



Cisco IOS XE Gibraltar 16.11.x (Catalyst 9300 スイッチ) レイヤ2 コンフィギュレーションガイド

初版：2019年3月29日

最終更新：2020年2月16日

シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先：シスコ コンタクトセンター

0120-092-255 (フリーコール、携帯・PHS含む)

電話受付時間：平日 10:00～12:00、13:00～17:00

<http://www.cisco.com/jp/go/contactcenter/>

【注意】 シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2019 Cisco Systems, Inc. All rights reserved.



目次

第 1 章

スパニングツリー プロトコルの設定 1

スパニングツリープロトコルの制約事項 1

スパニング ツリー プロトコルに関する情報 2

スパニングツリー プロトコル 2

スパニングツリー トポロジとブリッジプロトコル データ ユニット 3

ブリッジ ID、デバイス プライオリティ、および拡張システム ID 4

ポート プライオリティとパス コスト 5

スパニングツリー インターフェイス ステート 5

デバイスまたはポートがルート デバイスまたはルート ポートになる仕組み 8

スパニングツリーおよび冗長接続 9

スパニングツリー アドレスの管理 9

接続を維持するためのエイジング タイムの短縮 10

スパニングツリー モードおよびプロトコル 10

サポートされるスパニングツリー インスタンス 11

スパニングツリーの相互運用性と下位互換性 11

スパニング ツリー プロトコルと IEEE 802.1Q トランク 12

スパニングツリーとスイッチ スタック 12

スパニングツリー機能のデフォルト設定 13

スパニングツリープロトコルの設定方法 14

スパニングツリー モードの変更 14

(任意) スパニングツリーのディセーブル化 15

(任意) ルート デバイスの設定 16

(任意) セカンダリ ルート デバイスの設定 17

(任意) ポート プライオリティの設定 18

(任意) パス コストの設定	20
(任意) VLAN のデバイス プライオリティの設定	21
(任意) Hello Time の設定	22
(任意) VLAN の転送遅延時間の設定	23
(任意) VLAN の最大エージング タイムの設定	24
(任意) 転送保留カウンタの設定	25
スパンニングツリープロトコルのモニタリングの設定ステータス	26
スパンニングツリープロトコルに関する追加情報	26
スパンニングツリープロトコルの機能履歴	27

第 2 章

複数のスパンニング ツリー プロトコルの設定	29
マルチ スパンニングツリー プロトコルの前提条件	29
MSTP の制約事項	30
MSTP について	30
マルチ スパンニングツリー プロトコルの設定	30
マルチ スパンニングツリー プロトコルの設定時の注意事項	31
ルート スイッチの設定	31
MST リージョン	32
Internal Spanning Tree (IST) 、Common and Internal Spanning Tree (CIST) 、Common Spanning Tree (CST)	33
マルチ スパンニングツリーのリージョン内の動作	33
マルチ スパンニングツリーのリージョン間の動作	34
IEEE 802.1s の用語	34
マルチ スパンニング ツリーのリージョンの図	35
ホップ カウント	36
境界ポート	37
IEEE 802.1s の実装	37
ポートの役割名の変更	38
レガシーデバイスと標準デバイスの相互運用	38
単一方向リンク障害の検出	39
マルチ スパンニングツリー プロトコルとスイッチ スタック	40

IEEE 802.1D スパニングツリープロトコルとの相互運用性	40
高速スパニングツリー プロトコルの概要	41
ポートの役割およびアクティブ トポロジ	41
高速コンバージェンス	42
ポート ロールの同期	44
ブリッジプロトコル データ ユニットの形式および処理	45
トポロジの変更	46
プロトコル移行プロセス	47
マルチ スパニングツリー プロトコルのデフォルトの設定	47
MSTP および MSTP パラメータの設定方法	48
マルチ スパニング ツリー リージョン設定の指定とマルチ スパニング ツリー プロトコル のイネーブル化	48
(任意) ルート デバイスの設定	50
(任意) セカンダリ ルート デバイスの設定	51
(任意) ポート プライオリティの設定	52
(任意) パス コストの設定	53
(任意) デバイス プライオリティの設定	55
(任意) Hello Time の設定	56
転送遅延時間の設定	57
最大エージング タイムの設定	57
(任意) 最大ホップ カウントの設定	58
(任意) 高速移行を保証するリンク タイプの指定	59
(任意) ネイバー タイプの指定	60
プロトコル移行プロセスの再開	61
MSTP に関する追加情報	62
MSTP の機能の履歴	62
第 3 章	
オプションのスパニングツリー機能の設定	65
オプションのスパニングツリー機能について	65
PortFast	65
ブリッジプロトコル データ ユニット ガード	66

ブリッジプロトコル データ ユニット フィルタリング	66
UplinkFast	67
クロススタック UplinkFast	70
クロススタック UplinkFast の動作	70
高速コンバージェンスを発生させるイベント	72
BackboneFast	72
EtherChannel ガード	76
ルート ガード	76
ループ ガード	77
オプションのスパニングツリー機能の設定方法	77
(任意) PortFast のイネーブル化	77
BPDU ガードのイネーブル化	79
BPDU フィルタリングのイネーブル化	80
(任意) 冗長リンク用 UplinkFast のイネーブル化	82
(任意) UplinkFast のディセーブル化	83
(任意) BackboneFast のイネーブル化	84
(任意) EtherChannel ガードのイネーブル化	85
(任意) ルート ガードのイネーブル化	86
(任意) ループ ガードのイネーブル化	87
スパニングツリー ステータスのモニタリング	88
オプションのスパニング ツリー機能に関する追加情報	88
オプションのスパニングツリー機能の機能履歴	88

第 4 章

EtherChannel の設定 91

EtherChannel の制約事項	91
EtherChannel について	91
EtherChannel の概要	91
チャンネル グループおよびポートチャンネル インターフェイス	92
Port Aggregation Protocol; ポート集約プロトコル	93
ポート集約プロトコル モード	94
ポート集約プロトコルの学習方法と優先度	95

ポート集約プロトコルと他の機能との連携動作	96
Link Aggregation Control Protocol (LACP)	96
Link Aggregation Control Protocol モード	97
Link Aggregation Control Protocol とリンクの冗長性	97
Link Aggregation Control Protocol とその他の機能との連携動作	98
EtherChannel の On モード	98
ロードバランシングおよび転送方式	98
MAC アドレス転送	99
IP アドレス転送	99
ロードバランシングの利点	100
EtherChannel とスイッチ スタック	100
スイッチスタックおよび PAgP	101
スイッチ スタックと Link Aggregation Control Protocol	101
EtherChannel のデフォルト設定	101
EtherChannel 設定時の注意事項	102
レイヤ 2 EtherChannel 設定時の注意事項	103
レイヤ 3 EtherChannel 設定時の注意事項	103
Auto-LAG	103
Auto-LAG 設定時の注意事項	104
EtherChannel の設定方法	105
レイヤ 2 EtherChannel の設定	105
レイヤ 3 EtherChannel の設定	107
(任意) EtherChannel ロードバランシングの設定	110
EtherChannel 拡張ロードバランシングの設定	112
(オプション) ポート集約プロトコルの学習方法と優先度の設定	113
Link Aggregation Control Protocol ホットスタンバイ ポートの設定	114
LACP の最大バンドルの設定	115
Link Aggregation Control Protocol ポートチャンネル スタンドアロンの無効化の設定	115
LACP ポートチャンネルの MinLink の設定	116
(任意) Link Aggregation Control Protocol システム優先順位の設定	117
(任意) Link Aggregation Control Protocol ポート優先順位の設定	118

Link Aggregation Control Protocol 1:1 冗長高速レート タイマーの設定	119
グローバルな Auto-LAG の設定	120
ポート インターフェイスでの Auto-LAG の設定	121
Auto-LAG での持続性の設定	122
EtherChannel、ポート集約プロトコル、および Link Aggregation Control Protocol の状態のモニタリング	122
EtherChannel の設定例	123
例：レイヤ 2 EtherChannel の設定	123
例：レイヤ 3 EtherChannel の設定	124
例：LACP ホットスタンバイポートの設定	125
例：Auto-LAG の設定	125
EtherChannels の追加リファレンス	126
EtherChannel の機能履歴	126
<hr/>	
第 5 章	高精度時間プロトコル (PTP) の設定 129
PTP の制約事項と制限	129
Precision Time Protocol について	130
イーサネット スイッチと遅延	131
メッセージベースの同期	131
PTPv2 メッセージタイプ	132
PTP イベント メッセージ シーケンス	133
エンドツーエンドの遅延メカニズム	133
ピアツーピアの遅延メカニズム	135
ローカルクロックの同期	136
ベスト マスター クロック アルゴリズム	136
PTP クロック	137
PTP プロファイル	139
Default Profile	139
PTP の設定方法	139
レイヤ 2 PTP Default プロファイルの設定	140
レイヤ 3 PTP Default プロファイルの設定	143

インターフェイスでの PTP の無効化	147
PTP タイマーの設定	148
Precision Time Protocol のクロック値の設定	149
例：レイヤ 2 およびレイヤ 3 PTP の設定	150
PTP の機能の履歴	154

第 6 章

Generalized Precision Time Protocol の設定 157

Generalized Precision Time Protocol について	157
Generalized Precision Time Protocol の設定方法	158
Generalized Precision Time Protocol のイネーブル化	158
インターフェイスでの Generalized Precision Time Protocol の有効化	158
Precision Time Protocol のクロック値の設定	159
Generalized Precision Time Protocol のモニタリング	160
例：Generalized Precision Time Protocol の確認	160
Generalized Precision Time Protocol の機能履歴	163

第 7 章

Resilient Ethernet Protocol の設定 165

Resilient Ethernet Protocol について	165
リンク完全性	167
高速コンバージェンス	168
VLAN ロード バランシング	168
スパニングツリー インタラクション	170
Resilient Ethernet Protocol ポート	171
Resilient Ethernet Protocol の設定方法	171
Resilient Ethernet Protocol のデフォルトの設定	171
Resilient Ethernet Protocol の構成ガイドライン	172
Resilient Ethernet Protocol 管理 VLAN の設定	173
REP インターフェイスの設定	175
VLAN ロード バランシングの手動によるプリエンプションの設定	180
Resilient Ethernet Protocol の簡易ネットワーク管理プロトコルのトラップの構成	181
Resilient Ethernet Protocol 設定のモニタリング	182

Resilient Ethernet Protocol に関する追加情報 183

Resilient Ethernet Protocol の機能履歴 183

第 8 章

単方向リンク検出の設定 185

単方向リンク検出の設定の制限事項 185

単方向リンク検出の概要 185

動作モード 186

通常モード 186

アグレッシブモード 186

単一方向の検出方法 187

ネイバー データベース メンテナンス 187

イベントドリブン検出およびエコー 187

単方向リンク検出のリセット オプション 188

単方向リンク検出のデフォルトの設定 188

UDLD の設定方法 189

単方向リンク検出のグローバルにイネーブル化 189

インターフェイスでの単方向リンク検出のイネーブル化 190

光ファイバ LAN インターフェイスでの単方向リンク検出のディセーブル化 191

単方向リンク検出のモニタリングと保守 192

単方向リンク検出に関するその他の参考資料 192

単方向リンク検出の機能履歴 193

第 9 章

IEEE 802.1Q トンネリングの設定 195

IEEE 802.1Q トンネリングについて 195

サービス プロバイダー ネットワークにおける IEEE 802.1Q トンネルポート 195

ネイティブ VLAN 198

システム MTU 199

IEEE 802.1Q トンネリングおよびその他の機能 200

IEEE 802.1Q トンネリングのデフォルト設定 201

IEEE 802.1Q トンネリングの設定方法 201

トンネリング ステータスのモニタリング 203

例：IEEE 802.1Q トンネリング ポートの設定 204

IEEE 802.1Q トンネリングの機能履歴 204

第 10 章

VLAN マッピングの設定 207

VLAN マッピングの前提条件 207

VLAN マッピングについて 207

One-to-One の VLAN マッピング 209

VLAN マッピング設定時の注意事項 210

One-to-One VLAN マッピングの設定時の注意事項 210

VLAN マッピングの設定方法 211

One-to-One の VLAN マッピング 211

VLAN マッピングの機能履歴 213

第 11 章

VXLAN BGP EVPN の設定 215

VXLAN BGP EVPN の注意事項と制約事項 215

VXLAN BGP EVPN に関する情報 216

VXLAN BGP EVPN 展開の考慮事項 217

VXLAN 展開に対するネットワークの考慮事項 218

転送ネットワークの考慮事項 219

VXLAN BGP EVPN の設定方法 220

ブリッジモードでの VXLAN BGP EVPN の設定 220

VTEP とスパイン間のアンダーレイトランスポート（ユニキャストおよびマルチキャスト）の設定 220

VTEP の設定 222

スパインでの eBGP 設定 224

VTEP での eBGP の設定 228

NVE インターフェイスと VNI の設定 231

すべての VTEP での L2VPN EVPN の設定 232

アクセスカスタマー側 VLAN VTEP の設定 233

VxLAN 間ルーティングに対応した VTEP での IP VRF の設定 235

VXLAN BGP EVPN 設定の確認 236

VXLAN BGP EVPN (EBGP) の設定例	237
ブリッジモードでの VXLAN BGP EVPN の設定例	237
例：eBGP Multi-AS EVPN VXLAN 設計モデルの設定	238
例：すべての VTEP とスパイン間のアンダーレイトランスポート (ユニキャストおよびマルチキャスト) の設定	238
例：スパインと VTEP 間の EVPN アドレスファミリーを使用した eBGP の設定	240
例：すべての VTEP での NVE の設定	241
例：VTEP での L2VPN EVPN の設定	241
例：アクセスカスタマー側 VLAN VTEP の設定	242
例：VTEP での追加の VNI、EVI、および VLAN の設定	242
例：VXLAN 間ルーティングに対応した VTEP での IP VRF の設定	243
例：VTEP でのアクセス VLAN インターフェイス (SVI) の設定	243
例：NVE インターフェイスでの追加の L3-VNI の設定	243
例：コア側 VLAN および VLAN インターフェイスの設定	244
例：iBGP/IGP EVPN VXLAN 設計モデルの設定	244
例：NVE での L2/L3 VNI の確認	247
例：マルチキャストルーティングテーブルのマルチキャストの確認	247
例：EVPN マネージャでの EVPN インスタンスの確認	249
例：MAC テーブルの確認	249
例：EVPN マネージャでの MAC エントリの確認	250
例：BGP での MAC ルートの確認	250
例：レイヤ 2 ルーティング情報ベースでの MAC ルートの確認	250
例：すべての SVI での IP VRF の確認	251
例：MAC VRF (EVI) の MAC/IP エントリの確認	251
例：L3VNI (IP VRF) でのリモート MAC/IP および IP プレフィックスルートの確認	251
例：IP ルートが L3 VNI (IP VRF) にインストールされていることの確認	252
例：EVPN マネージャでの MAC/IP エントリの確認	252
例：レイヤ 2 ルーティング情報ベースの MAC/IP ルートの確認	253
VXLAN BGP EVPN の機能の履歴と情報	253
第 12 章	VXLAN EVPN 入力複製の設定 255

VXLAN EVPN 入力複製の前提条件	255
VXLAN EVPN 入力複製に関する情報	255
VXLAN EVPN 入力複製の設定	256
複製タイプの設定	256
カプセル化タイプの設定	257
NVE への VNI ノードの追加	258
VxLAN EVPN 入力複製の設定例	259
例：EVPN VxLAN を介した IMET 入力複製の設定	259
IMET IR ルートの作成と管理	259
例：EVPN マネージャでのローカル IMET ルートの作成	259
例：L2RIB ローカル IMET ルート	260
例：VxLAN カプセル化と VNI を使用した BGP ローカル IMET ルート	260
IMET IR ルートの受信とプログラミング	261
例：BGP で VxLAN カプセル化を使用して IMET ルートをインポートし、VNI を表示する	261
例：L2FIB リモート IMET ルート	261
例：L2RIB リモート IMET ルート	262
例：リモート IMET ルートのトンネル隣接関係	262
例：VxLAN カプセル化を使用した BGP ローカル IMET ルートおよび VxLAN と MPLS を使用したリモート IMET ルート	263
VxLAN EVPN 入力複製の機能情報	264

第 13 章

オーディオ ビデオ ブリッジング	265
オーディオ ビデオブリッジング ネットワークの概要	265
オーディオ ビデオブリッジング (AVB) について	265
AVB をサポートするライセンス	266
AVB の利点	266
オーディオ ビデオブリッジング ネットワークのコンポーネント	266
オーディオ ビデオブリッジングでサポートされる SKU	268
Generalized Precision Time Protocol (gPTP) について	268
Multiple Stream Reservation Protocol (MSRP) について	268

Multiple Stream Reservation Protocol の機能	269
階層型 QoS の概要	269
マルチ VLAN 登録プロトコル (MVRP) について	270
AVB ネットワークの設定	271
AVB の設定	271
スイッチでの AVB のイネーブル化	271
デバイスでの AVB の設定	272
gPTP の設定	274
gPTP の有効化	274
Precision Time Protocol のクロック値の設定	275
HQoS の設定	276
HQoS のイネーブル化	276
階層型 QoS ポリシーの形式	276
MVRP の設定	277
MVRP のイネーブル化	277
スイッチ インターフェイスでの MVRP の設定	278
AVB ネットワークのモニタリング	280
AVB のモニタリング	280
gPTP のモニタリング	280
Multiple Stream Reservation Protocol のモニタリング	280
階層型 QoS のモニタリング	281
マルチ VLAN 登録プロトコルのモニタリング	281
AVB 設定とモニタリングの例	281
AVB の例	281
gPTP の例	284
MSRP の例	287
HQoS の例	290
MVRP の例	302
オーディオ ビデオブリッジングの機能履歴	303



第 1 章

スパンニングツリー プロトコルの設定

この章では、Catalyst デバイスのポートベース VLAN 上でスパンニングツリープロトコル (STP) を設定する方法について説明します。このデバイスは、IEEE 802.1D 標準に準拠した Per-VLAN Spanning-Tree plus (PVST+) とシスコ独自の拡張機能の組み合わせか、もしくは IEEE 802.1w 標準に準拠した Rapid Per-VLAN Spanning-Tree plus (Rapid PVST+) プロトコルのいずれかを使用できます。デバイススタックは、ネットワークのその他の部分に対しては単一のスパンニングツリーノードに見え、すべてのスタックメンバが同一のブリッジ ID を使用します。

- [スパンニングツリープロトコルの制約事項 \(1 ページ\)](#)
- [スパンニング ツリー プロトコルに関する情報 \(2 ページ\)](#)
- [スパンニングツリープロトコルの設定方法 \(14 ページ\)](#)
- [スパンニングツリープロトコルのモニタリングの設定ステータス \(26 ページ\)](#)
- [スパンニングツリープロトコルに関する追加情報 \(26 ページ\)](#)
- [スパンニングツリープロトコルの機能履歴 \(27 ページ\)](#)

スパンニングツリープロトコルの制約事項

- ルートデバイスとしてデバイスを設定しようとする場合、ルートデバイスにするために必要な値が 1 未満だと、失敗します。
- ネットワークが、拡張システム ID をサポートするデバイスとサポートしないものの両方で構成されている場合、拡張システム ID をサポートするデバイスがルートデバイスになる可能性は低くなります。古いソフトウェアを実行している接続デバイスのプライオリティより VLAN 番号が大きい場合は常に、拡張システム ID によってデバイスプライオリティ値が増加します。
- 各スパンニングツリーインスタンスのルートデバイスは、バックボーンまたはディストリビューション デバイスでなければなりません。アクセスデバイスをスパンニングツリープライマリ ルートとして設定しないでください。

スパンニングツリー プロトコルに関する情報

ここでは、スパンニングツリープロトコルについて説明します。

スパンニングツリー プロトコル

スパンニングツリープロトコル (STP) は、ネットワーク内のループを回避しながらパスを冗長化するためのレイヤ2リンク管理プロトコルです。レイヤ2イーサネットネットワークが正常に動作するには、任意の2つのステーション間で存在できるアクティブパスは1つだけです。エンドステーション間に複数のアクティブパスがあると、ネットワークにループが生じます。このループがネットワークに発生すると、エンドステーションにメッセージが重複して到着する可能性があります。デバイスは、複数のレイヤ2 インターフェイスのエンドステーション MAC アドレスを学習する可能性もあります。このような状況によって、ネットワークが不安定になります。スパンニングツリーの動作は透過的であり、エンドステーション側で、単一LAN セグメントに接続されているのか、複数セグメントからなるスイッチド LAN に接続されているのかを検出することはできません。

STPは、スパンニングツリーアルゴリズムを使用し、スパンニングツリーのルートとして冗長接続ネットワーク内のデバイスを1つ選択します。アルゴリズムは、次に基づき、各ポートに役割を割り当て、スイッチドレイヤ2ネットワークを介して最良のループフリーパスを算出します。アクティブトポロジでのポートの役割：

- ルート：スパンニングツリートポロジに対して選定される転送ポート
- 指定：各スイッチドLANセグメントに対して選定される転送ポート
- 代替：スパンニングツリーのルートブリッジへの代替パスとなるブロックポート
- バックアップ：ループバックコンフィギュレーションのブロックポート

すべてのポートに役割が指定されているデバイス、またはバックアップの役割が指定されているデバイスはルートデバイスです。少なくとも1つのポートに役割が指定されているデバイスは、指定デバイスを意味します。

冗長データパスはスパンニングツリーによって、強制的にスタンバイ（ブロックされた）ステータにされます。スパンニングツリーのネットワークセグメントでエラーが発生したときに冗長パスが存在する場合は、スパンニングツリーアルゴリズムがスパンニングツリートポロジを再計算し、スタンバイパスをアクティブにします。デバイスは、スパンニングツリーフレーム（ブリッジプロトコルデータユニット (BPDU) と呼ばれる）を定期間隔で送受信します。デバイスはこれらのフレームを転送せずに、ループのないパスを構成するために使用します。BPDUには、送信側デバイスおよびそのポートについて、デバイスおよびMACアドレス、デバイスプライオリティ、ポートプライオリティ、パスコストなどの情報が含まれます。スパンニングツリーはこの情報を使用して、スイッチドネットワーク用のルートデバイスおよびルートポートを選定し、さらに、各スイッチドセグメントのルートポートおよび指定ポートを選定します。

デバイスの2つのポートがループの一部である場合、spanning-tree および、パスコスト設定は、どのポートがフォワーディングステータになるか、およびどのポートがブロッキングス

テートになるかを制御します。スパニングツリー ポート プライオリティ値は、ネットワーク トポロジにおけるポートの位置とともに、トラフィック転送におけるポートの位置がどれだけ 適切であるかを表します。The コスト値は、メディア速度を表します。



(注) ショートパスコスト方式は、デフォルトのSTPパスコスト方式です。



(注) デバイスは、STPに加えて、キープアライブ メッセージを使用してループを検出します。デフォルトでは、キープアライブはレイヤ2ポートで有効になっています。キープアライブを無効にするには、インターフェイス コンフィギュレーションモードで、**no keepalive** コマンドを使用します。

スパニングツリー トポロジとブリッジ プロトコル データ ユニット

スイッチド ネットワーク内の安定したアクティブ スパニングツリー トポロジは、次の要素によって制御されます。

- デバイス上の各 VLAN に関連付けられた一意のブリッジ ID (デバイスプライオリティおよび MAC アドレス)。スイッチスタックでは、任意のスパニングツリー インスタンスに対し、すべてのスイッチが同一のブリッジ ID を使用します。
- ルートデバイスに対するスパニングツリーパスコスト。
- 各レイヤ2 インターフェイスに対応付けられたポート ID (ポート プライオリティおよび MAC アドレス)。

ネットワーク内のデバイスに電源が入ると、各機能はルートデバイスとして機能します。各デバイスは、そのすべてのポートからコンフィギュレーション BPDU を送信します。BPDU によって通信が行われ、スパニングツリー トポロジが計算されます。各設定 BPDU には、次の情報が含まれています。

- 送信デバイスがルートデバイスとして識別するデバイスの一意のブリッジ ID。
- ルートまでのスパニングツリー パス コスト
- 送信デバイスのブリッジ ID
- メッセージエージ
- 送信側インターフェイス ID
- hello タイマー、転送遅延タイマー、および max-age プロトコル タイマーの値

デバイスは、優位な情報 (より小さいブリッジ ID、より低いパスコストなど) が含まれているコンフィギュレーション BPDU を受信すると、そのポートに対する情報を保存します。この BPDU をデバイスのルートポート上で受信した場合、そのデバイスが指定デバイスとなっているすべての接続 LAN に、更新したメッセージを付けて BPDU を転送します。

デバイスは、そのポートに現在保存されている情報よりも下位の情報を含むコンフィギュレーション BPDU を受信した場合は、その BPDU を廃棄します。デバイスが下位 BPDU を受信した LAN の指定デバイスである場合、そのポートに保存されている最新情報を含む BPDU をその LAN に送信します。このようにして下位情報は廃棄され、優位情報がネットワークで伝播されます。

BPDU の交換によって、次の処理が行われます。

- ネットワーク内の 1 つのデバイスが ルート スイッチ (スイッチド ネットワークのスパニングツリートポロジーの論理的な中心)。箇条書きの項目の下の図を参照してください。
VLAN ごとに、デバイスプライオリティが最も高い (最も小さい数字の優先順位の値) デバイスがルートスイッチとして選択されます。すべてのデバイスがデフォルトのプライオリティ (32768) で設定されている場合、VLAN 内で MAC アドレスの最も小さいデバイスがルートデバイスになります。デバイスのプライオリティ値は、ブリッジ ID の最上位ビットを占めます。
- デバイスごとに (ルートスイッチを除く)、ルートポートが 1 つ選択されます。このポートは、デバイスがルートスイッチにパケットを転送するとき、最適な (コストが最小の) パスを提供します。
- ルートスイッチへの最短距離は、パスコストに基づいてデバイスごとに計算されます。
- LAN セグメントごとに指定デバイスが選択されます。指定デバイスは、その LAN からルートスイッチにパケットを転送するときの最小パスコストを提供します。指定デバイスが LAN への接続に使用したポートは、指定ポートと呼ばれます。

スイッチド ネットワーク上のすべての地点からルート スイッチに到達する場合に必要なないパスはすべて、スパニングツリー ブロックモードになります。

ブリッジ ID、デバイス プライオリティ、および拡張システム ID

IEEE 802.1D 標準では、各デバイスは一意である必要があります。ルートスイッチの選択を制御するブリッジ識別子 (ブリッジ ID) が必要です。各 VLAN は PVST+ と Rapid PVST+ によって異なる論理ブリッジと見なされるので、同一のデバイスは設定された各 VLAN とは異なるブリッジ ID を保有している必要があります。デバイス上の各 VLAN には一意の 8 バイトブリッジ ID が設定されます。上位の 2 バイトはデバイスプライオリティに使用され、残りの 6 バイトがデバイスの MAC アドレスから取得されます。

従来はデバイスプライオリティに使用されていた 2 バイトが、4 ビットのプライオリティ値と 12 ビットの拡張システム ID 値 (VLAN ID と同じ) に割り当てられています。

表 1: デバイス プライオリティ値および拡張システム ID

プライオリティ値				拡張システム ID (VLAN ID と同設定)									
ビット 16	ビット 15	ビット 14	ビット 13	ビット 12	ビット 11	ビット 10	ビット 9	ビット 8	ビット 7	ビット 6	ビット 5	ビット 4	ビット 3
32768	16384	8192	4096	2048	1024	512	256	128	64	32	16	8	4

スパンニングツリーは、ブリッジ ID を VLAN ごとに一意にするために、拡張システム ID、デバイスプライオリティ、および割り当てられたスパンニングツリー MAC アドレスを使用します。

拡張システム ID のサポートにより、ルートスイッチ、セカンダリ ルートスイッチ、および VLAN のスイッチプライオリティの手動での設定方法に影響が生じます。たとえば、スイッチのプライオリティ値を変更すると、ルートスイッチとして選定される可能性も変更されることになります。大きい値を設定すると可能性が低下し、値が小さいと可能性が増大します。

ポート プライオリティとパス コスト

ループが発生した場合、スパンニングツリーはポートプライオリティを使用して、フォワーディングステートにするインターフェイスを選択します。最初に選択されるインターフェイスには高いプライオリティ値（小さい数値）を割り当て、最後に選択されるインターフェイスには低いプライオリティ値（高い数値）を割り当てることができます。すべてのインターフェイスに同じプライオリティ値が与えられている場合、スパンニングツリーはインターフェイス番号が最小のインターフェイスをフォワーディングステートにし、他のインターフェイスをブロックします。

スパンニングツリーパスコストのデフォルト値は、インターフェイスのメディア速度に基づきます。ループが発生した場合、スパンニングツリーはコストを使用して、フォワーディングステートにするインターフェイスを選択します。最初に選択されるインターフェイスには低いコスト値を割り当て、最後に選択されるインターフェイスには高いコスト値を割り当てることができます。すべてのインターフェイスに同じコスト値が与えられている場合、スパンニングツリーはインターフェイス番号が最小のインターフェイスをフォワーディングステートにし、他のインターフェイスをブロックします。

デバイスがスイッチスタックのメンバーの場合は、最初に選択させたいインターフェイスには小さいコスト値を与え、最後に選択させたいインターフェイスには（ポートプライオリティを調整せずに）大きいコスト値を与えます。

スパンニングツリー インターフェイス ステート

プロトコル情報がスイッチド LAN を通過するとき、伝播遅延が生じることがあります。その結果、スイッチド ネットワークのさまざまな時点および場所でトポロジーの変化が発生します。インターフェイスがスパンニングツリートポロジーに含まれていない状態からフォワーディングステートに直接移行すると、一時的にデータループが形成されることがあります。インターフェイスは新しいトポロジー情報がスイッチド LAN 上で伝播されるまで待機し、フレーム転送を開始する必要があります。インターフェイスはさらに、古いトポロジーで使用されていた転送フレームのフレーム生存時間を満了させることも必要です。

スパンニングツリーを使用しているデバイスの各レイヤ 2 インターフェイスは、次のいずれかのステートになります。

- **ブロッキング**：インターフェイスはフレーム転送に関与しません。
- **リスニング**：インターフェイスをフレーム転送に関与させることをスパンニングツリーが決定した場合、ブロッキングステートから最初に移行するステートです。
- **ラーニング**：インターフェイスはフレーム転送に関与する準備をしている状態です。

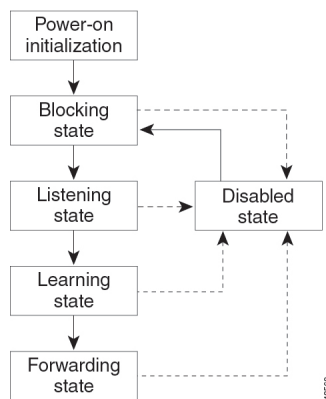
- フォワーディング：インターフェイスはフレームを転送します。
- ディセーブル：インターフェイスはスパンニングツリーに含まれません。シャットダウンポートであるか、ポート上にリンクがないか、またはポート上でスパンニングツリーインスタンスが稼働していないためです。

インターフェイスは次のように、ステートを移行します。

- 初期化からブロッキング
- ブロッキングからリスニングまたはディセーブル
- リスニングからラーニングまたはディセーブル
- ラーニングからフォワーディングまたはディセーブル
- フォワーディングからディセーブル

図 1: スパンニングツリー インターフェイス ステート

インターフェイスはこれらのステート間を移動します。



デフォルト設定では、デバイスを起動するとスパンニングツリーがイネーブルになります。その後、デバイスの各インターフェイス、VLAN、ネットワークがブロッキングステートからリスニングおよびラーニングという移行ステートを通過します。スパンニングツリーは、フォワーディングステートまたはブロッキングステートで各インターフェイスを安定させます。

スパンニングツリー アルゴリズムがレイヤ 2 インターフェイスをフォワーディングステートにする場合、次のプロセスが発生します。

1. スパンニングツリーがインターフェイスをブロッキングステートに移行させるプロトコル情報を待つ間、インターフェイスはリスニングステートになります。
2. スパンニングツリーは転送遅延タイマーの満了を待ち、インターフェイスをラーニングステートに移行させ、転送遅延タイマーをリセットします。
3. ラーニングステートの間、デバイスが転送データベースのエンドステーションの位置情報を学習しているとき、インターフェイスはフレーム転送をブロックし続けます。
4. 転送遅延タイマーが満了すると、スパンニングツリーはインターフェイスをフォワーディングステートに移行させ、このときラーニングとフレーム転送の両方が可能になります。

ブロッキング ステート

ブロッキング ステートのレイヤ2インターフェイスはフレームの転送に関与しません。初期化後、デバイスの各インターフェイスにBPDUが送信されます。デバイスは最初、他のデバイスとBPDUを交換するまで、ルートとして動作します。この交換により、ネットワーク内でどのデバイスがルートまたはルートデバイスになるかが確立されます。ネットワーク内にデバイスが1つしかない場合は交換は行われず、転送遅延タイマーが満了し、インターフェイスがリスニングステートになります。インターフェイスはデバイスの初期化後、必ずブロッキングステートになります。

ブロッキング ステートのインターフェイスは、次の機能を実行します。

- インターフェイス上で受信したフレームを廃棄します。
- 転送用に他のインターフェイスからスイッチングされたフレームを廃棄します。
- アドレスを学習しません。
- BPDU を受信します。

リスニング ステート

リスニング ステートは、ブロッキング ステートを経て、レイヤ2インターフェイスが最初に移行するステートです。インターフェイスがリスニング ステートになるのは、スパニングツリーによってそのインターフェイスのフレーム転送への関与が決定された場合です。

リスニング ステートのインターフェイスは、次の機能を実行します。

- インターフェイス上で受信したフレームを廃棄します。
- 転送用に他のインターフェイスからスイッチングされたフレームを廃棄します。
- アドレスを学習しません。
- BPDU を受信します。

ラーニング ステート

ラーニング ステートのレイヤ2インターフェイスは、フレームの転送に関与できるように準備します。インターフェイスはリスニング ステートからラーニング ステートに移行します。

ラーニング ステートのインターフェイスは、次の機能を実行します。

- インターフェイス上で受信したフレームを廃棄します。
- 転送用に他のインターフェイスからスイッチングされたフレームを廃棄します。
- アドレスを学習します。
- BPDU を受信します。

フォワーディング ステート

フォワーディングステートのレイヤ2インターフェイスは、フレームを転送します。インターフェイスはラーニング ステートからフォワーディング ステートに移行します。

フォワーディング ステートのインターフェイスは、次の機能を実行します。

- インターフェイス上でフレームを受信して転送します。
- 他のインターフェイスからスイッチングされたフレームを転送します。
- アドレスを学習します。
- BPDU を受信します。

ディセーブル ステート

ブロッキングステートのレイヤ2インターフェイスは、フレームの転送やスパニングツリーに関与しません。ディセーブル ステートのインターフェイスは動作不能です。

ディセーブル インターフェイスは、次の機能を実行します。

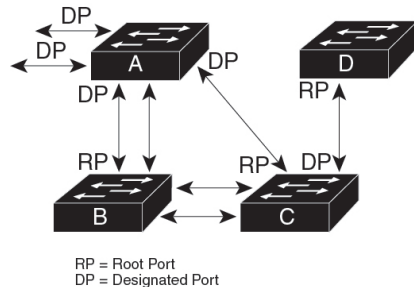
- インターフェイス上で受信したフレームを廃棄します。
- 転送用に他のインターフェイスからスイッチングされたフレームを廃棄します。
- アドレスを学習しません。
- BPDU を受信しません。

デバイスまたはポートがルート デバイスまたはルート ポートになる仕組み

ネットワーク上のすべてのデバイスがデフォルトのスパニングツリー設定で有効になっている場合、最小の MAC アドレスを持つデバイスがルートデバイスになります。

図 2: スパニングツリー トポロジ

スイッチ A はルートデバイスとして選択されます。すべてのデバイスのデバイスプライオリティがデフォルト (32768) に設定されていて、デバイス A の MAC アドレスが最も小さいためです。ただし、トラフィックパターン、転送インターフェイスの数、またはリンクタイプによっては、スイッチ A が最適なルートデバイスとは限りません。ルートデバイスになるように、最適なデバイスのプライオリティを引き上げる (数値を引き下げる) と、スパニングツリーの再計算が強制的に行われ、最適なデバイスをルートとした新しいトポロジが形成されます。



スパニングツリー トポロジがデフォルトのパラメータに基づいて算出された場合、スイッチドネットワークの送信元エンドステーションから宛先エンドステーションまでのパスが最適にならない場合があります。たとえば、ルートポートよりプライオリティの高いインターフェイスに高速リンクを接続すると、ルートポートが変更される可能性があります。最高速のリンクをルートポートにすることが重要です。

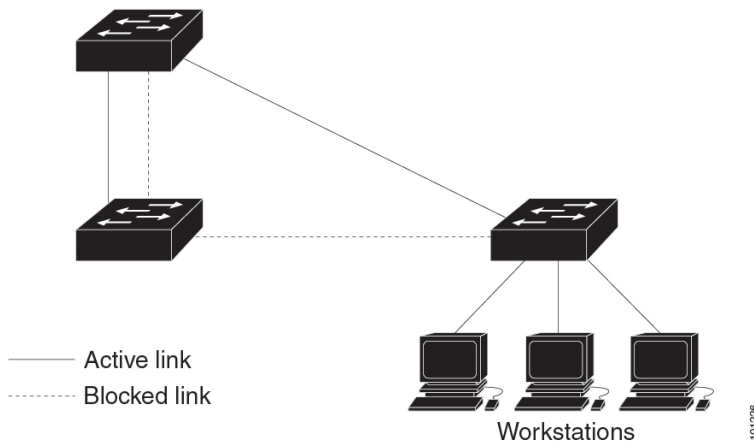
たとえば、スイッチBのあるポートがギガビットイーサネットリンクで、別のポート（10/100リンク）がルートポートであると仮定します。ネットワークトラフィックはギガビットイーサネットリンクに流す方が効率的です。ギガビットイーサネットポートのスパニングツリーポートプライオリティをルートポートより高くする（数値を小さくする）と、ギガビットイーサネットポートが新しいルートポートになります。

スパニングツリーおよび冗長接続

2つのスイッチインターフェイスを別の1台のデバイス、または2台の異なるデバイスに接続することにより、スパニングツリーを使用して冗長バックボーンを作成できます。スパニングツリーは一方のインターフェイスを自動的にディセーブルにし、他方でエラーが発生した場合にはそのディセーブルにしていた方をイネーブルにします。一方のリンクが高速で、他方が低速の場合、必ず、低速の方のリンクがディセーブルになります。速度が同じ場合、ポート優先度とポートIDが加算され、最大値を持つリンクがスパニングツリーによって無効にされます。

図3: スパニングツリーおよび冗長接続 (9 ページ) は、スパニングツリー トポロジでの冗長接続を示しています。

図3: スパニングツリーおよび冗長接続



EtherChannel グループを使用して、デバイス間に冗長リンクを設定することもできます。

スパニングツリー アドレスの管理

IEEE 802.1D では、各種ブリッジプロトコルに使用させるために、0x00180C2000000 ~ 0x0180C2000010 の範囲で17のマルチキャストアドレスが規定されています。これらのアドレスは削除できないスタティック アドレスです。

スパニングツリーステートに関係なく、スタック内の各では0x0180C2000000 ~ 0x0180C200000F のアドレス宛ての packets を受信しますが、転送は行いません。

スパニングツリーがイネーブルの場合、スイッチまたはスタック内の各スイッチの CPU は 0x0180C2000000 および 0x0180C2000010 宛ての packets を受信します。スパニングツリーがディセーブルの場合は、スイッチまたはスタック内の各スイッチは、それらの packets を不明のマルチキャストアドレスとして転送します。

接続を維持するためのエージングタイムの短縮

ダイナミックアドレスのエージングタイムはデフォルトで5分です。これは、**mac address-table aging-time** グローバル コンフィギュレーション コマンドのデフォルトの設定です。ただし、スパニングツリーの再構成により、多数のステーションの位置が変更されることがあります。このようなステーションは、再構成中、5分以上にわたって到達できないことがあるので、アドレステーブルからステーションアドレスを削除し、改めて学習できるように、アドレスエージングタイムが短縮されます。スパニングツリー再構成時に短縮されるエージングタイムは、転送遅延パラメータ値 (**spanning-tree vlan vlan-id forward-time seconds** グローバル コンフィギュレーション コマンド) と同じです。

各 VLAN はそれぞれ独立したスパニングツリー インスタンスなので、スイッチは VLAN 単位でエージングタイムを短縮します。ある VLAN でスパニングツリーの再構成が行われると、その VLAN で学習されたダイナミック アドレスがエージングタイム短縮の対象になります。他の VLAN のダイナミック アドレスは影響を受けず、スイッチで設定されたエージングタイムがそのまま適用されます。

スパニングツリー モードおよびプロトコル

このデバイスでサポートされるモードおよびプロトコルは、次のとおりです。

- **PVST+** : このスパニングツリー モードは、IEEE 802.1D 標準およびシスコ独自の拡張機能に準拠します。PVST+ はデバイス上の各 VLAN でサポートされる最大数まで動作し、各 VLAN にネットワーク上でのループフリーパスを提供します。

PVST+ は、対象となる VLAN にレイヤ 2 ロード バランシングを提供します。ネットワーク上の VLAN を使用してさまざまな論理トポロジを作成し、特定のリンクに偏らないようにすべてのリンクを使用できるようにします。VLAN 上の PVST+ インスタンスごとに、それぞれ 1 つのルートスイッチがあります。このルートスイッチは、その VLAN に対応するスパニングツリー情報を、ネットワーク上の他のすべてのデバイスに伝送します。このプロセスにより、各デバイスがネットワークに関する共通の情報を持つため、ネットワークトポロジが確実に維持されます。

- **Rapid PVST+** : デバイスのデフォルト STP モードは Rapid PVST+ です。このスパニングツリーモードは、IEEE 802.1w 標準に準拠した高速コンバージェンスを使用する以外は PVST+ と同じです。高速コンバージェンスを行うため、Rapid PVST+ はトポロジ変更を受信すると、ポート単位でダイナミックに学習した MAC アドレス エントリをただちに削除します。このような場合、PVST+ では、ダイナミックに学習した MAC アドレス エントリには短いエージングタイムが使用されます。

Rapid PVST+ は PVST+ と同じ設定を使用しているため（特に明記する場合を除く）、デバイスで必要なことは最小限の追加設定のみです。Rapid PVST+ の利点は、大規模な PVST+ のインストール ベースを Rapid PVST+ に移行する際に、複雑なマルチ スパニングツリー

プロトコル (MSTP) 設定の学習やネットワーク再設定の必要がないことです。RapidPVST+ モードでは、各 VLAN は独自のスパンニングツリー インスタンスを最大数実行します。

- **MSTP** : このスパンニングツリーモードは IEEE 802.1s 標準に準拠しています。複数の VLAN を同一のスパンニングツリー インスタンスにマッピングし、多数の VLAN をサポートする場合に必要なスパンニングツリーインスタンスの数を減らすことができます。MSTP は Rapid Spanning-Tree Protocol (RSTP) (IEEE 802.1w 準拠) 上で実行され、転送遅延を解消し、ルートポートおよび指定ポートをフォワーディング ステートにすばやく移行することにより、スパンニングツリーの高速度コンバージェンスを可能にします。スイッチ スタックでは、クロススタック高速移行 (CSRT) 機能が RSTP と同じ機能を実行します。RSTP または CSRT を使用しなければ、MSTP は稼働できません。

サポートされるスパンニングツリー インスタンス

Cisco IOS XE Gibraltar 16.11.1 リリース以降、PVST+ または Rapid PVST+ モードでは、デバイスまたはデバイススタックは最大 256 のスパンニングツリー インスタンスをサポートします。

MSTP モードでは、デバイスまたはデバイススタックは最大 65 の MST インスタンスをサポートします。特定の MST インスタンスにマッピング可能な VLAN 数に制限はありません。

スパンニングツリーの相互運用性と下位互換性

MSTP および PVST+ が混在したネットワークでは、Common Spanning-Tree (CST) のルートは MST バックボーンの内側に配置する必要があり、PVST+ デバイスを複数の MST リージョンに接続することはできません。

ネットワーク内に Rapid PVST+ を実行しているデバイスと PVST+ を実行しているデバイスが存在する場合、Rapid PVST+ デバイスと PVST+ デバイスを別のスパンニングツリー インスタンスに設定することを推奨します。RapidPVST+ スパンニングツリーインスタンスでは、ルートスイッチは Rapid PVST+ デバイスでなければなりません。PVST+ インスタンスでは、ルートスイッチは PVST+ デバイスでなければなりません。PVST+ デバイスはネットワークのエッジに配置する必要があります。

すべてのスタック メンバーが、同じバージョンのスパンニングツリーを実行します (すべて PVST+、すべて Rapid PVST+、またはすべて MSTP)。

表 2: PVST+、MSTP、Rapid PVST+ の相互運用性と互換性

	PVST+	MSTP	Rapid PVST+
PVST+	あり	あり (制限あり)	あり (PVST+ に戻る)
MSTP	あり (制限あり)	あり	あり (PVST+ に戻る)
Rapid PVST+	あり (PVST+ に戻る)	あり (PVST+ に戻る)	あり

スパニングツリー プロトコルと IEEE 802.1Q トランク

VLAN トランクに関する IEEE 802.1Q 規格は、ネットワークのスパニングツリー戦略に一定の制限を設けています。この規格では、トランク上で使用できるすべての VLAN に対して、1つのスパニングツリー インスタンスしか認められません。ただし、IEEE 802.1Q トランクを介して接続される Cisco デバイスのネットワークにおいて、デバイスはトランク上で許容される VLAN ごとに1つのスパニングツリー インスタンスを維持します。

IEEE 802.1Q トランクを介して Cisco デバイスを他社製のデバイスに接続する場合、Cisco デバイスは PVST+ を使用してスパニングツリーの相互運用性を実現します。Rapid PVST+ がイネーブルの場合、デバイスは PVST+ ではなく Rapid PVST+ を使用します。デバイスは、トランクの IEEE 802.1Q VLAN のスパニングツリー インスタンスと他社の IEEE 802.1Q デバイスのスパニングツリー インスタンスを結合します。

ただし、PVST+ または Rapid PVST+ の情報はすべて、他社製の IEEE 802.1Q デバイスからなるクラウドにより分離された Cisco デバイスによって維持されます。Cisco デバイスを分離する他社製の IEEE 802.1Q クラウドは、デバイス間の単一トランクリンクとして扱われます。

PVST+ は IEEE 802.1Q トランクで自動的に有効になるので、ユーザー側で設定する必要はありません。アクセスポートおよび ISL (スイッチ間リンク) トランクポートでの外部スパニングツリーの動作は、PVST+ の影響を受けません。

スパニングツリーとスイッチ スタック

スイッチスタックが PVST+ または Rapid PVST+ モードで動作している場合：

- スイッチスタックは、ネットワークのその他の部分に対しては単一のスパニングツリー ノードに見え、すべてのスタックメンバが与えられたスパニングツリーに同一のブリッジ ID を使用します。ブリッジ ID は、アクティブスイッチの MAC アドレスから取得されます。
- 新しいデバイスがスタックに加わると、そのデバイスは、アクティブスイッチのブリッジ ID を自分のブリッジ ID として設定します。新しく追加されたデバイスの ID が最も小さく、ルートパスコストがすべてのスタックメンバー間で同じ場合は、新しく追加されたデバイスがスタックルートになります。
- スタックメンバがスタックから除外されると、スタック内でスパニングツリーの再コンバージェンスが発生します (スタック外で発生する場合があります)。残っているスタックメンバのうち最も低いスタックポート ID を持つスタックメンバが、スタックルートになります。
- スイッチスタックがスパニングツリールートで、アクティブスイッチで障害が発生した、またはスタックから外れた場合、スタンバイスイッチが新しいアクティブスイッチになり、ブリッジ ID は同じままで、スパニングツリーの再コンバージェンスが発生する可能性があります。
- スタック外にあるネイバーデバイスに障害が発生したか、またはその電源が停止した場合、通常のスパニングツリー処理が発生します。スパニングツリーの再コンバージェンスは、アクティブなトポロジ内のデバイスが失われたことにより発生する場合があります。

- スイッチスタック外にある新しいデバイスがネットワークに追加された場合、通常のスパニングツリー処理が発生します。スパニングツリーの再コンバージェンスは、ネットワークにデバイスが追加されたことにより発生する場合があります。

スパニングツリー機能のデフォルト設定

表 3: スパニングツリー機能のデフォルト設定

機能	デフォルト設定
イネーブル ステート	VLAN 1 上でイネーブル
スパニングツリー モード	RapidPVST+ (PVST+ と M ブル)
デバイスプライオリティ	32768
スパニングツリーポートプライオリティ (インターフェイス単位で設定可能)	128
スパニングツリー ポート コスト (インターフェイス単位で設定可能)	10 Mbps : 100 100 Mbps : 19 1 Gbps : 4 10 Gbps : 2 25 Gbps : 1 40 Gbps : 1
スパニングツリー VLAN ポートプライオリティ (VLAN 単位で設定可能)	128
スパニングツリー VLAN ポート コスト (VLAN 単位で設定可能)	10 Mbps : 100 100 Mbps : 19 1 Gbps : 4 10 Gbps : 2 25 Gbps : 1 40 Gbps : 1
スパニングツリー タイマー	hello タイム : 2 秒 転送遅延時間 : 15 秒 最大エージング タイム : 転送保留カウント : 6 BPI



(注) Cisco IOS Release 15.2(4)E 以降では、デフォルトの STP モードは Rapid PVST+ です。

スパンニングツリープロトコルの設定方法

ここでは、スパンニングツリープロトコルの設定について説明します。

スパンニングツリー モードの変更

スイッチは次の3つのスパンニングツリー モードをサポートします。Per-VLAN Spanning-Tree Plus (PVST+)、Rapid PVST+、またはマルチスパンニングツリープロトコル (MSTP)。デフォルトでは、デバイスは Rapid PVST+ プロトコルを実行します。

デフォルト モード以外のモードをイネーブルにする場合、この手順は必須です。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	spanning-tree mode {pvst mst rapid-pvst} 例： Device(config)# spanning-tree mode pvst	スパンニングツリーモードを設定します。 すべてのスタックメンバーは、同じバージョンのスパンニング ツリーを実行します。 <ul style="list-style-type: none"> • PVST+ をイネーブルにするには、pvst を選択します。 • MSTP をイネーブルにするには、mst を選択します。 • rapid PVST+ をイネーブルにするには、rapid-pvst を選択します。
ステップ 4	interface interface-id 例：	設定するインターフェイスを指定し、インターフェイス コンフィギュレーションモードを開始します。有効なインター

	コマンドまたはアクション	目的
	Device(config)# interface GigabitEthernet1/0/1	フェイスとしては、物理ポート、VLAN、ポート チャネルなどがあります。VLAN ID の範囲は1～4094です。指定できるポートチャネルの範囲は1～48です。
ステップ 5	spanning-tree link-type point-to-point 例： Device(config-if)# spanning-tree link-type point-to-point	このポートのリンク タイプがポイントツーポイントであることを指定します。 このポート（ローカルポート）をポイントツーポイントリンクでリモートポートと接続し、ローカルポートが指定ポートになると、デバイスはリモートポートとネゴシエーションし、ローカルポートをフォワーディングステートにすばやく変更します。
ステップ 6	end 例： Device(config-if)# end	特権 EXEC モードに戻ります。
ステップ 7	clear spanning-tree detected-protocols 例： Device# clear spanning-tree detected-protocols	デバイス上のいずれかのポートがレガシー IEEE 802.1D デバイス上のポートに接続されている場合は、このコマンドによりデバイス全体のプロトコル移行プロセスを再開します。 このステップは、このデバイスで Rapid PVST+ が稼働していることを指定デバイスが検出する場合のオプションです。

(任意) スパニングツリーのディセーブル化

スパニングツリーはデフォルトで、VLAN 1 およびスパニングツリー限度を上限として新しく作成されたすべての VLAN 上でイネーブルです。スパニングツリーをディセーブルにするのは、ネットワーク トポロジにループがないことが確実な場合だけにしてください。



注意 スパニングツリーがディセーブルでありながら、トポロジにループが存在していると、余分なトラフィックが発生し、パケットの重複が無限に繰り返されることによって、ネットワークのパフォーマンスが大幅に低下します。

スパニング ツリーを無効にするには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	no spanning-tree vlan vlan-id 例： Device(config)# no spanning-tree vlan 300	<i>vlan-id</i> に指定できる範囲は 1 ~ 4094 です。
ステップ 4	end 例： Device(config)# end	特権 EXEC モードに戻ります。

(任意) ルート デバイスの設定

特定の VLAN でデバイスをルートとして設定するには、**spanning-tree vlan vlan-id root** グローバル コンフィギュレーション コマンドを使用して、デバイスのプライオリティをデフォルト値 (32768) から、それより大幅に小さい値に変更します。このコマンドを入力すると、ソフトウェアが各 VLAN について、ルート スイッチのスイッチ プライオリティをチェックします。拡張システム ID をサポートするため、スイッチは指定された VLAN の自身のプライオリティを 24576 に設定します。この値によって、このスイッチを指定された VLAN のルートに設定できます。

レイヤ 2 ネットワークの直径（つまり、レイヤ 2 ネットワーク上の任意の 2 つのエンドステーション間デバイスの最大ホップカウント）を指定するには、**diameter** キーワードを指定します。ネットワーク直径を指定すると、デバイスは、その直径のネットワークで最適な hello タイム、転送遅延時間、最大エージングタイムを自動的に設定し、これによって収束時間が大幅に短縮されます。**hello** キーワードを使用して、自動的に計算される hello タイムを上書きできます。

ルート デバイスを設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例：	特権 EXEC モードを有効にします。

	コマンドまたはアクション	目的
	Device> enable	パスワードを入力します (要求された場合)。
ステップ 2	configure terminal 例 : Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	spanning-tree vlan <i>vlan-id</i> root primary [diameter <i>net-diameter</i>] 例 : Device(config)# spanning-tree vlan 20-24 root primary diameter 4	指定された VLAN のルートになるように、デバイスを設定します。 <ul style="list-style-type: none"> • <i>vlan-id</i> には、VLAN ID 番号で識別された単一の VLAN、ハイフンで区切られた範囲の VLAN、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は 1 ~ 4094 です。 • (任意) diameter <i>net-diameter</i> には、任意の 2 つのエンドステーション間デバイスの最大数を指定します。範囲は 2 ~ 7 です。
ステップ 4	end 例 : Device(config)# end	特権 EXEC モードに戻ります。

次のタスク

ルートスイッチとしてスイッチを設定した後で、**spanning-tree vlan *vlan-id* hello-time**、**spanning-tree vlan *vlan-id* forward-time**、および **spanning-tree vlan *vlan-id* max-age** グローバル コンフィギュレーション コマンドを使用して、hello タイム、転送遅延時間、および最大エージングタイムを手動で設定することは推奨できません。

(任意) セカンダリ ルート デバイスの設定

スイッチをセカンダリ ルートとして設定すると、スイッチ プライオリティがデフォルト値 (32768) から 28672 に変更されます。このプライオリティにより、プライマリ ルートスイッチで障害が発生した場合に、このスイッチが指定された VLAN のルートスイッチになる可能性が高くなります。これは、他のネットワーク スイッチがデフォルトのスイッチ プライオリティ 32768 を使用し、ルート スイッチになる可能性が低いことが前提です。

複数のスイッチでこのコマンドを実行すると、複数のバックアップ ルート スイッチを設定できます。**spanning-tree vlan *vlan-id* root primary** グローバル コンフィギュレーション コマンドでプライマリ ルート スイッチを設定したときと同じネットワーク 直径および hello タイム値を使用してください。

セカンダリ ルート デバイスを設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	spanning-tree vlan <i>vlan-id</i> root secondary [<i>diameter net-diameter</i>] 例： Device(config)# spanning-tree vlan 20-24 root secondary diameter 4	指定された VLAN のセカンダリルートになるように、デバイスを設定します。 <ul style="list-style-type: none"> • <i>vlan-id</i> には、VLAN ID 番号で識別された単一の VLAN、ハイフンで区切られた範囲の VLAN、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は1～4094 です。 • (任意) <i>diameter net-diameter</i> には、任意の2つのエンドステーション間デバイスの最大数を指定します。指定できる範囲は2～7です。 <p>プライマリルートスイッチを設定したときと同じネットワーク直径を使用してください。</p>
ステップ 4	end 例： Device(config)# end	特権 EXEC モードに戻ります。

(任意) ポート プライオリティの設定

ポートの優先順位を設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	interface interface-id 例： Device(config)# interface gigabitethernet 1/0/2	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。 有効なインターフェイスは、物理ポートおよびポートチャンネル論理インターフェイス (port-channel port-channel-number) です。
ステップ 4	spanning-tree port-priority priority 例： Device(config-if) # spanning-tree port-priority 0	インターフェイスのポート プライオリティを設定します。 <i>priority</i> に指定できる範囲は 0～240 で、16 ずつ増加します。デフォルトは 128 です。有効な値は 0、16、32、48、64、80、96、112、128、144、160、176、192、208、224、240 です。その他の値はすべて拒否されます。値が小さいほど、プライオリティが高くなります。
ステップ 5	spanning-tree vlan vlan-id port-priority priority 例： Device(config-if) # spanning-tree vlan 20-25 port-priority 0	VLAN のポート プライオリティを設定します。 <ul style="list-style-type: none"> • <i>vlan-id</i> には、VLAN ID 番号で識別された単一の VLAN、ハイフンで区切られた範囲の VLAN、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は 1～4094 です。 • <i>priority</i> に指定できる範囲は 0～240 で、16 ずつ増加します。デフォルトは 128 です。有効な値は 0、16、32、48、64、80、96、112、128、144、160、176、192、208、224、240 です。その他の値はすべて拒否

	コマンドまたはアクション	目的
		されます。値が小さいほど、プライオリティが高くなります。
ステップ 6	end 例： Device(config-if)# end	特権 EXEC モードに戻ります。

(任意) パス コストの設定

パス コストを設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します (要求された場合)。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	interface interface-id 例： Device(config)# interface gigabitethernet 1/0/1	設定するインターフェイスを指定し、インターフェイス コンフィギュレーションモードを開始します。有効なインターフェイスは、物理ポートおよびポートチャネル論理インターフェイス (port-channel port-channel-number) です。
ステップ 4	spanning-tree cost cost 例： Device(config-if)# spanning-tree cost 250	インターフェイスのコストを設定します。 ループが発生した場合、スパニングツリーはパスコストを使用して、フォワーディング ステートにするインターフェイスを選択します。低いパス コストは高速送信を表します。 <i>cost</i> の範囲は 1 ~ 200000000 です。デフォルト値はインターフェイスのメディア速度から派生します。

	コマンドまたはアクション	目的
ステップ 5	spanning-tree vlan <i>vlan-id</i> cost <i>cost</i> 例 : Device(config-if) # spanning-tree vlan 10,12-15,20 cost 300	VLAN のコストを設定します。 ループが発生した場合、スパニングツリーはパスコストを使用して、フォワーディング ステートにするインターフェイスを選択します。低いパス コストは高速送信を表します。 <ul style="list-style-type: none"> • <i>vlan-id</i> には、VLAN ID 番号で識別された単一の VLAN、ハイフンで区切られた範囲の VLAN、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は1～4094 です。 • <i>cost</i> の範囲は1～200000000 です。デフォルト値はインターフェイスのメディア速度から派生します。
ステップ 6	end 例 : Device(config-if) # end	特権 EXEC モードに戻ります。

show spanning-tree interface *interface-id* 特権 EXEC コマンドによって表示されるのは、リンクアップ動作可能状態のポートの情報だけです。そうでない場合は、**show running-config** 特権 EXEC コマンドを使用して設定を確認してください。

(任意) VLAN のデバイス プライオリティの設定

スイッチ プライオリティを設定して、スタンドアロン スイッチまたはスタック内のスイッチがルート スイッチとして選択される可能性を高めることができます。



- (注) このコマンドの使用には注意してください。通常、スイッチのプライオリティを変更するには **spanning-tree vlan *vlan-id* root primary** および **spanning-tree vlan *vlan-id* root secondary** グローバル コンフィギュレーション コマンドを使用することを推奨します。

VLAN のデバイス優先順位を設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	spanning-tree vlan <i>vlan-id</i> priority <i>priority</i> 例： Device(config)# spanning-tree vlan 20 priority 8192	VLAN のデバイスプライオリティを設定します。 <ul style="list-style-type: none"> • <i>vlan-id</i> には、VLAN ID 番号で識別された単一の VLAN、ハイフンで区切られた範囲の VLAN、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は 1～4094 です。 • <i>priority</i> の範囲は 0～61440 で、4096 ずつ増加します。デフォルトは 32768 です。数値が小さいほど、スイッチがルートスイッチとして選択される可能性が高くなります。 有効なプライオリティ値は 4096、8192、12288、16384、20480、24576、28672、32768、36864、40960、45056、49152、53248、57344、61440 です。その他の値はすべて拒否されます。
ステップ 4	end 例： Device(config-if)# end	特権 EXEC モードに戻ります。

(任意) Hello Time の設定

Hello Time はルート スイッチによって設定メッセージが生成されて送信される時間の間隔です。

Hello Time を設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	spanning-tree vlan <i>vlan-id</i> hello-time <i>seconds</i> 例： Device(config)# spanning-tree vlan 20-24 hello-time 3	VLAN の hello タイムを設定します。 Hello Time はルート スイッチによって設定メッセージが生成されて送信される時間の間隔です。これらのメッセージは、スイッチがアクティブであることを意味します。 <ul style="list-style-type: none"> • <i>vlan-id</i> には、VLAN ID 番号で識別された単一の VLAN、ハイフンで区切られた範囲の VLAN、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は 1～4094 です。 • <i>seconds</i> に指定できる範囲は 1～10 です。デフォルトは 2 です。
ステップ 3	end 例： Device(config-if) # end	特権 EXEC モードに戻ります。

(任意) VLAN の転送遅延時間の設定

VLAN の転送遅延時間を設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。

(任意) VLAN の最大エージング タイムの設定

	コマンドまたはアクション	目的
ステップ 3	spanning-tree vlan <i>vlan-id</i> forward-time <i>seconds</i> 例 : Device(config)# spanning-tree vlan 20,25 forward-time 18	VLAN の転送時間を設定します。転送遅延時間は、スパニングツリー ラーニング ステートおよびリスニング ステートからフォワーディング ステートに移行するまでに、インターフェイスが待機する秒数です。 <ul style="list-style-type: none"> • <i>vlan-id</i> には、VLAN ID 番号で識別された単一の VLAN、ハイフンで区切られた範囲の VLAN、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は 1～4094 です。 • <i>seconds</i> に指定できる範囲は 4～30 です。デフォルトは 15 です。
ステップ 4	end 例 : Device(config)# end	特権 EXEC モードに戻ります。

(任意) VLAN の最大エージング タイムの設定

VLAN の最大エージング タイムを設定するには、次の作業を行います。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します (要求された場合)。
ステップ 2	configure terminal 例 : Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	spanning-tree vlan <i>vlan-id</i> max-age <i>seconds</i> 例 : Device(config)# spanning-tree vlan 20 max-age 30	VLAN の最大エージング タイムを設定します。最大エージング タイムは、再構成を試行するまでにスイッチがスパニングツリー コンフィギュレーション メッセージを受信せずに待機する秒数です。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> • <i>vlan-id</i> には、VLAN ID 番号で識別された単一の VLAN、ハイフンで区切られた範囲の VLAN、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は 1～4094 です。 • <i>seconds</i> に指定できる範囲は 6～40 です。デフォルトは 20 です。
ステップ 4	end 例： Device(config-if) # end	特権 EXEC モードに戻ります。

(任意) 転送保留カウンタの設定

転送保留カウンタ値を変更することで、BPDU のバースト サイズを設定できます。



- (注) このパラメータをより高い値に変更すると、(特に Rapid PVST+ モードで) CPU の使用率に大きく影響します。逆に、この値を低く設定すると、セッションによってはコンバージェンスを抑えることができます。この値は、デフォルト設定で使用することを推奨します。

転送保留カウンタを設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します (要求された場合)。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	spanning-tree transmit hold-count value 例： Device(config) # spanning-tree transmit hold-count 6	1 秒間停止する前に送信できる BPDU 数を設定します。 <i>value</i> に指定できる範囲は 1～20 です。デフォルト値は 6 です。

	コマンドまたはアクション	目的
ステップ 4	end 例： Device (config) # end	特権 EXEC モードに戻ります。

スパニングツリープロトコルのモニタリングの設定ステータス

表 4: STP 設定ステータスを表示するためのコマンド

show spanning-tree active	STP アクティブインターフェイスに関する情報を表示
show spanning-tree detail	インターフェイス情報の詳細サマリーを表示します。
show spanning-tree vlan <i>vlan-id</i>	指定された VLAN の STP コンフィギュレーション情報を表示
show spanning-tree interface <i>interface-id</i>	指定されたインターフェイスの STP コンフィギュレーション情報を表示します。
show spanning-tree interface <i>interface-id</i> portfast	指定されたインターフェイスの STP portfast 情報を表示し
show spanning-tree summary [totals]	インターフェイス ステートのサマリーを表示します。また、ステート セクションのすべての行を表示します。

STP カウンタをクリアするには、**clear spanning-tree [interface *interface-id*]** 特権 EXEC コマンドを使用します。

スパニングツリープロトコルに関する追加情報

関連資料

関連項目	マニュアル タイトル
この章で使用するコマンドの完全な構文および使用方法の詳細。	<i>Command Reference (Catalyst 9300 Series Switches)</i> の「Layer 2/3 Commands」の項を参照してください

スパニングツリープロトコルの機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

表 5:新しい機能の履歴

リリース	機能	機能情報
Cisco IOS XE Everest 16.5.1a	スパニングツリー プロトコル	STP は、ネットワーク上でループを防止しながら、パスの冗長性を実現するレイヤ 2 リンク管理プロトコルです。
Cisco IOS XE Gibraltar 16.11.1	スパニングツリー インスタンス	サポートされるスパニングツリーインスタンスの数が 256 に増えました。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> [英語] からアクセスします。



第 2 章

複数のスパンニング ツリー プロトコルの設定

- マルチ スパンニングツリー プロトコルの前提条件 (29 ページ)
- MSTP の制約事項 (30 ページ)
- MSTP について (30 ページ)
- MSTP および MSTP パラメータの設定方法 (48 ページ)
- MSTP に関する追加情報 (62 ページ)
- MSTP の機能の履歴 (62 ページ)

マルチ スパンニングツリー プロトコルの前提条件

- 2つ以上のデバイスを同じマルチスパンニングツリー (MST) リージョンに設定するには、その2つに同じ VLAN/インスタンスマッピング、同じコンフィギュレーション リビジョン番号、同じ名前を設定しなければなりません。
- ネットワーク内の冗長パスでロード バランシングを機能させるには、すべての VLAN/インスタンスマッピングの割り当てが一致している必要があります。一致していないと、すべてのトラフィックが1つのリンク上で伝送されます。
- Per-VLAN Spanning-Tree Plus (PVST+) と MST クラウドの間、または Rapid-PVST+ と MST クラウドの間でロード バランシングが機能するためには、すべての MST 境界ポートがフォワーディングでなければなりません。MST クラウドの内部スパンニングツリー (IST) のルートが共通スパンニングツリー (CST) のルートである場合、MST 境界ポートはフォワーディングです。MST クラウドが複数の MST リージョンから構成されている場合、いずれかの MST リージョンに CST ルートを含める必要があります、その他すべての MST リージョンに、PVST+ クラウドまたは高速 PVST+ クラウドを通るパスよりも、MST クラウド内に含まれるルートへのパスが良くする必要があります。クラウド内のデバイスを手動で設定しなければならない場合もあります。

MSTP の制約事項

- スイッチスタックは、最大 65 個の MST インスタンスをサポートします。特定の MST インスタンスにマッピング可能な VLAN 数に制限はありません。
- PVST+、Rapid PVST+、および MSTP はサポートされますが、アクティブにできるのは 1 つのバージョンだけです（たとえば、すべての VLAN で PVST+ を実行する、すべての VLAN で Rapid PVST+ を実行する、またはすべての VLAN で MSTP を実行します）。
- MST コンフィギュレーションの VLAN トランキング プロトコル (VTP) 伝搬はサポートされません。ただし、コマンドラインインターフェイス (CLI) または簡易ネットワーク管理プロトコル (SNMP) サポートを通じて、MST リージョン内の各デバイスで MST コンフィギュレーション (リージョン名、リビジョン番号、および VLAN とインスタンスのマッピング) を手動で設定することは可能です。
- ネットワークを多数のリージョンに分割することは推奨できません。ただし、どうしても分割せざるを得ない場合は、スイッチド LAN をルータまたは非レイヤ 2 デバイスで相互接続された小規模な LAN に分割することを推奨します。
- リージョンは、同じ MST コンフィギュレーションを持つ 1 つまたは複数のメンバーで構成されます。リージョンの各メンバーは高速スパニングツリープロトコル (RSTP) ブリッジプロトコルデータユニット (BPDU) を処理する機能を備えている必要があります。ネットワーク内の MST リージョンの数に制限はありませんが、各リージョンは最大 65 のスパニングツリー インスタンスのみをサポートできます。VLAN には、一度に 1 つのスパニングツリー インスタンスのみ割り当てることができます。

MSTP について

ここでは、Multiple Spanning-Tree Protocol (MSTP) について説明します。

マルチ スパニングツリー プロトコルの設定

高速コンバージェンスのために高速スパニングツリープロトコル (RSTP) を使用するマルチ スパニングツリープロトコル (MSTP) では、複数の VLAN をグループ化して同じスパニングツリー インスタンスにマッピングすることが可能で、多くの VLAN をサポートするのに必要なスパニングツリー インスタンスの数を軽減できます。MSTP は、データトラフィックに複数の転送パスを提供し、ロードバランシングを実現して、多数の VLAN をサポートするのに必要なスパニングツリー インスタンスの数を減らすことができます。MSTP を使用すると、1 つのインスタンス (転送パス) で障害が発生しても他のインスタンス (転送パス) は影響を受けないので、ネットワークのフォールトトレランスが向上します。



