# 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

## 目次


概要
前提条件
要件
使用するコンポーネント
表記法
背景説明
基本設定
Catalyst コントロール プレーン プロトコル
VLANトランキング プロトコル
拡張 VLAN と MAC アドレスの削減
自動ネゴシエーション
ギガビット イーサネット
ダイナミック トランキング プロトコル
スパニング ツリー プロトコル
EtherChannel
単方向リンク検出
ジャンボ フレーム
管理設定
ネットワーク構成図
インバンド管理
アウトオブバンド管理
システム テスト
システムとハードウェアのエラー検出
EtherChannel とリンク エラーの処理
Catalyst 6500/6000 のパケット バッファの診断
システム ロギング
Simple Network Management Protocol ( SNMP; 簡易ネットワーク管理プロトコル )
リモート モニタリング
ネットワーク タイム プロトコル
Cisco 発見プロトコル
セキュリティ設定
基本的なセキュリティ機能
Terminal Access Controller Access Control System
設定チェックリスト

関連情報

# 概要

このドキュメントでは、ネットワーク上の 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ています。 ドキュメント内で説明されている設定とコマンドは、Catalyst OS ( CatOS ) General Deployment ソフトウェア 6.4(3) 以降が稼働していることを前提としています。 設計上の考慮事項もいくつか示していますが、このドキュメントは全体的なキャンパス設計を目的とするものではありません。

# 前提条件

## 要件

このドキュメントでは、読者が『Catalyst 6500 シリーズ コマンド リファレンス、7.6』について理解していることが前提となっています。

一般に公開されているオンライン資料への参照がドキュメント中に示されていますが、その他にも、次のような基礎的または教育的な参照資料があります。

- Cisco ISP の必須事項：各 ISP で考慮する必要のある IOS の必須機能
- 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
- 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
- Cisco SAFE:

## 使用するコンポーネント

このドキュメントは、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

ここで紹介するソリューションには、数多くの最大規模のお客様や複雑なネットワークに長年にわたり取り組んできた Cisco エンジニアのフィールドでの経験が反映されています。 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、現実的なコンフィギュレーション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ものであり、リスクが非常に低いソリューション。
- 決定論的な結果を得るために、一部の柔軟性を犠牲にしてシンプルな形をとっているソリューション。
- 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。

- アベイラビリティと安定性の向上を促進するソリューション。

このドキュメントは次の 4 つのセクションに分かれています。

- 基本設定：Spanning Tree Protocol（STP; スパニング ツリー プロトコル）やトランキングなど、ほとんどのネットワークで使用される機能。
- 管理設定：Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）、Remote Monitoring（RMON; リモート モニタリング）、Syslog、Cisco Discovery Protocol（CDP）、Network Time Protocol（NTP; ネットワーク タイム プロトコル）を使用したシステムおよびイベントの監視に関連する、設計上の考慮事項。
- セキュリティ設定：パスワード、ポート セキュリティ、物理的なセキュリティ、TACACS+ を使用した認証。
- 設定チェックリスト：推奨される設定テンプレートの要約。

# 基本設定

このセクションでは、ほとんどの Catalyst ネットワークが装備している機能について説明しています。

## Catalyst コントロール プレーン プロトコル

この項では、正常に動作しているスイッチの間で実行されるプロトコルを紹介します。 これらのプロトコルの基本を押さえておけば、各セクションの内容を理解する上で役立ちます。

### 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。 このようなプロトコルには、CDP のように Cisco 独自のものや、IEEE 802.1d（STP）のように標準ベースのものがありますが、いずれも、Catalyst シリーズに実装された場合には共通の要素があります。

基本的なフレーム転送では、ユーザ データ フレームがエンドシステムから発信されます。このフレームの送信元アドレスと宛先アドレスは、レイヤ 2（L2）スイッチ ドメイン全体を通じて変更されることはありません。 送信元アドレスの学習プロセスによって、各スイッチのスーパーバイザ エンジン上にある Content Addressable Memory（CAM）ルックアップ テーブルにデータが入力されます。このテーブルを参照することで、受信した各フレームをどの出力ポートから転送する必要があるかがわかります。 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。

スイッチはまた、システムを通じてスイッチングするフレームと、スイッチの CPU 自体（Network Management Processor（NMP; ネットワーク管理プロセッサ）とも呼ばれる）に送る必要があるフレームを識別する必要があります。

Catalyst コントロール プレーンは、トラフィックの受信と内部スイッチ ポート上の NMP への転送の目的で、**システム エントリ**と呼ばれる CAM テーブルの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。 次のように、スイッチで show CAM system コマンドを発行すると、これがわかります。

```
>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. ...
```

Cisco では、イーサネット MAC アドレスとプロトコル アドレスの範囲を次の表のように予約しています。 各項目については、このドキュメントの後の方で取り上げています。 便宜上、次の表に要約を示しています。

| 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; ポート集約プロトコル） | 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 |
| UniDirectional Link Detection（UDLD; 単方向リンク検出） | 0x0111 | 01-00-0c-cc-cc-cc |
| Cisco 発見プロトコル | 0x2000 | 01-00-0c-cc-cc-cc |
| Dynamic Trunking（DTP; ダイナミック トランキング プロトコル） | 0x2004 | 01-00-0c-cc-cc-cc |
| STP アップリンク ファースト | 0x200a | 01-00-0c-cd-cd-cd |
| IEEE スパニング ツリー 802.1d | N/A：DSAP 42 SSAP 42 | 01-80-c2-00-00-00 |
| Inter Switch Link（ISL; スイッチ間リンク） | N/A | 01-00-0c-00-00-00 |
| VLAN Trunking（VTP; VLAN トランク プロトコル） | 0x2003 | 01-00-0c-cc-cc-cc |
| IEEE ポーズ、802.3x | N/A：DSAP 81 SSAP 80 | 01-80-C2-00-00-00>0F |

Cisco の制御プロトコルのほとんどでは、**LLC 0xAAAA03, OUI 0x00000C** のように、IEEE 802.3 SNAP カプセル化を使用しています。これは、LAN アナライザのトレースで確認できます。 この他にも、これらのプロトコルには次のような共通の性質があります。

- 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 が Cisco 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、フレームの解釈と取り込みを行わないデバイスでは、それらのフレームが単純にフラッディングされるためです。 ただし、マルチベンダー環境を経由したポイントツーマルチポイント接続は一貫性のない動作を引き起こすおそれがあるため、通常は使用しないでください。
- これらのプロトコルはレイヤ3（L3）ルータで終端します; 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 Application-Specific Integrated Circuit（ASIC; 特定用途向け集積回路）の処理およびスケジューリングでは、ユーザ データよりも優先されます。

ここまで制御プロトコルの宛先アドレスについて説明しましたが、完全を期すために送信元アドレスについても説明します。 スイッチ プロトコルは、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 MAC アドレスを取得して使用します。 **show module コマンドを発行すると、STP Bridge Protocol Data Unit（BPDU; ブリッジ プロトコル データ ユニット）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できるアドレスの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 スーパーバイザ エンジンはトランキング時に、常にデフォルトの VLAN である VLAN 1 を使用して、CDP、VTP、PAgP などの多数の制御プロトコルや管理プロトコルをタグ付けします。 すべてのポートは、内部 sc0 インターフェイスを含んで VLANの構成員 1.であるために、デフォルトで設定されます。 すべてのトランクはより 5.4 が、それ VLAN 1.のユーザのデータをブロックしてできなかった CatOS ソフトウェア バージョンの VLAN 1 を、先にデフォルトで運び。

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

- マネージメントVLAN は sc0 が常駐するところにです; この VLAN は変更できます。
- ネイティブ VLAN は、非トランキング時にポートが復帰する VLAN として定義されています。ネイティブ VLAN は 802.1Q トランクではタグ付けされません。 デフォルトでは、VLAN1 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:** トランクのネイティブ VLAN に設定する前に、その VLAN を作成してください。

ネットワークを調整し、VLAN 1 に属する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。

- 他の VLAN と同様に、VLAN 1 の直径が（特に STP の観点から）安定性が損なわれるおそれがあるほど大きい場合は、VLAN 1 をプルーニングする必要があります。 これについての詳細は、このドキュメントの「インバンド管理」セクションを参照してください。
- VLAN 1 のコントロール プレーン データはユーザ データから分離する必要があります。これ

により、トラブルシューティングが容易になり、最大限の CPU サイクルを利用できるようになります。
- 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 の L2 ループを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する必要があります。

- **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 データ用に VLAN 1 を削除しても、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 に送出されます。 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 でなくなっている場合でも同様です。 802.1Q トランクでは、DTP パケットがネイティブ VLAN で送出されます。 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、共通スパニング ツリーの VLAN 1 上をタグなしで **802.1Q IEEE BPDU** が転送されます。 これは、ネイティブ VLAN の設定にかかわらず同様です。 **Cisco PVST+ BPDU** は、他のすべての VLAN についてタグ付きで送信されます。 詳細は、このドキュメントの「スパニング ツリー プロトコル」セクションを参照してください。
- ISL と 802.1Q の両方のトランクとも、802.1s Multiple Spanning Tree ( MST; 多重スパニング ツリー ) BPDU は常に VLAN 1 に送出されます。 この動作は、VLAN 1 がトランクから削除されていても変わりません。
- MST ブリッジと PVST+ ブリッジの間のトランクの VLAN1 を削除または無効にしないでください。 しかし、VLAN 1 が無効になっている場合は、すべての VLAN で MST ブリッジの境界ポートが「root-inconsistent」状態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。 詳細は、『多重スパニング ツリー プロトコル ( 802.1s ) について』を参照してください。

## 推奨事項

クライアントやホストが VLAN に接続されていない状態で VLAN を **up/up** 状態に保つためには、その VLAN に少なくとも 1 台の物理デバイスを接続しておく必要があります。 そうしないと、VLAN は **up/down** 状態になります。 現状では、その VLAN のスイッチにアクティブ ポートがない場合に、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、その VLAN の任意のポートにループバック プラグを接続します。 別の方法として、同じスイッチで、その VLAN の 2 つのポートにクロスケーブルを接続してみることもできます。 この方法ではポートが強制的に **up** 状態になります。 詳細は、『T1/56K 回線のループバック テスト』の「ループバック プラグ」セクションを参照してください。

ネットワークがサービス プロバイダーにマルチホームされている場合には、そのネットワークが 2 つのサービス プロバイダーの間の中継ネットワークとして機能します。 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、パケットで受信した VLAN 番号を変換または変更する必要がある場合は、QinQ 機能を使用して VLAN 番号を変換することを推奨いたします。

# VLANトランキング プロトコル

VLAN を作成する前に、ネットワークで使用する VTP モードを決定します。 VTP を使用すれば、1 台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。 これらの変更は、ドメイン内のすべてのスイッチに自動的に伝搬します。

## 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、VLAN の追加、削除、および名前の変更をネットワーク全体で管理します。 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、VTP サーバの NVRAM にコンフィギュレーション ファイルとは別に保存されています。

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、スイッチ間で通信します。 VTP は非トランク ポートでは機能しないため（VTP は ISL または 802.1Q のペイロードです）、DTP によってトランクがオンラインになるまでメッセージを送信することはできません。

メッセージ タイプには、5 分間隔で生成される要約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、VTP プルーニングが有効な場合の加入などがあります。 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 のメンバだったポートが非アクティブ状態に移行します。 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無効になります。

さまざまな VTP モードの機能比較の要約を次の表に示します。

| **機能** | **server** | **クライアント** | **トランスペアレント** | **オフ1** |
|---|---|---|---|---|
| VTP メッセージの発信 | ○ | ○ | なし | なし |
| VTP メッセージの受信 | ○ | ○ | なし | なし |
| VTP メッセージの転送 | ○ | ○ | ○ | なし |
| VLAN の作成 | ○ | なし | （ローカルで意味がある場合のみ） | （ローカルで意味がある場合のみ） |
| VLAN の記憶 | ○ | なし | （ローカルで意味がある場合のみ） | （ローカルで意味がある場合のみ） |

VTP transparent モードでは、VTP アップデートは無視されます（制御フレームを選択してスーパーバイザ エンジンに送るために通常使用されるシステム CAM から VTP マルチキャスト MAC アドレスが除去されます）。 このプロトコルはマルチキャスト アドレスを使用するため、transparent モードのスイッチ（または他のベンダーのスイッチ）はドメイン内の他の Cisco 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 には、off モードを使用して VTP を無効にするオプションが追加されています。 VTP off モードでは、VTP transparent モードに非常によく似た方法でスイッチが動作します。ただし、off モードでは、VTP アップデートの転送も抑止される点が異なります。

次の表に初期設定の要約を示します。

| 機能 | デフォルト値 |
|---|---|
| VTP ドメイン名 | Null |
| VTP モード | server |
| VTP バージョン | バージョン 1 は有効に なります |
| VTP パスワード | なし |
| VTP プルーニング | 無効 |

VTP バージョン 2（VTPv2）には次の柔軟な機能が含まれていますが、 VTP バージョン 1（VTPv1）との相互運用はできません。

- トークン リングのサポート。
- 認識されていないVTP情報サポート; スイッチは今解析できない値を伝搬させます。
- バージョン依存 透過モード; もはやドメイン名をチェックしません。 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。
- バージョン番号伝搬; VTPv2 がすべてのスイッチで可能性のあるである場合、完全に単一 のスイッチの設定によって有効に なることができます。

詳細は、『VLAN トランク プロトコル（VTP）の説明と設定』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 には、VTP バージョン 3（VTPv3）のサポートが追加されています。 VTPv3 では、既存のバージョンの機能が拡張されています。 これらの機能拡張により、次のことが可能になりました。

- 拡張 VLAN のサポート
- プライベート VLAN の作成と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 マッピング伝搬インスタンスのサポート（CatOS リリース 8.3 でサポート）
- サーバ認証の強化
- 間違ったデータベースが偶発的に VTP ドメインに挿入された場合に対する保護
- VTPv1 および VTPv2 とのやりとり
- ポート単位の設定機能

VTPv3 の実装とそれよりも前のバージョンの主な違いの 1 つは、VTP プライマリ サーバの導入です。 理想的には、ドメインがパーティション化されていない場合、VTPv3 ドメインには 1 つだけのプライマリ サーバが存在する必要があります。 VTP ドメインに伝搬されるためには、

VTP ドメインに対する変更が VTP プライマリ サーバで実行されることが必要です。 VTPv3 ドメイン内に、セカンダリ サーバとも呼ばれる複数のサーバが存在する場合があります。 スイッチがサーバとして設定されると、デフォルトでは、そのスイッチはセカンダリ 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。 スイッチから引き継ぎが正常に行われると、セカンダリ サーバがプライマリ サーバになることができます。

VTPv3 が稼働するスイッチでは、現在のプライマリ サーバよりも高いバージョン番号の VTP データベースだけが受け入れられます。 この処理は、VTPv1 および VTPv2 とは大幅に異なります。VTPv1 および VTPv2 では、スイッチでは常に、同じドメインのネイバーから上位の設定を受け入れていました。 VTPv3 におけるこの変更により、保護が実現されます。 VTP リビジョン番号が大きい新しいスイッチをネットワークに追加しても、ドメイン全体の VLAN 設定が上書きされることはありません。

また、VTPv3 では、VTP がパスワードを処理する方法も機能拡張されています。 パスワード非表示設定オプションを使用してパスワードを「hidden ( 非表示 )」に設定すると、次のように処理されます。

- コンフィギュレーションでパスワードがプレーンテキストでは表示されません。 パスワードは秘密 16 進数形式でコンフィギュレーションに保存されます。
- 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、パスワードの入力を求めるプロンプトが表示されます。 入力したパスワードが秘密パスワードと一致すると、スイッチがプライマリ サーバになり、ドメインを設定できるようになります。

**注:** プライマリ サーバが必要になるのはインスタンスの VTP 設定を変更する必要がある場合だけであるということを覚えておくことが重要です。 **セカンダリ サーバによってリロード時にも設定の持続性が確保されるので、**アクティブなプライマリ サーバなしでも VTP ドメインは動作できます。 プライマリ サーバの状態が終了するのは、下記の場合です。

- スイッチのリロード
- アクティブなスーパーバイザ エンジンと冗長スーパーバイザ エンジンの間の高可用性スイッチオーバー
- 別のサーバからの引き継ぎ
- モード設定の変更
- いずれかの VTP ドメイン設定の変更。次の項目の変更です。バージョンドメイン名ドメインパスワード

また、VTPv3 では、VTP の複数のインスタンスにスイッチが参加できます。 この場合、異なる VTP インスタンスには固有の VTP モードがあるので、同じスイッチが、1 つのインスタンスに対しては VTP サーバになり、別のインスタンスに対してクライアントになることができます。 たとえば、MST インスタンスに対してはスイッチが transparent モードで動作するようにして、VLAN インスタンスに対しては server モードになるようにスイッチを設定できます。

VTPv1 および VTPv2 とのやりとりについては、すべてのバージョンの VTP のデフォルト動作では、新しいバージョンのアップデートをそれよりも前のバージョンの VTP が単純に廃棄するようになっていました。 VTPv1 および VTPv2 のスイッチが transparent モードでない限り、すべての VTPv3 アップデートは廃棄されます。 他方、VTPv3 スイッチは、従来の VTPv1 または VTPv2 のフレームをトランクで受信すると、スケールダウンされたバージョンのデータベース アップデートを VTPv1 および VTPv2 のスイッチに渡します。 ただし、この情報交換は片方向だけで、VTPv1 および VTPv2 のスイッチからのアップデートは VTPv3 のスイッチでは受け入れられません。 トランク接続では、トランク ポート経由での VTPv2 と VTPv3 のネイバーに対応するために、スケールダウンされたアップデートと完全な VTPv3 アップデートを VTPv3 スイッチが引き続き送出します。

拡張 VLAN で VTPv3 をサポートするために、VTP で VLAN ごとに 70 バイトが割り当てられている 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、従来のプロトコル用の未変更のフィールドを伝送するのではなく、デフォルトではない値だけをコーディングすることが可能になります。 この変更により、変更後の VLAN データベースのサイズは 4K VLAN サポートになります。

## 推奨事項

VTP クライアント/サーバ モードと VTP 透過モードのどちらを使用するかについての特別な推奨事項はありません。 一部のお客様では、後述する注意事項があるものの、管理の容易さを優先して VTP client/server モードが使用されています。 この場合は、冗長性を確保するために、各ドメインに 2 台のサーバ モード スイッチ ( 通常は 2 台のディストリビューション レイヤ スイッチ ) を設定することを推奨します。 ドメイン内の残りのスイッチは client モードに設定する必要があります。 VTPv2 を使用して client/server モードを実装する際には、同じ VTP ドメインでぱ、より大きなリビジョン番号が常に受け入れられることに注意してください。 VTP client か server のどちらかのモードに設定されているスイッチを VTP ドメインに追加した場合、そのリビジョン番号が既存の VTP サーバより大きいと、そのVTP ドメイン内の VLAN データベースが上書きされます。 設定の変更が意図したものではなく、VLAN が削除される場合には、この上書きによって大規模な障害がネットワークで発生する可能性があります。 client または server のスイッチが、サーバーの設定リビジョン番号よりも常に小さな設定リビジョン番号になるようにするためには、標準の名前とは異なる名前にクライアント VTP ドメイン名を変更します。 その後、標準の名前に再び変更します。 このようにすれば、クライアントの設定リビジョン番号が 0 に設定されます。

ネットワークを簡単に変更できる 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、VTP transparent モードの注意深いアプローチが好まれています。

