トラブルシューティング

オンボーディングの問題

スイッチの LED は、スイッチに関するトラブルシューティング情報を提供します。これにより、起動の失敗、ポート接続の問題、およびスイッチ全体の性能を把握できます。Web UI、CLI または SNMP ワークステーションから統計情報を入手することもできます。詳細については、Cisco IE3500、IE3505 高耐久性シリーズ スイッチのソフトウェア設定ガイドまたは SNMP アプリケーションに付属しているドキュメントを参照してください。

スイッチ LED

スイッチの障害対応を行う際は、ポートの LED を確認します。LED の色とそれらの意味については「LED」を参照してください。

スイッチの接続状態

不良または破損したケーブル

ケーブルにわずかでも傷や破損がないか必ず確認してください。物理層の接続に問題がないように見えるケーブルでも、配線やコネクタのごくわずかな損傷が原因でパケットが破損することがあります。ポートでパケットエラーが多く発生したり、ポートがフラッピング（リンクの切断および接続）を頻繁に繰り返したりする場合は、ケーブルにこのような破損がある場合があります。

- 銅線ケーブルまたは光ファイバ ケーブルを問題がないことがわかっているケーブルに交換します。
- ケーブル コネクタで破損または欠落したピンがないか確認します。
- 発信元と宛先の間のパッチ パネルの接続やメディア コンバータに問題がないことを確認します。可能な場合は、パッチ パネルをバイパスするか、メディア コンバータ（光ファイバ/銅線）を除去します。
- ケーブルを別のポートに接続して、問題が発生するかどうかを確認します。

イーサネット ケーブルと光ファイバケーブル

ケーブルが適切であることを確認します。

- イーサネットの場合、10 Mb/s UTP 接続にはカテゴリ 3 の銅線ケーブルを使用します。10/100、10/100/1000 Mbps、PoE 接続には、カテゴリ 5、カテゴリ 5e、またはカテゴリ 6 の UTP を使用します。
- 距離やポート種別に適した光ファイバ ケーブルであることを確認します。接続先装置のポートが同種の符号化、光周波数、およびファイバ種別を使用するよう一致していることを確認します。
- 銅線のストレート ケーブルを使用すべきところにクロス ケーブルが使用されていたり、クロス ケーブルを使用すべきところにストレート ケーブルが使用されていたりしないかを確認します。スイッチの Auto-MDIX を有効にするか、ケーブルを交換します。

リンクステータス

両側でリンクが確立されていることを確認します。配線が切れていたり、ポートがシャットダウンしていたりすると、片側ではリンクが表示されても反対側では表示されない可能性があります。

ポート LED が点灯していても、ケーブルが正常なことを示しているわけではありません。物理的な応力がかかっている場合は、限界レベルで動作している可能性があります。ポート LED が点灯しない場合は、次のことを確認します。

- ケーブルをスイッチから外して、問題のない装置に接続します。
- ケーブルの両端が正しいポートに接続されていることを確認します。
- 両方の装置の電源が入っていることを確認します。
- 正しい種別のケーブルが使用されていることを確認します。詳細については、「ケーブルとコネクタ」を参照してください。
- 接触不良がないか確認します。完全に接続されているように見えても、そうでないことがあります。ケーブルをいったん外して、接続し直してください。

10/100/1G ポートの接続

ポートが異常を示している場合は、次のことを確認します。

- LED を調べて、すべてのポートのステータスを確認します。詳細については、スイッチ LED （1 ページ）を参照してください。
- **show interfaces** EXEC コマンドを使用して、ポートが error-disabled、disabled、または shutdown の状態になっていないかどうかを確認します。必要に応じて、ポートを再び有効化します。
- ケーブル種別を確認します。

SFP モジュール

Cisco SFP モジュール以外は使用しないでください。各シスコ製モジュールには、セキュリティ情報が符号化されたシリアル EEPROM が組み込まれています。この符号化によって、モジュールがスイッチの要件を満たしていることが確認されます。

- SFP モジュールを調査します。疑わしい SFP モジュールを故障していないことがわかっているモジュールに交換します。
- モジュールが使用するプラットフォームでサポートされていることを確認します。（Cisco.com にあるスイッチのリリース ノートに、スイッチがサポートする SFP モジュールの一覧が示されています）。
- **show interfaces** 特権 EXEC コマンドを使用して、ポートまたはモジュールが error-disabled、disabled、または shutdown の状態になっていないかどうかを確認します。必要に応じて、ポートを再度有効にします。
- 光ファイバの接続部分がクリーンな状態で、しっかりと接続されていることを確認します。

