



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 スイッチの問題を特定し、解決する方法について説明します。問題を特定して解決する場合には、問題の性質に応じて、CLI（コマンドライン インターフェイス）または Cluster Management Suite（CMS）を使用することができます。

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

この章で説明する内容は、次のとおりです。

- [XMODEM プロトコルによるソフトウェア障害からの回復 \(p.36-2\)](#)
- [パスワードを忘れた場合の回復 \(p.36-4\)](#)
- [スイッチ スタック問題の回避 \(p.36-10\)](#)
- [コマンド スイッチ障害からの回復 \(p.36-11\)](#)
- [クラスタ メンバーとの接続の回復 \(p.36-15\)](#)



(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 \(p.36-15\)](#)
- [PoE スイッチ ポートのトラブルシューティング \(p.36-16\)](#)
- [SFP モジュールのセキュリティと識別 \(p.36-16\)](#)
- [ping の使用 \(p.36-17\)](#)
- [レイヤ 2 traceroute の使用 \(p.36-19\)](#)
- [IP traceroute の使用 \(p.36-21\)](#)
- [TDR の使用 \(p.36-23\)](#)
- [debug コマンドの使用 \(p.36-25\)](#)
- [show platform forward コマンドの使用例 \(p.36-27\)](#)
- [crashinfo ファイル \(p.36-30\)](#)

XMODEM プロトコルによるソフトウェア障害からの回復

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

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

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する必要があります。

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。

```
switch% tar -tvf image_filename.tar
drwxr-xr-x 9658/25      0 Apr 21 13:20 2003 c3750-i5-mz.121.11-AX/
drwxr-xr-x 9658/25      0 Apr 18 18:31 2003 c3750-i5-mz.121.11-AX/html/
-rw-r--r-- 9658/25     4005 Apr 18 15:56 2003
c3750-i5-mz.121.11-AX/html/homepage.htm
-rw-r--r-- 9658/25     1392 Apr 18 15:56 2003
c3750-i5-mz.121.11-AX/html/not_supported.html
-rw-r--r-- 9658/25     9448 Apr 18 15:56 2003
c3750-i5-mz.121.11-AX/html/common.js
-rw-r--r-- 9658/25    22152 Apr 18 15:56 2003
c3750-i5-mz.121.11-AX/html/cms_splash.gif
-rw-r--r-- 9658/25     1211 Apr 18 15:56 2003
c3750-i5-mz.121.11-AX/html/cms_13.html
-rw-r--r-- 9658/25     2823 Apr 18 15:56 2003
c3750-i5-mz.121.11-AX/html/cluster.html
-rw-r--r-- 9658/25     4195 Apr 18 15:56 2003
c3750-i5-mz.121.11-AX/html/Redirect.jar
-rw-r--r-- 9658/25    14984 Apr 18 15:56 2003
c3750-i5-mz.121.11-AX/html/mono_disc.sgz
-rw-r--r-- 9658/25   1329516 Apr 18 15:56 2003
c3750-i5-mz.121.11-AX/html/CMS.sgz
-rw-r--r-- 9658/25   140105 Apr 18 15:56 2003
c3750-i5-mz.121.11-AX/html/images.sgz
-rw-r--r-- 9658/25   213848 Apr 18 15:56 2003
c3750-i5-mz.121.11-AX/html/help.sgz
-rw-r--r-- 9658/25   135599 Apr 18 15:56 2003
c3750-i5-mz.121.11-AX/html/CiscoChartPanel.sgz
-rwxr-xr-x 9658/25    58860 Apr 18 18:31 2003
c3750-i5-mz.121.11-AX/html/cms_boot.jar
-rw-r--r-- 9658/25   3970586 Apr 21 12:00 2003
c3750-i5-mz.121.11-AX/c3750-i5-mz.121.11-AX.bin
-rw-r--r-- 9658/25     391 Apr 21 13:20 2003 c3750-i5-mz.121.11-AX/info
-rw-r--r-- 9658/25     98 Apr 18 16:46 2003 info
```

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 c3750-i5-mz.121.11-AX/c3750-i5-mz.121.11-AX.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
c3750-i5-mz.121.11-AX/c3750-i5-mz.121.11-AX.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 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は、9600 にリセットされています。エミュレーション ソフトウェアの回線速度をスイッチのコンソール ポートに合わせて変更します。

