Cisco IOS が動作している Catalyst 6500/6000 シリーズおよび Catalyst 4500/4000 シリーズ スイッチのベスト プラクティス

目次

概要

このドキュメントでは、スーパーバイザ エンジンで Cisco IOS® ソフトウェアを実行する Catalyst 6500/6000 および 4500/4000 シリーズ スイッチのベスト プラクティスについて説明します。

Catalyst 6500/6000 および Catalyst 4500/4000 シリーズ スイッチでは、スーパーバイザ エンジンで稼働する次の 2 つのオペレーティング システムのいずれかがサポートされます。

- Catalyst OS（CatOS）
- Cisco IOS ソフトウェア

CatOS では、次のようなルータのドーター カードやモジュールで Cisco IOS ソフトウェアを稼働させることもできます。

- Catalyst 6500/6000 の Multilayer Switch Feature Card（MSFC; マルチレイヤ スイッチ フィーチャ カード）
- Catalyst 4500/4000 の 4232 レイヤ 3（L3）モジュール

このモードでは、設定用に次の 2 つのコマンドラインがあります。

- スイッチング用の CatOS コマンドライン
- ルーティング用の Cisco IOS ソフトウェア コマンドライン

CatOS は、スーパーバイザ エンジン上で稼働するシステム ソフトウェアです。 ルーティング モジュールで Cisco IOS ソフトウェアを稼働させるオプションを使用するには、CatOS システム ソフトウェアが必要です。

Cisco IOS ソフトウェアの場合、設定用のコマンドラインは 1 つだけです。 このモードでは、CatOS の機能が Cisco IOS ソフトウェアに統合されています。 この統合により、スイッチングとルーティングの両方の設定を 1 つのコマンドラインで行えるようになっています。 このモードでは、CatOS ではなく、Cisco IOS ソフトウェアがシステム ソフトウェアになります。

CatOS と Cisco IOS ソフトウェア オペレーティング システムは両方とも、重要なネットワークで利用されています。 ルータのドーター カードおよびモジュール用の Cisco IOS ソフトウェア オプションを備えた CatOS は、次のスイッチ シリーズでサポートされています。

- Catalyst 6500/6000
- Catalyst 5500/5000
- Catalyst 4500/4000

Cisco IOS システム ソフトウェアは、次のスイッチ シリーズでサポートされています。

- Catalyst 6500/6000
- Catalyst 4500/4000

このドキュメントでは、Cisco IOS システム ソフトウェアについて説明していますので、CatOS に関する情報については、『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』を参照してください。

Cisco IOS システム ソフトウェアを使用すると、ユーザには次のような利点があります。

- 単一のユーザ インターフェイス
- 統合されたネットワーク管理プラットフォーム
- 拡張された QoS 機能

- 分散型スイッチングのサポート

このドキュメントでは、設定の手引きをモジュール単位で記述しています。 そのため、各セクションを個別に読んで、段階的に設定の変更を行えます。 このドキュメントでは、読者が Cisco IOS ソフトウェアのユーザ インターフェイスに関する基本的な知識を持っていることを前提としています。 全体的なキャンパス ネットワークの設計については、このドキュメントでは取り扱っていません。

はじめに

背景説明

このドキュメントで紹介するソリューションは、数多くの大規模企業のお客様と協力しながら長年にわたって複雑なネットワークに取り組んできた Cisco エンジニアの現場経験から生まれたものです。 その結果、このドキュメントはネットワークを適切に運用するための、現実的な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

参考資料

Cisco.com には、Catalyst 6500/6000 および Catalyst 4500/4000 製品ラインに関連する参照サイトが数多く用意されています。 このセクションに示す参考資料では、このドキュメントで説明されているトピックがさらに詳しく説明されています。

この資料が取り扱っているトピックの何れかに関する詳細については LANスイッチング技術 サポートを参照して下さい。 このサポート ページには、製品マニュアルだけでなく、トラブルシューティングや設定に関するドキュメントもあります。

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

- Cisco ISP Essentials
- Catalyst 6500 シリーズ スイッチ用の Cisco Catalyst および Cisco IOS オペレーティング システムの比較
- Cisco LAN Switching (CCIE Professional Development series)
- Building Cisco Multilayer Switched Networks
- Performance and Fault Management
- SAFE:
- Cisco Field Manual: Catalyst Switch Configuration

基本設定

このセクションでは、ほとんどの Catalyst ネットワークを利用する際に導入する機能について説

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 エンジン 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、Cisco Discovery Protocol（CDP）のように Cisco 独自のものや、IEEE 802.1D（スパニング ツリー プロトコル（STP））のように標準ベースのものがありますが、Catalyst シリーズに実装された場合、いずれも共通の要素が備わっています。

基本的なフレーム転送では、ユーザ データ フレームがエンド システムから発信されます。 このデータ フレームの送信元アドレス（SA）と宛先アドレス（DA）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。 SA 学習プロセスにより、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。 このテーブルにより、受信した各フレームをどの出力ポートから転送するかが決まります。 宛先が不明な場合や、フレームの宛先がブロードキャスト アドレスまたはマルチキャスト アドレスである場合は、アドレス学習プロセスが不完全になります。 アドレス学習プロセスが不完全になると、その VLAN 内のすべてのポートにフレームが転送（フラッディング）されます。 スイッチでは、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 自体に送る必要があるフレームを識別する必要もあります。 スイッチの CPU は Network Management Processor（NMP; ネットワーク管理プロセッサ）とも呼ばれます。

Catalyst コントロール プレーンは、CAM テーブル内の特別なエントリを使用して作成されます。 これらの特別なエントリは、システム エントリと呼ばれます。 コントロール プレーンは、内部スイッチ ポートでトラフィックを受信して、NMP にトラフィックを送ります。 そのため、既知の宛先 MAC アドレスが設定されたプロトコルを使用することにより、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。

Cisco では、このセクションの表に示すように、イーサネット MAC アドレスとプロトコル アドレスの範囲を予約しています。 このドキュメントでは、それぞれの予約アドレスについて詳しく説明していますが、便宜上、次の表には要約だけを記載しています。

機能	SNAP1 HDLC2 プロトコル タイプ	宛先マルチキャスト MAC
PAgP3	0x0104	01-00-0c-cc-cc-cc
PVST+、RPVST+4	0x010b	01-00-0c-cc-cc-cd
VLAN ブリッジ	0x010c	01-00-0C-CD-CD-CE
UDLD5	0x0111	01-00-0c-cc-cc-cc
CDP	0x2000	01-00-0c-cc-cc-cc
DTP6	0x2004	01-00-0c-cc-cc-cc
STP UplinkFast	0x200a	01-00-0c-cd-cd-cd

IEEE スパニング ツリー 802.1D	N/A—DSAP 7 42 SSAP8 42	01-80-c2-00-00-00
ISL9	N/A	01-00-0c-00-00-00
VTP10	0x2003	01-00-0c-cc-cc-cc
IEEE Pause 802.3x	N/A：DSAP 81 SSAP 80	01-80-C2-00-00-00>0F

1 SNAP = Subnetwork Access Protocol（サブネットワーク アクセス プロトコル）。

2 HDLC = High-Level Data Link Control（ハイレベル データリンク コントロール）。

3 PAgP = Port Aggregation Protocol（ポート集約プロトコル）。

4 PVST+ = Per VLAN Spanning Tree+ および RPVST+ = Rapid PVST+。

5 UDLD = UniDirectional Link Detection（単方向リンク検出）。

6 DTP = Dynamic Trunking Protocol（ダイナミック トランキング プロトコル）。

7 DSAP = Destination Service Access Point（宛先サービス アクセス ポイント）。

8 SSAP = Source Service Access Point（送信元サービス アクセス ポイント）。

9 ISL = Inter-Switch Link（スイッチ間リンク）。

10 VTP = VLAN Trunk Protocol（VLAN トランク プロトコル）。

Cisco の制御プロトコルの大部分では、Logical Link Control（LLC; 論理リンク制御）0xAAAA03 と Organizational Unique Identifier（OUI; 組織固有識別子）0x00000C を含む、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。

これらのプロトコルはポイントツーポイント接続を前提としています。 マルチキャストの宛先アドレスを意図的に使用することで、2 台の Catalyst スイッチが 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えないデバイスがそれらのフレームを単純にフラッディングするようになるためです。 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ります。 一般的には、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避けてください。 これらのプロトコルはレイヤ 3 ルータで終端されるため、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。

次に、SA の説明に移ります。 スイッチ プロトコルでは、使用可能なアドレスのバンクから割り当てられた MAC アドレスが使用されます。 使用可能なアドレスのバンクは、シャーシの EPROM によって提供されます。 **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から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。 次に、コマンドの出力例を示します。

```
>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 !--- These are the MACs for
sourcing traffic.
```

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、デフォルトの VLAN である VLAN 1 を常に使用して、多数の制御プロトコルや管理プロトコルのタグ付けを行います。 そのようなプロトコルには、CDP、VTP、PAgP などがあります。 デフォルトでは、内部 sc0 インターフェイスを含むすべてのスイッチ ポートが VLAN 1 のメンバとなるように設定されています。 デフォルトでは、すべてのトランクで VLAN 1 が伝搬に使用されます。

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。

- 管理 VLAN とは、CatOS スイッチやローエンド スイッチ向けの sc0 が存在する VLAN のことです。 この VLAN は変更できます。 CatOS スイッチと Cisco IOS スイッチの間でインターワーキングを行うときには、このことを念頭においてください。
- ネイティブ VLAN とは、トランキングが行われていない場合にポートが戻される VLAN のことです。 また、ネイティブ VLAN とは、IEEE 802.1Q トランク上でタグ付けされない VLAN のことでもあります。

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。 詳細は、「スイッチ管理インターフェイスとネイティブ VLAN」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 でのレイヤ 2 ループを避けてください。 レイヤ 2 ループを避けるには、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 データ用の VLAN 1 を削除しても、引き続き VLAN 1 を使用して送信されているコントロール プレーン トラフィックには影響しません。
- ISL トランクでは、DTP パケットが VLAN1 に送出されます。 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、802.1Q IEEE BPDU が共通スパニング ツリーの VLAN 1 上をタグなしで転送されます。 これは、ネイティブ VLAN の設定にかかわらず同様です。 **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、「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。 ただし、VLAN 1 がディセーブル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。

標準機能

このセクションでは、あらゆる環境に共通する基本的なスイッチング機能について説明しています。 これらの機能は、ネットワーク内にあるすべての Cisco IOS ソフトウェア Catalyst スイッチング デバイスで設定する必要があります。

VLAN トランク プロトコル

目的

VLAN 管理ドメインとも呼ばれる VTP ドメインは、同じ VTP ドメイン名を共有するトランクによって相互接続された 1 台以上のスイッチで構成されています。 VTP を使用すると、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。 VTP では、これらの変更が (ネットワーク) VTP ドメイン内の他のすべてのスイッチに自動的に伝搬されます。 1 台のスイッチが所属できるのは、1 つの VTP ドメインのみです。 VLAN を作成する前に、ネットワークで使用する VTP モードを決定する必要があります。

動作の概要

VTP はレイヤ 2 メッセージング プロトコルです。 VTP では、VLAN 設定の整合性を維持するために、VLAN の追加、削除、および名前の変更がネットワーク全体で管理されます。 VTP を使用すると、さまざまな問題に至る可能性のある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。 そのような問題には、VLAN 名の重複、不適切な VLAN タイプの指定、セキュリティ違反などがあります。

デフォルトでは、スイッチは VTP サーバ モードで動作し、管理ドメインが存在しない状態になります。 これらのデフォルト設定は、ドメインについてのアドバタイズメントがトランク リンク経由でスイッチに届いた際、または管理ドメインが設定された際に変更されます。

VTP プロトコルでは、既知のイーサネット宛先マルチキャスト MAC (01-00-0c-cc-cc-cc) と SNAP HDLC プロトコル タイプ 0x2003 を使用して、スイッチ間での通信が行われます。 VTP では、他の基盤プロトコルと同様に、LLC 0xAAAA03 と OUI 0x00000C を含む IEEE 802.3 SNAP カプセル化が使用されます。 これは、LAN アナライザのトレースで確認できます。 VTP は非トランク ポートでは機能しません。 そのため、DTP によってトランクが起動されるまではメッセージを送信できません。 つまり、VTP は ISL または 802.1Q のペイロードです。

メッセージ タイプには、次のものがあります。

- 300 秒間隔で生成される「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 プルーニングがイネーブルになっている場合の「加入」

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、ドメイン全体にこの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 inactive 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非アクティブ化されます。

ほとんどの Catalyst スイッチは、次のいずれかの VTP モードで動作するように設定できます。

- サーバ：VTP サーバモードでは、次のことを行えます。VLAN の作成VLAN の修正VLAN の削除VTP ドメイン全体に対する他の設定パラメータ（VTP バージョンや VTP プルーニングなど）の指定VTP サーバは、自身の VLAN 設定を同一 VTP ドメイン内の他のスイッチにアドバタイズします。 また、VTP サーバは、トランク リンク経由で受信したアドバタイズメントに基づいて、自身の VLAN 設定を他のスイッチと同期します。 VTP サーバがデフォルトのモードです。
- クライアント：VTP クライアントは VTP サーバと同じように動作します。 ただし、VTP クライアントでは、VLAN の作成、変更、削除を行えません。 さらに、クライアントでは、VLAN 情報が NVRAM に書き込まれないので、リブート後には VLAN が記憶されていません。
- トランスペアレント：VTP トランスペアレント スイッチは、VTP に参加しません。 VTP トランスペアレント スイッチでは、VLAN 設定がアドバタイズされることも、受信したアドバタイズメントに基づいて VLAN 設定が同期されることもありません。 ただし、VTP バージョン 2 では、トランスペアレント スイッチの場合でも、受信した VTP アドバタイズメントがトランク インターフェイス経由で転送されます。

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	
VTP メッセージの受信	○	○	なし	
VLAN の作成	○	なし	（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）	

1 Cisco IOS ソフトウェアには、off モードを使用して VTP をディセーブルにするオプションがありません。

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 がイネーブル
VTP プルーニング	無効

VTP トランスペアレント モードでは、VTP アップデートは単に無視されます。 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、既知の VTP マルチキャスト MAC アドレスが除去されます このプロトコルではマルチキャスト アドレスが使用されるため、トランスペアレント モードのスイッチ（または他のベンダーのスイッチ）はドメ

イン内の他の Cisco スイッチにフレームを単純にフラッディングします。

VTP バージョン 2（VTPv2）には次の一覧に示す柔軟な機能が含まれています。 ただし、VTPv2 と VTP バージョン 1（VTPv1）を相互運用することはできません。

- トークン リングのサポート。
- 認識されない VTP 情報のサポート。スイッチで解析できない値も伝搬されるようになりました。
- バージョンに依存したトランスペアレント モード。トランスペアレント モードではドメイン名がチェックされなくなりました。 そのため、トランスペアレント ドメインを越えて複数のドメインをサポートできます。
- バージョン番号の伝搬。すべてのスイッチで VTPv2 が使用可能な場合は、1 台のスイッチを設定することですべてのスイッチをイネーブルにできます。

詳細は、『VLAN Trunk Protocol（VTP）について』を参照してください。

Cisco IOS ソフトウェアでの VTP の動作

CatOS の設定変更は、変更直後に NVRAM に書き込まれます。 それとは対照的に、Cisco IOS ソフトウェアでは、**copy run start** コマンドを発行しないと、設定変更が NVRAM に保存されません。 VTP クライアントおよびサーバ システムでは、他の VTP サーバからの VTP アップデートが、ユーザの介入なしにすぐに NVRAM に保存される必要があります。 CatOS のデフォルトの動作は VTP アップデートの要件を満たしますが、Cisco IOS ソフトウェアのアップデート モデルではこれに代わるアップデート動作が必要になります。

この変更のため、Catalyst 6500 用の Cisco IOS ソフトウェアでは VLAN データベースが導入されています。これは、VTP クライアントおよびサーバのための VTP アップデートを即座に保存するために導入されたものです。 一部のソフトウェア バージョンでは、この VLAN データベースは vlan.dat ファイルという個別のファイルの形式で NVRAM に保存されています。 ソフトウェアのバージョンを確認して、VLAN データベースのバックアップが必要かどうかを判断してください。 **show vtp status** コマンドを発行すると、VTP クライアントまたは VTP サーバの vlan.dat ファイルに保存された VTP または VLAN 情報を表示できます。

これらのシステムでは、**copy run start** コマンドを発行しても、NVRAM 内の startup config ファイルにすべての VTP および VLAN 設定が保存されるわけではありません。 この動作は、VTP トランスペアレント モードで稼働しているシステムには該当しません。 VTP トランスペアレント モードのシステムでは、**copy run start** コマンドを発行すると、すべての VTP および VLAN 設定が NVRAM 内の startup config ファイルに保存されます。

Cisco IOS ソフトウェア リリース 12.1(11b)E よりも前の Cisco IOS ソフトウェア リリースでは、VLAN データベース モードでのみ、VTP および VLAN の設定を行えます。 VLAN データベース モードは、グローバル コンフィギュレーション モードとは別のモードです。 このような設定要件が存在する理由は、VTP サーバ モードまたは VTP クライアント モードのデバイスを設定した際に、VTP ネイバーが VTP アドバタイズメントにより VLAN データベースを動的にアップデートする可能性があるからです。 しかし、これらのアップデートが設定に自動的に伝搬されるのは好ましくありません。 そのため、VLAN データベースと VTP 情報は、メインのコンフィギュレーションにではなく、NVRAM 内の vlan.dat ファイルに保存されます。

次の例では、VLAN データベース モードでイーサネット VLAN を作成する方法を示しています。

```
Switch#vlan database Switch(vlan)#vlan 3 VLAN 3 added: Name: VLAN0003 Switch(vlan)#exit APPLY
completed. Exiting....
```

Cisco IOS ソフトウェア バージョン 12.1(11b)E 以降では、VLAN データベース モードとグロー

バル コンフィギュレーション モードのいずれかを使用して VTP と VLAN を設定できます。 VTP モードがサーバ モードまたはトランスペアレント モードになっている場合は、VLAN を設定すると NVRAM 内の vlan.dat ファイルが引き続きアップデートされます。 ただし、これらのコマンドは、コンフィギュレーションには保存されません。 そのため、実行コンフィギュレーションには、これらのコマンドは表示されません。

詳細は、『*VLAN の設定*』の「グローバル コンフィギュレーション モードでの VLAN の設定」セクションを参照してください。

次の例は、グローバル コンフィギュレーション モードでイーサネット VLAN を作成して設定を確認する方法を示しています。

```
Switch#configure terminal Switch(config#vtp mode transparent Setting device to VTP TRANSPARENT
mode. Switch(config#vlan 3 Switch(config-vlan)#end Switch# OR Switch#vlan database
Switch(vlan#vtp server Switch device to VTP SERVER mode. Switch(vlan#vlan 3 Switch(vlan#exit
APPLY completed. Exiting.... Switch#
```

注: VLAN 設定は、不揮発性メモリ内の vlan.dat ファイルに保存されます。 設定を完全にバックアップするには、設定とともに vlan.dat ファイルをバックアップに含める必要があります。 その後、スイッチ全体またはスーパーバイザ エンジン モジュールを交換する必要がある場合は、ネットワーク管理者が次のファイルを両方ともアップロードして、設定全体を回復する必要があります。

- vlan.dat ファイル
- コンフィギュレーション ファイル

VTP と拡張 VLAN

拡張システム ID 機能を使用すると、範囲を拡張した VLAN の識別が可能になります。 拡張システム ID をイネーブルにすると、VLAN スパニング ツリーに使用される MAC アドレス プールがディセーブルになり、スイッチを識別する MAC アドレスが 1 つだけ残ります。 Cisco IOS ソフトウェア リリース 12.1(11b)EX と 12.1(13)E では、Catalyst 6000/6500 用に拡張システム ID が導入されており、IEEE 802.1Q 規格に準拠して 4096 個の VLAN がサポートされます。 Catalyst 4000/4500 スイッチの場合、この機能は Cisco IOS ソフトウェア リリース 12.1(12c)EW で導入されています。 これらの VLAN は複数の範囲で構成されており、それぞれ異なった用途に使用できます。 VTP を使用している場合、これらの VLAN の一部はネットワーク内の他のスイッチに伝搬されます。 拡張範囲の VLAN は伝搬されないので、拡張範囲の VLAN については、ネットワーク デバイスごとに手動で設定する必要があります。 この拡張システム ID 機能は、Catalyst OS の MAC アドレス削減機能に相当します。

VLAN 範囲の説明を次の表に示します。

VLAN	範囲	用途	VTP による伝搬
0、4095	予約済み	システム専用。 これらの VLAN は表示も使用もできません。	
1	Normal	Cisco のデフォルト。 この VLAN は使用できますが、削除できません。	○
2 – 1001	Normal	イーサネット VLAN 用。 これらの VLAN は、作成、使用、および削除が可能です。	○

1002 – 1005	Normal	FDDI およびトークン リング用の Cisco のデフォルト。 1002 ~ 1005 の VLAN は削除できません。	○
1006 – 4094	予約済み	イーサネット VLAN 専用。	なし

スイッチ プロトコルでは、PVST+ および RPVST+ 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 6000/6500 および Catalyst 4000/4500 スイッチでは、シャーシ タイプに応じて 1024 個または 64 個の MAC アドレスがサポートされます。

1024 個の MAC アドレスを持つ Catalyst スイッチの場合、デフォルトでは拡張システム ID はイネーブルになりません。 MAC アドレスは順番に割り当てられます。範囲内の最初の MAC アドレスは VLAN 1 に割り当てられ、範囲内の 2 番目の MAC アドレスは VLAN 2 に割り当てられ、順次同様に割り当てられていきます。 これにより、1024 個の VLAN をスイッチでサポートできるようになり、各 VLAN で一意なブリッジ ID を使用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 アドレスを持つシャーシでは拡張システム ID がデフォルトでイネーブルになり、この機能をディセーブルにすることはできません。

詳細は、『*STP および IEEE 802.1s MST の設定*』の「ブリッジ ID の概要」セクションを参照してください。

1024 個の MAC アドレスを持つ Catalyst シリーズ スイッチの場合、拡張システム ID をイネーブルにすると、スイッチに必要な MAC アドレスの数を増やさずに、PVST+ で動作する 4096 個の VLAN をサポートしたり、16 個の MISTP インスタンスに一意な ID を設定したりできます。 拡張システム ID を使用すると、STP に必要な MAC アドレスの数が、VLAN または MISTP インスタンスごとに 1 つから、スイッチごとに 1 つに減ります。

次の図は、拡張システム ID がイネーブルになっていない場合のブリッジ ID 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。

拡張システム ID では、Bridge Protocol Data Unit (BPDU; ブリッジ プロトコル データ ユニット) の Spanning Tree Protocol (STP; スパニング ツリー プロトコル) ブリッジ ID の部分が変更されます。 オリジナル 2 バイト 優先順位フィールドは 2 フィールドに分割されます; 4 ビット ブリッジ優先順位 フィールドおよび 0-4095 の VLAN 番号を可能にする 12 ビット システム ID 拡張 。

Catalyst スイッチで拡張システム ID をイネーブルにして、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拡張システム ID を有効にする必要があります。 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。 拡張システム ID が有効に なれば、ルートブリッジ 優先順位は VLAN ID と 4096 の倍数になります。 拡張システム ID のないスイッチはブリッジID の選択でより細かい粒状度があるので可能性のあるルートを不注意に要求できます。

同じ STP ドメイン内では拡張システム ID の設定をすべてのデバイスで一致させることを推奨しますが、64 個の MAC アドレスを持つ新しいシャーシを STP ドメインに導入する場合、すべてのネットワーク デバイスで拡張システム ID を適用するのは実用的ではありません。 ただし、2 つのシステムに同じスパニング ツリー プライオリティが設定されている場合、拡張システム ID の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を理解しておくことが重要です。 拡張システム ID の設定をイネーブルにするには、次のコマンドを発行します。

spanning-tree extend system-id

内部 VLAN は、VLAN 1006 から昇順で割り当てられます。 ユーザ VLAN と内部 VLAN の競合を避けるために、ユーザ VLAN は VLAN 4094 にできるだけ近い部分に割り当てることを推奨します。 内部的に割り当てられた VLAN を表示するには、スイッチで **show vlan internal usage** コマンドを発行します。

```
Switch#show vlan internal usage VLAN Usage ---- -------------------- 1006 online diag vlan0 1007
online diag vlan1 1008 online diag vlan2 1009 online diag vlan3 1010 online diag vlan4 1011
online diag vlan5 1012 PM vlan process (trunk tagging) 1013 Port-channel100 1014 Control Plane
Protection 1015 L3 multicast partial shortcuts for VPN 0 1016 vrf_0_vlan0 1017 Egress internal
vlan 1018 Multicast VPN 0 QOS vlan 1019 IPv6 Multicast Egress multicast 1020 GigabitEthernet5/1
1021 ATM7/0/0 1022 ATM7/0/0.1 1023 FastEthernet3/1 1024 FastEthernet3/2 ------deleted------
```

ネイティブ IOS では、内部 VLAN が降順で割り当てられるように **vlan internal allocation policy descending** を設定できます。 これに相当する CatOS ソフトウェアの CLI コマンドは、正式にはサポートされていません。

vlan internal allocation policy descending

Cisco の推奨する設定

Catalyst 6500/6000 が VTP サーバ モードで動作しているときは、VTP ドメイン名がなくても VLAN を作成できます。 Cisco IOS システム ソフトウェアが稼働している Catalyst 6500/6000 で VLAN を設定する場合は、まず VTP ドメイン名を設定してください。 この順序で設定を行うことにより、CatOS が稼働している他の Catalyst スイッチとの整合性を維持できます。

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。 一部のお客様は、このセクションに記載されている推奨事項よりも、管理の容易さを重視して VTP クライアント/サーバ モードを使用しています。 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クライアント モードに設定します。 VTPv2 を使用してクライアント/サーバ モードを実装する場合、同じ VTP ドメインでは、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 クライアント モードまたはサーバ 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。 この設定変更が意図どおりのものではなく、VLAN が削除された場合は、この上書きによって大規模なネットワーク障害が発生する可能性があります。 クライアント スイッチまたはサーバ スイッチの設定リビジョン番号がサーバの設定リビジョン番号よりも常に低くなるようにするには、クライアントの VTP ドメイン名を標準以外の名前に変更してから、再び標準の名前に戻します。 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、注意深いアプローチが好まれるため、VTP transparent モードが使用されています。

- スイッチまたはトランク ポート上の VLAN 変更要件を 1 台のスイッチごとに検討する必要があるため、この方法では適切な変更管理が実践できる。
- VTP トランスペアレント モードを使用すると、誤って VLAN を削除するなどの管理上のミスが少なくなる。 そのようなミスは、ドメイン全体に影響を及ぼす可能性があります。
- VLAN をトランクからプルーニングして、その VLAN 内にポートを持たないスイッチに戻すことができる。 その結果、フレーム フラッディング時の帯域幅効率が向上します。 また、手動でプルーニング (削除) することにより、スパニングツリーの直径が小さくなります。 詳細は、「ダイナミック トランキング プロトコル」セクションを参照してください。 この方法は、スイッチごとに VLAN を設定する場合にも効果的です。
- 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。
- Cisco IOS ソフトウェアの VTP トランスペアレント モードは、CiscoWorks2000 の一部である Campus Manager 3.2 でサポートされています。 VTP ドメイン内に少なくとも 1 台のサーバを必要とする以前の制約はすでに解消されています。

VTP コマンド	**コメント**
VTP ドメイン *名*	CDP では、ドメイン間の配線のミスを防止するために名前が確認されます。 ドメイン名の大文字と小文字は区別されます。
VTP モード{サーバ | client | 透過的な}	VTP は、3 つのモードのいずれかで動作します。
vlan *vlan_number*	指定した ID を持つ VLAN が作成されます。
switchport trunk allowed *vlan_ra*	必要に応じて VLAN をトランク経由で伝送するためのインターフェイス コマンドです。 デフォルトはすべての VLAN です。

nge	
switchport trunk pruning *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手動プルーニングを行うことにより、STP の直径を制限するインターフェイス コマンドです。 デフォルトでは、すべての VLAN がプルーニングの対象になります。

その他のオプション

VTPv2 はトークン リング環境では必須要件であり、クライアント/サーバ モードを使用することが強く推奨されます。

このドキュメントの「Cisco の推奨する設定」セクションでは、VLAN をプルーニングすることで不要なフレーム フラッディングを削減できるという利点を挙げています。 **vtp pruning** コマンドを設定すると VLAN が自動的にプルーニングされ、必要とされていない場所へのフレームの非効率的なフラッディングが回避されます。

注: 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。

IEEE により、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が策定されています。 Generic VLAN Registration Protocol（GVRP）は、802.1Q Generic Attribute Registration Protocol（GARP）のメンバであり、異なるベンダー間における VLAN 管理の相互運用を可能にします。 ただし、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: Cisco IOS ソフトウェアには VTP オフ モードの機能がなく、プルーニング機能を含む VTPv2 と VTPv1 のみがサポートされています。

ファスト イーサネットの自動ネゴシエーション

目的

自動ネゴシエーションは、IEEE 802.3u ファスト イーサネット（FE）規格のオプション機能です。 自動ネゴシエーションを使用すると、速度とデュプレックスに関する情報を、デバイス間のリンク経由で自動的に交換できます。 自動ネゴシエーションは、レイヤ 1（L1）で動作します。 この機能は、一時的なユーザやデバイスがネットワークに接続するために使用する領域に割り当てられるポートを対象としています。 たとえば、アクセス層のスイッチやハブなどがこれに該当します。

動作の概要

自動ネゴシエーションでは、10BASE-T デバイスで使用されるリンク完全性テストの修正版を使用して、速度のネゴシエーションと他の自動ネゴシエーション パラメータの交換が行われます。 元の 10BASE-T リンク完全性テストは、Normal Link Pulse（NLP; ノーマル リンク パルス）と呼ばれています。 10/100 Mbps の自動ネゴシエーション用に修正されたリンク完全性テストは、Fast Link Pulse（FLP; ファスト リンク パルス）と呼ばれています。 10BASE-T デバイスでは、リンク完全性テストの一環として 16（+/-8）ミリ秒ごとにバースト パルスが発生することが想定されています。 10/100 Mbps の自動ネゴシエーション用の FLP では、これらの 16（+/-8）ミリ秒ごとのバーストに加えて、62.5（+/-7）マイクロ秒ごとにもパルスが送信されます。 バースト

シーケンス内のパルスによって、リンク パートナー間の互換性情報の交換に使用されるコード ワードが生成されます。

10BASE-T では、ステーションが起動するたびにリンク パルスが送出されます。 これは 16 ミリ秒毎に送信 される 単一パルスです 10BASE-T デバイスはまた 16 ms 毎にリンク パルスをリンクがアイドル状態である送信 します。 これらのリンク パルスは、ハートビートまたは NLP とも呼ばれます。

