまたはスタック マスターに電源コードを再接続します。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 が一時的にオレンジになってからグリーンに点灯するまで 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.50-4）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.50-6）に進んで、その手順に従います。

ステップ 5　パスワードの回復後、スイッチまたはスタック マスターをリロードします。

Catalyst 3560-X スイッチの場合：

```
Switch> reload
Proceed with reload? [confirm] y
```

Catalyst 3750-X スイッチの場合：

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

ステップ 6　Catalyst 3750-X スイッチの場合は、スイッチ スタックの残りのメンバーの電源を入れます。

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  switch_image
   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、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
```

（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　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、SVI 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** 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、**no shutdown** コマンドを入力します。

ステップ 14　スイッチまたはスイッチ 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 switch_image
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、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#
```

（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、SVI 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** 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、**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スイッチ スタックから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 インストレーション 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; 着脱可能小型フォーム ファクタ）モジュールになります。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、スタックはフル帯域幅では動作していません。
- 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、「スタック メンバー番号」（P.5-7）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（1 つまたは複数）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 Plus 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、「スイッチ スタック情報の表示」（P.5-26）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。詳細については、第 6 章「スイッチのクラスタ化」を参照してください。詳細については、第 6 章「スイッチのクラスタ化」および第 43 章「HSRP の設定」を参照してください。Cisco.com で利用できる『*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、各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 ポートまたはイーサネット管理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.50-9）
- 「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.50-11）

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 ポートまたはイーサネット管理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 インストレーション ガイドを参照してください。イーサネット管理ポートの詳しい使用方法については、「イーサネット管理ポートの使用」（P.13-24）およびハードウェア 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、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ー 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** 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　クラスタに名前を割り当て、**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は、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 ポートまたはイーサネット管理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 インストレーション ガイドを参照してください。イーサネット管理ポートの詳しい使用方法については、「イーサネット管理ポートの使用」（P.13-24）およびハードウェア コンフィギュレーション 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、特権 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、新しいスイッチの 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** 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　クラスタに名前を割り当て、**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-X、Catalyst 3750-E、Catalyst 3750、Catalyst 356-X、Catalyst 3560-E、Catalyst 3560、Catalyst 3550、Catalyst 3500 XL、Catalyst 2970、Catalyst 2960、CGESM、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-X、Catalyst 3750-E、Catalyst 3750、Catalyst 3560-X、Catalyst 3560-E、Catalyst 3560、Catalyst 3550、Catalyst 2970、Catalyst 2960、CGESM、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 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

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 error-disabled ステートになることがあります。error-disabled 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、error-disabled ステートから回復することもできます。

Catalyst 3750-X スイッチの場合、**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 error-disabled 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

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 error-disabled 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; 電気的に消去可能でプログラミング可能な 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 error-disabled 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、error-disabled ステートから回復するタイム インターバルを入力します。このインターバルが経過すると、スイッチは error-disabled 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 特権 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 リファレンスに記載された **show interfaces transceiver** コマンドの説明を参照してください。

温度のモニタ

スイッチは温度条件をモニタし、温度情報を使用してファンを制御します。

温度の値、状態、しきい値を表示するには、**show env temperature** status 特権 EXEC コマンドを使用します。温度の値は、スイッチ内の温度であり、外部の温度ではありません。**system env temperature threshold yellow** *value* 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イエローのしきい値レベル（摂氏）だけを設定し、イエローのしきい値およびレッドのしきい値の差を設定できます。グリーンまたはレッドのしきい値は設定できません。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。

ping の使用

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（*ホスト名*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 41 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 41 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
ping ip *host* | *address*	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 50-1 で、ping の文字出力について説明します。

表 50-1　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

レイヤ 2 traceroute の概要

レイヤ 2 traceroute 機能により、送信元デバイスから宛先デバイスまでにパケットが通過する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 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内で検出すると、スイッチはレイヤ 2 トレース クエリ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まで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。

使用上の注意事項

- 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。

  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過す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 27 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でき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までの物理パス内に存在しないスイッチ上で、**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; アドレス解決プロトコル）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

