# CatOS が稼働する Catalyst 4500/4000、5500/5000 および 6500/6000 シリーズ スイッチの設定と管理のベスト プラクティス

## 内容

関連情報

# 概要

このドキュメントでは、ネットワーク内の Cisco Catalyst シリーズ スイッチ、特に、Catalyst 4500/4000、5500/5000、および 6500/6000 プラットフォームの実装について説明します。設定とコマンドについては、Catalyst OS ( CatOS ) General Deployment ソフトウェア 6.4(3) 以降を実行していることを前提にして説明します。設計上の考慮事項が一部含まれていますが、このドキュメントはキャンパス設計全体を網羅しているわけではありません。

# 前提条件

## 要件

このドキュメントは、読者が Catalyst 6500 シリーズ コマンド リファレンス、7.6 [英語] に精通していることを前提としています。

このドキュメントでは、さらに詳しい情報を得られるように、オンラインで公開されている資料に言及していますが、基本的な教育用資料としては、次のような資料もあります。

- Cisco ISP Essentials：すべての ISP が検討する必要がある必須の IOS 機能。
- シスコのネットワーク監視およびイベント関連付けのガイドライン [英語]
- ギガビット キャンパス ネットワークの設計：原則およびアーキテクチャ [英語]
- Cisco SAFE：エンタープライズ ネットワークのセキュリティ設計 [英語]

## 使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

## 表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

## 背景説明

このドキュメントで紹介するソリューションは、数多くの大規模企業のお客様と協力しながら長年にわたって複雑なネットワークに取り組んできたシスコのエンジニアの現場経験から生まれたものです。その結果、このドキュメントはネットワークを適切に運用するための、現実的な構成に重点を置くものとなっています。このドキュメントでは次のようなソリューションを紹介しています。

- 統計的に見て現場で最も幅広く利用されてきた、リスクが最も低いソリューション。
- 確定的な結果を得るために、一部の柔軟性を犠牲にしているシンプルなソリューション。
- ネットワーク運用チームによる管理と設定が容易なソリューション。
- 高可用性と高い安定性を促進するソリューション。

このドキュメントは次の 4 つの項で構成されています。

- 基本設定：スパニング ツリー プロトコル（STP）やトランキングなど、ネットワークの大部分で使用される機能。
- 管理設定：設計上の考慮事項、および Simple Network Management Protocol（SNMP）、リモート モニタリング（RMON）、syslog、Cisco Discovery Protocol（CDP）、および Network Time Protocol（NTP）を使用したシステムとイベントのモニタリング。
- セキュリティの設定：TACACS+ を使用したパスワード、ポート セキュリティ、物理的セキュリティ、および認証。
- 設定チェックリスト：推奨の設定テンプレートの概要。

# 基本設定

この項では、ほとんどの Catalyst ネットワークで導入される機能について説明します。

## Catalyst コントロール プレーン プロトコル

この項では、通常動作時にスイッチ間で実行されるプロトコルを紹介します。それらのプロトコルの基本を理解すると、各項の内容を理解するのに役立ちます。

### スーパーバイザ トラフィック

Catalyst ネットワークで使用可能な機能のほとんどには、協調して動作する複数のスイッチが必要です。そのため、制御された方法でキープアライブ メッセージ、設定パラメータ、管理上の変更などを交換する必要があります。そのようなプロトコルは、CDP のようにシスコ独自のものであるか、IEEE 802.1d（STP）のように標準ベースのプロトコルであるため、Catalyst シリーズに実装された場合、すべてに一定の共通要素が備わっています。

基本的なフレーム転送では、ユーザ データ フレームはエンド システムから発信され、各データ フレームの発信元アドレスと宛先アドレスは、レイヤ 2（L2）スイッチド ドメイン内では変更されません。各スイッチの Supervisor Engine にある Content Addressable Memory（CAM）ルックアップ テーブルは、発信元アドレスの学習プロセスによって読み込まれ、受信した各フレームの転送先出力ポートが示されます。アドレス学習プロセスが不完全な場合（宛先が不明な場合や、フレームがブロードキャストまたはマルチキャスト アドレス宛ての場合）は、その VLAN 内のすべてのポートからフレームが送出（フラッディング）されます。

スイッチでは、システム経由でスイッチングするフレーム、およびスイッチの CPU（ネットワーク管理プロセッサ（NMP）としても知られる）自体に送信するフレームも識別する必要があります。

Catalyst コントロール プレーンは、内部スイッチ ポートでトラフィックを受信して、NMP にトラフィックを送信にするために、CAM テーブル内にある**システム エントリと呼ばれる特別なエントリを使用して作成されます。**そのため、既知の宛先 MAC アドレスを持つプロトコルを使用することで、コントロール プレーン トラフィックをデータ トラフィックから分離できます。次に示すように、スイッチに対して **show CAM system コマンドを発行してこの点を確認します。**

```
>show cam system

* = Static Entry. + = Permanent Entry. # = System Entry. R = Router Entry.
X = Port Security Entry
VLAN  Dest MAC/Route Des    [CoS]  Destination Ports or VCs / [Protocol Type]
----  -----------------    -----  ------------------------------------------
```

```
1     00-d0-ff-88-cb-ff  #          1/3
!--- NMP internal port. 1 01-00-0c-cc-cc-cc # 1/3 !--- CDP and so on. 1 01-00-0c-cc-cc-cd # 1/3
!--- Cisco STP. 1 01-80-c2-00-00-00 # 1/3 !--- IEEE STP. 1 01-80-c2-00-00-01 # 1/3 !--- IEEE
flow control. 1 00-03-6b-51-e1-82 R# 15/1 !--- Multilayer Switch Feature Card (MSFC) router. ...
```

シスコでは、次の表に示されているイーサネット MAC アドレスとプロトコル アドレスの範囲を予約しています。各アドレスについては、後述していますが、便宜上、次の表には要約のみ提示しています。

| 機能 | SNAP HDLC プロトコル タイプ | 宛先マルチキャスト MAC |
|---|---|---|
| Port Aggregation Protocol（PAgP） | 0x0104 | 01-00-0c-cc-cc-cc |
| スパニング ツリー PVSTP+ | 0x010b | 01-00-0c-cc-cc-cd |
| VLAN ブリッジ | 0x010c | 01-00-0c-cd-cd-ce |
| 単方向リンク検出（UDLD） | 0x0111 | 01-00-0c-cc-cc-cc |
| Cisco Discovery Protocol | 0x2000 | 01-00-0c-cc-cc-cc |
| Dynamic Trunking Protocol（DTP） | 0x2004 | 01-00-0c-cc-cc-cc |
| STP UplinkFast | 0x200a | 01-00-0c-cd-cd-cd |
| IEEE スパニング ツリー 802.1d | 該当なし：DSAP 42 SSAP 42 | 01-80-c2-00-00-00 |
| Inter Switch Link（ISL） | N/A | 01-00-0c-00-00-00 |
| VLAN Trunking Protocol（VTP） | 0x2003 | 01-00-0c-cc-cc-cc |
| IEEE ポーズ、802.3x | 該当なし：DSAP 81 SSAP 80 | 01-80-C2-00-00-00>0F |

シスコの大部分の制御プロトコルでは、**LLC 0xAAAA03、OUI 0x00000C** を含む、IEEE 802.3 SNAP カプセル化を使用しており、LAN アナライザのトレースで確認できます。これらのプロトコルのその他の共通プロパティには、次のものがあります。

- これらのプロトコルはポイントツーポイント接続を前提としています。マルチキャストの宛先アドレスを意図的に使用することで、2 台の Catalyst スイッチがシスコ以外のスイッチを経由して透過的に通信できるようになります。これは、フレームの解釈と傍受を行わないデバイスがフレームを単純にフラッディングするためです。ただし、マルチベンダー環境を経由するポイントツーマルチポイント接続では動作の一貫性が失われることがあるため、一般的には避ける必要があります。
- これらのプロトコルはレイヤ 3（L3）ルータで終端し、スイッチ ドメイン内でのみ機能します。
- これらのプロトコルは、入力側の特定用途集積回路（ASIC）処理とスケジューリングによって、ユーザ データより優先して受信されます。

制御プロトコルの宛先アドレスを紹介したら、完全を期して発信元アドレスについても説明する

必要があります。スイッチ プロトコルでは、シャーシの EPROM によって提供される使用可能なアドレスのバンクから取得される MAC アドレスが使用されます。**show module コマンドを発行すると、STP ブリッジ プロトコル データ ユニット（BPDU）や ISL フレームなどのトラフィックを各モジュールが発信するときに使用可能なアドレス範囲が表示されます。**

```
>show module

...
Mod MAC-Address(es)                         Hw      Fw          Sw
--- --------------------------------------- ------ ---------- -----------------
1   00-01-c9-da-0c-1e to 00-01-c9-da-0c-1f 2.2    6.1(3)     6.1(1d)
    00-01-c9-da-0c-1c to 00-01-c9-da-0c-1
    00-d0-ff-88-c8-00 to 00-d0-ff-88-cb-ff
!--- MACs for sourcing traffic. ... VLAN 1
```

## VLAN 1

VLAN 1 は Catalyst ネットワークにおいて特別な意味を持ちます。

Catalyst Supervisor Engine はトランキング時にデフォルトの VLAN である VLAN 1 を常に使用して、多数の制御プロトコルや管理プロトコル（CDP、VTP、および PAgP など）のタグ付けを行います。デフォルトでは、内部 sc0 インターフェイスを含むすべてのポートが VLAN 1 のメンバとなるように設定されています。すべてのトランクがデフォルトで VLAN 1 を伝送し、5.4 より前の CatOS ソフトウェア バージョンでは VLAN 1 のユーザ データをブロックできませんでした。

Catalyst のネットワーキングでよく使用されるいくつかの用語を明確にするために、用語の定義を次に示します。

- 管理 VLAN は sc0 が存在する場所です。この VLAN は変更できます。
- ネイティブ VLAN は、トランキングが行われていない場合にポートが戻される VLAN として定義されます。また、802.1Q トランク上のタグなし VLAN のことです。デフォルトでは、VLAN 1 がネイティブ VLAN です。
- ネイティブ VLAN を変更するには、set vlan vlan-id mod/port コマンドを発行します。**注：VLANを**作成してから、トランクのネイティブVLANとして設定してください。

ネットワークを調整して、VLAN 1 のポートの動作を変更する理由には、次のようなものがあります。

- その他すべての VLAN と同様、VLAN 1の直径が（特に、STP の観点から）安定性に対するリスクとなるほど大きくなった場合はプルーニングする必要があります。詳細については、このドキュメントの「インバンド管理」の項を参照してください。
- VLAN 1 のコントロール プレーン データは、トラブルシューティングを簡素化し、最大限の CPU サイクルを利用可能にするためにユーザ データから分離する必要があります。
- STP を使用せずにマルチレイヤ キャンパス ネットワークを設計する場合は、VLAN 1 での L2 ループは避ける必要があります。それでも、複数の VLAN や IP サブネットが存在する場合は、アクセス レイヤへのトランキングが必要です。これを実現するには、トランク ポートから VLAN 1 を手動で削除します。

要約すると、トランクについては次の点に注意してください。

- **CDP、VTP、および PAgP のアップデートは、トランクでは常に VLAN 1 のタグ付きで転送されます。**これは、VLAN 1 がトランクから削除されていてネイティブ VLAN でない場合で

も同様です。ユーザ データ用の VLAN 1 を削除しても、引き続き VLAN 1 を使用して送信されているコントロール プレーン トラフィックには影響しません。

- ISLトランクでは、DTPパケットがVLAN1に送信されます。これは、VLAN 1がトランクからクリアされ、ネイティブVLANではなくなった場合でも同様です。802.1Q トランクでは、DTP パケットがネイティブ VLAN で送信されます。これは、ネイティブ VLAN がトランクから削除されている場合でも同様です。
- PVST+ では、VLAN 1 がトランクから削除されていない限り、他のベンダーとの相互運用性を確保するために、**802.1Q IEEE BPDU が Common Spanning Tree の VLAN 1 上をタグなしで転送されます。**これは、ネイティブ VLAN の設定にかかわらず同様です。**その他すべての VLAN に対しては、Cisco PVST+ BPDU がタグ付きで送信されます。**詳細については、このドキュメントの「スパニング ツリー プロトコル」の項を参照してください。
- ISL と 802.1Q の両トランクでは、802.1s マルチ スパニング ツリー ( MST ) BPDU は常に VLAN 1 で送信されます。これは、VLAN 1 がトランクから削除されている場合でも当てはまります。
- MST ブリッジと PVST+ ブリッジ間にあるトランクの VLAN1 を削除したり、無効にしたりしないでください。ただし、VLAN 1 が無効になっている場合、すべての VLAN で MST ブリッジの境界ポートが root-inconsistent ステートにならないようにするために、MST ブリッジがルートになる必要があります詳細については、Multiple Spanning Tree Protocol ( 802.1s ) の概要 [英語] を参照してください。

### 推奨事項

クライアントもホストも接続されていない VLAN を **up/up の状態で維持するためには、その VLAN に少なくとも 1 台の物理デバイスが接続されている必要があります。**接続されているデバイスがない場合、その VLAN は **up/down 状態になります。**現在、当該 VLAN のスイッチにアクティブなポートが存在しない場合、VLAN インターフェイスを **up/up 状態にするコマンドはありません。**

デバイスを接続したくない場合は、当該 VLAN の任意のポートにループバック プラグを接続します。あるいは、同じスイッチ上にある当該 VLAN の 2 つのポートを接続するクロス ケーブルを使用してみてください。この方法だとポートが強制的に起動します。詳細については、T1/56K 回線のループバック テスト [英語] の「ループバック プラグ」の項を参照してください。

あるネットワークが 2 つのサービス プロバイダーにマルチホームされている場合、そのネットワークは 2 つのサービス プロバイダー間の中継ネットワークとして機能します。パケットで受信した VLAN 番号を、1 つのサービス プロバイダーから別のサービス プロバイダーに渡す際に変換または変更する必要がある場合、QinQ 機能を使用して VLAN 番号を変更することを推奨します。

## VLAN Trunking Protocol

VLAN を作成する前に、ネットワークで使用される VTP モードを決定します。VTP を使用すると、1 つまたは複数のスイッチで VLAN の設定を一元的に変更できます。それらの変更はドメイン内のその他すべてのスイッチに自動的に伝達されます。

### 動作の概要

VTP は、VLAN 設定の整合性を維持する L2 メッセージング プロトコルです。VTP では、ネットワーク全体にわたって VLAN の追加、削除、名前の変更が管理されます。VTP を使用すると、VLAN 名の重複、不適切な VLAN タイプの仕様、セキュリティ違反などのさまざまな問題を引き

起こす設定ミスや設定の不整合を最小限に抑えることができます。VLAN データベースはバイナリ ファイルであり、VTP サーバの NVRAM に設定ファイルとは別に保存されます。

VTPプロトコルは、イーサネット宛先マルチキャストMACアドレス(01-00-0c-cc-cc-cc)とSNAP HDLCプロトコルタイプOx2003を使用してスイッチ間で通信を行います。非トランクポートでは動作しません（VTPはISLまたは8802.1Q） DTPがトランクをオンラインにするまで送信されます。

メッセージ タイプには、5 分ごとに生成されるサマリー アドバタイズメント、変更があったときに生成されるサブセット アドバタイズメントと要求アドバタイズメント、および VTP プルーニングが有効になっている場合の参加が含まれます。サーバで VTP 設定が変更されると、そのたびに VTP 設定のリビジョン番号が 1 増加し、ドメイン全体に新しいテーブルが伝搬されます。

VLAN を削除すると、その VLAN のメンバーだったポートは非アクティブ状態になります。同様に、クライアント モードのスイッチがブートアップ時に（VTP サーバまたは別の VTP クライアントから）VTP VLAN テーブルを受信できなかった場合、デフォルトの VLAN 1 を除く VLAN のすべてのポートが非アクティブ化されます。

次の表に、さまざまな VTP モードの機能比較の概要を示します。

| 機能 | サーバ | クライアント | トランスペアレント | オフ[1] |
|---|---|---|---|---|
| 送信元 VTP メッセージ | Yes | Yes | No | No |
| VTP メッセージのリッスン | Yes | Yes | No | No |
| VTP メッセージの転送 | Yes | Yes | Yes | No |
| VLAN の作成 | Yes | No | はい（ローカルでのみ有意） | はい（ローカルでのみ有意） |
| VLAN の記憶 | Yes | No | はい（ローカルでのみ有意） | はい（ローカルでのみ有意） |

VTP VTP VTP MAC CAM このプロトコルではマルチキャスト アドレスが使用されるため、トランスペアレント モードのスイッチ（または他のベンダーのスイッチ）はドメイン内のその他のシスコ スイッチにフレームを単純にフラッディングします。

1 CatOS ソフトウェア リリース 7.1 では、 VTP VTP VTP VTP

次の表に、初期設定の概要を示します。

| 機能 | デフォルト値 |
|---|---|
| VTPドメイン名 | ヌル |
| VTP モード | サーバ |

| | |
|---|---|
| VTP バージョン | バージョン 1 がイネーブル |
| VTP パスワード | なし |
| VTP Pruning | Disabled |

VTP バージョン 2（VTPv2）には、次の機能上の柔軟性があります。ただし、VTP バージョン 1（VTPv1）とは相互運用できません。

- トークン リングのサポート。
- 認識されない VTP 情報のサポート。スイッチで解析できない値も伝達されるようになりました。
- バージョン依存のトランスペアレント モード。 そのため、トランスペアレント ドメインを越えて複数のドメインをサポートできます。
- バージョン番号の伝達。すべてのスイッチで VTPv2 が使用可能な場合、1 台のスイッチを設定することですべてのスイッチを有効にできます。

詳細については、VLAN トランク プロトコル（VTP）の説明と設定 [英語] を参照してください。

## VTP バージョン 3

CatOS ソフトウェア リリース 8.1 では、VTP バージョン 3（VTPv3）のサポートが導入されています。VTPv3 には、既存バージョンに対する拡張機能があります。それらの拡張機能により次のことが可能になります。

- 拡張 VLAN のサポート
- プライベート VLAN の作成およびアドバタイズメントのサポート
- VLAN インスタンスおよび MST マッピング伝達インスタンス（CatOS リリース 8.3 でサポート）のサポート
- サーバ認証の向上
- 「誤った」データベースが偶発的に VTP ドメインに挿入されることからの保護
- VTPv1 と VTPv2 との相互作用
- ポート単位の設定機能

VTPv3 の実装と以前のバージョンの実装間の主な違いの 1 つは、VTP プライマリ サーバの導入です。ドメインがパーティション化されていない場合、1 つの VTPv3 ドメインに 1 つのプライマリ サーバのみあるのが理想的です。VTP ドメインに加える変更はすべて、VTP プライマリ サーバで実行して VTP ドメインに伝達する必要があります。1 つの VTPv3 ドメイン内に複数のサーバを設定することもでき、それらは、セカンダリ サーバとしても知られています。スイッチがサーバになるように設定されている場合、そのスイッチはデフォルトでセカンダリ サーバになります。セカンダリ サーバにはドメインの設定を保存できますが、設定を変更することはできません。セカンダリ サーバは、スイッチからのテイクオーバーに成功するとプライマリ サーバになることができます。

VTPv3 を実行するスイッチは、現在のプライマリ サーバよりも大きいリビジョン番号の VTP データベースのみ受け入れます。このプロセスは、スイッチが常に同じドメイン内のネイバーからの優れた設定を受け入れる VTPv1 や VTPv2 とは大きく異なります。この VTPv3 での変更により保護が提供されます。より大きい VTP リビジョン番号を持つ新しいスイッチがネットワークに導入されても、ドメイン全体の VLAN 設定は上書きされません。

VTPv3 では、VTP によるパスワード処理に対する拡張機能も導入されています。パスワードを「hidden」として設定するために、hidden パスワード設定オプションを使用すると、次の状態が生じます。

- パスワードが設定のプレーン テキストに表示されず、シークレット 16 進形式のパスワードが設定に保存されます。
- スイッチをプライマリ サーバとして設定しようとすると、パスワード入力を要求されます。パスワードがシークレット パスワードに一致すれば、スイッチはプライマリ サーバとなり、ドメインの設定が可能となります。

**注：プライマ**リサーバは、任意のインスタンスのVTP設定を変更する必要がある場合にのみ必要であることに注意してください。セカンダリ サーバがリロードを通じて設定の持続性を保証するため、VTP ドメインは、アクティブなプライマリ サーバがなくても動作できます。プライマリ サーバの状態は、次の理由により終了します。

- スイッチのリロード
- アクティブおよび冗長スーパバイザ エンジン間のハイ アベイラビリティ スイッチオーバー
- 別のサーバからのテイクオーバー
- モード設定の変更
- 次のような、VTP ドメイン設定の変更バージョンドメイン名ドメイン パスワード

VTPv3 では、スイッチが VTP の複数のインスタンスに参加することもできます。この場合、VTP モードは各 VTP インスタンスごとに固有であるため、同じスイッチを 1 つのインスタンスの VTP サーバおよび別のインスタンスのクライアントに設定できます。たとえば、1 台のスイッチを MST インスタンスの VLAN

VTPv1 と VTPv2 との相互運用の点では、VTP のすべてのバージョンのデフォルト動作は同じで、VTP の旧バージョンでは新しいバージョンの更新が単純に破棄されていました。VTPv1 スイッチと VTPv2 スイッチが VTPv3 一方で、VTPv3 スイッチは、レガシーの VTPv1 または VTPv2 フレームをトランクで受信すると、それぞれのデータベース更新の縮小バージョンを VTPv1 スイッチと VTPv2 スイッチに渡します。ただし、この情報交換は、VTPv1 スイッチと VTPv2 スイッチからの更新が VTPv3 スイッチによって受け入れられないという点で単方向の交換です。トランク接続では、VTPv3 スイッチは、トランク ポート全体で VTPv2 ネイバーと VTPv3 ネイバーの存在に応じるために、縮小された更新と VTPv3 の本格的な更新の送信を続けます。

拡張 VLAN に対する VTPv3 のサポートを提供するために、VTP により VLAN ごとに 70 バイトが割り当てられる VLAN データベースの形式が変更されています。この変更により、レガシー プロトコルの未変更フィールドを伝達する代わりに、デフォルト値以外のコーディングのみ許可されます。この変更のために、4K VLAN のサポートが結果として作成される VLAN データベースのサイズに影響します。

## 推奨事項

VTP / VTP 一部のお客様は、後述のような考慮事項はありますが、VTP クライアント/サーバ モードの管理の容易さを好んでいます。冗長性を確保するためにドメインごとに 2 つの 2 ドメイン内の残りのスイッチは VTPv2 を使用して/ VTP VTP VTP VTP VTP VLAN この設定変更が意図したものではなく、VLAN が削除された場合、この上書きによってネットワークの大規模な停止が発生する可能性があります。 VTP 再び標準の名前に戻します。この操作により、クライアントのコンフィギュレーション リビジョン番号が 0 に設定されます。

ネットワークに簡単に変更を加えられる VTP の機能には長所と短所があります。多くの企業では、次の理由により、注意深いアプローチが好まれるため、VTP

- スイッチまたはトランク ポート上の VLAN の変更要件を 1 台のスイッチごとに検討する必要があるため、適切な変更管理が実践できる。
- 誤って VLAN を削除するなど、ドメイン全体に影響を及ぼす管理者のエラーのリスクを限定

できる。
- より大きい VTP リビジョン番号を持つ新しいスイッチがネットワークに導入されて、ドメイン全体の VLAN 設定が上書きされるリスクがなくなる。
- 実行中のトランクから VLAN をプルーニングして、その VLAN 内にポートを持たないスイッチに戻すことができる。その結果、フレーム フラッディング時の帯域幅効率が向上します。また、手動でプルーニングすることで、スパニング ツリーの直径が小さくなります（このドキュメントの「DTP」の項を参照してください）。ポート チャネル トランクの未使用の VLAN をプルーニングする前に、IP フォンに接続されているすべてのポートが音声 VLAN があるアクセス ポートとして設定されていることを確認します。
- CatOS 6.x および CatOS 7.x の拡張 VLAN の範囲（1025 ~ 4094）は、この方法でのみ設定できる。詳細については、このドキュメントの「拡張 VLAN と MAC アドレス リダクション」の項を参照してください。
- VTP `Cisco Works 2000 Campus Manager 3.1` VTP ドメイン内に少なくとも 1 台のサーバが必要だった以前の制限は削除されています。

| サンプルVTPコマンド | 注 |
| --- | --- |
| set vtp domain name password x | CDP では、ドメイン間の配線のミスをチェックするために名前が確認されます。簡単なパスワードは、意図しない変更に対する有用な予防策となります。名前は大文字と小文字が区別されます。また、ペーストする場合はスペースに注意してください。 |
| s | |

| | |
|---|---|
| **set vtp mode transparent** | |
| **set vlan vlan number name name** | VLAN にポートを持つスイッチごとに設定します。 |
| **set trunk m** | 必要に応じてトランク経由の VLAN 伝送を可能にします。デフォルトはすべての VLAN です。 |

| | |
|---|---|
| od/portvlanrange | |
| clear trunk mod/portvlanrange | ディストリビューション レイヤからアクセス レイヤへのトランクなど、VLAN が存在しないトランクで手動プルーニングを行うことにより、STP の直径を制限します。 |

**注： setコマンド**でVLANを指定すると、VLANは追加されるだけで、クリアされません。たとえば、set trunk x/y 1-10コマンドは、許可リストをVLAN 1 ~ 10だけに設定しません。目的の結果を得るには、clear trunk x/y 11-1005コマンドを発行します。

トークン リング スイッチングはこのドキュメントの範囲外ですが、VTP TR-ISL トークン リング スイッチングの基本は、ドメイン全体が 1 つの分散マルチポート ブリッジを形成することです。そのため、すべてのスイッチの VLAN 情報が同じである必要があります。

## その他のオプション

VTPv2 はトークン リング環境では必須であり、/

VTPv3 には、より厳密な認証およびコンフィギュレーション リビジョンの制御を実装する機能があります。VTPv3 では、基本的に VTPv1/VTPv2 の また、VTPv3 はレガシーの VTP バージョンとは部分的に互換性があります。

このドキュメントでは、VLAN をプルーニングすることでフレームの不要なフラッディングが削減されるという利点を挙げました。**set vtp pruning enable コマンドを使用すると、VLAN が自動的にプルーニングされ、必要でない場所へのフレームの非効率的なフラッディングが停止されます。**手動での VLAN プルーニングとは異なり、自動プルーニングではスパニング ツリーの直径は制限されません。

CatOS 5.1 以降では、Catalyst スイッチは 1000 よりも大きい 802.1Q VLAN 番号を ISL VLAN 番号にマッピングできます。CatOS 6.x では、Catalyst 6500/6000 スイッチは IEEE 802.1Q 規格に従って 4096 個の VLAN をサポートします。これらの VLAN は次の 3 つの範囲に分けられており、その中の一部だけが、VTP に対応したネットワーク内のスイッチに伝達されます。

- 通常範囲 VLAN：1–1001
- 拡張範囲 VLAN：1025-4094（VTPv3でのみ伝播できる）
- 予約範囲 VLAN：0、1002 ~ 1024、4095

IEEE は、VTP と同じ結果を実現する標準ベースのアーキテクチャを作成しました。802.1Q Generic Attribute Registration Protocol（GARP）のメンバーとして、Generic VLAN Registration Protocol（GVRP）は異なるベンダー間における VLAN 管理の相互運用を可能にします。ただし、これはこのドキュメントの範囲外です。

**注**：CatOS 7.xでは、VTPをオフモードに設定するオプションが導入されトランスペアレントに非常に似たモードす。ただし、スイッチは VTP フレームを転送しません。これは、管理制御の範囲外にあるスイッチにトランキングするような設計の場合に役立つことがあります。

## 拡張 VLAN と MAC アドレス リダクション

MAC アドレス リダクション機能により、拡張範囲 VLAN の識別が可能になります。MAC アドレス リダクションを有効にすると、VLAN スパニング ツリーに使用される MAC アドレス プールが無効になり、1 つの MAC アドレスが残ります。スイッチは、この MAC アドレスで識別されます。CatOS ソフトウェア リリース 6.1(1) には、Catalyst 6500/6000 スイッチと Catalyst 4500/4000 スイッチに対する MAC アドレス リダクションのサポートが導入されており、IEEE 802.1Q 標準に準拠して 4096 個の VLAN がサポートされます。

### 動作の概要

スイッチ プロトコルでは、PVST+ 下で動作する VLAN のブリッジ ID の一部としてシャーシの EPROM によって提供される、使用可能なアドレスのバンクから取得される MAC アドレスが使用されます。Catalyst 6500/6000 スイッチおよび Catalyst 4500/4000 スイッチでは、シャーシ タイプに応じて 1024 個または 64 個の MAC アドレスがサポートされます。

1024 個の MAC アドレスを使用する Catalyst スイッチの場合、MAC アドレス リダクションはデフォルトでは有効になりません。MAC アドレスは連続的に割り当てられるため、範囲内の最初の MAC アドレスは VLAN 1 に割り当てられます。範囲内の 2 番目の MAC は VLAN 2 に割り当てられ、順次同様に割り当てられます。このため、それぞれが固有のブリッジ ID を使用する 1024 個の VLAN をスイッチがサポートできます。

| シャーシ タイプ | シャ |
| --- | --- |

| | ーシアドレス |
|---|---|
| WS-C4003-S1、WS-C4006-S2 | 1024 |
| WS-C4503、WS-C4506 | 64[1] |
| WS-C6509-E、WS-C6509、WS-C6509-NEB、WS-C6506-E、WS-C6506、WS-C6009、WS-C6006、OSR-7609-AC、OSR-7609-DC | 1024 |
| WS-C6513、WS-C6509-NEB-A、WS-C6504-E、WS-C6503-E、WS-C6503、CISCO7603、CISCO7606、CISCO7609、CISCO7613 | 64[1] |

1 64 個の MAC アドレスがあるスイッチでは MAC アドレス リダクションがデフォルトで有効になります。この機能を無効にすることはできません。

1024 個の MAC アドレスがある Catalyst シリーズ スイッチの場合、MAC アドレス リダクションを有効にすると、スイッチに必要な MAC アドレスの数を増やさずに、PVST+ 下で動作する 4096 個の VLAN をサポートしたり、Multiple Instance STP（MISTP）の 16 個のインスタンスに固有の ID を設定したりできます。MAC アドレス リダクションを使用すると、STP で必要な MAC アドレス数が、VLAN または MISTP インスタンスごとに 1 つから、スイッチごとに 1 つへと減少します。

次の図は、ブリッジ ID MAC アドレス リダクションが有効になっていない場合を示しています。ブリッジ ID は、2 バイトのブリッジ プライオリティと 6 バイトの MAC アドレスで構成されています。


MAC アドレス リダクションでは、BPDU の STP ブリッジ ID 部分が変更されます。元の 2 バイトのプライオリティ フィールドは 2 つのフィールドに分割されます。分割後、4 ビットのブリッジ プライオリティ フィールドと 0 から 4095 までの VLAN 番号を割り当てられる 12 ビットのシステム ID 拡張部分になります。


拡張範囲 VLAN を利用するために、Catalyst スイッチで MAC アドレス リダクションを有効にする場合は、同じ STP ドメイン内のすべてのスイッチで MAC アドレス リダクションを有効にします。この手順は、すべてのスイッチの STP ルート計算の一貫性を保つために必要です。MAC アドレス リダクションを有効にすると、ルート ブリッジのプライオリティは、4096 の倍数に VLAN ID を加えた値になります。MAC アドレス リダクションが設定されていないスイッチは、ブリッジ ID の選択精度が高くなるため、意図せずにルートになろうとすることがあります。

## 設定のガイドライン

拡張範囲 VLAN を設定する際には、特定のガイドラインに従う必要があります。スイッチは、内部使用の目的で、拡張範囲から VLAN のブロックを割り当てることができます。たとえば、スイッチは、ルーテッド ポートや Flex WAN モジュール用の VLAN を割り当てることができます。VLAN のブロックの割り当ては、常に VLAN 1006 から昇順に割り当てられます。Flex WAN モジュールが必要とする範囲内の VLAN がある場合、ユーザの VLAN エリアからは VLAN が割り当てられないため、必要なすべての VLAN が割り当てられなくなります。ユーザ割り当ての VLAN と内部使用の VLAN の両方を表示するには、**show vlan コマンドまたは show vlan summary コマンドをスイッチで発行します。**

```
>show vlan summary

Current Internal Vlan Allocation Policy - Ascending

Vlan status    Count  Vlans
-------------  -----  -----------------------------------------
VTP Active         7   1,17,174,1002-1005

Internal           7   1006-1011,1016
!--- These are internal VLANs. >show vlan
---- -------------------------------- --------- ------- --------

1    default                          active    7       4/1-48


!--- Output suppressed. 1006 Online Diagnostic Vlan1 active 0 internal 1007 Online Diagnostic
Vlan2 active 0 internal 1008 Online Diagnostic Vlan3 active 0 internal 1009 Voice Internal Vlan
active 0 internal 1010 Dtp Vlan active 0 internal 1011 Private Vlan Internal Vlan suspend 0
internal 1016 Online SP-RP Ping Vlan active 0 internal !--- These are internal VLANs.
```

さらに、拡張範囲 VLAN を使用する前に、802.1Q から ISL への既存のマッピングをすべて削除する必要があります。また、VTPv3 よりも前のバージョンでは、VTP VLAN 詳細については、VLAN の設定 [英語] の「*拡張範囲 VLAN の設定ガイドライン*」の項を参照してください。

**注：ソフ**トウェアリリース8.1(1)より前のソフトウェアでは、拡張範囲VLANのVLAN名を設定できません。この機能は、VTP のバージョンまたはモードに関係ありません。

## 推奨事項

同じ STP ドメイン内では、一貫性のある MAC アドレス リダクションの設定を維持するようにしてください。ただし、64 個の MAC アドレスが設定された新しいシャーシを STP ドメインに導入する場合、すべてのネットワーク デバイスで MAC アドレス リダクションを実施するのは現実的ではない場合があります。64 個の MAC アドレスがあるスイッチでは MAC アドレス リダクションがデフォルトで有効になっており、この機能を無効にすることはできません。同じスパニング ツリー プライオリティが 2 つのシステムに設定されている場合、MAC アドレス リダクションが設定されていないシステムのスパニング ツリー プライオリティの方が高くなることに注意してください。MAC アドレス リダクションを有効または無効にするには、次のコマンドを発行します。

```
set spantree macreduction enable | disable
```

