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 インストレーション ガイドを参照してください。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

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。

関連トピック

ソフトウェア障害からの回復，（11 ページ）

のパスワードを紛失したか忘れた場合 スイッチ

スイッチのデフォルト設定では、スイッチに物理的にアクセスしているエンドエンド ユーザは、スイッチの電源投入中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、スイッチに物理的にアクセスする必要があります。

（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ことに同意した場合に限り、エンド ユーザによるパスワードのリセットを許可することによって、この機能の一部をディセーブルにできます。パスワード回復がディセーブルになっている場合に、エンド ユーザがパスワードをリセットしようとすると、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）。

関連トピック

パスワードを忘れた場合の回復，（13 ページ）

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 および 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。受電装置が PoE ポートにだけ接続されている場合、受電装置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、『』（Catalyst 9300 スイッチ）の「Configuring PoE」の章を参照してください *Interface and Hardware Component Configuration Guide*（*Catalyst 3850 Switches*） *Interface Configuration Guide*（*Cisco WLC 5700 Series*）。

関連トピック

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）

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。error-disabled 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、error-disabled ステートから回復することもできます。

スイッチの場合、**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 error-disabled 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 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。

ping

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。

関連トピック

ping の実行, （21 ページ）
例：IP ホストの ping, （33 ページ）

レイヤ 2 Traceroute

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。transroute は、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。スイッチがパス内でレイヤ 2 traceroute をサポートしていないデバイスを検知した場合、スイッチはレイヤ 2 trace クエリーを送信し続け、タイムアウトにします。

スイッチは、送信元デバイスから宛先デバイスへのパスのみを識別できます。パケットが通過する、送信元ホストから送信元デバイスまで、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 をディセーブルにしないでください。

  物理パス内のデバイスが CDP に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、このスイッチは別のスイッチから到達可能といえます。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の間の物理パス内にないスイッチで、**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。

- **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の IP アドレスが同一サブネットに属する場合、**traceroute mac ip** コマンド出力にレイヤ2パスが表示されます。IPアドレスを指定した場合、スイッチは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 を関連付けます。
  - 指定の IP アドレスに ARP のエントリが存在している場合、スイッチは関連する MAC アドレスを使用して、物理パスを識別します。
  - ARP のエントリが存在しない場合、スイッチは ARP クエリを送信し、IP アドレスの解決を試みます。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。

IP Traceroute

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、特定のパケットをルーティングするマルチレイヤ スイッチの場合、中間スイッチは traceroute の出力にホップとして表示されます。

traceroute 特権 EXEC コマンドは、IP ヘッダーの存続可能時間（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 番めのルータは、TTL フィールドの値から 1 を差し引いて次のルータにデータグラムを送信します。2 番めのルータは、TTL 値が 1 であることを確認すると、このデータグラムを廃棄し、time-to-live-exceeded メッセージを送信元へ返します。このように、データグラムが宛先ホストに到達するまで（または TTL の最大値に達するまで）TTL の値は増分され、処理が続けられます。

データグラムが宛先に到達したことを学習するために、traceroute は、データグラムの UDP 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ことは、このメッセージが宛先ポートから送信されたことを意味します。

関連トピック

IP traceroute の実行，（22 ページ）

例：IP ホストに対する traceroute の実行，（34 ページ）

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 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 ギガビット イーサネット ポートまたは SFP モジュール ポートではサポートされません。

TDR は、10/100/1000 銅線イーサネット ポートと、マルチギガビット イーサネット（100Mbps/1/2.5/5/10 Gbps）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 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。

（注） マルチギガビット イーサネット ポートでこの機能を使用する場合は、オープン条件またはショート条件が検出された場合にのみケーブル長が表示されます。

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 の実行時、次の場合にスイッチ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、次の場合にスイッチ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

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。デバッギン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。

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。

関連トピック

デバッグおよびエラー メッセージ出力のリダイレクト，（23 ページ）

例：すべてのシステム診断をイネーブルにする，（35 ページ）

crashinfo ファイル

crashinfo ファイルには、シスコのテクニカル サポート担当者が 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 2 個のファイル（fullcore および crashinfo）を生成します。

この crashinfo 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、およびスタック トレースです。この情報は、**show tech-support** 特権 EXEC コマンドを使用することによって、シスコのテクニカル サポート担当者に提出できます。

