



ソフトウェア設定のトラブルシューティング

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

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ールガイドを参照してください。

- [ソフトウェア設定のトラブルシューティングに関する情報 \(1 ページ\)](#)
- [ソフトウェア設定のトラブルシューティング方法 \(11 ページ\)](#)
- [ソフトウェア設定のトラブルシューティングの確認 \(25 ページ\)](#)
- [ソフトウェア設定のトラブルシューティングのシナリオ \(28 ページ\)](#)
- [ソフトウェアのトラブルシューティングの設定例 \(33 ページ\)](#)
- [ソフトウェア設定のトラブルシューティングに関する追加情報 \(35 ページ\)](#)
- [ソフトウェア設定のトラブルシューティングの機能履歴 \(35 ページ\)](#)

ソフトウェア設定のトラブルシューティングに関する情報

スイッチのソフトウェア障害

スイッチソフトウェアがアップグレード中に破損する原因として、誤ったファイルがスイッチにダウンロードされた場合やイメージファイルが削除された場合があります。いずれの場合にも、スイッチは電源投入時自己診断テスト (POST) に失敗し、接続できなくなります。ソフトウェア障害から回復するには、「[ソフトウェア障害からの回復 \(11 ページ\)](#)」セクションで説明されている手順を実行します。

デバイスのパスワードを紛失したか忘れた場合

デバイスのデフォルト設定では、デバイス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、デバイスを直接操作してください。



(注) これらのデバイスでは、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ー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、エンドユーザーがパスワードをリセットしようとする、ステータスメッセージで回復プロセスの間はデフォルトの設定に戻すように指示されます。



(注) Cisco WLC の設定を複数の Cisco WLC 間でコピーすると、暗号化パスワード キーを回復できなくなります (RMA の場合)。

パスワードを紛失または忘れた場合にそのパスワードを回復するには、[パスワードを忘れた場合の回復 \(15 ページ\)](#) の項で説明する手順に従います。

Power over Ethernet (PoE) ポート

Power over Ethernet (PoE) スイッチポートでは、回路に電力が供給されていないことをスイッチが検知した場合、接続している次のデバイスに電力が自動的に供給されます。

- シスコ先行標準受電デバイス (Cisco IP Phone や Cisco Aironet アクセス ポイントなど)
- IEEE 802.3af 準拠の受電装置
- IEEE 802.3at 準拠の受電装置

受電デバイスが PoE スイッチポートおよび AC 電源に接続されている場合、冗長電力として利用できます。受電デバイスが PoE ポートにだけ接続されている場合、受電デバイスには冗長電力は供給されません。

受電デバイスを検出すると、スイッチは受電デバイスの電力要件を判断し、受電デバイスへの電力供給を許可または拒否します。また、スイッチは消費電力をモニタリングおよびポリシングすることで、装置の電力の消費をリアルタイムに検知できます。

詳細については、『*Interface and Hardware Component Configuration Guide (Catalyst 9300 Switches)*』の「Configuring PoE」の章を参照してください。

PoE のさまざまなトラブルシューティング シナリオについては、[Power over Ethernet \(PoE\) に関するトラブルシューティングのシナリオ \(28 ページ\)](#) の項を参照してください。

電力消失によるポートの障害

PoE デバイスポートに接続され、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。デバイス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。

デバイスの場合、**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あと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。

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 **errdisable** 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。

ping

デバイスは IP の ping をサポートしており、これを使用し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* メッセージが返されます。
- 不明なホスト：ホストが存在しない場合、*unknown host* メッセージが返されます。
- 宛先到達不能：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* メッセージが返されます。
- ネットワークまたはホストへの到達不能：ルートテーブルにホストまたはネットワークのエントリがない場合、*network or host unreachable* メッセージが返されます。

ping の動作を理解するには、[ping の実行（22 ページ）](#) の項を参照してください。

レイヤ 2 トレースルート

レイヤ 2 トレースルート機能により、パケットが通過する送信元デバイスから宛先デバイスまでの物理パスを識別できます。レイヤ 2 トレースルートは、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。トレースルートは、パス内にあるデバイスの MAC アドレステーブルを使用してパスを識別します。デバイスがパス内でレイヤ 2 トレースルートを

サポートしていないデバイスを検知した場合、デバイスはレイヤ2トレースクエリを送信し続け、タイムアウトにします。

デバイスは、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。

レイヤ2の traceroute のガイドライン

- ネットワーク内のすべてのデバイスで、Cisco Discovery Protocol (CDP) をイネーブルにする必要があります。レイヤ2 traceroute が適切に動作するために、CDP を無効にしないでください。