次のいずれかの特権 EXEC コマンドを使用して、送信元デバイスから宛先デバイスまでパケットが通過する物理パスを表示できます。

- **tracetroute mac** [**interface** *interface-id*] {*source-mac-address*} [**interface** *interface-id*] {*destination-mac-address*} [**vlan** *vlan-id*] [**detail**]
- **tracetroute 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。

IP traceroute の使用

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** 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。中継スイッチが同じ 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 の出力に中継スイッチは表示されません。ただし、中継スイッチが、特定のパケットをルーティングするマルチレイヤ スイッチの場合、中継スイッチは 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 Time To Live（TTL; 存続可能時間）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 を開始するには、TTL フィールドに 1 を設定し、User Datagram Protocol（UTP; ユーザ データグラム プロトコル）データグラムを宛先ホストに送信します。ルータが TTL 値 1 または 0 を検出すると、データグラムはドロップされ、Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）の time-to-live-exceeded メッセージが送信元に送られます。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 値を 2 に設定した UDP パケットを送信します。1 番めのルータは、TTL フィールドを 1 つ減らし、次のルータにデータグラムを送信します。2 番めのルータは、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て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ことは、このメッセージが宛て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、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*	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** 特権 EXEC コマンドに他のプロトコル 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。

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

  1 172.2.52.1 0 msec 0 msec 4 msec
  2 172.2.1.203 12 msec 8 msec 0 msec
  3 171.9.16.6 4 msec 0 msec 0 msec
  4 171.9.4.5 0 msec 4 msec 0 msec
  5 171.9.121.34 0 msec 4 msec 4 msec
  6 171.9.15.9 120 msec 132 msec 128 msec
  7 171.9.15.10 132 msec 128 msec 128 msec
Switch#
```

表示には、送信される 3 つのプローブごとに、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 50-2　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（始点抑制要求）
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

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、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。10 ギガビット イーサネット ポートまたは SFP モジュール ポート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
- ワイヤリング 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 の実行時、次の場合にスイッチは正確な情報をレポートします。

- ギガビット リンク用のケーブルが単線コア ケーブル
- オープンエンド ケーブルが未終端

TDR の実行時、次の場合にスイッチは正確な情報をレポートしません。

- ギガビット リンク用のケーブルがツイストペア ケーブルまたは連続接続された単線コア ケーブル
- リンクが 10 Mb または 100 Mb
- より線ケーブル
- リンク パートナーが Cisco IP Phone
- リンク パートナーが IEEE 802.3 に準拠していない

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* 特権 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* 特権 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

注意　デバッグ出力には、CPU プロセスで高優先順位が与えられるので、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

Catalyst 3750-X スイッチ スタックでデバッグ機能をイネーブルにする場合、スタック マスター上でだけ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* 特権 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** コマンドは引数がありません。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、特権 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、特権 EXEC モードで次のコマンドを入力します。

```
Switch# no debug span-session
```

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 span-session
```

各デバッグ オプションのステートを表示するには、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 ポートまたはイーサネット管理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 サーバが稼動している UNIX ホストです。Syslog 形式は、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 マスターに存在します。

（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 33 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 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、転送宛て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; 特定用途向け集積回路）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ッ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  Dscpv
Gi1/0/1    0005 0001.0001.0001  0002.0002.0002

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

Port       Vlan      SrcMac          DstMac    Cos  Dscpv
Gi0/2    0005 0001.0001.0001  0002.0002.0002

----------------------------------------
<output truncated>
----------------------------------------
Packet 10
 Lookup                    Key-Used                      Index-Hit  A-Data
OutptACL 50_0D020202_0D010101-00_40000014_000A0000     01FFE   03000000
Packet dropped due to failed DEJA_VU Check on Gi0/2
```

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
OutptACL 50_0D020202_0D010101-00_40000014_000A0000     01FFE   03000000

Port       Vlan      SrcMac          DstMac    Cos  Dscpv
Gi1/0/2    0005 0001.0001.0001  0009.43A8.0145
```