- スイッチまたはトランク ポート上の VLAN 変更要件は一度に 1 台のスイッチについて検討する必要があるため、この方法では適切な変更管理手法が実践できる。
- VLAN の誤削除のようなドメイン全体に影響が及ぶ管理者のミスが発生する危険が少くなる。
- 大きい VTP リビジョン番号を持つ新規スイッチをネットワークに導入した場合でも、ドメイン全体の VLAN 設定が上書きされるおそれがない。
- VTP transparent モードでは、ある特定の VLAN に属するポートがないスイッチにトランクが接続している場合、そのトランクからの VLAN のプルーニングが促進される。 これにより、フレームがフラッディングされるときの帯域の使用効率が向上します。 手動のプルーニングには、スパニング ツリーの直径が小さくなるという利点もあります ( このドキュメントの「DTP」セクションを参照 )。 ポート チャネル トランクにある未使用の VLAN をプルーニングする前に、IP Phone に接続されているすべてのポートが音声 VLAN を備えたアクセス 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 で拡張された番号 1025 ~ 4094 の VLAN の範囲は、この方法でなければ設定できない。 詳細は、このドキュメントの「拡張 VLAN と MAC アドレスの削減」セクションを参照してください。
- Campus Manager 3.1 の VTP 、Cisco Works 2000 の一部サポートされます。 VTP ドメインの少なくとも 1 サーバ必要とされる取除かれたこと古い制約事項。

| VTP コマンドの例 | コメント |
|---|---|
| set | CDP は、ドメイン間の配線のミスをチェックす |

| | |
|---|---|
| **vtp domain name** pass word **x** | るために名前を確認します。 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。 |
| **set vtp mode transparent** | |
| **set vlan vlan number** name **name** | VLAN 内にポートを持つスイッチ単位。 |
| **set trunk mod/port vlan range** | トランクを有効にし、必要に応じて VLAN を伝送します。デフォルトではすべての VLAN が伝送されます。 |
| **clear trunk mod/port vlan range** | 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 VLAN を手動でプルーニングすることにより、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 が追加されるだけで削除されません。 たとえば、set trunk x/y 1-10 コマンドはちょうど VLAN に許可されたリストを 1-10 設定 しません。 望ましい結果を実現させるために clear trunk x/y 11-1005 コマンドを発行して下さい。

トークン リング スイッチングについてはこのドキュメントでは扱いませんが、TR-ISL ネットワークでは VTP transparent モードが推奨されない点に注意が必要です。 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。したがって、すべてのスイッチが同じ VLAN 情報を持つことになります。

## その他のオプション

VTPv2 は/強く推奨されているトークンリング環境の要件です。

VTPv3 では、より厳密な認証および設定リビジョン番号制御を実装できます。 VTPv3 では、基本的に VTPv1 や VTPv2 の transparent モードと同じレベルの機能が実現されていますが、セキュリティ機能が拡張されています。 さらに、VTPv3 は従来の VTP バージョンと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ています。 必要ではないフレームの非能率的なフラッディングを停止する set vtp pruning enable コマンドは VLAN を自動的にプルーニングします。 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 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搬されます。

- VLAN 1 – 1001
- 拡張されたバーチャルLAN（VLAN）: 1025 – 4094 （しか VTPv3 によって伝搬することができません）
- 予約範囲 VLAN: 0、1002 ～ 1024、4095

IEEE では、VTP と同様の結果を実現する標準ベースのアーキテクチャを策定しました。 802.1Q Generic Attribute Registration Protocol（GARP）のメンバとして、Generic VLAN Registration Protocol（GVRP）は VLAN 管理における異なるベンダー間の相互運用を可能にします。ただし、GVRP については、このドキュメントでは取り上げていません。

**注:** CatOS 7.x には、transparent に非常によく似た off モードに VTP を設定するオプションが追加されています。 ただしこの場合、スイッチは VTP フレームを転送しません。 この設定は、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 アドレスの削減

MAC アドレス削減機能により、範囲を拡張した VLAN の識別が可能になります。 MAC アドレス削減を有効にすると、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 アドレス削減サポートが追加されており、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の 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 個か 64 個のどちらかの MAC アドレスがサポートされています。

1024 個の MAC アドレスを使用する Catalyst スイッチの場合、デフォルトでは MAC アドレス削減は有効になりません。 MAC アドレスは、シーケンシャルに割り当てられます。 範囲の最初の MAC アドレスは VLAN 1.に割り当てられます。 範囲の第 2 MAC アドレスは VLAN 2 に、等割り当てられます。 このようにして、それぞれが一意なブリッジ ID を使用する 1024 個の VLAN をスイッチがサポートできるようになります。

| 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 アドレス削減がデフォルトで有効になり、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 アドレスの削減を有効にすると、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一意な ID を設定したりできます。 MAC アドレスの削減では、STP に必要な MAC アドレスの数が、VLAN または MISTP ごとに 1 つからスイッチごとに 1 つに減ります。

次の図は、ブリッジ ID MAC アドレスの削減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 アドレスの削減では、BPDU の STP ブリッジ ID の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。 分割後は、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。


Catalyst スイッチで MAC アドレスの削減を有効にして、拡張範囲 VLAN を利用する場合は、同じ STP ドメイン内のすべてのスイッチで MAC アドレスの削減を有効にします。 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 した後、ルートブリッジ 優先順位は VLAN ID と 4096 の倍数になります。 MAC アドレス リダクションのないスイッチはこれらのスイッチにブリッジID の選択でより細かい粒状度があるのでルートを不注意に要求できます。

## 設定のガイドライン

拡張された VLAN の範囲を設定する際には、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、拡張された範囲から 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 モジュール用に 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 から始まって数字が大きくなる

方向に割り当てられていきます。 Flex WAN モジュールが必要とする範囲内の VLAN を割り当ててしまうと、VLAN がユーザ VLAN エリアから割り当てられることがないため、必要な VLAN すべてが割り当てられなくなります。 **show vlan コマンドか show vlan summary コマンドをスイッチで発行すると、ユーザ割り当てと内部使用の VLAN の両方を表示できます。**

```
>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、拡張範囲の 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 transparent モードを使用して各スイッチに拡張 VLAN を静的に設定する必要があります。 詳細は、『VLAN の設定』の「拡張範囲の VLAN の設定ガイドライン」を参照してください。

**注:** ソフトウェア リリース 8.1(1) よりも前のソフトウェアでは、拡張範囲の VLAN に VLAN 名を設定できません。 この機能は、VTP のバージョンやモードには依存しません。

## 推奨事項

同じ STP ドメイン内では、一貫した MAC アドレス削減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 ドメインに追加する際に、すべてのネットワーク デバイスで MAC アドレスの削減を実施するのが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 アドレス削減がデフォルトで有効になっており、この機能を無効にはできません。 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と、MAC アドレスの削減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 アドレスの削減の有効と無効を設定するには、次のコマンドを実行します。

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

内部 VLAN のアロケーションは昇順にあり、VLAN 1006 で開始します。 ユーザ VLAN と内部 VLAN 間の競合を避けるために VLAN 4094 にユーザ VLAN をと可能な限り同様に密接に割り当てて下さい。 Catalyst 6500 スイッチを使うと Cisco IOS® システム ソフトウェアを実行する、降順の内部 VLAN アロケーションを設定できます。 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/ファースト イーサネット

自動ネゴシエーションはファスト イーサネット（FE）規格（IEEE 802.3u）のオプション機能であり、これを使用すると、デバイス間で**速度**と**デュプレックス**に関する情報を、リンクを通じて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に関する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場合です。 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 プロセスによって統一されなかった場合にしばしば発生します。 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。 このときの典型的な症状としては、スイッチでの Frame Check Sequence（FCS; フレーム チェック シーケンス）、Cyclic Redundancy Check（CRC; 巡回冗長検査）、アラインメント、またはラント カウンタの増加が挙げられます。

自動ネゴシエーションについては、次のドキュメントに詳細が説明されています。 次のドキュメントには、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は、一方のリンク パートナーを 100 Mbps 全二重に手動で設定しておけば、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トされるものと一般に誤解されています。 実際にこのように設定してみると、デュプレックスのミスマッチが起こります。 これは一方のリンク パートナーでの自動ネゴシエーション プロセスで、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たことを示します。

## 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いますが、このことは show port capabilities mod/port コマンドによって確認できます。

## FEFI

自動ネゴシエーションが物理層/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 ワイヤがはずれている場合など、一方のステーションでは検出できるものの、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ており、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しています。 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していません。 そのようなリモート障害を検出する 100BASE-FX ステーションはリモート障害をネイバーに知らせるために特別なビット 構成を（FEFI アイドル パターンと言われる）送信 するように伝送されたアイドルストリームを修正できます; FEFI-IDLE パターンは続いてリモートポート（errdisable）のシャットダウンを引き起こします。 障害保護についての詳細は、このドキュメントの「UDLD」セクション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 スイッチとの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、問題が生じる可能性があります。 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高度な機能のために、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： これの例のための CAT4K/6K に接続する Intel Pro/1000T NIC においてのパフォーマンス上の問題。

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場合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、リンクの両側でハード 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。 理想的な状況では、自動ネゴシエーションは、サーバや固定されたワークステーションのような非一時的デバイス、スイッチ同士の間、およびスイッチとルータとの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。 このような場合は、ドキュメント中に示されている 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 ポートでポート速度を auto に設定すると、速度とデュプレックスの両方が自動ネゴシエートされます。 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 コードする場合は、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 以降には、オプションの **auto-10-100** キーワードが追加されています。 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、10/100 Mbps のポートで速度が **auto** に設定されているのと同じようにポートが動作するようになります。 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 障害表示も機能しなくなることがあります。 障害検出を強化するには、アグレッシブ UDLD などの L2 プロトコルが役立ちます。

# 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しかサポートされていません）。

**注:** 802.3z はすでに IEEE 802.3:2000 仕様で置き換えられています。 行 LAN/MAN 規格サブスクリプションの IEEE規格を参照して下さい: 詳細についてはアーカイブ。

## 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一致している必要があります。 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、リンクがアップになります。 この動作は、遠端の自動ネゴシエーション設定には依存しません。 たとえば 2 つのデバイスが、A および B.あると、仮定して下さい。 各デバイスは自動ネゴシエーション イネーブルまたはディセーブルがある場合があります。 次の表は、可能な設定とそれぞれのリンク状態を示しています。

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

GE では、同期化と自動ネゴシエーション（イネーブルになっている場合）は、予約されたリンク コード ワードの特別なシーケンスを使用して、リンクの起動時に実行されます。

**注:** 有効なワードの辞書が備わっており、GE ではすべての単語が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、次のような特徴があります。


同期が失われるとは、リンク ダウンが MAC で検出されることです。 同期が失われると、自動ネゴシエーションが有効か無効かが適用されます。 無効なワードを 3 回連続で受信するなど、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 状態に変わります。 同期が失われると、再同期するためには、3 回連続の有効なアイドルが必要になります。 受信（Rx）信号の喪失など、他の壊滅的なイベントも、link-down イベントを発生させます。

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わります。 ただし、スイッチは引き続きリンクの状態を監視します。 ポートの自動ネゴシエーションが無効になると、「autoneg」フェーズを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ポートで行えます。

**注:** GE ファイバ仕様では、デュプレックスのネゴシエーション、フロー制御、およびリモート障害検出が規定されているだけです。 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全体の時間を制御するためのソフトウェアの機能です。 この時間内に自動ネゴシエーションが正しく行われないと、デッドロックが存在する場合は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

GE 環境で自動ネゴシエーションを有効にするのは、10/100 環境でこれを有効にするよりもはるかに注意が必要です。 実際には、自動ネゴシエーションを無効にするのは、ネゴシエーションがサポートされ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に問題が生じているスイッチ ポートだけに限定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 つとして、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 ソフトウェアが稼働している Gigabit Switch Router（GSR; ギガビット スイッチ ルータ）に接続している場合があります。 この場合はこれら 2 つの機能をオフにします。そうしなければ、スイッチ ポートでは not connected と報告され、GSR ではエラーが報告します。 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が必要です。 PAUSE フレーム（**既知の MAC 01-80-C2-00-00-00 0F**）の送信や応答にデバイスが対応している場合とそうでない場合があります。 さらに、遠端のネイバーのフロー制御要求には同意できません。 入力バッファがいっぱいになりそうなポートからリンク パートナーに PAUSE フレームが送信されると、リンク パートナーでは送信を保留し、自身の出力バッファに以降のフレームを保持します。 これにで恒常的な加入過多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入力バッファを実質的に拡張できることになります。

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す。エンド ホストでは、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利点はそれほどありません。

スイッチ ポートでフロー制御を設定するには、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    Receive FlowControl   RxPause TxPause
       admin    oper       admin    oper
-----  -------- --------   -------- --------     ------- -------
 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は、すべての Catalyst モジュールが PAUSE フレームに応答します。 WS-X5410 や WS-X4306 などの一部のモジュールでは、そのようにネゴシエートされている場合でも、PAUSE フレームは送信されません。これは、これらのモジュールがブロッキングに非対応であるためです。

## 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 )、それらのフレームが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 の動作の概要

何年もの間、Cisco 独自の識別 ( タギング ) 方式である ISL が使用されてきました。 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 は実質的にはトンネリング 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 ポートとして設定されたポートでは、標準よりも大きいサイズのイーサネット フレームが到達し、処理されます。 ISL は 1024 の VLAN をサポートします。

**ISL フレーム形式**

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 40 ビット | 4 ビ | 4 ビ | 4 8 | 1 6 | 24 ビ | 2 4 | 1 5 | 1 ビ | 16 ビッ | 1 6 | 可変長 | 3 2 |

| | ビット | ビット | ビット | ビット | ビット | ビット | ビット | ビット | ト | ビット | | ビット |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Dest. アドレス | タイプ | USER | SA | 長さ | SNAP LLC | HSA | VLAN | BPDU | インデックス | 予約 | カプセル化されたフレーム | FCS |
| 01-00-0c-00-00 | | | | | AAAA03 | 000000C | | | | | | |

詳細は、『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 の動作の概要

IEEE 802.1Q 規格では、カプセル化タイプだけでなく、スパニング ツリーの拡張機能、GARP（このドキュメントの「VTP」セクションを参照）、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ています。一方、スイッチでは、ホストが QoS シグナリングとして 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する可能性のあるアクセス ポート上ですら、ベビージャイアント フレームが受信されるものと想定されています。 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 グループの成果です。 802.1Q では、4096 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 については、入力スイッチ ポート設定に基づく暗黙的なタグがあります）。 ネイティブ VLAN の帯は送信されたタグが付いていなく普通タグが付いていない受け取られて常に。 ただし、それらはまたタグ付けされた受け取ることができます。

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 | Priority | 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、802.1Q だけがサポートされているものもあります）、新しく実装する場合はすべて IEEE 802.1Q 規格に準拠するようにして、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間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、これはどのような Cisco 環境にとっても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 に比べて小さく、これも、小さいながら 802.1Q の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」セクション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 上を転送されます。

また、このドキュメントの「VLAN 1」セクション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 上を送信されます。 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、なおかつスイッチでネイティブ VLAN が変更されている場合は、タグ付き CDP フレームを受信し、ルータに CDP ネイバー情報を提供するために、VLAN 1 でサブインターフェイスが必要になります。

**注:** dot1q では、ある VLAN から別の VLAN へルータを通さずにフレームを送信できる場合があります。これはネイティブ VLAN の暗黙的なタギングによるもので、セキュリティの観点から注意が必要です。 refer to VLAN 実装の脆弱性そこにありますか。 を参照してください。 この問題を回避するには、トランクのネイティブ VLAN の VLAN ID として、エンド ユーザ アクセスに使用していないものを使用します。 Cisco 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 ポートに VLAN 1 以外の VLAN を割り当てるという単純な方法で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連する各種パラメータ（設定されたカプセル化タイプ、ネイティブ VLAN、ハードウェア機能など）が、トランクの両端にあるスイッチの間で確実に合意されることを目的としています。 また、ポートとその近接デバイスが一貫した状態を保つようにすることで、重大なセキュリティ上の危険になり得る、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防御の役割も果たします。

## 動作の概要

DTP は、スイッチ ポートとその近接デバイス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 が使用されます。 次の表に設定モードの要約を示します。

| モード | 機能 | DTP フレームの送信 | 最終的な状態（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 または desirable モードに設定されている場合、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 |
| | ポートは常にトランキング モードになり、リンクをトランクに変換するかどうかをネゴシエートします。 隣接ポートが変更に同意しなかった場合でも、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、近接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。 | なし | トランキング、**無条件** |
| | ポートは能動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 または auto モードに設定されている場合、ポートはトランク ポートになります。 | 送信する、定期的 | リモート モードが on、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 | 安定状態では送信しない。ただ | 非トランキング |

| | | | |
|---|---|---|---|
| | 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。 | し、on からの変更後、リモート エンドで迅速に検出されるようにするため、通知を送信する。 | |

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、Cisco デバイスでサポートされているのはポイントツーポイントの 802.1Q トランク ポートだけです。
- DTP ネゴシエーションの間、ポートは STP に参加しません。 ポートがなる後やっと 3 つの DTP 型（アクセス、ISL、または 802.1Q）の 1 つは STP にポートを追加されますします。他では PAgP は、もし設定するなら、ポートが STP に加わる前に動作するべき次のプロセスです。
- 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 モードでは、DTP パケットは **VTP ドメイン名**（アップするにはネゴシエートされたトランクと合っている必要あり）に加えて、トランク設定と **admin status** を転送します。
- メッセージはネゴシエーション中には 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 の各モードはポートが最終的にどの状態になるかを明示的に指定することを理解してください。 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 モードのポートでは DTP フレームが定期的に送信されます。auto または desirable モードのポートは、DTP パケットを 5 分間受信しなかった場合、非トランクに設定されます。

ISL についての詳細は、『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』を参照してください。 802.1Q についての詳細は、『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』を参照してください。

## 推奨事項

Cisco では、リンクの両端で desirable の明示的なトランク設定を使用することを推奨しています。 このモードでは、on モードと異なり、ネットワーク オペレータは、ポートがアップしてトランキング状態にあるという syslog メッセージおよびコマンドライン ステータス メッセージを信頼できます。それに対して on モードでは、ネイバーの設定が正しくない場合でも、ポートがアップしているように見える場合があります。 さらに、desirable モードのトランクは、リンクの一方がトランクになれない場合や、トランク状態でなくなった場合にも、安定して動作します。desirable モードに設定するには、次のコマンドを発行します。

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

**注:** すべての非トランク ポートでは、トランクを off に設定してください。 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。 このコマンドはまた set port host コマンドが使用されるとき実行されます; 詳細については STP セクションを参照して下さい。 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 モードを使用し、アクセス レイヤでは最も簡単なデフォルト設定（auto モード）を使用する方法があります。

いくつかのスイッチは、Catalyst 2900XL のような、Cisco IOS ルータ、DTP によってか他の開発元 デバイス、現在 トランクニゴシエーションをサポートしません。 キャンパスを渡るよくある設定で標準化を助けることができるこれらのデバイスによって無条件でトランキングするためにポートを設定 するために Catalyst 4500/4000、5500/5000、およびスイッチ 6500/6000 のの使用できます。 また、nonegotiate モードを実装して、全体的なリンク初期化時間を短縮することもできます。

**注:** チャネル モードや STP 設定などの要因も、初期化時間に影響する可能性があります。

nonegotiate モードに設定するには、次のコマンドを発行します。

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

ブリッジングを実行しているときに、on モードから受信された 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 ルータへの接続時にぱ nonegotiate を使用することを推奨します。 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 が有効な場合、スイッチは DTP フレームを送信しません。

## スパニング ツリー プロトコル

### 基本的な注意事項

Spanning Tree Protocol（STP; スパンニング ツリー プロトコル）は、冗長なスイッチ ネットワークおよびブリッジ 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 がなければ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することになるため、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 の改良が今後も追加される予定です。 また、CatOS 7.x では、IEEE 802.1 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、ルート Bridge Identifier（BID; ブリッジ識別子）の最も小さいスイッチがルート ブリッジとして選出されます。 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 が送信されますが、これには各スイッチの 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。 これを使用して、ルート ブリッジと、ルートへの最小コスト パスが決定されます。 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コンバージが行われます。

1. スパニング ツリー ドメイン全体で 1 台のルート ブリッジが選出されます。
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 つ選出されます。
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 つ選出されます。
4. 非指定ポートがブロッキング ステートになります。

詳細は、『スパニング ツリーの設定』を参照してください。

| 基本タイマーのデフォルト（秒） | 名前 | 機能 |
|---|---|---|
| 2 | Hello | BPDU の送信を制御します。 |
| 15 | Fwddelay | 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の長さを制御するもので、トポロジ変更プロセスが調整されます（次セクションを参照）。 |
| 20 | Maxage | スイッチが現在のトポロジを維持する時間の長さを制御します。この時間が過ぎると、代替パスの検索が始まります。Maxage 秒が経過すると、BPDU は期限切れになったものと見なされ、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。 使用可能なブロッキング 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と宣言します。 |

| ポートの状態 | 意味 | 次の状態に移行するデフォルトのタイミング |
|---|---|---|
| | 管理上の目的でダウンに設定されている。 | N/A |

| | | |
|---|---|---|
| Blocking | BPDU を受信する。ユーザ データは転送しない。 | BPDU の受信を監視します。Maxage がタイムアウトするまで 20 秒待ちます。直接または ローカルのリンクの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 秒待つ ) |
| | トポロジおよび CAM テーブルを構築する。 | Fwddelay タイマー ( 15 秒待つ ) |
| | データを送受信する。 | |
| | **基本的なトポロジ変更に要する時間の合計：** | **Maxage がタイムアウトするまで待つ場合は 20 + 2 (15) = 50 秒。直接的な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 Topology Change Notification ( TCN; トポロジ変更通知 ) BPDU の 2 つのタイプがあります。

## 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。 安定状態では、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と、そのたびに新しい BPDU が Catalyst の中央 NMP で処理され、ルートの情報を含んだまま送出されます。 言い換えると、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は、BPDU が受信されなくなります ( maxage タイマーによって再選出が始まるまで ) 。

## 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た場合にリーフ スイッチから発信され、ルート ブリッジに向けて送られます。 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、途中の各ステップで確認応答されるため、これは信頼できるメカニズムです。 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 フラグを設定したコンフィギュレーション BPDU を **maxage + fwddelay** 時間 ( デフォルトでは 35 秒間 ) 発信し、トポロジが変更されたことをドメイン全体に通知します。 これを受けて、すべてのスイッチでは、自身の通常の CAM エージング タイムが 5 分 ( デフォルト ) から **fwddelay** で指定された間隔 ( デフォルトでは 15 秒 ) に変更されます。 詳細は、『スパニング ツリー プロトコル トポロジの変更について』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 通りがあります。

- すべての VLAN で 1 つのスパニング ツリーを実行するモノ スパニング ツリー プロトコル（IEEE 802.1Q など）
- VLAN ごとにスパニング ツリーを実行する共有スパニング ツリー（Cisco PVST など）
- VLAN のセットごとにスパニング ツリーを実行する多重スパニング 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 バランシングを考慮することはできません。 STP ブロッキング ポートはすべての VLAN をブロックし、データをいっさい伝送しません。

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 の処理に必要な CPU プロセスも増えます。 CatOS リリース ノートに、スイッチ単位のスパニング ツリーで推奨される論理ポートの数についてのガイド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×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 をこれら 2 つのツリーにマッピングすることが可能です。 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 を数千単位の VLAN に展開できます。

## 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 の STP 実装が拡張されて IEEE 802.1Q モノ スパニング ツリー領域に渡るトンネリングのサポートが追加され、PVST+ が誕生しました。 したがって PVST+ は、IEEE 802.1Q の MST プロトコルと Cisco PVST プロトコルのどちらとも互換性があります。そのために特別なコマンドや設定は必要ありません。 また、PVST+ には、すべてのスイッチの間でポート 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 上で実行されるため、この VLAN を、他のベンダーと相互運用するトランクで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 共有スパニング ツリー MAC アドレスにも送信されます。
- PVST+ では、802.1Q VLAN 領域に渡り、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 の共有スパニング ツリー 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、他のすべての VLAN ではタグが付けられます。
- PVST+ はポートと VLAN の不一致をチェックします。 PVST+ はフォワーディング ループを

避けるため、一致しない BPDU を受信したポートをブロックします。 また、設定のミスマッチが見つかった場合は、syslog メッセージを通じて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。 すなわち、各 BPDUタイプはリンク ローカルです; 変換問題がありません。

## 推奨事項

すべての Catalyst スイッチでは、デフォルトで STP が有効になります。 これは、L2 ループを含まない設計を選んだために、ブロッキング 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.
```