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。

- ping 特権 EXEC コマンドを使用して接続をテストできれば、このデバイスは別のデバイスから到達可能であると定義できます。物理パス内のすべてのデバイスは、他のデバイスから相互に到達可能でなければなりません。
- パス内で識別可能な最大ホップ数は 10 です。
- 送信元デバイスと宛先デバイス間の物理パス内にないデバイスで、**traceroute mac** または **traceroute mac ip** の特権 EXEC コマンドを実行できます。パス内のすべてのデバイスは、このスイッチから到達可能でなければなりません。
- 指定された送信元および宛先アドレスが同じ VLAN にある場合、**traceroute mac** コマンド出力はレイヤ2パスを表示します。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。
- 指定された送信元および宛先の IP アドレスが同一のサブネット内にある場合、**traceroute mac ip** コマンド出力はレイヤ2パスを表示します。IP アドレスを指定した場合、デバイスは Address Resolution Protocol (ARP) 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 を対応させます。
 - 指定の IP アドレスの ARP のエントリが存在している場合、デバイスは関連付けられた 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、デバイスは ARP クエリを送信し、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。
- レイヤ2 トレースルートは、ユーザデータグラム プロトコル (UDP) ポート 2228 でリスニングソケットを開きます。このポートは、任意の IPv4 アドレスを使用してリモートからアクセスでき、認証は必要ありません。この UDP ソケットにより、VLAN 情報、リンク、特定の MAC アドレスの存在、および CDP ネイバー情報をデバイスから読み取ることができます。この情報を使用することにより、最終的にレイヤ2 ネットワークトポロジの全体像を構築できます。
- レイヤ2 トレースルートはデフォルトで有効になっており、グローバルコンフィギュレーション モードで **no l2 traceroute** コマンドを実行することによって無効にできます。レイヤ2 トレースルートを再度有効にするには、グローバル コンフィギュレーション モードで **l2 traceroute** コマンドを使用します。

IP トレースルート

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。

デバイスは、**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、**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。デバイスを **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。中間デバイスが同じ 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、中間デバイスが特定の packets をルーティングするマルチレイヤデバイスの場合、このデバイスは **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 ヘッダーの存続可能時間 (TTL) 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、ユーザデータグラム プロトコル (UDP) データグラムを、TTL フィールドが 1 に設定されている宛先ホストへ送信することから始まります。ルータで TTL 値が 1 または 0 であることを検出すると、データグラムをドロップし、インターネット制御メッセージプロトコル (ICMP) **time-to-live-exceeded** メッセージを送信元に送信します。**traceroute** は、ICMP **time-to-live-exceeded** メッセージの送信元アドレス フィールドを調べて、最初のホップのアドレスを判別します。

ネクスト ホップを識別するために、**traceroute** は TTL 値が 2 の UDP パケットを送信します。1 番目のルータは、TTL フィールドの値から 1 を差し引いて次のルータにデータグラムを送信します。2 番目のルータは、TTL 値が 1 であることを確認すると、このデータグラムを廃棄し、**time-to-live-exceeded** メッセージを送信元へ返します。このように、データグラムが宛先ホストに到達するまで (または TTL の最大値に達するまで) TTL の値は増分され、処理が続けられます。

データグラムが宛先に到達したことを学習するために、**tracert** 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。

例：IP ホストに対する **tracert** の実行 (34 ページ) に進み、IP **tracert** プロセスの例を参照してください。

Time Domain Reflector ガイドライン

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。

- デバイスの交換
- 配線クローゼットの設定
- リンクが確立できない、または適切に動作していない場合における、2つのデバイス間の接続のトラブルシューティング

TDR の実行時、次の場合にデバイスは正確な情報をレポートします。

- ギガビット リンク用のケーブルが単線コア ケーブル
- オープンエンド ケーブルが未終端

TDR の実行時、次の場合にデバイスは正確な情報をレポートしません。

- ギガビット リンク用のケーブルがツイストペア ケーブルまたは連続接続された単線コア ケーブル
- リンクが 10 Mb または 100 Mb
- より線ケーブル

- リンク パートナーが Cisco IP Phone
- リンク パートナーが IEEE 802.3 に準拠していない

[TDR の実行および結果の表示 \(23 ページ\)](#) に移動し、TDR のコマンドを確認します。

debug コマンド



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お勧めします。デバッグをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が低くなります。

debug コマンドはすべて特権 EXEC モードで実行します。ほとんどの **debug** コマンドは引数を取りません。

システム レポート

システム レポートまたは `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。明瞭度と整合性の高い重要なクラッシュ情報を迅速かつ確実に収集することが必要です。さらに、この情報の収集とバンドルが、特定のクラッシュの発生に対し関連付けが特定ができるような方法で行われることが必要です。

システム レポートは次の状況で生成されます。

- スイッチ障害の場合：システム レポートは障害が発生したメンバーで生成されます。スタック内の他のメンバーではレポートは生成されません。
- スイッチオーバーの場合：システム レポートはハイアベイラビリティ（HA）のメンバースイッチでのみ生成されます。非 HA メンバーについてはレポートは生成されません。

リロード時はレポートは生成されません。

クラッシュ プロセス時は、次の情報がスイッチからローカルに収集されます。

1. 完全なプロセス `core`
2. トレースログ
3. IOS の `syslog`（非アクティブなクラッシュの場合には保証されません）
4. システムプロセス情報
5. ブートアップログ

6. リロードログ

7. 特定のタイプの /proc 情報

この情報は個別のファイルに格納されてから、アーカイブされて1つのバンドルに圧縮されます。これにより、クラッシュのスナップショットを1つの場所で取得して、分析のためにボックス外に移動できるようになります。このレポートは、スイッチが ROMmon/ブートローダにダウンする前に生成されます。