ファイル名は次の形式になります。

```
 [fullcore | crashinfo]_[process that crashed]_[date]-[timestamp]-UTC
```

IOS から、次のコマンドを使用して各スイッチ上の crashinfo ファイルを表示できます。

```
Switch

dir crashinfo?Switch#
crashinfo-1: crashinfo-2: crashinfo-3: crashinfo:
#
```

たとえば、スイッチ 1 の crashinfo ディレクトリにアクセスするには、以下のように入力します。

```
Switch dir crashinfo-1
```

ROMMON プロンプトで、**dir** コマンドを使用して crashinfo ファイルを確認できます。

```
Switch: dir sda1
```

次は crashinfo ファイルの出力例を示します。

```
Switch# dir crashinfo:

Directory of crashinfo:/

   12  -rwx        2768  Dec 31 1969 16:00:15 -08:00  koops.dat
   15  -rwx           0  Jan 12 2000 22:53:40 -08:00  deleted_crash_files
   16  -rwx     4246576  Jan 12 2000 22:53:40 -08:00  crashinfo_stack-mgr_20000113-065250-UTC

   17  -rwx          50   Oct 2 2012 03:18:42 -08:00  last_crashinfo
   26  -rwx          39  Jan 22 2013 14:14:14 -08:00  last_systemreport
   18  -rwx     2866565  Jan 12 2000 22:53:41 -08:00  fullcore_stack-mgr_20000113-065250-UTC

   20  -rwx     4391796   Feb 1 2000 17:50:44 -08:00  crashinfo_stack-mgr_20000202-014954-UTC

   21  -rwx     2920325   Feb 1 2000 17:50:45 -08:00  fullcore_stack-mgr_20000202-014954-UTC
34817  -rw-     1050209  Jan 10 2013 20:26:23 -08:00  system-report_1_20130111-042535-UTC.gz
18434  -rw-     1016913  Jan 11 2013 10:35:28 -08:00  system-report_1_20130111-183440-UTC.gz
18435  -rw-     1136167  Jan 22 2013 14:14:11 -08:00  system-report_1_20130122-221322-UTC.gz
34821  -rw-     1094631   Jan 2 2013 17:59:23 -08:00  system-report_1_20130103-015835-UTC.gz

 6147  -rw-      967429   Jan 3 2013 10:32:44 -08:00  system-report_1_20130103-183156-UTC.gz
34824  -rwx          50  Jan 22 2013 14:14:14 -08:00  deleted_sysreport_files
6155  -rwx         373  Jan 22 2013 14:14:13 -08:00  last_systemreport_log

145898496 bytes total (18569216 bytes free)
stack3#

The file name of the most recent crashinfo file is stored in last_crashinfo.
The file name of the most recent system report is stored in last_systemreport.
```

```
Switch#
```

システム レポート

スイッチのクラッシュが発生すると、スイッチ スタックの各スイッチについて、システム レポートが自動的に生成されます。システム レポート ファイルは、すべてのトレース バッファ、およびスイッチ上にあるその他のシステム全体のログをキャプチャします。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
```

スイッチのクラッシュの後には、システム レポート ファイルが生成されているかどうか確認する必要があります。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場合には、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。

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、スイッチ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 サポート担当者がスイッチ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。スイッチおよび Small Form-Factor Pluggable（SFP）モジュールに関する情報が収集されます。スイッチは、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 スイッチまたはスイッチ 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 スイッチまたはスタック 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 スイッチまたはスタック 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
- イーサネット経由の電源供給（PoE）：スタンドアロン スイッチまたはスイッチ 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 スイッチまたはスタック メンバの温度
- 稼働時間：スタンドアロン スイッチまたはスタック メンバが起動されたときの時刻、スイッチが再起動された理由、およびスイッチ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 スイッチまたはスタック 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。

スイッチの稼働中には、**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。スイッチ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スイッチ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。

関連トピック

OBFL の設定，（24 ページ）
OBFL 情報の表示，（25 ページ）

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、スイッチ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.
```

スイッチが過熱状態となり、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。スイッチ内の複数のファンに障害が発生した場合、スイッチ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、スイッチが 2 つめのファンの障害を検知すると、スイッチは 20 秒待機してからシャットダウンします。

