CHAPTER 52

トラブルシューティング

この章では、IE 3000 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。問題の特定と解決には、問題の性質に応じて、CLI（コマンドライン インターフェイス）、デバイス マネージャ、または Network Assistant を使用できます。

ハードウェア インストレーション ガイドにも、LED に関する説明など、その他のトラブルシューティング情報が記載されています。

（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。

（注） 回復手順を実行するには、スイッチに物理的にアクセスする必要があります。

ソフトウェア障害からの回復

アップグレード時に、誤ったファイルをスイッチにダウンロードした場合や、イメージ ファイルを削除した場合に、スイッチ ソフトウェアが破損することがあります。いずれの場合も、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、接続できません。

この手順では、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 プロトコルは多数のソフトウェア パッケージでサポートされており、使用しているエミュレーション ソフトウェアによって手順が異なります。

この回復手順を実行するには、スイッチに物理的にアクセスする必要があります。

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

Cisco IOS イメージが bin ファイルとして、tar ファイル内のディレクトリに格納されます。Cisco.com 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 では、tar ファイルの読み取り機能を持つ zip プログラムを使用します。zip プログラムを使用して、bin ファイルに移動し、抽出します。
- UNIX では、次の手順を実行します。

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-1% 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。

```
unix-1% tar -xvf image_filename.tar image_filename.bin
x ies-lanbase-mz.122-52.SE/ies-ipservices-mz.122-52.SE.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。

```
unix-1% ls -l image_filename.bin
-rwxr-xr-x   1 bschuett eng      6365325 May 19 13:03
ies-lanbase-mz.122-52.SE/ies-ipservices-mz.122-52.SE.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の情報と手順が表示されます。

```
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 ポートの速度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、ターミナル 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　新しくダウンロードした 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、ソフトウェア イメージをスイッチに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 イメージが正常に動作す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。

```
11  -rwx       5825   Mar 01 1993 22:31:59  config.text
```

コマンド スイッチ障害からの回復

ここでは、コマンド スイッチの障害から回復する方法について説明します。Hot Standby Router Protocol（HSRP; ホットスタンバイ ルータ プロトコル）を使用すると、冗長コマンド スイッチ グループを設定できます。詳細については、第 6 章「スイッチのクラスタ化」および第 45 章「HSRP の設定」を参照してください。また、Cisco.com の『*Getting Started with Cisco Network Assistant*』も参照してください。

（注）　クラスタに冗長性を持たせるには、HSRP の使用を推奨します。

スタンバイ コマンド スイッチを設定していない場合に、コマンド スイッチに電源故障などの障害が発生すると、メンバー スイッチとの管理接続が失われ、新しいコマンド スイッチに交換する必要が生じます。ただし、接続されているスイッチ間の接続は影響を受けず、メンバー スイッチは通常どおりパケットを転送します。メンバーは、コンソール ポートを通してスタンドアロンのスイッチとして管理できます。また、メンバーに IP アドレスがある場合は、他の管理インターフェイスを通して管理することもできます。

コマンド スイッチ障害に備えるには、コマンド対応のメンバー スイッチやその他のスイッチに IP アドレスを割り当て、コマンド スイッチのパスワードを書き留め、メンバー スイッチと交換用コマンド スイッチの間に冗長接続が得られるようにクラスタを配線します。ここでは、故障したコマンド スイッチの 2 通りの交換方法について説明します。

- 「故障したコマンド スイッチをクラスタ メンバーに交換する場合」（P.52-4）
- 「故障したコマンド スイッチを別のスイッチに交換する場合」（P.52-6）

これらの回復手順を実行するには、スイッチに物理的にアクセスする必要があります。

コマンド対応スイッチの詳細については、リリース ノートを参照してください。

故障したコマンド スイッチをクラスタ メンバーに交換する場合

故障したコマンド スイッチを、同じクラスタ内にあるコマンド対応のメンバー スイッチに交換するには、次の手順を実行します。

ステップ 1　コマンド スイッチとメンバー スイッチの接続を解除し、クラスタからコマンド スイッチを物理的に取り外します。

ステップ 2　故障したコマンド スイッチの代わりにメンバー スイッチを取り付け、同じようにクラスタ メンバーと接続します。

ステップ 3　新しいコマンド スイッチで CLI セッションを開始します。

CLI にはコンソール ポートを使用してアクセスできます。また、スイッチに IP アドレスが割り当てられている場合は、Telnet も使用できます。コンソール ポートの使用方法の詳細については、スイッチのハードウェア インストレーション ガイドを参照してください。

ステップ 4　スイッチ プロンプトで特権 EXEC モードを開始します。