ステップ 9 ヘルパー ファイルをロードします。

```
switch: load_helper
```

ステップ 10 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 11 XMODEM 要求が表示されたら、端末エミュレーション ソフトウェアの適切なコマンドを使用して伝送を開始し、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、新規ソフトウェア 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、スイッチに物理的にアクセスするエンドユーザは、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、パスワードをなくした状態から回復できます。これらの回復手順を実行するには、スイッチを直接操作する必要があります。



(注)

これらのスイッチでは、エンドユーザがデフォルト設定に戻すことに同意するだけでパスワードをリセットできます。それにより、システム管理者はこの機能の一部をディセーブルにできます。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。2 つの回復手順があります。

- [パスワード回復がイネーブルになっている場合の手順 \(p.36-5\)](#)
- [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 \(p.36-7\)](#)

パスワード回復をイネーブルまたはディセーブルにするには、**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 **Mode** ボタンを押しながら、電源コードを再度スタンドアロン スイッチまたはスタック マスターに接続します。

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、パスワード回復手順がディセーブルになっていないかどうか通知されます。

- 次のような開始のメッセージが表示された場合

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

「パスワード回復がイネーブルになっている場合の手順」(p.36-5) に進んで、その手順を実行します。

- 次のような開始のメッセージが表示された場合

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

「パスワード回復がディセーブルになっている場合の手順」(p.36-7) に進んで、その手順を実行します。

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は、9600 にリセットされています。エミュレーション ソフトウェアの回線速度をスイッチのコンソール ポートに合わせて変更します。

ステップ 3 ヘルパー ファイルをロードします。

```
switch: load_helper
```

ステップ 4 フラッシュ メモリの内容を表示します。

```
switch: dir flash:
```

スイッチのファイル システムが表示されます。

```
Directory of flash:
 13 drwx          192  Mar 01 1993 22:30:48 c3750-i5-mz-121-1.0
 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
```

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

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

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

```
Switch> enable
```

ステップ 8 コンフィギュレーション ファイルを元の名前に戻します。

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



(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 コンフィギュレーション ファイルをメモリにコピーします。

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

確認を求めるプロンプトに、**Return** キーを押して応答します。

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

ステップ 10 グローバル コンフィギュレーション モードを開始します。

```
Switch# configure terminal
```

ステップ 11 パスワードを変更します。

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

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

ステップ 12 イネーブル EXEC モードに戻ります。

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

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

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

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



(注)

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

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 コンフィギュレーション ファイルの有無を確認してください。

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

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

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

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

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

ステップ 2 ヘルパー ファイルをロードします。

```
Switch: load_helper
```

ステップ 3 フラッシュ メモリの内容を表示します。

```
switch: dir flash:
```

スイッチのファイル システムが表示されます。

```
Directory of flash:
13 drwx          192   Mar 01 1993 22:30:48 c3750-i5-mz-121-1.0

16128000 bytes total (10003456 bytes free)
```

ステップ 4 システムを起動します。

```
Switch: boot
```

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

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

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

```
Switch> enable
```

ステップ 6 グローバル コンフィギュレーション モードを開始します。

```
Switch# configure terminal
```

ステップ 7 パスワードを変更します。

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

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

ステップ 8 イネーブル EXEC モードに戻ります。

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



(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、シャットダウン インターフェイスの VLAN ID を指定します。スイッチがインターフェイス コンフィギュレーション モードの状態では、**no shutdown** コマンドを入力します。

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

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 Gbps) 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 つのみ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、または再編成する場合は、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.5-6) 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、「[スイッチ スタックに関する情報の表示](#)」(p.5-17) を参照してください。

コマンドスイッチ障害からの回復

ここでは、コマンドスイッチ障害から回復する手順について説明します。冗長コマンドスイッチグループを設定するには、Hot Standby Router Protocol (HSRP) を使用します。詳細については、第 6 章「スイッチのクラスタ設定」および第 32 章「HSRP の設定」を参照してください。



(注) HSRP は、クラスタに冗長性を持たせる方法として適しています。

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

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

- [故障したコマンドスイッチをクラスタメンバーに交換する場合 \(p.36-11\)](#)
- [故障したコマンドスイッチを他のスイッチに交換する場合 \(p.36-13\)](#)