(注) マルチ スパニングツリー (MST) 実装は IEEE 802.1s 標準に準拠しています。

MSTPを導入する場合、最も一般的なのは、レイヤ2スイッチドネットワークのバックボーンおよびディストリビューションレイヤへの導入です。MSTPの導入により、サービスプロバイダー環境に求められる高可用性ネットワークを実現できます。

デバイスがMSTモードの場合、IEEE 802.1w 準拠のRSTPが自動的にイネーブルになります。RSTPは、IEEE 802.1Dの転送遅延を軽減し、ルートポートおよび指定ポートをフォワーディングステートにすばやく移行する明示的なハンドシェイクによって、スパニングツリーの高速コンバージェンスを実現します。

MSTPとRSTPは、既存のシスコ独自のMultiple Instance STP (MISTP)、および既存のCisco PVST+とRapid Per-VLAN Spanning-Tree plus (Rapid PVST+)を使用して、スパニングツリーの動作を改善し、(オリジナルの) IEEE 802.1D スパニングツリーに準拠した機器との下位互換性を保持しています。

デバイススタックは、ネットワークのその他の部分に対しては単一のスパニングツリーノードに見え、すべてのスタックメンバが同一のデバイスIDを使用します。

マルチ スパニングツリー プロトコルの設定時の注意事項

- **spanning-tree mode mst** グローバル コンフィギュレーション コマンドを使用して、MSTをイネーブルにすると、RSTPが自動的にイネーブルになります。
- UplinkFast、BackboneFast、クロススタック UplinkFast の設定のガイドラインについては、関連項目のセクションの該当するセクションを参照してください。
- デバイスがMSTモードの場合は、パスコスト値の計算に、ロングパスコスト計算方式 (32ビット) が使用されます。ロングパスコスト計算方式では、次のパスコスト値がサポートされます。

速度	パス コスト値
10 Mb/s	2,000,000
100 Mb/s	200,000
1 Gb/s	20,000
10 Gb/s	2,000
100 Gb/s	200

ルート スイッチの設定

スイッチは、スパニングツリーインスタンスをVLANグループとマッピングして維持します。各インスタンスには、スイッチプライオリティとスイッチのMACアドレスからなるデバイスIDが対応付けられます。VLANグループの場合は、最小のデバイスIDを持つスイッチがルートスイッチになります。

スイッチをルートとして設定するときは、スイッチが指定されたスパニングツリーインスタンスのルートスイッチになるように、スイッチプライオリティをデフォルト値 (32768) から著しく小さい値に変更します。このコマンドを入力すると、スイッチは、ルートスイッチのスイッチプライオリティを確認します。拡張システム ID のサポートのため、スイッチは指定されたインスタンスについて、自身のプライオリティを 24576 に設定します (この値によって、このスイッチが指定されたスパニングツリーインスタンスのルートになる場合)。

指定されたインスタンスのルートスイッチに、24576 に満たないスイッチプライオリティが設定されている場合は、スイッチは自身のプライオリティを最小のスイッチプライオリティより 4096 だけ小さい値に設定します (4096 は 4 ビットスイッチプライオリティの最下位ビットの値です。詳細については、「ブリッジ ID、スイッチプライオリティ 優先順位、および拡張システム ID」を参照してください。 [ブリッジ ID、デバイスプライオリティ、および拡張システム ID \(4 ページ\)](#))

ネットワーク上に拡張システム ID をサポートするスイッチとサポートしないスイッチが混在する場合は、拡張システム ID をサポートするスイッチがルートスイッチになることはほぼありません。拡張システム ID によって、旧ソフトウェアが稼働する接続スイッチのプライオリティより VLAN 番号が大きくなるたびに、スイッチプライオリティ値が増大します。

各スパニングツリーインスタンスのルートスイッチは、バックボーンスイッチまたはディストリビューションスイッチにする必要があります。アクセススイッチをスパニングツリーのプライマリルートとして設定しないでください。

レイヤ 2 ネットワークの直径 (つまり、レイヤ 2 ネットワーク上の任意の 2 つのエンドステーション間の最大スイッチホップカウント) を指定するには、**diameter** キーワードを指定します (MST インスタンス 0 の場合のみ使用可)。ネットワークの直径を指定すると、その直径のネットワークに最適な hello タイム、転送遅延時間、および最大エージングタイムをスイッチが自動的に設定するので、コンバージェンスの所要時間を大幅に短縮できます。**hello** キーワードを使用して、自動的に計算される hello タイムを上書きできます。

MST リージョン

スイッチを MST インスタンスに加入させるには、同じ MST コンフィギュレーション情報を使用して矛盾のないようにスイッチを設定する必要があります。同じ MST 設定の相互接続スイッチの集まりによって MST リージョンが構成されます。

MST 設定により、各デバイスが属する MST リージョンが制御されます。この設定には、領域の名前、バージョン番号、MST VLAN とインスタンスの割り当てマップが含まれます。その中で MST リージョンの設定を指定することにより、リージョンのデバイスを設定します。MST インスタンスに VLAN をマッピングし、リージョン名を指定して、リージョン番号を設定できます。手順と例については、関連項目の「MST リージョン設定の指定と MSTP のイネーブル化」リンクをクリックします。

リージョンには、同一の MST コンフィギュレーションを持った 1 つまたは複数のメンバが必要です。さらに、各メンバは、RSTP ブリッジプロトコルデータユニット (BPDU) を処理できる必要があります。ネットワーク内の MST リージョンの数に制限はありませんが、各リージョンは最大 65 のスパニングツリーインスタンスをサポートできます。インスタンスは、0

～4094 の範囲の任意の番号で識別できます。VLAN には、一度に1つのスパニングツリーインスタンスのみ割り当てることができます。

Internal Spanning Tree (IST) 、 Common and Internal Spanning Tree (CIST) 、 Common Spanning Tree (CST)

すべてのスパニングツリーインスタンスが独立している PVST+ および Rapid PVST+ とは異なり、MSTP は次の2つのタイプのスパニングツリーを確立して保持しています。

- Internal Spanning-Tree (IST) は、1つの MST リージョン内で稼働するスパニングツリーです。

各 MST リージョン内の MSTP は複数のスパニングツリーインスタンスを維持しています。インスタンス 0 は、リージョンの特殊なインスタンスで、IST と呼ばれています。その他すべての MSTI には、1～4094 の番号が付きます。

IST は、BPDU を送受信する唯一のスパニングツリーインスタンスです。他のスパニングツリーの情報はすべて、MSTP BPDU 内にカプセル化されている M レコードに格納されています。MSTP BPDU はすべてのインスタンスの情報を伝送するので、複数のスパニングツリーインスタンスをサポートする処理に必要な BPDU の数を大幅に減少できます。

同一リージョン内の MST インスタンスはすべて、同じプロトコル タイマーを共有しますが、各 MST インスタンスは独自のトポロジパラメータ (ルートスイッチ ID、ルートパスコストなど) を持っています。デフォルトでは、すべての VLAN が IST に割り当てられます。

MSTI はリージョンにローカルです。たとえばリージョン A およびリージョン B が相互接続されていても、リージョン A の MSTI 1 は、リージョン B の MSTI 1 に依存しません。

- Common and Internal Spanning-Tree (CIST) は、各 MST リージョン内の IST と、MST リージョンおよびシングルスパニングツリーを相互接続する Common Spanning-Tree (CST) の集合です。

1つのリージョン内で計算されたスパニングツリーは、スイッチドドメイン全体を網羅する CST のサブツリーと見なされます。CIST は、IEEE 802.1w、IEEE 802.1s、および IEEE 802.1D 標準をサポートするスイッチ間で実行されるスパニングツリーアルゴリズムによって形成されます。MST リージョン内の CIST は、リージョン外の CST と同じです。

マルチ スパニングツリーのリージョン内の動作

IST は1つのリージョン内のすべての MSTP スイッチを接続します。IST が収束すると、IST のルートは CIST リージョナルルートになります。これは、リージョン内で最も小さいデバイス ID、および CIST ルートに対するパスコストを持つスイッチです。ネットワークに領域が1つしかない場合、CIST リージョナルルートは CIST ルートにもなります。CIST ルートがリージョンの外部にある場合、リージョンの境界に位置する MSTP スイッチの1つが CIST リージョナルルートとして選択されます。

MSTP スイッチは初期化時に、自身が CIST のルートおよび CIST リージョナルルートであることを主張するため、CIST ルートと CIST リージョナルルートへのパス コストがいずれもゼロに設定された BPDU を送信します。スイッチはさらに MST インスタンスをすべて初期化し、自身がこれらすべてのインスタンスのルートであると主張します。スイッチは、ポート用に現在保存されているものより上位の MST ルート情報（低いデバイス ID、低いパスコストなど）を受信した場合、CIST リージョナルルートとしての主張を放棄します。

リージョンには、初期化中に多くのサブリージョンが含まれて、それぞれに独自の CIST リージョナルルートが含まれることがあります。スイッチは、優位の IST 情報を受信すると、古いサブリージョンを脱退して、真の CIST リージョナルルートが含まれている新しいサブリージョンに加入します。真の CIST リージョナルルートが含まれている以外のサブリージョンは、すべて縮小します。

正常な動作のためには、MST リージョン内のすべてのスイッチが同じ CIST リージョナルルートを承認する必要があります。共通の CIST リージョナルルートに収束する場合、そのリージョン内にある 2 つのスイッチは、1 つの MST インスタンスに対するポートの役割のみを同期させます。

マルチ スパニングツリーのリージョン間の動作

ネットワーク内に複数のリージョンまたは IEEE 802.1D 準拠のレガシースイッチが混在している場合、MSTP は、ネットワーク内のすべての MST リージョンとすべてのレガシー STP スイッチからなる CST を構築して維持します。MSTI は、リージョンの境界にある IST と組み合わせたり、CST になります。

IST は、リージョン内のすべての MSTP スイッチに接続し、スイッチドドメイン全体を網羅する CIST のサブツリーとして見なされます。サブツリーのルートは CIST リージョナルルートです。MST リージョンは、隣接する STP スイッチや MST リージョンからは仮想スイッチとして認識されます。

BPDU を送受信するのは、CST インスタンスだけです。MST インスタンスは自身のスパニングツリー情報を BPDU に追加して、ネイバー スイッチと通信し、最終的なスパニングツリー トポロジを計算します。したがって、BPDU 伝送に関連するスパニングツリーパラメータ（hello タイム、転送時間、最大エージング タイム、最大ホップ カウントなど）は、CST インスタンスだけで設定されますが、その影響はすべての MST インスタンスに及びます。スパニングツリー トポロジに関連するパラメータ（スイッチ プライオリティ、ポート VLAN コスト、ポート VLAN プライオリティなど）は、CST インスタンスと MST インスタンスの両方で設定できます。

MSTP スイッチは、バージョン 3 RSTP BPDU または IEEE 802.1D STP BPDU を使用して、レガシー IEEE 802.1D デバイスと通信します。MSTP スイッチは、MSTP BPDU を使用して MSTP デバイスと通信します。

IEEE 802.1s の用語

シスコの先行標準実装で使用される一部の MST 命名規則は、一部の内部パラメータまたはリージョンパラメータを識別するように変更されました。これらのパラメータは、ネットワーク全体に関連している外部パラメータと違い、MST リージョン内でのみ影響があります。CIST は

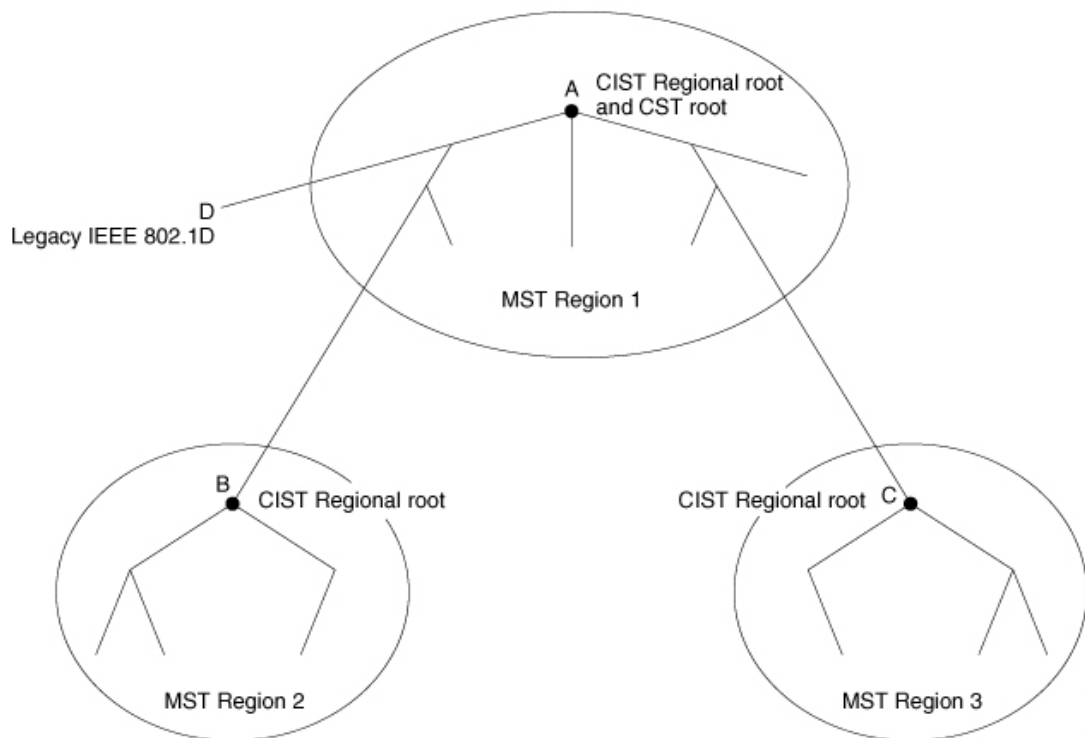
ネットワーク全体を網羅するスパニングツリーインスタンスのため、CIST パラメータのみ、内部修飾子やリージョナル修飾子ではなく外部修飾子が必要です。

- CIST ルートは、ネットワーク全体を網羅する一意のインスタンスのためのルートスイッチです。
- CIST 外部ルートパス コストは、CIST ルートまでのコストです。このコストは MST 領域内で変化しません。CIST では、MST リージョンが単一のスイッチのように見えるので注意してください。CIST 外部ルートパス コストは、この仮想デバイス、およびどの領域にも属さないデバイスの中で計算されるルートパス コストです。
- CIST ルートが領域内にある場合、CIST リージョナルルートは CIST ルートです。または、CIST リージョナルルートがそのリージョンで CIST ルートに最も近いスイッチになります。CIST リージョナルルートは IST のルートスイッチとして動作します。
- CIST 内部ルートパス コストは、領域内の CIST リージョナルルートまでのコストです。このコストは、IST つまりインスタンス 0 だけに関連します。

マルチスパニングツリーのリージョンの図

この図は、3 個の MST リージョンとレガシー IEEE 802.1D デバイス (D) を示しています。リージョン 1 の CIST リージョナルルート (A) は、CIST ルートでもあります。リージョン 2 の CIST リージョナルルート (B)、およびリージョン 3 の CIST リージョナルルート (C) は、CIST 内のそれぞれのサブツリーのルートです。RSTP はすべてのリージョンで稼働しています。

図 4: MST リージョン、CIST リージョナルルート、CST ルート



ホップカウント

ISTおよびMSTインスタンスは、スパニングツリートポロジの計算に、コンフィギュレーション BPDU のメッセージ有効期間と最大エージング タイムの情報を使用しません。その代わりに、IP Time To Live (TTL) メカニズムに似た、ルートまでのパス コストおよびホップ カウントメカニズムを使用します。

spanning-tree mst max-hops グローバル コンフィギュレーション コマンドを使用すると、領域内で最大ホップ カウントを設定し、その領域の IST およびすべての MST インスタンスに適用できます。ホップ カウントを設定すると、メッセージエージング情報を設定するのと同様の結果が得られます（再構成の開始時期を決定します）。インスタンスのルートスイッチは、常にコストを 0、ホップ カウントを最大値に設定して BPDU（または M レコード）を送信します。この BPDU を受信したスイッチは、受信 BPDU の残存ホップ カウントから 1 だけ差し引いた値を残存ホップ カウントとする BPDU を生成し、これを伝播します。このホップ カウントが 0 になると、スイッチはその BPDU を廃棄し、ポート用に維持されていた情報を期限切れにします。

BPDU の RSTP 部分に格納されているメッセージ有効期間と最大エージング タイムの情報は、リージョン全体で同じままであり、そのリージョンの境界に位置する指定ポートによって同じ値が伝播されます。

境界ポート

シスコ先行標準の実装では、境界ポートは、RSTP が稼働する単一のスパニングツリー リージョン、PVST+ または Rapid PVST+ が稼働する単一のスパニングツリー リージョン、または異なる MST コンフィギュレーションを持つ別の MST リージョンに MST リージョンを接続します。また、境界ポートは、指定デバイスがシングル スパニングツリー スイッチまたは異なる MST コンフィギュレーションを持つスイッチのいずれかである LAN に接続されます。

IEEE 802.1s 標準では、境界ポートの定義はなくなりました。IEEE 802.1Q-2002 標準では、ポートが受信できる 2 種類のメッセージを識別します。

- 内部（同一リージョンから）
- 外部（別のリージョンから）

メッセージが内部の場合、CIST の部分は CIST によって受信されるので、各 MST インスタンスは個々の M レコードだけを受信します。

メッセージが外部である場合、CIST だけが受信します。CIST の役割がルートや代替ルートの場合、または外部 BPDU のトポロジが変更された場合は、MST インスタンスに影響する可能性があります。

MST リージョンには、デバイスおよび LAN の両方が含まれます。セグメントは、DP のリージョンに属します。そのため、セグメントの指定ポートではなく異なるリージョンにあるポートは境界ポートになります。この定義では、リージョン内部の 2 つのポートが、別のリージョンに属するポートとセグメントを共有し、内部メッセージおよび外部メッセージの両方を 1 つのポートで受信できるようになります。

シスコ先行標準の実装との主な違いは、STP 互換モードを使用している場合、指定ポートが境界ポートとして定義されない点です。



(注) レガシー STP デバイスがセグメントに存在する場合、メッセージは常に外部と見なされます。

シスコ先行標準の実装から他に変更された点は、送信デバイス ID を持つ RSTP またはレガシー IEEE 802.1Q デバイスの部分に、CIST リージョナルルートデバイス ID フィールドが加えられたことです。リージョン全体は、一貫した送信者デバイス ID をネイバーデバイスに送信し、単一仮想デバイスのように動作します。この例では、A または B がセグメントに指定されているかどうかに関係なく、ルートの一貫した送信者デバイス ID が同じである BPDU をスイッチ C が受信します。

IEEE 802.1s の実装

シスコの IEEE MST 標準の実装には、標準の要件を満たす機能だけでなく、すでに公開されている標準には含まれていない一部の（要望されている）先行標準の機能が含まれています。

ポートの役割名の変更

境界の役割は最終的に MST 標準に含まれませんでした。境界の概念自体はシスコの実装に投影されています。ただし、リージョン境界にある MST インスタンスのポートは、対応する CIST ポートのステータスに必ずしも従うわけではありません。現在、2つの境界の役割が存在しています。

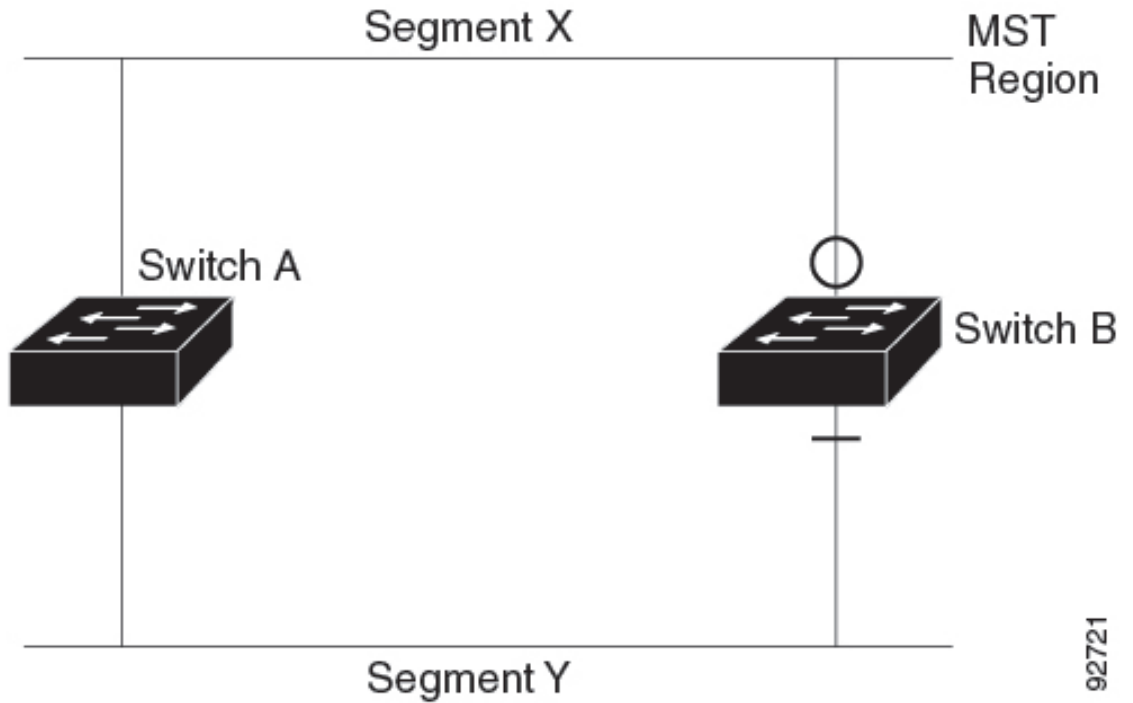
- 境界ポートが CIST リージョナルルートのルートポートである場合：CIST インスタンスポートを提案されて同期中の場合、対応するすべての MSTI ポートの同期を取り終わった後であれば（その後フォワーディングします）、その場合のみ合意を返信してフォワーディングステータスに移行できます。MSTI ポートには、特別なプライマリロールがありません。
- 境界ポートが CIST リージョナルルートのルートポートでない：MSTI ポートは、CIST ポートのステータスおよび役割に従います。標準では提供される情報が少ないため、MSTI ポートが BPDU (M レコード) を受信しない場合、MSTI ポートが BPDU を代わりにブロックできる理由がわかりにくい場合があります。この場合、境界の役割自体は存在していませんが、**show** コマンドで見ると、出力される *type* カラムで、ポートが境界ポートとして認識されていることがわかります。

レガシーデバイスと標準デバイスの相互運用

先行標準デバイスの自動検出はエラーになることがあるので、インターフェイスコンフィギュレーションコマンドを使用して先行標準ポートを識別できます。標準デバイスと先行標準デバイスの間にあるリージョンは形成できませんが、CIST を使用することで相互運用できます。このような特別な方法を採用しても、失われる機能は、異なるインスタンス上のロードランシングだけです。ポートが先行標準の BPDU を受信すると、CLI (コマンドラインインターフェイス) にはポートの設定に応じて異なるフラグが表示されます。デバイスが先行標準 BPDU 送信用に設定されていないポートで先行標準 BPDU を初めて受信したときは、Syslog メッセージも表示されます。

図 5: 標準デバイスと先行標準デバイスの相互運用

A を標準スイッチ、B を先行標準のスイッチと仮定してください。両方とも同じリージョンに設定されています。A は CIST のルートスイッチであり、B にはセグメント X にルートポート (BX)、セグメント Y に代替ポート (BY) があります。セグメント Y がフラップして BY のポートが代替になってから 1 つの準規格 BPDU を送信すると、準規格スイッチが Y に接続されていることを AY は検出できず、規格 BPDU の送信を続けます。ポート BY は境界に固定され、A と B との間でのロードランシングは不可能になります。セグメント X にも同じ問題がありますが、B はトポロジの変更であれば送信する場合があります。



(注) 規格 MST 実装と準規格 MST 実装間の相互作用を最低限に抑えることを推奨します。

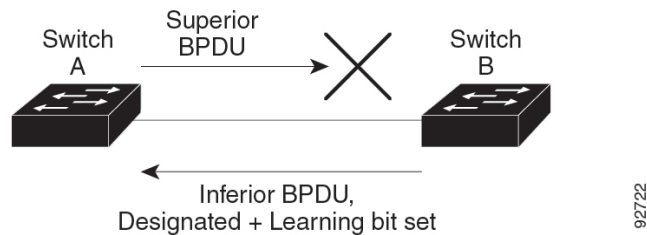
単一方向リンク障害の検出

IEEE MST 標準にはこの機能が存在していませんが、Cisco IOS Release には加えられています。ソフトウェアは、受信した BPDU でポートのロールおよびステートの一貫性をチェックし、ブリッジンググループの原因となることがある単方向リンク障害を検出します。

指定ポートは、矛盾を検出すると、その役割を維持しますが、廃棄ステートに戻ります。一貫性がない場合は、接続を中断した方がブリッジンググループを解決できるからです。

図 6: 単一方向リンク障害の検出

次の図に、ブリッジンググループの一般的な原因となる単方向リンク障害を示します。スイッチ A はルートデバイスであり、スイッチ B へのリンクで BPDU は失われます。RSTP および MST BPDU には、送信側ポートの役割と状態が含まれます。この情報があれば、スイッチ A は、送信した優位 BPDU にスイッチ B が反応しないこと、さらにスイッチ B はルートスイッチではなく指定スイッチであることを検出できます。この結果、スイッチ A は、そのポートをブロックし（またはブロックし続け）、ブリッジンググループが防止されます。



マルチ スパニングツリー プロトコルとスイッチ スタック

スイッチ スタックは、ネットワークのその他の部分に対しては単一のスパニングツリー ノードに見え、すべてのスタック メンバが与えられたスパニングツリーに同一のブリッジ ID を使用します。ブリッジ ID は、デバイスの MAC アドレスから取得されます。

スタックがネットワークのルートで、スタック内でルートの選択が行われていない場合は、アクティブスイッチがスタックルートになります。

スイッチスタックがスパニングツリールートで、アクティブスイッチで障害が発生した、またはスタックから外れた場合、スタンバイスイッチが新しいアクティブスイッチになり、ブリッジ ID は同じままで、スパニングツリーの再コンバージェンスが発生する可能性があります。

MSTP をサポートしていないデバイスが、MSTP またはリバースをサポートしているスイッチスタックに追加されると、デバイスはバージョンが不一致の状態になります。可能な場合、デバイスは、スイッチスタックで実行中のソフトウェアと同じバージョンに自動的にアップグレードまたはダウングレードされます。

IEEE 802.1D スパニングツリープロトコルとの相互運用性

MSTP が稼働しているデバイスは、IEEE 802.1D 準拠のレガシーデバイスとの相互運用を可能にする組み込み型のプロトコル移行メカニズムをサポートします。このデバイスは、レガシー IEEE 802.1D コンフィギュレーション BPDU（プロトコルバージョンが 0 に設定されている BPDU）を受信すると、そのポート上では IEEE 802.1D BPDU のみを送信します。また、MSTP デバイスは、レガシー BPDU、別のリージョンに関連付けられている MSTP BPDU（バージョン 3）、または RSTP BPDU（バージョン 2）を受信することによって、ポートがリージョンの境界に位置していることを検出できます。

ただし、デバイスが IEEE 802.1D BPDU を受信していない場合は、自動的に MSTP モードに戻りません。これはレガシースイッチが指定デバイスでない限り、レガシースイッチがリンクから削除されたかどうか検出できないためです。このデバイスの接続先デバイスが領域に加わったとき、デバイスは境界ルールをポートに割り当て続けることもあります。プロトコル移行プロセスを再開するには（強制的にネイバーデバイスと再びネゴシエーションするには）、**clear spanning-tree detected-protocols** 特権 EXEC コマンドを使用します。

リンク上のすべてのレガシースイッチが RSTP デバイスであれば、これらのデバイスは、RSTP BPDU 同様に MSTP BPDU を処理できます。したがって、MSTP デバイスは、バージョン 0 コンフィギュレーションと TCN BPDU またはバージョン 3 MSTP BPDU のいずれかを境界ポート

で送信します。境界ポートは、指定デバイスがシングル スパンニングツリー スイッチまたは異なる MST コンフィギュレーションを持つスイッチのいずれかである LAN に接続されます。

高速スパンニングツリー プロトコルの概要

RSTP は、ポイントツーポイントの配線を利用して、スパンニングツリーの高速コンバージェンスを実現します。また、1 秒未満の間に、スパンニングツリーを再構成できます (IEEE 802.1D スパンニングツリーのデフォルトに設定されている 50 秒とは異なります)。

ポートの役割およびアクティブ トポロジ

RSTP は、ポートに役割を割り当てて、アクティブ トポロジを学習することによって高速コンバージェンスを実現します。RSTP はデバイスをルートデバイスとして最も高いデバイスプライオリティ (プライオリティの数値が一番小さい) に選択するために、IEEE 802.1D STP 上に構築されます。RSTP は、次のうちいずれかのポートの役割をそれぞれのポートに割り当てます。

- ルートポート：デバイスがルートスイッチにパケットを転送するとき、最適な (コストが最小の) パスを提供します。
- 指定ポート：指定デバイスに接続し、その LAN からルートスイッチにパケットを転送するとき、パスコストを最低にします。指定デバイスが LAN への接続に使用したポートは、指定ポートと呼ばれます。
- 代替ポート：現在のルート ポートが提供したパスに代わるルート スイッチへの代替パスを提供します。
- バックアップポート：指定ポートが提供した、スパンニングツリーのリーフに向かうパスのバックアップとして機能します。2つのポートがポイントツーポイントリンクによってループバックで接続した場合、または共有 LAN セグメントへの複数の接続がデバイスにある場合に限り、バックアップ ポートは存在できます。
- ディセーブルポート：スパンニングツリーの動作において何も役割が与えられていません。

ルート ポートまたは指定ポートのロールを持つポートは、アクティブなトポロジに含まれます。代替ポートまたはバックアップ ポートのロールがあるポートは、アクティブ トポロジから除外されます。

ネットワーク全体のポートの役割に矛盾のない安定したトポロジでは、RSTPは、すべてのルートポートおよび指定ポートがただちにフォワーディング状態に移行し、代替ポートとバックアップポートが必ず廃棄状態 (IEEE 802.1D のブロッキング状態と同じ) になるように保証します。ポートの状態により、転送処理および学習処理の動作が制御されます。

表 6: ポート状態の比較

運用ステータス	STP ポートステート (IEEE 802.1D)	RSTP ポートステート	ポートがアクティブトポロジに含まれているか
イネーブル	ブロッキング	廃棄	×

運用ステータス	STP ポートステート (IEEE 802.1D)	RSTP ポートステート	ポートがアクティブトポロジに含まれているか
イネーブル	リスニング	廃棄	×
イネーブル	ラーニング	ラーニング	○
イネーブル	転送	転送	○
ディセーブル	ディセーブル	廃棄	×

Cisco STP の実装との一貫性を保つため、このマニュアルでは、ポート ステートを廃棄ではなくブロッキングとして定義します。DP はリスニング ステートから開始します。

高速コンバージェンス

RSTP は、デバイス、デバイスポート、LAN のうちいずれかの障害のあと、接続の高速回復を提供します。エッジポート、新しいルートポート、ポイントツーポイントリンクで接続したポートに、高速コンバージェンスが次のように提供されます。

- エッジポート : **spanning-tree portfast** インターフェイス コンフィギュレーション コマンドを使用して RSTP デバイスでエッジポートとしてポートを設定した場合、エッジポートはフォワーディングステートにすぐに移行します。エッジポートは **Port Fast** 対応ポートと同じであり、単一エンドステーションに接続しているポートだけでイネーブルにする必要があります。
- ルートポート : RSTP は、新しいルートポートを選択した場合、古いルートポートをブロックし、新しいルートポートをフォワーディングステートにすぐに移行します。
- ポイントツーポイントリンク : ポイントツーポイントリンクによってあるポートと別のポートを接続することでローカルポートが指定ポートになると、提案合意ハンドシェイクを使用して他のポートと急速な移行がネゴシエートされ、トポロジにループがなくなります。

図 7: 高速コンバージェンスの提案と合意のハンドシェイク

スイッチ A がスイッチ B にポイントツーポイントリンクで接続され、すべてのポートはブロッキングステートになっています。スイッチ A のプライオリティがスイッチ B のプライオリティよりも数値的に小さいとします。スイッチ A は提案メッセージ (提案フラグを設定した設定 BPDU) をスイッチ B に送信し、指定デバイスとしてそれ自体を提案します。

スイッチ B は、提案メッセージを受信すると、提案メッセージを受信したポートを新しいルートポートとして選択し、すべての非エッジポートをブロッキングステートにします。さらに、新しいルートポート経由で合意メッセージ (合意フラグが設定された BPDU) を送信します。

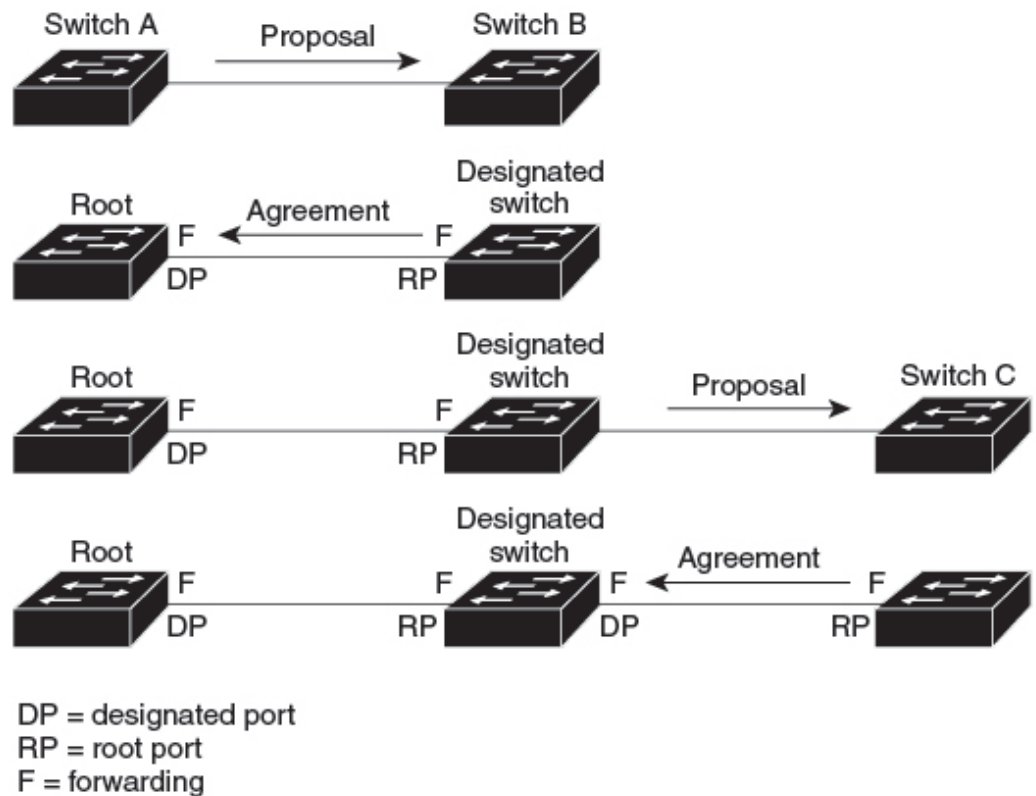
スイッチ A は、スイッチ B の合意メッセージを受信すると、ただちに自身の指定ポートをフォワーディングステートにします。スイッチ B はその非エッジポートをすべてブロッ

くし、またスイッチ A とスイッチ B はポイントツーポイントリンクで接続されているので、ネットワークにループは形成されません。

スイッチ C がスイッチ B に接続された場合も、同様のハンドシェイクメッセージが交換されます。スイッチ C はスイッチ B に接続されたポートをルートポートとして選択し、両端のポートはただちにフォワーディングステートに移行します。このハンドシェイク処理を繰り返して、もう1つのデバイスがアクティブトポロジに加わります。ネットワークが収束すると、この提案/合意ハンドシェイクがルートからスパニングツリーのリーフへと進みます。

スイッチスタックでは、Cross-Stack Rapid Transition (CSRT) 機能を使用すると、ポートがフォワーディングステートに移行する前に、スタックメンバで、提案/合意ハンドシェイク中にすべてのスタックメンバから確認メッセージを受信できます。デバイスが MST モードの場合、CSRT は自動的に有効にされます。

デバイスはポートのデュプレックスモードによってリンクタイプを学習します。全二重ポートはポイントツーポイント接続と見なされ、半二重接続は共有接続と見なされます。デュプレックス設定によって制御されるデフォルト設定を無効にするには、**spanning-tree link-type** インターフェイスコンフィギュレーションコマンドを入力します。



88760

ポート ロールの同期

デバイスがそのルータのポートの1つで提案メッセージを受信し、そのポートが新しいルートポートとして選択されると、RSTPによってその他すべてのポートが新しいルートの情報と強制的に同期化します。

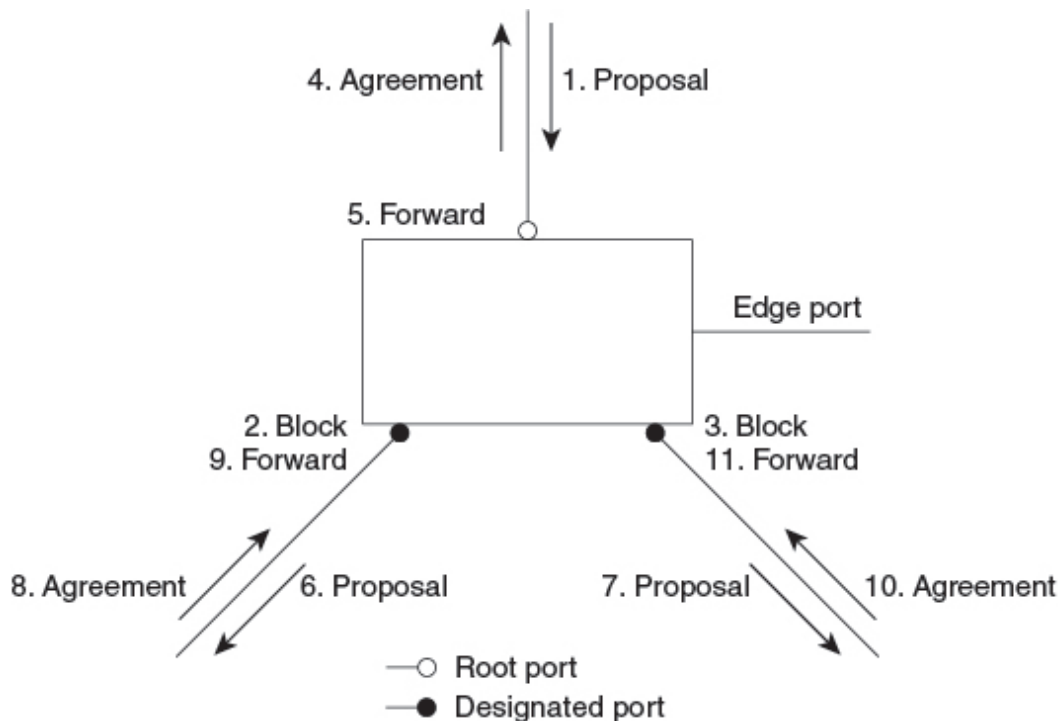
その他すべてのポートを同期化する場合、ルートポートで受信した優位ルート情報でデバイスは同期化されます。デバイスのそれぞれのポートは、次のような場合に同期化します。

- ポートがブロッキング ステートである。
- エッジポートである（ネットワークのエッジに存在するように設定されたポート）。

指定ポートがフォワーディング ステートでエッジポートとして設定されていない場合、RSTPによって新しいルート情報と強制的に同期されると、その指定ポートはブロッキングステートに移行します。一般的にRSTPがルート情報でポートを強制的に同期化し、ポートが上の条件を満たしていない場合、そのポートステートはブロッキングに設定されます。

図 8: 高速コンバージェンス中のイベントのシーケンス

すべてのポートが同期化されてから、デバイスは、ルートポートに対応する指定デバイスに合意メッセージを送信します。ポイントツーポイントリンクで接続されたデバイスがポートの役割で合意すると、RSTPはポートステートをフォワーディングにすぐに移行します。



88761

ブリッジプロトコルデータユニットの形式および処理

RSTP BPDU のフォーマットは、プロトコルバージョンが 2 に設定されている点を除き、IEEE 802.1D BPDU のフォーマットと同じです。新しい 1 バイトのバージョン 1 の Length フィールドは 0 に設定されます。これはバージョン 1 のプロトコルの情報がないことを示しています。

表 7: RSTP BPDU フラグ

ビット	機能
0	トポロジーの変化 (TC)
1	提案
2 ~ 3:	ポートの役割:
00	不明
01	代替ポート
10	ルートポート
11	指定ポート
4	ラーニング
5	転送
6	合意
7	トポロジー変更確認応答 (TCA)

送信側デバイスは RSTP BPDU の提案フラグを設定し、その LAN の指定デバイスとして自分自身を提案します。提案メッセージのポートの役割は、常に DP に設定されます。

送信側デバイスは、RSTP BPDU の合意フラグを設定して以前の提案を受け入れます。合意メッセージ内のポート ロールは、常にルートポートに設定されます。

RSTP には個別のトポロジ変更通知 (TCN) BPDU はありません。TC フラグが使用されて、TC が示されます。ただし、IEEE 802.1D デバイスとの相互運用性を保つために、RSTP デバイスは TCN BPDU の処理と生成を行います。

ラーニングフラグおよびフォワーディングフラグは、送信側ポートのステータスに従って設定されます。

上位ブリッジプロトコルデータユニット情報の処理

ポートに現在保存されているルート情報よりも優位のルート情報 (小さいデバイス ID、低いパスコストなど) をポートが受け取ると、RSTP は再構成を開始します。ポートが新しいルートポートとして提案されて選択されると、RSTP は強制的にその他すべてのポートを同期化します。

受信した BPDU が、提案フラグが設定されている RSTP BPDU である場合、デバイスは他のすべてのポートが同期化されてから合意メッセージを送信します。BPDU が IEEE 802.1D BPDU の場合、デバイスは提案フラグを設定せずに、そのポートの転送遅延タイマーを起動します。新しいルートポートでは、フォワーディングステートに移行するために、2倍の転送遅延時間が必要となります。

ポートで優位の情報が受信されたために、そのポートがバックアップポートまたは代替ポートになる場合、RSTP はそのポートをブロッキングステートに設定し、合意メッセージは送信しません。DP は、転送遅延タイマーが失効するまで、提案フラグを設定して BPDU を送信し続け、転送遅延タイマーの失効時に、ポートはフォワーディングステートに移行します。

下位ブリッジプロトコル データ ユニット情報の処理

指定ポートの役割を持つ下位 BPDU（そのポートに現在保存されている値より大きいデバイス ID、高いパスコストなど）を指定ポートが受信した場合、その指定ポートはただちに現在の自身の情報で応答します。

トポロジの変更

ここでは、スパニングツリー トポロジの変更処理について、RSTP と IEEE 802.1D の相違を説明します。

- 検出：IEEE 802.1D では、どのようなブロッキングステートとフォワーディングステートとの間の移行でもトポロジの変更が発生しますが、RSTP でトポロジの変更が発生するのは、ブロッキングステートからフォワーディングステートに移行する場合だけです（トポロジの変更と見なされるのは、接続数が増加する場合だけです）。エッジポートにおけるステート変更は、TC の原因になりません。RSTP デバイスは、TC を検出すると、TCN を受信したポートを除く、エッジ以外のすべてのポートで学習した情報を削除します。
- 通知：IEEE 802.1D は TCN BPDU を使用しますが、RSTP は使用しません。ただし、IEEE 802.1D との相互運用性を保つために、RSTP デバイスは TCN BPDU の処理と生成を行います。
- 確認：RSTP デバイスは、指定ポートで IEEE 802.1D デバイスから TCN メッセージを受信した場合、TCA ビットが設定された IEEE 802.1D コンフィギュレーション BPDU で応答します。ただし、IEEE 802.1D デバイスに接続されたルートポートで TC 時間タイマー（IEEE 802.1D のトポロジ変更タイマーと同じ）がアクティブであり、TCA ビットが設定されたコンフィギュレーション BPDU が受信された場合、TC 時間タイマーはリセットされます。

この処理は、IEEE 802.1D デバイスをサポートする目的でのみ必要とされます。RSTP BPDU は TCA ビットが設定されていません。

- 伝播：RSTP デバイスは、DP またはルートポートを介して別のデバイスから TC メッセージを受信すると、エッジ以外のすべての DP、およびルートポート（TC メッセージを受信したポートを除く）に変更を伝播します。デバイスはこのようなすべてのポートで TC-while タイマーを開始し、そのポートで学習した情報を消去します。

- プロトコルの移行：IEEE 802.1D デバイスとの下位互換性を保つため、RSTP は IEEE 802.1D コンフィギュレーション BPDU および TCN BPDU をポート単位で必要に応じて送信します。

ポートが初期化されると、移行遅延タイマーが開始され（RSTP BPDU が送信される最低時間を指定）、RSTP BPDU が送信されます。このタイマーがアクティブである間、デバイスはそのポートで受信したすべての BPDU を処理し、プロトコルタイプを無視します。

デバイスはポートの移行遅延タイマーが満了した後に IEEE 802.1D BPDU を受信した場合、IEEE 802.1D デバイスに接続されていると想定し、IEEE 802.1D BPDU のみの使用を開始します。ただし、RSTP デバイスが1つのポートで IEEE 802.1D BPDU を使用していて、タイマーが満了した後に RSTP BPDU を受信した場合、タイマーが再起動し、そのポートで RSTP BPDU の使用が開始されます。

プロトコル移行プロセス

MSTP が稼働しているデバイスは、IEEE 802.1D 準拠のレガシーデバイスとの相互運用を可能にする組み込み型のプロトコル移行メカニズムをサポートします。このデバイスは、レガシー IEEE 802.1D コンフィギュレーション BPDU（プロトコルバージョンが 0 に設定されている BPDU）を受信すると、そのポート上では IEEE 802.1D BPDU のみを送信します。また、MSTP デバイスは、レガシー BPDU、別のリージョンに関連付けられている MST BPDU（バージョン 3）、または RST BPDU（バージョン 2）を受信することによって、ポートがリージョンの境界に位置していることを検出できます。

ただし、デバイスが IEEE 802.1D BPDU を受信していない場合は、自動的に MSTP モードに戻りません。これはレガシースイッチが指定デバイスでない限り、レガシースイッチがリンクから削除されたかどうか検出できないためです。また、接続するデバイスがリージョンに加入していると、デバイスはポートに境界の役割を割り当て続ける場合があります。

マルチ スパニングツリー プロトコルのデフォルトの設定

表 8: MSTP のデフォルト設定

機能	デフォルト設定
スパニングツリー モード	
デバイスプライオリティ（CIST ポートごとに設定可能）	32768
スパニングツリー ポート プライオリティ（CIST ポート単位で設定可能）	128
スパニングツリー ポート コスト（CIST ポート単位で設定可能）	
hello タイム	
転送遅延時間	

機能	デフォルト設定
最大エージング タイム	20 秒
最大ホップ カウント	20 ホップ

MSTP および MSTP パラメータの設定方法

ここでは、MSTP および MSTP パラメータの設定について説明します。

マルチ スパンニング ツリー リージョン設定の指定とマルチ スパンニング ツリー プロトコルのイネーブル化

2つ以上のスイッチを同じ MST リージョンに設定するには、その2つのスイッチに同じ VLAN/インスタンス マッピング、同じコンフィギュレーション リビジョン番号、同じ名前を設定しなければなりません。

リージョンには、MST設定が同一である、1つ以上のメンバーを含めることができます。各メンバーでは、RSTP BPDU を処理できる必要があります。ネットワーク内の MST リージョンの数に制限はありませんが、各リージョンは最大 65 のスパンニングツリー インスタンスのみをサポートできます。VLAN には、一度に1つのスパンニングツリー インスタンスのみ割り当てることができます。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	spanning-tree mst configuration 例： Device(config)# spanning-tree mst configuration	MST コンフィギュレーションモードを開始します。
ステップ 4	instance instance-id vlan vlan-range 例： Device(config-mst)# instance 1 vlan 10-20	VLAN を MSTI にマップします。 • <i>instance-id</i> に指定できる範囲は、0 ~ 4094 です。

	コマンドまたはアクション	目的
		<p>• vlan <i>vlan-range</i> に指定できる範囲は、1 ~ 4094 です。</p> <p>VLAN を MSTI にマップする場合、マッピングは増加され、コマンドに指定した VLAN は、以前マッピングした VLAN に追加されるか、そこから削除されます。</p> <p>VLAN の範囲を指定するには、ハイフンを使用します。たとえば instance 1 vlan 1-63 では、VLAN 1 ~ 63 が MSTI 1 にマップされます。</p> <p>VLAN を列挙して指定する場合は、カンマを使用します。たとえば instance 1 vlan 10, 20, 30 と指定すると、VLAN 10、20、30 が MST インスタンス 1 にマッピングされます。</p>
ステップ 5	<p>name <i>name</i></p> <p>例 :</p> <pre>Device(config-mst)# name region1</pre>	<p>コンフィギュレーション名を指定します。<i>name</i> 文字列の最大の長さは 32 文字であり、大文字と小文字が区別されます。</p>
ステップ 6	<p>revision <i>version</i></p> <p>例 :</p> <pre>Device(config-mst)# revision 1</pre>	<p>設定リビジョン番号を指定します。指定できる範囲は 0 ~ 65535 です。</p>
ステップ 7	<p>show pending</p> <p>例 :</p> <pre>Device(config-mst)# show pending</pre>	<p>保留中の設定を表示し、設定を確認します。</p>
ステップ 8	<p>exit</p> <p>例 :</p> <pre>Device(config-mst)# exit</pre>	<p>すべての変更を適用し、グローバルコンフィギュレーションモードに戻ります。</p>
ステップ 9	<p>spanning-tree mode mst</p> <p>例 :</p> <pre>Device(config)# spanning-tree mode mst</pre>	<p>MSTP をイネーブルにします。RSTP もイネーブルになります。</p> <p>スパンニング ツリー モードを変更すると、すべてのスパンニング ツリー インスタンスは以前のモードであるため停止し、新しいモードで再起動するので、トラフィックを中断させる可能性があります。</p>

	コマンドまたはアクション	目的
		MSTP と PVST+ または MSTP と Rapid PVST+ を同時に実行することはできません。
ステップ 10	end 例： Device(config)# end	特権 EXEC モードに戻ります。

(任意) ルート デバイスの設定

ルート デバイスを設定するには、次の手順を実行します。

始める前に

- MST が、デバイスで指定されて有効になっている必要があります。
- 指定された MST インスタンス ID も把握する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	spanning-tree mst instance-id root primary 例： Device(config)# spanning-tree mst 0 root primary	デバイスをルートデバイスとして設定します。 <i>instance-id</i> には、単一のインスタンス、ハイフンで区切られた範囲のインスタンス、またはカンマで区切られた一連のインスタンスを指定できます。指定できる範囲は 0 ~ 4094 です。
ステップ 4	end 例： Device(config)# end	特権 EXEC モードに戻ります。

(任意) セカンダリ ルート デバイスの設定

拡張システム ID をサポートするデバイスをセカンダリルートとして設定する場合、デバイスプライオリティはデフォルト値 (32768) から 28672 に修正されます。プライマリルートデバイスで障害が発生した場合は、このデバイスが指定インスタンスのルートデバイスになる可能性があります。ここでは、その他のネットワークデバイスが、デフォルトのデバイスプライオリティの 32768 を使用しているためにルートデバイスになる可能性が低いことが前提となっています。

このコマンドを複数のデバイスに対して実行すると、複数のバックアップルートデバイスを設定できます。**spanning-tree mst instance-id root primary** グローバル コンフィギュレーション コマンドでプライマリルートデバイスを設定したときと同じネットワーク直径および hello タイム値を使用してください。

セカンダリ ルート デバイスを設定するには、次の手順を実行します。

始める前に

- MST が、デバイスで指定されて有効になっている必要があります。
- 指定された MST インスタンス ID も把握する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します (要求された場合)。
ステップ 2	configure terminal 例 : Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	spanning-tree mst instance-id root secondary 例 : Device(config)# spanning-tree mst 0 root secondary	デバイスをセカンダリルートデバイスとして設定します。 <i>instance-id</i> には、単一のインスタンス、ハイフンで区切られた範囲のインスタンス、またはカンマで区切られた一連のインスタンスを指定できます。指定できる範囲は 0 ~ 4094 です。
ステップ 4	end 例 : Device(config)# end	特権 EXEC モードに戻ります。

(任意) ポート プライオリティの設定

ループが発生した場合、MSTPはポートプライオリティを使用して、フォワーディングステートにするインターフェイスを選択します。最初に選択されるインターフェイスには高いプライオリティ値（小さい数値）を割り当て、最後に選択されるインターフェイスには低いプライオリティ値（高い数値）を割り当てることができます。すべてのインターフェイスに同じプライオリティ値が与えられている場合、MSTPはインターフェイス番号が最小のインターフェイスをフォワーディングステートにし、他のインターフェイスをブロックします。



- (注) デバイスがスイッチスタックのメンバーの場合、**spanning-tree mst[instance-id] port-priority priority** インターフェイス コンフィギュレーション コマンドの代わりに、**spanning-tree mst[instance-id] cost cost** インターフェイス コンフィギュレーション コマンドを使用し、フォワーディングステートにするポートを選択する必要があります。最初に選択させたいポートには、より小さいコスト値を割り当て、最後に選択させたいポートには、より大きいコスト値を割り当てることができます。

ポートの優先順位を設定するには、次の手順を実行します。

始める前に

- MST が、デバイスで指定されて有効になっている必要があります。
- 指定された MST インスタンス ID と使用されるインターフェイスも把握する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	interface interface-id 例： Device(config)# interface gigabitethernet 1/0/1	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	spanning-tree mst instance-id port-priority priority	ポートプライオリティを設定します。

	コマンドまたはアクション	目的
	<p>例 :</p> <pre>Device(config-if)# spanning-tree mst 0 port-priority 64</pre>	<ul style="list-style-type: none"> • <i>instance-id</i> には、単一のインスタンス、ハイフンで区切られた範囲のインスタンス、またはカンマで区切られた一連のインスタンスを指定できます。指定できる範囲は 0 ~ 4094 です。 • <i>priority</i> 値の範囲は 0 ~ 240 で、16 ずつ増加します。デフォルト値は 128 です。値が小さいほど、プライオリティが高くなります。 <p>使用可能な値は、0、16、32、48、64、80、96、112、128、144、160、176、192、208、224、240 だけです。その他の値はすべて拒否されます。</p>
ステップ 5	<p>end</p> <p>例 :</p> <pre>Device(config-if)# end</pre>	特権 EXEC モードに戻ります。

show spanning-tree mst interface interface-id 特権 EXEC コマンドで情報が表示されるのは、ポートがリンクアップ動作可能な状態にある場合に限られます。そうでない場合は、**show running-config interface** 特権 EXEC コマンドを使用して設定を確認してください。

(任意) パス コストの設定

MSTP パス コストのデフォルト値は、インターフェイスのメディア速度に基づきます。ループが発生した場合、MSTP はコストを使用して、フォワーディング ステートにするインターフェイスを選択します。最初に選択されるインターフェイスには低いコスト値を割り当て、最後に選択されるインターフェイスには高いコスト値を割り当てることができます。すべてのインターフェイスに同じコスト値が与えられている場合、MSTP はインターフェイス番号が最小のインターフェイスをフォワーディング ステートにし、他のインターフェイスをブロックします。

パス コストを設定するには、次の手順を実行します。

始める前に

- MST が、デバイスで指定されて有効になっている必要があります。
- 指定された MST インスタンス ID と使用されるインターフェイスも把握する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	interface interface-id 例： Device(config)# interface gigabitethernet 1/0/1	設定するインターフェイスを指定し、インターフェイス コンフィギュレーションモードを開始します。有効なインターフェイスには、物理ポートとポートチャネル論理インターフェイスがあります。指定できるポートチャネルの範囲は1～48です。
ステップ 4	spanning-tree mst instance-id cost cost 例： Device(config-if)# spanning-tree mst 0 cost 17031970	コストを設定します。 ループが発生した場合、MSTP はパスコストを使用して、フォワーディングステートにするインターフェイスを選択します。低いパス コストは高速送信を表します。 <ul style="list-style-type: none">• <i>instance-id</i> には、単一のインスタンス、ハイフンで区切られた範囲のインスタンス、またはカンマで区切られた一連のインスタンスを指定できます。指定できる範囲は 0 ～ 4094 です。• <i>cost</i> の範囲は 1 ～ 200000000 です。デフォルト値はインターフェイスのメディア速度から派生します。
ステップ 5	end 例： Device(config-if)# end	特権 EXEC モードに戻ります。

show spanning-tree mst interface interface-id 特権 EXEC コマンドによって表示されるのは、リンクアップ動作可能状態のポートの情報だけです。そうでない場合は、**show running-config** 特権 EXEC コマンドを使用して設定を確認してください。

(任意) デバイス プライオリティの設定

デバイスのプライオリティを変更すると、スタンドアロンスイッチまたはスタック内のスイッチであるかに関係なく、ルートスイッチとして選択される可能性が高くなります。



- (注) このコマンドの使用には注意してください。通常のネットワーク設定では、**spanning-tree mst instance-id root primary** および **spanning-tree mst instance-id root secondary** グローバル コンフィギュレーションコマンドを使用して、デバイスをルートまたはセカンダリルートデバイスとして指定することをお勧めします。これらのコマンドが動作しない場合にのみデバイスプライオリティを変更する必要があります。

デバイス優先順位を設定するには、次の手順を実行します。

始める前に

- MST が、デバイスで指定されて有効になっている必要があります。
- 使用する指定された MST インスタンス ID も把握する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーションモードを開始します。
ステップ 3	spanning-tree mst instance-id priority priority 例： Device(config)# spanning-tree mst 0 priority 40960	デバイスプライオリティを設定します。 <ul style="list-style-type: none"> • <i>instance-id</i> には、単一のインスタンス、ハイフンで区切られた範囲のインスタンス、またはカンマで区切られた一連のインスタンスを指定できます。指定できる範囲は 0 ~ 4094 です。 • <i>priority</i> の範囲は 0 ~ 61440 で、4096 ずつ増加します。デフォルトは 32768 です。この値が低いほど、デバイスがルートスイッチとして選択される可能性が高くなります。

	コマンドまたはアクション	目的
		使用可能な値は、0、4096、8192、12288、16384、20480、24576、28672、32768、36864、40960、45056、49152、53248、57344、61440 です。これらは唯一の許容値です。
ステップ 4	end 例： Device(config-if) # end	特権 EXEC モードに戻ります。

(任意) Hello Time の設定

hello タイムはルートデバイスによって設定メッセージが生成されて送信される時間の間隔です。

Hello Time を設定するには、次の手順を実行します。

始める前に

MST が、デバイスで指定されて有効になっている必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	spanning-tree mst hello-time seconds 例： Device(config)# spanning-tree mst hello-time 4	すべての MST インスタンスについて、hello タイムを設定します。hello タイムはルートデバイスによって設定メッセージが生成されて送信される時間の間隔です。このメッセージは、デバイスが活動中であることを表します。 <i>seconds</i> に指定できる範囲は 1 ~ 10 です。デフォルトは 3 です。

	コマンドまたはアクション	目的
ステップ 4	end 例： Device(config)# end	特権 EXEC モードに戻ります。

転送遅延時間の設定

転送遅延時間を設定するには、次の手順を実行します。

始める前に

MST が、デバイスで指定されて有効になっている必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーションモードを開始します。
ステップ 3	spanning-tree mst forward-time seconds 例： Device(config)# spanning-tree mst forward-time 25	すべての MST インスタンスについて、転送時間を設定します。転送遅延時間は、スパニングツリー ラーニング ステートおよびリスニング ステートからフォワーディング ステートに移行するまでに、ポートが待機する秒数です。 <i>seconds</i> に指定できる範囲は 4 ~ 30 です。デフォルトは 20 です。
ステップ 4	end 例： Device(config)# end	特権 EXEC モードに戻ります。

最大エイジング タイムの設定

最大エイジング タイムを設定するには、次の手順を実行します。

(任意) 最大ホップ カウントの設定

始める前に

MST が、デバイスで指定されて有効になっている必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	spanning-tree mst max-age seconds 例： Device(config)# spanning-tree mst max-age 40	すべての MST インスタンスについて、最大経過時間を設定します。最大エージングタイムは、デバイスが再設定を試す前にスパンニングツリー設定メッセージを受信せずに待機する秒数です。 <i>seconds</i> に指定できる範囲は 6 ~ 40 です。デフォルトは 20 です。
ステップ 4	end 例： Device(config)# end	特権 EXEC モードに戻ります。

(任意) 最大ホップ カウントの設定

最大ホップ カウントを設定するには、次の手順を実行します。

始める前に

MST が、デバイスで指定されて有効になっている必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例：	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	Device# configure terminal	
ステップ 3	spanning-tree mst max-hops hop-count 例： Device(config)# spanning-tree mst max-hops 25	BPDUを廃棄してポート用に保持していた情報を期限切れにするまでの、リージョンでのホップ数を設定します。 <i>hop-count</i> に指定できる範囲は 1 ~ 255 です。デフォルト値は 20 です。
ステップ 4	end 例： Device(config)# end	特権 EXEC モードに戻ります。

(任意) 高速移行を保証するリンク タイプの指定

ポイントツーポイントリンクでポート間を接続し、ローカルポートがDPになると、RSTPは提案と合意のハンドシェイクを使用し、別のポートと高速移行をネゴシエーションし、ループがないトポロジを保証します。

デフォルトの場合、リンクタイプはインターフェイスのデュプレックスモードから制御されます。全二重ポートはポイントツーポイント接続、半二重ポートは共有接続と見なされます。MSTPを実行しているリモートデバイスの単一ポートに、半二重リンクを物理的にポイントツーポイントで接続した場合は、リンクタイプのデフォルト設定を無効にして、フォワーディング状態への高速移行をイネーブルにすることができます。

リンクタイプを指定して迅速な遷移を保証するには、次の手順を実行します。

始める前に

- MSTが、デバイスで指定されて有効になっている必要があります。
- 指定されたMSTインスタンスIDと使用されるインターフェイスも把握する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	interface interface-id 例： Device(config)# interface gigabitethernet 1/0/1	設定するインターフェイスを指定し、インターフェイス コンフィギュレーションモードを開始します。有効なインターフェイスには、物理ポート、VLAN、およびポート チャネル論理インターフェイスがあります。VLAN ID の範囲は 1 ~ 4094 です。指定できるポートチャネルの範囲は 1 ~ 48 です。
ステップ 4	spanning-tree link-type point-to-point 例： Device(config-if)# spanning-tree link-type point-to-point	ポートのリンク タイプがポイントツーポイントであることを指定します。
ステップ 5	end 例： Device(config-if)# end	特権 EXEC モードに戻ります。

(任意) ネイバー タイプの指定

トポロジには、先行標準に準拠したデバイスと IEEE 802.1s 標準準拠のデバイスの両方を加えることができます。デフォルトの場合、ポートは準規格デバイスを自動的に検出できますが、規格 BPDU および準規格 BPDU の両方を受信できます。デバイスとそのネイバーの間に不一致がある場合は、CIST だけがインターフェイスで動作します。

準規格 BPDU だけを送信するようにポートを設定できます。先行標準のフラグは、ポートが STP 互換モードにある場合でも、すべての **show** コマンドで表示されます。

ネイバータイプを指定するには、次の手順を実行します。

始める前に

MST が、デバイスで指定されて有効になっている必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーションモードを開始します。

	コマンドまたはアクション	目的
ステップ 3	interface interface-id 例： Device(config)# interface gigabitethernet 1/0/1	設定するインターフェイスを指定し、インターフェイス コンフィギュレーションモードを開始します。有効なインターフェイスには、物理ポートが含まれます。
ステップ 4	spanning-tree mst pre-standard 例： Device(config-if)# spanning-tree mst pre-standard	ポートが準規格 BPDU だけを送信できることを指定します。
ステップ 5	end 例： Device(config-if)# end	特権 EXEC モードに戻ります。

プロトコル移行プロセスの再開

この手順では、プロトコル移行プロセスを再開し、ネイバーデバイスとの再ネゴシエーションを強制します。また、デバイスを MST モードに戻します。これは、IEEE 802.1D BPDU の受信後にデバイスがそれらを受信しない場合に必要です。

デバイスでプロトコルの移行プロセスを再開する（隣接するデバイスで再ネゴシエーションを強制的に行う）手順については、これらの手順に従ってください。

始める前に

- MST が、デバイスで指定されて有効になっている必要があります。
- コマンドのインターフェイス バージョンを使用する場合は、使用する MST インターフェイスが分かっている必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	次のいずれかのコマンドを入力します。 • clear spanning-tree detected-protocols	デバイスが MSTP モードに戻り、プロトコルの移行プロセスが再開されます。

	コマンドまたはアクション	目的
	<ul style="list-style-type: none"> • clear spanning-tree detected-protocols interface interface-id 例 : <pre>Device# clear spanning-tree detected-protocols</pre> または <pre>Device# clear spanning-tree detected-protocols interface gigabitethernet 1/0/1</pre>	

次のタスク

この手順は、デバイスでさらにレガシー IEEE 802.1D コンフィギュレーション BPDU（プロトコルバージョンが 0 に設定された BPDU）を受信する場合に、繰り返しが必要なことがあります。

MSTP に関する追加情報

関連資料

関連項目	マニュアル タイトル
この章で使用するコマンドの完全な構文および使用方法の詳細。	<p><i>Command Reference (Catalyst 9600 Series Switches)</i> の「Layer 2/3 Commands」の項を参照してください</p> <p><i>Command Reference (Catalyst 9300 Series Switches)</i> の「Layer 2/3 Commands」の項を参照してください</p>

MSTP の機能の履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Everest 16.5.1a	複数のスパニングツリープロトコル	高速コンバージェンスのために RSTP を使用する MSTP では、複数の VLAN をグループ化して同じスパニングツリー インスタンスにマッピングすることが可能で、多くの VLAN をサポートするのに必要なスパニングツリー インスタンスの数を軽減できます。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> [英語] からアクセスします。



第 3 章

オプションのスパニングツリー機能の設定

- オプションのスパニングツリー機能について (65 ページ)
- オプションのスパニングツリー機能の設定方法 (77 ページ)
- スパニングツリー ステータスのモニタリング (88 ページ)
- オプションのスパニングツリー機能に関する追加情報 (88 ページ)
- オプションのスパニングツリー機能の機能履歴 (88 ページ)

オプションのスパニングツリー機能について

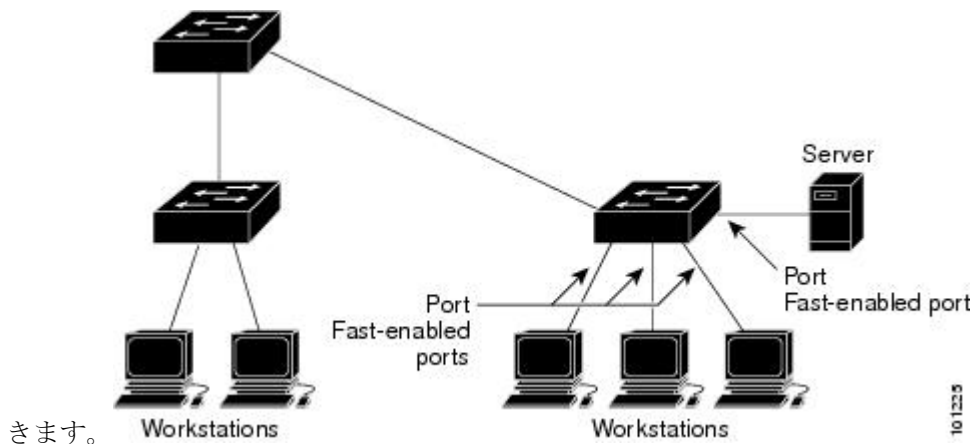
ここでは、オプションのスパニングツリー機能について説明します。

PortFast

PortFast 機能を使用すると、アクセスポートまたはトランクポートとして設定されているインターフェイスが、リスニング状態およびラーニング状態を経由せずに、ブロッキング状態から直接フォワーディング状態に移行します。

図 9: PortFast が有効なインターフェイス

1 台のワークステーションまたはサーバに接続されているインターフェイス上で PortFast を使用すると、スパニングツリーが収束するのを待たずにデバイスをすぐにネットワークに接続で



1台のワークステーションまたはサーバに接続されたインターフェイスがブリッジプロトコルデータユニット (BPDU) を受信しないようにする必要があります。スイッチを再起動すると、PortFast が有効に設定されているインターフェイスは通常のスパニングツリー ステータスの遷移をたどります。

インターフェイスまたはすべての非トランク ポートで有効にして、この機能を有効にできます。

ブリッジプロトコルデータユニットガード

ブリッジプロトコルデータユニット (BPDU) ガード機能はスイッチ上でグローバルにイネーブルにすることも、ポート単位でイネーブルにすることもできます。ただし、これらの動作は次の点で異なります。

PortFast 対応ポート、上でグローバルレベルで BPDU ガードをイネーブルにすると、スパニングツリーは、BPDU が受信されると、PortFast 動作 ステートのポートをシャットダウンします。有効な設定では、PortFast 対応ポートは BPDU を受信しません。PortFast 対応ポートが BPDU を受信した場合は、許可されていないデバイスの接続などの無効な設定が存在することを示しており、BPDU ガード機能によってポートは error-disabled ステートになります。この状態になると、スイッチは違反が発生したポート全体をシャットダウンします。

PortFast 機能、をイネーブルにせずにインターフェイスレベルでポート上の BPDU ガードをイネーブルにした場合、ポートが BPDU を受信すると、error-disabled ステートになります。