100BASE-T デバイスでは、FLP が送出されます。 このパルスは、1 つのパルスではなく、バーストとして送出されます。 このバーストは 2 ミリ秒以内に完了し、16 ミリ秒ごとに繰り返されます。初期化が完了すると、デバイスから 16 ビットの FLP メッセージがリンク パートナーに送信されて、速度、デュプレックス、フロー制御のネゴシエーションが行われます。 この 16 ビットのメッセージは、パートナーからの確認応答があるまで、繰り返し送信されます。

注: IEEE 802.3u の仕様によれば、一方のリンク パートナーを 100 Mbps 全二重に手動で設定した場合、もう一方のリンク パートナーが自動ネゴシエーションによって全二重に設定されることはありません。 一方のリンク パートナーを 100 Mbps 全二重に設定して、もう一方のリンク パートナーを自動ネゴシエーションに設定しようとすると、デュプレックスのミスマッチが発生します。 ディプレックスのミスマッチが生じる原因は、一方のリンク パートナーで自動ネゴシエーション プロセスが開始されても、もう一方のリンク パートナーから自動ネゴシエーション パラメータが送信されないためです。 この場合、最初のリンク パートナーはデフォルトで半二重に設定されます。

Catalyst 6500 のすべてのイーサネット スイッチング モジュールでは、10/100 Mbps および半二重または全二重がサポートされています。 この機能を他の Catalyst スイッチで確認するには、**show interface capabilities** コマンドを発行します。

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の 1 つは、リンクの一方のポートが半二重で動作し、もう一方のポートが全二重で動作していることです。 この状態は、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、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この状況が発生します。 次の作業を行えば、パフォーマンス関連のサポート コールが不要になります。

- すべての非一時的デバイスに対して必要な動作を実行するためにポートの設定を要求するポリシーを作成する
- 十分な変更管理対策を講じた上で上記ポリシーを適用する

パフォーマンス問題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）、アライメント、ラントの各カウンタの増加が挙げられます。

半二重モードには、一対の受信ワイヤと一対の送信ワイヤが存在します。 両方のワイヤを同時に使用することはできません。 受信側にパケットがあるときは、デバイスからパケットを送信できません。

同様に、全二重モードにも、一対の受信ワイヤと送信ワイヤが存在します。 ただし、キャリア検知機能と衝突検出機能がディセーブルになっているので、両方のワイヤを同時に使用できます。 デバイスは送受信を同時に行えます。

そのため、半二重から全二重への接続は可能ですが、半二重側で大量の衝突が発生するためパフォーマンスの低下を招きます。 このような衝突が発生する原因は、全二重に設定されたデバイスがデータの送受信を同時に行えるためです。

自動ネゴシエーションについての詳細は、次のドキュメントを参照してください。 これらのドキュメントでは、自動ネゴシエーションの動作方法とさまざまな設定オプションが説明されています。

- イーサネット 10/100/1000 Mb 半二重/全二重オート ネゴシエーションの設定とトラブルシューティング
- 「Troubleshooting Cisco Catalyst Switches to NIC Compatibility Issues（Cisco Catalyst スイッチと NIC との互換性に関する問題のトラブルシューティング）」

自動ネゴシエーションでは、一方のリンク パートナーを 100 Mbps 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 パラメータを受信できず、デフォルトで半二重に設定されることが原因です。

ほとんどの Catalyst イーサネット モジュールでは、10/100 Mbps および半二重/全二重がサポートされています。 **show interface *mod/port* capabilities** コマンドを発行すると、このことを確認できます。

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、一方のステーションでは検出できるものの、もう一方のステーションでは検出できない種類のリンク エラーです。 その一例として、送信ワイヤが接続されていない場合などがあります。 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。 しかし、送信側ステーションでは、もう一方のステーションで送信内容が受信されていないことを検出できません。 そのようなリモート障害を検出した 100BASE-FX ステーションは、ネイバーにリモート障害を通知するために、IDLE ストリームを修正して特別なビットパターンを送信できます。 この特別なビット パターンは、FEFI-IDLE パターンと呼ばれます。 FEFI-IDLE パターンが届くと、リモート ポートがシャットダウンされます（errDisable）。 障害保護についての詳細は、このドキュメントの「単方向リンク検出」セクションを参照してください。

FEFI をサポートしているモジュールおよびハードウェアは次のとおりです。

- 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

Cisco のインフラストラクチャ ポートに関する推奨事項

10/100 Mbps リンクで自動ネゴシエーションを設定するか、速度とデュプレックスを固定設定するかは、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、Network Interface Card（NIC; ネットワーク インターフェイス カード）やベンダーのスイッチがこの仕様に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。 さらに、10/100 Mbps 自動ネゴシエーションに関する IEEE 802.3u 仕様で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。 そのような高度な機能には、自動極性切り替えや配線の完全性などがあります。 次のドキュメントに例が

記載されています。

- フィールド警告: Intel Pro/1000T NIC が CAT4K/6K に接続している場合のパフォーマンスの問題

状況によっては、ホスト、ポート速度、デュプレックスを設定する必要があります。 一般には、次の基本的なトラブルシューティング手順を実行します。

- リンクの両端で自動ネゴシエーションが設定されているか、リンクの両端で固定設定が行われていることを確認します。
- リリース ノートの一般的な注意事項をチェックします。
- NIC ドライバのバージョンや、稼働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。 また、自動ネゴシエーションは、次のようなリンクでも適切に動作します。

- サーバや固定されたワークステーションなどの非一時的デバイスとのリンク
- スイッチからスイッチへのリンク
- スイッチからルータへのリンク

ただし、このセクションで説明した理由により、ネゴシエーションの問題が生じる場合があります。 そのような問題が発生した場合の基本的なトラブルシューティング手順については、『イーサネット 10/100/1000Mb 半二重/全二重オートネゴシエーションの設定とトラブルシューティング』を参照してください。

次のポートでは、自動ネゴシエーションをディセーブルにします。

- スイッチやルータなどのネットワーク インフラストラクチャ デバイスをサポートするポート
- その他の非一時的エンド システム（サーバやプリンタなど）のポート

これらのポートでは常に、速度とデュプレックスを固定設定する必要があります。

次の 10/100 Mbps リンクでは、速度とデュプレックスを手動で設定してください（通常は 100 Mbps 全二重）。

- スイッチからスイッチへのリンク
- スイッチからサーバへのリンク
- スイッチからルータへのリンク

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、次のインターフェイス コマンドを発行します。

```
Switch(config)#interface fastethernet slot/port Switch(config-if)#speed auto !--- This is the default.
```

速度とデュプレックスを設定するには、次のインターフェイス コマンドを発行します。

```
Switch(config)#interface fastethernet slot/port Switch(config-if)#speed {10 | 100 | auto}
Switch(config-if)#duplex {full | half}
```

Cisco のアクセス ポートに関する推奨事項

エンド ユーザ、モバイル ワーカー、および一時的なホストに対しては、これらのホストの管理を

最小限に抑えるために自動ネゴシエーションを設定する必要があります。 自動ネゴシエーションは Catalyst スイッチに対しても機能します。 多くの場合、最新の NIC ドライバが必要です。

ポート速度の自動ネゴシエーションをイネーブルにするには、次のグローバル コマンドを発行します。

```
Switch(config)#interface fastethernet slot/port Switch(config-if)#speed auto
```

注: 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。 自動ネゴシエーション ポートのデュプレックス モードを変更することはできません。

NIC やベンダーのスイッチが IEEE 802.3u 仕様に厳密に準拠していない場合、障害が発生することがあります。 さらに、10/100 Mbps 自動ネゴシエーションに関する IEEE 802.3u 仕様で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。 そのような高度な機能には、自動極性切り替えや配線の完全性などがあります。

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がディセーブルになっている場合は、ある種の問題に関するレイヤ 1 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 などのレイヤ 2 プロトコルを使用します。

自動ネゴシエーションがイネーブルになっていても、次の状態は自動ネゴシエーションでは検出されません。

- ポートが正常に動作しておらず、送受信が行われていない
- 回線の一方が up なのに、もう一方が down のままである
- ファイバ ケーブルが正しく配線されていない

これらの問題は物理層で発生していないので、自動ネゴシエーションでは検出されません。 これらの問題は、STP ループやトラフィックのブラックホールの原因となる可能性があります。

UDLD では、これらすべてのケースを検出でき、リンクの両端で UDLD が設定されている場合は、リンクの両方のポートが errdisable 状態になります。 このようにして、UDLD では、STP ループやトラフィックのブラックホールが防止されます。

ギガビット イーサネットの自動ネゴシエーション

目的

ギガビット イーサネット (GE) では、10/100 Mbps イーサネット (IEEE 802.3z) で使用される手順よりも高度な自動ネゴシエーション手順が実行されます。 GE ポートでは、自動ネゴシエーションを使用して次の情報が交換されます。

- フロー制御パラメータ
- リモート障害情報
- デュプレックス情報**注:** Catalyst シリーズの GE ポートでは、全二重モードのみがサポートされています。

IEEE 802.3z はすでに IEEE 802.3:2000 仕様で置き換えられています。 詳細は、『Local and Metropolitan Area Networks + Drafts (LAN/MAN 802s) Standards Subscription』 を参照してください。

動作の概要

10/100 Mbps FE の自動ネゴシエーションとは異なり、GE の自動ネゴシエーションにはポート速度のネゴシエーションは含まれていません。 また、**set port speed** コマンドを発行して自動ネゴシエーションをディセーブルにすることもできません。 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。 リンクの両端のポートで設定が一致しない場合（つまり、交換されるパラメータが異なる場合）は、リンクがアップしません。

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。 次の表に、可能な設定とそれぞれのリンク状態を示します。

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ますが、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ディセーブルになると、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: ただし、GE ファイバ仕様では、デュプレックス、フロー制御、およびリモート障害検出のネゴシエーションしか規定されていません。 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。 **sync-restart-delay** コマンドは、自動ネゴシエーションが enable に設定されている場合にのみ機能します。

Cisco のインフラストラクチャ ポートに関する推奨事項

GE 環境での自動ネゴシエーションの設定は、10/100 Mbps 環境での設定よりもはるかに重要です。 自動ネゴシエーションをディセーブルにするのは、次の場合だけにしてください。

- ネゴシエーションをサポートしていないデバイスにスイッチ ポートが接続されている場合
- 相互運用性の問題により接続の問題が生じている場合

ギガビット ネゴシエーションは、すべてのスイッチ間リンクおよび（通常は）すべての GE デバイスでイネーブルにしてください。 ギガビット インターフェイスでのデフォルト値は自動ネゴシエーションです。 次のコマンドを発行すると、自動ネゴシエーションがイネーブルになっていることを確認できます。

```
switch(config)#interface type slot/port switch(config-If)#no speed !--- This command sets the port to autonegotiate Gigabit parameters.
```

既知の例外の 1 つとして、Cisco IOS ソフトウェア 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）よりも前の 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）に接続する場合があります。 この場合は、これら 2 つの機能をオフにします。 これらの機能をオフにしないと、スイッチ ポートの状態が not connected と報告され、GSR によりエラーが報告されます。 次にインターフェイス コマンド シーケンスの例を示します。

```
flowcontrol receive off flowcontrol send off speed nonegotiate
```

Cisco のアクセス ポートに関する推奨事項

FLP はベンダーごとに異なる可能性があるので、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。 Cisco 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。 NIC ベンダーから特に指示がない限り、すべてのデバイスでギガビット自動ネゴシエーションを使用してください。

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。 フロー制御を使用する場合はネゴシエーションが必要です。 デバイスの中には、PAUSE フレーム（既知の MAC 01-80-C2-00-00-00 0F）の送信や応答に対応しているものと、対応していないものがあります。 さらに、遠端のネイバーのフロー制御要求に同意できないデバイスもあります。 入力バッファが満杯になりつつあるポートからは、リンク パートナーに PAUSE フレームが送信されます。 これにより、リンク パートナーからの転送が停止し、残りのフレームはリンク パートナーの出力バッファ内に保持されます。 この機能によって定常状態のオーバーサブスクリプションの問題が解決することはありません。 ただし、バースト時にパートナーの出力バッファの一部が使用されることにより、入力バッファが実質的に拡大することになります。

PAUSE 機能は、短期的で一時的なトラフィックの過負荷によるバッファ オーバーフロー状態のために、デバイス（スイッチ、ルータ、またはエンド ステーション）で受信されたフレームが不必要に廃棄されるのを防止することを目的としています。 トラフィックの過負荷の状態にあるデバイスでは、PAUSE フレームを送信することにより、内部バッファのオーバーフローを防止できます。 PAUSE フレームには、全二重のパートナーが新しいデータ フレームを送信するまで待機する期間を指定するパラメータが含まれています。 PAUSE フレームを受信したパートナーでは、指定された期間、データ フレームの送信が中断されます。 このタイマーの期間が経過すると、中断した時点からデータの送信が再開されます。

PAUSE を発行したステーションでは、期間パラメータをゼロに設定した新しい PAUSE フレームを送信できます。 これにより、残りの PAUSE 期間をキャンセルできます。 つまり、現在進行中のすべての PAUSE 処理が無効になり、新たに受信された PAUSE フレームが優先されます。

また、PAUSE フレームを発行したステーションは、PAUSE 期間を延長することもできます。その場合は、最初の PAUSE 期間が経過する前に、期間パラメータをゼロ以外の値に設定した新しい PAUSE フレームを発行します。

この PAUSE 処理は、レート ベースのフロー制御ではありません。 この操作は、トラフィックが多いために PAUSE フレームを送信したデバイスに、バッファの輻輳を軽減する機会を与えるための単純な開始/停止メカニズムです。

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効果的です。このリンクでは、エンド ホストの出力バッファが仮想メモリと同じサイズに設定されている可能性があります。 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、次のインターフェイス コマンドを発行します。

```
flowcontrol {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

目的

トランクでは、デバイス間の VLAN を拡張するために、元のイーサネット フレームが一時的に識別されてタグ付け (リンクローカル) されます。 この動作により、フレームを単一のリンク上で多重化できるようになります。 また、この動作により、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。

動作の概要

DTP は第 2 世代の Dynamic ISL (DISL) です。 DISL では ISL のみがサポートされていました。DTP では、ISL と 802.1Q の両方がサポートされています。 このサポートにより、トランクの両端にあるスイッチが、トランキング フレームのさまざまなパラメータに関して合意できるようになります。 たとえば、次のようなパラメータがあります。

- 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

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は深刻なセキュリティ リスクにつながる可能性がありますが、DTP はこの問題を回避する上でも役立ちます。 DTP を使用すると、ポートとネイバーの状態の整合性を保てるので、このようなフラッディングを防止できます。

トランキング モード

DTP は、スイッチ ポートとそのネイバーとの間で設定パラメータをネゴシエートするレイヤ 2 プロトコルです。 DTP では、別の既知のマルチキャスト MAC アドレスである 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、設定可能な DTP ネゴシエーション モードと、それぞれの機能を示します。

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)
Dynamic Auto (CatOS では Auto モードに相当)	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。	はい、定期的	
Trunk (CatOS では ON モードに相当)	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。	はい、定期的	トランキング (無条件)
`Nonegotiate`	ポートは常に trunking モードになりますが、DTP フレームは生成されません。 トランク リンクを確立するには、隣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)

Dynamic desirable（CatOS では desirable コマンドに相当）	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。	はい、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。
access	ポートは常に non-trunking モードになり、リンクを非トランク リンクに変換するかどうかをネゴシエートします。 隣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。	安定状態では送信しない。ただし、on から変更されたときは、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。	

注: 設定またはネゴシエートが可能なカプセル化タイプは、ISL と 802.1Q です。

デフォルト設定の場合、DTP では、リンクに次の特性があると仮定されます。

- ポイントツーポイント接続および Cisco デバイスでは、ポイントツーポイントの 802.1Q トランク ポートのみがサポートされます。
- DTP ネゴシエーションの間、ポートは STP に参加しません。 ポート タイプが次の 3 タイプのいずれかになって初めて、ポートは STP に追加されます。accessISL802.1Qポートが STP に参加する前に実行される次のプロセスは PAgP です。 PAgP は EtherChannel の自動ネゴシエーションに使用されます。
- VLAN 1 は、常にトランク ポート上に存在します。 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。 ポートが ISL モードでトランキングしていない場合（802.1Q のトランキング ポートまたは非トランキング ポート ポートの場合）は、ネイティブ VLAN に DTP パケットが送出されます。
- DTP パケットは、VTP ドメイン名に加えて、トランク設定と admin status を転送します。ネゴシエートされたトランクが起動するためには、VTP ドメイン名が一致している必要があります。 これらのパケットは、ネゴシエーション中は 1 秒間隔で送信され、ネゴシエーション後は 30 秒間隔で送信されます。 auto または desirable モードのポートは、DTP パケットを 5 分間検出しなかった場合、非トランクに設定されます。

注意： どの状態をポートが行きつかせるかモードがで、`nonegotiate` 理解して下さい、明示的に規定 しますことを。 設定が不適切な場合は、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なるおそれがあります。

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。

カプセル化タイプ

ISL の動作の概要

ISL は Cisco 独自のトランキング プロトコル（VLAN タギング方式）です。 ISL は、長年使用されてきました。 これに対して、802.1Q は最近の仕様ですが、IEEE 標準です。

ISL では 2 レベルのタギング方式で元のフレームが完全にカプセル化されます。 そのため、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。 そのため、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。

フレーム形式（ISL タグは灰色で表示）

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 規格の適用範囲はイーサネットのみですが、この規格ではカプセル化タイプ以外にも多くの事項が定義されています。 802.1Q には、他の Generic Attribute Registration Protocol（GARP）に加えて、スパニングツリーの拡張機能や、802.1p の QoS タギング機能も含まれています。 詳細は、『IEEE Standards Online』 を参照してください。

802.1Q フレーム形式では、元のイーサネット SA と DA が保持されます。 ただし、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しておく必要があります。 このタグは 4 バイトです。 そのため、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 グループにより策定されたものです。 802.1Q では、4096 個の VLAN に対応する番号領域もサポートされています。

送受信されるすべてのデータ フレームには、802.1Q タグが付けられます。ただし、ネイティブ VLAN 上のデータ フレームは例外です。 この場合は、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 上のフレームは常にタグなしで送信され、通常はタグなしで受信されます。 ただし、これらのフレームがタグ付きで受信される場合もあります。

詳細は、次のドキュメントを参照してください。

- VLAN の相互運用性
- IEEE 802.1Q 方式を使用した Catalyst 4000 5000 6000 スイッチ間のトランキング

802.1Q/802.1p フレーム形式

Cisco の推奨する設定

Cisco で重視されている設計原則の 1 つは、可能な限りネットワークの整合性を高めることです。 最近のすべての Catalyst 製品では 802.1Q がサポートされていますが、一部の製品（Catalyst 4500/4000 および Catalyst 6500 シリーズの以前のモジュールなど）では 802.1Q のみがサポートされています。 そのため、新しく実装するシステムではすべて IEEE 802.1Q 規格に準拠し、古いネットワークを ISL から徐々に移行する必要があります。

特定のポートで 802.1Q トランキングをイネーブルにするには、次のインターフェイス コマンドを発行します。

```
Switch(config)#interface type slot#/port# Switch(config-if)#switchport !--- Configure the interface as a Layer 2 port. Switch(config-if)#switchport trunk encapsulation dot1q
```

IEEE 規格では異なるベンダー間の相互運用が可能です。 802.1p 対応の新しいホスト NIC やデバイスが使用可能になるため、ベンダー間の相互運用性は、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 の実装はどちらも安定していますが、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。 また、802.1Q のカプセル化のオーバーヘッドは ISL に比べて小さいですが、これは利点としてはそれほど大きなものではありません。

完全を期すためには、ネイティブ VLAN で暗黙的なタギングを行うことには、セキュリティ面の考慮が必要になります。 1 つの VLAN（VLAN X）から別の VLAN（VLAN Y）に、ルータを介さずにフレームが転送される可能性があります。 発信元ポート（VLAN X）が同じスイッチの 802.1Q トランクのネイティブ VLAN と同じ VLAN にある場合は、ルータを介さずにフレームが転送される可能性があります。 この問題を回避するには、トランクのネイティブ VLAN としてダミーの VLAN を使用します。

特定のポートで特定の VLAN を 802.1Q トランキング用のネイティブ（デフォルト）VLAN として確立するには、次のインターフェイス コマンドを発行します。

```
Switch(config)#interface type slot#/port# Switch(config-If)#switchport trunk native vlan 999
```

最近のハードウェアはすべて 802.1Q をサポートしているため、新しく実装するシステムはすべて IEEE 802.1Q 規格に準拠させるようにして、以前のネットワークを ISL から徐々に移行してください。 最近まで、多くの Catalyst 4500/4000 モジュールでは、ISL がサポートされていませんでした。 そのため、イーサネットのトランキングに使用できる方式は 802.1Q のみでした。 **show interface capabilities** コマンドの出力、または（CatOS の場合は）**show port capabilities** コマンドの出力を参照してください。 トランキングをサポートするには適切なハードウェアが必要になるため、802.1Q をサポートしないモジュールを使用している場合は、802.1Q をサポートできません。 ソフトウェアをアップグレードしても 802.1Q をサポートできるようにはなりません。 Catalyst 6500/6000 スイッチおよび Catalyst 4500/4000 スイッチ用の新しいハードウェアでは、ほとんどの場合、ISL と 802.1Q の両方がサポートされています。

「スイッチ管理インターフェイスとネイティブ VLAN」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、制御プロトコルは NMP によって引き続き VLAN 1 上で転送されます。 そのような制御プロトコルには、CDP や VTP などがあります。

また、「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 に送出されます。 dot1q（802.1Q）カプセル化を使用している場合、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あり、スイッチでネイティブ VLAN が変更された場合は、タグ付き CDP フレームを受信してルータに 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: ネイティブ VLAN の暗黙的なタギングが原因で、dot1q に関連するセキュリティ上の問題が発

生する可能性があります。 1 つの VLAN から別の VLAN に、ルータを介さずにフレームが転送される可能性があります。 詳細は、『Intrusion Detection FAQ』を参照してください。 回避策はエンドユーザ アクセスのために使用しないトランクのネイティブ VLAN のために VLAN ID を使用することです。 Cisco のほとんどのお客様では、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簡単な方法でこの問題が解決されています。

Cisco では、リンクの両端でトランク モードを明示的に dynamic desirable に設定することを推奨しています。 このモードは、デフォルトのモードです。 このモードでは、ネットワーク オペレータは、ポートが up 状態でありトランキングが行われているという 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。 このモードは、on モードとは異なります。on モードでは、ネイバーの設定が正しくない場合でも、ポートがアップ状態であると報告される場合があります。 また、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、trunk 状態でなくなった場合にも、安定して動作します。

スイッチ間で DTP を使用してカプセル化タイプがネゴシエートされている場合、両端で ISL がサポートされていると、デフォルトで ISL が選択されます。この場合、dot1q1 を指定するには、次のインターフェイス コマンドを発行する必要があります。

switchport trunk encapsulation *dot1q*

1 WS-X6548-GE-TX や WS-X6148-GE-TX などのモジュールでは、ISL トランキングがサポートされていません。 これらのモジュールでは、**switchport trunk encapsulation *dot1q*** コマンドが受け付けられません。

注: ポート上のトランクをディセーブルにするには、**switchport mode access** コマンドを発行します。 トランクをディセーブルにすると、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。

Switch(config-if)#**switchport host**

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は、ディストリビューション レイヤで dynamic 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（dynamic auto モード）を使用する方法があります。 現在のところ、Catalyst 2900XL などの一部のスイッチ、Cisco IOS ルータ、または他のベンダーのデバイスでは、DTP によるトランク ネゴシエーションはサポートされていません。 この場合は、nonegotiate モードを使用すると、それらのデバイスに対して無条件にポートをトランクに設定できます。 このモードは、キャンパス全体を共通の設定で標準化するのに便利な場合があります。

Cisco IOS ルータに接続する場合は、nonegotiate を使用することを推奨します。 ブリッジング中に、**switchport mode trunk** で設定したポートから受信された 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ります。 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。 再ネゴシエートを行うために、スイッチ ポートはトランクをいったん down 状態にしてから再度 up 状態にします。 nonegotiate が有効な場合、スイッチは DTP フレームを送信しません。

switch(config)#**interface type** *slot#/port#* switch(config-if)#**switchport mode dynamic desirable** *!--- Configure the interface as trunking in desirable !--- mode for switch-to-switch links with multiple VLANs. !--- And...* switch(config-if)#**switchport mode trunk** *!--- Force the interface into trunk mode without negotiation of the trunk connection. !--- Or...* switch(config-if)#**switchport nonegotiate** *!--- Set trunking mode to not send DTP negotiation packets !--- for trunks to routers.* switch(config-if)#**switchport access vlan** *vlan_number !--- Configure a fallback VLAN for the interface.* switch(config-if)#**switchport trunk native vlan 999** *!--- Set the*

native VLAN. switch(config-if)#**switchport trunk allowed vlan** *vlan_number_or_range !--- Configure the VLANs that are allowed on the trunk.*

スパニング ツリー プロトコル

目的

スパニング ツリーは、冗長構成のスイッチド 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レイヤ 2 環境を維持します。 STP がないと、フレームがループするか、限りなく増殖することになります。 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の動作が中断されることになるため、ネットワークのメルトダウンが発生します。

元々、STP はソフトウェアベースの低速なブリッジ仕様（IEEE 802.1D）向けに開発されているため、旧式のプロトコルという側面があります。 ただし、次のような条件に該当する大規模なスイッチド ネットワークでも確実に実装できる複雑さも STP は兼ね備えています。

- 多数の VLAN
- ドメイン内に多数のスイッチが存在する
- マルチベンダー サポートが必要
- より新しい IEEE 機能拡張

Cisco IOS システム ソフトウェアには、STP の新たな発展が取り入れられています。 802.1w Rapid STP や 802.1s Multiple Spanning Tree などの新しい IEEE 標準プロトコルでは、高速コンバージェンス、ロード シェアリング、コントロール プレーンのスケーリングなどがサポートされています。 さらに、RootGuard、BPDU フィルタリング、PortFast BPDU ガード、ループガードなどの STP 拡張機能により、レイヤ 2 フォワーディング ループに対する保護がいっそう強化されています。

PVST+ の動作の概要

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に、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。 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、ルート情報を含む BPDU が送出されます。

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 blocking 状態になります。

詳細は、次のドキュメントを参照してください。

- STP および IEEE 802.1s MST の設定

- 高速スパニングツリー プロトコル（802.1w）について

基本タイマーのデフォルト	名前	機能
2 秒	hello	BPDU の送信を制御します。
15 秒	転送遅延（Fwddelay）	ポートが listening 状態または learning 状態にとどまる時間の長さを制御し、トポロジ変更プロセスに影響を与えます。
20 秒	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、代替パスの検索がスイッチにより開始されます。 最大エージング（maxage）時間が経過すると、BPDU は期限切れになったものとみなされ、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。

安定性に悪影響を及ぼすおそれがあるため、タイマーの値は変更しないことを推奨します。 実際に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。 詳細は、「単方向リンク検出」セクションを参照してください。

STP タイマーに関する注：

デフォルトの STP タイマー値は、ネットワークの直径が 7 台のスイッチから構成されている（つまり、ルートからネットワーク エッジまでのスイッチ ホップ数が 7 である）と仮定した計算と、ルート ブリッジから 7 ホップ先にあるネットワークのエッジ スイッチに BPDU を転送するために必要な時間に基づいて設定されています。 この仮定に基づくと、ほとんどのネットワークで許容可能なタイマー値が算出されます。 ただし、ネットワーク トポロジ変更時のコンバージェンス時間を短縮するために、これらのタイマーをさらに最適な値に変更することもできます。

ルート ブリッジで特定の VLAN のネットワーク直径を設定すると、それに従ってタイマー値が計算されます。 変更が必要な場合は、VLAN のルート ブリッジで diameter パラメータとオプションの hello-time パラメータのみを設定することを推奨します。

