CHAPTER **43**

トラブルシューティング

この章では、スイッチが稼動する 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、Command-Line Interface（CLI; コマンドライン インターフェイス）またはデバイス マネージャを使用して、問題を特定し解決できます。

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.43-2）
- 「パスワードを忘れた場合の回復」（P.43-4）

（注） 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。

- 「自動ネゴシエーションの不一致の防止」（P.43-9）
- 「SFP モジュールのセキュリティおよび識別」（P.43-9）
- 「SFP モジュール ステータスのモニタリング」（P.43-10）
- 「ping の使用」（P.43-10）
- 「レイヤ 2 traceroute の使用」（P.43-11）
- 「IP traceroute の使用」（P.43-13）
- 「debug コマンドの使用」（P.43-15）
- 「show platform forward コマンドの使用」（P.43-16）
- 「crashinfo ファイルの使用」（P.43-18）
- 「メモリ整合性検査ルーチン」（P.43-19）
- 「CPU 使用率に関するトラブルシューティング」（P.43-21）

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。

次の手順では、XMODEM プロトコルを使用して、破損したイメージ ファイルまたは誤ったイメージ ファイルを回復します。XMODEM プロトコルをサポートするソフトウェア パッケージは多くあり、この手順は使用しているエミュレーション ソフトウェアに大きく依存します。

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する必要があります。スイッチ ブートローダでは、Break キー検出機能を使用して自動ブート シーケンスを停止し、回復を行います。

（注） Break キー文字は、オペレーティング システムによって異なります。

UNIX を実行している SUN ワークステーションでは、Ctrl+C が Break キーです。

Windows XP または 2000 でハイパーターミナルを実行している PC では、Ctrl+Break が Break キーです。

Cisco TAC では、一般的なオペレーティング システムの Break キーと、Break キーをサポートしないターミナル エミュレータのための代替の *Break* キー *シーケンス*の表を用意しています。この一覧については、http://www.cisco.com/warp/public/701/61.html#how-to を参照してください。

次の手順に従って、破損したイメージ ファイルまたは誤ったイメージ ファイルを回復します。

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が可能な zip プログラムを使用します。zip プログラムを使用して bin ファイルを特定し、抽出します。
- UNIX を使用している場合は、次の手順に従ってください。

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

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

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

```
hostname% tar -xvf image_filename.tar image_filename.bin
x cbs30x0-i612-mz.122.25-SEE/cbs30x0-i612-mz.122.25-SEE.bin, 2928176 bytes, 5720
tape blocks
```

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

```
switch% ls -l image_filename.bin
-rw-r--r-- 1 boba 2928176 Apr 21 12:01
cbs30x0-i612-mz.122.25-SEE/cbs30x0-i612-mz.122.25-SEE.bin
```

ステップ 3　XMODEM プロトコルをサポートするターミナル エミュレーション ソフトウェアを使用して、PC をスイッチ 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　スイッチの前面にあるリリース ラッチを開位置まで押します。

ステップ 6　電源が切れる位置までスイッチをモジュール ベイから少しだけ引き出して、もう一度押し込みます。スイッチがサーバ シャーシに装着し直されると、再起動します。スイッチに電力が供給されると、POST が実行されます。

ステップ 7　スイッチの前面にあるリリース ラッチを閉位置まで押します。

ステップ 8　POST の実行が終わると、スイッチでは自動ブート プロセスが開始されます。ブートアップ シーケンス中に次のメッセージが表示されたら Break キー文字を入力します。

```
Initializing Flash
```

次に、ユーザが Break キーを入力した後でコンソールに表示されるメッセージの例を示します。

```
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
```

（注）　**reload** EXEC コマンドを使用するかまたは Dell Remote Access Controller/Modular Chassis（DRAC/MC）管理ボードで提供されるインターフェイスを使用して、スイッチにオペレーティング システムがリロードされるようにすることもできます。

DRAC/MC を使用してスイッチを接続する方法については、スタートアップ ガイドの「Connecting through the DRAC/MC」を参照してください。