Cisco では、次のような理由から STP を有効のまま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 が動作していれば、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事態を回避できます。
- 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、現場での使用実績が豊富です。 使用実績が高いということは、一般にコードが安定していることを意味します。
- 二重に接続された NIC の動作不良（またはサーバ上で有効にされたブリッジング）に対する保護。
- 多くのプロトコルのためのソフトウェアは STP と（PAgP、IGMP Snooping およびトランキングのような）密接に関連しています。 STP なしの実行は望ましくない結果をもたらす場合があります。

**安定性に悪影響を及ぼすおそれがあるため、タイマーを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できる hello-interval や Maxage などの単純な STP タイマーは、それ自体、他に装備された組み込みタイマーを複雑に組み合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ことは困難です。 また、UDLD による保護の効果が失われるおそれもあります。

**ユーザ トラフィックを管理 VLAN から切り離すことが理想的です。** 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 ステーションから発信されたブロードキャスト パケットによってスーパーバイザ エンジン プロセッサの負荷が非常に高くなり、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、制御を調節できる最近のスイッチを使用すれば、この問題は緩和されます。 詳細は、このドキュメントの「インバンド管理」セクションを参照してください。

**冗長性を過剰に設計しないで下さい。** これは、大量のブロッキング ポートにより長期的な安定性が悪影響を受けるという、トラブルシューティングの悪夢につながるおそれがあります。 **SPT 全体の直径は 7 ホップ未満に抑えてください。** 可能であれば、ネットワーク設計時には Cisco のマルチレイヤ モデルに基づき、より小さいスイッチ ドメイン、STP トライアングル、および確定的なブロッキング 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』に説明があります）。

**ルート機能とブロッキング ポートの位置を操作して把握し、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キング ポートから始まります。ポートがどのような理由でブロッキング ステートからフォワーディング ステートに変更されたかが、しばしば根本原因分析の鍵となります。 **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と考えられているためです。 L3 および HSRP の、L2 データ転送パスに最適なオーバーレイをチェックします。 このコマンドはブリッジ優先順位を設定するマクロです; ルートはセカンダリ ルートはデフォルトより低いそれを適度に設定 するがそれをデフォルトより多くの下部の 設定 します（32768）、:

```
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。

**不必要な VLAN をトランクポートからプルーニングしてください**（双方向で実施してください）。 こうすることで 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、トランクから STP は除去されません。 詳細は、このドキュメントの「VTP」セクションを参照してください。 CatOS 5.4 以降では、デフォルトの VLAN 1 もトランクから削除できます。

詳細は、『スパニング ツリー プロトコルのトラブルシューティング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

Cisco には **VLAN ブリッジ**という別の STP があります。 このプロトコルは、宛先 MAC アドレス **01-00-0c-cd-cd-ce**、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またはレガシー プロトコルをブリッジす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起こり得ます）、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もう 1 つのトポロジが提供されます。

シスコでは、MSFC などの Cisco 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。

## PortFast

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、リンク初期化後にエンドステーションが接続するサービスとの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、リンク状態がアップした直後にアクセス 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』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 blocking モードから forwarding モードに直接移行することにより、STP の通常の listening 状態と learning 状態が省略されます。 この機能が有効でなければ、STP によりポートが forwarding モードに移行できることが確認されるまで、ユーザ データはすべて廃棄されます。 これには ForwardDelay の 2 倍の時間（デフォルトでは合計 30 秒）がかかる可能性があります。

PortFast モードには、ポート状態が learning から forwarding 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（朝出勤した人々が一斉に PC の電源を入れた場合によく見られます）、コンバージェンス時間が不必要に長くなるおそれがあります。

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。 これらの環境の TCN は場合があります老化させます静的なCGMP CAMテーブルエントリをキャッシュのサイズによって次の IGMP レポートまでのマルチキャスト パケット損失という結果に終る、および/または再製される必要があり、ルータCPUスパイクという結果に終る可能性がある同じ高さの MLSキャッシュ エントリを。 （IGMP Snooping から学習される Catalyst 6500/6000 MLS は実装およびマルチキャストエントリ影響を受けていません。）

## 推奨事項

シスコでは、アクティブなホスト ポートについてはすべて 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つい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、スイッチの近接デバイス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、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に大きく貢献します。**

```
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 を設定しても、それらのポートでスパニング ツリーがまったく実行されなくなるわけではありません。 BPDU は通常どおり送受信され、処理されます。

## その他のオプション

PortFast の BPDU ガードでは、非トランキング ポートで BPDU が受信された場合に、そのポートを errdisable ステートに移行することによってループが防止されます。

PortFast に設定されたアクセス ポートでは、BPDU パケットが受信されてはなりません。これは、ホスト ポートはスイッチに接続してはならないためです。 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、PortFast が設定されたインターフェイスで BPDU が受信された場合に、スパ

ニング ツリーによりそのインターフェイスが STP の blocking ステートにされるのではなく、シャットダウンされます。

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可能です。 詳細は、このドキュメントの「UDLD」セクションを参照してください。 その他の情報については、『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:** CatOS 7.x でトランク ポート用の PortFast が導入されましたが、これは以前のリリースのトランク ポートには効果がありません。 トランク ポート用 PortFast の設計目的は、L3 ネットワークのためにコンバージェンス時間を長くすることです。 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、ネットワークのアクセス レイヤで直接的な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 は変更されていません。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です。 詳細は、『アップリンク ファースト機能の説明と設定について』を参照してください。

## 動作の概要

アクセス レイヤで Cisco 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に、ブロッキング アップリンクが、listening ステートと learning ステートをバイパスして即時に forwarding ステートに移行します。

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 ポートとバックアップ 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。 このプライマリ ルート接続になんらかの原因で障害が発生した場合は、通常のような 30 秒間のコンバージェンス遅延が起こらずに、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。

これによって通常の STP トポロジ変更処理プロセス（listening と learning）が実質的にバイパスされるため、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通じ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。 そのため、UplinkFast を実行しているアクセス レイヤ スイッチは、CAM テーブル内の 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、ブロッキング 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）で 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 リンクという暗黙的なトポロジ情報を持たないスイッチ（Cisco 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、設定対象のスイッチがルート ブリッジになる危険性を最小限に抑えるため**ブリッジ プライオリティ**を、また、または指定ポートになる危険を最小限に抑えるため**ポート プライオリティ**を、それぞれ高い値に設定します。スイッチがルート ブリッジまたは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際には、この機能を無効にし、「clear uplink」によってアップリンク 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元に戻す必要があります。

**注:** プロトコル フィルタリング機能を有効にする場合は、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 テーブルには 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。 **比率** キーワードは uplinkfast トポロジアップデート帯のパケット毎秒を示します。 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 は間接的な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キング ポートが代表ブリッジから不良 BPDU を受信したときに動作を開始します。 このような事態が起こるのは、ダウンストリーム スイッチがルートへの接続を失い、新しいルートを選出するために自身の BPDU を送信し始めた場合です。 **不良 BPDU** は 1 台のスイッチをルート ブリッジと指定ブリッジの両方として識別します。

通常のスパニングツリー規則では、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 ) が経過するまで不良 BPDU を無視します。 しかし、BackboneFast が有効であれば、スイッチは不良 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を探します。 このプロトコル追加により、スイッチでルートがまだ使用可能かどうかを確認できるようになり、blocked ポートを forwarding ステートにさらに速く移行して、不良 BPDU を送信していると確認されたスイッチにはルートがまだ存在することが通知されます。

このプロトコルの動作には次のような特徴があります。

- スイッチが RLQ パケットを送出するのはルート ポートからのみです ( つまり、ルート ブリッジに向けてのみ送出されます ) 。
- 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場合は、ルート ポートからクエリーを転送します。
- 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 ポートで応答が受信された場合は廃棄されます。

maxage がタイムアウトす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。

詳細は、『Catalyst スイッチ上の Backbone Fast の概要と設定』を参照してください。

## 推奨事項

Cisco 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認識される必要がある機能を 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

2900XL および 3500 では BackboneFast はサポートされていません。 スイッチ ドメイン内に、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 Cisco 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 ビジー
- BPDU の通常の転送を妨げる何らかの要因

冗長構成のトポロジで、ブロックされているポートが誤って forwarding 状態に移行すると、STP ループが発生します。 この状態の移行は、物理的に冗長構成になっているトポロジのポートの 1 つ ( ブロックされているポートとは限りません ) が BPDU を受信しなくなったために発生します。

ループ ガードが役立つのは、スイッチがポイントツーポイントで接続されているスイッチド ネットワークの場合だけです。 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、代表ブリッジが不良 BPDU を送信するかリンクをダウンさせるかしない限り、代表ブリッジが認識されなくな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 ガードについての詳細は、『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 ガードでは、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が調べられます。 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再び BPDU が受信され始めるまで、ポートを inconsistent 状態（ブロック中）にします。 inconsistent 状態のポートでは、BPDU の送信は行われません。 そのようなポートで再び BPDU が受信されると、ポート（およびリンク）は再び実行可能とみなされます。 ポートが loop-inconsistent 状態ではなくなると、回復が自動的に行われ、STP がポートの状態を判断します。

ループ ガードにより障害の切り分けが行なわれ、障害リンクや障害ブリッジを外した安定したトポロジにスパニング ツリーが収束されます。 ループ ガードは、現在使用中の STP バージョンの速度で STP ループを防止します。 STP 自身（802.1d または 802.1w）には依存せず、STP タイマー調整時の影響もありません。 これらの理由により、STP に依存するトポロジで、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、UDLD とともにループ ガードを実装してください。

ループ ガードによって不整合ポートがブロックされると、次のメッセージがログに記録されます。

```
set spantree backbonefast enable
```

STP が loop-inconsistent 状態のポートで BPDU が受信されると、ポートは STP の別の状態に移行します。 受信された BPDU に従って、自動的にリカバリが行われるので、人間が介入する必要はありません。 リカバリの後には、次のメッセージがログに記録されます。

```
set spantree backbonefast enable
```

## 他の STP 機能とのやりとり

- **ルート ガード**ルート ガードにより、ポートは常に指定ポートになります。 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だけ有効です。 これらの機能は、相互に排他的に機能します。 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 ガードがルート ポートを blocking 状態にすると、UplinkFast は新しいルート ポートを forwarding 状態にします。 さらに、UplinkFast が loop-inconsistent 状態のポートをルート ポートに選択す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。 代表ブリッジから不良 BPDU を受信すると、BackboneFast が起動されます。 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。
- **PortFast**PortFast では、リンクアップするとすぐにポートが forwarding designated 状態に移行します。 PortFast が有効なポートは、ルート ポートや代替ポートになれないので、ループ ガードと PortFast は相互に排他的に機能します。
- **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ことが必要です。 PAgP では、チャネルを形成するすべての物理ポートに対して、ループ ガードを均一に設定できます。**注:** EtherChannel にループ ガードを設定するときには、次の点に注意が必要です。STP はチャネル内で最初に動作可能なポートを常に選択して BPDU を送信する。 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ても

、ループ ガードがチャネルをブロックします。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る。 新しいチャネル ポートは、指定ポートの役割が指定された forwarding 状態になることができます。チャネルがループ ガードによってブロックされて、機能しない場合、STP ではすべての状態情報が失われる。 チャネルを形成していた 1 つ以上のリンクが単方向になっていても、個々の物理ポートは、指定ポートの役割が指定された forwarding 状態になることができます。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は、ループが発生する可能性があります。 しかし、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 機能は一部重なっています。 どちらも、単方向リンクによって発生する STP の障害からの保護を行います。 しかし、これら 2 つの機能の問題に対するアプローチは異なり、機能も異なります。 具体的には、CPU が BPDU を送信しない場合に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、アグレッシブな 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可能性があります。

共有リンクまたはリンクアップ時から単方向になっているリンクでは、ループ ガードは機能しません。 リンクアップ時から単方向になっているリンクの場合、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可能性があるので、このケースはループ ガードの対象にはなりません。 UDLD を使用すれば、このようなシナリオに対しても防止が可能です。

最高度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「ループ ガードと UDLD の対比」セクションを参照してください。

## 推奨事項

物理的ループのあるスイッチド ネットワークでは、グローバルにループ ガードを有効にすることを推奨します。 Catalyst ソフトウェア バージョン 7.1(1) 以降では、すべてのポートに対してループ ガードをグローバルに有効にできます。 実際には、この機能はすべてのポイントツーポイント リンクに対して有効になります。 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。 デュプレックスが全二重のリンクは、ポイントツーポイント リンクとみなされます。 グローバルにループ 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 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 チャネルのポートも含む個々のポートすべてでこの機能を有効にします。 指定ポートにループ 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、スパニング ツリーが正しく再コンバージされるときに指定ポートが実際にルート ポートになる場合があり、そのようなときにはループ ガード機能がそのポートで役立つことになります。 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
```
ループのないトポロジのネットワークでも、偶発的にループが発生した場合にループ ガードが役立つ可能性があります。 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、ネットワークの孤立の問題につながる場合があります。 ループのないトポロジを構築してネットワークの孤立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または個々に無効にします。 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.
  ```

## スパニング ツリー ルート ガード

ルート ガード機能により、ネットワーク内でのルート ブリッジの配置を指定する手段が提供されます。 ルート ガードでは、ルート ガードが有効なポートが必ず指定ポートになります。 通常、ルート ブリッジ ポートは、そのルート ブリッジの 2 つ以上のポートが相互に接続されていない限り、すべて指定ポートです。 ルート ガードがイネーブルになっているポートで上位の STP BPDU を受信したブリッジは、そのポートの STP 状態を root-inconsistent に変更します。 この root-inconsistent ステートは、事実上はリスニング ステートと同等になります。 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 ガードでは、ルート ブリッジの位置が維持されます。 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 ガードには自身のタイマーはなく、BPDU の受信だけに依存しています。 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 ポートになれません。 BPDU の受信を契機としてスパニング ツリーの収束が行われ、指定ポートがルート ポートになる場合は、そのポートが root-inconsistent 状態になります。 この処理は、syslog メッセージに次のように表示されます。

```
set spantree guard none mod/port
!--- This is the default port configuration.
```
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 listening 状態から learning 状態になり、最終的には forwarding 状態に移行します。 回復は自動的に行われるので、人間が介入する必要はありません。 次に syslog メッセージの例を示します。

```
set spantree guard none mod/port
!--- This is the default port configuration.
```
ルート ガードは、ポートを強制的に指定ポートにします。一方、ループ ガードが有効なのは、ポートがルート ポートか代替ポートの場合にだけです。 そのため、これら 2 つの機能は、相互に排他的に機能します。 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

Cisco 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 ガード機能をイネーブル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ための 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にアルゴリズムの違いが生じるのは、分散を決定するに当たってフレームのヘッダー情報をどのようにして取得するかがハードウェアのタイプごとに異なるためです。

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 標準では特定の分散アルゴリズムが規定されていないため、PAgP および 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、どの分散アルゴリズムでも、フレームの受信時には、アルゴリズムによって特定のカンバセーションの一部の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）情報をワイヤ速度で読み取ることで、単純な MAC L2 情報によるよりも、多重化に関して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異なります。 **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。**