スイッチを再起動するには、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症状が発生する可能性がありますが、他の原因で発生する場合もあります。

（注） Cisco Catalyst 4500E Supervisor Engine 8-E をワイヤレス モードで使用すると、システムのメモリ使用率が上がることがあります。

- 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

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

はじめる前に

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 スイッチの電源コードを取り外します。

ステップ 5 [Mode]**Mode**ボタンを押しながら、電源コードを再度スイッチに接続します。

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

a) 次のコマンドを実行して、IP アドレス を設定します。**switch: set IP_ADDRESS** *ip_address subnet_mask*

例：
```
switch: set IP_ADDRESS 192.0.2.123/255.255.255.0
```

b) 次のコマンドを実行して、デフォルト ルータ IP アドレスを設定します。**switch: set DEFAULT_ROUTER** *ip_address*

例：
```
switch: set DEFAULT_ROUTER 192.0.2.1
```

c) 次のコマンドを実行して、TFTP サーバに 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 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。
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。

例：

```
switch: dir sda9:
Directory of sda9:/

    2  drwx  1024       .
    2  drwx  1024       ..
   11  -rw-  18923068   c3850-recovery.bin

36939776 bytes available (20830208 bytes used)
switch:
```

ステップ 8 ブートローダ（ROMMON）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://192.0.2.47/cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin

The bootflash will be erased during install operation, continue (y/n)?y
Starting emergency recovery
(tftp://192.0.2.47/cat3k/cat3k_caa-universalk9.SPA.03.02.00.SE.150-1.EX.bin)...
Reading full image into memory......................done
Nova Bundle Image
--------------------------------------
Kernel Address : 0x6042e5cc
Kernel Size : 0x318261/3244641
Initramfs Address : 0x60746830
Initramfs Size : 0xdb0fb9/14356409
Compression Format: .mzip

Bootable image at @ ram:0x6042e5cc
Bootable image segment 0 address range [0x81100000, 0x81b80000] is in range [0x80180000, 0x90000000].
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
File "sda9:c3850-recovery.bin" uncompressed and installed, entry point: 0x811060f0
Loading Linux kernel with entry point 0x811060f0 ...
Bootloader: Done loading app on core_mask: 0xf

### Launching Linux Kernel (flags = 0x5)



Initiating Emergency Installation of bundle
tftp://192.0.2.47/cat3k/cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin


Downloading bundle
tftp://192.0.2.47/cat3k/cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin...
Validating bundle
tftp://192.0.2.47/cat3k/cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin...
Installing bundle
tftp://192.0.2.47/cat3k/cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin...
Verifying bundle
tftp://192.0.2.47/cat3k/cat3k_caa-universalk9.SSA.03.12.02.EZP.150-12.02.EZP.150-12.02.EZP.bin...
Package cat3k_caa-base..pkg is Digitally Signed
Package cat3k_caa-drivers.SPA.03.02.00.SE.pkg is Digitally Signed
```

```
Package cat3k_caa-infra.SPA.03.02.00.SE.pkg is Digitally Signed
Package cat3k_caa-iosd-universalk9.SPA.03.02.00.SE.pkg is Digitally Signed
Package cat3k_caa-platform.SPA.03.02.00.SE.pkg is Digitally Signed
Package cat3k_caa-wcm.SPA.03.02.00.SE.pkg is Digitally Signed
Preparing flash...
Syncing device...
Emergency Install successful... Rebooting
Restarting system.


Booting...(use DDR clock 667 MHz)Initializing and Testing RAM +++@@@@####...++@@++@@++@@++@
```

関連トピック

スイッチのソフトウェア障害, （2 ページ）

パスワードを忘れた場合の回復

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

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

手順の概要

1. 端末または PC をスイッチに接続します。
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。
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。
4. 電源コードまたはアクティブ スイッチを再度接続します。15 秒以内に [**Mode**] ボタンを押します。このときシステム LED はグリーンに点滅しています。**Mode** ボタンを長押しして、プロンプトが表示されたら **Mode** ボタンから手を離します。
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。

手順の詳細

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。
- PC を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 電源コードまたはアクティブ スイッチを再度接続します。15 秒以内に [**Mode**] ボタンを押します。このときシステム LED はグリーンに点滅しています。**Mode** ボタンを長押しして、プロンプトが表示されたら **Mode** ボタンから手を離します。

```
Switch:
Xmodem file system is available.
Base ethernet MAC Address: 20:37:06:4d:e9:80
Verifying bootloader digital signature.


