



CHAPTER 49

トラブルシューティング

この章では、スイッチが稼働する Cisco IOS ソフトウェアに関連する問題を特定し、解決する方法について説明します。問題の性質に応じて、コマンドライン インターフェイス (CLI)、デバイス マネージャ、または Network Assistant を使用して、問題を特定し解決できます。

特に明記しない限り、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 スタックを指します。

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。

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.49-2)
- 「パスワードを忘れた場合の回復」 (P.49-4)
- 「スイッチ スタックの問題の防止」 (P.49-9)



(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.49-10)
- 「SFP モジュールのセキュリティと識別」 (P.49-11)
- 「SFP モジュール ステータスのモニタリング」 (P.49-11)
- 「温度のモニタ」 (P.49-11)
- 「ping の使用」 (P.49-12)
- 「レイヤ 2 traceroute の使用」 (P.49-13)
- 「IP traceroute の使用」 (P.49-15)
- 「TDR の使用」 (P.49-16)
- 「debug コマンドの使用」 (P.49-18)
- 「show platform forward コマンドの使用」 (P.49-20)
- 「crashinfo ファイルの使用」 (P.49-22)
- 「メモリの整合性検査ルーチンの使用」 (P.49-23)
- 「オンボード障害ロギングの使用」 (P.49-24)

- 「CPU 使用率に関するトラブルシューティング」(P.49-26)

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。

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。

また、端末または PC をスイッチに接続し、スイッチをイーサネット経由で CMC に接続することもできます。内部イーサネット管理ポートの詳細については、「[内部イーサネット管理ポートの使用](#)」(P.11-14) およびハードウェア インストール ガイドを参照してください。

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、dell.com または 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。dell.com または 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
```

2. **tar -xvf <image_filename.tar> <image_filename.bin>** UNIX コマンドを使用して、出力内の bin ファイル名を特定し、抽出します。

```
switch% tar -xvf image_filename.tar image_filename.bin
x cbs31x0-universal-mz.122-40.EX1/cbs31x0-universal-mz.122-40.EX1.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
cbs31x0-universal-mz.122-40.EX1/cbs31x0-universal-mz.122-40.EX1.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witchの電源コードを取り外します。

ステップ 5 スタッキング対応スイッチでは、次のいずれかの方法でスイッチの電源を切ります。

- スタンドアロンのスイッチの電源を切るか、CMC GUI を使用してスイッチ スタック全体の電源を切ります。
- スイッチまたはスタック メンバーをエンクロージャから取り外します。

スタッキング非対応スイッチの場合は、CMC GUI を使用してスイッチの電源を切るか、エンクロージャからスイッチを取り外します。

ステップ 6 Mode ボタンを押しながら、次のいずれかの方法でスイッチの電源を入れます。

- スwitchの電源を CMC GUI を使用して切断した場合は、GUI を使用してスイッチまたはスタックの電源を入れます。
- エンクロージャから取り外す方法でスイッチの電源を切った場合は、スタンドアロン スイッチまたはスタック メンバーをエンクロージャに再度挿入します。

点滅していたシステムの LED がグリーンの点灯になったら、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 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 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 9 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 10 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 11 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 12 **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 13 **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 14 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.49-5)
- 「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.49-8)

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 マスター上で入力した場合、コマンドはスタック全体に伝播され、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 ソフトウェアが稼働している 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。
- イーサネット接続経由で PC を CMC 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 CMC 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、「内部イーサネット管理ポートの使用」 (P.11-14) およびハードウェア インストール ガイドを参照してください。

ステップ 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 スタッキング対応スイッチでは、次のいずれかの方法でスイッチの電源を切ります。

- スタンドアロンのスイッチの電源を切るか、CMC GUI を使用してスイッチ スタック全体の電源を切ります。
- スイッチまたはスタック メンバーをエンクロージャから取り外します。

スタッキング非対応スイッチの場合は、CMC GUI を使用してスイッチの電源を切るか、エンクロージャからスイッチを取り外します。

ステップ 4 次のいずれかの方法でスイッチの電源を入れます。

- スイッチの電源を CMC GUI を使用して切断した場合は、GUI を使用してスイッチまたはスタックの電源を入れます。
- エンクロージャから取り外す方法でスイッチの電源を切った場合は、スタンドアロン スイッチまたはスタック メンバーをエンクロージャに再度挿入します。

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 が一瞬オレンジに点灯してからグリーンになるまで **Mode** ボタンを押したままにしてください。グリーンになったら **Mode** ボタンを離します。