完全な core およびトレースログ以外はテキスト ファイルです。

コアダンプを生成するには、**request platform software process core fed switch active** コマンドを使用します。

```
Device# request platform software process core fed switch active
SUCCESS: Core file generated.
```

```
Device# dir bootflash:/core
Directory of bootflash:/core/
16430  -rw-          10941657  Apr 6 2022 00:15:20 +00:00
Switch_1_RP_0_fed_18469_20220406-001511-UTC.core.gz
16812  -rw-           1  Apr 6 2022 00:01:48 +00:00  .callhome
16810  drwx           4096  Jan 18 2022 21:10:35 +00:00  modules
```

crashinfo ファイル

デフォルトでは、生成されたシステム レポート ファイルは /crashinfo ディレクトリに格納されます。Ifit は、領域不足のため crashinfo パーティションに保存できません。そのため、/flash ディレクトリに保存されます。

ファイルを表示するには、**dir crashinfo:** コマンドを入力します。次に crashinfo ディレクトリの出力例を示します。

```
Device# dir crashinfo:
Directory of crashinfo:/

23665 drwx 86016 Jun 9 2017 07:47:51 -07:00 tracelogs
11 -rw- 0 May 26 2017 15:32:44 -07:00 koops.dat
12 -rw- 4782675 May 29 2017 15:47:16 -07:00 system-report_1_20170529-154715-PDT.tar.gz
1651507200 bytes total (1519386624 bytes free)
```

システムレポートは、次の形式で crashinfo ディレクトリにあります。

```
system-report_[switch number]_[date]-[timestamp]-UTC.gz
```

スイッチがクラッシュしたら、システムレポートファイルを確認します。最後に生成されたシステムレポートファイルは crashinfo ディレクトリの下に last_systemreport というファイル名で保存されます。問題のトラブルシューティングを行う際、システム レポートおよび crashinfo ファイルが TAC の役に立ちます。

生成されたシステム レポートは、TFTP や HTTP などいくつかのオプションを使用して、さらにコピーできます。

```
Device# copy crashinfo: ?
crashinfo: Copy to crashinfo: file system
flash: Copy to flash: file system
ftp: Copy to ftp: file system
```



```

http:          Copy to http: file system
https:         Copy to https: file system
null:          Copy to null: file system
nvram:         Copy to nvram: file system
rcp:           Copy to rcp: file system
running-config Update (merge with) current system configuration
scp:           Copy to scp: file system
startup-config Copy to startup configuration
syslog:        Copy to syslog: file system
system:        Copy to system: file system
tftp:          Copy to tftp: file system
tmpsys:        Copy to tmpsys: file system

```

TFTP サーバーにコピーするための一般的な構文は次のとおりです。

```

Device# copy crashinfo: tftp:
Source filename [system-report_1_20150909-092728-UTC.gz]?
Address or name of remote host []? 1.1.1.1
Destination filename [system-report_1_20150909-092728-UTC.gz]?

```

スタックの全メンバーからのトレースログは、`trace archive` コマンドを発行することで収集できます。このコマンドには、時間帯オプションがあります。コマンド構文は次のとおりです。

```

Device# request platform software trace archive ?
last      Archive trace files of last x days
target    Location and name for the archive file

```

`crashinfo`: または `flash`: ディレクトリに格納されている過去 3650 日以内のトレースログが取得できます。

```

Device# request platform software trace archive last ?
<1-3650> Number of days (1-3650)
Device# request platform software trace archive last 3650 days target ?
crashinfo: Archive file name and location
flash:     Archive file name and location

```



- (注) 一度コピーされたら、システムレポートやトレースのアーカイブを `flash` ディレクトリまたは `crashinfo` ディレクトリからクリアし、トレースログやその他の目的に使用できる領域を確保することが重要です。

複雑なネットワークでは、システムレポートファイルの送信元を追跡することは困難です。システムレポートファイルが一意に識別できる場合、この作業は簡単になります。Cisco IOS XE Amsterdam 17.3.x リリース以降、システムレポートファイル名の前にホスト名が追加され、レポートが一意に識別できるようになります。

次の例では、ホスト名が先頭に追加されたシステムレポートファイルを表示します。

```

HOSTNAME# dir flash:/core | grep HOSTNAME
40486 -rw-          108268293  Oct 21 2019 16:07:50 -04:00
HOSTNAME-system-report_20191021-200748-UTC.tar.gz
40487 -rw-           17523    Oct 21 2019 16:07:56 -04:00
HOSTNAME-system-report_20191021-200748-UTC-info.txt
40484 -rw-          48360998  Oct 21 2019 16:55:24 -04:00
HOSTNAME-system-report_20191021-205523-UTC.tar.gz
40488 -rw-           14073    Oct 21 2019 16:55:26 -04:00
HOSTNAME-system-report_20191021-205523-UTC-info.txt

```

スイッチのオンボード障害ロギング

オンボード障害ロギング (OBFL) 機能を使用すれば、デバイスに関する情報を収集できます。この情報には稼働時間、温度、電圧などの情報が含まれており、シスコのテクニカルサポート担当者がデバイスの問題をトラブルシューティングする際に役立ちます。OBFL はイネーブルにしておき、フラッシュメモリに保存されたデータは消さないようにすることを推奨します。