```
Switch> enable
Switch#
```

ステップ 5　*故障したコマンド スイッチ*のパスワードを入力します。

ステップ 6　グローバル コンフィギュレーション モードを開始します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

ステップ 7　メンバー スイッチをクラスタから削除します。

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

ステップ 8　特権 EXEC モードに戻ります。

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

ステップ 9　セットアップ プログラムを使用して、スイッチの IP 情報を設定します。このプログラムを実行すると、IP アドレス情報とパスワードの入力を求められます。特権 EXEC モードで「**setup**」と入力し、Return を押します。

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

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

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

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

ステップ 10　最初のプロンプトに「**Y**」と入力します。

セットアップ プログラムで表示されるプロンプトは、コマンド スイッチとして選択したメンバー スイッチによって異なります。

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

または

```
Configuring global parameters:
```

このプロンプトが表示されない場合は、「**enable**」と入力し、Return を押します。「**setup**」と入力し、Return を押して、セットアップ プログラムを開始します。

ステップ 11　セットアップ プログラムの質問に応答します。

ホスト名が要求されたら、コマンド スイッチでは 28 文字以内、メンバー スイッチでは 31 文字以内に制限されていることに注意してください。どのスイッチのホスト名でも、最後の文字には *-n*（*n* は数字）を使用しないでください。

Telnet（仮想端末）パスワードが要求されたら、1 ～ 25 文字の英数字を使用できること、大文字と小文字の区別があること、スペースは使用できるが先行スペースは無視されることに注意してください。

ステップ 12　**イネーブル シークレット** パスワードと**イネーブル** パスワードが要求されたら、再度、*故障したコマンド スイッチ*のパスワードを入力します。

ステップ 13　プロンプトが表示されたら、スイッチをクラスタ コマンド スイッチとしてイネーブルにし、Return を押します。

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

クラスタ名には、1 ～ 31 文字の英数字、ダッシュ、および下線を使用できます。

ステップ 15　初期設定が表示されたら、アドレスが正しいことを確認します。

ステップ 16　表示された情報が正しい場合は、「**Y**」と入力して Return を押します。

この情報が正しくない場合は、「**N**」と入力して Return を押し、ステップ 9 からやり直します。

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

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

故障したコマンド スイッチを別のスイッチに交換する場合

故障したコマンド スイッチを、クラスタ外にあるコマンド対応のスイッチに交換するには、次の手順を実行します。

ステップ 1　故障したコマンド スイッチの代わりに新しいスイッチを取り付け、同じようにクラスタ メンバーと接続します。

ステップ 2　新しいコマンド スイッチで CLI セッションを開始します。

CLI にはコンソール ポートを使用してアクセスできます。また、スイッチに IP アドレスが割り当てられている場合は、Telnet も使用できます。コンソール ポートの使用方法の詳細については、スイッチのハードウェア インストレーション ガイドを参照してください。

ステップ 3　スイッチ プロンプトで特権 EXEC モードを開始します。

```
Switch> enable
Switch#
```

ステップ 4　*故障したコマンド スイッチ*のパスワードを入力します。

ステップ 5　セットアップ プログラムを使用して、スイッチの IP 情報を設定します。

このプログラムを実行すると、IP アドレス情報とパスワードの入力を求められます。特権 EXEC モードで「**setup**」と入力し、Return を押します。

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

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

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

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

ステップ 6　最初のプロンプトに「**Y**」と入力します。

セットアップ プログラムで表示されるプロンプトは、コマンド スイッチとして選択したスイッチによって異なります。

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

または