（注）　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 9　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 10　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 11　XMODEM プロトコルを使用してファイル転送を開始します。

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

ステップ 12　XMODEM 要求が表示されたら、ターミナル エミュレーション ソフトウェアで適切なコマンドを使用して、転送を開始し、ソフトウェア イメージをフラッシュ メモリにコピーします。

ステップ 13　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 14　スイッチにソフトウェア イメージおよびデバイス マネージャをダウンロードするには、**archive download-sw** 特権 EXEC コマンドを使用して tar ファイルをダウンロードします。

（注）　この手順は任意です。

ステップ 15　**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 16　スイッチから、flash:*image_filename.bin* ファイルを削除します。

パスワードを忘れた場合の回復

スイッチのデフォルト設定では、スイッチを直接操作するエンド ユーザが、スイッチの電源投入時に起動プロセスを中断して新しいパスワードを入力することにより、パスワードを紛失した状態から回復できます。ここで紹介する回復手順を実行するには、スイッチを直接操作してください。

（注）　これらのスイッチでは、システム管理者はデフォルト設定に戻す場合に限りエンド ユーザによるパスワードのリセットを許可することによって、この機能の一部をディセーブルにできます。パスワード回復がディセーブルになっている場合に、エンド ユーザがパスワードをリセットしようとすると、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。

スイッチ ブートローダでは、Break キー検出機能を使用して自動ブート シーケンスを停止し、パスワードの回復を行います。

（注）　Break キー文字は、オペレーティング システムによって異なります。

UNIX を実行している SUN ワークステーションでは、Ctrl+C が Break キーです。

Windows XP または 2000 でハイパーターミナルを実行している PC では、Ctrl+Break が Break キーです。

Cisco TAC では、一般的なオペレーティング システムの Break キーと、Break キーをサポートしないターミナル エミュレータのための代替の *Break* キー シーケンスの表を用意しています。この一覧については、http://www.cisco.com/warp/public/701/61.html#how-to を参照してください。

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.43-5）
- 「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.43-7）

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。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　ターミナル エミュレーション ソフトウェアが稼動している端末または PC をスイッチのコンソール ポートに接続します。

ステップ 2　エミュレーション ソフトウェアの回線速度を 9600 ボーに設定します。

ステップ 3　スイッチの前面にあるリリース ラッチを開位置まで押します。

ステップ 4　電源が切れる位置までスイッチをモジュール ベイから少しだけ引き出して、もう一度押し込みます。スイッチがサーバ シャーシに装着し直されると、再起動します。スイッチに電力が供給されると、POST が実行されます。

ステップ 5　スイッチの前面にあるリリース ラッチを閉位置まで押します。

ステップ 6　POST の実行が終わると、スイッチでは自動ブート プロセスが開始されます。ブートアップ シーケンス中に次のメッセージが表示されたら Break キー キャラクタを入力します。

```
Initializing Flash
```

Break キーを入力したら、次のように操作します。

- 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.43-5）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.43-7）に進んで、その手順に従います。

（注）　**reload** EXEC コマンドを使用するかまたは Dell Remote Access Controller/Modular Chassis（DRAC/MC）管理ボードで提供されるインターフェイスを使用して、スイッチにオペレーティング システムがリロードされるようにすることもできます。

DRAC/MC を使用してスイッチを接続する方法については、スタートアップ ガイドの「Connecting through the DRAC/MC」を参照してください。

（注）　パスワードを回復したら、スイッチをリロードします。

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

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
```

次の手順を実行して、パスワード回復をイネーブルにします。

ステップ 1　フラッシュ ファイル システムを初期化します。

```
switch: flash_init
```

ステップ 2　コンソール ポートの速度を 9600 以外に設定していた場合、9600 にリセットされます。エミュレーション ソフトウェアの回線速度をスイッチのコンソール ポートに合わせて変更します。

ステップ 3　ヘルパー ファイルがある場合にはロードします。

