Cisco Nexus 3000 シリーズ NX-OS インターフェイス コンフィギュレーション ガイド リリース 7.x

初版：2015 年 08 月 10 日

最終更新：2016 年 05 月 16 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

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

目 次

第 1 章

新機能および変更された機能に関する情報

この章の内容は、次のとおりです。

このリリースの新規および変更情報

次の表では、このコンフィギュレーション ガイドでの重要な変更点の概要を示します。この表は、このマニュアルのすべての変更点、または特定のリリースのすべての新機能をまとめたリストではありません。

機能	説明	追加または変更されたリリース	参照先
SVI の VRF メンバーシップの変更のサポート	SVI の VRF メンバーシップの変更のサポートが追加されました。	7.0(3)I4(1)	インターフェイスの VRF メンバーシップの変更，（42 ページ）
ポートプロファイルの設定	ポートプロファイルのサポートが追加されました。	7.0(3)I4(1)	ポート プロファイル，（95 ページ）
VXLAN BGP EVPN の設定	VXLAN BGP EVPN の設定のサポートが追加されました。	7.0(3)I4(1)	VXLAN 展開に対する BGP EVPN の考慮事項，（149 ページ）
VXLAN EVPN ファブリックでの IPv6	VXLAN EVPN ファブリックでの IPv6 のサポートが追加されました。	7.0(3)I4(1)	VXLAN EVPN ファブリックでの IPv6 の概要，（181 ページ）

機能	説明	追加または変更されたリリース	参照先
IP アンナンバード	IP アンナンバードコマンドのサポートが追加されました。	7.0(3)I3(1)	IP アンナンバード, （44 ページ） イーサネットインターフェイスでの IP アンナンバードの設定, （53 ページ）
イーサネットインターフェイスの設定に関するガイドライン	イーサネットインターフェイスの設定に関する追加のガイドラインです。	7.0(3)I2(1)	イーサネットインターフェイスの設定に関するガイドライン, （16 ページ）
VXLAN マルチキャストカプセル化パス上の重複ポート	VXLAN マルチキャストカプセル化パスは、vPC ピアのリロード後に重複したポートを持ちます。	7.0(3)I2(1)	VXLAN 導入に関する vPC の注意事項と制約事項, （127 ページ）
portmode を QSFP から SFP+に変更する場合のインターフェイスブレイクアウトの設定	portmode を QSFP から SFP+に変更する場合のインターフェイスブレイクアウトの設定に関する追加情報です。	7.0(3)I2(1)	QSFP ポートと SFP+ ポートの切り替え, （23 ページ）
QSFP ポートでのブレイクアウトの設定に関する running-config の出力の更新	**speed 10000** を使用して QSFP ポートでブレイクアウトを設定すると、running-config の出力に **interface breakout module module number port port range map 10g-4x** が追加されます。	7.0(3)I2(1)	ブレイクアウト 10 ギガビットインターフェイス速度ポートの設定, （22 ページ）

機能	説明	追加または変更されたリリース	参照先
CLI コマンドの **sh vpc brief** の出力の更新	CLI コマンドの **sh vpc brief** の出力に、Delay-restore status と Delay-restore SVI status の 2 つの追加のフィールドが表示されます。	7.0(3)I2(1)	VRF に関する注意事項と制約事項, （198 ページ） VLAN ごとの整合性ステータスの表示, （203 ページ） グレースフル タイプ 1 検査ステータスの表示, （200 ページ） インターフェイス別タイプ 1 不整合の表示, （201 ページ）
LACP 最小リンクのサポート	サポートされる LACP 最小リンクの最大値は 16 です。	7.0(3)I2(1)	LACP ポート チャネルの MinLink の設定, （88 ページ）
ポートを 4x10G モードにブレイクアウトまたは 40G モードにブレイクインするとブレイクアウト ポートが管理上有効な状態になる	ポートを 4x10G モードにブレイクアウトするか 40G モードにブレイクインすると、ブレイクアウト ポートが管理上有効な状態になります。以前のリリースからアップグレードする場合は、復元された設定によって、ポートの適切な管理状態の復元が処理されます。	7.0(3)I2(1)	40 ギガビット イーサネット インターフェイスの速度, （8 ページ）
設定の削除後、VLAN/SVI がレイヤ 3 インターフェイス テーブルから削除されない	設定の削除後、VLAN/SVI はレイヤ 3 インターフェイス テーブルから削除されません。VLAN 自体をレイヤ 3 インターフェイス テーブルから削除する必要があります。	7.0(3)I2(1)	レイヤ 3 インターフェイスの注意事項および制約事項, （44 ページ）

機能	説明	追加または変更されたリリース	参照先
ポートの LACP レートの設定	管理上ダウンしているポートでのみ LACP レートを設定できます。	7.0(3)I2(1)	LACP 高速タイマーレートの設定, （90 ページ）
VXLAN マルチキャスト グループの拡張	拡張された環境で使用されるマルチキャストグループと OIFL の合計数を 1024（マルチキャスト VXLAN VP の現在の範囲）以外にしないことを推奨します。	7.0(3)I2(1)	VXLAN の注意事項と制約事項, （124 ページ）
正規表現および送信元インターフェイス コマンド オプション	正規表現および送信元インターフェイス コマンドオプションに関する追加情報です。	7.0(3)I2(1)	イーサネットインターフェイスの設定に関するガイドライン, （16 ページ）

第 2 章

レイヤ 2 インターフェイスの設定

この章の内容は、次のとおりです。

イーサネット インターフェイスの概要

イーサネット ポートは、サーバまたは LAN に接続される標準のイーサネット インターフェイスとして機能します。

イーサネット インターフェイスはデフォルトでイネーブルです。

インターフェイス コマンド

interface コマンドを使用すれば、イーサネット インターフェイスのさまざまな機能をインターフェイスごとにイネーブルにできます。**interface** コマンドを入力する際には、次の情報を指定します。

- インターフェイス タイプ：物理イーサネットインターフェイスには、常にキーワード **ethernet** を使用します。
- スロット番号：
  - スロット 1 にはすべての固定ポートが含まれます。
  - スロット 2 には上位拡張モジュールのポートが含まれます（実装されている場合）。
  - スロット 3 には下位拡張モジュールのポートが含まれます（実装されている場合）。

◦スロット 4 には下位拡張モジュールのポートが含まれます（実装されている場合）。

- ポート番号：グループ内のポート番号。

Cisco Nexus ファブリック エクステンダとの使用をサポートするために、インターフェイスのナンバリング規則は、次のように拡張されています。

switch(config)# **interfaceethernet** [*chassis*/]*slot*/*port*

- シャーシ ID は、接続されている ファブリック エクステンダのポートをアドレス指定するために使用できる任意のエントリです。インターフェイス経由で検出された ファブリック エクステンダ を識別するために、シャーシ ID はスイッチ上の物理イーサネットまたは EtherChannel インターフェイスに設定されます。シャーシ ID の範囲は、100 ～ 199 です。

UDLD パラメータ

シスコ独自の単一方向リンク検出（UDLD）プロトコルでは、光ファイバまたは銅線（たとえば、カテゴリ 5 のケーブル）のイーサネット ケーブルで接続されているポートでケーブルの物理的な構成をモニタリングし、単一方向リンクの存在を検出できます。スイッチが単方向リンクを検出すると、UDLD は関連する LAN ポートをシャットダウンし、ユーザに警告します。単方向リンクは、スパニングツリー トポロジ ループをはじめ、さまざまな問題を引き起こす可能性があります。

UDLD は、レイヤ 1 プロトコルと協調してリンクの物理ステータスを検出するレイヤ 2 プロトコルです。レイヤ 1 では、物理的シグナリングおよび障害検出は、自動ネゴシエーションによって処理されます。UDLD は、ネイバーの ID の検知、誤って接続された LAN ポートのシャットダウンなど、自動ネゴシエーションでは実行不可能な処理を実行します。自動ネゴシエーションと UDLD の両方をイネーブルにすると、レイヤ 1 とレイヤ 2 の検出が協調して動作して、物理的な単一方向接続と論理的な単一方向接続を防止し、その他のプロトコルの異常動作を防止できます。

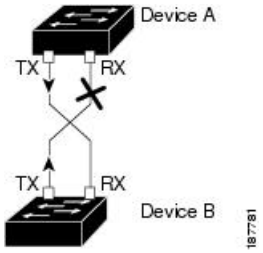
リンク上でローカル デバイスから送信されたトラフィックはネイバーで受信されるのに対し、ネイバーから送信されたトラフィックはローカル デバイスで受信されない場合には常に、単方向リンクが発生します。対になっているファイバ ケーブルのいずれかの接続が切断された場合、自動ネゴシエーションがアクティブであれば、そのリンクは存続できません。この場合、論理リンクは不定であり、UDLD は何の処理も行いません。レイヤ 1 で両方の光ファイバが正常に動作している場合は、レイヤ 2 で UDLD が、これらの光ファイルが正しく接続されているかどうか、および正しいネイバー間でトラフィックが双方向に流れているかを調べます。自動ネゴシエーションはレイヤ 1 で動作するため、このチェックは、自動ネゴシエーションでは実行できません。

Cisco Nexus デバイスは、UDLD がイネーブルになっている LAN ポート上のネイバー デバイスに定期的に UDLD フレームを送信します。一定の時間内にフレームがエコーバックされてきて、特定の確認応答（echo）が見つからなければ、そのリンクは単一方向のフラグが立てられ、その LAN ポートはシャットダウンされます。UDLD プロトコルにより単方向リンクが正しく識別されその使用が禁止されるようにするためには、リンクの両端のデバイスで UDLD がサポートされている必要があります。

次の図は、単方向リンクが発生した状態の一例を示したものです。デバイス B はこのポートでデバイス A からのトラフィックを正常に受信していますが、デバイス A は同じポート上でデバイス

B からのトラフィックを受信していません。UDLD によって問題が検出され、ポートがディセーブルになります。

図 *1*：単方向リンク



UDLD のデフォルト設定

次の表は、UDLD のデフォルト設定を示したものです。

表 *1*：*UDLD* のデフォルト設定

機能	デフォルト値
UDLD グローバル イネーブル ステート	グローバルにディセーブル
UDLD アグレッシブ モード	ディセーブル
ポート別の UDLD イネーブル ステート（光ファイバ メディア用）	すべてのイーサネット光ファイバ LAN ポートでイネーブル
ポート別の UDLD イネーブル ステート（ツイストペア（銅製）メディア用）	すべてのイーサネット 10/100 および 1000BASE-TX LAN ポートでディセーブル

UDLD アグレッシブ モードと非アグレッシブ モード

デフォルトでは、UDLD アグレッシブ モードはディセーブルになっています。UDLD アグレッシブ モードは、UDLD アグレッシブ モードをサポートするネットワーク デバイスの間のポイントツーポイントのリンク上に限って設定できます。UDLD アグレッシブ モードがイネーブルになっている場合、UDLD ネイバー関係が確立されている双方向リンク上のポートが UDLD フレームを受信しなくなったとき、UDLD はネイバーとの接続の再確立を試行します。この再試行に 8 回失敗すると、ポートはディセーブルになります。

スパニングツリー ループを防止するため、間隔がデフォルトの 15 秒である非アグレッシブな UDLD でも、（デフォルトのスパニングツリー パラメータを使用して）ブロッキング ポートがフォワーディング ステートに移行する前に、単方向リンクをシャットダウンすることができます。

UDLD アグレッシブ モードをイネーブルにすると、次のようなことが発生します。

- リンクの一方にポート スタックが生じる（送受信どちらも）
- リンクの一方がダウンしているにもかかわらず、リンクのもう一方がアップしたままになる

このような場合、UDLD アグレッシブ モードでは、リンクのポートの 1 つがディセーブルになり、トラフィックが廃棄されるのを防止します。

Interface Speed

Cisco Nexus 3000 シリーズ スイッチには、固定の 10 ギガビットのポートが多数装備され、各ポートには SFP+ インターフェイス アダプタが装着されています。Cisco Nexus 3100 シリーズ スイッチは、32 個の Quad Same Factor Pluggable（QSFP）ポートと 4 つの SFP+ インターフェイス アダプタを備えています。これらの 32 個のポートのデフォルト速度は 40 Gbps です。

40 ギガビット イーサネット インターフェイスの速度

Cisco Nexus 3132 スイッチおよび Cisco Nexus 3172 スイッチでは、QSFP ポートを 40 ギガビット イーサネット モードまたは 4x10 ギガビット イーサネット モードで動作させることができます。デフォルトでは、40 ギガビット イーサネット モードの 32 個のポートがあります。これらの 40 ギガビット イーサネット ポートには、2 タプルの命名規則で番号が割り当てられます。たとえば、2 番目の 40 ギガビット イーサネット ポートには 1/2 という番号が割り当てられます。40 ギガビット イーサネットから 10 ギガビット イーサネットに設定を変更するプロセスは「ブレイクアウト」と呼ばれ、10 ギガビット イーサネットからギガビット イーサネットに設定を変更するプロセスは「ブレイクイン」と呼ばれます。40 ギガビット イーサネット ポートを 10 ギガビット イーサネット ポートにブレイクアウトする場合、得られたポートには 3 タプルの命名規則を使用して番号が割り当てられます。たとえば、2 番目の 40 ギガビット イーサネット ポートのブレイクアウト ポートには 1/2/1、1/2/2、1/2/3、1/2/4 という番号が割り当てられます。

（注） Release 7.0(3)I2(1) 以降では、ポートを 4x10G モードにブレイクアウトした後、または、ポートを 40G モードにブレイクインした後に、ブレイクアウト ポートが管理上有効な状態になります。以前のリリースからアップグレードする場合は、復元された設定によって、ポートの適切な管理状態の復元が処理されます。

speed 10000 コマンドを使用し、スプリッタ ケーブルで複数のピア スイッチに接続することにより、40 ギガビット イーサネット ポートを 4 個の 10 ギガビット イーサネット ポートにブレイクアウトできます。**speed 40000** コマンドを使用することにより、4 個の 10 ギガビット イーサネット ポートを 40 ギガビット イーサネット ポートにブレイクインできます。40 ギガビット イーサネットから 10 ギガビット イーサネットへ、および 10 ギガビット イーサネットから 40 ギガビット イーサネットへの設定の変更は、すぐに反映されます。スイッチをリロードする必要はありません。QSFP トランシーバ セキュリティ チェックも実行されます。

（注） 40 ギガビット イーサネットから 10 ギガビット イーサネットにブレイクアウトするか、10 ギガビット イーサネットから 40 ギガビット イーサネットにブレイクインすると、すべてのインターフェイス設定がリセットされ、影響を受けるポートは管理上使用できなくなります。これらのポートを使用可能にするには、**no shut** コマンドを使用します。

（注） Release 6.0(2)U5(1) 以降、新しい QSFP+ 40-Gb トランシーバが Cisco Nexus 3000 シリーズ スイッチでサポートされるようになりました。新しい QSFP+（40-Gb）トランシーバは、4 個の 10Gb SFP-10G-LR トランシーバに分岐するケーブルを備えています。これを使用するには、ポートが 4x10G モードである必要があります。ブレークアウト ケーブルを使用する場合は、40G ポートを 4x10G モードで動作させる必要があります。

40 ギガビット イーサネット ポートを 4 個の 10 ギガビット イーサネット ポートに動的にブレイクアウトする機能および 4 個の 10 ギガビット イーサネット ポートを 40 ギガビット イーサネット ポートに動的にブレイクインする機能により、任意のブレイクアウト対応ポートを使用して、それらを永続的に定義することなく、40 ギガビット イーサネット モードまたは 10 ギガビット イーサネット モードを利用できます。

Cisco Nexus 3132Q スイッチでは、イーサネット インターフェイス 1/1 が 40 ギガビット イーサネット モードである場合、最初の QSFP ポートがアクティブになります。ブレイクアウト後は、イーサネット インターフェイス 1/1/1 ～ 4 が 10 ギガビット イーサネット モードである場合、QSFP ポートまたは SFP+ ポートのいずれかを選択できます。ただし、最初の QSFP ポートと 4 個の SFP+ ポートの両方を同時にアクティブにすることはできません。

ポート モード

Cisco Nexus 3100 シリーズ スイッチにはさまざまなポート モードがあります。Cisco NX-OS Release 6.0(2)U(2)1 では、Cisco Nexus 3132Q スイッチにのみ、ブレイクアウトをサポートするポート モードがあります。Cisco NX-OS Release 6.0(2)U(2)3 では、Cisco Nexus 3172PQ スイッチのブレイクアウト ポート モードが導入されました。

（注） 6.0(2)U5(1) より前のリリースでは、Cisco Nexus 3132Q および Cisco Nexus 3132CR シリーズ スイッチのデフォルト モードは Fixed32x40G モードでした。Release 6.0(2)U5(1) 以降では、write erase を実行した後の Cisco Nexus 3132Q および Cisco Nexus 3132CR シリーズ スイッチのデフォルト ポート モードは 32x40G モードです。

（注） 1 つの QSFP to SFP アダプタは 2 つの QSFP ポート（アップおよびダウン）に適合し、8 つの SFP+ インターフェイスを提供します。リリース 7.0(3)I4(1) 以降、QSFP to SFP アダプタを N3K-C3132Q-40GX または N3K-C3132Q-V プラットフォームの最初の 2 ポートに挿入したり、**hardware profile front portmode sfp-plus** コマンドを使用すると、最初の QSFP ポートは非アクティブになり、アダプタへのアクセスは無効になります。そのため、リリース 7.0(3)I4(1) 以降で、QSFP to SFP アダプタがポート 1 および 2 にある場合、**hardware profile front portmode sfp-plus** コマンドを使用しないでください。