```
spanning-tree vlan vlan-id [root {primary | secondary}] [diameter diameter-value [hello hello-time]] !--- This command needs to be on one line.
```

このマクロを実行すると、このスイッチが VLAN のルートになり、指定した直径と hello タイムに基づいて新しいタイマー値が計算され、この情報を含む設定 BPDU がトポロジ内の他のすべてのスイッチに伝播されます。

802.1D STP の詳細、および 802.1D STP と Rapid STP（RSTP）の比較については、「新しいポートの状態とポートの役割」セクションを参照してください。 RSTP についての詳細は、『

Rapid Spanning Tree Protocol（802.1w）の概要』を参照してください。

新しいポートの状態とポートの役割

802.1D では、次の 4 つのポート状態が定義されています。

- リスニング
- ラーニング
- Blocking（ブロッキング）
- フォワーディング

詳細は、「ポート状態」セクションの表を参照してください。 アクティブなトポロジでポートが果たす役割（ルート ポート、指定ポートなど）と同様に、ポートの状態（トラフィックをブロックするか転送するか）も複雑に入り混じっています。 たとえば、動作上の観点からは、blocking 状態と listening 状態のポートに違いはありません。 どちらの状態でも、フレームは廃棄され、MAC アドレスは学習されません。 実際の違いは、スパニング ツリーによってポートに割り当てられる役割にあります。 listening 状態のポートは、指定ポートまたはルート ポートのいずれかであり、forwarding 状態に移行する途上にあると考えて間違いありません。 残念ながら、いったん forwarding 状態になった後は、ポートの状態から、そのポートがルート ポートであるか指定ポートであるかを推測できなくなります。 この点は、状態ベースのテクノロジーの欠点です。 RSTP では、ポートの役割と状態が切り離されているので、この欠点は解消されています。

ポートの状態

STP 802.1D のポート状態

ポート状態	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。	
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。直接または口ーカルのリンク障害が検出された場合は即座に変更されます。
	BPDU を送受信し、blocking 状態に戻る必要があるかをチェックする。	Fwddelay が経過するまで 15 秒待ちます。
	トポロジおよび CAM テーブルを構築する。	Fwddelay が経過するまで 15 秒待ちます。
	データを送受信する。	

基本的なトポロジ変更に要する合計時間は次のとおりです。

- 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が発生した場合は、30 秒

RSTP に残されているポート状態は 3 種類だけであり、起こりうる 3 つの動作状態にそれぞれ対応しています。 802.1D の disabled、blocking、listening の各状態は、802.1w 独自の discarding 状態に統合されています。

STP（802.1D）のポート状態	RSTP（802.1w）のポートの状態	ポートはアクティブなトポロジに含まれるか	ポートは MAC アドレスを学習するか。
無効	Discarding	なし	なし
Blocking（ブロッキング）	Discarding	なし	なし
リスニング	Discarding	○	なし
ラーニング	ラーニング	○	○
フォワーディング	フォワーディング	○	○

ポートの役割

役割は、特定のポートに割り当てられる変数として扱われるようになりました。 ルート ポートと指定ポートの役割に変更はありませんが、ブロッキング ポートの役割は 2 つの役割（バックアップ ポートと代替ポート）に分割されました。 ポートの役割は、BPDU に基づき Spanning Tree Algorithm（STA; スパニング ツリー アルゴリズム）で決定されます。 議論を簡素化するために、BPDU については次の点を覚えておいてください。 2 つの BPDU を比較して、どちらの方が有用であるかを決定する方法は常に存在します。 この決定の根拠になるのは、BPDU に保存されている値ですが、ときには、BPDU が受信されたポートが根拠になる場合もあります。 以後、このセクションでは、ポートの役割に対する実用的なアプローチについて説明します。

ルート ポートの役割

ブリッジ上で最良の BPDU を受け取るポートがルート ポートになります。 つまり、パス コストの点からルート ブリッジに最も近いポートです。 STA では、ブリッジ型ネットワーク全体から（VLAN ごとに）1 つのルート ブリッジが選出されます。 ルート ブリッジが送信する BPDU は、他のブリッジが送信するものより有用です。 ルート ブリッジは、ネットワーク内でルート ポートを持たない唯一のブリッジです。 他のすべてのブリッジは、少なくとも 1 つのポートで BPDU を受信します。

指定ポートの役割

自身が接続されているセグメントで最善の BPDU を送信できるポートは、指定ポートになります。 802.1D ブリッジは、複数のセグメント（イーサネット セグメントなど）を相互に関連付けて、ブリッジ型ドメインを形成します。 各セグメントでは、ルート ブリッジに向かうパスは 1 つしか存在できません。 2 つのパスが存在すると、ネットワーク内でブリッジング ループが発生します。 同じセグメントに接続されたすべてのブリッジは、他のブリッジの BPDU をリッスンし、最善の BPDU を送信するブリッジをセグメントの代表ブリッジにすることに同意します。 そのブリッジで対応するポートが、指定ポートになります。

代替ポートとバックアップ ポートの役割

これら 2 つのポートの役割は、802.1D の blocking 状態に対応します。 blocking 状態のポートとは、指定ポートでもルート ポートでもないポートのことです。 blocking 状態のポートは、自身のセグメントで自身が送出する BPDU よりも有用な BPDU を受信します。 ポートがブロックされた状態を維持するには、BPDU の受信が必須であることに注意してください。 RSTP では、この目的のために、次の 2 つの役割が追加されています。

代替ポートとは、他のブリッジから、より有用な BPDU を受信することによってブロックされているポートのことです。 次の図に例を示します。

バックアップ ポートとは、そのポートがある同じブリッジから、より有用な BPDU を受信することによってブロックされているポートのことです。 次の図に例を示します。

802.1D では、この区別が内部的に処理されていました。 基本的に、それがシスコの UplinkFast 機能の仕組みです。 この背景にある基本原理は、代替ポートを介してルート ブリッジへの代替パスを提供することです。 そのため、ルート ポートで障害が発生した場合は、代替ポートがルート ポートに置き換わることができます。 もちろん、バックアップ ポートは同じセグメントに冗長接続を提供するので、ルート ブリッジへの代替接続は保証できません。 そのため、バックアップ ポートは、アップリンク グループからは除外されていました。

したがって、RSTP では、802.1D とまったく同じ基準を使用してスパニング ツリーの最終的なトポロジが計算されます。 各種のブリッジ プライオリティやポート プライオリティの使用方法に変更はありません。 blocking という名前は、シスコの実装では discarding 状態を示すために使用されています。 CatOS リリース 7.1 以降では、引き続き listening 状態と learning 状態が表示されるので、IEEE 標準で要求されている内容よりも多くのポート情報が提供されることになります。 ただし、プロトコルで決められたポートの役割と、現在のポート状態が異なっている時間帯がある点が新しい特徴です。 たとえば、ポートが指定ポートになるのと同時にblocking 状態になることが今では完全に有効です。 通常、このような状況が発生するのは非常に短期間であり、指定ポートが forwarding 状態に移行するまでの過渡的な状況を示しているにすぎません。

STP による VLAN とのやりとり

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 に対して 1 つのスパニング ツリーを実行する Common Spanning Tree（CST; 共通スパニング ツリー）プロトコル（IEEE 802.1D 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 Multiple Spanning Tree（MST; 多重スパニング ツリー）（IEEE 802.1s など）

設定上の観点からすると、これら 3 種類のスパニング ツリー モードは、VLAN とのやりとりに関連して、次の 3 つのモードのいずれかに設定できます。

- **pvst**：VLAN 別のスパニング ツリー。 このモードでは、実際には PVST+ が実装されますが、Cisco IOS ソフトウェアでは単に PVST と表記されます。
- **rapid-pvst**：802.1D 規格が進化し、コンバージェンス時間が改善され、標準ベース（802.1w）のプロパティ（UplinkFast および BackboneFast）が組み込まれました。
- **mst**：このモードは、VLAN または MST のセットごとにスパニング ツリーを作成する 802.1s 規格です。 この規格には、802.1w の高速コンポーネントも組み込まれています。

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（つまり、PVST+）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 リソースも増加します。

新しい 802.1s 規格（MST）では、アクティブな STP インスタンスまたはトポロジを 16 個まで定義し、すべての VLAN をこれらのインスタンスにマッピングすることが可能です。 一般的なキャンパス環境で定義する必要があるインスタンスは 2 つだけです。 この手法を使用すると、ロード バランシングを実行しながら、STP を数千単位の VLAN に展開できます。

Catalyst 6500 に関しては、Rapid-PVST と標準化前の MST のサポートが Cisco IOS ソフトウェア リリース 12.1(11b)EX と 12.1(13)E で導入されています。 Cisco IOS ソフトウェア リリース 12.1(12c)EW 以降が稼働している Catalyst 4500 では、標準化前の MST がサポートされています。 Catalyst 4500 プラットフォームに関しては、Rapid PVST のサポートが Cisco IOS ソフトウェア リリース 12.1(19)EW で導入されています。 標準に準拠した MST は、Cisco IOS ソフトウェア リリース 12.2(18)SXF が稼働している Catalyst 6500 シリーズ スイッチ、および Cisco IOS ソフトウェア リリース 12.2(25)SG が稼働している Catalyst 4500 シリーズ スイッチでサポートされます。

詳細は、『Rapid Spanning Tree Protocol（802.1w）の概要』および『Multiple Spanning Tree Protocol（802.1s）の概要』を参照してください。

スパニング ツリーの論理ポート

Catalyst 4500 および 6500 のリリース ノートに、スイッチごとのスパニング ツリーの論理ポート数に関するガイドラインが記載されています。 すべての論理ポートの合計数は、スイッチのトランク数に、トランク上でアクティブな VLAN の数を掛け、その値にスイッチの非トランク インターフェイスの数を足した値と等しくなります。 Cisco IOS ソフトウェアでは、論理インターフェイスの最大数が制限を超えると、システム ログ メッセージが生成されます。 ガイドラインを超えないようすることを推奨します。

次の表に、各種の STP モードとスーパーバイザ タイプでサポートされる論理ポート数の比較を示します。

Supervisor（スーパバイザ）	PVST+	RPVST+	MST
Catalyst 6500 Supervisor 1	スイッチング モジュール毎に 6,000[1] 合計 1,200	スイッチング モジュール毎に 6,000 合計 1,200	25,000 合計 スイッチング モジュールごとに 3,000[2]
Catalyst 6500 Supervisor 2	13,000[1] 合計 スイッチング モジュールごとに 1,800[2]	10,000 合計 スイッチング モジュールごとに 1,800[2]	50,000 合計 スイッチング モジュールごとに 6,000[2]

Catalyst 6500 Supervisor 720	13,000 合計 スイッチング モジュールごとに 1,800[2]	10,000 合計 スイッチング モジュールごとに 1,800[2]	50,0003 合計 スイッチング モジュールごとに 6,000[2]
Catalyst 4500 Supervisor II plus	1,500 (合計)	1,500 (合計)	25,000 (合計)
Catalyst 4500 Supervisor II plus-10GE	1,500 (合計)	1,500 (合計)	25,000 (合計)
Catalyst 4500 Supervisor IV	3,000 (合計)	3,000 (合計)	50,000 (合計)
Catalyst 4500 Supervisor V	3,000 (合計)	3,000 (合計)	50,000 (合計)
Catalyst 4500 Supervisor V 10GE	3,000 (合計)	3,000 (合計)	80,000 (合計)

1 Cisco IOS ソフトウェア リリース 12.1(13)E よりも前の PVST+ でサポートされる論理ポートの最大合計数は 4,500 です。

2 10 Mbps、10/100 Mbps、および 100 Mbps のスイッチング モジュールでは、モジュール 1 台当たり最大 1,200 個の論理インターフェイスがサポートされます。

3 Cisco IOS ソフトウェア リリース 12.2(17b)SXA よりも前の MST でサポートされる論理ポートの最大合計数は 30,000 です。

推奨事項

ハードウェア、ソフトウェア、デバイス数、VLAN 数などの詳細情報がないと、特定のスパニング ツリー モードを推奨するのは困難です。 一般に、論理ポート数が推奨ガイドラインを超えない限り、新規に配備するネットワークでは Rapid PVST モードを使用することを推奨します。 Rapid PVST モードでは、Backbone Fast や Uplink Fast などの追加設定を行わなくても、高速なネットワーク コンバージェンスを実現できます。 スパニング ツリーを Rapid-PVST モードに設定するには、次のコマンドを発行します。

```
spanning-tree mode rapid-pvst
```

その他のオプション

従来のハードウェアや古いソフトウェアが混在するネットワークでは、PVST+ モードを使用することを推奨します。 スパニング ツリーを PVST+ モードに設定するには、次のコマンドを発行します。

```
spanning-tree mode pvst ----This is default and it shows in the configuration.
```

多数の VLAN が存在し、あらゆる場所で VLAN を利用するネットワーク設計では、MST モードを使用することを推奨します。 このようなネットワークでは、論理ポートの合計数が PVST および Rapid-PVST のガイドラインを超える可能性があります。 スパニング ツリーを MST モードに

設定するには、次のコマンドを発行します。

```
spanning-tree mode mst
```

BPDU のフォーマット

Cisco では、IEEE 802.1Q 規格をサポートするために、既存の PVST プロトコルを拡張して PVST+ プロトコルを開発しました。 PVST+ では、IEEE 802.1Q のモノ スパニング ツリー領域にわたるリンクのサポートが追加されています。 PVST+ は IEEE 802.1Q モノ スパニング ツリーおよび既存の Cisco PVST プロトコルの両方と互換性があります。 また、PVST+ には、すべてのスイッチ間でポート トランキングと VLAN ID の設定が一致していることを保証する確認メカニズムがあります。 PVST+ は、新しい Command Line Interface (CLI; コマンドライン インターフェイス) コマンドや設定を追加しなくても使用でき、PVST とプラグアンドプレイの互換性があります。

次に PVST+ プロトコルの動作原理の要点を説明します。

- PVST+ は、802.1Q のモノ スパニング ツリーと相互運用可能です。 PVST+ は、802.1Q トランキングを使用して共通 STP を実行している 802.1Q 準拠のスイッチと相互運用可能です。 デフォルトでは、共通スパニング ツリーは VLAN 1 (ネイティブ VLAN) にあります。 802.1Q リンク間では、IEEE 標準のブリッジグループ MAC アドレス (01-80-c2-00-00-00、プロトコル タイプ 0x010c) を使用して、1 個の共通スパニング ツリー BPDU が送受信されます。 共通スパニング ツリーのルートは、PVST またはモノ スパニング ツリー領域に置くことができます。
- 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。 トランク上の各 VLAN では、Cisco の共有 STP (SSTP) MAC アドレス (01-00-0c-cc-cd) を使用して BPDU が送受信されます。 Port VLAN Identifier (PVID) と同じ ID を持つ VLAN では、BPDU にタグが付けられません。 その他すべての VLAN では、BPDU にタグが付けられます。
- PVST+ は、ISL トランキングを使用して 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、以前の Cisco PVST と同様に ISL トランクを使用して送受信されます。
- PVST+ では、ポートと VLAN の不一致がチェックされます。 PVST+では、フォワーディング ループの発生を避けるために、一致しない BPDU を受信したポートがブロックされます。 また、不整合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されます。

注: ISL ネットワークでは、すべての BPDU が IEEE の MAC アドレスを使用して送信されます。

Cisco の推奨する設定

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。 レイヤ 2 ループを含まない設計を選択し、ポートの blocking 状態を能動的に維持するために STP をイネーブルにしていない場合でも、次の理由により、この機能は有効のままにしておくことを推奨します。

- 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 データによって問題が悪化することを防止できる。 多くの場合、ループは接続ミスやケーブル不良などの原因により発生します。
- EtherChannel の障害からネットワークを保護できる。
- 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ある。 使用実績が高いということは、一般にコードがより安定していることを意味します。

- 二重に接続された NIC の誤動作（またはサーバ上でイネーブルにされたブリッジング）からネットワークを保護できる。
- コード レベルで STP と密接な関係があるプロトコルが多い。 次に例を示します。 PAgPInternet Group Management Protocol（IGMP; インターネット グループ管理プロトコル）スヌーピングトランキングSTP なしで稼働させていると、望ましくない結果になる場合があります。
- ネットワークの障害が報告されたとき、STP を使用していないことが主な原因であることを Cisco のエンジニアが示唆する場合が多い。

すべての VLAN でスパニング ツリーをイネーブルにするには、次のグローバル コマンドを発行します。

```
Switch(config)#spanning-tree vlan vlan_id !--- Specify the VLAN that you want to modify.
Switch(config)#default spanning-tree vlan vlan_id !--- Set spanning-tree parameters to default values.
```

安定性に悪影響を及ぼすおそれがあるため、タイマーの値は変更しないでください。 実際に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。 この推奨事項は、Catalyst 6500/6000 シリーズの Cisco IOS スイッチには当てはまりません。 ただし、別個の管理インターフェイスを設定でき、Cisco IOS スイッチと統合する必要がある下位モデルの Cisco IOS スイッチや CatOS スイッチでは、この推奨事項を尊重する必要があります。 特に、古い Catalyst スイッチ プロセッサを使用している場合は、STP に関する問題を回避するために、管理 VLAN をユーザ データから常に切り離してください。 正常に動作していない 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極端に高くなると、1 つまたは複数の BPDU が失われる可能性があります。 ただし、より強力な CPU を搭載し、スロットリング制御機能を備えた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「スイッチ管理インターフェイスとネイティブ VLAN」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ください。 そのような設計では、多数のブロッキング ポートが存在することになり、長期的な安定性に悪影響を与えるおそれがあります。 STP 全体の直径は 7 ホップ以下に抑えてください。 可能であれば、必ず Cisco のマルチレイヤ モデルに基づいて設定を行ってください。 このモデルには、次の特徴があります。

- スイッチド ドメインが比較的小さい
- STP トライアングル
- ブロッキング ポートを決定論的に設定できる

詳細についてはギガビットキャンパス ネットワーク設計を参照して下さい。

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、 その情報をトポロジ ダイアグラムに記入してください。 トラブルシューティングを行う際には、スパニング ツリーのトポロジを理解していることが不可欠です。 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。 blocking 状態から forwarding 状態に変化した理由を調べることが、しばしば根本原因を分析する際の手がかりとなります。 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。その理由は、これらのレイヤがネットワーク内で最も安定した部分と考えられているためです。 レイヤ 3 および Hot Standby Router Protocol（HSRP; ホットスタンバイ ルータ プロトコル）の、レイヤ 2 データ転送パスに最適なオーバーレイをチェックしてください。

次のコマンドは、ブリッジ プライオリティを設定するためのマクロです。 root を指定すると、ブリッジ プライオリティがデフォルト（32,768）よりもはるかに小さい値に設定され、secondary を指定すると、デフォルトよりも適度に小さい値に設定されます。

```
Switch(config)#interface type slot/port Switch(config)#spanning-tree vlan vlan_id root primary
!--- Configure a switch as root for a particular VLAN.
```

注: このマクロを実行すると、ルート プライオリティは次のいずれかの値に設定されます。

- 8192（デフォルト）
- 現在のルート プライオリティから 1 を引いた値（別のルート ブリッジがわかっている場合）
- 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の MAC アドレスよりも小さい場合）

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。これは、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。 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**と呼ばれるもう 1 つの STP プロトコルがあります。このプロトコルは、既知の宛先 MAC アドレス **01-00-0c-cd-cd-ce** とプロトコル タイプ 0x010c を使用して動作します。

このプロトコルは、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必要がある場合に最も役立ちます。 非ブリッジ トラフィック用の VLAN インターフェイスがレイヤ 2 トラフィックをブロックするようになると、オーバーレイしているレイヤ 3 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。 非ブリッジ トラフィック用の 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、このようなレイヤ 2 のブロックが容易に起こり得ます。 VLAN ブリッジは、ブリッジ型プロトコルに対する別個の STP インスタンスです。 このプロトコルを使用すると、IP トラフィックに影響を与えずに操作できる別個のトポロジが提供されます。

MSFC などの Cisco ルータで VLAN 間のブリッジングが必要な場合は、VLAN ブリッジ プロトコルを実行してください。

STP PortFast 機能

PortFast を使用すると、アクセス ポート上で通常のスパニング ツリー処理をバイパスできます。 PortFast により、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。 Microsoft の DHCP 実装を使用する場合、IP アドレスを要求して受信するには、リンク状態が up になった直後にアクセス ポートが forwarding モードになっている必要があります。 Internetwork Packet Exchange（IPX）/Sequenced Packet Exchange（SPX）などの一部のプロトコルで Get Nearest Server（GNS）の問題を回避するには、リンク状態が up になった直後にアクセス ポートが forwarding モードになっている必要があります。

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。

PortFast の動作の概要

PortFast では、STP の通常の listening 状態、learning 状態、および forwarding 状態が省略されます。 この機能では、リンクが up 状態になると、ポートのモードが blocking から forwarding に直接移行します。 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。 この処理には ForwardDelay の 2 倍の時間がかかる可能性があります（デフォルトでは 30 秒）。

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 Topology Change Notification（TCN; トポロジ変更通知）が生成されるのを避ける効果もあります。 TCN が生成されること自体は正常な動作です。 ただし、大量の TCN がルート ブリッジに押し寄せると、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。 多くの場合、大量の TCN は、従業員が一斉に PC の電源を入れる朝の時間帯に発生します。

Cisco のアクセス ポートの設定に関する推奨事項

イネーブルになっているホスト ポートについてはすべて、STP PortFast を on に設定します。 また、スイッチ間リンクや未使用のポートについては、STP PortFast を明示的に off に設定します。

アクセス ポートに関するこれらの推奨設定を実装するには、インターフェイス設定モードで **switchport host** マクロ コマンドを発行します。 次の設定は、自動ネゴシエーションや接続のパフォーマンス向上にも大きく貢献します。

```
switch(config)#interface type slot#/port# switch(config-if)#switchport host switchport mode will be set to access spanning-tree portfast will be enabled channel group will be disabled !--- This macro command modifies these functions.
```

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。 LAN が十分に機能するためには、スパニング ツリーは不可欠です。 ループの検知およびブロッキングがなければ、1 つのループによって LAN 全体が意図せず短期間にダウンしてしまう可能性があります。

また、すべてのホスト ポートに対するトランキングとチャネリングをディセーブルにします。 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でネゴシエーションを行う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、望ましくない状況が発生する可能性があります。 その場合、ワークステーションからの初期パケット（DHCP 要求や IPX 要求など）が転送されなくなってしまいます。

グローバル コンフィギュレーション モードで次のコマンドを使用して、デフォルトで PortFast を設定することを推奨します。

```
Switch(config)#spanning-tree portfast enable
```

次に、1 つの VLAN のみにハブまたはスイッチが存在するアクセス ポートに対して、**interface** コマンドを使用して、各インターフェイスの PortFast 機能をディセーブルにします。

```
Switch(config)#interface type slot_num/port_num Switch(config-if)#spanning-tree portfast disable
```

その他のオプション

PortFast の BPDU ガード機能を使用すると、ループを防止できます。 BPDU ガードにより、

BPDU を受信した非トランキング ポートは errDisable 状態に移行します。

通常は、PortFast に設定されているアクセス ポートで BPDU パケットが受信されることはありません。 BPDU が着信する場合は、設定が正しくないことを示しています。 その場合は、該当するアクセス ポートをシャットダウンするのが最善の方法です。

Cisco IOS システム ソフトウェアでは、UplinkFast がイネーブルになっているポートで自動的に BPDU-ROOT-GUARD をイネーブルにする便利なグローバル コマンドが用意されています。 このコマンドは、*常に*使用してください。 こ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。

BPDU-ROOT-GUARD をイネーブルにするには、次のグローバル コマンドを発行します。

```
Switch(config)#spanning-tree portfast bpduguard default
```

ポートがダウンした場合は、Simple Network Management Protocol (SNMP; 簡易ネットワーク管理プロトコル) 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 ポートの自動リカバリ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「単方向リンク検出」セクションを参照してください。

詳細は、『スパニング ツリー PortFast BPDU ガード機能拡張』を参照してください。

注: トランク ポートのための PortFast は Cisco IOS ソフトウェア リリース 12.1(11b)E で導入されました。 トランク ポート用 PortFast の設計目的は、レイヤ 3 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。 この機能を使用する場合は、インターフェイス単位で BPDU ガードと BPDU フィルタを必ずディセーブルにしてください。

UplinkFast

目的

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 は STP に変更を加えなくことなく動作します。 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。 『UplinkFast 機能の説明と設定』を参照してください。

動作の概要

アクセス レイヤで Cisco のマルチレイヤ設計モデルを採用すると、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 アップリンクが即時に forwarding 状態に移行します。 この機能では、listening 状態と learning 状態がバイパスされます。

アップリンク グループは VLAN ごとのポートのセットであり、ルート ポートとバックアップ ルート ポートとみなすことができます。 通常の場合、ルート ポートはアクセスからルートへの接続を確保します。 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。

UplinkFast では通常の 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が必要になります。 そのメカニズムでは、代替パスを通じてローカル エンド ステーションに到達できるようになったという情報を、ドメイン内のスイッチに伝播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 スイッチでは、CAM テーブル内の MAC アドレスごとに、既知のマルチキャスト MAC アドレス

（01-00-0c-cd-cd-cd、HDLC プロトコル 0x200a）宛てのフレームが生成されます。 この処理により、ドメイン内の全スイッチの CAM テーブルが新しいトポロジ情報で更新されます。

Cisco の推奨事項

802.1D スパニング ツリーを実行している場合は、ブロッキング ポートがあるアクセス スイッチで UplinkFast をイネーブルにすることを推奨します。 バックアップ ルート リンクについての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 UplinkFast を使用しないでください。 原則的に、ネットワークからの出口が 3 つ以上あるスイッチでは UplinkFast をイネーブルにしないでください。 スイッチが複雑なアクセス環境内にあり、複数のブロッキング リンクとフォワーディング リンクがある場合は、そのスイッチでこの機能を使用しないようにするか、アドバンスト サービスのエンジニアに相談してください。

UplinkFast をイネーブルにするには、次のグローバル コマンドを発行します。

```
Switch(config)#spanning-tree uplinkfast
```

Cisco IOS ソフトウェアでこのコマンドを発行しても、すべてのブリッジ プライオリティが自動的に高い値に調整されるわけではありません。 このコマンドでは、手動で他の値に変更されていないブリッジ プライオリティを持つ VLAN だけが変更されます。 また、CatOS の場合とは異なり、UplinkFast がイネーブルになっていたスイッチを復旧する際には、このコマンドに no を付けた形式（**no spanning-tree uplinkfast**）で発行することで、変更された値がすべてデフォルトに戻されます。 そのため、このコマンドを使用する際は、使用前後にブリッジ プライオリティの状態を確認して、期待どおりの結果が得られていることを**必ず**確認してください。

注: プロトコル フィルタリング機能がイネーブルになっている場合は、UplinkFast コマンドで **all protocols** キーワードを使用する必要があります。 プロトコル フィルタリングがイネーブルになっている場合、CAM テーブルには MAC 情報や 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される必要があります。 **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。 RSTP には UplinkFast メカニズムがネイティブに含まれており、RSTP ではこのメカニズムが自動的にイネーブルになるので、UplinkFast を手動で設定する必要はありません。

BackboneFast

目的

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。 BackboneFast により、コンバージェンス時間がデフォルトの 50 秒から約 30 秒に短縮され、STP の機能が強化されます。 この機能は 802.1D を実行している場合にのみ使用できます。 Rapid PVST や MST を実行している場合は、この機能を設定しないでください（Rapid PVST や MST には高速コンポーネントが含まれています）。

動作の概要

BackboneFast 機能は、代表ブリッジからスイッチのルート ポートまたはブロッキング ポートに不良 BPDU が届いたときに動作を開始します。 通常、これらのポートが不良 BPDU を受信するのは、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 BPDU の送信を開始した場合です。 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 ルールでは、受信側スイッチは、設定された maxage 時間が経過するまで不良 BPDU を無視します。 デフォルトで、maxage は 20 秒です。 しかし、BackboneFastと、スイッチはトポロジーの可能性のある変更の場合として不良BPDU を見ます。 スイッチは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判断します。 この RLQ プロトコルの追加により、スイッチでは、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ます。 RLQ では、blocking から forwarding へのポート状態の移行が早期に行われ、不良 BPDU を送信したスイッチに対して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、このパケットはルートに向けて送出されます) 。
- RLQ を受信したスイッチは、自身がルート スイッチである場合、または自身がルートへの接続をすでに失っていることを認識している場合は、RLQ に応答します。 これらの事実を認識していないスイッチは、自身のルート ポートからクエリーを転送します。
- 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、その応答は廃棄されます。

この動作では、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を最大で 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。

Cisco の推奨事項

スパニング ツリー ドメイン全体で BackboneFast 機能をサポートできる場合にのみ、STP を実行しているすべてのスイッチで BackboneFast をイネーブルにすることを推奨します。 この機能は実稼働ネットワークの動作を中断せずに追加できます。

BackboneFast をイネーブルにするには、次のグローバル コマンドを発行します。

```
Switch(config)#spanning-tree backbonefast
```

注: このグローバルレベル コマンドは、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。 このコマンドを設定すると、すべてのスイッチが認識する必要のある機能が STP に追加されます。

その他のオプション

Catalyst 2900XL および 3500XL では BackboneFast はサポートされていません。 スイッチ ドメインにこれらのスイッチが含まれている場合は、BackboneFast を有効にしないでください。 XL スイッチが含まれる環境で BackboneFast 機能を実装する場合、厳密なトポロジの下で、XL スイッチがラインの最終スイッチであり、2 つの場所でコアにのみ接続されていれば、BackboneFast 機能をイネーブルにできます。 XL スイッチのアーキテクチャがデイジーチェーン方式である場合は、この機能を実装しないでください。

RSTP や 802.1w には BackboneFast メカニズムがネイティブに含まれており、RSTP ではこのメカニズムが自動的にイネーブルになるので、BackboneFast を手動で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、ネットワーク インターフェイスの動作不良や CPU のビジー状態など、BPDU の正常な転送を妨げるなんらかの要因により発生するループからレイヤ 2 ネットワークを保護します。 冗長構成のトポロジで、blocking 状態のポートが誤って forwarding 状態に移行すると、STP ループが発生します。 この状況は、物理的に冗長構成になっているトポロジ内のポートの 1 つ (ブロッキング 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 ガードが効果を発揮するのは、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 ネットワークにおいてのみです (これは、最近のキャンパス ネットワークやデータセンター ネットワークの大半に当てはまります)。 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 6500 スイッチでは Cisco IOS ソフトウェア リリース 12.1(13)E で、Catalyst 4500 スイッチでは Cisco IOS ソフトウェア リリース 12.1(9)EA1 で導入されました。

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 ポートまたは代替/バックアップ ルート ポートで BPDU が受信されているかどうかがチェックされます。 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、STP によってポートの状態が判断されます。 このようにして、リカバリが自動的に行われます。

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 ループが防止されます。 STP 自体 (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 ガードを実装することを推奨します。

ループ ガードにより inconsistent 状態の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。

```
%SPANTREE-SP-2-LOOPGUARD_BLOCK: Loop guard blocking port GigabitEthernet2/1 on VLAN0010
```

STP 状態が loop-inconsistent になっているポートで BPDU が受信されると、そのポートは別の STP 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。

```
%SPANTREE-SP-2-LOOPGUARD_UNBLOCK: Loop guard unblocking port GigabitEthernet2/1 on
VLAN0010
```

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。 一方、ループ ガードは、ルート ポートまたは代替ポートに対してのみ有効です。つまり、ループ ガードとルート ガードは相互に排他的です。 そのため、ループ ガードとルート ガードを 1 つのポートで同時にイネーブルにすることはできません。

UplinkFast

ループ ガードは UplinkFast と互換性があります。 ループ ガードによってルート ポートが blocking 状態に変更された場合は、UplinkFast によって新しいルート ポートが forwarding 状態に変更されます。 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 がこのリンクから届くので、ループ ガードは作動しません。 従って、BackboneFast およびループ ガード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 がイネーブルになっているポートは、ルート ポートや代替ポートではないので、ループ ガードと PortFast は相互に排他的です。

PAgP

ループ ガードでは、STP に認識されているポートが使用されます。 そのため、ループ ガードでは、PAgP で実現される論理ポートの抽象化を利用できます。 ただし、チャネルを形成するためには、チャネルとしてグループ化され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ために、すべての物理ポートに対して同一のループ ガード設定が適用されます。 EtherChannel に対してループ ガードを設定するときには、次の点に注意する必要があります。

- STP は常にチャネル内で機能している最初のポートを選択して 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 ガードによってすでにブロックされているポートのセットがグループ化されてチャネルが形成された場合、STP ではそれらのポートの状態情報がすべて失われ、新しいチャネル ポートが forwarding 状態になって指定ポートの役割を担う可能性がある。
- 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た場合でも、個々の物理ポートは forwarding 状態になって指定ポートの役割を担う可能性があります。

最後の 2 つのケースでは、UDLD によって障害が検出されるまでは、ループが発生する可能性があります。 しかし、ループ ガードではこのような障害を検出できません。

ループ ガードと UDLD 機能の比較

ループ ガード機能と UDLD 機能は、単方向リンクによって生じる STP 障害を防止するという意味で、部分的に共通するところがあります。 しかし、これら 2 つの機能では、問題に対するアプローチが異なり、動作も異なります。 具体的には、CPU の過負荷が原因で BPDU が送信されない場合の障害など、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。

UDLD とループ ガードの両方をイネーブルにすると、最高度の保護が実現します。 ループ ガードと UDLD の詳細な機能比較については、次のドキュメントを参照してください。

- 『*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
- このドキュメントの「UDLD」セクション

Cisco の推奨事項

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。 ループ ガードはすべてのポートに対してグローバルにイネーブルにできます。 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。 ポイントツーポイント リンクは、各リンクのデュプレックス ステータスによって検出されます。 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。

```
Switch(config)#spanning-tree loopguard default
```

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すべてのポートでこの機能をイネーブルにすることを推奨します。 指定ポートでループ ガードをイネーブルにしても利点はありませんが、イネーブルにしても特に問題はありません。 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。

```
Switch(config)#interface type slot#/port# Switch(config-if)#spanning-tree guard loop
```

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 ガードをイネーブルにすると、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、ループ ガードをグローバルにディセーブルにするか、個々のポートで個別にディセーブルにします。 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。

```
Switch(config)#no spanning-tree loopguard default !--- This is the global configuration.
```

または