```
switch: load_helper
```

ステップ 4　フラッシュ メモリの内容を表示します。

```
switch: dir flash:
```

スイッチ ファイル システムが表示されます。

```
Directory of flash:
   13  drwx         192   Mar 01 1993 22:30:48  cbs30x0-lanbase-mz.122-25.SEE
   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、パスワード定義が格納されています

```
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。プロンプトで **N** を入力します。

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

ステップ 7　スイッチ プロンプトで、特権 EXEC モードを開始します。

```
Switch> enable
```

ステップ 8　コンフィギュレーション ファイルを元の名前に戻します。

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

ステップ 9　コンフィギュレーション ファイルをメモリにコピーします。

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

確認を求めるプロンプトに、**Return** を押して応答します。

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

ステップ 10　グローバル コンフィギュレーション モードを開始します。

```
Switch# configure terminal
```

ステップ 11　パスワードを変更します。

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

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

ステップ 12　特権 EXEC モードに戻ります。

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

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

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

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

（注）　上記の手順を実行すると、スイッチの仮想インターフェイスがシャットダウン 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て、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、Break キー を入力し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 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   cbs30x0-lanbase-mz.122-25.SEE
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#
```

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、**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
```

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 Mbs、100 Mbs、および 1000 Mbs、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 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および識別

Cisco Small Form-Factor Pluggable（SFP; 着脱可能小型フォーム ファクタ）モジュールには、モジュールのシリアル番号、ベンダーの名前と 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）の情報を格納した EEPROM が搭載されています。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、ベンダー名とベンダー ID、セキュリティ コード、または CRC が無効な場合は、セキュリティ エラー メッセージが生成され、インターフェイスが errdisable 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、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 モジュールはサポートしていません。エラー メッセージのテキストに GBIC インターフェイスまたはモジュールとあっても、セキュリティ メッセージであれば、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意味します。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。

他社製の SFP モジュールを使用している場合は、その SFP モジュールをスイッチから取り外し、シスコ製のモジュールと交換します。シスコ製の SFP モジュールを挿入したら、**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、ポートの状態を確認し、errdisable ステートから回復する期間を入力します。この期間が経過すると、スイッチは errdisable ステートから回復し、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 モジュールであると識別されたにも関わらず、その正確性を確認するためのベンダー データの読み込みに失敗した場合は、SFP モジュールのエラー 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、もう一度取り付けます。エラーが解決しない場合は、SFP モジュールが故障してい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

SFP モジュールの物理ステータスまたは動作ステータスをチェックするには、**show interfaces transceiver** 特権 EXEC コマンドを使用します。このコマンドは、動作ステータスを表示します。動作ステータスには、特定インターフェイス上の SFP モジュールの温度や電流、アラーム ステータスなどがあります。また、このコマンドを使用して、SFP モジュールの速度とデュプレックスの設定をチェックすることもできます。詳細については、このリリースに対応するコマンド リファレンスにある **show interfaces transceiver** コマンド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.43-10）
- 「ping の実行」（P.43-10）

ping の概要

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

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

ping の実行

別の IP サブネットワーク内のホストに ping を実行する場合は、ネットワークへのスタティック ルートを定義するか、またはこれらのサブネット間でルーティングされるように IP ルーティングを設定する必要があります。詳細については、第 37 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 37 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、特権 EXEC モードで次の手順を実行します。

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 43-1 で、ping の文字出力について説明します。

表 43-1　ping の出力表示文字

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

ping セッションを終了するには、エスケープ シーケンス（デフォルトは **Ctrl+^ X**）を入力します。**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.43-11）
- 「使用上のガイドライン」（P.43-12）
- 「物理パスの表示」（P.43-13）

レイヤ 2 traceroute の概要

レイヤ 2 traceroute 機能により、パケットが通過する、送信元デバイスから宛先デバイスへの物理パスを識別できます。レイヤ 2 traceroute はユニキャスト送信元および宛先 Media Access Control（MAC; メディア アクセス制御）アドレスだけをサポートします。パスにあるスイッチの MAC アドレス テーブルを使用してパスを検索します。スイッチがレイヤ 2 traceroute をサポートしないデバイスをパスで検出すると、スイッチはレイヤ 2 トレース キューを送信し続けてタイムアウトにしてしまいます。

スイッチは、送信元デバイスから宛先デバイスへのパスだけが識別できます。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; シスコ検出プロトコル）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.43-12）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 25 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。
- パス内で識別できるホップ数は最大で 10 です。
- 送信元デバイスから宛先デバイスの物理パス内にないスイッチに、**traceroute mac** または **traceroute mac ip** 特権 EXEC コマンドを実行できます。パス内のすべてのスイッチは、このスイッチから到達可能でなければなりません。
- 指定した送信元および宛先 MAC アドレスが同一 VLAN に属する場合、**traceroute mac** コマンド出力はレイヤ 2 パスだけを表示します。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 を指定する必要があります。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 IP 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 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、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 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。

- **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

ここでは、次の情報について説明します。

- 「IP traceroute の概要」（P.43-13）
- 「IP traceroute の実行」（P.43-14）

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 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、User Datagram Protocol（UDP; ユーザ データグラム プロトコル）データグラムを、TTL フィールドが 1 に設定されている宛先ホストへ送信することから始まります。ルータが、TTL 値が 1 または 0 であることを検出すると、データグラムをドロップし、Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）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検索します。

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。最初のルータは、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 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
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#
```