次の表は、リストされた各プラットフォームでのフレーム分散アルゴリズムについての詳細をまとめたものです。

| プラットフォーム | チャネル ロード バランシング アルゴリズム |
|---|---|
| Catalyst 5500/5000 シリー | 必要なモジュールを装備した Catalyst 5500/5000 では、FEC1 あたり 2 ~ 4 のリンクを接続できます。ただし、それらのリンクはすべて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、送信元および宛 |

| | |
|---|---|
| ズ | 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 演算を行います。 このオペレーションは 4 つの結果の 1 つをもたらします: (0 0)、(0 1)、(1 0)、または(1 1)。 これらの値のそれぞれが 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 の場合は、X-OR 演算には 1 ビットのみが使用されます。 発信元と宛先のペアのうち、片方のアドレスが不変である場合があります。 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ケースとして、宛先がルータの場合も考えられます。 この場合は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。 |
| Catalyst 4500/4000 シリーズ | Catalyst 4500/4000 の EtherChannel は、各フレームの送信元および宛先 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の間でフレームを分散させます。 Catalyst 5500/5000 と比べて、アルゴリズムはより複雑で、MAC DA（バイト 3、5、6）、のこれらのフィールドの決定論ハッシュを SA（バイト 3、5、6）、入力ポートおよび VLAN ID 使用します。 フレームの分散方法は設定不可能です。 |
| Catalyst 6500/6000 シリーズ | スーパーバイザ エンジン ハードウェアに応じて 2 種類のハッシング 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、どのような場合でも MAC アドレス、IP アドレス、または IP TCP/UDP2 ポート番号を使用して、このアルゴリズムで 3 ビットの値を生成します。 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。 その結果の XOR をとって 3 ビット値をもう 1 つ生成し、この値を使用して、チャネル内のどのポートでパケットを転送するかを決定します。 Catalyst 6500/6000 では、任意のモジュール上のポート（最大 8 ポート）の間でチャネルを構成できます。 |

1 FEC = Fast EtherChannel

2 UDP = User Datagram Protocol

次の表は、さまざまな Catalyst 6500/6000 スーパーバイザ エンジン 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 | 初期 Supervisor Engine 1 | L2 MAC： SA; DA; SA 及び DA |

| | | |
|---|---|---|
| ン ） | | |
| WS-F6020A （ L2 エンジン ） WS-F6K-PFC （ L3 エンジン ） | 後期 Supervisor Engine 1 および Supervisor Engine 1A ( PFC1 付 ） | L2 MAC： SA; DA; SA 及び DA L3 IP: SA; DA; SA および DA （ デフォルト ） |
| WS-F6K-PFC2 | Supervisor Engine 2 ( PFC2 付 ）（ CatOS 6.x が必要 ） | L2 MAC： SA; DA; SA 及び DA L3 IP: SA; DA; SA 及び DA （ デフォルト ） L4 セッション: S ポート; D ポート; S 及び D ポート ( デフォルト ） |
| WS-F6K-PFC3BXL WS-F6K-PFC3B WS-F6K-PFC3A | Supervisor Engine 720/PFC3A （ 必要 CatOS 8.1.x ） Supervisor Engine 720/Supervisor エンジン 32/PFC3B （ 必要 CatOS 8.4.x ） Supervisor Engine 720/PFC3BXL （ 必要 CatOS 8.3.x ） | L2 MAC： SA; DA; SA 及び DA L3 IP: SA; DA; SA 及び DA （ デフォルト ） L4 セッション: S ポート; D ポート; S 及び D ポート IP-VLAN-L4 セッション: SA 及び VLAN 及び S ポート; DA 及び VLAN 及び D ポート; SA 及び DA 及び VLAN 及び S ポート及び D ポート |

**注:** L4 分散では、最初の断片化パケットが 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 ソフトウェアを実行している Catalyst 4500/4000、5500/5000、および 6500/6000 スイッチ間での 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

## 推奨事項

Catalyst 6500/6000 シリーズのスイッチでは、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、チャネルを通じて通信している主なデバイスが 2 台しかない場合は、すべてのトラフィックについて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、集約スループットの統計情報を収集することは可能ですが、Cisco では、各物理インターフェイスを個別に管理することで、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ことを推奨しています。

CatOS 6.x の新しいコマンドである show channel traffic コマンドでは、CatOS 5.x で 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よりも簡単に、分散統計情報のパーセンテージを表示できます。 CatOS 6.x の別の新しいコマンドである show channel hash コマンドでは、CatOS 6.x で、分散モードに基づいて、特定のアドレスまたはポート番号のどちらかまたは両方に対する発信ポートとして、どのポートが選択されるかを調べることができます。 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 アルゴリズムでの相対的な制限が問題で、良好な統計的ロード バランシングが達成されない場合に、考えられる対策を次に示します。

- Catalyst 6500/6000 スイッチを要所に配置する。
- たとえば、複数の FE ポートから 1 つの GE ポートへ、または複数の GE ポートから 1 つの 10 GE ポートへ移行することにより、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 を提供する。

## EtherChannel の設定ガイドラインと制限

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限はスイッチ 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 が有効な場合に、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、EtherChannel バンドリングの QoS ポート アトリビュート チェックを no mls qos channel-consistency ポートチャネル インターフェイス コマンドで無効にできます。 QoS ポート アトリビュート チェックを無効にする同等のコマンドは CatOS にはありません。 QoS ポートの機能を表示して、ポートに互換性があるかどうかを確認するには、show port capability mod/port コマンドを発行できます。

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』（Catalyst 6500/6000）の「EtherChannel の設定ガイドライン」セクション
- 『Fast EtherChannel と Gigabit EtherChannel の設定』（Catalyst 4500/4000）の「EtherChannel の設定ガイドラインと制限」セクション
- 『Fast EtherChannel と Gigabit EtherChannel の設定』（Catalyst 5000）の「EtherChannel

の設定ガイドラインと制限」セクション

**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 スイッチにより最大 128 の EtherChannel がサポートされています。 ソフトウェア リリース 6.2(2) 以降では、ポート ID はスパニング ツリー機能により処理されます。 そのため、6 または 9 スロット シャーシの場合、サポートされる EtherChannel の最大数は 126 で、13 スロット シャーシの場合には 63 になります。

## ポート集約プロトコル

PAgP は、リンクの両端でパラメータが一致しているかどうかをチェックし、リンクの障害または追加が発生したときにチャネルの適応を助け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、チャネルのすべてのポートが同じ VLAN に属すか、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異なる VLAN に変更できるため、EtherChannel のメンバには含まれません）
- 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、異なる速度または二重モードで動作するポートをグループ化しません。 バンドルされた状態で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二重モードを変更します。

## 動作の概要

PAgP ポートは、個々の物理ポート（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。 ただし、プロトコル値は 0x0104 です。 次にプロトコル動作の要約を示します。

- 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、安定状態では 30 秒間隔で送信されます。
- PAgP パケットが到達するのを監視します。PAgP パケットは、物理ポートが別の PAgP 対応デバイスに双方向で接続していることを証明します。
- 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受信されない場合、PAgP 状態は解除されます。

## 通常の処理

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から構成された論理ポート。固有の SNMP ifIndex によって識別されます。 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; 従ってそれは非稼動ポートが含まれている可能性がありま

す（agport はチャネルのサブセットです）。 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 agport が 1 つまたは複数の物理ポートに関連付けられるまで、パケットを送受信できません。

- **グループ機能**：物理ポートと agport はそれぞれ、group-capability と呼ばれる設定パラメータを持っています。 ある物理ポートが別の物理ポートと集約できるのは、両方のポートが同じグループ機能を持つ場合に限られます。
- **集約手順**：物理ポートは UpData または UpPAgP ステートになると、適切な agport に関連付けられます。 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。

| State | 意味 |
|---|---|
| UpData | PAgP パケットはまだ受信されていません。 PAgP パケットが送信されます。 この状態の物理ポートは、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 | ちょうど 1 つの PAgP パケットが受信されました。 このことは、厳密に 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ます。受信されることもあります。 |
| UpPAgP | この物理ポートは、おそらく他の物理ポートと集約されて、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達するとき、新しい物理ポートのグループ機能を一致する BiDir か UpPAgPにあり、メンバー 物理ポートがある agport に割り当てられます。（BiDir そのようポートは UpPAgP に同時に変えられます。）どの agport のメンバ物理ポートのパラメータも、新たに使用可能になった物理ポートと互換性がない場合、その物理ポートは、適切なパラメータを持つ、物理ポートが 1 つも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近接デバイスに関して発生します。 タイムアウトしたポートは agport から除去されます。 同じ agport 上のタイマーがすでにタイムアウトしている物理ポートもすべて同時に除去されます。 これにより、agport は、相手側がダウンした場合に物理ポートを 1 つずつではなく一斉に除くことができます。

## 障害時の動作

既存のチャネルのリンクで障害が発生すると（たとえば、ポートのケーブルが抜けた、ギガビット インターフェイス コンバータ（GBIC）が取りはずされた、ファイバが破損したなど）、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され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 ) には損失はありません。 障害が発生したリンクの回復を契機として、agport がもう一度アップデートされて、トラフィックが再びハッシュされます。

**注:** モジュールの電源をオフにした、またはモジュールを取りはずしたことによってチャネルのリンクで障害が発生した場合は、動作が異なる場合があります。 定義上、チャネルが形成されるには 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 は除かれ、元の物理ポートがスパニング ツリーに基づい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できる状態になるまで、トラフィックが廃棄される可能性があることを意味します。

Catalyst 6500/6000 のこのルールへ例外があります。 先のバージョン CatOS 6.3 よりでは、agport はモジュールの削除の間にチャネルがモジュール 1 および 2 のポートでしか構成されない場合中断 されません。

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。 モジュールの活性挿抜 ( ホットスワップ ) を行う場合に STP のトポロジ変更通知を考慮することが必要になる場合があるからです。 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 によってチャネルの物理リンクを個別に管理することが重要です。

Catalyst 6500/6000 で不必要なトポロジ変更が起こるのを軽減するために推奨される対策を次に示します。

- 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 つのモジュールにわたる場合は、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 つのカード上で 2 ポートのチャネルが必要な場合は、スーパーバイザ エンジンのポートのみを使用します。
- CatOS 6.3 にアップグレードします。これにより、チャネルが複数のモジュールに分かれている場合にモジュールを取りはずしても、STP は再計算されなくなります。

## 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説明を示します。

| モード | 設定可能なオプション |
|---|---|
| | PAgP は有効ではありません。 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す。 隣接ポートのモードがON の場合は、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。 ポートは受動的なネゴシエーション状態になり、送信元が desirable モードで動作していることを示す PAgP パケットが少なくとも 1 つ受信されない限り、インターフェイスから PAgP パケットは送信されません。 |

| | |
|---|---|
| | |
| | PAgP プロトコルによって集約が制御されます。 ポートは能動的なネゴシエーション状態になり、PAgP パケットを送信して他の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-silent（Catalyst 5500/5000 のファイバ FE および GE ポートのデフォルト） | auto または desirable モードのキーワード。 インターフェイスでデータ パケットが受信されない場合、インターフェイスは agport に関連付けられず、データ用に使用できません。 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分解される特定の Catalyst 5500/5000 ハードウェアのために提供されています。 non-silent モードが有効なので、リカバリ中の隣接ポートが再びアップ状態になることが許可されず、チャネルが不必要に分解されます。 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用意されています。 |
| Silent（Catalyst 6500/6000 および 4500/4000 のすべてのポートおよび 5500/5000 の銅ポートでのデフォルト） | auto または desirable モードのキーワード。 インターフェイスでデータ パケットが受信されない場合、15 秒のタイムアウトが経過した後、そのインターフェイスは自動的に agport に関連付けられ、データ送信に使用できるようになります。 Silent モードは、PAgP を送信しないアナライザやサーバがパートナーの場合にチャネルを運用することを想定しています。 |

silent/non-silent 設定は、単方向トラフィックを引き起こす状況に対してポートがどのように対応するか、つまりポートが適切なフェールオーバーをどのように実現するかに影響を与えます。 物理サブレイヤ（PHY）の障害や、ファイバやケーブルの破損などが原因でポートが送信できなくなった場合、その隣接ポートはその後も動作状態のままである場合があります。 パートナーはデータを送信し続けますが、リターン トラフィックが受信されないために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 ループが生じるおそれもあります。

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）。 このような機能があればパートナー ポートが非稼働状態に移行し、実質的に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、なおかつ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、受信データが存在し、リンクが双方向であると確認されるまで、ポートが稼働状態にならないようにするために、non-silent モードを使用する必要があります。 PAgP が単方向リンクを検出するために要する時間は、およそ 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。 silent モードのポートは、受信データの有無にかかわらず、強制的に接続されて稼働状態になります。 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、ポートに単方向状態を検出する機能がある場合は、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 モードをまとめたものです。 一部の組み合せでは、STP によってチャネル作成側のポートが errdisable ステートになります（つまり、チャネル作成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 | チャネルの状態 |
|---|---|---|
| | | チャネル（非 PAgP） |
| | | 非チャネル（errdisable） |
| | Auto | 非チャネル（errdisable） |
| | | 非チャネル（errdisable） |
| | | 非チャネル（errdisable） |
| | | |
| | Auto | |
| | | |
| Auto | | 非チャネル（errdisable） |
| Auto | | |
| Auto | Auto | |
| Auto | | PAgP |
| | | 非チャネル（errdisable） |
| | | |
| | Auto | PAgP |
| | | PAgP |

## 推奨事項

Cisco では、on モードを使用せずに、すべてのスイッチ間チャネル接続で PAgP を有効にすることを推奨しています。 最適な方法は、リンクの両端で desirable モードを設定することです。 さらに、silent/non-silent キーワードをデフォルトのまま、つまり Catalyst 6500/6000 および 4500/4000 では silent、Catalyst 5500/5000 のファイバ ポートでは non-silent にしておくことも推奨しています。

このドキュメントで述べたように、他のすべてのポートでチャネリングを明示的にオフに設定しておくと、迅速なデータ転送に役立ちます。 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。これは特に、ポートが STP に引き渡されるのが、その後になるためです。この場合、STP でデータ転送が可能になるまでに 30 秒、場合によっては DTP にさらに 5 秒必要となり、合計で 50 秒かかる可能性があります。 **set port host** コマンドについては、このドキュメントの「STP」セクションに詳しい説明があります。

```
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。これは show channel group コマンドで確認できます。** 必要であれば、管理番号により、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では、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 に設定し、アクセス レイヤ スイッチはデフォルトの auto のままにしておくという設定がよく使用されています。

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。 これには、サーバ、Local Director、コンテント 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 などのデバイスが当てはまります。 次のコマンドを発行します。

```
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、異なるプラットフォームやベンダー間で相互運用できる利点があるため、長期的には PAgP に取って代わると予想されます。

## Link Aggregation Control Protocol ( LACP )

LACP は、同様の特性を持つポートが、隣接している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、Cisco のスイッチおよびライセンスを持つベンダーが提供するスイッチだけで動作する Cisco 独自のプロトコルです。 しかし、IEEE 802.3ad で定義されている LACP を使用すれば、802.3ad 仕様に準拠したデバイスを使用したイーサネットのチャネリングを Cisco の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 サポートが追加されています。

機能的には、LACP と PAgP には、ほとんど違いがありません。 両方のプロトコルとも、チャネルごとに最大 8 ポートまでをサポートし、バンドルが形成される前に、同じポート プロパティかどうか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。

- Speed
- 二重モード
- 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 は全二重ポートだけで実行でき、半二重ポートはサポートされていない。
- LACP では、ホットスタンバイ ポートがサポートされる。 LACP では、ハードウェアが許容する最大数（8 ポート）まで、互換性のあるポートをできるだけ多く、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は、チャネルにアクティブに含めることができないすべてのポートが hot standby 状態になり、使用中のポートのいずれかに障害が発生したときだけに使用されます。 互換性のあるすべてのポートを LACP で集約できない場合の例としては、リモート側の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、同じ管理鍵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、ハードウェアが許容する最大数（8 ポート）まで、互換性のあるポートをできるだけ多く、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 MAC アドレス **01-80-c2-00-00-02** を使用して送信されます。 タイプまたはフィールドの値は 0x8809 で、サブタイプは 0x01 です。 次にプロトコル オペレーションの要約を示します。

- 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る。 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、安定状態では 30 秒間隔で送信される。
- 「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、どのアクションを実行するかを決定する。
- ハードウェアが許容する最大数（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る。
- 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、集約が維持される。 リンク障害などの原因で、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（LACPDU）の転送に加えて、状態情報に変更があれば、イベント駆動の LACPDU がパートナーに送信される。 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どうか、および集約の観点から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、次のパラメータを確立できることが必要になります。

- リンクの集約に参加する各システム用のグローバルに一意な IDLACP 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。 デフォルトシステム 優先順位は 32768 です。 このシステム プライオリティは主にシステムの MAC アドレスと組み合せてシステム ID を作成するために使用されます。
- 特定のシステムが把握している、ポートごと、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りプライオリティを割り当てる必要があります。 デフォルトは 128 です。 このプライオリティはポート番号

と組み合せてポート ID を作成するために使用されます。
- リンク集約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 ビットの整数に要約されています。このパラメータは「鍵」と呼ばれています。 各鍵は、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 レートデュプレックス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限各ポートには、次の 2 つの鍵が関連付けられています。管理鍵：この鍵では、管理者が鍵値を操作できます。 ユーザはこの鍵を選択できます。動作鍵：この鍵は、システムが集約を形成するために使用します。 ユーザはこの鍵を選択することも、直接変更することもできません。同じ動作鍵値を共有するシステム内の一連のポートを、同じ鍵グループのメンバと呼びます。

2 つのシステムがあり、同じ管理鍵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を集約しようとします。 それぞれのシステムが、最もプライオリティの高いシステムで最も高いプライオリティが設定されたポートから集約を開始します。 それぞれのシステムが自分とパートナーのプライオリティを把握しているので、この動作が可能になります。自分のプライオリティはユーザかシステムによって割り当てられ、パートナーのプライオリティは LACP パケットから取得されています。

## 障害時の動作

LACP の障害時の動作は、PAgP の動作と同じです。 既存の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する場合があります。

- ポートが抜かれた
- GBIC が外された
- ファイバが破損した
- 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され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）には損失はありません。 障害が発生したリンクの回復を契機として、agport がもう一度アップデートされて、トラフィックが再びハッシュされます。

## 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。これを次の表に要約します。

| 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、リンクの集約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。 隣接ポートのモードがON の場合は、チャネルが形成されます。 |
| | 隣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。 |
| | これは、PAgP における 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（「active」状態）は、LACP パケットを送出してネゴシ |

| | |
|---|---|
| | エーションを開始します。 スイッチはパケットを受信して応答し、最終的にはピアと集約チャネルを形成します。 |
| Active | このモードは、PAgP の desirable モードに似ています。 aglink を形成するために、スイッチはネゴシエーションを開始します。 相手側で LACP が active モードまたは passive モードで動作している場合は、リンク集約が形成されます。 |

## 検証 ( LACP と LACP )

このセクションの表は、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 モードをまとめたものです。 一部の組み合せでは、STP によってチャネル作成側のポートが errdisable ステートになります。 つまり、一部の組み合せでは、チャネル作成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 |
|---|---|---|---|
| | | チャネル ( 非 LACP ) | チャネル ( 非 LACP ) |
| | | 非チャネル ( errdisable ) | |
| | パッシブ | 非チャネル ( errdisable ) | |
| | Active | 非チャネル ( errdisable ) | |
| | | | |
| | パッシブ | | |
| | Active | | |
| パッシブ | パッシブ | | |
| パッシブ | Active | LACP | LACP |
| Active | Active | LACP | LACP |

## 検証 ( LACP と PAgP )

このセクションの表は、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 のチャネリング モードをまとめたものです。 一部の組み合せでは、STP によってチャネル作成側のポートが errdisable ステートになります。 つまり、一部の組み合せでは、チャネル作成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 |
|---|---|---|---|
| | | チャネル（非 LACP） | チャネル（非 PAgP） |
| | | 非チャネル（errdisable） | |
| | Auto | 非チャネル（errdisable） | |
| | | 非チャネル（errdisable） | |
| | | | 非チャネル（errdisable） |
| | | | |
| | Auto | | |
| | | | |
| パッシブ | | | 非チャネル（errdisable） |
| パッシブ | | | |
| パッシブ | Auto | | |
| パッシブ | | | |
| Active | | | 非チャネル（errdisable） |
| Active | | | |
| Active | Auto | | |
| Active | | | |