Nexus 3100 シリーズ スイッチ	ポート	ポート モード
Cisco Nexus 3132Q	32 個の QSFP ポートおよび 4 個の SFP+ ポート	次のポート モードはブレイクアウトをサポートしています。 • 32x40G：これはオーバーサブスクライブ ポート モードです。32 個のポートはすべて、オーバーサブスクライブされており、最初の 24 個の QSFP ポートがブレイクアウトに対応しています。ポート 25 ~ 32 については **speed 10000** コマンドを入力できません。Release 6.0(2)U5(1) 以降では、32x40G ブレイクアウト モードがデフォルトのポート モードです。 • 26x40G：これはオーバーサブスクライブ ポート モードです。26 個のポートのうちの 12 個はオーバーサブスクライブされていません（カットスルー）。これらのポートは、2、4 ～ 8、14、および 16 ～ 20 です。残りの 14 個のポートはオーバーサブスクライブされています。使用可能なすべての QSFP ポートがブレイクアウトに対応しています。 • 24x40G：これは、非オーバーサブスクライブ（カットスルー）のみのモードです。使用可能なすべての QSFP ポートがブレイクアウトに対応しています。 Fixed32x40G ポート モードはブレイクアウトをサポートしません。

Nexus 3100 シリーズ スイッチ	ポート	ポート モード
Cisco Nexus 3172PQ	6 個の QSFP ポートおよび 48 個の SFP+ ポート	次のポート モードがデフォルトであり、ブレイクアウトをサポートします。 • 48x10G+breakout6x40G 次のポートはブレイクアウトをサポートしない固定ポート モードです。 • 48x10G+6x40G • 72x10G

SVI 自動ステート

スイッチ仮想インターフェイス（SVI）は、デバイスの VLAN のブリッジング機能とルーティング機能間の論理インターフェイスを表します。デフォルトでは、VLAN インターフェイスに複数のポートがある場合、VLAN 内のすべてのポートがダウンすると、SVI はダウン状態になります。

自動ステートの動作は、対応する VLAN のさまざまなポートの状態によって管理されるインターフェイスの動作状態です。VLAN の SVI インターフェイスは、VLAN に STP フォワーディング ステートのポートが少なくとも 1 個ある場合にアップになります。同様に、このインターフェイスは最後の STP 転送ポートがダウンするか、別の STP 状態になったとき、ダウンします。

デフォルトでは、自動ステートの計算はイネーブルです。SVI インターフェイスの自動ステートの計算をディセーブルにし、デフォルト値を変更できます。

（注） Nexus 3000 シリーズ スイッチは、2 つの VLAN の一方の SVI が同じデバイス上にブリッジング リンクとして存在する場合に、それらの VLAN 間のブリッジングをサポートしません。そのデバイスに着信し、その SVI を宛先とするトラフィックは、IPv4 廃棄としてドロップされます。これは、BIA MAC アドレスが、SVI の MAC を変更するオプションを持たない VLAN/SVI 間で共有されるためです。

Cisco Discovery Protocol

Cisco Discovery Protocol（CDP）は、すべてのシスコ デバイス（ルータ、ブリッジ、アクセス サーバ、およびスイッチ）のレイヤ 2（データリンク層）で動作するデバイス検出プロトコルです。ネットワーク管理アプリケーションは CDP を使用することにより、既知のデバイスのネイバーであるシスコ デバイスを検出することができます。また、下位レイヤのトランスペアレント プロトコルが稼働しているネイバー デバイスのデバイス タイプや、簡易ネットワーク管理プロトコル

（SNMP）エージェントアドレスを学習することもできます。この機能によって、アプリケーションからネイバー デバイスに SNMP クエリーを送信できます。

CDP は、サブネットワーク アクセス プロトコル（SNAP）をサポートしているすべてのメディアで動作します。CDP はデータリンク層でのみ動作するため、異なるネットワーク層プロトコルをサポートする 2 つのシステムで互いの情報を学習できます。

CDP が設定された各デバイスはマルチキャストアドレスに定期的にメッセージを送信して、SNMP メッセージを受信可能なアドレスを 1 つまたは複数アドバタイズします。このアドバタイズには、受信側デバイスで CDP 情報を廃棄せずに保持する時間を表す存続可能時間、つまりホールドタイム情報も含まれます。各デバイスは他のデバイスから送信されたメッセージも待ち受けて、ネイバー デバイスについて学習します。

このスイッチは、CDP バージョン 1 とバージョン 2 の両方をサポートします。

CDP のデフォルト設定

次の表は、CDP のデフォルト設定を示したものです。

表 *2*：*CDP* のデフォルト設定

機能	デフォルト設定
CDP インターフェイス ステート	イネーブル
CDP タイマー（パケット更新頻度）	60 秒
CDP ホールドタイム（廃棄までの時間）	180 秒
CDP バージョン 2 アドバタイズ	イネーブル

error-disabled ステート

インターフェイスが（**no shutdown** コマンドを使用して）管理上イネーブルであるが、プロセスによってランタイム時にディセーブルになる場合、そのインターフェイスは error-disabled（err-disabled）ステートです。たとえば、UDLD が単方向リンクを検出した場合、そのインターフェイスは実行時にシャットダウンされます。ただし、インターフェイスは管理上イネーブルなので、インターフェイス ステータスは err-disabled として表示されます。いったん err-disabled ステートになったインターフェイスは、手動でイネーブルにする必要があります。ただし、自動回復までのタイムアウト値を設定することもできます。err-disabled 検出はすべての原因に対してデフォルトでイネーブルです。自動回復はデフォルトでは設定されていません。

インターフェイスが errdisable ステートになった場合は、**errdisable detect cause** コマンドを使用して、そのエラーに関する情報を取得してください。

time 変数の変更によって起きる特定の err-disabled に対しては自動 err-disabled リカバリ タイムアウトを設定できます。

errdisable recovery cause コマンドを使用すると、300 秒後に自動回復します。回復までの時間を変更する場合は、**errdisable recovery interval** コマンドを使用して、タイムアウト時間を指定します。指定できる値は 30 ～ 65535 秒です。

errdisabled ステートからインターフェイスのリカバリをディセーブルにするには、**no errdisable recovery cause** コマンドを使用します。

errdisable recover cause コマンドには、以下のようなさまざまなオプションがあります。

- all：すべての原因からタイマーが回復できるようにします。
- bpduguard：ブリッジ プロトコル データ ユニット（BPDU）ガードの error-disabled ステートからタイマーが回復できるようにします。
- failed-port-state：スパニングツリープロトコル（STP）のポート状態設定障害からタイマーが回復できるようにします。
- link-flap：リンクステート フラッピングからタイマーが回復できるようにします。
- pause-rate-limit：ポーズ レート リミットの error-disabled ステートからタイマーが回復できるようにします。
- udld：単方向リンク検出（UDLD）の error-disabled ステートからタイマーが回復できるようにします。
- loopback：ループバックの error-disabled ステートからタイマーが回復できるようにします。

原因に対する err-disabled 回復をイネーブルにしない場合、そのインターフェイスは **shutdown** コマンドおよび **no shutdown** コマンドが入力されるまで err-disabled ステートのままです。原因に対して回復をイネーブルにすると、そのインターフェイスの errdisable ステートは解消され、すべての原因がタイムアウトになった段階で動作を再試行できるようになります。エラーの原因を表示する場合は、**show interface status err-disabled** コマンドを使用します。

デフォルト インターフェイス

デフォルト インターフェイス機能を使用して、イーサネット、ループバック、管理、VLAN、およびポートチャネルインターフェイスなどの物理インターフェイスおよび論理インターフェイスの両方に対する設定済みパラメータを消去できます。

デバウンス タイマー パラメータ

デバウンス タイマーを設定するとリンク変更の通知が遅くなり、ネットワークの再設定によるトラフィック損失が減少します。デバウンスタイマーはイーサネットポートごとに個別に設定します。遅延時間はミリ秒単位で指定できます。遅延時間の範囲は 0～5000 ミリ秒です。デフォルトでは、このパラメータはデバウンス タイマーが作動しない 100 ミリ秒に設定されています。このパラメータが 0 ミリ秒に設定されると、デバウンス タイマーがディセーブルです。

注意 デバウンス タイマーをイネーブルにするとリンクダウン検出が遅くなり、デバウンス期間中のトラフィックが失われます。この状況は、一部のレイヤ 2 とレイヤ 3 プロトコルのコンバージェンスと再コンバージェンスに影響する可能性があります。

MTU 設定

Cisco Nexus デバイス スイッチは、フレームをフラグメント化しません。そのためスイッチでは、同じレイヤ 2 ドメイン内の 2 つのポートに別々の最大伝送単位（MTU）を設定することはできません。物理イーサネット インターフェイス別 MTU はサポートされていません。代わりに、MTU は QoS クラスに従って設定されます。クラス マップとポリシー マップを設定して、MTU を変更します。

（注） インターフェイス設定を表示すると、物理イーサネット インターフェイスのデフォルト MTU は 1500 と表示されます。

カウンタの値

設定、パケット サイズ、増加するカウンタの値、およびトラフィックに関する次の情報を参照してください。

設定	パケット サイズ	増加するカウンタ	Traffic
L2 ポート：MTU 設定なし	6400 および 10000	ジャンボ、Giant、および入力エラー	Dropped
L2 ポート：ネットワーク QoS 設定にジャンボ MTU 9216 あり	6400	Jumbo	Forwarded
L2 ポート：ネットワーク QoS 設定にジャンボ MTU 9216 あり	10000	ジャンボ、Giant、および入力エラー	Dropped
レイヤ 3 ポート：ネットワーク QoS 設定にデフォルト レイヤ 3 MTU およびジャンボ MTU 9216 あり	6400	Jumbo	パケットは、CPU にパントされ（CoPP 設定の対象）、断片化された後に、ソフトウェアによって転送される。

設定	パケット サイズ	増加するカウンタ	Traffic
レイヤ 3 ポート：ネットワーク QoS 設定にデフォルト レイヤ 3 MTU およびジャンボ MTU 9216 あり	6400	Jumbo	パケットは、CPU にパントされ（CoPP 設定の対象）、断片化された後に、ソフトウェアによって転送される。
レイヤ 3 ポート：ネットワーク QoS 設定にデフォルト レイヤ 3 MTU およびジャンボ MTU 9216 あり	10000	ジャンボ、Giant、および入力エラー	Dropped
レイヤ 3 ポート：ネットワーク QoS 設定にジャンボ レイヤ 3 MTU およびジャンボ MTU 9216 あり	6400	Jumbo	断片化なしで転送される。
レイヤ 3 ポート：ネットワーク QoS 設定にジャンボ レイヤ 3 MTU およびジャンボ MTU 9216 あり	10000	ジャンボ、Giant、および入力エラー	Dropped
レイヤ 3 ポート：ジャンボ レイヤ 3 MTU およびデフォルト L2 MTU 設定あり	6400 および 10000	ジャンボ、Giant、および入力エラー	Dropped

（注）

- 適切な CRC を持つ 64 バイト未満のパケット：ショート フレーム カウンタが増加します。
- 不適切な CRC を持つ 64 バイト未満のパケット：ラント カウンタが増加します。
- 不適切な CRC を持ち 64 バイトを超えるパケット：CRC カウンタが増加します。

ダウンリンク遅延

Cisco Nexus 3048 スイッチのリロード後、ダウンリンク RJ-45 ポートの前にアップリンク SFP+ ポートを動作上有効にできます。SFP+ ポートが有効になるまで、ハードウェアの RJ-45 ポートの有効化を遅延させる必要があります。

リロード時に、指定されたタイムアウト時間が経過した後にのみハードウェアのダウンリンク RJ-45 ポートを有効にするタイマーを設定できます。このプロセスにより、アップリンク SFP+ ポートを最初に使用可能にすることができます。このタイマーは、管理上有効なポートについてのみ、ハードウェアで有効になります。

ダウンリンク遅延はデフォルトでは無効になっており、明示的に有効にする必要があります。有効になっている場合、遅延タイマーが指定されないと、デフォルトの 20 秒の遅延に設定されます。

物理イーサネットのデフォルト設定

次の表に、すべての物理イーサネット インターフェイスのデフォルト設定を示します。

パラメータ	デフォルト設定
Duplex	オート（全二重）
カプセル化	ARPA
MTU[1]	1500 バイト
Port Mode	アクセス
速度	オート（10000）

[1] MTU を物理イーサネット インターフェイスごとに変更することはできません。MTU の変更は、QoS クラスのマップを選択することにより行います。

イーサネット インターフェイスの設定

イーサネット インターフェイスの設定に関するガイドライン

Release 7.0(3)I2(1) 以降では、Cisco Nexus 3000 シリーズ スイッチでのインターフェイス イーサネット コマンドの設定における動作の変更があります。たとえば、**sh int ethernet Eth1/1 transceiver** コマンドは機能しなくなりました。このコマンドは **sh int ethernet 1/1 transceiver** と設定する必要があります。

UDLD モードの設定

単一方向リンク検出（UDLD）を実行するように設定されているデバイス上のイーサネット インターフェイスには、ノーマル モードまたはアグレッシブ モードの UDLD を設定できます。インターフェイスの UDLD モードをイネーブルにするには、そのインターフェイスを含むデバイス上で UDLD を事前にイネーブルにしておく必要があります。UDLD は他方のリンク先のインターフェイスおよびそのデバイスでもイネーブルになっている必要があります。

ノーマル UDLD モードを使用するには、ポートの 1 つをノーマル モードに設定し、他方のポートをノーマル モードまたはアグレッシブ モードに設定する必要があります。アグレッシブ UDLD モードを使用するには、両方のポートをアグレッシブ モードに設定する必要があります。

（注） 設定前に、リンクされている他方のポートとそのデバイスの UDLD をイネーブルにしておかなければなりません。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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 2	switch(config)# **feature udld**	デバイスの UDLD をイネーブルにします。
ステップ 3	switch(config)# **no feature udld**	デバイスの UDLD をディセーブルにします。
ステップ 4	switch(config)# **show udld global**	デバイスの UDLD ステータスを表示します。
ステップ 5	switch(config)# **interface***typeslot*/*port*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 6	switch(config-if)# **udld** {**enable** | **disable** | **aggressive**}	ノーマル UDLD モードをイネーブルにするか、UDLD をディセーブルにするか、またはアグレッシブ UDLD モードをイネーブルにします。
ステップ 7	switch(config-if)# **show udld***interface*	インターフェイスの UDLD ステータスを表示します。

次の例は、スイッチの UDLD をイネーブルにする方法を示しています。

```
switch# configure terminal
switch(config)# feature udld
```

次の例は、イーサネット ポートのノーマル UDLD モードをイネーブルにする方法を示しています。

```
switch# configure terminal
switch(config)# interface ethernet 1/4
switch(config-if)# udld enable
```

次の例は、イーサネット ポートのアグレッシブ UDLD モードをイネーブルにする方法を示しています。

```
switch# configure terminal
switch(config)# interface ethernet 1/4
switch(config-if)# udld aggressive
```

次の例は、イーサネット ポートの UDLD をディセーブルにする例を示しています。

```
switch# configure terminal
switch(config)# interface ethernet 1/4
switch(config-if)# udld disable
```

次の例は、スイッチの UDLD をディセーブルにする方法を示しています。

```
switch# configure terminal
switch(config)# no feature udld
```

リンク ステート整合性チェッカのトリガー

リンク ステート整合性チェッカを手動でトリガーして、インターフェイスのハードウェアおよびソフトウェア リンク ステータスを比較し、その結果を表示することができます。リンク ステート整合性チェッカを手動でトリガーして結果を表示するには、次のコマンドを特定のモードで使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **show consistency-checker link-state module***slot*	指定されたモジュールのリンク ステート整合性検査を開始し、その結果を表示します。

次に、リンク ステート整合性検査をトリガーして結果を表示する例を示します。

```
switch# show consistency-checker link-state module 1
Link State Checks: Link state only
Consistency Check: FAILED
No inconsistencies found for:
   Ethernet1/1
   Ethernet1/2
   Ethernet1/3
   Ethernet1/4
   Ethernet1/5
   Ethernet1/6
   Ethernet1/7
   Ethernet1/8
```

```
   Ethernet1/9
   Ethernet1/10
   Ethernet1/12
   Ethernet1/13
   Ethernet1/14
   Ethernet1/15
Inconsistencies found for following interfaces:
   Ethernet1/11
```

インターフェイスのポート モードの変更

hardware profile*portmode* コマンドを使用して、Quad Small Form-Factor Pluggable（QSFP+）ポートを設定できます。デフォルトに戻す場合は、これらのコマンドの **no** 形式を使用します。Cisco Nexus 3172PQ スイッチのデフォルト ポート モードは、48x10g+breakout6x40g です。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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 2	switch(config)# **copy running-configbootflash**: *my-config.cfg*	実行コンフィギュレーションをブートフラッシュにコピーします。このファイルは、後でデバイスの設定を行う際に使用することができます。
ステップ 3	switch(config)# **write erase**	インターフェイス設定をすべて削除します。
ステップ 4	switch(config)# **reload**	Cisco NX-OS ソフトウェアをリロードします。
ステップ 5	switch(config)# [**no**] **hardware profile portmode***portmode*	インターフェイスのポート モードを変更します。
ステップ 6	switch(config)# **hardware profile portmode***portmode***2-tuple**	（任意） デフォルトの 3 タプル規則モードではなく、2 タプル モードでポート名を表示します。
ステップ 7	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。
ステップ 8	switch(config)# **reload**	Cisco NX-OS ソフトウェアをリロードします。 すべてのインターフェイス設定を手動で適用します。以前に保存したコンフィギュレーション ファイルを参照することもできます。 （注） ポートが 40G モードから 4x10G モードに、またはその逆に変更されると、インターフェイスのナンバリングが変更されます。

	コマンドまたはアクション	目的

次に、QSFP+ ポートのポート モードを 48x10g+breakout6x40g に変更する例を示します。

```
switch# configure terminal
switch(config)# copy running-config bootflash:my-config.cfg
switch(config)# write erase
switch(config)# reload
WARNING: This command will reboot the system
Do you want to continue? (y/n) [n] y
switch(config)# hardware profile portmode 48x10g+breakout6x40g
Warning: This command will take effect only after saving the configuration and reload!
Port configurations could get lost when port mode is changed!
switch(config)# copy running-config startup-config
switch(config)# reload
WARNING: This command will reboot the system
Do you want to continue? (y/n) [n] y
```