```
Configuring global parameters:
```

このプロンプトが表示されない場合は、「**enable**」と入力し、Return を押します。「**setup**」と入力し、Return を押して、セットアップ プログラムを開始します。

ステップ 7　セットアップ プログラムの質問に応答します。

ホスト名が要求されたら、コマンド スイッチでは 28 文字以内に制限されていることに注意してください。どのスイッチのホスト名でも、最後の文字には *-n*（*n* は数字）を使用しないでください。

Telnet（仮想端末）パスワードが要求されたら、1 ～ 25 文字の英数字を使用できること、大文字と小文字の区別があること、スペースは使用できるが先行スペースは無視されることに注意してください。

ステップ 8　**イネーブル シークレット** パスワードと**イネーブル** パスワードが要求されたら、再度、*故障したコマンド スイッチ*のパスワードを入力します。

ステップ 9　プロンプトが表示されたら、スイッチをクラスタ コマンド スイッチとしてイネーブルにし、Return を押します。

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

クラスタ名には、1 ～ 31 文字の英数字、ダッシュ、および下線を使用できます。

ステップ 11　初期設定が表示されたら、アドレスが正しいことを確認します。

ステップ 12　表示された情報が正しい場合は、「**Y**」と入力して Return を押します。

この情報が正しくない場合は、「**N**」と入力して **Return** を押し、ステップ 9 からやり直します。

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

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

クラスタ メンバーとの接続が切断された場合の回復

構成によっては、コマンド スイッチとメンバー スイッチとの間の接続を維持できない場合があります。メンバーとの管理接続を維持できないが、メンバー スイッチ自体は正常にパケットを転送している場合は、次の点を確認してください。

- メンバー スイッチ（Catalyst 3750、Catalyst 3560、Catalyst 3550、Catalyst 3500 XL、Catalyst 2970、Catalyst 2960、Catalyst 2950、Catalyst 2900 XL、Catalyst 2820、および Catalyst 1900 スイッチ）を、ネットワーク ポートとして定義されたポートを通してコマンド スイッチに接続できません。
- Catalyst 3500 XL、Catalyst 2900 XL、Catalyst 2820、および Catalyst 1900 メンバー スイッチは、同じ管理 VLAN に属するポートを通してコマンド スイッチに接続する必要があります。
- セキュア ポートを通してコマンド スイッチに接続されたメンバー スイッチ（Catalyst 3750、Catalyst 3560、Catalyst 3550、Catalyst 2970、Catalyst 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、スイッチの速度（SFP モジュール ポートを除く 10 Mbps、100 Mbps、および 1000 Mbps）およびデュプレックス（半二重または全二重）の設定を管理します。このプロトコルによって設定の不一致が生じ、パフォーマンスが低下する場合があります。次のような場合に不一致が発生します。

- 手動で設定した速度またはデュプレックス パラメータが、接続先ポートの手動で設定された速度またはデュプレックス パラメータと異なる。
- 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。

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実にするには、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

シスコの着脱可能小型フォーム ファクタ（SFP）モジュールに搭載されているシリアル EEPROM 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、および Cyclic Redundancy Check（CRC; 巡回冗長検査）が記録されています。SFP モジュールをスイッチに取り付けると、スイッチ ソフトウェアが 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 コードと 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、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 ファシリティが参照されます。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 モジュールまたはモジュール 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、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。シスコ製 SFP モジュールを取り付けた後、**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、スイッチはインターフェイスを errdisable ステートから復帰させ、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正確な情報であるかどうかを確認できない場合は、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てから、取り付け直してください。それでもエラーが発生する場合は、SFP モジュールが破損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

show interfaces transceiver 特権 EXEC コマンドを使用すると、SFP モジュールの物理ステータスまたは動作ステータスを確認できます。このコマンドで表示される動作ステータスは、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 ステータスなどです。また、このコマンドを使用すると、SFP モジュールの速度とデュプレックスの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 リファレンスで、**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

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 ping をサポートしています。ping は、アドレスに対してエコー要求パケットを送信し、応答を待機します。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* is alive）は、ネットワーク トラフィックによって異なりますが、1 ～ 10 秒以内に返されます。
- 宛先が応答しない：ホストが応答しない場合は、*no-answer* メッセージが返されます。
- 不明ホスト：ホストが存在しない場合は、*unknown host* メッセージが返されます。
- 宛先到達不能：指定し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* メッセージが返されます。
- 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* メッセージが返されます。

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、サブネット間の 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 41 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。

デフォルトでは、すべてのスイッチ上で IP ルーティングがディセーブルになっています。IP ルーティングのイネーブル化または設定が必要な場合は、第 41 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装置に対してスイッチから ping を実行するには、特権 EXEC モードで次のコマンドを使用します。

コマンド	目的