インターフェイスの設定

インターフェイスが無効になっていないか、電源が切れていないかを確認してください。リンクの片側でインターフェイスを手動でシャットダウンした場合は、そのインターフェイスが再度有効にされるまで復活しません。**show interfaces** 特権 EXEC コマンドを使用して、インターフェイスが errordisabled、disabled、または shutdown の状態になっていないかどうかを確認します。必要に応じて、インターフェイスを再度有効にします。

端末装置への ping

ping を使用して、最初は直接接続されているスイッチから始めて、接続できない原因となっている箇所を突き止めるまで、ポートごと、インターフェイスごと、トランクごとに段階的にさかのぼって調べます。各スイッチの連想メモリ（CAM）テーブル内に、端末装置の MAC アドレスが存在していることを確認します。

スパニングツリーのループ

スパニングツリープロトコル（STP）にループが発生すると、重大な性能上の問題が引き起こされ、その状況がポートやインターフェイスの問題のように見えることがあります。

ループは、単方向リンクによって引き起こされることがあります。つまり、スイッチから送信されたトラフィックがネイバーで受信されるが、ネイバーからのトラフィックがスイッチで受信されない場合に発生します。破損したケーブル、その他のケーブル配線の問題、またはポートの問題によって、この単方向通信が引き起こされる可能性があります。

スイッチで単方向リンク検出（UDLD）を有効にすると、単方向リンク問題の特定に役立ちます。スイッチでUDLDを有効にする方法の詳細については、Cisco.comにあるスイッチ ソフトウェア コンフィギュレーション ガイドの「UDLDの概要」の項を参照してください。

スイッチの性能

速度、デュプレックス、および自動ネゴシエーション

ポートの統計情報に、アライメント エラー、フレーム チェック シーケンス（FCS）、またはレイト コリジョン エラーが大量に表示される場合は、速度またはデュプレックスの不一致を示している可能性があります。

2台のスイッチ間、スイッチとルータ間、またはスイッチとワークステーション/サーバー間でデュプレックスと速度の設定が一致しない場合は、共通の問題が発生します。この不一致は、速度およびデュプレックスを手動で設定した場合や、2台の装置間における自動ネゴシエーションの問題が原因となることがあります。

スイッチの性能を最大限に引き出してリンクを保証するには、次のいずれかのガイドラインに従ってデュプレックスまたは速度の設定を変更してください。

- 両方のポートで、速度とデュプレックスの両方を自動ネゴシエーションします。
- 接続の両端でインターフェイス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。
- 遠端の装置が自動ネゴシエートしない場合は、2つのポートのデュプレックス設定を同じにします。速度パラメータは、接続先ポートが自動ネゴシエーションを実行しない場合でも自動的に調整されます。

自動ネゴシエーションと NIC

スイッチとサードパーティ製ネットワーク インターフェイス カード（NIC）間で問題が発生する場合があります。デフォルトで、スイッチ ポートとインターフェイスは自動ネゴシエートします。一般的にはラップトップ コンピュータやその他の装置も自動ネゴシエーションに設定されていますが、それでも問題が発生することがあります。

自動ネゴシエーションの問題をトラブルシューティングする場合は、接続の両側で手動設定を試してください。それでも問題が解決しない場合は、NIC上のファームウェアまたはソフト

ウェアに問題がある可能性があります。その場合は、NIC ドライバを最新バージョンにアップグレードして問題を解決してください。

ケーブル接続の距離

ポート統計情報に、過剰な FCS、レイト コリジョン、またはアライメント エラーが示されている場合は、スイッチから接続先の装置までのケーブル長が推奨ガイドラインに従っていることを確認してください。「ケーブルおよびアダプタ」を参照してください。

スイッチのリセット

次の場合、スイッチのスタートアップ設定を工場出荷時設定にリセットすることをお勧めします。

- スイッチをネットワークに設置したが、誤った IP アドレスを割り当てたため、スイッチに接続できない。
- スイッチのパスワードをリセットする必要がある。

（注） スイッチをリセットすると、設定が削除されてスイッチが再起動されます。すべてのデータを安全に消去するには、セキュアデータワイプ （6 ページ）を参照してください。

注意 スイッチの電源を入れる際に Express Setup ボタンを押すと、自動ブート シーケンスが停止され、ブートローダ モードが開始されます。

スイッチをリセットするには、次の手順を実行します。

手順

ステップ 1 ペーパー クリップまたは類似のもので [Express Setup] ボタン（前面プレートの小さな穴の後ろに埋め込み）を約 15 秒間押し続けます。