The system has been interrupted prior to loading the operating
system software, console will be reset to 9600 baud rate.
```

「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
```

関連トピック

のパスワードを紛失したか忘れた場合 スイッチ, （2 ページ）

パスワード回復がイネーブルになっている場合の手順

パスワード回復動作がイネーブルになっている場合は、次のメッセージが表示されます。

ステップ 1 フラッシュ ファイル システムを初期化します。

```
Switch: flash_init
```

ステップ 2 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。

```
Switch: SWITCH_IGNORE_STARTUP_CFG=1
```

ステップ 3 *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。

```
Switch: boot flash:packages.conf
```

ステップ 4 **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 5 スイッチ プロンプトで、特権 EXEC モードを開始します。

```
Switch> enable
Switch#
```

ステップ 6 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。

```
Switch# 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 7 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。

```
Switch# configure terminal
Switch(config)#
```

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。

```
Switch(config)# 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。

```
Switch# show boot
```

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

ステップ 10 スイッチをリロードします。

```
Switch# reload
```

ステップ 11 （ステップ 2 と 3 で変更した）ブートローダ パラメータを元の値に戻します。

```
switch: SWITCH_IGNORE_STARTUP_CFG=0
```

ステップ 12 フラッシュからのスイッチ *packages.conf* を起動します。

```
Switch: boot flash:packages.conf
```

ステップ 13 スイッチ のブート後に、スイッチ で手動ブートをディセーブルにします。

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

- **n**（no）を入力すると、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。

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。

```
Switch: dir flash:
```

スイッチのファイル 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
cat3k_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。

```
Switch: boot
```

セットアッププログラムを起動するように求められます。パスワード回復手順を継続するには、プロンプトに **N** を入力します。

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

ステップ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
```

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。