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** コマンドには他のプロトコル キーワードもありますが、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 52-1 に、表示される ping 文字出力について説明します。

表 52-1　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になったことを意味します。
U	宛先到達不能エラー PDU 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。
&	パケットの存続時間を超過しました。

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。Ctrl、Shift、6 の各キーを同時に押してから放し、次に 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.52-10）
- 「使用上の注意事項」（P.52-11）
- 「物理パスの表示」（P.52-12）

レイヤ 2 traceroute の概要

レイヤ 2 traceroute 機能を使用すると、送信元装置から宛先装置までパケットが通過する物理パスを、スイッチで識別できます。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。パスの検索には、パス上のスイッチの MAC アドレス テーブルが使用されます。レイヤ 2 traceroute をサポートしていない装置をパス上で検出すると、スイッチはレイヤ 2 トレース クエリーを送信し続け、タイムアウトにします。

スイッチで識別できるのは、送信元装置から宛先装置までのパスだけです。送信元ホストから送信元装置へ、または宛先装置から宛先ホストへのパケットのパスを識別できません。

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。

- ネットワーク内のすべての装置で、Cisco Discovery Protocol（CDP; シスコ検出プロトコル）をイネーブルにする必要があります。CDP をディセーブルにすると、レイヤ 2 traceroute が正しく動作しません。

  レイヤ 2 traceroute をサポートするスイッチの一覧については、「使用上の注意事項」（P.52-11）を参照してください。物理パス内のいずれかの装置が CDP に対してトランスペアレントである場合、スイッチはその装置を通るパスを識別できません。CDP のイネーブル化の詳細については、第 32 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れば、そのスイッチは別のスイッチから到達可能です。物理パス内のすべてのスイッチは、互いに到達可能である必要があります。
- パス内で識別できるホップ数は最大で 10 です。
- 送信元装置から宛先装置までの物理パス上にないスイッチでは、**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ある必要があります。
- **traceroute mac** コマンドの出力結果としてレイヤ 2 パスが表示されるのは、指定の送信元および宛先 MAC アドレスが、同一の VLAN に属している場合だけです。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。
- マルチキャストの送信元または宛先 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 にある場合、送信元および宛先 MAC アドレス両方の属する VLAN を指定する必要があります。VLAN が指定されないと、パスは識別されず、エラー メッセージが表示されます。
- **traceroute mac ip** コマンドの出力結果にレイヤ 2 パスが表示されるのは、指定の送信元および宛先 IP アドレスが同一のサブネットに属している場合です。IP アドレスを指定した場合、スイッチは Address Resolution Protocol（ARP; アドレス解決プロトコル）を使用し、IP アドレスとそれに対応する MAC アドレスおよび VLAN ID を関連付けます。
  - 指定の IP アドレスの ARP のエントリが存在していた場合、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と、パスは識別されず、エラー メッセージが表示されます。
- 複数の装置がハブを介して 1 つのポートに接続されている場合（1 つのポート上で複数の CDP ネイバーが検出された場合など）は、レイヤ 2 traceroute 機能が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

パケットが通過した送信元装置から宛先装置までの物理パスを表示するには、次のいずれかの特権 EXEC コマンドを使用します。

- **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

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、ホップバイホップ ベースで識別できます。コマンド出力には、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、ネットワーク レイヤ（レイヤ 3）のすべての装置が表示されます。

スイッチは、**traceroute** 特権 EXEC コマンドの送信元または宛先になることができますが、**traceroute** コマンド出力にホップとして表示されるとは限りません。スイッチが traceroute の宛先である場合、traceroute の出力には最終的な宛先として表示されます。同じ VLAN 内のポート間でパケットをブリッジするだけの中間スイッチは、traceroute 出力に表示されません。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 スイッチである場合は、traceroute 出力にホップとして表示されます。

traceroute 特権 EXEC コマンドでは、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、ルータやサーバから特定のメッセージが返されるようにします。traceroute は、まず、TTL フィールドを 1 に設定した User Datagram Protocol（UDP; ユーザ データグラム プロトコル）データグラムを宛先ホストに送信します。ルータは、TTL 値 1 または 0 を検出すると、データグラムを廃棄し、Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）の time-to-live-exceeded メッセージを送信元に返します。traceroute は、この ICMP time-to-live-exceeded メッセージの送信元アドレス フィールドを調べることによって、最初のホップのアドレスを判別します。

次のホップを特定するために、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 フィールドを 1 だけ減らし、次のルータにデータグラムを送信します。2 番めのルータが TTL 値 1 を検出すると、データグラムを廃棄して、time-to-live-exceeded メッセージを送信元に返します。データグラムが宛先ホストに到達できる値に TTL が増分されるまで（または最大 TTL に達するまで）、このプロセスが続行されます。

データグラムが宛先に到達したことを判別できるように、traceroute では、データグラムの UDP 宛先ポート番号を、実際の宛先ホストで使用されないような非常に大きい値に設定します。宛先のホストが受け取ったデータグラムに、ローカルで使用されていない宛先ポート番号が含まれていると、ICMP の *port-unreachable* エラーが送信元に返されます。port-unreachable エラー以外のエラーはすべて中間ホップから生成されるため、port-unreachable エラーの受信は、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上で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*	パケットがネットワーク上で通過するパスを追跡します。

（注）　**traceroute** 特権 EXEC コマンドには他のプロトコル キーワードもありますが、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#
```