Express Setup LED は、埋め込みボタンが押し込まれている間、赤/緑色に点滅します。

ステップ 2 スイッチがリブートします。スイッチのリブートが完了すると、システム LED が緑色に点灯します。

ステップ 3 もう一度 [Express Setup] ボタンを 3 秒間押します。スイッチのイーサネットポートが緑色に点滅します。

これで、このスイッチは未設定のスイッチと同様に動作します。スイッチの設定は、CLI を使用したスイッチの設定に説明されている CLI セットアップ手順に従って行うことができます。

緊急リカバリインストール

注目 Emergency Recovery イメージは製造時にインストールされており、現場では更新できません。セキュリティ上の脆弱性が含まれている可能性があり、後続の IOS イメージに追加された機能をサポートしていない場合があります。

Emergency Recovery イメージは、システムに常に存在する IOS のバージョンです。**emgy0:** パーティションにインストールされており、誤って削除されないよう書き込み保護されています。

dir emgy0: コマンドを使用して Emergency Recovery イメージを表示し、**boot emgy0:**<*image name*> コマンドを使用して起動します。

Emergency Recovery イメージを使用する場合は、外部ネットワーク インターフェイスの切断、リモートアクセスの遮断など、スイッチを隔離することを推奨します。

セキュアデータワイプ

セキュアデータワイプは、スイッチから機密情報を削除するために使用されます。

この機能は、以下のすべてのライセンスレベルでサポートされています。

- IE3500
- IE3505

セキュアデータワイプを実行すると、以下を含め、ユーザーがアクセス可能なフラッシュメモリのほとんどが消去されます。

- ユーザー設定とパスワード
- Cisco IOS XE イメージ
- Embedded MultiMediaCard（eMMC）
- rommon 変数
- TPM セキュアストレージ

（注） セキュア データ ワイプ プロセスにより、SD カードおよび USB デバイスの格納ファイルが消去されます。または、外部ストレージ装置を手動で消去または再フォーマットすることもできます。

セキュアデータワイプ後、スイッチは工場出荷時設定で rommon プロンプトに戻ります。

（注） 有効なイメージの入った sdflash/usbflash が挿入されている場合、装置は起動の優先順位に基づいて外部メディア内のイメージで起動します。イメージを含む外部メディアがデバイスに挿入されていない場合にのみ、装置は rommon になります。

セキュアデータワイプの実行

セキュアデータワイプを有効にするには、次の例に示すように、特権EXECモードで**factory-reset all secure** コマンドを入力します。

```
Switch#factory-reset ?
  all                 All factory reset operations
  keep-licensing-info  Keep license usage info
Switch#factory-reset all ?
secure  Securely reset all
Switch#factory-reset all secure
The factory reset operation is irreversible for securely reset all. Are you sure?
[confirm]Y
```

factory-reset コマンドオプション：

- **factory-reset all**：フラッシュからすべてを削除します。
- **factory-reset keep-licensing-info**：工場出荷時状態へのリセット後もライセンス情報を保持し、他のすべてをフラッシュから削除します。
- **factory-reset all secure**：フラッシュからすべてを削除し、マウントを解除してパーティションをサニタイズしてからマウントし直します。これにより、これらのパーティションのデータを回復できないようにします。

重要 **factory-reset all secure** 操作には時間がかかる場合があります。電源を入れ直さないでください。

スイッチがコマンドを実行した後にログを確認するには、IOS XE を起動し、次の **show** コマンドを入力します。

```
Switch#show platform software factory-reset secure log
Factory reset log:
#CISCO DATA SANITIZATION REPORT:# IE3200
Purge ACT2 chip at 12-08-2022, 15:17:28
ACT2 chip Purge done at 12-08-2022, 15:17:29
mtd and backup flash wipe start at 12-08-2022, 15:17:29
mtd and backup flash wipe done at 12-08-2022, 15:17:29.
```

スイッチのシリアル番号の確認

シスコの技術サポートに問い合わせを行う場合は、スイッチのシリアル番号を確認する必要があります。**show version** 特権 EXEC コマンドを使用して、スイッチのシリアル番号を取得することもできます。

また、スイッチのシリアル番号は、装置のラベルに記載されています。

パスワードの回復方法

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ーが、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） これらの装置では、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、この機能の一部を無効にできます。パスワード回復が無効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。

スイッチをリセットして新しいパスワードを入力する手順については、スイッチのリセット（5 ページ）を参照してください。

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。