内部 VLAN の割り当ては VLAN 1006 から昇順に行われます。ユーザ VLAN と内部 VLAN の競合

を避けるために、VLAN 4094 にできるだけ近いユーザ VLAN を割り当てます。Cisco IOS® システム ソフトウェアが稼働する Catalyst 6500 スイッチでは、内部 VLAN の割り当てを降順に設定できます。CatOS ソフトウェア用のコマンドライン インターフェイス（CLI）相当の機能は正式にはサポートされていません。

## 自動ネゴシエーション

### イーサネット/ファスト イーサネット

自動ネゴシエーションは IEEE ファスト イーサネット（FE）規格（802.3u）のオプション機能であり、デバイス間で**速度とデュプレックス**機能に関する情報をリンク経由で自動的に交換できます。自動ネゴシエーションはレイヤ 1（L1）で動作し、PC などの**一時的なユーザがネットワークに接続するアクセス レイヤ ポートを対象とします。**

### 動作の概要

10/100 Mbps イーサネット リンクでパフォーマンスの問題が発生する最も一般的な原因は、リンクの一方のポートが半二重で動作し、もう一方のポートが全二重で動作していることにあります。これは、リンクの一方または両方のポートがリセットされた後、両リンク パートナーの設定が自動ネゴシエーション プロセスによって同じに設定にならない場合にときどき発生します。また、管理者がリンクの一方を再設定しながら、他方の再設定を忘れた場合にも発生します。この場合の典型的な症状としては、スイッチでのフレーム チェック シーケンス、Cyclic Redundancy Check（CRC; 巡回冗長検査）、配置カウンタ、またはラント カウンタの増加があります。

自動ネゴシエーションについては、次のドキュメントで詳細に説明されています。次のドキュメントでは、自動ネゴシエーションの動作方法および設定オプションも説明されています。

- 「Configuring and Troubleshooting Ethernet 10/100Mb Half/Full Duplex Auto-Negotiation（イーサネット 10/100 Mb 半/全二重 自動ネゴシエーションの設定とトラブルシューティング）」
- 「Troubleshooting Cisco Catalyst Switches to NIC Compatibility Issues（Cisco Catalyst スイッチと NIC との互換性に関する問題のトラブルシューティング）」

自動ネゴシエーションでは、一方のリンク パートナーを 100 Mbps の全二重に手動で設定すれば、もう一方のリンク パートナーは全二重に自動ネゴシエーションされるものと一般に誤解されています。実際は、このように設定すると、デュプレックス ミスマッチが起こります。つまり、一方のリンク パートナーで自動ネゴシエーションが行われた結果、もう一方のリンク パートナーからの自動ネゴシエーション パラメータが認識されず、半二重にデフォルト設定されてしまいます。

ほとんどの Catalyst イーサネット モジュールでは 10/100 Mbps と半二重/全二重がサポートされており、この点は show port capabilities mod/port コマンドで確認できます。

### FEFI

自動ネゴシエーションが物理層およびシグナリング関連の障害から 100BASE-TX（銅線）を保護するのに対し、Far End Fault Indication（FEFI）は 100BASE-FX（ファイバ）およびギガビット インターフェイスを保護します。

**遠端障害は、TX ワイヤが外れている場合など、一方のステーションでは検出でき、もう一方では検出できない種類のリンク エラーです。**この例では、送信側ステーションは有効なデータを受信

し、リンク完全性モニタを通じてリンクが良好であることを検出できますが、自身が送信したデータが相手側ステーションで受信されていないことは検出できません。このようなリモート障害を検出した 100BASE-FX ステーションは、ネイバーにリモート障害を通知するために、送信された IDLE ストリームを修正して特別なビットパターン（FEFI IDLE パターンと呼ばれる）を送信できます。その後、FEFI-IDLE パターンによってリモート ポートのシャットダウンがトリガーされます（errdisable）。 障害保護の詳細については、このドキュメントの「UDLD」の項を参照してください。

FEFI は次のハードウェアとモジュールでサポートされています。

- Catalyst 5500/5000：WS-X5201R、WS-X5305、WS-X5236、WS-X5237、WS-U5538、WS-U5539
- Catalyst 6500/6000 および 4500/4000：すべての 100BASE-FX モジュールと GE モジュール

## 推奨事項

10/100 リンクで自動ネゴシエーションを設定するか、または速度とデュプレックスをハードコードするかは、リンク パートナーのタイプ、または Catalyst スイッチ ポートに接続したエンド デバイスのタイプによって最終的に決まります。エンド デバイスと Catalyst スイッチ間の自動ネゴシエーションは、通常は適切に動作し、Catalyst スイッチは IEEE 802.3u 仕様に準拠しています。ただし、NIC やベンダーのスイッチが厳密に準拠していない場合は、問題が生じることがあります。自動極性や配線の完全性など、10/100 Mbps 自動ネゴシエーションに関する IEEE 802.3u 仕様に規定されていないベンダー固有の拡張機能のために、ハードウェアの非互換性などの問題が生じることもあります。詳細については、Field Notice：Intel Pro/1000T NIC が CAT4K/6K に接続している場合のパフォーマンスの問題 [英語] を参照してください。

ホスト、ポート速度、およびデュプレックスの設定が必要になる状況があることを想定してください。一般には、次のトラブルシューティング手順に従います。

- リンクの両側で自動ネゴシエーションが設定されているか、または両側でハードコーディングが設定されていることを確認します。
- CatOS のリリース ノートを参照し、一般的な注意事項を確認します。
- NIC ドライバのバージョンや、実行しているオペレーティング システムのバージョンを確認します。最新のドライバやパッチが必要な場合があります。

原則として、リンク パートナーのタイプにかかわらず、最初は自動ネゴシエーションを使用してみます。ラップトップなどの一時的なデバイスのために自動ネゴシエーションを設定することには明らかな利点があります。理想的な環境では、自動ネゴシエーションは、サーバや固定ワークステーションなどの非一時的デバイス、スイッチ間、およびスイッチとルータ間でも適切に動作します。ただし、前述のような理由から、ネゴシエーションの問題が生じる場合があります。そのような場合は、記載されている TAC リンクの説明に従って基本的なトラブルシューティング手順を実行します。

10/100 Mbps イーサネット ポート上でポート速度を `auto` ポートを auto に設定するには、次のコマンドを発行します。

```
set port speed port range auto
!--- This is the default.
```

ポートをハードコーディングする場合は、次の設定コマンドを発行します。

**set port speed** *port range 10 | 100* **set port duplex** *port range full | half*

CatOS 8.3 以降では、オプションの **auto-10-100 キーワードが導入されています。**10/100/1000 Mbps の速度をサポートするポートで、1000 Mbps に自動ネゴシエーションされるのが望ましくない場合には、**auto-10-100 キーワードを使用します。auto-10-100 キーワードを使用すると、そのポートを、速度が auto** に設定されている 10/100 Mbps のポートと同様に動作させることができます。10/100 Mbps のポートだけに対して速度とデュプレックスがネゴシエートされ、1000 Mbps の速度はネゴシエーションの対象になりません。

**set port speed** *port_range* **auto-10-100**

## その他のオプション

スイッチ間で自動ネゴシエーションを使用しない場合は、ある種の問題に関する L1 障害表示も表示されなくなることがあります。アグレッシブ UDLD などの L2 プロトコルを使用すると、障害検出の強化に役立ちます。

# ギガビット イーサネット

ギガビット イーサネット（GE）の自動ネゴシエーション手順（IEEE 802.3z）は 10/100 Mbps イーサネットの手順よりも幅広い機能に対応しており、フロー制御パラメータ、リモート障害情報、およびデュプレックス情報の交換に使用されます（ただし、Catalyst シリーズの GE ポートでは全二重モードのみサポートされます）。

**注：**802.3zはIEEE 802.3:2000仕様に置き換えられました。詳細については、IEEE Standards On Line LAN/MAN Standards Subscription:アーカイブ 』を参照してください。

## 動作の概要

GE ポートのネゴシエーションはデフォルトで有効になっており、GE リンクの両端のポートで設定が同一である必要があります。FE とは異なり、リンクの両端のポートで自動ネゴシエーションの設定が異なっていると GE リンクがアップしません。ただし、自動ネゴシエーションが無効になっているポートでは、遠端から有効なギガビット シグナルを受信するだけでリンクがアップします。この動作は、遠端の自動ネゴシエーションの設定には依存しません。たとえば、A、B という 2 台のデバイスがあり、各デバイスの自動ネゴシエーションをイネーブルまたはディセーブルにできるとします。次の表は、可能な設定とそれぞれのリンク ステートを示しています。

| ネゴシエーション | B 有効 | B 無効 |
|---|---|---|
| A 有効 | up | A down、B up |
| A 無効 | A up、B down | up |

GE では、同期と自動ネゴシエーション（有効な場合）は、予約済みの特別なシーケンスのリンク コード ワードを使用して、リンクの起動時に実行されます。

**注：有効な**単語の辞書が存在し、すべての単語がGEで有効なわけではありません。

GE 接続のライフサイクルには、次のように表すことができます。


同期の損失とはリンク ダウンが MAC で検出されることを意味します。同期の損失は自動ネゴシエーションの有効/無効に関係なく適用されます。無効なワードを 3 回続けて受信するなど、特定の障害条件を満たすと同期が失われます。この状態が 10 ミリ秒間続くと、「sync fail」状態がアサートされて、リンクが `link_down` 同期が失われた後に再同期するためには、有効なアイドルが 3 回連続する必要があります。受信（Rx）信号の損失など、その他の壊滅的なイベントも link-down イベントの原因となります。

自動ネゴシエーションはリンクアップ プロセスの一部です。リンクがアップすると、自動ネゴシエーションは終了します。ただし、スイッチは引き続きリンクのステータスをモニタします。ポートの自動ネゴシエーションが無効になっている場合、「autoneg」フェーズは使用できなくなります。

GE 銅線仕様（1000BASE-T）では、Next Page Exchange による自動ネゴシエーションがサポートされています。Next Page Exchange では、10/100/1000 Mbps の速度の自動ネゴシエーションを銅線ポートで実行できます。

**注：GEファイバ**仕様では、デュプレックス、フロー制御、およびリモート障害検出のネゴシエーションの規定のみが規定されています。GE ファイバ ポートでは、ポート速度のネゴシエーションは行われません。自動ネゴシエーションについての詳細は、IEEE 802.3-2002 仕様のセクション 28 と 37 を参照してください。

同期の再起動遅延は、自動ネゴシエーションの合計時間を制御するソフトウェア機能です。この時間内に自動ネゴシエーションが正常に行われず、デッドロックが存在する場合、ファームウェアにより自動ネゴシエーションが再起動されます。set port sync-restart-delay コマンドが有効なのは、自動ネゴシエーションが enable に設定されている場合だけです。

## 推奨事項

自動ネゴシエーションの有効化は、10/100 環境の場合よりも GE 環境においてはるかに重要です。実際には、ネゴシエーションをサポートしていないデバイスに接続されたスイッチ ポート、または相互運用性の問題が原因で接続の問題が生じているスイッチ ポートでのみ自動ネゴシエーションを無効にする必要があります。シスコでは、すべてのスイッチ間リンクおよび通常はすべての GE デバイスでギガビット ネゴシエーションを有効（デフォルト）にすることを推奨しています。自動ネゴシエーションを有効にするには、次のコマンドを発行します。

```
set port negotiation port range enable
!--- This is the default.
```

既知の例外の 1 つは、リリース 12.0(10)S（フロー制御と自動ネゴシエーションが追加されたリリース）より前の Cisco IOS ソフトウェアを実行中のギガビット スイッチ ルータに接続している場合です。この場合はこれら 2 つの機能をオフにします。そうしないと、スイッチ ポートでは `not connected` と報告され、GSR ではエラーが報告されます。次にコマンド シーケンスの例を示します。

**set port flowcontrol receive** *port range* **off set port flowcontrol send** *port range* **off set port negotiation** *port range* **disable**

スイッチとサーバ間の接続はケースバイケースで対応する必要があります。シスコのお客様からは、Sun、HP、および IBM サーバでギガビット ネゴシエーションに関する問題が報告されています。

## その他のオプション

フロー制御は 802.3x 仕様のオプション部分ですが、使用する場合はネゴシエーションする必要があります。デバイスは、PAUSE **既知の MAC 01-80-C2-00-00-00 0F** ）の送信や応答に対応している場合と対応していない場合があります。 また、遠端のネイバーのフロー制御要求には同意できません。入力バッファが一杯になりそうなポートからそのリンク パートナーに PAUSE これで定常状態のオーバーサブスクリプション問題が解決されることはありませんが、バースト時にはパートナーの出力バッファの一部分だけで入力バッファを効率的に拡張できます。

この機能は、アクセスポートとエンド ホスト間のリンクで使用するのが最も有効で、エンド ホストの出力バッファを最大で仮想メモリと同じサイズまで拡張できます。スイッチ間で使用しても限られたメリットしかありません。

スイッチ ポートでこの制御を行うには、次のコマンドを発行します。

**set port flowcontrol** *mod/port receive | send off |on | desired*

>**show port flowcontrol**

| Port | Send FlowControl admin | Send FlowControl oper | Receive FlowControl admin | Receive FlowControl oper | RxPause | TxPause |
|---|---|---|---|---|---|---|
| 6/1 | off | off | on | on | 0 | 0 |
| 6/2 | off | off | on | on | 0 | 0 |
| 6/3 | off | off | on | on | 0 | 0 |

**注：ネゴシエートさ**れた場合、すべてのCatalystモジュールがPAUSEムに応答します。WS-X5410 や WS-X4306 などの一部のモジュールはノンブロッキング モジュールであるため、送信するようにネゴシエートされている場合でも、PAUSE

# ダイナミック トランキング プロトコル

## カプセル化タイプ

トランクでは、元のイーサネット フレームを一時的に識別してタグ付けし ( リンクローカル ) 、それらのフレームを単一リンク上で多重化できるようにすることで、デバイス間の VLAN が拡張されます。これにより、独立した複数の VLAN ブロードキャスト ドメインとセキュリティ ドメインがスイッチ間で確実に維持されます。スイッチ内部では、CAM テーブルによってフレームと VLAN のマッピングが保持されます。

トランキングは、ATM LANE、FDDI 802.10、イーサネットなどの各種 L2 メディアでサポートさ

れています。ただし、ここではイーサネットについてのみ説明しています。

## ISL の動作概要

長年、シスコ独自の識別またはタギング方式である ISL が使用されてきましたが、現在では 802.1Q IEEE 規格も使用できます。

元のフレームを 2 レベルのタギング方式で完全にカプセル化することから、ISL は事実上トンネリング プロトコルであり、非イーサネット フレームを伝送できるという付加的な利点もあります。ISL では標準のイーサネット フレームに 26 バイトのヘッダーと 4 バイトの FCS が追加されます。つまり、トランクとして設定されたポートでは、標準よりも大きいイーサネット フレームが到達して処理されます。ISL は 1024個 の VLAN をサポートします。

### ISL フレーム形式

| 40 ビット | 4 ビット | 4 ビット | 48 ビット | 16 ビット | 24 ビット | 24 ビット | 15 ビット | ビット | 16 ビット | 16 ビット | 可変長 | 32 ビット |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 着信アドレス | Type | ユーザ | SA | LEN | SNAP LLC | HSA | VLAN | BPDU | インデックス | 予約 | カプセル化フレーム | FCS |
| 01-00-0c-00-00 | | | | | AAAA03 | 000000C | | | | | | |

詳細については、『スイッチ間リンクと IEEE 802.1Q のフレーム形式』を参照してください。

## 802.1Q の動作概要

IEEE 802.1Q 規格では、カプセル化タイプだけではなく、スパニング ツリーの拡張機能、GARP ( このドキュメントの「VTP」の項を参照 )、802.1p Quality of Service ( QoS ) タギングなどが規定されています。

802.1Q フレーム形式では元のイーサネット送信元アドレスと宛先アドレスが保持されます。一方、スイッチは、ホストが QoS シグナリングの 802.1p ユーザ プライオリティを示すためにタギングを使用できるアクセス ポートの場合でも、ベビー ジャイアント フレームの受信を想定する必要があります。タグは 4 バイトなので、802.1Q イーサネット v2 フレームは 1522 バイトになります。これは IEEE 802.3ac ワーキング グループが決めたものです。802.1Q では、4096 個の VLAN に対応する番号領域もサポートされています。

送受信されるすべてのデータ フレームには、ネイティブ VLAN 上のフレームを除き、802.1Q タグが付けられます ( ネイティブ VLAN には、入力スイッチ ポートの設定に基づく暗黙的なタグがあります )。 ネイティブ VLAN 上のフレームは常にタグなしで送信され、通常はタグなしで受信されますが、タグ付きで受信される場合もあります。

詳細については、『IEEE 802.10 による VLAN の標準化』または『Get IEEE 802』 を参照してください。

### 802.1Q/801.1p フレーム形式

| | | タグ ヘッダー | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | TPID | TCI | | | | | |
| 48 ビット | 48 ビット | 16 ビット | 3 ビット | 1 ビット | 12 ビット | 16 ビット | 可変長 | 32 ビット |
| DA | SA | TPID | 優先順位 | CFI | VLAN ID | 長さ/タイプ | データ（PAD を含む） | FCS |
| | | 0x8100 | 0 ~ 7 | 0 ~ 1 | 0 ~ 4095 | | | |

## 推奨事項

最近のハードウェアではすべて 802.1Q がサポートされているため（Catalyst 4500/4000 シリーズや CSS 11000 などは 802.1Q のみサポート）、新しく実装する場合はすべて IEEE 802.1Q 規格に準拠して、古いネットワークを ISL から徐々に移行することを推奨します。

IEEE 規格では異なるベンダーの相互運用が可能です。新しいホストの 802.1p 対応の NIC やデバイスが使用可能になるため、この点はすべてのシスコ環境に利点をもたらします。ISL と 802.1Q の実装はどちらも成熟していますが、最終的には IEEE 規格の方が現場で広く利用されるようになり、サードパーティによるネットワーク アナライザなどのサポートも IEEE 規格が中心になると考えられます。802.1Q のカプセル化のオーバーヘッドは ISL に比べて小さいため、802.1Q の小さな利点として挙げられます。

カプセル化タイプは DTP を使用してスイッチ間でネゴシエートされます。両端で ISL がサポートされている場合はデフォルトで ISL が選択されるため、次のコマンドを発行して dot1q を指定する必要があります。

```
set trunk mod/port mode dot1q
```

このドキュメントの「インバンド管理」の項で説明されているように、トランクから VLAN 1 が削除されると、ユーザ データは送受信されなくなりますが、CDP や VTP などの制御プロトコルは、NMP によって引き続き VLAN 1 で転送されます。

また、このドキュメントの「VLAN 1」の項で説明されているように、CDP、VTP、および PAgP パケットは、トランキングされている場合は常に VLAN 1 で送信されます。dot1q カプセル化を使用している場合に、スイッチのネイティブ VLAN が変更されると、これらの制御フレームは VLAN 1 でタグ付けされます。ルータへの dot1q トランキングが有効で、スイッチのネイティブ VLAN が変更されている場合、タグ付き CDP フレームを受信し、ルータに CDP ネイバーの可視

性を提供するために、VLAN 1 にサブインターフェイスが必要になります。

**注**：dot1qには、ネイティブVLANの暗黙的なタギングが原因で発生するセキュリティ上の問題が存在する可能性があります。これは、あるVLANから別のVLANにルータなしでフレームを送信できるためです。詳細については、Are there Vulnerabilities in VLAN Implementations? を参照してください。この問題を回避するには、エンド ユーザ アクセスに使用していない、トランクのネイティブ VLAN の VLAN ID を使用します。シスコのお客様のほとんどは、トランクのネイティブ VLAN を VLAN 1 のままとし、アクセス ポートを VLAN 1 以外の VLAN に割り当てることで簡単にこの問題を解決しています。

## トランキング モード

DTP は Dynamic ISL（DISL）の第 2 世代で、ISL フレームや 802.1Q フレームの送信に関係する各種パラメータ（設定済みのカプセル化タイプ、ネイティブ VLAN、ハードウェア機能など）を、トランクの両端にあるスイッチ間で一致させるために存在します。また、ポートとそのネイバーが一貫性のある状態を保つようにすることで、重大なセキュリティ リスクになり得る、非トランク ポートからのタグ付きフレームのフラッディングに対する保護の役割を果たします。

## 動作の概要

DTP は、スイッチ ポートとそのネイバーとの間で設定パラメータをネゴシエートする L2 プロトコルです。別のマルチキャストMACアドレス(**01-00-0c-cc-cc-cc**)とSNAPプロトコルタイプ0x2004を使用します。次の表に、コンフィギュレーションモードの要約を示します。

| **モード** | **機能** | **DTP フレーム送信** | **最終状態（ローカル ポート）** |
|---|---|---|---|
| `Auto` | ポートは自発的にリンクをトランクに変換しようとします。隣接ポートが `on desirable` | 送信する、定期的 | トランキング |
| | ポートを永続的なトランキング モードにし、リンクをトランクに変換するようにネゴシエートします。隣接ポートが変更に同意しなくても、ポートはトランク ポートになります。 | 送信する、定期的 | トランキング、**無条件** |
| `Nonegotiate` | ポートは常にトランキング モードになりますが、DTP フレームを生成しません。トランク リンクを確立するには、ネイバー ポートを手動でトランク ポートとして設定する必要があります。これはデバイスが DTP をサポートしていない場合に役立ちます。 | No | トランキング、**無条件** |
| `Desi` | リンクからトランク リンクへの変換をポートに積極的に試行させます。隣接ポートが | 送信する、定期的 | リモート モードが `on`、 |

| | | | |
|---|---|---|---|
| rable | on、desirable、または auto | | auto、または desirable の場合のみ、トランキング状態になります。 |
| | ポートは常に非トランキング モードになり、リンクを非トランク リンクに変換するかどうかをネゴシエートします。近接ポートが変更に同意しなかった場合でも、ポートは非トランク ポートになります。 | 定常状態では送信しない。ただし、on からの変更後、リモート エンドでの検出を迅速化するために通知を送信する。 | 非トランキング |

このプロトコルには次のような特徴があります。

- DTP ではポイントツーポイント接続が前提となっており、シスコ デバイスではポイントツーポイントの 802.1Q トランク ポートのみサポートしています。
- DTP ネゴシエーションの間、ポートは STP に参加しません。ポートは、3 つの DTP タイプ（access、ISL、802.1Q）のいずれかになって初めて STP に追加されます。PAgP が設定されている場合、ポートが STP に参加する前に実行されるプロセスは PAgP です。
- ポートが ISL モードでトランキングしている場合、DTP パケットは VLAN 1 に送出されます。それ以外の場合（802.1Q トランキングまたは非トランキング ポートの場合）はネイティブ VLAN に送出されます。
- desirable DTP VTP **admin status** を転送します。
- メッセージは、ネゴシエーション中は 1 秒ごとに送信され、その後は 30 秒ごとに送信されます。
- on、nonegotiate、および off 不適切な設定は、一方がトランキングで、もう一方がトランキングでないという、整合性のない危険な状態につながるおそれがあります。
- on、auto、または desirable DTP auto desirable DTP 5

ISL の詳細については、Catalyst 5500/5000 および 6500/6000 ファミリ スイッチでの ISL トランキングの設定 [英語] を参照してください。802.1Q の詳細については、Cisco CatOS システム ソフトウェアによる 802.1Q カプセル化を使用した Catalyst 4500/4000、5500/5000、および 6500/6000 シリーズ スイッチ間のトランキング [英語] を参照してください。

## 推奨事項

シスコではリンクの両端でトランク設定を明示的に desirable このモードでは、on syslog on また、desirable desirable

**set trunk** *mod/port* **desirable** *ISL* | *dot1q*

**注：トランク**ル以外のすべてのポトランクをオフに設定します。こうすれば、ホスト ポートが起動するときに無駄なネゴシエーション時間を費やさずに済みます。このコマンドは、[set port host コマンドを使用した場合にも実行されます。](#)詳細については、「[STP」の項を参照してください。](#)特定範囲のポートでトランクを無効にするには、次のコマンドを発行します。

```
set trunk port range off
!--- Ports are not trunking; part of the set port host command.
```

### その他のオプション

お客様がよく使用されるその他の設定として、ディストリビューション レイヤでのみ `desirable auto`

Catalyst 2900XL などの一部のスイッチ、Cisco IOS ルータ、または他のベンダーのデバイスでは現在、DTP によるトランク ネゴシエーションはサポートされていません。Catalyst 4500/4000、5500/5000、および 6500/6000 スイッチで `nonegotiate` また、`nonegotiate`

**注：チャネ**ルモードやSTPの設定などの要因も、初期化時間に影響を与える可能性があります。

`nonegotiate`

```
set trunk mod/port nonegotiate ISL | dot1q
```

ブリッジングを実行しているときに、**on モードで受信した DTP フレームの一部がトランク ポートに戻される場合があるので、Cisco IOS ルータに接続している場合は** `nonegotiate` DTP フレームを受信すると、スイッチ ポートは不必要な再ネゴシエートを試みます（つまり、トランクがいったんダウンして再度アップします）。`nonegotiate` `DTP`

## スパニング ツリー プロトコル

### 基本的な注意事項

スパニング ツリー プロトコル（STP）は、冗長なスイッチド ネットワークおよびブリッジ型ネットワークにおいてループのない L2 環境を維持します。STP がないと、フレームは無限に増加しながらループし続け、その結果、大量のトラフィックによってブロードキャスト ドメイン内のすべてのデバイスで絶えず割り込みが発生し、ネットワークがメルトダウンします。

STP は当初ソフトウェアベースの低速なブリッジ仕様（IEEE 802.1d）のために開発された、成熟したプロトコルという側面がありますが、その一方で、多数の VLAN が存在し、ドメイン内に多くのスイッチが配置されていて、マルチベンダー サポートや新しい IEEE 拡張機能も取り込んだ大規模なスイッチ ネットワークでも十分に実装できる複雑さも兼ね備えています。

今後の参考のために述べると、CatOS 6.x には、MISTP、ループガード、ルートガード、BPDU 到達時間のスキュー検出などの STP の新機能が今後も追加されます。また、CatOS 7.x では、IEEE 802.1s 共有スパニング ツリーや IEEE 802.1w 高速コンバージェンス スパニング ツリーなどの今後標準化されるプロトコルが使用可能になります。

### 動作の概要

VLAN ごとに、最も小さいルート ブリッジ ID（BID）のスイッチがルート ブリッジとして選択されます。 BID は、ブリッジ プライオリティとスイッチの MAC アドレスを組み合わせたものです。

最初にすべてのスイッチから BPDU が送信されます。BPDU には各スイッチの BID とそのスイッチに到達するためのパス コストが含まれています。これで、ルート ブリッジとルートへの最小コスト パスを決定できます。ネットワーク全体で一致したタイマーを使用するため、ルートからの BPDU で伝送された設定パラメータによってローカルに設定されたパラメータが上書きされます。

続いて、次の手順でトポロジの統合が行われます。

1. スパニング ツリー ドメイン全体で 1 つのルート ブリッジが選択されます。
2. すべての非ルート ブリッジでルート ポート（ルート ブリッジに面するポート）が 1 つ選択されます。
3. すべてのセグメントで、BPDU を転送するための指定ポートが 1 つ選択されます。
4. 非指定ポートがブロッキング ステートになります。

詳細については、スパニング ツリーの設定 [英語] を参照してください。

| 基本タイマーのデフォルト（秒） | [名前(Name)] | 機能 |
|---|---|---|
| 0 | Hello | BPDU の送信を制御します。 |
| 15 | Forward DelayFwddelay | ポートがリスニングまたはラーニング ステートにとどまる時間を制御し、トポロジ変更プロセスに影響を与えます（次の項を参照）。 |
| 20 | Max age | スイッチが代替パスの検索を始める前に、現在のトポロジを維持する時間を制御します。Maxage 秒を経過すると、BPDU は古いと見なされ、スイッチはブロッキング ポートのプールから新しいルート ポートを探します。使用可能なブロックされたポートがない場合、スイッチは指定ポートで自身がルートになることを宣言します。 |

| ポートステート | 意味 | 次の状態に移行するデフォルトのタイミング |
|---|---|---|
| Disabled | 管理上ダウンされています。 | N/A |

| | | |
|---|---|---|
| | BPDU を受信する。ユーザ データは転送しない。 | BPDU の受信をモニタします。Maxage が期限切れになるまで 20 秒待ちます。直接リンクまたはローカル リンク障害が検出された場合は即座に変更されます。 |
| | BPDU を送受信し、ブロッキング ステートに戻る必要があるかをチェックする。 | Fwddelay タイマー ( 15 秒待機 ) |
| | トポロジおよび CAM テーブルが構築されます。 | Fwddelay タイマー ( 15 秒待機 ) |
| | データを送受信します。 | |
| | **基本的なトポロジ変更に要する時間の合計 :** | **Maxage が期限切れになるまで待つ場合は 20 + 2 ( 15 ) = 50 秒。直接リンク障害の場合は 30 秒** |

STP の BPDU には、コンフィギュレーション BPDU とトポロジ変更通知 ( TCN ) BPDU の 2 種類があります。

## コンフィギュレーション BPDU のフロー

コンフィギュレーション BPDU は、スパニング ツリーの状態を維持するために、Hello インターバルごとにルート ブリッジのすべてのポートから発信され、すべてのリーフ スイッチに渡されます。定常状態では、BPDU フローは単方向です。つまり、ルート ポートとブロッキング ポートはコンフィギュレーション BPDU を受信するだけで、指定ポートはコンフィギュレーション BPDU を送信するだけです。

ルートからの BPDU がスイッチで受信されるたびに、新しい BPDU が Catalyst の中央 NMP で処理され、ルート情報を含んだ状態で送信されます。つまり、ルート ブリッジが失われた場合、またはルート ブリッジへのすべてのパスが失われた場合、( maxage タイマーによる再選択が開始されるまで ) BPDU の受信が停止します。

## TCN BPDU のフロー

TCN BPDU は、スパニング ツリーでトポロジの変更が検出されると、リーフ スイッチから発信され、ルート ブリッジに向けて送信されます。ルート ポートは TCN を送信するだけで、指定ポートは TCN を受信するだけです。

TCN BPDU はルート ブリッジに向かって進み、各ステップで確認応答されるため、これは信頼性の高いメカニズムです。TCN BPDU がルート ブリッジに到達すると、ルート ブリッジは TCN フラグが `maxage + fwddelay 35 BPDU` これにより、すべてのスイッチで通常のCAMエージングタイムが5分（デフォルト）から`fwddelay15`れます。 詳細については、スパニング ツリー プロトコル トポロジの変更について [英語] を参照してください。

## スパニング ツリーのモード

VLAN をスパニング ツリーと関連付ける方法には次の 3 つの方法があります。

- すべての VLAN で 1 つのスパニング ツリーを実行する、つまりモノ スパニング ツリー プロトコル（IEEE 802.1Q など）
- VLAN ごとに 1 つのスパニング ツリーを実行する、つまり共有スパニング ツリー（Cisco PVST など）
- 一連の VLAN ごとに 1 つのスパニング ツリーを実行する、つまりマルチ スパニング ツリー（Cisco MISTP や IEEE 802.1s など）

すべての VLAN に対してモノ スパニング ツリーを実行すると、アクティブなトポロジが 1 つだけになるため、ロード バランシングは行われません。STP のブロックされたポートはすべての VLAN をブロックし、データを伝送しません。

VLAN ごとに 1 つのスパニング ツリーを実行すると、ロード バランシングは可能になりますが、VLAN の数が増えるに従って BPDU に必要な CPU 処理も増えます。CatOS リリース ノートに、スイッチごとにスパニング ツリーで推奨される論理ポートの数についてのガイダンスが記載されています。たとえば、Catalyst 6500/6000 Supervisor Engine 1 での公式は次のとおりです。

ポートの数 + ( トランクの数 X トランク上の VLAN の数 ) < 4000

Cisco MISTP と新しい 802.1s 規格では、アクティブな STP インスタンスまたはトポロジを 2 つだけ定義し、すべての VLAN を 2 つのツリーのどちらかにマッピングできます。この手法を使用すると、ロード バランシングを有効にしながら、STP を何千もの VLAN に拡張できます。

## BPDU のフォーマット

IEEE 802.1Q 規格をサポートするために、既存の Cisco STP 実装が拡張され、IEEE 802.1Q モノ スパニング ツリー領域にわたるトンネリングのサポートが追加されて PVST+ になりました。そのため、PVST+ は、IEEE 802.1Q MST プロトコルと Cisco PVST プロトコルの両方と互換性があり、特別なコマンドや設定は必要ありません。また、PVST+ には、スイッチ間でポート トランキングと VLAN ID の設定が一致していることを保証する検証メカニズムがあります。

PVST+ プロトコルの動作には、次のような特徴があります。

- PVST+ は、802.1Q トランク上のいわゆる Common Spanning Tree（CST）を通じて 802.1Q モノ スパニング ツリーと相互運用できます。CST は常に VLAN 1 にあるため、他のベンダーと相互運用するためにはトランク上でこの VLAN を有効にする必要があります。CST BPDU は、常にタグなしで IEEE 標準ブリッジグループ（MAC アドレス 01-80-c2-00-00-00、DSAP 42、SSAP 42）に送信されます。 完全を期すために付け加えると、BPDU のパラレル セットが VLAN 1 の Cisco Shared Spanning Tree MAC アドレスにも送信されます。
- PVST+ では、802.1Q VLAN 領域全体で PVST BPDU がマルチキャスト データとしてトンネリングされます。Cisco Shared Spanning Tree BPDU は、トランク上の VLAN ごとに MAC アドレス 01-00-0c-cc-cc-cd（SNAP HDLC プロトコル タイプ 0x010b）に送信されます。BPDU はネイティブ VLAN ではタグなしで、その他すべての VLAN ではタグ付きです。
- PVST+ はポートと VLAN の不一致をチェックします。PVST+ は転送ループを避けるために、一致しない BPDU を受信したポートをブロックします。また、設定の不一致が見つかった場合は、syslog メッセージでユーザに通知します。
- PVST+ は、ISL トランクで PVST を実行している既存の Cisco スイッチと下位互換性があります。ISL によってカプセル化された BPDU は、通常どおり IEEE MAC アドレスを使用して送受信されます。つまり、各 BPDU タイプはリンクローカルであり、変換の問題は発生しま