この表示には、ホップ カウント、ルータの IP アドレス、および送信された 3 つのプローブそれぞれのラウンドトリップ時間（ミリ秒単位）が示されています。

表 52-2　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	管理上の理由で到達不能です。通常、この出力は、アクセス リストでトラフィックがブロックされていることを意味します。
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（始点抑制要求）です。
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（デフォルトは Ctrl+^+X）を入力します。Ctrl、Shift、6 の各キーを同時に押してから放し、次に 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

Time Domain Reflector（TDR; タイム ドメイン反射率計）機能を使用すると、ケーブル接続の問題を診断および解決できます。TDR を実行すると、ローカルの装置がケーブルに信号を送信し、反射した信号を最初の信号と比較します。

TDR は、銅線のイーサネット 10/100 および 10/100/1000 ポートでサポートされます。SFP モジュール ポートではサポートされません。

TDR で検出できるケーブル接続の問題は、次のとおりです。

- ツイストペア ワイヤのオープン、破損、切断：ワイヤが、リモート装置のワイヤと接続されていません。
- ショートしたツイストペア ワイヤ：ワイヤどうしが接触しているか、リモート装置のワイヤと接触しています。たとえば、ツイストペアのワイヤの一方をもう一方にはんだ付けすると、ショートする可能性があります。

ツイストペア ワイヤの一方がオープンである場合、TDR でオープンであるワイヤの長さを特定できます。

次のような場合にケーブル接続の問題を診断および解決するには、TDR を使用します。

- スイッチの交換
- 配線クローゼットの設定
- 2 つの装置間の接続で、リンクを確立できない場合や、リンクが正常に動作しない場合のトラブルシューティング

TDR の実行と結果の表示

TDR を実行するには、**test cable-diagnostics tdr interface** *interface-id* 特権 EXEC コマンドを入力します。