これらの回復手順を実行するには、スイッチを直接操作する必要があります。

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

故障したコマンドスイッチをクラスタメンバーに交換する場合

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

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

CLI には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 メンバー スイッチをクラスタから削除します。

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

ステップ 8 イネーブル EXEC モードに戻ります。

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

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

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

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

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

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

ステップ 10 最初のプロンプトに **Y** を入力します。

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

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

または

```
Configuring global parameters:
```

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

ステップ 11 セットアップ プログラムの質問に回答します。

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

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

ステップ 12 **enable secret** および **enable** パスワードの入力を求めるプロンプトが表示された場合は、故障したコマンドスイッチのパスワードを再入力します。

ステップ 13 プロンプトが表示されたら、スイッチをクラスタ コマンド スイッチとしてイネーブルにすることを確認し、**Return** キーを押します。

ステップ 14 プロンプトが表示されたら、クラスタに名前を割り当て、**Return** キーを押します。

クラスタ名は 1 ~ 31 文字で、英数字、ダッシュ、または下線を使用することができます。

ステップ 15 最初のコンフィギュレーションが表示されたら、アドレスが正しいことを確認します。

ステップ 16 表示された情報が正しい場合はプロンプトに **Y**を入力し、**Return** キーを押します。

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

ステップ 17 ブラウザを起動して、新しいコマンドスイッチの IP アドレスを入力します。

ステップ 18 クラスタに追加する候補スイッチのリストを表示するには、Cluster メニューから **Add to Cluster** を選択します。

故障したコマンド スイッチを他のスイッチに交換する場合

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

ステップ 1 故障したコマンド スイッチの位置に新しいスイッチを追加し、同じようにクラスタ メンバーと接続します。

ステップ 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、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、スイッチの IP 情報を設定します。

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

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

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

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

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

ステップ 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変わります。

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

または

```
Configuring global parameters:
```

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

ステップ 7 セットアッププログラムの質問に応答します。

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

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

ステップ 8 **enable secret** および **enable** パスワードの入力を求めるプロンプトが表示された場合は、故障したコマンドスイッチのパスワードを再入力します。

ステップ 9 プロンプトが表示されたら、スイッチをクラスタ コマンドスイッチとしてイネーブルにすることを確認し、**Return** キーを押します。

ステップ 10 プロンプトが表示されたら、クラスタに名前を割り当て、**Return** キーを押します。

クラスタ名は 1 ~ 31 文字で、英数字、ダッシュ、または下線を使用することができます。

ステップ 11 最初のコンフィギュレーションが表示されたら、アドレスが正しいことを確認します。

ステップ 12 表示された情報が正しい場合はプロンプトに **Y** を入力し、**Return** キーを押します。

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

ステップ 13 ブラウザを起動して、新しいコマンドスイッチの IP アドレスを入力します。

ステップ 14 クラスタに追加する候補スイッチのリストを表示するには、Cluster メニューから **Add to Cluster** を選択します。

クラスタメンバーとの接続の回復

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管理アクセスを維持できない場合があります。メンバーに対する管理アクセスを維持できなくなり、メンバースイッチが正常にパケットを伝送している場合は、次に示す矛盾がないかどうかを確認してください。

- メンバースイッチ (Catalyst 3750、Catalyst 3560、Catalyst 3550、Catalyst 3500 XL、Catalyst 2970、Catalyst 2950、Catalyst 2900 XL、Catalyst 2820、および Catalyst 1900 スイッチ) を、ネットワークポートとして定義されたポートを通してコマンドスイッチに接続することはできません。
- Catalyst 3500 XL、Catalyst 2900 XL、Catalyst 2820、および Catalyst 1900 メンバースイッチを、同じ管理 VLAN に属するポートを通してコマンドスイッチに接続する必要があります。
- セキュアポートを通してコマンドスイッチに接続されたメンバースイッチ (Catalyst 3750、Catalyst 3560、Catalyst 3550、Catalyst 2970、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 (米国電気電子学会) 802.3ab 自動ネゴシエーションプロトコルは、スイッチの速度 (SFP 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。このプロトコルでは、状況によって設定の不一致が生じ、その結果パフォーマンスの低下を招くことがあります。設定の不一致は、次の状況下で発生します。