OBFL は、デフォルトでイネーブルになっています。デバイスおよび Small Form-Factor Pluggable (SFP) モジュールに関する情報が収集されます。デバイスは、次の情報をフラッシュメモリに保存します。

- CLI コマンド：スタンドアロンデバイスまたはスイッチスタックメンバに入力された OBFL CLI コマンドの記録。
- 環境データ：スタンドアロンデバイスまたはスイッチスタックメンバおよび接続されているすべての FRU デバイスの一意のデバイス ID (UDI) 情報、製品 ID (PID)、バージョン ID (VID)、およびシリアル番号。
- メッセージ：スタンドアロンデバイスまたはスイッチスタックメンバにより生成されたハードウェア関連のシステムメッセージの記録。
- Power over Ethernet (PoE)：スタンドアロンデバイスまたはスイッチスタックメンバの PoE ポートの消費電力の記録。
- 温度：スタンドアロンデバイスまたはスイッチスタックメンバの温度。
- 稼働時間：スタンドアロンデバイスまたはスイッチスタックメンバが起動された際の時刻、デバイスが再起動された理由、およびデバイスが最後に再起動されて以来の稼働時間。
- 電圧：スタンドアロンデバイス またはスイッチスタックメンバのシステム電圧。

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

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

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

ファン障害

デフォルトでは、この機能はディセーブルです。現場交換可能ユニット (FRU) または電源装置の複数のファンが故障した場合、デバイスはシャットダウンせず、次のようなエラーメッセージが表示されます。

```
Multiple fan(FRU/PS) failure detected. System may get overheated. Change fan quickly.
```

デバイスが過熱状態となり、シャットダウンすることもあります。

ファン障害機能をイネーブルにするには、**system env fan-fail-action shut** 特権 EXEC コマンドを入力します。デバイス内の複数のファンに障害が発生した場合、デバイスは自動的にシャットダウンし、次のようなエラーメッセージが表示されます。

```
Faulty (FRU/PS) fans detected, shutting down system!
```

最初のファンの停止後、デバイスが2つ目のファンの障害を検知すると、デバイスは20秒待機してからシャットダウンします。

デバイスを再起動するには、電源をオフにしてから再度オンにする必要があります。

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現象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。次にその一部を示します。

- 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

ソフトウェア設定のトラブルシューティング方法

ソフトウェア障害からの回復

始める前に

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。

ここで紹介する手順では、破損したイメージファイルまたは不適切なイメージファイルの回復に **boot loader** コマンドおよび TFTP を使用します。

スイッチのコンソールポートのデフォルトレートである 9600 ビット/秒 (bps) と一致するように、端末のボーレートを設定します。ボーレートが 9600 bps 以外の値に設定されている場合、速度がデフォルトに戻るまでコンソールへのアクセスは失われます。

手順

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

ステップ2 TFTP サーバーにソフトウェア イメージをロードします。

ステップ3 PC をスイッチのイーサネット管理ポートに接続します。

ステップ4 スwitchの電源コードを取り外します。

ステップ5 [Mode] 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。

ステップ6 ブートローダープロンプトで、TFTP サーバーに ping を実行できることを確認します。

a) スwitchの IP アドレスを設定します：**set IP_ADDRESS ip_address**

例：

```
switch: set IP_ADDRESS 192.0.2.123
```

b) スwitchのサブネットマスクを設定します：**set IP_SUBNET_MASK subnet_mask**

例：

```
switch: set IP_SUBNET_MASK 255.255.255.0
```

c) デフォルトゲートウェイを設定します：**set DEFAULT_GATEWAY ip_address**

例：

```
switch: set DEFAULT_ROUTER 192.0.2.1
```

d) 次のコマンドを実行して、TFTP サーバーに ping を実行できることを確認します。**switch: ping ip_address_of_TFTP_server**

例：

```
switch: ping 192.0.2.15
ping 192.0.2.1 with 32 bytes of data...
Host 192.0.2.1 is alive.
switch:
```

ステップ7 次のいずれかを選択します。

- ブートローダープロンプトで、**boot tftp** コマンドを開始します。これにより、スイッチでソフトウェアイメージを容易に回復できます。

```
switch: boot tftp://10.168.0.1/cat9k/cat9k_iosxe.2017-08-25_09.41.bin
attempting to boot from [tftp://10.168.0.1/cat9k/cat9k_iosxe.2017-08-25_09.41.SSA.bin]
```

```
interface : eth0
macaddr   : E4:AA:5D:59:7B:44
ip        : 10.168.247.10
netmask   : 10.255.0.0
gateway   : 10.168.0.1
server    : 10.168.0.1
file      : cat9k/cat9k_iosxe.2017-08-25_09.41.bin
```

Restricted Rights Legend

Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c) of the Commercial Computer Software - Restricted Rights clause at FAR sec. 52.227-19 and subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS sec. 252.227-7013.

cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706

Cisco IOS Software [Everest], Catalyst L3 Switch Software (CAT9K_IOSXE), Version 16.6.1 RELEASE SOFTWARE (fc2)
Copyright (c) 1986-2017 by Cisco Systems, Inc.
Compiled Thu 24-Aug-17 13:23 by mcpre

Cisco IOS-XE software, Copyright (c) 2005-2017 by cisco Systems, Inc. All rights reserved. Certain components of Cisco IOS-XE software are licensed under the GNU General Public License ("GPL") Version 2.0. The software code licensed under GPL Version 2.0 is free software that comes with ABSOLUTELY NO WARRANTY. You can redistribute and/or modify such GPL code under the terms of GPL Version 2.0. For more details, see the documentation or "License Notice" file accompanying the IOS-XE software, or the applicable URL provided on the flyer accompanying the IOS-XE software.