インターフェイスを手動で再び動作させなければならない場合、無効な設定を防ぐには、BPDU ガード機能が役に立ちます。サービスプロバイダー ネットワーク内でアクセス ポートがスパニングツリーに参加しないようにするには、BPDU ガード機能を使用します。

ブリッジプロトコルデータユニットフィルタリング

BPDU フィルタリング機能はスイッチ上でグローバルにイネーブルにすることも、インターフェイス単位でイネーブルにすることもできます。ただし、これらの動作は次の点で異なります。

PortFast 対応インターフェイスで、グローバルレベルで BPDU フィルタリングをイネーブルにすると、PortFast 動作状態にあるインターフェイスが BPDU を送受信しなくなります。ただし、リンクが確立してからスイッチが発信 BPDU のフィルタリングを開始するまでの間に、このインターフェイスから BPDU がいくつか送信されます。これらのインターフェイスに接続されたホストが BPDU を受信しないようにするには、スイッチ上で BPDU フィルタリングをグローバルにイネーブルにする必要があります。BPDU が、PortFast 対応インターフェイス、で受信された場合、インターフェイスは、PortFast 動作ステータス、を失い、BPDU フィルタリングはディセーブルになります。

PortFast 機能をイネーブルにせずに、インターフェイスで BPDU フィルタリングをイネーブルにすると、インターフェイスでの BPDU の送受信が防止されます。



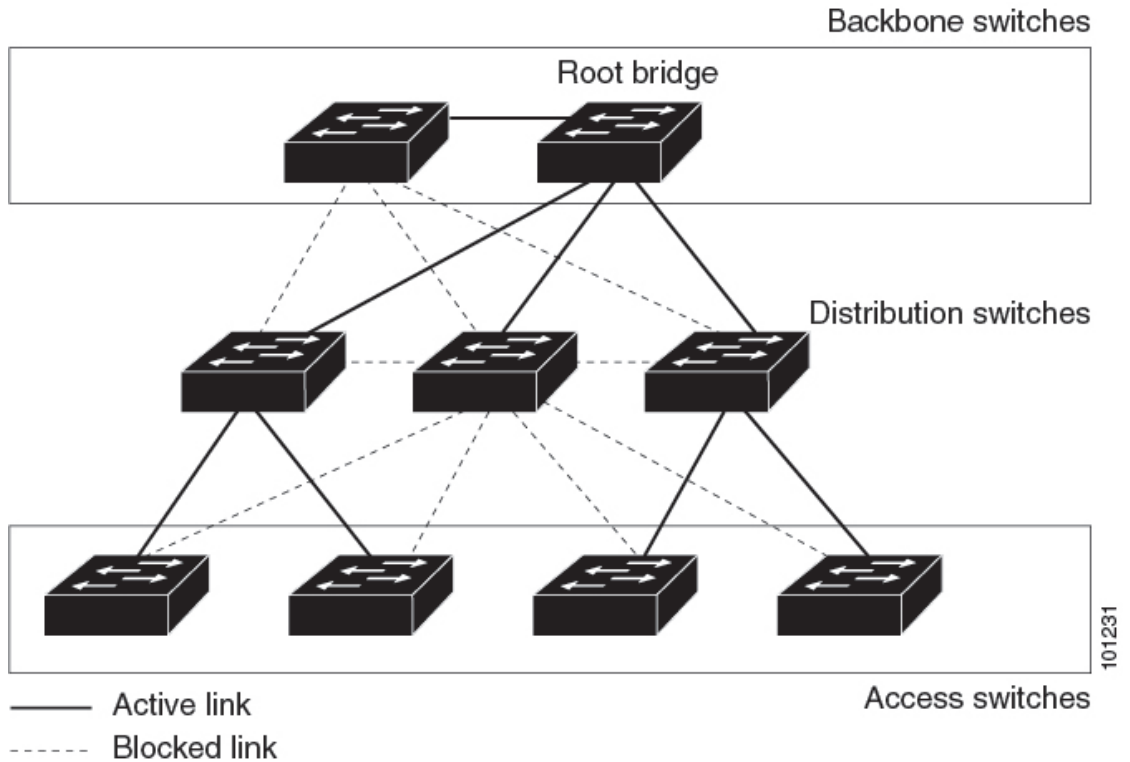
注意 BPDUフィルタリングを特定のインターフェイス上でイネーブルにすることは、そのインターフェイス上でスパニングツリーをディセーブルにすることと同じであり、スパニングツリーループが発生することがあります。

スイッチ全体または1つのインターフェイスでBPDUフィルタリング機能をイネーブルにできません。

UplinkFast

図 10: 階層型ネットワークのスイッチ

階層型ネットワークに配置されたスイッチは、バックボーンスイッチ、ディストリビューションスイッチ、およびアクセススイッチに分類できます。この複雑なネットワークには、ディストリビューションスイッチとアクセススイッチがあり、ループを防止するために、スパニングツリーがブロックする冗長リンクが少なくとも1つあります。



スイッチの接続が切断されると、スイッチはスパニングツリーが新しいルートポートを選択した時点で代替パスの使用を開始します。リンクやスイッチに障害が発生した場合、またはスパニングツリーがUplinkFastの有効化によって自動的に再設定された場合に、新しいルートポートを短時間で選択できます。ルートポートは、通常のスパニングツリー手順とは異なり、リスニングステートおよびラーニングステートを経由せず、ただちにフォワーディングステートに移行します。

スパニングツリーが新規ルートポートを再設定すると、他のインターフェイスはネットワークにマルチキャスト packets をフラッディングし、インターフェイス上で学習した各アドレスに packets を送信します。max-update-rate パラメータの値を小さくすることで、これらのマルチキャストトラフィックのバーストを制限できます（このパラメータはデフォルトで毎秒150 packets です）。ただし、0 を入力すると、ステーション学習フレームが生成されないため、接続切断後スパニングツリー トポロジがコンバージェンスする速度が遅くなります。



- (注) UplinkFast は、ネットワークのアクセスまたはエッジに位置する、ワイヤリングクローゼットのスイッチで非常に有効です。バックボーン デバイスには適していません。他のアプリケーションにこの機能を使用しても、有効とは限りません。

UplinkFast は、直接リンク障害発生後に高速コンバージェンスを行い、アップリンク グループを使用して、冗長レイヤ2リンク間でロードバランシングを実行します。アップリンク グループは、（VLAN ごとの）レイヤ2 インターフェイスの集合であり、いかなるときも、その中の1つのインターフェイスだけが転送を行います。つまり、アップリンク グループは、（転送を行う）ルートポートと、（セルフループを行うポートを除く）ブロックされたポートの集合で構成されます。アップリンク グループは、転送中のリンクで障害が起きた場合に代替パスを提供します。

図 11: 直接リンク障害が発生する前の UplinkFast の例

このトポロジにはリンク障害がありません。ルートスイッチであるスイッチ A は、リンク L1 を介してスイッチ B に、リンク L2 を介してスイッチ C に直接接続されています。スイッチ B に直接接続されているスイッチ C のレイヤ2 インターフェイスは、ブロッキング ステートです。

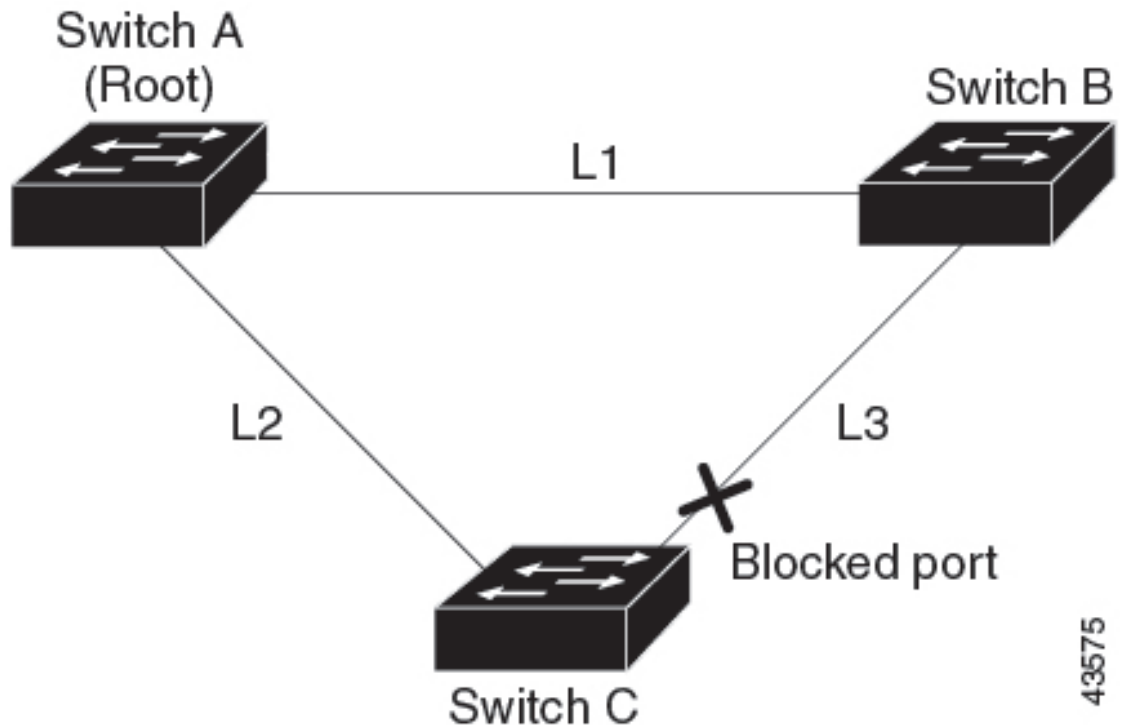
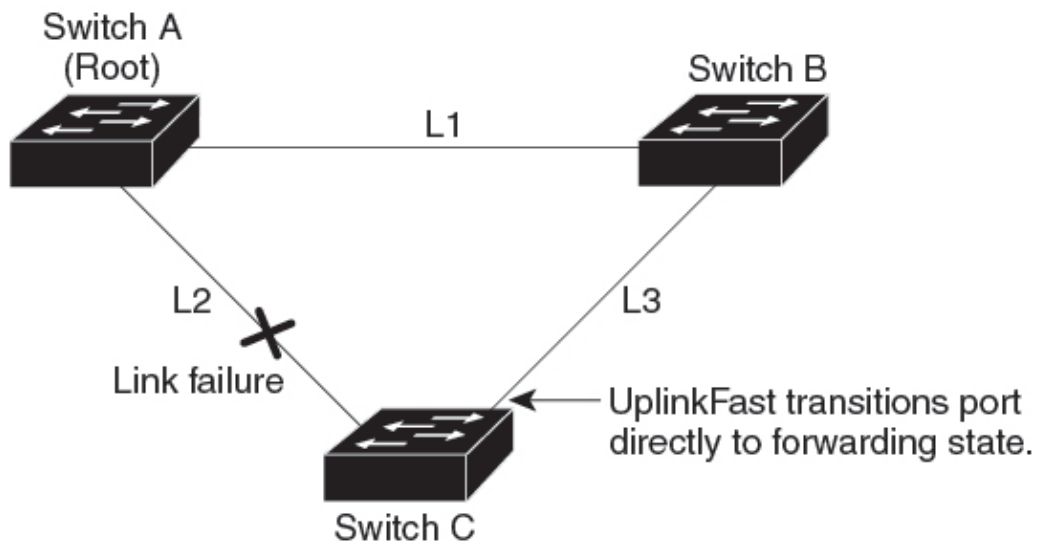


図 12: 直接リンク障害が発生したあとの UplinkFast の例

スイッチ C が、ルート ポートの現在のアクティブ リンクである L2 でリンク障害（直接リンク障害）を検出すると、UplinkFast がスイッチ C でブロックされていたインターフェイスのブロックを解除し、リスニング ステートおよびラーニング ステートを経由せずに、直接フォワーディング ステートに移行させます。この切り替えに必要な時間は、約 1 ～ 5 秒です。



クロススタック UplinkFast

クロススタック UplinkFast (CSUF) は、スイッチ スタック全体にスパニングツリー高速移行（通常のネットワーク状態の下では1秒未満の高速コンバージェンス）を提供します。高速移行の間は、スタック上の代替冗長リンクがフォワーディングステートになり、一時的なスパニングツリーループもバックボーンへの接続の損失も発生させません。一部の設定では、この機能により、冗長性と復元力を備えたネットワークが得られます。CSUF は UplinkFast 機能をイネーブルにすると、自動的にイネーブルになります。

CSUF で高速移行が得られない場合もあります。この場合は、通常のスパニングツリー移行が発生し、30 ～ 40 秒以内に完了します。詳細については、「関連項目」を参照してください。

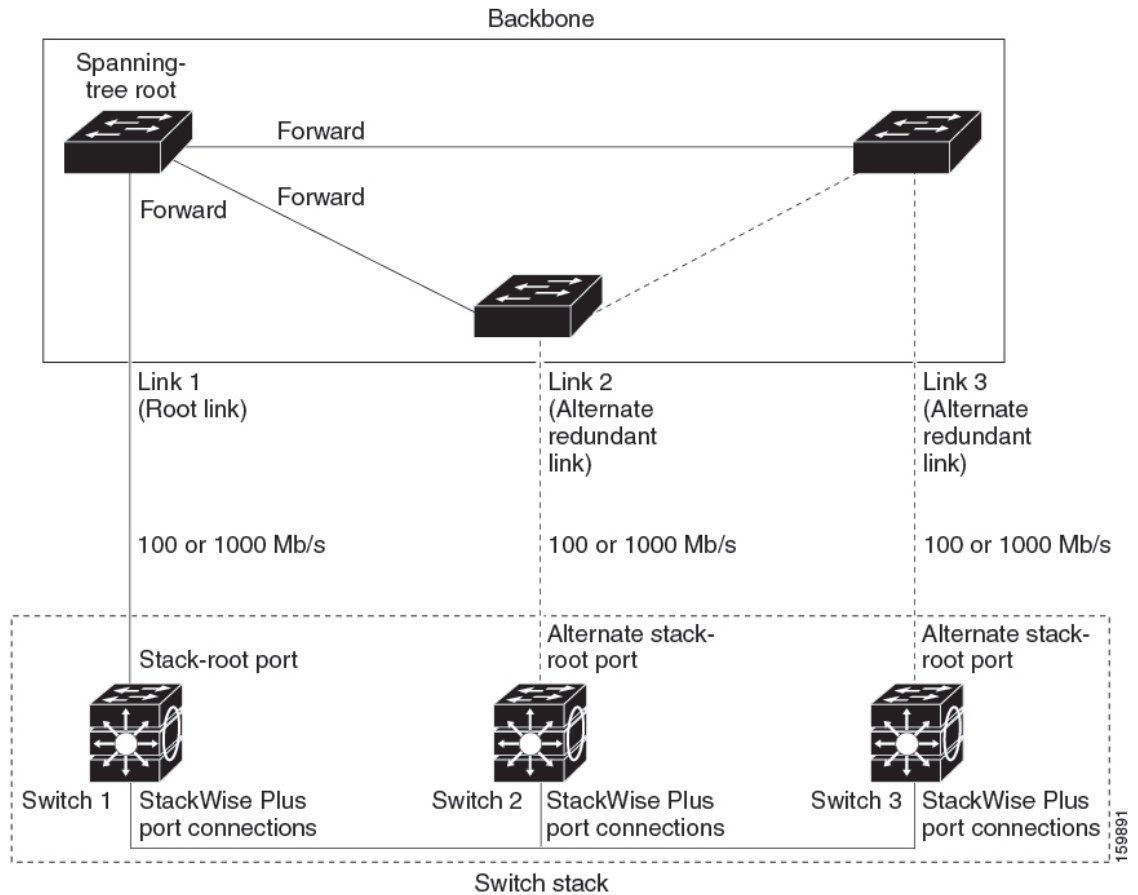
クロススタック UplinkFast の動作

クロススタック UplinkFast (CSUF) によって、ルートへのパスとしてスタック内で1つのリンクが確実に選択されます。

図 13: クロススタック UplinkFast トポロジ

スイッチ1のスタックルートポートは、スパニングツリーのルートへパスを提供しています。スイッチ2およびスイッチ3の代替スタックルートポートは、現在のスタックルートスイッチに障害が発生したか、またはそのスパニングツリールートへのリンクに障害が発生した場合に、スパニングツリールートへの代替パスを提供できます。

ルートリンクである Link 1 は、スパニングツリーフォワーディングステートになっていません。Link 2 と Link 3 は、スパニングツリーブロッキングステートになっている代替冗長リンクです。スイッチ1に障害が発生したか、そのスタックルートポートに障害が発生したか、または Link 1 に障害が発生した場合には、CSUF が、1秒未満でスイッチ2またはスイッチ3のいずれかにある代替スタックルートポートを選択して、それをフォワーディングステートにします。



特定のリンク損失またはスパニングツリーイベントが発生した場合（次のトピックを参照）、Fast Uplink Transition Protocol は、ネイバーリストを使用して、高速移行要求をスタックメンバーに送信します。

高速移行要求を送信するスイッチは、ルートポートとして選択されたポートをフォワーディングステートへ高速移行する必要があります。また、高速移行を実行するには、事前に各スタックから確認応答を取得しておく必要があります。

スタック内の各スイッチが、ルート、コスト、およびブリッジ ID を比較することにより、このスパニングツリーインスタンスのスタックルートとなるよりも送信スイッチの方がよりよい選択肢であるかどうかを判断します。スタックルートとして送信スイッチが最も良い選択である場合は、スタック内の各スイッチが確認応答を返します。それ以外の場合は、高速移行要求を送信します。この時点では、送信スイッチは、すべてのスタックスイッチから確認応答を受け取っていません。

すべてのスタックスイッチから確認応答を受け取ると、送信スイッチの Fast Uplink Transition Protocol は代替スタックルートポートをすぐにフォワーディングステートに移行させます。送信スイッチがすべてのスタックスイッチからの確認応答を取得しなかった場合、通常のスパニングツリー移行（ブロッキング、リスニング、ラーニング、およびフォワーディング）が行われ、スパニングツリートポロジが通常のレート（ $2 \times$ 転送遅延時間 + 最大エイジングタイム）で収束します。

Fast Uplink Transition Protocol は、VLAN ごとに実装されており、一度に 1 つのスパニングツリーインスタンスにしか影響しません。

高速コンバージェンスを発生させるイベント

CSUF 高速コンバージェンスは、ネットワークイベントまたはネットワーク障害に応じて、発生する場合もあれば発生しない場合もあります。

高速コンバージェンス（通常のネットワーク状態で 1 秒未満）は、次のような状況で発生します。

- スタック ルート ポート リンクに障害が発生した。
スタック内の 2 つのスイッチがルートへの代替パスを持つ場合、それらのスイッチの片方だけが高速移行を行います。
- スタック ルートをスパニングツリールートに接続するリンクに障害が発生し、回復した。
- ネットワークの再設定により、新しいスタック ルート スイッチが選択された。
- ネットワークの再設定により、現在のスタック ルート スイッチ上で新しいポートがスタック ルート ポートとして選択された。



(注) 複数のイベントが同時に発生すると、高速移行が行われなくなる場合もあります。たとえば、スタック メンバの電源がオフになり、それと同時にスタック ルートをスパニングツリー ルートに接続しているリンクが回復した場合、通常のスパニングツリーコンバージェンスが発生します。

通常のスパニングツリーコンバージェンス（30～40 秒）は、次のような状況で発生します。

- スタック ルート スイッチの電源がオフになったか、またはソフトウェアに障害が発生した。
- 電源がオフになっていたか、または障害が発生していたスタック ルート スイッチの電源が入った。
- スタック ルートになる可能性のある新しいスイッチがスタックに追加された。

BackboneFast

BackboneFast は、バックボーンのコアにおける間接障害を検出します。BackboneFast は、UplinkFast 機能を補完するテクノロジーです。UplinkFast は、アクセス スイッチに直接接続されたリンクの障害に対応します。BackboneFast は、最大エージングタイマーを最適化します。最大エージングタイマーによって、スイッチがインターフェイスで受信したプロトコル情報を保存しておく時間の長さが制御されます。スイッチが別のスイッチの指定ポートから下位BPDU

を受信した場合、BPDUは他のスイッチでルートまでのパスが失われた可能性を示すシグナルとなり、BackboneFastはルートまでの別のパスを見つけようとします。

スイッチのルートポートまたはブロックされたインターフェイスが、指定スイッチから下位BPDUを受け取ると、BackboneFastが開始します。下位BPDUは、ルートブリッジと指定スイッチの両方を宣言しているスイッチを識別します。スイッチが下位BPDUを受信した場合、そのスイッチが直接接続されていないリンク（間接リンク）で障害が発生したことを意味します（指定スイッチとルートスイッチ間の接続が切断されています）。スパニングツリーのルールに従い、スイッチは最大エージングタイム（デフォルトは20秒）の間、下位BPDUを無視します。

スイッチは、ルートスイッチへの代替パスの有無を判別します。下位BPDUがブロックインターフェイスに到達した場合、スイッチ上のルートポートおよび他のブロックインターフェイスがルートスイッチへの代替パスになります（セルフループポートはルートスイッチの代替パスとは見なされません）。下位BPDUがルートポートに到達した場合には、すべてのブロックインターフェイスがルートスイッチへの代替パスになります。下位BPDUがルートポートに到達し、しかもブロックインターフェイスがない場合、スイッチはルートスイッチへの接続が切断されたものと見なし、ルートポートの最大エージングタイムが経過するまで待ち、通常のスパンニングツリールールに従ってルートスイッチになります。

スイッチが代替パスでルートスイッチに到達できる場合、スイッチはその代替パスを使用して、Root Link Query (RLQ) 要求を送信します。スイッチは、スタックメンバーがルートスイッチへの代替ルートを持つかどうかを学習するために、すべての代替パスにRLQ要求を送信し、ネットワーク内およびスタック内の他のスイッチからのRLQ応答を待機します。スイッチは、すべての代替パスにRLQ要求を送信し、ネットワーク内の他のスイッチからのRLQ応答を待機します。

スタックメンバーが、ブロックインターフェイス上の非スタックメンバーからRLQ応答を受信し、その応答が他の非スタックスイッチ宛てのものであった場合、そのスタックメンバーは、スパニングツリーインターフェイスステートに関係なく、その応答パケットを転送します。

スタックメンバーが非スタックメンバーからRLQ応答を受信し、その応答がスタック宛てのものであった場合、そのスタックメンバーは、他のすべてのスタックメンバーがその応答を受信するようにその応答を転送します。

ルートへの代替パスがまだ存在していると判断したスイッチは、下位BPDUを受信したインターフェイスの最大エージングタイムが経過するまで待ちます。ルートスイッチへのすべての代替パスが、スイッチとルートスイッチ間の接続が切断されていることを示している場合、スイッチはRLQ応答を受信したインターフェイスの最大エージングタイムを満了させます。1つまたは複数の代替パスからルートスイッチへ引き続き接続できる場合、スイッチは下位BPDUを受信したすべてのインターフェイスを指定ポートにして、（ブロッキングステートになっていた場合）ブロッキングステートを解除し、リスニングステート、ラーニングステートを経てフォワーディングステートに移行させます。

図 14: 間接リンク障害が発生する前の BackboneFast の例

これは、リンク障害が発生していないトポロジ例です。ルートスイッチであるスイッチ A はリンク L1 を介してスイッチ B に、リンク L2 を介してスイッチ C に直接接続されています。

スイッチ B に直接接続されているスイッチ C のレイヤ 2 インターフェイスは、ブロッキングステートです。

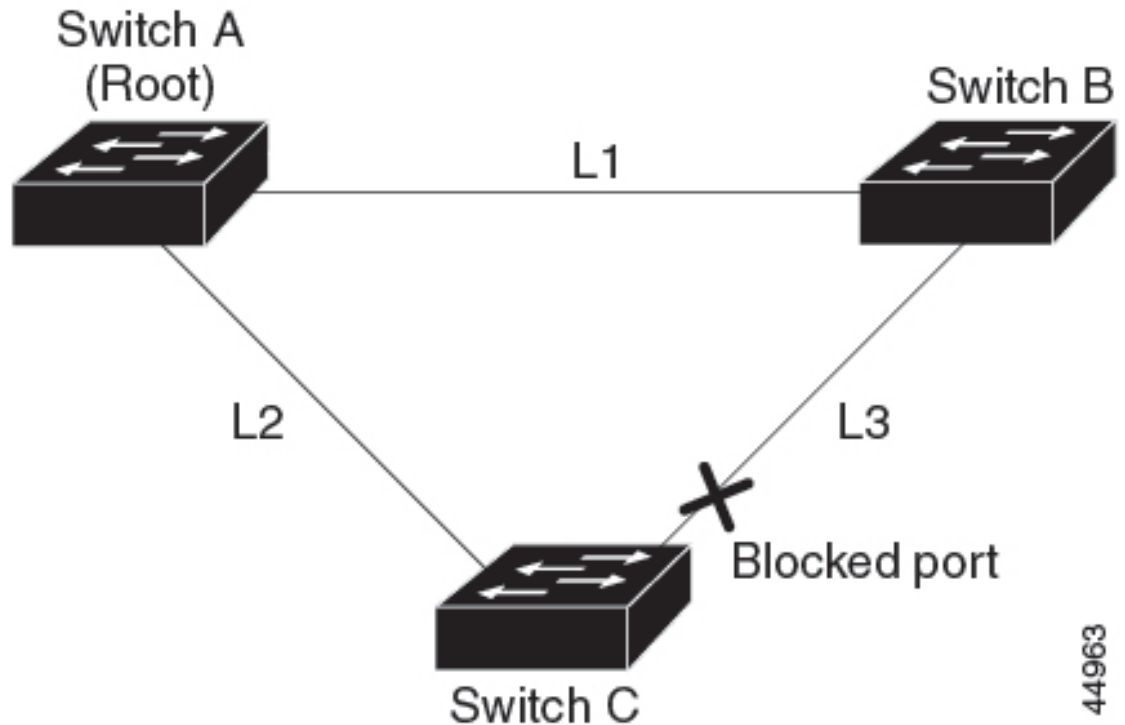
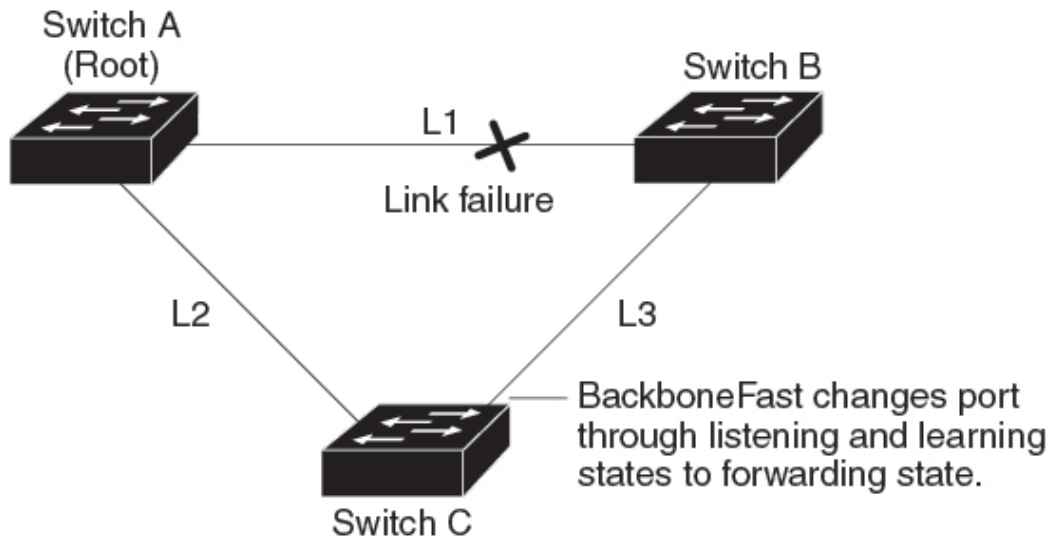


図 15: 間接リンク障害が発生したあとの *BackboneFast* の例

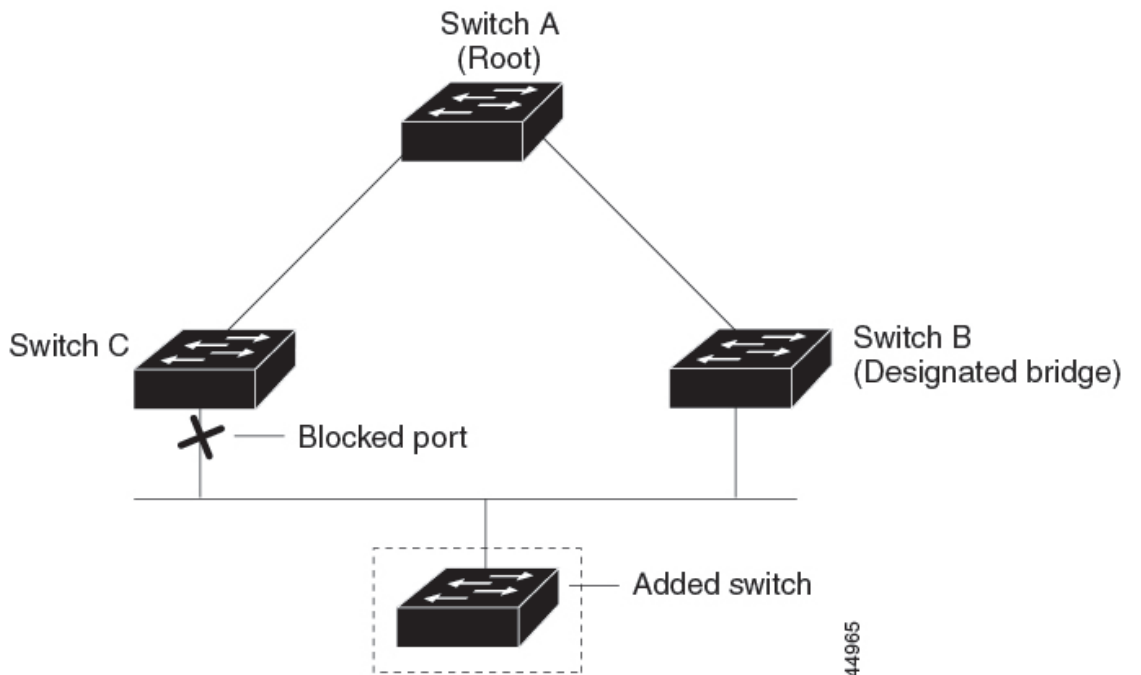
リンク L1 で障害が発生した場合、スイッチ C はリンク L1 に直接接続されていないので、この障害を検出できません。一方スイッチ B は、L1 によってルートスイッチに直接接続されているため障害を検出し、スイッチ B 自身をルートとして選定して、自らをルートとして特定した状態で BPDU をスイッチ C へ送信し始めます。スイッチ B から下位 BPDU を受信したスイッチ C は、間接障害が発生していると見なします。この時点で、*BackboneFast* は、スイッチ C のブロック インターフェイスを、インターフェイスの最大エージング タイムが満了するまで待たずに、ただちにリスニング ステートに移行させます。*BackboneFast* は、次に、スイッチ C のレイヤ 2 インターフェイスをフォワーディング ステートに移行させ、スイッチ B からスイッチ A へのパスを提供します。ルートスイッチの選択には約 30 秒必要です。これは転送遅延時間がデフォルトの 15 秒に設定されていればその倍の時間です。*BackboneFast* がリンク L1 で発生した障害に応じてトポロジを再設定します。



44964

図 16: メディア共有型トポロジにおけるスイッチの追加

新しいスイッチがメディア共有型トポロジに組み込まれた場合、認識された指定スイッチ（スイッチ B）から下位 BPDU が届いていないので、BackboneFast はアクティブになりません。新しいスイッチは、自身がルートスイッチであることを伝える下位 BPDU の送信を開始します。ただし、他のスイッチはこれらの下位 BPDU を無視し、新しいスイッチはスイッチ B がルートスイッチであるスイッチ A への指定スイッチであることを学習します。



44965

EtherChannel ガード

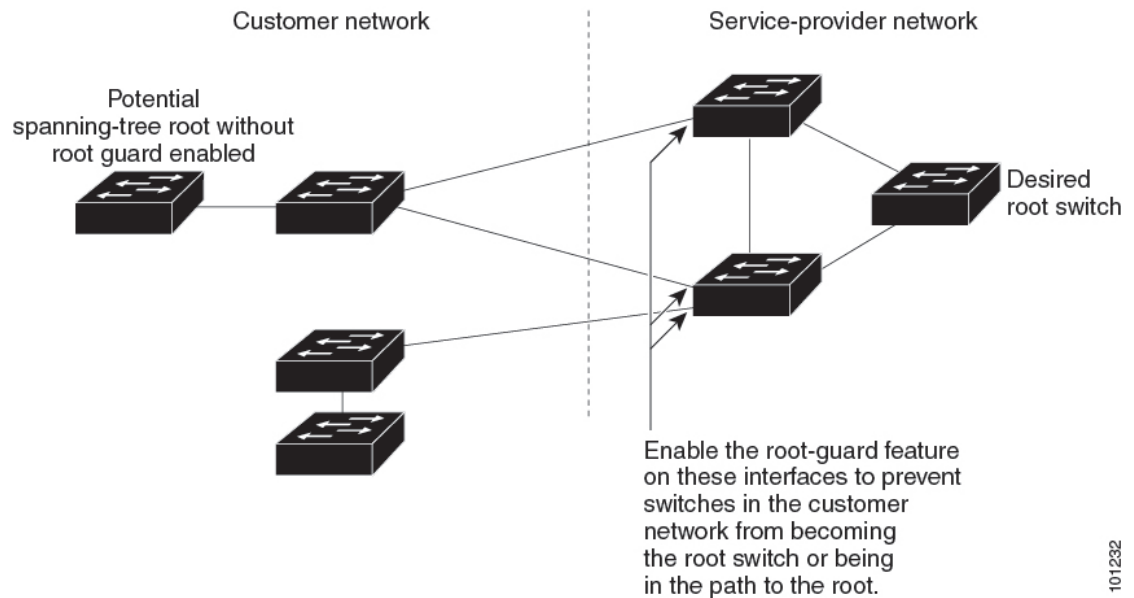
EtherChannel ガードを使用すると、スイッチと接続したデバイス間での EtherChannel の設定の矛盾を検出できます。スイッチ インターフェイスは EtherChannel として設定されているものの、もう一方のデバイスのインターフェイスではその設定が行われていない場合、設定の矛盾が発生します。また、EtherChannel の両端でチャンネルのパラメータが異なる場合にも、設定の矛盾が発生します。

スイッチが、他のデバイス上で設定の矛盾を検出した場合、EtherChannel ガードは、スイッチのインターフェイスを errdisable ステートにし、エラー メッセージを表示します。

ルート ガード

図 17: サービス プロバイダー ネットワークのルート ガード

サービス プロバイダー (SP) のレイヤ 2 ネットワークには、SP 以外が所有するスイッチへの接続が多く含まれている場合があります。このようなトポロジでは、スパニングツリーが再構成され、カスタマー スイッチをルート スイッチとして選択する可能性があります。この状況を防ぐには、カスタマー ネットワーク内のスイッチに接続する SP スイッチ インターフェイス上でルートガード機能を有効に設定します。スパニングツリーの計算によってカスタマー ネットワーク内のインターフェイスがルートポートとして選択されると、ルートガードがそのインターフェイスを root-inconsistent (ブロッキング) ステートにして、カスタマーのスイッチがルート スイッチにならないようにするか、ルートへのパスに組み込まないようにします。



SP ネットワーク外のスイッチがルート スイッチになると、インターフェイスがブロックされ (root-inconsistent ステートになり)、スパニングツリーが新しいルート スイッチを選択します。カスタマーのスイッチがルート スイッチになることはありません。ルートへのパスに組み込まれることもありません。

101232

スイッチが MST モードで動作している場合、ループガードが強制的にそのインターフェイスを指定ポートにします。また、境界ポートがループガードによって Internal Spanning-Tree (IST) インスタンスでブロックされている場合にも、このインターフェイスはすべての MST インスタンスでもブロックされます。境界ポートは、指定スイッチが IEEE 802.1D スイッチまたは異なる MST リージョン設定を持つスイッチのいずれかである LAN に接続されるインターフェイスです。

1つのインターフェイス上でループガードをイネーブルにすると、そのインターフェイスが所属するすべての VLAN にループガードが適用されます。VLAN は、MST インスタンスに対してグループ化された後、マッピングされます。



注意 ループガード機能を誤って使用すると、接続が切断されることがあります。

ループガード

ループガードを使用すると、代替ポートまたはルートポートが、単一方向リンクの原因となる障害によって指定ポートになることを防ぎます。この機能は、スイッチドネットワーク全体でイネーブルにした場合に最も効果があります。ループガードによって、代替ポートおよびルートポートが指定ポートになることが防止され、スパニングツリーがルートポートまたは代替ポートで BPDU を送信することはありません。

スイッチが PVST+ または Rapid PVST+ モードで動作している場合、ループガードによって、代替ポートおよびルートポートが指定ポートになることが防止され、スパニングツリーがルートポートまたは代替ポートで BPDU を送信することはありません。

スイッチが MST モードで動作しているとき、ループガードによってすべての MST インスタンスでインターフェイスがブロックされている場合でのみ、非境界ポートで BPDU を送信しません。境界ポートでは、ループガードがすべての MST インスタンスでインターフェイスをブロックします。

オプションのスパニングツリー機能の設定方法

ここでは、オプションのスパニングツリー機能の設定について説明します。

(任意) PortFast のイネーブル化

PortFast 機能がイネーブルに設定されているインターフェイスは、標準の転送遅延時間の経過を待たずに、すぐにスパニングツリー フォワーディング ステートに移行されます。

音声 VLAN 機能をイネーブルにすると、PortFast 機能が自動的にイネーブルになります。音声 VLAN をディセーブルにしても、PortFast 機能は自動的にディセーブルになりません。

スイッチで PVST+、Rapid PVST+、または MSTP が稼働している場合、この機能をイネーブルにできます。



注意 PortFast を使用するのには、1つのエンドステーションがアクセスポートまたはトランクポートに接続されている場合に限定されます。スイッチまたはハブに接続するインターフェイス上でこの機能をイネーブルにすると、Spanningツリーがネットワークループを検出または阻止できなくなり、その結果、ブロードキャストストームおよびアドレスラーニングの障害が起きる可能性があります。

PortFast を有効にするには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーションモードを開始します。
ステップ 3	interface interface-id 例： Device(config)# interface gigabitethernet 1/0/2	設定するインターフェイスを指定し、インターフェイス コンフィギュレーションモードを開始します。
ステップ 4	spanning-tree portfast [trunk] 例： Device(config-if)# spanning-tree portfast trunk	単一ワークステーションまたはサーバーに接続されたアクセスポート上で PortFast をイネーブルにします。 trunk キーワードを指定すると、トランクポート上で PortFast をイネーブルにできます。

	コマンドまたはアクション	目的
		<p>(注)</p> <p>トランク ポートで PortFast をイネーブルにするには、spanning-tree portfast trunk インターフェイス コンフィギュレーション コマンドを使用する必要があります。spanning-tree portfast コマンドは、トランクポート上では機能しません。</p> <p>トランク ポート上で PortFast をイネーブルにする場合は、事前に、トランク ポートとワークステーションまたはサーバーの間にループがないことを確認してください。</p> <p>デフォルトでは、PortFast はすべてのインターフェイスでディセーブルです。</p>
ステップ 5	<p>end</p> <p>例 :</p> <pre>Device(config-if) # end</pre>	特権 EXEC モードに戻ります。

次のタスク

spanning-tree portfast default グローバル コンフィギュレーション コマンドを使用すると、すべての非トランクポート上で PortFast 機能をグローバルにイネーブルにできます。

BPDU ガードのイネーブル化

スイッチで PVST+、Rapid PVST+、または MSTP が稼働している場合、BPDU ガード機能をイネーブルにできます。



注意 PortFast は、エンドステーションに接続するポートのみに設定します。それ以外に設定すると、予期しないトポロジループが原因でデータのパケットループが発生し、スイッチおよびネットワークの動作が妨げられることがあります。

この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	interface interface-id 例： Device(config)# interface gigabitethernet 1/0/2	エンドステーションに接続するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	spanning-tree portfast bpduguard default 例： Device(config-if)# spanning-tree portfast bpduguard default	BPDU ガードをイネーブルにします。
ステップ 5	spanning-tree portfast 例： Device(config-if)# spanning-tree portfast	PortFast 機能をイネーブルにします。
ステップ 6	end 例： Device(config-if)# end	特権 EXEC モードに戻ります。

次のタスク

ポートをシャットダウンしないようにするには、**errdisable detect cause bpduguard shutdown vlan** グローバルコンフィギュレーションコマンドを使用して、違反が発生したポート上の原因となっている VLAN だけをシャットダウンします。

PortFast 機能をイネーブルにしなくても、**spanning-tree bpduguard enable** インターフェイス コンフィギュレーション コマンドを使用して、任意のポートで BPDU ガードをイネーブルにすることもできます。BPDU を受信したポートは、**errdisable** ステートになります。

BPDU フィルタリングのイネーブル化

をイネーブルにしなくても、**spanning-tree bpdupfilter enable** インターフェイス コンフィギュレーション コマンドを使用して、任意のインターフェイスで BPDU フィルタリングをイネー

ブルにすることもできます。このコマンドを実行すると、インターフェイスはBPDUを送受信できなくなります。



注意 BPDUフィルタリングを特定のインターフェイス上でイネーブルにすることは、そのインターフェイス上でスパニングツリーをディセーブルにすることと同じであり、スパニングツリーループが発生することがあります。

スイッチでPVST+、Rapid PVST+、またはMSTPが稼働している場合、BPDUフィルタリング機能をイネーブルにできます。



注意 は、エンドステーションに接続するインターフェイスのみに設定します。それ以外に設定すると、予期しないトポジループが原因でデータのパケットループが発生し、スイッチおよびネットワークの動作が妨げられることがあります。

この手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーションモードを開始します。
ステップ 3	spanning-tree portfast bpdupfilter default 例： Device (config)# spanning-tree portfast bpdupfilter default	BPDU フィルタリングをグローバルにイネーブルにします。 BPDU フィルタリングは、デフォルトではディセーブルに設定されています。
ステップ 4	interface interface-id 例： Device (config)# interface gigabitethernet 1/0/2	エンドステーションに接続するインターフェイスを指定し、インターフェイス コンフィギュレーションモードを開始します。
ステップ 5	spanning-tree portfast 例： Device (config-if)# spanning-tree portfast	指定したインターフェイスで PortFast 機能をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 6	end 例： Device(config-if)# end	特権 EXEC モードに戻ります。

(任意) 冗長リンク用 UplinkFast のイネーブル化



- (注) UplinkFast をイネーブルにすると、スイッチまたはスイッチスタックのすべての VLAN に影響します。個々の VLAN について UplinkFast を設定することはできません。

Rapid PVST+ または MSTP に対して UplinkFast または Cross-Stack UplinkFast (CSUF) 機能を設定できますが、この機能は、スパニングツリーのモードを PVST+ に変更するまではディセーブル (非アクティブ) になったままです。

UplinkFast および CSUF をイネーブルにするには、次の手順に従います。

始める前に

スイッチプライオリティが設定されている VLAN 上で UplinkFast をイネーブルにすることはできません。スイッチプライオリティが設定されている VLAN 上で UplinkFast をイネーブルにする場合は、最初に **no spanning-tree vlan *vlan-id* priority** グローバル コンフィギュレーション コマンドを使用することによって、VLAN のスイッチプライオリティをデフォルト値に戻す必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します (要求された場合)。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	spanning-tree uplinkfast [max-update-rate <i>pkts-per-second</i>] 例： Device(config)# spanning-tree uplinkfast max-update-rate 200	UplinkFast をイネーブルにします。 (任意) <i>pkts-per-second</i> に指定できる範囲は毎秒 0 ~ 32000 パケットです。デフォルト値は 150 です。 0 を入力すると、ステーション学習フレームが生成されないため、接続切断後

	コマンドまたはアクション	目的
		スパニングツリー トポロジがコンバージェンスする速度が遅くなります。 このコマンドを入力すると、すべての非スタック ポート インターフェイス上で CSUF もイネーブルになります。
ステップ 4	end 例 : Device(config)# end	特権 EXEC モードに戻ります。

UplinkFast をイネーブルにすると、すべての VLAN のスイッチプライオリティは 49152 に設定されます。UplinkFast をイネーブルにする場合、または UplinkFast がすでにイネーブルに設定されている場合に、パス コストを 3000 未満の値に変更すると、すべてのインターフェイスおよび VLAN トランクのパス コストが 3000 だけ増加します (パス コストを 3000 以上の値に変更した場合、パス コストは変更されません)。スイッチプライオリティおよびパス コストを変更すると、スイッチがルートスイッチになる可能性が低くなります。

デフォルト値を変更していない場合、UplinkFast をディセーブルにすると、すべての VLAN のスイッチプライオリティとすべてのインターフェイスのパス コストがデフォルト値に設定されます。

次の手順に従って UplinkFast 機能をイネーブルにすると、CSUF は非スタック ポート インターフェイスで自動的にグローバルにイネーブルになります。

(任意) UplinkFast のディセーブル化

UplinkFast および Cross-Stack UplinkFast (SUF) をディセーブルにするには、次の手順に従います。

始める前に

UplinkFast を有効にする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します (要求された場合)。
ステップ 2	configure terminal 例 : Device# configure terminal	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	no spanning-tree uplinkfast 例： Device(config)# no spanning-tree uplinkfast	スイッチおよびそのスイッチのすべての VLAN で UplinkFast および CSUF をディセーブルにします。
ステップ 4	end 例： Device(config)# end	特権 EXEC モードに戻ります。

デフォルト値を変更していない場合、UplinkFast をディセーブルにすると、すべての VLAN のスイッチプライオリティとすべてのインターフェイスのパス コストがデフォルト値に設定されます。

次の手順に従って UplinkFast 機能をディセーブルにすると、CSUF は非スタック ポート インターフェイスで自動的にグローバルにディセーブルになります。

(任意) BackboneFast のイネーブル化

BackboneFast をイネーブルにすると、間接リンク障害を検出し、スパニングツリーの再構成をより早く開始できます。

Rapid PVST+ または MSTP に対して BackboneFast 機能を設定できます。ただし、スパニングツリーモードを PVST+ に変更するまで、この機能はディセーブル (非アクティブ) のままです。

スイッチ上で BackboneFast をイネーブルにするには、次の手順に従います。

始める前に

BackboneFast を使用する場合は、ネットワーク上のすべてのスイッチでイネーブルする必要があります。BackboneFast は、トークンリング VLAN ではサポートされません。この機能は他社製スイッチでの使用にサポートされています。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します (要求された場合)。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	spanning-tree backbonefast 例： Device(config)# spanning-tree backbonefast	BackboneFast をイネーブルにします。
ステップ 4	end 例： Device(config)# end	特権 EXEC モードに戻ります。

(任意) EtherChannel ガードのイネーブル化

デバイスで PVST+、Rapid PVST+、または MSTP が稼働している場合、EtherChannel の設定の矛盾を検出する EtherChannel ガード機能をイネーブルにできます。

デバイスで EtherChannel ガードをイネーブルにするには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	spanning-tree etherchannel guard misconfig 例： Device(config)# spanning-tree etherchannel guard misconfig	EtherChannel ガードをイネーブルにします。
ステップ 4	end 例： Device(config)# end	特権 EXEC モードに戻ります。

次のタスク

show interfaces status err-disabled 特権 EXEC コマンドを使用することで、EtherChannel の設定矛盾が原因でディセーブルになっているデバイスポートを表示できます。リモートデバイス上では、特権 EXEC モードで **show etherchannel summary** コマンドを使用して、EtherChannel の設定を確認できます。

設定を修正した後、誤って設定していたポートチャネルインターフェイス上で、**shutdown** および **no shutdown** インターフェイス コンフィギュレーション コマンドを入力してください。

(任意) ルートガードのイネーブル化

1つのインターフェイス上でルートガードをイネーブルにすると、そのインターフェイスが所属するすべてのVLANにルートガードが適用されます。UplinkFast機能が使用するインターフェイスで、ルートガードをイネーブルにしないでください。UplinkFastを使用すると、障害発生時に（ブロック状態の）バックアップインターフェイスがルートポートになります。ただし、同時にルートガードもイネーブルになっていた場合は、UplinkFast機能が使用するすべてのバックアップインターフェイスが **root-inconsistent**（ブロック）状態になり、フォワーディング状態に移行できなくなります。



(注) ルートガードとループガードの両方を同時にイネーブルにすることはできません。

スイッチでPVST+、Rapid PVST+、またはMSTPが稼働している場合、この機能をイネーブルにできます。

スイッチ上でルートガードをイネーブルにするには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	interface interface-id 例： Device(config)# interface gigabitethernet 1/0/2	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	spanning-tree guard root 例： Device(config-if)# spanning-tree guard root	インターフェイス上でルートガードをイネーブルにします。 デフォルトでは、ルートガードはすべてのインターフェイスでディセーブルです。

	コマンドまたはアクション	目的
ステップ 5	end 例： Device(config-if)# end	特権 EXEC モードに戻ります。

(任意) ループガードのイネーブル化

ループガードを使用すると、代替ポートまたはルートポートが、単一方向リンクの原因となる障害によって指定ポートになることを防ぎます。この機能は、スイッチドネットワーク全体に設定した場合に最も効果があります。ループガードは、スパニングツリーがポイントツーポイントと見なすインターフェイス上でのみ動作します。



(注) ループガードとルートガードの両方を同時にイネーブルにすることはできません。

デバイスで PVST+、Rapid PVST+、または MSTP が稼働している場合、この機能をイネーブルにできません。

デバイスでループガードをイネーブルにするには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	次のいずれかのコマンドを入力します。 • show spanning-tree active • show spanning-tree mst 例： Device# show spanning-tree active または Device# show spanning-tree mst	どのインターフェイスが代替ポートまたはルートポートであるかを確認します。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーションモードを開始します。
ステップ 3	spanning-tree loopguard default 例： Device(config)# spanning-tree loopguard default	ループガードをイネーブルにします。 ループガードは、デフォルトではディセーブルに設定されています。
ステップ 4	end 例：	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
	Device (config) # end	

スパニングツリーステータスのモニタリング

表 9: スパニングツリーステータスをモニタリングするコマンド

コマンド	目的
show spanning-tree active	アクティブ インターフェイスに関するスパニングツリーを表示します。
show spanning-tree detail	インターフェイス情報の詳細サマリーを表示します。
show spanning-tree interface <i>interface-id</i>	指定したインターフェイスのスパニングツリー情報を表示します。
show spanning-tree mst interface <i>interface-id</i>	指定インターフェイスの MST 情報を表示します。
show spanning-tree summary [totals]	インターフェイス ステートのサマリーを表示します。マスタリングツリー ステート セクションのすべての行を表示します。
show spanning-tree mst interface <i>interface-id</i> portfast	指定したインターフェイスのスパニングツリー portfast 情報を表示します。

オプションのスパニング ツリー機能に関する追加情報

関連資料

関連項目	マニュアル タイトル
この章で使用するコマンドの完全な構文および使用方法の詳細。	<i>Command Reference (Catalyst 9300 Series Switches)</i>

オプションのスパニングツリー機能の機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Everest 16.5.1a	オプションのスパニングツリープロトコル	STP のオプション機能は、ループの防止を強化し、ユーザーの設定ミスをなくし、プロトコルパラメータに関する制御力を高めます。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> [英語] からアクセスします。



第 4 章

EtherChannel の設定

- [EtherChannel の制約事項 \(91 ページ\)](#)
- [EtherChannel について \(91 ページ\)](#)
- [EtherChannel の設定方法 \(105 ページ\)](#)
- [EtherChannel、ポート集約プロトコル、および Link Aggregation Control Protocol の状態のモニタリング \(122 ページ\)](#)
- [EtherChannel の設定例 \(123 ページ\)](#)
- [EtherChannels の追加リファレンス \(126 ページ\)](#)
- [EtherChannel の機能履歴 \(126 ページ\)](#)

EtherChannel の制約事項

次に、EtherChannels の制約事項を示します。

- EtherChannel のすべてのポートは同じ VLAN に割り当てるか、またはトランクポートとして設定する必要があります。
- LACP 1:1 冗長性機能は、ポート チャネル インターフェイスでのみサポートされます。

EtherChannel について

ここでは、EtherChannel と、EtherChannel を設定するためのさまざまなモードについて説明します。

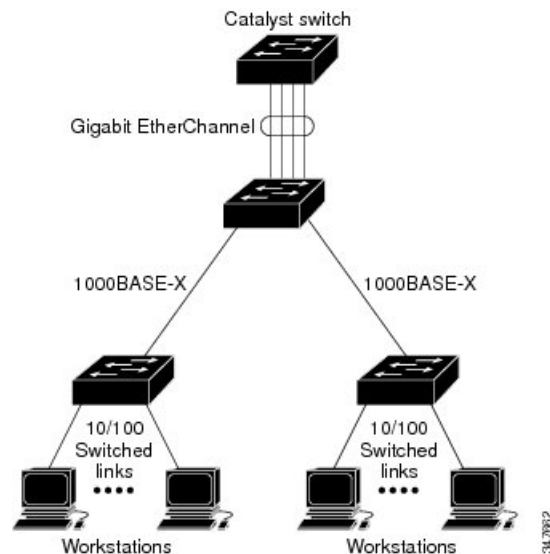
EtherChannel の概要

EtherChannel は、スイッチ、ルータ、およびサーバ間にフォールトトレラントな高速リンクを提供します。EtherChannel を使用して、ワイヤリングクローゼットとデータセンター間の帯域幅を増やすことができます。さらに、ボトルネックが発生しやすいネットワーク上のあらゆる場所に EtherChannel を配置できます。EtherChannel は、他のリンクに負荷を再分散させること

によって、リンク切断から自動的に回復します。リンク障害が発生した場合、EtherChannel は自動的に障害リンクからチャンネル内の他のリンクにトラフィックをリダイレクトします。

EtherChannel は、単一の論理リンクにバンドルする個別のイーサネットリンクで構成されます。

図 18: 一般的な EtherChannel 構成

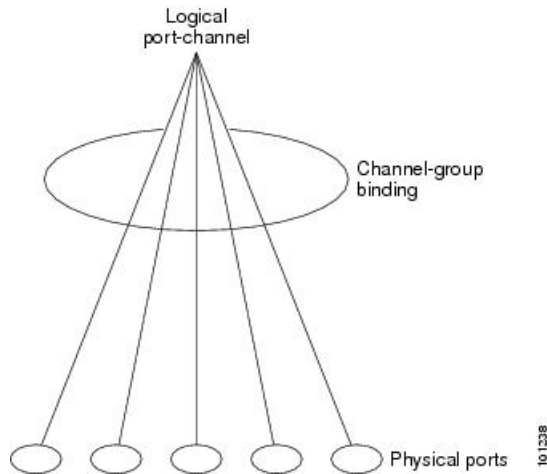


各 EtherChannel は、互換性のある設定のイーサネットポートを 8 つまで使用して構成できます。

チャンネルグループおよびポートチャンネルインターフェイス

EtherChannel は、チャンネルグループとポートチャンネルインターフェイスから構成されます。チャンネルグループはポートチャンネルインターフェイスに物理ポートをバインドします。ポートチャンネルインターフェイスに適用した設定変更は、チャンネルグループにまとめてバインドされるすべての物理ポートに適用されます。

Figure 19: 物理ポート、チャンネルグループおよびポートチャンネル インターフェイスの関係



channel-group コマンドは、物理ポートおよびポートチャンネル インターフェイスをまとめてバインドします。各 EtherChannel には 1 ~ 128 までの番号が付いたポートチャンネル論理インターフェイスがあります。ポートチャンネル インターフェイス番号は、**channel-group** インターフェイス コンフィギュレーション コマンドで指定した番号に対応しています。

- レイヤ 2 ポートの場合は、**channel-group** インターフェイス コンフィギュレーション コマンドを使用して、ポートチャンネル インターフェイスを動的に作成します。

また、**interface port-channel port-channel-number** グローバル コンフィギュレーション コマンドを使用して、ポートチャンネル論理インターフェイスを手動で作成することもできます。ただし、その場合、論理インターフェイスを物理ポートにバインドするには、

channel-group channel-group-number コマンドを使用する必要があります。

channel-group-number は **port-channel-number** と同じ値に設定することも、違う値を使用することもできます。新しい番号を使用した場合、**channel-group** コマンドは動的に新しいポートチャンネルを作成します。

- レイヤ 3 ポートの場合は、**interface port-channel** グローバル コンフィギュレーション コマンド、およびそのあとに **no switchport** インターフェイス コンフィギュレーション コマンドを使用して、論理インターフェイスを手動で作成する必要があります。その後、**channel-group** インターフェイス コンフィギュレーション コマンドを使用して、手動で EtherChannel にインターフェイスを割り当てます。
- レイヤ 3 ポートでレイヤ 3 インターフェイスとしてインターフェイスを設定するには、**no switchport** インターフェイスコマンドを使用した上で **channel-group** インターフェイス コンフィギュレーション コマンドを使用して動的にポートチャンネル インターフェイスを作成します。

Port Aggregation Protocol; ポート集約プロトコル

ポート集約プロトコル (PAgP) はシスコ独自のプロトコルで、Cisco デバイスおよび PAgP をサポートするベンダーによってライセンス供与されたデバイスでのみ稼働します。PAgP を使

用すると、イーサネット ポート間で PAgP パケットを交換することにより、EtherChannel を自動的に作成できます。PAgP はクロススタック EtherChannel でイネーブル化できます。

スイッチまたはスイッチ スタックは PAgP を使用することによって、PAgP をサポートできるパートナーの識別情報、および各ポートの機能を学習します。次に、設定が類似している（スタック内の単一デバイス上の）ポートを、単一の論理リンク（チャンネルまたは集約ポート）に動的にグループ化します。設定が類似しているポートをグループ化する場合の基準は、ハードウェア、管理、およびポート パラメータ制約です。たとえば、PAgP は速度、デュプレックスモード、ネイティブ VLAN、VLAN 範囲、トランッキング ステータス、およびトランッキング タイプが同じポートをグループとしてまとめます。リンクを EtherChannel にグループ化した後で、PAgP は単一デバイスポートとして、スパニングツリーにそのグループを追加します。

ポート集約プロトコル モード

PAgP モードは、PAgP ネゴシエーションを開始する PAgP パケットをポートが送信できるか、または受信した PAgP パケットに応答できるかを指定します。

Table 10: EtherChannel PAgP モード

モード	説明
auto	ポートをパッシブ ネゴシエーション ステートにします。この場合、ポートは受信する PAgP パケットに応答しますが、PAgP パケット ネゴシエーションを開始することはありません。これにより、PAgP パケットの送信は最小限に抑えられます。
desirable	ポートをアクティブ ネゴシエーション ステートにします。この場合、ポートは PAgP パケットを送信することによって、相手ポートとのネゴシエーションを開始します。

スイッチポートは、**auto** モードまたは **desirable** モードに設定された相手ポートとだけ PAgP パケットを交換します。**on** モードに設定されたポートは、PAgP パケットを交換しません。

auto モードおよび **desirable** モードはともに、相手ポートとネゴシエーションして、ポート速度などの条件に基づいて（レイヤ 2 EtherChannel の場合は、トランクステートおよび VLAN 番号などの基準に基づいて）、ポートで EtherChannel を形成できるようにします。

PAgP モードが異なっても、モード間で互換性がある限り、ポートは EtherChannel を形成できます。次に例を示します。

- **desirable** モードのポートは、**desirable** または **auto** モードの別のポートと EtherChannel を形成できます。
- **auto** モードのポートは、**desirable** モードの別のポートと EtherChannel を形成できます。

両ポートとも LACP ネゴシエーションを開始しないため、**auto** モードのポートは、**auto** モードの別のポートと EtherChannel を形成することはできません。

サイレントモード

PAgP 対応のデバイスにスイッチを接続する場合、**non-silent** キーワードを使用すると、スイッチポートを非サイレント動作用に設定できます。**auto** モードまたは **desirable** モードとともに **non-silent** モードを指定しなかった場合は、サイレントモードが指定されていると見なされません。

サイレントモードを使用するのは、PAgP 非対応で、かつほとんどパケットを送信しないデバイスにスイッチを接続する場合です。サイレントパートナーの例は、トラフィックを生成しないファイルサーバ、またはパケットアナライザなどです。この場合、サイレントパートナーに接続された物理ポート上で PAgP を稼働させると、このスイッチポートが動作しなくなります。ただし、サイレントを設定すると、PAgP が動作してチャンネルグループにポートを結合し、このポートが伝送に使用されます。

ポート集約プロトコルの学習方法と優先度

ネットワークデバイスは、PAgP 物理ラーナーまたは集約ポートラーナーに分類されます。物理ポートによってアドレスを学習し、その知識に基づいて送信を指示するデバイスは物理ラーナーです。集約（論理）ポートによってアドレスを学習するデバイスは、集約ポートラーナーです。学習方式は、リンクの両端で同一の設定にする必要があります。

デバイスとそのパートナーが両方とも集約ポートラーナーの場合、論理ポートチャンネル上のアドレスを学習します。デバイスは EtherChannel のいずれかのポートを使用することによって、送信元にパケットを送信します。集約ポートラーナーの場合、どの物理ポートにパケットが届くかは重要ではありません。

PAgP は、パートナー デバイスが物理ラーナーの場合およびローカル デバイスが集約ポートラーナーの場合には自動検出できません。したがって、物理ポートでアドレスを学習するには、ローカルデバイスに手動で学習方式を設定する必要があります。また、負荷の分散方式を送信元ベース分散に設定して、指定された送信元 MAC アドレスが常に同じ物理ポートに送信されるようにする必要があります。

グループ内の1つのポートですべての伝送を行うように設定して、他のポートをホットスタンバイに使用することもできます。選択された1つのポートでハードウェア信号が検出されなくなった場合は、数秒以内に、グループ内の未使用のポートに切り替えて動作させることができます。パケット伝送用に常に選択されるように、ポートを設定するには、**pagp port-priority** インターフェイスコンフィギュレーションコマンドを使用してプライオリティを変更します。プライオリティが高いほど、そのポートが選択される可能性が高まります。



- (注) CLIで **physical-port** キーワードを指定した場合でも、デバイスがサポートするのは、集約ポート上でのアドレスラーニングのみです。 **pagp learn-method** コマンドおよび **pagp port-priority** コマンドは、デバイスハードウェアには影響を及ぼしませんが、Catalyst 1900 スイッチなど、物理ポートによるアドレスラーニングのみをサポートしているデバイスと PAgP の相互運用性を確保するために必要です。

デバイスのリンクパートナーが物理ラーナーである場合、 **pagp learn-method physical-port** インターフェイス コンフィギュレーション コマンドを使用して物理ポートラーナーとしてデバイスを設定することを推奨します。また、 **port-channel load-balance src-mac** グローバル コンフィギュレーションコマンドを使用して、送信元 MAC アドレスに基づいて負荷分散方式を設定することを推奨します。すると、デバイスは送信元アドレスを学習した EtherChannel 内の同じポートを使用して、物理ラーナーにパケットを送信します。この状況では、 **pagp learn-method** コマンドのみを使用します。

ポート集約プロトコルと他の機能との連携動作

ダイナミック トランキング プロトコル (DTP) および Cisco Discovery Protocol (CDP) は、EtherChannel の物理ポートを使用してパケットを送受信します。トランクポートは、番号が最も小さい VLAN 上で PAgP プロトコルデータ ユニット (PDU) を送受信します。

レイヤ 2 EtherChannel では、チャンネル内で最初に起動するポートが EtherChannel に MAC アドレスを提供します。このポートがバンドルから削除されると、バンドル内の他のポートの 1 つが EtherChannel に MAC アドレスを提供します。レイヤ 3 EtherChannel の場合、 (**interface port-channel** グローバルコンフィギュレーションコマンドを経由して) インターフェイスが作成された直後に、アクティブなデバイスにより MAC アドレスが割り当てられます。

PAgP が PAgP PDU を送受信するのは、PAgP が auto モードまたは desirable モードでイネーブルになっている、稼働状態のポート上だけです。

Link Aggregation Control Protocol (LACP)

LACP は IEEE 802.3ad で定義されており、シスコデバイスが IEEE 802.3ad プロトコルに適合したデバイス間のイーサネットチャンネルを管理できるようにします。LACP を使用すると、イーサネットポート間で LACP パケットを交換することにより、EtherChannel を自動的に作成できます。

スイッチまたはスイッチスタックは LACP を使用することによって、LACP をサポートできるパートナーの識別情報、および各ポートの機能を学習します。次に、設定が類似しているポートを単一の論理リンク (チャンネルまたは集約ポート) に動的にグループ化します。設定が類似しているポートをグループ化する場合の基準は、ハードウェア、管理、およびポートパラメータ制約です。たとえば、LACP は速度、デュプレックスモード、ネイティブ VLAN、VLAN 範囲、トランキングステータス、およびトランキングタイプが同じポートをグループとしてまとめます。リンクをまとめて EtherChannel を形成した後で、LACP は単一デバイスポートとして、スパンニングツリーにそのグループを追加します。

ポート チャンネル内のポートの独立モード動作が変更されます。CSCtn96950 では、デフォルトでスタンダロンモードが有効になっています。LACP ピアから応答が受信されない場合、ポート チャンネル内のポートは中断状態に移動されます。

Link Aggregation Control Protocol モード

LACP モードでは、ポートが LACP パケットを送信できるか、LACP パケットの受信のみができるかどうかを指定します。

Table 11: EtherChannel LACP モード

モード	説明
active	ポートをアクティブ ネゴシエーション ステートにします。この場合、ポートは LACP パケットを送信することによって、相手ポートとのネゴシエーションを開始します。
passive	ポートはパッシブ ネゴシエーション ステートになります。この場合、ポートは受信する LACP パケットに応答しますが、LACP パケット ネゴシエーションを開始することはありません。これにより、LACP パケットの送信を最小限に抑えます。

active モードおよび **passive** LACP モードはともに、相手ポートとネゴシエーションして、ポート速度などの条件に基づいて（レイヤ 2 EtherChannel の場合は、トランクステートおよび VLAN 番号などの基準に基づいて）、ポートで EtherChannel を形成できるようにします。

LACP モードが異なっても、モード間で互換性がある限り、ポートは EtherChannel を形成できます。次に例を示します。

- **active** モードのポートは、**active** または **passive** モードの別のポートと EtherChannel を形成できます。
- 両ポートとも LACP ネゴシエーションを開始しないため、**passive** モードのポートは、**passive** モードの別のポートと EtherChannel を形成することはできません。

Link Aggregation Control Protocol とリンクの冗長性

LACP ポートチャンネルの最小リンクおよび LACP の最大バンドルの機能を使用して、LACP ポートチャンネル動作、帯域幅の可用性およびリンク冗長性をさらに高めることができます。

LACP ポートチャンネルの最小リンク機能：

- LACP ポート チャンネルでリンクし、バンドルする必要があるポートの最小数を設定します。
- 低帯域幅の LACP ポート チャンネルがアクティブにならないようにします。
- 必要な最低帯域幅を提供する十分なアクティブ メンバ ポートがない場合、LACP ポートチャンネルが非アクティブになるようにします。

LACP の最大バンドル機能：

- LACP ポート チャンネルのバンドル ポートの上限数を定義します。
- バンドルポートがより少ない場合のホットスタンバイポートを可能にします。たとえば、5 個のポートがある LACP ポート チャンネルで、3 個の最大バンドルを指定し、残りの 2 個のポートをホットスタンバイポートとして指定できます。

Link Aggregation Control Protocol とその他の機能との連携動作

DTP および CDP は、EtherChannel の物理ポートを介してパケットを送受信します。トランクポートは、番号が最も小さい VLAN 上で LACP PDU を送受信します。

レイヤ 2 EtherChannel では、チャンネル内で最初に起動するポートが EtherChannel に MAC アドレスを提供します。このポートがバンドルから削除されると、バンドル内の他のポートの 1 つが EtherChannel に MAC アドレスを提供します。レイヤ 3 EtherChannel の場合、**interface port-channel** グローバルコンフィギュレーションコマンドを経由してインターフェイスが作成された直後に、アクティブなデバイスにより MAC アドレスが割り当てられます。

LACP が LACP PDU を送受信するのは、LACP が active モードまたは passive モードでイネーブルになっている稼働状態のポートとの間だけです。

EtherChannel の On モード

EtherChannel **on** モードは、EtherChannel を手動で設定するために使用できます。**on** モードでは、ネゴシエーションを行わずにポートは強制的に EtherChannel に参加されます。**on** モードは、リモートデバイスが PAgP または LACP をサポートしていない場合に役立つことがあります。**on** モードでは、リンクの両端のデバイスが **on** モードに設定されている場合のみ、使用可能な EtherChannel が存在します。

同じチャンネルグループ内で **on** モードに設定されているポートは、互換性のあるポート特性（速度やデュプレックスなど）を備えている必要があります。互換性のないポートは、**on** モードに設定されている場合でも、一時停止されます。



Caution **on** モードを使用する場合は、注意する必要があります。これは手動の設定であり、EtherChannel の両端のポートには、同一の設定が必要です。グループの設定を誤ると、パケット損失またはスパンニングツリーループが発生することがあります。

ロードバランシングおよび転送方式

EtherChannel は、フレーム内のアドレスに基づいて形成されたバイナリ パターンの一部を、チャンネル内の 1 つのリンクを選択する数値に縮小することによって、チャンネル内のリンク間でトラフィックのロードバランシングを行います。MAC アドレス、IP アドレス、送信元アドレス、宛先アドレス、または送信元と宛先両方のアドレスに基づいた負荷分散など、複数の異なる

るロードバランシングモードから1つを指定できます。選択したモードは、デバイス上で設定されているすべての EtherChannel に適用されます。



Note レイヤ3等コストマルチパス (ECMP) のロードバランシングは、送信元 IP アドレス、宛先 IP アドレス、送信元ポート、宛先ポート、およびレイヤ4プロトコルに基づいています。フラグメント化されたパケットは、これらのパラメータを使用して計算されたアルゴリズムに基づいて2つの異なるリンクで処理されます。これらのパラメータのいずれかを変更すると、ロードバランシングが実行されます。