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

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

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



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

PoE スイッチ ポートのトラブルシューティング

Power over Ethernet (PoE) スイッチ ポートに接続され、AC 電源から給電されている電源装置 (Cisco IP Phone 7910 など) に対し電力が AC 電源から供給されない場合、装置はエラー ディセーブル ステートになることがあります。エラー ディセーブル ステートから回復するには、**shutdown** インターフェイス コンフィギュレーション コマンドを入力してから、**no shutdown** インターフェイス コマンドを入力します。エラー ディセーブル ステートからインターフェイスを回復する別の方法は、スイッチ上で自動回復を設定します。**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、一定時間ののち、自動的にインターフェイスをエラー ディセーブル ステートから復帰させます。

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 ポートの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

SFP モジュールのセキュリティと識別

シスコ認定の SFP モジュールに搭載されているシリアル Electrically Erasable Programmable Read-Only Memory (EEPROM; 電氣的消去再書き込み可能 ROM) には、モジュールのシリアル番号、ベンダーの名前と ID、固有のセキュリティ コード、Cyclic Redundancy Check (CRC; 巡回冗長検査) が格納されています。SFP モジュールがスイッチに搭載されると、スイッチのソフトウェアが EEPROM を読み取り、シリアル番号とベンダーの名前、ベンダー ID をチェックして、セキュリティ コードと CRC を再計算します。シリアル番号、ベンダーの名前またはベンダー ID、セキュリティ コード、CRC のどれかが無効である場合は、セキュリティ エラー メッセージが生成され、そのインターフェイスはエラー ディセーブル ステートになります。



(注)

セキュリティ エラー メッセージでは、BIC_SECURITY ファシリティが参照されます。Catalyst 3750 スイッチは SFP モジュールをサポートしますが、GBIC (ギガビット インターフェイス コンバータ) モジュールをサポートしません。エラー メッセージ テキストでは GBIC インターフェイスおよびモジュールが参照されますが、セキュリティ メッセージが実際に参照するのは SFP モジュールおよびモジュール インターフェイスです。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。

シスコ認定製品以外の SFP モジュールを使用している場合は、スイッチから SFP モジュールを取り外し、シスコ認定モジュールと交換してください。シスコ認定の SFP モジュールを取り付けたあと、**errdisable recovery cause gbic-invalid** グローバル コンフィギュレーション コマンドを使用してポートのステータスを検証し、errdisable ステートから回復するためのタイム インターバルを開始します。タイム インターバルが経過すると、スイッチはそのインターフェイスを errdisable ステートから復帰させ、再起動します。**errdisable recovery** コマンドの詳細については、このリリースのコマンド リファレンスを参照してください。

モジュールがシスコ 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場合は、SFP モジュールによってエラー メッセージが生成されます。この場合は、SFP モジュールを取り外して、取り付け直す必要があります。それでも障害が発生する場合は、SFP モジュールに障害がある可能性があります。

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.36-17)
- ping の実行 (p.36-17)

ping の概要

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

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

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。

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

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



(注)