次に、VLAN 5 内のポート 1 に着信するパケットの宛先 MAC アドレスが VLAN 5 内のルータ MAC アドレスに設定されていて、宛先 IP アドレスが不明である場合の出力例を示します。デフォルト ルートが設定されていないため、パケットはドロップされます。

```
Switch# show platform forward gigabitethernet1/0/1 vlan 5 1.1.1 03.e319.ee44 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_41000014_000A0000     01FFA   03000000
L3Local  00_00000000_00000000-90_00001400_0D020202     010F0   01880290
L3Scndr  12_0D020202_0D010101-00_40000014_000A0000     034E0   000C001D_00000000
Lookup Used:Secondary
Station Descriptor:02260000, DestIndex:0226, RewriteIndex:0000
```

次に、VLAN 5 内のポート 1 に着信するパケットの宛先 MAC アドレスが VLAN 5 内のルータ MAC アドレスに設定されていて、宛先 IP アドレスが IP ルーティング テーブル内の IP アドレスに設定されている場合の出力例を示します。パケットはルーティング テーブルの指定どおりに転送されます。

```
Switch# show platform forward gigabitethernet1/0/1 vlan 5 1.1.1 03.e319.ee44 ip 110.1.5.5
16.1.10.5
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_10010A05_0A010505-00_41000014_000A0000     01FFA   03000000
L3Local  00_00000000_00000000-90_00001400_10010A05     010F0   01880290
L3Scndr  12_10010A05_0A010505-00_40000014_000A0000     01D28   30090001_00000000
Lookup Used:Secondary
Station Descriptor:F0070007, DestIndex:F007, RewriteIndex:0007

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

----------------------------------------
Packet 1
 Lookup                   Key-Used                    Index-Hit  A-Data
OutptACL 50_10010A05_0A010505-00_40000014_000A0000     01FFE   03000000

Port       Vlan      SrcMac          DstMac    Cos  Dscpv
Gi1/0/2    0007 XXXX.XXXX.0246  0009.43A8.0147
```

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に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：システム障害の発生時に、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、およびスタック トレースです。**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。

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は変更できません。ただし、ファイルが作成されたあとに、**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。

拡張 crashinfo ファイル

スイッチは、システム障害の発生時に拡張 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** 特権 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。

OBFL の使用

スイッチ情報の収集に On-Board-Failure Logging（OBFL）を使用できます。収集される情報には、動作期間、温度、および電圧などの情報が含まれ、シスコのテクニカル サポート担当者がスイッチの問題をトラブルシューティングするのに役立ちます。OBFL はイネーブルにしておき、フラッシュ メモリに保存された情報は消去しないことを推奨します。

OBFL の概要

デフォルトでは、OBFL がイネーブルに設定されています。OBFL はスイッチおよび Small Form-Factor Pluggable（SFP）モジュールについての情報を収集します。スイッチは、次の情報をフラッシュ メモリに保存します。

- CLI コマンド：スタンドアロン スイッチまたはスイッチ スタック メンバーに入力した OBFL CLI コマンドの記録
- 環境データ：スタンドアロン スイッチまたはスタック メンバー、および接続されたすべての FRU デバイスの Unique Device Identifier（UDI）に関する情報（Product Identification（PID; 製品 ID）、Version Identification（VID; バージョン ID）、およびシリアル番号）
- メッセージ：スタンドアロン スイッチまたはスタック メンバーが生成するハードウェア関連のシステム メッセージ記録
- PoE：スタンドアロン スイッチまたはスタック メンバーの PoE ポートの電力消費量の記録
- 温度：スタンドアロン スイッチまたはスタック メンバーの温度
- 動作期間：スタンドアロン スイッチまたはスタック メンバーの起動時刻、スイッチの再起動の理由、最後の再起動からの経過時間
- 電圧：スタンドアロン スイッチまたはスタック メンバーのシステム電圧

システム クロックを、手動または Network Time Protocol（NTP）を使用して設定してください。

OBFL データは、スイッチの稼動中に **show logging onboard** 特権 EXEC コマンドを使用して取得できます。スイッチの障害が発生したときは、シスコのテクニカル サポート担当者にデータの取得方法を問い合わせてください。

