CHAPTER 41

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 Metro 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。

その他のトラブルシューティング情報については、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 12.2 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。

（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。

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、接続ができなくなります。

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。
  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`
  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。bin ファイル名（*image_filename.bin*）が出力に表示されなければなりません。
     `switch% ls -l image_filename.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　スイッチ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
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** 特権 EXEC コマンドを使用して、スイッチにソフトウェア イメージをダウンロードします。

ステップ 14　**reload** 特権 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。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.41-5）
- 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.41-7）

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。

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　スイッチの電源を切ります。

ステップ 4　**Mode** ボタンを押しながら、電源コードを再度スイッチに接続します。

ポート 1 の上の LED が消灯してから 1 ～ 2 秒後に、**Mode** ボタンを離します。ソフトウェアに関する数行分の情報と指示が表示され、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が通知されます。

- 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.41-5）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.41-7）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
```

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 ファイル システムがディレクトリに表示されます。

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、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** 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　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、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になっている場合は、次のメッセージが表示されます。

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

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

注意　スイッチをデフォルト設定に戻すと、既存の設定がすべて失われます。システム管理者に問い合わせて、バックアップ スイッチと VLAN コンフィギュレーション ファイル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かった場合のように、通常の起動プロセスが継続されます。ブート ローダー 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 ファイル システムがディレクトリに表示されます。

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、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　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、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。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。

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（1000 BASE-T SFP がインストールされていない場合は、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。

SFP モジュールのセキュリティと識別

シスコの SFP モジュールに搭載されているシリアル Electrically Erasable Programmable Read-Only Memory（EEPROM; 電気的に消去可能でプログラミング可能な ROM）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 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、BIC_SECURITY ファシリティが参照されます。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、シスコ製モジュールと交換してください。シスコの 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。

SFP モジュール ステータスのモニタ

show interfaces transceiver 特権 EXEC コマンドを使用すると、SFP モジュールの物理的または動作上のステータスを確認できます。このコマンドは、特定のインターフェイス上の SFP の温度や電流、およびアラーム ステータスなど、動作上の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。

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

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 34 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 34 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	説明
ping ip *host* | *address*	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 41-1 に、表示される ping 文字出力の説明を示します。

表 41-1　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離し、**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

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（メディア アクセス制御）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 クエリーを送信し続け、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。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過す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 25 章「CDP の設定」を参照してください。

- **ping** 特権 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** 特権 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 クエリーを送信して 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、次の特権 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

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** 特権 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パケット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** 特権 EXEC コマンドで IP ヘッダーの 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 UDP を宛先ホストに送信し、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、特権 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** 特権 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

  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 41-2　traceroute 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、トラフィックがアクセス リストによりブロックされていることを表します。
H	ホストに到達不能です。
N	ネットワークに到達不能です。
P	プロトコルに到達不能です。
Q	送信元が消滅しています。
U	ポートに到達不能です。

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。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離し、**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。具体的な内容は次のとおりです。

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にください。**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

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** コマンドには引数が必要ありません。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
```

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、設定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期間は、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、特権 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、特権 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
```

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、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** 特権 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 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。**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いる **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。

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 29 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 特権 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 Enhanced-Services（ES）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 gigabitethernet1/1/1 vlan 10 1.1.1 2.2.2 ip 172.18.18.3
172.18.18.1 udp 10 20
Global Port Number:472, Asic Number:1
Src Real Vlan Id:10, Mapped Vlan Id:2

Ingress:
 Lookup                    Key-Used                      Index-Hit  A-Data
InptACL  40_AC121201_AC121203-00_40000014_000A0000     01FFA   03000000
L2Local  80_00020002_00020002-00_00000000_00000000     01850   0000003A
Station Descriptor:02D30000, DestIndex:02D5, RewriteIndex:F002

========================================
Egress:Asic 0, switch 1
Output Packets:

----------------------------------------
Packet 1
 Lookup                    Key-Used                      Index-Hit  A-Data
OutptACL 50_AC121201_AC121203-00_40000014_000A0000     01FFE   03000000

Port       Vlan      SrcMac          DstMac    Cos  Dscpv
Gi1/0/1    0010 0001.0001.0001  0002.0002.0002

----------------------------------------
Packet 2
 Lookup                    Key-Used                      Index-Hit  A-Data
OutptACL 50_AC121201_AC121203-00_40000014_000A0000     01FFE   03000000

Port       Vlan      SrcMac          DstMac    Cos  Dscpv
Fa1/0/2    0010 0001.0001.0001  0002.0002.0002

----------------------------------------
Packet 3
 Lookup                    Key-Used                      Index-Hit  A-Data
OutptACL 50_AC121201_AC121203-00_40000014_000A0000     01FFE   03000000

Port       Vlan      SrcMac          DstMac    Cos  Dscpv
Fa1/0/3    0010 0001.0001.0001  0002.0002.0002

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

----------------------------------------
Packet 4
 Lookup                    Key-Used                      Index-Hit  A-Data
OutptACL 50_AC121201_AC121203-00_40000014_000A0000     01FFE   03000000
Packet dropped due to failed DEJA_VU Check on Gi1/1/1
```

次に、VLAN 5 内の ES 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 gigabitethernet1/1/1 vlan 5 1.1.1 0009.43a8.0145 ip
13.1.1.1 13.2.2.2 udp 10 20
Global Port Number:472, Asic Number:1
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
Fa1/0/5    0005 0001.0001.0001  0009.43A8.0145
```

次に、VLAN 5 内の ES 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 gigabitethernet1/1/1 vlan 5 1.1.1 03.e319.ee44 ip
13.1.1.1 13.2.2.2 udp 10 20
Global Port Number:472, Asic Number:1
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 ES 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 gigabitethernet1/1/1 vlan 5 1.1.1 03.e319.ee44 ip
110.1.5.5 16.1.10.5
Global Port Number:472, Asic Number:1
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 1e
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
Gi1/0/1    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場合、**show tech-support** 特権 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存されます。

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たあとに、**rename** 特権 EXEC コマンドを使用して名前を変更することもできますが、**show stacks** または **show tech-support** 特権 EXEC コマンドを実行しても、名前が変更されたファイルの内容は表示されません。crashinfo ファイルを削除する場合は、**delete** 特権 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** 特権 EXEC コマンドを使用します。**more** や **copy** 特権 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。