結果を表示するには、**show cable-diagnostics tdr interface** *interface-id* 特権 EXEC コマンドを入力します。表示されるフィール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。

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および解決する方法について説明します。

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だけにしてください。**debug** コマンドは、ネットワーク トラフィックが少なく、ユーザ数が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）に関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
```

スイッチからの出力の生成は、このコマンドの **no** 形式を入力するまで続きます。

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、次の可能性が考えられます。

- 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、デバッグをイネーブルにした時点で、モニタ対象のトラフィック タイプが生成されていない可能性があります。デバッグ対象の機能に応じて、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てください。

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、この代わりに、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
```

システム全体の診断のイネーブル化

システム全体の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 トラフィックよりも優先されます。また、**debug all** 特権 EXEC コマンドでは、他の **debug** コマンドよりも大量の出力が生成されます。このため、スイッチのパフォーマンスが大幅に低下したり、場合によっては使用不能になったりする可能性があります。**debug** コマンドは、対象をなるべく限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、誤ってイネーブルにされたままの **debug** コマンドも、確実にディセーブルにできます。

デバッグ メッセージとエラー メッセージのリダイレクト

デフォルトでは、ネットワーク サーバからの **debug** コマンド出力やシステム エラー メッセージがコンソールに送信されます。このデフォルトを使用する場合、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て、デバッグ出力をモニタすることもできます。

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、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 およびその派生 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異なります。ログ メッセージの宛先をコンソールにすると、オーバーヘッドが非常に大きくなりますが、宛先を仮想端末にすると、それよりも小さくなります。ログ メッセージの宛先を syslog サーバにすると、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 ロギングの詳細については、第 35 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 コマンドを使用すると、システム経由でインターフェイスに入るパケットの転送結果に関して、有用な情報が出力されます。パケットに関して入力されたパラメータに応じて、検索テーブル結果、転送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のコマンド リファレンスを参照してください。

このコマンド出力の大部分はテクニカル サポート担当者向けの情報で、スイッチの application-specific integrated circuit（ASIC; 特定用途向け集積回路）に関する調査に役立ちます。しかし、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 に入るパケットの宛先が未知の MAC アドレスである場合の、**show platform forward** コマンドの出力例を示します。このパケットは、VLAN 5 内のすべてのポートにフラッディングされます。

```
Switch# show platform forward gigabitethernet1/1 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
Gi1/1    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
Gi1/1    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 Gi1/2
```

次に、VLAN 5 のポート 1 に着信するパケットが、VLAN 内の別のポートで学習済みのアドレスに送信される場合の出力例を示します。この場合、アドレスが学習されているポートから転送されます。

```
Switch# show platform forward gigabitethernet1/1 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
```

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 内のルータ MAC アドレスに設定されており、宛先 IP アドレスが未知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 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 内のルータ MAC アドレスに設定されており、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。この場合、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 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
Gi1/2    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）の原因となる問題をデバッグする際に役立つ情報が保存されます。スイッチのクラッシュ情報は、障害発生時にコンソールに出力されます。スイッチによって作成される crashinfo ファイルは、次の 2 種類です。

- 基本 crashinfo ファイル：障害発生後、初めて Cisco IOS イメージを起動するときに、自動的に作成されます。
- 拡張 crashinfo ファイル：システム障害発生時に自動的に作成されます。

基本 crashinfo ファイル

基本ファイルには、障害が発生した Cisco IOS のイメージ名とバージョン、プロセッサ レジスタのリスト、およびその他のスイッチ固有の情報が含まれます。**show tech-support** 特権 EXEC コマンドを使用すると、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 システムの次のディレクトリに格納されます。

flash:/crashinfo/

ファイル名は crashinfo_*n*（*n* はシーケンス番号）です。

新しい crashinfo ファイルが作成されるたびに、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ます。したがって、最大のシーケンス番号を持つファイルには、最新の障害が記述されています。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。ファイル作成時にシステムによって使用されるファイル名を変更できません。ファイルの作成後に、**rename** 特権 EXEC コマンドを使用して名前を変更することはできますが、ファイル名を変更した場合、**show tech-support** 特権 EXEC コマンドで内容を表示できなくなります。**delete** 特権 EXEC コマンドを使用すると、crashinfo ファイルを削除できます。