```
Switch(config)#interface type slot#/port# Switch(config-if)#no spanning-tree guard loop !---
This is the interface 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 ブリッジの位置が指定されます。 ルート ガードは、初期の Cisco IOS ソフトウェア リリース 12.1E 以降で使用できます。

動作の概要

ルート ガードは STP の組み込みメカニズムです。 ルート ガードには独自のタイマーはなく、BPDU の受信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、そのポートがルート ポートになる可能性はなくなります。 BPDU の受信を契機としてスパニング ツリーのコンバージェンスが開始され、指定ポートがルート ポートになった場合、そのポートは root-inconsistent 状態になります。 次に syslog メッセージの例を示します。

```
%SPANTREE-SP-2-ROOTGUARD_BLOCK: Root guard blocking port GigabitEthernet2/1 on VLAN0010
```

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 により、このポートは listening 状態から learning 状態に移行し、最終的には forwarding 状態に移行します。 この移行は、syslog メッセージで次のように表示されます。

```
%SPANTREE-SP-2-ROOTGUARD_UNBLOCK: Root guard unblocking port GigabitEthernet2/1
on VLAN0010
```

リカバリは自動的に行われます。 人間が介入する必要はありません。

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。一方、ループ ガードはルート ポートまたは代替ポートに対してのみ有効です。そのため、ルート ガードとループ ガードは相互に排他的です。 したがって、ループ ガードとルート ガードを 1 つのポートで同時にイネーブル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。

Cisco の推奨事項

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 ガードを設定するには、インターフェイス設定モードで次のコマンドを使用します。

```
Switch(config)#interface type slot#/port# Switch(config-if)#spanning-tree guard root
```

EtherChannel

目的

EtherChannel では、コンポーネントの 10/100 Mbps 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が実行されます。 このフレーム分散アルゴリズムでは、複数のチャネルを 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、次の共通点を理解しておく必要があります。

- 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が必要です。 Catalyst スイッチの場合、この要件はハードウェアに関係します。 次に例を示します。 Catalyst 5500/5000：モジュールに Ethernet Bundling Chip（EBC）が搭載されているかどうかCatalyst 6500/6000：フレームの内容を読み取り、IP アドレスに基づいて多重化を行うアルゴリズムが実装されているかどうか
- レイヤ 2 の EtherChannel かレイヤ 3 の EtherChannel かに応じて、単一の STP インスタンスを実行できるようにするために、または単一のルーティング ピアリングを利用できるようにするために、1 つの論理チャネルが作成されます。
- リンクの両端でパラメータの整合性をチェックして、リンクの障害または追加が発生したときにバンドリングのリカバリを支援する管理プロトコルがあります。 このプロトコルとしては、PAgP または Link Aggregation Control Protocol（LACP）を使用できます。

動作の概要

EtherChannel では、コンポーネントの 10/100 Mbps リンク、ギガビット リンク、または 10 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が実行されます。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を使用しても、フレームの受信時に、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。

次の表は、各プラットフォームで使用される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 3750 シリーズ	Cisco IOS ソフトウェアが稼働している Catalyst 3750 では、MAC アドレスまたは IP アドレスと、メッセージ発信元またはメッセージ宛先（あるいはその両方）を使用するアルゴリズムのロード バランシングが行われます。
Catalyst 4500 シリーズ	Cisco IOS ソフトウェアが稼働している Catalyst 4500 では、MAC アドレス、IP アドレスまたはレイヤ 4（L4）ポート番号、メッセージ発信元またはメッセージ宛先（あるいはその両方）を使用するアルゴリズムのロード バランシングが行われます。
Catalyst 6500/6000 シリーズ	スーパーバイザ エンジン ハードウェアのタイプに応じて、使用できるハッシュ アルゴリズムが 2 種類あります。 ハッシュはハードウェアに実装された 17 次多項式です。 いずれの場合でも、ハッシュでは MAC、IP アドレス、または IP TCP/UDP ポート番号が使用され、アルゴリズムを適用して 3 ビットの値が生成されます。 この処理は SA と DA の両方に対して個別に実行されます。 次に、それらの結果に対して XOR 演算が実行されて、3 ビットの値がもう 1 つ生成されます。 この値により、チャネル内のどのポートを使用してパケットを転送するかが決定されます。 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。

次の表は、各種の 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を示しています。 この表には、デフォルトの動作も記載されています。

ハードウェア	説明	分散方式

WS-F6020A（レイヤ2エンジン）WS-F6K-PFC（レイヤ3エンジン）	より遅い Supervisor Engine I および Supervisor Engine IA Supervisor Engine IA/Policy 特殊機構カード 1（PFC1）	レイヤ 2 MAC： SA; DA; SA および DA レイヤ3 IP: SA; DA; SA および DA（デフォルト）
WS-F6K-PFC2	Supervisor Engine II（PFC2 付）	レイヤ 2 MAC： SA; DA; SA および DA レイヤ3 IP: SA; DA; SA および DA（デフォルト）レイヤ4 セッション: S ポート; D ポート; S および D ポート
WS-F6K-PFC3A WS-F6K-PFC3B WS-F6K-PFC3BXL	Supervisor Engine 720/PFC3A Supervisor Engine 720/Supervisor エンジン 32/PFC3B Supervisor Engine 720/PFC3BXL	レイヤ 2 MAC： SA; DA; SA および DA レイヤ3 IP: SA; DA; SA および DA（デフォルト）レイヤ4 セッション: S ポート; D ポート; S および D ポート

注: レイヤ 4 分散では、最初の断片化パケットによってレイヤ 4 分散が使用されます。 後続のパケットではすべてレイヤ 3 分散が使用されます。

注: 他のプラットフォームでの EtherChannel のサポート、および EtherChannel 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
- レイヤ 3 およびレイヤ 2 EtherChannel の設定（Catalyst 6500 シリーズ Cisco IOS ソフトウェア コンフィギュレーション ガイド、12.2SX）
- レイヤ 3 およびレイヤ 2 EtherChannel の設定（Catalyst 6500 シリーズ Cisco IOS ソフトウェア コンフィギュレーション ガイド、12.1E）
- EtherChannel の設定（Catalyst 4500 シリーズ スイッチ Cisco IOS ソフトウェア コンフィギュレーション ガイド、12.2(31)SG）
- EtherChannel の設定（Catalyst 3750 スイッチ ソフトウェア コンフィギュレーション ガイド、12.2(25)SEE）
- 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

Cisco の推奨事項

Catalyst 3750、Catalyst 4500、および Catalyst 6500/6000 シリーズ スイッチでは、デフォルトで発信元 IP アドレスと宛先 IP アドレスの両方をハッシュ化することによりロード 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場合には、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。

```
port-channel load-balance src-dst-ip !--- This is the default.
```

その他のオプション

同じ発信元 IP アドレスと宛先 IP アドレスの間のトラフィックが全体の大部分を占める場合、トラフィック フローによっては、レイヤ 4 分散を使用するとロード バランシングが改善されます。 レイヤ 4 分散を設定する際は、レイヤ 4 の発信元ポートと宛先ポートのみがハッシュ化されることを理解しておく必要があります。 この方式では、レイヤ 3 の IP アドレスはハッシュ アルゴリズムに取り入れられません。 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。

```
port-channel load-balance src-dst-port
```

注: Catalyst 3750 シリーズ スイッチでは、レイヤ 4 分散を設定できません。

フレーム分散ポリシーを確認するには、**show etherchannel load-balance** コマンドを発行します。

ハードウェア プラットフォームによっては、フレーム分散ポリシーに基づいて、EtherChannel 内のどのインターフェイスが特定のトラフィック フローを転送しているかを CLI コマンドで確認できます。

Catalyst 6500 スイッチの場合は、**remote login switch** コマンドを発行して、Switch Processor（SP; スイッチ プロセッサ）コンソールにリモート ログインします。 それから、**テスト EtherChannel ロードバランス interface port-channel** *数***{IP を**発行して下さい **| l4port | MAC}** [*source_ip_add | source_mac_add | source_l4_port*] [*dest_ip_add | dest_mac_add | dest_l4_port*] コマンド。

Catalyst 3750 スイッチに関しては、**テスト EtherChannel ロードバランス interface port-channel** *数***{IP を**発行して下さい **| MAC}** [*source_ip_add | source_mac_add*] [*dest_ip_add | dest_mac_add*]コマンド。

Catalyst 4500 には、これに相当するコマンドがまだ用意されていません。

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、ここに示すガイドラインと制限に従ってください。 たとえば、QoS がイネーブルになっている場合、異なる QoS 機能を持つ Catalyst 6500/6000 シリーズ スイッチング モジュールをバンドリングすると EtherChannel が形成されません。 Cisco IOS ソフトウェアが稼働している Catalyst 6500 スイッチでは、EtherChannel バンドリングに対する 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 コマンドでディセーブルにできます。 また、**show interface capability** *mod/port* コマンドを使用すると、ポートの QoS 機能を表示して、ポート間に互換性があるかどうかを確認できます。

設定上の問題を回避するには、次に示すプラットフォーム別のガイドラインに従ってください。

- レイヤ 3 およびレイヤ 2 EtherChannel の設定（Catalyst 6500 シリーズ Cisco IOS ソフトウェア コンフィギュレーション ガイド、12.2SX）
- レイヤ 3 およびレイヤ 2 EtherChannel の設定（Catalyst 6500 シリーズ Cisco IOS ソフトウェア コンフィギュレーション ガイド、12.1E）
- EtherChannel の設定（Catalyst 4500 シリーズ スイッチ Cisco IOS ソフトウェア コンフィギュレーション ガイド、12.2(31)SG）
- EtherChannel の設定（Catalyst 3750 スイッチ ソフトウェア コンフィギュレーション ガイド

、12.2(25)SEE ）
サポートされる EtherChannel の最大数は、ハードウェア プラットフォームとソフトウェア リリースによって異なります。 Cisco IOS ソフトウェア リリース 12.2(18)SXE 以降が稼働している Catalyst 6500 スイッチでは、最大 128 個のポートチャネル インターフェイスがサポートされます。 Cisco IOS ソフトウェア リリース 12.2(18)SXE よりも前のソフトウェア リリースでは、最大 64 個のポートチャネル インターフェイスがサポートされます。 設定可能なグループ番号は、ソフトウェア リリースにかかわらず 1 ~ 256 です。 Catalyst 4500 シリーズ スイッチでは、最大 64 個の EtherChannel がサポートされます。 Catalyst 3750 スイッチでは、48 個を超える EtherChannel をスイッチ スタックで設定しないことを推奨します。

スパニング ツリーのポート コスト計算

EtherChannel を使用する場合は、スパニング ツリーのポート コスト計算を理解しておく必要があります。 EtherChannel のスパニング ツリー ポート コストは、ショート方式またはロング方式のいずれかで計算できます。 デフォルトでは、ショート モードでポート コストが計算されます。

この表は帯域幅に基づいてレイヤ2 EtherChannel のために要されるスパニングツリーポートを説明したものです:

帯域幅	古い STP 値	新しく長い STP 値
10 Mbps	100	2,000,000
100 Mbps	19	200,000
1 Gbps	4	20,000
N X 1 Gbps	3	6660
10 Gbps	2	2,000
100 Gbps	N/A	200
1 Tbps	N/A	20
10 Tbps	N/A	2

注: CatOS では、ポート チャネルのメンバ リンクに障害が発生した後も、EtherChannel のスパニング ツリー ポート コストは変化しません。 Cisco IOS ソフトウェアでは、EtherChannel のポート コストが即座に更新されて、新しく使用可能になった帯域幅が反映されます。 不必要なスパニング ツリー トポロジの変更を避ける方が望ましい場合は、**spanning-tree cost** ***cost*** コマンドを使用して、スパニング ツリー ポート コストを静的に設定できます。

Port Aggregation Protocol (PAgP; ポート集約プロトコル)

目的

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する管理プロトコルです。 PAgP には、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支援する機能もあります。 PAgP には、次のような特徴があります。

- 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 では、ポートが他の VLAN に強制的に変更される可能性があるので、ダイナミック VLAN は EtherChannel のメンバに含まれません。
- 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、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。 そのような変更の例としては、VLAN の変更や trunking モードの変更などがあります。
- 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、グループ化される個々の物理ポート（または論理ポート）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 アドレスを使用して送信されます。 この MAC アドレスは 01-00-0c-cc-cc-cc です。 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。

- 物理ポートがアップしている間、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。
- 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、そのポートは PAgP 非対応デバイスに接続されているものと判断されます。
- PAgP パケットの到達が監視されます。PAgP パケットが到達した場合は、その物理ポートが別の PAgP 対応デバイスに双方向で接続されていることが証明されます。
- 物理ポートのグループでこのようなパケットが 2 つ受信されると、即座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

このプロトコルの動作を理解する上で役立つ、いくつかの概念を次に示します。

- 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。 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単位。 チャネルには非稼働状態のポートも含まれる場合があり、agport のスーパーセットになっています。 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。 ある物理ポートを別の物理ポートと集約できるのは、group-capability が一致する場合に限られます。
- 集約手順：物理ポートは UpData または UpPAgP 状態になると、適切な agport に関連付けられます。 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、各状態の詳細を示します。

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、agport に接続している唯一のポートです。 この物理ポートと agport の間では非 PAgP パケットが受け渡されます。
BiDi	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

r	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。 この物理ポートと agport の間では非 PAgP パケットが受け渡されます。

両方の接続の両端で、グルーピングに合意する必要があります。 グルーピングとは、接続の両端で許容される agport 内の最大のポート グループです。

UpPAgP 状態に移行した物理ポートは、そのポートと同じ group-capability を持つ BiDir 状態または UpPAgP 状態の物理ポートから構成される agport に割り当てられます。 このような BiDir ポートは、同時に UpPAgP 状態に移行します。 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ち、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、物理ポートで認識されている最後のネイバー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。 同時に、同じ agport 上ですでにタイムアウトしている物理ポートもすべて除去されます。 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

既存のチャネル内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損失なくハッシュ化されます。 そのような障害には、次のケースがあります。

- ポートのケーブルがはずされた
- Gigabit Interface Converter（GBIC; ギガビット インターフェイス コンバータ）が取りはずされた
- ファイバが破損した

注: モジュールの電源をオフにしたり、モジュールを取りはずしたことにより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 は抹消され、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。 この場合、STP によってポートが再びデータを転送できる状態になるまでは、トラフィックが廃棄される可能性があります。

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。 オンラインの状態でモジュールを抜き挿しする場合は、STP トポロジの変更が発生する可能性があるため、その点を考慮する必要があります。 agport は障害発生時にも影響を受けない場合があるため、Network Management System（NMS; ネットワーク管理システム）を使用してチャネルの物理リンクを個別に管理する必要があります。

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します（合計 3 ポート）。
- 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 つのポートを使用します

（合計 4 ポート）。
- 2 つのカードにわたって 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。

設定オプション

次の表に示すように、EtherChannel はさまざまなモードに設定できます。

モード	設定可能なオプション
	PAgP は動作していません。 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。
Auto	PAgP によって集約が制御されます。 ポートは受動的な negotiating 状態になります。 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 によって集約が制御されます。 ポートは能動的な negotiating 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 これ Catalyst 5500/5000 ファイバ FE および GE ポートのデフォルトです。	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、その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 モードをイネーブルにすると、リカバリ中の隣接ポートが再びアップ状態になってチャネルが不必要に分解されることが防止されます。 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。
これはすべての Catalyst 6500/6000 およびポート 4500/4000 ののデフォルト、また銅線	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 秒のタイムアウト期間が経過した後、そのインターフェイスは自動的に agport に関連付けられます。 そのため、このインターフェイスはデータ転送に使用できます。 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。

用ポート 5500/5000 のです。	

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に影響を与えます。 物理インターフェイスの障害や、ファイバやケーブルの破損などが原因でポートがトラフィックを送信できなくなった場合でも、その隣接ポートは引き続き稼働状態のままで動作できます。 パートナーは引き続きデータを送信します。 ただし、リターン トラフィックを受信できないので、データは失われます。 また、単方向リンクの性質により、スパニング ツリー ループが生じるおそれもあります。

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）。 この処理が実行されると、パートナー ポートが非稼働状態になり、実質的にリンクの両端のポートがダウンします。

データ（BPDU）を送信するデバイスを使用していて、単方向状態を検出できない場合は、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。 単方向リンクを検出するために PAgP を奪取 すること時間は約 3.5 * 30 秒 = 105 秒です。 30 秒は PAgP 2 つの連続的なメッセージ間の時間です。 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。

データを送信しないデバイスを使用している場合は、silent モードを使用します。 silent モードを使用すると、受信データの有無にかかわらず、ポートが強制的に接続されて稼働状態になります。 また、単方向状態を検出する機能がポートにある場合は、デフォルトで silent モードが使用されます。 そのようなポートの例としては、レイヤ 1 FEFI および UDLD を使用する最近のプラットフォームなどがあります。

インターフェイスでチャネリングをオフにするには、**no channel-group** *number* コマンドを発行します。

```
Switch(config)#interface type slot#/port# Switch(config-if)#no channel-group 1
```

確認

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 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 状態になる場合があります。つまり、そのような組み合せでは、チャネル作成側のポートがシャットダウンされます。 EtherChannel 設定ミス ガード機能は、デフォルトでイネーブルになっています。

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
オン	オン	チャネル（非 PAgP）	チャネル（非 PAgP）
オン	Not configured	非チャネル（errdisable）	非チャネル
オン	Auto	非チャネル（errdisable）	非チャネル
オン	望まし	非チャネル	非チャネル

	い	（errdisable）	
Not configured	オン	非チャネル	非チャネル（errdisable）
Not configured	Not configured	非チャネル	非チャネル
Not configured	Auto	非チャネル	非チャネル
Not configured	望ましい	非チャネル	非チャネル
Auto	オン	非チャネル	非チャネル（errdisable）
Auto	Not configured	非チャネル	非チャネル
Auto	Auto	非チャネル	非チャネル
Auto	望ましい	PAgP チャネル	PAgP チャネル
望ましい	オン	非チャネル	非チャネル
望ましい	Not configured	非チャネル	非チャネル
望ましい	Auto	PAgP チャネル	PAgP チャネル
望ましい	望ましい	PAgP チャネル	PAgP チャネル

L2 チャネルに関する Cisco の推奨設定

すべての EtherChannel リンクで PAgP をイネーブルにし、desirable-desirable の設定を使用することを推奨します。 詳細は、次の出力を参照してください。

```
Switch(config)#interface type slot#/port# Switch(config-if)#no ip address !--- This ensures that there is no IP !--- address that is assigned to the LAN port. Switch(config-if)#channel-group number mode desirable !--- Specify the channel number and the PAgP mode.
```

次の方法で設定を確認します。

```
Switch#show run interface port-channel number Switch#show running-config interface type slot#/port# Switch#show interfaces type slot#/port# etherchannel Switch#show etherchannel number port-channel
```

EtherChannel の設定エラーの防止

EtherChannel の設定を誤ると、スパニングツリーのループが発生する可能性があります。 このような設定エラーは、スイッチの処理に重大な悪影響を及ぼす可能性があります。 Cisco IOS システム ソフトウェアには、この問題を防止するために spanning-tree etherchannel guard

misconfig 機能が組み込まれています。

システム ソフトウェアとして Cisco IOS ソフトウェアが稼働しているすべての Catalyst スイッチで、次の設定コマンドを発行してください。

```
Switch(config)#spanning-tree etherchannel guard misconfig
```

その他のオプション

PAgP をサポートしていないが LACP はサポートしている 2 台のデバイスを使用してチャネルを形成する場合は、両側のデバイスで LACP の設定をアクティブにして LACP をイネーブルにすることを推奨します。 詳細は、このドキュメントの「Link Aggregation Control Protocol (LACP)」セクションを参照してください。

PAgP および LACP をサポートしていないデバイスを使用してチャネルを形成する場合は、チャネルを on モードに固定設定する必要があります。 この要件は、次のようなデバイスに適用されます。

- 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稼働しているスイッチ
- Catalyst 2900XL/3500XL スイッチ
- Catalyst 8540

次のコマンドを発行します。

```
Switch(config)#interface type slot#/port# Switch(config-if)#channel-group number mode on
```

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 のスイッチおよび認定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。

LACP は、次のプラットフォームとバージョンでサポートされています。

- Cisco IOS ソフトウェア リリース 12.1(11b)EX 以降が稼働する Catalyst 6500/6000 シリーズ
- Cisco IOS ソフトウェア リリース 12.1(13)EW 以降が稼働する Catalyst 4500 シリーズ
- Cisco IOS ソフトウェア リリース 12.1(14)EA1 以降が稼働する Catalyst 3750 シリーズ

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、ポート プロパティが一致している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 とトランキング タイプ

LACP と PAgP の間には次の顕著な違いがあります。

- LACP プロトコル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 プロトコルでは、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（たとえば、リモート側のシステムのハードウェア制限の方が厳しい場合）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にだけ使用されます。

注: Catalyst 4500 シリーズ スイッチでは、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 ソフトウェアが稼働する Catalyst 6500 および 3750 スイッチの 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 では、バンドルされる物理（または論理）ポートが個別に制御されます。 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。 次にプロトコル動作の要約を示します。

- 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、集約可能な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。
- 集約可能なリンク上のパートナーは、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、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、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、イベント駆動式の 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

LACP が一組のリンクが同じシステムに接続したかどうか、そして確認するようにするためにそれらのリンクが集約の視点から互換性があれば、確立ことはできることは必要です:

- 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 ID。LACP が動作する各システムには、自動的に（デフォルトのプライオリティは 32768）または管理者によって選択されたプライオリティを割り当てる必要があります。 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、自動的に（デフォルトのプライオリティは 128）または管理者によってプライオリティを割り当てる必要があります。 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、ゼロよりも大きい単純な 16 ビットの整数パラメータによって

要約されます。このパラメータは鍵と呼ばれます。 それぞれの鍵は、次のような要因に基づいて決定されます。ポートの物理的特性（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など）ネットワーク管理者が決定した設定上の制約各ポートには、次の 2 つの鍵が関連付けられています。管理鍵動作鍵管理鍵の値は管理者が操作できるので、ユーザはこの鍵を選択できます。 動作鍵は、集約を形成するためにシステムによって使用されます。 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。 同じ動作鍵の値を持つ特定のシステム内のポートのセットは、同じ鍵グループのメンバと呼ばれます。2 つのシステムがあり、同じ管理鍵を持つポートのセットがある場合、各システムでは、最もプライオリティの高いシステムで、最もプライオリティの高いポートから順にポート集約が開始されます。 この動作が可能になるのは、各システムで次のプライオリティが認識されているためです。

- ユーザまたはソフトウェアによって割り当てられた自身のプライオリティ
- LACP パケットを介して通知されたパートナーのプライオリティ

障害時の動作

LACP の障害時の動作は、PAgP の障害時の動作と同じです。 既存のチャネル内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はずされたり、GBIC が取りはずされたり、ファイバが破損したりすると）、agport がアップデートされ、トラフィックは残りのリンク上で 1 秒以内にハッシュ化されます。 障害発生後に再ハッシュ化する必要がないトラフィック（同じリンク上で引き続き送信されるトラフィック）には損失はありません。 障害が発生したリンクが復旧すると、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化されます。

設定オプション

次の表に示すように、LACP EtherChannel はさまざまなモードに設定できます。

モード	**設定可能なオプション**
オン	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。
Off（または）Not Configured	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。
Passive（デフォルト）	このモードは、PAgP の **auto** モードに似ています。 スイッチではチャネルの起動は行われませんが、着信 LACP パケットの認識は行われます。 active 状態のピアが（LACP パケットを送出することにより）ネゴシエーションを開始し、スイッチがそのパケットを受信して応答し、最終的にピアとの間で集約チャネルが形成されます。
Active（アクテ	このモードは、PAgP の **desirable** モードに似ています。 スイッチは集約リンクを形成するためにネゴシエーションを開始します。 相手側で

ィブ ）	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。

LACP では、LACP EtherChannel が確立された後、30 秒のインターバル タイマー（ Slow_Periodic_Time ）が使用されます。 長いタイムアウト（ 3 × Slow_Periodic_Time ）を使用している場合は、受信した LACPDU 情報を無効化するのに 90 秒かかります。 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 タイマーは調整できず、現在のところ、Protocol Data Unit（ PDU; プロトコル データ ユニット ）の高速送信（ 1 秒ごと ）を使用して、チャネル形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はできません。

確認

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、EtherChannel ガードによってチャネル作成側のポートが errdisable 状態になる場合があります。 EtherChannel 設定ミス ガード機能は、デフォルトでイネーブルになっています。

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
オン	オン	チャネル（ 非 LACP ）	チャネル（ 非 LACP ）
オン	オフ	非チャネル（ errdisable ）	非チャネル
オン	パッシブ	非チャネル（ errdisable ）	非チャネル
オン	Active（ アクティブ ）	非チャネル（ errdisable ）	非チャネル
オフ	オフ	非チャネル	非チャネル
オフ	パッシブ	非チャネル	非チャネル
オフ	Active（ アクティブ ）	非チャネル	非チャネル
パッシブ	パッシブ	非チャネル	非チャネル
パッシブ	Active（ アクティブ ）	LACP チャネル	LACP チャネル
Active（ アクティブ ）	Active（ アクティブ ）	LACP チャネル	LACP チャネル

Cisco の推奨事項

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 2 台のデバイスを使用してチャネルを形成する場合は、両側のデバイスで LACP の設定をアクティブにして LACP をイネーブルにすることを推奨します。

CatOS が稼働するスイッチでは、Catalyst 4500/4000 および Catalyst 6500/6000 のすべてのポートで、PAgP チャネル プロトコルがデフォルトで使用されます。 LACP を使用するようにポートを設定するには、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。 この制限は Cisco IOS ソフトウェアが稼働するスイッチには当てはまりません。 Cisco IOS ソフトウェアが稼働するスイッチでは、PAgP と LACP を同じモジュールでサポートできます。 LACP チャネル モードを active に設定して、管理鍵番号を割り当てるには、次のコマンドを発行します。

```
Switch(config)#interface range type slot#/port# Switch(config-if)#channel-group admin_key mode active
```

show etherchannel summary コマンドを発行すると、次の情報を含む要約がチャネル グループごとに 1 行ずつ表示されます。

- グループ番号
- ポート チャネル番号
- ポートのステータス
- チャネルを構成しているポート

show etherchannel port-channel コマンドを発行すると、すべてのチャネル グループの詳細なポート チャネル情報が表示されます。 この出力には、次の情報が含まれています。

- チャネルのステータス
- 使用されているプロトコル
- ポートがバンドルされてからの時間

特定のチャネル グループの各ポートに関する詳細情報を個別に表示するには、**show etherchannel** *channel_number* **detail** コマンドを使用します。 このコマンドの出力には、パートナーの詳細とポート チャネルの詳細が含まれます。 詳細は、『Catalyst 6500/6000 と Catalyst 4500/4000 間の LACP (802.3ad) の設定』を参照してください。

その他のオプション

PAgP および LACP をサポートしていないチャネル デバイスを使用する場合は、チャネルを on モードに固定設定する必要があります。 この要件は、次のデバイスに適用されます。

- 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稼働しているスイッチ
- Catalyst 2900XL/3500XL スイッチ
- Catalyst 8540

次のコマンドを発行します。

```
Switch(config)#interface range type slot#/port# Switch(config-if)#channel-group admin_key mode on
```

単方向リンク検出

目的

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。 ただし、レイヤ 1 検出メカニズムでは不十分な場合があります。 その場合は、次のような結果につなが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 インターフェイスにおける次のような障害状況に対処できます。

- 物理的なケーブル構成の監視：配線が正しくないポートを errDisabled 状態にしてシャットダウンします。
- 単方向リンクに対する保護：メディアやポート/インターフェイスの動作不良により発生した単方向リンクが検出されると、対象のポートを errDisabled 状態にしてシャットダウンします。 対応する syslog メッセージも生成されます。
- 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によって使用不可になった場合に、接続が失われていないかどうかがチェックされます。 UDLD アグレッシブ モードでは、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、通常モードの UDLD では対処できない障害状態におけるトラフィックのブラック ホール化を回避することです。

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。

スパニング ツリーには定常的な単方向 BPDU フローがあるため、このセクションに記載されている障害が発生する場合があります。 特定のポートが突然 BPDU を送信しなくなると、隣接ポートの STP 状態が blocking から forwarding に変わります。 ただし、そのポートでの受信はまだ可能であるため、ループは引き続き存在します。

動作の概要

UDLD は LLC レイヤ上で動作するレイヤ 2 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 レイヤ 1 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 を使用すると、FEFI や自動ネゴシエーションでは実現できない機能と保護効果が提供されます。 そのような機能には、次のものがあります。

- 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でないリンクにおける論理インターフェイス/ポートの動作不良および障害の検出**注:** ポイントツーポイントでないリンクとは、メディアコンバータやハブを経由するリンクです。

UDLD では、次の 2 種類の基本メカニズムが採用されています。

1. 隣接ポートの情報を学習し、ローカル キャッシュの情報を最新に保つ。
2. 新しい隣接ポートを検出したり、隣接ポートからキャッシュの再同期化を要求されるたびに、一連の UDLD プローブ/エコー（hello）メッセージを送信する。

UDLD はすべてのポートでプローブ/エコー メッセージを絶えず送信します。 対応する UDLD メッセージがポートで受信されると、検出フェーズおよび検証プロセスが開始されます。 有効な条

件がすべて満たされている場合、そのポートはイネーブルになります。 ポートが双方向で、正しく配線されている場合は、条件が満たされています。 条件が満たされていない場合、そのポートは errDisabled 状態になり、次の syslog メッセージが生成されます。

```
UDLD-3-AGGRDISABLE: Neighbor(s) of port disappeared on bidirectional link.
   Port disabled
UDLD-3-AGGRDISABLEFAIL: Neighbor(s) of port disappeared on bidirectional link.
   Failed to disable port
UDLD-3-DISABLE: Unidirectional link detected on port disabled.
UDLD-3-DISABLEFAIL: Unidirectional link detected on port, failed to disable port.
UDLD-3-SENDFAIL: Transmit failure on port.
UDLD-4-ONEWAYPATH: A unidirectional link from port to port of device [chars]
   was detected.
```

UDLD イベントを含む、ファシリティごとのすべてのシステム メッセージのリストについては、「UDLD メッセージ」（『Cisco IOS システム メッセージ第 2/2 集』）を参照してください。

いったんリンクが確立し、双方向とみなされると、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。

次の表に、ポート状態の詳細を示します。

ポート状態	備考
不定	検出中、またはネイバーの UDLD がディセーブルになっている。
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、ポートがディセーブルになっている。
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 対応インターフェイスがディセーブルになったり、デバイスがリセットされると、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。 このクリア動作により、UDLD キャッシュの完全性が維持されます。 また、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必要があることを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関する情報を学習したり、同期がとれていないネイバーから再同期要求を受信するたびに、自分側の接続で検出ウィンドウを開始または再開し、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 エコーバックが返されることを期待します。 有効な応答メッセージをまったく受信せずに検出ウィンドウが終了すると、そのリンクは単方向とみなされます。 この時点で、リンクの再確立または ポートのシャットダウン処理が起動される場合があります。 また、ごくまれに次のような異常状態が検出されることもあります。

