LAN スイッチング コンフィギュレーション ガイド、Cisco IOS XE Release 3S（Cisco ASR 1000）

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。

目 次

ERSPAN の設定 1

機能情報の確認 1

ERSPAN 設定時の制約事項 2

ERSPAN の設定に関する情報 2

ERSPAN の概要 2

ERSPAN 送信元 4

ERSPAN 宛先ポート 5

ローカル SPAN としての ERSPAN の使用 6

WAN インターフェイスでの ERSPAN サポート 6

ERSPAN の設定方法 6

ERSPAN 送信元セッションの設定 6

ERSPAN 宛先セッションの設定 10

ERSPAN の設定例 13

例：ERSPAN 送信元セッションの設定 13

例：WAN インターフェイスの ERSPAN 送信元セッションの設定 13

例：ERSPAN 宛先セッションの設定 13

例：ローカル SPAN としての ERSPAN の設定 14

ERSPAN の設定に関する追加情報 14

ERSPAN の設定に関する機能情報 15

IEEE 802.1Q カプセル化を使用する VLAN 間のルーティング設定 17

機能情報の確認 17

IEEE 802.1Q カプセル化を使用する VLAN 間のルーティング設定の制約事項 18

IEEE 802.1Q カプセル化を使用する VLAN 間のルーティング設定に関する情報 18

IEEE 802.1Q カプセル化を使用する VLAN 間のルーティング設定 18

IEEE 802.1Q カプセル化を使用する VLAN 間のルーティング設定方法 18

IEEE 802.1Q での IP ルーティングの設定 18

IP ルーティングのイネーブル化 19

VLAN カプセル化方式の定義 19
ネットワーク インターフェイスへの IP アドレスの割り当て 21
VLAN サブインターフェイスのモニタリングおよびメンテナンス 22
IEEE 802.1Q カプセル化を使用する VLAN 間のルーティング設定の設定例 23
IEEE 802.1Q での IP ルーティングの設定例 23
その他の関連資料 23
IEEE 802.1Q カプセル化を使用する VLAN 間のルーティング設定の機能情報 25
IEEE 802.1Q-in-Q VLAN タグ終端 27
機能情報の確認 27
IEEE 802.1Q-in-Q VLAN タグ終端に関する情報 28
サブインターフェイスでの IEEE 802.1Q-in-Q VLAN タグ終端機能 28
一義的なサブインターフェイスとあいまいなサブインターフェイス 29
IEEE 802.1Q-in-Q VLAN タグ終端の設定方法 30
IEEE 802.1Q-in-Q VLAN タグ終端のインターフェイスの設定 30
IEEE 802.1 Q-in-Q VLAN タグ終端機能の確認 32
IEEE 802.1Q-in-Q VLAN タグ終端の設定例 34
IEEE 802.1Q-in-Q VLAN タグ終端のサブインターフェイスでの任意のキーワードの設定例 34
その他の関連資料 36
IEEE 802.1Q-in-Q VLAN タグ終端に関する機能情報 37
ギガビット EtherChannel メンバー リンクへの VLAN マッピング 39
機能情報の確認 39
GEC メンバー リンクへの VLAN マッピングの前提条件 40
GEC メンバー リンクへの VLAN マッピングの制約事項 40
GEC メンバー リンクの VLAN マッピングに関する情報 40
手動 VLAN ロード バランシング 40
VLAN からポート チャネル メンバーへのリンク マッピング 42
VLAN のプライマリ リンクおよびセカンダリ リンクの関連付け 42
チャネル メンバー リンクの追加 44
メンバー リンクの削除 45
ポート チャネル リンク ダウン通知 45
ポート チャネル リンク アップ通知 45

EtherChannel でのロード バランスのディセーブル化 45
EtherChannel のメンバー リンクの削除 46
GEC リンクへの VLAN マッピングの設定方法 46
VLAN ベースの手動ロード バランシングの設定 46
トラブルシューティングのヒント 48
GEC メンバー リンクへの VLAN マッピングの設定例 48
例：VLAN 手動ロード バランシングの設定 48
例：トラブルシューティング 50
その他の関連資料 51
GEC メンバー リンクへの VLAN マッピングの機能情報 51
EtherChannel フローベース限定 1:1 冗長性 53
機能情報の確認 53
EtherChannel フローベース限定 1:1 冗長性に関する情報 54
EtherChannel フローベース限定 1:1 冗長性 54
EtherChannel フローベース限定 1:1 冗長性の設定方法 54
EtherChannel フローベース限定 1:1 冗長性のファストスイッチオーバーとの設定 54
キャリア遅延のスイッチオーバー レートの設定 57
EtherChannel フローベース限定 1:1 冗長性の確認 58
EtherChannel フローベース限定 1:1 冗長性の設定例 59
EtherChannel 1:1 アクティブ スタンバイの例 59
LACP を使用した 1:1 冗長性のプライオリティ設定の例 60
その他の関連資料 61
EtherChannel フローベース限定 1:1 冗長性の機能情報 62
フローベースのポートチャネルごとのロード バランシング 65
機能情報の確認 65
フローベースのポートチャネルごとのロード バランシングの制約事項 66
フローベースのポートチャネルごとのロード バランシングに関する情報 66
フローベースのロード バランシング 66
フローベースのロード バランシング用のバケット 66
ポート チャネルのロード バランシング 68
フローベースのポートチャネルごとのロード バランシングをイネーブルにする方法 70
ポート チャネルのロード バランシングの設定 70

GEC インターフェイスのロードバランシング設定の確認 72
フローベースのポートチャネルごとのロード バランシングの設定例 73
フローベースのロード バランシングの例 73
その他の関連資料 74
フローベースのポートチャネルごとのロード バランシングの機能情報 75
Resilient Ethernet Protocol（REP） 77
機能情報の確認 77
Resilient Ethernet Protocol の制約事項 78
REP に関する情報 78
REP セグメント 78
リンク完全性 80
短時間でのコンバージェンス 81
VLAN ロード バランシング 81
スパニングツリー プロトコルの対話 82
REP ポート 83
VPLS との REP 統合 83
REP のデフォルト設定 84
REP セグメントと REP 管理 VLAN 84
REP 設定時の注意事項 84
トランク EFP の REP サポート 85
REP 設定可能タイマー 86
REP Fast Hello での SSO サポート 86
REP 非ネイバー エッジ サポート 87
REP の設定方法 88
REP 管理 VLAN の設定 88
インターフェイスのトランク EFP の設定 89
トランク EFP の REP サポートの設定 91
VLAN ロード バランシングのプリエンプションの設定 94
制約事項 94
REP の SNMP トラップ設定 95
REP 設定のモニタリング 97
REP 設定可能タイマーの設定 98

非ネイバー エッジ ポートとしての REP の設定 101
REP の設定例 103
REP 管理 VLAN の設定 103
トランク EFP の REP サポートの設定 103
VLAN ロード バランシングのプリエンプションの設定 104
REP の SNMP トラップ設定 104
REP 設定のモニタリング 104
REP 設定可能タイマーの設定 105
REP 非ネイバー エッジ サポートの設定 105
その他の関連資料 105
Resilient Ethernet Protocol の機能情報 106

第 1 章

ERSPAN の設定

このモジュールは、Encapsulated Remote Switched Port Analyzer（ERSPAN）を設定する方法について説明します。 Cisco ERSPAN 機能を使用すると、1 つ以上のポートまたは VLAN のトラフィックをモニタし、1 つ以上の宛先ポートに、モニタされたトラフィックを送信できます。

（注） ERSPAN 機能は、レイヤ 2 スイッチング インターフェイスではサポートされません。

- 機能情報の確認，1 ページ
- ERSPAN 設定時の制約事項，2 ページ
- ERSPAN の設定に関する情報，2 ページ
- ERSPAN の設定方法，6 ページ
- ERSPAN の設定例，13 ページ
- ERSPAN の設定に関する追加情報，14 ページ
- ERSPAN の設定に関する機能情報 ，15 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の警告および機能情報については、『Bug Search Tool』およびご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

ERSPAN 設定時の制約事項

- Cisco ASR 1000 シリーズ ルータで許可される ERSPAN セッションの最大数は 1024 です。 Cisco ASR 1000 シリーズ ルータは、ERSPAN 送信元デバイス（送信元セッションだけ設定可能）、ERSPAN 宛先デバイス（宛先セッションだけ設定可能）、または ERSPAN 送信元/宛先デバイス（送信元セッションと宛先セッションを両方とも設定可能）として使用できます。 ただし、セッションの合計数が 1024 を超えないようにする必要があります。
- 各 ERSPAN セッションで使用可能な最大ポート数は 128 です。
- Cisco ASR 1000 シリーズ ルータの ERSPAN は、送信元セッションの送信元ポートとしてファストイーサネット、ギガビットイーサネット、TenGigabitイーサネット、およびポートチャネル インターフェイスをサポートします。
- Cisco ASR 1000 シリーズ ルータの ERSPAN ユーザは、送信元としてポートのリストまたはソースとしてVLANのリストを設定できますが、特定のセッションに両方を設定することはできません。
- ERSPAN コンフィギュレーション CLI を介してセッションが設定されると、セッション ID とセッション タイプは変更できません。 これらを変更するには、まずコンフィギュレーション コマンドの **no** 形式を使用してセッションを削除してから、セッションを再設定する必要があります。
- **monitor session** *span-session-number* **type local** コマンドは、Cisco ASR 1000 シリーズ ルータではサポートされません。
- フィルタ VLAN オプションは、WAN インターフェイス上の ERSPAN モニタリング セッションでは機能しません。

ERSPAN の設定に関する情報

ERSPAN の概要

Cisco ERSPAN 機能を使用すると、1 つ以上のポートまたは VLAN のトラフィックを監視し、1 つ以上の宛先ポートに、監視されたトラフィックを送信できます。 ERSPAN は、スイッチ プローブ デバイスやその他のリモート モニタリング（RMON）プローブなどのネットワーク アナライザにトラフィックを送信します。 ERSPAN は、異なるルータ上のソース ポート、ソース VLAN、および宛先ポートをサポートして、ネットワーク上での複数のルータのリモート モニタリングを提供します（次の図を参照）。

Cisco ASR 1000 シリーズ ルータでは、ERSPAN は、最大 9180 バイトのカプセル化パケットをサポートします。 デフォルト ERSPAN 最大伝送単位（MTU）のサイズは 1500 バイトです。 カプセル化された IPv4 ヘッダー、総称ルーティング カプセル化（GRE）のヘッダー、ERSPAN ヘッダー、および元のパケットで構成される ERSPAN ペイロード長が ERSPAN MTU サイズを超過すると、複製されたパケットはデフォルトの ERSPAN MTU サイズに切り捨てられます。

ERSPAN は、ERSPAN 送信元セッション、ルーティング可能な ERSPAN GRE カプセル化トラフィック、ERSPAN 宛先セッションで構成されています。

ERSPAN 送信元セッション、ERSPAN 宛先セッション、またはその両方を Cisco ASR 1000 シリーズ ルータで設定できます。 ERSPAN 送信元セッションだけが設定されたデバイスは、ERSPAN 送信元デバイスと呼ばれ、ERSPAN 宛先セッションだけが設定されたデバイスは ERSPAN 終端デバイスと呼ばれます。 Cisco ASR 1000 シリーズ ルータは、ERSPAN 送信元デバイスと ERSPAN 終端デバイスの両方として機能できます。 宛先セッションを持つ ERSPAN セッションは、同一の Cisco ASR 1000 シリーズ ルータで終了できます。

ERSPAN 送信元セッションは、次のパラメータによって定義されます。

- セッション ID
- セッションでモニタされる送信元ポートまたは送信元 VLAN の一覧
- キャプチャされたトラフィックの GRE エンベロープの宛先 IP アドレスおよび送信元 IP アドレスとしてそれぞれ使用される、宛先および元の IP アドレス
- ERSPAN フロー ID
- IP タイプ オブ サービス（TOS）および IP 有効時間（TTL）などの、GRE エンベロープに関連したオプション属性

ERSPAN 宛先セッションは、次によって定義されます。

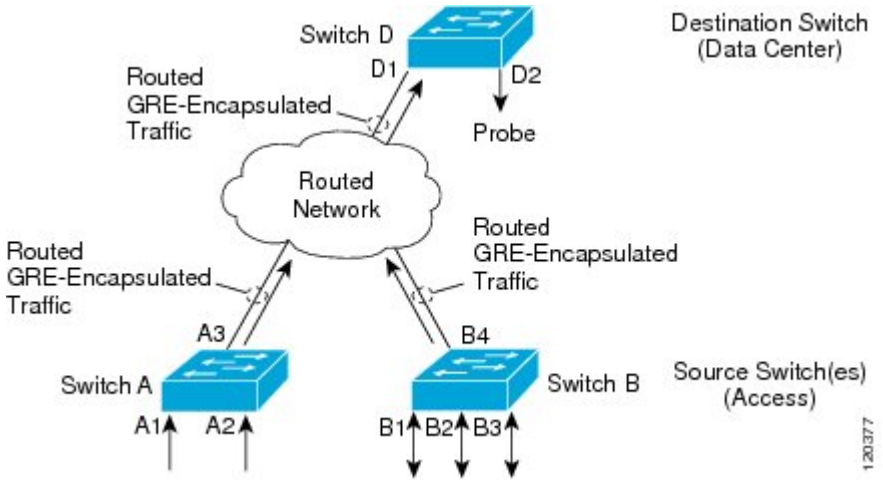
- セッション ID
- 宛先ポート
- 送信元 IP アドレス（対応する送信元セッションの宛先 IP アドレスと同じ）
- 宛先セッションを送信元セッションと照合するための ERSPAN フロー ID

ERSPAN 送信元セッションは、ERSPAN GRE カプセル化されたトラフィックを送信元ポートからコピーしません。 ERSPAN 送信元セッションごとに、送信元としてポートまたは VLAN を使用することはできますが、両方は使用できません。

各 ERSPAN 送信元セッションは、送信元ポートまたは送信元 VLAN からトラフィックをコピーし、ルーティング可能な GRE カプセル化されたパケットを使用して、そのトラフィックを ERSPAN

宛先セッションに転送します。 ERSPAN 宛先セッションは、トラフィックを宛先ポートに切り替えます。

図 *1*：*ERSPAN* の設定



監視対象トラフィック

送信元ポートまたは送信元 VLAN については、ERSPAN は、入力トラフィック、出力トラフィック、または入出力トラフィックを監視できます。 デフォルトでは、ERSPAN は、マルチキャストおよびブリッジ プロトコル データ ユニット（BPDU）フレームを含む、すべてのトラフィックを監視します。

ERSPAN 送信元

Cisco ERSPAN 機能は次の送信元をサポートします。

- 送信元ポート：トラフィック分析のためにモニタされる送信元ポートです。 任意の VLAN の送信元ポートを設定することができ、トランク ポートは、非トランク送信元ポートとともに送信元ポートとして設定できます。
- 送信元 VLAN：トラフィック分析のためにモニタされる VLAN です。

次のトンネル インターフェイスが送信元セッションの送信元ポートとしてサポートされます。

- GRE
- IPinIP
- IPv6
- IPv6 over IP トンネル
- マルチポイント GRE（mGRE）
- セキュア仮想トンネル インターフェイス（SVTI）

（注） SVTI および IPinIP トンネル インターフェイスは、IPsec 保護されたトンネル パケットと、IPsec 保護されていないトンネル パケットの両方をモニタできます。 トンネル パケットのモニタリングでは、そのトンネルが IPsec 保護されている場合は、IPsec 復号化後にクリアテキスト トンネル パケットを見ることができます。

次の制約事項は Cisco IOS XE Release 3.4S で導入された機能拡張に適用されます。

- IPsec 保護されていないトンネル パケットのモニタリングは、IPv6 および IPv6 over IP のトンネル インターフェイスでサポートされます。
- 機能拡張は、ERSPAN 宛先セッションには適用されず、ERSPAN 送信元セッションだけに適用されます。

ERSPAN は、Cisco IOS XE Release 3.4S で次の動作を行います。

- トンネル インターフェイスは、トンネル インターフェイスが削除されるときに、すべてのレベルの ERSPAN データベースから削除されます。 同じトンネルを再作成する場合は、トンネル トラフィックをモニタし続けるために、そのトンネルを手動でソース モニタ セッションで設定します。
- レイヤ 2 イーサネット ヘッダーは、0 に設定された送信元と宛先の両方の MAC アドレスで生成されます。

Cisco IOS XE Release 3.5S では、送信元セッションの送信元ポートとして、次のタイプの WAN インターフェイスのサポートが追加されました。

- シリアル（T1/E1、T3/E3、DS0）
- SONET（POS）（OC3、OC12）を経由するパケット
- マルチリンク PPP
- **multilink**、**pos**、および **serial** キーワードが、**source interface** コマンドに追加されました。

ERSPAN 宛先ポート

宛先ポートは、ERSPAN が分析用のトラフィックを送信するレイヤ 2 LAN ポートまたはレイヤ 3 LAN ポートです。

宛先ポートとしてポートを設定すると、そのポートはトラフィックを受信できなくなり、ERSPAN 機能によってのみ使用される専用のポートになります。 ERSPAN 宛先ポートでは、ERSPAN セッションに必要なトラフィック以外の転送は行われません。トランク ポートを宛先ポートとして設定することができます。これによって、宛先トランク ポートがカプセル化したトラフィックを転送することができます。

ローカル SPAN としての ERSPAN の使用

1 つ以上のポートまたは VLAN を介してトラフィックをモニタリングするために ERSPAN を使用するには、ERSPAN 送信元および ERSPAN 宛先のセッションを作成する必要があります。

同じルータまたは別のルータに 2 つのセッションを作成できます。 2 つのセッションが 2 つの異なるルータに作成された場合、モニタリング トラフィックは、ERSPAN によって送信元から宛先に転送されます。 ただし、2 つのセッションが同じルータに作成された場合、データ フローは、ローカル SPAN と同様に、ルータ内で行われます。

ERSPAN をローカル SPAN として使用するときには、次が該当します。

- 両方のセッションが同じ ERSPAN ID になります。
- 両方のセッションが同じ IP アドレスになります。 この IP アドレスは、ルータ自体の IP アドレスです。つまり、任意のポートに設定されたループバック IP アドレスまたは IP アドレスです。

WAN インターフェイスでの ERSPAN サポート

Cisco IOS Release 3.5S で、WAN の ERSPAN 送信元は、WAN インターフェイス上のトラフィックのモニタリングのために追加されます。 ERSPANは、元のフレームを複製し、WANインターフェイスのファブリック インターフェイス ASIC（FIA）エントリを追加して、IP または GRE パケット内部の複製されたフレームをカプセル化します。 複製されたパケットのフレーム ヘッダーがキャプチャ用に変更されます。 カプセル化後に、ERSPANはネットワーク上のデバイスにIPネットワークを介して IP または GRE パケットを送信します。 このデバイスは、ネットワーク デバイスに直接接続されている分析デバイスに元のフレームを送信します。