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

次に、IP ホストに ping を実行する例を示します。

```
Switch# ping 172.20.52.3

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

表 36-1 に、表示される ping 文字出力の説明を示します。

表 36-1 ping 出力表示文字

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

ping セッションを終了するには、エスケープシーケンス (デフォルトは **Ctrl-^ X**) を入力します。デフォルトのエスケープシーケンスを入力するには、**Ctrl**、**Shift**、および **6** キーを同時に押してから放し、**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 \(p.36-19\)](#)
- [使用上の注意事項 \(p.36-19\)](#)
- [物理パスの表示 \(p.36-20\)](#)

レイヤ 2 traceroute の概要

レイヤ 2 traceroute 機能により、パケットが通過する送信元デバイスから宛先デバイスへの物理パスをスイッチが識別できます。レイヤ 2 traceroute は、ユニキャスト送信元および宛先 MAC アドレスのみをサポートしています。パスにあるスイッチの MAC アドレス テーブルを使用してパスを判別します。スイッチがレイヤ 2 traceroute に対応していない装置をパス上に検出した場合、スイッチはレイヤ 2 trace クエリを送信し続け、タイムアウトにします。

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

使用上の注意事項

レイヤ 2 traceroute の使用上の注意事項は次のとおりです。

- Cisco Discovery Protocol (CDP) は、ネットワークの全デバイスでイネーブルになっていなければなりません。レイヤ 2 traceroute を適切に機能させるには、CDP をディセーブルにしないでください。
レイヤ 2 traceroute をサポートするスイッチのリストについては、「[使用上の注意事項 \(p.36-19\)](#)」を参照してください。物理パス内のデバイスが CDP にトランスペアレントの場合、スイッチはこれらのデバイスを通るパスを識別できません。



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

- **ping** イネーブル EXEC コマンドを使用して接続をテストできる場合、スイッチは他のスイッチから到達可能です。物理パス内の全スイッチは、互いに到達可能でなければなりません。
- パス内で識別される最大ホップ数は 10 です。
- 送信元デバイスから宛先デバイスへの物理パス上にないスイッチに、**traceroute mac** または **traceroute mac ip** イネーブル EXEC コマンドを入力できます。パス内の全スイッチは、互いに到達可能でなければなりません。
- 指定された送信元および宛先 MAC アドレスが同じ VLAN に属している場合、**traceroute mac** コマンド出力は、レイヤ 2 パスのみを表示します。異なる VLAN に属する送信元および宛先 MAC アドレスを指定した場合、レイヤ 2 パスは識別されず、エラーメッセージが表示されます。
- マルチキャスト送信元 MAC アドレスまたはマルチキャスト宛先 MAC アドレスを指定した場合、パスは識別されず、エラーメッセージが表示されます。
- 複数の VLAN に属する送信元または宛先 MAC アドレスを指定した場合、送信元および宛先 MAC アドレスの両方が属する VLAN を指定しなければなりません。VLAN を指定しない場合、パスは識別されず、エラーメッセージが表示されます。

- 指定された送信元および宛先 IP アドレスが同じサブネットに属している場合、**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と、スイッチは Address Resolution Protocol (ARP) を使用して IP アドレスと対応する MAC アドレスおよび VLAN ID を対応付けます。
 - 指定した IP アドレスに対して ARP が存在する場合、スイッチは対応する MAC アドレスを使用して物理パスを識別します。
 - ARP エントリが存在しない場合、スイッチは ARP クエリを送信して IP アドレスを解釈しようとします。IP アドレスが解釈されない場合、パスは識別されず、エラーメッセージが表示されます。
- 複数のデバイスがハブを通じて 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 1 つのポートで検出される場合)、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 つのポートで検出されると、レイヤ 2 パスは識別されず、エラーメッセージが表示されます。
- この機能は、トークンリング VLAN ではサポートされていません。

物理パスの表示

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

- **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*]

この詳細については、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。

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 \(p.36-21 \)](#)
- [IP traceroute の実行 \(p.36-21 \)](#)

IP traceroute の概要

IP traceroute を使用すると、パケットがネットワークを通過するパスをホップ単位で識別できます。コマンド出力では、トラフィックが宛先までに通過する、ルータなどのネットワーク レイヤ (レイヤ 3) デバイスがすべて表示されます。

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参加できますが、**traceroute** コマンド出力にホップとして表示されるかは、不明です。スイッチが traceroute の宛先である場合、traceroute 出力では、最終宛先として表示されます。中間スイッチは、同じ VLAN のポート間でパケットのブリッジングだけを行っている場合、traceroute 出力では表示されません。ただし、中間スイッチが特定の packets をルーティングしているマルチレイヤ スイッチである場合、traceroute 出力ではこのスイッチをホップとして表示します。

ルータおよびサーバが特定の戻りメッセージを生成するには、**traceroute** イネーブル EXEC コマンドで IP ヘッダの Time To Live (TTL) フィールドを使用します。traceroute は、TTL フィールドを 1 に設定した User Datagram Protocol (UDP) を宛先ホストに送信することから処理を始めます。ルータは 1 または 0 の TTL 値を発見すると、データグラムを廃棄して、送信元に Internet Control Message Protocol (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。

次の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。最初のルータは、TTL フィールドを 1 減らして、次のルータにデータグラムを送信します。次のルータでは、TTL 値が 1 であるパケットを確認して、データグラムを廃棄し、送信元に time-to-live-exceeded メッセージを戻します。このプロセスは、データグラムが宛先ホストに到達するのに十分な TTL 値に増分されるまで (または最大 TTL 値になるまで) 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 ポート到達不可能エラーを送信します。ポート到達不可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、ポート到達不可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、イネーブル EXEC モードで次の手順を実行します。

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

次に、IP ホストに **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#
```