せん。

## 推奨事項

Catalyst スイッチはすべて、デフォルトで STP が有効になります。これは、L2 ループを含めない設計を選択したために、ブロックされたポートがアクティブに維持されるという意味で STP が有効でない場合でも推奨されます。

```
set spantree enable all
!--- This is the default.
```

シスコでは、次のような理由から STP を有効にしておくことを推奨しています。

- パッチのミスやケーブル不良などによってループが発生した場合、STP により、マルチキャスト データやブロードキャスト データによってネットワークに悪影響が生じるのを防ぐことができます。
- EtherChannel の障害に対する保護。
- STP はほとんどのネットワークで設定されているため、現場で広く利用されています。広く利用されるのは、コードが安定しているからです。
- 二重接続された NIC の動作不良（またはサーバ上で有効になっているブリッジング）に対する保護。
- PAgP、IGMP スヌーピング、トランキングなど、多くのプロトコルのソフトウェアは STP と密接に関係しているため、STP を無効にした状態で実行すると、望ましくない結果が生じることがあります。

**安定性に悪影響を及ぼすことがあるため、タイマーは変更しないでください。**展開されているネットワークのほとんどは調整されていません。コマンド ラインからアクセス可能な Hello インターバルや Maxage などの単純な STP タイマーはそれ自体、その他の装備された組み込みタイマーを複雑に組み合わせて構成されています。そのため、すべての影響を考慮しながらタイマーを調整するのは困難です。さらに、UDLD による保護の効果が失われるおそれがあります。

**ユーザ トラフィックと管理 VLAN を分離するのが理想的です。**特に古い Catalyst スイッチ プロセッサでは、管理 VLAN をユーザ データから切り離すことで、STP に関する問題を回避するのが最善です。正常に動作しない 1 台のエンド ステーションからのブロードキャスト パケットによってスーパバイザ エンジン プロセッサがビジー状態になり、1 つまたは複数の BPDU が失われる可能性があります。ただし、より強力な CPU を搭載し、スロットリングを制御できる新しいスイッチを使用すれば、この問題は緩和されます。詳細については、このドキュメントの「インバンド管理」の項を参照してください。

**冗長性を過剰に設計しないでください。**結果的に、大量のブロッキング ポートにより長期的な安定性に悪影響が生じる、トラブルシューティングの悪夢につながることがあります。**SPT 全体の直径は 7 ホップ未満にしてください。**可能な場合は、設計時にはシスコのマルチレイヤ モデルに基づき、より小さいスイッチド ドメイン、STP トライアングル、および確定的なブロックされたポートを使用してください（ギガビット キャンパス ネットワーク設計：基本方針とアーキテクチャ [英語] を参照）。

**ルート機能とブロックされたポートの位置を動かして把握し、それらの位置をトポロジ図に記入してください。**STP のトラブルシューティングはブロックされたポートから始まります。多くの場合、ポートがブロッキング ステートからフォワーディング ステートに変わった理由が根本原因の分析の重要な部分となります。**ルートまたはセカンダリ ルートの位置にはディストリビューション レイヤとコア レイヤを選択してください。**これは、これらのレイヤがネットワークの最も安

定した部分だと考えられているためです。L2 データ転送パスに最適な L3 および HSRP のオーバーレイを確認します。次のコマンドは、ブリッジ プライオリティを設定するためのマクロです。root を指定すると、ブリッジ プライオリティがデフォルト（32768）よりもはるかに小さい値に設定され、root secondary を指定すると、デフォルトよりも適度に小さい値に設定されます。

```
set spantree root secondary vlan range
```

**注：このマクロはルート プライオリティを 8192（デフォルト）、現在のルート プライオリティ - 1（別のルート ブリッジがわかっている場合）、または現在のルート プライオリティ（自身の MAC アドレスが現在のルートよりも小さい場合）のいずれかに設定します。**

**不要な VLAN をトランク ポートからプルーニングしてください**（双方向で実施）。プルーニングすることで STP の直径が制限され、特定の VLAN を必要としないネットワーク部分で NMP 処理のオーバーヘッドが小さくなります。VTP の自動プルーニングでは、STP はトランクから削除されません。詳細については、このドキュメントの「VTP」の項を参照してください。CatOS 5.4 以降を使用している場合、デフォルトの VLAN 1 もトランクから削除できます。

詳細については、『スパニング ツリー プロトコルの問題点と設計上の考慮事項』を参照してください。

## その他のオプション

シスコには VLAN ブリッジという別の STP もあります。このプロトコルは、宛先 MAC アドレス **01-00-0c-cd-cd-ce、およびプロトコル タイプ 0x010c を使用して動作します。**

これは、VLAN で実行されている IEEE スパニング ツリー インスタンスの動作を妨げることなく、それらの VLAN 間でルーティング不能プロトコルやレガシー プロトコルをブリッジする必要がある場合に最も役立ちます。非ブリッジ トラフィック用の VLAN インターフェイスで L2 トラフィックがブロックされるようになると（これは、VLAN インターフェイスが IP VLAN と同じ STP に参加している場合は容易に発生します）、オーバーレイしている L3 トラフィックも誤ってプルーニングされます。これは望ましくない副作用です。そのため、VLAN ブリッジはブリッジ プロトコルの STP とは異なるインスタンスになっており、IP トラフィックに影響を与えずに操作できる別のトポロジが提供されます。

シスコでは、MSFC などのシスコ ルータで VLAN 間のブリッジングが必要な場合に、VLAN ブリッジを実行することを推奨しています。

## ポートファスト

PortFast を使用すると、アクセス ポート上での通常のスパニング ツリーの動作がバイパスされるため、エンド ステーションと、リンクの初期化後にエンド ステーションが接続する必要があるサービス間の接続時間が短縮されます。IPX/SPX などの一部のプロトコルでは、GNS 問題を回避するために、リンク ステートがアップになった直後にアクセス ポートがフォワーディング モードになっていることが重要です。

詳細については、PortFast と他のコマンドを使用したワークステーションの接続始動遅延の修復 [英語] を参照してください。

## 動作の概要

PortFast では、リンクが稼働中であることが確認された後、ポートを STP この機能が有効になっていない場合、ポートが STP これには、ForwardDelay 2 30

PortFast モードには、ポート状態がに移行するたびに STP TCN が生成されるのを防ぐ効果もあります。TCN 自体は問題ではありませんが、TCN の波がルート ブリッジに押し寄せると（朝に人々が一斉に PC の電源を入れた場合など）、コンバージェンス時間が不必要に長くなることがあります。

STP PortFast は、マルチキャスト CGMP ネットワークと Catalyst 5500/5000 MLS ネットワークでは特に重要です。これらの環境では、TCN が原因で静的な CGMP CAM テーブル エントリがエージ アウトし、その結果、次の IGMP レポートまでマルチキャスト パケットが失われる可能性があります。また、その後再構築される必要がある MLS キャッシュ エントリがフラッシュされ、キャッシュのサイズによってはルータの CPU スパイクが発生することがあります（Catalyst 6500/6000 の MLS 実装と、IGMP スヌーピングから学習したマルチキャスト エントリは影響を受けません）。

## 推奨事項

シスコでは、すべてのアクティブなホスト ポートに対しては STP PortFast を有効にし、スイッチ間リンクおよび未使用のポートに対しては無効にすることを推奨しています。

トランキングとチャネリングも、すべてのホスト ポートで無効にする必要があります。各アクセス ポートではトランキングとチャネリングがデフォルトで有効になっていますが、ホスト ポートでは設計上、スイッチのネイバーは想定されていません。これらのプロトコルをネゴシエートする設定のままにしておくと、ポートがアクティブになるまでの遅延によって、ワークステーションからの初期パケット（DHCP 要求など）が転送されないという望ましくない状況が発生する可能性があります。

CatOS 5.2 では、マクロ コマンド set port host port range が導入されています。このコマンドはアクセス ポートに次の設定を実装し、自動ネゴシエーションと接続のパフォーマンスを大幅に向上させます。

```
set port host port range
!--- Macro command for these commands: set spantree portfast port range enable set trunk port
range off set port channel port range mode off
```

**注：PortFastは、スパニングツリーがそれらのポートで実行されていないことを意味しません。** BPDU は通常どおり送受信されて、処理されます。

## その他のオプション

PortFast BPDU ガード機能は、非トランキング ポートで BPDU を受信した場合にそのポートを errdisable

PortFast に設定されたアクセス ポートでは、BPDU パケットを受信できません。これは、ホストポートはスイッチに接続できないためです。BPDU が確認される場合は、設定が無効で危険を秘めていることを示しており、管理上の対処が必要となります。BPDU ガード機能を有効にすると、BPDU を受信する PortFast が設定されたインターフェイスは、STP の

次のコマンドはポート単位ではなく、スイッチ単位で機能します。

```
set spantree portfast bpdu-guard enable
```

ポートがダウンした場合は、SNMP トラップまたは syslog メッセージによってネットワーク管理者に通知されます。errdisabled ポートに対して自動回復時間を設定することもできます。詳細については、このドキュメントの「UDLD」の項を参照してください。詳細については、『スパニング ツリー PortFast BPDU ガード機能拡張』を参照してください。

**注：トランクポートの**PortFastはCatOS 7.xで導入されました。以前のリリースでは、トランクポートには影響しません。トランク ポート用の PortFast は、L3 ネットワークのコンバージェンス時間が長くなるように設計されています。この機能を補完するため、CatOS 7.x では PortFast BPDU ガードをポート単位で設定する機能も導入されています。

## UplinkFast

UplinkFast は、ネットワーク アクセス レイヤで直接リンク障害が発生したときに、迅速な STP コンバージェンスを実現します。UplinkFast では STP は変更されません。その目的は、通常は 30 秒かかるコンバージェンス時間を、特定の環境において 3 秒未満に短縮することにあります。詳細については、『UplinkFast 機能の説明と設定』を参照してください。

## 動作の概要

アクセス レイヤでシスコのマルチレイヤ設計モデルを使用すると、フォワーディング アップリンクが失われた場合、ブロッキング アップリンクは

アップリンク グループは VLAN 単位のポートのセットで、ルート ポートおよびバックアップ ルート ポートと見なすことができます。通常の状態では、ルート ポートはアクセスからルートへの接続を確立しています。何らかの理由でこのプライマリ ルート接続に障害が発生した場合、通常の 30 秒間のコンバージェンス遅延なしに、即時にバックアップ ルート リンクが使用可能になります。

このため、通常の STP トポロジ変更処理プロセス（ ）が事実上バイパスされるので、代わりのトポロジ修正メカニズムを使用して、ローカル エンド ステーションが代替パスを介して到達できるドメイン内のスイッチをアップデートする必要があります。また、UplinkFast を実行しているアクセス レイヤ スイッチは、CAM 内の MAC アドレスごとにマルチキャスト MAC アドレス（01-00-0c-cd-cd-cd、HDLC プロトコル 0x200a）宛てのフレームを生成し、新しいトポロジに関係するドメイン内の全スイッチの CAM テーブルを更新します。

## 推奨事項

シスコでは、ブロックされたポートを持つスイッチ（通常はアクセス レイヤのスイッチ）に対して UplinkFast を有効にすることを推奨しています。バックアップ ルート リンクの暗黙的なトポロジ情報を持たないスイッチ（シスコのマルチレイヤ設計では通常、ディストリビューション スイッチとコア スイッチ）では使用しないでください。この機能は実稼働ネットワークを中断せずに追加できます。UplinkFast を有効にするには、次のコマンドを発行します。

```
set spantree uplinkfast enable
```

このコマンドはまた、**ブリッジ プライオリティを高い値に設定して、設定対象のスイッチがルー**

**ト ブリッジになるリスクを最小限に抑え、ポート プライオリティを高い値に設定して、指定ポートになるリスクを最小限に抑えます。スイッチがルート ブリッジや指定ポートになると機能が破綻します。**UplinkFast が有効になっていたスイッチを復元する場合は、この機能を無効にし、「clear uplink」を使用してアップリンク データベースをクリアして、ブリッジ プライオリティを手動で復元する必要があります。

**注：プロトコルフィルタリング機能が有効**になっている場合は、UplinkFastコマンドのall protocolsキーワードが必要です。プロトコル フィルタリングが有効な場合、CAM には MAC および VLAN 情報とともにプロトコル タイプが記録されるため、UplinkFast フレームは各 MAC アドレスのプロトコルごとに生成する必要があります。**rate キーワードでは、UplinkFast トポロジ アップデート フレームの 1 秒間のパケット数を指定します。**デフォルトが推奨されています。Rapid STP（RSTP）や IEEE 802.1w には BackboneFast がネイティブに含まれており、RSTP では自動的に有効になるので、BackboneFast を設定する必要はありません。

## BackboneFast

BackboneFast は間接リンク障害からの迅速なコンバージェンスを実現します。STP にこの機能を追加すると、通常はコンバージェンス時間がデフォルトの 50 秒から 30 秒に短縮されます。

## 動作の概要

BackboneFast 機能は、スイッチのルート ポートまたはブロックされたポートが代表ブリッジから下位 BPDU を受信すると動作を開始します。この状況は、ダウンストリーム スイッチがルートへの接続を失い、新しいルートを選択するために自身の BPDU の送信を開始すると発生します。**下位 BPDU では、1 つのスイッチがルート ブリッジと代表ブリッジの両方として識別されます。**

通常のスパニング ツリー ルールでは、受信側スイッチは、設定された最大エージング タイム（デフォルトでは 20 秒）が経過するまで下位 BPDU を無視します。ただし、BackboneFast が有効な場合、スイッチは下位 BPDU をトポロジが変更されたことを示す信号として認識し、Root Link Query（RLQ）BPDU を使用して、ルート ブリッジへの代替パスがあるかどうか確認します。このプロトコルを追加することで、スイッチはルートがまだ使用可能かどうか確認でき、
BPDU

このプロトコルの動作には次のような特徴があります。

- スイッチはルート ポートからのみ RLQ パケットを送信します（つまり、ルート ブリッジに向けて送信されます）。
- RLQ を受信したスイッチは、自身がルート スイッチの場合、または問題のルートへの接続をすでに失っている場合は応答します。これらの情報を持っていないスイッチは、ルート ポートからクエリを転送する必要があります。
- 問題のルートへの接続をすでに失っているスイッチは、このクエリーに対して否定応答します。
- 応答は、クエリーが到達したポートからのみ送出されます。
- ルート スイッチはこのクエリーに対して常に肯定応答します。
- 非ルート ポートで受信された応答は廃棄されます。

Maxage が期限切れになるまで待つ必要がないため、STP コンバージェンス時間は最大 20 秒短縮できます。

詳細については、Catalyst スイッチ上の BackboneFast の概要と設定 [英語] を参照してください、

## 推奨事項

シスコでは、STP を実行しているすべてのスイッチで BackboneFast を有効にすることを推奨しています。この機能は実稼働ネットワークを中断せずに追加できます。BackboneFast を有効にするには、次のコマンドを発行します。

```
set spantree backbonefast enable
```

**注：このグローバル レベル コマンドは、すべてのスイッチで理解されなければならない機能を STP プロトコルに追加するため、ドメイン内のすべてのスイッチで設定する必要があります。**

## その他のオプション

BackboneFast は 2900XL および 3500 ではサポートされていません。スイッチ ドメインに、Catalyst 4500/4000、5500/5000、および 6500/6000 スイッチに加えてこれらのスイッチがある場合は BackboneFast を有効にしないでください。

RSTP や IEEE 802.1w には BackboneFast がネイティブに含まれており、RSTP では自動的に有効になるので、BackboneFast を設定する必要はありません。

## スパニング ツリー ループ ガード

ループ ガードは、STP に対するシスコ独自の最適化機能です。ループ ガードは、次の原因で発生するループから L2 ネットワークを保護します。

- ネットワーク インターフェイスの誤動作
- CPU の過負荷
- BPDU の通常転送を妨害する要因

STP ループは、冗長なトポロジにおいてブロッキング ポートが誤ってフォワーディング ステートに移行すると発生します。この移行は通常、物理的に冗長なトポロジ内のポートの 1 つ（ブロッキング ポートとは限らない）が BPDU の受信を中断すると発生します。

ループ ガードは、スイッチがポイントツーポイント リンクによって接続されているスイッチド ネットワークでのみ有効です。最近のキャンパス ネットワークやデータセンター ネットワークは、ほとんどがこのタイプのネットワークです。ポイントツーポイント リンクでは、下位 BPDU を送信するか、リンクをダウンしない限り、代表ブリッジは消えることはありません。STP ループ ガード機能は、Catalyst 4000 および Catalyst 5000 プラットフォーム用の CatOS バージョン 6.2(1) および Catalyst 6000 プラットフォーム用のバージョン 6.2(2) で導入されています。

ループ ガードの詳細については、『ループ ガードと BPDU スキュー検出機能によるスパニング ツリー プロトコルの拡張機能』を参照してください。

## 動作の概要

ループ ガードは、ルート ポートや代替またはバックアップ用のルート ポートで BPDU が受信されているかどうかをチェックします。ポートで BPDU が受信されていない場合、ループ ガードはそのポートで BPDU の受信が再開されるまで、ポートを不整合状態（ブロッキング）にします。不整合状態のポートは BPDU を送信しません。そのようなポートが BPDU を再び受信すると、ポート（およびリンク）は再び動作可能であると見なされます。ポートの loop-inconsistent 状

態が解消します。このような復元は自動で行われるため、ポートの状態は STP によって決定されます。

ループ ガードは障害を切り離して、スパニング ツリーを障害リンクや障害ブリッジのない安定したトポロジに収束させます。ループ ガードは、使用中の STP バージョンの速度で STP ループを防止します。STP 自体 ( 802.1d または 802.1w ) に依存関係はなく、STP タイマーの調整時の影響もありません。これらの理由により、ループ ガード機能がソフトウェアでサポートされている場合は、STP に依存するトポロジに UDLD とともにループ ガードを実装してください。

Loop Guard によって loop-inconsistent ポートがブロックされると、次のメッセージが表示されます。

```
%SPANTREE-2-ROOTGUARDBLOCK: Port 1/1 tried to become non-designated
in VLAN 77. Moved to root-inconsistent state.
```

STP loop-inconsistent ステートのポートで BPDU が受信されると、そのポートは別の STP ステートに移行します。受信された BPDU に従って自動的にリカバリが行われるため、操作は不要です。リカバリ後、次のメッセージがログに記録されます。

```
SPANTREE-2-LOOPGUARDUNBLOCK: port 3/2 restored in vlan 3.
```

## その他の STP 機能との相互作用

- **ルート ガード**ルート ガードでは、ポートが常に強制的に指定されます。ループ ガードは、ポートがルート ポートか代替ポートの場合にのみ有効です。これらの機能は相互排他的です。ループ ガードとルート ガードを 1 つのポートで同時に有効にすることはできません。
- **UplinkFast**ループ ガードは UplinkFast と互換性があります。ループ ガードによってルート ポートがブロッキング ステートに設定されると、UplinkFast によって新しいルート ポートがフォワーディング ステートに設定されます。また、UplinkFast によって loop-inconsistent ステートのポートがルート ポートとして選択されることはありません。
- **BackboneFast**ループ ガードは BackboneFast と互換性があります。代表ブリッジからの下位 BPDU を受信すると、BackboneFast がトリガーされます。BPDU はこのリンクから受信されるので、ループ ガードはアクティブになりません。そのため、BackboneFast とループ ガードには互換性があります。
- **ポートファスト**PortFast では、リンクアップするとすぐにポートがフォワーディング指定ステートに移行します。PortFast が有効なポートは、ルート ポートや代替ポートにはなれないため、ループ ガードと PortFast は相互排他的です。
- **PAgP**ループ ガードでは、STP に認識されているポートが使用されます。そのため、ループ ガードでは、PAgP で実現される論理ポートの抽象化を利用できます。ただし、チャネルを形成するためには、チャネルにグループ化されているすべての物理ポートの設定に互換性がある必要があります。PAgP は、チャネルを形成するために、すべての物理ポート上でルート ガードの設定を均一にします。**注：EtherChannelで**ループガードを設定する場合は、次の点に注意してください。STP は、BPDU を送信するためにチャネル内で最初に動作可能なポートを常に選択します。そのリンクが単方向になると、チャネルの他のリンクが正しく機能している場合でも、ループ ガードによってそのチャネルがブロックされます。ループ ガードですでにブロックされているポートがチャネルを形成するためにグループ化されると、STP ではそれらのポートの状態情報がすべて失われます。新しいチャネル ポートは、指定された権限を使用してフォワーディング ステートに移行できます。チャネルがループ ガードによってブロックされ、チャネルが切断されると、STP からすべての状態情報が失われます。チャネルを形成していた 1 つ以上のリンクが単方向である場合も、各物理ポートは指定された権

限を使用してフォワーディング ステートに移行できます。このリストの最後の 2 つのケースでは、UDLD が障害を検出するまでループが発生する可能性がありますが、ループ ガードはループを検出できません。

## ループ ガードと UDLD 機能の比較

ループ ガードの機能と UDLD 機能は部分的にオーバーラップしています。どちらも、単方向リンクによって生じる STP の障害から保護しますが、この 2 つの機能では、問題に対するアプローチが異なり、機能も異なります。具体的には、BPDU を送信しない CPU によって発生する障害のように、UDLD では検出できない特定の単方向障害があります。さらに、アグレッシブ STP タイマーおよび RSTP モードを使用すると、UDLD が障害を検出する前にループが発生することがあります。

ループ ガードは、共有リンクやリンクがリンクアップ時から単方向である状況では機能しません。リンクがリンクアップ時から単方向である場合、ポートは BPDU を受信することなく、指定ポートになります。この動作は正常である場合もあるため、このケースはループ ガードの対象にはなりません。UDLD では、そのようなシナリオでも保護されます。

最高レベルの保護を実現するためには、UDLD とループ ガードの両方を有効にします。ループ ガードと UDLD の機能比較については、『ループ ガードと BPDU スキュー検出機能によるスパニング ツリー プロトコルの拡張機能』の「*Loop Guard vs. Unidirectional Link Detection*」を参照してください。

## 推奨事項

シスコでは、物理的ループのあるスイッチ ネットワークでは、ループ ガードをグローバルに有効にすることを推奨しています。Catalyst ソフトウェア バージョン 7.1(1) 以降では、すべてのポートでループ ガードをグローバルに有効にできます。この機能は事実上、すべてのポイントツーポイント リンクで有効になります。リンクのデュプレックス ステータスによってポイントツーポイント リンクが検出されます。全二重の場合、リンクはポイントツーポイントであると見なされます。ループ ガードをグローバルに有効にするには、次のコマンドを発行します。

```
set spantree global-default loopguard enable
```

## その他のオプション

グローバルなループ ガード設定がサポートされていないスイッチの場合は、ポート チャネルのポートを含む、個々のすべてのポートでこの機能を有効にします。指定ポートでループ ガードを有効にしても利点はありませんが、有効にしても問題はありません。さらに、有効なスパニング ツリーの再コンバージェンスにより、指定ポートが実質的にルート ポートに変わり、ループ ガード機能がこのポートに役立つことがあります。ループ ガードを有効にするには、次のコマンドを発行します。

```
set spantree guard loop mod/port
```

ループフリー トポロジのネットワークでも、ループが偶発的に発生した場合にループ ガードが役立つことがあります。ただし、このタイプのトポロジでループ ガードを有効にすると、ネットワ

ークの分離の問題が発生することがあります。ループフリー トポロジを構築してネットワークの分離の問題を回避するには、次のコマンドを発行してループ ガードをグローバルに、または個別に無効にします。共有リンクではループ ガードを有効にしないでください。

- 

  ```
  set spantree global-default loopguard disable
  !--- This is the global default.
  ```

  または

- 

  ```
  set spantree guard none mod/port
  !--- This is the default port configuration.
  ```

## Spanning Tree Root Guard

ルート ガード機能には、ネットワークにルート ブリッジを強制的に配置する方法があります。ルート ガード機能により、ルート ガードが有効になっているポートが指定ポートになります。通常、ルート ブリッジの 2 つ以上のポートが互いに接続されている場合を除き、ルート ブリッジのポートはすべて指定ポートになります。ブリッジは、ルート ガードが有効になっているポートで上位の STP BPDU を受信すると、そのポートを root-inconsistent STP ステートに移行します。root-inconsistent ステートは、実質的にはリスニング ステートと同じです。このポートからはトラフィックは転送されません。このようにして、ルート ガードはルート ブリッジを強制的に配置します。ルート ガードは、Catalyst 29xx、4500/4000、5500/5000、および 6500/6000 用の CatOS ソフトウェア バージョン 6.1.1 以降で使用できます。

## 動作の概要

ルート ガードは STP の組み込みメカニズムです。ルート ガードには独自のタイマーはなく、BPDU の受信にのみ依存しています。ルート ガードをポートに適用すると、そのポートはルート ポートになれなくなります。BPDU を受信するとスパニング ツリーのコンバージェンスがトリガーされ、指定ポートがルート ポートになり、そのポートが root-inconsistent ステートになります。このアクションは、syslog メッセージに次のように表示されます。

```
%SPANTREE-2-ROOTGUARDBLOCK: Port 1/1 tried to become non-designated
in VLAN 77. Moved to root-inconsistent state
```

ポートが上位の BPDU を送信しなくなると、ポートのブロックが再び解除されます。STP によって、ポートはリスニング ステートからラーニング ステートになり、最終的にはフォワーディング ステートに移行します。リカバリは自動的に行われるので、人の介入は不要です。次に syslog メッセージの例を示します。

```
%SPANTREE-2-ROOTGUARDUNBLOCK: Port 1/1 restored in VLAN 77
```

ルート ガードはポートを強制的に指定ポートにしますが、ループ ガードはポートがルート ポートか代替ポートの場合にのみ有効です。そのため、この 2 つの機能は相互排他的です。ループ ガードとルート ガードを 1 つのポートで同時に有効にすることはできません。

詳細については、『スパニング ツリー プロトコル ルート ガード機能拡張』を参照してください。

## 推奨事項

シスコでは、直接管理下にないネットワーク デバイスに接続されているポートに対しては、ルート ガード機能を有効にすることを推奨しています。ルート ガード機能を設定するには、次のコマンドを発行します。

```
set spantree guard root mod/port
```

## EtherChannel

EtherChannel テクノロジーを使用すると、複数のチャネル（Catalyst 6500/6000 では最大 8 チャネル）を 1 つの論理リンクに逆多重化できます。各プラットフォームでの実装はそれぞれ異なりますが、次の共通要件を理解することが重要です。

- 複数のチャネル上で複数のフレームを統計的に多重化するアルゴリズム
- 単一インスタンスの STP を実行できるようにする 1 つの論理ポートの作成
- PAgP や Link Aggregation Control Protocol（LACP）などのチャネル管理プロトコル

### フレーム多重化

EtherChannel は、コンポーネントの 10/100 リンクまたはギガビット リンクの間でフレームを効率的に多重化するフレーム分散アルゴリズムを実行します。プラットフォームごとのアルゴリズムの違いは、分散を決定するためのフレーム ヘッダー情報を抽出する機能が各ハードウェアのタイプによって異なるために生じます。

負荷分散アルゴリズムは、両方のチャネル制御プロトコルに対するグローバル オプションです。IEEE 規格では特定の分散アルゴリズムの使用が必須になっていないため、PAgP と LACP ではフレーム分散アルゴリズムが使用されます。ただし、いずれの分散アルゴリズムでも、フレーム受信時にアルゴリズムによって特定のカンバセーションの一部であるフレームの順序が変わったり、フレームが重複したりすることはありません。

**注：次の情報**を考慮する必要があります。

- Catalyst 6500/6000 は Catalyst 5500/5000 よりも新しいスイッチング ハードウェアを備えており、IP レイヤ 4（L4）情報をワイヤ スピードで読み取ることで、単純な MAC L2 情報の場合よりも、多重化に関してよりインテリジェントな判断を下すことができます。
- Catalyst 5500/5000 の機能は、モジュールに Ethernet Bundling Chip（EBC）が搭載されているかどうかによって決まります。各ポートにどのような機能があるかを確認するには、show port capabilities mod/port コマンドを使用します。

次の表に、リストされた各プラットフォームのフレーム分散アルゴリズムの詳細を示します。

| Platform | チャネル ロード バランシング アルゴリズム |
|---|---|
| Catalay | 必要なモジュールを搭載した Catalyst 5500/5000 では、FEC[1] あたり 2 ~ 4 のリンクを接続できます。ただし、それらのリンクは同じモジュール上に存在する必要があります。フレームを転送するためのリンクは |

| | |
|---|---|
| st 5 5 0 0/ 5 0 0 0 シリーズ | 、送信元および宛先 MAC アドレスのペアに基づいて決定されます。送信元 MAC アドレスと宛先 MAC アドレスの最下位 2 ビットで X-OR 演算が行われます。この演算の結果は、次の 4 つのうちいずれかになります：(0 0)、(0 1)、(1 0)、または (1 1)。 それぞれの値が FEC バンドル内の 1 つのリンクを指します。2 ポートの Fast EtherChannel の場合、X-OR 演算には 1 ビットだけが使用されます。状況によっては、送信元/宛先ペアのアドレスの 1 つが一定になることがあります。たとえば、宛先がサーバの場合がそうです。さらに可能性が高いのは宛先がルータの場合です。この場合、送信元アドレスが常に異なるため、統計的なロード バランシングが発生します。 |
| C at al y st 4 5 0 0/ 4 0 0 0 シリーズ | Catalyst 4500/4000 の EtherChannel は、各フレームの送信元と宛先の MAC アドレスの下位ビットに基づいて、（単一モジュール上の）1 つのチャネル内のリンク間でフレームを分散させます。このアルゴリズムは Catalyst 5500/5000 よりも複雑で、MAC DA（バイト 3、5、6）、SA（バイト 3、5、6）、入力ポート、および VLAN ID の各フィールドの確定ハッシュが使用されます。フレーム分散方式は設定可能ではありません。 |
| C at al y st 6 5 0 0/ 6 0 0 0 シリーズ | Supervisor Engine ハードウェアに応じて 2 種類のハッシュ アルゴリズムがあります。ハッシュはハードウェアに実装された 17 次多項式で、すべての場合に、MAC アドレス、IP アドレス、または IP TCP/UDP2 ポート番号が使用されて、3 ビットの値を生成するためのアルゴリズムが適用されます。この処理が送信元アドレスと宛先アドレスの両方に対して個別に実行されます。その結果、XOR で別の 3 ビット値が生成され、その値を使用して、パケットの転送に使用するチャネル内のポートが決まります。Catalyst 6500/6000 のチャネルは、任意のモジュール上のポート（最大 8 ポート）の間で形成できます。 |

1 FEC = Fast EtherChannel

2 UDP = User Datagram Protocol

次の表は、さまざまな Catalyst 6500/6000 Supervisor Engine モデルでサポートされている分散

方式と、それぞれのデフォルトの動作を示しています。

| ハードウェア | 説明 | 分散方式 |
|---|---|---|
| WS-F6020（L2 エンジン） | 初期 Supervisor Engine 1 | L2 MAC：SA、DA、SA および DA |
| WS-F6020A（L2 エンジン）WS-F6K-PFC（L3 エンジン） | 後期 Supervisor Engine 1 および Supervisor Engine1A/PFC1 | L2 MAC：SA、DA、SA および DA L3 IP：SA、DA、SA および DA（デフォルト） |
| WS-F6K-PFC2 | Supervisor Engine 2/PFC2（CatOS 6.x が必要） | L2 MAC：SA、DA、SA および DA L3 IP：SA、DA、SA および DA（デフォルト）L4 セッション：S ポート、D ポート、S および D ポート（デフォルト） |
| WS-F6K-PFC3BXL WS-F6K-PFC3B WS-F6K-PFC3A | Supervisor Engine 720/PFC3A（CatOS 8.1.x が必要）Supervisor Engine 720/Supervisor Engine 32/PFC3B（CatOS 8.4.x が必要）Supervisor Engine 720/PFC3BXL（CatOS 8.3.x が必要） | L2 MAC：SA、DA、SA および DA L3 IP：SA、DA、SA および DA（デフォルト）L4 セッション：S ポート、D ポート、S および D ポート IP-VLAN-L4 セッション：SA、VLAN、および S ポート、DA、VLAN、および D ポート、SA、DA、VLAN、S ポート、および D ポート |

**注**：L4分散では、最初の断片化パケットはL4分散を使用します。後続のパケットはすべて L3 分散を使用します。

他のプラットフォームでの EtherChannel のサポートの詳細、および各プラットフォームでの設定方法とトラブルシューティング方法については、次のドキュメントを参照してください。

- Catalyst スイッチでの EtherChannel のロード バランシングと冗長性について
- CatOS システム ソフトウェアが動作する Catalyst 4500/4000, 5500/5000 スイッチと 6500/6000 スイッチの間の EtherChannel の設定
- Catalyst 6500/6000 と Catalyst 4500/4000 間の LACP（802.3ad）の設定
- レイヤ 3 とレイヤ 2 の EtherChannel の設定 [英語]

## 推奨事項

Catalyst 6500/6000 シリーズ スイッチでは、デフォルトで IP アドレスによるロード バランシングが実行されます。IP が主要なプロトコルであると仮定して、CatOS 5.5 ではこの方法を推奨します。ロード バランシングを設定するには、次のコマンドを発行します。

```
set port channel all distribution ip both
!--- This is the default.
```