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 つのプローブぞ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 43-2　traceroute の出力表示文字

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

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。**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。

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。

- 「特定機能に関するデバッグのイネーブル化」（P.43-15）
- 「システム全体診断のイネーブル化」（P.43-16）
- 「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.43-16）

注意　デバッグ出力には、CPU プロセスで高いプライオリティが割り当てられるので、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。このような時間帯を選んで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利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

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ため、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 フォーマットは、4.3 Berkeley Standard Distribution（BSD）UNIX およびそのバリエーションと互換性があります。

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

システム メッセージ ロギングの詳細については、第 30 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 内のポート 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 gigabitethernet0/1 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
Gi0/1    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

----------------------------------------
<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 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 gigabitethernet0/1 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
Gi0/2    0005 0001.0001.0001  0009.43A8.0145
```

次に、VLAN 5 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 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 gigabitethernet0/1 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 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 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
Gi0/2    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 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。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 種類の 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

基本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。**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、フラッシュ ファイル システム内の次のディレクトリに保存されます。

flash:/crashinfo/

ファイル名は crashinfo_*n* です。*n* にはシーケンス番号が入ります。

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い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。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 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 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

Cisco IOS Release 12.2(25)SEC 以降では、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 crashinfo ファイルには、スイッチの障害の原因を判別するのに役立つその他の追加情報が含まれます。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、フラッシュ ファイル システム内の次のディレクトリに保存されます。

flash:/crashinfo_ext/

ファイル名は crashinfo_ext_*n* になります。*n* にはシーケンス番号が入ります。

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。

メモリ整合性検査ルーチン

スイッチはメモリ整合性検査ルーチンを実行することで、スイッチのパフォーマンスに影響を与える、無効な Ternary Content Addressable Memory（TCAM）テーブル エントリを検出および修正します。

スイッチがエラーを修正できなかった場合は、システム エラー メッセージが記録され、エラーが発見された次の TCAM 空間が指定されます。

- 未割り当て空間：現在の SDM テンプレートに対する未割り当ての TCAM テーブル エントリが含まれます。
- Hulc Forwarding TCAM Manager（HFTM）空間：レイヤ 2 およびレイヤ 3 フォワーディング テーブルに関連する情報が含まれます。

- Hulc Quality of Service（QoS）/Access Control List（ACL）TCAM Manager（HQATM）空間：ACL、および QoS 分類やポリシー ルーティングなどの ACL に似たテーブルに関連する情報が含まれます。

show platform tcam errors 特権 EXEC コマンドの出力からは、スイッチ上での TCAM メモリ整合性の完全性に関する情報が得られます。

TCAM メモリ整合性検査エラーの表示

特権 EXEC モードでこのコマンドを使用すると、スイッチで検出された TCAM メモリ整合性検査エラーが表示されます。

コマンド	目的
show platform tcam errors	Hulc QoS/ACL TCAM Manager（HQATM）、Hulc Forwarding TCAM Manager（HFTM）、および TCAM 上の未割り当て空間にある TCAM メモリ整合性検査エラーが表示されます。

この例は、スイッチ上での TCAM メモリ整合性の完全性に関する情報を示しています。