ERSPAN の設定方法

ERSPAN では、個別の送信元セッションおよび宛先セッションを使用します。 同じルータまたは異なるルータのいずれかで送信元および宛先セッションを設定します。

ERSPAN 送信元セッションの設定

ERSPAN 送信元セッションは、セッション設定パラメータおよびモニタするポートまたは VLAN を定義します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *interface-type interface-number*
4. **plim ethernet vlan filter disable**
5. **monitor session** *span-session-number* **type erspan-source**
6. **description** *string*
7. **source interface** *interface-name interface-number*
8. **source vlan** {*id-single* | *id-list* | *id-range* | *id-mixed*} [**rx** | **tx** | **both**]
9. **filter vlan** {*id-single* | *id-list* | *id-range* | *id-mixed*}
10. **destination**
11. **erspan-id** *erspan-flow-id*
12. **ip address** *ip-address*
13. **ip prec** *prec-value*
14. **ip dscp** *dscp-value*
15. **ip ttl** *ttl-value*
16. **mtu** *mtu-size*
17. **origin ip address** *ip-address* [**force**]
18. **vrf** *vrf-id*
19. **no shutdown**
20. **end**

手順の詳細

	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 モードをイネーブルにします。 • 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-type interface-number* 例： `Device(config)# interface GigabitEthernet1/0/1`	ERSPAN送信元セッションを設定するインターフェイスを指定します。

	コマンドまたはアクション	目的
ステップ 4	**plim ethernet vlan filter disable** 例： `Device(config-if)# plim ethernet vlan filter disable`	（任意）イーサネット インターフェイスの VLAN フィルタリング オプションをディセーブルにします。 **vlan filter** コマンドを使用するか、送信元インターフェイスが dot1q カプセル化を使用する場合は、このコマンドを使用します。
ステップ 5	**monitor session** *span-session-number* **type erspan-source** 例： `Device(config)# monitor session 1 type erspan-source`	セッション ID とセッション タイプを使用して ERSPAN 送信元セッションを定義し、ERSPAN のモニタ送信元セッション コンフィギュレーション モードを開始します。 • *span-session-number* 引数の範囲は 1 ～ 1024 です。 同じセッション番号は複数回使用できません。 • 送信元セッションまたは宛先セッションのセッション ID は同じグローバルな ID スペース内にあるため、各セッション ID は両方のセッション タイプに対してグローバルに一意です。 • セッション ID（*span-session-number* 引数によって設定）およびセッション タイプ（**erspan-source** キーワードによって設定）は、入力後は変更できません。 セッションを削除するには、このコマンドの **no** 形式を使用し、新しいセッション ID または新しいセッション タイプでセッションを再作成します。
ステップ 6	**description** *string* 例： `Device(config-mon-erspan-src)# description source1`	（任意）ERSPAN 送信元セッションの説明を入力します。 • *string* 引数には最大 240 文字を使用できます。ただし、特殊文字またはスペースは使用できません。
ステップ 7	**source interface** *interface-name interface-number* 例： `Device(config-mon-erspan-src)# source interface GigabitEthernet1/0/1 rx`	単一 ERSPAN セッション内で複数の WAN インターフェイスを設定します。
ステップ 8	**source vlan** {*id-single* | *id-list* | *id-range* | *id-mixed*} [**rx** | **tx** | **both**] 例： `Device(config-mon-erspan-src)# source vlan 1`	（任意）ERSPAN 送信元セッション番号を VLAN に関連付け、モニタするトラフィックの方向を選択します。 • 送信元 VLAN とフィルタ VLAN を同じセッションに含めることはできません。 送信元 VLAN またはフィルタ VLAN のいずれかを含めることはできますが、同時に両方を含めることはできません。

	コマンドまたはアクション	目的
ステップ 9	**filter vlan** {*id-single* | *id-list* | *id-range* | *id-mixed*} 例： `Device(config-mon-erspan-src)# filter vlan 1`	（任意）ERSPAN 送信元がトランク ポートである場合、送信元 VLAN フィルタリングを設定します。 • 送信元 VLAN とフィルタ VLAN を同じセッションに含めることはできません。送信元VLANまたはフィルタVLANを使用することはできますが、両方を同時には使用できません。
ステップ 10	**destination** 例： `Device(config-mon-erspan-src)# destination`	ERSPAN送信元セッションの宛先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	**erspan-id** *erspan-flow-id* 例： `Device(config-mon-erspan-src-dst)# erspan-id 100`	ERSPANトラフィックを識別するため、送信元および宛先セッションで使用される ID を設定します。これは、ERSPAN 宛先セッションの設定でも入力する必要があります。
ステップ 12	**ip address** *ip-address* 例： `Device(config-mon-erspan-src-dst)# ip address 10.10.0.1`	ERSPAN トラフィックの宛先として使用される IP アドレスを設定します。
ステップ 13	**ip prec** *prec-value* 例： `Device(config-mon-erspan-src-dst)# ip prec 5`	（任意）ERSPAN トラフィック内のパケットの IP precedence 値を設定します。 • オプションで **ip prec** コマンドまたは **ip dscp** コマンドのいずれかを使用できますが、両方は使用できません。
ステップ 14	**ip dscp** *dscp-value* 例： `Device(config-mon-erspan-src-dst)# ip dscp 10`	（任意）回線エミュレーション（CEM）チャネルからのパケットに対して IP DiffServ コード ポイント（DSCP）の使用をイネーブルにします。 • オプションで **ip prec** コマンドまたは **ip dscp** コマンドのいずれかを使用できますが、両方は使用できません。
ステップ 15	**ip ttl** *ttl-value* 例： `Device(config-mon-erspan-src-dst)# ip ttl 32`	（任意）ERSPAN トラフィック内のパケットの IP TTL 値を設定します。

	コマンドまたはアクション	目的
ステップ 16	**mtu** *mtu-size* 例： `Device(config-mon-erspan-src-dst)# mtu 1500`	最大伝送単位（MTU）のサイズを、ERSPAN カプセル化用にバイト単位で設定します。 • 有効な値は、64 ～ 9180 です。 デフォルト値は 1500 です
ステップ 17	**origin ip address** *ip-address* [**force**] 例： `Device(config-mon-erspan-src-dst)# origin ip address 10.10.0.1`	ERSPAN トラフィックの送信元として使用される IP アドレスを設定します。
ステップ 18	**vrf** *vrf-id* 例： `Device(config-mon-erspan-src-dst)# vrf 1`	（任意）グローバル ルーティング テーブルの代わりに使用する VRF 名を設定します。
ステップ 19	**no shutdown** 例： `Device(config-mon-erspan-src-dst)# no shutdown`	インターフェイスで設定されたセッションをイネーブルにします。
ステップ 20	**end** 例： `Device(config-mon-erspan-src-dst)# end`	ERSPAN 送信元セッション宛先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。

ERSPAN 宛先セッションの設定

Encapsulated Remote Switched Port Analyzer（ERSPAN）宛先セッションを設定するには、この作業を実行します。 ERSPAN 宛先セッションは、セッション設定パラメータとモニタ対象トラフィックを受信するポートを定義します。

手順の概要

1. **enable**
2. **configure terminal**
3. **monitor session** *session-number* **type erspan-destination**
4. **description** *string*
5. **destination interface** {**gigabitethernet** | **port-channel**} [*interface-number*]
6. **source**
7. **erspan-id** *erspan-flow-id*
8. **ip address** *ip-address* [**force**]
9. **vrf** *vrf-id*
10. **no shutdown**
11. **end**

手順の詳細

	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 モードをイネーブルにします。 • 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	**monitor session** *session-number* **type erspan-destination** 例： `Device(config)# monitor session 1 type erspan-destination`	セッション ID とセッション タイプを使用して ERSPAN 宛先セッションを定義し、ERSPAN のモニタ宛先セッション コンフィギュレーション モードを開始します。 • *session-number* 引数の範囲は 1 ～ 1024 です。 セッション番号は一意である必要があり、複数回使用できません。 • 送信元セッションまたは宛先セッションのセッション ID は同じグローバルな ID スペース内にあるため、各セッション ID は両方のセッション タイプに対してグローバルに一意です。 • セッション ID（*session-number* 引数によって設定）およびセッション タイプ（**erspan-destination** によって設定）は、入力後は変更できません。 セッションを削除するには、このコマンドの **no** 形式を使用し、新しいセッション ID または新しいセッション タイプでセッションを再作成します。

	コマンドまたはアクション	目的
ステップ 4	**description** *string* 例： `Device(config-mon-erspan-dst)# description source1`	（任意）ERSPAN 宛先セッションの説明を入力します。 • *string* 引数には最大 240 文字まで入力できますが、特殊文字やスペースを含めることはできません。
ステップ 5	**destination interface** {**gigabitethernet** | **port-channel**} [*interface-number*] 例： `Device(config-mon-erspan-dst)# destination interface GigabitEthernet1/0/1`	ERSPAN宛先セッション番号を送信元ポートに関連付け、モニタするトラフィックの方向を選択します。
ステップ 6	**source** 例： `Device(config-mon-erspan-dst)# source`	ERSPAN宛先セッションの送信元コンフィギュレーション モードを開始します。
ステップ 7	**erspan-id** *erspan-flow-id* 例： `Device(config-mon-erspan-dst-src)# erspan-id 100`	ERSPANトラフィックを識別するため、送信元および宛先セッションで使用される ID を設定します。これは、ERSPAN 送信元セッションの設定でも入力する必要があります。
ステップ 8	**ip address** *ip-address* [**force**] 例： `Device(config-mon-erspan-dst-src)# ip address 10.10.0.1`	ERSPAN トラフィックの送信元として使用される IP アドレスを設定します。 • **ip address** *ip-address* **force** コマンドは、すべての ERSPAN 宛先セッションの送信元 IP アドレスを変更します。
ステップ 9	**vrf** *vrf-id* 例： `Device(config-mon-erspan-dst-src)# vrf 1`	（任意）グローバル ルーティング テーブルの代わりに使用する VRF 名を設定します。
ステップ 10	**no shutdown** 例： `Device(config-mon-erspan-dst-src)# no shutdown`	インターフェイスで設定されたセッションをイネーブルにします。
ステップ 11	**end** 例： `Device(config-mon-erspan-dst-src)# end`	ERSPAN宛先セッション送信元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。

ERSPAN の設定例

例：ERSPAN 送信元セッションの設定

次に、ERSPAN 送信元セッションを設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# monitor session 1 type erspan-source
Device(config-mon-erspan-src)# description source1
Device(config-mon-erspan-src)# source interface GigabitEthernet1/0/1 rx
Device(config-mon-erspan-src)# source interface GigabitEthernet1/0/4 - 8 tx
Device(config-mon-erspan-src)# source interface GigabitEthernet1/0/3
Device(config-mon-erspan-src)# destination
Device(config-mon-erspan-src-dst)# erspan-id 100
Device(config-mon-erspan-src-dst)# origin ip address 10.1.0.1
Device(config-mon-erspan-src-dst)# ip prec 5
Device(config-mon-erspan-src-dst)# ip ttl 32
Device(config-mon-erspan-src-dst)# mtu 1700
Device(config-mon-erspan-src-dst)# origin ip address 10.10.0.1
Device(config-mon-erspan-src-dst)# vrf 1
Device(config-mon-erspan-src-dst)# no shutdown
Device(config-mon-erspan-src-dst)# end
```

例：WAN インターフェイスの ERSPAN 送信元セッションの設定

次に、単一の ERSPAN 送信元モニタ セッションに複数の WAN インターフェイスを設定する例を示します。 複数のインターフェイスはカンマで区切られています。

```
monitor session 100 type erspan-source
    source interface Serial 0/1/0:0, Serial 0/1/0:6
```

例：ERSPAN 宛先セッションの設定

次に、ERSPAN 宛先セッションを設定する例を示します。

```
monitor session 2 type erspan-destination
 destination interface GigabitEthernet1/3/2
 destination interface GigabitEthernet2/2/0
 source
  erspan-id 100
  ip address 10.10.0.1
```

例：ローカル SPAN としての ERSPAN の設定

次の例に、ローカル SPAN として ERSPAN を設定する方法を示します。

```
monitor session 10 type erspan-source
 source interface GigabitEthernet0/0/0
 destination
 erspan-id 10
 ip address 10.10.10.1
 origin ip address 10.10.10.1
monitor session 20 type erspan-destination
destination interface GigabitEthernet0/0/1
 source
  erspan-id 10
  ip address 10.10.0.1
```

ERSPAN の設定に関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
LAN スイッチング コマンド：コマンド構文、コマンドモード、コマンド履歴、デフォルト、使用上のガイドライン、および例	『LAN Switching Command Reference』

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

ERSPAN の設定に関する機能情報

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。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

表 *1*：*ERSPAN* の設定に関する機能情報

機能名	リリース	機能情報
ERSPAN	Cisco IOS XE Release 2.1 Cisco IOS XE Release 3.8S	Cisco ERSPAN 機能を使用すると、1 つ以上のポートまたは VLAN のトラフィックを監視し、1 つ以上の宛先ポートに、監視されたトラフィックを送信できます。 次のコマンドがこの機能によって導入または変更されました。**description**、**destination**、**erspan-id**、**filter**、**ip dscp**、**ip prec**、**ip ttl**、**monitor permit-list**、**monitor session**、**origin ip address**、**show monitor permit-list**、**source**、**switchport**、**switchport mode trunk**、**switchport nonegotiate**、**switchport trunk encapsulation**、**vrf**。 Cisco IOS XE 3.8S リリースで、ERSPAN は最大で 9180 バイトの MTU データ サイズをサポートするように拡張されました。次のコマンドがこの機能によって追加されました。**mtu**

機能名	リリース	機能情報
WAN インターフェイスでの ERSPAN サポート	Cisco IOS XE Release 3.5S	ERSPAN は、ERSPAN 送信元として WAN インターフェイスをサポートするように拡張されました。 次のコマンドがこの機能によって変更されました。**source interface**。

第 2 章

IEEE 802.1Q カプセル化を使用する VLAN 間のルーティング設定

この章では、IEEE 802.1Q カプセル化を使用した VLAN 間のルーティングを設定する際に必要なタスクとオプションのタスクを説明します。

- 機能情報の確認，17 ページ
- IEEE 802.1Q カプセル化を使用する VLAN 間のルーティング設定の制約事項，18 ページ
- IEEE 802.1Q カプセル化を使用する VLAN 間のルーティング設定に関する情報，18 ページ
- IEEE 802.1Q カプセル化を使用する VLAN 間のルーティング設定方法，18 ページ
- IEEE 802.1Q カプセル化を使用する VLAN 間のルーティング設定の設定例，23 ページ
- その他の関連資料，23 ページ
- IEEE 802.1Q カプセル化を使用する VLAN 間のルーティング設定の機能情報，25 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の警告および機能情報については、『Bug Search Tool』およびご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

IEEE 802.1Q カプセル化を使用する VLAN 間のルーティング設定の制約事項

Cisco ASR 1000 シリーズ アグリゲーション サービス ルータの共有ポート アダプタ（SPA）には 8,000 の TCAM エントリの制限があり、単一の SPA で作成できる VLAN の数を制限します。

IEEE 802.1Q カプセル化を使用する VLAN 間のルーティング設定に関する情報

IEEE 802.1Q カプセル化を使用する VLAN 間のルーティング設定

IEEE 802.1Qプロトコルは、複数のスイッチおよびルータの相互接続や、VLAN トポロジの定義に使用されます。 IEEE 802.1Q 規格では、タグなしフレームに関しては非常に多くの制約があります。 この規格では、タグなしフレームについてはポート別VLANのソリューションしか提供されてません。 たとえば、タグなしフレームをVLANに割り当てる場合は、そのフレームの送信元となったポートしか考慮されません。 各ポートには、タグなしフレームの受信に割り当てる VLAN を指定する *permanent virtual identification*（ネイティブ VLAN）というパラメータがあります。

IEEE 802.1Q の主な特徴は次のとおりです。

- フィルタリングによって VLAN にフレームを割り当てます。
- この規格では、単一のスパニングツリーと、1 レベルのタグ付けによる明示的なタグ付け方式が存在することを前提としています。

IEEE 802.1Q カプセル化を使用する VLAN 間のルーティング設定方法

IEEE 802.1Q での IP ルーティングの設定

IEEE 802.1Q での IP ルーティングは、IEEE 802.1Q のカプセル化を使用する VLAN 構成における IP フレーム タイプのルーティングをサポートするよう、IP ルーティング機能を拡張します。

VLAN 間で IEEE 802.1Q による IP ルーティングを行うには、サブインターフェイスをカスタマイズして、それを使用する環境を作成する必要があります。 次のセクションで説明するタスクを、記載されている順序どおりに実行してください。

IP ルーティングのイネーブル化

IP ルーティングはルータの Cisco IOS XE ソフトウェアで自動的にイネーブルになります。 IP ルーティングがディセーブル化されている場合に再度イネーブルにするには、次の手順を実行します。

ルータで IP ルーティングをイネーブルにしたら、環境に合わせて特性をカスタマイズできます。必要に応じて、『*Cisco IOS XE IP Routing Protocols Configuration Guide*』のリリース 2 の IP 設定に関する章で、ガイドラインと IP 設定について参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip routing**
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • 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： `Router# 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 routing** 例： `Router(config)# ip routing`	ルータで IP ルーティングをイネーブルにします。
ステップ 4	**end** 例： `Router(config)# exit`	特権 EXEC モードを終了します。

VLAN カプセル化方式の定義

カプセル化形式を IEEE 802.1Q として定義するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface gigabitethernet** *card* / *spaslot* / *port* . *subinterface-number*
4. **encapsulation dot1q** *vlanid*
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • 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： `Router# 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** *card* / *spaslot* / *port* . *subinterface-number* 例： `Router(config)# interface gigabitethernet 0/0/0.101`	IEEE 802.1Q を使用するサブ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	**encapsulation dot1q** *vlanid* 例： `Router(config-subif)# encapsulation dot1q 101`	カプセル化形式を IEEE 802.1Q（**dot1q**）と定義し、VLAN 識別子を指定します。
ステップ 5	**end** 例： `Router(config-subif)# end`	サブインターフェイス コンフィギュレーション モードを終了します。

ネットワーク インターフェイスへの IP アドレスの割り当て

インターフェイスには、1 つのプライマリ IP アドレスを設定できます。 ネットワーク インターフェイスにプライマリ IP アドレスおよびネットワーク マスクを割り当てるには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface gigabitethernet** *card* / *spaslot* / *port* . *subinterface-number*
4. **ip address** *ip-address mask*
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • 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： `Router# 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** *card* / *spaslot* / *port* . *subinterface-number* 例： `Router(config)# interface gigabitethernet 0/0/0.101`	IEEE 802.1Q を使用するサブ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	**ip address** *ip-address mask* 例： `Router(config-subif)# ip address 10.0.0.0 255.0.0.0`	インターフェイスのプライマリ IP アドレスを設定します。 • インターフェイスのプライマリ IP アドレスを入力します。 （注） マスクで、IP アドレス中のネットワーク番号を示すビットが識別できます。マスクを使用してネットワークをサブネット化した場合、そのマスクはサブネット マスクと呼ばれます。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： `Router(config-subif)# end`	サブインターフェイス コンフィギュレーション モードを終了します。

VLAN サブインターフェイスのモニタリングおよびメンテナンス

VLAN がネイティブ VLAN かどうかを示すには、次の手順を実行します。

手順の概要

1. **enable**
2. **show vlans**
3. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**show vlans** 例： `Router# show vlans`	VLAN 情報を表示します。
ステップ 3	**end** 例： `Router# end`	特権 EXEC モードを終了します。

IEEE 802.1Q カプセル化を使用する VLAN 間のルーティング設定の設定例

IEEE 802.1Q での IP ルーティングの設定例

この設定例では、VLAN 101 で IP をルーティングします。