OBFL 対応スイッチが再起動されると、10 分経過後に新しいデータを記録できます。

OBFL の設定

OBFL をイネーブルにするには、**hw-module module** [*switch-number*] **logging onboard** [**message level** *level*] 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。Catalyst 3750-X スイッチでは、*switch-number* の範囲は 1 ～ 9 です。Catalyst 3750-X スイッチでは、スイッチ番号は常に 1 です。スイッチで生成され、フラッシュ メモリに保存されるハードウェア関連メッセージを指定するには、**message level** *level* パラメータを使用します。

OBFL データをローカル ネットワークまたは特定のファイル システムにコピーするには、**copy logging onboard module** *stack-member destination* 特権 EXEC コマンドを使用します。

注意　OBFL をディセーブルにしないこと、およびフラッシュ メモリに保存されたデータを削除しないことを推奨します。

OBFL をディセーブルにするには、**no hw-module module** [*switch-number*] **logging onboard** [**message level**] 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。

動作期間および CLI コマンド情報を除いたすべての OBFL データをフラッシュ メモリからクリアするには、**clear logging onboard** 特権 EXEC コマンドを使用します。

スイッチ スタックの場合、スタンドアロン スイッチまたはすべてのスタック メンバーの OBFL をイネーブルにするには、**hw-module module logging onboard** [**message level** *level*] 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。

スイッチ スタックの場合、Catalyst 3750 スイッチなどの OBFL をサポートしていないスタック メンバーで **hw-module module** [*switch-number*] **logging onboard** コマンドを入力すると、サポートされないことを意味するメッセージが表示されます。Catalyst 3750-X および 3750 スイッチが混在するスタックで、Catalyst 3750 スイッチがスタック マスターの場合、Catalyst 3750 スイッチで OBFL コマンドを入力すると、コマンドはスタック マスターで実行されず、スタック マスターは OBFL 設定情報をスタック メンバーに送信します。

コマンドの詳細情報については、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。

OBFL 情報の表示

OBFL 情報を表示するには、表 50-3 の特権 EXEC コマンドを 1 つまたは複数使用します。

表 50-3　OBFL 情報を表示するためのコマンド

コマンド	目的
show logging onboard [**module** [*switch-number*]] **clilog**	スタンドアロン スイッチまたは指定したスタック メンバーに入力された OBFL CLI コマンドを表示します。
show logging onboard [**module** [*switch-number*]] **environment**	スタンドアロン スイッチまたは指定したスタック メンバー、および接続されたすべての FRU デバイスの UDI 情報を指定します（PID、VID、およびシリアル番号）。
show logging onboard [**module** [*switch-number*]] **message**	スタンドアロン スイッチまたは指定したスタック メンバーが生成したハードウェア関連のメッセージを表示します。
show logging onboard [**module** [*switch-number*]] **poe**	スタンドアロン スイッチまたは指定したスタック メンバーの PoE ポートの電力消費量を表示します。
show logging onboard [**module** [*switch-number*]] **temperature**	スタンドアロン スイッチまたは指定したスイッチ スタック メンバーの温度を表示します。
show logging onboard [**module** [*switch-number*]] **uptime**	スタンドアロン スイッチまたは指定したスタック メンバーの起動時刻、再起動の理由、および最後の再起動以降の経過時間を表示します。
show logging onboard [**module** [*switch-number*]] **voltage**	スタンドアロン スイッチまたは指定したスタック メンバーのシステム電圧を表示します。

表 50-3 のコマンドの使用方法に関する詳細および OBFL データの例については、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。

トラブルシューティングに関する表

ここに掲載する表は、Cisco.com にあるトラブルシューティング関連のマニュアルの内容を簡潔にまとめたものです。

CPU 使用率のトラブルシューティング

次に、CPU がビジーすぎるために発生する可能性がある症状と、CPU の使用率に関する問題を検証する方法について説明します。表 50-4 に、識別可能な CPU 使用率の問題の主なタイプを示します。考えられる原因と是正措置も示します（Cisco.com の『*Troubleshooting High CPU Utilization*』へのリンクを含む）。