この表示では、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) を示しています。

表 36-2 traceroute 出力表示文字

文字	説明
*	プローブがタイムアウトです。
?	パケット タイプが不明です。
A	管理的に到達不可能です。この出力は、通常アクセス リストがトラフィックをブロックしていることを意味します。
H	ホストが到達不可能です。
N	ネットワークが到達不可能です。
P	プロトコルが到達不可能です。
Q	送信元がクエンチです。
U	ポートが到達不可能です。

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。

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 \(p.36-23 \)](#)
- [TDR の実行および結果の表示 \(p.36-23 \)](#)

TDR の概要

Cisco IOS Release 12.1(19)EA1 以上では、Time Domain Reflector (TDR) 機能を使用して、ケーブル接続の問題の診断および解決を行うことができます。TDR を実行すると、ローカル デバイスがケーブル経由で信号を送信して、反射信号を最初の信号と比較します。

TDR は、銅 Ethernet 10/100/1000 ポートでのみサポートされます。10/100 ポートまたは Small Form-factor Pluggable (SFP) モジュール ポートではサポートされません。

TDR は、次のケーブル接続の問題を検出できます。

- ツイストペア ワイヤのオープン、破損、切れ目 ワイヤは、リモート デバイスからのワイヤと接続されていない。
- ショートしたツイストペア ワイヤ ワイヤは相互に、またはリモート デバイスからのワイヤと接触している。たとえば、ツイストペア ケーブルは、一方のワイヤが他のワイヤにハンダ付けされる場合にショートする可能性があります。

ツイストペア ワイヤの一方が、オープンの場合、TDR はワイヤがオープンである長さを判別できません。

次の状況でのケーブル接続の問題を診断および解決するには、TDR を使用します。

- スイッチの交換
- 配線クローゼットの設定
- リンクを確立できない、またはリンクが適切に動作していない場合の、2 つのデバイス間の接続に関する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 を実行するには、***test cable-diagnostics tdr interface interface-id*** イネーブル EXEC コマンドを使用します。

```
Switch# test cable-diagnostics tdr interface gigabitethernet1/0/2
TDR test started on interface Gi1/0/2
A TDR test can take a few seconds to run on an interface
Use 'show cable-diagnostics tdr' to read the TDR results.
```

リンク ステータスがアップで、リンク速度が 10 または 100 Mbps のインターフェイス上で、***test cable-diagnostics tdr interface interface-id*** コマンドを入力すると、次のメッセージが表示されます。

```
Switch# test cable-diagnostics tdr interface gigabitethernet1/0/2
TDR test on Gi1/0/2 will affect link state and traffic
TDR test started on interface Gi1/0/2
A TDR test can take a few seconds to run on an interface
Use 'show cable-diagnostics tdr' to read the TDR results.
```

結果を表示するには、**show cable-diagnostics tdr interface interface-id** イネーブル EXEC コマンドを入力します。

```
Switch# show cable-diagnostics tdr interface gigabitethernet1/0/2
TDR test last run on: March 01 20:15:40
Interface Speed Local pair Pair length Remote pair Pair status
-----
Gig1/0/2 auto Pair A 0 +/- 2 meters N/A Open
          Pair B 0 +/- 2 meters N/A Open
          Pair C 0 +/- 2 meters N/A Open
          Pair D 0 +/- 2 meters N/A Open
```