```
!
ip routing
!
interface gigabitethernet 4/1/1.101
  encapsulation dot1q 101
  ip addr 10.0.0.0 255.0.0.0
!
```

その他の関連資料

関連資料

関連項目	マニュアル タイトル
IP LAN スイッチング コマンド：コマンド構文の詳細、コマンドモード、デフォルト、使用上の注意事項、および例	『Cisco IOS LAN Switching Services Command Reference』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能がサポートする新しい RFC または変更された RFC はありません。また、この機能は既存の規格に対するサポートに影響を及ぼしません。	--

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IEEE 802.1Q カプセル化を使用する VLAN 間のルーティング設定の機能情報

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。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

表 *2*：*IEEE 802.1Q* カプセル化を使用する *VLAN* 間のルーティング設定の機能情報

機能名	リリース	機能情報
IEEE 802.1Q カプセル化を使用する VLAN 間のルーティング設定	Cisco IOS XE Release 2.1	この機能は、Cisco ASR 1000 シリーズのアグリゲーション サービス ルータで導入されました。

第 3 章

IEEE 802.1Q-in-Q VLAN タグ終端

IEEE 802.1Q VLAN タグを 802.1Q 内にカプセル化すると、サービス プロバイダーは、1 つの VLAN を使用して、複数の VLAN を持つお客様をサポートできます。 サブインターフェイス レベルでの IEEE 802.1Q-in-Q VLAN タグ終端機能は VLAN ID をそのまま維持し、他のカスタマーの VLAN のトラフィックと区別します。

- 機能情報の確認，27 ページ
- IEEE 802.1Q-in-Q VLAN タグ終端に関する情報，28 ページ
- IEEE 802.1Q-in-Q VLAN タグ終端の設定方法，30 ページ
- IEEE 802.1Q-in-Q VLAN タグ終端の設定例，34 ページ
- その他の関連資料，36 ページ
- IEEE 802.1Q-in-Q VLAN タグ終端に関する機能情報，37 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の警告および機能情報については、『Bug Search Tool』およびご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

IEEE 802.1Q-in-Q VLAN タグ終端に関する情報

サブインターフェイスでの IEEE 802.1Q-in-Q VLAN タグ終端機能

IEEE 802.1Q-in-Q VLAN タグ終端機能は、単純にもう 1 つのレイヤの IEEE 802.1Q タグ（「メトロ タグ」または「PE-VLAN」と呼びます）を、ネットワークに渡される 802.1Q タグ付きパケットに追加します。 タグ付きパケットにタグ付けすることで「二重タグ付き」フレームを形成し、VLAN スペースを拡張することを目的としています。 拡張された VLAN スペースにより、サービス プロバイダーは特定の顧客向けの特定の VLAN によるインターネット アクセスといったサービスを提供できると同時に、他の VLAN を利用する他の顧客向けのその他のサービスも提供できます。

通常、サービス プロバイダーの顧客は、複数のアプリケーションを処理するために一定範囲の VLAN を必要とします。 サービス プロバイダーでは、顧客がこの機能を利用してサブインターフェイスに独自の VLAN ID を安全に割り当てることを許可できます。こうしたサブインターフェイスの VLAN ID は、サービス プロバイダーがその顧客に指定した VLAN ID 内でカプセル化されるからです。 そのため、お客様間で VLAN ID が重複することはなく、別のお客様のトラフィックが混合することもありません。 二重タグ付きフレームは、拡張 **encapsulation dot1q** コマンドにより、サブインターフェイスで「終端」する、つまり割り当てられます。このコマンドは、サブインターフェイスで終端される 2 つの VLAN ID タグ（外部 VLAN ID と内部 VLAN ID）を指定します（次の図を参照）。

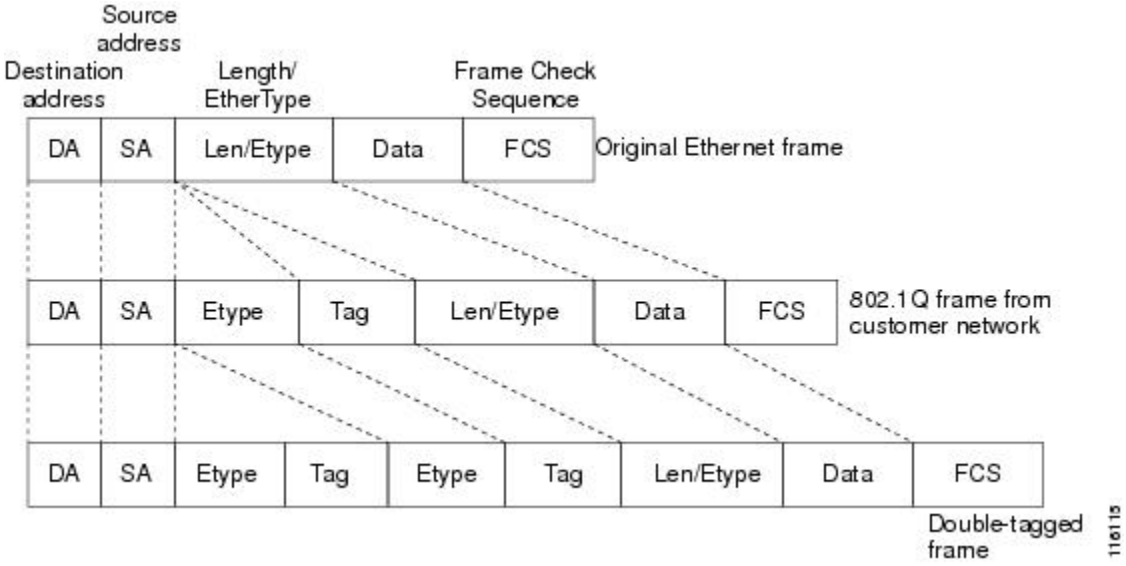
IEEE 802.1Q-in-Q VLAN タグ終端は、サブインターフェイスでサポートされる Cisco IOS XE 機能またはプロトコルにかかわらず、通常サポートされます。 制限事項は、内部 VLAN ID に一義的なサブインターフェイスと一義的でないサブインターフェイスのどちらを割り当てるかということだけです。 「一義的なサブインターフェイスとあいまいなサブインターフェイス」のセクションを参照してください。

サービス プロバイダーにとっての主要な利点は、同じ数の顧客に対してサポートする VLAN の数が減ることです。 この機能のその他の利点には次のようなものがあります。

- PPPoE のスケーラビリティ。 使用可能な VLAN スペースが 4096 からおよそ 1680 万（4096 × 4096）に拡大することで、特定のインターフェイス上で終端できる PPPoE セッションの数が倍増します。
- ホールセール モデルにギガバイト イーサネットの DSL アクセス マルチプレクサ（DSLAM）を導入する場合は、エンド カスタマーの仮想回線（VC）を表す内部 VLAN ID を割り当て、さらにサービス プロバイダーの ID を表す外部 VLAN ID を割り当てることができます。

スイッチでは、インターフェイスの IEEE 802.1Q トンネルを使用して二重タグ付きトラフィックを伝送する必要がありますが、ルータでは、Q-in-Q VLAN タグをもう 1 つのレベルの 802.1Q タグ内にカプセル化するだけで、正しい送信先にパケットを到達させることができます。

図 *2*：タグなし、*802.1Q* タグ付き、および二重タグ付きイーサネット フレーム



一義的なサブインターフェイスとあいまいなサブインターフェイス

サブインターフェイスでの Q-in-Q 終端を設定するには、**encapsulation dot1q** コマンドを使用します。 このコマンドは、1 つの外部 VLAN ID と、1 つまたは複数の内部 VLAN ID を受け入れます。外部 VLAN ID は常にある特定の値になりますが、内部 VLAN ID は特定の値または値の範囲にすることができます。

単一の内部 VLAN ID が設定されているサブインターフェイスは、一義的な Q-in-Q サブインターフェイスと呼ばれます。 次の例では、外部 VLAN ID が 101 で内部 VLAN ID が 1001 の Q-in-Q トラフィックが、ギガビットイーサネット 1/1/0.100 サブインターフェイスにマッピングされます。

```
Device(config)# interface gigabitEehernet1/1/0.100
Device(config-subif)# encapsulation dot1q 101 second-dot1q 1001
```

複数の内部 VLAN IDs が設定されているサブインターフェイスは、一義的でない Q-in-Q サブインターフェイスと呼ばれます。 一義的でない Q-in-Q サブインターフェイスでは、複数の内部 VLAN ID をグループ化できるため、設定をコンパクト化してメモリ使用率とスケーラビリティを向上させることができます。

次の例では、外部 VLAN ID が 101 で内部 VLAN ID が 2001～2100 または 3001～3100 の範囲内の Q-in-Q トラフィックが、ギガビットイーサネットの 1/1/0.101 サブインターフェイスにマッピングされます。

```
Device(config)# interface gigabitethernet1/1/0.101
Device(config-subif)# encapsulation dot1q 101 second-dot1q 2001-2100,3001-3100
```

あいまいなサブインターフェイスでは、**any** キーワードを使用して内部 VLAN ID を指定することもできます。

VLAN ID をサブインターフェイスに割り当てる方法と、あいまいなサブインターフェイスでの **any** キーワードの詳細な使用例については、「IEEE 802.1Q-in-Q VLAN タグ終端の設定例」を参照してください。

あいまいなサブインターフェイスでは PPPoE だけがサポートされます。 標準の IP ルーティングは、あいまいなサブインターフェイスではサポートされません。

IEEE 802.1Q-in-Q VLAN タグ終端の設定方法

IEEE 802.1Q-in-Q VLAN タグ終端のインターフェイスの設定

Q-in-Q 二重タギングに使用するメインインターフェイスを設定し、サブインターフェイスを設定するには、この作業を実行します。 この作業の任意の手順では、必要に応じて外部 VLAN タグの EtherType フィールドを 0x9100 に設定する方法を示しています。 サブインターフェイスを定義した後、二重タギングを使用するように 802.1Q カプセル化を設定します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **dot1q tunneling ethertype** *ethertype*
5. **interface** *type number* **.** *subinterface-number*
6. **encapsulation dot1q** *vlan-id* **second-dot1q** {**any** | *vlan-id* | *vlan-id* **-** *vlan-id* [*vlan-id* **-** *vlan-id*]}
7. **pppoe enable** [**group** *group-name*] [**max-sessions** *max-sessions-number*]
8. **exit**
9. ステップ 5 を繰り返して、別のサブインターフェイスを設定します。
10. サブインターフェイスで終端する VLAN タグを指定する場合、ステップ 6 および 7 を繰り返して行います。
11. **end**

手順の詳細

	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 モードをイネーブルにします。 • 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** *type number* 例： `Device(config)# interface gigabitethernet 1/0/0`	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	**dot1q tunneling ethertype** *ethertype* 例： `Device(config-if)# dot1q tunneling ethertype 0x9100`	（任意）Q-in-Q VLAN タギングを実装するときにピア装置で使用される Ethertype フィールドのタイプを定義します。
ステップ 5	**interface** *type number* **.** *subinterface-number* 例： `Device(config-if)# interface gigabitethernet 1/0/0.1`	サブインターフェイスを設定し、サブインターフェイス コンフィギュレーション モードを開始します。
ステップ 6	**encapsulation dot1q** *vlan-id* **second-dot1q** {**any** | *vlan-id* | *vlan-id* **-** *vlan-id* [*vlan-id* **-** *vlan-id*]} 例： `Device(config-subif)# encapsulation dot1q 100 second-dot1q 200`	（必須）VLAN の指定されたサブインターフェイス上で、トラフィックの 802.1Q カプセル化をイネーブルにします。 • **second-dot1q** キーワードと *vlan-id* 引数を使用して、サブインターフェイスで終端する VLAN タグを指定します。 • この例では、内部 VLAN ID を 1 つだけ指定するため、一義的な Q-in-Q サブインターフェイスが設定されます。 • 外部 VLAN ID が 100 で内部 VLAN ID が 200 の Q-in-Q フレームが終端されます。
ステップ 7	**pppoe enable** [**group** *group-name*] [**max-sessions** *max-sessions-number*] 例： `Device(config-subif)# pppoe enable group vpn1`	サブインターフェイスで PPPoE セッションをイネーブルにします。 この例では、サブインターフェイスの PPPoE セッションで PPPoE プロファイル vpn1 を使用す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 8	**exit** 例： `Device(config-subif)# exit`	サブインターフェイス コンフィギュレーション モードを終了し、インターフェイス コンフィギュレーション モードに戻ります。 • この手順をもう一度くり返して、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 9	ステップ 5 を繰り返して、別のサブインターフェイスを設定します。 例： `Device(config-if)# interface gigabitethernet 1/0/0.2`	（任意）サブインターフェイスを設定し、サブインターフェイス コンフィギュレーション モードを開始します。

ステップ 10	サブインターフェイスで終端するVLANタグを指定する場合、ステップ 6 および 7 を繰り返して行います。
	
	例：
	`Device(config-subif)# encapsulation dot1q 100 second-dot1q 100-199,201-600`
	
	例：
	`Device(config-subif)# pppoe enable group vpn1`
		ステップ6を実行して、VLANの指定されたサブインターフェイスでトラフィックのIEEE 802.1Qカプセル化をイネーブルにします。
		• **second-dot1q** キーワードと *vlan-id* 引数を使用して、サブインターフェイスで終端する VLAN タグを指定します。
		• この例では、一定範囲の内部VLAN ID を指定するため、一義的でない Q-in-Q サブインターフェイスが設定されます。
		• 外部 VLAN ID が 100 で、内部 VLAN ID が 100 ～ 199 または 201 ～ 600 の範囲内にある Q-in-Q フレームが終端されます。
		
		ステップ 7 は、サブインターフェイスで PPPoE セッションをイネーブルにします。 この例では、サブインターフェイスの PPPoE セッションで PPPoE プロファイル vpn1 を使用するように指定します。

ステップ 11	**end** 例： `Device(config-subif)# end`	サブインターフェイス コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

IEEE 802.1 Q-in-Q VLAN タグ終端機能の確認

IEEE 802.1Q-in-Q VLAN タグ終端機能の設定を確認するには、任意で次の作業を実行します。

手順の概要

1. **enable**
2. **show running-config**
3. **show vlans dot1q** [**internal** *interface-type interface-number* **.***subinterface-number*[**detail**] | **second-dot1q** *inner-id* **any**]] [**detail]**

手順の詳細

ステップ 1 **enable**
特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。

例：

```
Device> enable
```

ステップ 2 **show running-config**
このコマンドを使用して、デバイスで現在の実行コンフィギュレーションを表示します。 区切り文字を使用してコンフィギュレーションの関連する部分だけを表示できます。

例：

```
Device# show running-config
```

ステップ 3 **show vlans dot1q** [**internal** *interface-type interface-number* **.***subinterface-number*[**detail**] | **second-dot1q** *inner-id* **any**]] [**detail]**
このコマンドを使用して、すべての 802.1Q VLAN ID の統計情報を表示します。 この例では、外部 VLAN ID だけが表示されます。

例：

```
Router# show vlans dot1q
Total statistics for 802.1Q VLAN 1:
   441 packets, 85825 bytes input
   1028 packets, 69082 bytes output
Total statistics for 802.1Q VLAN 101:
   5173 packets, 510384 bytes input
   3042 packets, 369567 bytes output
Total statistics for 802.1Q VLAN 201:
   1012 packets, 119254 bytes input
   1018 packets, 120393 bytes output
Total statistics for 802.1Q VLAN 301:
   3163 packets, 265272 bytes input
   1011 packets, 120750 bytes output
Total statistics for 802.1Q VLAN 401:
   1012 packets, 119254 bytes input
   1010 packets, 119108 bytes output
```

IEEE 802.1Q-in-Q VLAN タグ終端の設定例

IEEE802.1Q-in-QVLANタグ終端のサブインターフェイスでの任意のキーワードの設定例

一部のあいまいなサブインターフェイスでは、内部 VLAN ID の指定に **any** キーワードを使用できます。 **any** は、他のインターフェイスで明示的に設定されていない任意の内部 VLAN ID を表します。 次の例では、外部 VLAN ID と内部 VLAN ID の組み合わせがそれぞれ異なるサブインターフェイスを 7 つ設定します。

（注） **any** キーワードは、物理インターフェイスと外部 VLAN ID が指定された 1 つのサブインターフェイスに対してのみ設定できます。