Catalyst 4500/4000 および 5500/5000 シリーズの L2 MAC アドレスに基づくフレーム分散は、ほとんどのネットワークで使用できます。ただし、チャネルを介して通信している主なデバイスが 2 台だけの場合、すべてのトラフィックで同じリンクが使用されます（SMAC と DMAC が一定であるため）。 これは通常、サーバのバックアップやサイズの大きいファイルの転送、または 2 台のルータ間のトランジット セグメントに対して問題になる可能性があります。

論理集約ポート（agport）を SNMP を使用して単独のインスタンスとして管理し、総スループットの統計情報を収集することは可能ですが、シスコでは、フレーム分散メカニズムの動作状況をチェックし、統計的ロード バランシングが実現されているかどうかを確認するために、各物理インターフェイスを個別に管理することを推奨しています。

CatOS 6.xの新しいコマンドshow channel trafficコマンドは、show counters *mod/port*コマンドまたはshow mac mod/portコマンドを使用して個々のポートカウンタをチェックする場合よりも、分散統計のパーセンテージを簡単に表示できます。CatOS 6.xの別の新しいコマンドshow channel hashコマンドを使用すると、ディストリビューションモードに基づいて、特定のアドレスやポート番号の発信ポートとして選択されるポートを確認できます。LACP チャネル用の同等のコマンドは、show lacp-channel traffic コマンドと show lacp-channel hash コマンドです。

## その他のオプション

Catalyst 4500/4000 または Catalyst 5500/5000 の MAC ベースのアルゴリズムの相対的な制限が問題で、良好な統計的ロード バランシングが実現されない場合に実行可能な手順を次に示します。

- Catalyst 6500/6000 スイッチを要所に展開する
- たとえば、複数の FE ポートから 1 つの GE ポートに、または複数の GE ポートから 1 つの 10 GE ポートに切り替えることでチャネリングせずに帯域幅を増やす
- 大量のフローを扱うエンド ステーションのペアのアドレスを変更する
- 高帯域幅デバイスに対して専用のリンクまたは VLAN をプロビジョニングする

## EtherChannel の設定ガイドラインと制約事項

EtherChannel では、互換性のあるポートが 1 つの論理ポートに集約される前に、すべての物理ポートのポート プロパティが確認されます。設定ガイドラインと制約事項はスイッチ プラットフォームごとに異なります。バンドリングの問題を回避するには、ガイドラインに従ってください。たとえば、QoS が有効な場合、Catalyst 6500/6000 シリーズのスイッチング モジュールを異なる QoS 機能とバンドリングすると EtherChannel が形成されません。Cisco IOS ソフトウェアでは、no mls qos channel-consistency port-channel interface コマンドを使用して、EtherChannel バンドリングの QoS ポート属性チェックを無効にできます。CatOS には、QoS ポート属性チェックを無効にする同等のコマンドはありません。show port capability *mod*/*port*コマンドを発行して、QoSポートの機能を表示し、ポートに互換性があるかどうかを確認できます。

設定上の問題を回避するには、各プラットフォームの次のガイドラインに従ってください。

- EtherChannel の設定 [英語]（Catalyst 6500/6000）の「*EtherChannel Configuration Guidelines*」
- Fast EtherChannel と Gigabit EtherChannel の設定 [英語]（Catalyst 4500/4000）の「*EtherChannel Configuration Guidelines and Restrictions*」
- Fast EtherChannel と Gigabit EtherChannel の設定 [英語]（Catalyst 5000）の「*EtherChannel Configuration Guidelines and Restrictions*」

**注**：Catalyst 4000がサポートするポートチャネルの最大数は126です。ソフトウェアリリース6.2(1)以前では、6スロットおよび9スロットのCatalyst 6500シリーズスイッチでサポートされるEtherChannelの最大数は128です。ソフトウェア リリース 6.2(2) 以降のリリースでは、スパニング ツリー機能がポート ID を処理します。したがって、サポートされる EtherChannel の最大数は、6 個または 9 個のスロットを持つシャーシでは 126、13 個のスロットを持つシャーシでは 63 です。

## Port Aggregation Protocol

PAgP は、リンクの両端でパラメータの一致をチェックし、リンクの障害や追加が発生したときにチャネルの適応を支援する管理プロトコルです。PAgP に関しては次の点に注意してください。

- PAgP では、チャネル内のすべてのポートが同じ VLAN に属しているか、またはトランク ポートとして設定されている必要があります。（ダイナミック VLAN はポートを強制的に別の VLAN に変更できるため、EtherChannel のメンバーには含まれません）。
- バンドルがすでに存在していて、1 つのポートの設定が変更された場合（VLAN やトランキング モードが変更された場合など）、バンドル内のすべてのポートがその設定にあわせて変更されます。
- PAgP は、異なる速度またはポート デュプレックスで動作しているポートをグループ化しません。バンドルが存在する場合に速度とデュプレックスが変更されると、PAgP はバンドル内のすべてのポートのポート速度とデュプレックスを変更します。

## 動作の概要

PAgP ポートは、各物理（または論理）ポートのグループ化を制御します。PAgP パケットは、CDP パケットに使用されるのと同じマルチキャスト グループ MAC アドレス **01-00-0c-cc-cc-cc** を使用して送信されます。プロトコル値は0x0104です。これは、プロトコルの動作の要約です。

- 物理ポートが up である間、PAgP パケットは、検出時には 1 秒間隔、定常状態では 30 秒間隔で送信されます。
- このプロトコルは、物理ポートが別の PAgP 対応デバイスに双方向接続していることを証明する PAgP パケットをリッスンします。
- データ パケットは受信されるものの、PAgP パケットが受信されない場合は、ポートが PAgP 非対応デバイスに接続していると想定されます。
- 物理ポートのグループで PAgP パケットが 2 つ受信されると、すぐに集約ポートの形成が試行されます。
- PAgP パケットが一定時間停止すると、PAgP の状態は切断されます。

## 通常処理

プロトコルの動作の理解を助けるために、いくつかの概念の定義を次に示します。

- **agport：同じ集約に含まれるすべての物理ポートで構成される論理ポート。固有の SNMP ifIndex で識別できます。**したがって、agport には非稼働状態のポートは含まれません。
- **チャネル：形成基準を満たす集約。**チャネルには非稼働状態のポートが含まれる場合があります（agport はチャネルのサブセット）。 agport を通じて PAgP 上で動作するプロトコルには、STP や VTP などがあります。CDP と DTP は、これには含まれません。これらのプロトコルはいずれも、PAgP によってそれぞれの agport が 1 つまたは複数の物理ポートに接続されるまでパケットを送受信できません。
- **グループ機能：各物理ポートと agport には、group-capability と呼ばれる設定パラメータがあります。**ある物理ポートを別の物理ポートと集約できるのは、両方のポートに同じ group-capability がある場合に限られます。
- **集約手順：物理ポートは UpData または UpPAgP 状態になると、適切な agport に接続されます。**この 2 つ以外の状態に移行すると、agport との関連付けは解除されます。

次の表に、状態の定義と作成手順を示します。

| 都道府県 | 意味 |
|---|---|
| UpData | まだ PAgP パケットを受信していませんが、PAgP パケットが送信されます。この物理ポートは、その agport に接続している唯一のポートです。物理ポートと agport の間で非 PAgP パケットが受け渡されます。 |
| BiDir | 厳密に 1 つの PAgP パケットを受信しました。これは 1 つのネイバーとの双方向接続が存在することを証明しています。この状態の物理ポートは、どの agport にも接続していません。PAgP パケットが送信され、受信することもあります。 |
| UpPAgP | この物理ポートは、おそらく他の物理ポートと関連付けられていて、1 つの agport に接続しています。物理ポート上で PAgP パケットが送受信されます。物理ポートと agport の間で非 PAgP パケットが受け渡されます。 |

接続の両端で許容される agport 内の最大のポート グループとして定義されている場合は、グルーピング結果について、両方の接続の両端が合意する必要があります。

物理ポートは `UpPAgP group-capability BiDir UpPAgP agport`（このような BiDir ポートはすべて、同時に `UpPAgP` 構成する物理ポートのパラメータが新しく使用可能になった物理ポートと互換性がある agport が存在しない場合、適切なパラメータを持つ、物理ポートが関連付けられていない agport に割り当てられます。

PAgP タイムアウトは、物理ポート上で認識されている最後のネイバーに対して発生します。タイムアウトしたポートは agport から削除されます。同時に、同じ agport 上のタイマーがタイムアウトしている物理ポートもすべて削除されます。これにより、相手側が停止した agport を、一度に 1 つの物理ポートを切断する代わりに、一斉に切断することができます。

## 障害時の動作

既存チャネルのリンクで障害（ポートのケーブルが抜ける、ギガビット インターフェイス コンバータ（GBIC）が外れる、光ファイバが破損するなど）が発生すると、agport がアップデートされ、トラフィックは残りのリンク上で 1 秒以内にハッシュされます。障害発生後に再ハッシュする必要がないトラフィック（同じリンク上で送信を続けるトラフィック）では損失は発生しません。障害が発生したリンクを復元すると、agport に対する別のアップデートがトリガーされて、トラフィックが再度ハッシュされます。

**注：電源**オフやモジュールの取り外しによってチャネルでリンクに障害が発生した場合の動作は、異なる場合があります。定義上、チャネルの形成には 2 つの物理ポートが必要です。2 ポート チャネルの一方のポートがシステムから失われると、論理的な agport は切断され、元の物理ポートがスパニング ツリーに対して再初期化されます。これは、STP によってポートが再びデータを送信可能になるまで、トラフィックが廃棄されることがあることを意味します。

Catalyst 6500/6000 では、この規則に例外があります。CatOS 6.3 よりも前のバージョンでは、チャネルがモジュール 1 と 2 のポートのみで構成されている場合、モジュールを取りはずしても agport は down にはなりません。

この 2 つの障害モードの違いは、ネットワークのメンテナンスを計画する際に重要になります。これは、モジュールをオンラインで削除または挿入する場合に考慮すべき STP TCN が存在することがあるためです。前述のように、agport は障害発生時にも影響を受けない場合があるため、NMS（ネットワーク管理システム）によってチャネルの各物理リンクを管理することが重要です。

Catalyst 6500/6000 での不要なトポロジ変更の発生を軽減するために推奨される手順を次に示します。

- モジュールごとに 1 つのポートを使用してチャネルを形成している場合は、3 つ以上のモジュールを使用する必要があります（合計 3 ポート以上）。
- チャネルが 2 つのモジュールにまたがっている場合は、各モジュールの 2 つのポートを使用する必要があります（合計 4 ポート）。
- 2 枚のカード上で 2 つのポート チャネルが必要な場合は、Supervisor Engine のポートだけを使用します。
- CatOS 6.3 にアップグレードします。これにより、複数のモジュールに分割されているチャネルの STP を再計算せずにモジュールを削除できます。

## 設定オプション

EtherChannel はさまざまなモードに設定できます。次の表に各モードの要約を示します。

| モード | 設定可能なオプション |
|---|---|
| | PAgP は有効ではありません。ポートは、ネイバー ポートの設定内容にかかわらず、チャネリングされます。ネイバー ポートのモードが on の場合、チャネルが形成されます。 |
| | 近接ポートがどのように設定されているかにかかわらず、ポートはチャネルを形成しようとしません。 |
| Auto | PAgP プロトコルによって集約が制御されます。ポートをパッシブ ネゴシエーション ステートにします。送信元が desirable PAgP 1 PAgP |

| | |
|---|---|
| | |
| Desirable | PAgP プロトコルによって集約が制御されます。ポートをアクティブ ネゴシエーション ステートにします。この場合、ポートは PAgP パケットを送信することによって、相手ポートとのネゴシエーションを開始します。相手側のポート グループが desirable または auto モードの場合にチャネルが形成されます。 |
| Non-silentCatalyst 5500/5000 FE GE | auto desirable データ パケットを受信していないインターフェイスは、agport に接続されることはなく、データ送信には使用でません。この双方向性チェックは、一部のリンク障害によってチャネルが壊れてしまう特定の Catalyst 5500/5000 ハードウェアのために提供されています。non-silent Catalyst 4500/4000 および 6500/6000 シリーズのハードウェアでは、より柔軟なバンドリングと改善された双方向チェックがデフォルトで提供されています。 |
| SilentCatalyst 6500/6000 4500/4000 5500/5000 | auto desirable データ パケットを受信していないインターフェイスは、15 秒のタイムアウト期間の後に、自動的に agport に接続され、データ送信に使用できるようになります。Silent PAgP |

silent/non-silent 物理サブレイヤ（PHY）の障害や、光ファイバやケーブルの破損などにより、あるポートが送信不能になった場合、そのネイバー ポートは引き続き動作状態であることがあります。パートナーはデータを送信し続けますが、リターン トラフィックは受信できないのでデータは失われます。また、単方向リンクの性質により、スパニング ツリー ループが生じることもあります。

ファイバ ポートの中には、受信信号を失ったときにポートを非稼働状態にするという望ましい機能を持つものがあります（FEFI）。 この機能により、パートナー ポートが非動作状態に移行し、事実上リンクの両端のポートがダウンします。

BPDU などのデータを送信し、単方向状態を検出できないデバイスを使用している場合は、non-silent PAgP が単方向リンクの検出に要する時間は、約 3.5 X 30 秒 = 105 秒です。ここで 30 秒は、2 つの連続した PAgP メッセージの間隔を表します。単方向リンクをより迅速に検出する方法として、UDLD を使用することが推奨されます。

データを送信しないデバイスを使用している場合は、silent モードを使用する必要があります。

これで、受信データの有無にかかわらず、ポートは強制的に接続されて動作状態になります。また、L1 FEFI および UDLD を使用する最近のプラットフォームのように、単方向状態を検出できるポートの場合、デフォルトで silent モードが使用されます。

## 確認

次の表は、直接接続された 2 台のスイッチ ( Switch-A と Switch-B ) の間で起こり得るすべての PAgP チャネリング モードのシナリオの要約です。 一部の組み合わせでは、STP によってチャネリング側のポートが errdisable

| Switch-A のチャネル モード | Switch-B のチャネル モード | チャネル状態 |
|---|---|---|
| | | Channel PAgP |
| | | Not Channelerrdisable |
| | | Not Channelerrdisable |
| | Desirable | Not Channelerrdisable |
| | | Not Channelerrdisable |
| | | Not Channel |
| | | Not Channel |
| | Desirable | Not Channel |
| | | Not Channelerrdisable |
| | | Not Channel |
| | | Not Channel |
| | Desirable | PAgP |
| Desirable | | Not Channelerrdisable |
| Desirable | | Not Channel |
| Desirable | | PAgP |
| Desirable | Desirable | PAgP |

## 推奨事項

シスコでは、on PAgP 推奨の方法は、リンクの両端で desirable さらに、silent/non-silent Catalyst 6500/6000 4500/4000 silentCatalyst 5500/5000 non-silent

前述したように、他のすべてのポートでチャネリングの設定を明示的にオフにしておくと、データ転送が高速になります。チャネリングに使用されないポートで PAgP がタイムアウトするまで 15 秒待つのは避けてください。これは、ポートがタイムアウト後に STP にハンドオーバーされるためです。STP ではデータ転送が可能になるまでに 30 秒かかり、場合によっては DTP のためにも 5 秒必要となり、合計で 50 秒かかることになります。set port host コマンドについては、このドキュメントの「STP」の項を参照してください。

```
set port channel port range mode desirable

set port channel port range mode off
!--- Ports not channeled; part of the set port hostcommand.
```

このコマンドは、チャネルに**管理グループ番号を割り当てます。この番号は** show channel group コマンドで確認できます。必要に応じて、管理番号を使用して、同じ agport に対するチャネリング ポートの追加と削除を管理できます。

## その他のオプション

アクセス レイヤで最小限の管理モデルを採用しているお客様がよく使用されるその他の設定としては、ディストリビューション レイヤとコア レイヤでモードを `desirable` `auto`

PAgP をサポートしていないデバイスに対してチャネルを形成する場合は、チャネルを `on` にハードコードする必要があります。これは、サーバ、Local Director、コンテンツ スイッチ、ルータ、古いソフトウェアが動作しているスイッチ、Catalyst XL スイッチ、Catalyst 8540 などのデバイスに当てはまります。次のコマンドを実行します。

```
set port channel port range mode on
```

CatOS 7.x で使用可能な新しい 802.3ad IEEE LACP 規格は、クロス プラットフォームやベンダー間での相互運用性という利点があるため、長期的には PAgP に取って代わる可能性があります。

## Link Aggregation Control Protocol（LACP）

LACP は、同様の特性を持つポートが隣接スイッチと動的にネゴシエーションしてチャネルを形成できるようにするプロトコルです。PAgP はシスコ独自のプロトコルであり、このプロトコルを使用できるのはシスコ製スイッチおよびシスコのライセンスに基づいてベンダーが販売しているスイッチだけです。IEEE 802.3ad で定義されている LACP を使用すると、802.3ad 仕様に準拠したデバイスを使用したイーサネット チャネリングをシスコ スイッチで管理できます。CatOS 7.x ソフトウェア リリースには、LACP のサポートが導入されています。

機能的には、LACP と PAgP の間の違いはごくわずかです。どちらのプロトコルも、チャネルごとに最大 8 ポートまでをサポートし、バンドルの形成前に同じポート プロパティがチェックされます。チェックされるポート プロパティには次のものが含まれます。

- 速度
- 二重
- ネイティブVLAN
- トランキング タイプ

LACP と PAgP の間には次の顕著な違いがあります。

- LACP は全二重ポートでのみ実行でき、半二重ポートはサポートしていない。
- LACP では、ホット スタンバイ ポートがサポートされている。LACP では、ハードウェアで許容される最大数（8 ポート）まで、互換性のあるポートの最大数を 1 つのチャネルに設定するように常に試みられます。 互換性があるすべてのポートを LACP で集約できない場合、チャネルにアクティブに含めることができないポートはすべてホット スタンバイ状態になり、使用中のポートのいずれかで障害が発生した場合にのみ使用されます。互換性のあるすべてのポートを LACP で集約できない状況の例としては、リモート システムのハードウェア制限がより厳しい場合が考えられます。

**注**：CatOSでは、同じ管理キーを割り当てることができるポートの最大数は8です。Cisco IOS ソフトウェアの LACP では、ハードウェアで許容される最大数（8 ポート）まで、互換性のあるポートの最大数を 1 つの EtherChannel に設定するように試みられます。 さらに 8 ポートをホット スタンバイ ポートとして設定できます。

## 動作の概要

LACP は、バンドルする個々の物理（または論理）ポートを個別に制御します。LACPパケットは、マルチキャストグループのMACアドレス**01-80-c2-00-00-02を使用して送信されます。タイプ/フィールド値は、サブタイプが0x01の0x8809です。プロトコル動作の要約を次に示します。**

- このプロトコルは、集約機能と状態情報のアドバタイズをデバイスに依存しています。送信は、「集約可能」リンク***ごとに***定期的に行われます。
- 物理ポートが upである間、LACP パケットは、検出時には 1 秒間隔、定常状態では 30 秒間隔で送信されます。
- 「集約可能」リンクにあるパートナーは、プロトコル内で送信される情報をリッスンして、実行するアクションを決定します。
- ハードウェアで許容される最大数（8 ポート）までの互換性のあるポートが 1 つのチャネルに設定されます。
- 最新の状態情報が定期的かつタイムリーにリンク パートナー間で交換されて、集約が維持されます。リンク障害などのために設定が変更されると、プロトコル パートナーがタイムアウトして、システムの新しい状態に基づいて適切なアクションが実行されます。
- 定期的な LACP データ ユニット（リンク集約制御プロトコル データ ユニット）の転送に加えて、状態情報に変更がある場合、イベント駆動型リンク集約制御プロトコル データ ユニットがパートナーに送信されます。プロトコル パートナーは、システムの新しい状態に基づいて適切なアクションを実行します。

## LACP パラメータ

一連のリンクが同じシステムに接続されているか、および集約の観点からそれらのリンクに互換性があるかを LACP が判断できるようにするためには、次のパラメータを設定できる機能が必要になります。

- リンク アグリゲーションに参加する各システムのグローバル一意識別子LACP が動作する各システムには、自動的または管理者によって選択できるプライオリティを割り当てる必要があります。デフォルトのシステム プライオリティは 32768 です。システム プライオリティは、システム ID を作成するために、主にシステムの MAC アドレスとともに使用されます。
- 特定のシステムが把握している、ポートごとおよびアグリゲータごとに関連付けられている一連の機能を識別する方法システムの各ポートには、自動的または管理者によってプライオリティを割り当てる必要があります。デフォルト値は 128 です。プライオリティは、ポート ID を作成するためにポート番号とともに使用されます。
- リンク アグリゲーション グループとそれに関連付けられているアグリゲータを識別する方法別のポートと集約できるポートの機能は、ゼロより大きな単純な 16 ビットの整数パラメータによって要約されています。このパラメータは「キー」と呼ばれています。 各キーは、次のような要因によって決定されます。ポートの次のような物理特性。データ レートDuplexityポイントツーポイントまたは共有メディアネットワーク管理者が決定する設定上の制約各ポートには、次の 2 つのキーが関連付けられています。管理キー：このキーの値は管理者が操作できます。ユーザはこのキーを選択できます。動作キー：このキーは、システムが集約を形成するために使用します。ユーザはこのキーを選択することも、直接変更することもできません。同じ動作キー値を共有するシステム内の一連のポートを、同じキー グループのメンバーと呼びます。

2 つのシステムがあり、同じ管理キーが設定された一連のポートがある場合、それぞれのシステムがポートの集約を試みます。各システムは、最も優先順位が高いシステムの最も高い優先順位

が設定されたポートから集約を開始します。この動作は、各システムがシステム自身の優先順位とパートナーの優先順位を把握しているため可能になります。システムの優先順位はユーザまたはシステムによって割り当てられ、パートナーの優先順位は LACP パケットから検出されています。

## 障害時の動作

LACP の障害時の動作は、PAgP の動作と同じです。既存チャネルのリンクで障害が発生すると、agport が更新され、トラフィックは残りのリンク上で 1 秒以内にハッシュされます。リンクの障害は次のような理由で発生します。

- ポートが取り外されている
- GBIC が削除されている
- 光ファイバが破損している
- ハードウェア障害（インターフェイスまたはモジュール）

障害発生後に再ハッシュする必要がないトラフィック（同じリンク上で送信を続けるトラフィック）では損失は発生しません。障害が発生したリンクを復元すると、agport に対する別のアップデートがトリガーされて、トラフィックが再度ハッシュされます。

## 設定オプション

LACP EtherChannel はさまざまなモードに設定できます。次の表に要約を示します。

| モード | 設定可能なオプション |
|---|---|
| | LACP ネゴシエーションなしで、リンク ネゴシエーションが強制的に形成されます。スイッチは、LACP パケットの送信も、着信 LACP パケットの処理も行いません。ネイバー ポートのモードが `on` の場合、チャネルが形成されます。 |
| | ポートは、ネイバー ポートの設定内容にかかわらず、チャネリングされません。 |
| `Passive` | このモードは、PAgP の `auto` モードに似ています。スイッチではチャネルの起動は行われませんが、着信 LACP パケットの認識は行われます。ピア（`LACP` スイッチはパケットを受信して応答し、最終的にはピアとともに集約チャネルを形成します。 |
| | これは、PAgP の `desirable` スイッチは aglink を形成するためにネゴシエーションを開始します。相手側が LACP `Active  Passive` |

## 検証（LACP と LACP）

この項の表は、直接接続された 2 台のスイッチ ( Switch-A と Switch-B ) の間で起こり得るすべての LACP チャネリング モードのシナリオの要約です。 一部の組み合わせでは、STP によってチャネリング側のポートが errdisable つまり、一部の組み合わせでは、チャネリング側のポートがシャットダウンされます。

| Switch-A のチャネル モード | Switch-B のチャネル モード | Switch-A のチャネル状態 | Switch-B のチャネル状態 |
|---|---|---|---|
| | | Channel LACP | Channel LACP |
| | | Not Channelerrdisable | Not Channel |
| | Passive | Not Channelerrdisable | Not Channel |
| | | Not Channelerrdisable | Not Channel |
| | | Not Channel | Not Channel |
| | Passive | Not Channel | Not Channel |
| | | Not Channel | Not Channel |
| Passive | Passive | Not Channel | Not Channel |
| Passive | | LACP Channel | LACP Channel |
| | | LACP Channel | LACP Channel |

## 検証 ( LACP と PAgP )

この項の表は、直接接続された 2 台のスイッチ ( Switch-A と Switch-B ) の間で起こり得るすべての LACP と PAgP チャネリング モードのシナリオの要約です。 一部の組み合わせでは、STP によってチャネリング側のポートが errdisable つまり、一部の組み合わせでは、チャネリング側のポートがシャットダウンされます。

| Switch-A のチャネル モード | Switch-B のチャネル モード | Switch-A のチャネル状態 | Switch-B のチャネル状態 |
|---|---|---|---|
| | | Channel LACP | Channel PAgP |
| | | Not Channelerrdisable | Not Channel |
| | | Not Channelerrdisable | Not Channel |
| | Desirable | Not Channelerrdisable | Not Channel |
| | | Not Channel | Not Channelerrdisable |
| | | Not Channel | Not Channel |
| | | Not Channel | Not Channel |
| | Desirable | Not Channel | Not Channel |
| Passive | | Not Channel | Not Channelerrdisable |
| Passive | | Not Channel | Not Channel |

| | | | |
|---|---|---|---|
| Passive | | Not Channel | Not Channel |
| Passive | Desirable | Not Channel | Not Channel |
| | | Not Channel | Not Channelerrdisable |
| | | Not Channel | Not Channel |
| | | Not Channel | Not Channel |
| | Desirable | Not Channel | Not Channel |

## 推奨事項

シスコでは、シスコ スイッチ間のチャネル接続で PAgP を有効にすることを推奨しています。PAgP はサポートしていないが LACP はサポートしているデバイスに対してチャネルを形成する場合は、両端のデバイスで LACP を `active LACP` どちらかのデバイスが LACP や PAgP をサポートしていない場合は、チャネルを `on` にハードコードする必要があります。

- **set channelprotocol lacp** *module*

  CatOS が動作するスイッチでは、Catalyst 4500/4000 および Catalyst 6500/6000 のすべてのポートで、チャネル プロトコル PAgP がデフォルトで使用されるため、LACP は実行しないでください。LACP を使用するようにポートを設定する場合は、モジュールのチャネル プロトコルを LACP に設定する必要があります。CatOS が動作するスイッチの同じモジュールで LACP と PAgP を実行することはできません。

- **set port lacp-channel** *port_range admin-key*

  **admin key（管理キー）パラメータは、LACP パケットで交換されます。**チャネルは、同じ admin key が設定されたポート間でのみ形成されます。**set port lacp-channel *port_range admin-key* コマンドで、チャネルに admin key 番号を割り当てます。**番号は **show lacp-channel group コマンドで表示できます。**set port lacp-channel *port_range admin-key* コマンドで、ポート範囲内のすべてのポートに同じ admin key を割り当てることができます。特定のキーを設定しない場合、admin key がランダムに割り当てられます。その場合、必要に応じて admin key を参照して、同じ agport に対するチャネリング ポートの追加と削除を管理できます。

- **set port lacp-channel** *port_range* **mode active**

  **set port lacp-channel *port_range mode active* コマンドでは、以前に同じ admin key を割り当てられていた一連のポートのチャネル モードを** `active`

さらに、LACP EtherChannel が確立された後、LACP では、30 秒のインターバル タイマー（Slow_Periodic_Time）が使用されます。長いタイムアウト（3 × Slow_Periodic_Time）を使用して、受信した LACPDU 情報を無効にするには 90 秒かかります。単方向リンクをより速く検出するには、UDLD を使用します。LACP タイマーは調整できません。現時点では、チャネル形成後のチャネル維持のために、高速 PDU 伝送（1 秒ごと）を使用するようにスイッチを設定することはできません。

## その他のオプション

アクセス レイヤで最小限の管理モデルを採用している場合は、ディストリビューション レイヤとコア レイヤでモードを `active` アクセス レイヤのスイッチはデフォルトの `passive`

## 単方向リンク検出

UDLD はシスコ独自の軽量プロトコルで、デバイス間の単方向通信のインスタンスを検出するために開発されました。FEFI のように、伝送メディアの双方向状態を検出する方法は他にもありますが、L1 検出メカニズムでは十分ではない場合があります。そのようなシナリオは、次のような事象が発生した場合に生じます。

- STP の予期しない動作
- 不正な、または過剰なパケットのフラッディング
- トラフィックのブラック ホール化

UDLD 機能は、光ファイバおよび銅線イーサネット インターフェイスの次のような障害状況に対処するための機能です。

- 物理的なケーブル構成をモニタし、配線が誤っているポートを `errdisable` としてシャットダウンします。
- 単方向リンクから保護します。メディアまたはポート/インターフェイスの動作不良に起因する単方向リンクが検出されると、影響を受けるポートが `errdisable` としてシャットダウンされ、対応する syslog メッセージが生成されます。
- さらに、UDLD アグレッシブ モードでは、以前に双方向と見なされていたリンクが、輻輳時に接続を失って使用不可になっていないかチェックされます。UDLD では、リンク全体の接続テストが継続的に実行されます。UDLD アグレッシブ モードの主な目的は、特定の障害状態におけるトラフィックのブラック ホール化を回避することです。

定常状態の単方向 BPDU フローを持つスパニング ツリーでは、これらの障害は重大な問題でした。あるポートが突然 BPDU を送信できなくなる状況は簡単に発生します。そのような状況になると、ネイバーの STP ステートがそのポートはまだ受信可能なため、この変更によりループが形成されます。

## 動作の概要

UDLD は LLC レイヤ上で動作する L2 プロトコルです（宛先 MAC 01-00-0c-cc-cc-cc、SNAP HDLC プロトコル タイプ 0x0111）。 UDLD を FEFI および自動ネゴシエーション L1 メカニズムと組み合わせて実行すると、リンクの物理的（L1）および論理的（L2）な整合性を検証できます。

UDLD では、FEFI および自動ネゴシエーションでは実行できない機能と保護が提供されます。具体的には、ネイバー情報の検出とキャッシング、正しく接続されていないポートのシャットダウン、ポイントツーポイント以外のリンク（メディア コンバータやハブを経由するリンク）での論理インターフェイスとポートの動作不良や障害の検出を実行できます。

UDLD には 2 つの基本的なメカニズムが採用されています。UDLD はネイバーについて学習し、最新情報をローカル キャッシュに保持します。そして、新しいネイバーが検出されるたび、またはネイバーからキャッシュの再同期要求を受けるたびに、一連の UDLD プローブ/エコー（Hello）メッセージを送信します。

UDLD は、UDLD が有効になっているすべてのポートでプローブ メッセージを絶えず送信します

。「トリガーとなる」特定の UDLD メッセージがポートで受信されるたびに、検出フェーズと検証プロセスが開始されます。このプロセスの最後ですべての有効な条件が満たされた場合、ポート状態は変更されません。条件を満たすためには、ポートが双方向であり、正しく配線されている必要があります。そうでない場合、そのポートは `errdisable` になり、syslog メッセージが表示されます。次のような syslog メッセージが表示されます。

- `UDLD-3-DISABLE:Unidirectional link detected on port [dec]/[dec].Port disabled`
- `UDLD-4-ONEWAYPATH:A unidirectional link from port [dec]/[dec] to port [dec]/[dec] of device [chars] was detected`

UDLD イベントを含む、ファシリティごとのすべてのシステム メッセージのリストについては、メッセージとリカバリ手順 [英語] ( Catalyst シリーズ スイッチ、7.6 ) を参照してください。

リンクが確立し、双方向として分類されると、UDLD は 15 秒間隔 ( デフォルト ) でプローブ/エコー メッセージをアドバタイズし続けます。次の表は、**show udld port コマンドの出力に表示される有効な UDLD リンクの状態を示しています。**

| ポートの状態 | コメント |
|---|---|
| 不確定 | 検出中であるか、または隣接する UDLD エンティティが無効になっているか、その送信がブロックされています。 |
| 該当なし | UDLD が無効になっています。 |
| シャットダウン | 単方向リンクが検出され、ポートが無効になっています。 |
| 双方向性 | 双方向リンクが検出されました。 |

- **ネイバー キャッシュのメンテナンス：UDLD は、UDLD ネイバー キャッシュの整合性を維持するために、すべてのアクティブ インターフェイスで Hello プローブ/エコー パケットを定期的に送信します。**Hello メッセージを受信すると、そのメッセージをキャッシュし、ホールドタイムとして定義されている最大時間が経過するまでメモリに保持します。ホールドタイムが経過すると、各キャッシュ エントリがエージング アウトします。ホールドタイム時間内に新しい Hello メッセージが受信されると、新しいメッセージによって古いエントリが置き換えられ、対応する存続可能時間タイマーがリセットされます。
- UDLD キャッシュの完全性を維持するため、UDLD 対応インターフェイスが無効になったとき、またはデバイスがリセットされたときは必ず、設定変更の影響を受けるインターフェイスの既存のキャッシュ エントリがすべてクリアされます。さらに、各ネイバーに対して、対応するキャッシュ エントリをフラッシュするよう通知するメッセージが少なくとも 1 つ送信されます。
- **エコー検出メカニズム：エコー メカニズムは検出アルゴリズムの基盤となります。**UDLD デバイスは新しいネイバーについて学習するか、同期していないネイバーから再同期要求を受信した場合は常に、接続の UDLD デバイス側で検出ウィンドウを開始または再開して、応答としてエコー メッセージをバースト送信します。この動作はすべてのネイバーで同じである必要があり、エコーの送信側は応答としてエコー バックを受信する予定でいます。検出ウィンドウが終了しても有効な応答メッセージを受信しない場合、そのリンクは単方向と見なされ、リンクの再確立またはポート シャットダウン プロセスがトリガーされます。

## コンバージェンス時間

STP ループを防止するため、CatOS 5.4(3) では UDLD のデフォルトのメッセージ間隔が 60 秒から 15 秒に短縮されました。これは、ブロックされたポートがフォワーディング ステートに移行