MAC アドレス転送

送信元 MAC アドレス転送の場合、EtherChannel に転送されたパケットは、着信パケットの送信元 MAC アドレスに基づいてチャンネルポート間で分配されます。したがって、ロードバランシングを行うために、送信元ホストが異なるパケットはそれぞれ異なるチャンネルポートを使用しますが、送信元ホストが同じパケットは同じチャンネルポートを使用します。

宛先 MAC アドレス転送の場合、EtherChannel に転送されたパケットは、着信パケットの宛先ホストの MAC アドレスに基づいてチャンネルポート間で分配されます。したがって、宛先が同じパケットは同じポートに転送され、宛先の異なるパケットはそれぞれ異なるチャンネルポートに転送されます。

送信元および宛先 MAC アドレス転送の場合、EtherChannel に転送されたパケットは、送信元および宛先の両方の MAC アドレスに基づいてチャンネルポート間で分配されます。この転送方式は、負荷分散の送信元 MAC アドレス転送方式と宛先 MAC アドレス転送方式を組み合わせたものです。特定のデバイスに対して送信元 MAC アドレス転送と宛先 MAC アドレス転送のどちらが適切であるかが不明な場合に使用できます。送信元および宛先 MAC アドレス転送の場合、ホスト A からホスト B、ホスト A からホスト C、およびホスト C からホスト B に送信されるパケットは、それぞれ異なるチャンネルポートを使用できます。

IP アドレス転送

送信元 IP アドレスベース転送の場合、パケットは、着信パケットの送信元 IP アドレスに基づいて EtherChannel ポート間で分配されます。ロードバランシングを行うために、IP アドレスが異なるパケットはチャンネルでそれぞれ異なるポートを使用しますが、IP アドレスが同じパケットはチャンネルで同じポートを使用します。

宛先 IP アドレスベース転送の場合、パケットは着信パケットの宛先 IP アドレスに基づいて EtherChannel ポート間で分配されます。ロードバランシングを行うために、同じ送信元 IP アドレスから異なる宛先 IP アドレスに送信されるパケットは、チャンネルの異なるチャンネルポートに送信できます。異なる送信元 IP アドレスから同じ宛先 IP アドレスに送信されるパケットは、常にチャンネルの同じポートに送信されます。

送信元と宛先 IP アドレスベース転送の場合、パケットは着信パケットの送信元および宛先の両方の IP アドレスに基づいて EtherChannel ポート間で分配されます。この転送方式は、送信元 IP アドレスベース転送方式と宛先 IP アドレスベース転送方式を組み合わせたもので、特定のデバイスに対して送信元 IP アドレスベース転送と宛先 IP アドレスベース転送のどちらが適

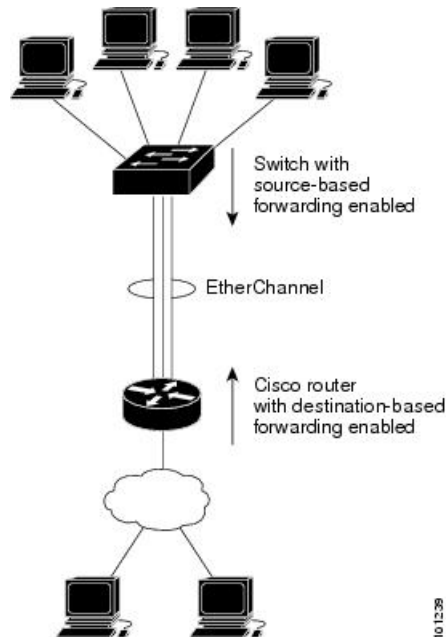
切であるか不明な場合に使用できます。この方式では、IP アドレス A から IP アドレス B に、IP アドレス A から IP アドレス C に、および IP アドレス C から IP アドレス B に送信されるパケットは、それぞれ異なるチャネルポートを使用できます。

ロードバランシングの利点

ロードバランシング方式には異なる利点があるため、ネットワーク内のデバイスの位置、および負荷分散が必要なトラフィックの種類に基づいて特定のロードバランシング方式を選択する必要があります。

図 20: 負荷の分散および転送方式

次の図では、4 台のワークステーションの EtherChannel がルータと通信します。ルータは単一 MAC アドレスデバイスであるため、スイッチ EtherChannel で送信元ベース転送を行うことにより、スイッチが、ルータで使用可能なすべての帯域幅を使用することが保証されます。ルータは、宛先アドレスベース転送を行うように設定されます。これは、多数のワークステーションで、トラフィックがルータ EtherChannel から均等に分配されることになっているためです。



設定で一番種類が多くなるオプションを使用してください。たとえば、チャネル上のトラフィックが単一 MAC アドレスを宛先とする場合、宛先 MAC アドレスを使用すると、チャネル内の同じリンクが常に選択されます。ただし、送信元アドレスまたは IP アドレスを使用した方が、ロードバランシングの効率がよくなる場合があります。

EtherChannel とスイッチ スタック

EtherChannel に加入しているポートが含まれているスタックメンバに、障害が発生するか、そのスタックメンバがスタックから除外された場合、アクティブなスイッチにより、障害が発生したスタックメンバスイッチポートが EtherChannel から削除されます。EtherChannel に残っているポートがある場合、接続は引き続き確保されます。

スイッチが既存スタックに追加されると、新しいスイッチでは、アクティブなスイッチから実行コンフィギュレーションを受信し、EtherChannel 関連のスタック設定でアップデートされます。スタックメンバでは、動作情報（動作中で、チャンネルのメンバであるポートのリスト）も受信します。

2つのスタック間で設定されている EtherChannel がマージされた場合、セルフループポートになります。スパニングツリーにより、この状況が検出され、必要な動作が発生します。正常な状態にあるスイッチスタックにある PAgP 設定または LACP 設定は影響を受けませんが、損失したスイッチスタックの PAgP 設定または LACP 設定は、スタックのリブート後に失われます。

スイッチスタックおよび PAgP

PAgP では、アクティブなスイッチに障害が発生するか、スタックを離れた場合、スタンバイスイッチが新しいアクティブスイッチになります。新しいアクティブスイッチはアクティブなスイッチの該当項目にスタックメンバの設定を同期します。PAgP 設定は、EtherChannel に古いアクティブスイッチ上にあるポートがない限り、アクティブなスイッチの変更後も影響を受けません。

スイッチスタックと Link Aggregation Control Protocol

LACP の場合、システム ID には、アクティブなスイッチから取得したスタック MAC アドレスが使用されます。アクティブスイッチに障害が発生したり、スタックを離れ、スタンバイスイッチが新しいアクティブスイッチが変更になっても、LACP システム ID は変更されません。デフォルトでは、LACP 設定はアクティブスイッチの変更後も影響を受けません。

EtherChannel のデフォルト設定

EtherChannel のデフォルト設定を、次の表に示します。

Table 12: EtherChannel のデフォルト設定

機能	デフォルト設定
チャンネルグループ	割り当てなし
ポートチャンネル論理インターフェイス	未定義
PAgP モード	デフォルトなし
PAgP 学習方式	すべてのポートで集約ポートラーニング
PAgP プライオリティ	すべてのポートで 128
LACP モード	デフォルトなし
LACP 学習方式	すべてのポートで集約ポートラーニング

機能	デフォルト設定
LACP ポート プライオリティ	すべてのポートで 32768
LACP システム プライオリティ	32768
LACP システム ID	LACP システムのプライオリティおよびスイッチまたはスタックの MAC アドレス
ロード バランシング	着信パケットの送信元 MAC アドレスに基づいてスイッチ上で負荷を分散 送信元 MAC アドレスは src-mac です。

EtherChannel 設定時の注意事項

EtherChannel ポートを正しく設定していない場合は、ネットワークループおよびその他の問題を回避するために、一部の EtherChannel インターフェイスが自動的にディセーブルになります。設定上の問題を回避するために、次の注意事項に従ってください。

- スイッチまたはスイッチスタックでは、最大 128 の EtherChannel がサポートされています。
- PAgP EtherChannel は、同じタイプのイーサネット ポートを 8 つまで使用して設定します。
- 同じタイプのイーサネット ポートを最大で 16 個備えた LACP EtherChannel を設定してください。最大 8 つのポートを active モードに、最大 8 つのポートを standby モードにできます。
- EtherChannel 内のすべてのポートを同じ速度および同じデュプレックスモードで動作するように設定します。
- EtherChannel 内のすべてのポートをイネーブルにします。 **shutdown** インターフェイス コンフィギュレーション コマンドを使用して無効にされた EtherChannel 内のポートはリンク障害として扱われ、そのトラフィックは EtherChannel 内の残りのポートのいずれかに転送されます。
- グループを初めて作成した際には、そのグループに最初に追加されたポートのパラメータ設定値をすべてのポートが引き継ぎます。次のパラメータのいずれかで設定を変更した場合は、グループ内のすべてのポートでも変更する必要があります。
 - 許可 VLAN リスト
 - 各 VLAN のスパニングツリー パス コスト
 - 各 VLAN のスパニングツリー ポート プライオリティ
 - スパニングツリー PortFast の設定
- 1 つのポートが複数の EtherChannel グループのメンバになるように設定しないでください。

- EtherChannel は、PAgP と LACP の両方のモードには設定しないでください。PAgP および LACP が稼働している複数の EtherChannel グループは、同じスイッチまたはスタック内の別のスイッチ上で共存できます。個々の EtherChannel グループは PAgP または LACP のいずれかを実行できますが、相互運用することはできません。
- アクティブまたはアクティブでない EtherChannel メンバであるポートを IEEE 802.1x ポートとして設定しないでください。EtherChannel ポートで IEEE 802.1x をイネーブルにしようとすると、エラーメッセージが表示され、IEEE 802.1x はイネーブルになりません。
- EtherChannel がデバイスインターフェイスに設定されている場合は、**dot1x system-auth-control** グローバル コンフィギュレーション コマンドを使用して、デバイス上で IEEE 802.1x をグローバルに有効にする前に、インターフェイスから EtherChannel 構成を削除します。

レイヤ 2 EtherChannel 設定時の注意事項

レイヤ 2 EtherChannels を設定する場合は、次の注意事項に従ってください。

- EtherChannel 内のすべてのポートを同じ VLAN に割り当てるか、またはトランクとして設定してください。複数のネイティブ VLAN に接続されるポートは、EtherChannel を形成できません。
- EtherChannel は、トランキング レイヤ 2 EtherChannel 内のすべてのポート上で同じ VLAN 許容範囲をサポートしています。VLAN 許容範囲が一致していないと、PAgP が **auto** モードまたは **desirable** モードに設定されていても、ポートは EtherChannel を形成しません。
- スパニングツリーパスコストが異なるポートは、設定上の矛盾がない限り、EtherChannel を形成できます。異なるスパニングツリーパスコストを設定すること自体は、EtherChannel を形成するポートの矛盾にはなりません。

レイヤ 3 EtherChannel 設定時の注意事項

レイヤ 3 EtherChannel の場合は、レイヤ 3 アドレスをチャンネル内の物理ポートでなく、ポートチャンネル論理インターフェイスに割り当ててください。

Auto-LAG

Auto-LAG 機能は、スイッチに接続されたポートで EtherChannel を自動的に作成できる機能です。デフォルトでは、Auto-LAG がグローバルに無効にされ、すべてのポートインターフェイスで有効になっています。Auto-LAG は、グローバルに有効になっている場合にのみ、スイッチに適用されます。

Auto-LAG をグローバルに有効にすると、次のシナリオが可能になります。

- パートナー ポート インターフェイス上に EtherChannel が設定されている場合、すべてのポートインターフェイスが自動 EtherChannel の作成に参加します。詳細については、次の表「アクターとパートナー デバイス間でサポートされる *Auto-LAG* 設定」を参照してください。

- すでに手動 EtherChannel の一部であるポートは、自動 EtherChannel の作成に参加することはできません。
- Auto-LAG がすでに自動で作成された EtherChannel の一部であるポート インターフェイスで無効になっている場合、ポート インターフェイスは自動 EtherChannel からバンドル解除されます。

次の表に、アクターとパートナー デバイス間でサポートされる Auto-LAG 設定を示します。

表 13: アクターとパートナー デバイス間でサポートされる Auto-LAG 設定

アクター/パートナー	アクティブ	パッシブ	自動
アクティブ	対応	対応	対応
パッシブ	対応	非対応	対応
自動	対応	対応	対応

Auto-LAG をグローバルに無効にすると、自動で作成されたすべての Etherchannel が手動 EtherChannel になります。

既存の自動で作成された EtherChannel で設定を追加することはできません。追加するには、最初に **port-channel<channel-number>persistent** を実行して、手動 EtherChannel に変換する必要があります。



- (注) Auto-LAG は自動 EtherChannel の作成に LACP プロトコルを使用します。一意のパートナー デバイスで自動的に作成できる EtherChannel は 1 つだけです。

Auto-LAG 設定時の注意事項

Auto-LAG 機能を設定するときには、次の注意事項に従ってください。

- Auto-LAG がグローバルで有効な場合、およびポート インターフェイスで有効な場合に、ポート インターフェイスを自動 EtherChannel のメンバーにたくない場合は、ポート インターフェイスで Auto-LAG を無効にします。
- ポート インターフェイスは、すでに手動 EtherChannel のメンバーである場合、自動 EtherChannel にバンドルされません。自動 EtherChannel にバンドルされるようにするには、まずポート インターフェイスで手動 EtherChannel のバンドルを解除します。
- Auto-LAG が有効になり、自動 EtherChannel が作成されると、同じパートナー デバイスで複数の EtherChannel を手動で作成できます。ただし、デフォルトでは、ポートはパートナー デバイスで自動 EtherChannel の作成を試行します。
- Auto-LAG は、レイヤ 2 EtherChannel でのみサポートされています。レイヤ 3 インターフェイスおよびレイヤ 3 EtherChannel ではサポートされていません。

- Auto-LAG は、Cross-Stack EtherChannel でサポートされています。

EtherChannel の設定方法

EtherChannel の設定後、ポートチャンネルインターフェイスに適用した設定変更は、そのポートチャンネルインターフェイスに割り当てられたすべての物理ポートに適用されます。また、物理ポートに適用した設定変更は、設定を適用したポートだけに作用します。

ここでは、EtherChannel のさまざまな設定情報について説明します。

レイヤ 2 EtherChannel の設定

レイヤ 2 EtherChannel を設定するには、インターフェイス コンフィギュレーション モードで **channel-group** コマンドを使用して、チャンネルグループにポートを割り当てます。このコマンドにより、ポートチャンネル論理インターフェイスが自動的に作成されます。

Procedure

	Command or Action	Purpose
ステップ 1	enable Example: Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	configure terminal Example: Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	interface interface-id Example: Device(config)# interface gigabitethernet 1/0/1	物理ポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 指定できるインターフェイスは、物理ポートです。 PAGP EtherChannel の場合、同じタイプおよび速度のポートを 8 つまで同じグループに設定できます。 LACP EtherChannel の場合、同じタイプのイーサネットポートを 16 まで設定できます。最大 8 つのポートを active モードに、最大 8 つのポートを standby モードにできます。

	Command or Action	Purpose
ステップ 4	switchport mode {access trunk} Example: Device(config-if)# switchport mode access	すべてのポートをスタティックアクセスポートとして同じ VLAN に割り当てるか、またはトランクとして設定します。 ポートをスタティックアクセスポートとして設定する場合は、ポートを1つの VLAN にのみ割り当ててください。指定できる範囲は 1 ~ 4094 です。
ステップ 5	switchport access vlan <i>vlan-id</i> Example: Device(config-if)# switchport access vlan 22	ポートをスタティックアクセスポートとして設定する場合は、ポートを1つの VLAN にのみ割り当ててください。指定できる範囲は 1 ~ 4094 です。
ステップ 6	channel-group <i>channel-group-number</i> mode {auto [non-silent] desirable [non-silent] on } { active passive} Example: Device(config-if)# channel-group 5 mode auto	チャンネルグループにポートを割り当て、PAgP モードまたは LACP モードを指定します。 mode には、次のキーワードのいずれか 1 つを選択します。 <ul style="list-style-type: none"> • auto – PAgP 装置が検出された場合に限り、PAgP をイネーブルにします。ポートをパッシブ ネゴシエーション状態にします。この場合、ポートは受信する PAgP パケットに応答しますが、PAgP パケットネゴシエーションを開始することはありません。 • desirable – 無条件に PAgP をイネーブルにします。ポートをアクティブ ネゴシエーション状態にします。この場合、ポートは PAgP パケットを送信することによって、相手ポートとのネゴシエーションを開始します。 • on – PAgP または LACP を使用せずにポートが強制的にチャンネル化されます。on モードでは、使用可能な EtherChannel が存在するのは、on モードのポートグループが、on モードの別のポートグループに接続する場合だけです。

	Command or Action	Purpose
		<ul style="list-style-type: none"> • non-silent – (任意) デバイスが PAgP 対応のパートナーに接続されている場合、ポートが auto または desirable モードになると非サイレント動作を行うようにデバイスポートを設定します。 non-silent を指定しなかった場合は、サイレントが指定されたものと見なされます。サイレント設定は、ファイル サーバまたはパケット アナライザとの接続に適しています。サイレントを設定すると、PAgP が動作してチャンネルグループにポートを結合し、このポートが伝送に使用されます。 • active : LACP 装置が検出された場合に限り、LACP をイネーブルにします。ポートをアクティブ ネゴシエーション ステートにします。この場合、ポートは LACP パケットを送信することによって、相手ポートとのネゴシエーションを開始します。 • passive – : ポート上で LACP をイネーブルにして、ポートをパッシブ ネゴシエーション ステートにします。この場合、ポートは受信する LACP パケットに応答しますが、LACP パケット ネゴシエーションを開始することはありません。
ステップ 7	end Example: Device (config-if) # end	特権 EXEC モードに戻ります。

レイヤ 3 EtherChannel の設定

レイヤ 3 EtherChannel にイーサネットポートを割り当てるには、この手順を実行します。この手順は必須です。

Procedure

	Command or Action	Purpose
ステップ 1	enable Example: Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	configure terminal Example: Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	interface interface-id Example: Device(config)# interface gigabitethernet 1/0/2	物理ポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 有効なインターフェイスには、物理ポートが含まれます。 PAgP EtherChannel の場合、同じタイプおよび速度のポートを 8 つまで同じグループに設定できます。 LACP EtherChannel の場合、同じタイプのイーサネットポートを 16 まで設定できます。最大 8 つのポートを active モードに、最大 8 つのポートを standby モードにできます。
ステップ 4	no ip address Example: Device(config-if)# no ip address	物理ポートに割り当てられている IP アドレスがないことを確認します。
ステップ 5	no switchport Example: Device(config-if)# no switchport	ポートをレイヤ 3 モードにします。
ステップ 6	channel-group channel-group-number mode { auto [non-silent] desirable [non-silent] on } { active passive } Example: Device(config-if)# channel-group 5 mode auto	チャンネルグループにポートを割り当て、PAgP モードまたは LACP モードを指定します。 mode には、次のキーワードのいずれか 1 つを選択します。 <ul style="list-style-type: none"> • auto : PAgP 装置が検出された場合に限り、PAgP をイネーブルにします。ポートをパッシブ ネゴシエーションステートにします。この場合、ポートは受信する PAgP パケッ

	Command or Action	Purpose
		<p>トに応答しますが、PAgP パケット ネゴシエーションを開始することはありません。EtherChannel メンバーがスイッチ スタック内で異なるスイッチに属している場合、このキーワードはサポートされません。</p> <ul style="list-style-type: none"> • desirable : 無条件に PAgP をイネーブルにします。ポートをアクティブ ネゴシエーション ステートにします。この場合、ポートは PAgP パケットを送信することによって、相手ポートとのネゴシエーションを開始します。EtherChannel メンバーがスイッチスタック内で異なるスイッチに属している場合、このキーワードはサポートされません。 • on : PAgP や LACP を使用しないで、ポートを強制的にチャンネル化します。on モードでは、使用可能な EtherChannel が存在するのは、on モードのポートグループが、on モードの別のポートグループに接続する場合だけです。 • non-silent (任意) デバイスが PAgP 対応のパートナーに接続されている場合、ポートが auto または desirable モードになると非サイレント動作を行うようにデバイスポートを設定します。non-silent を指定しなかった場合は、サイレントが指定されたものと見なされます。サイレント設定は、ファイル サーバまたはパケット アナライザとの接続に適しています。サイレントを設定すると、PAgP が動作してチャンネルグループにポートを結合し、このポートが伝送に使用されます。 • active : LACP 装置が検出された場合に限り、LACP をイネーブルにします。ポートをアクティブ ネゴシエーション ステートにします。こ

	Command or Action	Purpose
		<p>の場合、ポートはLACPパケットを送信することによって、相手ポートとのネゴシエーションを開始します。</p> <ul style="list-style-type: none"> • passive - : ポート上でLACPをイネーブルにして、ポートをパッシブネゴシエーションステートにします。この場合、ポートは受信するLACPパケットに応答しますが、LACPパケットネゴシエーションを開始することはありません。
ステップ 7	end Example: Device(config-if)# end	特権 EXEC モードに戻ります。

(任意) EtherChannel ロードバランシングの設定

複数の異なる転送方式の1つを使用するように EtherChannel ロードバランシングを設定できます。

EtherChannel ロードバランシングを設定するには、次の手順を実行します。

Procedure

	Command or Action	Purpose
ステップ 1	enable Example: Device> enable	<p>特権 EXEC モードを有効にします。</p> <p>パスワードを入力します (要求された場合)。</p>
ステップ 2	configure terminal Example: Device# configure terminal	グローバル コンフィギュレーションモードを開始します。
ステップ 3	port-channel load-balance {dst-ip dst-mac dst-mixed-ip-port dst-port extended src-dst-ip src-dst-mac src-dst-mixed-ip-port src-dst-port src-ip src-mac src-mixed-ip-port src-port } Example: Device(config)# port-channel load-balance src-mac	<p>EtherChannel のロードバランシング方式を設定します。</p> <p>デフォルトは src-mac です。</p> <p>次のいずれかの負荷分散方式を選択します。</p> <ul style="list-style-type: none"> • dst-ip : 宛先ホストの IP アドレスを指定します。

	Command or Action	Purpose
		<ul style="list-style-type: none"> • dst-mac : 着信パケットの宛先ホストの MAC アドレスを指定します。 • dst-mixed-ip-port : ホストの IP アドレスおよび TCP/UDP ポートを指定します。 • dst-port : 宛先 TCP/UDP ポートを指定します。 • src-dst-ip : 送信元および宛先ホストの IP アドレスを指定します。 • src-dst-mac : 送信元および宛先ホストの MAC アドレスを指定します。 • src-dst-mixed-ip-port : 送信元および宛先ホストの IP アドレスおよび TCP/UDP ポートを指定します。 • src-dst-port : 送信元および宛先 TCP/UDP ポートを指定します。 • extended : 標準コマンドで使用可能なもの以外に、送信元および宛先の方式を組み合わせた、拡張ロードバランシング方式を指定します。 • src-ip : 送信元ホストの IP アドレスを指定します。 • src-mac : 着信パケットの送信元 MAC アドレスを指定します。 • src-mixed-ip-port : 送信元ホストの IP アドレスおよび TCP/UDP ポートを指定します。 • src-port : 送信元 TCP/UDP ポートを指定します。
ステップ 4	end Example: Device(config)# end	特権 EXEC モードに戻ります。

EtherChannel 拡張ロードバランシングの設定

ロードバランシング方式を組み合わせる場合には、拡張ロードバランシングを設定します。

このタスクはオプションです。

Procedure

	Command or Action	Purpose
ステップ 1	enable Example: Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	configure terminal Example: Device# configure terminal	グローバル コンフィギュレーションモードを開始します。
ステップ 3	port-channel load-balance extended [dst-ip dst-mac dst-port ipv6-label l3-proto src-ip src-mac src-port] Example: Device(config)# port-channel load-balance extended dst-ip dst-mac src-ip	EtherChannel 拡張ロードバランシング方式を設定します。 デフォルトは src-mac です。 次のいずれかの負荷分散方式を選択します。 <ul style="list-style-type: none"> • dst-ip : 宛先ホストの IP アドレスを指定します。 • dst-mac : 着信パケットの宛先ホストの MAC アドレスを指定します。 • dst-port : 宛先 TCP/UDP ポートを指定します。 • ipv6-label : IPv6 フロー ラベルを指定します。 • l3-proto : レイヤ 3 プロトコルを指定します。 • src-ip : 送信元ホストの IP アドレスを指定します。 • src-mac : 着信パケットの送信元 MAC アドレスを指定します。 • src-port : 送信元 TCP/UDP ポートを指定します。

	Command or Action	Purpose
ステップ 4	end Example: Device(config)# end	特権 EXEC モードに戻ります。

(オプション) ポート集約プロトコルの学習方法と優先度の設定

PAgP ラーニング方式と優先順位を設定するには、次の手順を実行します。

Procedure

	Command or Action	Purpose
ステップ 1	enable Example: Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	configure terminal Example: Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	interface interface-id Example: Device(config)# interface gigabitethernet 1/0/2	伝送ポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	pagp learn-method physical-port Example: Device(config-if)# pagp learn-method physical port	PAgP 学習方式を選択します。 デフォルトでは、 aggregation-port learning が選択されています。つまり、EtherChannel 内のポートのいずれかを使用して、デバイスがパケットを送信元に送信します。集約ポート ラーナーの場合、どの物理ポートにパケットが届くかは重要ではありません。 is物理ポートラーナーである別のデバイスに接続する physical-port を選択します。 port-channel load-balance グローバル コンフィギュレーション コマンドを src-mac に設定してください。 学習方式はリンクの両端で同じ方式に設定する必要があります。

	Command or Action	Purpose
ステップ 5	pagp port-priority <i>priority</i> Example: Device(config-if) # pagp port-priority 200	選択したポートがパケット伝送用として選択されるように、プライオリティを割り当てます。 <i>priority</i> に指定できる範囲は 0 ~ 255 です。デフォルト値は 128 です。プライオリティが高いほど、ポートが PAgP 伝送に使用される可能性が高くなります。
ステップ 6	end Example: Device(config-if) # end	特権 EXEC モードに戻ります。

Link Aggregation Control Protocol ホットスタンバイ ポートの設定

LACP がイネーブルの場合、ソフトウェアはデフォルトで、チャンネルにおける LACP 互換ポートの最大数（最大 16 個のポート）の設定を試みます。一度にアクティブにできる LACP リンクは 8 つだけです。残りの 8 個のリンクがホットスタンバイモードになります。アクティブリンクの 1 つが非アクティブになると、ホットスタンバイモードのリンクが代わりにアクティブになります。

チャンネルでアクティブポートの最大数を指定することでデフォルト動作を上書きできます。この場合、残りのポートがホットスタンバイポートになります。たとえばチャンネルで最大 5 個のポートを指定した場合、11 個までのポートがホットスタンバイポートになります。

9 つ以上のリンクが EtherChannel グループとして設定された場合、ソフトウェアは LACP プライオリティに基づいてアクティブにするホットスタンバイポートを決定します。ソフトウェアは、LACP を操作するシステム間のすべてのリンクに、次の要素（プライオリティ順）で構成された一意のプライオリティを割り当てます。

- LACP システム プライオリティ
- システム ID (デバイス MAC アドレス)
- LACP ポート プライオリティ
- ポート番号

プライオリティの比較においては、数値が小さいほどプライオリティが高くなります。プライオリティは、ハードウェア上の制約がある場合に、すべての互換ポートが集約されないように、スタンバイモードにするポートを決定します。

アクティブポートかホットスタンバイポートかを判別するには、次の（2 つの）手順を使用します。まず、数値的に低いシステムプライオリティとシステム ID を持つシステムの方を選びます。次に、ポートプライオリティおよびポート番号の値に基づいて、そのシステムのアクティブポートとホットスタンバイポートを決定します。他のシステムのポートプライオリティとポート番号の値は使用されません。

ソフトウェアのアクティブおよびスタンバイリンクの選択方法に影響を与えるように、LACP システムプライオリティおよびLACPポートプライオリティのデフォルト値を変更できます。

LACP の最大バンドルの設定

ポートチャネルで許可されるバンドル化された LACP ポートの最大数を指定すると、ポートチャネル内の残りのポートがホットスタンバイポートとして指定されます。

ポートチャネルの LACP ポートの最大数を設定するには、特権 EXEC モードで開始して、次の手順に従います。この手順は任意です。

Procedure

	Command or Action	Purpose
ステップ 1	enable Example: Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	configure terminal Example: Device# configure terminal	グローバル コンフィギュレーションモードを開始します。
ステップ 3	interface port-channel channel-number Example: Device (config)# interface port-channel 2	ポートチャネルのインターフェイス コンフィギュレーションモードを開始します。 <i>channel-number</i> の範囲は 1 ~ 128 です。
ステップ 4	lcp max-bundle max_bundle_number Example: Device (config-if)# lcp max-bundle 3	ポートチャネルバンドルで LACP ポートの最大数を指定します。 指定できる範囲は 1 ~ 8 です。
ステップ 5	end Example: Device (config-if)# end	特権 EXEC モードに戻ります。

Link Aggregation Control Protocol ポートチャネル スタンドアロンの無効化の設定

ポートチャネルのスタンドアロン EtherChannel メンバーポートステートをディセーブルにするには、ポートチャネルインターフェイスで次の作業を行います。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例 :	特権 EXEC モードを有効にします。

	コマンドまたはアクション	目的
	Device> enable	パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	interface port-channel channel-group 例： Device(config)# interface port-channel channel-group	設定するポート チャネル インターフェイスを選択します。
ステップ 4	port-channel standalone-disable 例： Device(config-if)# port-channel standalone-disable	ポートチャネル インターフェイスのスタンドアロン モードをディセーブルにします。
ステップ 5	end 例： Device(config-if)# end	設定モードを終了します。
ステップ 6	show etherchannel 例： Device# show etherchannel channel-group port-channel Device# show etherchannel channel-group detail	設定を確認します。

LACP ポートチャネルの MinLink の設定

リンクアップ状態で、リンクアップステートに移行するポートチャネルインターフェイスの EtherChannel でバンドルする必要があるアクティブポートの最小数を指定できます。EtherChannel の最小リンクを使用して、低帯域幅 LACP EtherChannel がアクティブになることを防止できます。また、LACP EtherChannel にアクティブメンバー ポートが少なすぎて、必要な最低帯域幅を提供できない場合、この機能により LACP EtherChannel が非アクティブになります。

ポートチャネルに必要なリンクの最小数を設定する。次の作業を実行します。

Procedure

	Command or Action	Purpose
ステップ 1	enable Example: Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。

	Command or Action	Purpose
ステップ 2	configure terminal Example: Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	interface port-channel channel-number Example: Device (config)# interface port-channel 2	ポートチャネルのインターフェイス コンフィギュレーション モードを開始します。 <i>channel-number</i> の範囲は 1 ~ 128 です。
ステップ 4	port-channel min-links min-links-number Example: Device (config-if)# port-channel min-links 3	リンクアップ状態で、リンクアップステートに移行するポート チャネル インターフェイスの EtherChannel でバンドルする必要のあるメンバポートの最小数を指定できます。 <i>min-links-number</i> の範囲は 2 ~ 8 です。
ステップ 5	end Example: Device (config)# end	特権 EXEC モードに戻ります。

(任意) Link Aggregation Control Protocol システム優先順位の設定

lacp system-priority コマンドをグローバル コンフィギュレーション モードで使用して、LACP をイネーブルにしているすべての EtherChannel に対してシステムプライオリティを設定できます。LACP を設定済みの各チャネルに対しては、システムプライオリティを設定できません。デフォルト値を変更すると、ソフトウェアのアクティブおよびスタンバイリンクの選択方法に影響します。

どのポートがホットスタンバイモードにあるか確認するには、特権 EXEC モードで **show etherchannel summary** コマンドを使用します (H ポートステータスフラグで表示)。

LACP システム プライオリティを設定するには、次の手順に従います。

Procedure

	Command or Action	Purpose
ステップ 1	enable Example: Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します (要求された場合)。
ステップ 2	configure terminal Example: Device# configure terminal	グローバル コンフィギュレーション モードを開始します。

(任意) Link Aggregation Control Protocol ポート優先順位の設定

	Command or Action	Purpose
ステップ 3	lacp system-priority <i>priority</i> Example: Device(config)# lacp system-priority 32000	LACP システムプライオリティを設定します。 指定できる範囲は 1 ~ 65535 です。デフォルトは 32768 です。 値が小さいほど、システムプライオリティは高くなります。
ステップ 4	end Example: Device(config)# end	特権 EXEC モードに戻ります。

(任意) Link Aggregation Control Protocol ポート優先順位の設定

デフォルトでは、すべてのポートは同じポートプライオリティです。ローカルシステムのシステムプライオリティおよびシステムIDの値がリモートシステムよりも小さい場合は、LACP EtherChannel ポートのポートプライオリティをデフォルトよりも小さな値に変更して、最初にアクティブになるホットスタンバイリンクを変更できます。ホットスタンバイポートは、番号が小さい方が先にチャンネルでアクティブになります。どのポートがホットスタンバイモードにあるか確認するには、**show etherchannel summary** 特権 EXEC コマンドを使用します (H ポートステートフラグで表示)。



Note LACP がすべての互換ポートを集約できない場合 (たとえば、ハードウェアの制約が大きいリモートシステム)、EtherChannel 中でアクティブにならないポートはすべてホットスタンバイステートになり、チャンネル化されたポートのいずれかが機能しない場合に限り使用されます。

LACP ポートプライオリティを設定するには、次の手順に従います。

Procedure

	Command or Action	Purpose
ステップ 1	enable Example: Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します (要求された場合)。
ステップ 2	configure terminal Example: Device# configure terminal	グローバル コンフィギュレーションモードを開始します。

	Command or Action	Purpose
ステップ 3	interface <i>interface-id</i> Example: Device(config)# interface gigabitethernet 1/0/2	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	lacp port-priority <i>priority</i> Example: Device(config-if)# lacp port-priority 32000	LACP ポートプライオリティを設定します。 指定できる範囲は 1 ~ 65535 です。デフォルトは 32768 です。値が小さいほど、ポートが LACP 伝送に使用される可能性が高くなります。
ステップ 5	end Example: Device(config-if)# end	特権 EXEC モードに戻ります。

Link Aggregation Control Protocol 1:1 冗長高速レート タイマーの設定

LACP タイマー レートを変更することにより、LACP タイムアウトの時間を変更することができます。**lacp rate** コマンドを使用し、LACP がサポートされているインターフェイスで受信される LACP 制御パケットのレートを設定します。タイムアウト レートは、デフォルトのレート (30 秒) から高速レート (1 秒) に変更することができます。このコマンドは、LACP がイネーブルになっているインターフェイスでのみサポートされます。

LACP 1:1 冗長高速レート タイマーを設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します (要求された場合)。
ステップ 2	configure terminal 例 : Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	interface { fastethernet gigabitethernet tengigabitethernet } <i>slot/port</i> 例 : Device(config)# interface gigabitEthernet 2/1	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	lacp rate {normal fast} 例： Device(config-if)# lacp rate fast	LACP がサポートされているインターフェイスで受信される LACP 制御パケットのレートを設定します。 タイムアウトレートをデフォルトにリセットするには、 no lacp rate コマンドを使用します。
ステップ 5	end 例： Device(config)# end	特権 EXEC モードに戻ります。
ステップ 6	show lacp internal 例： Device# show lacp internal Device# show lacp counters	設定を確認します。

グローバルな Auto-LAG の設定

Auto-LAG をグローバルに構成するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーションモードを開始します。
ステップ 3	[no] port-channel auto 例： Device(config)# port-channel auto	スイッチ上の Auto-LAG 機能をグローバルで有効にします。スイッチ上の Auto-LAG 機能をグローバルで無効にするには、このコマンドの no 形式を使用します。 (注) デフォルトでは、auto-LAG 機能は各ポート上でイネーブルになっています。

	コマンドまたはアクション	目的
ステップ 4	end 例 : Device(config)# end	特権 EXEC モードに戻ります。
ステップ 5	show etherchannel auto 例 : Device# show etherchannel auto	EtherChannel が自動的に作成されたことが表示されます。

ポート インターフェイスでの Auto-LAG の設定

ポート インターフェイスで Auto-LAG を設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例 : Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	interface interface-id 例 : Device(config)# interface gigabitethernet 1/0/1	Auto-LAG を有効にするポート インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	[no] channel-group auto 例 : Device(config-if)# channel-group auto	（任意）個々のポート インターフェイスで Auto-LAG 機能を有効にします。 個々のポート インターフェイス上で Auto-LAG 機能を無効にするには、このコマンドの no 形式を使用します。 （注） デフォルトでは、auto-LAG 機能は各ポート上でイネーブルになっています。
ステップ 5	end 例 : Device(config-if)# end	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 6	show etherchannel auto 例： Device# show etherchannel auto	EtherChannel が自動的に作成されたことが表示されます。

Auto-LAG での持続性の設定

自動で作成された EtherChannel を手動のものに変更し、既存の EtherChannel に設定を追加するには、persistence コマンドを使用します。

Auto-LAG で永続性を構成するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	port-channel channel-number persistent 例： Device# port-channel 1 persistent	自動で作成された EtherChannel を手動のものに変更し、EtherChannel に設定を追加することができます。
ステップ 3	show etherchannel summary 例： Device# show etherchannel summary	EtherChannel 情報を表示します。

EtherChannel、ポート集約プロトコル、および Link Aggregation Control Protocol の状態のモニタリング

この表に記載されているコマンドを使用して EtherChannel、PAgP、および LACP ステータスを表示できます。

表 14: EtherChannel、PAgP、および LACP ステータスのモニタ用コマンド

コマンド	説明
clear lacp { <i>channel-group-number</i> counters counters }	LACP チャンネルグループ情報およびトラフィック カウンタをクリアします。
clear pagp { <i>channel-group-number</i> counters counters }	PAgP チャンネルグループ情報およびトラフィック カウンタをクリアします。

コマンド	説明
show etherchannel [<i>channel-group-number</i> { detail load-balance port port-channel protocol summary }] [detail load-balance port port-channel protocol auto summary]	EtherChannel 情報が簡潔、詳細に、1 行のサマリー形式で表示されます。負荷分散方式またはフレーム配布方式、ポート、ポートチャンネル、プロトコル、および Auto-LAG 情報も表示されます。
show pagp [<i>channel-group-number</i>] { counters internal neighbor }	トラフィック情報、内部 PAgP 設定、ネイバー情報などの PAgP 情報が表示されます。
show pagp [<i>channel-group-number</i>] dual-active	デュアルアクティブ検出ステータスが表示されます。
show lacp [<i>channel-group-number</i>] { counters internal neighbor sys-id }	トラフィック情報、内部 LACP 設定、ネイバー情報などの LACP 情報が表示されます。
show running-config	設定エントリを確認します。
show etherchannel load-balance	ポートチャンネル内のポート間のロードバランシング、またはフレーム配布方式を表示します。

EtherChannel の設定例

ここでは、EtherChannel のさまざまな設定例について説明します。

例：レイヤ 2 EtherChannel の設定

次に、スタック内の 1 つのスイッチに EtherChannel を設定する例を示します。2 つのポートを VLAN 10 のスタティックアクセスポートとして、PAgP モードが **desirable** であるチャンネル 5 に割り当てます。

```
Device# configure terminal
Device(config)# interface range gigabitethernet2/0/1 -2
Device(config-if-range)# switchport mode access
Device(config-if-range)# switchport access vlan 10
Device(config-if-range)# channel-group 5 mode desirable non-silent
Device(config-if-range)# end
```

次に、スタック内の 1 つのスイッチに EtherChannel を設定する例を示します。2 つのポートは VLAN 10 のスタティックアクセスポートとして、LACP モードが **active** であるチャンネル 5 に割り当てられます。 **active:**

```
Device# configure terminal
Device(config)# interface range gigabitethernet2/0/1 -2
Device(config-if-range)# switchport mode access
Device(config-if-range)# switchport access vlan 10
```

例：レイヤ 3 EtherChannel の設定

```
Device(config-if-range) # channel-group 5 mode active
Device(config-if-range) # end
```

次の例では、クロススタック EtherChannel を設定する方法を示します。LACP パッシブモードを使用して、VLAN 10 内のスタティックアクセスポートとしてスタックメンバ 1 のポートを 2 つ、スタックメンバ 2 のポートを 1 つチャンネル 5 に割り当てます。

```
Device# configure terminal
Device(config) # interface range gigabitethernet2/0/4 -5
Device(config-if-range) # switchport mode access
Device(config-if-range) # switchport access vlan 10
Device(config-if-range) # channel-group 5 mode passive
Device(config-if-range) # exit
Device(config) # interface gigabitethernet3/0/3
Device(config-if) # switchport mode access
Device(config-if) # switchport access vlan 10
Device(config-if) # channel-group 5 mode passive
Device(config-if) # exit
```

PoE または LACP ネゴシエーションのエラーは、スイッチからアクセスポイント (AP) に 2 つのポートを設定した場合に発生する可能性があります。このシナリオは、ポートチャンネルの設定をスイッチ側で行うと回避できます。詳細については、次の例を参照してください。

```
Device(config) # interface Port-channel1
Device(config-if) # switchport access vlan 20
Device(config-if) # switchport mode access
Device(config-if) # switchport nonegotiate
Device(config-if) # no port-channel standalone-disable
Device(config-if) # spanning-tree portfast
```



Note ポートがポートのフラッピングに関する LACP エラーを検出した場合は、次のコマンドも含める必要があります。 **no errdisable detect cause pagp-flap**

例：レイヤ 3 EtherChannel の設定

この例では、レイヤ 3 インターフェイスの設定方法を示します。2 つのポートは、LACP モードが **active** であるチャンネル 5 に割り当てられます。

```
Device# configure terminal
Device(config) # interface range gigabitethernet2/0/1 -2
Device(config-if-range) # no ip address
Device(config-if-range) # no switchport
Device(config-if-range) # channel-group 5 mode active
Device(config-if-range) # end
```

この例では、クロススタック レイヤ 3 EtherChannel の設定方法を示します。スタックメンバ 2 の 2 つのポートとスタックメンバ 3 の 1 つのポートは、LACP active モードでチャンネル 7 に割り当てられます。

```
Device# configure terminal
Device(config) # interface range gigabitethernet2/0/4 -5
Device(config-if-range) # no ip address
Device(config-if-range) # no switchport
Device(config-if-range) # channel-group 7 mode active
```

```
Device(config-if-range)# exit
Device(config)# interface gigabitethernet3/0/3
Device(config-if)# no ip address
Device(config-if)# no switchport
Device(config-if)# channel-group 7 mode active
Device(config-if)# exit
```

例 : LACP ホットスタンバイポートの設定

この例では、少なくとも3個のアクティブポートがある場合にアクティブ化される EtherChannel を設定する例を示します (ポートチャンネル2)。これは、7個のアクティブポートとホットスタンバイポートとしての最大9個の残りのポートから構成されます。

```
Device# configure terminal
Device(config)# interface port-channel 2
Device(config-if)# port-channel min-links 3
Device(config-if)# lacp max-bundle 7
```

例 : Auto-LAG の設定

次に、スイッチに Auto-LAG を設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# port-channel auto
Device(config-if)# end
Device# show etherchannel auto
```

次の例は、自動的に作成された EtherChannel の概要を示します。

```
Device# show etherchannel auto
Flags: D - down          P - bundled in port-channel
       I - stand-alone  s - suspended
       H - Hot-standby (LACP only)
       R - Layer3       S - Layer2
       U - in use       f - failed to allocate aggregator
       M - not in use, minimum links not met
       u - unsuitable for bundling
       w - waiting to be aggregated
       d - default port
       A - formed by Auto LAG
```

```
Number of channel-groups in use: 1
Number of aggregators:          1
```

Group	Port-channel	Protocol	Ports
1	Po1 (SUA)	LACP	Gi1/0/45 (P) Gi2/0/21 (P) Gi3/0/21 (P)

次の例は、**port-channel 1 persistent** コマンドを実行した後の自動 EtherChannel の概要を示します。

```
Device# port-channel 1 persistent

Device# show etherchannel summary
Switch# show etherchannel summary
Flags: D - down          P - bundled in port-channel
       I - stand-alone  s - suspended
       H - Hot-standby (LACP only)
```

```

R - Layer3      S - Layer2
U - in use      f - failed to allocate aggregator
M - not in use, minimum links not met
u - unsuitable for bundling
w - waiting to be aggregated
d - default port
A - formed by Auto LAG

Number of channel-groups in use: 1
Number of aggregators:          1

Group  Port-channel  Protocol  Ports
-----+-----+-----+-----
1      Po1 (SU)        LACP      Gi1/0/45 (P) Gi2/0/21 (P) Gi3/0/21 (P)

```

EtherChannels の追加リファレンス

関連資料

関連項目	マニュアルタイトル
この章で使用するコマンドの完全な構文および使用方法の詳細。	<i>Command Reference (Catalyst 9300 Series Switches)</i> の「Layer 2/3 Commands」の項を参照してください

EtherChannel の機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Everest 16.5.1a	EtherChannel	EtherChannel は、スイッチ、ルータ、およびサーバー間にフォールトトレラントな高速リンクを提供します。
Cisco IOS XE Amsterdam 17.3.1	LACP 1:1 冗長性とダンプニング	LACP 1:1 冗長性機能では、ホットスタンバイリンクへのファストスイッチオーバーとアクティブリンク 1 つによる EtherChannel 設定がサポートされます。 LACP 1:1 ホットスタンバイダンプニング機能は、アクティブになった後、プライオリティの高いポートへのスイッチオーバーを遅らせるタイマーを設定します。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> [英語] からアクセスします。



第 5 章

高精度時間プロトコル (PTP) の設定

- PTP の制約事項と制限 (129 ページ)
- Precision Time Protocol について (130 ページ)
- PTP の設定方法 (139 ページ)
- 例：レイヤ 2 およびレイヤ 3 PTP の設定 (150 ページ)
- PTP の機能の履歴 (154 ページ)

PTP の制約事項と制限

- 高精度時間プロトコル (PTP) は、C9300-48UXM スイッチモデルの最初の 16 個のみのダウンリンクポートと、すべてのアップリンクポートでサポートされます。
- デバイスの **show clock** コマンドの出力と、**show platform software fed switch active ptp domain** コマンドの出力に表示される PTP サーボクロックが同期していません。これらの出力は、スイッチで使用される 2 つの異なるクロックです。
- PTP トランスペアレントクロックモードでは、VLAN 間はサポートされません。
- PTP は、スタックされたデバイスではサポートされていません。
- スイッチは、IEEE 802.1AS および IEEE 1588 デフォルトプロファイルをサポートしており、どちらも相互に排他的です。スイッチで一度に有効化できるプロファイルは 1 つだけです。
- Cisco PTP の実装では、2 ステップクロックのみがサポートされ、1 ステップクロックはサポートされません。スイッチがグランドマスタークロックから 1 ステップメッセージを受信すると、メッセージはドロップされます。
- クロック同期の精度が低下するため、PTP が有効化されていないデバイスを PTP ネットワークに配置することは推奨されません。
- シグナリングメッセージは、Cisco IOS XE Gibraltar 16.12.1 ではサポートされていません。これらのメッセージは、処理されずにスイッチでドロップされます。
- 境界クロックモードが有効化されている場合、ブロードキャストターゲット ID を持つ管理メッセージはホップカウントを減らして転送されます。トランスペアレントクロック

モードが有効化されている場合、管理メッセージは境界ホップカウントを減らすことなく転送されます。

- ある PTP モードから別の PTP モードに直接移行することは推奨されません。 **no PTP mode** を使用して既存のモードをクリアし、新しいモードを設定します。
- IPv6 および VRF は PTP をサポートしません。
- トランスペアレントクロックモードは、ネイティブレイヤ 3 ポートおよび EtherChannel インターフェイスではサポートされません（境界クロックモードはネイティブレイヤ 3 ポートでサポートされます）。
- PTP はスーパーバイザモジュールのどのポートにも設定できません。
- ステートフルスイッチオーバー (SSO) は、PTP をサポートしていません。PTP プロトコルは、スイッチオーバー後に再起動します。
- Precision Time Protocol (PTP) を備えた MACsec はサポートされません。

Precision Time Protocol について

Precision Time Protocol (PTP) は、IEEE 1588 で、ネットワーク化された測定および制御システムのための高精度クロック同期として定義されており、さまざまな精度と安定性の分散デバイスクロックを含むパケットベースネットワークでクロックを同期させるために開発されました。PTP は、産業用のネットワーク化された測定および制御システム向けに特別に設計されており、最小限の帯域幅とわずかな処理オーバーヘッドしか必要としないため、分散システムでの使用に最適です。

Cisco IOS XE Fuji 16.8.1 以降では、レイヤ 2 PTP およびレイヤ 3 PTP のサポートが有効になっています。

PTP を使用する理由

ピーク時課金、仮想発電機、停電の監視/管理などのスマートグリッド電力自動化アプリケーションは、非常に正確な時刻精度と安定性を必要とします。タイミングの精度は、ネットワーク監視の精度とトラブルシューティング能力を向上させます。

時刻精度および同期の提供に加えて、PTP メッセージベースプロトコルは、イーサネットネットワークなどのパケットベースネットワークに実装することもできます。イーサネットネットワークで PTP を使用する利点は次のとおりです。

- 既存のイーサネットネットワークでコストを削減でき、セットアップも容易
- PTP データパケットは限られた帯域幅しか必要としない

イーサネット スイッチと遅延

Precision Time Protocol (PTP) は、IEEE 1588 で、ネットワーク化された測定および制御システムのための高精度クロック同期として定義されており、さまざまな精度と安定性の分散デバイス クロックを含むパケットベース ネットワークでクロックを同期させるために開発されました。PTPは、産業用のネットワーク化された測定および制御システム向けに特別に設計されており、最小限の帯域幅とわずかな処理オーバーヘッドしか必要としないため、分散システムでの使用に最適です。

PTP を使用する理由

イーサネット ネットワークでは、スイッチは、ネットワーク デバイス間の全二重通信パスを提供します。スイッチは、パケットに含まれるアドレス情報を使用して、データパケットをパケット宛先に送信します。スイッチは、複数のパケットを同時に送信しようとする場合、送信前に失われないようにパケットの一部をバッファします。バッファがいっぱいになると、スイッチはパケットの送信を遅延させます。この遅延により、ネットワーク上のデバイスクロックが相互に同期しなくなる可能性があります。

スイッチが MAC アドレステーブルを検索してパケット CRC フィールドを確認している間に、スイッチに入るパケットがローカルメモリに保存されると、追加の遅延が発生する可能性があります。このプロセスによりパケット転送時間のレイテンシが変動し、これらの変動によってパケット遅延時間が非対称になる場合があります。

PTP をネットワークに追加することで、デバイスクロックを正しく調整し、相互の同期を維持することにより、これらのレイテンシおよび遅延の問題を補うことができます。PTP により、ネットワークスイッチは、境界クロック (BC) やトランスペアレントクロック (TC) などの PTP デバイスとして機能することが可能になります。

メッセージベースの同期

クロック同期を確保するために、PTP では、時刻源 (マスター) と受信者 (スレーブ) の間の通信パス遅延を正確に測定する必要があります。PTP は、マスタ デバイスとスレーブ デバイスの間でメッセージを送信して、遅延測定を決定します。メッセージの種類については、[PTPv2 メッセージタイプ \(132 ページ\)](#) で詳しく説明しています。次に、PTP は正確なメッセージ送受信時間を測定し、これらの時間を使用して通信パス遅延を計算します。その後、PTP は、計算された遅延に対してネットワーク データに含まれる現在の時刻情報を調整し、より正確な時刻情報を生成します。

この遅延測定原理によってネットワーク上のデバイス間のパス遅延が決定され、マスターとスレーブの間で送信される一連のメッセージを使用して、この遅延に関してローカルクロックが調整されます。一方向の遅延時間は、送信メッセージと受信メッセージのパス遅延を平均化することによって計算されます。この計算は対称的な通信パスを前提としていますが、スイッチドネットワークは、バッファリングプロセスのために必ずしも対称的な通信パスを持つとは限りません。

PTP は、トランスペアレントクロックを使用し、スイッチをネットワーク上のマスター ノードとスレーブ ノードに対して一時的に透過的にして、ネットワーク タイミング パケットの時

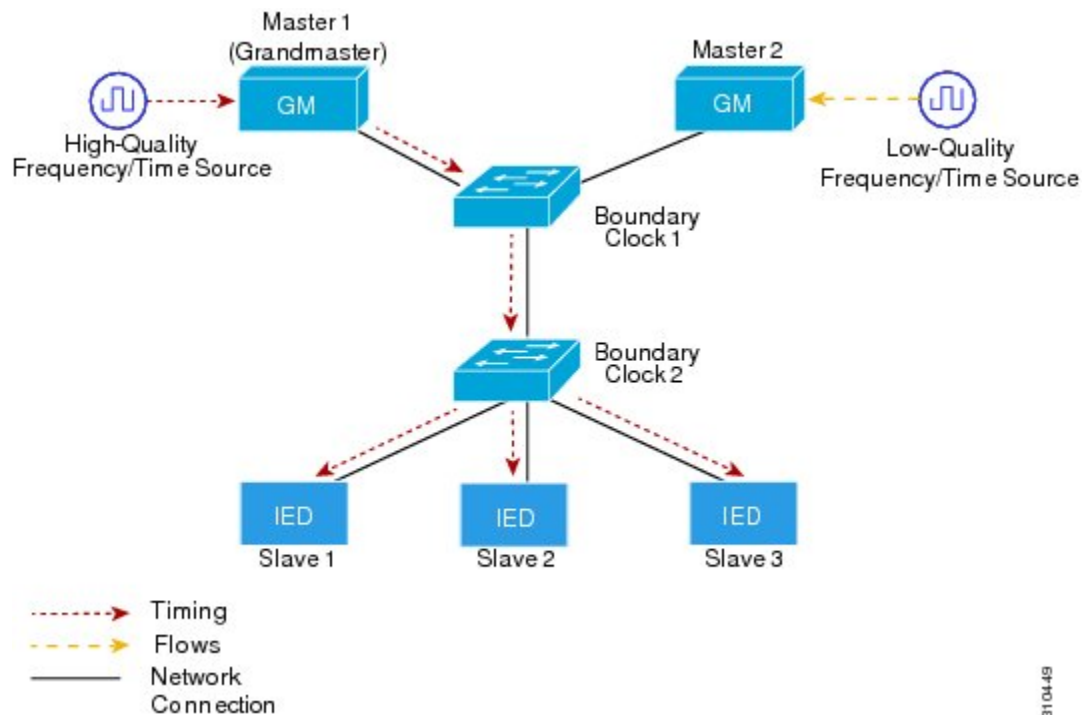
間隔フィールドの遅延を測定し、割り出す方法を提供します。エンドツーエンド透過クロックは、スイッチと同じ方法で、ネットワーク上のすべてのメッセージを転送します。



(注) Cisco PTP は、マルチキャスト PTP メッセージのみをサポートしています。

次の図に、グランドマスタークロック、境界クロックモードのスイッチ、およびデジタルリレーや保護デバイスなどのインテリジェントな電子機器 (IED) を含む標準的な 1588 PTP ネットワークを示します。この図では、Master 1 がグランドマスタークロックです。Master 1 が使用不能になると、同期のために境界クロックスレーブが Master 2 に切り替わります。

図 21: PTP ネットワーク



31049

PTPv2 メッセージタイプ

PTP メッセージは、次の 2 つのタイプに分類されます。

- イベントメッセージ: データパケットがポートに到達するとき、またはポートから出るときにタイムスタンプでタグ付けされ、タイムスタンプに基づいてリンク遅延を計算するために使用されます。イベントメッセージは次のとおりです。
 - Sync
 - Delay_Req
 - Pdelay_Req

- Pdelay_Resp

- 一般的なメッセージ：タイムスタンプでタグ付けされず、マスター/スレーブ階層を確立するために使用されます。一般的なメッセージは次のとおりです。

- アナウンス
- Follow_Up
- Delay_Resp
- Pdelay_Resp_Follow_Up

アナウンスメッセージは、同期階層を確立するために使用されます。

Sync、Delay_Req、Follow_Up、および Delay_Resp メッセージは、通常のクロックと境界クロックを同期するために使用されます。

Pdelay_Req、Pdelay_Resp、および Pdelay_Resp_Follow_Up メッセージは、トランスペアレントクロックのリンク遅延を測定するために使用されます。

ベストマスタークロックアルゴリズム は、グラントマスタークロックを選択し、ポートをマスターまたはスレーブとして割り当てます。これに続いて、すべてのマスターポートが、Sync メッセージとフォローアップメッセージを使用して、ダウンストリームスレーブへのクロックの供給を開始します。ダウンストリームスレーブはクロックを受信し、リンクの遅延、時間オフセット、周波数オフセット、および誤差パラメータを計算した後にクロックを更新します。

ダウンストリームスレーブは、以下のいずれかのメカニズムを使用してリンク遅延を計算します。

- [エンドツーエンドの遅延メカニズム \(133 ページ\)](#)
- [ピアツーピアの遅延メカニズム \(135 ページ\)](#)

PTP イベントメッセージシーケンス

ここでは、同期中に発生する PTP イベントメッセージシーケンスについて説明します。

エンドツーエンドの遅延メカニズム

遅延要求/応答メカニズム用に設定された通常クロックと境界クロックは、次のイベントメッセージを使用してタイミング情報を生成し、伝えます。

- Sync
- Delay_Req
- Follow_Up
- Delay_Resp

これらのメッセージは、次のシーケンスで送信されます。

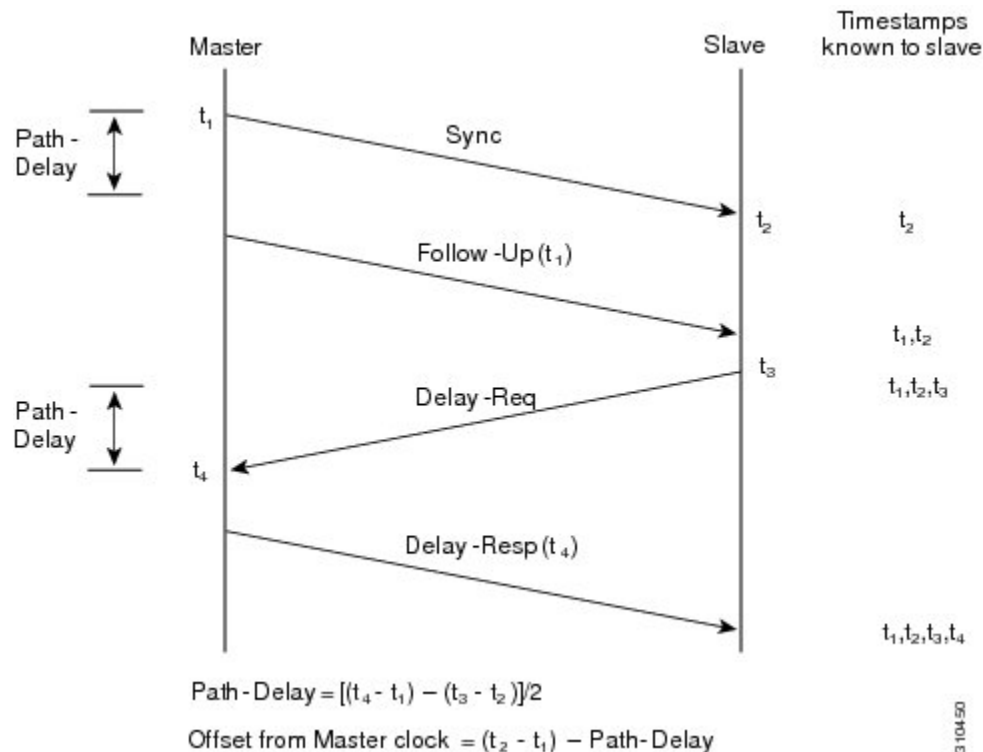
1. マスターが、スレーブに Sync メッセージを送信し、それが送信された時刻 (t1) を記録します。

2. スレーブが、Sync メッセージを受信し、受信した時刻 (t₂) を記録します。
3. マスターが、Follow_Up メッセージにタイムスタンプ t₁ を組み込むことによって、タイムスタンプ t₁ をスレーブに伝えます。
4. スレーブが、マスターに Delay_Req メッセージを送信し、それが送信された時刻 (t₃) を記録します。
5. マスターが、Delay_Req メッセージを受信し、受信した時刻 (t₄) を記録します。
6. マスターが、Delay_Resp メッセージにタイムスタンプ t₄ を組み込むことによって、タイムスタンプ t₄ をスレーブに伝えます。

このシーケンスの後、スレーブは4つのタイムスタンプをすべて保有します。これらのタイムスタンプを使用して、マスターに対するスレーブクロックのオフセットと、2つのクロック間のメッセージの平均伝達時間を計算できます。

オフセット計算は、メッセージがマスターからスレーブに伝達される時間がスレーブからマスターに伝達されるために必要な時間と同じであるという前提に基づいています。この前提は、非対称的なパケット遅延時間のためにイーサネットネットワーク上では必ずしも妥当ではありません。

図 22: 手順の詳細 : エンドツーエンドの遅延メカニズム



ピアツーピアの遅延メカニズム

ネットワークの階層内に複数のレベルの境界クロックが含まれており、それらの間に非PTP対応デバイスがある場合は、同期の精度が低下します。

ラウンドトリップ時間は `mean_path_delay/2` と等しいことが前提となっていますが、この前提はイーサネットネットワークでは必ずしも妥当ではありません。精度を向上させるために、各中間クロックの滞留時間がエンドツーエンド透過クロックのオフセットに追加されます。ただし、滞留時間にはピア間のリンク遅延が考慮されていません。ピア間のリンク遅延はピアツーピア透過クロックによって処理されます。

ピアツーピア透過クロックは、ピア遅延メカニズムを実装する2つのクロックポート間のリンク遅延を測定します。リンク遅延は、`Sync` メッセージと `Follow_Up` メッセージのタイミング情報を補正するために使用されます。

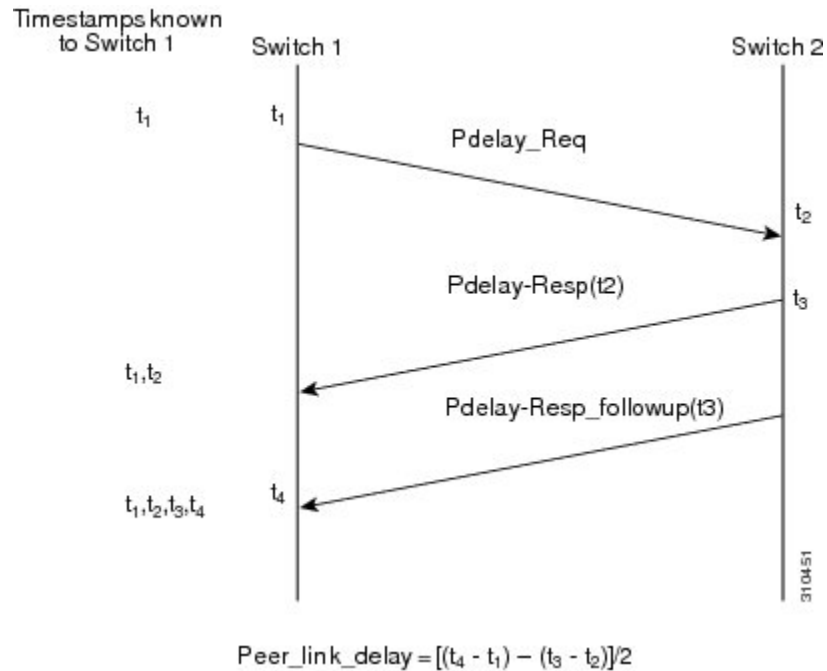
ピアツーピア透過クロックは、次のイベントメッセージを使用します。

- `Pdelay_Req`
- `Pdelay_Resp`
- `Pdelay_Resp_Follow_Up`

これらのメッセージは、次のシーケンスで送信されます。

1. ポート 1 が、`Pdelay_Req` メッセージのタイムスタンプ `t1` を生成します。
2. ポート 2 が、このメッセージを受信してタイムスタンプ `t2` を生成します。
3. ポート 2 が、`Pdelay_Resp` メッセージを返してタイムスタンプ `t3` を生成します。
2つのポート間の周波数オフセットによるエラーを最小限に抑えるために、ポート 2 は、`Pdelay_Req` メッセージを受信した後に、できるかぎり迅速に `Pdelay_Resp` メッセージを返します。
4. ポート 2 が、`Pdelay_Resp` メッセージと `Pdelay_Resp_Follow_Up` メッセージでそれぞれタイムスタンプ `t2` とタイムスタンプ `t3` を返します。
5. ポート 1 が、`Pdelay_Resp` メッセージを受信した後に、タイムスタンプ `t4` を生成します。その後、ポート 1 が、4つのタイムスタンプ (`t1`、`t2`、`t3`、`t4`) を使用して平均リンク遅延を計算します。

図 23: 手順の詳細: ピアツーピアの遅延メカニズム



ローカルクロックの同期

理想的な PTP ネットワークでは、マスタークロックとスレーブクロックは同じ周波数で動作します。ただし、このネットワークでは「ばらつき」が発生する可能性があります。このばらつきは、マスタークロックとスレーブクロックの間の周波数の差です。デバイスハードウェアのタイムスタンプ情報とフォローアップメッセージ（スイッチで代行受信）を使用してローカルクロックの周波数を調整し、マスタークロックの周波数と一致させることによって、ばらつきを補うことができます。

ベストマスタークロックアルゴリズム

ベストマスタークロックアルゴリズム (BMCA) は PTP 機能の基盤です。BMCA は、ネットワーク上の各クロックが、そのサブドメイン内で認識できるすべてのクロック（そのクロック自体を含む）のうちのベストマスタークロックを決定する方法を指定します。BMCA は、アナウンス間隔ごとにネットワーク内の各ポート上でローカルかつ継続的に動作し、ネットワーク構成における変更を迅速に調整します。IEEE 1588-2008 に基づく BMCA は、クロックプロパティのアドバタイジングに対するアナウンスメッセージを使用します。

BMCA は、次の基準を使用して、サブドメイン内のベストマスタークロックを決定します。

- クロック品質（たとえば、GPS は最高品質とみなされます）
- クロックの時刻基準のクロック精度
- 局部発振器の安定性
- グランドマスターに最も近いクロック

IEEE 1588-2008 に基づく BMCA は、受信したデータセットとともに独自のデータセットを使用し、次のプロパティを持つ属性に基づいて、指定された順序で最適なクロックを決定します。

- 優先順位 1：各クロックにユーザーが割り当てた優先順位。有効な範囲は 0 ～ 255 です。デフォルト値は 128 です。
- クラス：クロックが属するクラス。各クラスには独自の優先順位があります。
- 精度：クロックと UTC 間の精度 (ナノ秒)
- バリエーション：クロックの変動
- 優先順位 2：最終的な優先順位。有効な範囲は 0 ～ 255 です。デフォルト値は 128 です。
- 固有識別子：64 ビット拡張固有識別子 (EUI)

BMCA は、ベスト マスター クロックを特定するだけでなく、次のことを保証して、PTP ネットワーク上でのクロック競合の発生を確実に防止します。

- クロックが相互にネゴシエートする必要がない。
- マスター クロック 特定プロセスの結果として、マスター クロックが 2 つ存在する、またはマスター クロックが存在しないといった不適切な設定になっていない。

PTP クロック

PTP ネットワークは、PTP 対応デバイスで構成されます。PTP 対応デバイスは、通常、次のクロック タイプで構成されます。

グランドマスター クロック

PTP ドメイン内では、グランドマスター クロックが、PTP によるクロック同期の主時刻源です。グランドマスター クロックは、通常、GPS や原子時計などの非常に正確な時刻源を持っています。ネットワークが外部時刻リファレンスを必要とせず、内部で同期する必要のみがある場合、グランドマスター クロックはフリー ランできます。



(注) クロック精度の低下が懸念されるため、ネットワークでスイッチを GM クロックとして使用することは推奨されません。

オーディナリ クロック

オーディナリ クロックは、1 つの PTP ポートを持つ PTP クロックです。このクロックは PTP ネットワークでノードとして機能し、BMCA がサブドメイン内のマスターまたはスレーブとして選択できます。オーディナリ クロックは、同期が必要なデバイスに接続されているネットワーク上のエンドノードとして使用されるため、PTP ネットワーク上で最も一般的なクロック タイプです。オーディナリ クロックには、外部デバイスに対するさまざまなインターフェースがあります。

境界クロック

PTP ネットワークにおける境界クロックは、標準のネットワークにおけるスイッチやルータに代わる動作をします。境界クロックには複数の PTP ポートがあり、各ポートは個別の PTP 通信パスへのアクセスを提供します。境界クロックは、PTP ドメイン間のインターフェイスを提供します。このクロックは、すべての PTP メッセージを代行受信して処理し、他のすべてのネットワーク トラフィックを通過させます。また、境界クロックは、BMCA を使用して、任意のポートから見えるクロックから最善のものを選択します。選択されたポートは、スレーブとして設定されます。マスターポートはダウンストリームに接続されたクロックを同期させ、スレーブポートはアップストリーム マスター クロックと同期します。

トランスペアレントクロック

PTP ネットワークの透過クロックの役割は、PTP イベント メッセージの一部である時間間隔フィールドを更新することです。この更新により、スイッチの遅延が補われ、1 ピコ秒未満の精度が実現されます。

次の 2 種類の透過クロックがあります。

エンドツーエンド (E2E) トランスペアレントクロックは、SYNC メッセージと DELAY_REQUEST メッセージに関して PTP イベントメッセージ中継時間（「常駐時間」とも呼ばれる）を測定します。この測定された中継時間は、対応するメッセージのデータフィールド（補正フィールド）に追加されます。

- SYNC メッセージの測定された中継時間は、対応する SYNC メッセージまたは FOLLOW_UP メッセージの補正フィールドに追加されます。
- DELAY_REQUEST メッセージの測定された中継時間は、対応する DELAY_RESPONSE メッセージの補正フィールドに追加されます。

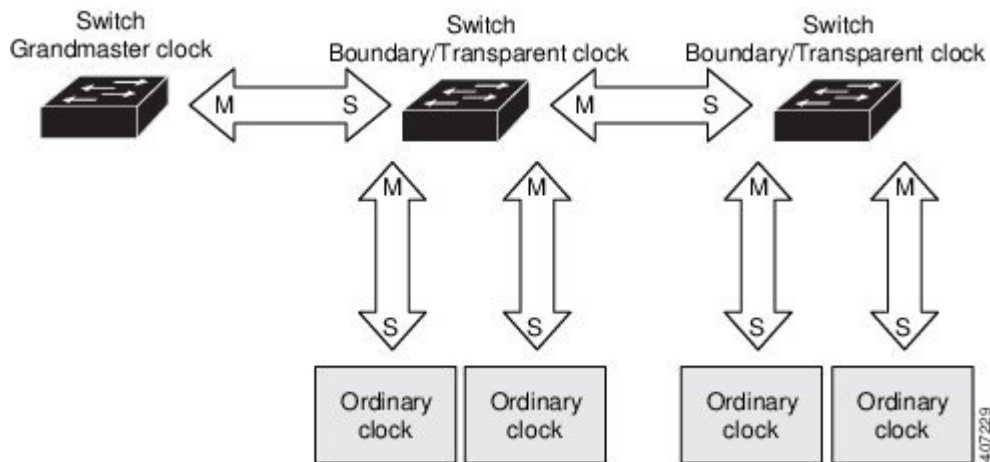
スレーブは、スレーブの時刻とマスターの時刻の間のオフセットを決定するときこの情報を使用します。E2E トランスペアレント クロックは、リンク自体の伝播遅延は修正しません。

ピアツーピア (P2P) 透過クロックは、前述のように、E2E 透過クロックと同じ方法で PTP イベントメッセージ中継時間を測定します。さらに、P2P 透過クロックは上流リンク遅延を測定します。上流リンク遅延は、上流の隣接する P2P 透過クロックと考慮対象の P2P 透過クロックの間の推定パケット伝搬遅延です。

これらの 2 つの時間（メッセージ中継時間とアップストリーム リンク遅延時間）は両方とも PTP イベントメッセージの修正フィールドに追加され、スレーブによって受信されるメッセージの修正フィールドにはすべてのリンク遅延の合計が含まれます。理論的には、これは、SYNC パケットのエンドツーエンドの遅延の合計（マスターからスレーブまで）です。

次の図に、PTP ネットワーク内のマスター/スレーブ階層に含まれる PTP クロックを示します。

図 24: PTP クロック階層



PTP プロファイル

PTP プロファイルの IEEE 1588 定義は、「デバイスに適用可能な、許容される一連の PTP 機能」です。PTP プロファイルは、通常、特定のタイプのアプリケーションまたは環境に固有のものであり、次の値を定義します。

- ベストマスタークロック アルゴリズム オプション
- 設定管理オプション
- パス遅延メカニズム (ピア遅延または遅延要求/応答)
- すべての PTP 設定可能属性およびデータセットメンバーの範囲とデフォルト値
- グランドマスターに最も近いクロック
- 必要な、許可される、または禁止されるトランスポートメカニズム
- 必要な、許可される、または禁止されるノードタイプ
- 必要な、許可される、または禁止されるオプション

Default Profile

スイッチのデフォルトの PTP プロファイルモードは、デフォルトプロファイルモードです。トランスポートの PTP モードはレイヤ 2 およびレイヤ 3 です。

デフォルトでは、PTP デフォルトプロファイルはこれらのプラットフォームでグローバルに無効化されています。

PTP の設定方法

次のセクションでは、PTP の設定について説明します。

レイヤ 2 PTP Default プロファイルの設定

レイヤ 2 PTP をグローバルに設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	<pre> {{}} } } ptp mode boundary delay-req e2transparent p2transparent </pre> 例： Device(config)# ptp mode boundary delay-req Device(config)# ptp mode boundary pdelay-req Device(config)# ptp mode e2transparent Device(config)# ptp mode p2transparent	同期クロックモードを指定します。 <ul style="list-style-type: none"> • boundary : スイッチが最良のマスタークロックを選択する作業に参加できるようにするモード。自らのクロックよりも優れたクロックが検出されない場合、スイッチはネットワークのグラウンドマスタークロックになり、接続しているすべての装置の親クロックになります。最良のマスターがスイッチに接続されたクロックであると判断された場合、スイッチはそのクロックにクロックの子として同期し、他のポートに接続された装置の親クロックとして機能します。最初の同期のあと、スイッチと接続済み装置は、タイミングメッセージを交換して、クロックのオフセットとネットワークの遅延による時間の歪みを修正します。このモードは、過負荷または重負荷の状態により大きな遅延ジッタが生じるときに使用します。 • e2transparent : すべてのスイッチポートをスイッチに接続されたグラウンドマスタークロックと同期させるためのスイッチのモード。これがデフォルトのクロックモードです。スイッチは、スイッチを通過するすべてのパケットが被る遅延（「滞留

	コマンドまたはアクション	目的
		<p>時間」 といいます) を修正します。 このモードでは、境界モードよりもジッタとエラーの蓄積が少なくなります。</p> <ul style="list-style-type: none"> • p2pttransparent : スイッチが自身のクロックをマスタークロックと同期させないようにするモード。このモードのスイッチは、マスタークロックの選択に参加せず、すべてのポートでデフォルト PTP クロックモードを使用します。 <p>PTP デフォルトプロファイルがデバイスでグローバルに有効になると、PTP はすべてのインターフェイスで有効になります。個別のインターフェイスで PTP を選択的に無効化するには、インターフェイスの設定で no ptp enable コマンドを使用します。</p> <p>PTP デフォルトプロファイル内では、PTP メッセージはデフォルトで VLAN 1 で処理されます。インターフェイス設定で ptp vlan vlan-name コマンドを使用して、特定の VLAN で PTP メッセージを処理できるようにします。これをデバイスの VLAN データベースに追加する必要があります。</p>
<p>ステップ 4</p>	<p>interface interface-id</p> <p>例 :</p> <pre>Device(config)# interface TenGigabitEthernet1/0/1</pre>	<p>設定する物理インターフェイスを指定し、インターフェイスコンフィギュレーションモードを開始します。</p>
<p>ステップ 5</p>	<p>switchport mode { access trunk }</p> <p>例 :</p> <pre>Device(config-if)# switchport mode trunk</pre>	<p>インターフェイスタイプ (アクセスまたはトランク) を設定します。</p> <ul style="list-style-type: none"> • access : インターフェイスを、非トランキング、タグなし、シングル VLAN インターフェイスとして設定します。アクセスポートは、1つの VLAN のトラフィックだけを伝送できます。デフォルトでは、アクセスポートは VLAN1 のトラフィックを伝送します。異なる VLAN のトラ

	コマンドまたはアクション	目的
		<p>フィックを伝送するようにアクセスポートを設定するには、switchport access vlan コマンドをステップ 5 で使用します。</p> <ul style="list-style-type: none"> • trunk : インターフェイスをイーサネットトランクポートとして設定します。トランク ポートは、同じ物理リンクで 1 つ以上の VLAN 内のトラフィックを伝送できます (各 VLAN はトランキングが許可された VLAN リストに基づいています)。デフォルトでは、トランクインターフェイスはすべての VLAN のトラフィックを伝送できます。特定のトランク上で特定の VLAN だけを許可するように指定するには、switchport trunk allowed vlan コマンドをステップ 6 で使用します。 <p>(注) スイッチポートモードがトランクの場合、ptp vlan vlan-id コマンドを使用して PTP VLAN を設定する必要があります。</p>
ステップ 6	<p>switchport access vlan <i>vlan-id</i></p> <p>例 :</p> <pre>Device(config-if)# switchport access vlan 5</pre>	<p>このアクセス ポートでトラフィックを伝送する VLAN を指定します。このコマンドを入力しないと、アクセスポートは VLAN1 だけのトラフィックを伝送します。このコマンドを使用して、アクセスポートがトラフィックを伝送する VLAN を変更できます。</p>
ステップ 7	<p>switchport trunk allowed vlan {{ add except remove } <i>vlan_list</i> all none }</p> <p>例 :</p> <pre>Device(config-if)# switchport trunk allowed vlan 2,10</pre>	<p>トランクインターフェイスの許可 VLAN を設定します。デフォルトでは、トランクインターフェイス上のすべての VLAN (1 ~ 3967 および 4048 ~ 4094) が許可されます。VLAN 3968 ~ 4047 は、内部利用のためにデフォルトで予約されている VLAN です。この VLAN グループは設定できません。デフォルトでは、すべ</p>

	コマンドまたはアクション	目的
		てのトランク インターフェイスですべての VLAN が許可されます。
ステップ 8	ptp vlan vlan-id 例 : Device(config-if) # ptp vlan 5	トランク ポートで PTP VLAN を設定します。範囲は 1 ~ 4094 です。デフォルトは、トランク ポートのネイティブ VLAN です。境界モードでは、PTP VLAN 内の PTP パケットのみが処理され、他の VLAN からの PTP パケットは破棄されます。インターフェイスで PTP VLAN を設定する前に、PTP VLAN を作成し、トランクポートで許可する必要があります。
ステップ 9	end 例 : Device(config-if) # end	特権 EXEC モードに戻ります。

レイヤ 3 PTP Default プロファイルの設定

レイヤ 3 PTP をグローバルに設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します (要求された場合)。
ステップ 2	configure terminal 例 : Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	ptp transport ipv4 udp 例 : Device(config) # ptp transport ipv4 udp	PTP 転送モードとして IPv4 を設定します。 (注) レイヤ 3 PTP の PTP 転送方式としてサポートされるのは IPv4 だけです。
ステップ 4	ptp mode boundary 例 :	同期クロックモードを指定します。 • boundary : スイッチが最良のマスタークロックを選択する作業に参

	コマンドまたはアクション	目的
	<pre>Device(config)# ptp mode boundary delay-req Device(config)# ptp mode boundary pdelay-req Device(config)# ptp mode e2etransparent Device(config)# ptp mode p2ptransparent</pre>	<p>加できるようにするモード。自らのクロックよりも優れたクロックが検出されない場合、スイッチはネットワークのグランドマスタークロックになり、接続しているすべての装置の親クロックになります。最良のマスターがスイッチに接続されたクロックであると判断された場合、スイッチはそのクロックにクロックの子として同期し、他のポートに接続された装置の親クロックとして機能します。最初の同期のあと、スイッチと接続済み装置は、タイミングメッセージを交換して、クロックのオフセットとネットワークの遅延による時間の歪みを修正します。このモードは、過負荷または重負荷の状態により大きな遅延ジッタが生じるときに使用します。</p> <ul style="list-style-type: none"> • e2etransparent : すべてのスイッチポートをスイッチに接続されたグランドマスタークロックと同期させるためのスイッチのモード。これがデフォルトのクロックモードです。スイッチは、スイッチを通過するすべてのパケットが被る遅延（「滞留時間」といいます）を修正します。このモードでは、境界モードよりもジッタとエラーの蓄積が少なくなります。 • p2ptransparent : スイッチが自身のクロックをマスタークロックと同期させないようにするモード。このモードのスイッチは、マスタークロックの選択に参加せず、すべてのポートでデフォルト PTP クロック モードを使用します。 <p>PTP デフォルトプロファイルがデバイスでグローバルに有効になると、PTP はすべてのインターフェイスで有効になります。個別のインターフェイスで</p>

	コマンドまたはアクション	目的
		<p>PTP を選択的に無効化するには、インターフェイスの設定で no ptp enable コマンドを使用します。</p> <p>PTP デフォルトプロファイル内では、PTP メッセージはデフォルトで VLAN 1 で処理されます。インターフェイス設定で ptp vlan vlan-name コマンドを使用して、特定の VLAN で PTP メッセージを処理できるようにします。これをデバイスの VLAN データベースに追加する必要があります。</p>
ステップ 5	interface vlan vlan-id 例 : Device(config)# interface vlan2	<p>設定する VLAN または SVI インターフェイスを指定し、インターフェイス コンフィギュレーションモードを開始します。</p> <p>(注) レイヤ 3 PTP は、VLAN および SVI インターフェイスでのみサポートされます。</p>
ステップ 6	ip address ip-address subnet-mask 例 : Device(config)# ip address 100.1.1.1 255.255.255.0	<p>IP アドレスおよび IP サブネットを設定します。</p>
ステップ 7	interface interface-id 例 : Device(config)# interface TenGigabitEthernet1/0/1	<p>設定する物理インターフェイスを指定し、インターフェイス コンフィギュレーションモードを開始します。</p>
ステップ 8	switchport mode { access trunk } 例 : Device(config-if)# switchport mode trunk	<p>インターフェイスタイプ (アクセスまたはトランク) を設定します。</p> <ul style="list-style-type: none"> • access : インターフェイスを、非トランキング、タグなし、シングル VLAN インターフェイスとして設定します。アクセスポートは、1 つの VLAN のトラフィックだけを伝送できます。デフォルトでは、アクセスポートは VLAN1 のトラフィックを伝送します。異なる VLAN のトラフィックを伝送するようにアクセスポートを設定する

	コマンドまたはアクション	目的
		<p>には、switchport access vlan コマンドをステップ 8 で使用します。</p> <ul style="list-style-type: none"> • trunk : インターフェイスをイーサネットトランクポートとして設定します。トランクポートは、同じ物理リンクで1つ以上の VLAN 内のトラフィックを伝送できます (各 VLAN はトランキングが許可された VLAN リストに基づいています)。デフォルトでは、トランク インターフェイスはすべての VLAN のトラフィックを伝送できます。特定のトランク上で特定の VLAN だけを許可するように指定するには、switchport trunk allowed vlan コマンドをステップ 9 で使用します。 <p>(注) スイッチポートモードがトランクの場合、ptp vlan vlan-id コマンドを使用して PTP VLAN を設定する必要があります。</p>
ステップ 9	<p>switchport access vlan <i>vlan-id</i></p> <p>例 :</p> <pre>Device(config-if)# switchport access vlan 5</pre>	<p>このアクセスポートでトラフィックを伝送する VLAN を指定します。このコマンドを入力しないと、アクセスポートは VLAN1 だけのトラフィックを伝送します。このコマンドを使用して、アクセスポートがトラフィックを伝送する VLAN を変更できます。</p>
ステップ 10	<p>switchport trunk allowed vlan {add except remove} <i>vlan_list</i> all none}</p> <p>例 :</p> <pre>Device(config-if)# switchport trunk allowed vlan 2,10</pre>	<p>トランク インターフェイスの許可 VLAN を設定します。デフォルトでは、トランク インターフェイス上のすべての VLAN (1 ~ 3967 および 4048 ~ 4094) が許可されます。VLAN 3968 ~ 4047 は、内部利用のためにデフォルトで予約されている VLAN です。この VLAN グループは設定できません。デフォルトでは、すべてのトランクイン</p>

	コマンドまたはアクション	目的
		ターフェイスですべての VLAN が許可されます。
ステップ 11	ptp vlan <i>vlan-id</i> 例 : Device (config-if) # ptp vlan 5	トランク ポートで PTP VLAN を設定します。範囲は 1 ~ 4094 です。デフォルトは、トランク ポートのネイティブ VLAN です。境界モードでは、PTP VLAN 内の PTP パケットのみが処理され、他の VLAN からの PTP パケットは破棄されます。インターフェイスで PTP VLAN を設定する前に、PTP VLAN を作成し、トランクポートで許可する必要があります。
ステップ 12	end 例 : Device (config-if) # end	特権 EXEC モードに戻ります。

インターフェイスでの PTP の無効化

デフォルトでは、すべてのポートで PTP がイネーブルになっています。インターフェイスで PTP を無効にするには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します (要求された場合)。
ステップ 2	configure terminal 例 : Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	interface <i>interface-id</i> 例 : Device (config) # interface gigabitethernet2/0/1	設定する物理ポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	[no] ptp enable 例 : Device (config-if) # no ptp enable	PTP を無効にするには、このコマンドの no 形式を使用します。

	コマンドまたはアクション	目的
ステップ 5	end 例： Device(config-if)# end	特権 EXEC モードに戻ります。

PTP タイマーの設定

PTP タイマー値をデフォルト値から必要な値に変更するには、次の手順を実行します。

始める前に

タイマー入力は、ログ平均メッセージ間隔値の単位で測定されます。**interval** キーワードの *value* (秒単位) を決定するには、対数目盛を使用します。次の表に、対数目盛で秒数に変換された *value* キーワードの例を示します。

入力される値	対数計算	秒単位の値
-1	2^{-1}	1/2
0	2^0	1

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します (要求された場合)。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	interface interface-id 例： Device(config)# interface gigabitethernet2/0/1	設定する物理ポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	ptp announce {interval value timeout count} 例： Device(config-if)# ptp announce interval 1	(任意) インターフェイス上の PTP アナウンス メッセージ間の間隔またはタイムアウトがインターフェイスで発生する前の PTP 間隔の数を設定します。 <ul style="list-style-type: none">• interval value : アナウンスメッセージを送信する対数平均間隔を設定し

	コマンドまたはアクション	目的
		<p>ます。範囲は0～4です。デフォルト値は0 (1秒) です。</p> <ul style="list-style-type: none"> • timeout count : タイムアウトメッセージをアナウンスする対数平均間隔を秒単位で設定します。範囲は2～10です。デフォルトは3 (8秒) です。
ステップ 5	<p>ptp sync {interval value limit offset-value}</p> <p>例 :</p> <pre>Device(config-if) # ptp sync interval 1</pre>	<p>(任意) インターフェイス上の PTP 同期メッセージの送信間隔を設定します。</p> <ul style="list-style-type: none"> • interval value : 同期メッセージを送信する対数平均間隔を設定します。範囲は、-3～1です。デフォルト値は0 (1秒) です。 • limit offset-value : PTP が再同期を試みるまでの、最大クロックオフセット値を設定します。範囲は50～500000000ナノ秒です。デフォルトは500000000ナノ秒です。
ステップ 6	<p>ptp delay-req interval value</p> <p>例 :</p> <pre>Device(config-if) # ptp delay-req interval 1</pre>	<p>(任意) ポートがマスターステートの場合に PTP 遅延要求メッセージ間で許可される対数平均間隔を設定します。指定できる範囲は0～5です。デフォルト値は0 (1秒) です。</p>
ステップ 7	<p>ptp pdelay-req interval value</p> <p>例 :</p> <pre>Device(config-if) # ptp pdelay-req interval 1</pre>	<p>(任意) ポートがマスターステートの場合に遅延要求メッセージ間で許可される対数平均間隔を設定します。指定できる範囲は0～5です。デフォルト値は0 (1秒) です。</p>
ステップ 8	<p>end</p> <p>例 :</p> <pre>Device(config-if) # end</pre>	<p>特権 EXEC モードに戻ります。</p>

Precision Time Protocol のクロック値の設定

PTP クロックの値 (優先順位 1 および優先順位 2) を設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 プロンプトが表示されたらパスワードを入力します。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	ptp priority1 value 例： Device(config)# ptp priority1 120	PTP クロックの優先順位 1 の値を設定します。有効な範囲は 0 ~ 255 です。デフォルト値は 128 です。 (注) 優先順位 1 の値が 255 に設定されると、クロックはグランドマスターとは見なされません。
ステップ 4	ptp priority2 value 例： Device(config)# ptp priority2 120	PTP クロックの優先順位 2 の値を設定します。有効な範囲は 0 ~ 255 です。デフォルト値は 128 です。
ステップ 5	exit 例： Device(config)# exit	グローバル コンフィギュレーション モードに戻ります。

例：レイヤ2およびレイヤ3 PTP の設定

例

show ptp port interface *interface-name*

PTP ポートの状態を確認するには、**show ptp port interface** *interface-name* コマンドを使用します。

すべてのインターフェイスの PTP ポートの状態を確認するには、**show ptp brief** コマンドを使用します。

次に、遅延要求メカニズムを使用した境界モード設定の出力例を示します。