## 推奨事項

Cisco では、Cisco 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 を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、両側のデバイスに LACP active を設定して LACP をアクティブにします。 どちらかの側のデバイスが LACP か 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ます。そのため、LACP は実行しないでください。 LACP がポートで使用されるように設定するには、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 が稼働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**（管理鍵）パラメータは、LACP パケットで交換されます。 チャネルが形成され

るのは、同じ admin key が設定されたポート間だけです。 set port lacp-channel port_range admin-key コマンドで、チャネルに admin key 番号を割り当てることができます。 show lacp-channel group コマンドでは、その番号を表示できます。 set port lacp-channel port_range admin-key コマンドで、ポート範囲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。 特定の鍵を設定しないと、admin key がランダムに割り当てられます。 その場合は、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 に変更できます。

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）が利用されます。 長いタイムアウト（3 x Slow_Periodic_Time）の使用の受け取られた LACPDU 情報の無効化の前の秒数は 90 です。 単方向リンクをより迅速に検出する方法としては、UDLD を使用することを推奨します。 LACP タイマーを調整することはできません。現在のところ、速い PDU の送信（1 秒ごと）を使用して、チャネル生成後のチャネルを維持するようにスイッチを設定することもできません。

### 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 にする設定がよく使用されています。 アクセス レイヤのスイッチはデフォルトの passive 設定のままにしておきます。

## 単方向リンク検出

UDLD は Cisco 固有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。 次のような場合に、そのようなシナリオになる可能性があります。

- STP の予期しない動作
- パケットの不正なフラッディングや過度のフラッディング
- トラフィックのブラック ホール化

UDLD 機能は、ファイバおよび銅線イーサネット インターフェイスで次のような障害状況に対処することを目的としています。

- 物理的なケーブル構成を監視し、配線が誤っているポートを errdisable としてシャットダウンする。
- 単方向リンクから保護する。 メディアまたはポート/インターフェイスの動作不良を原因とする単方向リンクが検出されると、対象のポートが 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、以前に双方向とみなされたリンクが、輻輳時に接続を失って使用不可にならないようにチェックされます。 UDLD では、リンク全体に対して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、特定の障害状態でトラフィックのブラック ホール化を回避することです。

定常的な単方向 BPDU フローを持つスパニング ツリーにとって、これらの障害は切実な問題でした。 あるポートがどのようにして突然 BPDU を送信できなくなるかを調べるのは簡単です。このような状況になると、隣接ポートの STP 状態が blocking から forwarding に変わります。 そ

のポートでの受信はまだ可能であるため、この変化により、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せて使用すると、リンクの物理的（L1）および論理的（L2）な完全性を検証できます。

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ュ、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/ポートの動作不良や障害の検出を行えます。

UDLD は 2 つの基本的なメカニズムを用います; それは相手について新しいネイバーを検出するか、またはネイバーがキャッシュの再同期化を要求する時はいつでも学び、ローカル キャッシュで情報を最新の状態に保ち、UDLD プローブ/エコー（HELLO）メッセージのトレインを送信 します。

UDLD は、UDLD が有効な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、検出フェーズおよび検証プロセスが開始されます。 このプロセスの最後にすべての有効な条件が満たされると、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、正しく配線されていることが必要です。そうでない場合は、ポートが 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:  [dec]/[dec] [[] DEC]/[DEC]`

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、『メッセージと回復手順』（Catalyst シリーズ スイッチ、7.6）を参照してください。

いったんリンクが確立し、双方向と見なされると、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 リンク状態を示しています。

| **ポート状態** | **備考** |
|---|---|
| 不定 | 検出中、またはネイバーの UDLD が無効になっているかその送信がブロックされた。 |
| 該当なし | UDLD が無効になっている。 |
| shutdown | 単方向リンクが検出され、ポートが無効になっている。 |
| Bidirectional | 双方向リンクが検出された。 |

- **ネイバー キャッシュのメンテナンス**：UDLD は、UDLD ネイバー キャッシュの完全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、同期がとれていないネイバーから再同期要求を受ける場合はいつでも、自分側の接続で検出ウィンドウを開始または開始し直し、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の間で同じであるため、エコー送信側デバイスは応答としてエコーバックが受信されることを期待します。検出ウィンドウが終了しても有効な応答メッセージがまったく受信されない場合、そのリンクは単方向と見なされ、リンク再確立またはポート シャットダウン プロセスが開始されます。

## 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 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、ブロッキング ポートがフォワーディング ステートに移行しないうちに単方向リンクをシャットダウンすることを目的としています。

**注:** 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頻度は、メッセージ インターバルの値によって決まります。 可能な場合は設定に一貫性があることが望ましいですが、リンクの両端でメッセージ インターバル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、設定されたインターバルが送信され、そのピアのタイムアウト インターバルが（3 × メッセージ インターバル）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関係がタイムアウトします。 それぞれの側のメッセージ インターバルが異なると、このタイムアウト値もそれぞれの側で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要するおおよその時間は（2.5 × メッセージ インターバル + 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とされる 50 秒よりも十分短い時間です。 NMP の CPU サイクルにいくらかの余力があり、その使用レベルを注意深く監視している場合は、メッセージ インターバルを最小で 7 秒にまで短縮できます。 このようにメッセージ インターバルを設定すると、検出を大幅にスピードアップするのに役立ちます。

このように 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する特性があるので、RSTP を実装する際にも代替メカニズムを検討します。 これらの場合には、UDLD とループ ガードを組み合せて使用して、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 バージョンの速度に合せて STP ループが防止され、UDLD では、個々の EtherChannel リンクで単方向接続が検出されるか、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 はすべての STP 障害状態を検出するわけではありません。たとえば、CPU が（2 * FwdDelay + Maxage）時間経過しても BPDU を送信しないことによって生じる障害は検出されません。 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：** UDLD の以前のリリースの設定不可能な 60 秒デフォルトメッセージインターバルを使用する用心して下さい。 これらのリリースでは、スパニング ツリー 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）場合に特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 モードの機能では、次のような危険な単方向リンク状態に対して、さらに手厚い保護を実現しています。

- UDLD の PDU の喪失が対称的で、両側がタイムアウトした場合は、どちらのポートも errdisable されない。
- リンクの一方でポート スタック（送信 [Tx] と Rx の両方）が生じている。
- リンクの一方が down になったのに、もう一方が up のままである。
- 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。
- L1 FEFI メカニズムへの依存度を下げることが望ましい。
- 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である。 具体的には、2 つのネイバー間の障害が許容できない場合、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。ハードビートが存在すれば、リンクが健全であることが保証されます。

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か使用できない場合に、バンドルのメンバに対して接続チェックを実行する場合です。 PAgP や LACP が有効になっていても、安定状態で使用される hello タイマーの値はあまり小さくないので、この機能は EtherChannel 接続の場合に特に有効です。 この場合、アグレッシブ UDLD には、スパニング ツリー ループが発生した場合にも保護できるという利点もあります。

UDLD プローブ パケットの対称的な喪失に至るような状況を特徴付けるのはさらに困難です。 通常の UDLD で、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ていることを理解しておく必要があります。 UDLD の目的は、STP ループを発生させる L2 問題を検出することです。安定状態では BPDU が 1 方向にだけ流れるので、通常これら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、ほとんどの場合は十分です。 しかし、両方向に輻輳が等しく影響するために、両方向で UDLD プローブの喪失が発生するような場合には、UDLD アグレッシブ モードに利点があります。 たとえば、リンクの両端の CPU 使用率が上がると、このような UDLD プローブの喪失が発生する可能性があります。 次のデバイスのいずれかに障害が発生した場合にも、両方向の接続性が失われます。

- Dense Wavelength Division Multiplexing（DWDM; 高密度波長分割多重方式）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:** この障害は自動ネゴシエーションでは検出できません。

アグレッシブ UDLD では、これらの障害状態のポートがエラー 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 パケットの転送が妨げられて、リンクが不必要にシャットダウンされる可能性があります。

ポートのすべてのネイバーがエイジング 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どちらかで実行されます。 早急な一連のメッセージ（8 回リトライに失敗した）後、リンクが引き続き「

undetermined」と見なされる場合は、ポートが errdisable 状態になります。

**注:** 一部のスイッチでは、アグレッシブ UDLD 機能を使用できません。 現在のところ、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、潜在的な STP ループから（デフォルトの STP パラメータを使用して）保護するのに十分な速さではないと考えられます。

## ルーテッド リンク上の UDLD

この説明では、ルーテッド リンクは次の接続タイプのどちらかであるとします。

- 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だけがサポートされている VLANたとえば、分割された L2 コア トポロジはその一例です。

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。 このセクションで説明するこの特性は、より広範に現在使用されている Open Shortest Path First（OSPF）プロトコルと 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重要になります。

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 接続がほとんど即座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 状態に移行するので、MSFC の自動状態機能によって、L2 と L3 のポート状態が約 2 秒以内に同期化されます。 この同期化によって、L3 VLAN インターフェイスが up/down 状態（回線プロトコルが「down」）になります。

デフォルト タイマー値が使用されていると仮定します。 OSPF が hello メッセージを 10 秒ごとに送信し、40 秒（4 * hello）のデッド インターバルが経過します。 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 ネットワークで一貫しています。 隣接関係を形成するために OSPF には双方向の通信が必要なので、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 デッド タイマーの期限切れ（約 40 秒）とよく似ているので、OSPF の L3 ポイントツーポイント リンクで UDLD の通常モードを設定しても限られた利点しかありません。

多くの場合、EIGRP の方が OSPF よりも速く収束します。 ただし、双方向通信できなくても、ルーティング情報をネイバーが交換できることに注意する必要があります。 中途半端に動作する障害の非常に特殊なシナリオでは、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続く、トラフィックのブラック ホール化に対する脆弱性が EIGRP に存在しすま。 UDLD の通常モードでは、このセクションで説明されている状況を緩和できます。 UDLD の通常モードでは、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 の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ハードウェアの故障などがあります。 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:** 最小タイマーが必要になる場合があります。
- フラッピングが発生しているリンクを errdisable 状態にする

- 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、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、銅ポートではデフォルトで無効になっています。 銅ポートは、ホスト アクセスによく使用されます。

**注:** UDLD は、ネイバーが双方向状態を確立する前にインターフェイス レベルでグローバルに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 秒の間に設定できます。

Errdisable 回復は、デフォルトでグローバルに無効になっています。 グローバルに有効にした後に、ポートが errdisable 状態になったら、選択したインターバル時間の経過後に自動的に再び有効になります。 デフォルトの時間は 300 秒です。この設定は、グローバル タイマーなので、スイッチにある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 に設定すれば、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:** このコマンドを使用できるかどうかは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 タイムアウト機能を使用することを検討します。errdisable 状態が発生するとネットワークから孤立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 状態のポートに対するタイムアウト期間の設定方法についての詳細は、『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』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 で十分です。 そのような機能やプロトコルには、次のようなものがあります。

- FEFI
- 自動ネゴシエーション
- ループ ガード

UDLD を配備するときには、双方向の接続性の継続的なテスト ( 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な場合は、L1 の障害検出は自動ネゴシエーションで補われるので、アグレッシブ モードは必要ありません。

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 Cisco 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、通常モードの UDLD 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 タイマーが想定されています。 さらに、冗長化と収束を 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 blocking 状態のポートが 1 つ以上存在するネットワークに適用されます。

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のためにエラー ディセーブル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、サポートされている場合は、もっと速く収束するように、それぞれの側の UDLD メッセージ インターバルの値を 7 ~ 90 秒の間で次のように調整できます。

```
set udld interval time
```

errdisable 状態になるとネットワークから孤立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。 アクセス レイヤの場合や、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は、通常そのような検討が必要になります。

ポートが errdisable 状態になった場合、デフォルトでは、そのポートはダウンしたままになります。 次のコマンドを発行すれば、タイムアウト間隔が経過した後、ポートが再び有効になります。

**注:** デフォルトでは、タイムアウト間隔は 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。 次のコマンドを発行します。

```
set udld disable port_range
```

## UDLD のテストと監視

不良 GBIC などの実際に故障しているコンポーネント、または単方向のコンポーネントを使用せずにラボで 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たものです。 たとえば、errdisable 状態を発生させるためにファイバの一方をコネクタから抜く簡単なテストを実行する場合は、L1 の自動ネゴシエーションをオフにする必要があります。 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 の通常モードでは、リモート エンドが undetermined 状態になります。 UDLD のアグレッシブ モードを使用している場合は、リモート エンドが errdisable 状態になります。

UDLD での隣接 PDU の喪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 フィルタを使用することにより、UDLD や CDP のハードウェア アドレスはブロックしながら、他のアドレスは通過させる方法です。

UDLD を監視するためには、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
```

**また、enable モードからも、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 ) チェックできます。** **多くの場合、**UDLD キャッシュを CDP キャッシュと比較して、プロトコル固有の異常がないかどうかを確認するのが便利な方法です。 CDP にも影響がある場合は、通常すべての PDU や BPDU にも影響があります。 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 の変更やルート ポートや指定ポートの配置変更がないかをチェックします。

```
>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 の UDLD SNMP MIB 変数を使用して監視できます。

## 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 Maximum Transmission Unit ( MTU; 最大伝送ユニット ) フレーム サイズは 1518 バイトです。 ジャンボ フレーム機能では、標準のイーサネット 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 Multi-Protocol Label Switching ( MPLS; マルチプロトコル ラベル スイッチング )、802.1Q トンネリング、および L2 Tunneling Protocol Version 3 ( L2TPv3; レイヤ 2 トンネリング プロトコル バージョン 3 ) 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 標準の仕様では、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 1522 バイトの最大イーサネット フレーム サイズが定義されています。 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 バイトを超える場合がある理由はさまざまです。 そのいくつかを例で示します。

- 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 サイズを指定できる。 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場合があるということを証明する研究結果があるために、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る。 現在、最も広く使用されている形態のトランキングは Cisco 独自の ISL カプセル化と IEEE 802.1Q です。
- MPLS： MPLS は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を増加する可能性があります。 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 バイト増える可能性があります。 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。

さまざまな Catalyst スイッチで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左右されます。 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。 ジャンボ フレーム機能がポートで有効になっていると、MTU サイズが 9216 バイトに増加します。 10/100 Mbps の Unshielded Twisted Pair（UTP; シールドなしツイストペア線）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 サイズ機能の有効化に制限はありません。 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、この機能を使用できます。
- 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ません。 ただし、802.1Q トランキングの場合は例外です。
- 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よって異なります。 一般的には、ジャンボ フレーム サイズ機能の有効化に制限はありません。 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、この機能を使用できます。 個々のポートでジャンボ フレームのサポートがイネーブルになった後のデフォルトの MTU サイズは 9216 バイトになります。 デフォルトの MTU を CatOS を使用して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 には、デフォルトの MTU を上書きする system jumbomtu コマンドが追加されています。**

詳細は、『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』を参照してください。

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 サイズを次の表に示します。

**注:** MTU サイズまたはパケットサイズは、イーサネット ペイロードだけを指しています。

| 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）9216 バイト（@ 10 Mbps） |
| 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）9216 バイト（@ 10 または 1000 Mbps） |
| 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）<br>7673 バイト（T1/E1） |
| Flex WAN | 7673 バイト（CT3 T1/DS0）<br>9216 バイト（OC3c POS）<br>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

CatOS によって MSFC で動作する Supervisor Engine および Cisco IOSソフトウェアで実行する、Catalyst 6500/6000 スイッチはまた PFC/MSFC2 の使用を Cisco IOS® ソフトウェアリリース 12.1(2)E およびそれ以降の L3 ジャンボフレームサポートに、PFC2/MSFC2、またはそれ以降 ハードウェア与えます。 入力と出力の VLAN の両方がジャンボ フレーム用に設定されている場合は、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も、出力の VLAN が設定されていない場合は、次の 2 つのシナリオがあります。

- 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）unreachable 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：バケットが 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。

さまざまなプラットフォームでの L3 ジャンボ サポートの要約を次の表に示します。

| L3 スイッチまたはモジ | 最大 L3 MTU サイズ |
|---|---|

| ユール | |
|---|---|
| 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 RSM1/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 = Route Switch Module

2 RSFC = Route Switch Feature Card

## 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範な研究が行われてきました。 次の公式は、次の要因で TCP のスループットが頭打ちになることを示しています。

- Maximum Segment Size（MSS; 最大セグメント サイズ）。これは MTU 長から TCP/IP ヘッダーの長さを引いた値です。
- Round Trip Time（RTT; ラウンドトリップ タイム）
- パケット損失

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

この数式に従って、達成可能の最大 TCP スループットは MSS に正比例しています。 一定した RTT およびパケットロスを使うと、二重パケットサイズ TCP スループットを倍増できます。 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。

2 番目の点として、サーバ ファームのパフォーマンス要求は増大し続けているので、Network File System（NFS）の UDP データグラムをより高速に処理できる、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保存メカニズムで、8400 バイトのデータグラムが使用されています。 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 ヘッダーなど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。 ソフトウェアは、別々の UDP データグラムに NFS ブロックを断片化する必要がないため、この機能に付随して、より効率的な Direct Memory Access（DMA; ダイレクト メモリ アクセス）転送がホスト上で可能になります。

## 推奨事項

ジャンボ フレーム サポートが必要な場合は、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だけに、ジャンボ フレームの使用を制限します。 このように設定すれば、パスのどこでも断片化を防止できます。 パスでサポートされるフレーム長より大きなジャンボ フレームを設定すると、断片化が必要になるので、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」セクションの表に示すように、サポートされている最大パケット サイズは、プラットフォームやラインカードによっ

て異なります。

ジャンボ フレーム対応のホストデバイスには、ホストデバイスがある L2 VLAN 全体のネットワーク ハードウェアで共通にサポートされている値のうち最小の値を MTU サイズとして指定します。 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 に使用可能な 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 が、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た値以下に必ずなります。 このようにすれば、VLAN から L3 インターフェイスを超えてトラフィックがルーティングされる際の断片化が防止されます。

# 管理設定

このセクションでは、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事項について説明しています。

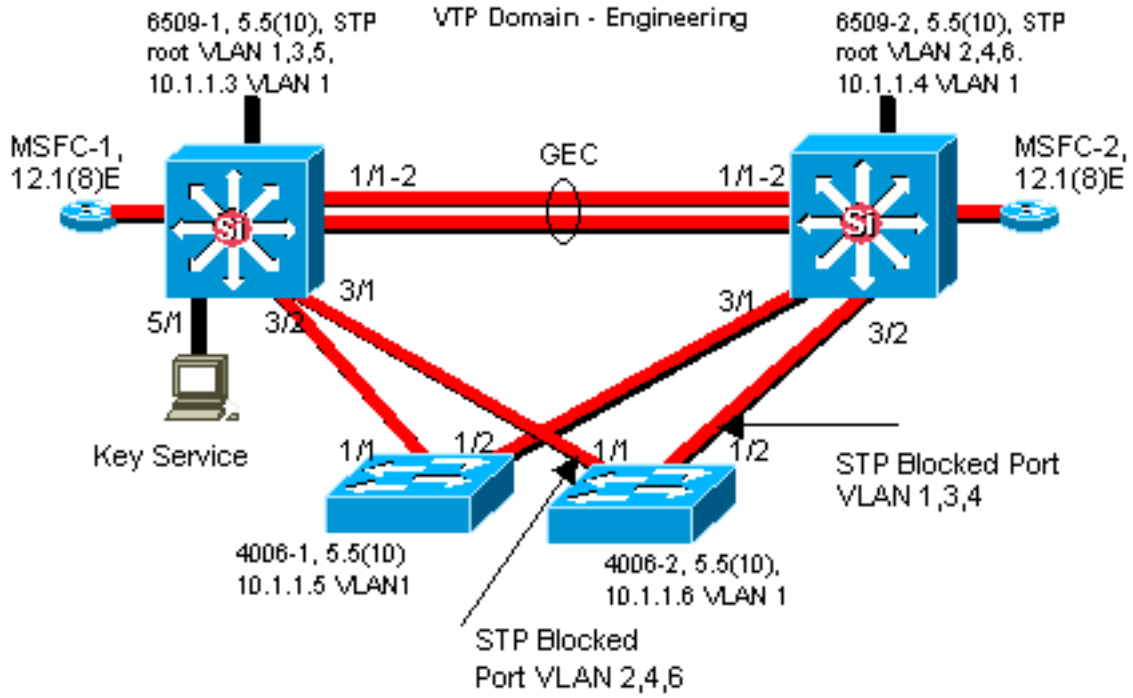
## ネットワーク構成図

明確なネットワーク図はネットワーク運用の基本的な要素です。 ネットワーク ダイアグラムはトラブルシューティングの際に重要となり、ネットワークが停止したときに情報をベンダーやパートナーにまで伝えるための、唯一最重要の手段となります。 ネットワーク ダイアグラム作成し、いつでも参照できるように準備しておく必要があります。