可能になる前に単方向リンクをシャットダウンするためです。

**注：メッセージ**間隔の値は、リンクアップまたは検出フェーズの後にネイバーがUDLDプローブを送信する速度を決定します。可能な場合は一貫性のある設定が望ましいですが、リンクの両端でメッセージ間隔が一致している必要はありません。UDLD ネイバーが確立されると、設定されたメッセージ間隔が送信され、そのピアのタイムアウト間隔が（3 X message_interval）になるように計算されます。 そのため、Hello（またはプローブ）が 3 回連続で受信されないとピアの関係がタイムアウトします。両側のメッセージ間隔が異なる場合、このタイムアウト値も異なることになります。

UDLD が単方向障害を検出するために必要な概算時間は（2.5 X message_interval + 4 秒）の式で表され、デフォルトのメッセージ間隔である 15 秒を代入すると約 41 秒になります。これは、STP の再コンバージェンスに通常必要な 50 秒よりもかなり短い時間です。NMP の CPU サイクルに多少余力があり、CPU 使用率のレベルを注意深くモニタしている場合は、メッセージ間隔を最小で 7 秒にまで短縮できます。このようなメッセージ間隔にすると、検出時間を大幅に短縮できます。

従って、UDLD は想定上、デフォルトのスパニング ツリー タイマーに依存しています。UDLD よりも短時間でコンバージするように STP を調整する場合は、CatOS 6.2 のループ ガード機能のような代替メカニズムを検討してください。トポロジによっては、RSTP（IEEE 802.1w）がミリ秒単位でコンバージェンスする特性があるため、RSTP を実装する際にも代替メカニズムを検討してください。このような場合には、UDLD とループ ガードを組み合わせて使用して、最大限の保護を実現します。ループ ガードでは、使用中の STP バージョンの速度で STP ループが防止され、UDLD では、個々の EtherChannel リンクで、または動作しなくなった方向に BPDU が流れない場合に単方向接続が検出されます。

**注**：UDLDでは、BPDUを送信しないCPUが原因で発生する障害(2 * FwdDelay + Maxage)など、すべてのSTP障害状況が検出されるわけではありません。 そのため、STP に依存するトポロジでは、UDLD を（CatOS 6.2 で導入された）ループ ガードとともに使用することを推奨します。

**注意：古いリリースの UDLD では、デフォルトのメッセージ間隔は 60 秒で、この時間は変更できません。**それらのリリースでは、スパニング ツリーのループ状態が起こりやすくなります。

## UDLD アグレッシブ モード

アグレッシブ UDLD は、双方向接続の継続的なテストが必要な、次のような（まれな）ケースに対処するために作成されました。そのため、アグレッシブ モード機能では、次のような危険な単方向リンクの状態に対する保護が強化されています。

- UDLD PDU の損失が対称的で、両側がタイムアウトした場合に、いずれのポートも errdisabled にならない場合。
- リンクの一方の側でポート スタック（送信（Tx）と Rx の両方）が生じている場合。
- リンクの一方の側がダウンしているが、もう一方の側がアップしたままの場合。
- 自動ネゴシエーションまたは別の L1 障害検出メカニズムが無効になっている場合。
- L1 FEFI メカニズムへの依存度を下げることが望ましい場合。
- ポイントツーポイントの FE/GE リンクの単方向リンク障害に対する最大限の保護が必要な場合。具体的には、2 つのネイバー間での障害を許容できない場合、UDLD のアグレッシブ プローブを「ハートビート」と見なすことができます。ハードビートの存在により、リンクの健全性が保証されます。

アグレッシブ UDLD を実装する最も一般的なケースは、自動ネゴシエーションや別の L1 障害検出メカニズムが無効になっているか、または使用できない場合に、バンドルのメンバーに対して

接続チェックを実行する場合です。これは EtherChannel 接続の場合に特に当てはまり、PAgP や LACP が有効になっている場合でも、定常状態では極端に小さい値の Hello タイマーは使用しないでください。この場合、アグレッシブ UDLD には、スパニング ツリー ループの発生を防止できるという利点もあります。

対称的な UDLD プローブ パケットの損失の一因となる状況を明らかにするのはさらに困難です。通常の UDLD では、リンクが双方向状態になった後でも、単方向リンク状態のチェックが行われることを理解しておく必要があります。UDLD の目的は、STP ループの原因になる L2 の問題を検出することです。BPDU は定常状態では一方向にのみ流れるため、通常、そのような問題は単方向の問題です。そのため、通常の UDLD を自動ネゴシエーションおよびループ ガード（STP に依存するネットワークの場合）とともに使用すれば、ほとんどの場合は問題ありません。しかし、輻輳が両方向に等しく影響を及ぼし、両方向で UDLD プローブの損失が生じるような場合には、UDLD アグレッシブ モードは有効です。たとえば、リンクの両端の CPU 使用率が上がると、UDLD プローブの損失が生じることがあります。また、次のいずれかのデバイスに障害が発生した場合にも、双方向の接続が失われます。

- 高密度波長分割多重（DWDM）トランスポンダ
- メディア コンバータ
- ハブ
- 別の L1 デバイス**注：障害**は自動ネゴシエーションでは検出できません。

このような障害状態では、アグレッシブ UDLD によってポートがエラー ディセーブルになります。ポイントツーポイントではないリンクで UDLD アグレッシブ モードを有効にする場合は、その影響を注意深く検討してください。メディア コンバータ、ハブ、または同様のデバイスを使用するリンクはポイントツーポイントではありません。中継デバイスにより UDLD パケットの転送が阻止され、リンクが不必要に強制シャットダウンされることがあります。

ポートのすべてのネイバーがエージ アウトすると、UDLD アグレッシブ モードが有効になっている場合には、同期がずれている可能性があるネイバーを再同期するために、リンクアップ シーケンスが再起動されます。この処理は、アドバタイズメントまたは検出フェーズのいずれかで実行されます。迅速な一連のメッセージ（8 回再試行に失敗した）後、リンクが引き続き「不確定」と見なされる場合、そのポートは `errdisable`

**注：一部の**スイッチでは、アグレッシブUDLDに対応していません。現時点では、Catalyst 2900XL と Catalyst 3500XL ではメッセージ間隔が 60 秒にハードコードされています。この間隔は、（デフォルトの STP パラメータを使用して）潜在的な STP ループから保護するには長すぎると考えられます。

## ルーテッド リンク上の UDLD

ここでは説明のために、ルーテッド リンクは次の 2 つの接続タイプのいずれかであるとします。

- 2 つのルータ ノード間のポイントツーポイントこのリンクは 30 ビットのサブネット マスクで設定されています。
- 複数のポートがあるが、ルーテッド接続のみをサポートしている VLAN例としては、分割された L2 コア トポロジです。

各 Interior Gateway Routing Protocol（IGRP）には、ネイバー関係とルートの収束の処理方法に関する独自の特性があります。この項で説明する特性は、現在広く使用されている Open Shortest Path First（OSPF）プロトコルおよび Enhanced IGRP（EIGRP）という 2 つのルーティング プロトコルと対比するときに関係してきます。

まず、ポイントツーポイントのルーテッド ネットワークで L1 または L2 の障害が発生すると、

L3 接続がほぼ瞬時に切断されることに注目してください。L1 または L2 で障害が発生すると、その VLAN のスイッチ ポートだけが not-connected 状態に移行するため、MSFC の自動状態機能によって、L2 と L3 のポート状態が約 2 秒で同期されます。この同期によって、L3 VLAN インターフェイスが up/down 状態（回線プロトコルは「down」）になります。

デフォルトのタイマー値が使用されていると仮定した場合、OSPF から 10 秒ごとに Hello メッセージが送信され、40 秒（4 X Hello）の dead 間隔が経過します。 これらのタイマーは OSPF ポイントツーポイント ネットワークとブロードキャスト ネットワークで一致しています。隣接関係（アジャセンシー）を形成するために OSPF には双方向通信が必要なため、最悪の場合のフェールオーバー時間は 40 秒になります。ポイントツーポイント接続の L1 または L2 の障害が全面的なものではなく、中途半端に動作するようなシナリオで、L3 プロトコルによる処理が必要になる場合でも、このフェールオーバーは発生します。UDLD の検出時間は OSPF dead タイマーの期限切れ時間（約 40 秒）と非常に近いため、OSPF の L3 ポイントツーポイント リンクに UDLD 通常モードを設定する利点は限られています。

多くの場合、EIGRP の方が OSPF よりも速く収束します。ただし、ネイバーがルーティング情報を交換するためには、必ずしも双方向通信が必要ではない点に注意してください。非常に特殊な中途半端に動作する障害のシナリオでは、他のイベントがそのネイバーを「active」にしてルートを作成するまで、トラフィックのブラック ホール化に対する脆弱性が EIGRP に存在します。UDLD 通常モードの場合、この項で説明されている状況を緩和できます。UDLD 通常モードでは、単方向リンク障害が検出されて、ポートがエラー ディセーブルになります。

任意のルーティング プロトコルを使用する L3 ルーテッド接続では、リンクの初期起動時の問題を UDLD 通常モードで引き続き保護できます。そのような問題には、ケーブル配線の間違いや障害のあるハードウェアなどがあります。さらに、UDLD アグレッシブ モードには、L3 ルーテッド接続に対して次の利点があります。

- トラフィックの不必要なブラック ホール化を防止する**注：場合**によっては最小タイマーが必要です。
- フラッピング リンクを `errdisable`
- L3 EtherChannel の設定に起因するループから保護する

## UDLD のデフォルト動作

UDLD はグローバルには無効ですが、ファイバ ポート上ではデフォルトですぐに有効になります。UDLD はスイッチ間でのみ必要となるインフラストラクチャ プロトコルなので、銅線ポートではデフォルトで無効になっています。銅線ポートは、ホスト アクセスによく使用されます。

**注：ネイバー**が双方向ステータスを取得するには、UDLDをグローバルかつインターフェイスレベルで有効にする必要があります。CatOS 5.4(3) 以降では、デフォルトのメッセージ間隔が 15 秒になっており、7 ~ 90 秒の間で設定できます。

errdisable 回復は、デフォルトではグローバルに無効になっています。errdisable 回復をグローバルに有効にすると、ポートは `errdisable` デフォルトの時間は 300 秒です。これは、グローバル タイマーの設定なので、スイッチ内のすべてのポートで維持されます。そのポートに対する errdisable タイムアウトを `disable` に設定すると、ポートの再有効化を手動で防止できます。set port errdisable-timeout *mod*/port disableコマンドを発行します。

**注：このコマンド**の使用は、使用しているソフトウェアのバージョンによって異なります。

アウトオブバンド ネットワーク管理機能を設定せずに UDLD アグレッシブ モードを実装する場合は、errdisable タイムアウト機能の使用を検討します。errdisable 状態が発生するとネットワー

クから分離する可能性があるアクセス レイヤやデバイスの場合には、特に検討が必要です。

errdisable イーサネット、ファスト イーサネット、ギガビット イーサネット、および 10 ギガビット イーサネット スイッチングの設定 [英語] を参照してください。

## 推奨事項

適切な機能やプロトコルとともに正しく使用すれば、ほとんどの場合、通常モードの UDLD で問題ありません。そのような機能やプロトコルには、次のものがあります。

- FEFI
- 自動ネゴシエーション
- ループ ガード

UDLD を展開する場合、双方向接続の継続的なテスト ( アグレッシブ モード ) が必要かどうかを検討します。通常、自動ネゴシエーションが有効になっている場合、L1 の障害検出は自動ネゴシエーションで補われるため、アグレッシブ モードにする必要はありません。

UDLD メッセージ間隔がデフォルトの 15 秒に設定されているシスコ スイッチ間のすべてのポイントツーポイント FE/GE リンクでは、UDLD 通常モードを有効にすることを推奨します。この設定では、デフォルトの 802.1d のスパニング ツリー タイマーの使用が想定されています。また、冗長性とコンバージェンスを STP に依存するネットワークでは、ループ ガードとともに UDLD を使用します。この推奨事項は、トポロジ内に STP ブロッキング ステートのポートが 1 つ以上存在するネットワークに当てはまります。

UDLD を有効にするには、次のコマンドを発行します。

```
set udld enable
!--- After global enablement, all FE and GE fiber !--- ports have UDLD enabled by default. set
udld enable port range
!--- This is for additional specific ports and copper media, if needed.
```

単方向リンクの症状が原因で error-disabled になっているポートは手動で有効にする必要があります。**set port enable コマンドを発行します。**

詳細については、『単方向リンク検出プロトコル機能の説明と設定』を参照してください。

## その他のオプション

単方向リンクによって生じる症状に対する保護を最大限に行うには、アグレッシブ モードの UDLD を次のように設定します。

```
set udld aggressive-mode enable port_range
```

さらに、コンバージェンスをより速くするために、両端の UDLD メッセージ間隔の値を 7 ~ 90 秒の間で次のように調整できます ( サポートされている場合 ) 。

```
set udld interval time
```

errdisable 状態になるとネットワークから分離する可能性があるデバイスには、errdisable タイムアウト機能の使用を検討します。この状況は、通常、アクセス レイヤや、アウトオブバンド ネットワーク管理機能を設定せずに UDLD アグレッシブ モードを実装する場合に当てはまります。

ポートが errdisable 次のコマンドを発行すると、タイムアウト間隔後に、ポートを再び有効にできます。

**注：タイ**ムアウト間隔はデフォルトで300秒です。

```
>set errdisable-timeout enable ?
bpdu-guard
!--- This is BPDU port-guard. channel-misconfig !--- This is a channel misconfiguration. duplex-
mismatch udld other !--- These are other reasons. all !--- Apply errdisable timeout to all
reasons.
```

パートナー デバイスが UDLD に対応していない場合 ( エンド ホストやルータなどの場合 ) は、UDLD を実行しないでください。次のコマンドを実行します。

```
set udld disable port_range
```

## UDLD のテストとモニタ

不良 GBIC などの、実際に障害のあるコンポーネントや単方向コンポーネントがない状態で、ラボで UDLD をテストするのは簡単ではありません。UDLD は、ラボで通常取り扱う障害シナリオよりも発生頻度の低いシナリオを検出するために設計されています。たとえば、目的の errdisable L1 そうしないと、物理ポートがダウンして、UDLD のメッセージ通信がリセットされます。UDLD 通常モードでは、リモート エンドは不確定状態に移行します。UDLD アグレッシブ モードを使用している場合、リモート エンドは errdisable

UDLD のネイバー PDU の損失をシミュレートするテスト方法はもう 1 つあります。MAC レイヤ フィルタを使用して、UDLD や CDP のハードウェア アドレスをブロックし、その他のアドレスを通過させる方法です。

UDLD をモニタするには、次のコマンドを発行します。

```
>show udld

UDLD              : enabled
Message Interval  : 15 seconds
```

```
>show udld port 3/1

UDLD              : enabled
Message Interval  : 15 seconds
Port      Admin Status  Aggressive Mode  Link State
--------  ------------  ---------------  ----------------
3/1       enabled       disabled         bidirectional
```

enable show udld neighbor 隠しコマンドを発行して、UDLD キャッシュの内容を ( CDP が行う方法で ) 確認できます。プロトコル固有の異常の有無を確認するには、多くの場合、UDLD キャッシュと CDP キャッシュを比較するのが便利な方法です。CDP も影響を受けている場合、通常

はすべての PDU と BPDU が影響を受けています。そのため、STP もチェックしてください。たとえば、最近のルート ID の変更、ルート ポートや指定ポートの配置変更をチェックします。

```
>show udld neighbor 3/1

Port  Device Name            Device ID    Port-ID OperState
----- -------------------- ------------ ------- ----------
3/1   TSC07117119M(Switch)   000c86a50433 3/1     bidirectional
```

また、UDLD のステータスと設定の一貫性は、Cisco UDLD SNMP MIB 変数を使用してモニタできます。

## ジャンボ フレーム

GE や 10 GE を含むすべてのイーサネット ポートのデフォルトの最大伝送ユニット（MTU）フレーム サイズは 1518 バイトです。ジャンボ フレーム機能を使用すると、イーサネットの標準フレーム サイズよりも大きなフレームにインターフェイスを切り替えることができます。この機能は、サーバ間のパフォーマンスを最適化し、元のフレームのサイズを大きくするマルチプロトコル ラベル スイッチング（MPLS）、802.1Q トンネリング、および L2 Tunneling Protocol Version 3（L2TPv3）などのアプリケーションをサポートするのに役立ちます。

### 動作の概要

IEEE 802.3 規格の仕様では、イーサネットの最大フレーム サイズは、通常フレームの場合は 1518 バイト、802.1Q カプセル化フレームの場合は 1522 バイトに規定されています。802.1Q カプセル化フレームは「ベビー ジャイアント」と呼ばれることもあります。 一般に、特定のイーサネット接続に指定されたイーサネットの最大長を超えるパケットはジャイアント フレームに分類されます。ジャイアント パケットは、ジャンボ フレームとも呼ばれます。

特定のフレームの MTU サイズが 1518 バイトを超えてしまう理由はさまざまです。次にいくつかの例を示します。

- ベンダー固有の要件：アプリケーションおよび特定の NIC では、標準の 1500 バイト以外の MTU サイズを指定できます。さまざまな研究により、イーサネット フレームのサイズを大きくすれば平均スループットが向上することが証明されているため、そのような MTU サイズを指定する傾向があります。
- トランキング：スイッチまたは他のネットワーク デバイス間で VLAN ID 情報を転送するために、トランキングを使用して標準のイーサネット フレームが拡張されています。現在、最も広く使用されている形態のトランキングはシスコ独自の ISL カプセル化と IEEE 802.1Q です。
- MPLS：MPLS がインターフェイスで有効になった後、パケットのフレーム サイズが拡張される可能性がある。この拡張は、MPLS タグが付いたパケットのラベル スタックにあるラベルの数によって異なります。1 つのラベルの合計サイズは 4 バイトです。ラベル スタックの合計サイズは n X 4 バイトです。ラベル スタックが形成されている場合は、フレームが MTU を超過する場合があります。
- 802.1Q トンネリング：802.1Q トンネリング パケットには、2 つの 802.1Q タグが含まれており、通常は 1 つのタグだけがハードウェアに認識されます。そのため、内部タグにより、MTU の値（ペイロード サイズ）に 4 バイトが追加されます。
- Universal Transport Interface（UTI）/L2TPv3：UTI/L2TPv3 では、IP ネットワーク上を転送される L2 データがカプセル化される。このカプセル化により、元のフレーム サイズが最大で 50 バイト増えることがあります。新しいフレームには、新しい IP ヘッダー（20 バイト

）、L2TPv3 ヘッダー（12 バイト）、および新しい L2 ヘッダーが含まれます。L2TPv3 のペイロードは、L2 ヘッダーを含む完全な L2 フレームで構成されています。

各 Catalyst スイッチのさまざまなフレーム サイズをサポートする能力は、ハードウェアとソフトウェアを含む多くの要因によって決まります。同じプラットフォーム内でも、特定のモジュールでは、他よりも大きなフレーム サイズがサポートできる場合があります。

- Catalyst 5500/5000 スイッチでは、CatOS 6.1 リリースでジャンボ フレームがサポートされています。ポート上でジャンボ フレーム機能を有効にすると、MTU サイズは 9216 バイトに増えます。10/100 Mbps のシールドなしツイスト ペア（UTP）ベースのライン カードでは、8092 バイトの最大フレーム サイズだけがサポートされています。この制限は ASIC の制限です。一般的には、ジャンボ フレーム サイズ機能を有効にした場合の制限はありません。この機能は、トランキング/非トランキングおよびチャネリング/非チャネリングで使用できます。
- Catalyst 4000 スイッチ（Supervisor Engine 1（WS-X4012）および Supervisor Engine 2（WS-X4013））では、ASIC の制限のためにジャンボ フレームはサポートされていません。ただし、802.1Q トランキングは例外です。
- Catalyst 6500 シリーズ プラットフォームでは、CatOS リリース 6.1(1) 以降でジャンボ フレーム サイズをサポートできます。ただし、このサポートは使用するライン カードのタイプに左右されます。一般的には、ジャンボ フレーム サイズ機能を有効にした場合の制限はありません。この機能は、トランキング/非トランキングおよびチャネリング/非チャネリングで使用できます。個々のポートでジャンボ フレームのサポートが有効になると、デフォルトの MTU サイズは 9216 バイトになります。CatOS を使用してデフォルトの MTU を設定することはできません。ただし、Cisco IOSソフトウェアリリース12.1(13)Eでは、デフォルトのMTUを上書きするため**に、system jumbomtuコ**マンドが導入されました。

詳細については、Catalyst スイッチでのジャンボ/ジャイアント フレーム サポートの設定例 [英語] を参照してください。

次の表に、Catalyst 6500/6000 シリーズ スイッチ用のさまざまなライン カードでサポートされる MTU サイズを示します。

**注：MTUサイズ**またはパケットサイズはイーサネットペイロードのみを参照します。

| ライン カード | MTUサイズ |
|---|---|
| デフォルト | 9216 バイト |
| WS-X6248-RJ-45、WS-X6248A-RJ-45 WS-X6248-TEL、WS-X6248A-TEL WS-X6348-RJ-45(V)、WS-X6348-RJ-21(V) | 8092 バイト（PHY チップによる制限） |
| WS-X6148-RJ-45(V)、WS-X6148-RJ-21(V) WS-X6148-45AF、WS-X6148-21AF | 9100 バイト（100 Mbps 時）9216 バイト（10 Mbps 時） |

| | |
|---|---|
| WS-X6148A-RJ-45、WS-X6148A-45AF、WS-X6148-FE-SFP | 9216 バイト |
| WS-X6324-100FX-MM、-SM、WS-X6024-10FL-MT | 9216 バイト |
| Supervisor Engine 1、2、32、および 720 の WS-X6548-RJ-45、WS-X6548-RJ-21、WS-X6524-100FX-MM WS-X6148X2-RJ-45、WS-X6148X2-45AF WS-X6196-RJ-21、WS-X6196-21AF WS-X6408-GBIC、WS-X6316-GE-TX、WS-X6416-GBIC WS-X6516-GBIC、WS-X6516A-GBIC、WS-X6816-GBIC アップリンク | 9216 バイト |
| WS-X6516-GE-TX | 8092 バイト（100 Mbps 時）9216 バイト（10 または 1000 Mbps 時） |
| WS-X6148-GE-TX、WS-X6148V-GE-TX、WS-X6148-GE-45AF、WS-X6548-GE-TX、WS-X6548V-GE-TX、WS-X6548-GE-45AF | 1500 バイト（ジャンボフレームのサポートなし） |
| WS-X6148A-GE-TX、WS-X6148A-GE-45AF、WS-X6502-10GE、WS-X67xx シリーズ | 9216 バイト |
| OSM ATM（OC12c） | 9180 バイト |
| OSM CHOC3、CHOC12、CHOC48、CT3 | 9216 バイト（OCx および DS3）7673 バイト（T1/E1） |
| Flex WAN | 7673 バイト（CT3 T1/DS0）9216 バイト（OC3c POS）7673 バイ |

| | |
|---|---|
| | ト（T1） |
| CSM（WS-X6066-SLB-APC） | 9216 バイト（CSM 3.1(5) および 3.2(1) の時点） |
| OSM POS OC3c、OC12c、OC48c。OSM DPT OC48c、OSM GE WAN | 9216 バイト |

## レイヤ 3 ジャンボ フレーム サポート

Supervisor Engine 上で動作する CatOS および MSFC 上で動作する Cisco IOS ソフトウェアを備えた Catalyst 6500/6000 スイッチでは、Cisco IOS® ソフトウェア リリース 12.1(2)E 以降で PFC/MSFC2、PFC2/MSFC2 またはそれ以降のハードウェアを使用する場合に L3 ジャンボ フレームがサポートされます。入力と出力の両方の VLAN がジャンボ フレーム用に設定されている場合、すべてのパケットが PFC によりワイヤ スピードでハードウェア スイッチングされます。入力の VLAN がジャンボ フレーム用に設定されていて、出力の VLAN が設定されていない場合のシナリオは次の 2 つです。

- エンド ホストから Don't Fragment（DF）ビットが設定されたジャンボ フレームが（パス MTU ディスカバリ用に）送信される場合：パケットが廃棄され、Internet Control Message Protocol（ICMP）到達不能メッセージがメッセージ コード fragment needed and DF set とともにエンド ホストに送信されます。
- エンドホストから DF ビットが設定されていないジャンボ フレームが送信される場合：パケットが MSFC2/MSFC3 にパントされ、ソフトウェアで断片化とスイッチングが行われます。

次の表は、さまざまなプラットフォームでの L3 ジャンボ フレームのサポートの要約です。

| **L3 スイッチまたはモジュール** | **最大 L3 MTU サイズ** |
|---|---|
| Catalyst 2948G-L3/4908G-L3 シリーズ | ジャンボ フレームはサポートされません。 |
| Catalyst 5000 RSM[1]/RSFC2 | ジャンボ フレームはサポートされません。 |
| Catalyst 6500 MSFC1 | ジャンボ フレームはサポートされません。 |
| Catalyst 6500 MSFC2 以降 | Cisco IOS ソフトウェア リリース 12.1(2)E：9216 バイト |

1 RSM = ルート スイッチ モジュール

2 RSFC = ルート スイッチ フィーチャ カード

## ネットワーク パフォーマンスの考慮事項

WAN（インターネット）上の TCP のパフォーマンスについては広く研究が行われてきました。次の公式は、TCP のスループットには次の要因に基づく上限があることを示しています。

- 最大セグメント サイズ（MSS）。MTU 長から TCP/IP ヘッダーの長さを引いた値です。
- ラウンド トリップ時間（RTT）
- パケット損失

$$Throughput \leq\sim 0.7 \times MSS / \left(RTT \times \sqrt{packet\_loss}\right)$$

この公式によれば、達成可能な TCP の最大スループットは、MSS と正比例の関係にあります。RTT とパケット損失が一定の場合、パケット サイズを 2 倍にすれば、TCP スループットを 2 倍にできます。同様に、1518 バイトのフレームの代わりにジャンボ フレームを使用すると、サイズが 6 倍になるので、イーサネット接続の TCP スループットが 6 倍に向上する可能性があります。

第二に、サーバ ファームのパフォーマンスへの要求は増大し続けているため、ネットワーク ファイル システム（NFS）の UDP データグラムをより高いデータ レートで処理できる、より効率的な方法が求められています。NFS は、UNIX ベースのサーバ間でファイルを転送するために最もよく利用されているデータ ストレージ メカニズムであり、8400 バイトのデータグラムが特長です。イーサネットの拡張 9 KB MTU では、（NFS などの）8 KB のアプリケーション データグラムとパケット ヘッダーのオーバーヘッドを 1 つのジャンボ フレームで十分に転送できます。NFS ブロックを別々の UDP データグラムにフラグメント化するためのソフトウェアは不要になるため、この機能により付随的に、ホスト上でのさらに効率的なダイレクト メモリ アクセス（DMA）転送が可能になります。

## 推奨事項

ジャンボ フレームのサポートが必要な場合、ジャンボ フレームの使用は、すべてのスイッチ モジュール（L2）とインターフェイス（L3）でジャンボ フレームがサポートされているネットワークのエリアに制限します。このように設定すれば、パス内のすべての場所でフラグメンテーションを防止できます。パスでサポートされるフレーム長より長いジャンボ フレームを設定すると、フラグメンテーションが必要になるため、この機能を使用する利点が失われます。この「ジャンボ フレーム」の項にある表に示されているように、サポートされる最大パケット サイズに関しては、プラットフォームやライン カードによって異なります。

ホスト デバイスがある L2 VLAN 全体に対しては、ネットワーク ハードウェアで一般的にサポートされている最小の値である MTU サイズを指定してジャンボ フレーム対応のホスト デバイスを設定します。ジャンボ フレームがサポートされているモジュールでジャンボ フレームのサポートを有効にするには、次のコマンドを発行します。

```
set port jumbo mod/port enable
```

さらに、L3 境界を越えてジャンボ フレームをサポートする場合は、該当するすべての VLAN インターフェイスで使用可能な MTU の最大値である 9216 バイトを設定します。VLAN インターフェイスで、次の **mtu コマンドを発行します。**

```
interface vlan vlan# mtu 9216
```

このように設定すれば、モジュールでサポートされる L2 ジャンボ フレーム MTU は常に、トラフィックが通過する L3 インターフェイスに設定されている値以下になります。これで、トラフ

ィックが VLAN から L3 インターフェイスを超えてルーティングされる場合のフラグメンテーションが防止されます。

# 管理設定

この項では、Catalyst ネットワークの制御、プロビジョニング、およびトラブルシューティングに役立つ考慮事項について説明します。

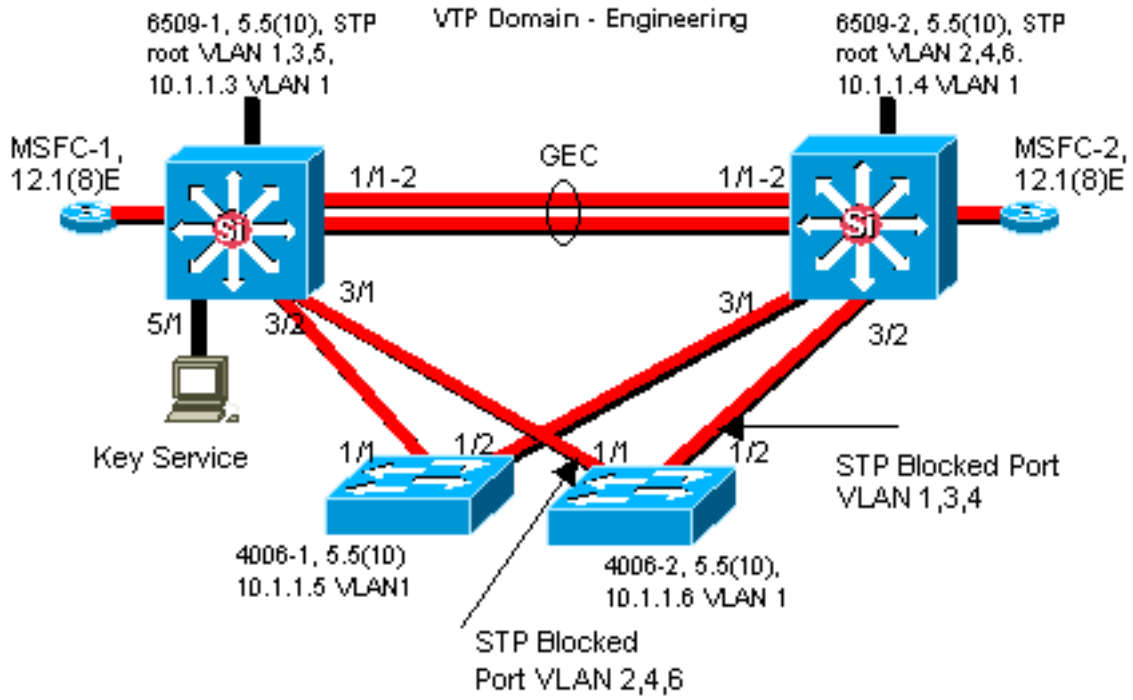
## ネットワーク図

明確なネットワーク図はネットワーク運用の基本部分です。ネットワーク図はトラブルシューティングの際に重要となり、ネットワーク停止時に情報をベンダーやパートナーにエスカレーションするための唯一の最も重要な手段となります。ネットワーク図の準備やアクセシビリティを過小評価しないでください。

### 推奨事項

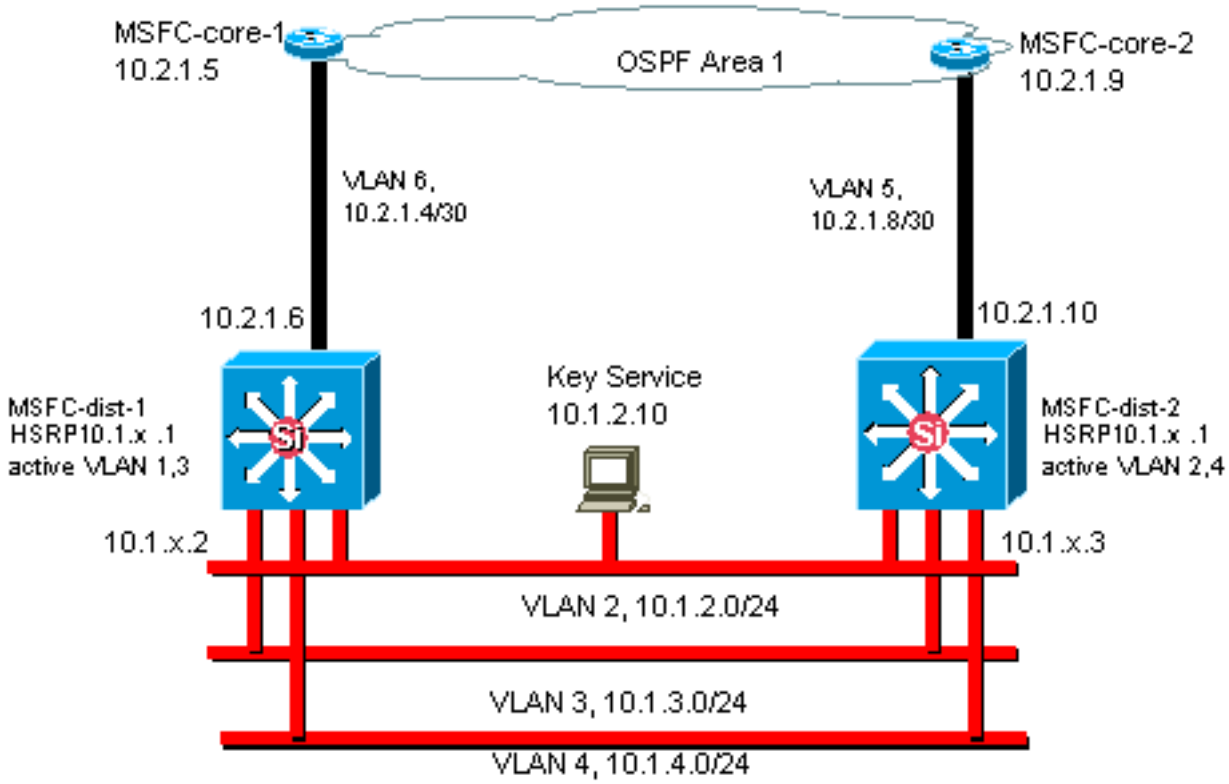
シスコでは、次の 3 つの図の作成を推奨しています。

- **全体図：最大規模のネットワークの場合でも、エンドツーエンドの物理接続と論理接続を示す図は重要です。**階層的な設計を実装している企業では、各レイヤを別々にドキュメント化するのが一般的です。ただし、計画時や問題解決時には、多くの場合、ドメインの全体的なリンク情報がわかれば十分です。
- **物理図：すべてのスイッチおよびルータ ハードウェアとその配線を示します。**トランク、リンク、速度、チャネル グループ、ポート番号、スロット、シャーシ タイプ、ソフトウェア、VTP ドメイン、ルート ブリッジ、バックアップ ルート ブリッジ プライオリティ、MAC アドレス、VLAN ごとのブロックされたポートなどを記入する必要があります。Catalyst 6500/6000 MSFC などの内部デバイスは、トランク経由で接続している枝上のルータとして表すとさらに明確になります。