FIPS: Flash Key Check : Begin
FIPS: Flash Key Check : End, Not Found, FIPS Mode Not Enabled

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
<http://www.cisco.com/wwl/export/crypto/tool/stqrg.html>

If you require further assistance please contact us by sending email to export@cisco.com.

cisco C9XXX (X86) processor (revision V00) with 869398K/6147K bytes of memory.
Processor board ID FXS1939Q3LZ
144 Gigabit Ethernet interfaces
16 Ten Gigabit Ethernet interfaces
4 Forty Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
15958516K bytes of physical memory.

```
11161600K bytes of Bootflash at bootflash:.
1638400K bytes of Crash Files at crashinfo:.
0K bytes of WebUI ODM Files at webui:.
```

```
%INIT: waited 0 seconds for NVRAM to be available
```

```
Press RETURN to get started!
```

- リカバリパーティションからソフトウェアをインストールします。この回復イメージは、**emergency-install** 機能を使用して回復を実施する場合に必要となります。

- a) 回復パーティション (sda9:) に回復イメージが存在することを確認します。

例 :

```
switch: dir sda9:

Size            Attributes      Name
-----
21680202       -rw-           cat9k-recovery.SSA.bin
-----
```

- b) ブートローダープロンプトで、**emergency-install** 機能を開始します。この機能を使用すると、スイッチでソフトウェアイメージを容易に回復できます。**警告** : **emergency-install** コマンドを実行すると、ブートブラッシュ全体が消去されます。

例 :

```
switch: emergency-install
tftp://10.255.254.254/auto/tftpboot/X86/cat9k_iosxe.16.05.01a.SPA.bin
WARNING: The system partition (bootflash:) will be erased during the system recovery
install process.
Are you sure you want to proceed? [y] y/n [n]: y
Starting system recovery
(tftp://10.255.254.254/auto/tftpboot/X86/cat9k_iosxe.16.05.01a.SPA.bin) ...
Attempting to boot from [sda9:cat9k-recovery.SSA.bin]
Located cat9k-recovery.SSA.bin
#####

Warning: ignoring ROMMON var "BOOT_PARAM"

PLATFORM_TYPE C9X00 speed 9600

Booting Recovery Image 16.5.1a

Initiating Emergency Installation of bundle
tftp://10.255.254.254/auto/tftpboot/X86/cat9k_iosxe.16.05.01a.SPA.bin

Downloading bundle
tftp://10.255.254.254/auto/tftpboot/X86/cat9k_iosxe.16.05.01a.SPA.bin...
curl_vrf=2
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left   Speed
100 485M  100 485M    0     0  5143k      0  0:01:36  0:01:36 ---:---: 5256k
100 485M  100 485M    0     0  5143k      0  0:01:36  0:01:36 ---:---: 5143k
```

```
Validating bundle
tftp://10.255.254.254/auto/tftpbboot/X86/cat9k_iosxe.16.05.01a.SPA.bin...
Installing bundle
tftp://10.255.254.254/auto/tftpbboot/X86/cat9k_iosxe.16.05.01a.SPA.bin...
Verifying bundle
tftp://10.255.254.254/auto/tftpbboot/X86/cat9k_iosxe.16.05.01a.SPA.bin...
Package cat9k-cc_srdriver.16.05.01a.SPA.pkg
/temp//stage/cat9k-cc_srdriver.16.05.01a.SPA.pkg is Digitally Signed
Package cat9k-espbase.16.05.01a.SPA.pkg /temp//stage/cat9k-espbase.16.05.01a.SPA.pkg
is Digitally Signed
Package cat9k-guestshell.16.05.01a.SPA.pkg
/temp//stage/cat9k-guestshell.16.05.01a.SPA.pkg is Digitally Signed
Package cat9k-rpbase.16.05.01a.SPA.pkg /temp//stage/cat9k-rpbase.16.05.01a.SPA.pkg
is Digitally Signed
Package cat9k-sipbase.16.05.01a.SPA.pkg /temp//stage/cat9k-sipbase.16.05.01a.SPA.pkg
is Digitally Signed
Package cat9k-sipspa.16.05.01a.SPA.pkg /temp//stage/cat9k-sipspa.16.05.01a.SPA.pkg
is Digitally Signed
Package cat9k-srdriver.16.05.01a.SPA.pkg /temp//stage/cat9k-srdriver.16.05.01a.SPA.pkg
is Digitally Signed
Package cat9k-webui.16.05.01a.SPA.pkg /temp//stage/cat9k-webui.16.05.01a.SPA.pkg is
Digitally Signed
Package cat9k-wlc.16.05.01a.SPA.pkg /temp//stage/cat9k-wlc.16.05.01a.SPA.pkg is
Digitally Signed
Package /cat9k-rpboot.16.05.01a.SPA.pkg /temp//rpboot/cat9k-rpboot.16.05.01a.SPA.pkg
is Digitally Signed
Preparing flash....
Flash filesystem unmounted successfully /dev/sdb3
Syncing device....
Emergency Install successful... Rebooting
Will reboot now

Initializing Hardware...

System Bootstrap, Version 16.5.2r, RELEASE SOFTWARE (P)
Compiled Wed 05/31/2017 15:58:35.22 by rel

Current image running:
Primary Rommon Image

Last reset cause: SoftwareReload
C9X00 platform with 8388608 Kbytes of main memory
```