```
interface GigabitEthernet1/0/0.1
 encapsulation dot1q 100 second-dot1q 100
interface GigabitEthernet1/0/0.2
 encapsulation dot1q 100 second-dot1q 200
interface GigabitEthernet1/0/0.3
 encapsulation dot1q 100 second-dot1q 300-400,500-600
interface GigabitEthernet1/0/0.4
 encapsulation dot1q 100 second-dot1q any
interface GigabitEthernet1/0/0.5
 encapsulation dot1q 200 second-dot1q 50
interface GigabitEthernet1/0/0.6
 encapsulation dot1q 200 second-dot1q 1000-2000,3000-4000
interface GigabitEthernet1/0/0.7
 encapsulation dot1q 200 second-dot1q any
```

次の表は、ギガビット イーサネット インターフェイス 1/0/0 で受信される Q-in-Q フレームの外部および内部 VLAN ID のさまざまな値に、どのサブインターフェイスがマッピングされるかを示しています。

表 *3*：*GE* インターフェイス *1/0/0* の外部 *VLAN ID* および内部 *VLAN ID* にマッピングされるサブインターフェイス

外部 VLAN ID	内部 VLAN ID	マッピングされるサブインターフェイス
100	1 ～ 99	GigabitEthernet1/0/0.4
100	100	GigabitEthernet1/0/0.1
100	101 ～ 199	GigabitEthernet1/0/0.4
100	200	GigabitEthernet1/0/0.2
100	201 ～ 299	GigabitEthernet1/0/0.4

外部 VLAN ID	内部 VLAN ID	マッピングされるサブインターフェイス
100	300 ～ 400	GigabitEthernet1/0/0.3
100	401 ～ 499	GigabitEthernet1/0/0.4
100	500 ～ 600	GigabitEthernet1/0/0.3
100	601 ～ 4095	GigabitEthernet1/0/0.4
200	1 ～ 49	GigabitEthernet1/0/0.7
200	50	GigabitEthernet1/0/0.5
200	51 ～ 999	GigabitEthernet1/0/0.7
200	1000 ～ 2000	GigabitEthernet1/0/0.6
200	2001 ～ 2999	GigabitEthernet1/0/0.7
200	3000 ～ 4000	GigabitEthernet1/0/0.6
200	4001 ～ 4095	GigabitEthernet1/0/0.7

ここで、次の新しいサブインターフェイスを設定します。

```
interface GigabitEthernet1/0/0.8
 encapsulation dot1q 200 second-dot1q 200-600,900-999
```

次の表は、200 の外部 VLAN ID の表に加えられた変更を示します。 **any** キーワードを使用して設定されたサブインターフェイス 1/0/0.7 の内部 VLAN ID のマッピングが変わっていることに注意してください。

表 *4*：*GE* インターフェイス *1/0/0* の外部 *VLAN ID* および内部 *VLAN ID* にマッピングされるサブインターフェイス：*GE* サブインターフェイス *1/0/0.8* を設定したことによる変更点

外部 VLAN ID	内部 VLAN ID	マッピングされるサブインターフェイス
200	1 ～ 49	GigabitEthernet1/0/0.7
200	50	GigabitEthernet1/0/0.5
200	51 ～ 199	GigabitEthernet1/0/0.7
200	200 ～ 600	GigabitEthernet1/0/0.8

外部 VLAN ID	内部 VLAN ID	マッピングされるサブインターフェイス
200	601 ～ 899	GigabitEthernet1/0/0.7
200	900 ～ 999	GigabitEthernet1/0/0.8
200	1000 ～ 2000	GigabitEthernet1/0/0.6
200	2001 ～ 2999	GigabitEthernet1/0/0.7
200	3000 ～ 4000	GigabitEthernet1/0/0.6
200	4001 ～ 4095	GigabitEthernet1/0/0.7

その他の関連資料

ここでは、IEEE 802.1Q-in-Q VLAN タグ終端機能に関連する参考資料を示します。

関連資料

関連項目	マニュアル タイトル
関連コマンド	『*Cisco IOS LAN Switching Command Reference*』

標準

標準	タイトル
IEEE 802.1Q	--

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

IEEE 802.1Q-in-Q VLAN タグ終端に関する機能情報

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。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *5*：*IEEE 802.1Q-in-Q VLAN* タグ終端に関する機能情報

機能名	リリース	機能情報
IEEE 802.1Q-in-Q VLAN タグ終端	Cisco IOS XE Release 2.1	この機能は、Cisco ASR 1000 シリーズのアグリゲーション サービス ルータで導入されました。 この機能のために、次のコマンドが変更されました。**dot1q tunneling ethertype**、**encapsulation dot1q**、および **show vlans dot1q**

第 4 章

ギガビット EtherChannel メンバー リンクへの VLAN マッピング

ギガビット EtherChannel（GEC）メンバー リンクへの VLAN マッピング機能を使用すると、GEC バンドル内の特定のメンバー リンクに VLAN ID で識別されるユーザ トラフィックのスタティックな割り当てを設定することができます。 プライマリおよびセカンダリ リンクに手動で仮想 LAN（VLAN）サブインターフェイスを割り当てることができます。 この機能は、ベンダー機器の能力に関係なく、ダウンストリーム機器へのロード バランシングを可能にし、プライマリ リンクに障害が発生すると、トラフィックをセカンダリ メンバー リンクにリダイレクトすることでフェールオーバー保護を提供します。 シャーシあたり最大 16 バンドルでメンバー リンクがサポートされます。

- 機能情報の確認，39 ページ
- GEC メンバー リンクへの VLAN マッピングの前提条件，40 ページ
- GEC メンバー リンクへの VLAN マッピングの制約事項，40 ページ
- GEC メンバー リンクの VLAN マッピングに関する情報，40 ページ
- GEC リンクへの VLAN マッピングの設定方法，46 ページ
- GEC メンバー リンクへの VLAN マッピングの設定例，48 ページ
- その他の関連資料，51 ページ
- GEC メンバー リンクへの VLAN マッピングの機能情報，51 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の警告および機能情報については、『Bug Search Tool』およびご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

GEC メンバー リンクへの VLAN マッピングの前提条件

- 各 VLAN で IEEE 802.1Q カプセル化を設定する必要があります。
- 各 VLAN に、プライマリ リンク 1 つとセカンダリ リンク 1 つを関連付ける必要があります。

GEC メンバー リンクへの VLAN マッピングの制約事項

次の制限は、ギガビット EtherChannel（GEC）リンクの IPv6 ロード バランシングに適用されます。

- IPv6 トラフィック分散はフローのロード バランシングのポート チャネル上でのみイネーブルになります。
- マルチプロトコル ラベル スイッチング（MPLS）トラフィック エンジニアリング（TE）は、ポート チャネルでサポートされていません。
- ポートチャネルの QinQ サブインターフェイスはサポートされません。
- Quality of Service（QoS）ポリシーは、次の条件が満たされた場合にポートチャネル サブインターフェイスに適用できます。
  - 手動仮想 LAN（VLAN）ロード バランシングがサポートされます。
  - ポリシー マップには、物理メンバー リンクで設定された適切なサービス フラグメントのポリシーがあります。

GEC メンバー リンクの VLAN マッピングに関する情報

手動 VLAN ロード バランシング

ロード バランシングが GEC リンクに設定されている場合、トラフィック フローはロード バランシング アルゴリズムによって示されるのとは異なるバケットにマッピングされます。各 EtherChannel に、16 のバケットのセットが作成されます。 EtherChannel モジュールで、バケットがメンバー リンク間でどのように配分されるかが決定されます。各バケットにアクティブ リンクが関連付けられ、同じバケットにマップされたすべてのフローに使用されるインターフェイスを表します。

同じ VLAN サブインターフェイスを介して転送されるすべてのパケットは、1 つのバケットにマッピングされているのと同じフローの一部であると見なされます。 各バケットにプライマリとセカ

ンダリのペアが関連付けられ、バケットはペア内のアクティブ インターフェイスをポイントします。 アクティブなペアは、一度に 1 つだけです。 複数の VLAN のフローは、（プライマリおよびセカンダリの）マッピングが同じ場合は同じバケットにマッピングできます。

手動 VLAN ロード バランシングがイネーブルになっている場合に、バケットが作成されます。 VLAN ロード バランシングが削除されると、バケットは削除されます。 すべてのポート チャネルで、手動 VLAN ロード バランシングか動的フローベースのロード バランシングが使用されます。フローベースのロードバランシングの詳細については、「フローベースのポートチャネルごとのロード バランシング」モジュールを参照してください。

特定の VLAN に、プライマリ リンク 1 つとセカンダリ リンク 1 つを関連付ける必要があります。手動 VLAN ロードバランシングがイネーブルになっている場合にだけ、プライマリとセカンダリのオプションを使用できます。次の条件を満たす場合、ロードバランシング情報がフォワーディング プレーンにダウンロードされます。 これらの条件が満たされない場合、ロード バランシング情報はフォワーディング プレーンから削除されます。

- VLAN ロード バランシングはグローバルにイネーブルにする必要があります。
- IEEE 802.1Q カプセル化を各 VLAN で設定する必要があります。
- EtherChannel リンクに VLAN トラフィックを手動でマッピングするために、1 つのプライマリと 1 つのセカンダリ メンバー リンクをイネーブルにする必要があります。
- プライマリおよびセカンダリ リンクは、これらのリンクを使用するために、トラフィックのポート チャネルの一部である必要があります。

プライマリ リンクだけが指定されている場合、セカンダリ リンクがデフォルトとして選択されます。 プライマリ リンクとセカンダリ リンクが明示的に設定されていない場合、プライマリ リンクとセカンダリ リンクはデフォルトで選択されます。 デフォルト リンクが選択されている場合は、リンク間で同等に VLAN 配布は行われません。

プライマリ リンクまたはセカンダリ リンクとして指定されたインターフェイスがポート チャネルの一部として設定されていない場合、またはグローバル VLAN ロードバランシングがイネーブルでない場合、警告メッセージが表示されます。

警告

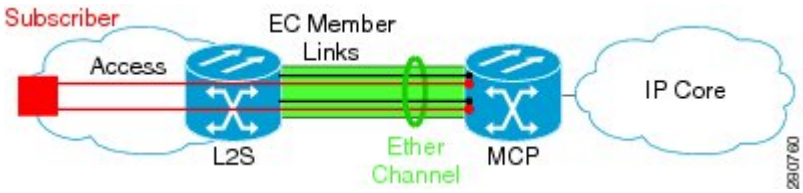
VLAN 500's main interface is not the channel group of primary：プライマリ インターフェイスでチャンネルグループが設定されるまで、GigabitEthernet 4/0/1 の VLAN ごとの手動ロードバランシングは有効になりません。

VLAN 500's main interface is not the channel group of secondary：プライマリ インターフェイスでチャンネルグループが設定されるまで、GigabitEthernet 1/0/0 の VLAN ごとの手動ロードバランシングは有効になりません。

VLAN からポート チャネル メンバーへのリンク マッピング

次の図は、VLAN からポート チャネルへのマッピングのトラフィック フローを示します。

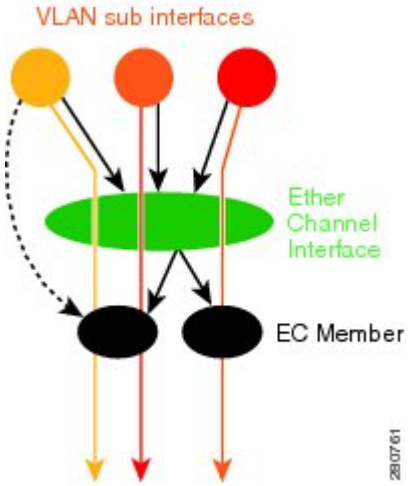
図 *3*：*VLAN* からポート チャネル メンバーへのリンク マッピング



黒い線は、レイヤ 2（L2）スイッチと MCP のルータを接続する物理 1 ギガビット イーサネット インターフェイスを表します。 これらのインターフェイスは、緑色で示されているポートチャネルと一緒にまとめられます。

次の図では、影付きのオレンジと赤で示される、加入者の VLAN サブインターフェイスは、EtherChannel インターフェイス上のレイヤ 3（L3）インターフェイスとして設定されます。 メンバー リンクへの VLAN のマッピング（黒い点線の矢印）が設定によって行われ、データプレーンにダウンロードされて、出力 VLA トラフィック（オレンジと赤の矢印）が関連するアクティブなプライマリまたはセカンダリ メンバー リンクを介して送信されます。 このモデルの QoS 設定は、VLAN サブインターフェイスとメンバー リンク インターフェイス レベルで適用され、QoS キューが両方のレベルで作成されたことを意味します。

図 *4*：*VLAN* からメンバー リンクへのマッピング



VLAN のプライマリ リンクおよびセカンダリ リンクの関連付け

ポートチャネルのトラフィック分散では、メンバー リンクのステートは、設定されたプライマリ ステートまたはセカンダリ ステート、および動作がアクティブなステートまたはスタンバイなス

テートになります。インターフェイスがアップになると、プライマリ リンクはアクティブになります。プライマリ リンクがダウンになった場合、インターフェイスは、プライマリでスタンバイステートになり、セカンダリ インターフェイスはセカンダリでアクティブ ステートになります。プライマリ リンクがアップになると、インターフェイスの動作がアップの場合でも、セカンダリ リンクはセカンダリ スタンバイになります。

プライマリおよびセカンダリ メンバー リンクはそれぞれ、ポートチャネル メイン インターフェイスに設定されたルーテッド VLAN と関連付けられます。 この VLAN へのトラフィックを転送する場合、プライマリ インターフェイスがアップの場合は、このインターフェイスが発信インターフェイスとして使用され、セカンダリ インターフェイスが動作可能である場合、このインターフェイスはプライマリ インターフェイスがダウンになった場合に使用されます。

VLAN ごとのトラフィック分散のすべての条件が満たされていない場合、マッピングはフォワーディングプレーンにダウンロードされません。 すべての条件が満たされると、データプレーンはこのマッピングで更新されます。

次の表は、プライマリおよびセカンダリ リンクの設定ステータスとその設定の結果の機能について説明します。

表 *6*：*VLAN* のプライマリおよびセカンダリ リンクのマッピング ステータス

プライマリ ステータス	セカンダリ ステータス	説明
設定済み	設定済み	プライマリ リンクおよびセカンダリ リンクの両方が **encapsulation dot1q** コマンドで指定されます。 `encapsulation dot1Q vlan-id primary`
デフォルト設定	デフォルト設定	プライマリ リンクとセカンダリ リンクのいずれも指定されません。 `encapsulation dot1Q vlan-id` 安定したシステムでは、すべてのVLANと同様に、プライマリ リンクおよびセカンダリ リンクの両方にデフォルトが選択されます。 ECに追加される最初のアップしたリンクはプライマリとして選択され、2番目のアップしたリンクはセカンダリとして選択されます。 アップしたリンクがない場合は、プライマリ リンクおよびセカンダリ リンクがダウンしたリンクから選択されます。
設定済み	デフォルト設定	プライマリ リンクだけが指定されます。 `encapsulation dot1Q vlan-id primary` プライマリ リンクと異なるセカンダリ リンクが内部的に選択されます。

プライマリ ステータス	セカンダリ ステータス	説明
設定済み	–	プライマリ リンクだけが指定され、1 つのリンクだけが定義されます。 `encapsulation dot1Q vlan-id primary` EC で 1 つのリンクしか定義されていない場合は、セカンダリ リンクはデフォルトとして選択されません。
デフォルト設定	–	プライマリ リンクとセカンダリ リンクのいずれも指定されておらず、1 つのリンクだけが定義されています。 `encapsulation dot1Q vlan-id` プライマリ リンクのデフォルトが選択されます。ただし、1 つのリンクだけが EC で定義されている場合は、セカンダリ リンクとしてデフォルト リンクは選択されません。
–	–	プライマリ リンクとセカンダリ リンクのいずれも指定されず、リンクは定義されません。 `encapsulation dot1Q vlan-id` デフォルトは選択されず、リンクは EC で定義されません。

（注） デフォルトマッピングは、ユーザ設定のマッピングが誤って定義されても、ユーザ設定のマッピングを上書きしません。 関連付け（VLAN、プライマリ、セカンダリ）が実行されると（CLI、デフォルト、またはその両方の組み合わせで）、システムでマッピングが検証され、データプレーンにダウンロードされます。 設定された VLAN がない場合、ポート チャネルを介して転送されるすべてのトラフィックはドロップされます。

チャネル メンバー リンクの追加

新しいメンバー リンクが追加されると、新しいバケットが作成され、データプレーンにダウンロードされます。 プライマリまたはセカンダリのいずれかのインターフェイスを持つすべての VLAN で、新しい VLAN からバケットへのマッピングがデータプレーンにダウンロードされます。プライマリおよびセカンダリのデフォルトを必要とするすべての VLAN で、デフォルト選択のアルゴリズムがトリガーされ、QoS 検証に合格すると、VLAN からバケットへのマッピングがダウンロードされます。 QoS ポリシーは、新しく追加されたリンクの VLAN キューを作成します。

メンバー リンクの削除

メンバー リンクが削除されると、警告メッセージが表示されます。 メンバー リンクからのすべての VLAN キュー、VLAN からバケットへのマッピング、影響を受けるすべてのバケットは削除されます。

ポート チャネル リンク ダウン通知

リンクがダウンすると、プライマリ リンクとして割り当てられたポートチャネルのリンクがある VLAN のすべてのトラフィックは、セカンダリ リンクが稼働中の場合はセカンダリ リンクに切り替える必要があります。 セカンダリとして割り当てられたポートチャネルのリンクを持つVLAN のトラフィックは影響を受けません。 ポート チャネル リンク ダウン通知によって、プライマリとセカンダのペア（プライマリ リンクがダウンし、セカンダリ リンクが稼働している場合）に関連付けられたすべてのバケットが、セカンダリ リンクで更新されるようになります。 データプレーンにこの変更が伝えられます。

プライマリとセカンダリのペア（セカンダリ リンクがダウン リンクでプライマリ リンクが稼働中）に関連付けられたすべてのバケットが更新され、プライマリ リンクがアクティブ リンクになります。 データプレーンにこの変更が伝えられます。

ポート チャネル リンク アップ通知

リンクがアップすると、プライマリとしてこのリンクが割り当てられている VLAN のすべてのトラフィックは、このリンクに切り替えられます。 セカンダリとしてこのリンクが割り当てられている VLAN のトラフィックは影響を受けません。 ポート チャネル リンク アップ通知により、プライマリ リンクがアップになったリンクで、セカンダリ リンクがアップしていた、プライマリとセカンダリのペアに関連付けられたすべてのバケットに、プライマリ リンクがアップであることが通知されます。 データプレーンにこの変更が伝えられます。

セカンダリ リンクがアップになったリンクで、プライマリ リンクがダウンしている、プライマリとセカンダリのペアに関連付けられているすべてのバケットに、セカンダリ リンクがプライマリ リンクになったことが通知されます。 データプレーンにこの変更が伝えられます。

EtherChannel でのロード バランスのディセーブル化

EtherChannel のロードバランシングをディセーブルにするには、**no port-channel load-balancing vlan-manual** コマンドを使用します。 VLAN サブインターフェイスが見つかった場合、次の警告メッセージが表示されます。

```
Warning: Removing the Global VLAN LB command will affect traffic
c for all dot1Q VLANs
```

EtherChannel のメンバー リンクの削除

EtherChannel（EC）からメンバー リンクを削除するには、**no channel-group** コマンドを使用します。

VLAN マッピングに含まれているメンバー リンクが EC から削除されると、次の警告メッセージが表示されます。