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

- 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.49-5)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.49-8)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、スタッキング非対応スイッチ、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。

スタッキング非対応スイッチの場合

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

スタッキング対応スイッチの場合

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

- ステップ 6** スタッキング対応スイッチの場合は、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:
 2 -rwx      5752   Mar 1 1993 00:06:02 +00:00  config.text
 3 -rwx         24   Mar 1 1993 00:06:02 +00:00  private-config.text
 4 -rwx    9995193   Mar 1 1993 00:04:31 +00:00  cbs31x0-universal-mz.122-40.EX1
 6 -rwx     1147   Mar 1 1993 00:40:29 +00:00  FHH105002F6_IPBase.lic
 9 -rwx     1155   Mar 1 1993 23:55:57 +00:00  FHH105002F6_IPServ.lic
10 -rwx     1161   Mar 1 1993 23:56:21 +00:00  FHH105002F6_AdvIPServ.lic
 8 -rwx     8016   Mar 1 1993 00:00:51 +00:00  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
```

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) ステップ 9 に進む前に、接続されているすべてのスタック メンバの電源を入れ、それらが完全に初期化されるまで待ちます。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 を押して応答します。

これで、コンフィギュレーション ファイルがリロードされ、パスワードを変更できます。

ステップ 10 グローバル コンフィギュレーション モードを開始します。

```
Switch# configure terminal
```

ステップ 11 パスワードを変更します。

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

シークレット パスワードは 1 ～ 25 文字の英数字です。数字で始めることができます。大文字と小文字が区別され、スペースを使用できますが、先行スペースは無視されます。

ステップ 12 特権 EXEC モードに戻ります。

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

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

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

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



(注) 上記の手順を実行すると、スイッチの仮想インターフェイスがシャットダウン 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 モードの状態では、**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の場合、次のメッセージが表示されます。

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

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



注意

スイッチをデフォルト設定に戻すと、既存の設定がすべて失われます。システム管理者に問い合わせ、バックアップスイッチと VLAN (仮想 LAN) コンフィギュレーションファイルがあるかどうかを確認してください。

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

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

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

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:
4  -rwx      9995193   Mar 1 1993 00:04:31 +00:00  cbs31x0-universal-mz.122-40.EX1.0
57931776 bytes total (35725824 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) ステップ 9 に進む前に、接続されているすべてのスタック メンバの電源を入れ、それらが完全に初期化されるまで待ちます。

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** 特権 EXEC コマンドを入力します。インターフェイスを再びイネーブルにするには、**interface vlan vlan-id** グローバル コンフィギュレーション コマンドを入力して、シャットダウン インターフェイスの VLAN ID を指定します。スイッチがインターフェイス コンフィギュレーション モードの状態では、**no shutdown** コマンドを入力します。

ステップ 10 ここでスイッチを再設定する必要があります。システム管理者によって、バックアップ スイッチと VLAN コンフィギュレーション ファイルが使用可能に設定されている場合は、これらを使用します。

ステップ 11 スイッチをリロードします。