あるいは、Telnetまたは管理ポートを通じてTFTPからローカルフラッシュにイメージをコピーした後、ローカルフラッシュからデバイスをブートします。

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、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。

手順

ステップ 1 端末または PC をスイッチに接続します。

- 端末または端末エミュレーションソフトウェアが稼働している PC をスイッチのコンソールポートに接続します。スイッチスタックのパスワードを回復する場合は、アクティブスイッチのコンソールポートに接続します。
- PC をイーサネット管理ポートに接続します。スイッチスタックのパスワードを回復する場合は、スタックメンバのイーサネット管理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 スタンドアロンスイッチまたはスイッチスタック全体の電源を切断します。

ステップ 4 スイッチまたはアクティブスイッチに電源コードを再接続します。システム LED が点滅したら、すぐに [Mode] ボタンを 2〜3 回押して放します。スイッチは ROMMON モードを開始します。

リロード中に次のコンソールメッセージが表示されます。

```
Initializing Hardware...
```

```
System Bootstrap, Version 16.6.1r [FC1], RELEASE SOFTWARE (P)
Compiled Sat 07/15/2017 8:31:57.39 by rel
```

```
Current image running:
Primary Rommon Image
```

```
Last reset cause: SoftwareReload <---- Start pressing and releasing the mode
button
C9300-24U platform with 8388608 Kbytes of main memory
```

```
attempting to boot from [flash:packages.conf]
```

```
Located file packages.conf
```

```
#
```

```
#####
```

```
Unable to load cat9k-rpboot.16.06.02b.SPA.pkg
Failed to boot file flash:user/packages.conf
ERROR: failed to boot from flash:packages.conf (Aborted) <--- will abort
switch:
switch: <---- ROMMON
```

「パスワード回復がイネーブルになっている場合の手順」セクションに記載されている手順を実行します。

ステップ5 パスワードの回復後、スイッチまたはアクティブスイッチをリロードします。

スイッチの場合

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

アクティブ スイッチの場合

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

ステップ6 スタック内の残りのスイッチに電源を投入します。

パスワード回復がイネーブルになっている場合の手順

手順

ステップ1 次のコマンドを使用して、スタートアップ コンフィギュレーションを無視します。

```
Device: SWITCH_IGNORE_STARTUP_CFG=1
```

ステップ2 `packages.conf` ファイルでスイッチをフラッシュからブートします。

```
Device: boot flash:packages.conf
```

ステップ3 **No** と応答して初期設定ダイアログを終了します。

```
Would you like to enter the initial configuration dialog? [yes/no]: No
```

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。

```
Device> enable  
Device#
```

ステップ5 スタートアップ コンフィギュレーションを実行コンフィギュレーションにコピーします。

```
Device# copy startup-config running-config 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6 グローバルコンフィギュレーションモードを開始して、イネーブルパスワードを変更します。

```
Device# configure terminal
```

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

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

ステップ7 特権 EXEC モードに戻ります。

```
Device(config)# exit
Device#
```

ステップ8 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。

```
Device# copy running-config startup-config
```

ステップ9 手動ブート モードがイネーブルになっていることを確認します。

```
Device# show boot

BOOT variable = flash:packages.conf;
Manual Boot = yes
Enable Break = yes
```

ステップ10 デバイスのリロード。

```
Device# reload
```

ステップ11 SWITCH_IGNORE_STARTUP_CFG パラメータを 0 に設定します。

```
Device(config)# no system ignore startupconfig switch all
Device(config)# end
Device# write memory
```

ステップ12 フラッシュの *packages.conf* ファイルを使用して、デバイスを起動します。

```
Device: boot flash:packages.conf
```

ステップ13 デバイスが起動したら、デバイスで手動ブートを無効にします。

```
Device(config)# no boot manual
```

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

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

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

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

手順

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 フラッシュメモリの内容を表示します。

```
Device: dir flash:
```

デバイスのファイルシステムが表示されます。

```
Directory of flash:/
.
.
.i'
15494 drwx      4096   Jan 1 2000 00:20:20 +00:00 kirch
15508 -rw-    258065648   Sep 4 2013 14:19:03 +00:00
cat9k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin
162196684
```

ステップ 3 システムを起動します。

```
Device: 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4 デバイスプロンプトで、特権 EXEC モードを開始します。

```
Device> enable
```

ステップ5 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。

```
Device# configure terminal
```

ステップ6 パスワードを変更します。

```
Device(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7 特権 EXEC モードに戻ります。

```
Device(config)# exit  
Device#
```

ステップ8 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。

```
Device# 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。

ステップ9 ここで、デバイスを再設定する必要があります。システム管理者によって、バックアップデバイスと 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。

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）に関するデバイス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。