高 CPU 使用率によって生じる可能性がある症状

CPU 使用率が高すぎると次のような症状が起こる可能性がありますが、これらの症状は別の原因で起こることもあります。

- スパニング ツリーのトポロジが変更される
- 通信が切断されたことにより、EtherChannel リンクがダウン状態になる
- 管理要求に応答できない（ICMP ping、SNMP タイムアウト、Telnet または SSH セッションが低速）
- UDLD フラッピング
- 許容可能なしきい値を超える SLA 応答が原因で、IP SLA に障害が生じる
- スイッチが要求を転送しない、または要求に応答しない場合に、DHCP または IEEE 802.1x に障害が生じる

Layer 3 スイッチの場合：

（注） レイヤ 3 機能は、LAN ベース フィーチャ セットが稼動しているスイッチではサポートされません。

- ソフトウェアで経路選択されるパケットがドロップされる、または遅延が増加する
- BGP または OSPF のルーティング トポロジが変更になる
- HSRP フラッピング

問題と原因の検証

高 CPU 使用率が問題であるかどうかを確認するには、**show processes cpu sorted** 特権 EXEC コマンドを入力します。出力例の 1 行めの、下線付きの情報を参照してください。

```
Switch# show processes cpu sorted
CPU utilization for five seconds: 8%/0%; one minute: 7%; five minutes: 8%
PID Runtime(ms) Invoked uSecs 5Sec 1Min 5Min TTY Process
309 42289103 752750 56180 1.75% 1.20% 1.22% 0 RIP Timers
140 8820183 4942081 1784 0.63% 0.37% 0.30% 0 HRPC qos request
```

```
100 3427318 16150534 212 0.47% 0.14% 0.11% 0 HRPC pm-counters
192 3093252 14081112 219 0.31% 0.14% 0.11% 0 Spanning Tree
143 8 37 216 0.15% 0.01% 0.00% 0 Exec
...
<output truncated>
```

この例は、CPU 使用率が通常の状態を示しています。この出力では、最後の 5 秒間の使用率は *8%/0%* となっていますが、これには次の意味があります。

- 合計 CPU 使用率は、Cisco IOS プロセスの稼動時間と、割り込みの処理にかかった時間を合せて 8% です。
- 割り込みの処理にかかった時間は 0% です。

表 50-4　CPU 使用率に関するトラブルシューティング

問題の種類	原因	是正措置
割り込みのパーセンテージ値が、合計 CPU 使用率と同じくらい高い。	CPU がネットワークから受信するパケット数が多すぎる。	ネットワーク パケットの送信元を特定します。フローを停止するか、スイッチの設定を変更します。「Analyzing Network Traffic」のセクションを参照してください。
割り込みの処理にかかった時間が最小限であるにもかかわらず、合計 CPU 使用率が 50% を超える。	1 つまたは複数の Cisco IOS プロセスが、CPU 時間を使い過ぎている。これは、通常、プロセスを起動したイベントによって起こる問題です。	異常なイベントを特定し、根本原因をトラブルシューティングしてください。「Debugging Active Processes」のセクションを参照してください。

CPU 使用率に関する情報と、使用率に伴う問題をトラブルシューティングする方法については、Cisco.com の『*Troubleshooting High CPU Utilization*』を参照してください。