- **論理図**：L3 機能（オブジェクトとしてルータ、イーサネット セグメントとして VLAN）のみを示します。IP アドレス、サブネット、セカンダリ アドレッシング、HSRP アクティブおよ

びスタンバイ、アクセスコア ディストリビューション レイヤ、ルーティング情報などを記入する必要があります。




## インバンド管理

設定によっては、スイッチのインバンド（内部）管理インターフェイス（sc0 として知られている）で次のデータを処理する必要があります。

- SNMP、Telnet、セキュア シェル（SSH）プロトコル、および syslog などのスイッチ管理プロトコル
- ブロードキャストやマルチキャストなどのユーザ データ
- STP BPDU、VTP、DTP、CDP などのスイッチ制御プロトコル

シスコのマルチレイヤ設計では、スイッチド ドメイン全体に広がり、すべての sc0 インターフェイスを含む管理 VLAN を 1 つ設定するのが普通です。こうすることで、管理トラフィックがユーザ トラフィックから分離されるため、スイッチ管理インターフェイスのセキュリティが向上します。この項では、デフォルトの VLAN 1 を使用して管理トラフィックをユーザ トラフィックと同じ VLAN 内のスイッチに送信することの意味と起こり得る問題について説明します。

## 動作の概要

ユーザ データに VLAN 1 を使用する際の一番の懸念事項は、Supervisor Engine の NMP は一般的に、エンド ステーションで生成される多くのマルチキャストおよびブロードキャスト トラフィックによって中断される必要がないことです。古い Catalyst 5500/5000 ハードウェア、特に Supervisor Engine I と Supervisor Engine II では、このトラフィックを処理するためのリソースは限定されています（もっとも、この原則はすべての Supervisor Engine に当てはまります）。Supervisor Engine の CPU、バッファ、またはバックプレーンへのインバンド チャネルが、不必要なトラフィックをリスニングするために完全に占有されている場合、制御フレームが失われるおそれがあり、最悪の場合、スパニング ツリーのループや EtherChannel の障害につながります。

Catalyst で show interface および show ip stats コマンドを発行すると、ユニキャスト トラフィックとブロードキャスト トラフィックの割合、および非 IP トラフィックと IP トラフィックの割合が表示されます ( 管理 VLAN では通常表示されません ) 。

古い Catalyst 5500/5000 ハードウェアのヘルス チェックをさらに行うには、**show inband** / *biga (隠しコマンド)* (リソースエラー(RscrcErrors)の場合、ルータでのバッファのドロップと同様)。このようなリソース エラーが増え続けている場合、管理 VLAN で大量のブロードキャスト トラフィックが発生している可能性があるため、システム パケットの受信にメモリを使用できない状況にあります。1 つのリソース エラーは、Supervisor Engine が BPDU などのパケットを処理できないことを意味します。その結果、スパニング ツリーなどのプロトコルにより、失われた BPDU が再送信されないため、すぐに問題が生じる可能性があります。

## 推奨事項

このドキュメントの「Cat Control」の項で説明したように、VLAN 1 は特別な VLAN で、ほとんどのコントロール プレーン トラフィックをタグ付けして処理します。VLAN 1 はデフォルトですべてのトランクで有効になっています。大規模なキャンパス ネットワークでは、VLAN 1 の **STP ドメイン**の直径に注意する必要があります。ネットワークの一部での不安定な状態が、 VLAN 1 に影響を与え、それによってコントロールプレーンの安定性、ひいては他のすべての VLAN での STP の安定性が影響を受ける可能性があります。CatOS 5.4 以降では、VLAN 1 でのユーザ データの伝送と STP の実行を次のコマンドで制限できます。

```
clear trunk mod/port vlan 1
```

ネットワーク アナライザで見るとわかりますが、このコマンドを実行しても、VLAN 1 のスイッチ間でのコントロール パケットの送信は停止されません。しかし、データは転送されず、STP はこのリンク上で実行されません。したがって、この手法を使用すれば VLAN 1 をより小さい障害ドメインに分割できます。

**注：** 現時点では、3500 および 2900XL シリーズで VLAN 1 トランクをクリアすることはできません。

キャンパス設計では、比較的小さいスイッチ ドメインと、それに対応した小規模の障害/L3 境界にユーザ VLAN を制限するように考慮している場合でも、一部のお客様では、管理 VLAN の扱いが異なっている傾向があり、ネットワーク全体を単一の管理サブネットでカバーしようとしています。中央の NMS アプリケーションが管理対象のデバイスと L2 で隣接していなければならない技術的な理由はなく、またセキュリティ上適切な理由もありません。シスコでは、管理 VLAN の直径をユーザ VLAN と同じルーテッド ドメイン構造に制限すること、およびネットワーク管理のセキュリティを向上する方法としてアウトオブバンド管理と CatOS 6.x の SSH サポートを検討することを推奨しています。

## その他のオプション

ただし、一部のトポロジでは、これらの推奨事項について設計上の考慮が必要です。たとえば、理想的で一般的なシスコ マルチレイヤ設計では、アクティブなスパニング ツリーの使用を避けます。そのためには、各 IP サブネットと VLAN を 1 台のアクセス レイヤ スイッチ、またはスイッチのクラスタに限定する必要があります。このような設計では、アクセス レイヤへのトランキングを設定できません。

L2 アクセス レイヤと L3 ディストリビューション レイヤ間で管理 VLAN を伝送するために、別

の管理 VLAN を作成してトランキングを有効にすべきかどうかという質問に対する簡単な答えはありません。シスコのエンジニアとの設計レビューでは、次の 2 つのオプションが検討されます。

- **オプション 1**：2 ~ 3 の固有の VLAN をディストリビューション レイヤから各アクセス レイヤ スイッチにトランキングする。これで、データ VLAN、音声 VLAN、管理 VLAN などを利用でき、STP が非アクティブだという利点も得られます（VLAN 1 がトランクから削除されている場合、追加の設定手順が必要です）。 このソリューションでは、障害回復中にルーティングされたトラフィックが一時的にブラック ホール化しないようにするために、次の点も設計時に考慮する必要があります。トランクの STP PortFast（CatOS 7.x 以降）または STP 転送との VLAN 自動ステート同期（CatOS 5.5(9) より後）。
- **オプション 2**：1 つの VLAN をデータと管理に使用することを容認する。より強力な CPU やコントロール プレーンのレート制限機構などを備えた最新のスイッチ ハードウェアでは、比較的小さいブロードキャスト ドメインの設計がマルチレイヤ設計で推奨されているため、多くのお客様にとって sc0 インターフェイスとユーザ データの分離は以前ほど重要な問題ではなくなっています。最終的には、その VLAN のブロードキャスト トラフィック プロファイルを調査し、スイッチ ハードウェアの能力についてシスコのエンジニアと話し合った上で判断するのが一番良いでしょう。実際に、管理 VLAN にそのアクセス レイヤ スイッチ上のすべてのユーザが含まれる場合は、このドキュメントの「セキュリティの設定」の項の説明に従い、スイッチをユーザから保護するために IP 入力フィルタを使用することを強く推奨します。

## アウトオブバンド管理

前の項の議論を一歩進めると、トラフィック駆動のイベントやコントロール プレーンのイベントが発生したとしても、リモートから常にデバイスに到達できるように、実稼働ネットワークの周囲に別の管理インフラストラクチャを構築することで、ネットワーク管理の可用性を大幅に向上させることができます。一般的には、次の 2 つのアプローチが取られます。

- 専用 LAN を使用したアウトオブバンド管理
- ターミナル サーバを使用したアウトオブバンド管理

### 動作の概要

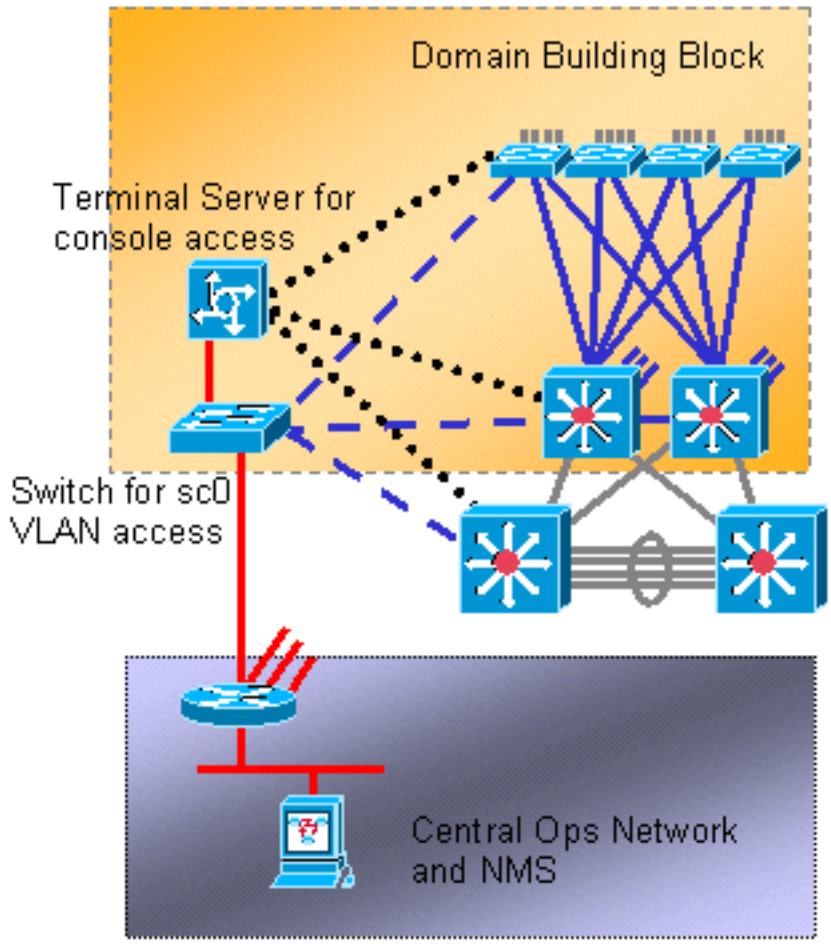
ネットワーク内のすべてのルータとスイッチには、管理 VLAN 上のアウトオブバンド イーサネット管理インターフェイスを搭載できます。デバイスごとに 1 つのイーサネット ポートを管理 VLAN に設定し、sc0 インターフェイスを介して、そのポートを実稼働ネットワークの外部にある別のスイッチド管理ネットワークにケーブル接続します。Catalyst 4500/4000 スイッチには Supervisor Engine 上に特別な me1 インターフェイスがあります。このインターフェイスはスイッチ ポートとしてではなく、アウトオブバンド管理用にのみ使用されます。

また、Cisco 2600 または 3600 から RJ-45 to シリアル ケーブルを介して、レイアウト内のすべてのルータとスイッチのコンソール ポートにアクセスするように構成することで、ターミナル サーバ接続を実現できます。ターミナル サーバを使用すると、バックアップ シナリオの構成（すべてのデバイスの補助ポートのモデムなど）が不要になります。ターミナル サーバの補助ポートにモデムを 1 台設定すれば、ネットワーク接続障害の発生時に他のデバイスへのダイヤルアップ サービスを提供できます。

### 推奨事項

この配置では、多数のインバンド パスに加えて、すべてのスイッチとルータに通じる 2 本のアウトオブバンド パスを使用できるため、可用性の高いネットワーク管理が可能になります。アウトオブバンドには次の役割があります。

- アウトオブバンドにより、管理トラフィックがユーザ データから分離される。
- アウトオブバンドは、分離したサブネット、VLAN、およびスイッチ内に管理 IP アドレスを持つため、セキュリティが向上する。
- アウトオブバンドにより、ネットワーク障害時でも管理データを確実に配信できる。
- アウトオブバンドには、管理 VLAN にアクティブなスパニング ツリーがない。冗長性は重要ではありません。




## システム テスト

### ブートアップ診断

システムのブートアップ時には、信頼性の高い動作可能なプラットフォームの利用を可能にするために多数のプロセスが実行されます。その結果、障害のあるハードウェアによるネットワークの中断を防止できます。Catalyst のブート診断は、POST ( 電源投入時自己診断テスト ) とオンライン診断に分かれています。

### 動作の概要

プラットフォームおよびハードウェアの設定に応じて、ブートアップ時とカードがシャーシにホットスワップされた場合には異なる診断が実行されます。診断レベルが高ければより多くの問題が検出されますが、ブート サイクルが長くなります。POST ( 電源投入時自己診断テスト ) 診断では次の 3 つのレベルを選択できます ( すべてのテストで DRAM、RAM、およびキャッシュの存

在とサイズがチェックされ、それらが初期化されます）。

| 動作の概要 | | | |
|---|---|---|---|
| バイパス | N/A | 3 | CatOS 5.5 以前を使用している 4500/4000 シリーズでは使用できません。 |
| 最小 | DRAM の最初の MB に対してのみパターン書き込みテストが実行されます。 | 30 | 5500/5000 および 6500/6000 シリーズのデフォルト。<br>4500/4000 シリーズでは使用できません。 |
| 完了 | すべてのメモリに対してパターン書き込みテストが実行されます。 | 60 | 4500/4000 シリーズのデフォルト。 |

## オンライン診断

これらのテストではスイッチ内部のパケット パスがチェックされます。したがって、オンライン診断は単純なポート テストではなく、システム全体のテストである点に注意してください。Catalyst 5500/5000 および 6500/6000 スイッチでは、最初にスタンバイ Supervisor Engine からテストが実行され、次にプライマリ Supervisor Engine から同じテストが実行されます。診断に要する時間はシステムの構成（スロット、モジュール、ポートの数）によって異なります。 テストには次の 3 つのカテゴリがあります。

- ループバック テスト：Supervisor Engine NMP から各ポートにパケットを送信し、NMP に戻ってきたパケットのエラーを調べます。
- バンドリング テスト：最大 8 ポートのチャネルを作成し、その agport に対してループバック テストを実行して、特定のリンクへのハッシングを確認します（詳細は、「EtherChannel」セクションを参照）。
- Enhanced Address Recognition Logic（EARL）テスト：中央のスーパーバイザ エンジンとインライン イーサネット モジュールの L3 リライト エンジンがどちらもテストされます。ハードウェア転送エントリとルーテッド ポートが作成された後、NMP から各モジュールのスイッチング ハードウェア経由で（プロトコル カプセル化タイプごとに）サンプル パケットが送信され、NMP に戻ります。このテストは Catalyst 6500/6000 PFC 以降のモジュールを対象としています。

完全なオンライン診断には約 2 分かかります。最小限の診断では、Supervisor Engine 以外のモジュールのバンドル テストやリライト テストは実行されず、約 90 秒で終了します。

メモリ テスト中に書き込まれたパターンとリード バックされたパターンに違いが見つかった場合、ポートの状態が `faulty` に変わります。これらのテスト結果は、検査対象のモジュール番号を指定して **show test コマンドを発行すると確認できます。**

```
>show test 9

Diagnostic mode: complete (mode at next reset: complete)
!--- Configuration setting. Module 9 : 4-port Multilayer Switch Line Card Status for Module 9 :
```

```
PASS Port Status : Ports 1 2 3 4 ----------------- . . . . Line Card Diag Status for Module 9 (.
= Pass, F = Fail, N = N/A) Loopback Status [Reported by Module 1] : Ports 1 2 3 4 ----------
--- . . F . !--- Faulty. Channel Status : Ports 1 2 3 4 ----------------- . . . .
```

## 推奨事項

シスコでは、最大限の障害検出を実現し、通常運用時のネットワーク停止を防止するために、すべてのスイッチで完全な診断を実行する設定にすることを推奨しています。

**注：この**変更は、次にデバイスを起動するまで有効になりません。完全な診断を設定するには、次のコマンドを発行します。

```
set test diaglevel complete
```

## その他のオプション

場合によっては、完全な診断の実行を待つよりもブートアップ時間の短縮が優先されることがあります。システムの起動には他にもさまざまな要素やタイミングが関係していますが、全体的に見ると、POST およびオンライン診断を実行するとブートアップ時間が 1/3 ほど長くなります。1 つの Supervisor Engine、9 スロット シャーシがフル構成されている Catalyst 6509 でテストした場合、合計ブート時間は、完全な診断で約 380 秒、最小限の診断で約 300 秒、診断をバイパスすると約 250 秒でした。バイパスを設定するには、次のコマンドを発行します。

```
set test diaglevel bypass
```

**注**：Catalyst 4500/4000では最小限の診断を設定できますが、この場合も完全なテストが実行されます。将来的には、このプラットフォームでも最小モードがサポートされる予定です。

## 実行時診断

システムが稼働可能になると、スイッチの Supervisor Engine では他のモジュールに対するさまざまなモニタリングが実行されます。管理メッセージ（アウトオブバンド管理バス上で動作する Serial Control Protocol（SCP））を介してモジュールに到達できない場合、Supervisor Engine はそのカードの再起動を試みるか、または適切なアクションを実行します。

## 動作の概要

Supervisor Engine ではさまざまなモニタリングが自動的に実行され、設定する必要はありません。Catalyst 5500/5000 および 6500/6000 の場合、スイッチの次の構成要素がモニタされます。

- NMP（ウォッチドッグでのモニタ）
- Enhanced EARL チップのエラー
- Supervisor Engine からバックプレーンへのインバンド チャネル
- モジュール（アウトオブバンド チャネル上でのキープアライブでのモニタ）（Catalyst 6500/6000）
- アクティブ Supervisor Engine（スタンバイ Supervisor Engine によるステータスのモニタリング）（Catalyst 6500/6000）

# システムおよびハードウェアのエラー検出

## 動作の概要

CatOS 6.2 以降には、重要なシステム コンポーネントとハードウェアレベルのコンポーネントをモニタするための機能が追加されています。次の 3 つのハードウェア コンポーネントがサポートされています。

- インバンド
- ポート カウンタ
- メモリ

この機能が有効になっているときにエラー状態が検出されると、スイッチから syslog メッセージが生成されます。このメッセージにより、顕著なパフォーマンスの低下が発生する前に、問題の存在が管理者に通知されます。CatOS バージョン 6.4(16)、7.6(12)、8.4(2) 以降では、3 つすべてのコンポーネントのデフォルト モードが disabled から enabled に変更されています。

## インバンド

インバンド エラーが検出された場合、著しいパフォーマンスの低下が発生する前に、Syslog メッセージによって問題が生じていることが通知されます。エラーには、発生したインバンド障害のタイプが表示されます。例をいくつか示します。

- インバンド スタック
- リソース エラー
- ブートアップ中のインバンド障害

この機能では、インバンドの ping 障害が検出されると、インバンド接続の現在の Tx レートと Rx レート、CPU、およびスイッチのバックプレーンの負荷のスナップショットを含む追加の syslog メッセージも報告されます。このメッセージにより、インバンドがスタックしている（Tx/Rx がない）か、過負荷（Tx/Rx が過度）であるかを正しく判断できます。 この追加情報は、インバンド ping 障害の原因を判断するのに役立ちます。

## ポート カウンタ

この機能を有効にすると、ポート カウンタをデバッグするプロセスが作成されて開始されます。ポート カウンタは、選択した内部ポート エラー カウンタを定期的にモニタします。ライン カードのアーキテクチャ、具体的には、モジュールの ASIC によって、この機能のクエリ対象カウンタが決まります。この情報は、シスコ テクニカル サポートや開発技術部門が問題をトラブルシュートするために使用します。この機能では、FCS、CRC、配置、ラントなどの、リンク パートナーの接続に直接関連するエラー カウンタはポーリングされません。この機能の組み込み方法については、このドキュメントの「EtherChannel やリンク エラーの処理」の項を参照してください。

ポーリングは 30 分ごとに実行され、選択したエラー カウンタのバックグラウンドで動作します。同じポートに対する連続した 2 回のポーリングでカウンタの値が上昇している場合、そのインシデントが syslog メッセージで報告され、モジュールやポート、およびエラー カウンタの詳細が表示されます。

ポート カウンタ オプションは Catalyst 4500/4000 プラットフォームではサポートされていません。

### メモリ

この機能を有効にすると、バックグラウンドのモニタリングが実行されて、DRAM の破損状態が検出されます。検出されるメモリ破損には、次のようなものがあります。

- 割り当て
- 解放
- 範囲外
- 配置不良

### 推奨事項

サポートされている場合は、インバンド、ポート カウンタ、メモリなど、すべてのエラー検出機能を有効にしてください。これらの機能を有効にすると、システムとハードウェア向けに強化されたプロアクティブな警告診断が Catalyst スイッチ プラットフォームで行われます。3 つのエラー検出機能をすべて有効にするには、次のコマンドを発行します。

```
set errordetection inband enable
!--- This is the default in CatOS 6.4(16), 7.6(12), 8.4(2), and later. set errordetection
portcounters enable
!--- This is the default in CatOS 6.4(16), 7.6(12), 8.4(2), and later. set errordetection memory
enable
!--- This is the default in CatOS 6.4(16), 7.6(12), 8.4(2), and later.
```

エラー検出機能が有効になっていることを確認するには、次のコマンドを発行します。

```
>show errordetection

Inband error detection:                  enabled
Memory error detection:                  enabled
Packet buffer error detection:           errdisable
Port counter error detection:            enabled
Port link-errors detection:              disabled
Port link-errors action:                 port-failover
Port link-errors interval:               30 seconds
```

## EtherChannel およびリンク エラーの処理

### 動作の概要

CatOS 8.4 以降には、EtherChannel にある 1 つのポートから同じ EtherChannel にある別のポートにトラフィックを自動フェールオーバーする新機能が導入されています。指定したインターバルの間に、チャネルにあるポートのいずれかが設定されたエラーしきい値を超えると、ポート フェールオーバーが発生します。ポート フェールオーバーが発生するのは、EtherChannel に動作可能なポートが存在する場合だけです。障害が発生したポートが EtherChannel にある最後のポートの場合、そのポートは `port-failover` 受信したエラーのタイプにかかわらず、そのポートはトラフィックを通過させ続けます。単一のチャネル化されていないポートは、`port-failover` 指定したインターバルの間に、エラーしきい値を超えた場合、これらのポートは `errdisable`

この機能が有効なのは、**set errordetection portcounters** を有効にした場合だけです。リンク エラーは、次の 3 つのカウンタに基づいてモニタされます。

- InErrors
- RxCRC ( CRCAlignErrors )
- TxCRC

エラー カウンタの数字を表示するには、スイッチで show counters コマンドを発行します。次に例を示します。

```
>show counters 4/48

.......

32 bit counters

0  rxCRCAlignErrors           =          0
.......

6  ifInErrors                 =          0
.......

12 txCRC                      =          0
```

次の表は、指定可能な設定パラメータとそれぞれのデフォルト設定を示しています。

| パラメータ | デフォルト |
|---|---|
| グローバル | Disabled |
| RxCRC 用のポート モニタ | Disabled |
| InErrors 用のポート モニタ | Disabled |
| TxCRC 用のポート モニタ | Disabled |
| アクション | Port-failover |
| 間隔 | 30 秒 |
| サンプリング カウント | 3 回連続 |
| 下限しきい値 | 1,000 |
| 上限しきい値 | 1001 |

この機能が有効になっていて、指定したサンプリング カウント期間内に、設定された上限しきい値にポートのエラー カウントが達した場合、設定可能なアクションはエラー ディセーブルかポート フェールオーバーになります。エラー ディセーブル アクションでは、ポートが `errdisable` ポート フェールオーバー アクションを設定すると、ポート チャネルの状態が考慮されます。ポートがチャネル内にあり、そのポートがチャネル内で動作可能な最後のポートではない場合にのみ、そのポートは errdisable 状態になります。さらに、設定されたアクションがポート フェールオーバーで、ポートが単一のポートまたはチャネル化されていない場合、ポートのエラー カウントが上限しきい値に達するとそのポートは `errdisable`

インターバルは、ポート エラー カウンタを読み込むためのタイマー定数です。link-errors インターバルのデフォルト値は 30 秒です。許容範囲は 30 ~ 1800 秒です。

予期しない単発イベントのために、ポートが偶発的にエラー ディセーブルになるリスクがあります。このリスクを最小限に抑えるために、この連続したサンプリング回数の間にこの状態が続いた場合にのみ、ポートに対するアクションが実行されます。デフォルトのサンプリング値は 3 で、許容範囲は 1 ~ 255 です。

しきい値は、link-errors インターバルに基づいてチェックされる絶対値です。デフォルトのlink-errorの低いしきい値は1000で、許容範囲は1 ~ 65,535です。デフォルトのlink-errorの高いしきい

値は1001です。連続したサンプリング回数が下限しきい値に達すると syslog が送信されます。連続したサンプリング回数が上限しきい値に達すると、syslog が送信されて、エラー ディセーブルまたはポート フェールオーバー アクションがトリガーされます。

**注：チャネル**内のすべてのポートに同じポートエラー検出設定を使用します。詳細については、Catalyst 6500 シリーズのソフトウェア コンフィギュレーション ガイドの次の各項を参照してください。

- 状態と接続の確認 [英語] の「*EtherChannel やリンクのエラー処理の設定*」
- イーサネット、ファスト イーサネット、ギガビット イーサネット、および 10 ギガビット イーサネット スイッチングの設定 [英語] の「*ポート エラー検出の設定*」

## 推奨事項

この機能では、データの記録と比較に SCP メッセージが使用されるため、アクティブ ポートが多数あると CPU の負荷が高くなります。このシナリオでは、しきい値の間隔が非常に小さな値に設定されると、さらに CPU 負荷が高くなります。この機能は、重要なリンクとして指定されていて、機密性の高いアプリケーションのトラフィックを転送するポートに対して、慎重に有効にしてください。リンク エラーの検出をグローバルに有効にするには、次のコマンドを発行します。

```
set errordetection link-errors enable
```

また、デフォルトのしきい値、インターバル、サンプリング パラメータを指定して使用を開始します。さらに、デフォルト アクションであるポート フェールオーバーを使用します。

個々のポートにグローバル link-error パラメータを適用するには、次のコマンドを発行します。

```
set port errordetection mod/port inerrors enable

set port errordetection mod/port rxcrc enable

set port errordetection mod/port txcrc enable
```

link-errors の設定を確認するには、次のコマンドを発行します。

```
show errordetection

show port errordetection {mod | mod/port}
```

## Catalyst 6500/6000 パケット バッファの診断

CatOS バージョン 6.4(7)、7.6(5)、および 8.2(1) には、Catalyst 6500/6000 のパケット バッファの診断機能が導入されています。デフォルトで有効になるパケット バッファの診断では、一時的なスタティック RAM ( SRAM ) 障害によって発生するパケット バッファの障害が検出されます。次の 48 ポート 10/100 Mbps ライン モジュールで検出が有効になります。

- WS-X6248-RJ45
- WS-X6248-RJ21
- WS-X6348-RJ45
- WS-X6348-RJ21
- WS-X6148-RJ45
- WS-X6148-RJ21

障害状態が発生すると、48 個の 10/100 Mbps ポートの内 12 個のポートが接続されたままになり、接続の問題がランダムに発生する可能性があります。この状態から回復する唯一の方法は、ライン モジュールの電源の再投入です。

## 動作の概要

パケット バッファの診断では、パケット バッファの特定のセクションに格納されたデータが一時的な SRAM の障害によって破損しているかどうかを判断するためのチェックが行われます。書き込まれたデータと異なるデータが読み取られた場合、次の 2 つの設定可能なリカバリ オプションが実行されます。

1. デフォルト アクションでは、バッファ障害の影響を受けるライン カードのポートがエラー ディセーブルにされます。
2. 2 番目のオプションでは、ライン カードの電源の再投入が行われます。

2 つの syslog メッセージが追加されています。それらのメッセージには、パケット バッファのエラーに伴い、ポートがエラー ディセーブルになること、またはモジュールの電源の再投入が行われることの警告が表示されます。

```
%SYS-3-PKTBUFFERFAIL_ERRDIS:Packet buffer failure detected.
Err-disabling port 5/1.
%SYS-3-PKTBUFFERFAIL_PWRCYCLE: Packet buffer failure detected.
Power cycling module 5.
```

8.3 および 8.4 よりも前のバージョンの CatOS の場合、ライン カードの電源の再投入時間は 30 ~ 40 秒の間です。ラピッドブート機能は、CatOSバージョン8.3および8.4で導入されました。この機能は、初期ブートプロセス中にインストールされたラインカードにファームウェアを自動的にダウンロードし、ブートアップ時間を最小限に抑えます。高速ブート機能では、電源の再投入時間が約 10 秒に短縮されます。

## 推奨事項

シスコでは、デフォルト オプションである *errdisable* を使用することを推奨しています。このアクションを使用すると、実稼働時間帯にネットワーク サービスに与える影響を最小限に抑えることができます。可能であれば、error-disabled ポートの影響を受けている接続を使用可能な他のスイッチ ポートに移動して、サービスを復元します。メンテナンスの時間帯に、手動でライン カードの電源の再投入を行うスケジュールを作成します。破損したパケット バッファの状態から完全に回復するためには、reset module *mod* コマンドを発行します。

**注：モジ**ュールのリセット後もエラーが続く場合は、モジュールを取り付け直してください。

*errdisable オプションを有効にするには、次のコマンドを発行します。*

```
set errordetection packet-buffer errdisable
!--- This is the default.
```

## その他のオプション

SRAM 障害が発生したすべてのポートを完全に回復するにはライン カードの電源の再投入が必要なため、代替回復アクションとして、電源の再投入オプションを設定する方法もあります。ネットワーク サービスの中断が 30 ~ 40 秒間続いても許容できるような状況では、このオプションが有効です。この中断時間は、ライン モジュールの電源の再投入が完全に行われ、高速ブート機能を使用せずにサービスが再開されるまでに必要な時間です。高速ブート機能では、電源の再投入オプションを有効にした状態でネットワーク サービスの中断時間を 10 秒に短縮できます。電源の再投入オプションを有効にするには、次のコマンドを発行します。

```
set errordetection packet-buffer power-cycle
```

## パケット バッファの診断

このテストは Catalyst 5500/5000 スイッチ専用です。このテストは、ユーザ ポートとスイッチ バックプレーンの間で 10/100 Mbps の接続を提供する特定のハードウェアを備えたイーサネット モジュールを使用している、Catalyst 5500/5000 スイッチで障害のあるハードウェアを検出するために設計されています。これらのスイッチにはトランキング フレームに対して CRC チェックを実行する機能がないため、実行時にポート パケット バッファで障害が起こった場合、パケットが破損して CRC エラーが発生する可能性があります。あいにく、これが原因で Catalyst 5500/5000 ISL ネットワークに不正フレームが伝達され、最悪の場合はコントロール プレーンの中断やブロードキャスト ストームが発生することがあります。

新しい Catalyst 5500/5000 モジュールおよび他のプラットフォームには最新のハードウェア エラー チェック機構が組み込まれているため、パケット バッファ テストは不要です。そのため、設定オプションもありません。

パケット バッファ診断が必要なライン モジュールは、WS-X5010、WS-X5011、WS-X5013、WS-X5020、WS-X5111、WS-X5113、WS-X5114、WS-X5201、WS-X5203、WS X5213/a、WS-X5223、WS-X5224、WS-X5506、WS-X5509、WS-U5531、WS-U5533、および WS-U5535 です。

## 動作の概要

この診断では、パケット バッファの特定のセクションに格納されたデータが、不良ハードウェアによって誤って破損されていないかがチェックされます。書き込まれたデータと異なるデータが読み取られた場合は、ポートでデータが破損する可能性があるため、そのポートがシャットダウンされて `failed` エラーのしきい値は不要です。障害ポートは、モジュールがリセット ( または交換 ) されない限り、再び有効にはなりません。

パケット バッファのテストには次の 2 つのモードがあります。「スケジュール」および「オンデマンド」。テストが始まると、テストの予想実行時間 ( 最も近い分数に切り上げられた時間 ) とテストが開始したことを示す syslog メッセージが生成されます。正確なテスト時間は、ポート タイプ、バッファのサイズ、および実行するテストのタイプによって異なります。

オンデマンド テストは数分間で完了するためにアグレッシブに実行されます。これらのテストはパケット メモリとアクティブに干渉するため、テストを開始する前に、ポートを管理上シャットダウンする必要があります。ポートをシャットダウンするには、次のコマンドを発行します。

```
> (enable) test packetbuffer 4/1
Warning: only disabled ports may be tested on demand - 4/1 will be skipped.
> (enable) set port disable 4/1
> (enable) test packetbuffer 4/1
Packet buffer test started. Estimated test time: 1 minute.
%SYS-5-PKTTESTSTART:Packet buffer test started
%SYS-5-PKTTESTDONE:Packet buffer test done. Use 'show test' to see test results
```