次の例は、QSFP+ ポートのポート モードを 48x10g+4x40g に変更する方法を示したものです。

```
switch# configure terminal
switch(config)# copy running-config bootflash:my-config.cfg
switch(config)# write erase
switch(config)# reload
WARNING: This command will reboot the system
Do you want to continue? (y/n) [n] y
switch(config)# hardware profile portmode 48x10g+4x40g
Warning: This command will take effect only after saving the configuration and reload!
Port configurations could get lost when port mode is changed!
switch(config)# copy running-config startup-config
switch(config)# reload
WARNING: This command will reboot the system
Do you want to continue? (y/n) [n] y
```

次の例は、QSFP+ ポートのポート モードを 48x10g+4x40g に変更し、その変更内容を確認する方法を示したものです。

```
switch# configure terminal
switch(config)# hardware profile portmode 48x10g+4x40g
Warning: This command will take effect only after saving the configuration and r
eload! Port configurations could get lost when port mode is changed!
switch(config)# show running-config
!Command: show running-config
!Time: Thu Aug 25 07:39:37 2011
version 5.0(3)U2(1)
feature telnet
no feature ssh
feature lldp
username admin password 5 $1$OOV4MdOM$BAB5RkD22YanT4empqqSM0 role network-admin
ip domain-lookup
switchname BLR-QG-5
ip access-list my-acl
10 deny ip any 10.0.0.1/32
20 deny ip 10.1.1.1/32 any
class-map type control-plane match-any copp-arp
class-map type control-plane match-any copp-bpdu
:
:
control-plane
service-policy input copp-system-policy
hardware profile tcam region arpacl 128
hardware profile tcam region ifacl 256
hardware profile tcam region racl 256
hardware profile tcam region vacl 512
hardware profile portmode 48x10G+4x40G
snmp-server user admin network-admin auth md5 0xdd1d21ee42e93106836cdefd1a60e062
```

```
<--Output truncated-->
switch#
```

次の例は、QSFP+ ポートのポート モードをデフォルトに戻す方法を示したものです。

```
switch# configure terminal
switch(config)# no hardware profile portmode
Warning: This command will take effect only after saving the configuration and r
eload! Port configurations could get lost when port mode is changed!
switch(config)#
```

インターフェイス速度の設定

（注） インターフェイスとトランシーバの速度が一致しない場合に **show interface ethernet***slot*/*port* コマンドを入力すると、SFP 検証失敗メッセージが表示されます。たとえば、**speed 1000** コマンドを設定せずに 1 ギガビット SFP トランシーバをポートに挿入すると、このエラーが発生します。デフォルトでは、すべてのポートが 10 Gbps です。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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 2	switch(config)# **interface***typeslot*/*port*	指定したインターフェイスに対してインターフェイス コンフィギュレーション モードを開始します。このインターフェイスに、1 ギガビット イーサネット SFP トランシーバが挿入されている必要があります。
ステップ 3	switch(config-if)# **speed***speed*	インターフェイスの速度を設定します。 このコマンドは、物理的なイーサネット インターフェイスにしか適用できません。*speed* 引数には次のいずれかを設定できます。 • 10 Mbps • 100 Mbps • 1 Gbps • 10 Gbps • automatic

次に、1 ギガビット イーサネット ポートの速度を設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/4
switch(config-if)# speed 1000
```

ブレイクアウト 10 ギガビット インターフェイス速度ポートの設定

デフォルトでは、Cisco Nexus 3132 スイッチ上のすべてのポートは 40 ギガビット イーサネットです。40 ギガビット イーサネット ポートを 4 個の 10 ギガビット イーサネット ポートにブレイクアウトできます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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 2	switch(config)# **interface***typeslot/port-range*	指定したインターフェイスに対してインターフェイス コンフィギュレーション モードを開始します。 （注） 40 ギガビット イーサネット インターフェイスに関しては、インターフェイス範囲はサポートされません。たとえば、Eth 1/2 ～ 5 はサポートされません。
ステップ 3	switch(config-if)# **speed 10000**	インターフェイスの速度を10 ギガビット/秒に設定します。 （注） **speed 10000** を使用して QSFP ポートでブレイクアウトを設定すると、running-config の出力に **interface breakout module <module number> port <port range> map 10g-4x** が追加されます。

次に、イーサネット インターフェイス 1/2 の速度を 10 ギガビット/秒に設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/49
switch(config-if)# speed 10000

switch(config-if)# sh running-config | grep port
  limit-resource port-channel minimum 0 maximum 511
interface breakout module 1 port 49 map 10g-4x ----------------------------------------->
 interface breakout is added on "speed" config
hardware profile portmode 48x10g+breakout6x40g
(config-if)#

(config)# int ethernet 1/49/1
(config-if)#no speed 10000 ----------------------------------> on "no speed", the interface
 breakout cmd is removed.

(config-if)#  sh running-config | grep port
```

```
  limit-resource port-channel minimum 0 maximum 511
hardware profile portmode 48x10g+breakout6x40g
```

ブレイクイン 40 ギガビット イーサネット インターフェイス速度ポートの設定

4 個の 10 ギガビット イーサネット ポートを 40 ギガビット イーサネット ポートにブレイクインできます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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 2	switch(config)# **interface***typeslot/port*	指定したインターフェイスに対してインターフェイス コンフィギュレーション モードを開始します。 （注） 10 ギガビット イーサネット インターフェイスに関しては、インターフェイス範囲がサポートされます。たとえば、Eth 1/2/1 ～ 4 はサポートされます。
ステップ 3	switch(config-if)# **speed 40000**	インターフェイスの速度を 40 Gbps に設定します。

次に、イーサネット インターフェイス 1/2/1 の速度を 40 Gbps に設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/2/1
switch(config-if)# speed 40000
```

QSFP ポートと SFP+ ポートの切り替え

ポートを 10-GbE モードにブレイクアウトする場合、最初の QSFP ポートと SFP+ ポート 1 ～ 4 を切り替えることができます。最初の QSFP ポートまたは 4 個の SFP+ ポートのいずれかを、いつでもアクティブにできます。QSFP は、インターフェイス速度が 40 Gbps のデフォルト ポートです。

最初の QSFP ポートが 40-GbE モードの場合、ポートを 4 個の SFP+ ポートに切り替えることはできず、ポートを 10-GbE モードにブレイクアウトするまで最初の QSFP ポートはアクティブです。これは、SFP+ ポートが 40-GbE モードをサポートしないためです。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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 2	switch(config)# **[no] hardware profile front portmodeqsfp** | **sfp-plus**	指定されたポート モードをアクティブにします。 • **qsfp**：前面パネルの QSFP ポートがアクティブです。 • **sfp-plus**：前面パネルの SFP+ ポート 1 ～ 4 がアクティブです。 このコマンドの **no** 形式を使用すると、QSFP ポートがアクティブになります。 （注） 最初の QSFP ポートの速度が 40 Gbps である場合、このコマンドは実行されますが、速度が 10 Gbps に変更されるまで SFP+ ポートはアクティブになりません。
ステップ 3	switch(config)# **interface breakout module***module number***port***port range***map 10g-4x**	モジュールを 10g モードで設定できるようにします。ポート モードを QSFP から SFP+ に変更する場合、**hardware profile front portmode** コマンドは、このコマンドに表示されている 最初の QSFP ポートがブレイクアウトされた後にのみ有効になります。
ステップ 4	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

次に、ポート モードを QSFP から SFP+ に変更する例を示します。

```
switch# show int e1/1 tranceiver
Ethernet1/1
transceiver is present
type is QSFP-40G-SR
name is CISCO
part number is AFBR-79EIPZ-CS1
revision is 02
serial number is AVP1645S1QT
nominal bitrate is 10300 MBit/sec per channel
Link length supported for 50/125um fiber is 30 m
Link length supported for 50/125um fiber is 100 m
cisco id is --
cisco extended id number is 16

switch# show running-config | inc portmode
hardware profile portmode 32X40G
hardware profile front portmode qsfp

switch# configure terminal
```

```
switch(config)# hardware profile front portmode sfp-plus
switch(config)# interface breakout module 1 port 1 map 10g-4x
switch(config)# copy running-config startup-config
```

次に、QSFP ポートをアクティブにする例を示します。

```
switch# configure terminal
switch(config)# no hardware profile front portmode
switch(config)# copy running-config startup-config
```

リンク ネゴシエーションのディセーブル化

デフォルトでは、自動ネゴシエーションはすべての 1G SFP+ および 40G QSFP ポートではイネーブル、10G SFP+ ポートではディセーブルです。自動ネゴシエーションは、デフォルトで、すべての 1G および 10G Base-T ポートでイネーブルです。1G および 10G Base-T ポートではディセーブルにできません。

このコマンドは、Cisco IOS の **speed non-negotiate** コマンドに相当します。

（注） 自動ネゴシエーションの設定は、10 ギガビット イーサネット ポートには適用されません。自動ネゴシエーションを 10 ギガビット ポートに設定すると、次のエラー メッセージが表示されます。

```
ERROR: Ethernet1/40: Configuration does not match the port capability
```

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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 2	switch(config)# **interface ethernet** *slot*/*port*	インターフェイスを選択し、インターフェイス モードを開始します。
ステップ 3	switch(config-if)# **no negotiate auto**	選択したイーサネット インターフェイス（1 ギガビット ポート）に対してリンク ネゴシエーションをディセーブルにします。
ステップ 4	switch(config-if)# **negotiate auto**	（任意） 選択したイーサネット インターフェイスに対してリンク ネゴシエーションをイネーブルにします。1 ギガビット イーサネット ポートに対してはデフォルトでイネーブルです。 （注） このコマンドは、10GBase-T ポートには適用できません。このコマンドを 10GBase-T ポートでは使用しないでください。

次に、指定したイーサネット インターフェイス（1 ギガビット ポート）で自動ネゴシエーションをディセーブルにする例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/1
switch(config-if)# no negotiate auto
switch(config-if)#
```

次に、指定したイーサネット インターフェイス（1 ギガビット ポート）で自動ネゴシエーションをイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/5
switch(config-if)# negotiate auto
switch(config-if)#
```

SVI 自動ステートのディセーブル化

対応する VLAN でインターフェイスが稼働していなくても、SVI がアクティブのままになるように設定できます。この機能拡張は自動ステートのディセーブル化と呼ばれます。

自動ステートの動作を有効または無効にすると、SVI ごとに自動ステートを設定しない限り、スイッチのすべての SVI に適用されます。

（注） 自動ステートの動作はデフォルトでイネーブルです。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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 2	switch(config)# **feature interface-vlan**	インターフェイス VLAN 機能をイネーブルにします。
ステップ 3	switch(config)# **system default interface-vlan** [**no**] **autostate**	自動ステートのデフォルト動作をイネーブルまたはディセーブルにするようにシステムを設定します。
ステップ 4	switch(config)# **interface vlan** *interface-vlan-number*	（任意） VLAN インターフェイスを作成します。number の範囲は 1 ～ 4094 です。
ステップ 5	switch(config-if)# [**no**] **autostate**	（任意） SVI ごとに自動ステートの動作をイネーブルまたはディセーブルにします。

	コマンドまたはアクション	目的
ステップ 6	switch(config)# **show interface-vlan** *interface-vlan*	（任意） SVI のイネーブルまたはディセーブルになっている自動ステートの動作を表示します。
ステップ 7	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

次に、スイッチのすべての SVI に対してシステムの自動ステートのデフォルトをディセーブルにする例を示します。

```
switch# configure terminal
switch(config)# feature interface-vlan
switch(config)# system default interface-vlan no autostate
switch(config)# interface vlan 50
switch(config-if)# no autostate
switch(config)# copy running-config startup-config
```

次に、システムの自動ステート設定を有効にする例を示します。

```
switch(config)# show interface-vlan 2
Vlan2 is down, line protocol is down, autostate enabled
Hardware is EtherSVI, address is 547f.ee40.a17c
MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec
```

デフォルト インターフェイスの設定

デフォルト インターフェイス機能によって、イーサネット、ループバック、管理、VLAN、およびポートチャネルインターフェイスなどの複数インターフェイスの既存コンフィギュレーションを消去できます。特定のインターフェイスでのすべてのユーザ コンフィギュレーションは削除されます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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 2	switch(config)# **default interface***typeinterface number*	インターフェイスの設定を削除しデフォルトの設定を復元します。サポートされるインターフェイスは次のとおりです。 • **ethernet** • **loopback**

	コマンドまたはアクション	目的
		• **mgmt** • **port-channel** • **vlan**
ステップ 3	switch(config)# **exit**	グローバル コンフィギュレーション モードを終了します。

次に、イーサネット インターフェイスの設定を削除し、デフォルト設定に戻す例を示します。

```
switch# configure terminal
switch(config)# default interface ethernet 1/3
.......Done
switch(config)# exit
```

CDP の特性の設定

Cisco Discovery Protocol（CDP）更新の頻度、情報を廃棄するまでの保持期間、およびバージョン 2 アドバタイズを送信するかどうかを設定することができます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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 2	switch(config)# [**no**] **cdp advertise** {**v1** | **v2** }	（任意） 使用するバージョンを設定して、CDP アドバタイズメントを送信します。バージョン 2 がデフォルト ステートです。 デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。
ステップ 3	switch(config)# [**no**] **cdp format device-id** {**mac-address** | **serial-number** | **system-name**}	（任意） CDP デバイス ID のフォーマットを設定します。デフォルトはシステム名です。完全修飾ドメイン名で表すことができます。 デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

	コマンドまたはアクション	目的
ステップ 4	switch(config)# [**no**] **cdp holdtime***seconds*	（任意） デバイスから送信された情報が受信デバイスで破棄されるまでの保持時間を指定します。指定できる範囲は 10 ～ 255 秒です。デフォルトは 180 秒です。 デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。
ステップ 5	switch(config)# [**no**] **cdp timer***seconds*	（任意） CDP アップデートの送信頻度を秒単位で設定します。指定できる範囲は 5 ～ 254 です。デフォルトは 60 秒です。 デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

次の例は、CDP 特性を設定する方法を示しています。

```
switch# configure terminal
switch(config)# cdp timer 50
switch(config)# cdp holdtime 120
switch(config)# cdp advertise v2
```

CDP のイネーブル化/ディセーブル化

CDP をイーサネット インターフェイスに対してイネーブルにしたり、ディセーブルにしたりできます。このプロトコルは、同一リンクの両方のインターフェイスでイネーブルになっている場合にだけ機能します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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 2	switch(config)# **interface***typeslot*/*port*	指定したインターフェイスに対してインターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# **cdp enable**	インターフェイスに対して CDP をイネーブルにします。 正常に機能するには、このパラメータが同一リンク上の両方のインターフェイスでイネーブルになっている必要があります。

	コマンドまたはアクション	目的
ステップ 4	switch(config-if)# **no cdp enable**	インターフェイスに対して CDP をディセーブルにします。

次に、イーサネット ポートに対して CDP をイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/4
switch(config-if)# cdp enable
```

このコマンドは、物理的なイーサネット インターフェイスにしか適用できません。

errdisable ステート検出のイネーブル化

アプリケーションでの errdisable ステート検出をイネーブルにすることができます。その結果、原因がインターフェイスで検出された場合、インターフェイスは err-disabled ステート（リンクダウン ステートに類似した動作ステート）となります。

（注） Cisco Nexus 5020 または 5010 スイッチと同様のポーズ レート制限により、Cisco Nexus 5500 の基本ポートは error disabled になりません。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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 2	switch(config)# **errdisable detect cause** {*all* | *link-flap* | *loopback*}	インターフェイスを err-disabled ステートにする条件を指定します。デフォルトではイネーブルになっています。
ステップ 3	switch(config)# **shutdown**	インターフェイスを管理的にダウンさせます。インターフェイスを err-disabled ステートから手動で回復させるには、最初にこのコマンドを入力します。
ステップ 4	switch(config)# **no shutdown**	インターフェイスを管理上アップにし、err-disabled ステートから手動で回復できるようにします。
ステップ 5	switch(config)# **show interface status err-disabled**	err-disabled ステートにあるインターフェイスについての情報を表示します。

	コマンドまたはアクション	目的
ステップ 6	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

次に、すべての場合に err-disabled 検出をイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# errdisable detect cause all
switch(config)# shutdown
switch(config)# no shutdown
switch(config)# show interface status err-disabled
switch(config)# copy running-config startup-config
```

errdisable ステート回復のイネーブル化

アプリケーションを指定してインターフェイスを error-disabled（err-disabled）ステートから抜け出させ、稼働を再試行できます。回復タイマーを設定しない限り、300 秒後にリトライします（**errdisable recovery interval** コマンドを参照）。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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 2	switch(config)# **errdisable recovery cause** {*all* | *udld* | *bpduguard* | *link-flap* | *failed-port-state* | *pause-rate-limit* | *loopback*}	インターフェイスが err-disabled ステートから自動的に回復し、デバイスがそのインターフェイスを再びアップ状態にする条件を指定します。デバイスは 300 秒待機してからリトライします。デフォルトではディセーブルになっています。
ステップ 3	switch(config)# **show interface status err-disabled**	err-disabled ステートにあるインターフェイスについての情報を表示します。
ステップ 4	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

次に、すべての条件下で err-disabled リカバリをイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# errdisable recovery cause loopback
switch(config)# show interface status err-disabled
switch(config)# copy running-config startup-config
```

errdisable ステート回復間隔の設定

下記の手順により、errdisable ステート回復のタイマー値を設定することができます。有効な範囲は 30 ～ 65535 秒です。デフォルトは 300 秒です。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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 2	switch(config)# **errdisable recovery interval***interval*	インターフェイスが errdisable ステートから回復する間隔を指定します。有効な範囲は 30 ～ 65535 秒です。デフォルトは 300 秒です。
ステップ 3	switch(config)# **show interface status err-disabled**	errdisable ステートにあるインターフェイスについての情報を表示します。
ステップ 4	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