```
Switch# reload
```

スイッチ スタックの問題の防止



- (注)
- スイッチ スタックにスイッチを追加したりそこから取り外したりする場合には、必ずスイッチの電源を切ってください。スイッチ スタックでの電源関連のあらゆる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」という章を参照してください。
 - スタック メンバを追加または削除した後は、スイッチ スタックが全帯域幅 (32 Gb/s) で稼働していることを確認してください。スタック モード LED が点灯するまで、スタック メンバの Mode ボタンを押します。スイッチの最後の 2 つのポート LED がグリーンになります。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 10 ギガビット イーサネット ポートのいずれかです。最後の 2 つのポート LED の片方または両方がグリーンになっていない場合は、スタックが全帯域幅で稼働していません。
 - スイッチ スタックを管理する場合は、1 つの CLI セッションだけを使用することを推奨します。複数の CLI セッションをスタック マスターに使用する場合は注意が必要です。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。

- スタック内での位置に従ってスタック メンバ番号を手動で割り当てると、リモートから行うスイッチ 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、後にスイッチを追加、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 メンバ番号の詳細については、「[スタック メンバ番号](#)」(P.7-8) を参照してください。

スタック メンバをまったく同じモデルで置き換えると、新しいスイッチは、置き換えられたスイッチとまったく同じ設定で稼働します。この場合、新しいスイッチは置き換えられたスイッチと同じメンバ番号を使用するものと想定されます。

電源が入った状態のスタック メンバを取り外すと、スイッチ スタックが、それぞれ同じ設定を持つ 2 つ以上のスイッチ スタックに分割 (パーティション化) されます。スイッチ スタックを分離されたままにしておきたい場合は、新しく作成されたスイッチ スタックの IP アドレス (複数の場合あり) を変更してください。パーティション化されたスイッチ スタックを元に戻すには、次の手順を実行します。

- 新しく作成されたスイッチ スタックの電源を切ります。
- 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。
- スイッチの電源を入れます。

スイッチ スタックおよびそのメンバをモニタリングするため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.7-29) を参照してください。

自動ネゴシエーションの不一致の防止

IEEE 802.3ab 自動ネゴシエーション プロトコルは、スイッチの速度 (10 Mb/s、100 Mb/s、および 1000 Mb/s。ただし、SFP モジュール ポートを除く) およびデュプレックス (半二重または全二重) に関する設定を管理します。このプロトコルは設定を適切に調整しないことがあり、その場合はパフォーマンスが低下します。不一致は次の条件で発生します。

- 手動で設定した速度またはデュプレックスのパラメータが、接続ポート上で手動で設定された速度またはデュプレックスのパラメータと異なっている場合。
- ポートを自動ネゴシエーションに設定したが、接続先ポートは自動ネゴシエーションを使用しない全二重に設定されている場合。

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

- 速度とデュプレックスの両方について、両方のポートで自動ネゴシエーションを実行させます。
- 接続の両側でポートの速度とデュプレックスのパラメータを手動で設定します。



(注)

接続先装置が自動ネゴシエーションを実行しない場合は、2 つのポートのデュプレックス設定を一致させます。速度パラメータは、接続先のポートが自動ネゴシエーションを実行しない場合でも自動調整が可能です。

SFP モジュールのセキュリティと識別

シスコの Small Form-Factor Pluggable (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、および巡回冗長検査 (CRC) が格納されたシリアル EEPROM (電氣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。SFP モジュールがスイッチに挿入されると、スイッチ ソフトウェアは EEPROM を読み出してシリアル番号、およびベンダーの名前と 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` 機能を参照します。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、操作を再実行します。`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リング

`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

ここでは、次の情報について説明します。

- 「ping の概要」(P.49-12)
- 「ping の実行」(P.49-12)

ping の概要

スイッチは IP の ping をサポートしており、これを使ってリモート ホストへの接続をテストできます。ping はアドレスにエコー要求パケットを送信し、応答を待ちます。ping は次のいずれかの応答を返します。

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

ping の実行

別の IP サブネットワーク内のホストに ping を実行する場合は、ネットワークへのスタティック ルートを定義するか、またはこれらのサブネットワーク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 39 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 39 章「IP ユニキャスト ルーティングの設定」を参照してください。

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

コマンド	目的
<code>ping ip host address</code>	IP またはホスト名やネットワーク アドレスを指定してリモートホストへ ping を実行します。



(注) ping コマンドでは、他のプロトコル キーワードも使用可能ですが、このリリースではサポートされていません。

次に、IP ホストに ping を実行する例を示します。