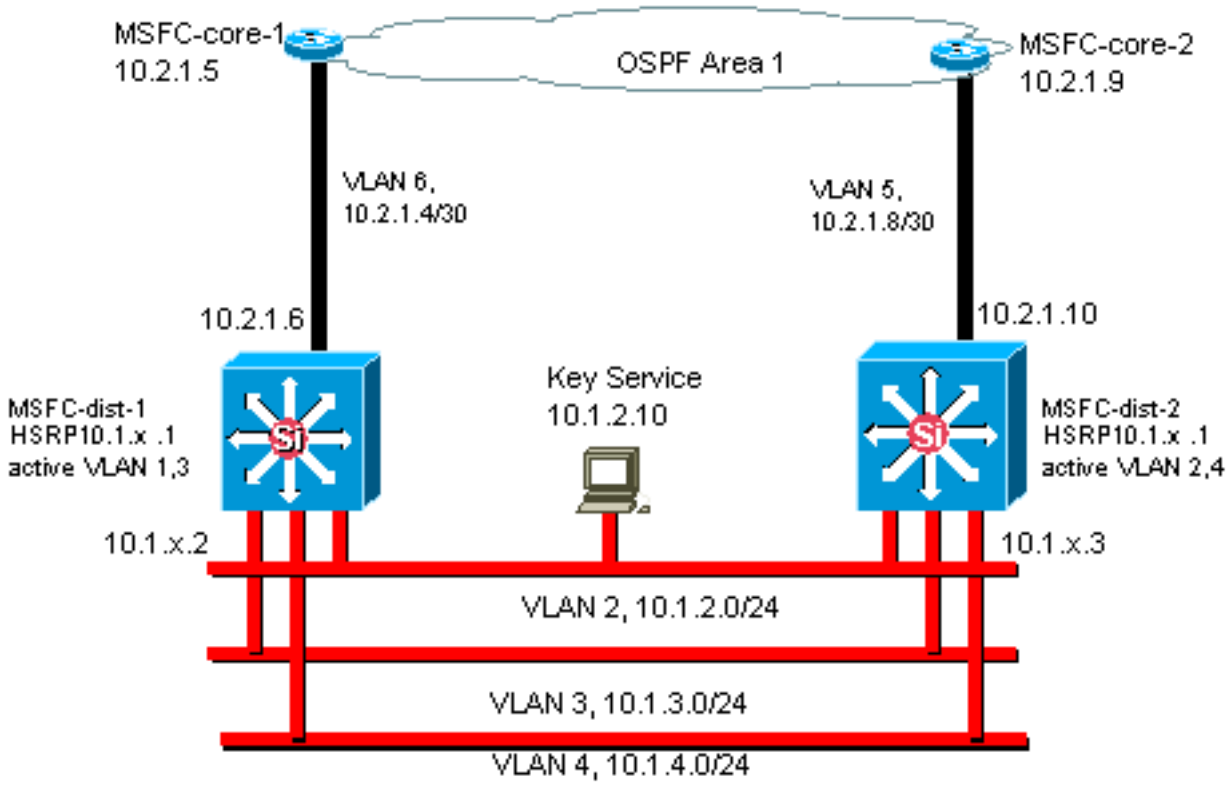
### 推奨事項

Cisco では、次の 3 つのダイアグラムの作成を推奨しています。

- **全体図**：どれだけ規模の大きいネットワークでも、エンドツーエンドの物理接続と論理接続を示すダイアグラムが重要です。 階層的な設計を実装している企業では、各レイヤを別々に文書化するのが普通です。 ただし、計画時や問題解決時には通常、ドメインがどのようにリンクしているか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 ごとのブロッキング 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を、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、より明快になります。




- **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 と呼ばれる）で次のデータを処理することが必要になる場合があります。

- SNMP、Telnet、Secure Shell（SSH; セキュア シェル）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

Cisco のマルチレイヤ設計では、スイッチ 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。 このセクションでは、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 データ用に VLAN 1 を使用する場合に最も懸念されるのは、スーパーバイザ エンジン NMP は一般的に、エンドステーションによって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取り扱うにはリソースが不足しています ( もっとも、この原理はすべてのスーパーバイザ エンジンに当てはまります )。 バックプレーンへのスーパバイザエンジンCPU、バッファ、または帯域内チャンネルが十分に不要なトラフィックを占められた受信なら、制御フレームが抜けている場合があることは可能性のあるです。 最悪のシナリオでは、これはスパニングツリーループかイーサチャネル障害の原因となる可能性があります。

**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 トラフィックの比率、および非 IP トラフィックと IP トラフィックの比率が示されます ( 管理 VLAN では通常は見られません )。**

より古い Catalyst 5500/5000 ハードウェアのためのそれ以上の健康診断は **show inband** の出力を検査することです / リソースエラー ( RscrcErrors 同じような ) のための *BIGA* ( 隠しコマンド )、ルータのバッファドロップと。 これらのリソース エラーが増え続けている場合は、おそらく管理 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 回のリソース エラーは、スーパーバイザ エンジンが BPDU などのパケットを処理できないことを意味します。スパニング ツリーなどのプロトコルでは BPDU が失われても再送されないため、これは即座に問題になる可能性があります。

## 推奨事項

この資料の Cat 制御セクションで強調表示されるように、VLAN 1 はコントロール プレーン トラフィックのほとんどをタグ付けし、処理する特定のVLAN です。 VLAN 1 は、すべてのトランクにおいて、デフォルトでイネーブルになっています。 より大きいキャンパスネットワークによって、注意は VLAN 1 **STP ドメイン**の直径について奪取 される必要があります; 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るようになっています。

```
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、このリンク上で STP も実行されません。 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、それに応じた狭い障害/L3 境界にユーザ VLAN を制限するように配慮されていたとしても、一部のお客様では、管理 VLAN を、これとは違ったように扱い、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されています。 中央の NMS アプリケーションが管理対象のデバイスと L2 で隣接しなければならないという技術的な理由はなく、またこれはセキュリティ上認められた理論でもありません。 Cisco では、管理 VLAN の直径をユーザ VLAN と同じルーティング 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強化する手段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、Cisco の提案するこれらの推奨事項について設計上注意が必要な点があります。 たとえば、理想的で一般的な Cisco 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ることです。 これには、各 IP サブネット/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制限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。

異なる管理 VLAN を作成し、トランキングを有効にして、L2 アクセス レイヤと L3 ディストリビューション レイヤの間で管理 VLAN を伝送するかどうかという問題は、簡単には答えが出ません。 Cisco 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：** 用途の決まった 2 ~ 3 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。 これはデータVLAN、voice VLAN およびマネージメントVLAN を STP が非アクティブであること、たとえば、およびまだ持っています利点を可能にします。 VLAN 1 がトランクからクリアされる場合（ことに注目して下さい、特別なコンフィギュレーション ステップがあります。）このソリューションでは、また障害復旧の間にルーテッドトラフィックの一時的なブラックホール化を避けるために考慮するべき設計ポイントがあります: トランク（CatOS 7.x およびそれ以降）のための STP PortFast または STP転送（CatOS 5.5[9] より以降）の VLAN Autostate 同期。
- **オプション 2：** データ用と管理用に 1 つの VLAN を共有することを容認する。 最近では高速な CPU やコントロールプレーンのレート制限機構などのスイッチ ハードウェアが登場しており、さらにブロードキャスト ドメインが比較的小さくなるような設計がマルチレイヤ設計によって提唱されているため、sc0 インターフェイスをユーザ データから切り離すことは以前ほど大きな問題ではないと考えているお客様が増えています。 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 Cisco のエンジニアと議論した上で判断するのがおそらく最もよいでしょう。 管理 VLAN が実際にそのアクセスレイヤ スイッチ上のすべてのユーザを含む場合は、スイッチをユーザから保護するために、このドキュメントの「セキュリティ設定」セクションで説明されているように、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

前のセクションの議論を一歩進めると、トラフィックが原因でどのようなイベントが起こっても、あるいはコントロールプレーンでどのようなイベントが起こっても、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アベイラビリティを大幅に向上させることができます。 これには、次の 2 つの方法が一般的です。

- 専用の 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

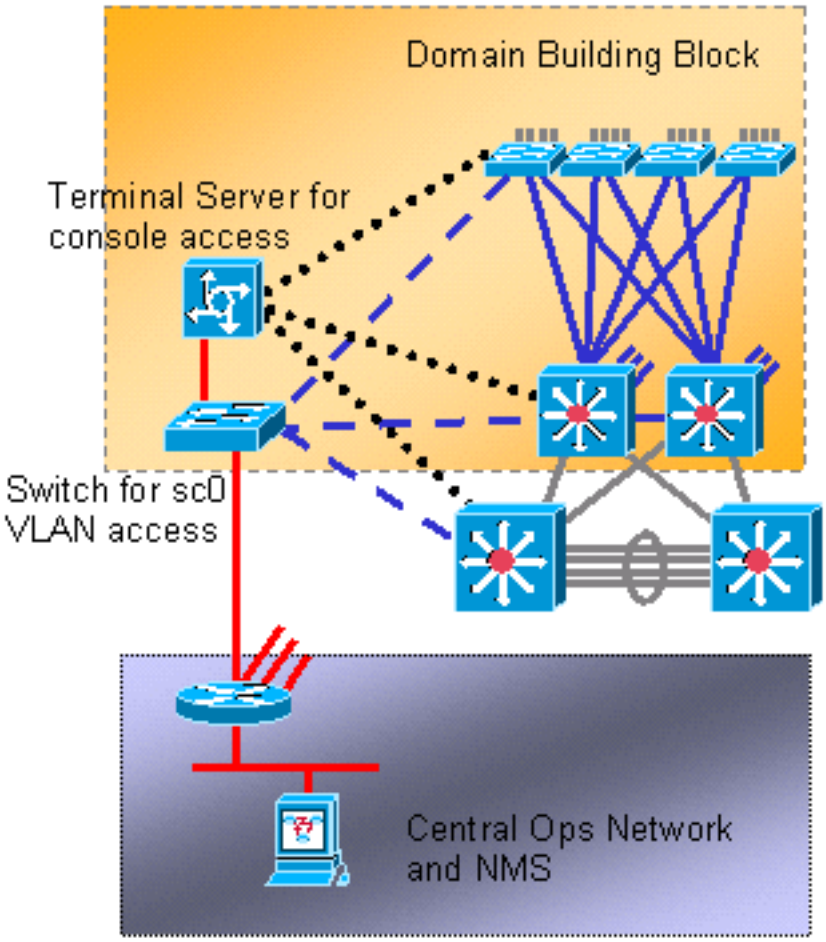
ネットワーク内のルータおよびスイッチはすべて、管理 VLAN 上にアウトオブバンド イーサネット管理インターフェイスを装備できます。 デバイスごとに 1 つのイーサネット ポートを管理 VLAN に設定し、そのポートを実稼働ネットワークの外部にある別のスイッチ管理ネットワークに sc0 インターフェイスを通じてケーブル接続します。 Catalyst 4500/4000 スイッチにはスーパーバイザ エンジン上に特別な me1 インターフェイスがあります。このインターフェイスはスイッチ ポートとしてではなく、アウトオブバンド管理のみに使用されます。

また、Cisco 2600 または 3600 から RJ-45-to-serial 変換ケーブルを介してレイアウト内のすべてのルータおよび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、すべてのデバイスの補助ポートにモデムを接続するなどのバックアップ シナリオを構築する必要もなくなります。 ターミナル サーバの補助ポートにモデムを 1 台接続すれば、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、すべてのスイッチおよびルータへと通じる 2 本のアウトオブバンド パスが使用できるため、ネットワーク管理のアベイラビリティが向上します。 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 データから切り離される。
- 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送できる。
- 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中には、正常に動作可能で信頼できるプラットフォームが利用できることを保証するために、多数のプロセスが実行されます。これにより、不良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、Power-On Self-Test ( POST; 電源投入時セルフテスト ) とオンライン診断に分かれます。

### 動作の概要

ブートアップ時、およびカードをシャーシにホットスワップしたときには、プラットフォームおよびハードウェアの設定に応じて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 サイクルが完了するまでに時間がかかります。 POST 診断では次の 3 つのレベルを選択できます ( どのテストでも、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 以前を使用した 4500/4000 シリーズでは使用できない。 |
| 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 | 30 | 5500/5000 および |

| | | | |
|---|---|---|---|
| | 行される。 | | 6500/6000 シリーズのデフォルト; 4500/4000 シリーズで使用不可能。 |
| 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る。 | 60 | 4500/4000 シリーズのデフォルト。 |

## オンライン診断

これらのテストはスイッチ内部でのパケット パスをチェックします。 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する必要があります。 Catalyst 5500/5000 および 6500/6000 スイッチでは、最初にスタンバイ スーパーバイザ エンジンからテストが実行され、次にプライマリ スーパーバイザ エンジンから同じテストが繰り返されます。 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：スーパーバイザ エンジン NMP から各ポートにパケットが送信され、NMP に戻ってきたところでエラーがないかどうかを調べます。
- 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。

完全オンライン診断は、完了までに約 2 分かかります。 最小診断はスーパーバイザ エンジン以外のモジュールでバンドル テストまたはリライト テストを実行せず、完了までに約 90 秒かかります。

メモリ テスト中に書き込まれたパターンと読み出されたパターンに違いが見つかった場合は、ポートの状態が faulty に変更されます。 これらのテスト結果を確認するには、対象のモジュール番号を指定して **show test** コマンドを発行します。

```
>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

Cisco では、障害を最大限検出し、通常運用時にネットワークの停止が発生しないようにするため、すべてのスイッチで完全診断を実行することを推奨しています。

**注:** この変更は、次にデバイスをブートするまで有効にはなりません。 完全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、完全な診断が実行されるまで待つよりも短時間でブートアップする方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 スーパーバイザ エンジン、9 スロット シャーシがフル構成されている Catalyst 6509 で完全にブートするまでの時間を調べてみると、完全診断で約 380 秒、最小診断で約 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 では最小診断の設定は可能ですが、このように設定しても実際には完全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

システムが稼働状態になると、スイッチのスーパーバイザ エンジンでは他のモジュールに対してさまざまな監視を実行します。 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; シリアル制御プロトコル））によってモジュールに到達できない場合、スーパーバイザ エンジンはそのカードの再起動を試みるか、または状況に応じた適切な措置を実行します。

### 動作の概要

Supervisor Engine は自動的にさまざまなモニタリングを遂行します; これには設定はいっさい必要ありません。 Catalyst 5500/5000 および 6500/6000 では、スイッチの次のコンポーネントが監視されます。

- NMP（ウォッチドッグによる監視）
- Enhanced EARL チップのエラー
- スーパーバイザ エンジン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による監視、Catalyst 6500/6000）
- アクティブ スーパーバイザ エンジン（スタンバイ スーパーバイザ エンジンによるステータスの監視、Catalyst 6500/6000）

## システムと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監視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

この機能が有効なときにエラー状態が検出されると、スイッチで syslog メッセージが生成されます。 目立ったパフォーマンスの劣化が発生する前に、問題があることがこのメッセージで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 に変更されます。

## インバンド

インバンド エラーが検出されると、目立ったパフォーマンスの劣化が発生する前に、問題があることが syslog メッセージで通知されます。 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。 次のような例が挙げられます。

- 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 の障害が検出されると、インバンド接続の現在の Tx と Rx のレート、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 ) かを正しく判断できます。 この追加情報は、インバンドの 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起動されます。 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監視します。 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、この機能の対象となるカウンタが決まります。 この情報は、Cisco 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ティングするために使用します。 この機能では、FCS、CRC、アラインメント、ラントなど、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。 この機能を組み込むには、このドキュメントの「EtherChannel やリンク エラーの処理」セクション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 2 回の連続したポーリングでカウンタの値が上昇している場合は、その事象が 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監視が実行されて、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

- Bad alignment

### 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、メモリなどの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予防的な警告診断が 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すべてを有効にするには、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 とリンク 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的にフェールオーバーする新機能が追加されています。 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エラーしきい値を超えた場合に、このポートのフェールオーバーが発生します。このエラーしきい値は設定変更が可能です。 ポートがフェールオーバーするのは、EtherChannel に動作可能なポートが残っている場合だけです。 障害が発生したポートが EtherChannel にある最後のポートの場合、ポートは port-failover 状態にはなりません。 受信したエラーのタイプにかかわらず、このポートはトラフィックを通過させ続けます。 チャネル化されていない単一ポートは、port-failover 状態にはなりません。 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 状態になります。

この機能が有効になるのは、**set errordetection link-errors** 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監視されます。

- 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 | 無効 |
| RxCRC 用のポート モニタ | 無効 |
| InErrors 用のポート モニタ | 無効 |
| TxCRC 用のポート モニタ | 無効 |
| Action | ポート フェールオーバー |
| 間隔 | 30 秒 |
| サンプリング カウント | 3 回連続 |
| 下限しきい値 | 1000 |
| 上限しきい値 | 1001 |

この機能が有効で、指定したサンプリング期間内に、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 状態になります。 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 チャネルの状態が検討されます。 その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ない場合にだけ、ポートがエラー ディセーブルされます。 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の場合またはチャネル化されていない場合、上限しきい値にポートのエラー カウントが到達した場合にポートが errdisable 状態になります。

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。 リンク エラー 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 秒の間です。

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、数回のサンプリング期間に連続してこの状態が続いたときにだけ、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、リンク エラー 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 リンク エラー 下限しきい値は 1000 であり、許容範囲は 1 から 65,535 です。 デフォルト リンク エラー 上限しきい値は 1001 です。 サンプリング時間の連続番号が下限しきい値に達するとき、syslog は送信 されます。 サンプリング期間の連続数に指定した回数分、上限しきい値に達すると、syslog が送信されて、エラー ディセーブルかポート フェールオーバーのアクションが起動されます。

**注:** 同じポート エラー検出設定をチャネル内のすべてのポートに使用してください。 詳細は、Catalyst 6500 シリーズのソフトウェア設定ガイドの次のセクションを参照してください。

- 『状態と接続性のチェック』の「EtherChannel やリンクのエラー処理の設定」セクション
- 『イーサネット、ファースト 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』の「ポート エラー検出の設定」セクション

### 推奨事項

この機能では、データの記録と比較に SCP メッセージを使用するので、アクティブ ポートが多数あると CPU の負荷が高くなる可能性があります。 このシナリオでは、しきい値のインターバル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、非常に重要なリンクで機密性の高いアプリケーションのトラフィックが転送されているポートに対して、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 パラメータで使用を開始します。 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 リンクエラー 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
```

リンクエラー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 のパケット 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追加されています。 デフォルトで有効になるパケット バッファの診断機能では、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オンになります。

- 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、接続上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ための唯一の方法は、ライン モジュールの電源を切って再投入することです。

### 動作の概要

パケット バッファの診断では、一時的な SRAM の障害によって破損しているかどうかを見きわめるために、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チェックされます。 書き込まれたデータと異なるものが読み出された場合は、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が切られて再投入されます。

2 つの syslog メッセージが追加されています。 このメッセージには、パケット バッファのエラーによる、ポートがエラー ディセーブルされることの警告か、モジュールの電源が切られて再投入されることの警告が表示されます。