```
Switch# configure terminal
```

ステップ 6 パスワードを変更します。

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

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

ステップ 7 特権 EXEC モードに戻ります。

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

（注） ステップ 9 に進む前に、接続されているすべてのスタック メンバの電源を入れ、それらが完全に初期化されるまで待ちます。

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。

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

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

ステップ 9 ここでスイッチを再設定する必要があります。システム管理者によって、バックアップ スイッチと VLAN コンフィギュレーション ファイルが使用可能に設定されている場合は、これらを使用します。

スイッチ スタック問題の回避

スイッチ スタックの問題を防止するには、次の作業を実行する必要があります。

- スイッチ スタックにスイッチを追加したり、そこから取り外したりする場合には、必ずスイッチの電源を切ってください。スイッチ スタックでの電源関連のあらゆる考慮事項については、ハードウェア インストレーション ガイドの「Switch Installation（スイッチのインストール）」の章を参照してください。
- スタック モード LED が点灯するまで、スタック メンバの **Mode** ボタンを押します。スイッチの最後の 2 つのポート LED がグリーンになります。スイッチ モデルに応じて、最後の 2 つのポートは 10/100/1000 ポートまたは Small Form-Factor Pluggable モジュールになります。最後の 2 つのポート LED の片方または両方がグリーンになっていない場合は、スタックが全帯域幅で稼働していません。
- スイッチ スタックを管理する場合は、1 つの CLI セッションだけを使用することを推奨します。アクティブ スイッチに複数の CLI セッションを使用する場合は注意が必要です。1 つのセッションで入力したコマンドは、別のセッションには表示されません。そのため、コマンドを入力したセッションを識別できなくなることがあります。
- スタック内での位置に従ってスタック メンバ番号を手動で割り当てると、リモートから行うスイッチ スタックのトラブルシューティングが容易になります。ただし、後からスイッチを追加したり、取り外したり、場所を入れ替えたりする際に、スイッチに手動で番号を割り当てたことを覚えておく必要があります。スタック メンバー番号を手動で割り当てるには、

switch *current-stack-member-number***renumber** *new-stack-member-number* グローバル コンフィギュレーション コマンドを使用します。

スタック メンバをまったく同じモデルで置き換えると、新しいスイッチは、置き換えられたスイッチとまったく同じ設定で稼働します。この場合、新しいスイッチは置き換えられたスイッチと同じメンバ番号を使用するものと想定されます。

電源が入った状態のスタック メンバを取り外すと、スイッチ スタックが、それぞれ同じ設定を持つ2つ以上のスイッチ スタックに分割（パーティション化）されます。スイッチ スタックを分離されたままにしておきたい場合は、新しく作成されたスイッチ スタックのIPアドレス（複数の場合あり）を変更してください。パーティション化されたスイッチ スタックを元に戻すには、次の手順を実行します。

1. 新しく作成されたスイッチ スタックの電源を切ります。
2. 新しいスイッチ スタックを、StackWise Plus ポートを介して元のスイッチ スタックに再度接続します。
3. スイッチの電源を入れます。

スイッチ スタックおよびそのメンバのモニタリングに使用できるコマンドについては、「*Displaying Switch Stack Information*」の項を参照してください。

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。

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（電気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。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。

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、error-disabled 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 error-disabled ステートからインターフェイスを復帰させ、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 の実行

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

IP ルーティングは、デフォルトではすべてのスイッチでディセーブルになります。

（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、スイッチ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* `Switch# 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。

関連トピック

ping, （3 ページ）
例：IP ホストの ping, （33 ページ）

温度のモニタリング

スイッチは温度条件をモニタし、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、スイッチ内の温度であり、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** *interface-id*] {*source-mac-address*} [**interface** *interface-id*] {*destination-mac-address*} [**vlan** *vlan-id*] [**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 {*source-ip-address* | *source-hostname*}{*destination-ip-address* | *destination-hostname*} [**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 ホスト `Switch# traceroute ip 192.51.100.1`	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。

関連トピック

IP Traceroute, （5 ページ）
例：IP ホストに対する traceroute の実行, （34 ページ）

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

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。

関連トピック

debug コマンド, （7 ページ）

show platform forward コマンドの使用

show platform forward**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。

このコマンドで出力される情報のほとんどは、主に、スイッチの用途別集積回路（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。デバッギン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。

詳細については、『*Cisco IOS Configuration Fundamentals Command Reference, Cisco IOS XE Release 16.1 (Catalyst 3850 Switches)*』を参照してください。

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。

- OBFL をイネーブルにするには、**hw-switch switch** [*switch-number*] **logging onboard** [**message level** *level*] グローバル コンフィギュレーション コマンドを使用します。スイッチの場合、*switch-number* に指定できる範囲は 1 ～ 9 です。スイッチが生成してフラッシュ メモリに保存するハードウェア関連のメッセージの重大度を指定するには、**message level** *level* パラメータを使用します。
- OBFL データをローカル ネットワークまたは指定したファイル システムにコピーするには、**copy onboard switch** *switch-number***url** *url-destination* 特権 EXEC コマンドを使用します。
- OBFL をディセーブルにするには、**no hw-switch switch** [*switch-number*] **logging onboard** [**message level**] グローバル コンフィギュレーション コマンドを使用します。
- フラッシュ メモリ内の稼働時間と CLI コマンド情報以外のすべての OBFL データをクリアするには、**clear onboard switch** *switch-number* 特権 EXEC コマンドを使用します。
- スイッチ スタックでは、**hw-switch switch** [*switch-number*] **logging onboard** [**message level** *level*] 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ことにより、スタンドアロン スイッチまたはすべてのスタック メンバの OBFL をイネーブルにできます。
- アクティブ スイッチのメンバ スイッチの OBFL をイネーブルまたはディセーブルにできます。

ここで説明した各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。

関連トピック

スイッチのオンボード障害ロギング, （9 ページ）
OBFL 情報の表示, （25 ページ）

WebUI の WSMA 設定

WSMA 設定は、デフォルトで Web UI にアクセスするために使用できます。設定を明示的に削除する場合は、以下のように再構成する必要があります。