```
Device# show ptp port GigabitEthernet1/0/45
PTP PORT DATASET: GigabitEthernet1/0/45
  Port identity: clock identity: 0xCC:46:D6:FF:FE:C5:24:0
  Port identity: port number: 45
```

```

PTP version: 2
Port state: SLAVE
Delay request interval(log mean): 0
Announce receipt time out: 3
Announce interval(log mean): 1
Sync interval(log mean): 0
Delay Mechanism: End to End
Peer delay request interval(log mean): 0
Sync fault limit: 500000000

```

次に、遅延要求メカニズムを使用した境界モード設定の出力例を示します。

```

Device# show ptp port GigabitEthernet1/0/45
PTP PORT DATASET: GigabitEthernet1/0/45
Port identity: clock identity: 0xCC:46:D6:FF:FE:C5:24:0
Port identity: port number: 45
PTP version: 2
Port state: MASTER
Delay request interval(log mean): 0
Announce receipt time out: 3
Announce interval(log mean): 1
Sync interval(log mean): 0
Delay Mechanism: Peer to Peer
Peer delay request interval(log mean): 0
Sync fault limit: 500000000

```

show ptp brief

すべてのインターフェイスの PTP ポートの状態を確認するには、**show ptp brief** コマンドを使用します。

次に、**show ptp brief** コマンドの出力例を示します。

```

Device# show ptp brief
Interface                               Domain    PTP State
TenGigabitEthernet1/0/1                 0        MASTER
TenGigabitEthernet1/0/2                 0        SLAVE
TenGigabitEthernet1/0/3                 0        FAULTY

```

show ptp clock

PTP クロックアイデンティティの詳細およびプライオリティ1とプライオリティ2の設定値を確認するには、**show ptp clock** コマンドを使用します。

次に、**show ptp clock** コマンドの出力例を示します。

```

Device# show ptp clock
PTP CLOCK INFO
PTP Device Type: Boundary clock
PTP Device Profile: Default Profile
Clock Identity: 0xCC:46:D6:FF:FE:C5:24:0 <<clock identity of this
switch>>
Clock Domain: 0
Number of PTP ports: 52
Priority1: 128
Priority2: 128

```

```

Clock Quality:
  Class: 248
  Accuracy: Unknown
  Offset (log variance): 16640
Offset From Master(ns): 0
Mean Path Delay(ns): 0
Steps Removed: 1

```

show ptp parent

境界モードでデバイスが同期されているグランドマスタークロック ID を特定するには、**show ptp parent** コマンドを使用します。



(注) **show ptp parent** は、デバイスがトランスペアレントクロック モードに設定されている場合、出力を表示しません。

次に、**show ptp parent** コマンドの出力例を示します。

```

Device# show ptp parent
PTP PARENT PROPERTIES
  Parent Clock:
    Parent Clock Identity: 0x0:11:1:FF:FE:0:0:1
    Parent Port Number: 1
    Observed Parent Offset (log variance): 16640
    Observed Parent Clock Phase Change Rate: N/A

  Grandmaster Clock:
    Grandmaster Clock Identity: 0x0:11:1:FF:FE:0:0:1      <<Grandmaster
clock identity to which the device is synced to>>
    Grandmaster Clock Quality:
      Class: 6
      Accuracy: Within 25ns
      Offset (log variance): 0
      Priority1: 128
      Priority2: 128

```

show platform software fed switch active ptp domain 0

遅延要求メカニズムを使用して境界モードで設定されたデバイスのグランドマスタークロックに対するローカルサーボ PTP クロックの同期を確認するには、**show platform software fed switch active ptp domain 0** コマンドを使用します。

```

Device# show platform software fed switch active ptp domain 0

Displaying data for domain number 0
=====

Profile Type : DEFAULT
Profile State: enabled
Clock Mode : BOUNDARY CLOCK
Delay mechanism: End-to-End

```

```
PTP clock : 2017-6-28 5:58:59
Transport Method: L2 Ethernet
```

デフォルトでは、デバイスが PTP グランドマスタークロックに同期されていない場合、ローカルの PTP クロックは EPOCH 時間 (1970 年 1 月 1 日) を表示します。

例

show ptp port interface *interface-name*

PTP ポートの状態を確認するには、**show ptp port interface** *interface-name* コマンドを使用します。

すべてのインターフェイスの PTP ポートの状態を確認するには、**show ptp brief** コマンドを使用します。

次に、遅延要求メカニズムを使用した境界モード設定の出力例を示します。

```
Device# show ptp port FortyGigabitEthernet1/0/10
PTP PORT DATASET: FortyGigabitEthernet1/0/10
Port identity: clock identity: 0x0:A3:D1:FF:FE:5A:12:0
Port identity: port number: 10
PTP version: 2
Port state: SLAVE
Delay request interval(log mean): 0
Announce receipt time out: 3
Announce interval(log mean): 1
Sync interval(log mean): 0
Delay Mechanism: End to End
    << PTP mode delay >>
Peer delay request interval(log mean): 0
Sync fault limit: 500000000
```

show ptp parent

境界モードでデバイスが同期されているグランドマスタークロック ID を特定するには、**show ptp parent** コマンドを使用します。



-
- (注) **show ptp parent** は、デバイスがトランスペアレント クロック モードに設定されている場合、出力を表示しません。
-

次に、**show ptp parent** コマンドの出力例を示します。

```
Device# show ptp parent
PTP PARENT PROPERTIES
Parent Clock:
Parent Clock Identity: 0x38:E:4D:FF:FE:81:FE:29
<< Immediate next Master >>
Parent Port Number: 196
Observed Parent Offset (log variance): 17258
Observed Parent Clock Phase Change Rate: N/A
```

```

Grandmaster Clock:
Grandmaster Clock Identity: 0x0:0:0:5:0:0:0:1
<< GM: External Clock Source acting Grand Master >>
Grandmaster Clock Quality:
  Class: 6
  Accuracy: Within 1us
  Offset (log variance): 0
  Priority1: 128
  Priority2: 128

```

show platform software fed switch active ptp domain 0

遅延要求メカニズムを使用して境界モードで設定されたデバイスのグランドマスタークロックに対するローカルサーボ PTP クロックの同期を確認するには、**show platform software fed switch active ptp domain 0** コマンドを使用します。

```

Device# show platform software fed switch active ptp domain 0
Displaying data for domain number 0
=====

Profile Type : DEFAULT
Profile State: enabled
Clock Mode : BOUNDARY CLOCK
Delay Mechanism: : END-TO-END
PTP clock : 2017-12-15 15:27:27
mean_path_delay 214 nanoseconds
Transport Method : udp-ipv4                                << PTP Transport Method
>>

```

表 15: debug コマンド

コマンド	目的
debug ptp messages	PTP メッセージのデバッグをイネーブルにします。
debug ptp error	PTP エラーのデバッグをイネーブルにします。
debug ptp bmc	PTP ベストマスタークロックアルゴリズムのデバッグをイネーブルにします。
debug ptp event	PTP ステート イベントのデバッグをイネーブルにします。

PTP の機能の履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Fuji 16.8.1a	IEEE 1588v2 高精度時間プロトコル (PTP) のサポート	PTP は、精度と安定性が異なる分散デバイスクロックを含むパケットベースのネットワークでクロックを同期させるために開発されました。 レイヤ 2 ポートでの PTP のサポートが導入されました。 この機能のサポートは、Cisco Catalyst 9300 シリーズスイッチの 9300 スイッチモデルでのみサポートされるようになりました。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> [英語] からアクセスします。



第 6 章

Generalized Precision Time Protocol の設定

- [Generalized Precision Time Protocol について](#) (157 ページ)
- [Generalized Precision Time Protocol の設定方法](#) (158 ページ)
- [Generalized Precision Time Protocol のモニタリング](#) (160 ページ)
- [例 : Generalized Precision Time Protocol の確認](#) (160 ページ)
- [Generalized Precision Time Protocol の機能履歴](#) (163 ページ)

Generalized Precision Time Protocol について

Generalized Precision Time Protocol (PTP) は IEEE 802.1AS 標準規格で、ネットワーク内でブリッジとエンドポイントデバイスのクロックを同期する機能を提供します。Generalized PTP では、時間認識ブリッジと送話者およびリスナー間でグランドマスタークロック (ベストマスタークロック アルゴリズム (BMCA) を使用) を選択するメカニズムが定義されます。グランドマスターは、時間認識ネットワークで確立され、下位のノードに時間を分散して同期を可能にする時間階層のルートです。

時刻同期には、ネットワーク ノードでのリンク遅延とスイッチ遅延の測定も必要です。Generalized PTP スイッチは IEEE 1588 境界クロックであり、ピアツーピア遅延機能を使用してリンク遅延の測定も行います。計算された遅延は PTP メッセージの修正フィールドに追加され、エンドポイントに伝えられます。送話者とリスナーはこの Generalized PTP 時刻を共有クロック基準として使用し、この時刻はメディアクロックを中継して回復するために使用されます。Generalized PTP は現在、Generalized PTP スイッチがサポートするドメイン 0 のみを定義しています。

ピアツーピア遅延メカニズムは、スパニングツリープロトコルでブロックされた (STP ブロックされた) ポートでも実行されます。他の PTP メッセージはブロックされたポート上で送信されません。

PTP ドメインでは、BMCA がクロックとポートを階層型方式 (クロックとポートの状態が含まれています) に編成します。

クロック

- グランドマスター (GM または GMC)
- 境界クロック (BC)

ポート ステート

- マスタ (M)
- スレーブ (S)
- パッシブ (P)

Generalized Precision Time Protocol の設定方法

この項では、Generalized PTP で使用可能なさまざまな設定について説明します。

Generalized Precision Time Protocol のイネーブル化

デバイスで Generalized PTP を有効化するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 プロンプトが表示されたらパスワードを入力します。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	[no]ptp profile dot1as 例： Device(config)# ptp profile dot1as	Generalized PTP はグローバルに有効化されます。Generalized PTP をグローバルに無効化するには、このコマンドの no 形式を使用します。
ステップ 4	end 例： Device(config)# end	特権 EXEC モードに戻ります。

インターフェイスでの Generalized Precision Time Protocol の有効化

インターフェイスで Generalized PTP を有効化するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 プロンプトが表示されたらパスワードを入力します。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	interface interface-id 例： Device(config)# interface tel1/1/1	トランクとして設定するインターフェイスを定義し、インターフェイスコンフィギュレーション モードを開始します。 指定するインターフェイスは、EtherChannel の一部にすることができます。
ステップ 4	ptp enable 例： Device(config-if)# ptp enable	すべてのインターフェイスで Generalized PTP を有効化します。 Generalized PTP をポートで無効化するには、このコマンドの no 形式を使用します。 Device(config-if)# no ptp enable
ステップ 5	end 例： Device(config-if)# end	特権 EXEC モードに戻ります。

Precision Time Protocol のクロック値の設定

PTP クロックの値（優先順位 1 および優先順位 2）を設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 プロンプトが表示されたらパスワードを入力します。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	ptp priority1 value 例： Device(config)# ptp priority1 120	PTP クロックの優先順位 1 の値を設定します。有効な範囲は 0 ~ 255 です。デフォルト値は 128 です。 (注) 優先順位 1 の値が 255 に設定されると、クロックはグランドマスターとは見なされません。
ステップ 4	ptp priority2 value 例： Device(config)# ptp priority2 120	PTP クロックの優先順位 2 の値を設定します。有効な範囲は 0 ~ 255 です。デフォルト値は 128 です。
ステップ 5	exit 例： Device(config)# exit	グローバル コンフィギュレーション モードに戻ります。

Generalized Precision Time Protocol のモニタリング

Generalized PTP をモニタリングするには、特権 EXEC モードで次のコマンドを使用します。

表 16: Generalized Precision Time Protocol をモニタリングするコマンド

コマンド	目的
show ptp brief	すべてのインターフェイスの PTP の簡易ステータスを表示します。
show ptp clock	PTP クロック情報を表示します。
show ptp parent	親クロックの情報を表示します。
show ptp port	PTP ポート情報を表示します。
show platform software fed switch active ptp if-id {interface-id}	ポートの PTP ステータスに関する詳細情報を表示します。

例 : Generalized Precision Time Protocol の確認

次に、**show ptp brief** コマンドの出力例を示します。

```

Device# show ptp brief
Interface                               Domain    PTP State
FortyGigabitEthernet1/1/1              0        FAULTY
FortyGigabitEthernet1/1/2              0        SLAVE
GigabitEthernet1/1/1                   0        FAULTY
GigabitEthernet1/1/2                   0        FAULTY
GigabitEthernet1/1/3                   0        FAULTY
GigabitEthernet1/1/4                   0        FAULTY
TenGigabitEthernet1/0/1                 0        FAULTY
TenGigabitEthernet1/0/2                 0        FAULTY
TenGigabitEthernet1/0/3                 0        MASTER
TenGigabitEthernet1/0/4                 0        FAULTY
TenGigabitEthernet1/0/5                 0        FAULTY
TenGigabitEthernet1/0/6                 0        FAULTY
TenGigabitEthernet1/0/7                 0        MASTER
TenGigabitEthernet1/0/8                 0        FAULTY
TenGigabitEthernet1/0/9                 0        FAULTY
TenGigabitEthernet1/0/10                0        FAULTY
TenGigabitEthernet1/0/11                0        MASTER
TenGigabitEthernet1/0/12                0        FAULTY
TenGigabitEthernet1/0/13                0        FAULTY
TenGigabitEthernet1/0/14                0        FAULTY
TenGigabitEthernet1/0/15                0        FAULTY
TenGigabitEthernet1/0/16                0        FAULTY
TenGigabitEthernet1/0/17                0        FAULTY
TenGigabitEthernet1/0/18                0        FAULTY
TenGigabitEthernet1/0/19                0        MASTER
TenGigabitEthernet1/0/20                0        FAULTY
TenGigabitEthernet1/0/21                0        FAULTY
TenGigabitEthernet1/0/22                0        FAULTY
TenGigabitEthernet1/0/23                0        FAULTY
TenGigabitEthernet1/0/24                0        FAULTY
TenGigabitEthernet1/1/1                 0        FAULTY
TenGigabitEthernet1/1/2                 0        FAULTY
TenGigabitEthernet1/1/3                 0        FAULTY
TenGigabitEthernet1/1/4                 0        FAULTY
TenGigabitEthernet1/1/5                 0        FAULTY
TenGigabitEthernet1/1/6                 0        FAULTY
TenGigabitEthernet1/1/7                 0        FAULTY
TenGigabitEthernet1/1/8                 0        FAULTY

```

次に、**show ptp clock** コマンドの出力例を示します。

```

Device# show ptp clock
PTP CLOCK INFO
  PTP Device Type: Boundary clock
  PTP Device Profile: IEEE 802/1AS Profile
  Clock Identity: 0x4:6C:9D:FF:FE:4F:95:0
  Clock Domain: 0
  Number of PTP ports: 38
  PTP Packet priority: 4
  Priority1: 128
  Priority2: 128
  Clock Quality:
    Class: 248
    Accuracy: Unknown
    Offset (log variance): 16640
  Offset From Master(ns): 0
  Mean Path Delay(ns): 0
  Steps Removed: 3
  Local clock time: 00:12:13 UTC Jan 1 1970

```

次に、**show ptp parent** コマンドの出力例を示します。

```

Device# show ptp parent
PTP PARENT PROPERTIES
  Parent Clock:
  Parent Clock Identity: 0xB0:7D:47:FF:FE:9E:B6:80
  Parent Port Number: 3
  Observed Parent Offset (log variance): 16640
  Observed Parent Clock Phase Change Rate: N/A

  Grandmaster Clock:
  Grandmaster Clock Identity: 0x4:6C:9D:FF:FE:67:3A:80
  Grandmaster Clock Quality:
    Class: 248
    Accuracy: Unknown
    Offset (log variance): 16640
    Priority1: 0
    Priority2: 128

```

次に、**show ptp port** コマンドの出力例を示します。

```

Device# show ptp port
PTP PORT DATASET: FortyGigabitEthernet1/1/1
  Port identity: clock identity: 0x4:6C:9D:FF:FE:4E:3A:80
  Port identity: port number: 1
  PTP version: 2
  Port state: FAULTY
  Delay request interval(log mean): 5
  Announce receipt time out: 3
  Peer mean path delay(ns): 0
  Announce interval(log mean): 1
  Sync interval(log mean): 0
  Delay Mechanism: End to End
  Peer delay request interval(log mean): 0
  Sync fault limit: 500000000

PTP PORT DATASET: FortyGigabitEthernet1/1/2
  Port identity: clock identity: 0x4:6C:9D:FF:FE:4E:3A:80
  Port identity: port number: 2
  PTP version: 2
  Port state: FAULTY
  Delay request interval(log mean): 5
  Announce receipt time out: 3
  Peer mean path delay(ns): 0
  Announce interval(log mean): 1
--More--

```

次に、インターフェイス用の **show ptp port** コマンドの出力例を示します。

```

Device# show ptp port gi1/0/26
PTP PORT DATASET: GigabitEthernet1/0/26
  Port identity: clock identity: 0x4:6C:9D:FF:FE:4E:3A:80
  Port identity: port number: 28
  PTP version: 2
  Port state: MASTER
  Delay request interval(log mean): 5
  Announce receipt time out: 3
  Peer mean path delay(ns): 0
  Announce interval(log mean): 1
  Sync interval(log mean): 0
  Delay Mechanism: Peer to Peer
  Peer delay request interval(log mean): 0
  Sync fault limit: 500000000

```

次に、インターフェイス用の **show platform software fed switch active ptp if-id** コマンドの出力例を示します。


```

Device# show platform software fed switch active ptp if-id 0x20
Displaying port data for if_id 20
=====

Port Mac Address 04:6C:9D:4E:3A:9A
Port Clock Identity 04:6C:9D:FF:FE:4E:3A:80
Port number 28
PTP Version 2
domain_value 0
dotlas capable: FALSE
sync_recpt_timeout_time_interval 375000000 nanoseconds
sync_interval 125000000 nanoseconds
neighbor_rate_ratio 0.000000
neighbor_prop_delay 0 nanoseconds
compute_neighbor_rate_ratio: TRUE
compute_neighbor_prop_delay: TRUE
port_enabled: TRUE
ptt_port_enabled: TRUE
current_log_pdelay_req_interval 0
pdelay_req_interval 0 nanoseconds
allowed_lost_responses 3
neighbor_prop_delay_threshold 2000 nanoseconds
is_measuring_delay : FALSE
Port state: : MASTER
sync_seq_num 22023
delay_req_seq_num 23857
num sync messages transmitted 0
num sync messages received 0
num followup messages transmitted 0
num followup messages received 0
num pdelay requests transmitted 285695
num pdelay requests received 0
num pdelay responses transmitted 0
num pdelay responses received 0
num pdelay followup responses transmitted 0
num pdelay followup responses received 0

```

Generalized Precision Time Protocol の機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Fuji 16.8.1a	Generalized Precision Time Protocol	Generalized Precision Time Protocol は IEEE 802.1AS 標準規格で、ネットワーク内でブリッジとエンドポイントデバイスのクロックを同期する機能を提供します。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> [英語] からアクセスします。



第 7 章

Resilient Ethernet Protocol の設定

- [Resilient Ethernet Protocol について \(165 ページ\)](#)
- [Resilient Ethernet Protocol の設定方法 \(171 ページ\)](#)
- [Resilient Ethernet Protocol 設定のモニタリング \(182 ページ\)](#)
- [Resilient Ethernet Protocol に関する追加情報 \(183 ページ\)](#)
- [Resilient Ethernet Protocol の機能履歴 \(183 ページ\)](#)

Resilient Ethernet Protocol について

Resilient Ethernet Protocol (REP) はシスコ独自のプロトコルで、スパンニングツリープロトコル (STP) に代わるプロトコルとして、ネットワークループの制御、リンク障害の処理、コンバージェンス時間の改善を実現します。REP は、セグメントに接続されているポートのグループを制御することで、セグメントがブリッジンググループを作成するのを防ぎ、セグメント内のリンク障害に応答します。REP は、より複雑なネットワークを構築するための基盤を提供し、VLAN ロード バランシングをサポートします。



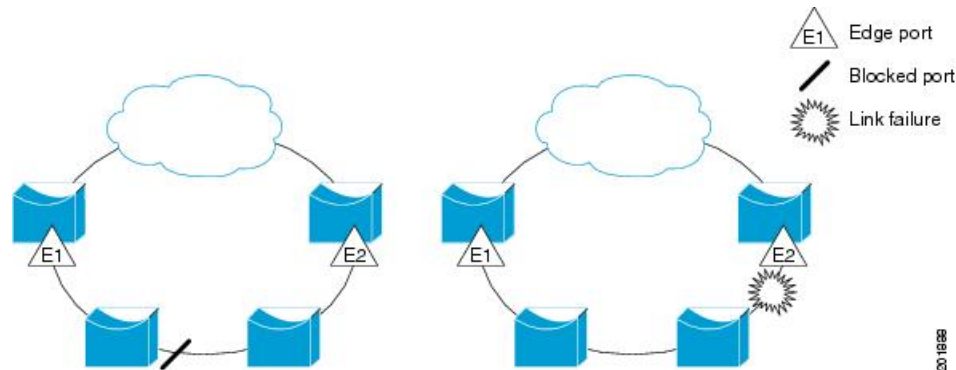
- (注) この機能は、Network Essentials ライセンスを実行している Cisco Catalyst シリーズ スイッチでサポートされています。

REP セグメントは、相互接続されたポートのチェーンで、セグメント ID が設定されます。各セグメントは、標準 (非エッジ) セグメントポートと、2つのユーザー設定エッジポートで構成されています。1 スイッチに、同じセグメントに属することができるポートは2つまでで、各セグメントポートにある外部ネイバーは1つだけです。セグメントは共有メディアを経由できますが、どのリンクでも同じセグメントに属することができるポートは2つだけです。REP は、トランクポートでのみサポートされます。

次の図に、4つのスイッチにまたがる6つのポートで構成されているセグメントの例を示します。ポート E1 および E2 がエッジポートとして設定されています。(左側のセグメントのように) すべてのポートが動作可能な場合、斜線で表しているように単一ポートがブロックされます。ブロックされたポートは、代替ポート (ALTポート) とも呼ばれます。ネットワークに

障害が発生した場合、ブロックされたポートがフォワーディングステートに戻り、ネットワークの中断を最小限に抑えます。

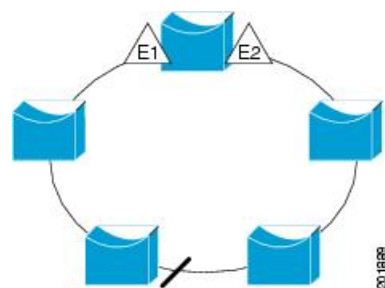
図 25: REP オープンセグメント



上の図に示されたセグメントは、オープンセグメントで、2つのエッジポート間は接続されていません。REP セグメントはブリッジンググループの原因とならないため、セグメントエッジを安全に任意のネットワークに接続できます。セグメント内のスイッチに接続されているすべてのホストには、エッジポートを通じて残りのネットワークに接続する方法が2つありますが、いつでもアクセス可能なのは1つだけです。いずれかのセグメントまたは REP セグメントのいずれかのポートに障害が発生した場合、REP はすべての ALT ポートのブロックを解除し、他のゲートウェイ経路で接続できるようにします。

下に示すセグメントはリングセグメントとも呼ばれる閉じたセグメントであり、同じルータ上に両方のエッジポートがあります。この設定を使用すると、セグメント内の任意の2ルータ間で冗長接続を形成することができます。

図 26: REP リングセグメント



REP セグメントには、次のような特徴があります。

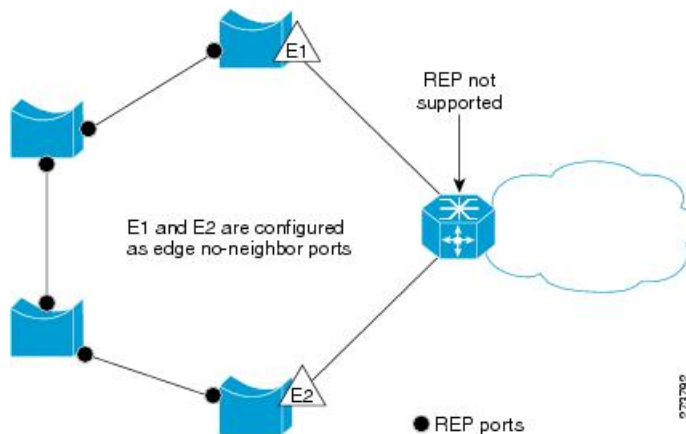
- セグメント内の全ポートが動作可能な場合、1ポート（ALTポートと呼ばれる）が各VLANでブロック状態となります。VLANロードバランシングが設定されている場合は、セグメント内の2つのALTポートがVLANのブロック状態を制御します。
- ポートが動作不能になり、リンク障害が発生すると、すべてのポートがすべてのVLANトラフィックを転送して、接続性を確保します。

- リンク障害の場合、できるだけ早期に代替ポートのブロックが解除されます。障害リンクが復旧すると、ネットワークの中断を最小限に抑えるように VLAN 単位で論理的にブロックされたポートが選択されます。

REP セグメントに基づいて、ほとんどのネットワーク タイプを構成することができます。

アクセスリングトポロジでは、下の図に示すように、ネイバースイッチで REP がサポートされない場合があります。この場合、そのスイッチ側のポート (E1 と E2) を非ネイバリエッジポートとして設定できます。非ネイバリエッジポートは、STP トポロジ変更通知 (TCN) をアグリゲーションスイッチに送信するように設定できます。

図 27: 非ネイバリエッジポート



REP には次のような制限事項があります。

- 各セグメント ポートを設定する必要があります。設定を間違えると、ネットワーク内でフォワーディングループが発生します。
- REP はセグメント内の単一障害ポートだけを管理できます。REP セグメント内の複数ポート障害の場合、ネットワークの接続が中断します。
- 冗長ネットワーク内だけに REP を設定します。冗長性のないネットワークに REP を設定すると、接続が失われます。

リンク完全性

REP は、リンク完全性の確認にエッジポート間でエンドツーエンドポーリング機能を使用しません。ローカルリンク障害検出を実装しています。REP リンクステータスレイヤ (LSL) が REP 対応ネイバリエッジポートを検出して、セグメント内の接続性を確立します。ネイバリエッジポートが検出されるまで、インターフェイス上ですべての VLAN がブロックされます。ネイバリエッジポートが特定されたあと、REP が代替ポートとなるネイバリエッジポートと、トラフィックを転送するポートを決定します。

セグメント内のポートごとに、一意のポート ID が割り当てられます。ポート ID フォーマットは、スパニングツリアルゴリズムで使用されるものと類似しており、ポート番号 (ブリッジ

上で一意)と、関連 MAC アドレス (ネットワーク内で一意) から構成されます。セグメントポートが起動すると、ポートの LSL がセグメント ID およびポート ID を含むパケットの送信を開始します。ポートは、同じセグメント内のネイバーとのスリーウェイハンドシェイクを実行したあとで、動作可能と宣言されます。

次のような場合、セグメントポートは動作可能になりません。

- ネイバーに同じセグメント ID がない
- 複数のネイバーに同じセグメント ID がある
- ネイバーがピアとして、ローカルポートに確認応答しない

各ポートは、直近のネイバーと隣接関係を確立します。ネイバーとの隣接関係が確立されると、代替ポートとして機能する、セグメントのブロックされたポートを決定するようにポートが相互にネゴシエートします。その他のすべてのポートのブロックは解除されます。デフォルトでは、REP パケットはブリッジプロトコルデータユニットクラスの MAC アドレスに送信されます。パケットは、シスコマルチキャストアドレスにも送信できますが、セグメントに障害が発生した場合にブロックされたポートのアドバタイズ (BPA) メッセージの送信だけに使用されます。パケットは、REP が動作していない装置によって廃棄されます。

高速コンバージェンス

REP は、物理リンク ベースで動作し、VLAN 単位ベースでは動作しません。すべての VLAN に対して 1 つの hello メッセージしか必要ないため、プロトコル上の負荷が軽減されます。指定セグメント内の全スイッチで継続的に VLAN を作成し、REP トランク ポート上に同じ許容 VLAN を設定することを推奨します。ソフトウェアでのメッセージのリレーによって発生する遅延を回避するために、REP ではいくつかのパケットを通常マルチキャストアドレスにフラッドすることも可能です。これらのメッセージはハードウェアフラッドレイヤ (HFL) で動作し、REP セグメントだけでなくネットワーク全体にフラッドされます。セグメントに属していないスイッチは、これらのメッセージをデータトラフィックとして扱います。ドメイン全体または特定のセグメントの管理 VLAN を設定することで、これらのメッセージのフラッドを制御することができます。

VLAN ロード バランシング

REP セグメント内の 1 つのエッジポートがプライマリ エッジポートとして機能し、もう一方がセカンダリ エッジポートとなります。セグメント内の VLAN ロード バランシングに常に参加しているのがプライマリ エッジポートです。REP VLAN バランシングは、設定された代替ポートでいくつかの VLAN をブロックし、プライマリ エッジポートでその他の全 VLAN をブロックすることで実行されます。VLAN ロード バランシングを設定する際に、次の 3 種類の方法のいずれかを使用して代替ポートを指定できます。

- インターフェイスにポート ID を入力します。セグメント内のポート ID を識別するには、ポートの **show interface rep detail** インターフェイス コンフィギュレーション コマンドを入力します。

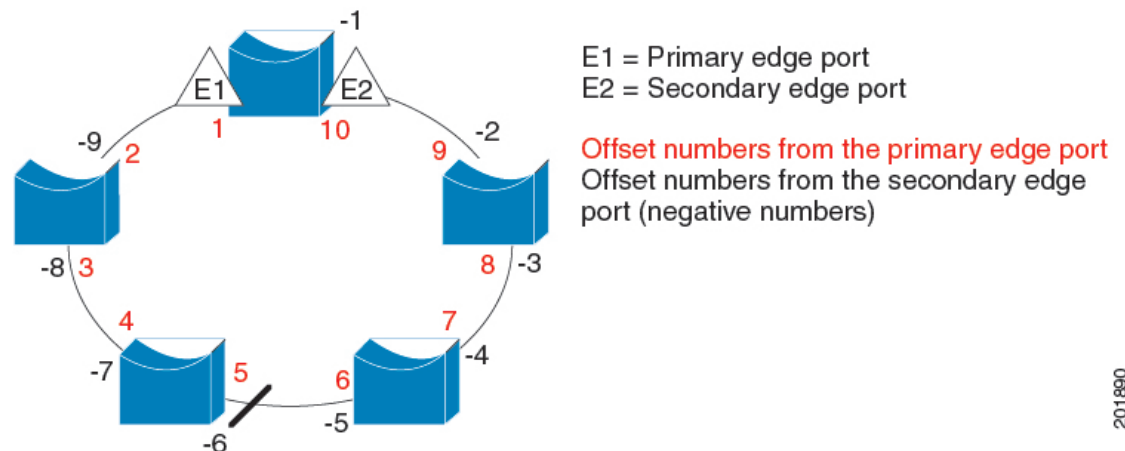
- **preferred** キーワードを入力します。これにより、**rep segment segment-id preferred** インターフェイス コンフィギュレーション コマンドで優先代替ポートとしてすでに設定されているポートを選択します。
- セグメント内のポートのネイバー オフセット番号を入力します。これは、エッジポートのダウンストリーム ネイバー ポートを識別するものです。ネイバー オフセット番号の範囲は、-256 ~ +256 で、0 値は無効です。プライマリ エッジポートはオフセット番号 1 です。1 を超える正数はプライマリ エッジポートのダウンストリーム ネイバーを識別します。負数は、セカンダリ エッジポート (オフセット番号 -1) とそのダウンストリーム ネイバーを示します。



(注) プライマリ (またはセカンダリ) エッジポートからポートのダウンストリーム位置を識別することで、プライマリ エッジポートのオフセット番号を設定します。番号 1 はプライマリ エッジポートのオフセット番号なので、オフセット番号 1 は入力しないでください。

次の図に、E1 がプライマリ エッジポートで E2 がセカンダリ エッジポートの場合の、セグメントのネイバーオフセット番号を示します。リングの内側にある赤い番号は、プライマリ エッジポートからのオフセット番号で、リングの外側にある黒い番号がセカンダリ エッジポートからのオフセット番号です。正のオフセット番号 (プライマリ エッジポートからのダウンストリーム位置) または負のオフセット番号 (セカンダリ エッジポートからのダウンストリーム位置) のいずれかにより、(プライマリ エッジポートを除く) 全ポートを識別できます。E2 がプライマリ エッジポートになるとオフセット番号 1 となり、E1 のオフセット番号が -1 になります。

図 28: セグメント内のネイバー オフセット番号



REP セグメントが完了すると、すべての VLAN がブロックされます。VLAN ロード バランシングを設定する際には、次の 2 種類の方法のいずれかを使用してトリガーを設定する必要があります。

- プライマリ エッジポートのあるスイッチ上で **rep preempt segment segment-id** 特権 EXEC コマンドを入力することで、いつでも手動で VLAN ロード バランシングをトリガーすることができます。
- **rep preempt delay seconds** インターフェイス コンフィギュレーション コマンドを入力すると、プリエンプション遅延時間を設定できます。リンク障害が発生して回復すると、設定されたプリエンプション期間の経過後に VLAN ロード バランシングが開始されます。設定時間が経過する前に別のポートで障害が発生した場合、遅延タイマーが再開されることに注意してください。



(注) VLAN ロード バランシングが設定されている場合、手動での介入またはリンク障害および回復によってトリガーされるまで、動作が開始されません。

VLAN ロード バランシングがトリガーされると、プライマリ エッジポートがメッセージを送信して、セグメント内の全インターフェイスにプリエンプションについて警告します。メッセージがセカンダリポートで受信されると、メッセージがネットワークに送信され、メッセージ内で指定された VLAN セットをブロックするように代替ポートに通知し、残りの VLAN をブロックするようにプライマリ エッジポートに通知します。

またすべての VLAN をブロックするために、セグメント内の特定ポートを設定できます。プライマリ エッジポートだけによって VLAN ロード バランシングが開始され、セグメントが各エッジポートによって終端されていない場合開始することができません。プライマリ エッジポートは、ローカル VLAN ロード バランシング設定を決定します。

ロード バランシングを再設定するには、プライマリ エッジポートを再設定します。ロード バランシング設定を変更すると、プライマリ エッジポートでは、**rep preempt segment** コマンドが実行されるか、ポート障害および復旧のあとで設定済みプリエンプト遅延期間が経過してから、新規設定が実行されます。エッジポートを通常セグメントポートに変更しても、既存の VLAN ロード バランシング ステータスは変更されません。新規エッジポートを設定すると、新規トポロジ設定になる可能性があります。

スパニングツリー インタラクション

REP は STP とやり取りしませんが、共存はできます。セグメントに属しているポートはスパニングツリーの制御から削除されるため、セグメントポートでは STP BPDU の送受信は行われません。したがって、STP はセグメント上で実行できません。

STP リング コンフィギュレーションから REP セグメント コンフィギュレーションに移行するには、まずリング内の単一ポートをセグメントの一部として設定し、次にセグメント数を最小限にするように隣接するポートを設定します。各セグメントには、常にブロックされたポートが含まれているので、セグメントが複数になるとブロックされたポートも複数になり、接続が失われる可能性があります。セグメントがエッジポートの場所まで両方向に設定されたら、次にエッジポートを設定します。

Resilient Ethernet Protocol ポート

REP セグメントは、障害ポート、オープンポート、および代替ポートで構成されます。

- 標準セグメントポートとして設定されたポートは、障害ポートとして起動します。
- ネイバーとの隣接関係が確立されると、ポートは代替ポートステートに移行して、インターフェイス内の全 VLAN をブロックします。ブロックされたポートのネゴシエーションが実施され、セグメントが安定すると、1つのブロックされたポートが代替ロールに留まり、他のすべてのポートがオープンポートになります。
- リンク内で障害が発生すると、すべてのポートが障害ステートに遷移します。代替ポートは、障害通知を受信すると、すべてのVLANを転送するオープンステートに遷移します。

通常セグメントポートをエッジポートに変換しても、エッジポートを通常セグメントポートに変換しても、必ずトポロジ変更が発生するわけではありません。エッジポートを通常セグメントポートに変更する場合、設定されるまで VLAN ロード バランシングは実装されません。VLAN ロード バランシングの場合、セグメント内に2つのエッジポートを設定する必要があります。

スパニングツリーポートとして再設定されたセグメントポートは、スパニングツリー設定に従って再起動します。デフォルトでは、これは指定ブロッキングポートです。PortFast が設定されていたり、STP がディセーブルの場合、ポートはフォワーディングステートになります。

Resilient Ethernet Protocol の設定方法

セグメントは、チェーンで相互接続されているポートの集合で、セグメント ID が設定されています。REPセグメントを設定するには、REP管理VLANを設定し（またはデフォルトVLAN 1を使用し）、次にインターフェイスコンフィギュレーションモードを使用してセグメントにポートを追加します。2つのエッジポートをセグメント内に設定して、デフォルトで1つをプライマリエッジポート、もう1つをセカンダリエッジポートにします。1セグメント内のプライマリエッジポートは1つだけです。別のスイッチのポートなど、セグメント内で2つのポートをプライマリエッジポートに設定すると、REPがそのうちのいずれかを選択してセグメントのプライマリエッジポートとして機能させます。必要に応じて、STCN および VLAN ロード バランシングが送信される場所を設定できます。

Resilient Ethernet Protocol のデフォルトの設定

REPはすべてのインターフェイス上でディセーブルです。イネーブルにする際に、エッジポートとして設定されていない場合はインターフェイスは通常セグメントポートになります。

REPをイネーブルにする際に、STCNの送信タスクはディセーブルで、すべてのVLANはブロックされ、管理VLANはVLAN 1になります。

VLANロードバランシングがイネーブルの場合、デフォルトは手動でのプリエンプションで、遅延タイマーはディセーブルになっています。VLANロードバランシングが設定されていない

い場合、手動でのプリエンプション後のデフォルト動作は、プライマリ エッジ ポートで全 VLAN がブロックとなります。

Resilient Ethernet Protocol の構成ガイドライン

REP の設定時には、次の注意事項に従ってください。

- REP は、10 ギガビット イーサネット インターフェイスでサポートされます。
- まず1 ポートの設定から始めて、セグメント数とブロックされたポートの数を最小限に抑えるように隣接するポートを設定することを推奨します。
- 外部ネイバーが設定されておらずセグメント内では3つ以上のポートに障害が発生した場合、1ポートがデータパス用のフォワーディングステートになり、設定中の接続性の維持に役立ちます。 **show rep interface** コマンド出力では、このポートのポートロールは「Fail Logical Open」と表示され、他の障害ポートのポートロールは「Fail No Ext Neighbor」と表示されます。障害ポートの外部ネイバーが設定されている場合、ポートは代替ポートステートに移行して、代替ポート選択メカニズムに基づいて最終的にオープンステートになるか、代替ポートのままになります。
- REP ポートは、レイヤ 2 IEEE 802.1Q またはトランク ポートのいずれかである必要があります。
- 同じ許可 VLAN のセットでセグメント内のすべてのトランク ポートを設定することを推奨します。
- Telnet 接続を通じて REP を設定する際には注意してください。これは、別の REP インターフェイスがブロック解除のメッセージを送信するまで、REP はすべての VLAN をブロックするためです。同じインターフェイス経由でルータにアクセスする Telnet セッションで REP をイネーブルにすると、ルータへの接続が失われることがあります。
- 同じセグメントやインターフェイスで REP と STP を実行することはできません。
- STP ネットワークを REP セグメントに接続する場合、接続はセグメント エッジであることを確認してください。エッジで実行されていない STP 接続は、REP セグメントでは STP が実行されないため、ブリッジング ループが発生する可能性があります。すべての STP BPDUs は、REP インターフェイスで廃棄されます。
- 同じ許容 VLAN セットでセグメント内のすべてのトランク ポートを設定する必要があります。そうでない場合、設定ミスが発生します。
- REP がスイッチの 2 ポートでイネーブルの場合、両方のポートが通常セグメント ポートまたはエッジ ポートである必要があります。REP ポートは以下の規則に従います。
 - スイッチ上の REP ポートの数に制限はありませんが、同じ REP セグメントに属することができるスイッチ上のポートは 2 つだけです。
 - セグメント内にスイッチ上の 1 ポートだけが設定されている場合、そのポートがエッジ ポートとなります。

- 同じセグメント内に属するスイッチに2つのポートがある場合、両方のポートがエッジポートであるか、両方のポートが通常セグメントポートであるか、一方が通常ポートでもう一方が非ネイバー エッジポートである必要があります。スイッチ上のエッジポートと通常セグメント ポートが同じセグメントに属することはできません。
- スイッチ上の2ポートが同じセグメントに属していて、1つがエッジポートとして設定され、もう1つが通常セグメントポートに設定されている場合（設定ミス）、エッジポートは通常セグメント ポートとして扱われます。
- REP インターフェイスはブロックされた状態になり、ブロック解除できるようになるまでブロックされた状態のまま残ります。突然の接続切断を避けるために、このステータスを認識しておく必要があります。
- REP はネイティブ VLAN 上においてすべての LSL PDU をタグなしフレームで送信します。シスコマルチキャストアドレスに送信された BPA メッセージは、管理 VLAN で送信されます。これはデフォルトで VLAN 1 です。
- ネイバーからの hello が受信されないままどのくらいの時間が経過すると REP インターフェイスがダウンするかを設定できます。 **rep lsl-age-timer** インターフェイス コンフィギュレーション コマンドを使用して、120～10000 ミリ秒の時間を設定します。LSL hello タイマーは、このエイジングタイマーの値を3で割った値に設定されます。通常の動作では、ピアスイッチのエイジングタイマーが満了になって hello メッセージが確認されるまでに LSL hello が3回送信されます。
 - EtherChannel ポート チャンネル インターフェイスでは、1000 ミリ秒未満の LSL エージングタイマー値はサポートされていません。ポート チャンネルで1000 ミリ秒未満の値を設定しようとすると、エラー メッセージが表示されてコマンドが拒否されます。
- REP ポートは、次のポートタイプのいずれかに設定できません。
 - スイッチド ポート アナライザ (SPAN) 宛先ポート
 - トンネル ポート
 - アクセスポート
- REP は EtherChannel でサポートされていますが、EtherChannel に属する個別のポートではサポートされません。
- スイッチごとに最大 64 の REP セグメントを設定できます。

Resilient Ethernet Protocol 管理 VLAN の設定

リンク障害メッセージ、およびロード バランシング時の VLAN ブロッキング通知によって作成される遅延を回避するため、REP はハードウェア フラッド レイヤ (HFL) で通常のマルチキャストアドレスにパケットをフラッディングします。これらのメッセージは REP セグメントだけではなくネットワーク全体にフラッディングされます。管理 VLAN を設定することで、これらのメッセージのフラッディングを制御できます。

REP 管理 VLAN を設定する場合、次の注意事項に従ってください。

- 管理 VLAN を設定しない場合、デフォルトは VLAN 1 です。
- すべてのセグメントに対し 1 つの管理 VLAN をスイッチで設定できます。
- 管理 VLAN は RSPAN VLAN になりません。

REP 管理 VLAN を設定するには、特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	rep admin vlan <i>vlan-id</i> 例： Device(config)# rep admin vlan 2	管理 VLAN を指定します。範囲は 2 ~ 4094 です。 管理 VLAN をデフォルトの 1 に設定するには、 no rep admin vlan グローバル コンフィギュレーション コマンドを入力します。
ステップ 4	end 例： Device(config)# end	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 5	show interface [<i>interface-id</i>] rep detail 例： Device# show interface gigabitethernet1/1 rep detail	（任意）REP インターフェイスの設定を検証します。
ステップ 6	copy running-config startup config 例： Device# copy running-config startup config	（任意）スイッチ スタートアップ コンフィギュレーション ファイルに設定を保存します。

REP インターフェイスの設定

REP を設定する場合、各セグメントインターフェイスで REP をイネーブルにして、セグメント ID を指定します。このタスクは必須で、他の REP 設定の前に実行する必要があります。また、各セグメントにプライマリおよびセカンダリ エッジ ポートを設定する必要があります。それ以外の手順はすべてオプションです。

インターフェイスで REP をイネーブルにし、設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	interface interface-id 例： Device(config)# interface gigabitethernet1/1	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。インターフェイスは物理レイヤ 2 インターフェイスまたはポートチャネル（論理インターフェイス）に設定できます。
ステップ 4	switchport mode trunk 例： Device(config-if)# switchport mode trunk	インターフェイスをレイヤ 2 トランクポートとして設定します。
ステップ 5	rep segment segment-id [edge [no-neighbor] [primary]] [preferred] 例： Device(config-if)# rep segment 1 edge no-neighbor primary	インターフェイス上で REP をイネーブルにして、セグメント番号を特定します。指定できるセグメント ID の範囲は 1 ~ 1024 です。 (注) 各セグメントに 1 つのプライマリ エッジ ポートを含めて、2 つのエッジポートを設定する必要があります。 これらの任意のキーワードは利用可能です。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> • (任意) edge : エッジポートとしてポートを設定します。各セグメントにあるエッジポートは2つだけです。 primary キーワードなしで edge キーワードを入力すると、ポートがセカンダリエッジポートとして設定されます。 • (任意) primary : プライマリエッジポート (VLAN ロードバランシングを設定できるポート) としてポートを設定します。 • (任意) no-neighbor : エッジポートとして外部REPネイバーを使用せずにポートを設定します。ポートはエッジポートのすべてのプロパティを継承し、エッジポートの場合と同様にプロパティを設定できます。 <p>(注) 各セグメントにあるプライマリエッジポートは1つだけですが、2つの異なるスイッチにエッジポートを設定して primary キーワードを両方のスイッチに入力しても、その設定は有効です。ただし、REPではセグメントプライマリエッジポートとして1つのポートだけが選択されます。特権 EXEC モードで show rep topology コマンドを入力すると、セグメントのプライマリエッジポートを特定できます。</p> <ul style="list-style-type: none"> • (任意) preferred : ポートが優先代替ポートであるか、VLAN ロードバランシングの優先ポートであるかを示します。

	コマンドまたはアクション	目的
		<p>(注) ポートを優先に設定しても、代替ポートになるとは限りません。同等に可能性のあるポートよりやや可能性が高くなるだけです。通常、前に障害が発生したポートが、代替ポートとなります。</p>
ステップ 6	<p>rep stcn {interface <i>interface id</i> segment <i>id-list</i> stp}</p> <p>例 :</p> <pre>Device(config-if)# rep stcn segment 25-50</pre>	<p>(任意) STCN を送信するようにエッジポートを設定します。</p> <ul style="list-style-type: none"> • interface <i>interface -id</i> : 物理インターフェイスまたはポートチャネルを指定して、STCN を受け取ります。 • segment <i>id-list</i> : STCN を受け取る 1 つ以上のセグメントを特定します。有効な範囲は 1 ~ 1024 です。 • stp : STCN を STP ネットワークに送信します。 <p>(注) STCN を STP ネットワークに送信するために rep stcn stp コマンドを設定する場合は、スパニング ツリー (MST) モードがネイバーなしのエッジノード上に必要です。</p>
ステップ 7	<p>rep block port {id <i>port-id</i> <i>neighbor-offset</i> preferred} vlan {<i>vlan-list</i> all}</p> <p>例 :</p> <pre>Device(config-if)# rep block port id 0009001818D68700 vlan 1-100</pre>	<p>(任意) プライマリエッジポートに VLAN ロードバランシングを設定して、3 つの方法のいずれかを使用して REP 代替ポートを特定し (id <i>port-id</i>、<i>neighbor_offset</i>、preferred)、代替ポートでブロックされるように VLAN を設定します。</p> <ul style="list-style-type: none"> • id <i>port-id</i> : ポート ID で代替ポートを特定します。セグメント内の各ポートにポート ID が自動的に生成されます。 show interface type number rep [detail] 特権 EXEC コマ

	コマンドまたはアクション	目的
		<p>ンドを入力し、インターフェイスポート ID を表示できます。</p> <ul style="list-style-type: none"> • <i>neighbor_offset</i> : エッジポートからのダウストリームネイバーとして代替ポートを特定するための番号。有効範囲は -256 ~ 256 で、負数はセカンダリエッジポートからのダウストリームネイバーを示します。0 の値が無効です。-1 を入力して、セカンダリエッジポートを代替ポートとして識別します。 <p>(注) プライマリ エッジポート (オフセット番号 1) に rep block port コマンドを入力するので、代替ポートを特定するのにオフセット値 1 を入力できません。</p> <ul style="list-style-type: none"> • preferred : すでに VLAN ロードバランシングの優先代替ポートとして指定されている通常セグメントポートを選択します。 • vlan vlan-list : 1 つの VLAN または VLAN の範囲をブロックします。 • vlan all : すべての VLAN をブロックします。 <p>(注) REP プライマリ エッジポート上にだけこのコマンドを入力します。</p>
ステップ 8	<p>rep preempt delay seconds</p> <p>例 :</p> <pre>Device(config-if)# rep preempt delay 100</pre>	<p>(任意) プリエンプト遅延時間を設定します。</p> <ul style="list-style-type: none"> • リンク障害が発生して復旧した後に、VLAN ロードバランシングを自動的にトリガーするには、このコマンドを使用します。 • 遅延時間の範囲は 15 ~ 300 秒です。デフォルトは、遅延時間のな

	コマンドまたはアクション	目的
		<p>い手動によるプリエンブションです。</p> <p>(注) REP プライマリ エッジポート上にだけこのコマンドを入力します。</p>
ステップ 9	<p>rep lsl-age-timer value</p> <p>例 :</p> <pre>Device(config-if)# rep lsl-age-timer 2000</pre>	<p>(任意) ネイバーからの hello が受信されないままのくらいの時間 (ミリ秒) が経過すると REP インターフェイスがダウンするかを設定します。</p> <p>指定できる範囲は 120 ~ 10000 ミリ秒 (40 ミリ秒単位) です。デフォルト値は 5000 ミリ秒 (5 秒) です。</p> <p>(注)</p> <ul style="list-style-type: none"> • EtherChannel ポートチャンネルインターフェイスでは、1000 ミリ秒未満の LSL エージングタイマー値はサポートされていません。 • リンクのフラップを避けるため、リンクの両方のポートに同じ LSL エージングが設定されている必要があります。
ステップ 10	<p>end</p> <p>例 :</p> <pre>Device(config-if)# end</pre>	<p>グローバル コンフィギュレーションモードを終了し、特権 EXEC モードに戻ります。</p>
ステップ 11	<p>show interface [interface-id] rep [detail]</p> <p>例 :</p> <pre>Device# show interface gigabitethernet1/1 rep detail</pre>	<p>(任意) REP インターフェイスの設定を表示します。</p>
ステップ 12	<p>copy running-config startup-config</p> <p>例 :</p> <pre>Device# copy running-config startup-config</pre>	<p>(任意) スイッチスタートアップコンフィギュレーションファイルに設定を保存します。</p>

VLAN ロード バランシングの手動によるプリエンプションの設定

プライマリエッジポートで **rep preempt delay seconds** インターフェイス コンフィギュレーション コマンドを入力しないで、プリエンプション時間遅延を設定する場合、デフォルトではセグメントで VLAN ロード バランシングを手動でトリガーします。手動で VLAN ロード バランシングをプリエンプトする前に、他のすべてのセグメント設定が完了しているかどうか確認してください。 **rep preempt delay segment segment-id** コマンドを入力すると、プリエンプションによってネットワークが中断する可能性があるため、コマンド実行前に確認メッセージが表示されます。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	rep preempt segment segment-id 例： Device(config)# rep preempt segment 100 The command will cause a momentary traffic disruption. Do you still want to continue? [confirm]	手動により、セグメント上の VLAN ロード バランシングをトリガーします。 実行前にコマンドを確認する必要があります。
ステップ 4	end 例： Device# end	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 5	show rep topology segment segment-id 例： Device# show rep topology segment 100	（任意）REP トポロジの情報を表示します。
ステップ 6	end 例： Device# end	特権 EXEC モードを終了します。

Resilient Ethernet Protocol の簡易ネットワーク管理プロトコルのトラップの構成

REP 固有のトラップを送信して、簡易ネットワーク管理プロトコル (SNMP) サーバーにリンクの動作状態の変更およびすべてのポート役割の変更を通知するようにルータを設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します (要求された場合)。
ステップ 2	configure terminal 例 : Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	snmp mib rep trap-rate value 例 : Device (config)# snmp mib rep trap-rate 500	スイッチで REP トラップの送信をイネーブルにして、1秒あたりのトラップの送信数を設定します。 <ul style="list-style-type: none">1秒あたりのトラップの送信数を入力します。範囲は 0 ~ 1000 です。デフォルトは 0 (制限なし、発生するたびにトラップが送信される) です。
ステップ 4	end 例 : Device (config)# end	特権 EXEC モードに戻ります。
ステップ 5	show running-config 例 : Device# show running-config	(任意) 実行コンフィギュレーションを表示します。これを使用して REP トラップ コンフィギュレーションを検証できます。
ステップ 6	copy running-config startup-config 例 : Device# copy running-config startup-config	(任意) スイッチ スタートアップ コンフィギュレーション ファイルに設定を保存します。

Resilient Ethernet Protocol 設定のモニタリング



(注) ピア側のポートがダウンしている場合、**show rep topology** コマンドはプライマリポートとセカンダリポートの両方をセカンダリポートとして表示します。

次の例では、**show interface [interface-id] rep [detail]** コマンドの出力を示します。この表示では、アップリンクポートの REP 設定とステータスを示します。