最新の基本 crashinfo ファイル（ファイル名末尾のシーケンス番号が最も大きいファイル）を表示するには、**show tech-support** 特権 EXEC コマンドを入力します。このファイルには、**more** または **copy** 特権 EXEC コマンドなど、コピーや表示を行うコマンドを使用してアクセスすることもできます。

拡張 crashinfo ファイル

スイッチの拡張 crashinfo ファイルは、システム障害発生時に作成されます。拡張ファイルには、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。この情報をシスコのテクニカル サポート担当者に提供するには、ファイルに手動でアクセスし、**more** または **copy** 特権 EXEC コマンドを使用します。

拡張 crashinfo ファイルは、フラッシュ ファイル システムの次のディレクトリに格納されます。
flash:/crashinfo_ext/

ファイル名は crashinfo_ext_*n*（*n* はシーケンス番号）です。

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、拡張 creashinfo ファイルが作成されないようにスイッチを設定できます。

トラブルシューティング用の表

次の表に、Cisco.com のトラブルシューティング関連マニュアルの抜粋を示します。

- 「CPU 使用率のトラブルシューティング」（P.52-19）

CPU 使用率のトラブルシューティング

ここでは、CPU 使用率が高すぎる場合に起きる可能性のある症状と、CPU 使用率の問題を確認する方法について説明します。表 52-3 に、特定可能な CPU 使用率の問題の主な種類を示します。考えられる原因と修正措置を述べ、Cisco.com の『*Troubleshooting High CPU Utilization*』へのリンクも示します。

高 CPU 使用率による症状

CPU 使用率が高すぎると次のような症状が起きることがありますが、これらの症状が他の原因で起きる場合もあります。

- スパニング ツリー トポロジの変更
- 通信切断による EtherChannel リンクのダウン
- 管理要求への応答なし（ICMP ping、SNMP タイムアウト、Telnet セッションや SSH セッションの速度低下）
- UDLD フラッピング
- 容認可能なスレッシュホールドを超えた SLA 応答が原因の IP SLA 障害

- スイッチが要求を転送しないか応答しない場合の DHCP または IEEE 802.1x の障害

レイヤ 3 スイッチの場合

- パケットの廃棄、またはソフトウェアでルーティングされるパケットの遅延増大
- 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

問題と原因の確認

高 CPU 使用率が問題になるかどうかを判断するには、**show processes cpu sorted** 特権 EXEC コマンドを入力します。出力例の最初の行の下線部を見てください。

```
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>
```

次に、正常な CPU 使用率の例を示します。出力によると、過去 5 秒間の使用率は *8%/0%* で、意味は次のとおりです。

- 合計 CPU 使用率は、Cisco IOS プロセスの実行時間と割り込みの処理時間を含めて 8% です。
- 割り込みの処理時間は 0% です。

表 52-3　CPU 使用率の問題のトラブルシューティング

問題の種類	原因	修正措置
割り込みの比率と合計 CPU 使用率の値がほぼ等しい。	CPU がネットワークから受け取るパケット数が多すぎます。	ネットワーク パケットの送信元を特定します。フローを停止するか、スイッチの設定を変更します。「Analyzing Network Traffic」を参照してください。
合計 CPU 使用率が 50% を超えているが、割り込みの処理時間が最小。	1 つ以上の Cisco IOS プロセスに非常に多くの CPU 時間が消費されています。通常、プロセスをアクティブ化したイベントがきっかけで発生します。	異常なイベントを特定し、根本原因をトラブルシューティングします。「Debugging Active Processes」を参照してください。

CPU 使用率と、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。