次に、すべての条件下で err-disabled リカバリをイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# errdisable recovery interval 32
switch(config)# show interface status err-disabled
switch(config)# copy running-config startup-config
```

error-disabled リカバリのディセーブル化

err-disabled ステートからのインターフェイスのリカバリを無効にできます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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 2	switch(config)# **no errdisable recovery cause** {*all* | *udld* | *bpduguard* | *link-flap* | *failed-port-state* | *pause-rate-limit* | *loopback*}	インターフェイスがデフォルトの err-disabled ステートに戻る条件を指定します。
ステップ 3	switch(config)# **show interface status err-disabled**	（任意） err-disabled ステートにあるインターフェイスについての情報を表示します。
ステップ 4	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

次に、err-disabled リカバリをディセーブルにする例を示します。

```
switch# configure terminal
switch(config)# no errdisable recovery cause loopback
switch(config)# show interface status err-disabled
switch(config)# copy running-config startup-config
```

デバウンス タイマーの設定

イーサネット ポートのデバウンス タイマーは、デバウンス時間をミリ秒単位（ms）で指定することによりイネーブル化でき、デバウンス時間に 0 を指定することによりディセーブル化できます。デフォルトでは、デバウンス タイマーは、デバウンス タイマーが作動しない 100 ミリ秒に設定されています。

show interface debounce コマンドを使用すれば、すべてのイーサネット ポートのデバウンス時間を表示できます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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 2	switch(config)# **interface***typeslot*/*port*	指定したインターフェイスに対してインターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# **link debounce time***milliseconds*	指定した時間（1 ～ 5000 ミリ秒）でデバウンス タイマーをイネーブルにします。 0 ミリ秒を指定すると、デバウンス タイマーはディセーブルになります。

次に、イーサネットインターフェイスのデバウンスタイマーをイネーブルにし、デバウンス時間を 1000 ミリ秒に設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 3/1
switch(config-if)# link debounce time 1000
```

次の例は、イーサネットインターフェイスでデバウンスタイマーをディセーブルにする方法を示しています。

```
switch# configure terminal
switch(config)# interface ethernet 3/1
switch(config-if)# link debounce time 0
```

説明パラメータの設定

イーサネット ポートのインターフェイスに関する説明を入力することができます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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 2	switch(config)# **interface***typeslot*/*port*	指定したインターフェイスに対してインターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# **description***test*	インターフェイスの説明を指定します。

次に、インターフェイスの説明を Server 3 Interface に設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/3
switch(config-if)# description Server 3 Interface
```

イーサネット インターフェイスのディセーブル化と再起動

イーサネット インターフェイスは、シャットダウンして再起動することができます。この操作により、すべてのインターフェイス機能がディセーブル化され、すべてのモニタリング画面でインターフェイスがダウンしているものとしてマークされます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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 2	switch(config)# **interface***typeslot*/*port*	指定したインターフェイスに対してインターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# **shutdown**	インターフェイスをディセーブルにします。
ステップ 4	switch(config-if)# **no shutdown**	インターフェイスを再起動します。

次に、イーサネット ポートをディセーブルにする例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/4
switch(config-if)# shutdown
```

次に、イーサネット インターフェイスを再起動する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/4
switch(config-if)# no shutdown
```

ダウンリンク遅延の設定

SFP+ ポートが有効になるまでハードウェアの RJ-45 ポートの有効化を遅延させることにより、Cisco Nexus 3048 スイッチのリロード後、ダウンリンク RJ-45 ポートの前にアップリンク SFP+ ポートを動作上有効にできます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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 2	switch(config)# **downlink delayenable** | **disable** [**timeout***time-out*]	ダウンリンク遅延を有効または無効にして、タイムアウトを設定します。

次に、スイッチでダウンリンク遅延を有効にして遅延タイムアウトを設定する例を示します。

```
switch# configure terminal
switch(config)# downlink delay enable timeout 45
```

インターフェイス情報の表示

定義済みインターフェイスに関する設定情報を表示するには、次のうちいずれかの手順を実行します。

コマンド	目的
switch# **show interface***typeslot*/*port*	指定したインターフェイスの詳細設定が表示されます。
switch# **show interface***typeslot*/*port***capabilities**	指定したインターフェイスの機能に関する詳細情報が表示されます。このオプションは、物理インターフェイスに関してのみ使用可能です。
switch# **show interface***typeslot*/*port***transceiver**	指定したインターフェイスに接続されているトランシーバに関する詳細情報が表示されます。このオプションは、物理インターフェイスに関してのみ使用可能です。
switch# **show interface brief**	すべてのインターフェイスのステータスが表示されます。
switch# **show interface flowcontrol**	すべてのインターフェイスでフロー制御設定の詳細なリストを表示します。

show interface コマンドは EXEC モードから呼び出され、インターフェイスの設定を表示することができます。引数を入力せずにこのコマンドを実行すると、スイッチ内に設定されたすべてのインターフェイスの情報が表示されます。

次に、物理イーサネット インターフェイスを表示する例を示します。

```
switch# show interface ethernet 1/1
  Ethernet1/1 is up
  Hardware is 1000/10000 Ethernet, address is 000d.eca3.5f08 (bia 000d.eca3.5f08)
  MTU 1500 bytes, BW 10000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 190/255, rxload 192/255
```

```
  Encapsulation ARPA
  Port mode is trunk
  full-duplex, 10 Gb/s, media type is 1/10g
  Input flow-control is off, output flow-control is off
  Auto-mdix is turned on
  Rate mode is dedicated
  Switchport monitor is off
  Last clearing of "show interface" counters never
  5 minute input rate 942201806 bytes/sec, 14721892 packets/sec
  5 minute output rate 935840313 bytes/sec, 14622492 packets/sec
  Rx
    129141483840 input packets 0 unicast packets 129141483847 multicast packets
    0 broadcast packets 0 jumbo packets 0 storm suppression packets
    8265054965824 bytes
    0 No buffer 0 runt 0 Overrun
    0 crc 0 Ignored 0 Bad etype drop
    0 Bad proto drop
  Tx
    119038487241 output packets 119038487245 multicast packets
   0 broadcast packets 0 jumbo packets
    7618463256471 bytes
    0 output CRC 0 ecc
    0 underrun 0 if down drop     0 output error 0 collision 0 deferred
    0 late collision 0 lost carrier 0 no carrier
    0 babble
    0 Rx pause 8031547972 Tx pause 0 reset
```

次に、物理イーサネットの機能を表示する例を示します。

```
switch# show interface ethernet 1/1 capabilities
Ethernet1/1
  Model:                 734510033
  Type:                  10Gbase-(unknown)
  Speed:                 1000,10000
  Duplex:                full
  Trunk encap. type:     802.1Q
  Channel:               yes
  Broadcast suppression: percentage(0-100)
  Flowcontrol:           rx-(off/on),tx-(off/on)
  Rate mode:             none
  QOS scheduling:        rx-(6q1t),tx-(1p6q0t)
  CoS rewrite:           no
  ToS rewrite:           no
  SPAN:                  yes
  UDLD:                  yes

  MDIX:                  no
  FEX Fabric:            yes
```

次に、物理イーサネット トランシーバを表示する例を示します。

```
switch# show interface ethernet 1/1 transceiver
Ethernet1/1
    sfp is present
    name is CISCO-EXCELIGHT
    part number is SPP5101SR-C1
    revision is A
    serial number is ECL120901AV
    nominal bitrate is 10300 MBits/sec
    Link length supported for 50/125mm fiber is 82 m(s)
    Link length supported for 62.5/125mm fiber is 26 m(s)
    cisco id is --
    cisco extended id number is 4
```

次に、インターフェイス ステータスの要約を表示する例を示します（簡潔にするため、一部の出力が削除されています）。

```
switch# show interface brief

--------------------------------------------------------------------------------
Ethernet      VLAN    Type Mode   Status  Reason                   Speed     Port
Interface                                                                    Ch #
```

```
--------------------------------------------------------------------------------
Eth1/1        200     eth  trunk  up      none                           10G(D) --
Eth1/2        1       eth  trunk  up      none                           10G(D) --
Eth1/3        300     eth  access down    SFP not inserted               10G(D) --
Eth1/4        300     eth  access down    SFP not inserted               10G(D) --
Eth1/5        300     eth  access down    Link not connected            1000(D) --
Eth1/6        20      eth  access down    Link not connected             10G(D) --
Eth1/7        300     eth  access down    SFP not inserted               10G(D) --
...
```

次に、CDP ネイバーを表示する例を示します。