PoE に関するトラブルシューティング

図 50-1　PoE に関するトラブルシューティングのシナリオ

症状または問題	考えられる原因と解決策
1 つのポートにだけ PoE がない。 問題は、1 つのスイッチ ポートにだけ発生しています。PoE や PoE 以外のデバイスはこのポートでは動作しませんが、他のポートでは動作します。	別の PoE ポートで、受電デバイスが動作するかどうかを確認します。 ポートがシャットダウンしていない、またはエラー ディセーブル状態になっていないことを確認するためには、**show run**、**show interface status**、または **show power inline detail** ユーザ EXEC コマンドを使用します。 **（注）** IEEE 仕様では任意の機能となっていますが、大半のスイッチは、ポートがシャットダウンすると、ポートの電源を切断します。 受電デバイスとスイッチ ポートを接続するイーサネット ケーブルに異常がないことを確認します。正常に動作することがわかっている非 PoE イーサネット デバイスをイーサネット ケーブルに接続し、受電デバイスがリンクを確立し、別のホストとトラフィックを送受信できることを確認します。 スイッチの前面パネルから、受電デバイスまでの合計ケーブル長は 100 メートル以内であることを確認します。 イーサネット ケーブルをスイッチ ポートから切断します。短いイーサネット ケーブルを使用し、スイッチの前面パネル（パッチパネルではない）のこのポートに、正常に動作することがわかっているイーサネット デバイスを直接接続します。イーサネット リンクが確立され、別のホストとトラフィックの送受信ができることを確認するか、ポートの VLAN SVI に ping を送信します。次に、受電デバイスをこのポートに接続し、電源がオンになることを確認します。 受電デバイスが、パッチコードを使用してスイッチ ポートに接続されても電源がオンにならない場合は、接続された受電デバイスの総数と、スイッチの電力バジェット（使用可能な PoE）を比較します。使用可能な電力を確認するためには、**show inline power** および **show inline power detail** コマンドを使用します。 詳細については、Cisco.com の「No PoE On One Port」を参照してください。

図 50-1　PoE に関するトラブルシューティングのシナリオ （続き）

症状または問題	考えられる原因と解決策
すべてのポート、またはポートのグループに PoE がない。 問題は、すべてのスイッチ ポートで発生しています。非受電イーサネット デバイスは、どのポートに対してもイーサネット リンクを確立できず、PoE デバイスもオンになりません。	電力に関するアラームが継続的に発生する、断続的に発生する、または再発する場合は、可能であれば電源モジュールを交換します（現場交換可能ユニットです）。それ以外の場合は、スイッチを交換します。 すべてのポートではなく、連続する一連のポートで問題が発生する場合は、電源モジュールにはおそらく問題はありません。スイッチの PoE レギュレータに問題がある可能性があります。 以前 PoE の状態やステータス変更を報告したアラーム、またはシステム メッセージを確認するためには、**show log** 特権 EXEC コマンドを使用します。 アラームがない場合は、**show interface status** コマンドを使用し、ポートがシャットダウンしていないか、また、error-disabled 状態になっていないかを確認します。ポートが error-disabled 状態の場合は、**shut** および **no shut** 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、ポートを再度イネーブルにします。 PoE のステータスと電力バジェット（使用可能な PoE）を確認するためには、**show env power** および **show power inline** 特権 EXEC コマンドを使用します。 ポートに **power inline never** が設定されていないことを確認するため、稼動中の設定を検証します。 非受電イーサネット デバイスを、スイッチ ポートに直接接続します。短いパッチコードだけを使用してください。既存のディストリビューション ケーブルを使用しないでください。**shut** および **no shut** 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、イーサネット リンクが確立していることを確認します。正常に接続される場合は、短いパッチコードを使用して、受電デバイスをこのポートに接続し、電源がオンになることを確認します。デバイスの電源がオンになる場合は、すべての中間パッチパネルが正しく接続されることを確認します。 スイッチ ポートから、1 本を除くすべてのイーサネット ケーブルを切断します。短いパッチコードを使用し、受電デバイスを 1 つの PoE ポートに接続します。受電デバイスが、スイッチ ポートから送られる電力以上の電力を必要としないことを確認します。 ポートがシャットダウンしていないときに、受電デバイスが電力を受けられるかどうかを確認するためには、**show power inline** 特権 EXEC コマンドを使用します。または、受電デバイスの電源がオンになることを確認します。 スイッチに受電デバイスが 1 台だけ接続されているときに、受電デバイスの電源がオンになる場合は、残りのポートで **shut** および **no shut** 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、イーサネット ケーブルを 1 本ずつスイッチの PoE ポートに再接続します。インライン パワーの統計情報とポート ステータスをモニタするためには、**show interface status** および **show power inline** 特権 EXEC コマンドを使用します。 それでも、どのポートにも PoE がない場合は、電源の PoE セクションでヒューズが開いている可能性があります。この状態になると、通常は、前にシステム メッセージで報告された Check the log again for alarms アラームが起こります。 詳細については、Cisco.com の「No PoE On Any Port or a Group of Ports」を参照してください。