スケジュール テストはオンデマンド テストほど強引ではなく、バックグラウンドで動作します。このテストは複数のモジュールにわたって並行に実行されます。ただし、一度に実行されるのはモジュールあたり 1 つのポートでのみです。このテストでは、ユーザ パケット バッファ データを復元する前に、パケット バッファ メモリの小さいセクションに対して保存、書き込み、および読み出しが行われます。そのため、エラーは発生しません。ただし、バッファ メモリへの書き込みが行われるため、数ミリ秒間着信パケットがブロックされ、混雑したリンクではパケット損失が生じることがあります。デフォルトでは、パケット損失を最小限に抑えるために、8 秒間隔でバッファ書き込みテストが行われます。これは、モジュールがフル構成されたシステムでパケット バッファ テストを実行する場合、完了までに 24 時間以上かかることを意味します。このスケジュール テストは、CatOS 5.4 以降ではデフォルトで有効になっており、毎週日曜日の 03:30 に実行されます。テスト ステータスを確認するには、次のコマンドを発行します。

```
>show test packetbuffer status

!--- When test is running, the command returns !--- this information: Current packet buffer test
details Test Type : scheduled Test Started : 03:30:08 Jul 20 2001 Test Status : 26% of ports
tested Ports under test : 10/5,11/2 Estimated time left : 11 minutes !--- When test is not
running, !--- the command returns this information: Last packet buffer test details Test Type :
scheduled Test Started : 03:30:08 Jul 20 2001 Test Finished : 06:48:57 Jul 21 2001
```

## 推奨事項

シスコでは、Catalyst 5500/5000 システムでスケジュール パケット バッファ テスト機能を使用することを推奨しています。これは、わずかなパケット損失のリスクよりも、モジュールの問題を検出できる利点の方が大きいためです。

テストは、ネットワーク全体で毎週決められた時刻に実行されるようにスケジュールします。そうすることで、必要に応じて障害のあるポートや RMA モジュールからリンクを変更できます。ネットワークの負荷によっては、テスト中に多少のパケット損失が生じる可能性があるため、日曜日の 3:30 AM ( デフォルト ) など、ネットワークの使用率が低い時間帯にスケジュールする必要があります。テスト時刻を設定するには、次のコマンドを発行します。

```
set test packetbuffer Sunday 3:30
!--- This is the default.
```

テストを有効にすると ( 初めて CatOS 5.4 以降にアップグレードしたときと同様 ) 、それまで隠れていたメモリまたはハードウェアの問題が明らかになり、結果としてポートが自動的にシャットダウンされることがあります。次のメッセージが表示される場合があります。

```
%SYS-3-PKTBUFBAD:Port 1/1 failed packet buffer test
```

## その他のオプション

毎週ポート単位でわずかなパケット損失が起こる可能性があるというリスクを許容できない場合は、停止時間をスケジュールした上でオンデマンド機能を使用することを推奨します。一定のポート範囲ごとにこの機能を手動で開始するには、次のコマンドを発行します ( ただし、ポートは

事前に管理上シャットダウンする必要があります）。

```
test packetbuffer port range
```

## システム ロギング

syslog メッセージはシスコ固有のもので、プロアクティブな障害管理の重要な部分です。syslog を使用することで、標準化された SNMP よりも広い範囲でネットワークやプロトコルの状態を報告できます。Cisco Resource Manager Essentials（RME）や Network Analysis Toolkit（NATkit）などの管理プラットフォームでは、次のようなタスクが実行されるため、syslog 情報を有効利用できます。

- 重大度、メッセージ、デバイスなどの項目別に分析を提供する
- 分析用に着信メッセージのフィルタリングを有効にする
- ポケットベルなどへのアラートや、インベントリおよび設定変更のオンデマンド収集をトリガーする

### 推奨事項

重要なことは、どのレベルのロギング情報がローカルに生成され、syslog サーバに送信されずにスイッチのバッファに保持されるかという点です（set logging server severity value コマンドを使用）。高レベルの情報を一元的にログに記録している組織もあれば、イベントの詳細なログを見る場合はスイッチ自体にアクセスする組織や、トラブルシューティング時にのみ高レベルの syslog の取得を有効にする組織もあります。

CatOS プラットフォームのデバッグは Cisco IOS ソフトウェアの場合と異なりますが、set logging session enable を使用することで、デフォルトでログに記録される情報を変更することなく、セッション単位で詳細なシステム ロギングを有効にできます。

シスコでは通常、spantree および system syslog 機能をレベル 6 に上げることを推奨しています。これらは追跡を行うための安定性に関する主要な機能です。また、マルチキャスト環境では、mcast 機能のロギング レベルを 4 に上げ、ルータ ポートが削除された場合に syslog メッセージが生成されるようにすることを推奨します。困ったことに、CatOS 5.5（5）より前のバージョンでこれを行うと、IGMP Join および Leave の syslog メッセージが記録される場合があります。これは量が多すぎて監視できません。最後に、IP 入力リストを使用している場合は、不正なログイン試行をキャプチャするために、最小のロギング レベルの 4 に設定することを推奨します。これらのオプションを設定するには、次のコマンドを発行します。

```
set logging buffer 500
!--- This is the default. set logging server syslog server IP address set logging server enable
!--- This is the default. set logging timestamp enable
set logging level spantree 6 default
!--- Increase default STP syslog level. set logging level sys 6 default
!--- Increase default system syslog level. set logging server severity 4
!--- This is the default; !--- it limits messages exported to syslog server. set logging console
disable
```

メッセージの量が多いときに低速または存在しない端末からの応答を待つことでスイッチがハングするリスクを防ぐために、コンソール メッセージをオフにします。コンソール ロギングは

CatOS では優先順位が高く、主にトラブルシューティング時やスイッチのクラッシュ時に最後のメッセージをローカルにキャプチャするために使用されます。

次の表に、Catalyst 6500/6000 での個々のロギング機能、デフォルト レベル、および推奨される変更を示します。各プラットフォームのロギング機能は、サポートされる機能によって多少異なります。

| ファシリティ | デフォルト レベル | 推奨処置 |
|---|---|---|
| acl | 5 | デフォルトのままにする。 |
| cdpcdp | 4 | デフォルトのままにする。 |
| cops | 3 | デフォルトのままにする。 |
| dtp | 8 | デフォルトのままにする。 |
| earl | 0 | デフォルトのままにする。 |
| ethc[1] | 5 | デフォルトのままにする。 |
| filesys | 0 | デフォルトのままにする。 |
| gvrp | 0 | デフォルトのままにする。 |
| ip | 0 | **IP 入力リストを使用している場合は 4 に変更する。** |
| kernel | 0 | デフォルトのままにする。 |
| 1日 | 3 | デフォルトのままにする。 |
| mcast | 0 | **マルチキャストを使用している場合は 4 に変更する（CatOS 5.5(5) 以降）。** |
| mgmt | 5 | デフォルトのままにする。 |
| mls | 5 | デフォルトのままにする。 |
| pagp | 5 | デフォルトのままにする。 |
| protfilt | 0 | デフォルトのままにする。 |
| pruning | 0 | デフォルトのままにする。 |
| Privatevlan | 3 | デフォルトのままにする。 |
| qos | 3 | デフォルトのままにする。 |
| radius | 0 | デフォルトのままにする。 |
| rsvp | 3 | デフォルトのままにする。 |
| セキュリティ | 0 | デフォルトのままにする。 |
| snmp | 0 | デフォルトのままにする。 |
| spantree | 0 | **6 に変更する。** |
| sys | 5 | **6 に変更する。** |
| tac | 0 | デフォルトのままにする。 |
| tcp | 0 | デフォルトのままにする。 |
| telnet | 0 | デフォルトのままにする。 |
| Tftp | 0 | デフォルトのままにする。 |
| UDLD | 4 | デフォルトのままにする。 |
| VMPS | 0 | デフォルトのままにする。 |
| VTP | 0 | デフォルトのままにする。 |

1 CatOS 7.x 以降では、LACP のサポートを反映するために、ethc ファシリティ コードが pagp ファシリティ コードの

代わりに使用されています。

**注**：現在、Catalystスイッチは、設定モードを終了した後にのみメッセージをトリガーするCisco IOSソフトウェアとは異なり、実行された各**set**または**clear**コマンドについて、**設定変更syslogレベル6メッセージをログに記録します。**このメッセージをトリガーとして、RME でリアルタイムに設定をバックアップする必要がある場合は、これらのメッセージも RME syslog サーバに送信する必要があります。ほとんどのお客様の場合、Catalyst スイッチの設定は定期的にバックアップするだけで十分であり、サーバ ロギングのデフォルトの重大度を変更する必要はありません。

NMS アラートを調整する場合は、システム メッセージ ガイド [英語] を参照してください。

## Simple Network Management Protocol

SNMP は、ネットワーク デバイスの Management Information Base（MIB）に保存された統計情報、カウンタ、およびテーブルを取得するために使用します。 収集した情報を HP Openview などの NMS で使用して、リアルタイムのアラートの生成、可用性の測定、キャパシティ プランニング情報の生成を行い、設定やトラブルシューティングのチェックを行うこともできます。

### 動作の概要

ネットワーク管理ステーションにはいくつかのセキュリティ メカニズムが搭載されており、SNMP プロトコルの get および get next 要求を使用して MIB の情報を取得し、**set コマンドを使用してパラメータを変更することができます。**また、ネットワーク デバイスは、リアルタイム アラートのために NMS 用のトラップ メッセージを生成するように設定できます。SNMP ポーリングでは IP UDP ポート 161 が使用され、SNMP トラップではポート 162 が使用されます。

シスコでは次のバージョンの SNMP をサポートしています。

- SNMPv1：RFC 1157 インターネット標準。セキュリティにはクリア テキストのコミュニティ ストリングを使用します。IP アドレスのアクセス コントロール リストとパスワードによって、エージェントの MIB にアクセスできるマネージャのコミュニティが定義されます。
- SNMPv2C：SNMPv2（RFC 1902 ~ 1907 で定義されたドラフト インターネット標準）と SNMPv2C（SNMPv2 用のコミュニティベースの管理フレームワーク。RFC 1901 で定義された実験的なドラフト）の組み合わせ。利点としては、テーブルおよび大量の情報の取得をサポートするバルク取得メカニズム、必要なラウンド トリップ数の最小化、エラー処理の改善などがあります。
- SNMPv3：RFC 2570 提案ドラフト。ネットワーク上での認証とパケットの暗号化を組み合わせることで、デバイスへのセキュアなアクセスを提供します。SNMPv3 では次のセキュリティ機能が提供されます。メッセージの完全性：パケットが伝送中に改ざんされていないことを保証します。認証：メッセージの送信元が有効かどうかを判別します。暗号化：パケットの内容を暗号化し、不正な送信元によってパケットの内容が表示されないようにします。

次の表に、セキュリティ モデルの組み合わせを示します。

| モデル レベル | [Authentication] | 暗号化 | 結果 |
|---|---|---|---|
| v | noAuthNo | N | コミュニティ ストリングの照合を使 |

| | | | |
|---|---|---|---|
| 1 | Priv、コミュニティストリング | o | 用して認証します。 |
| v2c | noAuthNoPriv、コミュニティストリング | No | コミュニティ ストリングの照合を使用して認証します。 |
| v3 | noAuthNoPriv、ユーザ名 | No | 認証にユーザ名の一致を使用する。 |
| v3 | authNoPriv、MD5 または SHA | Np | HMAC-MD5 または HMAC-SHA アルゴリズムに基づいて認証を行う。 |
| v3 | authPriv、MD5 または SHA | DES | HMAC-MD5 または HMAC-SHA アルゴリズムに基づいて認証を行う。CBC-DES（DES-56）標準に基づいて認証する以外に、DES 56ビット暗号化を行います。 |

**注**：SNMPv3オブジェクトに関しては、次の点に注意してください。

- 各ユーザは 1 つのグループに所属します。
- グループは、ユーザの集まりに対してアクセス ポリシーを定義します。
- アクセス ポリシーは、読み取り、書き込み、および作成のためにアクセスできる SNMP オブジェクトを定義します。
- グループは、ユーザが受信できる通知の一覧を決定します。
- グループは、そのユーザのセキュリティ モデルとセキュリティ レベルも定義します。

## SNMP トラップに関する推奨事項

SNMP はすべてのネットワーク管理の基盤となるもので、すべてのネットワークで有効であり、使用されています。スイッチの SNMP エージェントは、管理ステーションでサポートされている SNMP のバージョンを使用するように設定する必要があります。エージェントは複数のマネージャと通信できるため、たとえば、ある管理ステーションとは SNMPv1 プロトコルを使用して通信し、別の管理ステーションとは SNMPv2 プロトコルを使用して通信するように設定することができます。

現在、ほとんどの NMS ステーションでは、次の設定で SNMPv2C が使用されています。

```
set snmp community read-only string
!--- Allow viewing of variables only. set snmp community read-write string
!--- Allow setting of variables. set snmp community read-write-all string
!--- Include setting of SNMP strings.
```

シスコでは、使用中のすべての機能に対して SNMP トラップを有効にすることを推奨しています（使用していない機能は、必要に応じて無効にできます）。 有効になったトラップは、NMS でエラー（ポケットベルのアラートやポップアップなど）の適切な処理を設定した上で、test snmp コマンドを使用してテストできます。

デフォルトでは、トラップはすべて無効になっているため、個別にまたは次のように **all パラメータを使用して、設定に追加する必要があります。**

```
set snmp trap enable all
set snmp trap server address read-only community string
```

CatOS 5.5 で使用できるトラップは次のとおりです。

| トラップ | 説明 |
|---|---|
| auth | [Authentication] |
| ブリッジ | ブリッジ |
| シャーシ | シャーシ |
| config | コンフィギュレーション |
| entity | エンティティ |
| ippermit | IP 許可 |
| モジュール | モジュール |
| repeater | リピータ |
| stpx | スパニング ツリー拡張 |
| syslog | Syslog 通知 |
| vmps | VLAN Membership Policy Server; VLAN メンバーシップ ポリシー サーバ |
| vtp | VLAN Trunking Protocol（VLAN トランキング プロトコル） |

**注**：syslogトラップは、スイッチによって生成されたすべてのsyslogメッセージをSNMPトラップとしてNMSに送信します。Cisco Works 2000 RME などのアナライザによって syslog アラートがすでに実行されている場合、この情報を 2 回受信することになるため、必ずしも有効ではありません。

Cisco IOS ソフトウェアとは異なり、ポート レベルの SNMP トラップはデフォルトで無効になっています。これは、スイッチには何百ものアクティブなインターフェイスを設定できるためです。そのためシスコでは、ルータ、スイッチ、メイン サーバへのインフラストラクチャ リンクなどのキー ポートでポート レベルの SNMP トラップを有効にすることを推奨しています。ユーザ ホスト ポートなど、その他のポートでは有効にする必要はありません。これにより、ネットワーク管理を簡素化できます。

```
set port trap port range enable
!--- Enable on key ports only.
```

## SNMP ポーリングに関する推奨事項

具体的なニーズについて詳細に確認するためにネットワーク管理のレビューを行うことが推奨されますが、シスコには大規模ネットワークの管理に関する次のような基本理念があります。

- 単純なことを確実にやり遂げる。
- 過度のデータ ポーリングと収集、必要以上のツール、および大量の手動分析によるスタッフ

の過剰な負担を減らす。
- ネットワーク管理はごくわずかなツールだけで実行できる。たとえば、NMS としての HP Openview、設定、syslog、インベントリ、およびソフトウェア マネージャとしての Cisco RME、NMS データ アナライザとしての Microsoft Excel、Web への公開手段としての CGI。
- レポートを Web に公開すれば、シニア マネージャやアナリストなどのユーザが、多くの特別な要求で運用スタッフに負担をかけることなく自分で情報を入手できる。
- ネットワーク上で正常に動作しているものを調べ、それには手をつけない。正常に動作していないもののみに集中する。

NMS の実装の最初のフェーズでは、ネットワーク ハードウェアのベースラインを確立する必要があります。デバイスおよびプロトコルの状態については、ルータでは CPU、メモリ、およびバッファの使用率、スイッチでは NMP の CPU、メモリ、およびバックプレーンの使用率から多くのことを推測できます。ハードウェアのベースラインが確立して初めて、L2 および L3 トラフィックの負荷、ピーク、および平均のベースラインが十分に意味のあるものとなります。ベースラインの確立には通常、企業のビジネス サイクルに応じて、日、週、および四半期のトレンドを把握するために数ヵ月かかります。

ネットワークの多くは、過度のポーリングを原因とする NMS のパフォーマンスおよびキャパシティの問題を抱えています。そのため、ベースラインが確立されたら、デバイス自体にアラームとイベントの RMON しきい値を設定することを推奨します。これで、NMS にデバイスの異常な変化が通知され、ポーリング量が削減されます。つまり、継続的なポーリングによってすべてのものが正常に動作しているかどうかを確認するのではなく、ネットワークで何か正常でないことが起こったときにオペレータに通知できるようになります。しきい値は、最大値 + パーセンテージや、平均からの標準偏差など、さまざまな規則に基づいて設定できますが、それらはこのドキュメントの範囲外です。

NMS の実装の 2 番目のフェーズでは、特定のネットワーク領域に対して、SNMP を使用して詳細なポーリングを行います。領域には、疑わしい領域、変化が起こる前の領域、正常に稼働している領域が含まれます。NMS システムをサーチライトとしてネットワークを詳細にスキャンし、ホット スポットを明らかにします（ネットワーク全体を対象にしないでください）。

シスコのネットワーク管理コンサルティング グループでは、キャンパス ネットワークにおいて、次の主要な障害 MIB を分析またはモニタすることを推奨しています。ポーリングするパフォーマンス MIB などの詳細については、シスコ ネットワークの監視とイベント相関に関するガイドライン [英語] を参照してください。

| Object Name | オブジェクトの説明 | OID | ポーリング間隔 | しきい値 |
|---|---|---|---|---|
| **MIB-II** | | | | |
| sysUpTime | システム稼働時間（1/100 秒単位） | 1.3.6.1.2.1.1.3 | 5分 | < 30000 |

| Object Name | オブジェクトの説明 | OID | ポーリング間隔 | しきい値 |
|---|---|---|---|---|
| **CISCO-PROCESS-MIB** | | | | |
| cpmCPUTotal5min | 直近の 5 分間の CPU 全体のビジーパーセン | 1.3.6.1.4.1.9.9.109.1.1.1.1.5 | 10分 | ベースライン |

| | テージ | | | |
|---|---|---|---|---|
| **Object Name** | **オブジェクトの説明** | **OID** | **ポーリング間隔** | **しきい値** |
| CISCO-STACK-MIB | | | | |
| sysEnableChassisTraps | この MIB の chassisAlarmOn および chassisAlarmOff トラップの生成の有無を示します。 | 1.3.6.1.4.1.9.5.1.1.24 | 24時間 | 1 |
| sysEnableModuleTraps | この MIB の moduleUp および moduleDown トラップの生成の有無を示します。 | 1.3.6.1.4.1.9.5.1.1.25 | 24時間 | 1 |
| sysEnableBridgeTraps | BRIDGE-MIB（RFC 1493）の newRoot および topologyChange トラップの生成の有無を示します。 | 1.3.6.1.4.1.9.5.1.1.26 | 24時間 | 1 |
| sysEnableRepeaterTraps | REPEATER-MIB（RFC 1516）のトラップの生成の有無を示します。 | 1.3.6.1.4.1.9.5.1.1.29 | 24時間 | 1 |
| sysEnableIpPermitTraps | この MIB の IP 許可トラップの生成の有無を示します。 | 1.3.6.1.4.1.9.5.1.1.31 | 24時間 | 1 |
| sysEnableVmpsTraps | CISCO-VLAN-MEMBERSHIP-MIB で定義されている vmVmpsChange トラップの生成の有無を示します。 | 1.3.6.1.4.1.9.5.1.1.33 | 24時間 | 1 |
| sysEnableConfigTraps | この MIB の sysConfigChange トラップの生成の有無を示します。 | 1.3.6.1.4.1.9.5.1.1.35 | 24時間 | 1 |
| sysEnableStpxTrap | CISCO-STP-EXTENSIONS-MIB の stpxInconsistencyUpdate トラップの生成の有無を示 | 1.3.6.1.4.1.9.5.1.1.40 | 24時間 | 1 |

| | | | | |
|---|---|---|---|---|
| | します。 | | | |
| chassisPs1status | 電源 1 のステータス。 | 1.3.6.1.4.1.9.5.1.2.4 | 10分 | 0 |
| chassisPs1TestResult | 電源 1 のステータスに関する詳細情報。 | 1.3.6.1.4.1.9.5.1.2.5 | 必要に応じて行います。 | |
| chassisPs2Status | 電源 2 のステータス。 | 1.3.6.1.4.1.9.5.1.2.7 | 10分 | 0 |
| chassisPs2TestResult | 電源 2 のステータスに関する詳細情報。 | 1.3.6.1.4.1.9.5.1.2.8 | 必要に応じて行います。 | |
| chassisFanStatus | シャーシ ファンのステータス。 | 1.3.6.1.4.1.9.5.1.2.9 | 10分 | 0 |
| chassisFanTestResult | シャーシ ファンのステータスに関する詳細情報。 | 1.3.6.1.4.1.9.5.1.2.10 | 必要に応じて行います。 | |
| chassisMinorAlarm | シャーシのマイナー アラームのステータス。 | 1.3.6.1.4.1.9.5.1.2.11 | 10分 | 1 |
| chassis MajorAlarm | シャーシのメジャー アラームのステータス。 | 1.3.6.1.4.1.9.5.1.2.12 | 10分 | 1 |
| chassisTempAlarm | シャーシの温度アラームのステータス。 | 1.3.6.1.4.1.9.5.1.2.13 | 10分 | 1 |
| moduleStatus | モジュールの動作ステータス。 | 1.3.6.1.4.1.9.5.1.3.1.1.10 | 30分 | 0 |
| moduleTestResult | モジュールの状態に関する詳細情報。 | 1.3.6.1.4.1.9.5.7.3.1.1.11 | 必要に応じて行います。 | |
| moduleStandbyStatus | 冗長モジュールのステータス。 | 1.3.6.1.4.1.9.5.7.3.1.1.21 | 30分 | =1 または =4 |

| Object Name | オブジェクトの説明 | OID | ポーリング間隔 | しきい値 |
|---|---|---|---|---|
| CISCO-MEMORY-POOL-MIB | | | | |
| dot1dStpTimeSinceTopologyChange | エンティティによって最後にトポロジ変更が検出されてからの時間（1/100 秒単位）。 | 1.3.6.1.2.1.17.2.3 | 5分 | <3000 |

| | | | | |
|---|---|---|---|---|
| | | | | 0 |
| dot1dStpTopChanges | 管理エンティティが最後にリセット、または初期化されてから、このブリッジによって検知されたトポロジに対する変更の総数。 | 1.3.6.1.2.1.17.2.4 | 必要に応じて行います。 | |
| dot1dStpPortState [1] | スパニング ツリー プロトコルの適用によって定義されたポートの現在の状態。戻り値は次のいずれかになります。123456 | 1.3.6.1.2.1.17.2.15.1.3 | 必要に応じて行います。 | |

| Object Name | オブジェクトの説明 | OID | ポーリング間隔 | しきい値 |
|---|---|---|---|---|
| CISCO-MEMORY-POOL-MIB | | | | |
| ciscoMemoryPoolUsed | 管理対象デバイスのアプリケーションによって現在使用されているメモリ プールのバイト数を示します。 | 1.3.6.1.4.1.9.9.48.1.1.1.5 | 30分 | ベースライン |
| ciscoMemoryPoolFree | 管理対象装置で現在使用されていないメモリ プールのバイト数を示す。<br>**注**：ciscoMemoryPoolUsedとciscoMemoryPoolFreeの合計は、プール内のメモリの総量です。 | 1.3.6.1.4.1.9.9.48.1.1.1.6 | 30分 | ベースライン |
| ciscoMemoryPoolLargestFree | 管理対象デバイスで現在使用されていないメモリ プールの連続した最大バイト数を示します。 | 1.3.6.1.4.1.9.9.48.1.1.1.7 | 30分 | ベースライン |

Cisco MIB のサポートの詳細については、[シスコ ネットワーク管理ツールキット：MIB [英語] を参照してください。]

**注：一部の標準**MIBでは、特定のSNMPエンティティにMIBのインスタンスが1つだけ含まれていると想定されています。そのような標準 MIB には、MIB の特定のインスタンスに直接アクセスするために使用できるインデックスはありません。そのような場合は、コミュニティ ストリング インデックスを使用して標準 MIB の各インスタンスにアクセスします。構文は [コミュニティ ストリング]@[インスタンス番号] で、ここでのインスタンスは通常は VLAN 番号です。

## その他のオプション

SNMPv3 はセキュリティの観点から、いずれ SNMPv2 よりも使用されるようになると予想されるため、シスコではお客様の NMS 戦略の一環として、この新しいプロトコルを採用することを推奨しています。SNMPv3 の利点は、データの改ざんや破損を心配することなく、SNMP デバイスからデータを安全に収集できることです。スイッチの設定を変更する SNMP **set コマンド パケットなどの機密情報は暗号化できるため、その内容がネットワーク上に公開されるのを防ぐことができます。**また、ユーザ グループごとに異なる特権を与えることも可能です。

**注**：SNMPv3の設定はSNMPv2コマンドラインとは大きく異なるため、スーパーバイザエンジンのCPU負荷が増加することが予想されます。

# リモート モニタリング

RMON では、履歴ベースラインに基づく決定やしきい値分析の実行など、ネットワーク マネージャによる情報の一般的な使用や応用に対する準備として、ネットワーク デバイス自体による MIB データの前処理が可能です。

RFC 1757sで定義されているように、RMON 処理の結果は RMON MIB に保存され、後で NMS によって収集されます。

## 動作の概要

Catalyst スイッチでは各ポートのハードウェアでミニ RMON をサポートしています。ミニ RMON は 4 つの基本 RMON-1 グループ、つまり統計（グループ 1）、履歴（グループ 2）、アラーム（グループ 3）、イベント（グループ 9）で構成されています。

RMON-1 の最も強力な部分は、アラームおよびイベント グループによって提供されるしきい値のメカニズムです。前述したように、RMON しきい値を設定することで、異常状態が発生した際にスイッチから SNMP トラップを送信できます。キー ポートが特定されたら、SNMP を使用してカウンタまたは RMON 履歴グループをポーリングし、それらのポートの通常のトラフィック アクティビティを記録するベースラインを作成できます。次に、RMON の上昇しきい値と下降しきい値を設定し、ベースラインからの定義済みバリアンスが生じたときにアラームが通知されるよう設定できます。

アラームおよびイベント テーブルのパラメータ行を正しく作成するのは面倒なため、しきい値の設定には RMON 管理パッケージを使用するのが最適です。Cisco Traffic Director（Cisco Works 2000 の一部）などの商用 RMON NMS パッケージは GUI を備えており、RMON しきい値を容易に設定できます。

ベースラインの目的では、etherStats グループから有用な一連の L2 トラフィック統計が提供されます。このテーブルのオブジェクトは、ユニキャスト、マルチキャスト、およびブロードキャスト トラフィックに関する統計の取得のほか、各種 L2 エラーの取得にも使用できます。それらのサンプリング値を履歴グループに保存するように、スイッチの RMON エージェントを設定することもできます。この仕組みを利用すると、サンプル レートを低下させることなく、ポーリングの量を削減できます。RMON 履歴を使用すると、大量のポーリング オーバーヘッドが発生することなく、正確なベースラインが得られます。ただし、収集する履歴が多いほど、より多くのスイッチ リソースが使用されます。

スイッチによって提供されるのは RMON-1 の 4 つの基本グループだけですが、RMON-1 の残りのグループと RMON-2 があることを忘れないでください。すべてのグループは RFC 2021 で定義されており、これには UsrHistory（グループ 18）や ProbeConfig（グループ 19）などが含まれ

ます。L3 以上の情報をスイッチから取得するには、SPAN ポートまたは VLAN ACL リダイレクト機能を使用します。これらの機能を使用すれば、トラフィックを外部の RMON SwitchProbe や内部の Network Analysis Module（NAM）にコピーできます。

NAM はすべての RMON グループをサポートしており、**アプリケーション層のデータ**、たとえば、MLS が有効な場合に Catalyst からエクスポートされる Netflow データを調べることもできます。MLS が実行中ということは、ルータでフロー内のすべてのパケットが交換されていないことを意味するため、インターフェイス カウンタではなく Netflow データ エクスポートからのみ信頼性の高い VLAN アカウンティングが得られます。

SPAN ポートとスイッチ プローブを使用して特定のポート、トランク、または VLAN のパケット ストリームをキャプチャし、パケットをアップロードして RMON 管理パッケージで復号化できます。SPAN ポートは CISCO-STACK-MIB の SPAN グループを通じて SNMP で制御できるため、このプロセスは容易に自動化できます。Traffic Director はロービング エージェント機能でこれらの機能を利用します。

VLAN 全体で SPAN 機能を使用する場合は注意すべき点があります。1 Gbps プローブを使用している場合でも、1 つの VLAN または 1 つの 1 Gbps 全二重ポートからのパケット ストリームが全体で SPAN ポートの帯域幅を超えることがあります。SPAN ポートが常に帯域幅全体を使用している場合は、データが失われる可能性があります。詳細については、Catalyst Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）機能の設定 [英語] を参照してください。

## 推奨事項

シスコでは、SNMP ポーリング単独の場合よりもインテリジェントにネットワークを管理するために、RMON しきい値とアラートを設定することを推奨しています。これにより、ネットワーク管理トラフィックのオーバーヘッドが減り、ネットワークでベースラインからの変更が発生したときにインテリジェントにアラートを通知できます。RMON は Traffic Director などの外部エージェントによって制御する必要があります。CLI はサポートされていません。RMON を有効にするには、次のコマンドを発行します。

```
set snmp rmon enable
set snmp extendedrmon netflow enable mod
!--- For use with NAM module only.
```

スイッチの第一の機能はフレームを転送することであり、大型のマルチポート RMON プローブとして働くことではありません。したがって、複数のポートで複数の条件に関する履歴としきい値を設定すると、リソースが消費される点に注意してください。RMON を広範に展開する場合は NAM モジュールの導入を検討してください。また、次の重要なポート規則を遵守してください。「計画段階で重要と認められたポートに対してのみ、ポーリングを実行し、しきい値を設定する」。

## メモリ要件

RMON のメモリ使用量は、すべてのスイッチ プラットフォームの間で、統計、履歴、アラーム、およびイベントに関して一定です。RMON はバケットを使用して RMON エージェント（この場合はスイッチ）に履歴と統計を保存します。 バケット サイズは RMON プローブ（Switch Probe）または RMON アプリケーション（Traffic Director）で定義してから、スイッチに送信して設定します。通常、メモリの制約を考慮するのは DRAM が 32 MB 未満の古い Supervisor Engine の場合だけです。次のガイドラインを参照してください。

- ミニ RMON ( 統計、履歴、アラーム、イベントの 4 つの RMON グループ ) をサポートするために、NMP イメージに約 450 K のコード領域が追加されます。 RMON の動的なメモリ要件はランタイムの設定によって決まるため、一定ではありません。ミニ RMON グループごとの、RMON のランタイム メモリの使用情報は次のとおりです。イーサネット統計グループ：スイッチド イーサネット/FE インターフェイスごとに 800 バイトを使用します。履歴グループ：イーサネット インターフェイスの場合は、設定された 50 バケットの履歴制御エントリごとにおよそ 3.6 KB のメモリ領域を使用し、追加バケットごとに 56 バイトを使用する。アラームおよびイベント グループ：設定されたアラームと、それに対応するイベント エントリごとに 2.6 KB を使用する。
- RMON 関連の設定を保存すると、システムの合計 NVRAM サイズが 256 K 以上の場合は約 20 K、合計 NVRAM サイズが 128 K の場合は 10 K の NVRAM 領域が使用されます。

## Network Time Protocol ( NTP; ネットワーク タイム プロトコル )

NTP ( RFC 1305 ) は、分散配置されたタイムサーバとクライアントの間でタイムキーピングを同期化し、システム ログが作成されたときや時間に関係するイベントが発生したときにイベントを関連付けることができます。

一般に、NTP を使用した場合のクライアント時刻の精度は、Coordinated Universal Time ( UTC; 世界標準時 ) に同期したプライマリ サーバを基準として、LAN で 1 ミリ秒以内、WAN で数十ミリ秒以内です。 標準的な NTP の設定では、高い精度と信頼性を実現するために、複数の冗長サーバと多様なネットワーク パスを利用します。一部の設定には、偶発的または悪意のあるプロトコル攻撃を防ぐための暗号化認証が含まれています。

### 動作の概要

NTPはRFC 958で最初に文書化され 、RFC 1119 （ NTPバージョン2 ）を通じて進化し、現在はRFC 1305で定義されている3番目のバージョンです 。NTPはUDPポート123を介して動作します。すべてのNTP通信はUTCを使用します。これはグリニッジ標準時と同じ時刻です。

### 公開タイム サーバへのアクセス

現在 NTP サブネットには 50 を超える公開プライマリ サーバがあり、電波、衛星、またはモデムを通じて UTC に直接同期しています。通常、比較的少数のクライアントにサービスを提供するクライント ワークステーションやサーバは、プライマリ サーバに同期しません。プライマリ サーバに同期した公開セカンダリ サーバが約 100 台あり、このセカンダリ サーバがインターネット上の 100,000 を超えるクライアントとサーバに同期を提供しています。最新のリストは「List of Public NTP Servers」ページで管理されていて、定期的に更新されます。通常は公開されていないプライベートのプライマリおよびセカンダリ サーバも数多く存在します。公開 NTP サーバのリストと、それらの使用方法については、デラウェア大学の『Time Synchronization Server』の Web サイトを参照してください。

これらのインターネット上の公開 NTP サーバが利用できる保証や正確な時刻が提供される保証はないため、他の選択肢を検討することを強く推奨します。選択肢には、多数のルータに直接接続されたスタンドアロンの各種 Global Positioning Service ( GPS ) デバイスの利用が含まれます。

また、Stratum 1 マスターとして設定したルータを使用するという方法もあります。ただし、これは推奨されません。

### ストラタム

各 NTP サーバでは、そのサーバと外部の時刻源との距離を示すストラタムが採用されています。Stratum 1 サーバは、ラジオ クロックなどの、なんらかの外部時刻ソースにアクセスしています。ストラタム 2 サーバは指定されたストラタム 1 サーバ群から詳細な時刻を取得し、ストラタム 3 サーバはストラタム 2 サーバから詳細な時刻を取得します。後続も同様に取得されます。