```
show errordetection
```

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

CatOS バージョンが 8.3 および 8.4 よりも前の場合は、ラインカードの電源再投入の時間は 30 ~ 40 秒の間になります。 CatOS バージョン 8.3 および 8.4 には高速ブート機能が追加されています。 この機能では、ブートアップ時間を最短にするために、初期ブート処理時に、インストールされているラインカードにファームウェアが自動的にダウンロードされます。 高速ブート機能では、電源再投入の時間が約 10 秒に短縮されます。

## 推奨事項

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ます。 このアクションを使用すると、実稼働の時間帯のネットワーク 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、エラー ディセーブルになっている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、サービスを回復します。 メンテナンス用の時間帯に、ラインカードの電源を手動で切って再投入するスケジュールを立てます。 **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:** モジュールがリセットされた後エラーが続いたら、モジュールを再置することを試みて下さい。

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再投入が必要なので、別の回復アクションとして、power-cycle オプションを設定する方法があります。 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、このオプションが便利です。 この時間は、ライン モジュールが完全に電源再投入をして、高速ブート機能を使用せずにサービスを再開できるようになるまでに必要な時間の長さです。 高速ブート機能では、power-cycle オプション使用時のネットワーク サービスの中断時間を 10 秒に短縮できます。 power-cycle 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 モジュールを搭載した Catalyst 5500/5000 スイッチで、不良ハードウェアを検出するために設計されました。 これらのイーサネット モジュールにはトランキングされたフレームに対して 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に、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。 困ったことに、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搬し、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 ストームを引き起こすおそれがあります。

新しい Catalyst 5500/5000 モジュールや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 テストは必要ありません。したがって、それを設定する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ものが読み出された場合は、そのポートでデータが破損する可能性があるため、ポートがシャットダウンされて failed モードになります。 エラーのしきい値は必要ありません。 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。

パケットバッファテストにおける 2 つのモードがあります: スケジュールされるおよびオンデマンド式で。 テストが始まると、テストの予想時間 ( 最も近い分に切り上げられる ) とテストが始まったことを示す syslog メッセージが生成されます。 正確なテスト時間は、ポートのタイプ、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強引に動作します。 これらのテストはパケット メモリと干渉するため、テストを開始する前に、次のようにポートを管理シャットダウン状態に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ます。これにより、混雑したリンクではパケットが失われるおそれがあります。 デフォルトでは、パケットの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。しかしこれは、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 テストを実行した場合、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毎週日曜の 03:30 に始まるようになっています。テスト ステータスを確認するには、次のコマンドを使用し

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

Cisco 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、パケットがわずかに失われる危険よりも、モジュールの問題を検出する利点の方が大きいためです。

テストは、ネットワーク全体にわたって、毎週定められた日時に実行するようにスケジュールする必要があります。そうすれば、お客様は必要に応じて障害ポートまたは 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、テスト中にパケットの一部が失われる可能性があるため、デフォルトの日曜の朝 3:30 AM など、ネットワークのトラフィックが少ない時間帯にスケジュールしてください。 テストの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のように）、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、そのためにポートが自動的にシャットダウンされる可能性があります。 次のメッセージが表示される場合があります。

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

## 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。 この機能は、次のコマンドを発行して、一定のポート範囲ごとに手動で開始します（ポートは事前に管理シャットダウン状態に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 Cisco 独自の機能で、予防的な障害管理の重要な部分を占めます。 syslog は、規格化された 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します。 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ので、syslog 情報を有効に利用できます。

- 重大度、メッセージ、デバイスなどの項目別に分析結果を提供する。
- 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。
- ページャなどへのアラートの通知や、インベントリおよび設定変更のオンデマンドの収集をトリガする。

## 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）。** 高レベルの情報を中央で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し、トラブルシューティングのときだけ高レベルの syslog を収集する組織もあります。

**CatOS プラットフォームでのデバッグは 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、デフォルトでロギングされる情報を変更することなく、セッション単位での詳細なシステム ロギングを有効にできます。**

Cisco では一般に、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。これは、これらが安定性に影響する主要な機能であり、追跡が必要とされるためです。 また、マルチキャスト環境では、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ため、mcast 機能のロギング レベルを 4 に上げ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 レベルを 4 に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
```

大量のメッセージが生成されたときに低速または存在しないターミナルからの応答を待つことによってスイッチがハングする危険を防止するために、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、主として、トラブルシューティング時またはスイッチがクラッシュしたとき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します。

この表は Catalyst 6500/6000 に個々のロギングファシリティ、デフォルトレベルおよび推奨される変更を提供したものです。 各プラットフォームにサポートされる機能によってわずかに異なるファシリティが、あります。

| 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しておく |
| CDP | 4 | デフォルトのままにしておく |
| cops | 3 | デフォルトのままにしておく |
| dtp | 8 | デフォルトのままにしておく |
| earl | 2 | デフォルトのままにしておく |
| ethc1 | 5 | デフォルトのままにしておく |
| filesys | 2 | デフォルトのままにしておく |
| gvrp | 2 | デフォルトのままにしておく |
| ip | 2 | IP 入力リストを使用している場 |

| | | |
|---|---|---|
| | | **合は 4 に変更する** |
| kernel | 2 | デフォルトのままにしておく |
| 1d | 3 | デフォルトのままにしておく |
| mcast | 2 | **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しておく |
| mls | 5 | デフォルトのままにしておく |
| PAgP | 5 | デフォルトのままにしておく |
| protfilt | 2 | デフォルトのままにしておく |
| pruning | 2 | デフォルトのままにしておく |
| Privatevlan | 3 | デフォルトのままにしておく |
| QoS | 3 | デフォルトのままにしておく |
| radius | 2 | デフォルトのままにしておく |
| rsvp | 3 | デフォルトのままにしておく |
| セキュリティ | 2 | デフォルトのままにしておく |
| SNMP | 2 | デフォルトのままにしておく |
| spantree | 2 | **6 に変更する** |
| sys | 5 | **6 に変更する** |
| tac | 2 | デフォルトのままにしておく |
| tcp | 2 | デフォルトのままにしておく |
| Telnet | 2 | デフォルトのままにしておく |
| tftp | 2 | デフォルトのままにしておく |
| UDLD | 4 | デフォルトのままにしておく |
| VMPS | 2 | デフォルトのままにしておく |
| VTP | 2 | デフォルトのままにしておく |

1 CatOS 7.x 以降では、LACP サポートを反映するために、ethc ファシリティ コードで pagp ファシリティ コードが置き換えられています。

**注:** 現時点で Catalyst スイッチは、IOS とは異なり、**set** または **clear** コマンドを実行するたびに、設定変更 syslog レベル 6 メッセージをログに記録します。Cisco IOS ソフトウェアでは、設定モードを終了した後にメッセージが生成されるだけです。 このメッセージをトリガとして、RME でリアルタイムに設定をバックアップする場合は、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。 ほとんどのお客様では、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』を参照してください。

## Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）

SNMP は、ネットワーク デバイスの Management Information Base（MIB; 管理情報ベース）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

NMS ( HP Openview など ) で利用すれば、リアルタイム アラートの生成、アベイラビリティの測定、キャパシティ計画情報の生成などを実行できるほか、設定やトラブルシューティングのチェックにも役立ちます。

## 動作の概要

ネットワーク管理ステーションにはセキュリティ メカニズムが装備されており、MIB 情報の取得には SNMP プロトコルの get および get next 要求を、パラメータの変更には **set** コマンドをそれぞれ使用します。 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設定できます。 SNMP ポーリングは IP UDP ポート 161 を使用し、SNMP トラップはポート 162 を使用します。

Cisco 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を定義します。
- SNMPv2C： SNMPv2 の組み合せ、1907 年までに RFCs 1902 で、および SNMPv2C は定義された RFC 1901 で、草案インターネット規定 試験的ドラフトである SNMPv2 のためのコミュニティベースの管理フレームワーク定義しました。 ベネフィットは表およびたくさんの情報の検索をサポートし、必要な往復旅行の数を最小に し エラー処理を改善するバルク検索メカニズムが含まれています。
- 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せることで、デバイスへの安全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： 伝送中にパケットが改ざんされなかったことを保証します。認証： メッセージが正当なソースから発信されたかどうかを判定します。暗号化 ： パケットの内容をスクランブルして、不正なソースによってパケットが容易に読み取られないようにします。

次の表に、セキュリティ モデルの組み合せを示します。

| モデル レベル | 認証 | 暗号化 | 結果 |
|---|---|---|---|
| v1 | noAuthNoPriv、コミュニティ ストリング | なし | 認証にコミュニティ ストリングの一致を使用する。 |
| v2c | noAuthNoPriv、コミュニティ ストリング | なし | 認証にコミュニティ ストリングの一致を使用する。 |
| v3 | noAuthNoPriv、ユーザ名 | なし | 認証にユーザ名の一致を使用する。 |
| v3 | authNoPriv、MD5 ま | なし | HMAC-MD5 または HMAC-SHA アルゴリズムに基づいて認証を行う。 |

| | | | |
|---|---|---|---|
| | たは SHA | | |
| v 3 | authPriv、MD5 または SHA | D E S | HMAC-MD5 または HMAC-SHA アルゴリズムに基づいて認証を行う。DES 56 ビット暗号化機能と、CBC-DES（DES-56）標準をベースとする認証機構を提供する。 |

**注:** SNMPv3 オブジェクトについては、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、どの SNMP オブジェクトにアクセスできるかを定義します。
- グループは、そのユーザが受信できる通知のリストを定義します。
- 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、管理ステーションがサポートする 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 プロトコルで通信し、別の管理ステーションとは SNMPv2 プロトコルで通信するように設定することが可能です。

現在、ほとんどの NMS ステーションでは、次の設定のもとで SNMPv2C を使用しています。

```
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<string>
!--- Include setting of SNMP strings.
```

Cisco では、使用中のすべての機能について 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、無効にしてもかまいません）。 **有効にしたトラップは、NMS で適切なエラー処理（ページャへのアラートの通知やポップアップ）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。**

トラップはデフォルトではすべて無効になっているため、個別にコマンドを使用するか、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。

| Trap | 説明 |
|---|---|
| auth | 認証 |
| ブリッジ | ブリッジ |
| シャーシ | シャーシ |
| config | 設定 |
| エンティティ | エンティティ |

| | |
|---|---|
| ippermit | IP 許可 |
| モジュール | モジュール |
| リピータ | リピータ |
| stpx | スパニング ツリー拡張 |
| syslog | syslog 通知 |
| VMPS | VLAN メンバシップ ポリシー サーバ |
| vtp | VLAN トランク プロトコル |

**注:** syslog トラップは、スイッチで生成されたすべての syslog メッセージを、SNMP トラップのように NMS に送信します。 Cisco Works 2000 RME などのアナライザによってすでに syslog アラートを実行している場合は、この情報を 2 回受信することになるため、必ずしも実用的ではありません。

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、スイッチが数百ものアクティブなインターフェイスを持つことができるためです。 そのためシスコでは、キー ポート、たとえばルータ、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、それ以外のポートでは有効にする必要はありません。これにより、ネットワーク管理の複雑さを軽減できます。

```
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

ネットワーク管理確認は特定の必要を詳しく論議するために推奨されます。 ただし、大規模なネットワークの管理のためのいくつかの Ciscoの基本的な哲学はリストされています:

- 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 HP Openview、設定、syslog、インベントリ、およびソフトウェアを管理するマネージャとして Cisco RME、NMS データ アナライザとして Microsoft Excel、Web に公開する手段としての CGI など。
- レポートを Web に公開すれば、上級管理者やアナリストなどのユーザが、特別な要求によって運用スタッフの手を煩わせることなく、自由に情報を入手できる。
- ネットワーク上で正常に動作しているものを見極め、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 を実装するため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定して初めて、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 サイクルに応じた、日、週、および四半期のトレンドを把握するために、数ヶ月を要します。

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

およびイベント RMON しきい値を設定することを推奨します。これにより、NMS にデバイスの異常な変化が通知されるようになり、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のさまざまな規則に基づいて設定できますが、この文書の適用範囲を超えるため、ここでは説明しません。

NMS を実装するための 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 を使用した詳細なポーリングを行います。 これには、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などが対象となります。 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、問題の箇所に光を当てます（ネットワーク全体を照らし出そうとしないでください）。

Cisco 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、障害発見の手がかりとなる次の MIB を分析または監視することを推奨しています。 詳細（たとえば、ポーリングするパフォーマンス MIB など）は、『Cisco 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』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（Threshold） |
|---|---|---|---|---|
| **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（Threshold） |
|---|---|---|---|---|
| **CISCO-PROCESS-MIB** | | | | |
| cpmCPUTotal5min | 最後の 5 分間に CPU がビジー状態であった合計パーセント。 | 1.3.6.1.4.1.9.9.109.1.1.1.5 | 10 分 | 基準 |

| Object Name | オブジェクトの説明 | OID | ポーリング間隔 | しきい値（Threshold） |
|---|---|---|---|---|
| **CISCO-STACK-MIB** | | | | |
| sysEnableChassisTraps | この MIB の chassisAlarmOn および chassisAlarmOff トラップを生成する必要があるかどうかを示す。 | 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 トラップを生成する必要があるかどうかを示す | 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 トラップを生成する必要があるかどうかを示す。 | 1.3.6.1.4.1.9.5.1.1.26 | 24時間 | 1 |
| sysEnableRepeaterTraps | REPEATER-MIB（RFC 1516）のトラップを生成する必要があるかどうかを示す。 | 1.3.6.1.4.1.9.5.1.1.29 | 24時間 | 1 |
| sysEnableIpPermitTraps | この MIB の IP permit トラップを生成する必要があるかどうかを示す。 | 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 トラップを生成する必要があるかどうかを示す。 | 1.3.6.1.4.1.9.5.1.1.33 | 24時間 | 1 |
| sysEnableConfigTraps | この MIB の sysConfigChange トラップを生成する必要があるかどうかを示す。 | 1.3.6.1.4.1.9.5.1.1.35 | 24時間 | 1 |
| sysEnableStpxTrap | CISCO-STP-EXTENSIONS-MIB の stpxInconsistencyUpdate トラップを生成する必要があるかどうかを示す。 | 1.3.6.1.4.1.9.5.1.1.40 | 24時間 | 1 |
| chassisPs1status | 電源モジュール 1 のステータス。 | 1.3.6.1.4.1.9.5.1.2.4 | 10分 | 2 |
| chassisPs1TestResult | 電源モジュール 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 | |
| chassisPs2Status | 電源モジュール 2 のステータス。 | 1.3.6.1.4.1.9.5.1.2.7 | 10分 | 2 |
| chassisPs2TestResult | 電源モジュール 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 | |
| chassisFanStat | シャーシ ファンのステータス。 | 1.3.6.1.4.1.9.5. | 10分 | 2 |

| | | | | |
|---|---|---|---|---|
| us | | 1.2.9 | | |
| 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 | |
| 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 |
| chassisMajorAlarm | 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 | 2 |
| 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 | |
| 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（Threshold） |
|---|---|---|---|---|
| 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 | < 30000 |
| 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、このブリッジで検出されたトポロジ変更の合計回数。 | 1.3.6.1.2.1.17.2.4 | 必要に応じて | |
| 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。 戻り値はこれらの 1 つである場合もあります: ディセーブル（1）、ブロッキング（2）、 | 1.3.6.1.2.1.17.2.15.1.3 | 必要に応じて | |

| | | | | |
|---|---|---|---|---|
| | リスニング（3）、ラーニング（4）、フォワーディング（5）、解除（6）。 | | | |

| Object Name | オブジェクトの説明 | OID | ポーリング間隔 | しきい値（Threshold） |
|---|---|---|---|---|
| CISCO-MEMORY-POOL-MIB | | | | |
| ciscoMemoryPoolUsed | 管理対象装置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す。 | 1.3.6.1.4.1.9.9.48.1.1.1.5 | 30分 | 基準 |
| 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 の合計がメモリ プールの総量になります。 | 1.3.6.1.4.1.9.9.48.1.1.1.6 | 30分 | 基準 |
| ciscoMemoryPoolLargestFree | 管理対象装置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す。 | 1.3.6.1.4.1.9.9.48.1.1.1.7 | 30分 | 基準 |

Cisco MIB のサポートについての詳細は、『Cisco ネットワーク管理ツールキット：MIB』を参照してください。

**注:** 標準 MIB の中には、特定の SNMP エンティティに含まれる MIB のインスタンスが 1 つだけであると仮定しているものがあります。 そのような標準 MIB には、ユーザが 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するインデックスがありません。 この場合は、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 のセキュリティ側面は時間の SNMPv2 を上回ると使用が期待されることを意味します。 Cisco は顧客が NMS 戦略の一部としてこの新しいプロトコルの準備をすることを推奨します。 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露出する事態を防止できます。 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 のコマンドラインとは大きく異なります。また、スーパーバイザ エンジンの CPU の負荷が向上すると予想されます。

## リモート モニタリング

RMON では、履歴に基づくベースラインの決定やしきい値分析など、ネットワーク管理者が情報を一般的な用途で使用したり応用したりするための準備として、ネットワーク デバイスによる MIB データの前処理が可能になります。

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

4 つの基本的な RMON-1 グループで構成されている各ポートのハードウェアの Catalyst スイッチ サポート mini-RMON、: 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）

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。 前に説明したように、RMON しきい値を設定することで、異常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、それらのポートで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した変動が見られ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間違いなく作成するのは手間がかかるため、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 の 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 グループが有用な L2 トラフィック統計を提供します。 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。 サンプリングされたこれらの値を履歴グループに保存するよう、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、正確なベースラインが得られ、そのうえポーリングによる過剰なオーバーヘッドが発生することもありません。 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。

スイッチが RMON-1 の 4 人の基本的なグループだけ提供する間、RMON-1 および RMON-2 の他を忘れていないことは重要です。 すべてのグループは UsrHistory（グループ 18）およびを含む RFC 2021 で、ProbeConfig（19）グループ定義されます。 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、または内部の Network Analysis Module（NAM; ネットワーク解析モジュール）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 データなどを調べることもできます。 MLS が実行されているということは、ルータがフロー内のすべてのパケットを交換し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だけが信頼できる VLAN アカウンティングを提供します。

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 管理パッケージで解読できま

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 全体に対して SPAN 機能を使用する場合は注意すべき点があります。 1Gbps 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 1Gbps 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場合があります。 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。 詳細は、『Catalyst スイッチド ポート アナライザ（SPAN）機能の設定』を参照してください。

## 推奨事項

Cisco では、SNMP ポーリングだけ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 しきい値および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小さくなり、ベースラインからの変動があっ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 はトラフィックディレクターのような外部エージェントによって駆動される必要があります; CLI サポートがありません。 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ついて履歴およびしきい値を設定すると、リソースが消費されること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。 また重大 な ポート ルールを覚えて下さい: プラニングの段階で重要ように識別されるポートのしきい値だけをポーリングし、設定 して下さい。

## 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、設定するためにスイッチに送信します。 一般に、メモリ制約を考慮するのは DRAM の容量が 32 MB より少ない旧型のスーパーバイザ エンジンについてのみです。 次のガイドラインを参考にしてください。

- およそコード空間の 450K は NMP イメージに（サポートするために RMON の 4 グループである mini-RMON 追加されます: 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場合）。 RMON の動的なメモリ要件は実行時コンフィギュレーションによって決まるため、一定ではありません。 ミニ RMON グループ別の、RMON の実行時メモリ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 バイトを使用する。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 以上の場合はおよそ 20 K、合計 NVRAM サイズが 128 K の場合は 10 K の NVRAM 領域を消費します。

# 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。 偶発的または悪質なプロトコル攻撃を防ぐために暗号化認証を設定できるものもあります。

## 動作の概要

NTP は RFC 958 で最初に文書化されていますが 、RFC 1119 によって展開しました ( 2 ) NTP バージョンは RFC 1305 で定義されたように第 3 バージョンにおよび今あります 。 それは UDP ポート 123 を実行します。 NTP の通信ではすべて、グリニッジ標準時と同じ時刻である UTC が使用されます。

## 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。

インターネットで公開されているこれらの NTP サーバが利用できるかどうか、または正確な時刻を提供するかどうかは保証されていないため、他の方法を検討することを強く推奨します。 これには、多数のルータに直接接続されたスタンドアロンの Global Positioning Service ( GPS ) デバイスを利用するという方法があります。

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。

## Stratum

各 NTP サーバでは、そのサーバが外部の時刻ソースからどれだけ離れているかを示す層 ( stratum ) の概念を採用しています。 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。 それ以降、Stratum 2 サーバは指定された Stratum 1 サーバ群から詳細な時刻を取得し、Stratum 3 サーバは Stratum 2 サーバから詳細な時刻を取得する、というように続きます。

## サーバとピアの関係

- サーバはクライアントからの要求に応答するものであり、クライアント時刻ソースから日付

情報を取り込むものではありません。
- ピアは、クライアントからの要求に応答するものですが、クライアントの要求を、時刻ソースを向上させるための手段として、自身のクロック周波数の安定化に利用します。
- 真の意味でのピアになるためには、接続の両側がピア関係を結ぶ必要があります。一方のユーザがピアで、もう一方がサーバでは、真のピアにはなりません。 また、信頼できるホスト同士だけが互いにピアとして通信できるようにするため、ピア間で鍵を交換することが推奨されます。
- サーバへの Client 要求では、サーバはクライアントに答え、クライアントが質問をしたことを忘れています; ピアへの Client 要求では、サーバはクライアントに答え、どれだけうまくタイムキーピングでし、どんな層サーバを実行しているかトラッキングするためにクライアントについてのステート情報を保持します。**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 サーバで数千台のクライアントを処理するのは問題ありません。 ただし、ピア関係を数百も処理するとメモリへの負担がかかり、この状態を保持することで帯域幅だけでなく、装置の CPU 使用率も高くなります。

## 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、これは応答を得るために NTP が再びポーリングするまでの最大時間です。 現時点では、ユーザが Cisco デバイスに手動で POLL 時間を設定する方法はありません。

NTP ポーリング カウンターは $2^{6}$ 時で開始します ( 64 ) 秒は $2^{10}$ への 2 の電源によって ( 2 つのサーバが互いに同期すると同時に ) 、増分し。 つまり、設定したサーバまたはピアごとに、同期メッセージが 64、128、256、512、または 1024 秒間隔で送信されます。 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。 時間内にジッタが多い場合は、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は、ポーリング間隔が 1024 秒に収束します。

実際には、これは、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 ) 。応答が 1 つ受信されなかった場合は、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 時間少々かかります。

## 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。 ルータに **ntp broadcast** コマンドを設定すると、設定したインターフェイスから NTP ブロードキャストが発信されます。 NTP broadcastclient コマンドによりルータを引き起こしますまたは NTP を受信するスイッチは設定されるインターフェイスでブロードキャストします。

## 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 経由で中央サイトのコア ルータ（Stratum 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、サーバごとにおよそ 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、インターネット上からの信頼できる提供元やラジオクロックに同期させています。 しかし、多数のスイッチを運用している場合は、サーバ モードに代わる単純な方法として、スイッチ 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 モードにする方法があります。 このメカニズムは Catalyst の全体のドメインが単一 の ブロードキャスト同報通信メッセージからクロックを受け取るようにします。 ただし、時刻管理 の 正確性は情報 の 流れが一方向であるので多少損なわれます。

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 通り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
- 認証

イベントの時間相関は 2 つのケースで非常に有益です: トラブルシューティング および セキュリティ監査。 そのため、時刻ソースとデータを保護するための対策を講じる必要があります。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。

Cisco では次の設定を推奨しています。

**Catalyst の設定**

