



CHAPTER 51

トラブルシューティング

この章では、IE 3010 スイッチの Cisco IOS ソフトウェアに関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)

この章で使用してい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.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References] にある『Cisco IOS Commands Master List, 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.51-2)
- 「パスワードを忘れた場合の回復」(P.51-3)
- 「クラスタ メンバスイッチとの接続の回復」(P.51-4)



(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.51-4)
- 「PoE スイッチ ポートのトラブルシューティング」(P.51-4)
- 「SFP モジュールのセキュリティと識別」(P.51-5)
- 「SFP モジュール ステータスのモニタリング」(P.51-6)
- 「ping の使用」(P.51-6)
- 「レイヤ 2 traceroute の使用」(P.51-6)
- 「IP traceroute の使用」(P.51-8)
- 「TDR の使用」(P.51-10)
- 「debug コマンドの使用」(P.51-11)
- 「show platform forward コマンドの使用」(P.51-12)
- 「crashinfo ファイルの使用」(P.51-14)
- 「トラブルシューティング表」(P.51-15)

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。

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間違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 パッケージは多数あり、使用するエミュレーションソフトウェアによって、この手順は異なります。

ここで紹介する回復手順を実行するには、スイッチを直接操作する必要があります。

ステップ 1 PC 上で、Cisco.com から tar 形式のソフトウェア イメージファイル (*image_filename.tar*) をダウンロードします。

Cisco IOS イメージは、tar ファイルのディレクトリ内に bin ファイルとして格納されます。Cisco.com 上のソフトウェア イメージファイルの検索方法については、リリース ノートを参照してください。

ステップ 2 tar ファイルから bin ファイルを抽出します。

- Windows を使用している場合は、tar ファイルの読み取り機能を備えた zip プログラムを使用します。zip プログラムを使用して bin ファイルを特定し、抽出します。
- UNIX を使用している場合は、次の手順に従ってください。

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

```
switch% tar -tvf image_filename.tar
```

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

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

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

```
switch% ls -l image_filename.bin
-rw-r--r--  1 bobas      3970586 Apr 21 12:00 image_name.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 Express Setup ボタンを押しながら、電源コードをスイッチに再接続します。

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

```
The system has been interrupted prior to initializing the flash file system. The following
commands will initialize the flash file system, and finish loading the operating system
software#
```