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

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



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

SFP モジュールのセキュリティと識別に関するトラブルシューティング

シスコの Small Form-Factor Pluggable (SFP) モジュールは、モジュールのシリアル番号、ベンダー名とベンダー ID、一意のセキュリティコード、および巡回冗長検査 (CRC) が格納されたシリアル EEPROM (電氣的に消去可能でプログラミング可能な ROM) を備えています。デバイスに SFP モジュールを装着すると、デバイスソフトウェアは、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。

他社の SFP モジュールを使用している場合、デバイスから 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のステータスを確認し、**error-disabled** 状態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、デバイスは **error-disabled** 状態からインターフェイスを回復させ、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 の実行

別の IP サブネットワーク内のホストに ping を実行する場合は、ネットワークへのスタティックルートを定義するか、またはこれらのサブネットワーク間でルーティングされるように IP ルーティングを設定する必要があります。

IP ルーティングは、デフォルトではすべてのデバイスでディセーブルになります。



(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。

このコマンドは、デバイスからネットワーク上の他のデバイスに ping を実行する目的で使用します。

コマンド	目的
ping ip host address Device# ping 172.20.52.3	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に ping を実行します。

温度のモニタリング

デバイスは温度条件をモニターし、温度情報を使用してファンを制御します。

温度の値、状態、しきい値を表示するには、**show env temperature status** 特権 EXEC コマンドを使用します。温度の値は、デバイス内の温度であり、外部の温度ではありません。**system env temperature threshold yellow value** グローバル コンフィギュレーション コマンドを使用してイエローのしきい値レベル（摂氏）だけを設定し、イエローのしきい値およびレッドのしきい値の差を設定できます。グリーンまたはレッドのしきい値は設定できません。詳細については、このリリースのコマンドリファレンスを参照してください。

物理パスのモニタリング

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モニタできます。

表 1: 物理パスのモニタリング

コマンド	目的
tracetroute mac [interface <i>interface-id</i>] { <i>source-mac-address</i> } [interface <i>interface-id</i>] { <i>destination-mac-address</i> } [vlan <i>vlan-id</i>] [detail]	指定の送信元 MAC アドレスから、指定の宛先 MAC アドレスまでをパケットが通過するレイヤ 2 パスを表示します。
tracetroute mac ip { <i>source-ip-address</i> <i>source-hostname</i> } { <i>destination-ip-address</i> <i>destination-hostname</i> } [detail]	指定の送信元 IP アドレスまたはホスト名から、指定の宛先 IP アドレスまたはホスト名を通過するパケットのレイヤ 2 パスを表示します。

IP traceroute の実行



- (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。

コマンド	目的
traceroute ip <i>host</i> Device# <code>traceroute ip 192.51.100.1</code>	ネットワーク上でパケットが通過するパスを追跡します。

TDR の実行および結果の表示

TDR は、インターフェイス上で実行する場合、アクティブスイッチ上でもスタックメンバ上でも実行できます。

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

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。

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が **debug** コマンドからの出力とシステムエラーメッセージをコンソールに送信します。このデフォルトの設定を使用する場合は、コンソールポートま

たはイーサネット管理ポートに接続する代わりに、仮想端末接続によってデバッグ出力をモニターできます。

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。メッセージをコンソールに記録すると、非常に高いオーバーヘッドが発生します。仮想端末にメッセージを記録すると、発生するオーバーヘッドは低くなります。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 メッセージのロギングに関する詳細については、「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着信するパケットがシステムを介して送信された場合の転送結果に関する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。

このコマンドで出力される情報のほとんどは、主に、デバイス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。

show debug コマンドの使用方法

show debug コマンドは特権 EXEC モードで入力します。このコマンドは、スイッチで使用可能なすべてのデバッグ オプションを表示します。

すべての条件付きデバッグオプションを表示するには、コマンド **show debug condition** を実行します。コマンドは、条件 ID <1-1000> または *all* 条件を選択することで一覧表示できます。

デバッグを無効にするには、**no debug all** コマンドを使用します。



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。さらに、**debug** コマンドは、ネットワークトラフィックが少なく、ユーザも少ないときに使用することを推奨します。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低くなります。

OBFL の設定



注意 OBFLはディセーブルにせず、フラッシュメモリに保存されたデータは削除しないことを推奨します。

ソフトウェア設定のトラブルシューティングの確認

OBFL 情報の表示

表 2: OBFL 情報を表示するためのコマンド

コマンド	目的
show onboard switch <i>switch-number</i> cliilog Device# show onboard switch 1 cliilog	スタンドアロンスイッチまたは指定されたスタックメンバで入力された OBFL CLI コマンドを表示します。
show onboard switch <i>switch-number</i> environment Device# show onboard switch 1 environment	スタンドアロンスイッチまたは指定されたスタックメンバおよび接続されているすべての FRU デバイスの UDI 情報、PID、VID、およびシリアル番号を表示します。
show onboard switch <i>switch-number</i> message Device# show onboard switch 1 message	スタンドアロンスイッチまたは指定されたスタックメンバによって生成されたハードウェア関連のメッセージを表示します。
show onboard switch <i>switch-number</i> counter Device# show onboard switch 1 counter	スタンドアロンスイッチまたは指定したスタックメンバのカウンタ情報を表示します。
show onboard switch <i>switch-number</i> temperature Device# show onboard switch 1 temperature	スタンドアロンスイッチまたは指定されたスイッチスタックメンバの温度を表示します。