```
Device# show interfaces TenGigabitEthernet4/1 rep detail
```

```
TenGigabitEthernet4/1 REP enabled
Segment-id: 3 (Primary Edge)
PortID: 03010015FA66FF80
Preferred flag: No
Operational Link Status: TWO_WAY
Current Key: 02040015FA66FF804050
Port Role: Open
Blocked VLAN: <empty>
Admin-vlan: 1
Preempt Delay Timer: disabled
Configured Load-balancing Block Port: none
Configured Load-balancing Block VLAN: none
STCN Propagate to: none
LSL PDU rx: 999, tx: 652
HFL PDU rx: 0, tx: 0
BPA TLV rx: 500, tx: 4
BPA (STCN, LSL) TLV rx: 0, tx: 0
BPA (STCN, HFL) TLV rx: 0, tx: 0
EPA-ELECTION TLV rx: 6, tx: 5
EPA-COMMAND TLV rx: 0, tx: 0
EPA-INFO TLV rx: 135, tx: 136
```

次の例では、**show interface [interface-id] rep [detail]** コマンドの出力を示します。この表示では、ダウンリンクポートの REP 設定とステータスを示します。

```
Device# show interface TenGigabitEthernet5/0/27 rep detail
```

```
TenGigabitEthernet5/0/27 REP enabled
Segment-id: 1 (Segment)
PortID: 019B380E4D9ACAC0
Preferred flag: No
Operational Link Status: NO_NEIGHBOR
Current Key: 019B380E4D9ACAC0696B
Port Role: Fail No Ext Neighbor
Blocked VLAN: 1-4094
Admin-vlan: 1
Preempt Delay Timer: 100 sec
LSL Ageout Timer: 2000 ms
LSL Ageout Retries: 5
Configured Load-balancing Block Port: 09E9380E4D9ACAC0
Configured Load-balancing Block VLAN: 1-100
STCN Propagate to: segment 25
LSL PDU rx: 292, tx: 340
```

```
HFL PDU rx: 0, tx: 0
BPA TLV rx: 0, tx: 0
BPA (STCN, LSL) TLV rx: 0, tx: 0
BPA (STCN, HFL) TLV rx: 0, tx: 0
EPA-ELECTION TLV rx: 0, tx: 0
EPA-COMMAND TLV rx: 0, tx: 0
EPA-INFO TLV rx: 0, tx: 0
```

次の例では、**show rep topology [segment segment-id] [archive] [detail]** コマンドを示します。この表示では、すべてのセグメントの REP トポロジ情報を示します。

```
Device# show rep topology

REP Segment 1
-----
BridgeName      PortName      Edge Role
-----
10.64.106.63    Te5/4         Pri  Open
10.64.106.228  Te3/4         Open
10.64.106.228  Te3/3         Open
10.64.106.67   Te4/3         Open
10.64.106.67   Te4/4         Alt
10.64.106.63   Te4/4         Sec  Open

REP Segment 3
-----
BridgeName      PortName      Edge Role
-----
10.64.106.63    Gi50/1        Pri  Open
SVT_3400_2      Gi0/3         Open
SVT_3400_2      Gi0/4         Open
10.64.106.68   Gi40/2        Open
10.64.106.68   Gi40/1        Open
10.64.106.63   Gi50/2        Sec  Alt
```

Resilient Ethernet Protocol に関する追加情報

関連資料

関連項目	マニュアル タイトル
REP コマンド	<i>Command Reference (Catalyst 9300 Series Switches)</i> の「Layer 2/3 Commands」の項を参照してください

Resilient Ethernet Protocol の機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Everest 16.5.1a	Resilient Ethernet Protocol	REP はシスコ独自のプロトコルで、STP に代わるプロトコルとして、ネットワークループの制御、リンク障害の処理、コンバージェンス時間の改善を実現します。
Cisco IOS XE Fuji 16.9.1	ダウンリンクポートでの Resilient Ethernet Protocol のサポート	ダウンリンクポートでの REP 設定のサポートが導入されました。
Cisco IOS XE Amsterdam 17.2.1	Resilient Ethernet Protocol 用の複数の管理 VLAN	REP での複数の管理 VLAN 設定のサポートが導入されました。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> [英語] からアクセスします。



第 8 章

単方向リンク検出の設定

- [単方向リンク検出の設定の制限事項 \(185 ページ\)](#)
- [単方向リンク検出の概要 \(185 ページ\)](#)
- [UDLD の設定方法 \(189 ページ\)](#)
- [単方向リンク検出のモニタリングと保守 \(192 ページ\)](#)
- [単方向リンク検出に関するその他の参考資料 \(192 ページ\)](#)
- [単方向リンク検出の機能履歴 \(193 ページ\)](#)

単方向リンク検出の設定の制限事項

次に、単方向リンク検出 (UDLD) 設定の制約事項を示します。

- UDLD 対応ポートが別のデバイスの UDLD 非対応ポートに接続されている場合、このポートは単方向リンクを検出できません。
- モード (通常またはアグレッシブ) を設定する場合、リンクの両側に同じモードを設定します。



注意 ループガードは、ポイントツーポイントリンクでのみサポートされます。リンクの各終端には、STP を実行するデバイスを直接接続することを推奨します。

単方向リンク検出の概要

UniDirectional Link Detection (UDLD) は、光ファイバまたはツイストペアイーサネットケーブルを通して接続されたデバイスからケーブルの物理設定をモニタリングしたり、単方向リンクの存在を検出できるようにするためのレイヤ2プロトコルです。このプロトコルが単方向リンクを正常に識別してディセーブルにするには、接続されたすべてのデバイスで UDLD プロトコルがサポートされている必要があります。UDLD は単方向リンクを検出すると、影響を受けるポートをディセーブルにして警報を発信します。単方向リンクは、スパンニングツリートポロジープをはじめ、さまざまな問題を引き起こす可能性があります。

動作モード

UDLD サポートしています。通常（デフォルト）とアグレッシブです。通常モードの UDLD は、光ファイバ接続におけるポートの誤った接続による単一方向リンクを検出できます。アグレッシブモードの UDLD は、光ファイバリンクおよびツイストペアリンク上の片方向トラフィックと、光ファイバリンク上のポートの誤った接続による単一方向リンクも検出できます。

通常およびアグレッシブの両モードの UDLD は、レイヤ1のメカニズムを使用して、リンクの物理ステータスを学習します。レイヤ1では、物理的シグナリングおよび障害検出は、自動ネゴシエーションによって処理されます。UDLD は、ネイバー ID の検出、誤って接続されたポートのシャットダウンなど、自動ネゴシエーションでは実行不可能な処理を実行します。自動ネゴシエーションと UDLD の両方をイネーブルにすると、レイヤ1と2の検出機能が連動し、物理的および論理的な単一方向接続、および他のプロトコルの誤動作を防止します。

ローカルデバイスが送信したトラフィックをネイバーが受信するにもかかわらず、ネイバーから送信されたトラフィックをローカルデバイスが受信しない場合に、単一方向リンクが発生します。

通常モード

通常モードの UDLD は、光ファイバポートの光ファイバが誤って接続されている場合に単一方向リンクを検出しますが、レイヤ1メカニズムは、この誤った接続を検出しません。ポートが正しく接続されていてもトラフィックが片方向である場合、単一方向リンクを検出するのはレイヤ1メカニズムがこの状況を検出できないため、UDLD は単一方向リンクを検出できません。この場合、論理リンクは不確定と見なされ、UDLD はポートをディセーブルにしません。

UDLD が通常モードのときに、ペアの一方の光ファイバが切断されており、自動ネゴシエーションがアクティブであると、レイヤ1メカニズムがリンクの物理的な問題を検出するため、リンクは稼働状態でなくなります。この場合は、UDLD は何のアクションも行わず、論理リンクは不確定と見なされます。

アグレッシブモード

アグレッシブモードでは、UDLD はこれまでの検出方法で単一方向リンクを検出します。アグレッシブモードの UDLD は、2つのデバイス間の障害発生が許されないポイントツーポイントリンクの単一方向リンクも検出できます。また、次のいずれかの問題が発生している場合に、単一方向リンクも検出できます。

- 光ファイバリンクまたはツイストペアリンクで、ポートの1つがトラフィックを送受信できない。
- 光ファイバリンクまたはツイストペアリンクで、ポートの1つがダウンし、残りのインターフェイスが稼働している。
- ケーブルのうち1本の光ファイバが切断されている。

これらの場合、UDLD は影響を受けたポートをディセーブルにします。

ポイントツーポイントリンクでは、UDLDhello パケットをハートビートと見なすことができ、ハートビートがあればリンクは正常です。逆に、ハートビートがないということは、双方向リンクを再確立できない限り、リンクをシャットダウンする必要があることを意味しています。

レイヤ1の観点からケーブルの両方の光ファイバが正常な状態であれば、アグレッシブモードのUDLDはそれらの光ファイバが正しく接続されているかどうか、およびトラフィックが正しいネイバー間で双方向に流れているかどうかを検出します。自動ネゴシエーションはレイヤ1で動作するため、このチェックは自動ネゴシエーションでは実行できません。

単一方向の検出方法

UDLDは、2つの方法で動作します。

- ネイバー データベース メンテナンス
- イベントドリブン検出およびエコー

ネイバー データベース メンテナンス

UDLDは、アクティブな各ポート上でhello パケット（別名アドバタイズまたはプローブ）を定期的送信して、他のUDLD対応ネイバーに関して学習し、各デバイスがネイバーに関する情報を常に維持できるようにします。

デバイスがhello メッセージを受信すると、エージングタイム（ホールドタイムまたは存続可能時間）が経過するまで、情報をキャッシュします。古いキャッシュエントリの期限が切れる前に、デバイスが新しいhello メッセージを受信すると、デバイスが古いエントリを新しいエントリで置き換えます。

UDLDの実行中にポートがディセーブルになったり、ポート上でUDLDがディセーブルになったり、またはデバイスをリセットした場合、UDLDは設定変更の影響を受けるポートの既存のキャッシュエントリをすべてクリアします。UDLDは、ステータス変更の影響を受けるキャッシュの一部をフラッシュするよう、ネイバーに通知するメッセージを1つまたは複数送信します。このメッセージは、キャッシュを継続的に同期するためのものです。



- (注) インターフェイスは複数のUDLD ネイバーをサポートしません。入力UDLD プロトコルデータユニット (PDU) のエコータイプ、長さ、値 (TLV) に複数のデバイス ID がある場合、インターフェイスはエラーによるオフ状態になります。

イベントドリブン検出およびエコー

UDLDは検出動作としてエコーを利用します。UDLD デバイスが新しいネイバーを学習するか、または同期していないネイバーから再同期要求を受信すると、接続のUDLD デバイス側の検出ウィンドウを再起動して、エコーメッセージを返送します。この動作はすべてのUDLD ネイバーに対して同様に行われるため、エコー送信側では返信エコーを受信するように待機します。

検出ウィンドウが終了し、有効な応答メッセージが受信されなかった場合、リンクは、UDLD モードに応じてシャットダウンされることがあります。UDLD が通常モードにある場合、リンクは不確定と見なされ、シャットダウンされない場合があります。UDLD がアグレッシブモードにある場合は、リンクは単一方向と見なされ、ポートはディセーブルになります。

単方向リンク検出のリセットオプション

インターフェイスが UDLD でディセーブル化された場合、次のオプションの 1 つを使用して UDLD をリセットできます。

- **udld reset** インターフェイス コンフィギュレーション コマンドです。
- **no shutdown** インターフェイス コンフィギュレーション コマンドに続いて **shutdown** インターフェイス コンフィギュレーション コマンドを入力すると、ディセーブル化されたポートを再起動できます。
- **no udld {aggressive | enable}** グローバル コンフィギュレーション コマンドの後に **udld {aggressive | enable}** グローバル コンフィギュレーション コマンドが続くと、無効なポートが再度イネーブルになります。
- **no udld port** インターフェイス コンフィギュレーション コマンドに続いて **udld port [aggressive]** インターフェイス コンフィギュレーション コマンドを入力すると、無効なファイバー オプティック ポートがイネーブルになります。
- **errdisable recovery cause udld** グローバル コンフィギュレーション コマンドを使用すると、UDLD の **errdisable** ステートから自動回復するタイマーをイネーブルにできます。さらに、**errdisable recovery interval interval** グローバル コンフィギュレーション コマンドでは、**udld errdisable** ステートから回復する時間を指定します。

udld port disable コマンドは、光ファイバの LAN ポート上で UDLD をディセーブルにします。



(注) このコマンドは、光ファイバ LAN ポートでのみサポートされています。

単方向リンク検出のデフォルトの設定

表 17: UDLD のデフォルト設定

機能	デフォルト設定
UDLD グローバル イネーブル ステート	グローバルにディセーブル
ポート別の UDLD イネーブル ステート (光ファイバメディア用)	すべてのイーサネット光ファイバ ポート上 で
ポート別の UDLD イネーブルステート (ツイストペア (銅製) メディア用)	すべてのイーサネット 10/100 および 1000BAS 上でディセーブル

機能	デフォルト設定
UDLD アグレッシブ モード	ディセーブル

UDLD の設定方法

ここでは、UDLD の設定について説明します。

単方向リンク検出のグローバルにイネーブル化

アグレッシブモードまたは通常モードで UDLD をイネーブルにし、デバイス上のすべての光ファイバポートに設定可能なメッセージタイマーを設定するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーションモードを開始します。
ステップ 3	udld {aggressive enable message time message-timer-interval} 例： Device(config)# udld enable message time 10	UDLD モードの動作を指定します。 <ul style="list-style-type: none"> • aggressive : すべての光ファイバポートにおいて、アグレッシブモードで UDLD をイネーブルにします。 • enable : デバイス上のすべての光ファイバポート上で、UDLD を通常モードでイネーブルにします。UDLD はデフォルトでディセーブルです。 個々のインターフェイスの設定は、udld enable グローバル コンフィギュレーション コマンドの設定を上書きします。 • message time message-timer-interval : アドバタイズメント フェーズにあり、双方向リンクが検出されたポートでの UDLD プローブ メッセージ

	コマンドまたはアクション	目的
		<p>の時間間隔を設定します。有効な範囲は 1 ～ 90 秒です。デフォルト値は 15 です。</p> <p>(注) このコマンドが作用するのは、光ファイバポートだけです。他のポートタイプで UDLD をイネーブルにする場合は、udld インターフェイス コンフィギュレーション コマンドを使用します。</p> <p>UDLD をディセーブルにするには、このコマンドの no 形式を使用します。</p>
ステップ 4	end 例： Device(config)# end	特権 EXEC モードに戻ります。

インターフェイスでの単方向リンク検出のイネーブル化

アグレッシブ モードまたは通常モードをイネーブルにする、またはポート上で UDLD をディセーブルにするには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	<p>特権 EXEC モードを有効にします。</p> <p>パスワードを入力します（要求された場合）。</p>
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	interface interface-id 例： Device(config)# interface gigabitethernet 1/0/1	UDLD 用にイネーブルにするポートを指定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	udld port [aggressive] 例： Device(config-if)# udld port aggressive	UDLD はデフォルトでディセーブルです。 <ul style="list-style-type: none"> • udld port : 指定されたポート上で、UDLD を通常モードでイネーブルにします。 • udld port aggressive : (任意) 指定されたインターフェイスにおいて、アグレッシブ モードで UDLD をイネーブルにします。 (注) 特定の光ファイバポート上で UDLD をディセーブルにする場合は、 no udld port インターフェイス コンフィギュレーション コマンドを使用します。
ステップ 5	end 例： Device(config-if)# end	特権 EXEC モードに戻ります。

光ファイバ LAN インターフェイスでの単方向リンク検出のディセーブル化

光ファイバ LAN インターフェイス上で UDLD をディセーブルにするには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します (要求された場合)。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	interface <i>type number</i> 例： Device(config)# interface gigabitethernet 0/1/1	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	udld port disable 例： Device(config-if)# udld port disable	光ファイバの LAN ポート上で UDLD をディセーブルにします。 <ul style="list-style-type: none"> • udld port disable コマンドは、光ファイバ LAN ポートでのみサポートされています。 • no udld port disable コマンドを実行すると、udld enable グローバル コンフィギュレーション コマンド設定に戻ります。
ステップ 5	end 例： Device(config-if)# end	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

単方向リンク検出のモニタリングと保守

コマンド	目的
show udld [<i>interface-id</i> neighbors]	指定されたポートまたはすべてのポートの UDLD ステータスを表示します。

単方向リンク検出に関するその他の参考資料

関連資料

関連項目	マニュアル タイトル
この章で使用するコマンドの完全な構文および使用方法の詳細。	<i>Command Reference (Catalyst 9300 Series Switches)</i> の「Layer 2/3 Commands」の項を参照してください

単方向リンク検出の機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Everest 16.5.1a	単一方向リンク検出 (UDLD)	UDLD は、光ファイバまたはツイストペアイーサネット ケーブルを通して接続されたデバイスからケーブルの物理設定をモニターしたり、単一方向リンクの存在を検出したりできるようにするためのレイヤ 2 プロトコルです。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> [英語] からアクセスします。



第 9 章

IEEE 802.1Q トンネリングの設定

- [IEEE 802.1Q トンネリングについて \(195 ページ\)](#)
- [IEEE 802.1Q トンネリングの設定方法 \(201 ページ\)](#)
- [トンネリング ステータスのモニタリング \(203 ページ\)](#)
- [例 : IEEE 802.1Q トンネリング ポートの設定 \(204 ページ\)](#)
- [IEEE 802.1Q トンネリングの機能履歴 \(204 ページ\)](#)

IEEE 802.1Q トンネリングについて

IEEE 802.1Q トンネリングは、サービスプロバイダーのネットワークを越えて複数のカスタマーのトラフィックを運び、その他のカスタマーのトラフィックに影響を与えずに、それぞれのカスタマーの VLAN およびレイヤ 2 プロトコルの設定を維持する必要があるサービスプロバイダー用に設計された機能です。

サービスプロバイダーネットワークにおける IEEE 802.1Q トンネルポート

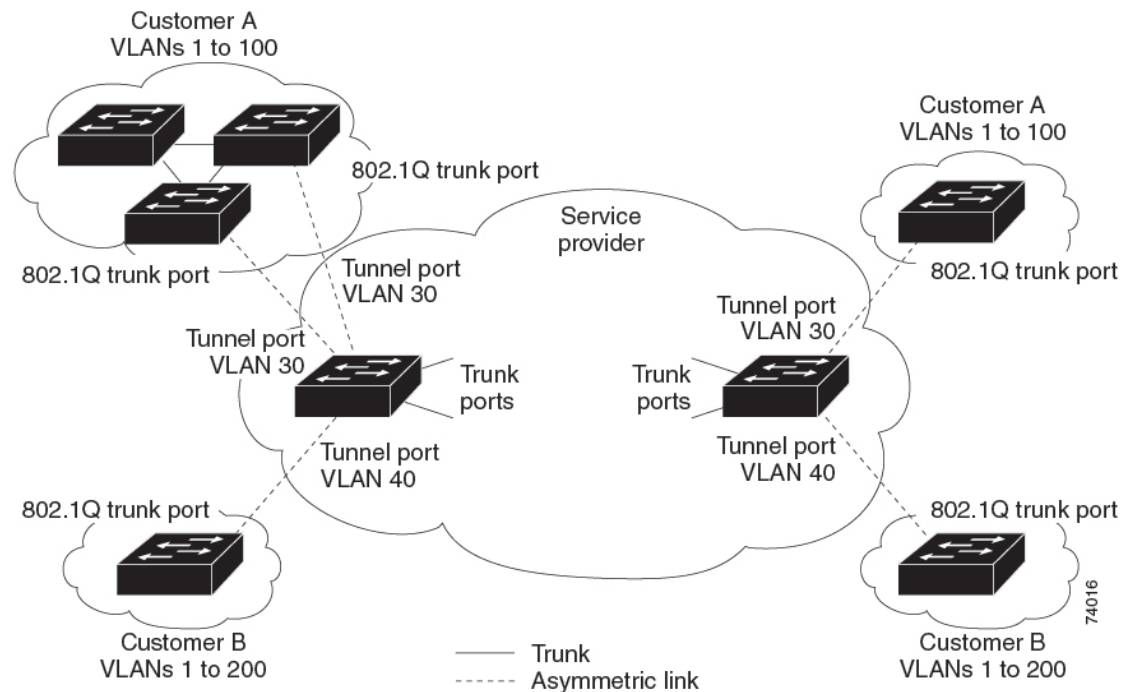
サービスプロバイダーのビジネスカスタマーには、多くの場合、サポートする VLAN ID および VLAN の数に固有の要件があります。同一サービスプロバイダー ネットワークのさまざまなカスタマーが必要とする VLAN 範囲は重複し、インフラストラクチャを通るカスタマーのトラフィックは混合してしまうことがあります。それぞれのカスタマーに VLAN ID の固有の範囲を割り当てると、カスタマーの設定が制限され、IEEE 802.1Q 仕様の VLAN 制限 (4096) を簡単に超えてしまうことがあります。

サービスプロバイダーは、IEEE 802.1Q トンネリング機能を使用すると、単一の VLAN を使用して、複数の VLAN を含むカスタマーをサポートできます。カスタマーの VLAN ID は、同一 VLAN にあるように見えても保護され、さまざまなカスタマーのトラフィックは、サービスプロバイダー ネットワーク内で区別されます。IEEE 802.1Q トンネリングを使用する場合、VLAN-in-VLAN 階層構造およびタグ付きパケットへの再タグ付けによって、VLAN スペースを拡張できます。IEEE 802.1Q トンネリングをサポートするように設定したポートは、トンネルポートと呼ばれます。トンネリングを設定する場合は、トンネリング専用の VLAN ID にト

ンネルポートを割り当てます。それぞれの顧客には別個のサービスプロバイダー VLAN ID が必要ですが、その VLAN ID ではすべての顧客の VLAN がサポートされます。

適切な VLAN ID で通常どおりにタグ付けされた顧客のトラフィックは、顧客デバイス IEEE 802.1Q トランクポートからサービスプロバイダーのエッジデバイスのトンネルポートに発信されます。顧客デバイスとエッジデバイス間のリンクは、片方が IEEE 802.1Q トランクポートとして設定され、もう一方がトンネルポートとして設定されるため、非対称です。それぞれの顧客に固有のアクセス VLAN ID には、トンネルポートインターフェイスを割り当てます。

図 29: サービス プロバイダー ネットワークにおける IEEE 802.1Q トンネルポート

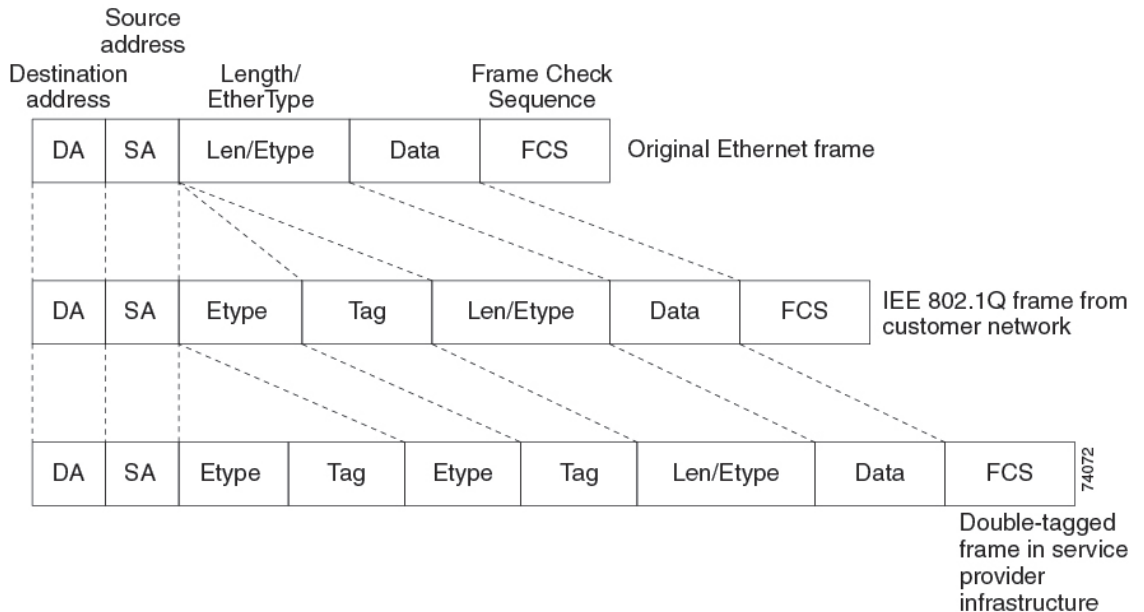


顧客のトランクポートからサービスプロバイダーのエッジデバイスのトンネルポートに発信されるパケットには、通常、適切な VLAN ID とともに IEEE 802.1Q タグが付いています。これらのタグ付きパケットは、デバイス内部ではそのまま保持され、トランクポートを出てサービスプロバイダー ネットワークに入る時点で、顧客に固有の VLAN ID を含む、IEEE 802.1Q タグのもう 1 つのレイヤ (メトロタグと呼ばれる) でカプセル化されます。顧客の元の IEEE 802.1Q タグは、カプセル化されたパケット内で保護されます。このため、サービスプロバイダー ネットワークに入るパケットには、顧客のアクセス VLAN ID を含む外部 (メトロ) タグ、および着信トラフィックのものである内部 VLAN ID という、二重のタグが付きます。

二重タグパケットがサービスプロバイダー コア デバイスの別のトランクポートに入ると、デバイスがパケットを処理するときに外部タグが外れます。パケットがその同じコアデバイスの別のトランクポートを出るとき、同じメトロタグがパケットに再び追加されます。

図 30:元の（通常）イーサネットパケット、IEEE 802.1Qイーサネットパケット、二重タグイーサネットパケットの形式

この図は、二重タグ付きパケットのタグ構造を示しています。



パケットがサービスプロバイダー出力デバイスのトランクポートに入ると、デバイスがパケットを内部処理する間に外部タグが再び外されます。ただし、パケットがエッジデバイスのトンネルポートからカスタマーネットワークに送信される時、メトロタグは追加されません。パケットは通常の IEEE 802.1Q タグ フレームとして送信され、カスタマー ネットワーク内で元の VLAN 番号は保護されます。

上記のネットワークの図では、カスタマー A に VLAN 30、カスタマー B に VLAN 40 が割り当てられています。エッジデバイスのトンネルポートに入る、IEEE 802.1Q タグが付いたパケットは、サービスプロバイダ ネットワークに入るとき、VLAN ID 30 または 40 を適切に含む外部タグ、および VLAN 100 などの元の VLAN 番号を含む内部タグが付いて二重タグになります。カスタマー A とカスタマー B の両方が、それぞれのネットワーク内で VLAN 100 を含んでも、外部タグが異なるので、サービスプロバイダー ネットワーク内で区別されます。それぞれの顧客は、その他の顧客が使用する VLAN 番号スペース、およびサービスプロバイダー ネットワークが使用する VLAN 番号スペースから独立した、独自の VLAN 番号スペースを制御します。

アウトバウンド トンネル ポートでは、顧客のネットワーク上の元の VLAN 番号が回復されます。トンネリングとタグ付けを複数レベルにすることもできますが、このリリースのデバイスでは 1 レベルだけがサポートされます。

顧客 ネットワークから発信されるトラフィックにタグ（ネイティブ VLAN フレーム）が付いていない場合、そのパケットのブリッジングまたはルーティングは通常パケットとして行われます。エッジデバイスのトンネルポートを通してサービスプロバイダ ネットワークに入るすべてのパケットは、タグが付いていないか、IEEE 802.1Q ヘッダーですでにタグが付いているかに関係なく、タグなしパケットとして扱われます。パケットは、IEEE 802.1Q トランクポートでサービスプロバイダー ネットワークを通じて送信される場合、メトロタグ VLAN ID

(トンネルポートのアクセス VLAN に設定) でカプセル化されます。メトロ タグの優先度フィールドは、トンネルポートで設定されているインターフェイス サービス クラス (CoS) 優先度に設定されます (設定されていない場合、デフォルトはゼロです)。

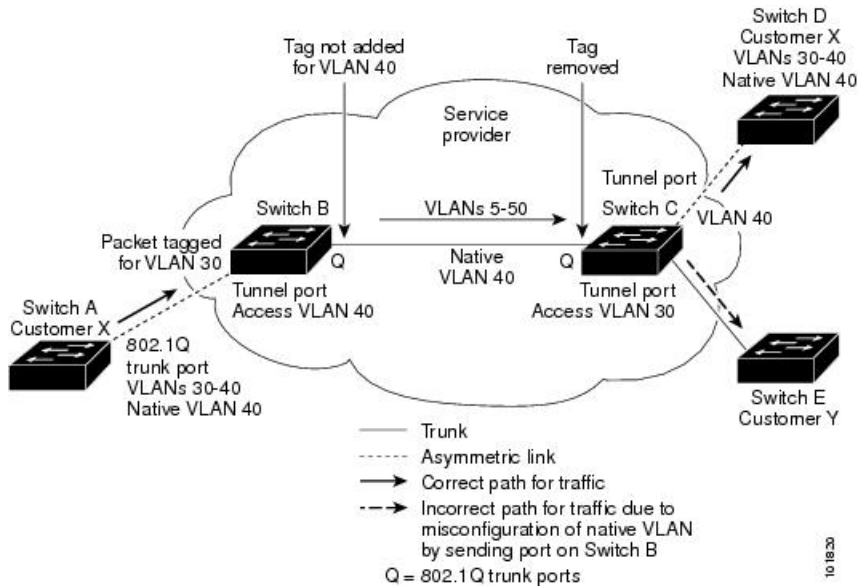
スイッチでは、802.1Q トンネリングはポート単位で設定されるため、スイッチがスタンドアロンデバイスであるか、またはスタックメンバーであるかは関係ありません。すべての設定は、アクティブスイッチで行われます。

ネイティブ VLAN

エッジデバイスで IEEE 802.1Q トンネリングを設定する場合、サービスプロバイダー ネットワークにパケットを送信するために、IEEE 802.1Q トランクポートを使用する必要があります。ただし、サービスプロバイダー ネットワークのコアを通過するパケットは、IEEE 802.1Q トランク、ISL トランク、非トランキングリンクのいずれかで送信できます。コアデバイスで IEEE 802.1Q トランクを使用する場合、IEEE 802.1Q トランクのネイティブ VLAN は、同一デバイスの非トランキング (トンネリング) ポートのネイティブ VLAN と同じであってはなりません。これは、ネイティブ VLAN のトラフィックは、IEEE 802.1Q 送信トランクポートではタグ付けされないためです。

以下のネットワーク図では、VLAN 40 は、サービスプロバイダー ネットワークの入力エッジスイッチ (スイッチ B) において、カスタマー X からの IEEE 802.1Q トランクポートのネイティブ VLAN として設定されています。カスタマー X のスイッチ A は、VLAN 30 のタグ付きパケットを、アクセス VLAN 40 に属する、サービスプロバイダー ネットワークのスイッチ B の入力トンネルポートに送信します。トンネルポートのアクセス VLAN (VLAN 40) は、エッジスイッチのトランクポートのネイティブ VLAN (VLAN 40) と同じであるため、トンネルポートから受信したタグ付きパケットには、メトロ タグが追加されません。パケットには VLAN 30 タグだけが付いて、サービスプロバイダー ネットワークで出力エッジスイッチ (スイッチ C) のトランクポートに送信され、出力スイッチ トンネルによってカスタマー Y に間違えて送信されます。

図 31: IEEE 802.1Q トンネリングおよびネイティブ VLAN に潜在する問題



この問題の解決方法は次のとおりです。

- **vlan dot1q tag native** グローバルコンフィギュレーションコマンドを使用することで、(ネイティブ VLAN を含む) IEEE 802.1Q トランクから発信されるすべてのパケットがタグ付けされるようにエッジスイッチを設定します。すべての IEEE 802.1Q トランクでネイティブ VLAN パケットにタグを付けるようにスイッチを設定した場合、スイッチはタグなしパケットをドロップし、タグ付きパケットだけを送受信します。
- エッジスイッチのトランクポートのネイティブ VLAN ID が、カスタマー VLAN 範囲に含まれないようにしてください。たとえばトランクポートが VLAN100～200 のトラフィックを運ぶ場合は、この範囲以外の番号をネイティブ VLAN に割り当てます。

システム MTU

デバイス上のトラフィックに関するデフォルトのシステム MTU は、1500 バイトです。

system mtu bytes グローバルコンフィギュレーションコマンドを使用すると、10 ギガビットイーサネットポートおよびギガビットイーサネットポートで1500バイトを超えるフレームをサポートするように設定できます。

システム MTU 値とシステムジャンボ MTU 値には、IEEE 802.1Q ヘッダーは含まれていません。IEEE 802.1Q トンネリング機能では、メトロタグが追加されるとフレームサイズが4バイト増加するため、システム MTU サイズに最低4バイトを追加することによって、サービスプロバイダーネットワークのすべてのデバイスが最大フレームを処理できるように設定する必要があります。

たとえば、デバイスはこの構成で最大 1496 バイトのフレームサイズをサポートしています。デバイスのシステム MTU 値が 1500 バイトで、**switchport mode dot1q tunnel** インターフェイ

ス コンフィギュレーション コマンドを使って 10 ギガビットイーサネットまたはギガビットイーサネット デバイス ポートが設定されています。

IEEE 802.1Q トンネリングおよびその他の機能

IEEE 802.1Q トンネリングはレイヤ 2 パケット スイッチングで適切に動作しますが、一部のレイヤ 2 機能およびレイヤ 3 スイッチングの間には非互換性があります。

- トンネル ポートはルーテッド ポートにできません。
- IEEE 802.1Q トンネル ポートを含む VLAN では IP ルーティングがサポートされません。トンネルポートから受信したパケットは、レイヤ 2 情報だけに基づいて転送されます。トンネルポートを含むスイッチ仮想インターフェイス (SVI) でルーティングがイネーブルである場合、トンネルポートから受信したタグなし IP パケットは、スイッチに認識されてルーティングされます。カスタマーは、ネイティブ VLAN を介してインターネットにアクセスできます。このアクセスが必要ない場合は、トンネルポートを含む VLAN で SVI を設定しないでください。
- フォールバック ブリッジングは、トンネル ポートでサポートされません。トンネルポートから受信したすべての IEEE 802.1Q タグ付きパケットは IP 以外のパケットとして扱われるので、トンネルポートが設定されている VLAN でフォールバック ブリッジングが有効である場合、IP パケットは VLAN を越えて不適切にブリッジングされます。このため、トンネルポートを含む VLAN ではフォールバック ブリッジングを有効にしないでください。
- トンネルポートでは IP アクセス コントロール リスト (ACL) がサポートされません。
- レイヤ 3 の Quality of Service (QoS) ACL およびレイヤ 3 情報に関連する他の QoS 機能は、トンネルポートではサポートされていません。MAC ベース QoS はトンネルポートでサポートされます。
- IEEE 802.1Q 設定が EtherChannel ポート グループ内で矛盾しない場合、EtherChannel ポート グループにはトンネルポートとの互換性があります。
- ポート集約プロトコル (PAgP) 、 Link Aggregation Control Protocol (LACP) 、単一方向リンク検出 (UDLD) は、IEEE 802.1Q トンネルポートでサポートされます。
- トンネルポートとトランクポートで非対称リンクを手動で設定する必要があるため、ダイナミック トランッキングプロトコル (DTP) には IEEE 802.1Q トンネリングとの互換性がありません。
- VLAN トランッキングプロトコル (VTP) は、非対称リンクで接続されているデバイス間、またはトンネルを通して通信を行うデバイス間で動作しません。
- IEEE 802.1Q トンネルポートでは、ループバック検出がサポートされます。
- IEEE 802.1Q トンネルポートとしてポートを設定すると、スパニングツリーブリッジプロトコルデータユニット (BPDU) フィルタリングがインターフェイスで自動的に有効になります。Cisco Discovery Protocol (CDP) は、インターフェイスで自動的にディセーブルに設定されます。



(注) IEEE 802.1Q トンネリングを設定している場合、スパンニングツリー BPDU フィルタが自動的に有効になるため、BPDU フィルタリング設定情報は表示されません。 **show spanning tree interface** コマンドを使用して BPDU フィルタ情報を確認できます。

- IEEE 802.1Q トンネルポートが SPAN 送信元として設定されている場合、パケット損失を回避するために、SVLAN に SPAN フィルタを適用する必要があります。
- IGMP/MLD パケット転送は、IEEE 802.1Q トンネルで有効にできます。これは、サービスプロバイダーネットワークで IGMP/MLD スヌーピングを無効にすることで実行できます。

IEEE 802.1Q トンネリングのデフォルト設定

デフォルトでは、デフォルト switchport モードが `dynamic auto` であるため、IEEE 802.1Q トンネルはディセーブルです。すべての IEEE 802.1Q トランク ポートにおける IEEE 802.1Q ネイティブ VLAN パケットのタグ付けもディセーブルです。

IEEE 802.1Q トンネリングの設定方法

ポートを IEEE 802.1Q トンネルポートとして設定するには、次の手順に従います。

始める前に

- カスタマーデバイスおよびエッジデバイス間で非対称リンクを常に使用する必要があります。カスタマーデバイスのポートを IEEE 802.1Q トランクポートに、エッジデバイスのポートをトンネルポートとして設定してください。
- トンネリングに使用する VLAN だけにトンネルポートを割り当ててください。
- ネイティブ VLAN と最大伝送単位 (MTU) の設定要件に従ってください。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーションモードを開始します。

	コマンドまたはアクション	目的
ステップ 3	interface interface-id 例 : Device(config)# interface gigabitethernet2/0/1	トンネルポートとして設定するインターフェイスのインターフェイスコンフィギュレーションモードを開始します。これは、カスタマーデバイスに接続するサービスプロバイダーネットワーク内のエッジポートである必要があります。有効なインターフェイスには、物理インターフェイスおよびポートチャンネル論理インターフェイス（ポートチャンネル1～48）が含まれます。
ステップ 4	switchport access vlan vlan-id 例 : Device(config-if)# switchport access vlan 2	インターフェイスがトランキングを停止した場合に使用されるデフォルトVLANを指定します。このVLAN IDは特定カスタマーに固有です。
ステップ 5	switchport mode dot1q-tunnel 例 : Device(config-if)# switchport mode dot1q-tunnel	IEEE 802.1Q トンネルポートとしてインターフェイスを設定します。 (注) ポートを dynamic desirable デフォルト状態に戻すには、 no switchport mode dot1q-tunnel インターフェイスコンフィギュレーションコマンドを使用します。
ステップ 6	exit 例 : Device(config-if)# exit	グローバルコンフィギュレーションモードに戻ります。
ステップ 7	vlan dot1q tag native 例 : Device(config)# vlan dot1q tag native	(任意) すべての IEEE 802.1Q トランクポートでネイティブVLANパケットのタグングがイネーブルになるようにデバイスを設定します。これを設定せず、カスタマーVLAN IDがネイティブVLANと同じである場合、トランクポートはメトロタグを適用せず、パケットは誤った宛先に送信される可能性があります。

	コマンドまたはアクション	目的
		(注) ネイティブ VLAN パケットのタグ付けをディセーブルにするには、 no vlan dot1q tag native グローバル コンフィギュレーションコマンドを使用します。
ステップ 8	end 例： Device(config)# end	特権 EXEC モードに戻ります。
ステップ 9	次のいずれかを使用します。 <ul style="list-style-type: none"> • show dot1q-tunnel • show running-config interface 例： Device# show dot1q-tunnel または Device# show running-config interface	IEEE 802.1Q トンネリング用に設定されたポートを表示します。 トンネリングモードになっているポートを表示します。
ステップ 10	show vlan dot1q tag native 例： Device# show vlan dot1q native	IEEE 802.1Q ネイティブ VLAN タギングステータスを表示します。
ステップ 11	copy running-config startup-config 例： Device# copy running-config startup-config	(任意) コンフィギュレーションファイルに設定を保存します。

トンネリングステータスのモニタリング

次の表では、トンネリングステータスをモニタするために使用するコマンドについて説明します。

表 18: トンネリングのモニタリングコマンド

コマンド	目的
show dot1q-tunnel	デバイスの IEEE 802.1Q トンネルポートを表示します。
show dot1q-tunnel interface interface-id	特定のインターフェイスがトンネルポートであるかどうかを確認します。

コマンド	目的
<code>show vlan dot1q tag native</code>	デバイスのネイティブVLANタグgingのステータスを表示します。

例：IEEE 802.1Q トンネリング ポートの設定

以下の例では、トンネルポートとしてインターフェイスを設定してネイティブVLANパケットのタグ付けをイネーブルにし、設定を確認する方法を示します。この設定では、スタックメンバー1のインターフェイス Gigabit Ethernet 7に接続するカスタマーのVLAN IDは、VLAN 22になります。

```
Device(config)# interface gigabitethernet1/0/7
Device(config-if)# switchport access vlan 22
% Access VLAN does not exist. Creating vlan 22
Device(config-if)# switchport mode dot1q-tunnel
Device(config-if)# exit
Device(config)# vlan dot1q tag native
Device(config)# end
Device# show dot1q-tunnel interface gigabitethernet1/0/7
Port
-----
Gi1/0/1Port
-----
Device# show vlan dot1q tag native
dot1q native vlan tagging is enabled
```

IEEE 802.1Q トンネリングの機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Everest 16.5.1a	IEEE 802.1Q トンネリング	IEEE 802.1Q トンネリングは、サービスプロバイダーのネットワークを越えて複数のカスタマーのトラフィックを運び、その他のカスタマーのトラフィックに影響を与えずに、それぞれのカスタマーのVLANおよびレイヤ2プロトコルの設定を維持する必要があるサービスプロバイダー用に設計された機能です。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> [英語] からアクセスします。



第 10 章

VLAN マッピングの設定

- [VLAN マッピングの前提条件](#) (207 ページ)
- [VLAN マッピングについて](#) (207 ページ)
- [VLAN マッピング設定時の注意事項](#) (210 ページ)
- [VLAN マッピングの設定方法](#) (211 ページ)
- [VLAN マッピングの機能履歴](#) (213 ページ)

VLAN マッピングの前提条件

- デフォルトで、VLAN マッピングは設定されていません。
- **Network Advantage** ライセンスを実行していることを確認します。VLAN マッピングは、**Network Advantage** ライセンスレベルでのみサポートされます。
- 一貫して制御トラフィックを処理するには、次のようにレイヤ2プロトコルトネリングをイネーブルにするか（推奨）、

```
!  
Device(config)# interface HundredGigE1/0/1  
Device(config-if)# switchport mode access  
Device(config-if)# l2protocol-tunnel stp  
Device(config-if)# end
```

または、次のようにスパニングツリーの BPDU フィルタを挿入します。

```
!  
Device(config)# interface HundredGigE1/0/1  
Device(config-if)# switchport mode trunk  
Device(config-if)# switchport vlan mapping 10 20  
Device(config-if)# spanning-tree bpdufilter enable  
Device(config-if)# end
```

VLAN マッピングについて

VLAN マッピングの一般的な配備で、サービスプロバイダーは、ローカルサイトの一部としてのリモートロケーションにおけるカスタマーのスイッチを含む、透過的なスイッチングイン

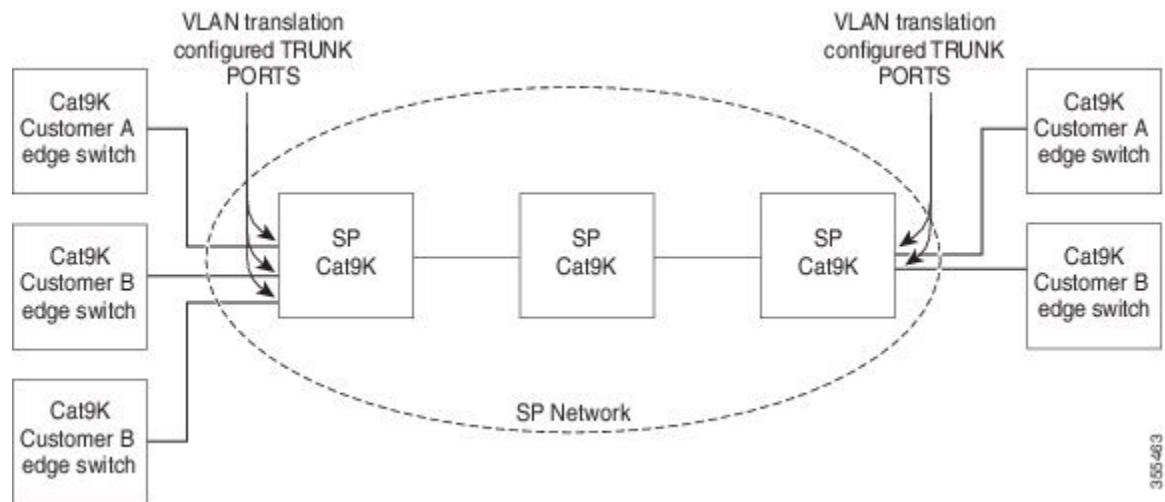
フラストラクチャを提供します。これにより、カスタマーは、同じ VLAN ID スペースを使用し、プロバイダーネットワークを介してレイヤ2制御プロトコルをシームレスに実行できます。このようなシナリオでは、サービスプロバイダーはその VLAN ID をカスタマーに適用しないことを推奨します。

変換済み VLAN ID (S-VLAN) を確立する1つ方法では、カスタマーネットワークに接続されたトランクポートで、サービスプロバイダー VLAN にカスタマーの VLAN をマッピングします (VLAN ID 変換とも呼ばれます)。ポートに入るパケットは、ポート番号とパケットの元のカスタマー VLAN-ID (C-VLAN) に基づいて、サービスプロバイダーの VLAN (S-VLAN) にマッピングされます。

サービスプロバイダーの内部割り当ては、カスタマーの VLAN と競合する場合があります。カスタマートラフィックを分離するために、サービスプロバイダーは、トラフィックがクラウドにある間に、特定の VLAN を別の VLAN にマッピングできます。

配備例

次の図では、サービスプロバイダーはレイヤ2 VPN サービスを2つの異なる顧客 A と B に提供します。サービスプロバイダーは、2つの顧客間およびプロバイダー自身の制御トラフィックからデータと制御トラフィックを分離します。また、サービスプロバイダーネットワークは、カスタマーエッジデバイスに対して透過的である必要があります。



Catalyst 9000 シリーズスイッチのすべての転送処理は、C-VLAN 情報ではなく、S-VLAN 情報を使用して実行されます。これは、VLAN ID が、入力時に S-VLAN にマッピングされるためです。



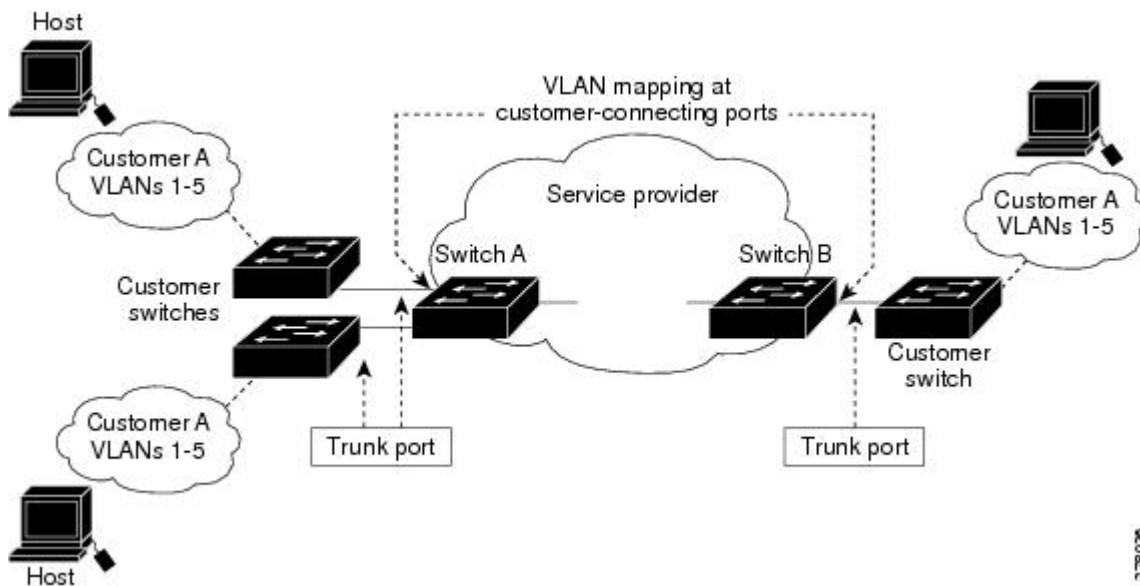
- (注) VLAN マッピングが設定されているポートで機能を設定する場合は、カスタマー VLAN-ID (C-VLAN) ではなく S-VLAN を常に使用します。

VLAN マッピングが設定されているインターフェイスでは、指定された C-VLAN パケットはポートに入るとき、指定された S-VLAN にマッピングされます。パケットがポートから出る場合も同様に、カスタマー C-VLAN にマッピングが行われます。

スイッチはトランクポートにおける次の種類の VLAN マッピングをサポートします。

- One-to-One の VLAN マッピング。

カスタマー VLAN からサービスプロバイダー VLAN へのマッピング



図は、カスタマーがサービスプロバイダーネットワークの両端の複数のサイトで同じ VLAN を使用する場合のトポロジを示します。サービスプロバイダーバックボーン経由でパケットを伝送できるように、カスタマー VLAN ID をサービスプロバイダー VLAN ID にマッピングします。サービスプロバイダーバックボーンの反対側でカスタマー VLAN ID が取り出され、別のカスタマーサイトで使用できます。サービスプロバイダーネットワークのそれぞれの側のカスタマー接続ポートで同じ VLAN マッピングセットを設定します。

One-to-One の VLAN マッピング

One-to-One VLAN マッピング。ポートへの入出時に実行され、802.1Q タグの C-VLAN ID が S-VLAN ID にマッピングされます。他のすべての VLAN ID を持つパケットが転送されるように指定することもできます。

VLAN マッピング設定時の注意事項



- (注)
- デフォルトで、VLAN マッピングは設定されていません。
 - サポートされる VLAN マッピング設定の最大数は、システム全体で 512 です。

ガイドラインは次のとおりです。

- VLAN マッピングが EtherChannel で有効になっている場合、設定は EtherChannel バンドルのすべてのメンバーポートには適用されず、EtherChannel インターフェイスにのみ適用されます。
- EtherChannel に属するポートが VLAN マッピングで設定され、EtherChannel が競合する VLAN マッピングで設定されている場合、ポートは EtherChannel から削除されます。
- ポートのモードが「トランク」モード以外に変更されると、EtherChannel のメンバーポートは EtherChannel バンドルから削除されます。
- 一貫して制御トラフィックを処理するには、次のようにレイヤ2プロトコルトネリングをイネーブルにするか（推奨）、

```
!
Device(config)# interface HundredGigE1/0/1
Device(config-if)# switchport mode trunk
Device(config-if)# switchport vlan mapping 20 300
Device(config-if)# l2protocol-tunnel stp
Device(config-if)# end
```

または、次のようにスパニングツリーの BPDU フィルタを挿入します。

```
!
Device(config)# interface HundredGigE1/0/1
Device(config-if)# switchport mode trunk
Device(config-if)# switchport vlan mapping 10 20
Device(config-if)# spanning-tree bpdufilter enable
Device(config-if)# end
```

- デフォルトのネイティブ VLAN、ユーザ設定のネイティブ VLAN、および予約済みの VLAN（範囲 1002 ~ 1005）は、VLAN マッピングに使用できません。
- VLAN マッピングに使用される S-VLAN は、EVPN や LISP などの他のレイヤ 3 コンフィギュレーションの一部にはできません。
- PVLAN サポートは、VLAN マッピングが設定されている場合は使用できません。

One-to-One VLAN マッピングの設定時の注意事項

- One-to-One の VLAN マッピングは、トランクポートでのみ設定でき、ダイナミックトランクでは設定できません。

- One-to-One の VLAN マッピングは、両方のポートで同一である必要があります。
- S-VLAN が作成され、One-to-One の VLAN マッピングが設定されているトランクポートの許可された VLAN リスト内に存在する必要があります。
- One-to-One の VLAN マッピングが設定されている場合、複数の C-VLAN を同じ S-VLAN にマッピングすることはできません。
- One-to-One の VLAN マッピングの場合、C-VLAN と S-VLAN スパニングツリートポロジのマージはサポートされません。

VLAN マッピングの設定方法

ここでは、VLAN マッピングの設定方法について説明します。

One-to-One の VLAN マッピング



(注) VLAN マッピングは、**network-advantage** ライセンスレベルでのみサポートされます。

サービスプロバイダー VLAN ID にカスタマー VLAN ID をマッピングするために、1対1の VLAN マッピングを設定するには、次の作業を行います。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーションモードを開始します。
ステップ 3	interface interface-id 例： Device(config)# interface gigabitethernet1/0/1	サービスプロバイダーネットワークに接続されるインターフェイスのインターフェイス コンフィギュレーションモードを開始します。物理インターフェイスまたは EtherChannel ポートチャンネルを入力できます。
ステップ 4	switchport mode trunk 例：	指定したインターフェイスをトランクポートとして設定します。

	コマンドまたはアクション	目的
	Device(config-if)# switchport mode trunk	
ステップ 5	switchport vlan mapping vlan-id translated-id 例： Device(config-if)# switchport vlan mapping 2 102	マッピングする VLAN ID を入力します。 <ul style="list-style-type: none"> • vlan-id : カスタマー ネットワークからスイッチに入るカスタマー VLAN ID (C-VLAN)。指定できる範囲は 1 ~ 4094 です。 • translated-id : 割り当てられた VLAN ID (S-VLAN)。指定できる範囲は 1 ~ 4094 です。
ステップ 6	exit 例： Device(config-if)# exit	グローバル コンフィギュレーション モードに戻ります。
ステップ 7	spanning-tree bpdudfilter enable 例： Device(config)# spanning-tree bpdudfilter enable	スパニングツリーの BPDU フィルタを挿入します。 (注) 一貫して制御トラフィックを処理するには、レイヤ 2 プロトコルトンネリングをイネーブルにするか (推奨)、またはスパニングツリーの BPDU フィルタを挿入します。
ステップ 8	end 例： Device(config)# end	特権 EXEC モードに戻ります。
ステップ 9	show vlan mapping 例： Device# show vlan mapping	設定を確認します。
ステップ 10	copy running-config startup-config 例： Device# copy running-config startup-config	(任意) コンフィギュレーションファイルに設定を保存します。

例

no switchport vlan mapping VLAN マッピング情報を削除するには、コマンドを使用します。**no switchport vlan mapping all** コマンドを入力すると、すべてのマッピング設定が削除されます。

この例では、カスタマーネットワークの VLAN ID 2～6 をサービスプロバイダーネットワークの VLAN ID 101～105 にマッピングする方法を示します (図 3～5)。スイッチ A とスイッチ B のポートに、同じ VLAN マッピングコマンドを設定します。他のすべての VLAN ID のトラフィックは通常のトラフィックとして転送されます。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitEthernet0/1
Device(config-if)# switchport vlan mapping 2 101
Device(config-if)# switchport vlan mapping 3 102
Device(config-if)# switchport vlan mapping 4 103
Device(config-if)# switchport vlan mapping 5 104
Device(config-if)# switchport vlan mapping 6 105
Device(config-if)# exit
```

前の例では、サービスプロバイダーネットワークの入力側で、カスタマーネットワークの VLAN ID 2～6 は、サービスプロバイダーネットワーク内の VLAN ID 101～105 にマッピングされます。サービスプロバイダーネットワークの出力側で、サービスプロバイダーネットワークの VLAN 101～105 は、カスタマーネットワークの VLAN ID 2～6 にマッピングされます。



- (注) VLAN マッピングが設定されている以外の VLAN ID を持つパケットは、通常のトラフィックとして転送されます。

設定された VLAN に関する情報を表示するには、**show vlan mapping** コマンドを使用します。

```
Device> enable
Device# configure terminal
Device(config)# show vlan mapping
Total no of vlan mappings configured: 1
Interface Po5:
VLANs on wire          Translated          VLAN Operation
-----
20                      30                  1-to-1
```

VLAN マッピングの機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Gibraltar 16.11.1	One-to-One の VLAN マッピング	カスタマーネットワークに接続されたトランクポート上での One-to-One の VLAN マッピングにより、カスタマー VLAN をサービスプロバイダー VLAN にマッピングできます。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> [英語] からアクセスします。



第 11 章

VXLAN BGP EVPN の設定

次のセクションでは、VXLAN BGP EVPN の設定について説明します。

- [VXLAN BGP EVPN の注意事項と制約事項 \(215 ページ\)](#)
- [VXLAN BGP EVPN に関する情報 \(216 ページ\)](#)
- [VXLAN BGP EVPN 展開の考慮事項 \(217 ページ\)](#)
- [VXLAN BGP EVPN の設定方法 \(220 ページ\)](#)
- [VXLAN BGP EVPN \(EBGP\) の設定例 \(237 ページ\)](#)
- [VXLAN BGP EVPN の機能の履歴と情報 \(253 ページ\)](#)

VXLAN BGP EVPN の注意事項と制約事項

Virtual Extensible LAN (VXLAN) Border Gateway Protocol (BGP) Ethernet VPN (EVPN) の制限事項は次のとおりです。

- VXLAN 経由のマルチキャストは現在サポートされていません。
- show コマンドで **internal** キーワードを指定することは、サポートされていません。
- EBGP では、シングル オーバーレイ EBGP EVPN セッションをループバック間で使用することを推奨します。
- NVE を、レイヤ 3 プロトコルで必要な他のループバック アドレスとは別のループバック アドレスにバインドします。VXLAN に対して専用のループバック アドレスを使用することがベストプラクティスです。
- VXLAN BGP EVPN は、非デフォルト VRF にある NVE インターフェイスをサポートしません。
- オーバーレイ BGP セッションのループバックで単一 BGP セッションを設定することを推奨します。
- VXLAN UDP ポート番号は VXLAN カプセル化に使用されます。これは IETF 標準に準拠しており、変更できません。

- VXLAN BGP EVPN は現在、リーフスイッチ機能のみをサポートしています。スパインスイッチ機能はサポートされていません。
- ルートリフレクタ、ユニキャストランデブーポイント、Multicast Source Discovery Protocol (MSDP) ランデブーポイントなどの統合されたアンダーレイテクノロジーはサポートされていません。
- ボーダーリーフ機能および BGP EVPN と従来のレイヤ 3 およびレイヤ 2 オーバーレイネットワーク間のインターワーキングはサポートされていません。
- IP VRF の自動ルート識別子および自動ルートターゲットはサポートされていません
- レイヤ 2 VXLAN ネットワーク識別子 (L2VNI) の集中型ゲートウェイはサポートされていません。
- BGP EVPN ネットワーク仮想化オーバーレイ MIB はサポートされていません。
- EVPN 展開では、VLAN がコア側の SVI に使用されると、どのトランクでも許可されません。コア側の SVI を正しく機能させるには、SVI で **no autostate** コマンドを設定する必要があります。

VXLAN BGP EVPN に関する情報

VXLAN は、レイヤ 2 セグメントを IP コア全体にストレッチできる IP/UDP オーバーレイの MAC です。そのため、レイヤ 3 トポロジのすべての利点を VXLAN で利用できます。VXLAN ヘッダーのカプセル化とカプセル化解除は、VXLAN トンネルエンドポイント (VTEP) に組み込まれた機能によって処理されます。VTEP 自体は、ソフトウェアまたはハードウェアのフォームファクタで実装できます。

VXLAN は、特定の VXLAN ネットワーク内の BU (ブロードキャスト、不明なユニキャスト) トラフィックおよびレイヤ 2 マルチキャストトラフィックが IP コアを介してそのネットワーク内のメンバーシップを持つすべての VTEP に送信される、**flood-n-learn** メカニズムでネイティブに動作します。IP マルチキャストは、このネットワークを介してトラフィックを送信する場合に使用します。受信 VTEP はパケットのカプセル化を解除し、内部フレームに基づいてレイヤ 2 MAC の学習を実行します。内部 SMAC アドレスは、送信元 VTEP に対応する外部送信元 IP アドレス (SIP) と照合して学習されます。このようにして、リバーストラフィックは、以前に学習したエンドホストにユニキャストできます。

オーバーレイアーキテクチャを使用する利点は次のとおりです。

- 拡張性：VXLAN は 1,600 万のテナントネットワークに拡張可能なインフラストラクチャを可能にするレイヤ 2 接続を提供します。VLAN の 4094 セグメントの制限を打破します。これは今日のマルチテナントクラウドの要件に対応するために必要です。
- 柔軟性：VXLAN を使用すると、マルチテナント環境で必要なトラフィックの分離とともにワークロードを任意の場所に配置できます。トラフィックの分離は、ネットワークセグメンテーション (セグメント ID または仮想ネットワーク識別子 [VNI]) を使用して行われます。テナントのワークロードは複数の物理デバイスに分散可能です (ワークロードは必

要に応じて利用可能なサーバースペースに追加されるため)。ただし、ワークロードは同じレイヤ 2 またはレイヤ 3 VNI によって識別される場合があります。

- モビリティ：VM はスパインスイッチテーブルを更新せずにデータセンター間を移動できます。これは、VXLAN/EVPN ファブリックセットアップの同じテナントネットワーク内のエンティティは、場所に関係なく同じ VXLAN セグメント ID を保持するためです。

VXLAN flood-n-learn の最大の制限の 1 つは、VTEP で学習が行われるようにするために必要な固有のフラディングです。従来の展開では、レイヤ 2 セグメントは、BU トラフィックも対象とするブロードキャストドメインを構成する VLAN で表されます。VXLAN を使用すると、レイヤ 2 セグメントは IP コア全体のはるかに大きな境界にまたがり、フラディングが IP マルチキャスト（または HER）に変換されます。その結果、flood-n-learn ベースのスキームでは、特にエンドホストの数が増えるにつれて、深刻な規模の問題が発生します。これは、エンドホストアドレスの配布用のコントロールプレーンを使用した学習によって対処されます。選択するコントロールプレーンは BGP EVPN です。

VXLAN BGP EVPN 展開の考慮事項

VXLAN BGP EVPN 展開では、次の事項を考慮する必要があります。

- `source-interface config` コマンドを使用する場合は、ループバックアドレスが必要です。ループバックアドレスは、ローカル VTEP IP を表します。
- コアで IP マルチキャストのルーティングを確立するには、IP マルチキャストの設定、PIM の設定、および RP の設定が必要です。
- VTEP to VTEP ユニキャストの到達可能性は、任意の IGP/BGP プロトコルを介して設定できます。
- エニーキャストゲートウェイ機能が特定の VNI で有効にされている場合、エニーキャストゲートウェイ機能はそうした VNI が設定されているすべての VTEP で有効にする必要があります。一部の VTEP だけで設定されたエニーキャストゲートウェイ機能を、特定の VNI でイネーブルにすることはサポートされていません。
- NVE 送信元インターフェイスのプライマリまたはセカンダリ IP アドレスを変更する場合、IP アドレスを変更する前に NVE インターフェイスをシャットダウンする必要があります。
- ベストプラクティスとして、マルチキャストグループの RP は、スパインレイヤ上でのみ設定する必要があります。RP のロードバランシングと冗長性のために、エニーキャスト RP を使用します。
- 各テナント VRF は、VRF オーバーレイ、VLAN および SVI を VXLAN ルーティングに必要とします。
- eBGP の使用例では、次の事項を考慮する必要があります。
 - ルートターゲット (RT) の手動設定が必要です。RT は、特定の EVPN インスタンス (EVI) の VTEP 間で一致する必要があります。

- BGP ルーティングプロセスの下にあるスパインノードで、**retain route-target all** BGP ノブを有効にする必要があります。
- EVPN ルートのネクストホップを適切な VTEP ノードに設定するには、スパインノードで **set ip next-hop changed** BGP ノブを有効にする必要があります。
- VTEP 間のピアリングを複数のスパインノードに行うと、冗長性を実現できます。
- 適切な VLAN データベースを作成するには、次のことを確認してください。
 - eBGP EVPN VxLAN 設計モデルのルートターゲットは、iBGP/IGP モデルのように自動生成できないため、EVPN インスタンス (EVI) ごとに手動で設定する必要があります。特定の EVI に一致する必要があります。ルートターゲットを手動で設定しないと、ルートがインストールされていないため、接続が失われ、不適切な操作が発生します。
 - EVPN VXLAN が正しく動作するようにするには、まず VLAN をアクセスインターフェイスとして割り当てて、VLAN を作成し、vlan.dat ファイルに保存します。トランクインターフェイスの場合、VLAN.dat に VLAN を作成する前に SVI を作成しようとすると、SVI がダウン状態になります。
- 範囲が設定されている場合、すべての L2 VNI をすべての VTEP スイッチで有効にする必要はありません。特定の VTEP で必要な場合にのみ有効になります。
- ルート識別子 (RD) は、IP VRF (L3 VNI) ごとに一意である必要があります。ルートターゲット (RT) は、特定の IP VRF (L3 VNI) と一致する必要があります。IP VRF (L3 VNI) の場合、RD または RT のいずれにも自動生成はありません。
- 範囲が設定されていない場合、すべての VTEP スイッチに同じ L2 VNI を設定する必要はありません。アクセス VLAN は、ホストに接続されている VLAN です。アクセス SVI には、VLAN が接続されているホストと同じサブネットの IP アドレスが必要です。エニーキャストゲートウェイをサポートするには、同じ VLAN のアクセス SVI がすべての VTEP で同じ IP アドレスと MAC アドレスに設定されている必要があります。
- Inter-VxLAN 通信が必要なすべての VTEP ノードで追加の L3 VNI を設定することが重要です。

VXLAN 展開に対するネットワークの考慮事項

VXLAN 展開では、次のネットワークに関する事項を考慮する必要があります。

転送ネットワークの MTU サイズ

MAC-to-UDP のカプセル化に起因して、VXLAN は元のフレームに 50 バイトのオーバーヘッドを導入しています。このため、転送ネットワークの最大転送単位 (MTU) は 50 バイト増やす必要があります。オーバーレイで 1500 バイトの MTU を使用する場合、転送ネットワークは、最低でも 1550 バイトのパケットに対応できるように設定する必要があります。オーバーレイ

アプリケーションで 1500 バイトを超えるフレーム サイズを頻繁に使用する場合は、転送ネットワークでジャンボ フレームのサポートが必要になります。

転送ネットワークの ECMP および LACP ハッシュ アルゴリズム

スイッチは、転送ネットワークの ECMP および LACP ハッシュに対する送信元 UDP ポートのエントロピーレベルを導入しています。この実装を強化する方法として、転送ネットワークは ECMP または LACP のハッシュ アルゴリズムを使用します。これらのアルゴリズムはハッシュの入力として UDP 送信元ポートを使用し、これにより VXLAN のカプセル化されたトラフィックに対して最適なロードシェアリングを実現します。