```
flash_init
load_helper
boot
```

ステップ 7 フラッシュ ファイル システムを初期化します。

```
switch: flash_init
```

- ステップ 8** コンソール ポートの速度を 9600 以外に設定していた場合、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 9** 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 10** 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 11** XMODEM 要求が表示されたら、端末エミュレーション ソフトウェアに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 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 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

パスワードを忘れた場合は、スイッチのパスワードを削除して新しく設定できます。

手順を開始する前に、次の点を確認してください。

- スイッチに物理的にアクセスできること。
- イネーブルになっていて装置に接続されていないスイッチ ポートが 1 つ以上あること。

スイッチのパスワードを削除して新しく設定するには、次の手順を実行します。

- ステップ 1** SETUP LED がグリーンに点滅し、使用可能なスイッチ ダウンリンク ポートの LED がグリーンに点滅するまで、Express Setup ボタンを押し続けます。
- PC またはラップトップの接続に使用できるスイッチ ダウンリンク ポートの空きがない場合は、いずれかのスイッチ ダウンリンク ポートから装置を接続解除します。もう一度、SETUP LED とポートの LED がグリーンに点滅するまで Express Setup ボタンを押し続けます。
- ステップ 2** LED がグリーンに点滅しているポートに、PC またはラップトップを接続します。
- SETUP LED とスイッチ ダウンリンク ポートの LED が点滅を中止し、グリーンに点灯します。
- ステップ 3** Express Setup ボタンを押し続けます。SETUP LED が再度グリーンに点滅し始めます。SETUP LED がグリーンに点灯するまで (約 5 秒間)、ボタンを押したままにします。すぐに Express Setup ボタンを放します。
- この手順によって、他の設定に影響を与えることなく、パスワードが削除されます。これで、パスワードを入力せずに、コンソール ポートまたはデバイス マネージャからスイッチにアクセスできるようになりました。

- ステップ 4** デバイス マネージャの [Express Setup] ウィンドウを使用するか、コマンドライン インターフェイスで **enable secret** 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、新しいパスワードを入力します。

## クラスタ メンバスイッチとの接続の回復

構成によっては、コマンドスイッチとメンバスイッチ間の接続を維持できない場合があります。メンバに対する管理接続を維持できなくなった場合で、かつ、メンバスイッチが正常にパケットを転送している場合は、次の矛盾がないかどうかを確認してください。

- メンバスイッチ (Catalyst 3750、Catalyst 3560、Catalyst 3550、Catalyst 3500 XL、Catalyst 2970、Catalyst 2960、Catalyst 2950、Catalyst 2900 XL、Catalyst 2820、および Catalyst 1900 スイッチ) は、ネットワーク ポートとして定義されたポートを介してコマンドスイッチに接続することはできません。
- Catalyst 3500 XL、Catalyst 2900 XL、Catalyst 2820、および Catalyst 1900 メンバスイッチは、同じ管理 VLAN に所属するポートを介してコマンドスイッチに接続する必要があります。
- セキュア ポートを介してコマンドスイッチに接続するメンバスイッチ (Catalyst 3750、Catalyst 3560、Catalyst 3550、Catalyst 2970、Catalyst 2960、Catalyst 2950、Catalyst 3500 XL、Catalyst 2900 XL、Catalyst 2820、および Catalyst 1900 スイッチ) は、セキュリティ違反が原因でポートがディセーブルになった場合、接続不能になることがあります。

## 自動ネゴシエーションの不一致の防止

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

- 手動で設定した速度またはデュプレックスのパラメータが、接続ポート上で手動で設定された速度またはデュプレックスのパラメータと異なっている場合。
- ポート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。

## PoE スイッチ ポートのトラブルシューティング

ここでは、Power over Ethernet (PoE) ポートのトラブルシューティングについて説明します。

## 電力消失によるポートの障害

PoE スイッチ ポートに接続され、AC 電源から電力が供給されている受電デバイス（Cisco IP Phone 7910 など）に AC 電源から電力が供給されない場合、そのデバイスは **errdisable** ステートになることがあります。**errdisable** ステートから回復するには、**shutdown** インターフェイス コンフィギュレーション コマンドを入力してから、**no shutdown** インターフェイス コマンドを入力します。スイッチで自動回復を設定し、**errdisable** ステートから回復することもできます。**errdisable recovery cause loopback** および **errdisable recovery interval seconds** グローバル コンフィギュレーション コマンドは、指定した期間が経過した後自動的にインターフェイスを **errdisable** ステートから復帰させます。

このリリースのコマンド リファレンスに記載されている次のコマンドを使用すると、PoE ポート ステータスをモニタできます。

- **show controllers power inline** 特権 EXEC コマンド
- **show power inline** 特権 EXEC コマンド
- **debug ilpower** 特権 EXEC コマンド

## 不正リンク アップによるポート障害

シスコ受電デバイスをポートに接続し、**power inline never** インターフェイス コンフィギュレーション コマンドを使用してポートを設定した場合は、不正リンク アップが発生し、ポートが **errdisable** ステートになることがあります。ポートを **error-disabled** ステートから回復するには、**shutdown** および **no shutdown** インターフェイス コンフィギュレーション コマンドを入力します。

**power inline never** コマンドで設定したポートにシスコ受電デバイスを接続しないでください。

## SFP モジュールのセキュリティと識別

シスコの SFP モジュールは、モジュールのシリアル番号、ベンダー名とベンダー ID、一意のセキュリティ コード、および巡回冗長検査（CRC）が格納されたシリアル EEPROM を備えています。スイッチに SFP モジュールを装着すると、スイッチ ソフトウェアは、EEPROM を読み取ってシリアル番号、ベンダー名、およびベンダー ID を確認し、セキュリティ コードおよび CRC を再計算します。シリアル番号、ベンダー名、ベンダー ID、セキュリティ コード、または CRC が無効な場合、ソフトウェアは、セキュリティ エラー メッセージを生成し、インターフェイスを **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。

## 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.51-6)
- 「レイヤ 2 traceroute の使用」(P.51-6)

## 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。

## 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.51-7)
- 「使用上のガイドライン」(P.51-7)
- 「物理パスの表示」(P.51-8)

## 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.51-7)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 30 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。
- パス内で識別される最大ホップ カウントは 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 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。
  - 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.51-8)
- 「[IP traceroute の実行](#)」 (P.51-9)

## 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へ送信します。**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事は、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

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

| コマンド                      | 目的                         |
|---------------------------|----------------------------|
| <b>traceroute ip host</b> | 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

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

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 51-1 **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.51-10)
- 「[TDR の実行および結果の表示](#)」 (P.51-10)

## 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。10/100 ポート、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 の実行および結果の表示

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.51-11)
- 「システム全体診断のイネーブル化」(P.51-12)
- 「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.51-12)

**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。ネットワーク トラフィック量やユーザ数が少ない期間に **debug** コマンドを使用することを推奨します。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

**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、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。

指定できる宛先として、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 33 章「システムメッセージロギングの設定」を参照してください。

## show platform forward コマンドの使用

**show platform forward** 特権 EXEC コマンドの出力からは、インターフェイスに入るパケットがシステムを介して送信された場合、転送結果に関して、有意義な情報がいくつか得られます。パケットに関して入力されたパラメータに応じて、参照テーブル結果、転送宛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、スイッチの特定用途向け集積回路 (ASIC) 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

<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
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
interface-id 0005 0001.0001.0001 0009.43A8.0145