表 36-3 に、**show cable-diagnostics tdr** コマンド出力のフィールドの説明を示します。

表 36-3 show cable-diagnostics tdr コマンド出力のフィールド説明

フィールド	説明
Interface	TDR が実行されたインターフェイス
Speed	現在の接続速度
Local pair	ローカル インターフェイスで TDR が試験中のワイヤ ペアの名前
Pair length	<ul style="list-style-type: none"> ケーブルが正しく接続されていて、リンクがアップ状態で、インターフェイス速度が 1000 Mbps の場合のケーブル長 ご使用のスイッチに関して、問題が発生しているケーブル上の場所 TDR は、次の場合のいずれか 1 つに関する問題の場所を判別できます。 <ul style="list-style-type: none"> ケーブルがオープンである。 ケーブルがショートしている。
Remote pair	ローカル ペアが接続されているワイヤ ペアの名前スイッチは、ケーブルが正しく接続されていて、リンクがアップ状態の場合でのみリモート ペアを判別することができます。
Pair status	TDR が稼働しているワイヤ ペアのステータス <ul style="list-style-type: none"> Normal ワイヤ ペアが正しく接続されています。 Not completed 試験中で、まだ終了していません。 Not supported インターフェイスは、TDR をサポートしていません。 Open ワイヤ ペアが切断されています。 Shorted ワイヤ ペアがショートしています。

TDR が稼働している場合、**show interface interface-id** コマンドの出力は次のとおりです。

```
Switch# show interface gigabitethernet1/0/2
gigabitethernet1/0/2 is up, line protocol is up (connected: TDR in Progress)
```

TDR が稼働していないインターフェイスで **show cable-diagnostics tdr interface interface-id** コマンドを入力した場合、出力は次のとおりです。

```
Switch# show cable-diagnostics tdr interface gigabitethernet1/0/2
% TDR test was never issued on Gig1/0/2
```

インターフェイスが TDR をサポートしていない場合、次のエラー メッセージが表示されます。

```
Switch# show cable-diagnostics tdr interface gigabitethernet1/0/1
% TDR test is not supported on switch 1
```

debug コマンドの使用

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

- 特定の機能に関するデバッグのイネーブル化 (p.36-25)
- 全システム診断のイネーブル化 (p.36-26)
- 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.36-26)



注意

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



(注)

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

特定の機能に関するデバッグのイネーブル化

デバッグをイネーブルにすると、スタック マスターでのみ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。その後、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
```

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

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

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

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

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

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

```
Switch# show debugging
```

全システム診断のイネーブル化

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

```
Switch# debug all
```



注意

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

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

デバッグおよびエラー メッセージ出力のリダイレクト

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

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



(注)

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

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

show platform forward コマンドの使用例

show platform forward イネーブル EXEC コマンドの出力から、システムを介してインターフェイスに入るパケットの転送結果に関して、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、このリリースのスイッチコマンド 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、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 内のギガビット イーサネット ポート 1 に入るパケットが未知の MAC アドレスにアドレッシングされる場合の **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
Gi1/0/2   0005   0001.0001.0001  0002.0002.0002
```

(テキスト出力は省略)

```
-----
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 Gi1/0/2
```

次に、VLAN 5 内のギガビット イーサネット 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した場合の出力例を示します。パケットは、アドレスを学習済みの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 内のギガビット イーサネット 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、パケットは廃棄されます。

```
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 内のギガビット イーサネット 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

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 Cisco IOS イメージの障害(クラッシュ)の原因となる問題をデバッグするときに役立つ情報が保存されています。クラッシュ情報は障害発生時にコンソールに出力され、障害後最初の Cisco IOS イメージ起動時にクラッシュ情報ファイルが作成されます(障害発生中は作成されません)。

ファイル内の情報には、障害が発生した Cisco IOS イメージの名前やバージョン、プロセッサレジスタのリスト、およびスタックトレースが含まれます。この情報をシスコのテクニカルサポートスタッフに提供するには、**show tech-support** イネーブル EXEC コマンドを使用します。

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管されます。

flash:/crashinfo/crashinfo_*n* ここで *n* はシーケンス番号

新たに作成される crashinfo ファイルごとに、既存のシーケンス番号よりも大きなシーケンス番号が使用されるため、シーケンス番号が最大であるファイルに最新の障害が記述されます。スイッチにはリアルタイムクロックがないため、タイムスタンプの代わりにバージョン番号が使用されます。ファイル作成時に使用されるファイル名は変更できません。ただし、ファイルが作成されたあとに、**rename** 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。crashinfo ファイルを削除する場合は、**delete** イネーブル EXEC コマンドを使用します。

最新の 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** や **copy** イネーブル EXEC コマンドなど、ファイルをコピーまたは表示するコマンドを使用し、ファイルにアクセスすることもできます。