- 同じポートの Rx コネクタに接続されたループバック状態の送信（Tx）ファイバ
- 共有メディア相互接続（ハブなどのデバイス）の配線ミス

コンバージェンス時間

Cisco IOS ソフトウェア リリース 12.1 以降では、STP ループを防止するために、UDLD のデフォルトのメッセージ インターバルが 60 秒から 15 秒に短縮されています。 この仕様変更は、802.1D スパニング ツリーで blocking 状態だったポートが forwarding 状態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。 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、設定されているメッセージ インターバルがネイバーに送信され、そのピアのタイムアウト インターバルが次のように計算されます。

```
3 * (message interval)
```

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 インターバルは異なるので、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、一方の側が障害をより速く検出することになります。

以前は安定していたリンクの単方向障害を UDLD で検出するために必要なおおよその時間は、次のように計算されます。

```
2.5 * (message interval) + 4 seconds
```

デフォルトのメッセージ インターバル（15 秒）を使用している場合、この時間は約 41 秒になります。 この時間は、STP の再コンバージェンスに通常必要とされる 50 秒よりも大幅に短い時間です。 NMP の CPU サイクルにいくらかの余力があり、その使用レベルをユーザが注意深く監視している場合は（監視することを推奨します）、メッセージ インターバルを最短で 7 秒にまで短縮できます。 また、このようにメッセージ インターバルを短くすると、検出を大幅にスピードアップするのにも役立ちます。

注: Cisco IOS ソフトウェア リリース 12.2(25)SEC の場合、最小値は 1 秒です。

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、STP ループ ガード機能などの代替メカニズムを検討してください。 また、RSTP（802.1w）は、トポロジによってはミリ秒単位でコンバージを行う特性があるので、RSTP を実装する場合も代替メカニズムを検討してください。 これらの場合には、UDLD とループ ガードを組み合せて使用すると、最大限の保護が実現します。 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 ループが防止されます。 UDLD では、個々の EtherChannel リンクでの単方向接続、または動作しなくなった方向に BPDU が流れない場合の単方向接続が検出されます。

注: UDLD は STP に依存していません。 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）の式で計算される時間を経過しても 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、ループ ガードと組み合せて UDLD を実装することを推奨します。

注意： 設定不可能の使用する 2900XL/3500XL スイッチの UDLD の以前のリリースの、60 秒デフォルトメッセージインターバル用心して下さい。 この状況では、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となる、次のようにまれなケースを特に想定して開発されました。 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する。 この場合は、どちらのポートも errdisable 状態にはなりません。
- リンクの一方でポート スタック（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レイヤ 1 障害検出メカニズムがディセーブルになっている。
- レイヤ 1 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み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。

UDLD のアグレッシブ モード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その他のレイヤ 1 障害検出メカニズムがディセーブルになっている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 がイネーブルになっていても、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 接続に対して特に有効です。 この場合、UDLD のアグレッシブ モードには、スパニング ツリー ループの発生を防止できるという利点もあります。

UDLD の通常モードでは、リンクが双方向状態になった後でも、単方向リンク状態のチェックが行われていることを理解しておくことが重要です。 UDLD の目的は、STP ループを発生させるレイヤ 2 問題を検出することです。安定状態では BPDU は 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、UDLD の通常モードを自動ネゴシエーションおよびループ ガードとともに使用すれば、ほとんどの場合は十分です（STP に依存するネットワークの場合）。
UDLD アグレッシブ モードがイネーブルになっている場合は、ポートのすべてのネイバーがエージング アウトすると、同期がずれている可能性があるネイバーとの再同期を行うために、アドバタイズメントまたは検出フェーズのいずれかで、リンクアップ シーケンスが再開されます。 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 とみなされる場合は、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 インターバルが 60 秒にハードコードされています。 この設定は、（デフォルトの STP パラメータを使用している場合には）潜在的な STP ループからネットワークを保護するのに十分な速さではないと考えられます。

UDLD リンクの自動リカバリ

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。 この機能をグローバルにイネーブルにした後でポートが errdisable 状態になると、選択したインターバル時間が経過した後、そのポートは自動的に再有効化されます。 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。 ソフトウェア リリースによっては、次のように UDLD の errdisable タイムアウト リカバリ メカニズムを使用してポ

ートをディセーブル化するように errdisable タイムアウトを設定すれば、ポートの再イネーブル化を手動で回避できます。

```
Switch(config)#errdisable recovery cause udld
```

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 状態のポートのタイムアウト期間を設定する方法については、「errdisable recovery」（『Catalyst 6500 シリーズ Cisco IOS コマンド リファレンス 12.1 E』）を参照してください。

キャンパス環境全体にアクセス スイッチが分散されていて、両方のアップリンクを再びイネーブルにするために各スイッチを手作業で操作するために相当な時間がかかる場合は、アクセス レイヤの UDLD において errdisable リカバリが特に重要になることがあります。

通常、コアへのエントリ ポイントは複数あり、コアで自動リカバリを実行すると繰り返し問題が発生する可能性があるので、ネットワークのコアでの errdisable リカバリは推奨されません。 そのため、UDLD によってコアのポートがディセーブルにされた場合は、手動で再度イネーブルにする必要があります。

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 2 つの接続タイプのいずれかであるものと仮定されています。

- 2 つのルータ ノード間のポイントツーポイント（30 ビットのサブネット マスクで設定）
- 複数のポートを持つが、ルーテッド接続だけをサポートしている VLAN（分割されたレイヤ 2 コア トポロジの場合など）

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。 このセクションでは、現在広範に使用されている 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 プロトコルを対比するときに重要となる特性について説明しています。

注: ポイントツーポイントのルーテッド ネットワークでレイヤ 1 またはレイヤ 2 の障害が発生すると、レイヤ 3 接続はほぼ瞬時に切断されます。 レイヤ 1 またはレイヤ 2 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、インターフェイスの自動状態機能によって、レイヤ 2 とレイヤ 3 のポート状態が約 2 秒以内に同期化され、レイヤ 3 の VLAN インターフェイスが up/down 状態（回線プロトコルが down 状態）になります。

デフォルトのタイマー値を使用している場合は、OSPF によって hello メッセージが 10 秒ごとに送信され、40 秒のデッド インターバル（hello メッセージ 4 回分）が使用されます。 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。 OSPF では隣接関係を形成するために双方向通信が必要となるので、状況が悪い場合のフェールオーバー時間は 40 秒になります。 これは、ポイントツーポイント接続におけるレイヤ 1 またはレイヤ 2 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、レイヤ 3 プロトコルによる処理が必要になる場合にも該当します。 UDLD の検出時間は OSPF デッド タイマーの検出時間切れ（約 40 秒）とよく似ているので、OSPF のレイヤ 3 ポイントツーポイント リンクで UDLD 通常モードを設定してもあまり利点はありません。

多くの場合、EIGRP の方が OSPF よりも速くコンバージします。 ただし、双方向で通信できなくても、ネイバー間でルーティング情報を交換できることに注意してください。 中途半端に動作

する障害のように非常に特殊なシナリオの場合、EIGRP は、他のイベントによってそのネイバーを経由するルートがアクティブになるまで継続するトラフィックのブラック ホール化に対して脆弱です。 UDLD の通常モードでは、単方向リンク障害が検出されるとポートが errdisable 状態になるので、このような状況を緩和できます。

任意のルーティング プロトコルを使用するレイヤ 3 ルーテッド接続では、ケーブル配線の間違いやハードウェアの故障など、リンクの初期起動時に発生する問題を UDLD の通常モードで引き続き保護できます。 さらに、UDLD アグレッシブ モードには、レイヤ 3 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（最小のタイマー値の設定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
- レイヤ 3 EtherChannel の設定に起因するループからネットワークを保護する

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ディセーブルになっています。これは、銅ポートがホスト アクセスに使用されることが多いためです。 ネイバー間で双方向状態を確立するには、UDLD をグローバルにイネーブル化し、インターフェイス レベルでもイネーブル化する必要があることに注意してください。 デフォルトのメッセージ インターバルは 15 秒です。 ただし、場合によっては、デフォルトのメッセージ インターバルが 7 秒と表示されることもあります。 詳細は、Cisco Bug ID CSCea70679（登録ユーザ専用）を参照してください。一部ツールについては、ゲスト登録のお客様にはアクセスできない場合がありますことを、ご了承ください。 デフォルトのメッセージ インターバルは 7 ~ 90 秒の間で設定でき、UDLD アグレッシブ モードはディセーブルになっています。 Cisco IOS ソフトウェア リリース 12.2(25)SEC では、このタイマーの最小値が 1 秒にまで短縮されています。

Cisco の推奨する設定

ほとんどの場合、デフォルトの 802.1D スパニング ツリー タイマーを使用する際は、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 UDLD 通常モードをイネーブルにし、UDLD メッセージ インターバルを 15 秒に設定することを推奨します。 また、ネットワークの冗長性とコンバージェンスが STP に依存している場合（つまり、トポロジ内に STP blocking 状態のポートが 1 つ以上ある場合）は、適切な機能やプロトコルと組み合せて UDLD を使用してください。 そのような機能には、FEFI、自動ネゴシエーション、ループ ガードなどがあります。 通常、自動ネゴシエーションがイネーブルにされている場合は、レイヤ 1 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 をイネーブルにするには、次の 2 つのコマンドのいずれかを発行します。

注: 構文は、各種のプラットフォームおよびバージョンによって異なります。

- `udld enable !--- Once globally enabled, all FE and GE fiber !--- ports have UDLD enabled by default.` `udld port` または
- `udld enable !--- The copper ports of some earlier Cisco IOS Software !--- releases can have UDLD enabled by individual port command.`

単方向リンクの症状のためにシャットダウンされているポートは手動でイネーブルにする必要があります。 次のいずれかの方法を使用してください。

```
udld reset !--- Globally reset all interfaces that UDLD shut down. no udld port udld port
[aggressive] !--- Per interface, reset and reenable interfaces that UDLD shut down.
```

errdisable recovery cause udld および **errdisable recovery interval** ***interval*** グローバル設定コマンドを使用すると、UDLD errdisable 状態から自動的にリカバリできます。

errdisable リカバリ メカニズムは、スイッチへの物理的なアクセスが困難な場合に、ネットワークのアクセス レイヤ内だけで使用し、リカバリ タイマーは 20 分以上に設定することを推奨します。 ポートがオンラインに戻ってもネットワークが不安定にならないように、ネットワークの安定化とトラブルシューティングの時間を見込んでおくのが最善の方法です。

このリカバリ メカニズムは、ネットワークのコアでは使用**しない**ことを推奨します。ネットワークのコアで使用すると、障害のあるリンクが up 状態に戻るたびにコンバージェンス イベントが発生して不安定状態になる可能性があるためです。 コア ネットワークを冗長構成にすると、障害が発生したリンクのバックアップ パスが提供され、UDLD 障害の原因を調査する時間を確保できます。

STP ループ ガードなしでの UDLD の使用

ループのない (blocking 状態のポートがない) STP トポロジが存在するレイヤ 3 ポイントツーポイント リンクやレイヤ 2 リンクでは、Cisco スイッチ間のポイントツーポイント FE/GE リンクでアグレッシブ UDLD をイネーブルにすることを推奨します。 この場合、メッセージ インターバルは 7 秒に設定され、802.1D STP でデフォルトのタイマーが使用されます。

EtherChannel での UDLD

STP ループ ガードが展開されているかどうかに関係なく、EtherChannel の設定では、desirable チャネル モードと組み合せて UDLD アグレッシブ モードを使用することを推奨します。 EtherChannel の設定では、スパニング ツリーの BPDU と PAgP 制御トラフィックを伝送するリンクに障害が発生してチャネル リンクのバンドルが解除されると、チャネル パートナー間で即座にループが発生します。 UDLD アグレッシブ モードでは、障害が発生したポートがシャットダウンします。 次に、PAgP (auto/desirable チャネル モード) で新しい制御リンクがネゴシエートされて、障害の発生したリンクが事実上チャネルから排除されます。

802.1w スパニング ツリーでの UDLD

最近のバージョンのスパニング ツリーを使用する場合、ループを防止するには、UDLD 通常モードおよび STP ループ ガードを 802.1w などの RSTP と組み合せて使用します。 UDLD では、リンクアップ フェーズの間に発生した単方向リンクに対する保護を実現でき、STP ループ ガードでは、UDLD によってリンクが双方向で確立された**後**にリンクが単方向になった場合の STP ループを防止できます。 UDLD は 802.1w のデフォルト タイマーよりも小さい値に設定できないので、冗長トポロジにおけるループを完全に防止するには、STP ループ ガードが必要になります。

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。

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ような簡単なテストを実行する場合は、最初にレイヤ 1 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 通常モー

ドの場合、リモート エンドは undetermined 状態に移行し、UDLD アグレッシブ モードを使用している場合にのみ errdisable 状態に移行します。

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。 この方法では、MAC レイヤ フィルタを使用して UDLD や CDP のハードウェア アドレスをブロックし、その他のアドレスを通過させます。 一部のスイッチでは、Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）の宛先としてポートが設定されていると、UDLD フレームが送信されません。この現象を利用すれば、無応答の UDLD ネイバーをシミュレートできます。

UDLD を監視するには、次のコマンドを使用します。

```
show udld gigabitethernet1/1 Interface Gi1/1 --- Port enable administrative configuration
setting: Enabled Port enable operational state: Enabled Current bidirectional state:
Bidirectional Current operational state: Advertisement - Single neighbor detected Message
interval: 7 Time out interval: 5
```

また、Cisco IOS ソフトウェア リリース 12.2(18)SXD 以降が稼働するスイッチの 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。 プロトコル固有の異常がないかどうかを確認する場合、UDLD キャッシュと CDP キャッシュを比較する方法が非常に便利です。 CDP にも影響がある場合、通常はすべての BPDU や PDU 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。

UDLD のステータスと設定の一貫性は、Cisco UDLD SNMP MIB 変数を使用して監視できます。

マルチレイヤ スイッチング

概要

Cisco IOS システム ソフトウェアが稼働する Catalyst 6500/6000 シリーズでは、MultiLayer Switching（MLS; マルチレイヤ スイッチング）が内部的にのみサポートされます。 つまり、ルータをスイッチに取り付ける必要があります。 最近の Catalyst 6500/6000 スーパーバイザ エンジンでは MLS CEF がサポートされており、ルーティング テーブルが各カードにダウンロードされます。 この機能を使用するには、Distributed Forwarding Card（DFC）など、追加のハードウェアが必要です。 ルータ カードで Cisco IOS ソフトウェアを使用する場合でも、CatOS ソフトウェアでは DFC はサポートされません。 DFC がサポートされるのは Cisco IOS システム ソフトウェアだけです。

Catalyst スイッチ上の NetFlow 統計情報をイネーブルにするために使用される MLS キャッシュは、Supervisor Engine I カードおよび旧式の Catalyst スイッチでレイヤ 3 スイッチングをイネーブルにするために使用されるフローベースのキャッシュです。 MSFC または MSFC2 搭載の Supervisor Engine 1（または Supervisor Engine 1A）では、MLS がデフォルトでイネーブルになっています。 デフォルトの MLS 機能を使用するために追加の設定作業を行う必要はありません。 MLS キャッシュは次の 3 つのモードのいずれかに設定できます。

- destination
- source-destination
- source-destination port

スイッチの MLS モードは、フロー マスクを使用して判別されます。 その後、これらのデータは、Supervisor Engine IA によってプロビジョニングされている Catalyst スイッチでレイヤ 3 フローをイネーブルにするために使用されます。 Supervisor Engine II ブレードでは、より一層スケー

ラブルなテクノロジーであるハードウェアベースの CEF がイネーブルになっているので、MLS キャッシュはパケットのスイッチングには使用されません。 MLS キャッシュは、NetFlow 統計情報のエクスポートをイネーブルにするためにのみ Supervisor Engine II カードで保持されています。 そのため、必要であれば、スイッチに影響を及ぼすことなく、Supervisor Engine II をフル フローに対してイネーブルにすることもできます。

設定

MLS のエージング時間は、すべての MLS キャッシュ エントリに適用されます。 エージング時間の値は、宛先モードのエージングに直接適用されます。 source-to-destination モードのエージング時間を求めるには、MLS エージング時間の値を 2 で割ります。 フル フローのエージング時間を求めるには、MLS エージング時間の値を 8 で割ります。 MLS エージング時間のデフォルト値は 256 秒です。

通常のエージング時間は、32 ~ 4092 秒の範囲で 8 秒単位で設定できます。 8 秒の倍数ではないどのエージング タイム値でも 8 秒の最も密接な倍数に合わせられます。 たとえば、65 という値は 64 に合わせられ、127 という値は 128 に合わせられます。

他のイベントによって MLS エントリが消去される場合があります。 そのようなイベントには、次のものがあります。

- ルーティングの変更
- リンク状態の変更PFC リンクのダウンなど。

MLS のキャッシュ サイズを 32,000 エントリ未満にしておくには、**mls aging** コマンドを発行した後に、次のパラメータをイネーブルにします。

```
Normal: configures the wait before aging out and deleting shortcut entries in
the L3 table.

Fast aging: configures an efficient process to age out entries created for flows that
only switch a few packets and then are never used again. The fast aging parameter uses
the time keyword value to check if at least the threshold keyword value of packets has
been switched for each flow. If a flow has not switched the threshold number of packets
during the time interval, then the entry in the L3 table is aged out.

Long: configures entries for deletion that have been up for the specified value even if
the L3 entry is in use. Long aging is used to prevent counter wraparound, which could
cause inaccurate statistics.
```

設定

一般的に削除されるキャッシュ エントリとしては、Domain Name Server (DNS; ドメイン ネーム サーバ) や TFTP サーバとの間のフローに関するエントリがあります。これらのエントリは、作成後に再利用されることはほとんどありません。 これらのエントリを検出してエージング アウトすれば、MLS キャッシュの領域を節約して他のデータ トラフィックに使用できます。

MLS エージングが速い時間を有効に する必要がある場合 128 秒に初期値を設定 して下さい。 MLSキャッシュのサイズが 32,000 のエントリに育ち続ける場合キャッシュサイズが 32,000 以下とどまるまで設定を減少させて下さい。 それでもキャッシュが引き続き 32,000 エントリを超える場合は、通常の MLS エージング時間の設定を下げます。

Cisco が推奨する MLS 設定

NetFlow のエクスポートが必要でない限りは、MLS をデフォルト値 (destination のみ) のままに

しておくことを推奨します。 NetFlow が必要な場合は、Supervisor Engine II システムでのみ MLS のフル フローをイネーブルにしてください。

MLS フローの destination モードをイネーブルにするには、次のコマンドを発行します。

```
Switch(config)#mls flow ip destination
```

ジャンボ フレーム

最大伝送ユニット

Maximum Transmission Unit (MTU; 最大伝送ユニット) とは、パケットを断片化せずにインターフェイスで送受信できるデータグラムまたはパケットの最大サイズをバイト単位で表したものです。

IEEE 802.3 規格によると、イーサネット フレームの最大サイズは次のように定義されています。

- 通常フレームの場合は **1518 バイト** (1500 バイト + イーサネット ヘッダーおよび CRC トレーラの 18 バイト)
- 802.1Q カプセル化フレームの場合は **1522 バイト** (1518 バイト + タギングの 4 バイト)

ベビー ジャイアント： スイッチがベビー ジャイアント機能に対応している場合は、IEEE イーサネット MTU よりも少し大きいパケットを通過させて転送することができます。それらのフレームがオーバーサイズと宣言されて廃棄されることはありません。

ジャンボ： このフレーム サイズは IEEE 規格で定められていないため、フレーム サイズの定義はベンダーごとに異なります。 ジャンボ フレームとは、標準のイーサネット フレーム サイズよりも大きいフレームを指します (標準のイーサネット フレーム サイズは 1518 バイトで、レイヤ 2 ヘッダーと Frame Check Sequence (FCS; フレーム チェック シーケンス) を含んでいます)。

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。

1518 バイトを超えるパケットが予想される場合

スイッチド ネットワーク間でトラフィックを転送するためには、転送するトラフィックの MTU が、スイッチ プラットフォームでサポートされている MTU を超えないようにする必要があります。 特定のフレームの MTU サイズが切り捨てられるケースに関しては、次のようにさまざまな原因があります。

- **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。 このような変更が行われる理由は、イーサネット フレームのサイズを大きくすると平均スループットが向上する場合があるという研究結果が報告されているためです。
- **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トランキングの 2 つの形式を次に示します。Cisco 独自の ISL カプセル化 802.1Q
- **Multiprotocol Label Switching (MPLS; マルチプロトコル ラベル スイッチング)**：MPLS をインターフェイスでイネーブルにすると、MPLS タグ付きパケットのラベル スタックに含ま

れるラベルの数によっては、パケットのフレーム サイズが大きくなる可能性がある。 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、次のように計算されます。`n * 4 bytes`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 つだけがハードウェアに認識される。 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）/Layer 2 Tunneling Protocol Version 3（Layer 2TPv3）**：UTI/Layer 2TPv3 では、IP ネットワーク上で転送されるレイヤ 2 データがカプセル化される。 UTI/Layer 2TPv3 を使用すると、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）、Layer 2TPv3 ヘッダー（12 バイト）、および新しいレイヤ 2 ヘッダーが含まれます。 Layer 2TPv3 のペイロードは、レイヤ 2 ヘッダーを含む完全なレイヤ 2 フレームで構成されています。

目的

高速な（1 Gbps および 10 Gbps）ハードウェア ベース スイッチングの出現により、スループットが最適にならない問題の具体的な解決策として、ジャンボ フレームが使用されるようになりました。 ジャンボ フレームのサイズは公的には定められていませんが、広く一般的に採用されている値は 9216 バイト（9 KB）です。

ネットワーク効率の考慮事項

パケット転送のネットワーク効率を計算するには、オーバーヘッド値とペイロード サイズを合計し、その合計値でペイロード サイズを割ります。

ジャンボ フレームの使用によるネットワーキング効率の向上は 94.9 %（1500 バイト）から 99.1 %（9216 バイト）とそれほど大きくはありませんが、ネットワーク デバイスとエンド ホストの処理オーバーヘッド（CPU 使用率）は、パケット サイズに比例して減少します。 ハイパフォーマンスの LAN および WAN ネットワーキング テクノロジーで大きな最大フレーム サイズが好まれる傾向があるのはこのためです。

パフォーマンスが向上するのは、長いデータ転送が行われる場合のみです。 たとえば、次のような場合に該当します。

- サーバのバックツーバック通信（Network File System（NFS; ネットワーク ファイル システム）のトランザクションなど）
- サーバのクラスタリング
- 高速データ バックアップ
- スーパーコンピュータの高速相互接続
- グラフィック アプリケーションのデータ転送

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。 下記の公式は、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

この数式に従って、最大達成可能な TCP スループットは MSS に正比例しています。 これは、一定した RTT およびパケット口スと、二重パケットサイズ TCP スループットを倍増できることを意味します。 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。

動作の概要

IEEE 802.3 規格の仕様では、イーサネット フレームの最大サイズは **1518** バイトと定義されています。 その後、IEEE Std 802.3ac-1998 の補遺により、1519 ~ 1522 バイトの長さを持つ 802.1Q カプセル化フレームが 802.3 仕様に追加されました。 この文献では、これらのフレームが**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対して指定されたイーサネット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。

ジャンボ フレームに関して最も混乱を招くポイントは設定です。 サポートされる最大パケット サイズはインターフェイスごとに異なるため、場合によっては、若干異なる方法で大きなパケットを処理する必要があります。

Catalyst 6500 シリーズ

Catalyst 6500 プラットフォームの各種カードで現在サポートされている MTU サイズを次の表にまとめます。

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、WS-X6348-RJ45V、WS-X6348-RJ-21、WX-X6348-RJ21V	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 で） 9216 バイト

	（10 Mbps で）
WS-X6516-GE-TX	8092 バイト（100 Mbps で） 9216 バイト（10 時または 1000 Mbps で）
WS-X6148(V)-GE-TX、WS-X6148-GE-45AF、 WS-X6548(V)-GE-TX、WS-X6548-GE-45AF	1500 バイト
OSM ATM（OC12c）	9180 バイト
OSM CHOC3、CHOC12、CHOC48、CT3	9216 バイト（OCx および DS3） 7673 バイト（T1/E1）
FlexWAN	7673 バイト（CT3 T1/DS0） 9216 バイト（OC3c POS）

	7673 バイト（T1）
WS-X6148-GE-TX、WS-X6548-GE-TX	非サポート

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。

Catalyst 6500/6000 の Cisco IOS ソフトウェアにおけるレイヤ 2 およびレイヤ 3 ジャンボ フレームのサポート

レイヤ 2 およびレイヤ 3 の物理インターフェイスとして設定されているすべての GE ポートでは、PFC/MSFC1、PFC/MSFC2、および PFC2/MSFC2 により、レイヤ 2 およびレイヤ 3 のジャンボ フレームがサポートされます。 このサポートは、これらのポートがトランキングとチャネリングのどちらを実行しているかに関係なく適用されます。 この機能は、Cisco IOS ソフトウェア リリース 12.1.1E 以降で利用できます。

- ジャンボ対応のすべての物理ポートの MTU サイズは、相互に関連付けられています。 いずれかのポートでサイズを変更すると、すべてのポートに変更が反映されます。 これらのポートがイネーブルになった後は、すべてのポートで同じジャンボ フレーム MTU サイズが常に維持されます。
- 設定時には、同じ VLAN 内のすべてのポートをジャンボ対応としてイネーブルにするか、あるいは、どのポートもジャンボ対応としてイネーブルにはしない必要があります。
- Switched Virtual Interface（SVI; スイッチ仮想インターフェイス）（VLAN インターフェイス）の MTU サイズは、物理ポートの MTU サイズとは別に設定されます。 物理ポートの MTU を変更しても、SVI の MTU サイズは変更されません。 また、SVI の MTU サイズを変更しても、物理ポートの MTU には影響しません。
- Cisco IOS ソフトウェア リリース 12.1(8a) EX01 以降では、FE インターフェイス上でレイヤ 2 およびレイヤ 3 のジャンボ フレームがサポートされます。 **mtu 1500** コマンドを使用すると FE でジャンボ フレームがディセーブルになり、**mtu 9216** コマンドを使用すると FE でジャンボ フレームがイネーブルになります。 Cisco Bug ID CSCdv90450（登録ユーザ専用）を参照してください。一部ツールについては、ゲスト登録のお客様にはアクセスできない場合がありますことを、ご了承ください。
- VLAN インターフェイス上のレイヤ 3 ジャンボ フレームは、次のカードでのみサポートされます。PFC/MSFC2（Cisco IOS ソフトウェア リリース 12.1(7a)E 以降）PFC2/MSFC2（Cisco IOS ソフトウェア リリース 12.1(8a)E4 以降）
- MSFC1 ではフラグメンテーションが期待どおりに処理されない可能性があるので、VLAN インターフェイス（SVI）に PFC/MSFC1 を使用している場合は、ジャンボ フレームを使用しないことを推奨します。
- 同じ VLAN 内のパケット（レイヤ 2 ジャンボ）に対しては、フラグメンテーションがサポートされません。
- VLAN またはサブネットをまたいでフラグメンテーションが必要になるパケット（レイヤ 3 ジャンボ）は、ソフトウェアに送信されてフラグメント化されます。

Catalyst 6500/6000 の Cisco IOS ソフトウェアにおけるジャンボ フレームのサポートについて

ジャンボ フレームとは、デフォルトのイーサネット フレーム サイズよりも大きなフレームのことです。 ジャンボ フレーム サポートをイネーブルにするには、デフォルトよりも大きな MTU サイズをポートまたは VLAN インターフェイスで設定し、Cisco IOS ソフトウェア リリース 12.1(13)E 以降で、グローバルな LAN ポート MTU サイズを設定します。

ブリッジングまたはルーティングされるトラフィックに対する Cisco IOS ソフトウェアのサイズ チェック

ライン カード	入力	出力
10、10/100、100 Mbps ポート	MTU サイズ チェックが行われる。 ジャンボ フレーム サポートにより、デフォルト以外の MTU サイズが設定されている入力側の 10、10/100、100 Mbps イーサネット ポートおよび 10-GE LAN ポートのグローバル LAN ポート MTU サイズと、入力トラフィックのサイズとが比較されます。 サイズが大きすぎるトラフィックはポートで廃棄されます。	MTU サイズ チェックは行われない。 デフォルト以外の MTU サイズが設定されたポートでは、64 バイトを超える任意のサイズのパケットを含むフレームが転送されます。 デフォルト以外の MTU サイズが設定されている場合、10、10/100、100 Mbps のイーサネット LAN ポートでは、出力フレームのサイズ チェックは行われません。
GE ポート	MTU サイズ チェックは行われない。 デフォルト以外の MTU サイズが設定されたポートでは、64 バイトを超える任意のサイズのパケットを含むフレームが受け入れられ、入力フレームのサイズ チェックは行われません。	MTU サイズ チェックが行われる。 ジャンボ フレーム サポートにより、デフォルト以外の MTU サイズが設定されている出力側の GE ポートおよび 10-GE LAN ポートのグローバル出力 LAN ポート MTU サイズと、出力トラフィックのサイズとが比較されます。 サイズが大きすぎるトラフィックはポートで廃棄されます。
10-GE ポート	MTU サイズ チェックが行われる。 サイズが大きすぎるトラフィックはポートで廃棄されます。	MTU サイズ チェックが行われる。 サイズが大きすぎるトラフィックはポートで廃棄されま

		す。
SVI	MTU サイズ チェックは行われない。 SVI では、入力側のフレーム サイズはチェックされません。	MTU サイズ チェックが行われる。 SVI の出力側では、MTU サイズがチェックされます。
	PFC	
ルーティング対象の全トラフィック	ルーティングが必要なトラフィックの場合、PFC のジャンボ フレーム サポートにより、設定された MTU サイズとトラフィックのサイズとが比較され、トラフィックを処理するのに十分な大きさの MTU サイズが設定されたインターフェイス間でジャンボ トラフィックのレイヤ 3 スイッチングが行われます。 十分な大きさの MTU サイズが設定されていないインターフェイス間では、次の処理が行われます。 • Don't Fragment (DF) ビットが設定されていない場合は、PFC から MSFC にトラフィックが送信され、フラグメント化とルーティングがソフトウェアによって実行されます。 • DF ビットが設定されている場合は、PFC によってトラフィックが廃棄されます。	

Cisco の推奨事項

ジャンボ フレームを正しく実装すると、フラグメンテーション オーバーヘッドの削減 (およびエンド デバイスの CPU オーバーヘッドの低減) により、イーサネット接続の TCP スループットが 6 倍向上する可能性があります。

指定した MTU サイズを処理できないデバイスが経路内に存在しないことを確認する必要があります。 そのようなデバイスによりパケットがフラグメント化されて転送されると、処理全体の意味がなくなります。 この結果、そのようなデバイスでパケットのフラグメント化と再構成が行われることにより、オーバーヘッドが増加する可能性があります。

そのような場合、IP パス MTU ディスカバリを使用すると、各パスでトラフィックを送信するのに適した最小の共通パケット長を送信元デバイスで確認できます。 あるいは、ネットワーク内でサポートされているすべての MTU サイズの最小値をジャンボ フレーム対応ホスト デバイスの MTU サイズとして設定する方法もあります。