```
Warning: Removing GigabitEthernet 4/0/0 from the port-channel will affect traffic for the
dot1Q VLANs that include this link in their mapping.
```

GEC リンクへの VLAN マッピングの設定方法

VLAN ベースの手動ロード バランシングの設定

VLAN ポートチャネルをリンクし、ポートチャネルで VLAN ロード バランシングをイネーブルにするには、この作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **port-channel load-balancing vlan-manual**
4. **interface port-channel** *channel-number*
5. **ip address** *ip-address address-mask*
6. **exit**
7. **interface** *type subinterface-number*
8. **channel-group** *channel-number*
9. **exit**
10. **interface port-channel** *interface-number.subinterface-number*
11. **encapsulation dot1Q** *vlan-id* **primary** *interface-type slot/port* **secondary** *interface-type slot/port*
12. **ip address** *ip-address address-mask*
13. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • 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： `Router# 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-balancing vlan-manual** 例： `Router(config)# port-channel load-balancing vlan-manual`	ルータ上で、ポートチャネル ロード バランシングをイネーブルにします。
ステップ 4	**interface port-channel** *channel-number* 例： `Router(config)# interface port-channel 1`	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、ポートチャネルとしてインターフェイスを定義します。
ステップ 5	**ip address** *ip-address address-mask* 例： `Router(config-if)# ip address 172.16.2.3 255.255.0.0`	IP アドレスおよびマスクを指定します。
ステップ 6	**exit** 例： `Router(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、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	**interface** *type subinterface-number* 例： `Router(config)# interface gigbabitethernet 1/1/0`	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	**channel-group** *channel-number* 例： `Router(config-if)# channel-group 1`	指定したチャネル グループにギガビットインターフェイスを割り当てます。 • チャネル番号は、ポートチャネル インターフェイスを作成したときに指定したチャネル番号と同じです。
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、グローバル コンフィギュレーション 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 10	**interface port-channel** *interface-number.subinterface-number* 例： `Device(config)# interface port-channel 1.100`	インターフェイスタイプ、インターフェイス番号、サブインターフェイス番号を指定します。
ステップ 11	**encapsulation dot1Q** *vlan-id* **primary** *interface-type slot/port* **secondary** *interface-type slot/port* 例： `Device(config-if)# encapsulation dot1Q 100 primary GigabitEthernet 1/1/1 secondary GigabitEthernet 1/2/1`	インターフェイス上で IEEE 802.1Q カプセル化をイネーブルにします。
ステップ 12	**ip address** *ip-address address-mask* 例： `Device(config-if)# ip address 172.16.2.100 255.255.255.0`	ポート チャネルの IP アドレスおよびマスクを指定します。
ステップ 13	**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。

トラブルシューティングのヒント

- 現在のポート チャネルのロードバランシング方式を表示するには、**show etherchannel load-balancing** コマンドを使用します。
- 現在のトラフィック分散を表示するには、**show interfaces port-channel etherchannel** コマンドを使用します。

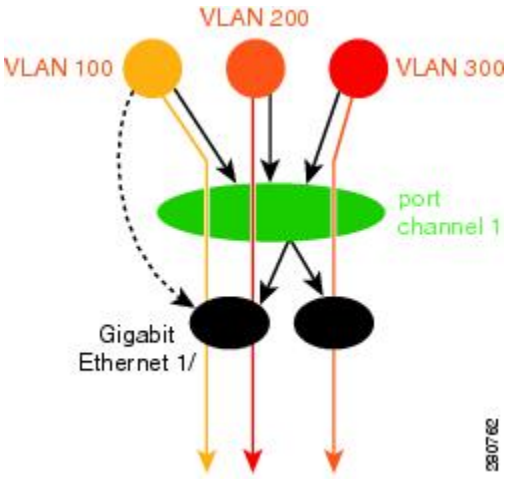
GEC メンバー リンクへの VLAN マッピングの設定例

例：VLAN 手動ロード バランシングの設定

次に、**port-channel load-balancing** コマンドを使用して、トラフィックを処理するポリシーを定義するために、ロードバランシングの設定をグローバルに適用する例を示します。 IEEE 802.1Q カ

プセル化は、各ポートチャネル インターフェイスで設定される点に注意してください。 次の図は、次の設定例で使用される 3 つの VLAN とポート チャネル バンドルを示しています。

図 *5*：ポート チャネル バンドル




```
port-channel load-balancing vlan-manual
!
class-map match-all BestEffort
!
class-map match-all video
!
class-map match-all voice
!
policy-map subscriber
  class voice
    priority level 1
  class video
    priority level 2
  class class-default service-fragment BE
    shape average 10000
    bandwidth remaining percent 80
policy-map aggregate-member-link
    class BestEffort service-fragment BE
    shape average 100000
!
interface Port-channel1
 ip address 172.16.2.3 255.255.0.0
!
interface Port-channel1.100
 encapsulation dot1Q 100 primary GigabitEthernet 1/1/1
               secondary GigabitEthernet 1/2/1
 ip address 172.16.2.100 255.255.255.0
 service-policy output subscriber
!
interface Port-channel1.200
 encapsulation dot1Q 200 primary GigabitEthernet 1/2/1
 ip address 172.16.2.200 255.255.255.0
 service-policy output subscriber
!
interface Port-channel1.300
 encapsulation dot1Q 300
 ip address 172.16.2.300 255.255.255.0
 service-policy output subscriber
!
interface GigabitEthernet 1/1/1
 no ip address
```

```
 channel-group 1 mode on
 service-policy output aggregate-member-link
!
interface GigabitEthernet 1/2/1
 no ip address
 channel-group 1 mode on
 service-policy output aggregate-member-link
```

例：トラブルシューティング

例 1：

```
Device# show etherchannel load-balancing

EtherChannel Load-Balancing Configuration: vlan-manual
```

例 2：

```
Device# show etherchannel load-balancing

EtherChannel Load-Balancing Configuration: not configured
```

現在使用中のトラフィック分散を表示するには、**show interfaces port-channel** コマンドを使用します。

```
Device# show interfaces port-channel 1 etherchannel

Active Member List contains 0 interfaces
 Passive Member List contains 2 interfaces
  Port: GigabitEthernet 4/0/0
    VLAN 1 (Pri, Ac, D, P)    VLAN 100 (Pri, Ac, C, P)    VLAN 200 (Sec, St, C, P)
  Port: GigabitEthernet 1/0/0
    VLAN 1 (Sec, St, D, P)    VLAN 100 (Sec, St, C, P)    VLAN 200 (Pri, Ac, C, P)
 Bucket Information for VLAN Manual LB:
    Bucket 0   (p=GigabitEthernet 4/0/0, s=GigabitEthernet 4/0/0) active GigabitEthernet
4/0/0
    Bucket 1   (p=Gigabitthernet 4/0/0, s=GigabitEthernet 1/0/0) active GigabitEthernet
4/0/0
    Bucket 4   (p=GigabitEthernet 1/0/0, s=GigabitEthernet 4/0/0) active GigabitEthernet
1/0/0
    Bucket 5   (p=GigabitEthernet 1/0/0, s=GigabitEthernet 1/0/0) active GigabitEthernet
1/0/0
```

プライマリおよびセカンダリ リンクへの VLAN マッピングを表示するには、**show vlans** コマンドを使用します。

```
Device# show vlans 100
VLAN ID: 100 (IEEE 802.1Q Encapsulation)
   Protocols Configured:          Received:        Transmitted:
VLAN trunk interfaces for VLAN ID 100:
Port-channel1.1 (100)
      Mapping for traffic load-balancing using bucket 1:
          primary   = GigabitEthernet 4/0/0 (active, C, P)
          secondary = GigabitEthernet 1/0/0 (standby, C, P)
      Total 0 packets, 0 bytes input
      Total 0 packets, 0 bytes output
No subinterface configured with ISL VLAN ID 100
```

その他の関連資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
LAN スイッチング コマンド	『*Cisco IOS LAN Switching Command Reference*』

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

GEC メンバー リンクへの VLAN マッピングの機能情報

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。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

表 7：ギガビット *EtherChannel* メンバー リンクへの *VLAN* マッピングの機能情報

機能名	リリース	機能情報
ギガビット EtherChannel メンバー リンクへの VLAN マッピング	Cisco IOS XE Release 2.1	ギガビット EtherChannel メンバー リンクへの VLAN マッピング機能を使用すると、GEC バンドル内の特定のメンバー リンクに VLAN ID で識別されるユーザ トラフィックのスタティックな割り当てを設定することができます。 プライマリおよびセカンダリ リンクに手動で VLAN サブインターフェイスを割り当てることができます。 この機能は、ベンダー機器の能力に関係なく、ダウンストリーム機器へのロード バランシングを可能にし、プライマリ リンクに障害が発生すると、トラフィックをセカンダリ メンバー リンクにリダイレクトすることでフェールオーバー保護を提供します。 シャーシあたり最大 16 バンドルでメンバー リンクがサポートされます。 次のコマンドが、この機能によって変更されました。 **encapsulation dot1q**、**port-channel load-balancing vlan-manual**、**show etherchannel load-balancing**、および **show interfaces port-channel vlan mapping**。

第 5 章

EtherChannel フローベース限定 1:1 冗長性

EtherChannel フローベース限定 1:1 冗長性は、上位層プロトコルが単一のリンク障害に対応して再コンバージェンスすることを防ぐために、MAC またはレイヤ 2 トラフィックを保護します。EtherChannel フローベース限定 1:1 冗長性を使用するには、2 つのポート（アクティブ 1 つとスタンバイ 1 つ）で EtherChannel を設定します。 アクティブ リンクがダウンしても、EtherChannel はアップしたままで、システムはホットスタンバイ リンクへのファスト スイッチオーバーを実行します。 優先順位の設定に応じて、障害リンクが再度動作可能になるときに、EtherChannel は、元のアクティブ リンクに戻るために、別のファスト スイッチオーバーを実行します。 すべてのポート プライオリティが同じ場合は、戻らずに現在のアクティブ リンクが維持されます。

1:1 冗長性が設定されていると、特定の時間にアクティブになるリンクは 1 つだけになるため、すべてのフローがアクティブ リンクを介して方向付けられます。

- 機能情報の確認，53 ページ
- EtherChannel フローベース限定 1:1 冗長性に関する情報，54 ページ
- EtherChannel フローベース限定 1:1 冗長性の設定方法，54 ページ
- EtherChannel フローベース限定 1:1 冗長性の設定例，59 ページ
- その他の関連資料，61 ページ
- EtherChannel フローベース限定 1:1 冗長性の機能情報，62 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の警告および機能情報については、『Bug Search Tool』およびご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

EtherChannel フローベース限定 1:1 冗長性に関する情報

EtherChannel フローベース限定 1:1 冗長性

EtherChannel フローベース限定 1:1 冗長性によって、アクティブ リンク 1 つで EtherChannel を設定し、ホットスタンバイ リンクにファスト スイッチオーバーを提供します。 EtherChannel フローベース限定 1:1 冗長性を使用するには、2 つのポート（アクティブ 1 つとスタンバイ 1 つ）で Link Aggregation Control Protocol（LACP）EtherChannel を設定します。 アクティブ リンクがダウンしても、EtherChannel はアップしたままで、システムはホットスタンバイ リンクへのファスト スイッチオーバーを実行します。 リンクの優先順位の設定に応じて、障害リンクが再度動作可能になるときに、EtherChannel は元のアクティブ リンクまたはより優先順位の高いリンクに戻すために、ファスト スイッチオーバーをもう 1 回実行します。

EtherChannel フローベース限定 1:1 冗長性（特にファスト スイッチオーバー機能）が正しく機能するには、リンクの両端でこの機能がイネーブル化されている必要があります。

EtherChannel フローベース限定 1:1 冗長性の設定方法

EtherChannel フローベース限定 1:1 冗長性のファストスイッチオーバーとの設定

LACP EtherChannel を 2 つのポート（アクティブ 1 つとスタンバイ 1 つ）で設定するには、次の手順を実行します。 この機能は、リンクの両端でイネーブルにする必要があります。

冗長性に使用されるリンクのプライオリティを設定することによって、どのリンクをプライマリ アクティブ リンクにするかを制御できます。 プライマリ リンクを設定し、EtherChannel が元のリンクに戻ることを可能にするために、1 つのリンクのプライオリティを他のリンクより高くし、LACP の max-bundle を 1 に設定する必要があります。 この設定によって、リンク 1 がアクティブになり、リンク 2 がホットスタンバイ ステートになります。

スイッチオーバーが戻ることを防ぐために、両方のリンクに同じプライオリティを割り当てることができます。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface port-channel** *channel -number*
4. **lacp fast-switchover**
5. **lacp max-bundle 1**
6. **exit**
7. **interface tengigabitethernet** *slot* / *port* / *number*
8. **channel-group 1 mode** *mode*
9. **lacp port-priority** *priority*
10. **exit**
11. **interface tengigabitethernet** *slot* / *port* / *number*
12. **channel-group 1 mode** *mode*
13. **lacp port-priority** *priority*
14. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • 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： `Router# 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* 例： `Router(config)# interface port-channel 1`	LACP 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	**lacp fast-switchover** 例： `Router(config-if)# lacp fast-switchover`	この EtherChannel のファスト スイッチオーバー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 5	**lacp max-bundle 1** 例： `Router(config-if)# lacp max-bundle 1`	アクティブなメンバー ポートの最大数を 1 に設定します。
ステップ 6	**exit** 例： `Router(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、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	**interface tengigabitethernet** *slot* / *port* / *number* 例： `Router(config)# interface tengigabitethernet 0/0/0`	ポート チャネルに追加する最初のインターフェイスを選択します。
ステップ 8	**channel-group 1 mode** *mode* 例： `Router(config-if)# channel-group 1 mode active`	メンバー リンクをポートチャネルに追加し、LACP ネゴシエーションにアクティブに参加します。
ステップ 9	**lacp port-priority** *priority* 例： `Router(config-if)# lacp port-priority 32768`	ポートチャネルのプライオリティを設定します。 このプライオリティはデフォルト値に設定されます。
ステップ 10	**exit** 例： `Router(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、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 11	**interface tengigabitethernet** *slot* / *port* / *number* 例： `Router(config)# interface tengigabitethernet 1/0/0`	ポート チャネルに追加するインターフェイスを選択します。

	コマンドまたはアクション	目的
ステップ 12	**channel-group 1 mode** *mode* 例： `Router(config-if)# channel-group 1 mode active`	メンバー リンクをポートチャネルに追加し、LACP ネゴシエーションにアクティブに参加します。
ステップ 13	**lacp port-priority** *priority* 例： `Router(config-if)# lacp port-priority 32767`	デフォルト値である 32768 より低い値を使用して、ポートのプライオリティを他のリンクより高く設定します。これにより、トラフィックをやり取りするときは必ず、このリンクがアクティブ リンクになります。
ステップ 14	**end** 例： `Router(config-if)# end`	インターフェイス コンフィギュレーション モードを終了します。

キャリア遅延のスイッチオーバー レートの設定

オプションで、各リンクのキャリア遅延を設定してアクティブとスタンバイ リンク間のスイッチオーバーの速度を制御できます。 **carrier-delay** コマンドは、他のモジュールにリンク状態に関する情報を Cisco IOS が伝播するためにどのくらいの時間がかかるかを制御します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface tengigabitethernet** *slot* / *port* / *number*
4. **carrier-delay msec** *msec*
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • 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： `Router# 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 tengigabitethernet** *slot* / *port* / *number* 例： `Router(config)# interface tengigabitethernet 0/1/0`	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、指定したインターフェイスの設定が表示されます。
ステップ 4	**carrier-delay msec** *msec* 例： `Router(config-if)# carrier-delay msec 11`	他のモジュールにリンク ステータスを伝播するためにかかる時間を設定します。
ステップ 5	**end** 例： `Router(config-if)# end`	インターフェイス コンフィギュレーション モードを終了します。

EtherChannel フローベース限定 1:1 冗長性の確認

これらの show コマンドを使用して、設定を確認し、ポート チャネルに関する情報を表示します。

手順の概要

1. **enable**
2. **show running-config interface** *type slot / port / number*
3. **show interfaces port-channel** *channel-number* **etherchannel**
4. **show etherchannel** *channel-number* **port-channel**
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**show running-config interface** *type slot / port / number* 例： `Router# show running-config interface tengigabitethernet 0/0/0`	設定を確認します。 • *type*：**gigabitethernet** または **tengigabitethernet**。
ステップ 3	**show interfaces port-channel** *channel-number* **etherchannel** 例： `Router# show interfaces port-channel 1 etherchannel`	現在使用中のバケットの分散が表示されます。
ステップ 4	**show etherchannel** *channel-number* **port-channel** 例： `Router# show etherchannel 1 port-channel`	ポート チャネル ファスト スイッチオーバー機能を表示します。
ステップ 5	**end** 例： `Router# end`	特権 EXEC モードを終了します。

EtherChannel フローベース限定 1:1 冗長性の設定例

EtherChannel 1:1 アクティブ スタンバイの例

次に、どのポートがアクティブになるかが優先設定されないように、ポートのプライオリティが同じ 1:1 リンク冗長性用にポート チャネルを設定する例を示します。

```
Router# enable
Router# configure terminal
```

```
Router(config)# interface port-channel 2
Router(config-if)# ip address 10.1.1.1 255.255.0.0
Router(config-if)# negotiation auto
Router(config-if)# lacp max-bundle 1
Router(config-if)# lacp fast-switchover
Router(config)# interface Tengigabitethernet0/1/0
Router(config-if)# channel-group 2 mode active
Router(config-if)# negotiation auto
Router(config)# interface Tengigabitethernet 2/1/0
Router(config-if)# channel-group 2 mode active
Router(config-if)# negotiation auto
Router(config)# interface GigabitEthernet0/1/6
Router(config-if)# negotiation auto
Router(config-if)# channel-group 19 mode active
Router(config)# interface GigabitEthernet0/1/7
Router(config-if)# negotiation auto
Router(config-if)# channel-group 19 mode active
Router(config-if)# interface Port-channel19
Router(config-if)# ip address 10.19.1.1 255.255.255.0
Router(config-if)# no negotiation auto
Router(config-if)# lacp fast-switchover
Router(config-if)# lacp max-bundle 1
Router(config-if)# end
```

show コマンドで、プライオリティ値が同じであることが示されています。

```
Router# show lacp internal
Flags: S - Device is requesting Slow LACPDUs
 F - Device is requesting Fast LACPDUs
 A - Device is in Active mode P - Device is in Passive mode
Channel group 19
LACP port Admin Oper Port Port
Port Flags State Priority Key Key Number State
Gi0/1/6 SA bndl 32768 0x13 0x13 0x47 0x3D
Gi0/1/7 FA hot-sby 32768 0x13 0x13 0x48 0x7
```

LACP を使用した 1:1 冗長性のプライオリティ設定の例

この例は、1:1 冗長性機能を備えた LACP EtherChannel を設定する方法を示しています。GigabitEthernet 0/1/7 は、高いプライオリティを与える低い値で設定されるため、アクティブなリンクになります。