```
Switch# ping 172.20.52.3
```

```
Type escape sequence to abort.
```

```

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

```

表 49-1 で、ping の文字出力について説明します。

表 49-1 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放し、その後 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.49-13)
- 「使用上のガイドライン」 (P.49-14)
- 「物理パスの表示」 (P.49-15)

レイヤ 2 traceroute の概要

レイヤ 2 traceroute 機能により、パケットが通過する、送信元デバイスから宛先デバイスへの物理パスを識別できます。レイヤ 2 Traceroute は、ユニキャストの送信元および宛先 MAC アドレスだけをサポートします。パス内にあるスイッチの 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のみを識別できます。パケットが通過する、送信元ホストから送信元デバイスまで、または宛先デバイスから宛先ホストまでのパスは識別できません。

使用上のガイドライン

レイヤ 2 traceroute の使用上の注意事項を次に示します。

- Cisco Discovery Protocol (CDP) がネットワーク上のすべてのデバイスでイネーブルでなければなりません。レイヤ 2 traceroute 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、「[使用上のガイドライン](#)」(P.49-14) を参照してください。物理パス内のデバイスが CDP に対して透過的な場合、スイッチはこれらのデバイスを通過するパスを識別できません。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する場合に他のスイッチから到達できます。物理パス内のすべてのスイッチは、他のスイッチから到達可能でなければなりません。
- パス内で識別可能な最大ホップ数は 10 です。
- 送信元デバイスから宛先デバイスの物理パス内にはないスイッチに、**traceroute mac** または **traceroute mac ip** 特権 EXEC コマンドを実行できます。パス内のすべてのスイッチは、このスイッチから到達可能でなければなりません。
- 指定した送信元および宛先 MAC アドレスが同一 VLAN に属する場合、**traceroute mac** コマンド出力はレイヤ 2 パスのみを表示します。指定した送信元および宛先 MAC アドレスが、それぞれ異なる VLAN に属している場合は、レイヤ 2 パスは識別されず、エラーメッセージが表示されます。
- マルチキャスト送信元または宛先 MAC アドレスを指定すると、パスは識別されず、エラーメッセージが表示されます。
- 送信元または宛先 MAC アドレスが複数の VLAN に属する場合は、送信元および宛先 MAC アドレスの両方が属している VLAN を指定する必要があります。VLAN を指定しないと、パスは識別されず、エラーメッセージが表示されます。
- 指定した送信元および宛先 MAC アドレスが同一サブネットに属する場合、**traceroute mac ip** コマンド出力はレイヤ 2 パスを表示します。IP アドレスを指定する場合、スイッチはアドレス解決プロトコル (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。
 - 指定の IP アドレスの ARP のエントリが存在している場合、スイッチは関連付けられた MAC アドレスを使用し、物理パスを識別します。
 - ARP のエントリが存在しない場合、スイッチは ARP クエリーを送信し、IP アドレスを解決しようと試みます。IP アドレスが解決されない場合は、パスは識別されず、エラーメッセージが表示されます。
- 複数のデバイスがハブを介して 1 つのポートに接続されている場合 (たとえば複数の CDP ネイバーがポートで検出された場合)、レイヤ 2 traceroute 機能はサポートされません。複数の CDP ネイバーが 1 つのポートで検出された場合、レイヤ 2 パスは特定されず、エラーメッセージが表示されます。
- この機能は、トークンリング VLAN ではサポートされません。

物理パスの表示

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

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

詳細については、このリリースのコマンド リファレンスを参照してください。

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.49-15)
- 「[IP traceroute の実行](#)」 (P.49-16)

IP traceroute の概要

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

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

traceroute 特権 EXEC コマンドは、IP ヘッダーの 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** 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。ルータで TTL 値が 1 または 0 であることを検出すると、データグラムをドロップし、インターネット制御メッセージプロトコル (ICMP) **time-to-live-exceeded** メッセージを送信元に送信します。**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先ポートから送信されたことを意味します。

IP traceroute の実行

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

コマンド	目的
<code>traceroute ip host</code>	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
 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#
```

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 49-2 traceroute の出力表示文字

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

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放し、その後 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.49-17)

- 「TDR の実行および結果の表示」 (P.49-17)

TDR の概要

Time Domain Reflector (TDR) 機能を使用すると、ケーブル配線の問題を診断して解決できます。TDR稼働時、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
- 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

TDR は、インターフェイス上で実行する場合、スタック マスター上でもスタック メンバ上でも実行できます。

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

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.49-18)
- 「システム全体診断のイネーブル化」(P.49-19)
- 「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.49-19)



注意

デバッグ出力は CPU プロセスで高プライオリティが割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。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ことをお勧めします。デバッグをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少なくなります。



(注)

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

特定機能に関するデバッグのイネーブル化

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 メンバのデバッグをイネーブルにするには、スタック マスターで **session switch-number** 特権 EXEC コマンドを使用してセッションを開始する必要があります。次に、スタック メンバのコマンドライン プロンプトで **debug** コマンドを入力します。

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** コマンドは引数を取りません。たとえば、スイッチド ポート アナライザ (SPAN) 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には、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タスを表示するには、特権 EXEC モードで次のコマンドを入力します。

```
Switch# show debugging
```

システム全体診断のイネーブル化

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

```
Switch# debug all
```



注意

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

no debug all 特権 EXEC コマンドを使用すると、すべての診断出力がディセーブルになります。いずれかの **debug** コマンドが誤ってイネーブルのままにならないようにするには、**no debug all** コマンドを使用すると便利です。

デバッグおよびエラー メッセージ出力のリダイレクト

ネットワーク サーバはデフォルトで、**debug** コマンドおよびシステム エラー メッセージの出力をコンソールに送信します。このデフォルトの設定を使用する場合は、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。