```

## 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、および他のスイッチ特有の情報です。**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 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

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。

## トラブルシューティング表

次の表は、Cisco.com のトラブルシューティング マニュアルから抽出した内容をまとめたものです。

- 「[CPU 使用率に関するトラブルシューティング](#)」(P-15)
- 「[PoE に関するトラブルシューティング](#)」(P-17)

## 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 51-2 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しており、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もあります。

- 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断するには、**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 51-2 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。「 <a href="#">Analyzing Network Traffic</a> 」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。「 <a href="#">Debugging Active Processes</a> 」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。



## PoE に関するトラブルシューティング

図 51-1 PoE に関するトラブルシューティングのシナリオ

症状または問題	考えられる原因と解決法
<p>あるポートでだけ PoE が機能しない。</p> <p>1 つのスイッチ ポートに限り問題が発生する。このポートでは PoE 装置と PoE 非対応の装置のいずれも動作しないが、他のポートでは動作します。</p>	<p>この受電デバイスが他の PoE ポートで動作するかを確認する。</p> <p>ポートがシャットダウンまたは <b>error disabled</b> になっていないかを確認するために、ユーザ特権 EXEC コマンドの <b>show run</b>、<b>show interface status</b>、または <b>show power inline detail</b> を使用します。</p> <p>(注) ほとんどのスイッチはポートがシャットダウンしているときはポートの電力供給をオフにします。これは、IEEE 仕様でこれがオプションに指定されている場合も同様です。</p> <p>受電デバイスからスイッチ ポートまでのイーサネット ケーブルの動作が正常であることを確認します。具体的には、既知の正常な PoE 非対応のイーサネット装置とイーサネット ケーブルを接続して、受電デバイスがリンクを確立し他のホストとトラフィックを交換することを確認します。</p> <p>スイッチのフロント パネルから受電デバイスまでのケーブル長の合計が 100 メートル以下であることを確認します。</p> <p>スイッチ ポートからイーサネット ケーブルを外します。短いイーサネット ケーブルを使用して、既知の正常なイーサネット装置を、スイッチのフロント パネルの (パッチ パネルではない) このポートに直接接続します。これによってイーサネット リンクが確立され他のホストとトラフィックを交換できることを確認します。あるいは、ポートの VLAN SVI で ping を実行してください。次に、受電デバイスをこのポートに接続し、電源がオンになることを確認します。</p> <p>パッチ コードをスイッチ ポートに接続しても受電デバイスの電源がオンにならない場合、接続する受電デバイスの合計数とスイッチのパワー バジェット (使用可能な PoE) とを比較してください。 <b>show inline power</b> コマンドおよび <b>show inline power detail</b> コマンドを使用して使用可能な電力量を確認します。</p> <p>詳細については、Cisco.com の「<a href="#">No PoE On One Port</a>」を参照してください。</p>

図 51-1 PoE に関するトラブルシューティングのシナリオ (続き)