```
set ntp broadcastclient enable
set ntp authentication enable
set ntp key key
!--- This is a Message Digest 5 (MD5) hash. set ntp
timezone <zone name>
set ntp summertime <date change details>
```

**Catalyst での別の設定**

```
!--- This more traditional configuration creates !---
more configuration work and NTP peerings. set ntp client
enable
set ntp server IP address of time server set timezone
zone name set summertime date change details
```

**ルータコンフィギュレーション**

```
!--- 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 発見プロトコル

CDP はデータリンク層を通じ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 Outside のネットワーク トポロジと物理構成を調べるために役立ちます。 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 の改良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。 イーサネットで、ATM および FDDI 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** 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。 CDP フレームはデフォルトでは 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近接デバイスに関する情報を収集し、保存します。

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 | タイプ | 説明 |
|---|---|---|
| 1 | デバイス 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。 |
| 2 | アドレス | 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 ブリッジまたは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 | プラットフォーム | 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がスイッチ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 が稼働している場合、v2 フレームは廃棄されます。 CDPv2 が稼働しているスイッチのインターフェイスで CDPv1 フレームが受信されると、そのインターフェイスか

らは CDPv2 フレーム以外に CDPv1 フレームも送出され始めます。

| パラメータ | タイプ | 説明 |
|---|---|---|
| 9 | 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、これはタグが付加されない 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が 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.
```

高レベルのセキュリティが必要なネットワーク部分（インターネットに面した DMZ など）では、次のコマンドのように 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。 スターでマークされるエントリは（*）Vlan不整合を示します; でマークされるエントリは a #二重モード の ミスマッチを示します。 これはトラブルシューティング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 電話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での電源管理に利用されます。

IP 電話に接続している 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（補助 VLAN）に配置できます。 これにより、スイッチでは VoIP トラフィックに対して異なる QoS を容易に適用できるようになります。

また、補助 VLAN が変更された場合（たとえば、電話機が特定の VLAN または特定のタギング方式を使用するようにする場合など）は、その情報は CDP を通じて電話機に送信されます。

| パラメータ | タイプ | 説明 |
|---|---|---|
| 14 | アプライアンス ID | 別の VLAN ID（auxiliary VLAN）を使用したりすることで、VoIP トラフィックを他のトラフィックと区別します。 |
| 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、現時点では 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、Cisco のどのツールとテクノロジーが適格であるかを定義する助けとなるセキュリティ ポリシーをすでに確立していることが望まれます。

**注:** CatOS ではなく Cisco IOS ソフトウェアのセキュリティについては、『Cisco ISP の必須事項』など、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。 パスワードは CatOS 5.x 以降、大文字と小文字が区別されるようになりました。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
```

ログインおよびイネーブル パスワードはすべて、最小長標準（例：最低 6 文字、文字と数字、大文字と小文字を混在させる）を満たす必要があります。 これらのパスワードは、MD5 ハッシング 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。 詳細は、このドキュメントの「TACACS+」セクション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 による暗号化を利用します。 SSH による暗号化がサポートされているのはスイッチに対するリモート ログインだけです。 スイッチから開始される Telnet セッションを暗号化することはできません。 SSH バージョン 1 は CatOS 6.1 でサポートされており、バージョン 2 のサポートは CatOS 8.3 で追加されています。 SSH バージョン 1 は Data Encryption Standard（DES; データ暗号規格）とトリプル DES（3-DES）の暗号化方式をサポートしており、SSH バージョン 2 は 3-DES と Advanced Encryption Standard（AES; 高度暗号化規格）の暗号化方式をサポートしています。 SSH による暗号化は、RADIUS と TACACS+ の認証に使用できます。 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 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 その他のプロトコルによる管理 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 アドレスおよびポートによる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、Telnetアクセスがこのコマンドで制限 されれば、CatOS デバイスへのアクセスは少数の信頼された端末を通してしか実現することができません。 このセットアップはトラブルシューティングの妨害である場合もあります。 IP アドレスをスプーフィングすることが可能で、フィルタによるアクセス制御を通過してしまう可能性もあります。そのため、これは保護の最初の層に過ぎないことを忘れないでください。

## 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、1 つまたは複数の既知の MAC アドレスからのデータしか特定のポートを通過できないようにする場合は、ポート セキュリティの利用を検討してください。 これを実現するには、次のように静的な 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
```
次のオプションが設定できます。

- 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。 分の有効な時刻は 10 - 1440 です。 デフォルトではエージングは設定されていません。
- 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 認証が導入されました。この認証方式を利用すると、クライアントが中央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することができます。 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

な指針とされる可能性があります。 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』を参照してください。

## ログイン バナー

不正なアクセスに対する措置を明確に示す適切なデバイス バナーを作成します。 サイト名や、不正なユーザに情報を提供するおそれのあるネットワーク データはアドバタイズしないでください。 これらのバナーは、万一デバイスに不正にアクセスされて、その実行者が捕まったときに、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

適切な許可なしに物理的にデバイスに近付けないようにする必要があります。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。 環境要因に悪質な細工が施されても、ネットワークがその影響を受けることなく正常に稼働し続けるようにするため、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、機器の温度（空調）を管理する必要があります。 悪意のある者が物理的に侵入した場合は、パスワード回復などによる破壊工作が行われる傾向が強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 セッションを通じ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 デバイスでのこれらの実装は時間がかかる上、中央集中型ではありません。 また、設定ミス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面倒です。

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

この章で述べる TACACS+ は、シスコ ネットワークでの導入例の多いシステムです。 TACACS+ には次のような機能があります。

- 認証：ユーザを識別し、確認するプロセス。 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対して各種コマンドの許可を付与できます。
- アカウンティング：デバイス上でユーザが現在行っている操作、または過去に行った操作の記録。

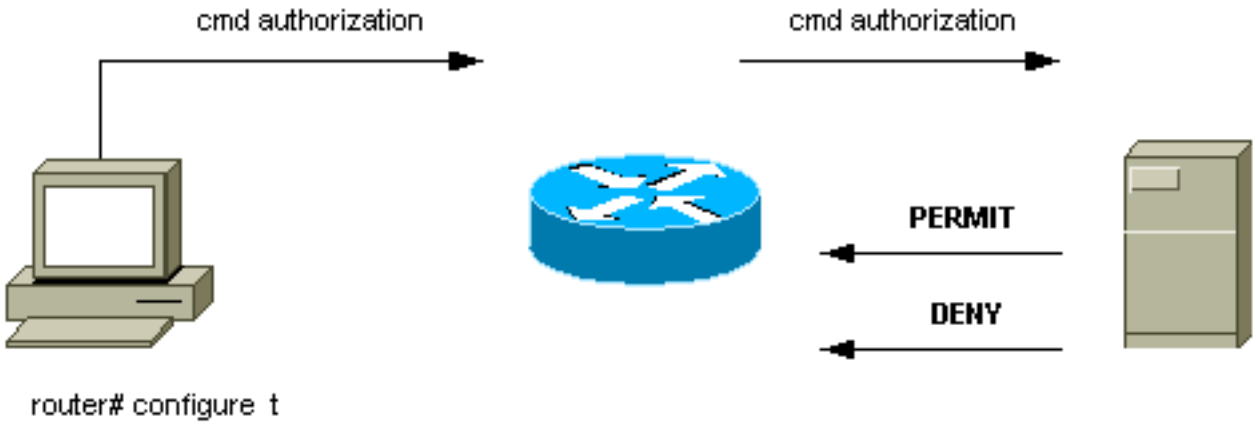
詳細は、『Cisco Catalyst スイッチの TACACS+、RADIUS および Kerberos の設定』を参照してください。

## 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。 それは転送 プロトコルとして TCPポート 49 を使用します; これは UDP 上のこれらの長所があります（RADIUS によって使用される）:

- 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負荷が現在どれだけ高くても、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許可チェックが必要となった場合、スイッチは TACACS+ を使用して、ユーザに特定のコマンドを使用する権限が付与されているかどうかを確認します。 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れば、特定のユーザが発行したコマンドの監査を、特定のネットワーク デバイスに接続したまま行うことができます。




TACACS+ を使用している環境では、ユーザがネットワーク デバイスにログインする際、通常は次のプロセスが発生します。

- 接続が確立されると、スイッチは TACACS+ デーモンに問い合せてユーザ名プロンプトを取得し、ユーザに対してそのプロンプトを表示します。 ユーザがユーザ名を入力すると、スイッチは TACACS+ デーモンに問い合せてパスワード プロンプトを取得します。 スイッチにパスワード プロンプトが表示されると、ユーザはパスワードを入力し、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 TACACS+ デーモンから、最終的に次の応答のいずれかを受け取ります。ACCEPT：ユーザが認証され、サービスが開始可能になりました。 認可を要求するようにネットワーク デバイスが設定されている場合は、この時点で認可が開始されます。リジェクト—ユーザは認証を受け損いました。 TACACS+ デーモンの設定に応じて、ユーザは以降のアクセスを拒否されるか、またはログイン シーケンスをリトライするためのプロンプトが表示されます。ERROR：認証のどこかの時点でエラーが発生しました。 このエラーはデーモンで起こる場合と、デーモンとスイッチ間のネットワーク接続で起こる場合があります。 ERROR 応答が受信されると、ネットワーク デバイスは通常、代替のユーザ認証方法を使用しようとします。CONTINUE：ユーザに対して追加の認証情報を入力するためのプロンプトが表示されます。
- ユーザは TACACS+ 認可に進む前に、TACACS+ 認証を正常に完了する必要があります。
- TACACS+ 認可が要求されている場合は、TACACS+ デーモンに再び問い合わせが発行され、認可の応答として ACCEPT または REJECT が返信されます。 ACCEPT 応答が受信された

場合は、その応答に、EXEC または NETWORK セッションを対象ユーザに向けるために使用するアトリビュート形式のデータが格納されており、これに基づいてユーザがアクセス可能なコマンドが判別されます。

## 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ため、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、どのお客様もこの領域では独自の要件を持っているため、推奨事項を提示することは困難です。 詳細は、『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』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、各ユーザが何を入力し、何を設定したかを示す監査証跡を残すことができます。 次に、コマンドの最後で監査情報を取得するという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
```

この設定には次のような機能があります。

- connect コマンドは、スイッチでの発信接続イベント（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。
- 1 分ごとにサーバに定期**アップデート**を送信することで、ユーザがまだログインしているかどうかを記録します。

## 設定チェックリスト

このセクションでは、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*
次のキーを、以下に示す表のコマンドとともに使用してください。

| **凡例：** |
| --- |
| **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** | **備考** |
| --- | --- |
| **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する。 |
| **set vtp mode transparent** | このドキュメントで説明されている VTP モードを選択する。 詳細は、このドキュメントの「VLAN Trunking Protocol」セクションを参照してください。 |
| set spantree enable all | すべての VLAN で STP を有効にする。 |
| **set spantree root vlan** | VLAN ごとのルート（およびセカンダリ ルート）ブリッジの設定用に推奨。 |
| **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する（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する（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の、ポートの自動シャットダウンを有効にする。 |
| **set udld enable** | 単方向リンク検出を有効にする（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する（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 チェックを有効にする（Catalyst 5500/5000 のみに適用）。 |
| set logging buffer 500 | 最大内部 syslog バッファを維持する。 |
| **set logging server IP address** | 外部システム メッセージを口ギングするように、ターゲット syslog サーバを設定する。 |
| **set logging server enable** | 外部口ギング サーバを有効にする。 |
| set logging timestamp enable | 口グでメッセージのタイムスタンプを有効にする。 |
| **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** | system 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 のみのエクスポートを可能にする。 |
| **set logging console disable** | トラブルシューティングを除き、コンソールを無効にする。 |
| **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可能にする。 |
| **set snmp community read-write string** | パスワードを設定し、リモートでの設定を可能にする。 |
| **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可能にする。 |
| **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 アラートを行う。 |
| **set snmp trap server address string** | NMS トラップ レシーバのアドレスを設定する。 |
| **set snmp rmon enable** | ローカルで統計を収集するよう RMON を有効にする。 詳細は、このドキュメントの「リモート モニタリング」セクションを参照してください。 |
| **set ntp broadcastclient enable** | アップストリーム ルータからの正確なシステム クロックの受信を有効にする。 |
| **set ntp timezone zone name** | デバイスのローカル時間帯を設定する。 |
| **set ntp summertime date change details** | 時間帯に適用可能である場合、サマータイムを設定する。 |

| | |
|---|---|
| **set ntp authentication enable** | セキュリティを確保するために時間情報の暗号化を設定する。 |
| **set ntp key key** | 暗号化鍵を設定する。 |
| set cdp enable | ネイバー検出を有効にする（デフォルトではポート上でも有効になる）。 |
| **set tacacs server IP address primary** | AAA サーバのアドレスを設定する。 |
| **set tacacs server IP address** | 可能であれば、AAA サーバを冗長化する。 |
| set tacacs attempts 3 | AAA ユーザ アカウントのパスワード入力を 3 回まで認める。 |
| **set tacacs key key** | AAA MD5 暗号化鍵を設定する。 |
| **set tacacs timeout 15** | サーバのタイムアウトを長くする（デフォルトは 5 秒）。 |
| **set authentication login tacacs enable** | ログインの認証に AAA を使用する。 |
| **set authentication enable tacacs enable** | イネーブル モードの認証に AAA を使用する。 |
| set authentication login local enable | デフォルト; ローカルにフォールバックを利用可能 な AAAサーバ許可しません。 |
| set authentication enable local enable | デフォルト; ローカルにフォールバックを利用可能 な AAAサーバ許可しません。 |

**ホスト ポートの設定コマンド**

| **コマンド** | **備考** |
|---|---|
| **set port host port range** | 不要なポート処理を無効にする。 このマクロは、スパニング ツリー PortFast を有効、チャネルをオフ、トランクをオフにそれぞれ設定します。 |
| set udld disable port range | 不要なポート処理を無効にする（銅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する。 |
| set port trap port range disable | 一般的なユーザ向けの SNMPトラップのための必要無し; トラック キーポートだけ。 |

**サーバ設定コマンド**

| **コマンド** | **備考** |
|---|---|
| **set port host port** | 不要なポート処理を無効にする |

| | |
|---|---|
| **range** | 。 このマクロは、スパニング ツリー PortFast を有効、チャネルをオフ、トランクをオフにそれぞれ設定します。 |
| set udld disable port range | 不要なポート処理を無効にする（銅ポートではデフォルトで無効）。 |
| **set port speed port range 10** / *100* | 通常スタティック/サーバポートを設定して下さい; さもなければ、自動ネゴシエーションを使用して下さい。 |
| **set port duplex port range full** / *半二重* | 通常静的/サーバポート; さもなければ、自動ネゴシエーションを使用して下さい。 |
| **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る。 |

**未使用ポートの設定コマンド**

| コマンド | 備考 |
|---|---|
| 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する。 |
| **set port disable port range** | 未使用ポートを無効にする。 |
| **set vlan unused dummy vlan port range** | ポートがイネーブル状態であれば、認可されていないトラフィックを未使用の VLAN へ送信する。 |
| **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する。 |
| **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する。 |

**インフラストラクチャ ポート（スイッチ同士の間、スイッチとルータとの間）**

| コマンド | 備考 |
|---|---|
| set udld enable port range | 単方向リンク検出を有効にする（銅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 モードを有効にする（デバイスでサポートされている場合）。 |
| set port negotiation **port range**enable | 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可能にする。 |

| | |
|---|---|
| **set port trap port range** enable | これらのキーポートに対して SNMP トラップを許可する。 |
| **set trunk port range** off | トランクを使用していない場合、機能を無効にする。 |
| **set trunk mod/port desirable ISL** / *dot1q* / *negotiate* | トランクを使用している場合、dot1q が優先される。 |
| **clear trunk mod/port vlan range** | トランクが必要でない場合、トランクから VLAN をプルーニングすることで STP の直径を制限する。 |
| **set port channel port range** mode off | チャネルを使用していない場合、機能を無効にする。 |
| **set port channel port range** mode desirable | チャネルを使用している場合、PAgP を有効にする。 |
| 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 バランシングを可能にする（Catalyst 6500/6000 ではデフォルト）。 |
| **set trunk mod/port nonegotiate ISL** / *dot1q* | ルータ、Catalyst 2900XL、3500、または他のベンダーにトランキングしている場合、DTP を無効にする。 |
| **set port negotiation mod/port** disable | 一部の古い GE デバイスに関しては、ネゴシエーションに互換性がない場合がある。 |

## 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
- Catalyst 5000/5500 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