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



(注)

デバッグの出力先がシステムのオーバーヘッドに影響を与えないように注意してください。コンソールでメッセージ ログを行うと、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 メンバでシステム エラー メッセージが生成された場合は、そのスタック マスターからすべてのスタック メンバに対してエラー メッセージが表示されます。**syslog** は、スタック マスター上にあります。



(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、必ず **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 ログの詳細については、第 32 章「システム メッセージ ログの設定」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
Gi1/0/2   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 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
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ています。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、スイッチがこのファイルを自動的に作成します。

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を変更することはできません。ただし、ファイルが作成されてから、rename 特権 EXEC コマンドを使用して名前を変更することもできますが、show stacks または show tech-support 特権 EXEC コマンドを実行しても、名前が変更されたファイルの内容は表示されません。delete 特権 EXEC コマンドを使用して crashinfo ファイルを削除できます。

最新の crashinfo ファイル（つまり、ファイル名の末尾のシーケンス番号が最大であるファイル）を表示する場合は、show stacks または show tech-support 特権 EXEC コマンドを使用します。more 特権 EXEC コマンド、copy 特権 EXEC コマンドなど、ファイルのコピーまたは表示が可能な任意のコマンドを使用して、ファイルにアクセスすることもできます。

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。

メモリの整合性検査ルーチンの使用

スイッチは、メモリの整合性検査ルーチンを実行して、スイッチのパフォーマンスに影響を与える可能性のある無効な Ternary Content Addressable Memory (TCAM; 3 値連想メモリ) テーブル エントリを検出し、修正します。

スイッチでエラーが修正できない場合は、システム エラー メッセージがログに記録され、エラーが発生している次の TCAM スペースが示されます。

- Hulp Forwarding TCAM Manager (HFTM) スペース : レイヤ 2 およびレイヤ 3 の転送テーブルに関連します。
- Hulp Quality of Service (QoS) / アクセス コントロール リスト (ACL) TCAM Manager (HQATM) スペース : ACL および QoS 分類やポリシー ルーティングなどの ACL と同様のテーブルに関連します。

show platform tcam errors 特権 EXEC コマンドからの出力に、スイッチの TCAM メモリの整合性に関する情報が示されます。

スイッチ上で検出された TCAM メモリ整合性検査エラーを表示するには、特権 EXEC モードで **show platform tcam errors** コマンドを使用します。

コマンド	目的
show platform tcam errors	HQATM および HFTM 内の TCAM メモリ整合性検査エラーを表示します。

次に、**show platform tcam errors** コマンドの出力例を示します。

```
DomainMember# show platform tcam errors
TCAM Memory Consistency Checker Errors
-----
TCAM Space   Values  Masks  Fixups  Retries  Failures
HFTM         0       0       0       0       0
HQATM        0       0       0       0       0
```

表 49-3 TCAM チェッカーの出力におけるフィールドの定義

文字	説明
Values	無効な値の数。
Masks	無効なマスクの数。
Fixups	無効な値またはマスクの修正を最初に試みた回数。
Retries	無効な値またはマスクの修正を繰り返し試みた回数。
Failures	無効な値またはマスクを修正できなかった回数。

show platform tcam errors 特権 EXEC 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。

オンボード障害ロギングの使用

オンボード障害ロギング (OBFL) 機能を使用すれば、スイッチに関する情報を収集できます。この情報には稼働時間、温度、電圧などの情報が含まれており、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際に役立ちます。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データは消さないようにすることを推奨します。

ここでは、次の情報について説明します。

- 「OBFL の概要」 (P.49-24)
- 「OBFL の設定」 (P.49-25)
- 「OBFL 情報の表示」 (P.49-25)

OBFL の概要

OBFL は、デフォルトでイネーブルになっています。OBFL はスイッチおよび Small Form-Factor Pluggable (SFP) モジュールに関する情報を収集します。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、および接続されているすべての FRU デバイスの Unique Device Identifier (UDI) 情報。この情報には、Product Identification (PID; 製造識別)、Version Identification (VID)、およびシリアル番号が含まれます。
- 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
- 動作時間データ: 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

システム時計は、手動で時刻を設定するか、またはネットワーク タイム プロトコル (NTP) を使用するように設定します。

スイッチの稼働中には、**show logging onboard** 特権 EXEC コマンドを使用することにより、OBFL データを取得できます。スイッチに障害が発生した場合のデータの取得方法については、お客様担当のシスコテクニカル サポート担当者にお問い合わせください。