```
switch# show cdp neighbors
Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute
Device ID              Local Intrfce   Hldtme  Capability  Platform      Port ID
d13-dist-1               mgmt0           148     S I      WS-C2960-24TC  Fas0/9
n5k(FLC12080012)         Eth1/5          8       S I s    N5K-C5020P-BA  Eth1/5
```

レイヤ 2 インターフェイスの MIB

MIB	MIB Link
IF-MIB	MIB を検索およびダウンロードするには、次の URL にアクセスしてください。 http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml
MAU-MIB サポートは次の MIB オブジェクトだけに限定されます。 • ifMauType（読み取り専用）GET • ifMauAutoNegSupported（読み取り専用）GET • ifMauTypeListBits（読み取り専用）GET • ifMauDefaultType（読み取りと書き込み）GET-SET • ifMauAutoNegAdminStatus（読み取りと書き込み）GET-SET • ifMauAutoNegCapabilityBits（読み取り専用）GET • ifMauAutoNegAdvertisedBits（読み取りと書き込み）GET-SET	

第 3 章

レイヤ 3 インターフェイスの設定

この章の内容は、次のとおりです。

レイヤ 3 インターフェイスについて

レイヤ 3 インターフェイスは、スタティックまたはダイナミック ルーティング プロトコルを使って、パケットを別のデバイスに転送します。レイヤ 2 トラフィックの IP ルーティングおよび内部 Virtual Local Area Network（VLAN）ルーティングにはレイヤ 3 インターフェイスが使用できます。

ルーテッド インターフェイス

ポートをレイヤ 2 インターフェイスまたはレイヤ 3 インターフェイスとして設定できます。ルーテッドインターフェイスは、IP トラフィックを他のデバイスにルーティングできる物理ポートです。ルーテッドインターフェイスはレイヤ 3 インターフェイスだけで、スパニングツリー プロトコル（STP）などのレイヤ 2 プロトコルはサポートしません。

イーサネット ポートはすべて、デフォルトではレイヤ 2（スイッチポート）です。このデフォルト動作は、インターフェイス コンフィギュレーション モードから **no switchport** コマンドを使用して変更できます。複数のポートを一度に変更するために、インターフェイスの範囲を指定してから **no switchport** コマンドを適用することができます。

ポートに IP アドレスを割り当て、ルーティングをイネーブルにし、このルーテッドインターフェイスにルーティング プロトコル特性を割り当てることができます。

レイヤ 3 インターフェイスに静的 MAC アドレスを割り当てることができます。レイヤ 3 インターフェイスのデフォルト MAC アドレスは、割り当て先の仮想デバイス コンテキスト（VDC）の MAC アドレスです。インターフェイス コンフィギュレーション モードから **mac-address** コマンドを使用して、レイヤ 3 インターフェイスのデフォルト MAC アドレスを変更できます。静的 MAC アドレスは、SVI、レイヤ 3 インターフェイス、ポート チャネル、レイヤ 3 サブインターフェイス、およびトンネルインターフェイスで設定できます。また、ポートおよびポートチャネルの範囲で静的 MAC アドレスを設定することもできます。ただし、すべてのポートは レイヤ 3にある必要があります。ポートの範囲内の 1 つのポートがレイヤ 2 にある場合でも、コマンドは拒否され、エラー メッセージが表示されます。MAC アドレスの設定については、デバイスの『Layer 2 Switching Configuration Guide』を参照してください。

ルーテッド インターフェイスからレイヤ 3 ポート チャネルも作成できます。

ルーテッドインターフェイスおよびサブインターフェイスは、指数関数的に減少するレート カウンタをサポートします。Cisco NX-OS はこれらの平均カウンタを用いて次の統計情報を追跡します。

- 入力パケット数/秒
- 出力パケット数/秒
- 入力バイト数/秒
- 出力バイト数/秒

サブインターフェイス

レイヤ 3 インターフェイスとして設定した親インターフェイスに仮想サブインターフェイスを作成できます。親インターフェイスは物理ポートでもポート チャネルでもかまいません。

親インターフェイスはサブインターフェイスによって複数の仮想インターフェイスに分割されます。これらの仮想インターフェイスに IP アドレスやダイナミック ルーティング プロトコルなど固有のレイヤ 3 パラメータを割り当てることができます。各サブインターフェイスの IP アドレスは、親インターフェイスの他のサブインターフェイスのサブネットとは異なります。

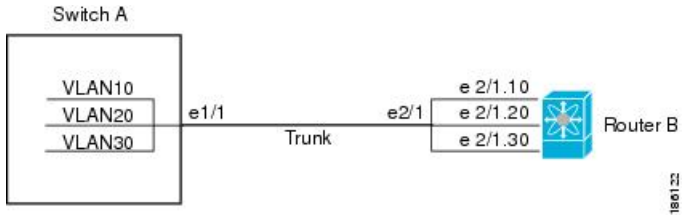
サブインターフェイスの名前は、親インターフェイスの名前（たとえば Ethernet 2/1）+ ピリオド（.）+そのインターフェイス独自の番号です。たとえば、イーサネット インターフェイス 2/1 に Ethernet 2/1.1 というサブインターフェイスを作成できます。この場合、.1 はそのサブインターフェイスを表します。

Cisco NX-OS では、親インターフェイスがイネーブルの場合にサブインターフェイスがイネーブルになります。サブインターフェイスは、親インターフェイスには関係なくシャットダウンできます。親インターフェイスをシャットダウンすると、関連するサブインターフェイスもすべてシャットダウンされます。

サブインターフェイスを使用すると、親インターフェイスがサポートする各 VLAN に独自のレイヤ 3 インターフェイスを実現できます。この場合、親インターフェイスは別のデバイスのレイヤ 2 トランキング ポートに接続します。サブインターフェイスを設定したら 802.1Q トランキングを使って VLAN ID に関連付けます。

次の図に、インターフェイス E 2/1 のルータ B に接続するスイッチのトランキング ポートを示します。このインターフェイスには 3 つのサブインターフェイスがあり、トランキング ポートに接続する 3 つの VLAN にそれぞれ関連付けられています。

図 *2*：*VLAN* のサブインターフェイス



VLAN インターフェイス

VLAN インターフェイスまたはスイッチ仮想インターフェイス（SVI）は、デバイス上の VLAN を同じデバイス上のレイヤ 3 ルータ エンジンに接続する仮想ルーテッド インターフェイスです。VLAN には 1 つの VLAN インターフェイスだけを関連付けることができますが、VLAN に VLAN インターフェイスを設定する必要があるのは、VLAN 間でルーティングする場合か、または管理 VRF（仮想ルーティング/転送）以外の VRF インスタンスを経由してデバイスを IP ホスト接続する場合だけです。VLAN インターフェイスの作成をイネーブルにすると、Cisco NX-OS によって

デフォルト VLAN（VLAN 1）に VLAN インターフェイスが作成され、リモート スイッチ管理が許可されます。

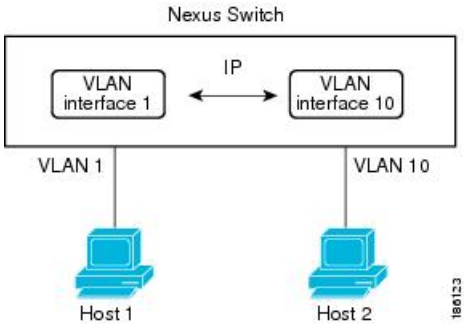
設定の前に VLAN ネットワーク インターフェイス機能をイネーブルにする必要があります。システムはこの機能をディセーブルにする前のチェックポイントを自動的に取得するため、このチェックポイントにロールバックできます。ロールバックとチェックポイントの詳細については、デバイスの『System Management Configuration Guide』を参照してください。

（注） VLAN 1 の VLAN インターフェイスは削除できません。

VLAN インターフェイスをルーティングするには、トラフィックをルーティングする VLAN ごとに VLAN インターフェイスを作成し、その VLAN インターフェイスに IP アドレスを割り当ててレイヤ 3 内部 VLAN ルーティングを実現します。IP アドレスと IP ルーティングの詳細については、デバイスの『Unicast Routing Configuration Guide』を参照してください。

次の図に、デバイス上の 2 つの VLAN に接続されている 2 つのホストを示します。VLAN ごとに VLAN インターフェイスを設定し、VLAN 間の IP ルーティングを使ってホスト 1 とホスト 2 を通信させることができます。VLAN 1 は VLAN インターフェイス 1 のレイヤ 3 で、VLAN 10 は VLAN インターフェイス 10 のレイヤ 3 で通信します。

図 *3*：*VLAN* インターフェイスによる *2* つの *VLAN* の接続



インターフェイスの VRF メンバーシップの変更

インターフェイスで **vrf member** コマンドを入力すると、インターフェイス設定の削除に関するアラートと、クライアント/リスナー（CLI サーバなど）にインターフェイスに関する設定の削除を通知するアラートを受信します。

system vrf-member-change retain-l3-config コマンドを（7.0(3)I4(1) 以降）を入力すると、インターフェイスで VRF メンバーを変更するときにレイヤ 3 設定を保持できます。これは、既存の設定の保存（バッファ）、古い VRF コンテキストからの設定の削除、および保存された設定の新しい VRF コンテキストでの再適用の通知をクライアント/リスナーに送信することによって実行されます。

（注） **system vrf-member-change retain-l3-config** コマンドが有効な場合、レイヤ 3 設定は削除されず、保存（バッファ）されたままになります。このコマンドが無効な場合（デフォルト モード）、VRF メンバーの変更時にレイヤ 3 設定は保持されません。

no system vrf-member-change retain-l3-config コマンドを使用して、レイヤ 3 設定の保持を無効にすることができます。このモードでは、VRF メンバーの変更時にレイヤ 3 設定は保持されません。

インターフェイスの VRF メンバーシップの変更に関する注意事項

- VRF 名を変更すると、一時的なトラフィック損失が発生する可能性があります。
- **system vrf-member-change retain-l3-config** コマンドが有効な場合、インターフェイス レベルでの設定のみが処理されます。VRF の変更後に、ルーティング プロトコルに適応するよう、ルータ レベルで手動で設定を処理する必要があります。
- **system vrf-member-change retain-l3-config** コマンドは、次を使用してインターフェイス レベルの設定をサポートします。
  - **ip address** および **ipv6 address**（セカンダリ）などの CLI サーバによって保持されたレイヤ 3 設定とインターフェイス 設定で使用できるすべての OSPF/ISIS/EIGRP CLI
  - HSRP
  - **ip dhcp relay address** [**use-vrf**] および **ipv6 dhcp relay address** [**use-vrf**] などの DHCP リレー エージェント CLI
- DHCP の場合：
  - ベスト プラクティスとして、クライアントおよびサーバ インターフェイス VRF は 1 つずつ変更する必要があります。そうしなければ、DHCP パケットをリレー エージェントで交換できません。
  - クライアントとサーバが別の VRF にある場合、**ip dhcp relay address** [**use-vrf**] コマンドを使用して、別の VRF を介してリレー エージェントで DHCP パケットを交換します。

ループバック インターフェイス

ループバック インターフェイスは、常にアップ状態にある単独のエンドポイントを持つ仮想インターフェイスです。ループバック インターフェイス経由で送信されたパケットはすべて、このインターフェイスでただちに受信されます。ループバック インターフェイスは物理インターフェイスをエミュレートします。

ループバック インターフェイスを使用すると、パフォーマンスの分析、テスト、ローカル通信が実行できます。ループバック インターフェイスは、ルーティング プロトコル セッションの終端アドレスとして設定することができます。ループバックをこのように設定すると、アウトバウン

ドインターフェイスの一部がダウンしている場合でもルーティング プロトコル セッションはアップしたままです。

IP アンナンバード

IP アンナンバード機能を使用すると、ポイント ツー ポイント（p2p）インターフェイスで明示的に一意の IP アドレスを設定せずに IP パケットを処理できます。このアプローチでは、別のインターフェイスから IP アドレスを借りて、ポイント ツー ポイント リンクのアドレス空間を節約します。

ポイント ツー ポイント モードに準拠したインターフェイスは、IP アンナンバード インターフェイスとして使用できます。7.0(3)I3(1) 以降では、IP アンナンバード機能は、イーサネット インターフェイスおよびサブインターフェイスでのみサポートされます。借りることができるインターフェイスは、ループバック インターフェイスのみです。これは、ナンバードインターフェイスと呼ばれます。

ループバック インターフェイスは、常に機能的にアップしているため、ナンバードインターフェイスとして理想的です。ただし、ループバック インターフェイスはスイッチ/ルータに対してローカルであるため、スタティック ルートを介したり、または OSPF や IS-IS などの内部ゲートウェイ プロトコルを使用して、最初にアンナンバードインターフェイスの到達可能性を確立する必要があります。

トンネル インターフェイス

Cisco NX-OS は、IP トンネルとしてトンネル インターフェイスをサポートします。IP トンネルを使うと、同じレイヤまたは上位レイヤのプロトコルをカプセル化して、2 台のルータ間で作成されたトンネルを通じて IP の結果を転送できます。

レイヤ 3 インターフェイスのライセンス要件

この機能には、ライセンスは必要ありません。ライセンス パッケージに含まれていない機能はすべて Cisco NX-OS システム イメージにバンドルされており、追加費用は一切発生しません。NX-OS ライセンス方式の詳細については、『*Cisco NX-OS Licensing Guide*』を参照してください。

レイヤ 3 インターフェイスの注意事項および制約事項

レイヤ 3 インターフェイスの設定には次の注意事項と制約事項があります。

- IP アンナンバード インターフェイスが設定されている場合、ループバック インターフェイスは IP アンナンバード インターフェイスと同じ VRF にある必要があります。
- ナンバード インターフェイスであるループバック インターフェイスで admin-shutdown コマンドを使用しても、IP ナンバード インターフェイスはダウンしません。これは、IP アンナ

ンバード インターフェイス上で動作するルーティング プロトコルが引き続きアップしていることを意味します。

- IP アンナンバード インターフェイス上で動作するスタティック ルートは、接続されたスタティック ルートを使用する必要があります。

（注） ルートが解決されている IP アンナンバード インターフェイスを指定する必要があります。

- IP アンナンバード機能を設定するには、メディア p2p を有効にする必要があります。
- Release 7.0(3)I2(1) 以降、VLAN/SVI は設定を削除しても、レイヤ 3 インターフェイス テーブルからは削除されません。VLAN 自体をレイヤ 3 インターフェイス テーブルから削除する必要があります。
- レイヤ 3 インターフェイスをレイヤ 2 インターフェイスに変更する場合、Cisco NX-OS はインターフェイスをシャットダウンしてインターフェイスを再度イネーブルにし、レイヤ 3 固有の設定をすべて削除します。
- レイヤ 2 インターフェイスをレイヤ 3 インターフェイスに変更する場合、Cisco NX-OS はインターフェイスをシャットダウンしてインターフェイスを再度イネーブルにし、レイヤ 2 固有の設定をすべて削除します。
- Cisco Nexus 3000 シリーズ スイッチは、レイヤ 3 MTU がすべてのレイヤ 3 インターフェイスで同じでない場合、および MTU QoS がジャンボに変更された場合に、マルチキャスト レイヤ 2 トラフィックを CPU にパントします。この問題を回避するために、すべてのレイヤ 3 インターフェイスは同じレイヤ 3 MTU を持つ必要があります。

レイヤ 3 インターフェイスのデフォルト設定

レイヤ 3 管理状態のデフォルト設定は Shut です。

SVI 自動ステートのディセーブル化

SVI 自動ステート ディセーブル化機能により、スイッチ仮想インターフェイス（SVI）は、対応する VLAN に「アップ」ステートのインターフェイスがない場合でも、「アップ」ステートになることができます。

SVI は、デバイス上の VLAN を同じデバイス上のレイヤ 3 ルータ エンジンに接続する仮想ルーテッド インターフェイスでもあります。VLAN のポートによって、対応する SVI の動作ステートが決定されます。VLAN の SVI インターフェイスは、対応する VLAN 内の少なくとも 1 個のポートがスパニングツリー プロトコル（STP）のフォワーディング ステートである場合に「アップ」になります。同様に、SVI インターフェイスは、最後の STP 転送ポートがダウンするか別のステートになったときに、「ダウン」になります。SVI のこの特性は、「自動ステート」と呼ばれます。

VLAN 上のレイヤ 2 またはレイヤ 3 境界を定義するためや、SVI インターフェイスを使用してデバイスを管理するために SVI を作成できます。2 番目のシナリオでは、SVI 自動ステートディセーブル化機能により、対応する VLAN に「アップ」ステートのインターフェイスがない場合でも SVI インターフェイスが「アップ」ステートになることが保証されます。

DHCP クライアント検出

Cisco NX-OS Release 6.0(2)U3(1) では、SVI での DHCP クライアント検出が導入されました。Cisco NX-OS Release 6.0(2)U4(1) は、IPv6 アドレスと物理イーサネットおよび管理インターフェイスの DHCP クライアント検出のサポートを追加します。**ip address dhcp** または **ipv6 address dhcp** コマンドを使用することにより、DHCP クライアントの IP アドレスを設定できます。これらのコマンドにより、DHCP サーバから IPv4 または IPv6 アドレスを得るための要求が DHCP クライアントから DHCP サーバに送信されます。Cisco Nexus スイッチ上の DHCP クライアントは、それ自体を DHCP サーバに識別させます。DHCP サーバは、この ID を使用して、DHCP クライアントに IP アドレスを返信します。

DHCP クライアントが SVI で DHCP サーバ送信ルータおよび DNS オプションによって設定されている場合、スイッチで **ip route** 0.0.0.0/0 *router-ip* コマンドと **ip name-server***dns-ip* コマンドが自動的に設定されます。

スイッチがリロードされ、同時に、サーバ側でルータおよびDNSオプションが無効になると、スイッチの起動後に新しい IP アドレスが SVI に割り当てられます。ただし、古い **ip route** コマンドおよび **ip name-server** コマンドは依然としてスイッチ設定に存在します。これらのコマンドは、手動で設定から削除する必要があります。

インターフェイスでの DHCP クライアント検出の使用に関する制限事項

次に、インターフェイスでのDHCPクライアント検出の使用に関する制限事項を示します。

- この機能は、物理イーサネットインターフェイス、管理インターフェイス、および SVI でのみサポートされます。
- Cisco NX-OS Release 6.0(2)U4(1) 以降、この機能は、非デフォルトの Virtual Routing and Forwarding（VRF）インスタンスでもサポートされるようになりました。
- **copy running-config startup-config** コマンドを入力すると、DNS サーバおよびデフォルト ルータ オプション関連の設定がスタートアップ コンフィギュレーションに保存されます。スイッチをリロードするとき、この設定が適切ではない場合は、この設定を削除しなければならない可能性があります。
- スイッチで設定できる DNS サーバは最大 6 つです。これは、スイッチの制限です。この最大数には、DHCP クライアントによって設定される DNS サーバと手動で設定される DNS サーバが含まれます。

- スイッチで 7 つ以上の DNS サーバが設定されている場合、DNS オプション セットによって SVI の DHCP オファーを取得すると、IP アドレスは SVI に割り当てられません。

MAC 組み込み IPv6 アドレス

Cisco NX-OS Release 6.0(2)U4(1) 以降では、BGP により IPv4 プレフィックスを IPv6 ネクスト ホップで伝送できます。IPv6 ネクストホップは、ネットワークからネイバー探索（ND）関連トラフィックを削除するために活用されます。これを行うために、MAC アドレスが IPv6 アドレスに組み込まれています。このようなアドレスは、MAC 組み込み IPv6（MEv6）アドレスと呼ばれます。ルータは、ND を経由せずに、MEv6 アドレスから MAC アドレスを直接取得します。ローカル インターフェイスおよびネクスト ホップの MAC アドレスは、IPv6 アドレスから取得されます。

MEv6 が有効になっている IPv6 インターフェイスでは、MEv6 から取得される同じ MAC アドレスが IPv4 トラフィックにも使用されます。MEv6 は、SVI を除くすべてのレイヤ 3 対応インターフェイスでサポートされます。

重要 MEv6 がインターフェイスで有効になっている場合、そのインターフェイスでは IPv6 リンク ローカル アドレス、OSPFv3、および BFDv6 への ping6 はサポートされません。

レイヤ 3 インターフェイスの設定

ルーテッド インターフェイスの設定

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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 2	switch(config)# **interface ethernet** *slot/port*	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 3	switch(conifg-if)# **no switchport**	インターフェイスをレイヤ 3 インターフェイスとして設定し、このインターフェイス上のレイヤ 2 固有の設定を削除します。 （注） レイヤ 3 インターフェイスを元のレイヤ 2 インターフェイスに変換するには、**switchport** コマンドを使用します。

	コマンドまたはアクション	目的
ステップ 4	switch(config-if)# [**ip**|**ipv6**]*ip-address/length*	このインターフェイスの IP アドレスを設定します。
ステップ 5	switch(config-if)# **medium** {**broadcast** | **p2p**}	（任意） インターフェイス メディアをポイント ツーポイントまたはブロードキャストのどちらかとして設定します。 （注） デフォルト設定は broadcast であり、この設定はどの **show** コマンドにも表示されません。ただし、**p2p** に設定を変更した場合、**show running config** コマンドを入力すると、この設定が表示されます。
ステップ 6	switch(config-if)# **show interfaces**	（任意） レイヤ 3 インターフェイスの統計情報を表示します。
ステップ 7	switch(config-if)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

次に、IPv4 ルーテッド レイヤ 3 インターフェイスを設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# no switchport
switch(config-if)# ip address 192.0.2.1/8
switch(config-if)# copy running-config startup-config
```

サブインターフェイスの設定

はじめる前に

- 親インターフェイスをルーテッド インターフェイスとして設定します。
- このポート チャネル上にサブインターフェイスを作成するには、ポート チャネル インターフェイスを作成します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch(config-if)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。
ステップ 2	switch(config)# **interface ethernet** *slot/port.number*	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。*slot* の範囲は 1 ～ 255 です。*port* の範囲は 1 ～ 128 です。
ステップ 3	switch(config-if)# [**ip** | **ipv6**] **address** *ip-address/length*	このインターフェイスの IP アドレスを設定します。
ステップ 4	switch(config-if)# **encapsulation dot1Q** *vlan-id*	サブインターフェイス上の IEEE 802.1Q VLAN カプセル化を設定します。*vlan-id* の範囲は 2 ～ 4093 です。
ステップ 5	switch(config-if)# **show interfaces**	（任意） レイヤ 3 インターフェイスの統計情報を表示します。
ステップ 6	switch(config-if)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

次に、サブインターフェイスを作成する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# ip address 192.0.2.1/8
switch(config-if)# encapsulation dot1Q 33
switch(config-if)# copy running-config startup-config
```

インターフェイスでの帯域幅の設定

ルーテッドインターフェイス、ポートチャネル、またはサブインターフェイスに帯域幅を設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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 2	switch(config)# **interface ethernet** *slot/port*	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。*slot* の範囲は 1 ～ 255 です。*port* の範囲は 1 ～ 128 です。
ステップ 3	switch(conifg-if)# **bandwidth** [*value* | **inherit** [*value*]]	次のように、ルーテッドインターフェイス、ポートチャネル、またはサブインターフェイスに帯域幅パラメータを設定します。 • *value*：帯域幅のサイズ（KB 単位）。指定できる範囲は 1 ～ 10000000 です。 • **inherit**：このインターフェイスのすべてのサブインターフェイスが、帯域幅の値（値が指定されている場合）または親インターフェイスの帯域幅（値が指定されていない場合）のどちらかを継承することを示します。
ステップ 4	switch(config-if)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

次に、イーサネット インターフェイス 2/1 に 80000 の帯域幅の値を設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# bandwidth 80000
switch(config-if)# copy running-config startup-config
```

VLAN インターフェイスの設定

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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 2	switch(config)# **feature interface-vlan**	VLAN インターフェイス モードをイネーブルにします。
ステップ 3	switch(config)# **interface vlan** *number*	VLANインターフェイスを作成します。*number* の有効範囲は 1 ～ 4094 です。
ステップ 4	switch(config-if)# [**ip** | **ipv6**] **address** *ip-address/length*	このインターフェイスの IP アドレスを設定します。
ステップ 5	switch(config-if)# **no shutdown**	インターフェイスを管理上アップさせます。
ステップ 6	switch(config-if)# **show interface vlan** *number*	（任意） VLAN インターフェイスの統計情報を表示します。*number* の有効範囲は 1 ～ 4094 です。
ステップ 7	switch(config-if)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーして、変更を継続的に保存します。

次に、VLAN インターフェイスを作成する例を示します。

```
switch# configure terminal
switch(config)# feature interface-vlan
switch(config)# interface vlan 10
switch(config-if)# ip address 192.0.2.1/8
switch(config-if)# copy running-config startup-config
```

VRF メンバーシップ変更時のレイヤ 3 保持の有効化

次の手順で、インターフェイスで VRF メンバーシップを変更するときにレイヤ 3 設定を保持できるようになります。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**system vrf-member-change retain-l3-config**
	
	例：
	`switch(config)# system vrf-member-change retain-l3-config`
	`Warning: Will retain L3 configuration when vrf member change on interface.`
		VRF メンバーシップの変更時にレイヤ 3 設定を保持できます。
		（注） レイヤ 3 設定の保持を無効にするには、**no system vrf-member-change retain-l3-config** コマンドを使用します。

ループバック インターフェイスの設定

はじめる前に

ループバック インターフェイスの IP アドレスが、ネットワークの全ルータで一意であることを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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 2	switch(config)# **interface loopback** *instance*	ループバック インターフェイスを作成します。*instance* の範囲は 0 ～ 1023 です。
ステップ 3	switch(config-if)# [**ip** | **ipv6**] **address** *ip-address/length*	このインターフェイスの IP アドレスを設定します。
ステップ 4	switch(config-if)# **show interface loopback** *instance*	（任意） ループバック インターフェイスの統計情報を表示します。*instance* の範囲は 0 ～ 1023 です。
ステップ 5	switch(config-if)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュ

	コマンドまたはアクション	目的
		レーションにコピーして、変更を継続的に保存します。

次に、ループバック インターフェイスを作成する例を示します。

```
switch# configure terminal
switch(config)# interface loopback 0
switch(config-if)# ip address 192.0.2.100/8
switch(config-if)# copy running-config startup-config
```

イーサネット インターフェイスでの IP アンナンバードの設定

イーサネット インターフェイスで IP アンナンバード機能を設定できます。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		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 2	**interface ethernet***slot/port*
	
	例：
	`switch(config)# interface ethernet 1/1`
	`switch(config-if)#`
		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 3	**mediump2p** 例： `switch(config-if)# medium p2p`	インターフェイス メディアをポイント ツー ポイントとして設定します。
ステップ 4	**ip unnumbered***typenumber* 例： `switch(config-if)# ip unnumbered loopback 100`	明示的な IP アドレスをインターフェイスに割り当てずにインターフェイス上の IP 処理をイネーブルにします。 *type* および *number* で、ルータに割り当て済みの IP アドレスがある別のインターフェイスを指定します。指定したインターフェイスを別のアンナンバードインターフェイスに設定することはできません。 （注） *type* は、**loopback** に限定されます。（7.0(3)I3(1) 以降）