指定した MTU サイズをサポートできるかどうかを確認するには、各デバイスを注意深くチェックする必要があります。 このセクションにある MTU サイズ サポートの表を参照してください。

ジャンボ フレーム サポートは、次のタイプのインターフェイスでイネーブルにできます。

- ポート チャネル インターフェイス
- SVI
- 物理インターフェイス (レイヤ 2/レイヤ 3)

ポート チャネルまたはポート チャネルに参加する物理インターフェイスではジャンボ フレームをイネーブルにできます。 すべての物理インターフェイスの MTU が一致していることを必ず確認してください。 そうしないと、インターフェイスが一時停止状態になる可能性があります。 ポ

ート チャネル インターフェイスの MTU を変更するとすべてのメンバ ポートの MTU が変更されるので、ポート チャネル インターフェイスの MTU を変更してください。

注: メンバ ポートが blocking 状態になっているために、そのポートの MTU を新しい値に変更できなかった場合は、ポート チャネルが一時停止状態になります。

SVI でジャンボ フレーム サポートを設定する前に、VLAN のすべての物理インターフェイスがジャンボ フレーム対応に設定されていることを必ず確認してください。 パケットの MTU は、SVI の入力側ではチェックされません。 ただし、SVI の出力側ではサイズがチェックされます。 パケットの MTU が SVI の出力 MTU よりも大きい場合、そのパケットは (DF ビットが設定されていなければ) ソフトウェアでフラグメント化されるため、パフォーマンスが低下します。 ソフトウェアによるフラグメント化が実行されるのは、レイヤ 3 スイッチングの場合のみです。 レイヤ 3 ポートまたはより小さな MTU が設定された SVI にパケットが転送されると、ソフトウェアによるフラグメント化が実行されます。

SVI の MTU は、VLAN 内のすべてのスイッチ ポートの間で最も小さい MTU よりも常に小さくしておく必要があります。

Catalyst 4500 シリーズ

ジャンボ フレームは、Catalyst 4500 ラインカードのノンブロッキング ポートで主にサポートされます。 次のノンブロッキング GE ポートはスーパーバイザ エンジンのスイッチング ファブリックに直接接続されており、ジャンボ フレームをサポートします。

- スーパーバイザ エンジンWS-X4515、WS-X4516：Supervisor Engine IV または V のアップリンク GBIC ポート (2 個) WS-X4516-10GE — 2 10-GE アップリンクおよび 4 1-GE 小さい形式要素 プラグイン可能 な (SFP) アップリンクWS-X4013+ — 2 1-GE アップリンクWS-X4013+10GE — 2 10-GE アップリンクおよび 4 1-GE SFP アップリンクWS-X4013+TS：1-GE ポート (20 個)
- ラインカードWS-X4306-GB — 6 ポート 1000BASE-X （ GBIC ） GE モジュールWS-X4506-GB-T — 6 ポート 10/100/1000 Mbps および 6 ポート SFPWS-X4302-GB — 2ポート 1000BASE-X （ GBIC ） GE モジュール18 ポート サーバ スイッチング GE モジュール (WS-X4418-GB) の最初の 2 つの GBIC ポートおよび WS-X4232-GB-RJ モジュールの GBIC ポート
- 固定設定のスイッチWS-C4948 — すべての 48 の 1-GE ポートWS-C4948-10GE — すべての 48 の 1-GE ポートおよび 2 つの 10-GE ポート

これらのノンブロッキング GE ポートを使用すると、9 KB のジャンボ フレームやハードウェア ブロードキャスト抑制 (Supervisor Engine IV のみ) をサポートできます。 他のすべてのラインカードでは、ベビー ジャイアント フレームがサポートされています。 ベビー ジャイアントは、MPLS のブリッジングや 1552 バイトの最大ペイロードによる Q in Q パススルーに使用できます。

注: ISL/802.1Q タグによってフレーム サイズが大きくなります。

Supervisor Engine IV および V を使用する場合、ベビー ジャイアントおよびジャンボ フレームは他の Cisco IOS 機能に対して透過的に扱われます。

Cisco IOS ソフトウェアのセキュリティ機能

基本的なセキュリティ機能

以前には、多くの場合、キャンパス設計ではセキュリティが軽視されていました。 しかし今では、すべての企業ネットワークにおいてセキュリティが不可欠な要素になっています。 一般的に、多くのお客様は、Cisco のどのツールとテクノロジーを応用できるかを判断するためのセキュリティ ポリシーをすでに確立されています。

パスワード保護の基本

ほとんどの Cisco IOS ソフトウェア デバイスには、2 レベルのパスワードが設定されています。第 1 レベルのパスワードは、デバイスに対する Telnet アクセス用のパスワードです。このアクセスは、vty アクセスとも呼ばれます。 vty アクセスが許可された後は、イネーブル モードまたは特権 EXEC モードにアクセスする必要があります。

スイッチのイネーブル モードの保護

イネーブル パスワードを使用すると、デバイスに対する完全なアクセス権がユーザに与えられます。 イネーブル パスワードは信頼できるユーザにのみ与えてください。

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

パスワードを設定する際は、次の規則に従ってください。

- パスワードは 1 ~ 25 個の大文字および小文字の英数字で構成されている必要があります。
- パスワードの最初の文字には数字を使用できません。
- 先頭に空白を入力することもできますが、これらの空白は無視されます。 中間と最後の空白は認識されます。
- パスワードの検査では大文字と小文字が区別されます。 たとえば、Secret と secret は異なるパスワードとして認識されます。

注: **enable secret** コマンドでは、一方向の暗号化 Message Digest 5（MD5）ハッシング機能が使用されます。 **show running-config** を発行すると、この機能により暗号化されたパスワードが表示されます。 また、**enable password** コマンドを使用してイネーブル パスワードを設定することもできます。 ただし、**enable password** コマンドで使用される暗号化アルゴリズムは脆弱なので、元のパスワードが簡単に推測されるおそれがあります。 そのため、**enable password** コマンドは使用しないでください。 よりセキュリティに優れた **enable secret** コマンドを使用してください。 詳細は、『Cisco IOS のパスワード暗号化情報』を参照してください。

スイッチに対する Telnet/VTY アクセスの保護

デフォルトの場合、Cisco IOS ソフトウェアではアクティブな Telnet セッションが 5 つまでサポートされます。 これらのセッションは vty 0 ~ 4 と表記されます。 これらの回線をイネーブルにするとアクセスが可能になります。 ただし、ログインできるようにするためには、これらの回線にパスワードを設定する必要があります。

```
Switch(config)#line vty 0 4 Switch(config-line)#login Switch(config-line)#password password
```

login コマンドを使用すると、これらの回線が Telnet アクセス用に設定されます。 パスワードを設定するには、**password** コマンドを使用します。 パスワードを設定する際は、次の規則に従ってください。

- 最初の文字には数字を使用できません。
- 文字列には、任意の英数字を最大 80 文字まで使用できます。 使用可能な文字には空白も含まれます。
- 「<数字>-<空白>-<文字>」という形式のパスワードは指定できません。 数字の後に空白があ

ると問題が発生します。 たとえば、hello 21 は有効なパスワードですが、21 hello は有効なパスワードではありません。
- パスワードの検査では大文字と小文字が区別されます。 たとえば、Secret と secret は異なるパスワードとして認識されます。

注: 上記の vty 回線の設定では、スイッチにパスワードが平文で保存されます。 そのため、**show running-config** コマンドを発行すれば、だれでもこのパスワードを表示できてしまいます。 この状況を回避するには、**service password-encryption** コマンドを使用します。 このコマンドでは、パスワードの簡易暗号化が行われます。 このコマンドでは、VTY 回線のパスワードと、**enable password** コマンドで設定されたイネーブル パスワードだけが暗号化されます。 **enable secret** コマンドを使用して設定されたイネーブル パスワードには、さらに強力な暗号化が適用されます。 パスワードの設定には **enable secret** コマンドを使用することを推奨します。

注: セキュリティの管理をより柔軟にするために、すべての Cisco IOS ソフトウェア デバイスで Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）セキュリティ モデルを必ず実装してください。 AAA ではローカル、RADIUS、および TACACS+ の各データベースを使用できます。 詳細は、「TACACS+ 認証の設定」セクションを参照してください。

AAA セキュリティ サービス

AAA の動作の概要

アクセス コントロールでは、スイッチにアクセスする権限を持つユーザと、それらのユーザが利用できるサービスの種類が制御されます。 AAA のネットワーク セキュリティ サービスは、スイッチのアクセス コントロールを設定するための主要なフレームワークを提供します。

このセクションでは、AAA のさまざまな側面について詳しく説明しています。

- Authentication（認証）：このプロセスでは、エンド ユーザやデバイスの身元が検証されます。 最初に、ユーザの認証に使用できるさまざまな方式が指定されます。 これらの方式により、実行する認証のタイプ（TACACS+ や RADIUS など）が定義されます。 また、これらの認証方式を試みる順序も定義されます。 その後、適切なインターフェイスにこれらの方式が適用され、認証がアクティブになります。
- Authorization（認可）：このプロセスでは、ユーザ、ユーザ グループ、システム、またはプロセスにアクセス権が付与されます。 AAA プロセスでは、1 回限りの認可やタスクごとの認可も可能です。 このプロセスでは、ユーザが実行できるサービスについてのアトリビュートが（AAA サーバ上で）定義されます。 ユーザがサービスを起動しようとするたびに、スイッチから AAA サーバに対して照会が行われ、ユーザにサービスの実行を認可するよう要求されます。 AAA サーバによって承認されると、ユーザはサービスを実行することを認可されます。 AAA サーバによって承認されなかった場合、ユーザにはそのサービスを実行する権限が与えられません。 このプロセスを使用すると、一部のユーザが特定のコマンドのみを実行できるように指定できます。
- Accounting（アカウンティング）：このプロセスでは、ユーザがアクセスしたサービスや、ユーザが使用したネットワーク リソースの量を追跡できます。 アカウンティングをイネーブルにすると、スイッチから AAA サーバにアカウンティング レコードが送信されて、ユーザのアクティビティが報告されます。 報告されるユーザ アクティビティには、セッション時間、開始時刻、終了時刻などが含まれます。 これらのアクティビティを分析すると、その結果を管理や課金の目的に利用できます。

AAA は最も推奨されるアクセス コントロール方式ですが、Cisco IOS ソフトウェアには、AAA

とは別に簡単なアクセス コントロール機能も用意されています。 そのような追加機能には、次のものがあります。

- ローカル ユーザ名認証
- 回線パスワード認証
- イネーブル パスワード認証

ただし、これらの機能では、AAA と同レベルのアクセス コントロールは実現できません。

AAA についての詳細は、次のドキュメントを参照してください。

- Authentication, Authorization, and Accounting（AAA; 認証、認可、およびアカウンティング）
- アクセス サーバの基本 AAA の設定
- TACACS+ と RADIUS の比較

これらのドキュメントでは、スイッチに直接言及していない場合もあります。 ただし、これらのドキュメントで説明されている AAA の概念はスイッチにも適用できます。

TACACS+

目的

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す。 これらのパスワードは、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。 各ネットワーク デバイスでこれらのパスワードを設定するのは時間がかかる上、集中管理の観点からも好ましくありません。 また、設定ミスが起こりやすい Access Control List（ACL; アクセス コントロール リスト）を使用してアクセス制限を実装するのも難しい作業です。 これらの問題を克服するには、中央サーバでユーザ名、パスワード、アクセス ポリシーを設定するときに、中央集中型のアプローチを採用します。 中央サーバには、Cisco Secure Access Control Server（ACS）または任意のサード パーティ製サーバを使用できます。 デバイス側では、これらの中央集中型データベースを使用して AAA 機能を実行するように設定を行います。 この場合、デバイスとは Cisco IOS ソフトウェア スイッチのことです。 デバイスと中央サーバの間で使用できるプロトコルには、次のものがあります。

- TACACS+
- RADIUS
- Kerberos

このセクションの主題である TACACS+ は、Cisco ネットワークでの導入例が特に多いプロトコルです。 TACACS+ には次のような機能があります。

- Authentication（認証）：ユーザを識別し、確認するプロセス。 ユーザの認証には複数の方法を使用できます。 ただし、最も一般的に使用されている方法は、ユーザ名とパスワードの組み合せなどです。
- Authorization（認可）：ユーザがコマンドを実行しようとしたときに、スイッチから TACACS+ サーバに問い合せて、ユーザにそのコマンドを使用する権限が与えられているかどうかを確認できます。
- Accounting（アカウンティング）：このプロセスでは、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が記録されます。

TACACS+ と RADIUS の比較については、『TACACS+ と RADIUS の比較』を参照してください

。

動作の概要

TACACS+ プロトコルでは、ユーザ名とパスワードが中央サーバに転送されます。 これらの情報は MD5 一方向ハッシングによりネットワーク上で暗号化されます。 詳細は、RFC 1321 を参照してください。 TACACS+ はトランスポート プロトコルとして TCP ポート 49 を使用します。これは UDP に比べて次のような利点があります。

注: RADIUS では UDP が使用されます。

- コネクション型の転送である。
- バックエンドの認証メカニズムの負荷がどれだけ高くても、要求が受信されたことを示す確認応答（TCP ACK）が別個に送信される。
- サーバ クラッシュが迅速に検出される（リセット（RST）パケット）。

セッション中に追加の認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。 この手順により、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さらに細かく制御できるようになります。 さらに、コマンド アカウンティングを使用すると、特定のユーザが特定のネットワーク デバイスに接続している間に発行したコマンドを監査できます。

次の図に認可のプロセスを示します。

TACACS+ を使用しているネットワーク デバイスに対して、ユーザが単純な ASCII ログインを試みた場合、通常は次の認証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ます。 次に、スイッチはそのプロンプトをユーザに表示します。 ユーザがユーザ名を入力すると、スイッチは TACACS+ デーモンに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。— ユーザは認証され、サービスは始まることができます。 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。— ユーザは認証を受け損いました。 ユーザは以降のアクセスを拒否されるか、ログイン シーケンスの再試行を求められます。 この動作は、TACACS+ デーモンによって異なります。— エラーは認証の間にある時点で発生しました。 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 応答が返されると、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試みます。continue – ユーザは追加認証情報のためにプロンプト表示されます。
- 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せが発行されます。 TACACS+ デーモンは、認可の応答として ACCEPT または REJECT を返します。 ACCEPT 応答が返された場合は、EXEC または NETWORK セッションを対象ユーザに振り向けるために使用するアトリビュート形式のデータが、その応答に格納されています。 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。

基本的な AAA の設定手順

基本的なプロセスを理解しておけば、AAA の設定は比較的簡単です。 Cisco ルータまたはアクセス サーバで AAA を使用してセキュリティを設定するには、次の手順を実行します。

1. AAA をイネーブルにするには、**aaa new-model** グローバル設定コマンドを発行します。 `Switch(config)#aaa new-model` **ヒント：** Aaa コマンドを設定する前に設定を保存して下さい。 その後、AAA の設定がすべて完了し、正常に動作することを確認してから、再び設定を保存してください。 こうすると、予期しないロックアウトが（設定を保存する前に）発生した場合でも、スイッチをリロードすることで元の状態を復元できます。
2. 別途、セキュリティ サーバを使用する場合は、RADIUS、TACACS+、Kerberos などのセキュリティ プロトコルのパラメータを設定します。
3. **aaa authentication** コマンドを使用して、認証の方式リストを定義します。
4. **login authentication** コマンドを使用して、特定のインターフェイスまたは回線に方式リストを適用します。
5. オプションの **aaa authorization** コマンドを発行して、認可を設定します。
6. オプションの **aaa accounting** コマンドを発行して、アカウンティングを設定します。
7. スイッチからの認証要求と認可要求を処理できるように外部の AAA サーバを設定します。 **注:** 詳細は、ご使用の AAA サーバのマニュアルを参照してください。

TACACS+ 認証の設定

TACACS+ 認証を設定するには、次の手順を実行します。

1. グローバル コンフィギュレーション モードで **aaa new-model** コマンドを発行して、スイッチ上で AAA をイネーブルにします。
2. TACACS+ サーバおよびそれに関連付けられた鍵を定義します。この鍵は TACACS+ サーバとスイッチの間のトラフィックを暗号化するために使用されます。 **tacacs-server host 1.1.1.1 key mysecretkey** コマンドでは、TACACS+ サーバの IP アドレスは 1.1.1.1 に、暗号化鍵は mysecretkey に設定されます。 スイッチから Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）ping を発行して、TACACS+ サーバに到達可能であることを確認します。
3. 方式リストを定義します。方式リストでは、各種サービスに対して試行する認証メカニズムの順序を定義します。 これらのサービスには、次のものが含まれます。 [Enable]Login（vty/Telnet アクセスの場合）**注:** vty/Telnet アクセスについては、このドキュメントの「基本的なセキュリティ機能」セクションを参照してください。コンソール次の例では、**login** のみを想定しています。 インターフェイスまたは回線には、次のように方式リストを適用する必要があります。 `Switch(config)#aaa authentication login METHOD-LIST-LOGIN group tacacs+ line Switch(config)#line vty 0 4 Switch(config-line)#login authentication METHOD-LIST-LOGIN Switch(config-line)#password hard_to_guess` この設定の **aaa authentication login** コマンドでは、METHOD-LIST-LOGIN という架空リスト名および tacacs+ という方式が使用され、さらにその後に line という方式が使用されます。 ユーザは、最初に、TACACS+ サーバを使用して認証を受けます。 TACACS+ サーバが応答しない場合、または ERROR メッセージが返された場合は、2 番目の方式として、回線（line）に設定されたパスワードが使用されます。 ただし、TACACS+ サーバから REJECT メッセージが返されてユーザが拒否された場合、AAA ではトランザクションが完了したとみなされて 2 番目の方法は使用されません。**注:** リスト（METHOD-LIST-LOGIN）を vty 回線に適用するまで、設定は完了しません。 この例に示すように、回線設定モードで **login authentication METHOD-LIST-LOGIN** コマンドを発行してください。**注:** この例では、TACACS+ サーバが使用できない場合に備えて、バックドアを作成しています。 セキュリティ管理者によっては、バッ

クドアの実装を認める場合と認めない場合があります。 このようなバックドアを実装するかどうかは、サイトのセキュリティ ポリシーに基づいて決定してください。

RADIUS 認証の設定

RADIUS の設定は、TACACS+ の設定とほとんど同じです。 設定の中の TACACS という単語を RADIUS に置き換えるだけです。 COM ポート アクセス用の RADIUS の設定例を次に示します。

```
Switch(config)#aaa new-model Switch(config)#radius-server host 1.1.1.1 key mysecretkey
Switch(config)#aaa authentication login METHOD-LIST-LOGIN group radius line Switch(config)#line
con 0 Switch(config-line)#login authentication METHOD-LIST-LOGIN Switch(config-line)#password
hard_to_guess
```

ログイン バナー

不正アクセスに対する具体的な措置を明記した適切なデバイス バナーを作成することを推奨します。 権限のないユーザにはサイト名やネットワーク情報などを公表しないようにしてください。 このようなバナーは、デバイスへの不正アクセスが発生し、その実行者が捕まった場合に、責任を追求するための根拠となります。 ログイン バナーを作成するには、次のコマンドを発行します。

```
Switch(config)#banner motd ^C *** Unauthorized Access Prohibited *** ^C
```

物理セキュリティ

適切な許可がない限りデバイスへ物理的にアクセスできないようにする必要があります。 機器は適正に管理された（施錠された）場所に保管してください。 不正な改ざんや環境的要因によりネットワークが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には、すべての機器に対して次の措置を講じる必要があります。

- 適切な Uninterruptible Power Supply（UPS; 無停電電源装置）を設置し、可能な場合は冗長電源を確保する
- 温度管理を行う（空調）

悪意のある人物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。

管理設定

ネットワーク構成図

目的

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ベンダーやパートナーにまで情報を伝えるための、唯一の最重要の手段となります。 ネットワーク ダイアグラムを作成し、いつでも参照できるように準備しておいてください。

推奨事項

次の 3 種類のダイアグラムが必要です。

- **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や論理接続を示すダイアグラムは重要です。 階層的な設計を実装している企業では、各レイヤを別々にドキュメント化するのが一般的です。 計画時や問題解決時には、各ドメインがどのようにリンクしているかを把握することが重要です。
- **物理図**：このダイアグラムは、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。 このダイアグラムには、次のような情報を記入してください。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数シャーシ 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 ブリッジのプライオリティMAC アドレスVLAN ごとのブロッキング ポートCatalyst 6500/6000 MSFC ルータ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**：このダイアグラムは、レイヤ 3 機能のみを示します。つまり、オブジェクトとしてルータのみを示し、イーサネット セグメントとして VLAN のみを示します。 このダイアグラムには、次のような情報を記入してください。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

スイッチ管理インターフェイスとネイティブ VLAN

目的

このセクションでは、デフォルトの VLAN 1 を使用することの意義と潜在的な問題について説明しています。 また、このセクションでは、6500/6000 シリーズ スイッチ上のユーザ トラフィックと同じ VLAN 内のスイッチに管理トラフィックを転送した場合に起こり得る問題についても説明しています。

Catalyst 6500/6000 シリーズ用のスーパーバイザ エンジンおよび MSFC のプロセッサでは、多数の制御プロトコルおよび管理プロトコル用に VLAN 1 が使用されます。 次に例を示します。

- スイッチ制御プロトコル：STP BPDUVTPDTPCDP
- 管理プロトコル：SNMPTelnetSecure Shell（SSH）プロトコルSyslog

このような方法で使用されている VLAN は、ネイティブ VLAN と呼ばれます。 デフォルトのスイッチ設定では、VLAN 1 が Catalyst トランク ポートのデフォルトのネイティブ VLAN になります。 VLAN 1 をネイティブ VLAN のままにしておくこともできます。 ただし、ネットワーク内の Cisco IOS システム ソフトウェアが稼働しているスイッチでは、デフォルトで、レイヤ 2 スイッチ ポートとして設定されたすべてインターフェイスが VLAN 1 のポートにアクセスするように設定されることに注意してください。 つまり、ネットワーク内にはユーザ トラフィック用の VLAN として VLAN 1 を使用しているスイッチが存在する可能性が高いということです。

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ブロードキャスト トラフィックやマルチキャスト トラフィックによって中断される必要がないことです。 特にマルチキャスト アプリケーションは、サーバとクライアントの間で大量のデータを送信する傾向があります。 これらはスーパーバイザ エンジンには無関係なデータです。 不必要なトラフィックを受信することによってスーパーバイザ エンジンのリソースやバッファが完全に占有されてしまうと、スーパーバイザ エンジンが管理パケットを受信できなくなり、（最悪の場合は）スパニングツリーのループや EtherChannel の障害が発生する可能性があります。

show interfaces ***interface_type slot/port*** **counters** コマンドと **show ip traffic** コマンドを使用すると、次の情報を入手できます。

- ユニキャスト トラフィックに対するブロードキャスト トラフィックの割合
- IP トラフィックに対する非 IP トラフィックの割合（通常、非 IP トラフィックは管理 VLAN では必要ありません）

VLAN 1 では、ほとんどのコントロール プレーン トラフィックがタグ付けされて処理されます。 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。 大規模なキャンパス ネットワークでは、VLAN 1 の STP ドメインの直径に注意する必要があります。 ネットワークの一部で不安定状態が発生すると VLAN 1 に影響し、それによってコントロール プレーンの安定性や、すべての VLAN に対する STP の安定性にも影響が出る可能性があります。 ただし、VLAN 1 でのユーザ データの転送や STP の動作をインターフェイスで制限する方法があります。 その方法とは、単にトランク インターフェイスで VLAN を設定しないことです。

ネットワーク アナライザで見るとわかりますが、このように設定しても、VLAN 1 内のスイッチ間での制御パケットの転送は停止されません。 しかし、データは転送されず、このリンク上では 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: Catalyst 2900XL/3500XL に接続されたトランクから VLAN 1 をクリアすることはできません。

ユーザ VLAN を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/レイヤ 3 境界に制限するように配慮されている場合でも、一部のお客様は、管理 VLAN を引き続き違った方法で扱おうとされている場合があります。 そのようなお客様は、ネットワーク全体を単一の管理サブネットでカバーしたいと考えています。 中央の NMS アプリケーションが管理対象のデバイスとレイヤ 2 上で隣接してい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。 管理 VLAN の直径は、ユーザ VLAN と同じルーティング ドメイン構造に制限してください。 また、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は、アウトオブバンド管理または SSH サポート（あるいはその両方）を使用することを検討してください。

その他のオプション

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の注意が必要になる点があります。 たとえば、好ましく、よくある Ciscoマルチレイヤ デザインはアクティブスパニングツリーの使用を避ける 1 つです。 この方法で設計する場合は、各 IP サブネット/VLAN を単一のアクセスレイヤ 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、トランキングをイネーブルにして、レイヤ 2 アクセス レイヤとレイヤ 3 ディストリビューション レイヤの間で管理 VLAN を伝送した方がよいのではないかという意見もあります。 しかし、この質問に対して答えるのは簡単ではありません。 Cisco のエンジニアと設計を検討する際には、次の 2 つのオプションを考慮してください。

- **オプション 1**：用途の決まった 2 ~ 3 つの 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。 この設定では、データ VLAN、音声 VLAN、管理 VLAN などを想定しており、STP をアクティブにしなくてよいという利点があります。 トランクから VLAN 1 をクリアするには、追加の設定手順が必要になります。 また、このソリューションでは、障害回復中にルーティング トラフィックが一時的にブラック ホールに吸い込まれないようにするために、設計上の考慮が必要になります。 トランクに対して STP PortFast を使用するか（将来）、STP フォワーディングとともに VLAN 自動ステート同期を使用してください。
- **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。 最近のスイッ

チ ハードウェアを使用すれば、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、以前ほど難しい問題ではなくなっています。 最近のハードウェアには、次のような特徴があります。より強力な CPU とコントロールプレーンのレート制限機構マルチレイヤ設計で奨励されているように、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最終的には、VLAN のブロードキャスト トラフィックの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 のエンジニアと協議した上で判断を下します。 そのアクセスレイヤ スイッチ上のすべてのユーザが管理 VLAN に含まれる場合は、「Cisco IOS ソフトウェアのセキュリティ機能」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してスイッチをユーザから保護してください。

管理インターフェイスとネイティブ VLAN に関する Cisco の推奨事項

管理インターフェイス

Cisco IOS システム ソフトウェアでは、各インターフェイスをレイヤ 3 インターフェイスとして設定することも、VLAN 内のレイヤ 2 スイッチ ポートとして設定することもできます。 Cisco IOS ソフトウェアで **switchport** コマンドを使用すると、デフォルトでは、すべてのスイッチ ポートが VLAN 1 のアクセス ポートになります。 つまり、明示的に設定しない限り、デフォルトでは、VLAN 1 にユーザ データも存在する可能性があります。

VLAN 1.以外マネージメントVLAN に VLAN にマネージメントVLAN からすべてのユーザのデータを保存させます。 代わりに、各スイッチで loopback0 インターフェイスを管理インターフェイスとして設定してください。

注: OSPF プロトコルを使用する場合は、これが OSPF ルータ ID にもなります。

このループバック インターフェイスには 32 ビットのサブネット マスクを設定し、スイッチ上の純粋なレイヤ 3 インターフェイスとして設定してください。 次に例を示します。

```
Switch(config)#interface loopback 0 Switch(config-if)#ip address 10.x.x.x 255.255.255.255
Switch(config-if)#end Switch#
```

ネイティブ VLAN

ネイティブ VLAN は、ルータ上で決してイネーブルになることがない明らかなダミー VLAN になるように設定してください。 従来、Cisco では VLAN 999 を推奨していましたが、現在は任意の VLAN を選択できます。

特定のポートで特定の VLAN を 802.1Q トランキング用のネイティブ (デフォルト) VLAN として確立するには、次のインターフェイス コマンドを発行します。

```
Switch(config)#interface type slot/port Switch(config-if)#switchport trunk native vlan 999
```

トランキング設定の推奨事項については、このドキュメントの「ダイナミック トランキング プロトコル」セクションを参照してください。

アウトオブバンド管理

目的

実稼働ネットワークの周辺に別個の管理インフラストラクチャを構築すると、ネットワーク管理のアベイラビリティが向上します。 このように設定すれば、現在処理されているトラフィックの種類や、コントロール プレーンで発生したイベントの種類に関係なく、リモートからデバイスに

到達可能になります。 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ケーブル接続します。

注: 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 ルータから RJ-45 シリアル ケーブルを介してレイアウト内のすべてのルータ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 サーバ接続が可能になります。 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は 1 台のモデムを接続できます。 このように構成すると、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。 詳細は、『Catalyst スイッチのコンソール ポートへのモデムの接続』を参照してください。

推奨事項

この構成では、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 パスを使用できます。 こうすることで、ネットワーク管理のアベイラビリティが向上します。 次のような利点があります。

- このように構成すると、管理トラフィックがユーザ データから切り離される。
- 管理 IP アドレスは、分離されたサブネット、VLAN、およびスイッチ内に存在するため、セキュリティが向上する。
- ネットワーク障害の発生時でも管理データを確実に配送できる。
- 管理 VLAN にはアクティブなスパニング ツリーがない。 ここでの冗長性は重要ではありません。

次の図にアウトオブバンド管理の概要を示します。

システム ロギング

目的

syslog メッセージは Cisco 独自の機能であり、標準の SNMP よりも応答性の高い正確な情報を提供します。 たとえば、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、syslog 情報を利用して、インベントリや設定の変更に関する情報が収集されます。

Cisco の推奨する Syslog 設定

システム ロギングは、システム運用時に一般に利用され広く受け入れられた手法です。 UNIX の syslog では、ルータに関する次のような情報やイベントをキャプチャして、分析を行えます。

- インターフェイスのステータス
- セキュリティ アラート
- 環境条件
- CPU プロセスの大量使用
- その他のイベント

Cisco IOS ソフトウェアでは、UNIX の syslog サーバに対して UNIX のロギングを出力できます。 Cisco の UNIX syslog フォーマットは、4.3 Berkeley Standard Distribution (BSD) UNIX と互換性があります。 次に示す Cisco IOS ソフトウェアのログ設定を使用してください。