コマンド	目的
show onboard switch <i>switch-number</i> uptime Device# show onboard switch 1 uptime	スタンドアロンスイッチまたは指定されたスタックメンバが起動した時刻、スタンドアロンスイッチまたは指定されたスタックメンバが再起動された理由、およびスタンドアロンスイッチまたは指定されたスタックメンバが最後に再起動されて以来の稼働時間を表示します。
show onboard switch <i>switch-number</i> voltage Device# show onboard switch 1 voltage	スタンドアロンスイッチまたは指定されたスタックメンバのシステム電圧を表示します。
show onboard switch <i>switch-number</i> status Device# show onboard switch 1 status	スタンドアロンスイッチまたは指定されたスタックメンバの状態を表示します。

例：高い CPU 使用率に関する問題と原因の確認

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。

```

Device# 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 3: CPU 使用率に関する問題のトラブルシューティング

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

ソフトウェア設定のトラブルシューティングのシナリオ

Power over Ethernet (PoE) に関するトラブルシューティングのシナリオ

表 4: Power over Ethernet 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>PoE がないポートは1つに限りません。</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>	

症状または問題	考えられる原因と解決法
	<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>show run または show interface status ユーザ 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か、または error-disabled になっていないかを確認します。</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>該当するインターフェイスまたはポートに power inline never が設定されていないことを確認します。</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>(注) シスコ受電装置は、ストレートケーブルでのみ機能します。クロスオーバーケーブルでは機能しません。</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電力バジェット（使用可能な PoE）とを比較してください。show power inline コマンドを使用して、利用可能な電力量を確認します。</p>

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>	

症状または問題	考えられる原因と解決法
	<p>電力に関するアラームが継続的に発生する、断続的に発生する、または再発する場合は、可能であれば電源モジュールを交換します（現場交換可能ユニットです）。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、show log 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、show interface status 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、または error-disabled になっていないかを確認します。ポートが error-disabled の場合、shut および no shut 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、ポートを再度有効にします。</p> <p>show env power および show power inline 特権 EXEC コマンドを使用して、PoE のステータスおよび電力バジェット（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、power inline never 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。shut および no shut 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>show power inline 特権 EXEC コマンドを使用して、ポートがシャットダウンされていない場合に、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</p>

症状または問題	考えられる原因と解決法
	<p>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際に電力が供給される場合、残りのポートで shut および no shut 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 本ずつ再接続してください。 show interface status および show power inline 特権 EXEC コマンドを使用して、インラインパワーの統計情報とポートの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>シスコ先行標準受電装置は、切断またはリセットされます。</p> <p>正常に動作した後で、シスコ電話機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。 show log 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ない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>

症状または問題	考えられる原因と解決法
<p>IEEE 802.3af 準拠または IEEE 802.3at 準拠の受電装置は、Cisco PoE スイッチでは機能しません。</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>show power inline コマンドを使用して、受電デバイスの接続前後に、スイッチの電力バジェット（使用可能な PoE）が枯渇していないか確認します。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>show interface status コマンドを使用して、接続されている受電デバイスがスイッチに検出されることを確認します。</p> <p>show log 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>

ソフトウェアのトラブルシューティングの設定例

例：IP ホストの ping

次に、IP ホストに ping を実行する例を示します。

```
Device# 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
Device#
```

表 5: ping の出力表示文字

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

例：IP ホストに対する **traceroute** の実行

文字	Description
?	パケット タイプが不明です。
&	パケットの存続時間を超過したことを示します。

pingセッションを終了するには、エスケープシーケンス（デフォルトではCtrl+^X）を入力してください。Ctrl キー、Shift キー、および6 キーを同時に押してから放し、その後 X キーを押します。

例：IP ホストに対する **traceroute** の実行

次に、IP ホストに **traceroute** を実行する例を示します。

```
Device# traceroute ip 192.0.2.10

Type escape sequence to abort.
Tracing the route to 192.0.2.10

 0 192.0.2.1 0 msec 0 msec 4 msec
 1 192.0.2.203 12 msec 8 msec 0 msec
 2 192.0.2.100 4 msec 0 msec 0 msec
 3 192.0.2.10 0 msec 4 msec 0 msec
```

ディスプレイには、送信される3つのプローブごとに、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 6: **traceroute** の出力表示文字

文字	Description
*	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。

ソフトウェア設定のトラブルシューティングに関する追加情報

関連資料

関連項目	マニュアルタイトル
この章で使用するコマンドの完全な構文および使用方法の詳細。	<i>Command Reference (Catalyst 9300 Series Switches)</i>

ソフトウェア設定のトラブルシューティングの機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Everest 16.5.1a	ソフトウェア設定のトラブルシューティング	ソフトウェア設定のトラブルシューティングでは、スイッチが稼働する Cisco IOS ソフトウェアに関連する問題を特定し、解決する方法について説明します。
Cisco IOS XE Amsterdam 17.3.1	システムレポートファイル	ホスト名がシステムレポートファイルの先頭に追加されます。これにより、システムレポートファイルが一意に識別可能になります。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> [英語] からアクセスします。

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。