```
Switch(config)#wsma agent exec
Switch(wsma-exec-agent)# profile httplistener
Switch(wsma-exec-agent)# profile httpslistener
Switch(wsma-exec-agent)#exit
Switch(config)#wsma agent config
Switch(wsma-config-agent)# profile httplistener
Switch(wsma-config-agent)# profile httpslistener
Switch(wsma-config-agent)#exit
Switch(config)#wsma agent filesys
Switch(wsma-filesys-agent)# profile httplistener
Switch(wsma-filesys-agent)# profile httpslistener
Switch(wsma-filesys-agent)#exit
Switch(config)#wsma agent notify
```

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 *switch-number* **clilog** `Switch# show onboard switch 1 clilog`	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 *switch-number* **environment** `Switch# 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 *switch-number* **message** `Switch# 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 *switch-number* **counter** `Switch# 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。

コマンド	目的
show onboard switch *switch-number* **temperature** `Switch# 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。
show onboard switch *switch-number* **uptime** `Switch# 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 *switch-number* **voltage** `Switch# 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 *switch-number* **status** `Switch# 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。

関連トピック

スイッチのオンボード障害ロギング，（9 ページ）
OBFL の設定，（24 ページ）

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別するには、**show processes cpu sorted** 特権 EXEC コマンドを入力します。出力例の 1 行目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 *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	Cause	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
PoE がないポートは 1 つに限りません。 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。	

症状または問題	考えられる原因と解決法
	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。 **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。 （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。 **power inline never** がそのインターフェイスまたはポートで設定されていないことを確認します。 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。 （注） シスコ受電デバイスは、ストレート ケーブルでのみ動作し、クロス ケーブルでは動作しません。 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。 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。 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 inline power** コマンドを使用して、利用可能な電源の量を確認します。

症状または問題	考えられる原因と解決法
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。 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。	

症状または問題	考えられる原因と解決法
	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。 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。 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を確認するには、**show log** 特権 EXEC コマンドを使用します。 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errdisable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びイネーブルにします。 特権 EXEC コマンドの **show env power** および **show power inline** 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。 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。 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。 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。 **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。

症状または問題	考えられる原因と解決法
	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 **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 本ずつ再び接続してください。**show interface status** および **show power inline** 特権 EXEC コマンドを使用して、インライン電源の統計情報およびポートの状態をモニタします。 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。
シスコ先行標準受電デバイスは、切断またはリセットされます。 正常に動作した後で、Cisco phone が断続的にリロードしたり、PoE から切断されたりします。	スイッチから受電デバイスまでのすべての電気系統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などが発生します。 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。 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。 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。 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）。 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があります。

症状または問題	考えられる原因と解決法
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。 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。	**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。 **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をスイッチが検出することを確認します。 **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。

関連トピック

Power over Ethernet（PoE）ポート, （2 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

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。

```
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 *5*：*Ping* の出力表示文字

文字	説明
!	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。

文字	説明
U	宛先到達不能エラー PDU を受信したことを示します。
C	輻輳に遭遇したパケットを受信したことを示します。
I	ユーザによりテストが中断されたことを示します。
?	パケット タイプが不明です。
&	パケットの存続時間を超過したことを示します。

ping セッションを終了するには、エスケープ シーケンス（デフォルトでは 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。

関連トピック

ping, （3 ページ）
ping の実行, （21 ページ）

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。

```
Switch# traceroute ip 192.0.2.10

Type escape sequence to abort.
Tracing the route to 192.0.2.10

  1 192.0.2.1 0 msec 0 msec 4 msec
  2 192.0.2.203 12 msec 8 msec 0 msec
  3 192.0.2.100 4 msec 0 msec 0 msec
  4 192.0.2.10 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	説明
*	プローブがタイムアウトになりました。

文字	説明
?	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。

関連トピック

IP Traceroute, （5 ページ）
IP traceroute の実行, （22 ページ）

例：すべてのシステム診断をイネーブルにする

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。

このコマンドは、すべてのシステム診断をディセーブルにします。

```
Switch# debug all
```

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。

関連トピック

debug コマンド, （7 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

関連資料

関連項目	マニュアル タイトル
システム管理コマンド	*System Management Command Reference (Catalyst 3850 Switches)System Management Command Reference (Cisco WLC 5700 Series)*
プラットフォームに依存しないコマンド リファレンス	*Configuration Fundamentals Command Reference, Cisco IOS XE Release 3S（Catalyst 3850 Switches）*
Platform_independent の設定情報	*Configuration Fundamentals Configuration Guide, Cisco IOS XE Release 3S（Catalyst 3850 Switches）*

標準および RFC

標準/RFC	Title
なし	—

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

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と情報

リリース	変更内容
Cisco IOS XE 3.2SE	この機能が導入されました。

関連トピック

機能情報の確認