図 50-1　PoE に関するトラブルシューティングのシナリオ （続き）

症状または問題	考えられる原因と解決策
Cisco IP Phone が切断、またはリセットされる。 正常に稼動したのち、Cisco Phone またはワイヤレス アクセス ポイントが断続的にリロードするか、PoE から切断されます。	このスイッチから受電デバイスへのすべての電気接続を確認します。不安定な接続があると、電力供給障害が発生したり、受電デバイスの動作が不正になったりすることがあります（受電デバイスの異常切断やリロードなど）。 スイッチ ポートと受電デバイス間のケーブル長が、100 メートル以内であることを確認します。 スイッチが設置されている場所で、電気環境の変化がありましたか。また、切断されたときに受電デバイスに何が起こっていますか。 切断と同時にエラー メッセージが表示されるかどうか確認します。エラー メッセージを確認するためには、**show log** 特権 EXEC コマンドを使用します。 リロードの直前に、IP Phone が Call Manager へのアクセスを失っていないことを確認します（PoE の問題ではなく、ネットワークの問題である可能性があります）。 受電デバイスを非 PoE デバイスに交換し、デバイスが正常に稼動することを確認します。非 PoE デバイスにリンクの問題があるか、エラー率が高い場合は、スイッチ ポートと受電デバイス間のケーブル接続が不安定になっている可能性があります。 詳細については、Cisco.com の「Cisco Phone Disconnects or Resets」を参照してください。
シスコ製以外の受電デバイスが、シスコ製 PoE スイッチ上で稼動しない。 シスコ製以外の受電デバイスがシスコ製の PoE スイッチに接続されているが、電源がオンにならない、または電源がオンになってもすぐにオフになります。非 PoE デバイスは正常に稼動します。	受電デバイスが接続される前、または接続されたあとに、スイッチの電力バジェット（使用可能な PoE）が消耗されないかどうかを確認するためには、**show power inline** コマンドを使用します。受電デバイスを接続する前に、十分な電力が確保できていることを確認します。 スイッチが、接続された受電デバイスを検出するかどうかを確認するためには、**show interface status** コマンドを使用します。 ポートの過電流状態を報告したシステム メッセージを確認するためには、**show log** コマンドを使用します。症状を正確に識別します。受電デバイスは当初は電源オンになったものの、そののちに切断されましたか。その場合は、初期 surge-in（または *inrush*）電流が、ポートの current-limit しきい値を超過したことが原因であると考えられます。 詳細については、Cisco.com の「Non-Cisco PD Does Not Work Correctly on Cisco PoE Switch」を参照してください。

StackWise のトラブルシューティング（Catalyst 3750-X スイッチ限定）

表 50-5　スイッチ スタックのトラブルシューティングのシナリオ

症状 / 問題	問題の確認方法	考えられる原因 / 解決策
スイッチ スタックに関する問題の一般的なトラブルシューティング	本マニュアルを確認してください。	問題の解決策とチュートリアルの情報については、『Troubleshooting Switch Stacks』を参照してください。