```
Router# configure terminal
Router(config)# interface GigabitEthernet0/1/6
Router(config-if)# lacp port-priority 32767
Router(config-if)# exit
Router(config)# interface GigabitEthernet0/1/7
Router(config-if)# lacp fast-switchover
Router(config-if)# lacp max-bundle 1
Router(config-if)# negotiation auto
Router(config-if)# channel-group 19 mode active
```

この例では、バンドル リンクに高いプライオリティが設定されています。これにより、スタンバイ設定でバンドル リンクが最初のアクティブ リンクとして使用されるようになります。

```
Router# show lacp internal

Flags: S - Device is requesting Slow LACPDUs
 F - Device is requesting Fast LACPDUs
 A - Device is in Active mode P - Device is in Passive mode
Channel group 19
LACP port Admin Oper Port Port
Port Flags State Priority Key Key Number State
Gi0/1/6 FA hot-sby 32768 0x13 0x13 0x47 0x7
Gi0/1/7 SA bndl 32767 0x13 0x13 0x48 0x3D
```

その他の関連資料

ここでは、EtherChannel フローベース限定 1:1 冗長性機能の関連資料を示します。

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
LAN スイッチング コマンド	『*Cisco IOS LAN Switching Command Reference*』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS XE ソフトウェア リリース、およびフィーチャ セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能がサポートする新しい RFC または変更された RFC はありません。また、この機能は既存の規格に対するサポートに影響を及ぼしません。	--

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

EtherChannel フローベース限定 1:1 冗長性の機能情報

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。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

表 *8* : *EtherChannel* フローベース限定 *1:1* 冗長性の機能情報

機能名	リリース	機能情報
EtherChannel フローベース限定 1:1 冗長性	Cisco IOS XE Release 2.4	EtherChannel フローベース限定 1:1 冗長性は、上位層プロトコルが単一のリンク障害に対応して再コンバージェンスすることを防ぐために、MAC またはレイヤ2 トラフィックを保護します。 EtherChannel フローベース限定 1:1 冗長性を使用するには、2 つのポート（アクティブ 1 つとスタンバイ 1 つ）で EtherChannel を設定します。 アクティブ リンクがダウンしても、EtherChannel はアップしたままで、システムはホットスタンバイ リンクへのファスト スイッチオーバーを実行します。 優先順位の設定に応じて、障害リンクが再度動作可能になるときに、EtherChannel は、元のアクティブ リンクに戻るために、別のファスト スイッチオーバーを実行します。 すべてのポート プライオリティが同じ場合は、戻らずに現在のアクティブ リンクが維持されます。 この機能をサポートするために変更または作成されたコマンドはありません。

第 6 章

フローベースのポートチャネルごとのロード バランシング

フローベースのポートチャネルごとのロード バランシング機能を使用すると、ギガビット EtherChannel（GEC）インターフェイス経由のトラフィックのさまざまなフローをパケット ヘッダーに基づいて識別し、ポート チャネルの異なるメンバー リンクにマッピングすることができます。 この機能により、フローベースのロード バランシングと手動 VLAN ロード バランシングを特定のポート チャネルに設定することができます。

- 機能情報の確認，65 ページ
- フローベースのポートチャネルごとのロード バランシングの制約事項，66 ページ
- フローベースのポートチャネルごとのロード バランシングに関する情報，66 ページ
- フローベースのポートチャネルごとのロード バランシングをイネーブルにする方法，70 ページ
- フローベースのポートチャネルごとのロード バランシングの設定例，73 ページ
- その他の関連資料，74 ページ
- フローベースのポートチャネルごとのロード バランシングの機能情報，75 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の警告および機能情報については、『Bug Search Tool』およびご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

フローベースのポートチャネルごとのロードバランシングの制約事項

- 最大で 64 の GEC インターフェイスをサポートします。
- GEC インターフェイスあたり最大で 4 つのメンバー リンクをサポートします。

フローベースのポートチャネルごとのロードバランシングに関する情報

フローベースのロード バランシング

フローベースのロードバランシングは、データ パケットのキーフィールドに基づいてトラフィックのさまざまなフローを識別します。フローを識別するために、たとえば、IPv4 送信元および宛先 IP アドレスを使用できます。 次に、さまざまなデータ トラフィックがポート チャネルの異なるメンバー リンクにマッピングされます。マッピングが完了したら、フローのデータ トラフィックは、割り当てられたメンバー リンクを通じて送信されます。 フロー マッピングは動的で、フローが割り当てられたメンバーリンクの状態が変わったときに変更されます。フローのマッピングは、メンバーリンクがGECインターフェイスに追加または削除された場合にも変更されます。複数のフローは、各メンバー リンクにマッピングできます。

フローベースのロード バランシング用のバケット

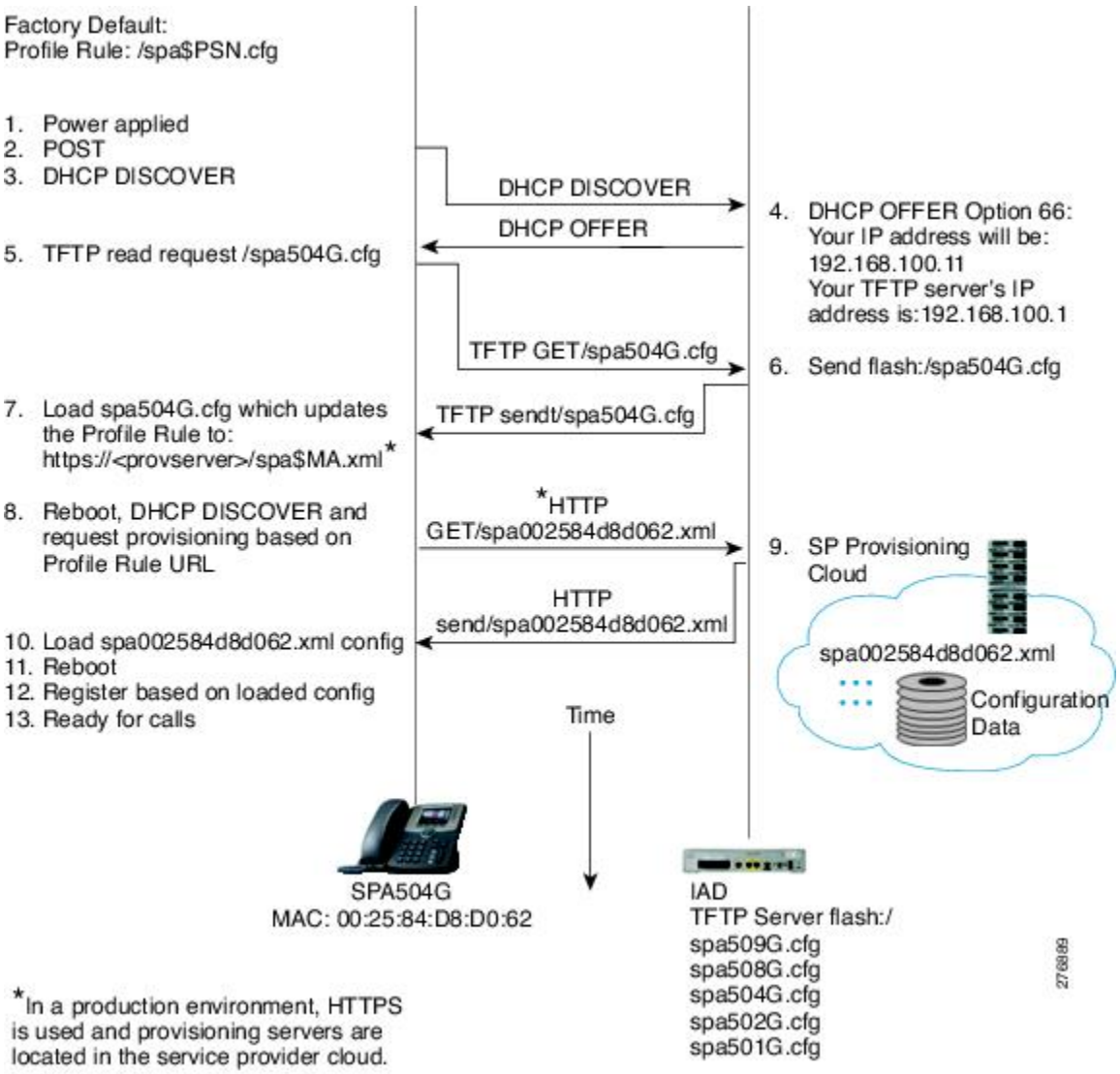
ロード バランシングは、バケットの概念によって、GEC インターフェイスのメンバー リンクへのトラフィック フローを動的にマッピングします。 多様な定義済みトラフィック フローがバケットにマップされ、バケットはメンバー リンク間で均等に配分されます。 各ポート チャネルで 16 のバケットが維持され、各バケットに 1 つのアクティブ メンバー リンクが関連付けられます。バケットにマッピングされたすべてのトラフィック フローは、バケットが割り当てられたメンバー リンクを使用します。

ルータは、ポートチャネルにフローベースのロードバランシングを適用するときに、バケットからメンバーへのリンク マッピングを作成し、ポート チャネルには少なくとも 1 つのアクティブ メンバー リンクが作成されます。 マッピングは、最初のメンバー リンクが追加または起動されるときにも作成され、ロードバランシング方式がフローベースに設定されます。

メンバー リンクがダウンするか、またはポート チャネルから削除されると、そのメンバー リンクに関連付けられたバケットはラウンドロビン方式で他のアクティブ メンバーリンク間で再配布されます。 メンバー リンクが起動するまたはポート チャネルに追加されると、他のリンクに関連付けられたバケットの一部がこのリンクに割り当てられます。

次の図は、3 つのメンバー リンク間で配布された 16 のバケットの例を示します。 バケットに表示される番号はバケット ID です。 最初のメンバー リンクに追加のバケットがあることに注意してください。

図 *6* : *3* つのメンバー リンクにマッピングされた *16* のバケットの例



ロードバランシング方式を変更する場合、フローベースのロードバランシング用のバケットからメンバーへのリンク マッピングは削除されます。 マッピングは、ポート チャネルが削除されるか、またはポート チャネルの最後のメンバー リンクが削除されるまたはダウンした場合にも削除されます。

ポート チャネルのロード バランシング

GEC インターフェイスは、動的なフローベースのロード バランシングまたは手動 VLAN ロード バランシングを使用できます。すべてのポートチャネルに対してグローバルにロードバランシング方式を設定するか、特定のポート チャネルに直接設定するかを設定できます。 グローバル コンフィギュレーションは、ロードバランシングが明示的には設定されていないポートチャネルだけに適用されます。 ポートチャネルの設定はグローバル コンフィギュレーションを上書きします。

フローベースのロード バランシングは、グローバル レベルでデフォルトでイネーブルになります。 VLAN ロード バランシングを明示的に設定しないと、ロードバランシング方式は、フローベースになります。

VLAN ロード バランシングの設定については、「ギガビット EtherChannel メンバー リンクへの VLAN マッピング」のモジュールを参照してください。

次の表は、設定に基づいてポート チャネルに適用されるロードバランシング方式をリストします。

表 *9*：フローベースのロード バランシングの設定オプション

グローバル設定	ポートチャネルの設定	適用されるロード バランシング
未設定	未設定	フローベース
	フローベース	フローベース
	手動 VLAN	手動 VLAN
手動 VLAN	未設定	手動 VLAN
	フローベース	フローベース
	手動 VLAN	手動 VLAN

次の表に、グローバル ロードバランシング方式を変更した場合の設定結果を示します。

表 *10*：グローバル コンフィギュレーションが変更された場合の結果

ポートチャネルの設定	グローバル設定	ポートチャネルで実行される処理	
–	From	To	–

ポートチャネルの設定	グローバル設定	ポートチャネルで実行される処理	
未設定	未設定	手動 VLAN	フローベースから手動 VLAN への変更
	手動 VLAN	未設定	手動 VLAN からフローベースへの変更
設定済み	Any	Any	変更なし

次の表に、ポートチャネル ロードバランシング方式が変更された場合の設定結果を示します。

表 *11*：ポートチャネルの設定が変更された場合の結果

グローバル設定	ポートチャネルの設定	ポートチャネルで実行される処理	
–	From	To	–
未設定	未設定	手動 VLAN	フローベースから手動 VLAN への変更
	未設定	フローベース	アクションなし
	手動 VLAN	フローベース	手動 VLAN からフローベースへの変更
	手動 VLAN	未設定	手動 VLAN からフローベースへの変更
	フローベース	手動 VLAN	フローベースから手動 VLAN への変更
	フローベース	未設定	アクションなし

グローバル設定	ポートチャネルの設定	ポートチャネルで実行される処理	
手動 VLAN	未設定	手動 VLAN	アクションなし
	未設定	フローベース	手動 VLAN からフローベースへの変更
	手動 VLAN	フローベース	手動 VLAN からフローベースへの変更
	手動 VLAN	未設定	アクションなし
	フローベース	手動 VLAN	フローベースから手動 VLAN への変更
	フローベース	未設定	フローベースから手動 VLAN への変更

フローベースのポートチャネルごとのロードバランシングをイネーブルにする方法

ポート チャネルのロード バランシングの設定

ポート チャネルにロード バランシングを設定するには、次の手順を実行します。 各 GEC インターフェイスに対してこの手順を繰り返して行います。

はじめる前に

すでに目的のロードバランシング方式をグローバルに設定しており、その方式をすべてのポートチャネルに使用する場合は、この作業を行う必要はありません。 ロードバランシングをグローバルに設定するには、**port-channel load-balancing vlan-manual** コマンドを使用します。 グローバルコマンドを設定しない場合、フローベースのロードバランシングがすべてのポートチャネルに適用されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface port-channel** *channel-number*
4. **load-balancing** {**flow** | **vlan**}
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • 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： `Router# 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* 例： `Router(config)# interface port-channel 1`	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、ポート チャネルとしてインターフェイスを定義します。
ステップ 4	**load-balancing** {**flow**	**vlan**} 例： `Router(config-if)# load-balancing flow`	特定のポート チャネルにロードバランシング方式を適用します。 • このコマンドを設定しない場合、ポートチャネルは、**port-channel load-balancing vlan-manual** コマンドで設定されたグローバル ロードバランシング方式を使用します。 グローバル デフォルトはフローベースです。
ステップ 5	**end** 例： `Router(config-if)# end`	コンフィギュレーション モードを終了します。

GEC インターフェイスのロードバランシング設定の確認

ロードバランシング設定を確認し、ポート チャネルのバケットの分散に関する情報を表示するには、これらの show コマンドを使用します。 任意の順序でこれらのコマンドを使用できます。

手順の概要

1. **show running-config interface port-channel** *channel-number*
2. **show etherchannel load-balancing**
3. **show interfaces port-channel** *channel-number* **etherchannel**

手順の詳細

ステップ 1 **show running-config interface port-channel** *channel-number*
ポート チャネルの設定を確認するには、このコマンドを使用します。

例：

```
Router# show running-config interface port-channel 1
Building configuration...

Current configuration : 88 bytes
!
interface Port-channel1
 ip address 10.1.1.1 255.0.0.0
 no negotiation auto
 load-balancing flow
end
```

ステップ 2 **show etherchannel load-balancing**
各ポート チャネルに適用されるロードバランシング方式を表示するには、このコマンドを使用します。 次に、VLAN に手動でグローバルに、フローベースでポート チャネル 1 に設定されたロード バランシングの設定の出力例を示します。

例：

```
Router# show etherchannel load-balancing


EtherChannel Load-Balancing Method:
Global LB Method: vlan-manual

  Port-Channel:                       LB Method
    Port-channel1                   :  flow-based
```

ステップ 3 **show interfaces port-channel** *channel-number* **etherchannel**
現在使用中のバケットの分散を表示するには、このコマンドを使用します。 次に、ロード バランシングがフローベースに設定されているインターフェイスの出力例を示します。

例：

```
Router(config)# show interface port-channel 2 etherchannel

 All IDBs List contains 3 configured interfaces
  Port: GigabitEthernet2/1/6 (index: 0)
  Port: GigabitEthernet2/1/7 (index: 1)
  Port: GigabitEthernet2/1/0 (index: 2)

 Active Member List contains 1 interfaces
  Port: GigabitEthernet2/1/0

 Passive Member List contains 2 interfaces
  Port: GigabitEthernet2/1/6

  Port: GigabitEthernet2/1/7

 Load-Balancing method applied: flow-based

 Bucket Information for Flow-Based LB:
 Interface:                                Buckets
    GigabitEthernet2/1/0:
                           Bucket 0 , Bucket 1 , Bucket 2 , Bucket 3
                           Bucket 4 , Bucket 5 , Bucket 6 , Bucket 7
                           Bucket 8 , Bucket 9 , Bucket 10, Bucket 11
                           Bucket 12, Bucket 13, Bucket 14, Bucket 15
```

フローベースのポートチャネルごとのロードバランシングの設定例

フローベースのロード バランシングの例

次に、フローベースのロード バランシングがポートチャネル 2 で設定され、VLAN 手動方式がグローバルに設定されている設定の例を示します。

```
!
no aaa new-model
port-channel load-balancing vlan-manual
ip source-route
.
.
.
interface Port-channel2
 ip address 10.0.0.1 255.255.255.0
 no negotiation auto
 load-balancing flow
!
interface Port-channel2.10
 ip rsvp authentication key 11223344
 ip rsvp authentication
!
interface Port-channel2.50
 encapsulation dot1Q 50
!
```