	コマンドまたはアクション	目的

IP アンナンバード インターフェイスの OSPF 設定

IP アンナンバード ループバック インターフェイスの OSPF を設定できます。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		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 2	**interface ethernet***slot/port*
	
	例：
	`switch(config)# interface ethernet 1/20.1`
	`switch(config-if)#`
		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 3	**encapsulation dot1Q***vlan-id* 例： `switch(config-if)# encapsulation dot1Q 100`	サブインターフェイス上の IEEE 802.1Q VLAN カプセル化を設定します。範囲は 2 ～ 4093 です。
ステップ 4	**mediump2p** 例： `switch(config-if)# medium p2p`	インターフェイス メディアをポイント ツー ポイントとして設定します。
ステップ 5	**ip unnumbered***typenumber* 例： `switch(config-if)# ip unnumbered loopback 101`	明示的な IP アドレスをインターフェイスに割り当てずにインターフェイス上の IP 処理をイネーブルにします。 *type* および *number* で、ルータに割り当て済みの IP アドレスがある別のインターフェイスを指定します。指定したインターフェイスを別のアンナンバード インターフェイスに設定することはできません。 （注） *type* は、**loopback** に限定されます。（7.0(3)I3(1) 以降）

	コマンドまたはアクション	目的
ステップ 6	**ip ospf authentication** 例： `switch(config-if)# ip ospf authentication`	（任意） インターフェイスの認証タイプを指定します。
ステップ 7	**ip ospf authentication-key***password* 例： `switch(config-if)# ip ospf authentication 3 b7bdf15f62bbd250`	（任意） OSPF 認証のパスワードを指定します。
ステップ 8	**ip router ospf***instance***area***area-number* 例： `switch(config-if)# ip router ospf 100 area 0.0.0.1`	インターフェイス上で IP のルーティング プロセスを設定して、エリアを指定します。 （注） **ip router ospf** コマンドは、アンナンバードおよびナンバード インターフェイスの両方に必要です。
ステップ 9	**no shutdown** 例： `switch(config-if)# no shutdown`	インターフェイスをアップにします（管理上）。
ステップ 10	**interface loopback***instance* 例： `switch(config)# interface loopback 101`	ループバック インターフェイスを作成します。範囲は 0 ～ 1023 です。
ステップ 11	**ip address***ip-address/length* 例： `switch(config-if)# 192.168.101.1/32`	インターフェイスに IP アドレスを設定します。
ステップ 12	**ip router ospf***instance***area***area-number* 例： `switch(config-if)# ip router ospf 100 area 0.0.0.1`	インターフェイス上で IP のルーティング プロセスを設定して、エリアを指定します。 （注） **ip router ospf** コマンドは、アンナンバードおよびナンバード インターフェイスの両方に必要です。

IP アンナンバード インターフェイスの ISIS 設定

IP アンナンバード ループバック インターフェイスの ISIS を設定できます。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		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 2	**feature isis** 例： `Switch(config)# feature isis`	ISIS を有効にします。
ステップ 3	**router isis***area-tag* 例： `Switch(config)# router isis 100`	IS-IS プロセスにタグを割り当て、ルータ 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	**net***network-entity-title* 例： `Switch(config-router)# net 49.0001.0100.0100.1001.00`	デバイスのネットワーク エンティティ タイトル（NET）を設定します。
ステップ 5	**end** 例： `Switch(config-router)# end`	ルータ コンフィギュレーション モードを終了します。
ステップ 6	**interface ethernet***slot/port* 例： `switch(config)# interface ethernet 1/20.1`	インターフェイス コンフィギュレーション モードを開始します。
ステップ 7	**encapsulation dot1Q***vlan-id* 例： `switch(config-subif)# encapsulation dot1Q 100`	サブインターフェイス上の IEEE 802.1Q VLAN カプセル化を設定します。範囲は 2 ～ 4093 です。
ステップ 8	**mediump2p** 例： `switch(config-subif)# medium p2p`	インターフェイス メディアをポイント ツーポイントとして設定します。
ステップ 9	**ip unnumbered***typenumber* 例： `switch(config-if)# ip unnumbered loopback 101`	明示的な IP アドレスをインターフェイスに割り当てずにインターフェイス上の IP 処理をイネーブルにします。 *type* および *number* で、ルータに割り当て済みの IP アドレスがある別のインターフェイスを指定します。指定したインターフェイスを別

	コマンドまたはアクション	目的
		のアンナンバード インターフェイスに設定することはできません。 （注） *type* は、**loopback** に限定されます。（7.0(3)I3(1) 以降）
ステップ 10	**ip router isis***area-tag* 例： `switch(config-subif)# ip router isis 100`	アンナンバードインターフェイスの ISIS を有効にします。
ステップ 11	**no shutdown** 例： `switch(config-subif)# no shutdown`	インターフェイスをアップにします（管理上）。

VRF へのインターフェイスの割り当て

はじめる前に

VRF 用のインターフェイスを設定した後で、トンネル インターフェイスに IP アドレスを割り当てます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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 2	switch(config)#**interface***interface-typenumber*	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 3	switch(conifg-if)#**vrf member** *vrf-name*	このインターフェイスを VRF に追加します。
ステップ 4	switch(config-if)# [**ip** | **ipv6**]*ip-address/length*	このインターフェイスの IP アドレスを設定します。このステップは、このインターフェイスを VRF に割り当てたあとに行う必要があります。

	コマンドまたはアクション	目的
ステップ 5	switch(config-if)# **show vrf** [*vrf-name*] **interface***interface-typenumber*	（任意） VRF 情報を表示します。
ステップ 6	switch(config-if)# **show interfaces**	（任意） レイヤ 3 インターフェイスの統計情報を表示します。
ステップ 7	switch(config-if)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

次に、VRF にレイヤ 3 インターフェイスを追加する例を示します。

```
switch# configure terminal
switch(config)# interface loopback 0
switch(config-if)# vrf member RemoteOfficeVRF
switch(config-if)# ip address 209.0.2.1/16
switch(config-if)# copy running-config startup-config
```

インターフェイス MAC アドレスの設定

静的 MAC アドレスは、SVI、レイヤ 3 インターフェイス、ポート チャネル、レイヤ 3 サブインターフェイス、およびトンネル インターフェイスで設定できます。また、ポートおよびポート チャネルの範囲で静的 MAC アドレスを設定することもできます。ただし、すべてのポートは レイヤ 3にある必要があります。ポートの範囲内の 1 つのポートがレイヤ 2 にある場合でも、コマンドは拒否され、エラー メッセージが表示されます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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 2	switch(config)# **interface ethernet***slot/port*	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 3	switch(config-if)# [**no**] **mac-address***static router MAC address*	インターフェイス MAC アドレスを設定します。設定を削除するには、**no** 形式を使用します。次の 4 つのサポートされる形式のいずれでも MAC アドレスを入力できます。 • E.E.E

	コマンドまたはアクション	目的
		• EE-EE-EE-EE-EE-EE • EE:EE:EE:EE:EE:EE • EEEE.EEEE.EEEE 次の無効なMACアドレスを入力しないでください。 • ヌル MAC アドレス：0000.0000.0000 • ブロードキャスト MAC アドレス：FFFF.FFFF.FFFF • マルチキャスト MAC アドレス：0100.DAAA.ADDD
ステップ 4	switch(config-if)# **show interface ethernet***slot/port*	（任意）インターフェイスのすべての情報を表示します。

次に、インターフェイス MAC アドレスを設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 3/3
switch(config-if)# mac-address aaaa.bbbb.dddd
switch(config-if)# show interface ethernet 3/3
switch(config-if)#
```

MAC 組み込み IPv6 アドレスの設定

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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 2	switch(config)# **interface***typeslot/port*	指定したインターフェイスのインターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# **no switchport**	インターフェイスをレイヤ3インターフェイスとして設定し、このインターフェイス上のレイヤ2固有の設定を削除します。 （注） レイヤ 3 インターフェイスを元のレイヤ 2 インターフェイスに変換するには、**switchport** コマンドを使用します。

	コマンドまたはアクション	目的
ステップ 4	switch(config-if)# **mac-address ipv6-extract**	インターフェイスで設定された IPv6 アドレスに組み込まれている MAC アドレスを取得します。 （注） MEv6 設定は、現時点では、IPv6 アドレスの EUI-64 形式でサポートされません。
ステップ 5	switch(config-if)# **ipv6 address***ip-address/length*	このインターフェイスの IPv6 アドレスを設定します。
ステップ 6	switch(config-if)# **ipv6 nd mac-extract** [**exclude nud-phase**]	ネクストホップ IPv6 アドレスに組み込まれているネクストホップ MAC アドレスを取得します。 **exclude nud-phase** オプションにより、ND フェーズでのみパケットがブロックされます。**exclude nud-phase** オプションが指定されていない場合は、ND フェーズと近隣到達不能検出（NUD）フェーズの両方でパケットがブロックされます。
ステップ 7	switch(config)# **show ipv6 icmp interface***type slot/port*	（任意） IPv6 Internet Control Message Protocol バージョン 6（ICMPv6）インターフェイスの情報を表示します。

次に、ND MAC 取得を有効にして MAC 組み込み IPv6 アドレスを設定する例を示します。

```
switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# interface ethernet 1/3
switch(config-if)# no switchport
switch(config-if)# mac-address ipv6-extract
switch(config-if)# ipv6 address 2002:1::10/64
switch(config-if)# ipv6 nd mac-extract
switch(config-if)# show ipv6 icmp interface ethernet 1/3
ICMPv6 Interfaces for VRF "default"
Ethernet1/3, Interface status: protocol-up/link-up/admin-up
  IPv6 address: 2002:1::10
  IPv6 subnet:  2002:1::/64
  IPv6 interface DAD state:  VALID
  ND mac-extract : Enabled
  ICMPv6 active timers:
      Last Neighbor-Solicitation sent: 00:01:39
      Last Neighbor-Advertisement sent: 00:01:40
      Last Router-Advertisement sent: 00:01:41
      Next Router-Advertisement sent in: 00:03:34
  Router-Advertisement parameters:
      Periodic interval: 200 to 600 seconds
      Send "Managed Address Configuration" flag: false
      Send "Other Stateful Configuration" flag: false
      Send "Current Hop Limit" field: 64
      Send "MTU" option value: 1500
      Send "Router Lifetime" field: 1800 secs
      Send "Reachable Time" field: 0 ms
      Send "Retrans Timer" field: 0 ms
      Suppress RA: Disabled
      Suppress MTU in RA: Disabled
  Neighbor-Solicitation parameters:
      NS retransmit interval: 1000 ms
  ICMPv6 error message parameters:
      Send redirects: true
```

```
      Send unreachables: false
  ICMPv6-nd Statisitcs (sent/received):
      RAs: 3/0, RSs: 0/0, NAs: 2/0, NSs: 7/0, RDs: 0/0
      Interface statistics last reset: never
switch(config)#
```

次に、ND MAC 取得を有効（NUD フェーズを除く）にして MAC 組み込み IPv6 アドレスを設定する例を示します。

```
switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# interface ethernet 1/5
switch(config-if)# no switchport
switch(config-if)# mac-address ipv6-extract
switch(config-if)# ipv6 address 2002:2::10/64
switch(config-if)# ipv6 nd mac-extract exclude nud-phase
switch(config-if)# show ipv6 icmp interface ethernet 1/5
ICMPv6 Interfaces for VRF "default"
Ethernet1/5, Interface status: protocol-up/link-up/admin-up
  IPv6 address: 2002:2::10
  IPv6 subnet:  2002:2::/64
  IPv6 interface DAD state:  VALID
  ND mac-extract : Enabled (Excluding NUD Phase)
  ICMPv6 active timers:
      Last Neighbor-Solicitation sent: 00:06:45
      Last Neighbor-Advertisement sent: 00:06:46
      Last Router-Advertisement sent: 00:02:18
      Next Router-Advertisement sent in: 00:02:24
  Router-Advertisement parameters:
      Periodic interval: 200 to 600 seconds
      Send "Managed Address Configuration" flag: false
      Send "Other Stateful Configuration" flag: false
      Send "Current Hop Limit" field: 64
      Send "MTU" option value: 1500
      Send "Router Lifetime" field: 1800 secs
      Send "Reachable Time" field: 0 ms
      Send "Retrans Timer" field: 0 ms
      Suppress RA: Disabled
      Suppress MTU in RA: Disabled
  Neighbor-Solicitation parameters:
      NS retransmit interval: 1000 ms
  ICMPv6 error message parameters:
      Send redirects: true
      Send unreachables: false
  ICMPv6-nd Statisitcs (sent/received):
      RAs: 6/0, RSs: 0/0, NAs: 2/0, NSs: 7/0, RDs: 0/0
      Interface statistics last reset: never
switch(config-if)#
```

SVI 自動ステートのディセーブル化の設定

対応する VLAN でインターフェイスが稼働していなくても、SVI がアクティブのままになるように設定できます。この機能拡張は自動ステートのディセーブル化と呼ばれます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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 2	switch(config)# **system default interface-vlan autostate**	VLAN のスイッチング仮想インターフェイス（SVI）でシステムのデフォルトの自動ステート動作を再度イネーブルにします。SVI での自動ステータス動作をディセーブルにするには、このコマンドの no 形式を使用します。
ステップ 3	switch(config)# **feature interface-vlan**	VLAN インターフェイス SVI の作成をイネーブルにします。
ステップ 4	switch(config)# **interface vlan***vlan id*	VLAN インターフェイスをディセーブルにして、インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	(config-if)# [**no**] **autostate**	VLAN インターフェイスで SVI のデフォルトの自動ステート動作をディセーブルにします。
ステップ 6	(config-if)# **end**	特権 EXEC モードに戻ります。
ステップ 7	**show running-config interface vlan***vlan id*	（任意）特定のポート チャネルの実行コンフィギュレーションを表示します。

次に、SVI 自動ステートのディセーブル化機能を設定する例を示します。

```
switch# configure terminal
switch(config)# system default interface-vlan autostate
switch(config)# feature interface-vlan
switch(config)# interface vlan 2
switch(config-if)# no autostate
switch(config-if)# end
```

インターフェイスでの DHCP クライアントの設定

SVI、管理インターフェイス、または物理イーサネット インターフェイスで DHCP クライアントの IP アドレスを設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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 2	switch(config)# **interface ethernet***typeslot/port* | **mgmt***mgmt-interface-number* | **vlan***vlan id*	物理イーサネット インターフェイス、管理インターフェイス、または VLAN インターフェイスを作成します。 *vlan id* の範囲は 1 ～ 4094 です。
ステップ 3	switch(config-if)# [**no**] **ip** | **ipv6 address dhcp**	IPv4 または IPv6 アドレスを DHCP サーバに要求します。 このコマンドの **no** 形式は、取得されたすべてのアドレスを削除します。
ステップ 4	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

次に、SVI で DHCP クライアントの IP アドレスを設定する例を示します。

```
switch# configure terminal
switch(config)# interface vlan 15
switch(config-if)# ip address dhcp
```

次に、管理インターフェイスで DHCP クライアントの IPv6 アドレスを設定する例を示します。

```
switch# configure terminal
switch(config)# interface mgmt 0
switch(config-if)# ipv6 address dhcp
```

レイヤ 3 インターフェイス設定の確認

次のいずれかのコマンドを使用して、設定を確認します。

コマンド	目的
show interface ethernet*slot/port*	レイヤ 3 インターフェイスの設定情報、ステータス、カウンタ（インバウンドおよびアウトバウンド パケット レートおよびバイト レートが 5 分間に指数関数的に減少した平均値を含む）を表示します。
show interface ethernet*slot/port***brief**	レイヤ 3 インターフェイスの動作ステータスを表示します。

コマンド	目的
show interface ethernet*slot/port***capabilities**	レイヤ3インターフェイスの機能（ポートタイプ、速度、およびデュプレックスを含む）を表示します。
show interface ethernet*slot/port***description**	レイヤ 3 インターフェイスの説明を表示します。
show interface ethernet*slot/port***status**	レイヤ3インターフェイスの管理ステータス、ポートモード、速度、およびデュプレックスを表示します。
show interface ethernet*slot/port.number*	サブインターフェイスの設定情報、ステータス、カウンタ（インバウンドおよびアウトバウンド パケット レートおよびバイト レートが 5 分間に指数関数的に減少した平均値を含む）を表示します。
show interface port-channel *channel-id.number*	ポート チャネル サブインターフェイスの設定情報、ステータス、カウンタ（インバウンドおよびアウトバウンド パケット レートおよびバイト レートが5分間に指数関数的に減少した平均値を含む）を表示します。
show interface loopback*number*	ループバック インターフェイスの設定情報、ステータス、カウンタを表示します。
show interface loopback*number***brief**	ループバック インターフェイスの動作ステータスを表示します。
show interface loopback*number***description**	ループバック インターフェイスの説明を表示します。
show interface loopback*number***status**	ループバック インターフェイスの管理ステータスおよびプロトコル ステータスを表示します。
show interface vlan*number*	VLANインターフェイスの設定情報、ステータス、カウンタを表示します。
show interface vlan*number***brief**	VLANインターフェイスの動作ステータスを表示します。
show interface vlan*number***description**	VLANインターフェイスの説明を表示します。

コマンド	目的
show interface vlan*number***private-vlan mapping**	VLANインターフェイスのプライベートVLAN情報を表示します。
show interface vlan*number***status**	VLANインターフェイスの管理ステータスおよびプロトコル ステータスを表示します。

レイヤ3インターフェイス整合性チェッカのトリガー

レイヤ3インターフェイス整合性チェッカを手動でトリガーして、モジュール上のすべての物理インターフェイスのハードウェア設定とソフトウェア設定を比較し、結果を表示することができます。レイヤ3インターフェイス整合性チェッカを手動でトリガーして結果を表示するには、次のコマンドを特定のモードで使用します。

手順

	コマンドまたはアクション	目的
ステップ1	**show consistency-checker l3-interface module***slot*	起動しているモジュールのすべてのレイヤ3物理インターフェイスに対するレイヤ3インターフェイス整合性検査を開始し、その結果を表示します。

次に、レイヤ3インターフェイス整合性検査をトリガーして結果を表示する例を示します。