```
Switch# show platform tcam errors

TCAM Memory Consistency Checker Errors
---------------------------------------
TCAM Space  Values  Masks   Fixups  Retries Failures
Unassigned  0       0       0       0       0
HFTM        0       0       0       0       0
HQATM       0       0       0       0       0

Switch#
```

この表示からは、完全性が検査された TCAM 部分に関する情報が得られます。

表 43-3　検査された TCAM 部分の詳細

カラム	説明
Values	TCAM テーブルで見つかった無効な値の数。
Masks	TCAM テーブルで見つかった無効なマスクの数。
Fixups	無効な値またはマスクを修正するための初期試行の回数。
Retries	無効な値またはマスクを修正するための試行の回数。
Failures	無効な値またはマスクを修正するための試行に失敗した回数。

show platform tcam errors 特権 EXEC コマンドの詳細については、このリリースに対応したコマンド 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 が過度にビジーになったことが原因で起こり得る問題の症状を一覧し、CPU の使用率に関する問題の検証方法を示します。表 43-4 に、CPU 使用率に関して特定できる問題の主な種類を示します。考えられる原因と対処方法、および Cisco.com の『*Troubleshooting High CPU Utilization*』へのリンクが記載されています。

CPU 使用率が高い場合に考えられる症状

CPU 使用率が過度に高くなると次の症状が現れる場合がありますが、これらは他の原因によって引き起こされる可能性もあることに留意してください。

- スパニング ツリー トポロジの変更
- 接続が切断されたために EtherChannel リンクが停止する
- 管理要求への応答の失敗（ICMP ping や SNMP のタイムアウト、Telnet または SSH セッションの低速化）
- UDLD のフラッピング
- SLA 応答が許容可能なしきい値を超過したことが原因の IP SLA の障害
- スイッチが要求を転送しないか要求に応答しない場合に発生する、DHCP または IEEE 802.1x の障害

レイヤ 3 スイッチの場合

- パケットのドロップまたは、ソフトウェアのルーテッド パケットの遅延の増加
- BGP または OSPF ルーティング トポロジの変更
- HSRP のフラッピング

問題および原因の検証

高い CPU 使用率が問題になっているかを判別するには、**show processes cpu sorted** 特権 EXEC コマンドを入力します。出力例の 1 行目の下線部分の情報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
...
<出力は省略>
```

この例では、CPU の使用率は正常であると示しています。出力によると、最後の 5 秒間の使用率が *8%/0%* であると示していますが、これは次のことを意味します。

- CPU の合計の使用率は 8% で、これには、Cisco IOS プロセスの実行時間と割り込み処理の所要時間の両方の合計が含まれています。
- 割り込みの処理の所要時間はゼロ % です。

表 43-4　CPU 使用率に関する問題のトラブルシューティング

問題の種類	原因	対処方法
割り込みのパーセント値が CPU 使用率の合計値と同じ程度に高い。	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 パケットの送信元を判別する。フローを停止するかスイッチの設定を変更してください。「Analyzing Network Traffic」を参照してください。
割り込みにかかった時間が最小限の CPU の合計使用率が 50% を超えている。	1 つ以上の Cisco IOS プロセスが過大な CPU の時間を消費している。これは通常、プロセスをアクティブにするイベントによってトリガされます。	異常なイベントを識別し、根本の原因をトラブルシューティングする。「Debugging Active Processes」を参照してください。

CPU 使用率および使用率の問題のトラブルシューティング方法の詳細については、Cisco.com の『*Troubleshooting High CPU Utilization*』を参照してください。