```
interface GigabitEthernet2/1/0
 no ip address
 negotiation auto
 cdp enable
 channel-group 2
!
```

その他の関連資料

ここでは、フローベースのポートチャネルごとのロードバランシング機能に関連する参考資料を示します。

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
Cisco IOS LAN スイッチング コマンド	『*Cisco IOS LAN Switching Command Reference*』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS XE ソフトウェア リリース、およびフィーチャ セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能がサポートする新しい RFC または変更された RFC はありません。また、この機能は既存の規格に対するサポートに影響を及ぼしません。	--

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

フローベースのポートチャネルごとのロードバランシングの機能情報

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。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

表 *12*：フローベースのポートチャネルごとのロード バランシングの機能情報

機能名	リリース	機能情報
フローベースのポートチャネルごとのロード バランシング	Cisco IOS XE Release 2.5	この機能を使用すると、GEC インターフェイスを経由するトラフィックのさまざまなフローを、異なるメンバー リンクに識別しマッピングすることができます。 また、特定のポートチャネルにロード バランシングを適用することもできます。 次のコマンドが導入または変更されました。**load-balancing**、**port-channel load-balancing vlan-manual**、**show etherchannel load-balancing**、**show interfaces port-channel etherchannel**。
GEC での IPv6 ロードバランシング	Cisco IOS XE Release 3.4S	GEC での IPv6 ロードバランシング機能は、Gigabit EtherChannel の IPv6 トラフィックにロードバランシングを提供します。

第 7 章

Resilient Ethernet Protocol（REP）

Resilient Ethernet Protocol（REP）はシスコ独自のプロトコルで、スパニングツリー プロトコル（STP）の代替となります。 REP はネットワーク 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 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、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。

- 機能情報の確認，77 ページ
- Resilient Ethernet Protocol の制約事項，78 ページ
- REP に関する情報，78 ページ
- REP の設定方法，88 ページ
- REP の設定例，103 ページ
- その他の関連資料，105 ページ
- Resilient Ethernet Protocol の機能情報，106 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の警告および機能情報については、『Bug Search Tool』およびご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

Resilient Ethernet Protocol の制約事項

- ルータが REP をサポートするのは、ルータがメトロ IP アクセスまたはメトロ アクセス イメージを実行している場合のみです。
- 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の高損失が発生します。
- 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、ネットワーク接続が失われます。

REP に関する情報

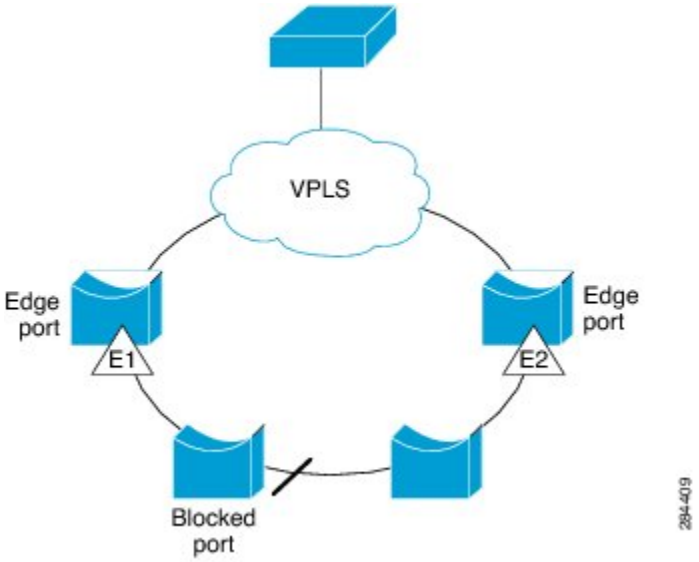
REP セグメント

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 つのユーザ設定のエッジ ポートで構成されています。 1 ルータは同じセグメントに属するポートを複数持たず、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 はトランクのイーサネット フロー ポイント（EFP）インターフェイス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の場合、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。

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。

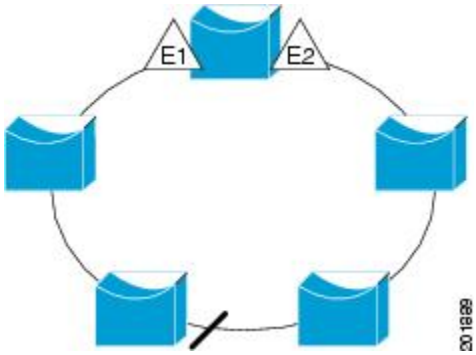
図 *7*：*REP* オープン セグメント



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 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。 セグメント内のルータ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 はすべてのポートのブロックを解除し、他のゲートウェイ経由で接続できるようにします。

下の図に示すセグメントはリングセグメントであり、同じルータ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 *8*：*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（代替ポートと呼ばれる）が各 VLAN でブロック ステートとなります。 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 つのポートが VLAN のブロック ステートを制御します。
- セグメント内の 1 つまたは複数のポートが動作不能になると、リンク障害が発生して、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。 また REP は、プライマリ エッジ ポートで制御されているが、セグメント内の任意のポートで発生する、VLAN ロード バランシングをサポートしています。

リンク完全性

REP は、リンク完全性を確認するためにエッジ ポート間でエンドツーエンド ポーリング メカニズムを使用していません。 ローカル リンク障害検出を実装しています。 インターフェイスがイネーブルの場合、REP リンク ステータス レイヤ（LSL）が REP 認識ネイバーを検出して、セグメント内の接続性を確立します。 REP LSL がネイバーを検出するまで、すべての VLAN がインターフェイスでブロックされます。 ネイバーが特定されたあと、REP が代替ポートとなるネイバー 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、スパニングツリー 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、LSL がセグメント ID とポート ID を含むパケットを送信します。 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。 セグメント ポートは、次のような状態で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。 ネイバー関係が確立されると、ポートがセグメントの1つのブロックされたポート（代替ポート）を決定するようにネゴシエートします。 その他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 PortFast ブリッジ プロトコル データ ユニット（BPDU）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、現時点でセグメントに障害が発生した場合に Blocked Port Advertisement（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。

短時間でのコンバージェンス

REP が物理リンク ベースで動作し、VLAN 単位ベースで動作しないため、全 VLAN で必要なのは 1 つの hello メッセージだけなので、プロトコルの負荷が低減します。 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 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のマルチキャストアドレスにフラッディング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 セグメントだけではなくネットワーク全体にフラッディングされます。 このセグメントに属さないスイッチは、メッセージをデータ トラフィックとして処理します。 ドメイン全体で専用の管理 VLAN を設定することで、これらのメッセージのフラッディングを制御することができます。

予想されるコンバージェンス復旧時間はローカル セグメントで 200 ms 未満です。

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 ロード 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場合、次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** コマンドを入力します。
- 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 ポート自体のオフセット番号なので、オフセット番号 1 は入力できません。

- **preferred** キーワードを入力することで、**rep segment preferred** 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。

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 バランシングは、次の 2 通りの方法のいずれかでトリガーできます。

- プライマリ エッジ ポートのあるルータ上で **rep preempt segment** *segment-id* 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* コマンドを入力すると、プリエンプト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ます。

（注） 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、VLAN ロード バランシングは開始されません。

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エッジポートで受信されると、ネットワークでメッセージが生成され、メッセージ内で特定された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 ポートによってしかVLAN ロード バランシングは開始されず、セグメントが各エンドでエッジ 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。

VLAN 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 ポートを再設定する必要があります。 VLANロードバランシング設定を変更するには、プライマリエッジポートで**rep preemt segement** コマンドを待機するか、ポート障害および復旧のあとで新しい VLAN ロード バランシング設定を実行する前に設定済プリエンプト遅延期間を待機します。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 プロトコルの対話

REP は STP または Flex Link と対話しませんが、両方と共存できます。 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で設定されたらエッジ ポートを設定できます。

REP ポート

REP セグメント内のポートは、3 つの役割またはステート（障害、オープン、または代替）のいずれかになります。

- 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発生し、セグメントが安定すると、ブロックされたポートの 1 つは代替ロールのままになり、他のすべてのポートがオープン ポートとなります。
- リンク内に障害が発生すると、すべてのポートが障害ステートに移行します。代替ポートが障害通知を受信すると、ポートはすべての VLAN を転送するオープン ステートに変更されます。

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、このポートは指定ブロッキング ポートです。 PortFast BPDU ガード拡張機能が設定されている場合、または STP がディセーブルになっている場合、ポートはフォワーディング ステートになります。

VPLS との REP 統合

一般に、Virtual Private LAN Service（VPLS）のネットワーク コアでは、すべてのノードが完全メッシュ トポロジで接続され、各ノードは他のすべてのノードと接続されています。 完全メッシュトポロジでは、ノードが他のノードにデータを再送信する必要はありません。 図 3 では、共通リングによって、パケットを他のネットワーク プロバイダー エッジ（N-PE）ルータに転送できるパスが提供され、スプリット ホライズン モデルを無効にします。

REP は共通リンク接続をエミュレーションするため、REP リングは VPLS の完全メッシュ モデルをサポートしますが、スプリット ホライズンのプロパティを維持するため、スーパーループは存在しません。 エミュレーションされた共通リンクは Clustering over the WAN（CWAN）ラインカードを使用します。これは VPLS アップリンクにも使用されます。 このエミュレーションされた共通リンクは、リングから VPLS アップリンクまたはリングの反対側にデータを転送し、VPLS コアネットワークから着信するデータをブロックして、Hierarchical-VPLS（H-VPLS）トポロジのアクセス疑似ワイヤを処理します。

REP のデフォルト設定

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ければ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。

REP セグメントと REP 管理 VLAN

セグメントは、チェーンで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 モードで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、1 つをプライマリ エッジ ポート、もう 1 つをデフォルトでセカンダリ 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。 たとえば、異なるスイッチのポートで、プライマリ エッジ ポートとしてセグメントで2つのポートを設定すると、REPはそのいずれかをプライマリ エッジ ポートとして選択します。 オプションで、セグメント STCN および VLAN ロード バランシングを送信する場所を設定することもできます。 REP 管理 VLAN の設定方法の詳細については、「*REP* 管理 *VLAN* の設定」のセクションを参照してください。

REP 設定時の注意事項

REP の設定時には、次の注意事項に従ってください。

- 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 inteface** 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 EFP 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 BPDU は、REP インターフェイスで廃棄されます。
- REP がルータの 2 つの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。
  - 1 つのルータ上で 1 つのポートだけがセグメントで設定される場合、このポートは 1 つのエッジ ポートである必要があります。
  - 1 つのルータ上で 2 つのポートが同じセグメントに属する場合、両方のポートはエッジ ポートであるか、通常のセグメント ポートである必要があります。
  - 1 つのルータ上で 2 つのポートが同じセグメントに属し、1 つがエッジ ポートとして設定され、もう 1 つが通常のセグメント ポートとして設定された場合（設定ミス）、エッジ ポートは通常のセグメント ポートとして処理されます。
- 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、この状態を意識しておく必要があります。
- 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
  - プライベート VLAN ポート
  - トンネル ポート
  - アクセス ポート
- ルータごとに最大 22 の REP セグメントを設定できます。

トランク EFP の REP サポート

Resilient Ethernet Protocol（REP）は、Cisco ASR 903 シリーズ ルータのインターフェイス レベルの EFP トランク ポートで設定できます。 トランク EFP ポートでは、複数のブリッジド VLAN サービスを実行することができます。 VLAN は、トランク EFP ポートでブロックまたはフォワーディング ステートに設定できます。 ユーザは、ポートで REP をイネーブルにする必要があります。 デフォルトでは、REP はすべてのポートでディセーブルです。

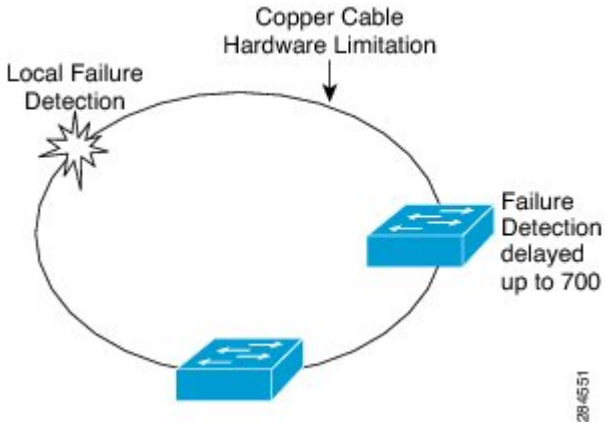
REP 設定可能タイマー

リング ネットワーク トポロジでは、Fast Last Link Status（LSL）プロセスがネイバー ポートを検出し、そのポートとの接続を維持します。 ポートのタイマーは、200 ～ 10000 ミリ秒の範囲で LSL フレームを受信するように設定できます。 LSL フレームがネイバー ポートから 200 ～ 10000 ミリ秒の範囲で受信されない場合、ルータ間のリンクはダウンしていると見なされます。 リンクを起動しトラフィックを復元するために、切断操作とアクションが実行されます。

リング ネットワーク トポロジでは、REP が 50 ミリ秒以内でトラフィックを収束できない場合があります。 たとえば、トポロジが銅ケーブルの場合、銅インターフェイスのハードウェア制限により、REP はトラフィックの収束に失敗する可能性があります。 このようなシナリオでは、リモート エンドがローカル ポートのシャットダウン障害を検出するために最大で 700 ミリ秒かかる場合があります。 REP LSL は、リモート側で高いタイマー粒度と速い障害検出を達成できるように強化されました。

次の図は、銅インターフェイスのハードウェア制限による障害検出の遅延を示します。

図 *9*：障害検出の遅延



REP Fast Hello での SSO サポート

ルータがクラッシュした場合、ルータがアクティブ モードになり、REP Fast Hello パケットの送信を開始するまで、3 ～ 5 秒かかります。 **lsl age out timer** コマンドで設定されたエージング アウト タイマーの値が、3 秒より短い場合、リモート エンドはポート障害を検出して再コンバージェンスします。 再コンバージェンス後に、ルータは特殊なタイプ、長さ、および値（TLV）を持つ BPDU を接続ポートに送信します。 ルータは、次の REP スリーウェイ リンク完全性チェックに失敗しないように、ポートのローカルおよびリモートのシーケンス番号を学習します。 REP のステートフル スイッチオーバー（SSO）のサポートは、LSL インターバルの期限が切れる前に、Fast Hello パケットがルータから送信できるようにします。

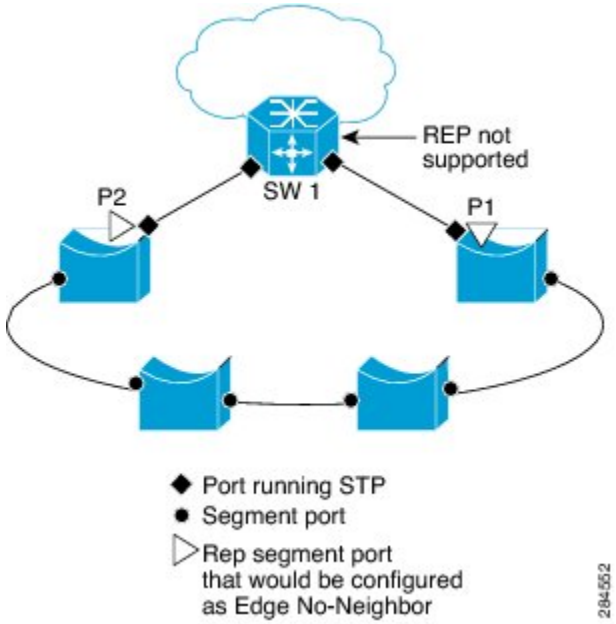
REP 非ネイバー エッジ サポート

リング ネットワーク トポロジでは、集約ノードで REP がサポートされません。 REP セグメントは、スイッチの収束を達成するために、ネイバーのないポートで作成できます。 次の図は、リング トポロジの非ネイバー エッジ ポートとしての P1 および P2 を示します。 この設定で P1 および P2 はトラフィックをブロックすることがあります。 リンクのいずれかに障害が発生した場合、REP 設定のすべてのスイッチが収束します。 P1 および P2 はエッジではないため、次のタスクをサポートしていません。

- VLAN ロード バランシングを実行します。
- 他のセグメントとスパニングツリー プロトコル（STP）へのトポロジ変更を検出します。
- プリエンプション処理できるポートを選択します。
- 完全なセグメント トポロジを表示します。

非ネイバーエッジサポートは、内部ネイバーがある新しいタイプのエッジを定義できるようにします。 次の図では、P1 および P2 は中間セグメント ポートではなく、非ネイバー エッジ ポートとして設定されます。 これらのポートはエッジポートのプロパティを継承し、上に示されている制約を克服します。 したがって、非ネイバー エッジ ポート（P1 または P2）はマルチ スパニング ツリー（MST）プロトコル、Topology Change Notification（TCN）、および別のセグメントの REP TCN を集約スイッチに送信できます。

図 *10*：非ネイバー エッジ ポートがあるリング トポロジ



REP の設定方法

REP 管理 VLAN の設定

VLAN ロード バランシング中のリンク障害または VLAN ブロッキング通知関連のメッセージ リレーで遅延が起こらないようにするには、REP は通常のマルチキャスト アドレスにハードウェア フラッド レイヤ（HFL）でパケットを大量に送信します。 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。 ドメイン全体の管理 VLAN を設定することで、これらのメッセージのフラッディングを制御することができます。

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。

- ルータとセグメント上には管理 VLAN は 1 つだけとなります。 ただし、これはソフトウェアによって強制的に設定されません。
- 管理 VLAN を設定しない場合、デフォルトは VLAN 1 です。
- インターフェイスで REP を設定するには、REP 管理 VLAN がトランクの EFP カプセル化のリストに含まれていることを確認します。

手順の概要

1. **enable**
2. **configure terminal**
3. **rep admin vlan** *vlan-id*
4. **end**
5. **show interface** [*interface-id*] **rep** [**detail**]
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • 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： `Router# 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	**rep admin vlan** *vlan-id* 例： `Router(config)# rep admin vlan 2`	REP 管理 VLAN を設定します。 • 管理 VLAN を指定します。範囲は 2 ～ 4094 です。デフォルトは VLAN 1 です。
ステップ 4	**end** 例： `Router(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show interface** [*interface-id*] **rep** [**detail**] 例： `Router# show interface gigabitethernet0/1 rep detail`	指定したインターフェイスの REP 設定およびステータスを表示します。 • 物理インターフェイスまたはポート チャネル ID を入力します。
ステップ 6	**copy running-config startup-config** 例： `Router# copy running-config startup-config`	（任意）ルータ 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。

インターフェイスのトランク EFP の設定

はじめる前に

REP 操作の場合、インターフェイスのトランク EFP を設定する必要があります。このタスクは必須で、トランク EFP の REP サポートを設定する前に行う必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **service instance trunk** *service-instance-id* **ethernet**
5. **encapsulation dot1q vlan** *range*
6. **rewrite ingress tag pop 1 symmetric**
7. **bridge-domain from-encapsulation**
8. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • 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： `Router# 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** *type number* 例： `Router(config)# interface GigabitEthernet 0/0/1`	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 ID を入力します。
ステップ 4	**service instance trunk** *service-instance-id* **ethernet** 例： `Router(config-if)# service instance trunk 1 ethernet`	インターフェイス上でサービス インスタンスを設定し、サービス インスタンス 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	**encapsulation dot1q vlan** *range* 例： `Router(config-if-srv)# encapsulation dot1q vlan 10`	インターフェイス上の dot1q フレーム入力を、適切なサービス インスタンスにマッピングするために使用する照合基準を定義します。 • VLAN-ID の範囲は 1 ～ 20 です。
ステップ 6	**rewrite ingress tag pop 1 symmetric** 例： `Router(config-if-srv)# rewrite ingress tag pop 1 symmetric`	サービス インスタンスへのフレーム入力で実行されるカプセル化調整を指定します。
ステップ 7	**bridge-domain from-encapsulation** 例： `Router(config-if-srv)# bridge-domain from-encapsulation`	カプセル化からブリッジ ドメインを取得します。
ステップ 8	**end** 例： `Router (config-if-srv)end`	特権 EXEC モードに戻ります。

トランク EFP の REP サポートの設定

はじめる前に

REP 動作の場合、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 を指定する必要があります。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。その他のステップはすべて任意です。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *interface type number*
4. **rep segment** *segment-id* [**edge** [**primary**]] [**preferred**]
5. **rep stcn** {**interface** *type number* | **segment** *id-list* | **stp**}
6. **rep block port** {**id** *port-id* | *neighbor-offset* | **preferred**} **vlan** {*vlan-list* | **all**}
7. **rep preempt delay** *seconds*
8. **end**
9. **show interface** *type number* **rep** [**detail**]
10. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • 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： `Router# 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 type number* 例： `Router(config)# interface GigabitEthernet 0/0/1`	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 タイプと番号を入力します。

	コマンドまたはアクション	目的
ステップ 4	**rep segment** *segment-id* [**edge** [**primary**]] [**preferred**] 例： `Router(config-if)# rep segment t1 edge preferred`	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。 • （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** 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。 （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。 **show rep topology** 特権 EXEC コマンドを入力すると、セグメントのプライマリ エッジ ポートを指定することができます。 • （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。 （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。
ステップ 5	**rep stcn** {**interface** *type number* | **segment** *id-list* | **stp**} 例： `Router(config-if)# rep stcn segment 2-5`	（任意）エッジ ポートを STCN を送信するように設定します。 • **interface** *type number* キーワードと引数のペアを使用して、STCNを受信するための物理インターフェイスまたはポート チャネルを指定します。 • **segment** *id-list* キーワードと引数のペアを使用して、STCNを受信する 1 つまたは複数のセグメントを識別します。 有効な範囲は 1 ～ 1024 です。 • **stp** を入力して、STCN を STP ネットワークに送信します。

	コマンドまたはアクション	目的
ステップ 6	**rep block port** {**id** *port-id* | *neighbor-offset* | **preferred**} **vlan** {*vlan-list* | **all**} 例： `Router(config-if)# rep block port 0009001818D68700 vlan all`	（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、代替ポートでブロックされるように VLAN を設定します。 • **id** *port-id* キーワードペアを入力して、ポート ID で代替ポートを識別します。 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**] コマンドを入力して、インターフェイス ポート ID を表示できます。 • *neighbor-offset* 番号を入力して、代替ポートをエッジ ポートからのダウンストリーム ネイバーとして特定します。 有効範囲は -256 ～ 256 で、負数はセカンダリ エッジ ポートからのダウンストリーム ネイバーを示します。 値 **0** は無効です。 **-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。 （注） プライマリ エッジ ポート（オフセット番号 1）にこの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。 • **preferred** キーワードを入力して、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* キーワードと引数のペアを入力して、1 つの VLAN または VLAN の範囲をブロックします。 • すべての VLAN をブロックするには、**vlan all** キーワードを入力します。 （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。
ステップ 7	**rep preempt delay** *seconds* 例： `Router(config-if)# rep preempt delay 60`	（任意）プリエンプト遅延時間を設定します。 • 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、遅延時間のない手動によるプリエンプションです。 （注） REP プライマリ エッジ ポート上にだけこのコマンドを使用します。
ステップ 8	**end** 例： `Router(config-if-srv)# 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 9	**show interface** *type number* **rep** [**detail**] 例： `Router# show interface Gigabitethernet0/0/1 rep detail`	（任意）REP インターフェイス コンフィギュレーションを確認します。 • インターフェイス タイプおよび番号と、任意で **detail** キーワードを必要に応じて入力します。
ステップ 10	**copy running-config startup-config** 例： `Router# 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。

VLAN ロード バランシングのプリエンプションの設定

VLAN ロード バランシングのプリエンプションを設定するには、プライマリ エッジ ポートを含むセグメントのあるルータ上で、以下の手順を完了します。

制約事項

プライマリ エッジ ポートでプリエンプション遅延時間を設定する **rep preempt delay** *seconds* コマンドを入力しない場合、デフォルトでは、セグメントでの VLAN ロードバランシングのトリガーは手動になっています。 **show rep topology** コマンドを使用して、セグメント内のどのポートがプライマリ エッジ ポートなのかを確認します。

はじめる前に

VLAN ロード バランシングのプリエンプションを設定する前に、他のすべてのセグメント設定が完了していることを確認してください。 VLAN ロードバランシングのプリエンプションはネットワークを中断する可能性があるため、**rep preempt segment** *segment-id* コマンドを入力した場合、このコマンドの実行前に確認メッセージが表示されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **rep preempt segment** *segment-id*
4. **end**
5. **show rep topology**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • 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： `Router# 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： `Router(config)# rep preempt segment 1`	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。 • セグメント ID を入力します。 （注） コマンドの実行前に、処理の確認を求められます。
ステップ 4	**end** 例： `Router(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show rep topology** 例： `Router# show rep topology`	REP トポロジ情報を表示します。

REP の SNMP トラップ設定

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。

手順の概要

1. **enable**
2. **configure terminal**
3. **snmp mib rep trap-rate** *value*
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • 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： `Router# 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： `Router(config)# snmp mib rep trap-rate 500`	ルータで 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。 • 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。 （注） トラップを削除するには、**no snmp mib rep trap-rate** コマンドを入力します。
ステップ 4	**end** 例： `Router(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： `Router# 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。

	コマンドまたはアクション	目的
ステップ 6	**copy running-config startup-config** 例： `Router# 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 設定のモニタリング

手順の概要

1. **enable**
2. **show interface** [*interface-id*] **rep** [**detail**]
3. **show rep topology** [**segment** *segment-id*] [**archive**] [**detail**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**show interface** [*interface-id*] **rep** [**detail**] 例： `Router# show interface gigabitethernet0/1 rep detail`	（任意）指定したインターフェイスの REP 設定およびステータスを表示します。 • 必要に応じて、物理インターフェイスまたはポート チャネル ID と、オプションの **detail** キーワードを入力します。
ステップ 3	**show rep topology** [**segment** *segment-id*] [**archive**] [**detail**] 例： `Router# show rep topology`	（任意）セグメント内のプライマリおよびセカンダリ エッジ ポートを含む、1 つのセグメントまたは全セグメントの REP トポロジ情報を表示します。 • 必要に応じてオプションのキーワードと引数を入力します。

REP 設定可能タイマーの設定

はじめる前に

REP 操作では、各セグメント インターフェイスで REP をイネーブルにする必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **rep segment** *segment-id* [**edge** [**no-neighbor**] [**primary**]] [**preferred**]
5. **rep stcn** {**interface** *type number* | **segment** *id-list* | **stp**}
6. **rep block port** {**id** *port-id* | *neighbor-offset* | **preferred**} **vlan** {*vlan-list* | **all**}
7. **rep lsl-retries** *number-of-tries*
8. **rep lsl-age-timer** *timer-value*
9. **rep preempt delay** *seconds*
10. **end**
11. **show interface** *type number* **rep** [**detail**]
12. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • 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： `Router# 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** *type number* 例： `Router(config)# interface Gigabitethernet 0/0/1`	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 タイプと番号を入力します。
ステップ 4	**rep segment** *segment-id* [**edge** [**no-neighbor**] [**primary**]] [**preferred**]	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。

	コマンドまたはアクション	目的
	例： `Router(config-if)# rep segment 1 edge preferred`	（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。 • （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）**no-neighbor**：ポートの外部 REP ネイバーを持たないものとしてセグメント エッジを設定します。 • （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。 （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。 **show rep topology** 特権 EXEC コマンドを入力すると、セグメントのプライマリ エッジ ポートを指定することができます。 • （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。 （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。
ステップ 5	**rep stcn** {**interface** *type number* | **segment** *id-list* | **stp**} 例： `Router(config-if)# rep stcn segment 2-5`	（任意）エッジ ポートを STCN を送信するように設定します。 • **interface** *type number* キーワードと引数のペアを使用して、STCN を受信するための物理インターフェイスまたはポート チャネルを指定します。 • **segment** *id-list* キーワードと引数のペアを使用して、STCN を受信する 1 つまたは複数のセグメントを識別します。 有効な範囲は 1 ～ 1024 です。 • STCN を STP ネットワークに送信するために、**stp** キーワードを入力します。

	コマンドまたはアクション	目的
ステップ 6	**rep block port** {**id** *port-id* | *neighbor-offset* | **preferred**} **vlan** {*vlan-list* | **all**} 例： `Router(config-if)# rep block port 0009001818D68700 vlan all`	（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、代替ポートでブロックされるように VLAN を設定します。 • **id** *port-id* キーワードと引数のペアを入力して、ポート ID で代替ポートを識別します。 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**] コマンドを入力して、インターフェイス ポート ID を表示できます。 • *neighbor-offset* 番号を入力して、代替ポートをエッジ ポートからのダウンストリーム ネイバーとして特定します。 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ンストリーム ネイバーを示します。 値 **0** は無効です。 **-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。 （注） プライマリ エッジポート（オフセット番号1）にこの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。 • **preferred** キーワードを入力して、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* キーワードと引数のペアを入力して、1 つの VLAN または VLAN の範囲をブロックします。 • すべての VLAN をブロックするには、**vlan all** キーワードを入力します。 （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。
ステップ 7	**rep lsl-retries** *number-of-tries* 例： `Router(config-if)# rep lsl-retries 3`	LSL によって許容されるリトライ回数を設定します。
ステップ 8	**rep lsl-age-timer** *timer-value* 例： `Router(config-if)# rep lsl-age-timer 200`	障害検出時間を設定します。 • 有効値は 120 ～ 10000 です。 パフォーマンスを考慮して、最小範囲を 200 に設定することを推奨します。
ステップ 9	**rep preempt delay** *seconds*	• （任意）プリエンプト遅延時間を設定します。

	コマンドまたはアクション	目的
	例： `Router(config-if)# rep preempt delay 60`	• 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、遅延時間のない手動によるプリエンプションです。 （注） REP プライマリ エッジ ポート上にだけこのコマンドを使用します。
ステップ 10	**end** 例： `Router(config-if-srv)# end`	特権 EXEC モードに戻ります。
ステップ 11	**show interface** *type number* **rep** [**detail**] 例： `Router# show interface Gigabitethernet0/0/1 rep detail`	（任意）REP インターフェイスの設定を表示します。 • インターフェイス タイプおよび番号と、任意で **detail** キーワードを必要に応じて入力します。
ステップ 12	**copy running-config startup-config** 例： `Router# 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。

非ネイバー エッジ ポートとしての REP の設定

はじめる前に

REP 操作では、各セグメント インターフェイスで REP をイネーブルにする必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **rep segment** *segment-id* [**edge** [**no-neighbor**] [**primary**]] [**preferred**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • 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： `Router# 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** *type number* 例： `Router(config)# interface GigabitEthernet 0/0/1`	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 タイプと番号を入力します。
ステップ 4	**rep segment** *segment-id* [**edge** [**no-neighbor**] [**primary**]] [**preferred**] 例： `Router(config-if)# rep segment 1 edge no-neighbor preferred`	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。 • （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** 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）**no-neighbor**：ポートの外部 REP ネイバーを持たないものとして、セグメント エッジを示します。 • （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。 （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。 **show rep topology** 特権 EXEC コマンドを入力すると、セグメントのプライマリ エッジ ポートを指定することができます。 • （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
		（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。

REP の設定例

REP 管理 VLAN の設定

次に、管理 VLAN を VLAN 100 として設定する例を示します。