- **no logging console**：デフォルトでは、すべてのシステム メッセージがシステム コンソールに送信されます。 Cisco IOS ソフトウェアでは、コンソール ロギングは優先度の高いタスクになっています。 この機能は、システム障害が発生する前にシステム オペレータに対してエラー メッセージを表示することを主な目的としています。 ルータやスイッチがターミナルからの応答を待っている間にハングするような事態を避けるために、すべてのデバイスの設定でコンソール ロギングをディセーブルにしてください。 ただし、コンソール メッセージは障害切り分けの際に役立つ場合があります。 そのような場合には、コンソール ロギングをイネーブルにしてください。 **logging console level** コマンドを発行すると、適切なレベルのメッセージ ロギングを取得できます。 指定できるロギング レベルは 0 ~ 7 です。
- **no logging monitor**：このコマンドを発行すると、システム コンソール以外のターミナル回線のロギングがディセーブルになります。 場合によっては、(**logging monitor debugging** または他のコマンド オプションを使用して) モニタ ロギングが必要になることがあります。 そのような場合は、該当するアクティビティを調べるために必要なロギング レベルを指定してモニタ ロギングをイネーブルにしてください。 ロギング レベルについての詳細は、この一覧にある **no logging console** の項を参照してください。
- **logging buffered 16384**：システム メッセージを内部ログ バッファでロギングするには、**logging buffered** コマンドを追加する必要があります。 ロギング バッファは循環使用されます。 ロギング バッファがいっぱいになると、古いエントリが新しいエントリで上書きされます。 ロギング バッファのサイズは、バイト単位でユーザが指定できます。 システム バッファのサイズはシステムごとに異なります。 16384 は適切なデフォルト値であり、ほとんどの場合に十分なロギングが行えます。
- **logging trap notifications**：このコマンドを発行すると、指定した syslog サーバに notification レベル (5) のメッセージが送信されます。 すべてのデバイス (コンソール、モニタ、バッファ、およびトラップ) のデフォルトのロギング レベルは、debugging (レベル 7) です。 トラップ ロギング レベルを 7 のままにしておくと、ネットワークの健全性にはほとんど関係のない余分なメッセージが大量に生成されます。 トラップのデフォルト ロギング レベルは 5 に設定してください。
- **logging facility local7**：このコマンドを発行すると、UNIX syslog のデフォルトのロギング ファシリティおよびレベルが設定されます。 同じファシリティおよびレベルのメッセージを受信するように syslog サーバを設定してください。
- **logging host**：このコマンドを発行すると、UNIX ロギング サーバの IP アドレスが設定されます。
- **logging source-interface loopback 0**：このコマンドを発行すると、syslog メッセージのデフォルト IP SA が設定されます。 ロギング SA を固定設定しておくと、メッセージを送信したホストの特定が容易になります。
- **service timestamps debug datetime localtime show-timezone msec**：デフォルトでは、ログ

メッセージにタイムスタンプは付加されません。 このコマンドを使用すると、ログ メッセージのタイムスタンプをイネーブルにして、システム デバッグ メッセージのタイムスタンプを設定できます。 タイムスタンプにより、ログに記録されたイベントの相対時間を把握できるので、リアルタイムでのデバッグが容易になります。 この情報は、お客様がテクニカル サポート担当者に支援を求めるためにデバッグ出力を送る際に特に役立ちます。 システム デバック メッセージのタイムスタンプをイネーブルにするには、グローバル コンフィギュレーション モードでこのコマンドを使用します。 このコマンドの効果は、デバッグがイネーブルになっている場合にのみ現れます。

注: さらに、すべてのインフラストラクチャ ギガビット インターフェイスで、リンク状態とバンドル状態に関するロギングをイネーブルにしてください。

Cisco IOS ソフトウェアは、syslog サーバを宛先とするすべてのシステム メッセージのファシリティとログ レベルを設定するための単一のメカニズムを提供します。 ロギング トラップ レベルは notification（レベル 5）に設定してください。 トラップ メッセージ レベルを notification に設定すると、syslog サーバに転送される情報メッセージの数を最小限に抑えることができます。 この設定により、ネットワーク上の syslog トラフィックの量を大幅に削減でき、syslog サーバのリソースへの影響を少なくできます。

syslog メッセージの送信をイネーブルにするには、Cisco IOS ソフトウェアが稼働する各ルータおよびスイッチの設定に次のコマンドを追加します。

- グローバルな syslog 設定コマンド
  no logging console no logging monitor logging buffered 16384 logging trap notifications logging facility local7 logging host-ip logging source-interface loopback 0 service timestamps debug datetime localtime show-timezone msec service timestamps log datetime localtime show-timezone msec
- インターフェイス レベルの syslog 設定コマンド
  logging event link-status logging event bundle-status

SNMP

目的

SNMP を使用すると、ネットワーク デバイスの MIB に保存された統計情報、カウンタ、およびテーブルを取得できます。 HP OpenView などの NMS では、この情報を使用して次のことを行えます。

- 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作成
- 設定チェックおよびトラブルシューティング チェックを実行するための準備

SNMP 管理インターフェイスの動作

SNMP は、SNMP マネージャとエージェントの間で通信を行うためのメッセージ フォーマットを提供するアプリケーション層のプロトコルです。 SNMP では、ネットワーク内のデバイスの監視と管理に使用できる標準フレームワークと共通言語が提供されます。

SNMP フレームワークは、次の 3 つの要素で構成されます。

- SNMP マネージャ

- SNMP エージェント
- MIB

SNMP マネージャは、SNMP を使用してネットワーク ホストのアクティビティの制御と監視を行うシステムです。 最も広く使用されている管理システムは、NMS と呼ばれています。 NMS という用語は、ネットワーク管理に使用される専用デバイス、またはそのようなデバイス上で使用されるアプリケーションのどちらにも適用されます。 さまざまなネットワーク管理アプリケーションが SNMP とともに使用可能です。 それらの中には、簡単な CLI アプリケーションから、CiscoWorks 製品のように豊富な機能を備える GUI まで、さまざまなアプリケーションがあります。

SNMP エージェントは、管理対象デバイスの内部で動作するソフトウェア コンポーネントであり、デバイスのデータを保持し、必要に応じて管理システムにそれらのデータを報告します。 エージェントと MIB はルーティング デバイス (ルータ、アクセス サーバ、またはスイッチ) 上に存在します。 Cisco ルーティング デバイス上の SNMP エージェントをイネーブルにするには、マネージャとエージェントの間の関係を定義する必要があります。

MIB は、ネットワーク管理情報用の仮想情報保管領域です。 MIB は、管理対象オブジェクトの集合体で構成されています。 MIB 内には、MIB モジュールで定義された関連オブジェクトの集合体があります。 MIB モジュールは、STD 58、RFC 2578 、RFC 2579 、および RFC 2580 で定義されているように、SNMP MIB モジュール言語で記述されています。

注: 個々の MIB モジュールも MIB と呼ばれます。 たとえば、インターフェイス グループ MIB (IF-MIB) は、システム上の MIB の中にある MIB モジュールです。

SNMP エージェントには MIB 変数が保存されており、SNMP マネージャは get 操作または set 操作を通じて、これらの値の取得または変更を要求できます。 マネージャでは、エージェントからの値の取得またはエージェントへの値の保存が可能です。 デバイス パラメータおよびネットワーク データに関する情報のリポジトリである MIB から、エージェントによって値が収集されます。 エージェントは、データの get または set がマネージャから要求された際に応答することもできます。

マネージャは、MIB 値の取得および設定の要求を送信できます。 エージェントはこれらの要求に応答できます。 このやりとりとは別に、エージェント側からは、任意の通知 (トラップまたはインフォーム) をマネージャに送信して、ネットワークの状況をマネージャに通知できます。 NMS 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 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発行できます。 また、リアルタイム アラートのために NMS へのトラップ メッセージを生成するようにネットワーク デバイスを設定することもできます。 トラップの転送には、IP UDP ポート 161 および 162 が使用されます。

SNMP 通知の動作の概要

SNMP の主要機能は SNMP エージェントからの通知を作成する機能です。 これらの通知を受信するために SNMP マネージャ側から要求を送信する必要はありません。 任意の (非同期の) 通知は、トラップまたはインフォーム要求として作成されます。 トラップは、SNMP マネージャにネットワークの状態に関する警告を与えるメッセージです。 インフォーム要求 (インフォーム) は、SNMP マネージャに対する受信確認の要求を含んだトラップです。 これらの通知を使用すると、次のような重要なイベントを報告できます。

- 不適切なユーザ認証
- 再起動
- 接続のクローズ
- 隣接ルータへの接続の喪失

- その他のイベント

トラップの場合、受信側はトラップを受信しても確認応答を返さないので、信頼性はインフォームよりも低くなります。 送信側は、トラップが受信されたかどうかを判断できません。 インフォーム要求の場合、SNMP マネージャは、要求を受信すると SNMP 応答 Protocol Data Unit (PDU; プロトコル データ ユニット) を使用して確認応答を返します。 マネージャがインフォーム要求を受信しなかった場合、応答は返されません。 応答がまったく返されない場合は、送信側からインフォーム要求を再び送信できます。 そのため、インフォームの方が、目的の宛先に到達できる可能性が高くなります。

ただし、インフォームはルータやネットワークのリソースをより多く消費するので、多くの場合、トラップの方が好んで使用されます。 トラップは送信されると即座に廃棄されます。 それに対し、インフォーム要求は、応答が返されるか、要求時間がタイムアウトになるまでメモリ内に残しておく必要があります。 さらに、トラップの送信回数は 1 回だけですが、インフォームは数回、繰り返し送信される場合があります。 再送信の回数が増えるとトラフィックが増加し、ネットワークのオーバーヘッドが高くなる原因にもなります。 このように、トラップとインフォーム要求の間には、信頼性とリソースのトレードオフの関係があります。 SNMP マネージャですべての通知を受信する必要がある場合は、インフォーム要求を使用してください。 ただし、ネットワークのトラフィック量やルータのメモリに関する懸念があり、必ずしもすべての通知を受信しなくてもよい場合は、トラップを使用してください。

次のダイアグラムはトラップとインフォーム要求の違いを示しています。

上のダイアグラムは、エージェント ルータから SNMP マネージャにトラップが正しく送信されたことを示しています。 マネージャはトラップを受信しますが、エージェントに確認応答を返しません。 エージェント側では、トラップが宛先に到達したかどうかを認識する方法はありません。

上のダイアグラムは、エージェント ルータからマネージャにインフォーム要求が正しく送信されたことを示しています。 マネージャはインフォーム要求を受信すると、エージェントに応答を返します。 そのため、エージェント側では、インフォーム要求が宛先に到達したことを認識できます。 この例では、トラフィックが 2 倍になっていることに注意してください。 ただし、エージェント側では、マネージャが通知を受信したことを認識しています。

上のダイアグラムは、エージェントからマネージャにトラップが送信されましたが、トラップがマネージャに到達しなかったことを示しています。 エージェント側では、トラップが宛先に到達しなかったことを認識する方法がないため、トラップは再送信されません。 そのため、マネージャはこのトラップを受信できません。

上のダイアグラムは、エージェントからマネージャにインフォーム要求が送信されましたが、インフォーム要求がマネージャに到達しなかったことを示しています。 マネージャがインフォーム要求を受信しなかったため、応答は返されません。 一定期間が過ぎると、エージェントはインフォーム要求を再送信します。 2 回目には、マネージャがインフォーム要求を受け取ったので、応答が送信されます。 この例では、トラフィックがさらに多くなっています。 ただし、通知は SNMP マネージャに到達しています。

Cisco の MIB および RFC の参考資料

一般的に、MIB モジュールは、RFC ドキュメントで定義されています。 RFC ドキュメントは、国際的な標準化機関である Internet Engineering Task Force (IETF; インターネット技術特別調査委員会) に提出されます。 RFC は個人または団体によって執筆され、Internet Society (ISOC; インターネット学会) およびインターネット コミュニティ全体で検討されます。 標準化のプロセスと IETF の活動については、Internet Society のホームページを参照してください。 Cisco のドキ

ュメントで参照されている RFC、Internet Draft (I-D; インターネット ドラフト) 、および STD の全文は、IETF のホームページで閲覧できます。

Cisco の SNMP 実装では、次の標準が採用されています。

- RFC 1213 に記述されている MIB II 変数の定義
- RFC 1215 に記述されている SNMP トラップの定義

Cisco では、すべてのシステムに独自の MIB 拡張機能を付加して提供しています。 Cisco のエンタープライズ MIB は、マニュアルに特別な記載がない限り、関連する RFC のガイドラインに準拠しています。 MIB モジュールの定義ファイルおよび各 Cisco プラットフォームでサポートされている MIB のリストは、Cisco の MIB ホームページで参照できます。

SNMP のバージョン

Cisco IOS ソフトウェアでは次のバージョンの SNMP がサポートされています。

- SNMPv1：RFC 1157 で定義されているすべてのインターネット標準。 RFC 1067 および RFC 1098 として公開された以前のバージョンは、RFC 1157 によって置き換えられました。セキュリティはコミュニティ ストリングに基づいて実現されています。
- SNMPv2c：SNMPv2 用のコミュニティ ストリング ベースの管理フレームワーク。 SNMPv2c (c はコミュニティの略) は、RFC 1901 、RFC 1905 、および RFC 1906 で定義されている実験的なインターネット プロトコルです。 SNMPv2c は、SNMPv2p (SNMPv2 Classic) のプロトコル動作とデータ型の更新版です。 SNMPv2c では、SNMPv1 のコミュニティ ベースのセキュリティ モデルが使用されます。
- SNMPv3：RFC 2273 、RFC 2274 、および RFC 2275 で定義されている相互運用可能な標準ベースのプロトコル。 SNMPv3 では、ネットワーク上での認証とパケット暗号化の組み合せにより、デバイスへのアクセスが保護されます。SNMPv3 には次のセキュリティ機能があります。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検出されないようにします。

SNMPv1 と SNMPv2c の両方では、コミュニティ ベースのセキュリティ方式が使用されています。 IP アドレスの ACL とパスワードを設定して、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 では、バルク取得メカニズムや、管理ステーションに対するより詳細なエラー メッセージの報告などがサポートされています。 バルク取得メカニズムでは、テーブルおよび大量の情報の取得がサポートされており、必要なラウンド トリップ回数を最小限に抑えることができます。 SNMPv2c で改善されたエラー処理サポートには、さまざまな種類のエラー状態を区別できるように拡張されたエラー コードが含まれます。 これらの状態は、SNMPv1 では単一のエラー コードで報告されていました。 エラー リターン コードで、エラー タイプが報告されるようになりました。

SNMPv3 では、セキュリティ モデルとセキュリティ レベルの両方が提供されています。 セキュリティ モデルとは、ユーザまたはユーザが属するグループに対して設定される認証戦略です。 セキュリティ レベルとは、セキュリティ モデル内で許可されるセキュリティのレベルです。 セキュリティ モデルとセキュリティ レベルの組み合せにより、SNMP パケットを処理する際にどのセキュリティ メカニズムを使用するかが決定されます。

一般的な SNMP の設定

SNMP 管理をイネーブルにするには、すべてのカスタマー スイッチで次のコマンドを発行します。

- SNMP ACL 用のコマンド：`Switch(config)#`**`access-list 98 permit`** *`ip_address !--- This is the SNMP device ACL.`*
- グローバルな SNMP コマンド：
  `!--- These are sample SNMP community strings.` `Switch(config)#`**`snmp-server community RO-community ro 98 snmp-server community RW-community rw 98 snmp-server contact Glen Rahn (Home Number) snmp-server location`** *`text`*

SNMP トラップに関する推奨事項

SNMP は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イネーブルになっており、使用されています。

SNMP エージェントは、複数のマネージャと通信可能です。 そのため、特定の管理ステーションとの通信には SNMPv1 を使用し、別の管理ステーションとの通信には SNMPv2 を使用するようにソフトウェアを設定することもできます。 NMS プラットフォームにおける SNMPv3 のサポートは、ネットワーク デバイスのサポート面で少し遅れているため、ほとんどの NMS では、引き続き SNMPv1 および SNMPv2c が使用されています。

使用中のすべての機能に対して SNMP トラップをイネーブルにしてください。 その他の機能は、必要に応じてディセーブルにできます。 トラップをイネーブルにした後は、**test snmp** コマンドを発行して、NMS で エラーが適切に処理されるように設定できます。 そのような処理の例には、ポケットベルへのアラート送信やポップアップなどがあります。

デフォルトでは、すべてのトラップはディセーブルになっています。 次の例に示すように、コア スイッチですべてのトラップをイネーブルにしてください。

`Switch(config)#`**`snmp trap enable`** `Switch(config)#`**`snmp-server trap-source loopback0`**
また、重要なポート (ルータやスイッチへのインフラストラクチャ リンクなど) および重要なサーバ ポートに関するポート トラップもイネーブルにしてください。 その他のポート (ホスト ポートなど) に関しては、トラップをイネーブルにする必要はありません。 ポートを設定して、リンク アップ/ダウン通知をイネーブルにするには、次のコマンドを発行します。

`Switch(config-if)#`**`snmp trap link-status`**
次に、トラップを受信して適切なアクションを実行するデバイスを指定します。 現在は、それぞれのトラップ宛先を SNMPv1、SNMPv2、または SNMPv3 の受信デバイスとして設定できるようになっています。 SNMPv3 デバイスには、UDP トラップではなく、信頼性の高いインフォームを送信できます。 次に設定例を示します。

`Switch(config)#`**`snmp-server host`** *`ip_address`* **`[traps | informs] [version {1 | 2c | 3}]`** *`community-string !--- This command needs to be on one line. !--- These are sample host destinations for SNMP traps and informs.`* **`snmp-server host 172.16.1.27 version 2c public snmp-server host 172.16.1.111 version 1 public snmp-server host 172.16.1.111 informs version 3 public snmp-server host 172.16.1.33 public`**

SNMP ポーリングに関する推奨事項

キャンパス ネットワークでは、次に示す主要な MIB を必ずポーリングまたは監視してください。

注: これは Cisco ネットワーク管理コンサルティング グループからの勧告です。

ネットワーク タイム プロトコル

目的

Network Time Protocol (NTP; ネットワーク タイム プロトコル) (RFC 1305) を使用すると、分散されたタイム サーバとクライアントの間でタイムキーピング処理が同期されます。 NTP を使用すると、システム ログが作成された際や、その他の定期的イベントが発生した際に、それぞれのイベントを相互に関連付けることができます。

動作の概要

NTP は RFC 958 で最初に明文化されました。 その後、NTP は RFC 1119 (NTP バージョン 2) でさらに進化しました。 現在の NTP は、RFC 1305 で定義されているバージョン 3 になっています。

NTP を使用すると、コンピュータ クライアントやサーバの時刻が、別のサーバまたは基準タイム ソース (無線、衛星受信機、モデムなど) と同期されます。 一般に、NTP を使用した場合のクライアント時刻の精度は、正確に同期されたプライマリ サーバを基準として、LAN で 1 ミリ秒以内、WAN で数 10 ミリ秒以内です。 たとえば、Global Positioning Service (GPS; 全地球測位システム) の受信機を利用して、世界標準時 (UTC) に合わせるために NTP を使用することもできます。

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。

NTP は UDP 上で動作し、UDP は IP 上で動作します。 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。

現在は、NTP バージョン 3 (NTPv3) と NTP バージョン 4 (NTPv4) の実装を利用できます。 現在開発中の最新のソフトウェア リリースは NTPv4 ですが、正式なインターネット標準は今のところ NTPv3 です。 また、このプロトコルの実装をカスタマイズして提供しているオペレーティング システム ベンダーもあります。

NTP セーフガード

NTP の実装には、時刻が正確でない可能性があるマシンとの同期を避ける機能もあります。 NTP では、この機能が次の 2 つの方法で実行されます。

- それ自身で同期処理を行っていないマシンとは同期しない。
- 複数のマシンから報告される時刻を常に比較し、他のマシンと大幅に時刻がずれているマシンとは、たとえそのマシンの Stratum 番号が小さくても同期しない。

アソシエーション

NTP を実行しているマシン間の通信はアソシエーションと呼ばれ、通常は静的に設定されています。 各マシンには、アソシエーションを形成する必要があるすべてのマシンの IP アドレスが通知されます。 アソシエーションを持つマシンのペアの間で NTP メッセージが交換されることにより、正確なタイムキーピングが可能になります。 ただし、LAN 環境では、IP ブロードキャスト メッセージを使用するように NTP を設定できます。 この方法を使用すると、ブロードキャスト メッセージを送受信するようにマシンを設定できますが、情報の流れが一方向であるため、タイムキーピングの精度は少し下がります。

Cisco の NTP 実装では、ネットワークがインターネットから孤立した場合に、実際には他の方法で時刻を決定していても、あたかも NTP を使用して同期しているように動作するようにマシンを設定できます。 他のマシンは NTP を使用して、そのマシンと同期します。

NTP アソシエーションは次のいずれかになります。

- ピア アソシエーションこのシステムは、自身の時刻を相手側のシステムに合わせて同期することも、相手側のシステムの時刻を自身に合わせて同期させることもできます。
- サーバ アソシエーションこのシステムは、相手側のシステムに合わせて自身の時刻を同期することのみが可能です。 相手のシステムは、このシステムの時刻には同期されません。

他のシステムとの間で NTP アソシエーションを形成するには、グローバル コンフィギュレーション モードで次のいずれかのコマンドを使用します。

コマンド	目的
ntp peer *ip-address* [normal-sync] [version *number*] [key *key-id*] [source *interface*] [prefer]	他のシステムとのピア アソシエーションの形成
ntp server *ip-address* [version *number*] [key *key-id*] [source *interface*] [prefer]	他のシステムとのサーバ アソシエーションの形成

注: アソシエーションを設定する必要があるのは、片側のみです。 相手側のシステムでは、自動的にアソシエーションが確立されます。

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 に直接同期されています。 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 サーバに同期されている公開セカンダリ サーバは約 100 台あります。 これらのサーバにより、インターネット上の合計 10 万台を超えるクライアントとサーバは同期されています。 最新のリストは、『Public NTP Servers』 のページに掲載されており、頻繁に更新されています。

また、通常は公開されていないプライベートのプライマリ サーバやセカンダリ サーバも数多く存在します。 公開 NTP サーバのリストとその使用方法については、『The Network Time Protocol Project』（University of Delaware）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、または正確な時刻が提供されるかどうかは保証されていません。 そのため、他のオプションを検討する必要があります。 たとえば、多数のルータに直接接続されたスタンドアロンの GPS デバイスを利用するという方法があります。

また、さまざまなルータを Stratum 1 マスターとして設定する方法もあります。 ただし、そのようなルータを使用することは推奨されません。

Stratum

NTP では、信頼できる時刻ソースからそのマシンが何ホップ離れているか示すために Stratum（層）という概念が使用されます。 Stratum 1 のタイム サーバには、電波時計や原子時計が直接接続されています。 Stratum 2 のタイム サーバは、Stratum 1 のタイム サーバから時刻を受信し、その時刻を順次下位のサーバに伝達します。 NTP を実行しているマシンは、NTP を使用して通信するように設定されているマシンの中で Stratum 番号が最も小さいマシンを自身の時刻ソースとして自動的に選択します。 この手法により、NTP スピーカの自動編成型ツリーが適

切に構築されます。

NTP では、時刻が正確でない可能性があるデバイスとの同期が回避されます。 詳細は、「ネットワーク タイム プロトコル」の「**NTP セーフガード**」セクションを参照してください。

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しますが、クライアントの時刻ソースから日付情報を取り込もうとはしません。
- ピアは、クライアントからの要求に応答するだけでなく、より正確な時刻ソースの候補としてクライアントの要求を利用し、自身のクロック周波数の安定化に役立てます。
- 真の意味でのピアになるためには、接続の両側でピア関係が確立される必要があります。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。 信頼できるホストどうし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ようにしてください。
- クライアントからサーバに要求が送信された場合、サーバがクライアントに応答した後は、クライアントから問い合せがあったことは記憶されません。
- クライアントからピアに要求された場合は、サーバがクライアントに応答します。 サーバ側ではクライアントの状態情報が保持され、タイムキーピングがどの程度正確に行われていて、どの Stratum サーバがクライアントで動作しているかが追跡されます。

NTP サーバは数千台のクライアントを問題なく処理できます。 ただし、多数のクライアント（最大で数百台のクライアント）を 1 台の NTP サーバで処理すると、状態情報を保持するためにサーバのメモリに影響が生じます。 推奨される量を超える処理を 1 台の NTP サーバで行う場合は、サーバの CPU リソースと帯域幅がさらに多く消費されます。

NTP サーバとの通信モード

サーバとの通信には、次の 2 つのモードがあります。

- ブロードキャスト モード
- クライアント/サーバ モード

ブロードキャスト モードでは、クライアントがリスニングします。 クライアント/サーバ モードでは、クライアントがサーバをポーリングします。 WAN リンクを経由しない場合は、速度の速い NTP ブロードキャストを使用できます。 WAN リンクを経由する場合は、クライアント/サーバ モード（ポーリング）を使用してください。 ブロードキャスト モードは LAN 環境向けのモードです。LAN では、多数のクライアントがサーバをポーリングする可能性があります。 ブロードキャスト モードを使用しないと、そのようなポーリングによってネットワーク上に大量のパケットが生成される可能性があります。 NTP マルチキャストは、NTPv3 ではまだ使用できませんが、NTPv4 では使用できます。

デフォルトでは、Cisco IOS ソフトウェアは NTPv3 を使用して通信を行います。 ただし、Cisco IOS ソフトウェアは以前のバージョンの NTP と下位互換性があります。

ポーリング

NTP プロトコルでは、クライアントがいつでもサーバに問い合せを発行できます。

Cisco デバイスで NTP が初めて設定されると、NTP_MINPOLL（2^4 = 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、2^14 秒（16,384 秒、つまり 4 時間 33 分 4 秒）です。 これは、NTP が応答を求めて再びポーリングを実行するまでの最大間隔になります。 現在のところ、ユーザが手動で POLL 時間を調整する方法はありません。

NTP ポーリング カウンターは 2^6 （64） 秒、または 1 最小値に、4 秒開始します。 今回は 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、増分します。 同期メッセージは、サーバまたはピアの設定に応じて、64、128、256、512、または 1024 秒のいずれかの間隔で送信されます。 フェーズロックループの動作によって現在のクロックがより安定するにつれて、ポーリングの間隔は長くなります。 フェーズロックループによりローカル クロックの水晶振動子が補正されることで、ポーリング間隔は最大で 1024 秒（17 分）になります。

この間隔は、64 秒から 1024 秒までの、2 の累乗秒（つまり、64、128、256、512、または 1024 秒）の間で変動します。 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います。 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。

NTP のポーリング間隔は、クライアントとサーバの接続が変更されると変わります。 接続が良好であるほど、ポーリング間隔は長くなります。 良好な接続とは、NTP クライアントが最後の 8 個の要求に対して 8 個の応答を受信できる状態を意味します。 その場合は、ポーリング間隔が 2 倍になります。 1 つでも応答を受信できなかった場合は、ポーリング間隔が半分になります。 ポーリング間隔は 64 秒に開始し、1024 秒の最大に行きます。 ポーリング間隔が 64 秒行くことができるからから 1024 秒があるやや以上 2 時間ように最高の状況で、必要な時間が。

ブロードキャスト

NTP のブロードキャストは転送されません。 **ntp broadcast** コマンドを発行すると、このコマンドが設定されたインターフェイスから NTP ブロードキャストの発信が開始されます。

一般的には、クライアント エンド ステーションおよびサーバに NTP サービスを提供するために、**ntp broadcast** コマンドを発行して NTP ブロードキャストを LAN に送出します。

時刻の同期

クライアントをサーバに同期するには、数回のパケット交換が必要になります。 交換が行われるたびに、要求と応答のペアが生成されます。 クライアントは要求を送信する際に、自身のローカル タイムを送信パケット内に記録します。 サーバはこのパケットを受信すると、自身が推定した現在時刻をパケット内に記録して、このパケットを返します。 クライアントはこの応答を受信すると、自身の受信時刻をもう一度記録して、パケットの移動時間を推定します。

これらの時間差に基づいて、サーバからクライアントにパケットを転送するために要した時間を推定できます。 現在時刻の推定では、この往復時間が考慮されます。 往復時間が短いほど、現在時刻の推定は正確になります。

対応するパケット交換が数回行われるまで、時刻は受け入れられません。 いくつかの必要な値が段階式のフィルタにかけられ、サンプルの品質が評価されます。 通常、NTP クライアントがサーバと同期するまでには約 5 分かかります。 興味深いことに、定義上まったく遅延がないローカル基準クロックでも、同様の現象が見られます。

さらに、ネットワーク接続の品質も、最終的な精度に影響します。 遅延の程度を予測できない低速なネットワークは、時刻の同期に悪影響を及ぼします。

NTP で同期を行うには、時間差が 128 ミリ秒未満に収まっている必要があります。 ネットワーク遅延の程度によりばらつきはありますが、インターネットの一般的な精度は、およそ 5 ~ 100 ミリ秒です。

NTP のトラフィック レベル

NTP で利用される帯域幅はごくわずかです。 通常、ピア間で交換されるポーリング メッセージの間隔は、17 分（1024 秒）ごとに 1 メッセージの間隔まで徐々に近づいていきます。 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ように設定してください。

収束した NTP クライアントは、サーバごとにおよそ 0.6 ビット/秒（bps）を消費します。

Cisco の推奨する NTP の設定

- 高い精度と信頼性を実現するために、複数のタイム サーバと多様なネットワーク パスを利用することを推奨します。 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。
- RFC によると、たとえポーリング対象のすべてのサーバが信頼できるかどうか確信を持てない場合でも、NTP は、複数の異なるタイム サーバをポーリングし、複雑な統計分析を使用して有効な時刻を導出できるように設計されています。 NTP では、すべてのクロックの誤差が推定されます。 そのため、すべての NTP サーバからは、現在の誤差の推定値とともに時刻が返されます。 複数のタイム サーバを使用する場合、NTP では、ある時点でこれらのサーバの時刻が一致することが期待されます。
- Cisco の NTP 実装では、Stratum 1 サービスがサポートされていません。 そのため、電波時計や電子時計には接続できません。 Cisco では、IP インターネット上の公開 NTP サーバのタイム サービスをネットワーク内で利用することを推奨しています。
- すべてのクライアント スイッチから NTP サーバに Time-of-Day 要求が定期的に送信されるように設定してください。 迅速に同期できるように、各クライアントで最大 10 個のサーバ/ピア アドレスを設定できます。
- プロトコル オーバーヘッドを削減するために、残りのローカルネット ホストに対しては、セカンダリ サーバから時刻を配信するように NTP を設定してください。 信頼性を高めるため、一部のホストに低精度の比較的安価なクロックを搭載しておくと、プライマリ サーバやセカンダリ サーバで障害が発生した場合や、サーバ間の通信パスで障害が発生した場合のバックアップとして利用できます。
- **ntp update-calendar**：通常、NTP では、システム クロックのみが変更されます。 このコマンドを使用すると、カレンダーの日時情報を NTP で更新できます。 更新されるのは、NTP 時刻が同期されている場合のみです。 そうでない場合、カレンダーの時刻は更新されず、NTP 時刻やシステム クロックも変更されません。 このコマンドは、常にハイエンド ルータで使用してください。
- **clock calendar-valid**：このコマンドを発行すると、カレンダー情報が有効であり、同期されていることが宣言されます。 このオプションは、NTP マスターで使用します。 このオプションが設定されていない場合、カレンダーを持つハイエンド ルータでは、NTP マスター回線が存在している場合でも、自身の時刻が引き続き信頼できないものとみなされます。
- 15 を超える Stratum 番号はすべて、同期されていないものとみなされます。 クロックが同期されていないルータで **show ntp status** コマンドを発行した場合、出力に Stratum 16 と表示されるのはこのためです。 マスターが公開 NTP サーバと同期されている場合は、NTP マスター回線の Stratum 番号が、ポーリング対象の公開サーバの中で最も高い Stratum 番号よりも 1 ~ 2 高く設定されていることを確認してください。
- 現在、お客様の多くは Cisco IOS ソフトウェア プラットフォームで NTP をサーバ モードに設定し、インターネット上の信頼できるタイム サーバや電波時計に同期させています。 社内では、多数のスイッチを運用している場合、サーバ モードに代わる単純な方法として、スイッチ ドメイン内の管理 VLAN 上で NTP をブロードキャスト モードにする方法があります。