マルチキャスト グループの拡張

VXLAN の実装では、ブロードキャスト、不明なユニキャスト、およびマルチキャストトラフィックの転送に対してマルチキャストトンネルを使用します。マルチキャスト転送を提供するには、1 つの VXLAN セグメントを 1 つの IP マルチキャスト グループにマッピングする方法が理想的です。ただし、複数の VXLAN セグメントは、コア ネットワーク内で 1 つの IP マルチキャスト グループを共有することが可能です。VXLAN は、ヘッダーの 24 ビット VNID フィールドを使用して最大 1600 万個の論理レイヤ 2 セグメントをサポートできます。VXLAN セグメントと IP マルチキャスト グループ間の 1 対 1 マッピングにより、VXLAN のセグメント数の増加に起因して、必要なマルチキャスト アドレス空間とコア ネットワーク デバイスのフォワーディング ステートの量が平行に増加します。ある時点で、転送ネットワークにおけるマルチキャスト スケーラビリティが問題になることがあります。この場合には、複数の VXLAN セグメントを 1 つのマルチキャスト グループにマッピングすると、コア デバイス上のマルチキャスト コントロール プレーンのリソースが節約され、目的の VXLAN のスケーラビリティを実現できるようになります。ただしこのマッピングは、次善のマルチキャスト転送を犠牲にして実現されます。1 つのテナントのマルチキャスト グループに転送されたパケットは、同じマルチキャスト グループを共有する他のテナントの VTEP に送信されます。このため、マルチキャスト データのプレーン リソースの使用が非効率的になります。したがってこのソリューションは、コントロール プレーンのスケーラビリティとデータ プレーンの効率性との二者択一になります。

次善のマルチキャスト複製と転送を実現しているにも関わらず、複数テナントの VXLAN ネットワークで 1 つのマルチキャスト グループを共有することで、テナント ネットワーク間のレイヤ 2 分離に影響をもたらすことはありません。マルチキャストグループからカプセル化されたパケットを受信すると、VTEP はパケットの VXLAN ヘッダー内の VNID をチェックし、検証します。VTEP は、不明な VNID が見つかったとパケットを廃棄します。VNID が VTEP のローカル VXLAN VNID のいずれかに一致する場合のみ、このパケットを VXLAN セグメントに転送します。他のテナントネットワークではパケットは受信されません。したがって、VXLAN セグメント間の分離は低下しません。

転送ネットワークの考慮事項

トランスポートネットワークの設定に関する考慮事項は次のとおりです。

- VTEP デバイス :

- IP マルチキャストを有効にして、設定します。
 - /32 IP アドレスで、ループバック インターフェイスを作成および設定します。
 - ループバック インターフェイスで IP マルチキャストを有効にします。
 - 転送ネットワークで実行されるルーティング プロトコル（スタティック ルート）を通じて、ループバック インターフェイス /32 アドレスをアドバタイズします。
 - アップリンクの出力物理インターフェイス上で IP マルチキャストを有効にします。
- 転送ネットワーク全体：
- IP マルチキャストを有効にして、設定します。

VXLAN BGP EVPN の設定方法

このセクションでは、VXLAN BGP EVPN の設定方法について説明します。

ブリッジモードでの VXLAN BGP EVPN の設定

このセクションでは、ブリッジモードで VXLAN BGP EVPN を設定する方法について説明します。

VTEP とスパイン間のアンダーレイトランスポート（ユニキャストおよびマルチキャスト）の設定

スパインでアンダーレイトランスポートを設定するには、次の手順に従います。



(注) この設定は、Cisco Nexus シリーズ スイッチに適用でき、Cisco Catalyst 9000 ファミリスイッチには適用できません。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	ip pim rp-address <i>rp-address</i> group-list <i>prefix</i> 例： Device(config)# ip pim rp-address 100.1.1.1 group-list 239.0.0.0/8	マルチキャストグループ範囲に PIM 静的ルートプロセッサ (RP) アドレスを設定し、静的 RP のグループ範囲を指定します。
ステップ 4	ip pim rp-candidate loopback <i>if_number</i> group-list <i>prefix</i> 例： Device(config)# ip pim rp-candidate loopback1 group-list 239.0.0.0/8	PIM アドレスを RP 候補として設定します。ループバックインターフェイスを指定します。RP によって処理されるグループ範囲を指定します。
ステップ 5	ip pim ssm range グループ 例： Device(config)# ip pim ssm range 232.0.0.0/8	SSM のグループ範囲を設定します。
ステップ 6	ip pim anycast-rp <i>rp-address</i> <i>anycast-rp-peer-address</i> 例： Device(config)# ip pim anycast-rp 100.1.1.1 10.1.1.1	指定した Anycast-RP アドレスに PIM Anycast-RP ピアを設定します。
ステップ 7	interface loopback <i>number</i> 例： Device(config)# interface loopback0	ループバックインターフェイスを作成し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 8	ip address <i>ip address</i> 例： Device(config-if)# ip address 10.1.1.1/32	インターフェイスの IP アドレスを定義します。
ステップ 9	ip pim sparse-mode 例： Device(config-if)# ip pim sparse-mode	Protocol Independent Multicast (PIM) スパースモードをインターフェイス上で有効にします。
ステップ 10	exit 例： Device(config-if)# exit	インターフェイス コンフィギュレーション モードを終了します。
ステップ 11	interface port-channel <i>channel-number</i> 例： Device(config)# interface port-channel1	設定するポートチャネルインターフェイスを指定し、インターフェイス コンフィギュレーションモードを開始します。

	コマンドまたはアクション	目的
ステップ 12	mtu bytes 例： Device(config-if)# mtu 9198	インターフェイス MTU サイズを設定します。
ステップ 13	medium p2p 例： Device(config-if)# medium p2p	インターフェイスメディアをポイントツーポイントとして設定します。
ステップ 14	ip address ip-address mask 例： Device(config-if)# ip address 10.10.1.1/30	インターフェイスの IP アドレスを定義します。
ステップ 15	ip pim sparse-mode 例： Device(config-if)# ip pim sparse-mode	Protocol Independent Multicast (PIM) スパースモードをインターフェイス上で有効にします。
ステップ 16	exit 例： Device(config-if)# exit	インターフェイス コンフィギュレーションモードを終了します。

VTEP の設定

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーションモードを開始します。
ステップ 3	ip multicast-routing 例： Device(config)# ip multicast-routing	IP マルチキャストルーティングをイネーブルにします。
ステップ 4	ip pim rp-address rp-address 例： Device(config)# ip pim rp-address 100.1.1.1	マルチキャストグループ範囲に、PIM 静的ルートプロセッサ (RP) アドレスを設定します。この手順で使用される

	コマンドまたはアクション	目的
		rp アドレスは、スパインで使用されるものと同じである必要があります。
ステップ 5	ip routing 例： Device(config)# ip routing	スイッチ上でルーティングを有効にします。IP ルーティングを以前有効にしていた場合でも、この手順で確実に有効にします。
ステップ 6	interface loopback number 例： Device(config)# interface Loopback0	ループバック インターフェイスを作成し、インターフェイス コンフィギュレーションモードを開始します。このループバック インターフェイスは、NVE インターフェイスに割り当てられます。
ステップ 7	ip address ip address 例： Device(config-if)# ip address 10.11.11.11 255.255.255.255	インターフェイスの IP アドレスを定義します。
ステップ 8	ip pim sparse-mode 例： Device(config-if)# ip pim sparse-mode	Protocol Independent Multicast (PIM) スパースモードをインターフェイス上で有効にします。
ステップ 9	exit 例： Device(config-if)# exit	インターフェイス コンフィギュレーションモードを終了します。
ステップ 10	interface loopback number 例： Device(config)# interface Loopback2	ループバック インターフェイスを作成し、インターフェイス コンフィギュレーションモードを開始します。このループバック インターフェイスは、L3 VNI に割り当てられます。
ステップ 11	ip vrf forwarding vrf name 例： Device(config-if)# vrf forwarding tenant_1	VRF をレイヤ 3 インターフェイスに対応付けます。
ステップ 12	ip address ip address 例： Device(config-if)# ip address 11.11.11.11 255.255.255.255	インターフェイスの IP アドレスを定義します。

	コマンドまたはアクション	目的
ステップ 13	exit 例： Device(config-if)# exit	インターフェイス コンフィギュレーション モードを終了します。
ステップ 14	interface tengigabitethernet slot/port 例： Device(config)# interface TenGigabitEthernet1/1/2	設定するポートを選択します。
ステップ 15	no switchport 例： Device(config-if)# no switchport	レイヤ 3 インターフェイスを可能になります。
ステップ 16	no ip address 例： Device(config-if)# no ip address	特定のインターフェイスで IP 処理を無効にします。
ステップ 17	channel-group number 例： Device(config-if)# channel-group 1 mode active	物理インターフェイスの EtherChannel への割り当ておよび設定を行います。
ステップ 18	exit 例： Device(config-if)# exit	インターフェイス コンフィギュレーション モードを終了します。

スパインでの eBGP 設定

次の手順に従って、スパインで EVPN アドレスファミリーを使用して eBGP を設定します。



(注) この設定は、Cisco Nexus シリーズ スイッチに適用でき、Cisco Catalyst 9000 ファミリスイッチには適用できません。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します (要求された場合)。

	コマンドまたはアクション	目的
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	ip prefix-list name [seq number] {permit deny} prefix [eq length] [ge length] [le length] 例： Device(config)# ip prefix-list lo_prefix seq 5 permit 0.0.0.0/0 le 32	IP パケットまたはルートと照合するプレフィックスリストを作成します。
ステップ 4	route-map name {permit deny} [sequence-number] 例： Device(config)# route-map NH-UNCHANGED permit 10	ルート マップのエントリを作成します。ルートマップ コンフィギュレーション モードを開始します。
ステップ 5	set ip next-hop unchanged 例： Device(config-route-map)# set ip next-hop unchanged	ルートマップを定義し、ネイバーの発信ポリシーを適用します。
ステップ 6	exit 例： Device(config-route-map)# exit	ルートマップ コンフィギュレーション モードを終了します。
ステップ 7	route-map name {permit deny} [sequence number] 例： Device(config)# route-map any_prefix permit 10	ルート マップのエントリを作成します。ルートマップ コンフィギュレーション モードを開始します。
ステップ 8	match ip address prefix-list name [name] 例： Device(config-route-map)# match ip address prefix-list lo_prefix	1 つ以上の IP アドレス プレフィックス リストと照合します。
ステップ 9	exit 例： Device(config-route-map)# exit	ルートマップ コンフィギュレーション モードを終了します。
ステップ 10	router bgp number 例： Device(config)# router bgp 1	BGP を設定します。

	コマンドまたはアクション	目的
ステップ 11	router id { <i>router id</i> } 例 : Device(config-router) # router-id 10.1.1.1	ルータ コンフィギュレーション モードで固定ルータ ID を指定します。
ステップ 12	bgp log-neighbor-changes 例 : Device(config-router) # log-neighbor-changes	BGP ネイバーのステータスが変更された場合に生成されるロギングメッセージの生成を有効にします。
ステップ 13	address-family ipv4 unicast 例 : Device(config-router) # address-family ipv4 unicast	アドレス ファミリ コンフィギュレーションモードを開始し、IPバージョン4ユニキャストアドレスプレフィックスを指定します。
ステップ 14	redistribute direct [route-map <i>map-name</i>] 例 : Device(config-router-af) # redistribute direct route-map any_prefix	インターフェイス上の直接接続されているルートを配布します。
ステップ 15	exit 例 : Device(config-router-af) # exit	アドレス ファミリ コンフィギュレーションモードを終了します。
ステップ 16	address-family l2vpn evpn 例 : Device(config-router) # address-family l2vpn evpn	L2VPN アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーションモードを開始します。evpn キーワードは、EVPN エンドポイントプロビジョニング情報が BGP ピアに配布されるように指定します。
ステップ 17	nexthop route-map <i>name</i> 例 : Device(config-router-af) # nexthop route-map NH-UNCHANGED	特定の特性に一致するルートがあるネクストホップのみを使用して、ボーダークトウェイプロトコル (BGP) ルートが解決されるように指定します。
ステップ 18	retain route-target all 例 : Device(config-router-af) # retain route-target all	指定されたルートターゲットで受信した更新を受け入れます。
ステップ 19	exit 例 :	アドレス ファミリ コンフィギュレーションモードを終了します。

	コマンドまたはアクション	目的
	Device (config-router-af) # exit	
ステップ 20	neighbor vtep1 loopback address remote-as number 例 : Device (config-router) # neighbor 10.11.11.11 remote-as 2	ルータ コンフィギュレーションモードで BGP またはマルチプロトコル BGP ネイバーテーブルにエントリを追加します。
ステップ 21	neighbor ip-address update-source interface-type interface-number 例 : Device (config-router) # neighbor 10.11.11.11 update-source loopback0	BGP セッションが、TCP 接続の動作インターフェイスを使用できるようにします。
ステップ 22	neighbor {ip address peer-group-name} ebgp-multihop [ttl] 例 : Device (config-router) # neighbor 10.11.11.11 ebgp-multihop 10	直接接続されていないネットワークに存在する外部ピアへの BGP 接続を許可します。
ステップ 23	address-family ipv4 unicast 例 : Device (config-router) # address-family ipv4 unicast	アドレス ファミリ コンフィギュレーションモードを開始し、IP バージョン 4 ユニキャストアドレスプレフィックスを指定します。
ステップ 24	neighbor {ip address peer-group-name} send-community both 例 : Device (config-router-af) # neighbor 10.11.11.11 send-community both	標準コミュニティと拡張コミュニティ両方の属性が、BGP ネイバーに送信されるように指定します。
ステップ 25	soft-reconfiguration inbound 例 : Device (config-router-af) # soft-reconfiguration inbound	BGP ピアアップデートの保存を開始するようにスイッチソフトウェアを設定します。
ステップ 26	exit 例 : Device (config-router-af) # exit	アドレス ファミリ コンフィギュレーション モードを終了します。
ステップ 27	address-family l2vpn evpn 例 : Device (config-router) # address-family l2vpn evpn	L2VPN アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーションモードを開始します。evpn キーワードは、EVPN エンドポイントプロビジョニング情報が BGP ピアに配布されるように指定します。

	コマンドまたはアクション	目的
ステップ 28	neighbor {ip address peer-group-name} send-community both 例： Device(config-router-af)# neighbor 10.11.11.11 send-community both	標準コミュニティと拡張コミュニティ両方の属性が、BGP ネイバーに送信されるように指定します。
ステップ 29	neighbor {ip address peer-group-name} route-map map-name {in out} 例： Device(config-router-af)# neighbor 10.11.11.11 route-map NH-UNCHANGED out	インバウンドルートマップを指定されたネイバーから受信したルートに適用します。もしくは、アウトバウンドルートマップを指定されたネイバーへアドバタイズされたルートへ適用します。
ステップ 30	exit 例： Device(config-router-af)# exit	アドレスファミリ コンフィギュレーション モードを終了します。

VTEP での eBGP の設定

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	router bgp number 例： Device(config)# router bgp 2	BGP を設定します。
ステップ 4	bgp router-id interface ループバック アドレス 例： Device(config-router)# bgp router-id interface Loopback0	ループバックアドレスをルータアドレスとして指定します。

	コマンドまたはアクション	目的
ステップ 5	bgp log-neighbor-changes 例 : Device(config-router)# bgp log-neighbor-changes	BGP ネイバーのステータスが変更された場合に生成されるロギングメッセージの生成を有効にします。
ステップ 6	bgp graceful-restart 例 : Device(config-router)# bgp graceful-restart	BGP ネイバーの BGP グレースフル リスタート機能をイネーブルにします。
ステップ 7	neighbor spine 1 loopback address remote-as number 例 : Device(config-router)# neighbor 10.1.1.1 remote-as 1	MP-BGP ネイバーを定義します。各ネイバーの下に <code>l2vpn evpn</code> を定義します。
ステップ 8	neighbor {ip address peer-group-name} ebgp-multihop [ttl] 例 : Device(config-router)# neighbor 10.1.1.1 ebgp-multihop 10	直接接続されていないネットワークに存在する外部ピアへの BGP 接続を許可します。
ステップ 9	neighbor {ip address group-name} update-source interface 例 : Device(config-router)# neighbor 10.1.1.1 update-source Loopback0	更新元を設定します。更新元は、ネイバーごとか、またはピアグループごとに設定できます。
ステップ 10	address-family ipv4 例 : Device(config-router)# address-family ipv4	アドレス ファミリ コンフィギュレーション モードを開始します。
ステップ 11	redistribute connected 例 : Device(config-router-af)# redistribute connected	別のルーティングプロトコルの接続ルートを再配布します。
ステップ 12	neighbor ip-address activate 例 : Device(config-router-af)# neighbor 10.1.1.1 activate	BGP ネイバーからの情報交換を有効にします。
ステップ 13	exit 例 :	アドレス ファミリ コンフィギュレーション モードを終了します。

	コマンドまたはアクション	目的
	Device(config-router-af) # exit-address-family	
ステップ 14	address-family l2vpn evpn 例 : Device(config-router) # address-family l2vpn evpn	L2VPN アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。
ステップ 15	neighbor ip-address activate 例 : Device(config-router-af) # neighbor 10.1.1.1 activate	BGP ネイバーからの情報交換を有効にします。
ステップ 16	neighbor ip-address send-community both 例 : Device(config-router-af) # neighbor 10.1.1.1 send-community both	BGP ネイバーに送信するコミュニティ属性を指定します。
ステップ 17	maximum-paths number-of-paths 例 : Device(config-router-af) # maximum-paths 2	IP ルーティングプロトコルがサポートできる、並列ルートの最大数を制御します。
ステップ 18	exit 例 : Device(config-router-af) # exit-address-family	アドレス ファミリ コンフィギュレーション モードを終了します。
ステップ 19	address-family ipv4 vrf vrf-name 例 : Device(config-router) # address-family ipv4 vrf tenant_1	後続のアドレスファミリ コンフィギュレーションモードコマンドと関連付ける VRF インスタンスの名前を指定します。
ステップ 20	advertise l2vpn evpn 例 : Device(config-router-af) # advertise l2vpn evpn	VXLAN EVPN ファブリックのテナント VFR 内の (L2VPN) EVPN ルートをアドバタイズします。
ステップ 21	redistribute connected 例 : Device(config-router-af) # redistribute connected	別のルーティングプロトコルの接続ルートを再配布します。
ステップ 22	exit 例 :	アドレス ファミリ コンフィギュレーション モードを終了します。

	コマンドまたはアクション	目的
	Device (config-router-af) # exit-address-family	

NVE インターフェイスと VNI の設定

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します (要求された場合)。
ステップ 2	configure terminal 例 : Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	interface nve-interface 例 : Device (config)# interface nve1	NVE インターフェイスを設定します。
ステップ 4	no ip address 例 : Device (config-if)# no ip address	インターフェイスで IP 処理を無効にします。
ステップ 5	source-interface loopback number 例 : Device (config-if)# source-interface Loopback1	ループバック インターフェイスを作成します。 (注) このインターフェイスは、アンダーレイに使用されるループバック インターフェイスとは別のループバックになります。
ステップ 6	host-reachability protocol bgp 例 : Device (config-if)# host-reachability protocol bgp	これはホスト到達可能性のアドバタイズメント機構として BGP を定義します。
ステップ 7	member vni vni associate-vrf 例 : Device (config-if)# member vni 11001 mcast-group 239.0.1.1	レイヤ 3 VNI を、テナント VRF ごとに 1 つずつ、オーバーレイに追加します。 (注) VXLAN ルーティングのみで必要です。

	コマンドまたはアクション	目的
ステップ 8	member vni vni mcast-group address 例 : Device(config-if)# member vni 900001 vrf tenant_1	レイヤ2 VNI をトンネルインターフェイスに追加し、マルチキャストグループを VNI に割り当てます。

すべての VTEP での L2VPN EVPN の設定

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します (要求された場合)。
ステップ 2	configure terminal 例 : Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	l2vpn evpn 例 : Device(config)# l2vpn evpn	L2VPN コンフィギュレーション モードを開始します。
ステップ 4	replication-type static 例 : Device(config-l2vpn)# replication-type static	包括的なマルチキャストイーサネットタグ (IMET) ルートの使用を抑制します。IP マルチキャストは BUM トラフィックに使用されます。
ステップ 5	router-id loopback number 例 : Device(config-l2vpn)# router-id Loopback1	自動生成ルート識別子で使用する IP アドレスを提供するインターフェイスを指定します。
ステップ 6	exit 例 : Device(config-l2vpn)# exit	L2VPN コンフィギュレーション モードを終了します。
ステップ 7	l2vpn evpn instance instance-number vlan-based 例 : Device(config)# l2vpn evpn instance 1 vlan-based	L2VPN コンフィギュレーション モードで VLAN ベースの EVI を設定します。 ルートターゲットまたはルート識別子を手動で設定する必要がない場合、このコマンドはオプションです。

	コマンドまたはアクション	目的
ステップ 8	encapsulation vxlan 例： Device(config-l2vpn)# encapsulation vxlan	カプセル化方式を VXLAN として定義します。
ステップ 9	route-target export route-target-id 例： Device(config-l2vpn)# route-target export 2:1	BGP ルート交換を設定します。
ステップ 10	route-target import route-target-id 例： Device(config-l2vpn)# route-target import 2:1	BGP ルート交換を設定します。
ステップ 11	no auto-route-target 例： Device(config-l2vpn)# no auto-route-target	自動生成されたルートターゲットを削除します。
ステップ 12	exit 例： Device(config-l2vpn)# exit	L2VPN コンフィギュレーション モードを終了します。
ステップ 13	vlan configuration vlan-id 例： Device(config)# vlan configuration 11	VLAN 機能コンフィギュレーション モードを開始します。
ステップ 14	member evpn-instance evpn-instance-number vni vni-number 例： Device(config-vlan)# member evpn-instance 1 vni 11001	EVPN VXLAN VNI インスタンスを設定します。

アクセスカスタマー側 VLAN VTEP の設定

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	interface gigabitethernet slot/port 例： Device(config)# interface GigabitEthernet1/0/11	ギガビット イーサネット インターフェイスでインターフェイス コンフィギュレーション モードを開始します。
ステップ 4	switchport access vlan vlan-id 例： Device(config-if)# switchport access vlan 11	インターフェイスがアクセス モードの場合にアクセス VLAN を設定します。
ステップ 5	switchport mode access 例： Device(config-if)# switchport mode access	トランキングなし、タグなしの単一 VLAN イーサネット インターフェイスとして、インターフェイスを設定します。
ステップ 6	exit 例： Device(config-if)# exit	インターフェイス コンフィギュレーション モードを終了します。
ステップ 7	interface gigabitethernet slot/port 例： Device(config)# interface TenGigabitEthernet1/1/7	ギガビット イーサネット インターフェイスでインターフェイス コンフィギュレーション モードを開始します。
ステップ 8	switchport trunk allowed vlan vlan_list 例： Device(config-if)# switchport trunk allowed vlan 11-210,901-905	インターフェイスに許可された VLAN の VLAN ID を設定します。
ステップ 9	switchport mode trunk 例： Device(config-if)# switchport mode trunk	インターフェイスをイーサネット トランク ポートとして設定します。

VxLAN 間ルーティングに対応した VTEP での IP VRF の設定

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	vrf definition vrf-name 例： Device(config)# vrf definition tenant_1	Virtual Routing and Forwarding (VRF) ルーティングテーブルインスタンスを設定し、VRF コンフィギュレーションモードを開始します。
ステップ 4	rd route-distinguisher 例： Device(config-vrf)# rd 1:1	VRF のルーティング テーブルと転送 テーブルを作成します。
ステップ 5	address-family ipv4 例： Device(config-vrf)# address-family ipv4	アドレス ファミリ コンフィギュレーション モードを開始します。
ステップ 6	route-target export route-target-id 例： Device(config-vrf-af)# route-target export 1:1	同じパラメータを持つ VRF のエクスポート RT のリストを作成します。
ステップ 7	route-target import route-target-id 例： Device(config-vrf-af)# route-target import 1:1	同じパラメータを持つ VRF のインポート RT のリストを作成します。
ステップ 8	route-target import route-target-id stitching 例： Device(config-vrf-af)# route-target import 1:1 stitching	一致するルートターゲット値を持つルートを EVPN BGP からのインポートするように設定します。

	コマンドまたはアクション	目的
ステップ 9	route-target export route-target-id stitching 例 : Device(config-vrf-af) # route-target export 1:1 stitching	VRF から EVPN BGP へのルートのエクスポートを設定し、指定されたルートターゲット識別子を BGP EVPN に割り当てます。
ステップ 10	exit-address-family 例 : Device(config-vrf-af) # exit-address-family	アドレスファミリ コンフィギュレーション モードを終了します。

VXLAN BGP EVPN 設定の確認

コマンド	目的
show nve vni	NVE に関連付けられている VNI を表示します。
show ip mroute	マルチキャストルーティングテーブル情報を表示します。
show ip mfib	IPv4 マルチキャスト転送情報ベース (MFIB) の転送エントリとインターフェイスを表示します。
show ip pim neighbors	PIM ネイバーテーブルを表示します。
show ip pim tunnel	インターフェイス上の PIM レジスタのカプセル化およびカプセル化解除トンネルに関する情報を表示します。
show ip pim rp	RP に関するマッピング情報を表示します。
show l2vpn evpn evi [evpn-id all]	特定の EVI またはすべての EVI の詳細情報を表示します。
show mac address-table vlan vlan id	特定の VLAN の情報を表示します。
show l2route evpn mac [all evi vlan-id]	EVPN コントロールプレーンでスイッチが学習した MAC アドレスと IP アドレス情報を表示します。
show bgp l2vpn evpn	L2VPN-EVPN アドレスファミリの BGP 情報を表示します。

コマンド	目的
<code>show ip vrf vrf-name</code>	現在のルータに存在するすべての VRF と、それらに関連付けられたルート識別子とインターフェイスの概要を表示します。
<code>show bgp vpnv4 unicast vrf vrf-name</code>	特定の VRF について、BGP テーブルの VPNv4 ルートを表示します。
<code>show ip route vrf vrf-name</code>	特定の VRF に関連付けられた IP ルーティングテーブルを表示します。
<code>show l2vpn evpn mac</code>	レイヤ 2 EVPN の MAC アドレスデータベースを表示します。
<code>show l2vpn evpn mac ip</code>	レイヤ 2 EVPN の IP アドレスデータベースを表示します。
<code>show l2route evpn mac ip</code>	MAC IP ルートを表示します。



- (注) BGP 設定の確認には `show ip bgp` コマンドが利用可能ですが、ベストプラクティスとして好ましいのは、その代わりに `show bgp` コマンドを使用することです。

VXLAN BGP EVPN (EBGP) の設定例

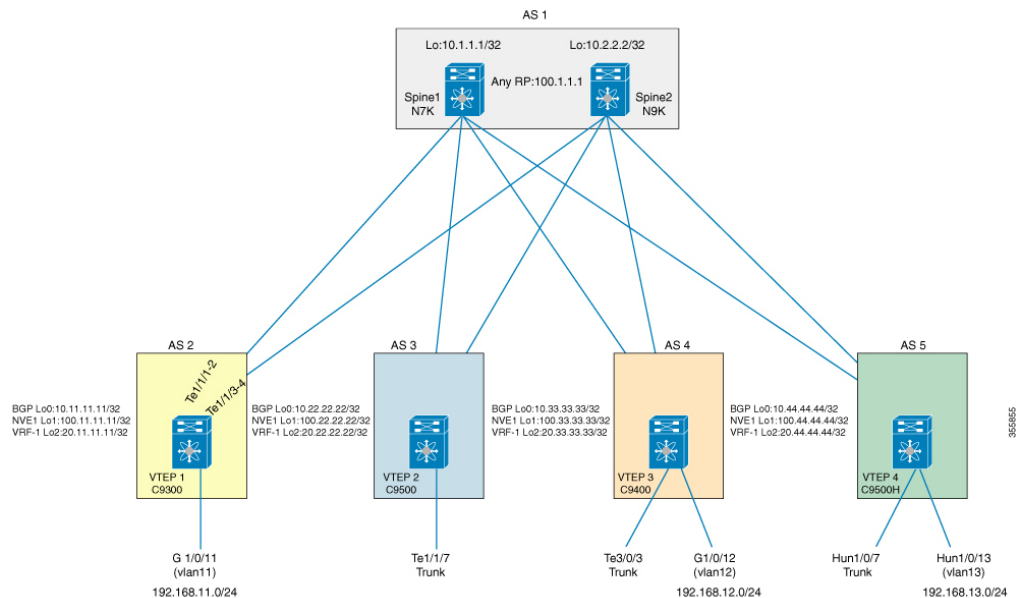
次のセクションでは、VXLAN BGP EVPN のさまざまな設定例を示します。

ブリッジモードでの VxLAN BGP EVPN の設定例

次のセクションでは、ブリッジモードでの VxLAN BGP EVPN のさまざまな例について説明します。

例：eBGP Multi-AS EVPN VxLAN 設計モデルの設定

図 32：eBGP Multi-AS 設計モデルで使用されるトポロジ



例：すべての VTEP とスパイン間のアンダーレイトランスポート（ユニキャストおよびマルチキャスト）の設定

例

スパインと VTEP 間の eBGP ピアリングには、IP 接続が必要です。これは、スタティックルートを使用して VTEP とスパイン間のループバックアドレスに到達することで実現できます。

スパインの設定



(注) 次のスパイン設定は、Cisco Nexus シリーズ スイッチに適用でき、Cisco Catalyst 9000 ファミリスイッチには適用できません。

```
Device(config)# ip pim rp-address 100.1.1.1 group-list 239.0.0.0/8
Device(config)# ip pim rp-candidate loopback1 group-list 239.0.0.0/8
Device(config)# ip pim anycast-rp 100.1.1.1 10.1.1.1
Device(config)# ip pim anycast-rp 100.1.1.1 10.2.2.2
!
Device(config)# interface loopback0
Device(config-if)# ip address 10.1.1.1/32
Device(config-if)# ip pim sparse-mode
!
Device(config)# interface loopback1
```

```

Device(config-if)# ip address 100.1.1.1/32
Device(config-if)# ip pim sparse-mode
!
Device(config)# interface port-channel1
Device(config-if)# mtu 9198
Device(config-if)# medium p2p
Device(config-if)# ip address 10.10.1.1/30
Device(config-if)# ip pim sparse-mode
!

```

```

Device(config)# interface port-channel2
Device(config-if)# mtu 9198
Device(config-if)# medium p2p
Device(config-if)# ip address 10.10.2.1/30
Device(config-if)# ip pim sparse-mode
!

```

```

Device(config)# interface port-channel3
Device(config-if)# mtu 9198
Device(config-if)# medium p2p
Device(config-if)# ip address 10.10.3.1/30
Device(config-if)# ip pim sparse-mode

```

VTEP の設定

```

Device(config)# ip multicast-routing
Device(config)# ip pim rp-address 100.1.1.1
!
Device(config)# ip routing
!
Device(config)# interface Loopback0
Device(config-if)# ip address 10.11.11.11 255.255.255.255
Device(config-if)# ip pim sparse-mode
Device(config-if)# exit
!
Device(config)# interface Loopback1
Device(config-if)# ip address 100.11.11.11 255.255.255.255
Device(config-if)# ip pim sparse-mode
Device(config-if)# exit
!
Device(config)# interface Loopback2
Device(config-if)# vrf forwarding tenant_1
Device(config-if)# ip address 11.11.11.11 255.255.255.255
Device(config-if)# exit
!
Device(config)# interface Port-channel1
Device(config-if)# no switchport
Device(config-if)# ip address 10.10.1.2 255.255.255.252
Device(config-if)# ip pim sparse-mode
Device(config-if)# exit
!
Device(config)# interface Port-channel11
Device(config-if)# no switchport
Device(config-if)# ip address 20.20.1.2 255.255.255.252
Device(config-if)# ip pim sparse-mode
Device(config-if)# exit
!
Device(config)# interface TenGigabitEthernet1/1/2
Device(config-if)# no switchport
Device(config-if)# no ip address
Device(config-if)# channel-group 1 mode active
Device(config-if)# exit
!
Device(config)# interface TenGigabitEthernet1/1/3

```

例：スパインと VTEP 間の EVPN アドレスファミリーを使用した eBGP の設定

```
Device(config-if)# no switchport
Device(config-if)# no ip address
Device(config-if)# channel-group 11 mode active
```

例：スパインと VTEP 間の EVPN アドレスファミリーを使用した eBGP の設定

例

次の例は、スパインの設定方法を示しています



(注) 次のスパイン設定は、Cisco Nexus シリーズ スイッチに適用でき、Cisco Catalyst 9000 ファミリスイッチには適用できません。

```
Device(config)# ip prefix-list lo_prefix seq 5 permit 0.0.0.0/0 le 32
Device(config)# route-map NH-UNCHANGED permit 10
Device(config-route-map)# set ip next-hop unchanged
Device(config-route-map)# exit
Device(config)# route-map any_prefix permit 10
Device(config-route-map)# match ip address prefix-list lo_prefix
Device(config-route-map)# exit
!
Device(config)# router bgp 1
Device(config-router)# router-id 10.1.1.1
Device(config-router)# log-neighbor-changes
Device(config-router)# address-family ipv4 unicast
Device(config-router-af)# redistribute direct route-map any_prefix
Device(config-router-af)# exit
Device(config-router)# address-family l2vpn evpn
Device(config-router-af)# nexthop route-map NH-UNCHANGED
Device(config-router-af)# retain route-target all
Device(config-router-af)# exit
!
Device(config-router)# neighbor 10.11.11.11 remote-as 2
Device(config-router)# neighbor 10.11.11.11 update-source loopback0
Device(config-router)# neighbor 10.11.11.11 ebgp-multihop 10
Device(config-router)# address-family ipv4 unicast
Device(config-router-af)# neighbor 10.11.11.11 send-community both
Device(config-router-af)# soft-reconfiguration inbound
Device(config-router-af)# exit
Device(config-router)# address-family l2vpn evpn
Device(config-router-af)# neighbor 10.11.11.11 send-community both
Device(config-router-af)# neighbor 10.11.11.11 route-map NH-UNCHANGED out
```

次の例は、VTEP の設定方法を示しています

```
Device(config)# router bgp 2
Device(config-router)# bgp router-id interface Loopback0
Device(config-router)# bgp log-neighbor-changes
Device(config-router)# bgp graceful-restart
Device(config-router)# neighbor 10.1.1.1 remote-as 1
Device(config-router)# neighbor 10.1.1.1 ebgp-multihop 10
Device(config-router)# neighbor 10.1.1.1 update-source Loopback0
!
Device(config-router)# address-family ipv4
Device(config-router-af)# redistribute connected
Device(config-router-af)# neighbor 10.1.1.1 activate
```

```
Device(config-router-af)# exit-address-family
!
Device(config-router)# address-family l2vpn evpn
Device(config-router-af)# neighbor 10.1.1.1 activate
Device(config-router-af)# neighbor 10.1.1.1 send-community both
Device(config-router-af)# maximum-paths 2
Device(config-router-af)# exit-address-family
!
Device(config-router)# address-family ipv4 vrf tenant_1
Device(config-router-af)# advertise l2vpn evpn
Device(config-router-af)# redistribute connected
Device(config-router-af)# exit-address-family
```

例：すべての VTEP での NVE の設定

例

次の例は、VTEP の設定方法を示しています

```
Device(config)# interface nve1
Device(config-if)# no ip address
Device(config-if)# source-interface Loopback1
Device(config-if)# host-reachability protocol bgp
Device(config-if)# member vni 11001 mcast-group 239.0.1.1
Device(config-if)# member vni 11002 mcast-group 239.0.1.1
Device(config-if)# member vni 900001 vrf tenant_1
```

例：VTEP での L2VPN EVPN の設定

例

次の例は、VTEP の設定方法を示しています

```
Device(config)# l2vpn evpn
Device(config-l2vpn)# replication-type static
Device(config-l2vpn)# router-id Loopback1
!
Device(config)# l2vpn evpn instance 1 vlan-based
Device(config-l2vpn)# encapsulation vxlan
Device(config-l2vpn)# route-target export 2:1
Device(config-l2vpn)# route-target import 2:1
Device(config-l2vpn)# no auto-route-target
!
Device(config)# l2vpn evpn instance 2 vlan-based
Device(config-l2vpn)# encapsulation vxlan
Device(config-l2vpn)# route-target export 2:2
Device(config-l2vpn)# route-target import 2:2
Device(config-l2vpn)# no auto-route-target
```

例：アクセスカスタマー側 VLAN VTEP の設定

例

次の例は、VTEP の設定方法を示しています

```
Device(config)# interface GigabitEthernet1/0/11
Device(config-if)# switchport access vlan 11
Device(config-if)# switchport mode access
!
Device(config)# interface TenGigabitEthernet1/1/7
Device(config-if)# switchport trunk allowed vlan 11-210,901-905
Device(config-if)# switchport mode trunk
```

例：VTEP での追加の VNI、EVI、および VLAN の設定

例

```
Device(config)# vlan 4000
Device(config-vlan)# state active
Device(config)# vlan configuration 4000
Device(config-vlan)# member evpn-instance 20000
```

例

次の例は、VTEP の設定方法を示しています

```
Device(config)# vlan 11
Device(config-vlan)# state active
Device(config)# vlan 12
Device(config-vlan)# state active
Device(config)# vlan 901
Device(config-vlan)# state active
!
Device(config)# vlan configuration 11
Device(config-vlan)# member evpn-instance 1 vni 11001
!
Device(config)# vlan configuration 12
Device(config-vlan)# member evpn-instance 2 vni 11002
!

Device(config)# vlan configuration 901
Device(config-vlan)# member vni 900001
!
Device(config)# interface Vlan901
description connected to vni_900001
Device(config-if)# vrf forwarding tenant_1
Device(config-if)# ip unnumbered Loopback2
!
Device(config)# interface nve1
Device(config-if)# no ip address
Device(config-if)# source-interface Loopback1
Device(config-if)# host-reachability protocol bgp
Device(config-if)# member vni 11001 mcast-group 239.0.1.1
Device(config-if)# member vni 11002 mcast-group 239.0.1.1
Device(config-if)# member vni 900001 vrf tenant_1
```


例 : VXLAN 間ルーティングに対応した VTEP での IP VRF の設定

例

次の例は、VTEP の設定方法を示しています

```
Device(config)# vrf definition tenant_1
Device(config-vrf)# rd 1:1
!
Device(config-vrf)# address-family ipv4
Device(config-vrf-af)# route-target export 1:1
Device(config-vrf-af)# route-target import 1:1
Device(config-vrf-af)# route-target export 1:1 stitching
Device(config-vrf-af)# route-target import 1:1 stitching
Device(config-vrf-af)# exit-address-family
```

例 : VTEP でのアクセス VLAN インターフェイス (SVI) の設定

例

次の例は、VTEP の設定方法を示しています

```
Device(config)# interface Vlan11
description vni_11001
mac-address 0001.0001.0001
Device(config-if)# vrf forwarding tenant_1
Device(config-if)# ip address 192.168.1.254 255.255.255.0
Device(config-if)# exit
Device(config)# interface Vlan12
description vni_11002
mac-address 0001.0001.0001
Device(config-if)# vrf forwarding tenant_1
Device(config-if)# ip address 192.168.2.254 255.255.255.0
Device(config-if)# exit
```

例 : NVE インターフェイスでの追加の L3-VNI の設定

例

次の例は、VTEP の設定方法を示しています

```
Device(config)# interface nve1
Device(config-if)# no ip address
Device(config-if)# source-interface Loopback1
Device(config-if)# host-reachability protocol bgp
Device(config-if)# member vni 11001 mcast-group 239.0.1.1
Device(config-if)# member vni 11002 mcast-group 239.0.1.1
Device(config-if)# member vni 900001 vrf tenant_1
```

例：コア側 VLAN および VLAN インターフェイスの設定

例

次の例は、VTEP の設定方法を示しています

```
Device(config)# vlan configuration 901
Device(config-vlan)# member vni 900001
Device(config)# exit
!
Device(config)# interface Vlan901
description connected to vni_900001
Device(config-if)# vrf forwarding tenant_1
Device(config-if)# ip unnumbered Loopback2
```

例：iBGP/IGP EVPN VxLAN 設計モデルの設定

例

スパインの設定



(注) 次のスパイン設定は、Cisco Nexus シリーズ スイッチに適用でき、Cisco Catalyst 9000 ファミリスイッチには適用できません。

```
Device(config)# feature-set fabric
Device(config)# hostname spine-1
!
Device(config)# feature telnet
Device(config)# feature scp-server
Device(config)# feature fabric forwarding
Device(config)# nv overlay evpn
Device(config)# feature ospf
Device(config)# feature bgp
Device(config)# feature pim
Device(config)# feature ipp
Device(config)# feature isis
Device(config)# feature fabric multicast
Device(config)# feature interface-vlan
Device(config)# feature lldp
Device(config)# feature fabric access
Device(config)# feature nv overlay
Device(config)# feature nxapi
!

Device(config)# ip pim rp-address 4.5.4.5 group-list 224.0.0.0/4
!

Device(config)# vlan 1
!

Device(config)# interface Vlan1
!

Device(config)# interface Ethernet1/1 ip address 10.14.1.4/24
```

```

Device(config-if)# ip router ospf 1 area 0.0.0.0
Device(config-if)# ip pim sparse-mode
Device(config-if)# no shutdown
!
Device(config)# interface loopback0
Device(config-if)# ip address 4.4.4.4/32
Device(config-if)# ip router ospf 1 area 0.0.0.0
Device(config-if)# ip pim sparse-mode
Device(config-if)# interface loopback1
Device(config-if)# ip address 4.5.4.5/32
Device(config-if)# ip router ospf 1 area 0.0.0.0
Device(config-if)# ip pim sparse-mode
!
Device(config)# router ospf 1
Device(config-router)# router-id 4.4.4.4
!
Device(config)# router bgp 100
Device(config-router)# router-id 4.4.4.4
Device(config-router)# address-family l2vpn evpn
Device(config-router-af)# neighbor 1.1.1.1 remote-as 100
Device(config-router-af)# update-source loopback0
Device(config-router-af)# address-family ipv4 unicast
Device(config-router-af)# send-community both
Device(config-router-af)# route-reflector-client
Device(config-router-af)# address-family l2vpn evpn
Device(config-router-af)# send-community both
Device(config-router-af)# route-reflector-client

```

VTEP の設定

```

Device(config)# vrf definition l3vni50000
Device(config-vrf)# rd 101:1
!
Device(config-vrf)# address-family ipv4
Device(config-vrf-af)# route-target export 100:1 stitching
Device(config-vrf-af)# route-target import 100:1 stitching
Device(config)# exit-address-family
!
Device(config)# ip multicast-routing
Device(config)# ip pim rp-address 4.5.4.5
!
Device(config)# l2vpn evpn
Device(config-l2vpn)# replication-type static
Device(config-l2vpn)# exit

!
Device(config)# vlan 10
Device(config-vlan)# State active
Device(config-vlan)# exit
Device(config)# vlan 11
Device(config-vlan)# State active
Device(config-vlan)# exit
Device(config)# vlan 501
Device(config-vlan)# state active
Device(config-vlan)# exit
!
Device(config)# vlan configuration 10
Device(config-vlan)# member evpn-instance 10 vni 100010
Device(config-vlan)# exit
!
Device(config)# vlan configuration 11
Device(config-vlan)# member evpn-instance 11 vni 100011
Device(config-vlan)# exit

```

```

!
Device(config)# vlan configuration 501
Device(config-vlan)# member vni 50000
Device(config-vlan)# exit
!
Device(config)# interface Loopback0
Device(config-if)# ip address 1.1.1.1 255.255.255.255
Device(config-if)# ip pim sparse-mode
Device(config-if)# ip ospf 1 area 0
Device(config-if)# exit
!
Device(config)# interface GigabitEthernet1/0/1
Device(config-if)# switchport mode trunk
Device(config-if)# exit
!
Device(config)# interface GigabitEthernet1/0/2
Device(config-if)# switchport access vlan 10
Device(config-if)# switchport mode access
Device(config-if)# exit
!
Device(config)# interface TenGigabitEthernet3/0/1
description To Spine1
Device(config-if)# no switchport
Device(config-if)# ip address 10.14.1.1 255.255.255.0
Device(config-if)# ip pim sparse-mode
Device(config-if)# ip ospf 1 area 0
Device(config-if)# exit
!
Device(config)# interface TenGigabitEthernet3/0/2
description To Spine1
Device(config-if)# no switchport
Device(config-if)# ip address 10.15.1.1 255.255.255.0
Device(config-if)# ip pim sparse-mode
Device(config-if)# ip ospf 1 area 0
Device(config-if)# exit
!
Device(config)# interface Vlan10
description connected to 100010
Device(config-if)# mac-address 0001.0001.0001
Device(config-if)# vrf forwarding 13vni50000
Device(config-if)# ip address 192.168.10.1 255.255.255.0
Device(config-if)# exit
!
Device(config)# interface Vlan11
description connected to 100011
Device(config-if)# mac-address 0001.0001.0001
Device(config-if)# vrf forwarding 13vni50000
Device(config-if)# ip address 192.168.11.1 255.255.255.0
Device(config-if)# exit
!
Device(config)# interface Vlan501
description connected to 50000
Device(config-if)# vrf forwarding 13vni50000
Device(config-if)# ip unnumbered Loopback0
Device(config-if)# exit
!
Device(config)# router ospf 1
Device(config-router)# router-id 1.1.1.1
Device(config-router)# nsr
Device(config-router)# exit
!
Device(config)# router bgp 100
Device(config-router)# bgp router-id 1.1.1.1

```

```

Device(config-router)# bgp log-neighbor-changes
Device(config-router)# bgp graceful-restart
Device(config-router)# neighbor 4.4.4.4 remote-as 100
Device(config-router)# neighbor 4.4.4.4 update-source Loopback0
!
Device(config-router)# address-family ipv4
Device(config-router-af)# redistribute connected
Device(config-router-af)# neighbor 4.4.4.4 activate
Device(config-router-af)# exit-address-family
!
Device(config-router)# address-family l2vpn evpn
Device(config-router-af)# neighbor 4.4.4.4 activate
Device(config-router-af)# neighbor 4.4.4.4 send-community both
Device(config-router-af)# exit-address-family
!
Device(config)# address-family ipv4 vrf l3vni50000
Device(config-vrf-af)# advertise l2vpn evpn
Device(config-vrf-af)# redistribute connected
Device(config-vrf-af)# exit-address-family
Device(config-vrf)# exit
!
Device(config)# interface nvel
Device(config-if)# no ip address
Device(config-if)# source-interface Loopback0
Device(config-if)# host-reachability protocol bgp
Device(config-if)# member vni 100010 mcast-group 227.0.0.1
Device(config-if)# member vni 100011 mcast-group 227.0.0.1
Device(config-if)# member vni 50000 vrf l3vni50000

```

例：NVE での L2/L3 VNI の確認

例

次は、**show nve vni** コマンドの出力例です。

```

Device# show nve vni

Interface VNI Multicast-group VNI state Mode VLAN cfg vrf
nvel 60519 233.1.1.19 Up L2CP 519 CLI N/A
nvel 60518 233.1.1.18 Up L2CP 518 CLI N/A

```

例：マルチキャストルーティングテーブルのマルチキャストの確認

例

次は、**show ip mroute** コマンドの出力例です。

```

Device# show ip mroute
IP Multicast Routing Table
Outgoing interface flags: H - Hardware switched, A - Assert winner, p - PIM Join
Timers: Uptime/Expires
Interface state: Interface, Next-Hop or VCD, State/Mode
(*, 239.0.1.1), 5d16h/stopped, RP 100.1.1.1, flags: SJCFx
Incoming interface: Port-channel11, RPF nbr 20.20.1.1
Outgoing interface list:
Tunnel0, Forward/Sparse-Dense, 5d16h/00:01:17
!

```

例：マルチキャストルーティングテーブルのマルチキャストの確認

```
(100.11.11.11, 239.0.1.1), 00:02:18/00:00:41, flags: FTx
Incoming interface: Loopback1, RPF nbr 0.0.0.0, Registering
Outgoing interface list:
Port-channell1, Forward/Sparse, 00:02:18/00:03:14
```

例

次は、**show ip mfib** コマンドの出力例です。

```
Device# show ip mfib
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts: Total/RPF failed/Other drops
I/O Item Counts: FS Pkt Count/PS Pkt Count
Default
(*,224.0.0.0/4) Flags: C HW
SW Forwarding: 0/0/0/0, Other: 0/0/0
HW Forwarding: 0/0/0/0, Other: 0/0/0
(*,224.0.1.40) Flags: C HW
SW Forwarding: 0/0/0/0, Other: 0/0/0
HW Forwarding: 0/0/0/0, Other: 0/0/0
Port-channell1 Flags: A NS
Loopback0 Flags: F IC NS
Pkts: 0/0
(*,239.0.1.1) Flags: C HW
SW Forwarding: 0/0/0/0, Other: 0/0/0
HW Forwarding: 187/0/190/0, Other: 0/0/0
Port-channell1 Flags: A NS
Tunnel0, VXLAN Decap Flags: F NS
Pkts: 0/0
(100.11.11.11,239.0.1.1) Flags: HW
SW Forwarding: 0/0/0/0, Other: 0/0/0
HW Forwarding: 0/0/0/0, Other: 0/0/0
Null0 Flags: A NS
Port-channell1 Flags: F NS
Pkts: 0/0
Tunnell1 Flags: F
Pkts: 0/0
```

例

次は、**show ip pim neighbors** コマンドの出力例です。

```
Device# show ip pim neighbors
PIM Neighbor Table
Mode: B - Bidir Capable, DR - Designated Router, N - Default DR Priority,
P - Proxy Capable, S - State Refresh Capable, G - GenID Capable,
L - DR Load-balancing Capable
Neighbor Interface Uptime/Expires Ver DR
Address Prio/Mode
10.10.1.1 Port-channell1 5d16h/00:01:40 v2 1 / G
20.20.1.1 Port-channell1 5d16h/00:01:20 v2 1 / G
```

例

次は、**show ip pim tunnel** コマンドの出力例です。

```
Device# show ip pim tunnel
Tunnell1*
```

```

Type : PIM Encap
RP : 100.1.1.1
Source : 20.20.1.2
State : UP
Last event : Created (5d16h)
# sh ip pim rp
Group: 239.0.1.1, RP: 100.1.1.1, uptime 5d16h, expires never

```

例：EVPN マネージャでの EVPN インスタンスの確認

例

次は、**show l2vpn evpn evi** コマンドの出力例です。

```

Device# show l2vpn evpn evi 1 detail
EVPN instance: 1 (VLAN Based)
RD: 100.11.11.11:1 (auto)
Import-RTs: 2:1
Export-RTs: 2:1
Per-EVI Label: none
State: Established
Encapsulation: vxlan
Vlan: 11
Ethernet-Tag: 0
State: Established
Core If: Vlan901
Access If: Vlan11
RMAC: ec1d.8b75.eac8
Core Vlan: 901
L2 VNI: 11001
L3 VNI: 900001
VTEP IP: 100.11.11.11
MCAST IP: 239.0.1.1
VRF: tenant_1
Pseudoports:
TenGigabitEthernet1/1/7 service instance 11

```

例：MAC テーブルの確認

例

次は、**show mac address-table vlan** コマンドの出力例です。

```

Device# show mac address-table vlan 11
Mac Address Table
-----
Vlan Mac Address Type Ports
-----
11 0001.0001.0001 STATIC V111 -----□ SVI mac for Anycast Gateway
11 0011.0011.0005 DYNAMIC Tel/1/7-----□ dynamically learned
Total Mac Addresses for this criterion: 2

```

例：EVPN マネージャでの MAC エントリの確認

例：EVPN マネージャでの MAC エントリの確認

例

次は、`show l2vpn evpn mac` コマンドの出力例です。

```
Device# show l2vpn evpn mac
MAC Address EVI VLAN ESI Ether Tag Next Hop
-----
0011.0011.00c9 1 11 0000.0000.0000.0000.0000 0 Te1/1/7:11
0012.0012.0001 1 11 0000.0000.0000.0000.0000 0 100.22.22.22
0013.0013.0001 1 11 0000.0000.0000.0000.0000 0 100.33.33.33
0014.0014.0001 1 11 0000.0000.0000.0000.0000 0 100.44.44.44
```

例：BGP での MAC ルートの確認

例

次は、`show bgp l2vpn evpn evi` コマンドの出力例です。

```
Device# show bgp l2vpn evpn evi 1
BGP table version is 654847, local router ID is 10.11.11.11
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
x best-external, a additional-path, c RIB-compressed,
t secondary path, L long-lived-stale,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found
Network Next Hop Metric LocPrf Weight Path
Route Distinguisher: 100.11.11.11:1
*> [2][100.11.11.11:1][0][48][0011001100c9][0][*]/20
:: 32768 ?
*> [2][100.11.11.11:1][0][48][001200120001][0][*]/20
100.22.22.22 0 1 3 ?
*> [2][100.11.11.11:1][0][48][001200120001][32][192.168.1.2]/24
100.22.22.22 0 1 3 ?
*> [2][100.11.11.11:1][0][48][001300130001][0][*]/20
100.33.33.33 0 1 4 ?
*> [2][100.11.11.11:1][0][48][001300130001][32][192.168.1.3]/24
100.33.33.33 0 1 4 ?
*> [2][100.11.11.11:1][0][48][001400140001][0][*]/20
100.44.44.44 0 1 4 ?
*> [2][100.11.11.11:1][0][48][001400140001][32][192.168.1.4]/24
100.44.44.44 0 1 4 ?
```

例：レイヤ2 ルーティング情報ベースでの MAC ルートの確認

例

次は、`show l2route evpn mac` コマンドの出力例です。

```
Device# show l2route evpn mac
EVI ETag Prod Mac Address Next Hop(s) Seq Number
-----
1 0 BGP 0012.0012.0001 V:11001 100.22.22.22 0
1 0 BGP 0013.0013.0001 V:11001 100.33.33.33 0
```



```
1 0 BGP 0014.0014.0001 V:11001 100.44.44.44 0
1 0 L2VPN 0011.0011.00c9 Te1/1/7:11 0
```

例：すべての SVI での IP VRF の確認

例

次は、**show ip vrf** コマンドの出力例です。

```
Device# show ip vrf
Name                Default RD          Interfaces
Mgmt-vrf            <not set>          Gi0/0
tenant_1            1:1                Lo2
                   V111
                   V112
```

例：MAC VRF (EVI) の MAC/IP エントリの確認

例

次は、**show bgp l2vpn evpn evi** コマンドの出力例です。

```
Device# show bgp l2vpn evpn evi 1 route-type 2
BGP routing table entry for [2][100.11.11.11:1][0][48][0011001100C9][32][10.0.0.2]/24,
version 7
Paths: (1 available, best #1, table evi_1)
  Advertised to update-groups:
    1
  Refresh Epoch 1
  Local
    :: (via default) from 0.0.0.0 (10.11.11.11)
      Origin incomplete, localpref 100, weight 32768, valid, sourced, local, best
      EVPN ESI: 00000000000000000000, Label1 11001-□ L2 VNI
      Extended Community: RT:2:1 ENCAP:8
      Local irb vxlan vtep:
        vrf:tenant_1, l3-vni:900001-----□ IP VRF and L3 VNI
        local router mac:EC1D.8B75.EAC8
        core-irb interface:Vlan901----□ core SVI
        vtep-ip:100.11.11.11
      rx pathid: 0, tx pathid: 0x0
```

例：L3VNI (IP VRF) でのリモート MAC/IP および IP プレフィックスルートの確認

例

次は、**show bgp vpnv4 unicast vrf** コマンドの出力例です。

```
Device# show bgp vpnv4 unicast vrf tenant_1
BGP table version is 8583, local router ID is 10.11.11.11
  Network          Next Hop          Metric LocPrf Weight Path
Route Distinguisher: 1:1 (default for vrf tenant_1)
AF-Private Import to Address-Family: L2VPN E-VPN, Pfx Count/Limit: 11/1000
*>  11.11.11.11/32  0.0.0.0           0           32768 ?
*>  11.22.22.22/32  100.22.22.22     0           1 3 ?
*>  11.33.33.33/32  100.33.33.33     0           1 4 ?
```

例：IP ルートが L3 VNI (IP VRF) にインストールされていることの確認

```
*> 11.44.44.44/32 100.44.44.44 0 1 4 ?
* 192.168.1.0 100.44.44.44 0 1 4 ?
* 100.33.33.33 0 1 4 ?
* 100.22.22.22 0 1 3 ?
*> 0.0.0.0 0 32768 ?
*> 192.168.1.2/32 100.22.22.22 0 1 3 ?
*> 192.168.1.3/32 100.33.33.33 0 1 4 ?
*> 192.168.1.4/32 100.44.44.44 0 1 4 ?
* 192.168.2.0 100.44.44.44 0 1 4 ?
* 100.33.33.33 0 1 4 ?
* 100.22.22.22 0 1 3 ?
*> 0.0.0.0 0 32768 ?
```

例：IP ルートが L3 VNI (IP VRF) にインストールされていることの確認

例

次に、**show ip route vrf** コマンドの出力例を示します。

```
Device# show ip route vrf tenant_1
Routing Table: tenant_1
Gateway of last resort is not set

11.0.0.0/32 is subnetted, 3 subnets
C 11.11.11.11 is directly connected, Loopback2
B 11.22.22.22 [20/0] via 100.22.22.22, 00:13:21, Vlan901
B 11.33.33.33 [20/0] via 100.33.33.33, 00:13:21, Vlan901
B 11.44.44.44 [20/0] via 100.44.44.44, 00:12:51, Vlan901
192.168.1.0/24 is variably subnetted, 4 subnets, 2 masks
C 192.168.1.0/24 is directly connected, Vlan11
B 192.168.1.3/32 [20/0] via 100.33.33.33, 16:26:48, Vlan901
B 192.168.1.4/32 [20/0] via 100.44.44.44, 2d19h, Vlan901
L 192.168.1.254/32 is directly connected, Vlan11
192.168.2.0/24 is variably subnetted, 4 subnets, 2 masks
C 192.168.2.0/24 is directly connected, Vlan12
B 192.168.2.3/32 [20/0] via 100.33.33.33, 02:52:20, Vlan901
B 192.168.2.4/32 [20/0] via 100.44.44.44, 2d19h, Vlan901
L 192.168.2.254/32 is directly connected, Vlan12
192.168.3.0/24 is variably subnetted, 4 subnets, 2 masks
C 192.168.3.0/24 is directly connected, Vlan13
B 192.168.3.3/32 [20/0] via 100.33.33.33, 2d19h, Vlan901
```

例：EVPN マネージャでの MAC/IP エントリの確認

例

次に、**show l2vpn evpn mac** コマンドの出力例を示します。

```
Device# show l2vpn evpn mac ip

IP Address EVI VLAN MAC Address Next Hop(s)
-----
10.0.0.1 1 11 0011.0011.00c9 Te1/1/7:11
10.0.0.2 1 11 0012.0012.0001 100.22.22.22
```

例：レイヤ2ルーティング情報ベースの MAC/IP ルートの確認

例

次に、`show l2route evpn mac` コマンドの出力例を示します。

```
Device# show l2route evpn mac ip
EVI ETag Prod Mac Address Host IP Next Hop(s)
-----
1 0 BGP 0012.0012.0001 10.0.0.2 V:11001 100.22.22.22
1 0 L2VPN 0011.0011.00c9 10.0.0.1 Te1/1/7:11
```

VXLAN BGP EVPN の機能の履歴と情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 19: VXLAN BGP EVPN の機能の履歴

リリース	機能情報
Cisco IOS XE Fuji 16.9.1	<p>VXLAN は、レイヤ2 セグメントを IP コア全体にストレッチできる IP/UDP オーバーレイの MAC です。VXLAN EVPN BGP は、ブリッジモードとルーテッドモードで動作します。</p> <p>この機能は、ブリッジモードでの IPv4 および IPv6 サポートと、ルーテッドモードでの IPv4 サポートで導入されました。</p>



第 12 章

VXLAN EVPN 入力複製の設定

このセクションでは、VxLAN EVPN の入力複製の設定に関連する手順について説明します。

- [VXLAN EVPN 入力複製の前提条件 \(255 ページ\)](#)
- [VXLAN EVPN 入力複製に関する情報 \(255 ページ\)](#)
- [VXLAN EVPN 入力複製の設定 \(256 ページ\)](#)
- [VxLAN EVPN 入力複製の設定例 \(259 ページ\)](#)
- [VxLAN EVPN 入力複製の機能情報 \(264 ページ\)](#)

VXLAN EVPN 入力複製の前提条件

- VXLAN を有効にする必要があります。
- VXLAN 経由の EVPN の入力複製では、IMET ルート（ルートタイプ 3 (RT3) と呼ばれる）が VXLAN カプセル化でサポートされる必要があります。
- スイッチは、300 個のリモート VTEP と、合計 200 個の L2VNI または VLAN をサポートする必要があります。

VXLAN EVPN 入力複製に関する情報

入力複製 (IR) 機能が BGP EVPN over VXLAN に導入され、ブロードキャスト、不明なユニキャスト、およびマルチキャスト (BUM) トラフィックをネットワーク内の関連する受信者に転送します。VXLAN EVPN の入力複製は、IP マルチキャストアンダーレイネットワークが使用されていない場合に展開されます。入力複製 (ヘッドエンドレプリケーション) はマルチデスティネーショントラフィックを処理するユニキャストアプローチです。入力複製を使用してネットワーク内の BUM トラフィックを処理する場合、入力デバイスでは、すべての BUM パケットが複製され、それらが個別のユニキャストとしてリモート出力デバイスに送信されません。

入力の複製の操作

BGP EVPN では、包括的なマルチキャストイーサネットタグ (IMET) ルーティング (ルートタイプ 3 (RT3) と呼ばれる) を介して入力複製を使用し、VXLAN 経由の BUM トンネルを設定するために、リモートピアを自動検出します。IMET ルートはリモートピアからアドバタイズされたリモート (出力) VNI を伝送します。これはローカル VNI とは異なる場合があります。これらのリモート VNI は、ダウンストリーム割り当て VNI と呼ばれます。

VXLAN トンネル隣接関係は、リモート NVE ピアから IMET IR ルートを受信した後に作成されます。トンネルの隣接関係は、VXLAN トンネルの IP または UDP のカプセル化を含む MID チェーンの隣接関係です。トンネルに複数の VNI がある場合、複数の VNI がそのトンネルを共有します。EVPN の IMET 入力複製では、リモートピアごとに複数のユニキャストトンネル隣接関係とさまざまな出力 VNI を設定できます。



(注) VXLAN トンネル隣接関係を使用する NVE ピアがない場合、トンネル隣接関係は削除されます。

フラッディングされた複製リスト (データプレースのフラッディングリストとも呼ばれる) は各 VTEP によってアドバタイズされたルートを使用して作成されます。ダイナミック複製リストには、BGP IMET ルートで検出された同じレイヤ 2 VNI 内のすべてのリモート宛先ピアが保存されます。VNI がリモートピアで設定されると、複製リストが更新されます。VXLAN カプセル化が作成され、対応するトンネル隣接関係にリンクされます。トンネル隣接関係と VXLAN カプセル化は、リモート NVE ピアから IMET IR ルートを受信されると、複製リストに追加されます。リモート NVE ピアで IMET IR ルートが取り消されると、トンネル隣接関係と VXLAN カプセル化は複製リストから削除されます。複製リストが作成されると、入力デバイスに到達するすべての BUM トラフィックが複製され、ネットワーク全体で VNI 内のすべてのリモートピアに転送されます。



(注) VXLAN EVPN 入力複製では、高可用性 (HA) とステートフルスイッチオーバー (SSO) がサポートされます。

VXLAN EVPN 入力複製の設定

このセクションでは、VxLAN EVPN の入力複製の設定に関連する手順について説明します。

複製タイプの設定

入力複製の複製タイプを設定するには、次のタスクを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権コンフィギュレーション モードを開始します。 • パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	l2vpn evpn 例： Device(config)# l2vpn evpn	EVPN コンフィギュレーション モードを開始します。
ステップ 4	replication-type ingress 例： Device(config-evpn)# replication-type ingress	L2VPN EVPN 複製タイプを入力複製として設定します。
ステップ 5	end 例： Device(config-evpn)# end	特権 EXEC モードに戻ります。

カプセル化タイプの設定

EVPN インスタンス (EVI) でカプセル化タイプを設定するには、次のタスクを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権コンフィギュレーション モードを開始します。 • パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例：	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	Device# configure terminal	
ステップ 3	l2vpn evpn instance evpn-identifier-value vlan-based 例： Device(config)# l2vpn evpn instance 1 vlan-based	指定した VLAN ベースの EVI の EVPN-EVI コンフィギュレーションモードを開始します。
ステップ 4	encapsulation vxlan 例： code Device(config-evpn-evi)# encapsulation vxlan	VLAN ベースの EVI のカプセル化タイプを VxLAN として設定します。
ステップ 5	end 例： Device(config-if-nve-vni)# end	特権 EXEC モードに戻ります。

NVE への VNI ノードの追加

仮想ネットワーク識別子 (VNI) ノードをネットワーク仮想化エッジ (NVE) に追加するには、次のタスクを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権コンフィギュレーションモードを開始します。 <ul style="list-style-type: none">パスワードを入力します (要求された場合)。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーションモードを開始します。
ステップ 3	interface nve-interface-name 例： Device(config)# interface nve1	トランクとして設定するインターフェイスを定義し、インターフェイスコンフィギュレーションモードを開始します。

	コマンドまたはアクション	目的
ステップ 4	host-reachability protocol bgp 例： Device(config-if)# host-reachability protocol bgp	インターフェイス上で BGP をホスト到達可能性プロトコルとして設定します。
ステップ 5	member vni vni-id ingress-replication 例： Device(config-if)# member vni 20015 ingress-replication	入力複製モードの VNI メンバーを NVE に追加します。
ステップ 6	end 例： Device(config-if-nve-vni)# end	特権 EXEC モードに戻ります。

VxLAN EVPN 入力複製の設定例

このセクションでは、VxLAN EVPN の IMET 入力複製の設定とモニタリングのさまざまな例を示します。

例：EVPN VxLAN を介した IMET 入力複製の設定

次に、VxLAN に IMET 入力複製を設定する例を示します。

```
Device# configure terminal
Device(config)# l2vpn evpn
Device(config-evpn)# replication-type ingress
Device(config-evpn)# exit
Device(config)# l2vpn evpn instance 1 vlan-based
Device(config-evpn-evi)# encapsulation vxlan
Device(config-evpn-evi)# exit
Device(config)# int nve1
Device(config-if)# host-reachability protocol bgp
Device(config-if)# member vni 20015 ingress-replication
```

IMET IR ルートの作成と管理

このセクションでは、IMET IR ルートの作成と管理のさまざまな例を示します。

例：EVPN マネージャでのローカル IMET ルートの作成

次の例は、EVPN マネージャによって作成されたローカル IMET ルートを示しています。

```
Device# show l2vpn evpn evi 1 detail

EVPN instance: 1 (VLAN Based)
```

例 : L2RIB ローカル IMET ルート

```

RD: 10.3.3.3:1 (auto)
Import-RTs: 3:1
Export-RTs: 3:1
Per-EVI Label: none
State: Established
Replication Type: Ingress (global)
Encapsulation: vxlan
IP Local Learn: Enable (global)
Vlan: 11
Ethernet-Tag: 0
State: Established
Core If: Vlan100
Access If: Vlan11
NVE If: nve1
RMAC: 2c5a.0f1c.da21
Core Vlan: 100
L2 VNI: 10000
L3 VNI: 100000
VTEP IP: 10.33.33.33
VRF: Red
IPv4 IRB: Enabled
IPv6 IRB: Enabled
Pseudoports:
GigabitEthernet1/0/7 service instance 11
GigabitEthernet1/0/8 service instance 11

```

例 : L2RIB ローカル IMET ルート

次の例は、L2RIB ローカル IMET ルートを示しています。

```

Device# l2route evpn imet detail

EVPN Instance: 1
Ethernet Tag: 0
Producer Name: BGP
Router IP Addr: 10.44.44.44
Route Ethernet Tag: 0
Tunnel Flags: 0
Tunnel Type: Ingress Replication
Tunnel Labels: 10001
Tunnel ID: 10.44.44.44
Next Hop(s): V:0 10.44.44.44

```

例 : VxLAN カプセル化と VNI を使用した BGP ローカル IMET ルート

次の例は、VxLAN カプセル化と VNI を使用した BGP ローカル IMET ルートを示しています。

```

Device# show ip bgp l2vpn evpn evi 1 route-type 3

BGP routing table entry for [3][10.10.10.10:1][0][32][10.10.10.1]/17, version 6
Paths: (1 available, best #1, table evi_1)
  Advertised to update-groups:
    1
  Refresh Epoch 1
  Local
  Updated on Jul 30 2018 18:16:34 PST
    :: (via default) from 0.0.0.0 (10.10.10.10)
      Origin incomplete, localpref 100, weight 32768, valid, sourced, local, best
      Extended Community: RT:1:1 ENCAP:8
      PMSI Attribute: Flags:0x0, Tunnel type:6, length 4, vni:10000 tunnel parameters:

```

```
0000 0000
  Local irb vxlan vtep:
    vrf:not found, l3-vni:0
    local router mac:0000.0000.0000
    core-irb interface:(not found)
    vtep-ip:10.10.10.1
    rx pathid: 0, tx pathid: 0x0
```

IMET IR ルートの受信とプログラミング

このセクションでは、IMET IR ルートの受信とプログラミングのさまざまな例を示します。

例：BGP で VXLAN カプセル化を使用して IMET ルートをインポートし、VNI を表示する

次の例は、BGP による VXLAN カプセル化を使用した IMET ルートのインポートと、VNI の表示を示しています。

```
Device# show ip bgp l2vpn evpn evi 1 route-type 3

BGP routing table entry for [3][10.10.10.10:1][1][32][10.1.1.1]/17, version 4
Paths: (1 available, best #1, table evi_1)
  Not advertised to any peer
  Refresh Epoch 1
  Local, imported path from [3][10.2.2.2:1000][1][32][10.1.1.1]/17 (global)
  Updated on Jul 30 2018 18:11:37 PST
    10.19.101.1 (via default) from 10.20.0.45 (19.0.0.1)
      Origin IGP, localpref 100, valid, internal, best
      Extended Community: RT:1:1 ENCAP:8
      Originator: 10.19.101.1, Cluster list: 10.19.0.1
      PMSI Attribute: Flags:0x0, Tunnel type:6, length 4, vni:16777215 tunnel parameters:
      1300 6501
```