## サーバとピアの関係

- サーバはクライアントの要求に応答しますが、クライアントの時刻源から日付情報を取得しようとはしません。
- ピアはクライアントの要求に応答しますが、クライアントの要求をより良い時刻源の候補として使用し、ピアのクロック周波数の安定のために利用しようとします。
- 真のピアになるためには、接続の両側がピアの関係になる必要があります。一方のユーザがピアで、もう一方のユーザがサーバでは真のピアにはなりません。また、信頼できるホスト同士のみが互いにピアとして通信できるようにするために、ピア間でキーを交換することが推奨されます。
- サーバへのクライアント要求では、サーバはクライアントに応答しますが、そのクライアントから要求が来たことは記憶されません。ピアへのクライアント要求では、サーバはクライアントに応答した上で、そのクライアントに関する状態情報を保持し、クライアントでの計時の状況、および実行中のストラタム サーバを追跡します。**注：CatOS は NTP クライアントとしてのみ動作可能です。**

1 台の NTP サーバで何千台ものクライアントを処理することも可能です。ただし、何百ものピアを処理するとメモリへの影響が生じ、その状態を維持すると帯域幅だけでなく、装置の CPU リソースの使用量も増加します。

## ポーリング

NTP プロトコルでは、クライアントが必要なときにいつでもサーバに問い合せを発行できます。実際には、Cisco デバイスで初めて NTP が設定されたときに、NTP_MINPOLL ( 24 = 16 秒 ) 間隔で連続して 8 個の問い合せが送出されます。NTP_MAXPOLL は 214 秒 ( これは 16,384 秒、つまり 4 時間 33 分 4 秒 ) で、応答を得るために NTP が再びポーリングするまでにかかる最大時間です。現時点では、ユーザが手動で POLL 時間を強制的に設定する方法はありません。

NTPポーリングカウンタは$2^6$(64)秒から始まり、2の累乗 ( 2台のサーバが互いに同期するため ) で$2^{10}$に増加します。つまり、同期メッセージは64、128、256、512、14のいずれかの4の4の4で4送信4に4送信4されます設定されたサーバまたはピアあたりの秒数。この間隔は、パケットを送受信するフェーズロックループに基づいて、64 秒から 1024 秒までの、2 の累乗秒の間で変動します。時間内にジッターが多い場合、ポーリング回数が増えます。基準クロックが正確で、ネットワーク接続が安定している場合、ポーリング間隔が 1024 秒に収束します。

これは実際には、クライアントとサーバ間の接続が変わると NTP ポーリング間隔も変わることを意味します。接続が良好なほど、ポーリング間隔は長くなります ( つまり、NTP クライアントが最後の 8 個の要求に対して 8 個の応答を受信すると、ポーリング間隔が 2 倍になります ) 。1 つの応答が受信されなかった場合、ポーリング間隔が半分になります。ポーリング間隔は 64 秒から始まり、最大値は 1024 秒です。最良の環境では、ポーリング間隔が 64 秒から 1024 秒になるまでに 2 時間強かかります。

## ブロードキャスト

NTP のブロードキャストは転送されません。ntp broadcast コマンドを使用すると、ルータは設定されたインターフェイス上で NTP ブロードキャストを発信します。ntp broadcastclient コマン

## ドを使用すると、ルータまたはスイッチは設定されたインターフェイス上の NTP ブロードキャストをリッスンします。

## NTP のトラフィック レベル

ピア間で交換されるポーリング メッセージの間隔が、17 分（1024 秒）ごとに 1 メッセージの間隔まで通常は徐々に戻っていくので、NTP で利用される帯域幅はごくわずかです。 計画が周到なものであれば、WAN リンクを経由するルータ ネットワーク内でこの間隔を維持できます。NTP クライアントは、WAN 経由でセントラル サイトのコア ルータ（ストラタム 2 サーバ）とピアリングするのではなく、ローカルの NTP サーバとピアリングする必要があります。

収束した NTP クライアントは、サーバごとに約 0.6 bps を消費します。

## 推奨事項

現在、お客様の多くは CatOS プラットフォームで NTP をクライアント モードに設定し、インターネット上の信頼性の高い提供元や電波時計と同期させています。しかし、多数のスイッチを稼働させている場合、サーバ モードに代わる単純な方法として、スイッチド ドメイン内の管理 VLAN 上で NTP をブロードキャスト クライアント モードで有効にする方法があります。このメカニズムでは、Catalyst のドメイン全体が 1 つのブロードキャスト メッセージからクロックを受信できます。ただし、情報のフローが一方向になるため、計時の精度が少し低くなります。

アップデートの送信元としてループバック アドレスを使用すると、一貫性が向上します。セキュリティの問題は次の 2 つの方法で対処できます。

- サーバ アップデートのフィルタリング
- [Authentication]

トラブルシューティングとセキュリティ監査においては、イベントの時間相関が非常に重要です。そのため、時刻源とデータを保護するための対策を採る必要があります。また、故意または過失によって重要なイベントが消去されないように、暗号化を使用することを推奨します。

シスコでは次の設定を推奨しています。

| Catalyst Configuration |
| --- |
| **set ntp broadcastclient enable**<br>**set ntp authentication enable**<br>**set ntp key** *key*<br>*!--- This is a Message Digest 5 (MD5) hash.* **set ntp timezone** |

| Catalyst の代替設定 |
| --- |
| *!--- This more traditional configuration creates !--- more configuration work and NTP peerings.* **set ntp client enable**<br>**set ntp server** *IP address of time server* **set timezone** |

```
zone name set summertime date change details
```

**ルータの設定**

```
!--- This is a sample router configuration to distribute
!--- NTP broadcast information to the Catalyst broadcast
clients. ntp source loopback0
ntp server IP address of time server ntp update-calendar
clock timezone zone name clock summer-time date change
details ntp authentication key key ntp access-group
access-list
!--- To filter updates to allow only trusted sources of
NTP information. Interface to campus/management VLAN
containing switch sc0 ntp broadcast
```

## Cisco Discovery Protocol

CDP はデータリンク層を介して隣接デバイス間で情報を交換します。CDP は、論理層または IP 層の外部のネットワーク トポロジと物理構成の判別に大変役立ちます。サポートされているデバイスは主にスイッチ、ルータ、および IP フォンです。この項では、CDP バージョン 1 に対するバージョン 2 の強化点について説明します。

### 動作の概要

CDP ではタイプ コード 2000 の SNAP カプセル化が使用されます。イーサネット、ATM、および FDDI では、宛先マルチキャスト アドレス **01-00-0c-cc-cc-cc、HDLC プロトコル タイプ 0x2000 が使用されます。**トークン リングでは、機能アドレス c000.0800.0000 が使用されます。デフォルトでは、CDP フレームは 1 分間隔で定期的に送信されます。

CDP メッセージには 1 つ以上のサブメッセージが含まれており、宛先デバイスはこのサブメッセージを使用してすべてのネイバー デバイスに関する情報を収集して保存できます。

CDP バージョン 1 では、次のパラメータがサポートされています。

| パラメータ | Type | 説明 |
|---|---|---|
| 1 | Device-ID | ASCII 形式でのデバイスのホスト名、またはハードウェア シリアル番号。 |
| 0 | 住所 | アップデートを送信したインターフェイスの L3 アドレス。 |
| 3 | ポート ID | CDP アップデートが送信されたポート。 |
| 4 | 機能 | 次にデバイスの機能を示します。ルータ：0x01 TB ブリッジ：0x02 SR ブリッジ：0x04 スイッチ：0x08 ( L2 または L3 スイッチングを提供する ) ホスト：0x10 IGMP 条件付きフィルタリング：0x20 ブリッジやスイッチは非ルータポートで IGMP レポート パケットを転送しません。リピータ：0x40 |

| | | |
|---|---|---|
| 5 | バージョン | ソフトウェア バージョンを含む文字列（**show version** と同じ）。 |
| 6 | Platform | ハードウェア プラットフォーム。WS-C5000、WS-C6009、Cisco RSP など。 |

CDP バージョン 2 では、追加のプロトコル フィールドが導入されました。CDP バージョン 2 ではすべてのフィールドがサポートされていますが、次にリストされているフィールドはスイッチド環境では特に役に立つもので、CatOS で使用されています。

**注：** スイッチで CDPv1 を実行している場合、v2 フレームは破棄されます。CDPv2 を実行中のスイッチのインターフェイスで CDPv1 フレームを受信すると、そのインターフェイスからは CDPv2 フレームに加えて CDPv1 フレームの送信も開始されます。

| パラメータ | Type | 説明 |
|---|---|---|
| 9 ミリ秒 | VTPドメイン | VTP ドメイン（デバイスで設定されている場合）。 |
| 10 | ネイティブVLAN | dot1q では、これはタグなし VLAN です。 |
| 11 | 全二重/半二重 | このフィールドには送信元ポートのデュプレックス設定が含まれます。 |

## 推奨事項

CDP はデフォルトで有効になっており、隣接デバイスの情報の取得やトラブルシューティングに不可欠です。また、ネットワーク管理アプリケーションで L2 トポロジ マップを作成するときにも使用されます。CDP を設定するには、次のコマンドを発行します。

```
set cdp enable
!--- This is the default. set cdp version v2
!--- This is the default.
```

高いレベルのセキュリティが必要なネットワークの部分（インターネットに面した DMZ など）では、次のコマンドを発行して、CDP をオフにする必要があります。

```
set cdp disable port range
```

show cdp neighbors コマンドはローカルの CDP テーブルを表示します。星印（*）の付いたエントリは VLAN の不一致を示し、# の付いたエントリはデュプレックス ミスマッチを示しています。この情報はトラブルシューティング時に役立つ場合があります。

```
>show cdp neighbors

* - indicates vlan mismatch.
# - indicates duplex mismatch.
Port  Device-ID          Port-ID Platform
----- ------------------ ------- ------------
```

```
 3/1   TBA04060103(swi-2) 3/1      WS-C6506
 3/8   TBA03300081(swi-3) 1/1      WS-C6506
15/1   rtr-1-msfc         VLAN 1   cisco    Cat6k-MSFC
16/1   MSFC1b             Vlan2    cisco    Cat6k-MSFC
```

### その他のオプション

Catalyst 6500/6000 などの一部のスイッチには、UTP ケーブルを通じて IP フォンに電力を供給する機能があります。CDP によって取得された情報がスイッチの電源管理に利用されます。

IP フォンに接続している PC があり、両方のデバイスが Catalyst の同じポートに接続している場合、スイッチは VoIP フォンを別の VLAN（Auxiliary VLAN）に配置できます。この機能により、スイッチでは VoIP トラフィックに対して異なる Quality of Service（QoS）を容易に適用できます。

また、Auxiliary VLAN が変更された場合（たとえば、電話機が特定の VLAN や特定のタギング方式を使用するように設定する場合）、この情報は CDP を通じて電話機に送信されます。

| パラメータ | Type | 説明 |
|---|---|---|
| 14 | アプライアンスID | 別の VLAN ID（Auxiliary VLAN）によって、VoIP トラフィックをその他のトラフィックと区別できます。 |
| 16 | 消費電力 | VoIP フォンが消費する電力量（ミリワット単位）。 |

**注**：Catalyst 2900および3500XLスイッチは現在CDPv2をサポートしていません。

## セキュリティ設定

理想的には、お客様が、シスコのどのツールと技術が適格であるかを定義するのに役立つセキュリティ ポリシーをすでに確立していることが望まれます。

**注：CatOSとは異**なり、Cisco IOSソフトウェアセキュリティは、Cisco ISP Essentialsなどの多くのドキュメントで取り上げられています。

### 基本的なセキュリティ機能

#### パスワード

ユーザ レベルのパスワード（ログイン）を設定します。 CatOS 5.x 以降、パスワードは大文字と小文字が区別されており、スペースを含めて 0 ~ 30 文字の長さで設定できます。次のように、イネーブル パスワードを設定します。

```
set password password set enablepass password
```

ログイン パスワードおよびイネーブル パスワードを使用する場合、すべてのパスワードが最小長

の基準（最低 6 文字、文字と数字、大文字と小文字を混在させるなど）を満たしている必要があります。これらのパスワードは、MD5 ハッシュ アルゴリズムを使用して暗号化されます。

パスワードのセキュリティとデバイスへのアクセスをより柔軟に管理できるように、シスコでは TACACS+ サーバの使用を推奨しています。詳細については、このドキュメントの「TACACS+」の項を参照してください。

## [Secure Shell]

スイッチへの Telnet セッションおよびその他のリモート接続に対するセキュリティを実現するには、SSH 暗号化を利用します。SSH 暗号化がサポートされるのは、スイッチにリモート ログインする場合だけです。スイッチから開始される Telnet セッションは暗号化できません。SSHバージョン1はCatOS 6.1でサポートされ、バージョン2はCatOS 8.3でサポートされました。SSHバージョン1はData Encryption Standard(DES)およびTriple-DES(3-DES)暗号化方式、SSHバージョン2は3-DESおよびAdvanced Encryption Standard(AES)暗号化方式ををサポートします。SSH 暗号化は、RADIUS 認証および TACACS+ 認証で使用できます。この機能は、SSH（k9）イメージでサポートされています。詳細については、『CatOS が稼働する Catalyst スイッチでの SSH の設定』を参照してください。

```
set crypto key rsa 1024
```

バージョン 1 のフォールバックを無効にして、バージョン 2 の接続を受け入れるには、次のコマンドを発行します。

```
set ssh mode v2
```

## IP 許可フィルタ

IP 許可フィルタは、Telnet やその他のプロトコルを介した管理 sc0 インターフェイスへのアクセスを保護するためのフィルタです。これは、管理用 VLAN にユーザ データも流れている場合に特に重要になります。IP アドレスとポートのフィルタリングを有効にするには、次のコマンドを発行します。

```
set ip permit enable
set ip permit IP address mask Telnet|ssh|snmp|all
```

ただし、このコマンドで Telnet アクセスが制限されると、少数の信頼できるエンド ステーションからのみ CatOS デバイスにアクセスできることになり、トラブルシューティング時の障害となる場合があります。IP アドレスをスプーフィングして、フィルタされたアクセスを欺くことができることに注意してください。そのため、これは保護の最初の層に過ぎません。

## ポート セキュリティ

たとえば、固定的なエンド ステーションが変更管理を通さずに新しいステーションと交換されないようにするために、ポート セキュリティを利用して、1 つまたは複数の既知の MAC アドレス

からのデータのみ特定のポートを通過できるようにすることを検討してください。 これを実現するには、次のようにスタティック MAC アドレスを使用します。

```
set port security mod/port enable MAC address
```

また、限定された MAC アドレスを動的に学習する方法もあります。

```
set port security port range enable
```

次のオプションを設定できます。

- **set port security mod/port age time value：ポートでアドレスが保持される時間を指定します。この時間が経過すると、新しいアドレスを学習できるようになります。**有効な時間は 10 ~ 1440 分で、デフォルトはエージングなしです。
- **set port securitymod/port maximum value：ポートで保持する MAC アドレスの最大数を指定するキーワード。**有効な値は 1（デフォルト）~ 1025 です。
- set port security mod/port violation shutdown：違反が発生した場合にポートをシャットダウンし（デフォルト）、syslog メッセージを送信して（デフォルト）、トラフィックを廃棄します。
- **set port security mod/port shutdown time value：ポートが無効状態にとどまる時間。**有効な値は 10 ~ 1440 分です。デフォルトではシャットダウンしたままになります。

CatOS 6.x 以降には 802.1x 認証が導入されています。この認証方式を利用すると、クライアントが中央管理サーバに認証されてから、データに対してポートを有効にできます。この機能は Windows XP などのプラットフォームでサポートされ始めたばかりですが、多くの企業で戦略的方向性として検討することができます。Cisco IOS ソフトウェアが稼働するスイッチでのポートセキュリティの設定方法については、ポート セキュリティの設定 [英語] を参照してください。

## ログイン バナー

不正アクセスに対して実行するアクションを明確に示す適切なデバイス バナーを作成します。不正ユーザに情報を提供する可能性があるサイト名やネットワーク データをアドバタイズしないでください。これらのバナーは、デバイスが不正アクセスされて、犯人が捕まったときに頼りになります。

```
# set banner motd ^C
*** Unauthorized Access Prohibited ***
***  All transactions are logged   ***
------------- Notice Board -------------
----Contact Joe Cisco at 1 800 go cisco for access problems----
^C
```

## 物理セキュリティ

デバイスには、適切な認証を行わないと物理的にアクセスできない必要があります。そのため、機器は管理された（ロックされた）スペースに設置してください。環境要因の悪意のある改ざんにより、ネットワークが影響を受けることなく稼働し続けるようにするために、すべての機器に適切な UPS（可能であれば冗長電源を使用）を設置し、温度（空調）を制御する必要があります

。 悪意のある者によって物理的アクセスが破られた場合、パスワードの回復などの方法による中断が生じる可能性が高いことを覚えておいてください。

## Terminal Access Controller Access Control System

デフォルトでは、非特権モードおよび特権モードのパスワードはグローバルであり、コンソール ポート、またはネットワーク経由の Telnet セッションを介してスイッチまたはルータにアクセスするすべてのユーザに適用されます。ネットワーク デバイスへのこれらの実装は時間がかかり、一元的には行われません。また、設定エラーが起こりやすいアクセス リストを使用してアクセス制限を実装するのも困難です。

ネットワーク デバイスへのアクセスの制御とポリシングに利用できるセキュリティ システムには、次の 3 つがあります。これらはクライアント/サーバ アーキテクチャを使用し、すべてのセキュリティ情報を 1 つの中央データベースに格納します。セキュリティ システムには次の 3 つがあります。

- TACACS+
- RADIUS
- Kerberos

この章で説明する TACACS+ は、シスコ ネットワークで一般的に導入されているシステムです。TACACS+ には次のような機能があります。

- 認証：ユーザの識別および検証プロセス。ユーザの認証にはいくつかの方法が使用できますが、最もよく使用されるのはユーザ名とパスワードの組み合せです。
- 認可：認証されたユーザに各種コマンドを付与できます。
- アカウンティング：デバイス上でユーザが行っている操作や過去に行った操作の記録。

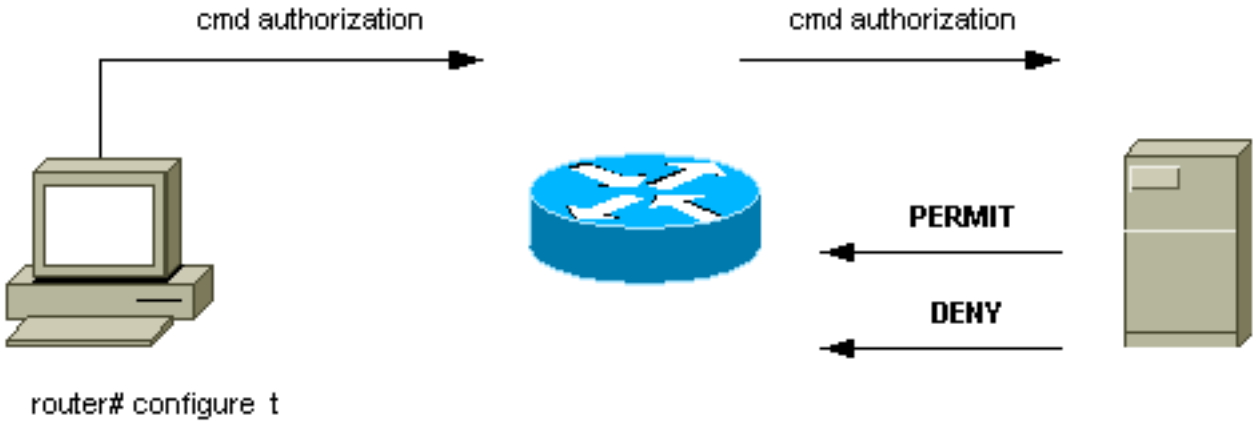
詳細については、『Cisco Catalyst スイッチにおける TACACS+、RADIUS、および Kerberos の設定』を参照してください。

### 動作の概要

TACACS+ プロトコルは、MD5 単方向ハッシング（RFC 1321 ）を使用してユーザ名とパスワードを暗号化した上で、ネットワークを通じて中央サーバに転送します。 TACACS+ はトランスポート プロトコルとして TCP ポート 49 を使用します。そのため、（RADIUS によって使用される）UDP に比べて次のような利点があります。

- コネクション型の転送
- バックエンドの認証メカニズムの現在の負荷にかかわらず、要求が受信されたことを示す確認応答（TCP ACK）が別に送信される
- サーバ クラッシュが迅速に検出される（RST パケット）

セッション中に追加の認可チェックが必要になった場合、スイッチは TACACS+ を使用して、ユーザに特定のコマンドの使用権限が付与されているかどうかをチェックします。これにより、スイッチで実行可能なコマンドを、認証メカニズムと切り離して制御できます。コマンド アカウンティングを使用すると、特定のネットワーク デバイスに接続した状態で特定のユーザが発行したコマンドの監査を行うことができます。




ユーザが TACACS+ を使用してネットワーク デバイスに対して認証を行うことで簡易 ASCII ログインを試みると、通常、次のプロセスが発生します。

- 接続が確立すると、スイッチは TACACS+ デーモンに接続してユーザ名プロンプトを取得し、ユーザに表示します。ユーザがユーザ名を入力すると、スイッチは TACACS+ デーモンにアクセスしてパスワード プロンプトを取得します。スイッチからパスワード プロンプトが表示され、ユーザがパスワードを入力すると、そのパスワードが TACACS+ デーモンに送信されます。
- ネットワーク デバイスは最終的に、TACACS+ デーモンから次のいずれかの応答を受信します。ACCEPT：ユーザは認証され、サービスを開始できます。ネットワーク デバイスの設定で認可が必要とされている場合、この時点で認可が開始されます。REJECT：ユーザは認証に失敗しました。TACACS+ デーモンに応じて、ユーザは今後のアクセスを拒否されるか、ログイン シーケンスの再試行を求められます。ERROR：認証中のある時点でエラーが発生しました。このエラーは、デーモンで発生する場合と、デーモンとスイッチ間のネットワーク接続で発生する場合があります。ERROR 応答を受信すると、ネットワーク デバイスは通常、代替のユーザ認証方式の使用を試行します。CONTINUE：追加の認証情報の入力を促すプロンプトがユーザに表示されます。
- ユーザは TACACS+ 認可に進む前に、まず TACACS+ 認証を正常に完了する必要があります。
- TACACS+ 認可が必要な場合、TACACS+ デーモンに再度接続し、ACCEPT または REJECT 認可応答が返されます。ACCEPT 応答が返された場合、応答にはそのユーザの EXEC または NETWORK セッション向けに使用される属性の形式でデータが含まれており、そのユーザがアクセスできるコマンドが決定されます。

## 推奨事項

シスコでは、CiscoSecure ACS for NT、UNIX、またはその他のサードパーティ製ソフトウェアを使用して簡単に実装できる TACACS+ の使用を推奨しています。TACACS+ の機能には、コマンドの使用とシステムの使用に関する統計情報を提供する詳細なアカウンティング、MD5 暗号化アルゴリズム、認証および認可プロセスの管理制御などがあります。

次の例では、ログインおよびイネーブル モードの認証に TACACS+ サーバを使用し、サーバが使用できない場合はローカル認証にフォールバックします。ローカル認証はほとんどのネットワークに残しておくべき重要なバック ドアです。TACACS+ を設定するには、次のコマンドを発行します。

```
set tacacs server server IP primary set tacacs server server IP
!--- Redundant servers are possible. set tacacs attempts 3
!--- This is the default. set tacacs key key
!--- MD5 encryption key. set tacacs timeout 15
!--- Longer server timeout (5 is default). set authentication login tacacs enable
set authentication enable tacacs enable
set authentication login local enable
set authentication enable local enable
!--- The last two commands are the default; they allow fallback !--- to local if no TACACS+
server available.
```

### その他のオプション

TACACS+ 認可を使用することで、個々のユーザまたはユーザ グループがスイッチで実行できるコマンドを制御できますが、この領域にはすべてのお客様が個別の要件を持っているため、推奨事項を提示するのは困難です。詳細については、認証、認可、およびアカウンティングを使用したスイッチへのアクセスの制御 [英語] を参照してください。

最後に、アカウンティング コマンドを使用することで、各ユーザの入力内容と設定内容に関する監査証跡を提供できます。次に、コマンドの最後で監査情報を受信する一般的な方法の使用例を示します。

```
set accounting connect enable start-stop tacacs+
set accounting exec enable start-stop tacacs+
set accounting system enable start-stop tacacs+
set accounting commands enable all start-stop tacacs+
set accounting update periodic 1
```

この設定には次の特長があります。

- connect コマンドは、スイッチでのアウトバウンド接続イベント ( Telnet など ) のアカウンティングを有効にします。
- exec コマンドは、スイッチでのログイン セッション ( 運用スタッフなど ) のアカウンティングを有効にします。
- system コマンドは、スイッチでのシステム イベント ( リロードやリセットなど ) のアカウンティングを有効にします。
- commands コマンドは、スイッチで入力されたコマンド ( show コマンドと設定コマンドの両方 ) のアカウンティングを有効にします。
- 定期的なアップデートを 1 分ごとにサーバに送信することで、ユーザがログイン中かどうかを記録するのに役立ちます。

## 設定チェックリスト

この項では、推奨される設定の要約を示します。ただし、セキュリティの詳細は除きます。

すべてのポートにラベルを付けておくと非常に便利です。ポートにラベルを付けるには、次のコマンドを発行します。

```
set port description descriptive name
```

次の凡例を、以下に示す表のコマンドとともに使用します。

| **ポイント：** |
| --- |
| **太字のテキスト**：推奨される変更 |
| 通常のテキスト：デフォルト、推奨される設定 |

### グローバル設定コマンド

| コマンド | コメント |
| --- | --- |
| **set vtp domain *name passwordx*** | 新しいスイッチからの不正な VTP アップデートを防止します。 |
| **set vtp mode transparent** | このドキュメントで推奨されている VTP モードを選択します。詳細については、このドキュメントの「VLAN Trunking Protocol」の項を参照してください。 |
| set spantree enable all | すべての VLAN で STP を有効にします。 |
| **set spantree root vlan** | VLAN ごとのルート（およびセカンダリ ルート）ブリッジの推奨位置。 |
| **set spantree backbonefast enable** | 間接的な障害からの迅速な STP コンバージェンスを有効にします（ドメイン内のすべてのスイッチがこの機能をサポートしている場合のみ）。 |
| **set spantree uplinkfast enable** | 直接的な障害からの迅速な STP コンバージェンスを有効にします（アクセス レイヤ スイッチの場合のみ）。 |
| **set spantree portfast bpdu-guard enable** | 不正なスパニング ツリー拡張が存在する場合、ポートの自動シャットダウンを有効にします。 |
| **set udld enable** | 単方向リンク検出を有効にします（ポート レベルの設定も必要）。 |
| **set test diaglevel complete** | ブートアップ時の完全診断を有効にします（Catalyst 4500/4000 ではデフォルト）。 |
| set test packetbuffer sun 3:30 | ポート バッファのエラー チェックを有効にします（Catalyst 5500/5000 のみに適用）。 |
| set logging buffer 500 | 最大の内部 syslog バッファを維持します。 |
| **set logging server *IP address*** | 外部のシステム メッセージ ロギング用のターゲット syslog サーバを設定します。 |

| | |
|---|---|
| **set logging server enable** | 外部ロギング サーバを許可します。 |
| set logging timestamp enable | ログ内のメッセージのタイムスタンプを有効にします。 |
| **set logging level spantree 6 default** | STP のデフォルト syslog レベルを上げます。 |
| **set logging level sys 6 default** | システムのデフォルト syslog レベルを上げます。 |
| set logging server severity 4 | より重大度の高い syslog のエクスポートのみ許可します。 |
| **set logging console disable** | トラブルシューティングの場合を除き、コンソールを無効にします。 |
| **set snmp community read-only string** | パスワードを設定し、リモートでのデータ収集を許可します。 |
| **set snmp community read-write string** | パスワードを設定し、リモートでの設定を許可します。 |
| **set snmp community read-write-all string** | パスワードを設定し、パスワードを含むリモートでの設定を許可します。 |
| **set snmp trap enable all** | NMS サーバに対する SNMP トラップを有効にして、障害およびイベント アラートを行います。 |
| **set snmp trap server address string** | NMS トラップの受信者のアドレスを設定します。 |
| **set snmp rmon enable** | ローカルで統計を収集するための RMON を有効にします。詳細については、このドキュメントの「リモート モニタリング」の項を参照してください。 |
| **set ntp broadcastclient enable** | 上流に位置するルータからの正確なシステム クロックの受信を有効にします。 |
| **set ntp timezone zone name** | デバイスのローカル タイムゾーンを設定します。 |
| **set ntp summertime date change details** | サマータイムを設定します（タイムゾーンに適用可能な場合）。 |
| **set ntp authentication enable** | セキュリティを確保するために、暗号化された時間情報を設定します。 |
| **set ntp key key** | 暗号キーを設定します。 |
| set cdp enable | ネイバー探索を有効にします（デフォルトではポート上でも有効になります）。 |
| **set tacacs server IP address primary** | AAA サーバのアドレスを設定します。 |

| | |
|---|---|
| **set tacacs server IP address** | 可能であれば、AAA サーバを冗長化します。 |
| set tacacs attempts 3 | AAA ユーザ アカウントのパスワード入力を 3 回まで認めます。 |
| **set tacacs key key** | AAA MD5 暗号キーを設定します。 |
| **set tacacs timeout 15** | サーバのタイムアウトを長くします（デフォルトは 5 秒）。 |
| **set authentication login tacacs enable** | ログインの認証に AAA を使用します。 |
| **set authentication enable tacacs enable** | イネーブル モードの認証に AAA を使用します。 |
| set authentication login local enable | デフォルト：AAA サーバが使用できない場合にローカル フォールバックを許可します。 |
| set authentication enable local enable | デフォルト：AAA サーバが使用できない場合にローカル フォールバックを許可します。 |

**ホスト ポートの設定コマンド**

| コマンド | コメント |
|---|---|
| **set port host port range** | 不要なポート処理を削除します。このマクロは、スパニング ツリーの PortFast を有効、チャネルをオフ、トランクをオフに設定します。 |
| set udld disable port range | 不要なポート処理を削除します（銅線ポートではデフォルトで無効）。 |
| set port speed port range auto | 最新のホスト NIC ドライバによる自動ネゴシエーションを使用します。 |
| set port trap port range disable | 一般ユーザの SNMP トラップは不要です。キー ポートのみ追跡されます。 |

**サーバ設定コマンド**

| コマンド | コメント |
|---|---|
| **set port host port range** | 不要なポート処理を削除します。このマクロは、スパニング ツリーの PortFast を有効、チャネルをオフ、トランクをオフに設定します。 |
| set udld disable port range | 不要なポート処理を削除します（銅線ポートではデフォルトで無効）。 |
| **set port speed port** | 通常はスタティック/サーバ ポー |

| | |
|---|---|
| range 10 / *100* | トを設定します。それ以外は自動ネゴシエーションを使用します。 |
| set port duplex port range full / *half* | 通常はスタティック/サーバ ポート。それ以外は自動ネゴシエーションを使用します。 |
| set port trap port range enable | キー サービス ポートはトラップを NMS に送信する必要があります。 |

### 未使用ポートの設定コマンド

| コマンド | コメント |
|---|---|
| set spantree portfast port range disable | STP 用に必要なポートの処理と保護を有効にします。 |
| set port disable port range | 未使用ポートを無効にします。 |
| set vlan unused dummy vlan port range | ポートが有効な場合、不正トラフィックを未使用の VLAN に送信します。 |
| set trunk port range off | 管理されるまでポートのトランキングを無効にします。 |
| set port channel port range mode off | 管理されるまでポートのチャネリングを無効にします。 |

### インフラストラクチャ ポート（スイッチ間、スイッチとルータ間）

| コマンド | コメント |
|---|---|
| set udld enable port range | 単方向リンク検出を有効にします（銅線ポートではデフォルトではない）。 |
| set udld aggressive-mode enable port range | アグレッシブ モードを有効にします（デバイスでサポートされている場合）。 |
| set port negotiation port rangeenable | リンク パラメータのデフォルトの GE 自動ネゴシエーションを許可します。 |
| set port trap port range enable | これらのキー ポートに対して SNMP トラップを許可します。 |
| set trunk port | トランクを使用していない場合、機能を無効にします。 |

| | |
|---|---|
| **range off** | |
| **set trunk mod/port desirable ISL / *dot1q* /ネゴシエート** | トランクを使用している場合、dot1q が優先されます。 |
| **clear trunk mod/port vlan range** | トランクが不要な場合、トランクから VLAN をプルーニングすることで STP の直径を制限します。 |
| **set port channel port range mode off** | チャネルを使用していない場合、機能を無効にします。 |
| **set port channel port range mode desirable** | チャネルを使用している場合、PAgP を有効にします。 |
| set port channel all distribution ip both | チャネルを使用している場合、L3 送信元/宛先ロード バランシングを許可します（Catalyst 6500/6000 ではデフォルト）。 |
| **set trunk mod/port nonegotiate ISL / *dot1q*** | ルータ、Catalyst 2900XL、3500、またはその他のベンダーにトランキングしている場合、DTP を無効にします。 |
| **set port negotiation mod/port disable** | ネゴシエーションは、一部の古い GE デバイスとは互換性がないことがあります。 |

## 関連情報

- Catalyst 4500/4000 シリーズ スイッチでの一般的な CatOS エラー メッセージ
- 「Common CatOS Error Messages on Catalyst 5000/5500 Series Switches（Catalyst 5000 および 5500 シリーズ スイッチでの一般的な CatOS エラー メッセージ）」
- Catalyst 6500/6000 シリーズ スイッチでの一般的な CatOS エラー メッセージ
- スイッチ製品に関するサポート ページ
- LAN スイッチング テクノロジーに関するサポート ページ
- テクニカル サポートとドキュメント – Cisco Systems