このメカニズムを使用すると、Catalyst は 1 つのブロードキャスト メッセージからクロックを取得できます。 ただし、情報の流れが一方向であるため、タイムキーピングの精度は少し下がります。
- アップデートの送信元としてループバック アドレスを使用すると、一貫性が向上します。 セキュリティ上の問題は次の 2 つの方法で対処できます。サーバのアップデートを制御する（Cisco が推奨する方法）認証を使用する

NTP グローバル設定コマンド

```
!--- For the client: clock timezone EST -5 ???? ntp source loopback 0 ????? ntp server ip_address key 1 ntp peer ip_address !--- This is for a peer association. ntp authenticate ntp authentication-key 1 md5 xxxx ntp trusted-key 1 !--- For the server: clock timezone EST -5 clock summer-time EDT recurring 1 Sun Apr 3:00 last Sun Oct 3:00 clock calendar-valid ntp source loopback0 ntp update-calendar !--- This is optional: interface vlan_id ntp broadcast !--- This sends NTP broadcast packets. ntp broadcast client !--- This receives NTP broadcast packets. ntp authenticate ntp authentication-key 1 md5 xxxxx ntp trusted-key 1 ntp access-group access-list !--- This provides further security, if needed.
```

NTP Status コマンド

```
show ntp status Clock is synchronized, stratum 8, reference is 127.127.7.1 nominal freq is 250.0000 Hz, actual freq is 249.9974 Hz, precision is 2**18 reference time is C6CF0C30.980CCA9D (01:34:00.593 IST Mon Sep 12 2005) clock offset is 0.0000 msec, root delay is 0.00 msec root dispersion is 0.02 msec, peer dispersion is 0.02 msec
```

これは、Cisco ルータが NTP マスターとして動作する場合に使用される、ルータの基準クロック アドレスです。 ルータがあらゆる NTP サーバと同期されない場合、ルータは参照 ID としてこのアドレスを使用します。 設定およびコマンドの詳細については、基本システム管理の実行の*設定 NTP* セクションを参照して下さい。

Cisco 発見プロトコル

目的

CDP は、すべての Cisco ルータ、ブリッジ、アクセス サーバ、およびスイッチで実行されるレイヤ 2（データリンク層）のプロトコルです。 CDP を使用すると、既知のデバイスに隣接している Cisco デバイスをネットワーク管理アプリケーションで発見できるようになります。 特に、下位層の透過的なプロトコルを実行している隣接デバイスをネットワーク管理アプリケーションで発見できるようになります。 CDP を使用すれば、ネットワーク管理アプリケーションで、隣接デバイスのデバイス タイプと SNMP エージェント アドレスを取得できます。 この機能を利用すれば、アプリケーションから、隣接デバイスに SNMP クエリーを送信できます。

CDP に関連する **show** コマンドを使用すると、ネットワーク エンジニアは次のような情報を入手できます。

- 隣接する CDP 対応デバイスのモジュール番号およびポート番号
- 隣接デバイスに割り当てられた次のアドレスMAC アドレスIP アドレスポートチャネル アドレス
- 隣接デバイスのソフトウェア バージョン
- 隣接デバイスに関する次の情報Speed二重モードVTP ドメインネイティブ VLAN の設定

「動作の概要」セクションでは、CDP バージョン 1（CDPv1）に対する CDP バージョン 2（CDPv2）の改良点について説明しています。

動作の概要

CDP は、SNAP をサポートするすべての LAN メディアおよび WAN メディア上で動作します。

CDP が設定された各デバイスは、マルチキャスト アドレスへ定期的にメッセージを送信します。 各デバイスは、自身が SNMP メッセージを受信するために使用できるアドレスを最低 1 つアドバタイズします。 このアドバタイズメントには、存続可能時間 (TTL) 、つまりホールド タイムの情報も含まれています。 ホールド タイムとは、受信側のデバイスが CDP 情報を廃棄する前に保持する必要のある期間のことです。

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

CDP メッセージには 1 つ以上のメッセージが含まれており、宛先デバイスはこのメッセージを使用してすべての隣接デバイスに関する情報を収集し、保存します。

次の表に、CDPv1 でサポートされるパラメータを示します。

パラメータ	タイプ	説明
1	デバイス ID	ASCII 形式で記述された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レイヤ 3 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	デバイスの機能が次のように示されます。 • ルータ： 0x01 • SR1 ブリッジ： 0x04 • スイッチ： 0x08 (レイヤ 2 およびレイヤ 3 のいずれかまたは両方のスイッチングが可能) • 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 ポートでは IGMP レポート パケットを転送しません。
5	バージョン	ソフトウェア バージョンを含む文字列 **注: show version** コマンドの出力にも同じ情報が表示されます。
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 RSP2 など)

1 SR = source-route（ソース ルート）。

2 RSP = Route Switch Processor（ルート スイッチ プロセッサ）。

CDPv2 では、新しい Type, Length, Value（TLV）が導入されています。 CDPv2 では、すべての TLV がサポートされています。 スイッチ環境で特に役に立ち、Catalyst ソフトウェアで使用されるパラメータを、次の表に示します。

スイッチで CDPv1 が稼働している場合、CDPv2 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 フレームに加えて 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、VLAN（ポートがトランキングされていない場合はその中のポート）のフレームは、タグ付けされないまま処理されます。 通常、これはネイティブ VLAN と呼ばれます。
11	全二重/半二重	この TLV には送信ポートのデュプレックス設定が含まれます。
14	アプライアンス VLAN ID	別の VLAN ID（auxiliary VLAN）を使用することで、VoIP トラフィックを他のトラフィックと区別できます。
16	消費電力	接続されているデバイスで消費される最大電力量の推定値（ミリワット単位）。
17	MTU	CDP フレームが送信されるインターフェイスの MTU。
18	Extended Trust	ポートが Extended Trust モードに設定されていることを示します。
19	信頼できないポートの COS	接続されているスイッチング デバイスの信頼できないポートで受信されたすべてのパケットのマーキングに使用する Class of Service（CoS; サービス クラス）値。
20	SysName	デバイスの完全修飾ドメイン名（不明な場合は 0）。
25	要求電力	適切な電力レベルをネゴシエートするために電源投入可能なデバイス側から送信されます。

26	使用可能電力	スイッチ側から送信されます。 電源投入可能なデバイスとネゴシエートして適切な電力設定を選択するために使用されます。

CDPv2 と Power over Ethernet

Catalyst 6500/6000 や 4500/4000 などの一部のスイッチには、Unshielded Twisted Pair (UTP; シールドなしツイストペア) ケーブルを通じて、電源投入可能なデバイスに電力を供給する機能があります。 CDP (パラメータ 16、25、26) によって受信された情報は、スイッチの電源管理を最適化する目的に使用されます。

CDPv2 と Cisco IP Phone のやりとり

Cisco IP Phone は、外付けの 10/100 Mbps イーサネット デバイスに接続できます。 このような接続が可能なのは、IP Phone に 3 ポートのレイヤ 2 スイッチが内蔵されているためです。 これらの内部スイッチ ポートは、次のように呼ばれています。

- P0 (内部 IP Phone デバイス)
- P1 (外部 10/100 Mbps ポート)
- P2 (スイッチに接続する外部 10/100 Mbps ポート)

dot1q アクセス トランク ポートを設定すると、スイッチ ポート上の別個の VLAN で音声トラフィックを転送できます。 この VLAN は補助 VLAN (CatOS) または音声 VLAN (Cisco IOS ソフトウェア) と呼ばれます。 したがって、dot1q タグの付いた IP Phone からのトラフィックは補助 VLAN または音声 VLAN 上で送信でき、タグなしのトラフィックはアクセス VLAN 経由で同じ IP Phone の外部 10/100 Mbps ポートから送信できます。

Catalyst スイッチは CDP （Parameter-14 によって Voice VLAN Id を IP Phone に知らせることができます: アプライアンス VLAN-ID TLV) 。 そのため、IP Phone では、適切な VLAN ID と 802.1p プライオリティを使用して、すべての VoIP 関連パケットにタグ付けが行われます。 この CDP TLV は、アプライアンス ID パラメータを介して IP Phone が接続されているかどうかを確認する目的にも使用されます。

この概念は、QoS ポリシーを作成するときにも利用できます。 Catalyst スイッチでは、次の 3 つの方法で IP Phone とやりとりを行うように設定することができます。

- Cisco IP Phone を信頼IP Phone が CDP によって検出された場合にのみ、条件付きで CoS を信頼します。 CDP パラメータ 14 によって IP Phone が検出された場合は常に、ポートの信頼状態が Trust COS に設定されます。 IP Phone が検出されない場合は、ポートの信頼状態が Untrusted に設定されます。
- Extended Trustスイッチは、CDP (パラメータ 18) を使用して、自身の外部 10/100 Mbps デバイス ポートで受信したすべてのフレームを信頼するように IP Phone に通知できます。
- Untrusted ポートの COS を書き換えスイッチは、CDP (パラメータ 19) を使用して、自身の外部 10/100 Mbps デバイス ポートで受信した 802.1p CoS 値を書き換えるように IP Phone に通知できます。**注:** デフォルトでは、IP Phone の外部 10/100 Mbps ポートで受信されたトラフィックはすべて Untrusted になります。

注: これは方法に関する設定例 スイッチにシスコ以外の IP Phone を接続するです。

注: 次に例を示します。

```
Switch(config)#interface gigabitEthernet 2/1 Switch(config-if)#switchport mode trunk !--- For example use VLAN 30 for voice VLAN, and VLAN 10 for access VLAN. Switch(config-if)#switchport
```

```
trunk native vlan 10 Switch(config-if)#switchport trunk allow vlan 10,30 Switch(config-if)#switchport voice vlan 30 Switch(config-if)#spanning-tree portfast trunk !--- And besides that enable LLDP as Non Cisco IP Phone do not use CDP. Switch(config)#lldp run
```

Cisco の推奨する設定

CDP によって提供される情報は、レイヤ 2 接続の問題のトラブルシューティングを行う際に非常に役に立つ場合があります。 CDP をサポートしているすべてのデバイスで CDP をイネーブルにしてください。 次のコマンドを発行します。

- スイッチで CDP をグローバルにイネーブルにする場合は、次のコマンドを発行します。
  `Switch(config)#cdp run`
- ポート単位で CDP をイネーブルにする場合は、次のコマンドを発行します。
  `Switch(config)#interface type slot#/port# Switch(config-if)#cdp enable`

設定チェックリスト

グローバル コマンド

スイッチ設定プロセスを開始するには、ログインして、イネーブル モードに切り替え、グローバル コンフィギュレーション モードに入ります。

```
Switch>enable Switch# Switch#configure terminal Switch(Config)#
```

汎用グローバル コマンド (全社対象)

この「グローバル コマンド」セクションには、企業ネットワーク内にあるすべてのスイッチに適用されるグローバル コマンドの一覧を掲載されています。

次の設定には、初期設定に追加することが推奨されるグローバル コマンドが含まれています。 テキストをコピーして CLI に貼り付ける前に、出力の値を変更する必要があります。 グローバル設定を適用するには、次のコマンドを発行します。

```
vtp domain domain_name vtp mode transparent spanning-tree portfast bpduguard spanning-tree etherchannel guard misconfig cdp run no service pad service password-encryption enable secret password clock timezone EST -5 clock summer-time EDT recurring 1 Sun Apr 3:00 last Sun Oct 3:00 clock calendar-valid ip subnet-zero ip host tftpserver your_tftp_server ip domain-name domain_name ip name-server name_server_ip_address ip name-server name_server_ip_address ip classless no ip domain-lookup no ip http server no logging console no logging monitor logging buffered 16384 logging trap notifications logging facility local7 logging syslog_server_ip_address logging syslog_server_ip_address logging source-interface loopback0 service timestamps debug datetime localtime show-timezone msec service timestamps log datetime localtime show-timezone msec access-list 98 permit host_ip_address_of_primary_snmp_server access-list 98 permit host_ip_address_of_secondary_snmp_server snmp-server community public ro 98 snmp-server community laneng rw 98 snmp-server enable traps entity snmp-server host host_address traps public snmp-server host host_address traps public banner motd ^CCCCC This is a proprietary system, NOT for public or personal use. All work products, communications, files, data or information directly or indirectly created, input or accessed on this system are and shall become the sole property of the company. This system is actively monitored and accessed by the company. By logging onto this system, the user consents to such monitoring and access. USE OF THIS SYSTEM WITHOUT OR IN EXCESS OF THE PROPER AUTHORIZATION MAY SUBJECT THE USER TO DISCIPLINE AND/OR CIVIL AND CRIMINAL PENALTIES ^C line console 0 exec-timeout 0 0 password cisco login transport input none line vty 0 4 exec-timeout 0 0 password cisco login length 25 clock calendar-valid ntp server ntp_server_ip_address ntp server ntp_server_ip_address ntp update-calendar
```

各スイッチ シャーシ固有のグローバル コマンド

このセクションに掲載されているグローバル コマンドは、ネットワーク内にインストールされているスイッチ シャーシごとに適用されます。

シャーシ固有の設定変数

日時を設定するには、次のコマンドを発行します。

```
Switch#clock set hh:mm:ss day month year
```

デバイスのホスト名を設定するには、次のコマンドを発行します。

```
Switch>enable Switch#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Switch(config)#hostname Cat6500
```

管理用のループバック インターフェイスを設定するには、次のコマンドを発行します。

```
CbrCat6500(config)#interface loopback 0 Cat6500(config-if)#description Cat6000 - Loopback address and Router ID Cat6500(config-if)#ip address ip_address subnet_mask Cat6500(config-if)#exit
```

スーパーバイザ エンジンの Cisco IOS ソフトウェアのリビジョンを表示するには、次のコマンドを発行します。

```
Cbrcat6500#show version | include IOS IOS (tm) MSFC Software (C6MSFC-DSV-M), Version 12.1(13)E9, EARLY DEPLOYMENT RELE ASE SOFTWARE (fc1) cat6500#
```

MSFC のブートファイルのリビジョンを表示するには、次のコマンドを発行します。

```
Cat6500#dir bootflash: Directory of bootflash:/ 1 -rw- 1879040 Aug 19 2003 19:03:29 c6msfc-boot-mz.121-19.E1a 15990784 bytes total (14111616 bytes free
```

SNMP サーバのコンタクト情報および場所を指定するには、次のコマンドを発行します。

```
Cat6500(config)#snmp-server contact contact_information Cat6500(config)#snmp-server location location_of_device
```

スタートアップ コンフィギュレーションを既存のスーパバイザ エンジンから新しい Supervisor Engine にコピーするために、設定の失います、たとえば、既存のスーパバイザのインターフェイスの設定いくつかがある可能性があります。 Cisco は設定をテキストファイルにコピーし、発生する設定 に関する 問題があるかどうか見るためにコンソールにセグメントにそれを貼り付けることを推奨します。

インターフェイス コマンド

Cisco の機能ポートのタイプ

Cisco IOS ソフトウェアでは、スイッチ ポートはインターフェイスと呼ばれています。 Cisco IOS ソフトウェアには次の 2 種類のインターフェイス モードがあります。

- レイヤ 3 ルーテッド インターフェイス
- レイヤ 2 スイッチ インターフェイス

インターフェイス機能は、そのポートがどのように設定されているかを表します。 各ポートは次のいずれかに設定できます。

- ルーテッド インターフェイス
- Switched Virtual Interface (SVI; スイッチ仮想インターフェイス)
- アクセス ポート
- トランク

- Etherchannel
- 上記の組み合せ

インターフェイス タイプとは、ポート タイプのことです。 ポートタイプは次のいずれかに設定できます。

- FE
- GE
- ポート チャネル

次の一覧では、Cisco IOS ソフトウェアのさまざまなインターフェイス機能について簡単に説明しています。

- ルーテッド物理インターフェイス（デフォルト）：スイッチの各インターフェイスは、Cisco ルータと同様に、デフォルトではルーテッド レイヤ 3 インターフェイスに設定されます。 ルーテッド インターフェイスは、独自の IP サブネットに属している必要があります。
- アクセス スイッチ ポート インターフェイス：この機能は、複数のインターフェイスを同じ VLAN に設定するときに使用されます。 ポートをルーテッド インターフェイスからスイッチ インターフェイスに変換する必要があります。
- SVI — SVI は VLAN 間ルーティングのためのアクセス スイッチポートが含まれている VLAN と関連付けることができます。 異なる VLAN 上のアクセス スイッチ ポート間でルーティングまたはブリッジ機能を使用する場合は、SVI を VLAN に関連付けます。
- トランク スイッチ ポート インターフェイス：この機能は、複数の VLAN を別のデバイスに伝送するときに使用されます。 ポートをルーテッド インターフェイスからトランク スイッチ ポートに変換する必要があります。
- EtherChannel：EtherChannel は、冗長性とロード バランシングを実現するために、個々のポートを単一の論理ポートにバンドルするために使用されます。

Cisco の機能ポート タイプに関する推奨事項

このセクションの情報を参考にして、インターフェイスに適用するパラメータを決定してください。

注: 可能な場合は、一部のインターフェイス固有のコマンドも含めて掲載しています。

自動ネゴシエーション

次のような状況では、自動ネゴシエーションを使用しないでください。

- スイッチやルータなどのネットワーク インフラストラクチャ デバイスをサポートするポートに対して
- その他の非一時的エンドシステム（サーバやプリンタなど）に対して

次の 10/100 Mbps リンク設定では、速度とデュプレックスを手動で設定してください。 通常、これらの設定では 100 Mbps 全二重を選択します。

- 100 MB リンク、スイッチどうし
- 100 MB リンク、スイッチとサーバの間
- 100 MB リンク、スイッチとルータの間

このように設定するには、次のコマンドを発行します。

```
Cat6500(config-if)#interface [type] mod#/port# Cat6500(config-if)#speed 100 Cat6500(config-if)#duplex full
```

エンド ユーザ用のリンクは 10/100 Mbps に設定することを推奨します。 モバイル ワーカーおよび一時的ホストに対しては、次の例に示すように、自動ネゴシエーションを設定する必要があります。

```
Cat6500(config-if)#interface [type] mod#/port# Cat6500(config-if)#speed auto
```

ギガビット インターフェイスのデフォルト値は auto-negotiation です。 ただし、次のコマンドを発行すれば、自動ネゴシエーションがイネーブルであることを確認できます。 ギガビット ネゴシエーションはイネーブルにしておくことを推奨します。

```
Cat6500(config-if)#interface gigabitethernet mod#/port# Cat6500(config-if)#no speed
```

スパニング ツリー ルート

ネットワークの設計を考慮して、各 VLAN のルートとして使用するのに最も適したスイッチを特定する必要があります。 通常は、ネットワークの中心に位置する強力なスイッチを選択することを推奨します。 ルート ブリッジをネットワークの中心に置き、サーバおよびルータに直接接続してください。 一般的に、このように設定すると、クライアントからサーバおよびルータまでの平均距離が短縮されます。 詳細は、「Spanning Tree Protocol Problems and Related Design Considerations (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。

スイッチを強制的に代表 VLAN のルートにするには、次のコマンドを発行します。

```
Cat6500(config)#spanning-tree vlan vlan_id root primary
```

スパニング ツリー 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 ツリー動作がバイパスされるため、エンドステーションがスイッチに接続されるときに発生する初期の接続遅延が短縮されます。 PortFast についての詳細は、『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。

単一のホストに接続されたすべてのイネーブルになっているアクセス ポートで STP PortFast を設定してください。 次に例を示します。

```
Cat6500(config-if)#interface [type] mod#/port# Cat6500(config-if)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single host. Connecting hubs, concentrators, switches, bridges, etc... to this interface when portfast is enabled, can cause temporary bridging loops. Use with CAUTION %Portfast has been configured on FastEthernet3/1 but will only have effect when the interface is in a non-trunking mode.
```

UDLD

ケーブルの物理構成を監視するには、ファイバに接続されたインフラストラクチャ ポートまたはイーサネットの銅線ケーブルでのみ UDLD をイネーブルにします。 UDLD を有効にするには、次のコマンドを発行します。

```
Cat6500(config)#interface [type] mod#/port# Cat6500(config-if)#udld enable
```

VLAN 設定情報

次のコマンドを使用して、VLAN を設定します。

```
Cat6500(config)#vlan vlan_number Cat6500(config-vlan)#name vlan_name Cat6500(config-vlan)#exit
Cat6500(config)#spanning-tree vlan vlan_id Cat6500(config)#default spanning-tree vlan vlan_id
```

VLAN ごとに上記のコマンドを繰り返した後、終了します。 次のコマンドを発行します。

```
Cat6500(config)#exit
```

すべての VLAN を確認するために、次のコマンドを発行します。

```
Cat6500#show vlan
```

ルーテッド SVI

インター VLAN ルーティングを行えるように SVI を設定します。 次のコマンドを発行します。

```
Cat6500(config)#interface vlan vlan_id Cat6500(config-if)#ip address svi_ip_address subnet_mask
Cat6500(config-if)#description interface_description Cat6500(config-if)#no shutdown
```

ルーテッド SVI が含まれているインターフェイス機能ごとに上記のコマンドを繰り返した後、終了します。 次のコマンドを発行します。

```
Cat6500(config-if)#^Z
```

ルーテッド単一物理インターフェイス

デフォルトのルーテッド レイヤ 3 インターフェイスを設定するには、次のコマンドを発行します。

```
Cat6500(config)#interface [type] mod#/port# Cat6500(config-if)#ip address ip_address subnet_mask
Cat6500(config-if)#description interface_description
```

ルーテッド物理インターフェイスが含まれているインターフェイス機能ごとに上記のコマンドを繰り返した後、終了します。 次のコマンドを発行します。

```
Cat6500(config-if)#^Z
```

ルーテッド EtherChannel (L3)

レイヤ 3 インターフェイスで EtherChannel を設定するには、このセクションのコマンドを発行します。

次のように論理ポートチャネル インターフェイスを設定します。

```
Cat6500(config)#interface port-channel port_channel_interface_# Cat6500(config-if)#description
port_channel_description Cat6500(config-if)#ip address port_channel_ip_address subnet_mask
Cat6500(config-if)#no shutdown
```

このチャネルを構成するポートに対して、このセクションの手順を実行します。 次の例に示すように、ポート チャネルに対して残りの情報を適用します。

```
Cat6500(config)#interface range [type] mod/port_range Cat6500(config-if)#channel-group 1-64 mode
[active | auto | desirable | on | passive] Cat6500(config-if)#no shutdown Cat6500(config-if)#^Z
```

注: EtherChannel を設定した後は、ポート チャネル インターフェイスに適用された設定によって、EtherChannel が影響を受けます。 LAN ポートに適用された設定は、設定が適用された LAN ポートのみに影響を与えます。

トランキングを使用する EtherChannel (L2)

次のように、レイヤ 2 EtherChannel をトランキング用に設定します。

```
Cat6500(config)#interface port-channel port_channel_interface_# Cat6500(config-if)#switchport
Cat6500(config-if)#switchport encapsulation encapsulation_type Cat6500(config-if)#switchport
trunk native vlan vlan_id Cat6500(config-if)#no shutdown Cat6500(config-if)#exit
```

このチャネルを構成するポートに対してのみ、このセクションの手順を実行します。

```
Cat6500(config)#interface range [type] mod/port_range Cat6500(config-if)#channel-group 1-64 mode
[active | auto | desirable | on | passive] Cat6500(config-if)#no shutdown Cat6500(config-
if)#exit
```

注: EtherChannel を設定した後は、ポート チャネル インターフェイスに適用された設定によって、EtherChannel が影響を受けます。 LAN ポートに適用された設定は、設定が適用された LAN ポートのみに影響を与えます。

すべての EtherChannel とトランクが作成されたことを確認します。 次に例を示します。

```
Cat6500#show etherchannel summary Cat6500#show interface trunk
```

アクセス ポート

インターフェイス機能が、単一のインターフェイスとして設定されたアクセス ポートである場合は、次のコマンドを発行します。

```
Cat6500(config)#interface [type] mod#/port# Cat6500(config-if)#switchport mode access
Cat6500(config-if)#switchport access vlan vlan_id Cat6500(config-if)#exit
```

レイヤ 2 スイッチ ポートとして設定する必要のある各インターフェイスに対して上記のコマンドを繰り返します。

スイッチ ポートをエンド ステーションに接続する場合は、次のコマンドを発行します。

```
Cat6500(config-if)#spanning-tree portfast
```

トランク ポート（単一物理インターフェイス）

インターフェイス機能が、単一のインターフェイスとして設定されたトランク ポートである場合は、次のコマンドを発行します。

```
Cat6500(config)#interface [type] mod#/port# Cat6500(config-if)#switchport Cat6500(config-
if)#switchport trunk encapsulation dot1q Cat6500(config-if)#switchport trunk native vlan vlan_id
Cat6500(config-if)#no shutdown Cat6500(config-if)#exit
```

トランク ポートとして設定する必要のある各インターフェイス機能でこれらのコマンドを繰り返します。

パスワード情報

パスワード情報を設定するには、次のコマンドを発行します。

```
Cat6500(config)#service password-encryption Cat6500(config)#enable secret password
CbrCat6500(config)#line con 0 Cat6500(config-line)#password password CbrCat6500(config-
line)#line vty 0 4 Cat6500(config-line)#password password Cat6500(config-line)#^Z
```

設定の保存

設定を保存するには、次のコマンドを発行します。

```
Cat6500#copy running-config startup-config
```

Cisco IOS ソフトウェア リリース 12.1(13)E の新機能

IP Phone サポートについての詳細は、『Cisco IP Phone サポートの設定』を参照してください。

LAN ポートの Network-Based Application Recognition (NBAR) についての詳細は、『Network-Based Application Recognition および分散型 Network-Based Application Recognition』を参照してください。

注：

- LAN ポートの NBAR は、MSFC2 上のソフトウェアでサポートされています。
- PFC2 では、NBAR を設定した LAN ポートでの入力 ACL をハードウェアでサポートします。
- PFC QoS がイネーブルになっている場合、NBAR が設定された LAN ポートを経由するトラフィックは、入力キュー、出力キュー、および廃棄しきい値を通過します。
- PFC QoS がイネーブルになっている場合は、MSFC2 によって出力 Class of Service (CoS; サービス クラス) が出力 IP precedence と同じ値に設定されます。
- 入力キューを通過したトラフィックは、NBAR が設定されている LAN ポートで MSFC2 のソフトウェアによって処理されます。
- 分散型 NBAR は、Cisco IOS ソフトウェア リリース 12.1(6)E 以降の FlexWAN インターフェイスで使用可能です。

NetFlow Data Export (NDE; NetFlow データ エクスポート) の拡張機能には次のものが含まれます。

- Destination-source-interface フローマスクと full-interface フローマスク
- PFC2 からの NDE バージョン 5
- サンプル NetFlow
- NDE レコードの次の追加フィールドにデータを設定するオプションネクストホップ ルータの IP アドレス入力インターフェイスの SNMP ifIndex出力インターフェイスの SNMP ifIndex発信元自律システム番号

これらの拡張機能についての詳細は、『NDE の設定』を参照してください。

他にも次のような拡張機能があります。

- UDLD の設定
- VTP の設定
- WCCP による Web キャッシュ サービスの設定

新しいコマンドは次のとおりです。

- **standby delay minimum reload**
- **link debounce**
- **VLAN 内部 割り当て ポリシー{上昇する | 下降}**
- **system jumbomtu**
- **clear catalyst6000 traffic-meter**

拡張されたコマンドは次のとおりです。

- **show vlan internal usage**：このコマンドは WAN インターフェイスで使用される VLAN を含めて指定できるように拡張されました。
- **show vlan id**：このコマンドは VLAN の範囲を入力できるように拡張されました。
- **show l2protocol-tunnel**：このコマンドは VLAN ID を入力できるように拡張されました。

Cisco IOS ソフトウェア リリース 12.1(13)E では、次のソフトウェア機能がサポートされていま

す（従来、これらの機能は Cisco IOS ソフトウェア リリース 12.1 EX の各リリースでサポートされていました）。

- DFC を搭載した各種スイッチング モジュール上のインターフェイスを含むレイヤ 2 EtherChannel の設定Cisco Bug ID CSCdt27074 （登録ユーザ専用）の「リリース 12.1(13)E で解決された一般的な警告情報」セクションを参照してください。一部ツールについては、ゲスト登録のお客様にはアクセスできない場合がありますことを、ご了承ください。
- Route Processor Redundancy Plus（RPR+）による冗長性『RPR または RPR+ によるスーパーバイザ エンジンの冗長性の設定』を参照してください。**注:** Cisco IOS ソフトウェア リリース 12.1(13)E 以降では、RPR および RPR+ の冗長化機能によって、Enhanced High System Availability（EHSA）の冗長化機能が置き換えられています。
- 4,096 個のレイヤ 2 VLAN『VLAN の設定』を参照してください。**注:** Cisco IOS ソフトウェア リリース 12.1(13)E 以降では、4,096 個のレイヤ 3 VLAN インターフェイスを設定できます。 Supervisor Engine II または Supervisor Engine I のいずれかを搭載した MSFC2 上には、合計 2,000 個を超えるレイヤ 3 VLAN インターフェイスおよびレイヤ 3 ポートを設定しないでください。MSFC 上には、合計 1,000 個を超えるレイヤ 3 VLAN インターフェイスおよびレイヤ 3 ポートを設定しないでください。
- IEEE 802.1Q トンネリング『IEEE 802.1Q トンネリングとレイヤ 2 プロトコル トンネリングの設定』を参照してください。
- IEEE 802.1Q プロトコル トンネリング『IEEE 802.1Q トンネリングとレイヤ 2 プロトコル トンネリングの設定』を参照してください。
- IEEE 802.1s Multiple Spanning Tree（MST; 多重スパニング ツリー）『STP および IEEE 802.1s MST の設定』を参照してください。
- IEEE 802.1w Rapid STP（RSTP）『STP および IEEE 802.1s MST の設定』を参照してください。
- IEEE 802.3ad LACP『レイヤ 3 とレイヤ 2 の EtherChannel の設定』を参照してください。
- PortFast BPDU フィルタリング『STP 機能の設定』を参照してください。
- VLAN ACL（VACL）をサポートするレイヤ 3 VLAN インターフェイスの自動作成『ネットワーク セキュリティの設定』を参照してください。
- あらゆる VLAN において任意のレイヤ 2 イーサネット ポートに設定可能な VACL キャプチャ ポート『ネットワーク セキュリティの設定』を参照してください。
- 個々の物理レイヤ 3 ポートの MTU サイズの設定変更『インターフェイス設定の概要』を参照してください。
- すべての SPAN トラフィックにタグが付けられるように SPAN 宛先ポートをトランクとして設定するオプション『ローカルおよびリモートの SPAN の設定』を参照してください。

関連情報

- ツールとリソース - Cisco Systems
- 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