```
switch# show consistency-checker l3-interface module 1
L3 LIF Checks: L3 Vlan, CML Flags, IPv4 Enable
Consistency Check: PASSED
No inconsistencies found for:
   Ethernet1/17
   Ethernet1/49
   Ethernet1/50
```

レイヤ3インターフェイスのモニタリング

次のいずれかのコマンドを使用して、機能に関する統計情報を表示します。

コマンド	目的
load-interval*seconds* | **counter** {**1** | **2** | **3**} *seconds*	ビットレートとパケットレートの統計情報に対して3つの異なるサンプリング間隔を設定します。範囲は5 ～ 300秒です。

コマンド	目的
show interface ethernet*slot*/*port***counters**	レイヤ3インターフェイスの統計情報を表示します（ユニキャスト、マルチキャスト、ブロードキャスト）。
show interface ethernet*slot*/*port***counters brief** *load-interval-id*	レイヤ3インターフェイスの入力および出力カウンタを表示します。 load-interval-id は、入力および出力レートを表示するための単一のロード インターバル ID を指定します。 ロードインターバル ID の範囲は 1 ~ 3. です。
show interface ethernet*slot*/*port***counters detailed** [**all**]	レイヤ3インターフェイスの統計情報を表示します。オプションとして、32 ビットと 64 ビットのパケットおよびバイト カウンタ（エラーを含む）をすべて含めることができます。
show interface ethernet*slot*/*port***counters error**	レイヤ3インターフェイスの入力および出力エラーを表示します。
show interface ethernet*slot*/*port***counters snmp**	SNMP MIB から報告されたレイヤ3インターフェイス カウンタを表示します。これらのカウンタはクリアできません。
show interface ethernet*slot*/*port*.*number***counters**	サブインターフェイスの統計情報（ユニキャスト、マルチキャスト、およびブロードキャスト）を表示します。
show interface port-channel*channel-id*.*number***counters**	ポート チャネル サブインターフェイスの統計情報（ユニキャスト、マルチキャスト、およびブロードキャスト）を表示します。
show interface loopback*number***counters**	ループバック インターフェイスの入力および出力カウンタ（ユニキャスト、マルチキャスト、およびブロードキャスト）を表示します。
show interface loopback*number***counters detailed** [**all**]	ループバック インターフェイスの統計情報を表示します。オプションとして、32 ビットと 64 ビットのパケットおよびバイト カウンタ（エラーを含む）をすべて含めることができます。

コマンド	目的
show interface loopback*number***counters errors**	ループバック インターフェイスの入力および出力エラーを表示します。
show interface vlan*number***counters**	VLANインターフェイスの入力および出力カウンタ（ユニキャスト、マルチキャスト、およびブロードキャスト）を表示します。
show interface vlan*number***counters detailed** [*all*]	VLANインターフェイスの統計情報を表示します。オプションとして、レイヤ3パケットおよびバイト カウンタをすべて含めることができます（ユニキャストおよびマルチキャスト）。
show interface vlan*counters***snmp**	SNMP MIB から報告された VLAN インターフェイス カウンタを表示します。これらのカウンタはクリアできません。

レイヤ 3 インターフェイスの設定例

次に、イーサネット サブインターフェイスを設定する例を示します。

```
switch# configuration terminal
switch(config)# interface ethernet 2/1.10
switch(config-if)# description Layer 3 for VLAN 10
switch(config-if)# encapsulation dot1q 10
switch(config-if)# ip address 192.0.2.1/8
switch(config-if)# copy running-config startup-config
```

次に、VLAN インターフェイスを設定する例を示します。

```
switch# configuration terminal
switch(config)# interface vlan 100
switch(config-if)# no switchport

switch(config-if)# ipv6 address 33:0DB::2/8
switch(config-if)# copy running-config startup-config
```

次に、スイッチング仮想インターフェイス（SVI）自動ステートのディセーブル化を設定する例を示します。

```
switch# configure terminal
switch(config)# system default interface-vlan autostate
switch(config)# feature interface-vlan
switch(config)# interface vlan 2
switch(config-if)# no autostate
switch(config-if)# end
switch# show running-config interface vlan 2
```

次に、ループバック インターフェイスを設定する例を示します。

```
switch# configuration terminal
switch(config)# interface loopback 3
```

```
switch(config-if)# no switchport
switch(config-if)# ip address 192.0.2.2/32
switch(config-if)# copy running-config startup-config
```

次に、イーサネット ポートの 3 つのサンプル ロード インターバルを設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/3
switch(config-if)# load-interval counter 1 5
switch(config-if)# load-interval counter 2 135
switch(config-if)# load-interval counter 3 225
switch(config-if)#
```

インターフェイスの VRF メンバーシップの変更例

- VRF メンバーシップの変更時に、レイヤ 3 設定を保持できるようにします。

```
switch# configure terminal
switch(config)# system vrf-member-change retain-l3-config

Warning: Will retain L3 configuration when vrf member change on interface.
```

- レイヤ 3 の保持を確認します。

```
switch# show running-config | include vrf-member-change

system vrf-member-change retain-l3-config
```

- VRF「blue」としてレイヤ 3 設定を使用して SVI インターフェイスを設定します。

```
switch# configure terminal
switch(config)# show running-config interface vlan 2002

interface Vlan2002
description TESTSVI
no shutdown
mtu 9192
vrf member blue
no ip redirects
ip address 192.168.211.2/27
ipv6 address 2620:10d:c041:12::2/64
ipv6 link-local fe80::1
ip router ospf 1 area 0.0.0.0
ipv6 router ospfv3 1 area 0.0.0.0
hsrp version 2
hsrp 2002
preempt delay minimum 300 reload 600
priority 110 forwarding-threshold lower 1 upper 110
ip 192.168.211.1
hsrp 2002 ipv6
preempt delay minimum 300 reload 600
priority 110 forwarding-threshold lower 1 upper 110
ip 2620:10d:c041:12::1
```

- SVI インターフェイス VRF を「red」に変更します。

```
switch# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# interface vlan 2002
switch(config-if)# vrf member red

Warning: Retain-L3-config is on, deleted and re-added L3 config on interface Vlan2002
```

- VRF の変更後に、SVI インターフェイスを確認します。

```
switch# configure terminal
switch(config)# show running-config interface vlan 2002

interface Vlan2002
description TESTSVI
no shutdown
mtu 9192
vrf member red
no ip redirects
ip address 192.168.211.2/27
ipv6 address 2620:10d:c041:12::2/64
ipv6 link-local fe80::1
ip router ospf 1 area 0.0.0.0
ipv6 router ospfv3 1 area 0.0.0.0
hsrp version 2
hsrp 2002
preempt delay minimum 300 reload 600
priority 110 forwarding-threshold lower 1 upper 110
ip 192.168.211.1
hsrp 2002 ipv6
preempt delay minimum 300 reload 600
priority 110 forwarding-threshold lower 1 upper 110
ip 2620:10d:c041:12::1
```

（注）

- VRF の変更時、レイヤ 3 設定の保持は次に影響します。
  - Physical Interface
  - ループバック インターフェイス
  - SVI インターフェイス
  - Sub-interface
  - トンネル インターフェイス
  - ポート チャネル
- VRF の変更時、既存のレイヤ 3 設定は削除され、再適用されます。OSPF/ISIS/EIGRP/HSRP などのすべてのルーティング プロトコルは、古い VRF でダウンし、新しい VRF でアップします。
- ダイレクト/ローカル IPv4/IPv6 アドレスは、古い VRF から削除され、新しい VRF にインストールされます。
- VRF の変更時に、いくつかのトラフィック損失が発生する可能性があります。

レイヤ 3 インターフェイスの関連資料

関連項目	マニュアル タイトル
コマンド構文	『*Cisco Nexus 3000 Series Command Reference*』

関連項目	マニュアル タイトル
IP	『*Cisco Nexus 3000 Series NX-OS Unicast Routing Configuration Guide*』の「Configuring IP」の章
VLAN	『*Cisco Nexus 3000 Series NX-OS Layer 2 Switching Configuration Guide*』の「Configuring VLANs」の章

レイヤ 3 インターフェイスの MIB

MIB	MIB Link
CISCO-IF-EXTENSION-MIB	MIB を検索およびダウンロードするには、次の URL にアクセスしてください。 http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml
ETHERLIKE-MIB	

レイヤ 3 インターフェイスの標準

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。

レイヤ 3 インターフェイスの機能履歴

機能名	リリース	機能情報
show interface vlan *vlan-id* **counters** command	5.0(3)U3(1)	**show interface vlan** *vlan-id* **counters** コマンドは、入力および出力パケットのカウントを正しく表示するように拡張されました。

第 4 章

ポート チャネルの設定

この章の内容は、次のとおりです。

ポート チャネルについて

ポート チャネルは、個別インターフェイスを 1 つのグループに集約して、帯域幅と冗長性の向上を実現します。これらの集約された各物理インターフェイス間でトラフィックのロード バランシ

ングも行います。ポート チャネルの物理インターフェイスが少なくとも 1 つ動作していれば、そのポート チャネルは動作しています。

ポート チャネルは、互換性のあるインターフェイスをバンドルすることによって作成します。スタティック ポート チャネルのほか、Link Aggregation Control Protocol（LACP）を実行するポート チャネルを設定して稼働させることができます。

変更した設定をポート チャネルに適用すると、そのポート チャネルのメンバ インターフェイスにもそれぞれ変更が適用されます。たとえば、スパニングツリー プロトコル（STP）のパラメータをポート チャネルに設定すると、Cisco NX-OS ソフトウェアでは、これらのパラメータがポート チャネルの各インターフェイスに適用されます。

関連するプロトコルを使用せず、スタティック ポート チャネルを使用すれば、設定を簡略化できます。IEEE 802.3ad に規定されている Link Aggregation Control Protocol（LACP）を使用すると、ポート チャネルをより効率的に使用することができます。LACP を使用すると、リンクによってプロトコル パケットが渡されます。

関連トピック

LACP の概要，（78 ページ）

ポート チャネルの概要

Cisco NX-OS は、ポート チャネルを使用することにより、広い帯域幅、冗長性、チャネル全体のロード バランシングを実現しています。

ポートを 1 つのスタティック ポート チャネルに集約するか、またはリンク集約制御プロトコル（LACP）をイネーブルにできます。LACP によるポート チャネルを設定する手順は、スタティック ポート チャネルの場合とは若干異なります。ポート チャネル設定の制約事項については、プラットフォームの『*Verified Scalability*』マニュアルを参照してください。ロード バランシングの詳細については、ポート チャネルを使ったロード バランシング，（75 ページ）を参照してください。

（注） Cisco NX-OS は、ポート チャネルに対するポート集約プロトコル（PAgP）をサポートしていません。

ポート チャネルは、個々のリンクを 1 つのチャネル グループにバンドルしたもので、それによりいくつかの物理リンクの帯域幅を集約した単一の論理リンクが作成されます。ポート チャネル内のメンバー ポートに障害が発生すると、障害が発生したリンクで伝送されていたトラフィックはポート チャネル内のその他のメンバー ポートに切り替わります。

各ポートにはポート チャネルが 1 つだけあります。ポート チャネル内のすべてのポートには互換性が必要です。つまり、回線速度が同じであり、かつ全二重モードで動作する必要があります。スタティック ポート チャネルを LACP なしで稼働すると、個々のリンクがすべて on チャネル モードで動作します。このモードを変更するには、LACP をイネーブルにする必要があります。

（注） チャネル モードを、on から active、または on から passive に変更することはできません。

ポート チャネル インターフェイスを作成することで、ポート チャネルを直接作成することができます。またチャネル グループを作成して個々のポートを 1 つに集約することもできます。インターフェイスをチャネル グループに関連付ける際、ポート チャネルがなければ、Cisco NX-OSでは対応するポートチャネルが自動的に作成されます。最初にポートチャネルを作成することもできます。その場合、Cisco NX-OS では、ポート チャネルと同じチャネル数で空のチャネル グループが作成され、デフォルトの設定が適用されます。

（注） 少なくともメンバ ポートの 1 つがアップしており、かつそのポートのチャネルが有効であれば、ポート チャネルは動作上アップ状態にあります。メンバ ポートがすべてダウンしていれば、ポート チャネルはダウンしています。

互換性要件

ポート チャネル グループにインターフェイスを追加すると、Cisco NX-OS では、そのインターフェイスとチャネル グループとの互換性が確保されるように、特定のインターフェイス属性のチェックが行われます。また Cisco NX-OS では、インターフェイスがポート チャネル集約に加えられることを許可する場合にも、事前にそのインターフェイスに関するさまざまな動作属性のチェックが行われます。

互換性チェックの対象となる動作属性は次のとおりです。

- ポート モード
- アクセス VLAN
- トランク ネイティブ VLAN
- 許可 VLAN リスト
- 速度
- 802.3x フロー制御設定
- MTU
- ブロードキャスト/ユニキャスト/マルチキャスト ストーム制御設定
- プライオリティ フロー制御
- タグなし CoS

Cisco NX-OS で使用される互換性チェックの全リストを表示する場合は、**show port-channel compatibility-parameters** コマンドを使用します。

チャネル モードセットを on に設定したインターフェイスだけをスタティック ポート チャネルに追加できます。またLACPを実行するポートチャネルには、チャネル モードがactiveまたはpassiveに設定されたインターフェイスだけを追加することもできますこれらのアトリビュートは個別のメンバ ポートに設定できます。

インターフェイスがポートチャネルに追加されると、次の各パラメータはそのポートチャネルに関する値に置き換えられます。

- 帯域幅
- MAC address
- スパニングツリー プロトコル

インターフェイスがポートチャネルに追加されても、次に示すインターフェイスパラメータは影響を受けません。

- 説明
- CDP
- LACP ポート プライオリティ
- デバウンス

channel-group force コマンドを使用して、ポートをチャネル グループへ強制的に追加できるようにした場合、パラメータは次のように処理されます。

- インターフェイスがポートチャネルに参加すると、次のパラメータは削除され、動作上ポート チャネルの値と置き換えられます。ただし、この変更は、インターフェイスの実行コンフィギュレーションには反映されません。
  - QoS
  - 帯域幅
  - 遅延
  - STP
  - サービス ポリシー
  - ACL
- インターフェイスがポート チャネルに追加またはポート チャネルから削除されても、次のパラメータはそのまま維持されます。
  - ビーコン
  - 説明
  - CDP
  - LACP ポート プライオリティ
  - デバウンス

- UDLD
- シャットダウン
- SNMP トラップ

ポート チャネルを使ったロード バランシング

Cisco NX-OS では、フレーム内のアドレスから生成されたバイナリ パターンの一部を数値に圧縮変換し、それを基にチャネル内のリンクを 1 つ選択することによって、ポート チャネルを構成するすべての動作中インターフェイス間でトラフィックのロード バランシングが行われます。ポート チャネルはデフォルトでロード バランシングを備えています。

基本設定では、次の基準を使用してリンクを選択します。

- レイヤ 2 フレームの場合は、送信元および宛先の MAC アドレスを使用します。
- レイヤ 3 フレームの場合は、送信元および宛先の MAC アドレスと送信元および宛先の Internet Protocol（IP）アドレスを使用します。
- レイヤ 4 フレームの場合は、送信元および宛先の MAC アドレスと送信元および宛先の Internet Protocol（IP）アドレスを使用します。

（注） レイヤ 4 フレームに対しては、必要に応じて送信元および宛先のポート番号を指定することもできます。

次のいずれかの方法（詳細については次の表を参照）を使用してポート チャネル全体をロード バランシングするようにスイッチを設定できます。

- 宛先 MAC アドレス
- 送信元 MAC アドレス
- 送信元および宛先 MAC アドレス
- 宛先 IP アドレス
- 送信元 IP アドレス
- 送信元および宛先 IP アドレス
- 宛先 TCP/UDP ポート番号
- 送信元 TCP/UDP ポート番号
- 送信元および宛先 TCP/UDP ポート番号

表 *3*：ポート チャネル ロードバランシング基準

設定	レイヤ 2 基準	レイヤ 3 基準	レイヤ 4 基準
宛先 MAC	宛先 MAC	宛先 MAC	宛先 MAC
送信元 MAC	送信元 MAC	送信元 MAC	送信元 MAC
送信元/宛先 MAC	送信元/宛先 MAC	送信元/宛先 MAC	送信元/宛先 MAC
Destination IP	宛先 MAC	宛先 MAC、宛先 IP	宛先 MAC、宛先 IP
Source IP	送信元 MAC	送信元 MAC、送信元 IP	送信元 MAC、送信元 IP
送信元/宛先 IP	送信元/宛先 MAC	送信元/宛先 MAC、送信元/宛先 IP	送信元/宛先 MAC、送信元/宛先 IP
宛先 TCP/UDP ポート	宛先 MAC	宛先 MAC、宛先 IP	宛先 MAC、宛先 IP、宛先ポート
送信元 TCP/UDP ポート	送信元 MAC	送信元 MAC、送信元 IP	送信元 MAC、送信元 IP、送信元ポート
送信元および宛先 TCP/UDP ポート	送信元/宛先 MAC	送信元/宛先 MAC、送信元/宛先 IP	送信元/宛先 MAC、送信元/宛先 IP、送信元/宛先ポート