表 50-5　スイッチ スタックのトラブルシューティングのシナリオ （続き）

症状 / 問題	問題の確認方法	考えられる原因 / 解決策
スイッチがスタックに参加できない。	**show switch** 特権 EXEC コマンドを入力します。	スタック メンバーと新規スイッチの間で、Cisco IOS バージョンの互換性がありません（「*Confirming Cisco IOS Versions*」を参照）。
	show version ユーザ EXEC コマンドを入力します。	Catalyst 3750-E スイッチでライセンス レベルの互換性がありません（「*Verifying Software License Compatibility*」を参照）。
	show platform stack-manager all コマンドを入力します。	スタック メンバーと新規スイッチの間で Cisco IOS バージョンの互換性がありません（「*Confirming Cisco IOS Versions*」を参照）。
	ケーブルと接続を入念に確認します。	StackWise ケーブルが不安定、または接続が完全ではありません（「*Testing StackWise Cables and Interfaces*」を参照）。
	show sdm prefer コマンドを入力します。	スイッチをスタックに追加する前に、そのスイッチが他のアプリケーションで使用されていた場合に、設定が不一致になります（SDM テンプレート）。スタック メンバーと新規スイッチの間で IOS バージョンの互換性がありません（「*Configuration Mismatch*」を参照）。
StackWise ポートのアップ / ダウン状態が頻繁に、または短時間で変わる（フラッピング）。	エラー メッセージに、スタックでリンクの問題が発生していることが報告されます。トラフィックが妨害されている可能性があります。	StackWise ケーブル接続またはインターフェイスが不安定になっています（「*StackWise Port Flapping*」を参照）。
スイッチ メンバーのポートがアップ状態にならない。	**show switch detail** 特権 EXEC コマンドを入力します。	StackWise ケーブル接続またはインターフェイスが不安定になっています（「*StackWise Port Flapping*」を参照）。
スタック リング帯域幅が減少している、またはスイッチ ポート間、あるいはスタック内のスイッチ間のスループットが低下している。	**show switch stack-ring speed** ユーザ EXEC コマンドを入力します。	StackWise ケーブル接続とスイッチのシャーシ コネクタ間の接続が正しくありません（「*Testing StackWise Cables and Interfaces*」を参照）。
	どのスタック ケーブルまたは接続が問題の原因となっているかを確認するためには、**show switch detail** ユーザ EXEC コマンドを入力します。	StackWise ケーブルに欠陥がある、または StackWise ケーブルがない（「*Testing StackWise Cables and Interfaces*」を参照）。
	• StackWise ケーブル コネクタの押さえネジを確認します。 • 新しいスイッチが Ready、Progressing、または Provisioned のどの状態であるかを確認するには、**show switch** 特権 EXEC コマンドを入力します。	• 押さえネジが緩んでいるか、強く締めすぎています（「*Verifying StackWise Cable Connections*」を参照）。 • スタック メンバーのステータスを確認します（「*Verifying StackWise Cable Connections*」を参照）。
1 つ以上のスイッチのポート番号付けが正しくないか、変更されている。	**show switch detail** ユーザ EXEC コマンドを入力します。	複数の StackWise ケーブルがスタック メンバーから切断され、2 つの個別のスタックになっています（「*Stack Master Election and Port Number Assignment*」を参照）。

表 50-5　スイッチ スタックのトラブルシューティングのシナリオ （続き）

症状 / 問題	問題の確認方法	考えられる原因 / 解決策
スタック リング全体でトラフィックが低速になっている。	スイッチ インターフェイスをテストします。	StackWise スイッチ インターフェイスに欠陥があります。 **（注）** 唯一の解決策は、スイッチを交換することだけです。
スタック マスターの選定に問題がある、スタックがマージしているか、新しいスイッチがスタックに参加している。	スタック マスターの選定ルールを確認します。	現在のスタック マスターが再起動または切断されています（「*Stack Master is Rebooted or Disconnected*」を参照）。
	ポート番号付けがオフになっている可能性があります。	ポート番号付けを確認してください（「*Stack Master Election and Port Number Assignment*」を参照）
	show switch 特権 EXEC コマンドを入力します。	ステート メッセージを確認します（「*Joining a Stack: Typical Sequence States and Rules*」を参照）。
スタック メンバーをアップグレードする必要がある。	スタック メンバーが、メジャー バージョンまたはマイナー バージョンが異なる Cisco IOS ソフトウェアを稼動しています。	StackWise スイッチ インターフェイスまたはケーブルに欠陥がある（「*Quick-and-Easy Catalyst 3750 and Catalyst 3750E Switch Stack Upgrades*」を参照）。
StackWise のリンク接続に問題がある。	LED の動作を確認してください。	スタックがフル帯域幅で稼動していません（「*Verifying StackWise Link Connections Using LEDs*」を参照）。