```
Router# configure terminal
Router(config)# rep admin vlan 100
Router(config-if)# end
```

トランク EFP の REP サポートの設定

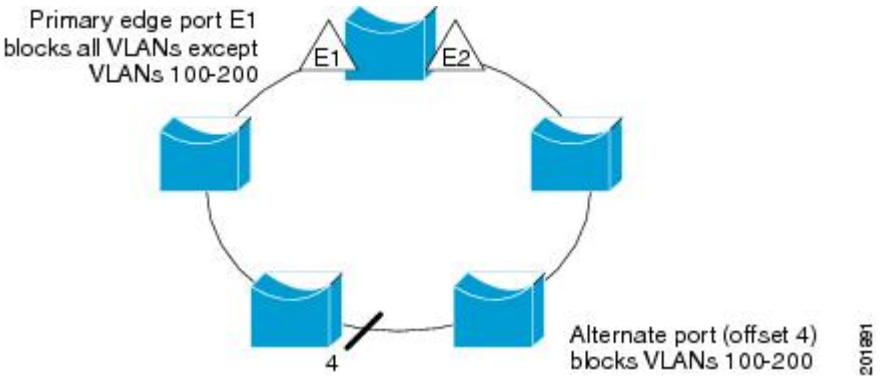
次に、トランク EFP の REP サポートを設定する例を示します。 セグメント 1 のプライマリ エッジ ポートがセグメント 5 を通じて STCN をセグメント 2 に送信するようにインターフェイスを設定し、ポート ID が 0009001818D68700 のポートがセグメント ポート障害とリカバリの後に 60 秒のプリエンプション遅延後、すべての VLAN をブロックするように代替ポートを設定します。

```
Router# configure terminal
Router(config)# interface gigabitethernet0/0/1
Router(config-if)# rep segment 1 edge primary
Router(config-if)# rep stcn segment 2-5
Router(config-if)# rep block port id 0009001818D68700 vlan all
Router(config-if)# rep preempt delay 60
Router(config-if)# service instance trunk 1 ethernet
Router(config-if-srv)# encapsulation dot1q
Router(config-if-srv)# rewrite ingress tag pop 1 symmetric
Router(config-if-srv)# bridge-domain from-encapsulation
Router(config-if-srv)# end
```

次の図に示すように VLAN ブロッキングを設定する方法を示します。 代替ポートは、ネイバー オフセット番号 4 のネイバーです。 手動によるプリエンプションのあとに、VLAN 100 ～ 200 が

このポートでブロックされ、その他のすべての VLAN がプライマリ エッジ ポート E1（ギガビット イーサネット ポート 0/0/1）でブロックされます。

図 *11* : ***VLAN*** ブロッキングの例




```
Router# configure terminal
Router(config)# interface gigabitethernet0/0/1
Router(config-if)# rep segment 1 edge primary
Router(config-if)# rep block port 4 vlan 100-200
Router(config-if)# end
```

VLAN ロード バランシングのプリエンプションの設定

```
Router>end
Router# configure terminal
Router(config)rep preempt segment 1
Router(config)# end
```

REP の SNMP トラップ設定

次の例は、1 秒あたり 10 トラップの割合で REP トラップを送信するようにルータを設定する方法を示します。

```
Router> enable
Router# configure terminal
Router(config)# snmp mib rep trap-rate 10
Router(config)# end
```

REP 設定のモニタリング

次に、**show interface rep detail** コマンドの出力例を示します。 REP インターフェイスの 1 つで **show interface rep detail** コマンドを使用して、REP 設定をモニタして検証します。

```
Router# show interface GigabitEthernet 0/0/1 rep detail

GigabitEthernet0/1 REP enabled
Segment-id: 2 (Edge)
PortID: 00010019E7144680
Preferred flag: No
Operational Link Status: TWO_WAY
```

```
Current Key: 0002001121A2D5800E4D
Port Role: Open
Blocked Vlan: <empty>
Admin-vlan: 100
Preempt Delay Timer: disabled
Load-balancing block port: none
Load-balancing block vlan: none
STCN Propagate to: none
LSL PDU rx: 3322, tx: 1722
HFL PDU rx: 32, tx: 5
BPA TLV rx: 16849, tx: 508
BPA (STCN, LSL) TLV rx: 0, tx: 0
BPA (STCN, HFL) TLV rx: 0, tx: 0
EPA-ELECTION TLV rx: 118, tx: 118
EPA-COMMAND TLV rx: 0, tx: 0
EPA-INFO TLV rx: 4214, tx: 4190
```

REP 設定可能タイマーの設定

```
Router# configure terminal
Router(config)# interface GigabitEthernet 0/0/4
Router(config-if)# rep segment 4 edge preferred
Router(config-if)# rep stcn segment 2-5
Router(config-if)# rep block port 0009001818D68700 vlan all
Router(config-if)# rep lsl-retries 3
Router(config-if)# rep lsl-age-timer 200
Router(config-if)# rep preempt delay
Router(config-if)# exit
Router# show interface GigabitEthernet 0/0/1 rep detail
Router# copy running-config startup-config
```

REP 非ネイバー エッジ サポートの設定

```
Router> enable
Router# configure terminal
Router(config)# interface GigabitEthernet0/2
Router(config-if)# rep segment t1 edge no-neighbor primary
```

その他の関連資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
LAN スイッチング コマンド：コマンド構文、コマンドモード、コマンド履歴、デフォルト、使用上のガイドライン、および例	『Cisco IOS LAN Switching Command Reference』
スパニングツリー プロトコルの概要	『Spanning Tree Protocol (STP)/802.1D』

関連項目	マニュアル タイトル
スパニングツリー PortFast BPDU ガード拡張機能	『Spanning Tree PortFast BPDU Guard Enhancement』

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

Resilient Ethernet Protocol 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。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

表 *13*：*Resilient Ethernet Protocol* の機能情報

機能名	リリース	機能情報
REP 設定可能タイマー	Cisco IOS XE Release 3.5.1S	REP 上の REP 設定可能タイマーは、リング トポロジでのルータ間のリンクでリンク障害を検出します。 Cisco IOS XE Release 3.5.1S では、Cisco ASR 903 ルータのサポートが追加されました。 この機能に関する詳細については、次の各項を参照してください。 REP 設定可能タイマー REP 設定可能タイマーの設定 REP 設定可能タイマーの設定
REP 非ネイバー エッジ サポート	Cisco IOS XE Release 3.5.1S	REP の非ネイバー エッジ サポートは、内部ネイバーがある新しいタイプのエッジを定義できるようにします。 Cisco IOS XE Release 3.5.1S では、Cisco ASR 903 ルータのサポートが追加されました。 REP 非ネイバー エッジ サポート REP 非ネイバー エッジ サポートの設定
トランク EVC の REP サポート	Cisco IOS XE Release 3.5S	REP は、ASR 903 シリーズ ルータのインターフェイス レベルで、トランクのイーサネット フローポイント（EFP）ポートで設定できます。 次のコマンドがこの機能により導入されました。**service instance trunk**。

機能名	リリース	機能情報
REP Fast Hello での SSO サポート	Cisco IOS XE Release 3.5.1S	REP Fast Hello での SSO サポートは、LSL タイムアウト インターバルが経過する前に、hello パケットがアクティブ ルータから送信されることを保障するために提供されます。 Cisco IOS XE Release 3.5.1S では、Cisco ASR 903 ルータのサポートが追加されました。 この機能に関する詳細については、次の各項を参照してください。 REP Fast Hello での SSO サポート