OBFL がイネーブルになっているスイッチが再起動された場合、新しいデータの記録が開始するまでに 10 分間の遅延があります。

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。スタッキング対応スイッチの場合、*switch-number* に指定できる範囲は 1 ~ 9 です。スタック非対応スイッチでは、スイッチ番号は常に 1 です。スイッチが生成してフラッシュ メモリに保存するハードウェア関連のメッセージの重大度を指定するには、**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指定したファイル 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 はディセーブルにせず、フラッシュ メモリに保存されたデータは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 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。

フラッシュ メモリ内の稼働時間と CLI コマンド情報以外のすべての OBFL データをクリアするには、**clear logging onboard** 特権 EXEC コマンドを使用します。

スイッチ スタックでは、**hw-module module logging onboard [message level level]** グローバル コンフィギュレーション コマンドを使用することにより、スタンドアロン スイッチまたはすべてのスタック メンバの OBFL をイネーブルにできます。

ここで説明した各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。

OBFL 情報の表示

OBFL 情報を表示するには、表 49-4 の特権 EXEC コマンドを 1 つまたは複数使用します。

表 49-4 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、および接続されているすべての FRU デバイスの UDI 情報を表示します。この情報には PID、VID、およびシリアル番号が含まれます。
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タック メンバーの温度を表示します。

表 49-4 OBFL 情報を表示するためのコマンド (続き)

コマンド	目的
<code>show logging onboard [module [switch-number]] uptime</code>	スタンダアロン スイッチまたは指定したスタック メンバーの起動時間、スタンダアロン スイッチまたは指定したスタック メンバーの再起動の理由、およびスタンダアロン スイッチまたは指定したスタック メンバーの最後の再起動からの経過時間を表示します。
<code>show logging onboard [module [switch-number]] voltage</code>	スタンダアロン 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 49-4 のコマンドの使用方法の詳細および OBFL データの例については、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。

CPU 使用率に関するトラブルシューティング

ここでは、CPU 利用の過重が原因で起こりうる問題の症状を一覧し、CPU 使用率の問題の検証方法について説明します。表 49-5 は、CPU 使用率に関する特定可能な主な問題を一覧しています。この表には、考えられる原因と修正措置が示されており、それぞれに Cisco.com の『[Troubleshooting High CPU Utilization](#)』へのリンクが張られています。

CPU 使用率が高い場合に起こりうる症状

CPU 使用率が高すぎることで次の症状が発生する可能性があります。他の原因で発生する場合があります。

- スパニングツリー トポロジの変更
- 通信が切断されたために EtherChannel リンクがダウンした
- 管理要求 (ICMP ping、SNMP のタイムアウト、低速な Telnet または SSH セッション) に応答できない
- UDLD フラッピング
- SLA の応答が許容可能なしきい値を超えたことによる IP SLA の失敗
- 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の DHCP または IEEE 802.1x の処理の失敗

レイヤ 3 スイッチの場合：

- ソフトウェアでルーティングされるパケットのドロップまたは遅延の増加
- BGP または OSPF ルーティング トポロジの変更
- HSRP フラッピング

問題と原因の検証

CPU 使用率が高いことが問題となっているかどうか判別するには、`show processes cpu sorted` 特権 EXEC コマンドを入力します。出力例の 1 行目にある下線が付いた部分に注目してください。

```
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、正常な CPU 使用率を示しています。この出力によると、最後の 5 秒間の使用率が 8%/0% となっていますが、この意味は次のとおりです。

- Cisco IOS の処理時間と割り込みの処理にかかった時間を合わせた CPU の合計の使用率は全体の 8%
- 割り込みの処理にかかった時間は全体の 0%

表 49-5 CPU 使用率に関する問題のトラブルシューティング

問題のタイプ	原因	修正措置
割り込みのパーセント値が合計の CPU 使用率の値とほぼ同程度に高い	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 パケットのソースを判別する。データの流れを遮断するか、スイッチの設定を変更します。「 Analyzing Network Traffic 」の項を参照してください。
割り込みの所要時間は最小限であったにもかかわらず CPU の合計使用率が 50% を超える	CPU 時間を過度に消費する Cisco IOS 処理が 1 つ以上存在する。これは通常、処理をアクティブ化するイベントによって始動されます。	異常なイベントを特定して根本的な原因を解消する。「 Debugging Active Processes 」の項を参照してください。

CPU 使用率の詳細および使用率の問題を解決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。