例：L2FIB リモート IMET ルート

次の例は、L2FIB リモート IMET ルートに関する詳細を示します。

```
Device# show l2fib bridge-domain 11 details

Bridge Domain : 11
Reference Count : 13
Replication ports count : 4
Unicast Address table size : 2
IP Multicast Prefix table size : 3

Flood List Information :
Olist: 1035, Ports: 4

VxLAN Information :

Port Information :
BD_PORT Gi1/0/7:11
BD_PORT Gi1/0/8:11
VXLAN_REP PL:1(1) T:VXLAN_REP [IR]10001:10.44.44.44
VXLAN_REP PL:57(1) T:VXLAN_REP [IR]10000:10.55.55.55

Unicast Address table information :
0013.0100.0001 VXLAN_CP L:10000:10.33.33.33 R:10000:10.55.55.55
```

例：L2RIB リモート IMET ルート

```
d4e8.80b0.99bf VXLAN_CP L:10000:10.33.33.33 R:10000:10.55.55.55

IP Multicast Prefix table information :
Source: *, Group: 224.0.0.0/24, IIF: Null, Adjacency: Olist: 1035, Ports: 4
Source: *, Group: 224.0.1.39, IIF: Null, Adjacency: Olist: 1035, Ports: 4
Source: *, Group: 224.0.1.40, IIF: Null, Adjacency: Olist: 1035, Ports: 4
```

```
Device# show l2fib output-list 1035
```

```
ID : 1035
Bridge Domain : 11
Reference Count : 4
Flags : flood list
Port Count : 4
Port(s) : BD_PORT Gi1/0/8:11
          : BD_PORT Gi1/0/7:11
          : VXLAN_REP PL:1(1) T:VXLAN_REP [IR]10001:10.44.44.44
          : VXLAN_REP PL:57(1) T:VXLAN_REP [IR]10000:10.55.55.55
```

例：L2RIB リモート IMET ルート

次の例は、L2RIB リモート IMET ルートを示しています。

```
Device# show l2route evpn imet det
```

```
EVPN Instance:          11
Ethernet Tag:           0
Producer Name:          BGP
Router IP Addr:         10.2.2.2
Route Ethernet Tag:     0
Tunnel Flags:           0
Tunnel Type:            Ingress Replication
Tunnel Labels:          20011
Tunnel ID:              10.2.2.2
Tunnel Encapsulation:   vxlan
```

例：リモート IMET ルートのトンネル隣接関係

次の例は、リモート IMET ルートのトンネル隣接関係を示しています。

```
Device# show adjacency tu0 10.2.2.2 internal
```

```
Protocol Interface      Address
IP          Tunnel0     10.2.2.2(4)
                                     237 packets, 92420 bytes
                                     epoch 0
                                     sourced in sev-epoch 2
                                     Encap length 28
                                     4500000000000000FF11AFE104040404
                                     0202020212B512B500000000
                                     Tun endpt
                                     Next chain element:
                                     IP adj out of Ethernet1/0, addr 10.3.1.2 7F21C7BE60A0
                                     parent oce 0x7F21C7BE6160
                                     frame originated locally (Null10)
                                     L3 mtu 4000
                                     Flags (0x4808C4)
```

```

Protocol Interface
Fixup enabled (0x2)
  IP tunnel
HWIDB/IDB pointers 0x7F21CDC4C218/0x7F21CDC4D5C8
IP redirect disabled
Switching vector: IPv4 midchain adj oce
Address
IP Tunnel stack to 10.2.2.2 in Default (0x0)
  nh tracking enabled: 10.2.2.2/32
  IP adj out of Ethernet1/0, addr 10.3.1.2
Adjacency pointer 0x7F21CE859D90
Next-hop 10.2.2.2

```

例：VxLAN カプセル化を使用した BGP ローカル IMET ルートおよび VxLAN と MPLS を使用したリモート IMET ルート

次の例に、VxLAN カプセル化を使用した BGP ローカル IMET ルートおよび VxLAN と MPLS を使用したリモート IMET ルートを示します。

```

Device# show ip bgp l2vpn evpn evi 1 route-type 3

BGP routing table entry for [3][10.10.10.10:1][0][32][10.10.10.1]/17, version 6
Paths: (1 available, best #1, table evi_1)
  Advertised to update-groups:
    1
  Refresh Epoch 1
  Local
  Updated on Jul 30 2018 18:16:34 PST
  :: (via default) from 0.0.0.0 (10.10.10.10)
  Origin incomplete, localpref 100, weight 32768, valid, sourced, local, best
  Extended Community: RT:1:1 ENCAP:8
  PMSI Attribute: Flags:0x0, Tunnel type:6, length 4, vni:10000 tunnel parameters:
0000 0000
  Local irb vxlan vtep:
    vrf:not found, l3-vni:0
    local router mac:0000.0000.0000
    core-irb interface:(not found)
    vtep-ip:10.10.10.1
  rx pathid: 0, tx pathid: 0x0
BGP routing table entry for [3][10.10.10.10:1][1][32][1.1.1.1]/17, version 4
Paths: (1 available, best #1, table evi_1)
  Not advertised to any peer
  Refresh Epoch 1
  Local, imported path from [3][2.2.2.2:1000][1][32][1.1.1.1]/17 (global)
  Updated on Jul 30 2018 18:11:37 PST
  19.0.101.1 (via default) from 20.0.0.45 (19.0.0.1)
  Origin IGP, localpref 100, valid, internal, best
  Extended Community: RT:1:1 ENCAP:8
  Originator: 19.0.101.1, Cluster list: 19.0.0.1
  PMSI Attribute: Flags: 0x0, Tunnel type: 6, length 4, vni:16777215 tunnel parameters:
1300 6501
  rx pathid: 0, tx pathid: 0x0
BGP routing table entry for [3][10.10.10.10:1][1][32][2.2.2.2]/17, version 5
Paths: (1 available, best #1, table evi_1)
  Not advertised to any peer
  Refresh Epoch 1
  Local, imported path from [3][2.2.2.2:1000][1][32][2.2.2.2]/17 (global)
  Updated on Jul 30 2018 18:11:37 PST
  19.0.101.2 (via default) from 20.0.0.45 (19.0.0.1)
  Origin IGP, localpref 100, valid, internal, best
  Extended Community: RT:1:1
  Originator: 19.0.101.2, Cluster list: 19.0.0.1

```

```
PMSI Attribute: Flags: 0x0, Tunnel type: 6, length 4, label:1048575 tunnel
parameters: 1300 6502
rx pathid: 0, tx pathid: 0x0
```

VxLAN EVPN 入力複製の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

リリース	変更内容
Cisco IOS XE Gibraltar 16.11.1	この機能が導入されました。



第 13 章

オーディオ ビデオブリッジング

- [オーディオ ビデオブリッジング ネットワークの概要 \(265 ページ\)](#)
- [AVB ネットワークの設定 \(271 ページ\)](#)
- [AVB ネットワークのモニタリング \(280 ページ\)](#)
- [AVB 設定とモニタリングの例 \(281 ページ\)](#)
- [オーディオ ビデオブリッジングの機能履歴 \(303 ページ\)](#)

オーディオ ビデオブリッジング ネットワークの概要

オーディオ ビデオブリッジング (AVB) について

オーディオとビデオの設備導入は従来、アナログの単一用途型ポイントツーポイント一方向リンクとなっています。デジタル伝送への移行もまた、ポイントツーポイント一方向リンクアーキテクチャを維持し続けていました。専用の接続モデルによって、プロフェッショナル向けおよびコンシューマ向けのアプリケーションの配線が多くなり、管理と運用が難しくなっていました。

相互運用可能な方法でイーサネットベースのオーディオ/ビデオ導入の採用を加速させるために、IEEE は IEEE オーディオ ビデオブリッジング標準 (IEEE 802.1BA) と同一水準に達しました。これにより、エンドポイントとネットワークが全体として機能し、コンシューマ向けアプリケーション間の高品質 A/V ストリーミングをイーサネットインフラストラクチャを介してプロフェッショナル向けオーディオ/ビデオにまで可能にするメカニズムが定義されます。



- (注)
- AVB は、スタック構成のシステムではサポートされません。
 - AVB は、EtherChannel インターフェイスではサポートされません。
 - AVB は、STP 対応ネットワークでのみサポートされます。

AVB をサポートするライセンス

AVB は、Network Advantage ライセンスでサポートされています。

AVB の利点

AVB は、イーサネット ベースの音声およびビデオの送信を可能にする標準ベースのメカニズムであり、次の利点があります。

- 最大遅延保証
- 時間同期
- 帯域幅保証
- プロフェッショナル グレード

オーディオビデオブリッジングネットワークのコンポーネント

AVB プロトコルは、すべてのデバイスが AVB 対応であるドメインでのみ動作します。AVB ネットワークは、AVB 送話者、AVB リスナー、AVB スイッチおよびグランドマスタクロックの送信元で構成されます。

- AVB 送話者：ストリームの送信元またはプロデューサである AVB エンドステーション。つまり、マイク、ビデオカメラなど。
- AVB リスナー：ストリームの宛先またはコンシューマである AVB エンドステーション。つまり、スピーカー、ビデオ画面など。
- AVB スイッチ：IEEE802.1 AVB 基準に準拠するイーサネット スイッチ。
- AVB ストリーム：ストリーム予約プロトコル (SRP) に準拠するストリームの予約に関連付けられているデータストリーム。

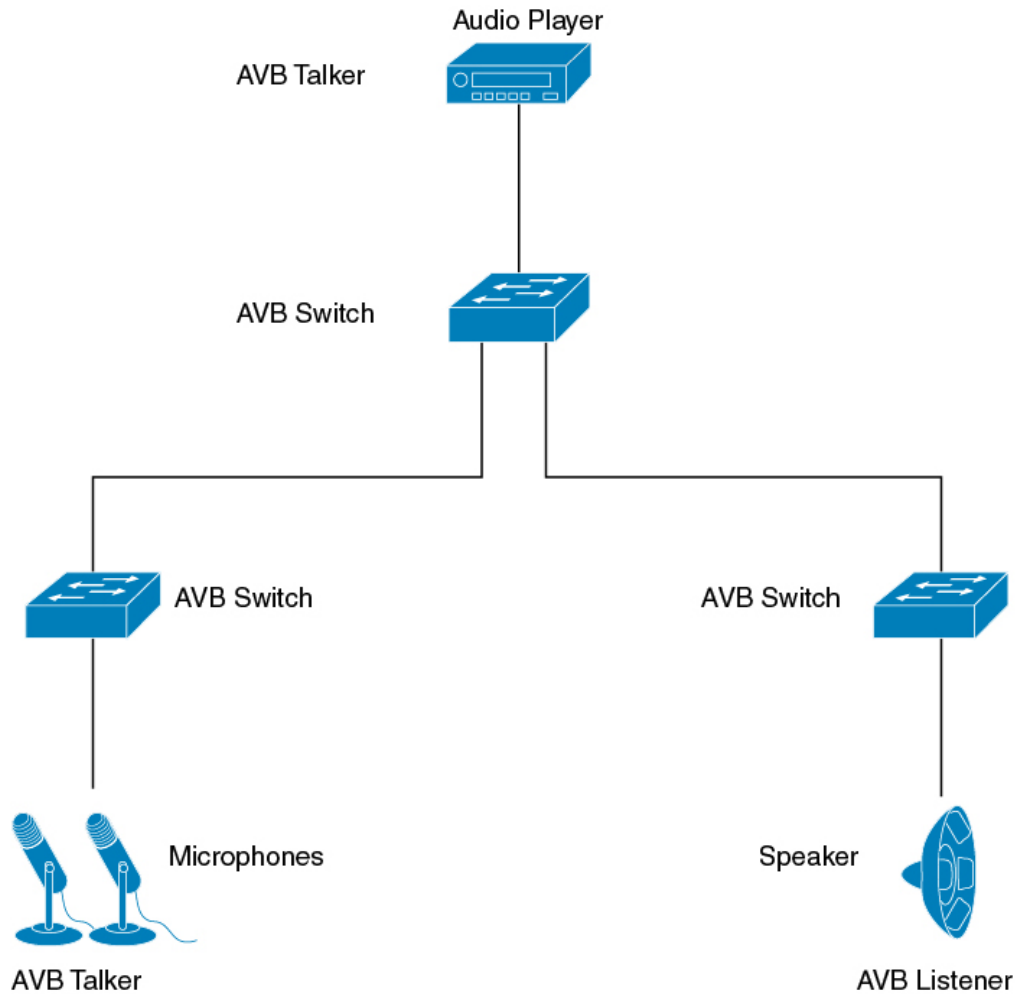


(注) 時には、「ブリッジ」という単語が使用されます。このコンテキストでは、スイッチと言及します。

IEEE 802.1BA 仕様では、AVB 送話者がグランドマスタに対応している必要があります。一般的な導入では、ネットワーク ノードをグランドマスタにすることもできますが、そのノードがグランドマスタ対応デバイスからタイミングを調達または引き出し、IEEE 802.1AS を使用して AVB ネットワークにそのタイミングを提供できることが条件となります。

図 1 に、さまざまなコンポーネントによる AVB ネットワークの簡略図を示します。 [図 33: AVB ネットワーク \(267 ページ\)](#)

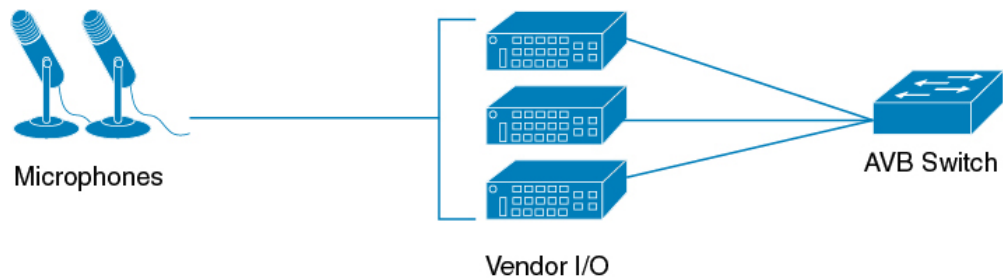
図 33: AVB ネットワーク



354698

多くの場合、音声/ビデオエンドポイント（マイク、スピーカーなど）は、アナログデバイスです。AVBエンドポイントベンダーは、[図 34: ベンダーのオーディオ I/O システム](#)（267 ページ）に示すように、広範な音声/ビデオ処理を提供し、AVB イーサネットインターフェイスにエンドポイントを集約する、デジタル信号プロセッサ（DSP）と I/O デバイスを導入します。

図 34: ベンダーのオーディオ I/O システム



354699

オーディオ ビデオ ブリッジングでサポートされる SKU

すべての Cisco Catalyst 9300 シリーズ スイッチは、次に示すものを除き、すべてのポート（アップリンクポートとダウンリンクポートの両方）で PTP または AVB をサポートします。

- C9300-48UXM : 1 ～ 16 個のみのダウンリンクポートおよびすべてのアップリンクポートでサポートされます。
- C9300-48UN : 1 ～ 36 個のみのダウンリンクポートおよびすべてのアップリンクポートでサポートされます。

Generalized Precision Time Protocol (gPTP) について

Generalized Precision Time Protocol (gPTP) は IEEE 802.1AS 標準規格で、AVB ネットワーク内でブリッジとエンドポイントデバイスのクロックを同期する機能を提供します。これにより、時間認識ブリッジと送話者およびリスナー間でグランドマスタークロック (BMCA) を選択するメカニズムが定義されます。グランドマスターは、時間認識ネットワークで確立され、下位のノードに時間を配信して同期を可能にする時間階層のルートです。

時刻同期には、ネットワーク ノードでのリンク遅延とスイッチ遅延の測定も必要です。gptp スイッチは IEEE 1588 境界クロックであり、ピアツーピア遅延機能を使用してリンク遅延の測定も行います。計算された遅延は PTP メッセージの修正フィールドに追加され、エンドポイントに伝えられます。送話者とリスナーはこの gPTP 時刻を共有クロック基準として使用し、この時刻はメディア クロックを中継して回復するために使用されます。gPTP は現在、ドメイン 0 のみを定義しており、これはスイッチがサポートするものです。

ピアツーピア遅延の機能は、STP によってブロックされたポートでも動作します。他の PTP メッセージはブロックされたポート上で送信されません。

PTP ドメインでは、ベスト マスター クロック (BMC) アルゴリズムがクロックとポートを階層型方式 (クロックとポートの状態が含まれています) に編成します。

クロック

- グランドマスタ (GM/GMC)
- 境界クロック (BC)

ポート ステート

- マスタ (M)
- スレーブ (S)
- パッシブ (P)

Multiple Stream Reservation Protocol (MSRP) について

Multiple Stream Reservation Protocol (MSRP) は、要求された QoS でネットワークを介してデータ ストリームの送信と受信を保証するネットワーク リソースを予約する機能をエンドステー

ションに提供します。これは、AVB デバイス（送話者、リスナーおよびスイッチ）に必要なコアプロトコルの 1 つです。これにより、送話者は AVB スイッチのネットワークを介してストリームをアダプタイズでき、リスナーはストリームを受信するための登録を行えるようになります。

MSRP は、AVB をサポートするための主要なソフトウェアプロトコルモジュールです。これにより、ストリームの確立とティアダウンが可能になります。これは gPTP と連動し、ストリームの遅延情報を更新します。また、QoS モジュールと連動し、ストリームに要求された帯域幅を保証するハードウェアリソースを設定します。クレジットベースのシェーパに必要な QoS シェーピングパラメータも提供します。

Multiple Stream Reservation Protocol の機能

MSRP が実行する機能は次のとおりです。

- 送話者がストリームをアダプタイズできるようにし、リスナーがストリームを検出して登録を行えるようにします。
- 1 人の送話者と 1 人以上のリスナーとの間にイーサネット経由のパスを確立します。
- AVB ストリームに保証された帯域幅を提供します。
- 遅延の上限を保証します。
- 送話者と各リスナーとの間で最も問題となるエンドツーエンド遅延を検出してレポートします。
- 送話者とリスナー間のパスが帯域幅要件を満たすことができない場合に、障害の原因と場所をレポートします。
- さまざまな遅延対象を含む複数のトラフィッククラスをサポートします。
- AVB トラフィックを制限することによってスタベーションからベストエフォート型トラフィックを保護します。
- MSRP 送話者宣言は、STP によってブロックされるポートでは転送されません。
- MSRP は、STP TCN 通知をリッスンし、ストリームを切断、変更、確立する MSRP 宣言を生成します。

階層型 QoS の概要

AVB ネットワークは、時間的に制約がある音声およびビデオストリームの帯域幅および最小遅延制限を保証します。AVB は、送話者からリスナーへのトラフィックで最も問題となる遅延対象に基づいて、クラス A およびクラス B を時間的に制約があるストリームとして定義します。

2 つのストリームの遅延対象は次のように示されます。

- SR-Class A : 2ms

- SR-Class B: 50ms

ホップごとの最も問題となる遅延の影響を要約すると、SR クラス A の場合は合計で 2 ms 以下、SR クラス B の場合は 50ms 以下の全体的なエンドツーエンド遅延となります。送話者からリスナーへの一般的な 7 ホップの AVB 導入は、これらの遅延要件を満たします。

優先度のコードポイントは、特定のストリームにトラフィックをマッピングします。フレームの転送動作は、この優先度に基づいています。クレジットベースのシェーパは、遅延対象が満たされるように、特定のアウトバウンドキューで予約済みの帯域幅に従って、これらのストリームの送信をシェーピングするために使用されます。

AVB は階層型 QoS をサポートします。AVB の階層型 QoS ポリシーは、2 レベルの親子ポリシーです。AVB 親ポリシーは、音声、ビデオトラフィックストリーム (SR クラス A、SR クラス B) と標準的なベストエフォートのイーサネットトラフィック (非 SR) からのネットワーク制御パケットを分離し、それに応じてストリームを管理します。階層型 QoS では、トラフィック管理をより細かい粒度で実行する、複数のポリシー レベルで QoS 動作を指定できます。階層型ポリシーは次のように使用できます。

- 親クラスが子ポリシー上で複数のキューをシェーピングする
- 集約トラフィックの特定のポリシー マップ アクションを適用する
- クラス固有のポリシー マップ アクションを適用する

policy-map AVB-Output-Child-Policy および **policy-map AVB-Input-Child-Policy** コマンドを使用して、入力および出力の HQoS 子ポリシーの **class-map** とその操作のみを変更できます。



(注) たとえば、SR クラス A Cos 3 や SR クラス B Cos 2 など、親ポリシーに設定された PCP でマッピングするように子ポリシーの PCP を変更してはいけません。

階層型ポリシング

階層型ポリシングは、入力および出力インターフェイスでサポートされます。階層型 QoS は、SR および非 SR クラス関連のルールをそれぞれ親ポリシーと子ポリシーに分けます。AVB SR クラスは、MSRP クライアントによって完全に制御されるため、SR クラス属性を含む親ポリシーは MSRP によって管理されます。エンドユーザーには、非 SR クラス属性を含む子ポリシーに対する完全な制御権があり、子ポリシーのみを変更できます。

AVB HQoS 子ポリシーは、ユーザーが変更可能で、ユーザーが **startup-config** への設定を保存すると、設定を保存するように NVGEN されます。したがって、AVB HQoS 子ポリシーの設定はリロード後も保持されます。

マルチ VLAN 登録プロトコル (MVRP) について

マルチ VLAN 登録プロトコル (MVRP) は、MRP に基づくアプリケーションです。MVRP は、各 VLAN ID に関するダイナミック VLAN 登録エントリのコンテンツのダイナミックメンテナンスを行い、含まれている情報を他のブリッジに伝達する機能を提供します。この情報を使用

して、MVRP 対応デバイスは、現在アクティブなメンバーを持つ VLAN に関連付けられている VLAN ID のセットの知識を動的に確立して更新することができ、それによって、ポートとそのメンバーは到達可能になります。

AVB の観点から、MVRP は送話者とリスナーで必須です。AVB とは関係なく、MVRP は VLAN 対応スイッチでの IEEE 802.1Q 要件です。ただし、AVB の場合は、スイッチでの VLAN の手動設定で十分です。



- (注) MVRP が機能するには、VTP を無効モードまたはトランスペアレントモードにする必要があります。

AVB ネットワークの設定

AVB の設定

この項では、AVB で使用可能なさまざまな設定について説明します。

スイッチでの AVB のイネーブル化

スイッチで次のコマンドを使用して、AVB を有効にできます。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーションモードを開始します。
ステップ 3	avb 例： Device(config)# avb	スイッチで AVB をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 4	avb strict 例 : Device (config) # avb strict	スイッチで AVB をイネーブルにします。このコマンドは、AVB を有効にする avb コマンドと組み合わせて使用します。 (注) このコマンドは、将来のリリースでは廃止される予定です。
ステップ 5	end 例 : Device (config) # end	特権 EXEC モードに戻ります。

次のタスク

スイッチで AVB を無効にするには、このコマンドの "no" 形式を使用します。

デバイスでの AVB の設定

次のコマンドを使用して、dot1q トランク ポートとして AVB デバイスの接続パスに沿ってインターフェイスを設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Device> enable	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> パスワードを入力します (要求された場合)。
ステップ 2	configure terminal 例 : Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	interface interface-id 例 : Device (config) # interface tel1/1/1	トランクとして設定するインターフェイスを定義し、インターフェイスコンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	switchport mode trunk 例 : Device(config-if) # switchport mode trunk	ポートをトランクポートとして設定します。
ステップ 5	exit 例 : Device(config-if) # exit	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	vlan 2 例 : Device(config) # vlan 2	スイッチで VLAN 2 を設定します。 (注) VLAN 2 がデフォルトの AVB VLAN です。別の VLAN をデフォルトの AVB VLAN として設定する必要がある場合は、ステップ 7 のコマンドを使用します。
ステップ 7	avb vlan vlan-id 例 : Device(config) # avb vlan 10	(任意) 指定された VLAN をスイッチのデフォルトの AVB VLAN として設定します。このコマンドは、VLAN2 以外をデフォルトの AVB VLAN として設定する必要がある場合に使用します。 <i>vlan-id</i> の範囲は 2 ~ 4094 です。
ステップ 8	avb 例 : Device(config-vlan) # avb	指定されたインターフェイスで AVB を設定します。
ステップ 9	end 例 : Device(config) # end	特権 EXEC モードに戻ります。

次のタスク

スイッチで AVB を無効にするには、このコマンドの "no" 形式を使用します。

gPTP の設定

この項では、gPTP で使用可能なさまざまな設定について説明します。

gPTP の有効化

AVB がスイッチで有効になると、AVB の gPTP も有効になります。

また、次に示すコマンドを使用してグローバルに gPTP を有効にすることもできます。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	[no]ptp profile dot1as 例： Device(config)# ptp profile dot1as	AVB を有効にすると、gPTP がグローバルに有効になります。ポートで gPTP を無効にするには、このコマンドの no 形式を使用します。
ステップ 4	end 例： Device(config)# end	特権 EXEC モードに戻ります。

インターフェイス上での gPTP のイネーブル化

また、次に示すコマンドを使用してインターフェイス上で gPTP を有効にすることもできます。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーションモードを開始します。
ステップ 3	interface interface-id 例： Device(config)# interface tel1/1/1	トランクとして設定するインターフェイスを定義し、インターフェイスコンフィギュレーションモードを開始します。
ステップ 4	ptp enable 例： Device(config-if)# ptp enable	指定されたインターフェイスで gPTP をイネーブルにします。 インターフェイスで gPTP をディセーブルにするには、次に示すようにこのコマンドの no 形式を使用します。 Device(config-if)# no ptp enable
ステップ 5	end 例： Device(config-if)# end	特権 EXEC モードに戻ります。

Precision Time Protocol のクロック値の設定

PTP クロックの値（優先順位 1 および優先順位 2）を設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 プロンプトが表示されたらパスワードを入力します。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーションモードを開始します。
ステップ 3	ptp priority1 value 例： Device(config)# ptp priority1 120	PTP クロックの優先順位 1 の値を設定します。有効な範囲は 0 ～ 255 です。デフォルト値は 128 です。 (注) 優先順位 1 の値が 255 に設定されると、クロックはグランドマスターとは見なされません。

	コマンドまたはアクション	目的
ステップ 4	ptp priority2 value 例： Device(config)# ptp priority2 120	PTPクロックの優先順位2の値を設定します。有効な範囲は0～255です。デフォルト値は128です。
ステップ 5	exit 例： Device(config)# exit	グローバル コンフィギュレーションモードに戻ります。

HQoS の設定

この項では、HQoS で使用可能なさまざまな設定について説明します。

HQoS のイネーブル化

AVB がスイッチで有効になると、AVB の HQoS も有効になります。

階層型 QoS ポリシーの形式

次に、入力インターフェイスでの階層型再マーキング ポリシーの例を示します。

```

policy-map AVB-Input-Child-Policy
  class VOIP-DATA-CLASS
    set dscp EF
  class MULTIMEDIA-CONF-CLASS
    set dscp AF41
  class BULK-DATA-CLASS
    set dscp AF11
  class TRANSACTIONAL-DATA-CLASS
    set dscp AF21
  class SCAVENGER-DATA-CLASS
    set dscp CS1
  class SIGNALING-CLASS
    set dscp CS3
  class class-default
    set dscp default

policy-map AVB-Input-Policy-Remark-AB
  class AVB-SR-A-CLASS
    set cos 0 (set 0 for boundary & SR class A PCP value for core port)
  class AVB-SR-B-CLASS
    set cos 0 (set 0 for boundary & SR class B PCP value for core port)
  class class-default
    service-policy AVB-Input-Child-Policy

policy-map AVB-Input-Policy-Remark-A
  class AVB-SR-A-CLASS
    set cos 0 (set 0 for boundary & SR class A PCP value for core port)
  class class-default
    service-policy AVB-Input-Child-Policy

policy-map AVB-Input-Policy-Remark-B
  class AVB-SR-B-CLASS
    set cos 0 (set 0 for boundary & SR class B PCP value for core port)
  class class-default

```

```
service-policy AVB-Input-Child-Policy

policy-map AVB-Input-Policy-Remark-None
class class-default
  service-policy AVB-Input-Child-Policy
```

次に、出力インターフェイスでの階層型キューイング ポリシーの例を示します。

```
policy-map AVB-Output-Child-Policy
class VOIP-PRIORITY-QUEUE
  bandwidth remaining percent 30
  queue-buffers ratio 10
class MULTIMEDIA-CONFERENCING-STREAMING-QUEUE
  bandwidth remaining percent 15
  queue-limit dscp AF41 percent 80
  queue-limit dscp AF31 percent 80
  queue-limit dscp AF42 percent 90
  queue-limit dscp AF32 percent 90
  queue-buffers ratio 10
class TRANSACTIONAL-DATA-QUEUE
  bandwidth remaining percent 15
  queue-limit dscp AF21 percent 80
  queue-limit dscp AF22 percent 90
  queue-buffers ratio 10
class BULK-SCAVENGER-DATA-QUEUE
  bandwidth remaining percent 15
  queue-limit dscp AF11 percent 80
  queue-limit dscp AF12 percent 90
  queue-limit dscp CS1 percent 80
  queue-buffers ratio 15
class class-default
  bandwidth remaining percent 25
  queue-buffers ratio 25

policy-map AVB-Output-Policy
class AVB-SR-A-CLASS
  priority level 1 (Shaper value based on stream registration)
class AVB-SR-B-CLASS
  priority level 2 (Shaper value based on stream registration)
class CONTROL-MGMT-QUEUE
  priority level 3 percent 15
class class-default
  bandwidth remaining percent 100
  queue-buffers ratio 80
  service-policy AVB-Output-Child-Policy
```

MVRP の設定

この項では、MVRP で使用可能なさまざまな設定について説明します。

MVRP のイネーブル化

次のコマンドを使用して、トポロジ内のスイッチで MVRP を有効にして Vlan 伝達を有効にできます。



(注) MVRP を介したダイナミック VLAN の作成を有効にする前に、VTP モードをトランスペアレントモードまたはオフモードに変更する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	mvrp global 例： Device(config)# mvrp global	MVRP グローバルコンフィギュレーション モードを開始します。
ステップ 4	vtp mode {transparent off} 例： Device(config)# vtp mode transparent 例： Device(config)# vtp mode off	VTP をトランスペアレント モードまたはオフ モードに設定します。
ステップ 5	mvrp vlan create 例： Device(config)# mvrp vlan create	スイッチで MVRP をイネーブルにします。

スイッチインターフェイスでの MVRP の設定

次のコマンドを使用して、スイッチインターフェイスに MVRP を設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
	Device> enable	
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	interface interface-id 例： Device(config)# interface tel1/1/1	トランクとして設定するインターフェイスを定義し、インターフェイスコンフィギュレーション モードを開始します。
ステップ 4	mvrp registration {fixed forbidden normal} 例： Device(config-if) # mvrp registration fixed	MAD インスタンスに MVRP を登録します。 <ul style="list-style-type: none">• fixed : 固定登録• forbidden : 禁止登録• normal : 通常の登録
ステップ 5	mvrp timer {join leave leave-all periodic} 例： Device(config-if) # mvrp timer join	MVRP タイマーを設定します。 <ul style="list-style-type: none">• join : タイマーは、ASM に適用される送信機会の間の間隔を制御します。• leave : タイマーは、MT ステートに移行する前に LV ステートで待機する RSM を制御します。• leave-all : タイマーは、LeaveAll SM が LeaveAll PDU を生成する頻度を制御します。• periodic : 定期タイマー
ステップ 6	exit 例： Device(config-if) # exit	グローバル コンフィギュレーション モードに戻ります。

AVB ネットワークのモニタリング

AVB のモニタリング

AVB の詳細を表示するには、次の表のコマンドを使用します。

コマンド	目的
show avb domain	AVB ドメインを表示します。
show avb streams	AVB ストリーム情報を表示します。

gPTP のモニタリング

gPTP プロトコルの詳細を表示するには、次の表のコマンドを使用します。

コマンド	目的
show ptp brief	インターフェイスの ptp の簡易ステータスを表示します。
show ptp clock	ptp クロック情報を表示します。
show ptp parent	親クロックの情報を表示します。
show ptp port	ptp ポート情報を表示します。
show platform software fed switch active ptp if-id {interface-id}	ポートの ptp ステータスに関する詳細情報を表示します。

Multiple Stream Reservation Protocol のモニタリング

MSRP の詳細を表示するには、次の表のコマンドを使用します。

コマンド	目的
show msrp streams	MSRP ストリーム情報を表示します。
show msrp streams detailed	MSRP ストリームの詳細情報を表示します。
show msrp streams brief	MSRP ストリームの概要情報を表示します。
show msrp port bandwidth	MSRP ポート帯域幅情報を表示します。

階層型 QoS のモニタリング

HQoS の詳細を表示するには、次の表のコマンドを使用します。

コマンド	目的
show run	すべての子ポリシー マップの詳細を表示します。
show policy-map	ポリシー マップ設定の詳細を表示します。
show platform hardware fed switch active qos queue stats interface interface-id	AVB の異なるキュー マッピングの QoS 統計情報を表示します。
show platform hardware fed switch active qos queue config interface interface-id	QoS キュー構成を表示します。
show policy-map interface interface-id [input output]	AVB QoS 統計情報を表示します。入力のパケット カウンタと出力のバイト カウンタは、QoS 統計情報のために考慮されます。

マルチ VLAN 登録プロトコルのモニタリング

MVRP の詳細を表示するには、次の表のコマンドを使用します。

コマンド	目的
show mvrp summary	MVRP サマリー情報を表示します。
show mvrp interface	インターフェイスの MVRP 情報を表示します。

AVB 設定とモニタリングの例

AVB の例

次に、AVB ドメインを表示する例を示します。

```
Device#show avb domain

AVB Class-A
  Priority Code Point      : 3
  VLAN                    : 2
  Core ports              : 1
  Boundary ports          : 67

AVB Class-B
  Priority Code Point      : 2
```

```

VLAN                : 2
Core ports          : 1
Boundary ports      : 67

```

Interface	State	Delay	PCP	VID	Information
Te1/0/1	down	N/A			Oper state not up
Te1/0/2	down	N/A			Oper state not up
Te1/0/3	down	N/A			Oper state not up
Te1/0/4	down	N/A			Oper state not up
Te1/0/5	up	N/A			Port is not asCapable
Te1/0/6	down	N/A			Oper state not up
Te1/0/7	down	N/A			Oper state not up
Te1/0/8	down	N/A			Oper state not up
Te1/0/9	down	N/A			Oper state not up
Te1/0/10	down	N/A			Oper state not up
Te1/0/11	down	N/A			Oper state not up
Te1/0/12	down	N/A			Oper state not up
Te1/0/13	down	N/A			Oper state not up
Te1/0/14	down	N/A			Oper state not up
Te1/0/15	down	N/A			Oper state not up
Te1/0/16	down	N/A			Oper state not up
Te1/0/17	down	N/A			Oper state not up
Te1/0/18	down	N/A			Oper state not up
Te1/0/19	up	N/A			Port is not asCapable
Te1/0/20	down	N/A			Oper state not up
Te1/0/21	down	N/A			Oper state not up
Te1/0/22	down	N/A			Oper state not up
Te1/0/23	up	N/A			Port is not asCapable
Te1/0/24	down	N/A			Oper state not up
Te1/0/25	down	N/A			Oper state not up
Te1/0/26	down	N/A			Oper state not up
Te1/0/27	down	N/A			Oper state not up
Te1/0/28	down	N/A			Oper state not up
Te1/0/29	up	N/A			Port is not asCapable
Te1/0/30	down	N/A			Oper state not up
Te1/0/31	down	N/A			Oper state not up
Te1/0/32	down	N/A			Oper state not up
Te1/0/33	down	N/A			Oper state not up
Te1/0/34	down	N/A			Oper state not up
Te1/0/35	up	N/A			Port is not asCapable
Te1/0/36	down	N/A			Oper state not up
Te1/0/37	down	N/A			Oper state not up
Te1/0/38	down	N/A			Oper state not up
Te1/0/39	up	507ns			
Class-	A	core	3	2	
Class-	B	core	2	2	
Te1/0/40	down	N/A			Oper state not up


```

Te1/0/41      down      N/A      Oper state not up
Te1/0/42      down      N/A      Oper state not up
Te1/0/43      down      N/A      Oper state not up
Te1/0/44      down      N/A      Oper state not up
Te1/0/45      down      N/A      Oper state not up
Te1/0/46      down      N/A      Oper state not up
Te1/0/47      down      N/A      Oper state not up
Te1/0/48      down      N/A      Oper state not up
Te1/1/1       down      N/A      Oper state not up
Te1/1/2       down      N/A      Oper state not up
Te1/1/3       down      N/A      Oper state not up
Te1/1/4       down      N/A      Oper state not up
Te1/1/5       down      N/A      Oper state not up
Te1/1/6       down      N/A      Oper state not up
Te1/1/7       down      N/A      Oper state not up
Te1/1/8       down      N/A      Oper state not up
Te1/1/9       down      N/A      Oper state not up
Te1/1/10      down      N/A      Oper state not up
Te1/1/11      down      N/A      Oper state not up
Te1/1/12      down      N/A      Oper state not up
Te1/1/13      down      N/A      Oper state not up
Te1/1/14      down      N/A      Oper state not up
Te1/1/15      down      N/A      Oper state not up
Te1/1/16      down      N/A      Oper state not up
Fo1/1/1       down      N/A      Oper state not up
Fo1/1/2       down      N/A      Oper state not up
Fo1/1/3       down      N/A      Oper state not up
Fo1/1/4       down      N/A      Oper state not up

```

次に、AVB ストリーム情報を表示する例を示します。

```
Device#show avb streams
```

```

Stream ID:      0011.0100.0001:1      Incoming Interface:  Te1/1/1
Destination   : 91E0.F000.FE00
Class         : A
Rank          : 1
Bandwidth     : 6400 Kbit/s

```

```
Outgoing Interfaces:
```

```

-----
Interface      State      Time of Last Update      Information
-----
Te1/1/1       Ready     Tue Apr 26 01:25:40.634

```

```
Stream ID:          0011.0100.0002:2      Incoming Interface:  Tel1/1/1
Destination   : 91E0.F000.FE01
Class         : A
Rank          : 1
Bandwidth     : 6400 Kbit/s
```

Outgoing Interfaces:

```
-----
```

Interface	State	Time of Last Update	Information
Tel1/1/1	Ready	Tue Apr 26 01:25:40.634	

```
-----
```

gPTP の例

このコマンドは、インターフェイスの `ptp` の簡易ステータスを表示するために使用できます。

```
Device# show ptp brief
```

Interface	Domain	PTP State
FortyGigabitEthernet1/1/1	0	FAULTY
FortyGigabitEthernet1/1/2	0	SLAVE
GigabitEthernet1/1/1	0	FAULTY
GigabitEthernet1/1/2	0	FAULTY
GigabitEthernet1/1/3	0	FAULTY
GigabitEthernet1/1/4	0	FAULTY
TenGigabitEthernet1/0/1	0	FAULTY
TenGigabitEthernet1/0/2	0	FAULTY
TenGigabitEthernet1/0/3	0	MASTER
TenGigabitEthernet1/0/4	0	FAULTY
TenGigabitEthernet1/0/5	0	FAULTY
TenGigabitEthernet1/0/6	0	FAULTY
TenGigabitEthernet1/0/7	0	MASTER
TenGigabitEthernet1/0/8	0	FAULTY
TenGigabitEthernet1/0/9	0	FAULTY
TenGigabitEthernet1/0/10	0	FAULTY
TenGigabitEthernet1/0/11	0	MASTER
TenGigabitEthernet1/0/12	0	FAULTY
TenGigabitEthernet1/0/13	0	FAULTY
TenGigabitEthernet1/0/14	0	FAULTY
TenGigabitEthernet1/0/15	0	FAULTY
TenGigabitEthernet1/0/16	0	FAULTY
TenGigabitEthernet1/0/17	0	FAULTY
TenGigabitEthernet1/0/18	0	FAULTY
TenGigabitEthernet1/0/19	0	MASTER

```
TenGigabitEthernet1/0/20      0      FAULTY
TenGigabitEthernet1/0/21      0      FAULTY
TenGigabitEthernet1/0/22      0      FAULTY
TenGigabitEthernet1/0/23      0      FAULTY
TenGigabitEthernet1/0/24      0      FAULTY
TenGigabitEthernet1/1/1       0      FAULTY
TenGigabitEthernet1/1/2       0      FAULTY
TenGigabitEthernet1/1/3       0      FAULTY
TenGigabitEthernet1/1/4       0      FAULTY
TenGigabitEthernet1/1/5       0      FAULTY
TenGigabitEthernet1/1/6       0      FAULTY
TenGigabitEthernet1/1/7       0      FAULTY
TenGigabitEthernet1/1/8       0      FAULTY
```

このコマンドは、ptp クロック情報を表示するために使用できます。

```
Device# show ptp clock
```

```
PTP CLOCK INFO
PTP Device Type: Boundary clock
PTP Device Profile: IEEE 802/1AS Profile
Clock Identity: 0x4:6C:9D:FF:FE:4F:95:0
Clock Domain: 0
Number of PTP ports: 38
PTP Packet priority: 4
Priority1: 128
Priority2: 128
Clock Quality:
  Class: 248
  Accuracy: Unknown
  Offset (log variance): 16640
Offset From Master(ns): 0
Mean Path Delay(ns): 0
Steps Removed: 3
Local clock time: 00:12:13 UTC Jan 1 1970
```

このコマンドは、親のクロック情報を表示するために使用できます。

```
Device# show ptp parent
```

```
PTP PARENT PROPERTIES
Parent Clock:
Parent Clock Identity: 0xB0:7D:47:FF:FE:9E:B6:80
Parent Port Number: 3
Observed Parent Offset (log variance): 16640
Observed Parent Clock Phase Change Rate: N/A

Grandmaster Clock:
Grandmaster Clock Identity: 0x4:6C:9D:FF:FE:67:3A:80
```

```

Grandmaster Clock Quality:
  Class: 248
  Accuracy: Unknown
  Offset (log variance): 16640
  Priority1: 0
  Priority2: 128

```

このコマンドは、ptp ポート情報を表示するために使用できます。

```
Device# show ptp port
```

```

PTP PORT DATASET: FortyGigabitEthernet1/1/1
  Port identity: clock identity: 0x4:6C:9D:FF:FE:4E:3A:80
  Port identity: port number: 1
  PTP version: 2
  Port state: FAULTY
  Delay request interval(log mean): 5
  Announce receipt time out: 3
  Peer mean path delay(ns): 0
  Announce interval(log mean): 1
  Sync interval(log mean): 0
  Delay Mechanism: End to End
  Peer delay request interval(log mean): 0
  Sync fault limit: 500000000

```

```

PTP PORT DATASET: FortyGigabitEthernet1/1/2
  Port identity: clock identity: 0x4:6C:9D:FF:FE:4E:3A:80
  Port identity: port number: 2
  PTP version: 2
  Port state: FAULTY
  Delay request interval(log mean): 5
  Announce receipt time out: 3
  Peer mean path delay(ns): 0
  Announce interval(log mean): 1
--More--

```

このコマンドは、特定のインターフェイスのポート情報を表示するために使用できます。

```
Device# show ptp port gi1/0/26
```

```

PTP PORT DATASET: GigabitEthernet1/0/26
  Port identity: clock identity: 0x4:6C:9D:FF:FE:4E:3A:80
  Port identity: port number: 28
  PTP version: 2
  Port state: MASTER
  Delay request interval(log mean): 5
  Announce receipt time out: 3
  Peer mean path delay(ns): 0
  Announce interval(log mean): 1

```

```

Sync interval(log mean): 0
Delay Mechanism: Peer to Peer
Peer delay request interval(log mean): 0
Sync fault limit: 500000000

```

このコマンドは、を表示するために使用できます。

```
Device# show platform software fed switch active ptp if-id 0x20
```

```
Displaying port data for if_id 20
```

```
=====
```

```

Port Mac Address 04:6C:9D:4E:3A:9A
Port Clock Identity 04:6C:9D:FF:FE:4E:3A:80
Port number 28
PTP Version 2
domain_value 0
dot1as_capable: FALSE
sync_recpt_timeout_time_interval 375000000 nanoseconds
sync_interval 125000000 nanoseconds
neighbor_rate_ratio 0.000000
neighbor_prop_delay 0 nanoseconds
compute_neighbor_rate_ratio: TRUE
compute_neighbor_prop_delay: TRUE
port_enabled: TRUE
ptt_port_enabled: TRUE
current_log_pdelay_req_interval 0
pdelay_req_interval 0 nanoseconds
allowed_lost_responses 3
neighbor_prop_delay_threshold 2000 nanoseconds
is_measuring_delay : FALSE
Port state: : MASTER
sync_seq_num 22023
delay_req_seq_num 23857
num sync messages transmitted 0
num sync messages received 0
num followup messages transmitted 0
num followup messages received 0
num pdelay requests transmitted 285695
num pdelay requests received 0
num pdelay responses transmitted 0
num pdelay responses received 0
num pdelay followup responses transmitted 0
num pdelay followup responses received 0

```

MSRP の例

次に、MSRP ストリーム情報を表示する例を示します。

```
Device# show msrp streams
```

```
-----
Stream ID Talker Listener
Advertise Fail Ready ReadyFail AskFail
R | D R | D R | D R | D R | D
-----
YY:YY:YY:YY:YY:YY:0001 1 | 2 0 | 0 1 | 0 0 | 1 1 | 0
zz:zz:zz:zz:zz:zz:0002 1 | 0 0 | 1 1 | 0 0 | 0 0 | 1
-----
```

次に、詳細な MSRP ストリーム情報を表示する例を示します。

```
Device# show msrp streams detail
```

```
Stream ID:          0011.0100.0001:1
  Stream Age: 01:57:46 (since Mon Apr 25 23:41:11.413)
  Create Time: Mon Apr 25 23:41:11.413
  Destination Address: 91E0.F000.FE00
  VLAN Identifier: 1
  Data Frame Priority: 3 (Class A)
  MaxFrameSize: 100
  MaxIntervalFrames: 1 frames/125us
  Stream Bandwidth: 6400 Kbit/s
  Rank: 1
  Received Accumulated Latency: 20
  Stream Attributes Table:
```

```
-----
Interface          Attr State      Direction      Type
-----
Gi1/0/1            Register        Talker         Advertise
Attribute Age: 01:57:46 (since Mon Apr 25 23:41:11.413)
MRP Applicant: Very Anxious Observer, send None
MRP Registrar: In
Accumulated Latency: 20
-----
Te1/1/1            Declare         Talker         Advertise
Attribute Age: 00:19:52 (since Tue Apr 26 01:19:05.525)
MRP Applicant: Quiet Active, send None
MRP Registrar: In
Accumulated Latency: 20
-----
Te1/1/1            Register        Listener       Ready
Attribute Age: 00:13:17 (since Tue Apr 26 01:25:40.635)
MRP Applicant: Very Anxious Observer, send None
MRP Registrar: In
```

```

-----
  Gil/0/1          Declare          Listener    Ready
  Attribute Age: 00:13:17 (since Tue Apr 26 01:25:40.649)
  MRP Applicant: Quiet Active, send None
  MRP Registrar: In

```

次に、MSRP ストリーム情報を簡潔に表示する例を示します。

```
Device# show msrp streams brief
```

```
Legend: R = Registered, D = Declared.
```

```

-----
Stream ID          Destination          Bandwidth    Talkers
Listeners  Fail          Address          (Kbit/s)    R | D      R |
-----
D
0011.0100.0001:1  91E0.F000.FE00    6400         1 | 1      1 |
  1    No
0011.0100.0002:2  91E0.F000.FE01    6400         1 | 1      1 |
  1    No
0011.0100.0003:3  91E0.F000.FE02    6400         1 | 1      1 |
  1    No
0011.0100.0004:4  91E0.F000.FE03    6400         1 | 1      1 |
  1    No
0011.0100.0005:5  91E0.F000.FE04    6400         1 | 1      1 |
  1    No
0011.0100.0006:6  91E0.F000.FE05    6400         1 | 1      1 |
  1    No
0011.0100.0007:7  91E0.F000.FE06    6400         1 | 1      1 |
  1    No
0011.0100.0008:8  91E0.F000.FE07    6400         1 | 1      1 |
  1    No
0011.0100.0009:9  91E0.F000.FE08    6400         1 | 1      1 |
  1    No
0011.0100.000A:10 91E0.F000.FE09    6400         1 | 1      1 |
  1    No

```

次に、MSRP ポート帯域幅情報を表示する例を示します。

```
Device# show msrp port bandwidth
```

```

-----
Ethernet          Capacity          Assigned          Available          Reserved
Interface        (Kbit/s)         A | B             A | B             A | B
-----

```

```

Te1/0/1      10000000      75 | 0      75 | 75      0 | 0
Te1/0/2      10000000      75 | 0      75 | 75      0 | 0
Te1/0/3      10000000      75 | 0      75 | 75      0 | 0
Te1/0/4      10000000      75 | 0      75 | 75      0 | 0
Te1/0/5      10000000      75 | 0      75 | 75      0 | 0
Te1/0/6      10000000      75 | 0      75 | 75      0 | 0
Te1/0/8      10000000      75 | 0      75 | 75      0 | 0
Te1/0/9      10000000      75 | 0      75 | 75      0 | 0
Te1/0/10     10000000      75 | 0      75 | 75      0 | 0
Te1/0/11     10000000      75 | 0      75 | 75      0 | 0
Te1/0/12     10000000      75 | 0      75 | 75      0 | 0
Te1/0/13     10000000      75 | 0      75 | 75      0 | 0
Te1/0/14     10000000      75 | 0      75 | 75      0 | 0
Te1/0/15     10000000      75 | 0      75 | 75      0 | 0
Te1/0/16     10000000      75 | 0      75 | 75      0 | 0
Te1/0/17     10000000      75 | 0      75 | 75      0 | 0
Te1/0/18     10000000      75 | 0      75 | 75      0 | 0
Te1/0/19     10000000      75 | 0      75 | 75      0 | 0
Te1/0/20     10000000      75 | 0      75 | 75      0 | 0
Te1/0/21     10000000      75 | 0      75 | 75      0 | 0
Te1/0/22     10000000      75 | 0      75 | 75      0 | 0
Te1/0/23     10000000      75 | 0      75 | 75      0 | 0
Te1/0/24     10000000      75 | 0      75 | 75      0 | 0
Gi1/1/1      10000000      75 | 0      75 | 75      0 | 0
Gi1/1/2      10000000      75 | 0      75 | 75      0 | 0
Gi1/1/3      10000000      75 | 0      75 | 75      0 | 0
Gi1/1/4      10000000      75 | 0      75 | 75      0 | 0
Te1/1/1      10000000      75 | 0      75 | 75      0 | 0
Te1/1/2      10000000      75 | 0      75 | 75      0 | 0
Te1/1/3      10000000      75 | 0      75 | 75      0 | 0
Te1/1/4      10000000      75 | 0      75 | 75      0 | 0
Te1/1/5      10000000      75 | 0      75 | 75      0 | 0
Te1/1/6      10000000      75 | 0      75 | 75      0 | 0
Te1/1/7      10000000      75 | 0      75 | 75      0 | 0
Te1/1/8      10000000      75 | 0      75 | 75      0 | 0
Fo1/1/1      40000000      75 | 0      75 | 75      0 | 0
Fo1/1/2      40000000      75 | 0      75 | 75      0 | 0

```

HQoS の例

次に、AVB が有効になっている場合に、すべてのポリシー マップ設定の詳細を表示する例を示します。

```

Device# show policy-map

Policy Map AVB-Input-Policy-Remark-B
  Class AVB-SR-CLASS-A
    set cos 3
  Class AVB-SR-CLASS-B
    set cos 0

```



```
Class class-default
  service-policy AVB-Input-Child-Policy

Policy Map AVB-Input-Policy-Remark-A
Class AVB-SR-CLASS-A
  set cos 0
Class AVB-SR-CLASS-B
  set cos 2
Class class-default
  service-policy AVB-Input-Child-Policy

Policy Map AVB-Output-Policy-Default
Class AVB-SR-CLASS-A
  priority level 1 1 (%)
Class AVB-SR-CLASS-B
  priority level 2 1 (%)
Class AVB-CONTROL-MGMT-QUEUE
  priority level 3 15 (%)
Class class-default
  bandwidth remaining 100 (%)
  queue-buffers ratio 70
  service-policy AVB-Output-Child-Policy

Policy Map AVB-Input-Policy-Remark-AB
Class AVB-SR-CLASS-A
  set cos 0
Class AVB-SR-CLASS-B
  set cos 0
Class class-default
  service-policy AVB-Input-Child-Policy

Policy Map AVB-Input-Policy-Remark-None
Class AVB-SR-CLASS-A
  set cos 3
Class AVB-SR-CLASS-B
  set cos 2
Class class-default
  service-policy AVB-Input-Child-Policy

Policy Map AVB-Input-Child-Policy
Class AVB-VOIP-DATA-CLASS
  set dscp ef
Class AVB-MULTIMEDIA-CONF-CLASS
  set dscp af41
Class AVB-BULK-DATA-CLASS
  set dscp af11
Class AVB-TRANSACTIONAL-DATA-CLASS
  set dscp af21
Class AVB-SCAVENGER-DATA-CLASS
  set dscp cs1
Class AVB-SIGNALING-CLASS
```

```

    set dscp cs3
Class class-default
    set dscp default

Policy Map AVB-Output-Child-Policy
Class AVB-VOIP-PRIORITY-QUEUE
    bandwidth remaining 30 (%)
    queue-buffers ratio 30
Class AVB-MULTIMEDIA-CONF-STREAMING-QUEUE
    bandwidth remaining 15 (%)
    queue-limit dscp af41 percent 80
    queue-limit dscp af31 percent 80
    queue-limit dscp af42 percent 90
    queue-limit dscp af32 percent 90
    queue-buffers ratio 15
Class AVB-TRANSACTIONAL-DATA-QUEUE
    bandwidth remaining 15 (%)
    queue-limit dscp af21 percent 80
    queue-limit dscp af22 percent 90
    queue-buffers ratio 15
Class AVB-BULK-SCAVENGER-DATA-QUEUE
    bandwidth remaining 15 (%)
    queue-limit dscp af11 percent 80
    queue-limit dscp af12 percent 90
    queue-limit dscp cs1 percent 80
    queue-buffers ratio 15
Class class-default
    bandwidth remaining 25 (%)
    queue-buffers ratio 25

```

次に、AVB が無効になっている場合に、すべてのポリシー マップ設定の詳細を表示する例を示します。

```

Device# show policy-map

Building configuration...

Current configuration : 2079 bytes
!
policy-map AVB-Input-Child-Policy
class AVB-VOIP-DATA-CLASS
    set dscp ef
class AVB-MULTIMEDIA-CONF-CLASS
    set dscp af41
class AVB-BULK-DATA-CLASS
    set dscp af11
class AVB-TRANSACTIONAL-DATA-CLASS

```

```
    set dscp af21
class AVB-SCAVENGER-DATA-CLASS
  set dscp cs1
class AVB-SIGNALING-CLASS
  set dscp cs3
class class-default
  set dscp default
policy-map AVB-Output-Child-Policy
class AVB-VOIP-PRIORITY-QUEUE
  bandwidth remaining percent 30
  queue-buffers ratio 30
class AVB-MULTIMEDIA-CONF-STREAMING-QUEUE
  bandwidth remaining percent 15
  queue-limit dscp af41 percent 80
  queue-limit dscp af31 percent 80
  queue-limit dscp af42 percent 90
  queue-limit dscp af32 percent 90
  queue-buffers ratio 15
class AVB-TRANSACTIONAL-DATA-QUEUE
  bandwidth remaining percent 15
  queue-limit dscp af21 percent 80
  queue-limit dscp af22 percent 90
  queue-buffers ratio 15
class AVB-BULK-SCAVENGER-DATA-QUEUE
  bandwidth remaining percent 15
  queue-limit dscp af11 percent 80
  queue-limit dscp af12 percent 90
  queue-limit dscp cs1 percent 80
  queue-buffers ratio 15
class class-default
  bandwidth remaining percent 25
  queue-buffers ratio 25
!
end
```

次に、AVB が有効になっている場合に、すべてのクラス マップ設定の詳細を表示する例を示します。

```
Device# show class-map

Class Map match-any AVB-VOIP-DATA-CLASS (id 31)
  Match dscp ef (46)
  Match cos 5

Class Map match-any AVB-BULK-DATA-CLASS (id 33)
  Match access-group name AVB-BULK-DATA-CLASS-ACL

Class Map match-any AVB-VOIP-PRIORITY-QUEUE (id 37)
```

```
Match dscp cs4 (32) cs5 (40) ef (46)
Match precedence 4 5
Match cos 5

Class Map match-any AVB-MULTIMEDIA-CONF-CLASS (id 32)
  Match access-group name AVB-MULTIMEDIA-CONF-CLASS-ACL

Class Map match-any AVB-SIGNALING-CLASS (id 36)
  Match access-group name AVB-SIGNALING-CLASS-ACL

Class Map match-any AVB-MULTIMEDIA-CONF-STREAMING-QUEUE (id 38)
  Match dscp af41 (34) af42 (36) af43 (38)
  Match dscp af31 (26) af32 (28) af33 (30)
  Match cos 4

Class Map match-any AVB-BULK-SCAVENGER-DATA-QUEUE (id 40)
  Match dscp cs1 (8) af11 (10) af12 (12) af13 (14)
  Match precedence 1
  Match cos 1

Class Map match-any AVB-TRANSACTIONAL-DATA-CLASS (id 34)
  Match access-group name AVB-TRANSACTIONAL-DATA-CLASS-ACL

Class Map match-any AVB-TRANSACTIONAL-DATA-QUEUE (id 39)
  Match dscp af21 (18) af22 (20) af23 (22)

Class Map match-any AVB-SR-CLASS-B (id 42)
  Match cos 2

Class Map match-any AVB-SR-CLASS-A (id 41)
  Match cos 3

Class Map match-any AVB-SCAVENGER-DATA-CLASS (id 35)
  Match access-group name AVB-SCAVENGER-DATA-CLASS-ACL

Class Map match-any AVB-CONTROL-MGMT-QUEUE (id 43)
  Match ip dscp cs2 (16)
  Match ip dscp cs3 (24)
  Match ip dscp cs6 (48)
  Match ip dscp cs7 (56)
  Match ip precedence 6
  Match ip precedence 7
  Match ip precedence 3
  Match ip precedence 2
  Match cos 6
  Match cos 7
```

次に、AVB が無効になっている場合に、すべてのクラス マップ設定の詳細を表示する例を示します。

```
Device# show class-map

Building configuration...

Current configuration : 2650 bytes
!
class-map match-any AVB-VOIP-DATA-CLASS
match dscp ef
  match cos 5
class-map match-any AVB-BULK-DATA-CLASS
match access-group name AVB-BULK-DATA-CLASS-ACL
class-map match-any AVB-VOIP-PRIORITY-QUEUE
match dscp cs4 cs5 ef
  match precedence 4 5
  match cos 5
class-map match-any AVB-MULTIMEDIA-CONF-CLASS
match access-group name AVB-MULTIMEDIA-CONF-CLASS-ACL
class-map match-any AVB-SIGNALING-CLASS
match access-group name AVB-SIGNALING-CLASS-ACL
class-map match-any AVB-MULTIMEDIA-CONF-STREAMING-QUEUE
match dscp af41 af42 af43
  match dscp af31 af32 af33
  match cos 4
class-map match-any AVB-BULK-SCAVENGER-DATA-QUEUE
match dscp cs1 af11 af12 af13
  match precedence 1
  match cos 1
class-map match-any AVB-TRANSACTIONAL-DATA-CLASS
match access-group name AVB-TRANSACTIONAL-DATA-CLASS-ACL
class-map match-any AVB-TRANSACTIONAL-DATA-QUEUE
match dscp af21 af22 af23
class-map match-any AVB-SCAVENGER-DATA-CLASS
match access-group name AVB-SCAVENGER-DATA-CLASS-ACL
end
```

次に、すべての AVB QoS 統計情報を表示する例を示します。

```
Device# show policy-map interface gigabitEthernet 1/0/15

GigabitEthernet1/0/15

Service-policy input: AVB-Input-Policy-Remark-AB

Class-map: AVB-SR-CLASS-A (match-any)
  0 packets
  Match: cos 3
    0 packets, 0 bytes
    5 minute rate 0 bps
  QoS Set
```

```
cos 0

Class-map: AVB-SR-CLASS-B (match-any)
  0 packets
  Match: cos 2
    0 packets, 0 bytes
    5 minute rate 0 bps
  QoS Set
    cos 0

Class-map: class-default (match-any)
  0 packets
  Match: any

Service-policy : AVB-Input-Child-Policy

Class-map: AVB-VOIP-DATA-CLASS (match-any)
  0 packets
  Match: dscp ef (46)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos 5
    0 packets, 0 bytes
    5 minute rate 0 bps
  QoS Set
    cos 3

Class-map: AVB-MULTIMEDIA-CONF-CLASS (match-any)
  0 packets
  Match: access-group name AVB-MULTIMEDIA-CONF-CLASS-ACL
    0 packets, 0 bytes
    5 minute rate 0 bps
  QoS Set
    dscp af41

Class-map: AVB-BULK-DATA-CLASS (match-any)
  0 packets
  Match: access-group name AVB-BULK-DATA-CLASS-ACL
    0 packets, 0 bytes
    5 minute rate 0 bps
  QoS Set
    dscp af11

Class-map: AVB-TRANSACTIONAL-DATA-CLASS (match-any)
  0 packets
  Match: access-group name AVB-TRANSACTIONAL-DATA-CLASS-ACL
    0 packets, 0 bytes
    5 minute rate 0 bps
  QoS Set
    dscp af21
```

```
Class-map: AVB-SCAVENGER-DATA-CLASS (match-any)
  0 packets
  Match: access-group name AVB-SCAVENGER-DATA-CLASS-ACL
    0 packets, 0 bytes
    5 minute rate 0 bps
  QoS Set
    dscp cs1

Class-map: AVB-SIGNALING-CLASS (match-any)
  0 packets
  Match: access-group name AVB-SIGNALING-CLASS-ACL
    0 packets, 0 bytes
    5 minute rate 0 bps
  QoS Set
    dscp cs3

Class-map: class-default (match-any)
  0 packets
  Match: any
  QoS Set
    dscp default

Service-policy output: AVB-Output-Policy-Default

queue stats for all priority classes:
  Queueing
  priority level 3

  (total drops) 0
  (bytes output) 7595

queue stats for all priority classes:
  Queueing
  priority level 2

  (total drops) 0
  (bytes output) 0

queue stats for all priority classes:
  Queueing
  priority level 1

  (total drops) 0
  (bytes output) 0

Class-map: AVB-SR-CLASS-A (match-any)
  0 packets
  Match: cos 3
    0 packets, 0 bytes
    5 minute rate 0 bps
  Priority: 1% (10000 kbps), burst bytes 250000,
```

```
Priority Level: 1

Class-map: AVB-SR-CLASS-B (match-any)
  0 packets
  Match: cos 2
    0 packets, 0 bytes
    5 minute rate 0 bps
  Priority: 1% (10000 kbps), burst bytes 250000,

Priority Level: 2

Class-map: AVB-CONTROL-MGMT-QUEUE (match-any)
  0 packets
  Match: ip dscp cs2 (16)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: ip dscp cs3 (24)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: ip dscp cs6 (48)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: ip dscp cs7 (56)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: ip precedence 6
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: ip precedence 7
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: ip precedence 3
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: ip precedence 2
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos 6
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos 7
    0 packets, 0 bytes
    5 minute rate 0 bps
  Priority: 15% (150000 kbps), burst bytes 3750000,

Priority Level: 3

Class-map: class-default (match-any)
  0 packets
  Match: any
```


Queueing

```
(total drops) 0
(bytes output) 0
bandwidth remaining 80%
queue-buffers ratio 70
```

Service-policy : AVB-Output-Child-Policy

```
Class-map: AVB-VOIP-PRIORITY-QUEUE (match-any)
  0 packets
  Match: dscp cs4 (32) cs5 (40) ef (46)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: precedence 4 5
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos 5
    0 packets, 0 bytes
    5 minute rate 0 bps
Queueing
```

```
(total drops) 0
(bytes output) 0
bandwidth remaining 30%
queue-buffers ratio 30
```

```
Class-map: AVB-MULTIMEDIA-CONF-STREAMING-QUEUE (match-any)
  0 packets
  Match: dscp af41 (34) af42 (36) af43 (38)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: dscp af31 (26) af32 (28) af33 (30)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos 4
    0 packets, 0 bytes
    5 minute rate 0 bps
Queueing
```

```
queue-limit dscp 26 percent 80
queue-limit dscp 28 percent 90
queue-limit dscp 34 percent 80
queue-limit dscp 36 percent 90
(total drops) 0
(bytes output) 0
bandwidth remaining 15%

queue-buffers ratio 15
```

Class-map: AVB-TRANSACTIONAL-DATA-QUEUE (match-any)

```
0 packets
Match: dscp af21 (18) af22 (20) af23 (22)
      0 packets, 0 bytes
      5 minute rate 0 bps
Match: cos 0
      0 packets, 0 bytes
      5 minute rate 0 bps
Queueing

queue-limit dscp 18 percent 80
queue-limit dscp 20 percent 90
(total drops) 0
(bytes output) 0
bandwidth remaining 15%

queue-buffers ratio 15

Class-map: AVB-BULK-SCAVENGER-DATA-QUEUE (match-any)
0 packets
Match: dscp cs1 (8) af11 (10) af12 (12) af13 (14)
      0 packets, 0 bytes
      5 minute rate 0 bps
Match: precedence 1
      0 packets, 0 bytes
      5 minute rate 0 bps
Match: cos 1
      0 packets, 0 bytes
      5 minute rate 0 bps
Queueing

queue-limit dscp 8 percent 80
queue-limit dscp 10 percent 80
queue-limit dscp 12 percent 90
(total drops) 0
(bytes output) 0
bandwidth remaining 15%

queue-buffers ratio 15

Class-map: class-default (match-any)
0 packets
Match: any
Queueing

(total drops) 0
(bytes output) 0
bandwidth remaining 25%
queue-buffers ratio 25
```

次に、**show platform hardware fed switch active qos queue config interface interface-id** コマンドの出力例を示します。

```
Device# show platform hardware fed switch active qos queue config interface t1/0/11
DATA Port:2 GPN:11 AFD:Disabled QoSMap:2 HW Queues: 16 - 23
  DrainFast:Disabled PortSoftStart:1 - 3600
```

	DTS	Hardmax	Softmax	PortSMin	GlblSMin	PortStEnd
0	0	9	33	3	33	0 0 0 0 1 4800
1	0	9	33	4	2400	99 99 0 0 1 4800
2	1	6	30	4	2400	90 90 0 0 1 4800
3	1	5	0	4	2400	189 189 63 63 1 4800
4	1	5	0	4	2400	90 90 30 30 1 4800
5	1	5	0	4	2400	90 90 30 30 1 4800
6	1	5	0	4	2400	90 90 30 30 1 4800
7	1	5	0	4	2400	153 153 51 51 1 4800
Priority	Shaped/shared			weight	shaping_step	
0	1	Shaped		16383	163	
1	2	Shaped		16383	163	
2	3	Shaped		125	153	
3	7	Shared		50	0	
4	7	Shared		100	0	
5	7	Shared		100	0	
6	7	Shared		100	0	
7	7	Shared		60	0	

次に、**show platform hardware fed switch active qos queue stats interface interface-id** コマンドの出力例を示します。

```
Device# show platform hardware fed switch active qos queue stats interface t1/0/15
DATA Port:8 Enqueue Counters
```

Queue	Buffers	Enqueue-TH0	Enqueue-TH1	Enqueue-TH2
0	1	0	0	23788459506
1	0	0	0	30973507838
2	0	0	12616270	13164040
3	0	0	0	0
4	0	0	0	0
5	0	0	0	0
6	0	0	0	0
7	0	0	0	119616

```
DATA Port:8 Drop Counters
```

Queue	Drop-TH0	Drop-TH1	Drop-TH2	SBufDrop	QebDrop
0	0	0	0	0	0

1	0	0	0	0	0	0
2	0	0	0	0	0	0
3	0	0	0	0	0	0
4	0	0	0	0	0	0

MVRP の例

次に、MVRP サマリー情報を表示する例を示します。

```
Device# show mvrp summary
```

```
MVRP global state           : enabled
MVRP VLAN creation         : enabled
VLANs created via MVRP     : 2,567
MAC learning auto provision : disabled
Learning disabled on VLANs : none
```

次に、インターフェイス MVRP 情報を表示する例を示します。

```
Device# show mvrp interface
```

```
Port          Status      Registrar State
Tel1/0/47     on          normal
Tel1/1/3     off         normal

Port          Join Timeout      Leave Timeout      Leaveall Timeout
Periodic

Timeout
Tel1/0/47     20                60                 1000              100
Tel1/1/3     20                60                 1000              100

Port          Vlans Declared
Tel1/0/47     1-2,567,900
Tel1/1/3     none

Port          Vlans Registered
Tel1/0/47     2,567
Tel1/1/3     none

Port          Vlans Registered and in Spanning Tree Forwarding State
Tel1/0/47     2,567
Tel1/1/3     none
```

オーディオビデオブリッジングの機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Fuji 16.8.1a	オーディオビデオブリッジ (AVB) : IEEE 802.1BA	AVB は、エンドポイントとネットワークが全体として機能し、コンシューマ向けアプリケーション間の高品質 A/V ストリーミングをイーサネットインフラストラクチャを介してプロフェッショナル向けオーディオ/ビデオにまで可能にする、標準ベースのメカニズムです。 この機能のサポートは、Cisco Catalyst 9500 シリーズスイッチのすべてのモデルで導入されました。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> [英語] からアクセスします。

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。