症状または問題	考えられる原因と解決法
<p>すべてのポートまたは 1 つのポートグループで PoE が機能しない。</p> <p>すべてのスイッチポートで問題が発生する。電力が供給されていないイーサネット装置がどのポートでもイーサネットリンクを確立できず、PoE 装置の電源がオンになりません。</p>	<p>電源関連のアラームが連続的または断続的に発生したり、繰り返し発生したりする場合は、電源装置を交換するか (Field-Replaceable Unit の場合)、そうでない場合はスイッチを交換してください。</p> <p>連続する複数のポートで問題があるものの、すべてのポートで問題が発生するわけではない場合、電源の故障ではないと考えられ、スイッチの PoE レギュレータに関連した異常の可能性があります。</p> <p>PoE の状況やステータスの変更について過去に報告されているアラームまたはシステムメッセージがないか、<b>show log</b> 特権 EXEC コマンドを使用して調べます。</p> <p>アラームがない場合は、<b>show interface status</b> コマンドを使用して、ポートがシャットダウンしていないか <b>errdisable</b> になっていないかを確認します。ポートが <b>errdisable</b> の場合、<b>shut</b> および <b>no shut</b> インターフェイス コンフィギュレーション コマンドを使用してポートを再びイネーブルにします。</p> <p>特権 EXEC コマンドの <b>show env power</b> および <b>show power inline</b> を使用して、PoE のステータスおよびパワー バジェット (使用可能な PoE) を調べます。</p> <p>実行コンフィギュレーションを調べて <b>power inline never</b> がこのポートに設定されていないことを確認します。</p> <p>受電していないイーサネット装置をスイッチポートに直接接続します。接続には短いパッチコードだけを使用します。既存の配線ケーブルは使用しないでください。<b>shut</b> および <b>no shut</b> インターフェイス コンフィギュレーション コマンドを入力し、イーサネットリンクが確立されていることを確認します。正しく接続している場合、短いパッチコードを使用して受電デバイスをこのポートに接続し、電源がオンになることを確認します。装置の電源がオンになったら、すべての中間パッチパネルが正しく接続されているか確認してください。</p> <p>1 本を除くすべてのイーサネットケーブルをスイッチポートから抜きます。短いパッチコードを使用して、1 つの PoE ポートにだけ受電デバイスを接続します。スイッチポートからの受電に比較して、受電デバイスが多くの電力を必要としないことを確認してください。</p> <p><b>show power inline</b> 特権 EXEC コマンドを使用して、ポートがシャットダウンしていない場合に、受電デバイスに電力が供給されることを確認します。あるいは、受電デバイスを観察して電源がオンになることを確認してください。</p> <p>1 台の受電デバイスだけがスイッチに接続しているときに電力が供給される場合、残りのポートで <b>shut</b> および <b>no shut</b> インターフェイス コンフィギュレーション コマンドを入力してから、イーサネットケーブルをスイッチの PoE ポートに 1 本ずつ再び接続してください。<b>show interface status</b> および <b>show power inline</b> 特権 EXEC コマンドを使用して、インライン電力統計およびポートステータスをモニタします。</p> <p>すべてのポートで、まだ PoE が機能しない場合は、電源装置の PoE セクションでヒューズを開くことができる場合があります。この場合、アラームが生成されるのが一般的です。過去にシステムメッセージでアラームが報告されていないか、ログをもう一度チェックしてください。</p> <p>詳細については、Cisco.com の「<a href="#">No PoE On Any Port or a Group of Ports</a>」を参照してください。</p>

図 51-1 PoE に関するトラブルシューティングのシナリオ (続き)

症状または問題	考えられる原因と解決法
<p>Cisco IP Phone が切断またはリセットされる。</p> <p>正常に動作した後で、Cisco phone またはワイヤレス アクセス ポイントが断続的にリロードしたり、PoE から切断されたりします。</p>	<p>スイッチから受電デバイスまでのすべての電気システムを確認してください。信頼性の低い接続は、電力供給の中断や受電デバイスの機能が不安定になる原因となり、受電デバイスの断続的な切断やリロードが発生します。</p> <p>スイッチ ポートから受電デバイスまでのケーブル長が 100 メートル以下であることを確認してください。</p> <p>スイッチが配置されている場所で電気環境にどのような変化があるか、切断時に、受電デバイスに何が起きるかについて注意してください。</p> <p>切断と同時にエラー メッセージが表示されたか注意します。 <b>show log</b> 特権 EXEC コマンドを使用してエラー メッセージを確認します。</p> <p>リロードの発生直前に IP Phone から Call Manager へのアクセスが失われているか確認してください (PoE の障害ではなくネットワークに問題が発生している場合があります)。</p> <p>受電デバイスを PoE 非対応の装置に交換し、装置が正しく動作することを確認します。PoE 非対応の装置にリンク障害または高いエラー率がある場合、スイッチ ポートと受電デバイスを接続する信頼性の低いケーブル接続が問題の可能性もあります。</p> <p>詳細については、Cisco.com の「<a href="#">Cisco Phone Disconnects or Resets</a>」を参照してください。</p>
<p>シスコ以外の受電デバイスがシスコ PoE スイッチで動作しない。</p> <p>シスコ PoE スイッチに接続するシスコ以外の受電デバイスに電源が供給されないか、電源投入後すぐに電源が切れます。PoE 非対応装置は正常に動作します。</p>	<p><b>show power inline</b> コマンドを使用して、受電デバイスの接続前後に、スイッチのパワー バジェット (使用可能な PoE) が使い果たされていないか確認してください。受電デバイスを接続する前に、このタイプの装置に十分な電力が使用可能であることを確認します。</p> <p><b>show interface status</b> コマンドを使用して、接続されている受電デバイスをスイッチが検出することを確認します。</p> <p><b>show log</b> コマンドを使用して、ポートの過電流状態を報告したシステム メッセージがないか確認します。症状を正確に特定してください。最初に電力が受電デバイスに供給され、その後、切断される状態ですか。その場合は、問題は最初のサージ電流 (突入電流) が原因で、ポートの電流上限しきい値が超過した可能性があります。</p> <p>詳細については、Cisco.com の「<a href="#">Non-Cisco PD Does Not Work Correctly on Cisco PoE Switch</a>」を参照してください。</p>