使用している設定で最も多様なバランス基準を提供するオプションを使用してください。たとえば、ポート チャネルのトラフィックが 1 つの MAC アドレスにだけ送られ、ポート チャネルでのロード バランシングの基準としてその宛先 MAC アドレスが使用されている場合、ポート チャネルでは常にそのポート チャネル内の同じリンクが選択されます。したがって、送信元アドレスまたはIPアドレスを使用すると、結果的により優れたロードバランシングが行われることになります。

設定されているロードバランシング アルゴリズムにかかわらず、マルチキャスト トラフィックは次の方式を使用してポート チャネルのロード バランシングを行います。

- レイヤ 4 情報を持つマルチキャスト トラフィック：送信元 IP アドレス、送信元ポート、宛先 IP アドレス、宛先ポート
- レイヤ 4 情報を持たないマルチキャスト トラフィック：送信元 IP アドレス、宛先 IP アドレス
- 非 IP マルチキャスト トラフィック：送信元 MAC アドレス、宛先 MAC アドレス

（注） ハードウェア マルチキャスト hw-hash コマンドは、Cisco Nexus 3000 シリーズ スイッチおよび Cisco Nexus 3100 シリーズ スイッチではサポートされません。これらのスイッチではこのコマンドを設定しないことを推奨します。デフォルトでは、Cisco Nexus 3000 シリーズ スイッチおよびCisco Nexus 3100 シリーズ スイッチは、マルチキャスト トラフィックをハッシュします。

（注） ハードウェア マルチキャスト hw-hash コマンドは、Cisco Nexus 3500 シリーズ スイッチではサポートされません。これらのスイッチではこのコマンドを設定しないことを推奨します。

復元力のあるハッシュ

データセンターで使用される物理リンクの数が急増すると、障害物理リンクの数も増加する可能性があります。ポート チャネルまたは等コスト マルチパス（ECMP）グループのメンバー間でのフローのロードバランシングに使用される静的ハッシュ システムでは、各フローがリンクにハッシュされます。あるリンクで障害が発生すると、残りの現用リンク間ですべてのフローが再ハッシュされます。リンクへのフローのこの再ハッシュにより、障害リンクにハッシュされなかったフローであっても一部のパケットが間違った順序で配信されます。

この再ハッシュは、リンクがポート チャネルまたは等コスト マルチパス（ECMP）グループに追加された場合にも発生します。すべてのフローが、リンクの新しい番号全体にわたって再ハッシュされ、その結果として、一部のパケットが間違った順序で配信されます。復元力のあるハッシュは、ユニキャスト トラフィックだけをサポートします。

Cisco Nexus 3100 シリーズ スイッチの復元力のあるハッシュ システムは、フローを物理ポートにマッピングします。リンクに障害が発生すると、障害リンクに割り当てられているフローは、現用リンク間で均等に再分配されます。現用リンクを通過する既存のフローは再ハッシュされず、それらのパケットは間違った順序で配信されません。

復元力のあるハッシュは、ECMP グループによってのみ、またポート チャネル インターフェイスでのみサポートされます。リンクがポート チャネルまたはECMP グループに追加されると、既存のリンクにハッシュされるフローの一部が、既存のすべてのリンクにではなく、新しいリンクに再ハッシュされます。

復元力のあるハッシュは、IPv4およびIPv6ユニキャストトラフィックをサポートしますが、IPv4 マルチキャスト トラフィックはサポートしません。

NVGRE トラフィックのハッシュ

Network Virtualization using Generic Routing Encapsulatoin（NVGRE）を使用してネットワークを仮想化し、拡張することによって、分散データセンター間でレイヤ 2 およびレイヤ 3 トポロジが作成されるようにすることができます。NVGREはカプセル化とトンネリングを使用します。NVGRE エンドポイントは、物理ネットワークと仮想ネットワークの間のインターフェイスとして機能するネットワーク デバイスです。

データ フレームは、NVGRE エンドポイントで、GRE トンネリングを使用してカプセル化またはカプセル化解除されます。エンドポイントは、テナント ネットワーク ID（TNI）から各データ フレームの宛先アドレスを取得します。GRE ヘッダーの Key フィールドは、24 ビットの TNI を保持します。各 TNI は、特定のテナントのサブネット アドレスを表します。

Cisco NX-OS Release 6.0(2)U2(1) は、中継 NVGRE トラフィックのハッシュをサポートします。NVGRE トラフィックがポート チャネルまたは等コスト マルチパス（ECMP）経由で転送される際に GRE ヘッダーに存在する GRE Key フィールドがハッシュ計算に含まれるようにスイッチを設定できます。

対称ハッシュ

ポートチャネル上のトラフィックを効果的にモニタするには、ポートチャネルに接続された各インターフェイスがフォワードとリバースの両方のトラフィック フローを受信することが不可欠です。通常、フォワードとリバースのトラフィック フローが同じ物理インターフェイスを使用する保証はありません。ただし、ポート チャネルで対称ハッシュを有効にすると、双方向トラフィックが同じ物理インターフェイスを使用するように強制され、ポート チャネルの各物理インターフェイスが効果的に一連のフローにマッピングされます。

Cisco NX-OS Release 6.0(2)U2(3) で対称ハッシュが導入されました。対称ハッシュが有効になっている場合、ハッシュに使用されるパラメータ（送信元と宛先の IP アドレスなど）は、ハッシュ アルゴリズムに入る前に標準化されます。このプロセスにより、パラメータがリバースされる（フォワード トラフィックの送信元がリバース トラフィックの宛先になる）場合にハッシュ出力が同じになることが保証されます。このため、同じインターフェイスが選択されます。

対称ハッシュは、Cisco Nexus 3100 シリーズ スイッチでのみサポートされます。

対称ハッシュをサポートするのは、次のロードバランシング アルゴリズムのみです。

- source-dest-ip-only
- source-dest-port-only
- source-dest-ip
- source-dest-port
- source-dest-ip-gre

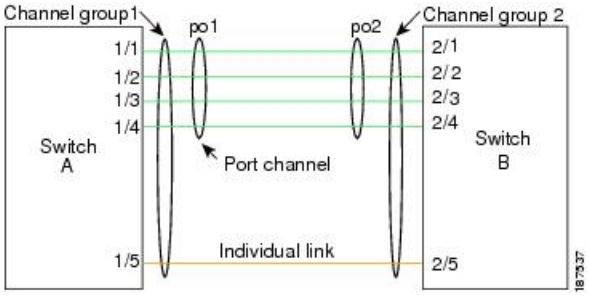
LACP の概要

LACP の概要

（注） LACP 機能を設定して使用にする場合は、あらかじめ LACP 機能をイネーブルにしておく必要があります。

次の図は、個々のリンクを個別リンクとして機能させるだけでなく LACP ポート チャネルおよびチャネル グループに組み込む方法を示したものです。

図 *4*: 個々のリンクをポート チャネルに組み込む



LACP を使用すると、スタティック ポート チャネルの場合と同じように、最大 16 個のインターフェイスを 1 つのチャネル グループにバンドルすることができます。

（注） ポート チャネルを削除すると、関連付けられたチャネル グループも Cisco NX-OS によって自動的に削除されます。すべてのメンバ インターフェイスは以前の設定に戻ります。

LACP 設定が 1 つでも存在する限り、LACP をディセーブルにはできません。

LACP ID パラメータ

LACP では次のパラメータが使用されます。

- LACP システム プライオリティ：LACP を稼働している各システムは、LACP システム プライオリティ値を持っています。このパラメータのデフォルト値である 32768 をそのまま使用するか、1 ～ 65535 の範囲で値を設定できます。LACP は、このシステム プライオリティと MAC アドレスを組み合わせてシステム ID を生成します。また、システム プライオリティを他のデバイスとのネゴシエーションにも使用します。システム プライオリティ値が大きいほど、プライオリティは低くなります。

（注） LACP システム ID は、LACP システム プライオリティ値と MAC アドレスを組み合わせたものです。

- LACP ポート プライオリティ：LACP を使用するように設定された各ポートには、LACP ポート プライオリティが割り当てられます。デフォルト値である 32768 をそのまま使用するか、1 ～ 65535 の範囲で値を設定できます。LACP では、ポート プライオリティおよびポート番号によりポート ID が構成されます。また、互換性のあるポートのうち一部を束ねることができない場合に、どのポートをスタンバイ モードにし、どのポートをアクティブ モードにするかを決定するのに、ポート プライオリティを使用します。LACP では、ポート プライオ

リティ値が大きいほど、プライオリティは低くなります。指定ポートが、より低い LACP プライオリティを持ち、ホット スタンバイ リンクではなくアクティブ リンクとして選択される可能性が最も高くなるように、ポート プライオリティを設定できます。

- LACP 管理キー：LACP は、LACP を使用するように設定された各ポート上のチャネル グループ番号に等しい管理キー値を自動的に設定します。管理キーにより、他のポートとともに集約されるポートの機能が定義されます。他のポートとともに集約されるポートの機能は、次の要因によって決まります。
  - ポートの物理特性（データ レート、デュプレックス機能、ポイントツーポイントまたは共有メディア ステートなど）
  - ユーザが作成した設定に関する制約事項

チャネル モード

ポートチャネルの個別インターフェイスは、チャネルモードで設定します。プロトコルを使用せずにスタティック ポート チャネルを稼働すると、そのチャネル モードは常に on に設定されます。デバイス上で LACP をグローバルにイネーブルにした後、各チャネルの LACP をイネーブルにします。それには、各インターフェイスのチャネル モードを active または passive に設定します。LACP チャネル グループを構成する個々のリンクについて、どちらかのチャネル モードを設定できます。

（注） active または passive のチャネル モードで、個々のインターフェイスを設定するには、まず、LACP をグローバルにイネーブルにする必要があります。

次の図は、チャネル モードをまとめたものです。

表 *4*：ポート チャネルの個別リンクのチャネル モード

チャネル モード	説明
passive	ポートをパッシブなネゴシエーション状態にする LACP モード。この状態では、ポートは受信した LACP パケットに応答はしますが、LACP ネゴシエーションを開始することはありません。
active	ポートをアクティブ ネゴシエーション ステートにする LACP モード。この場合ポートでは LACPパケットを送信することにより、他のポートとのネゴシエーションが開始されます。

チャネル モード	説明
on	すべてのスタティック ポート チャネル（つまり LACP を稼働していないポート チャネル）は、このモードのままになります。LACP をイネーブルにする前にチャネル モードを active または passive に変更しようとすると、デバイスがエラー メッセージを返します。 チャネルで LACP をイネーブルにするには、そのチャネルのインターフェイスでチャネル モードを active または passive に設定します。LACP は、on 状態のインターフェイスとネゴシエートする場合、LACP パケットを受信しないため、そのインターフェイスと個別のリンクを形成します。つまり、LACP チャネル グループには参加しません。

passive と active のどちらのモードでも、ポート速度やトランキング ステートなどの基準に基づいてポート チャネルを構成可能かどうかを判定するため、LACP によるポート間のネゴシエーションが行われます。passive モードは、リモート システム、つまり、パートナーが、LACP をサポートしているかどうかが不明な場合に便利です。

次の例に示したとおり、ポートは、異なる LACP モードであっても、それらのモード間で互換性があれば、LACP ポート チャネルを構成することができます。

- active モードのポートは、active モードの別のポートとともにポート チャネルを正しく形成できます。
- active モードのポートは、passive モードの別のポートとともにポート チャネルを形成できます。
- passive モードのポート同士ではポート チャネルを構成できません。これは、どちらのポートもネゴシエーションを開始しないためです。
- on モードのポートは LACP を実行していません。

LACP マーカー レスポンダ

ポート チャネルを使用すると、リンク障害やロード バランシング動作に伴って、データ トラフィックが動的に再配信される場合があります。LACP では、マーカー プロトコルを使用して、こうした再配信によってフレームが重複したり順序が変わったりしないようにします。Cisco NX-OS は、マーカー レスポンダだけをサポートしています。

LACP がイネーブルのポート チャネルとスタティック ポート チャネルの相違点

次の表は、LACP がイネーブルのポート チャネルとスタティック ポート チャネルとの主な相違点をまとめたものです。設定の最大制限値の詳細については、デバイスの『*Verified Scalability*』マニュアルを参照してください。

表 *5*：*LACP* がイネーブルのポート チャネルとスタティック ポート チャネル

構成	LACP がイネーブルのポート チャネル	スタティック ポート チャネル
適用されるプロトコル	グローバルにイネーブル化	なし。
リンクのチャネル モード	次のいずれか。 • Active • Passive	on モードのみ

LACP ポート チャネルの最小リンクおよび MaxBundle

ポート チャネルは、同様のポートを集約し、単一の管理可能なインターフェイスの帯域幅を増加させます。最小リンクおよび MaxBundle 機能の導入により、LACP ポート チャネル動作を改善し、単一の管理可能なインターフェイスの帯域幅を増加させます。

LACP ポート チャネルの MinLink 機能は次の処理を実行します。

- LACP ポート チャネルにリンクし、バンドルする必要があるポート チャネル インターフェイスの最小数を設定します。
- 低帯域幅の LACP ポート チャネルがアクティブにならないようにします。
- 少数のアクティブ メンバ ポートだけが必要な最小帯域幅を提供する場合、LACP ポート チャネルが非アクティブになります。

LACP MaxBundle は、LACP ポート チャネルで許可されるバンドル ポートの最大数を定義します。LACP MaxBundle 機能では、次の処理が行われます。

- LACP ポート チャネルのバンドル ポート数の上限を定義します。
- バンドル ポートがより少ない場合のホット スタンバイ ポートを可能にします（たとえば、5 つのポートを含む LACP ポート チャネルにおいて、ホット スタンバイ ポートとしてそれらのポートの 2 つを指定できます）。

（注） 最小リンクおよびmaxbundle機能は、LACPポート チャネルだけで動作します。ただし、デバイスでは非LACPポート チャネルでこの機能を設定できますが、機能は動作しません。

ポート チャネルの設定

ポート チャネルの作成

チャネル グループを作成する前にポート チャネルを作成します。Cisco NX-OSは、対応するチャネル グループを自動的に作成します。

（注） LACPベースのポート チャネルを使用する場合は、LACPをイネーブルにする必要があります。

手順

	コマンドまたはアクション	目的
ステップ1	switch# **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2	switch(config)# **interface port-channel***channel-number*	設定するポート チャネル インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。範囲は1～4096です。チャネル グループがまだ存在していなければ、Cisco NX-OSによって自動的に作成されます。
ステップ3	switch(config)# **no interface port-channel***channel-number*	ポート チャネルを削除し、関連するチャネル グループを削除します。

次の例は、ポート チャネルの作成方法を示しています。

```
switch# configure terminal
switch (config)# interface port-channel 1
```

ポート チャネルへのポートの追加

新規のチャネル グループ、または他のポートがすでに属しているチャネル グループにポートを追加できます。ポート チャネルがない場合は、Cisco NX-OSによってこのチャネル グループに関連付けられたポート チャネルが作成されます。

（注） LACP ベースのポート チャネルを使用する場合は、LACP をイネーブルにする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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 2	switch(config)# **interface***typeslot*/*port*	チャネル グループに追加するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# **switchport mode trunk**	（任意） 指定したインターフェイスをトランク ポートとして設定します。
ステップ 4	switch(config-if)# **switchport trunk** {**allowed vlan***vlan-id* | **native vlan***vlan-id*}	（任意） トランク ポートに必要なパラメータを設定します。
ステップ 5	switch(config-if)# **channel-group***channel-number*	チャネル グループ内にポートを設定し、モードを設定します。channel-number の指定できる範囲は 1 ～ 4096 です。ポート チャネルがない場合は、Cisco NX-OS によってこのチャネル グループに関連付けられたポート チャネルが作成されます。これを、暗黙的なポート チャネル作成と言います。
ステップ 6	switch(config-if)# **no channel-group**	（任意） チャネル グループからポートを削除します。チャネル グループから削除されたポートは元の設定に戻ります。

次に、イーサネット インターフェイス 1/4 をチャネル グループ 1 に追加する例を示します。

```
switch# configure terminal
switch (config)# interface ethernet 1/4
switch(config-if)# switchport mode trunk
switch(config-if)# channel-group 1
```

ポート チャネルを使ったロード バランシングの設定

デバイス全体に適用されるポート チャネル用のロードバランシング アルゴリズムを設定できます。

（注） LACP ベースのポート チャネルを使用する場合は、LACP をイネーブルにする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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 2	switch(config)# **port-channel load-balance ethernet** {[**destination-ip** | **destination-ip-gre** |**destination-mac** | **destination-port** | **source-dest-ip** | **source-dest-ip-gre** |**source-dest-mac** | **source-dest-port** | **source-ip** | **source-ip-gre** |**source-mac** | **source-port**] **symmetric** | **crc-poly**}	デバイスのロードバランシング アルゴリズムおよびハッシュを指定します。指定可能なアルゴリズムはデバイスによって異なります。デフォルトは **source-dest-mac** です。 （注） ハッシュ計算にNVGREキーが含まれるようにするには、オプションの **destination-ip-gre**、**source-dest-ip-gre**、および **source-ip-gre** キーワードを使用します。ポート チャネルの場合、デフォルトではNVGREキーが含まれません。これらのオプションのキーワードを使用して明示的に設定する必要があります。 対称ハッシュを有効または無効にするには、オプションの **symmetric** キーワードを使用します。対称ハッシュにより、双方向のトラフィックで同じ物理インターフェイスを使用することが強制されます。対称ハッシュをサポートするのは、次のロードバランシング アルゴリズムのみです。 • source-dest-ip-only • source-dest-port-only • source-dest-ip • source-dest-port • source-dest-ip-gre
ステップ 3	switch(config)# **no port-channel load-balance ethernet**	（任意） ロードバランシング アルゴリズムをデフォルトの source-dest-mac に戻します。

	コマンドまたはアクション	目的
ステップ 4	switch# **show port-channel load-balance**	（任意） ポート チャネル ロードバランシング アルゴリズムを表示します。

次の例は、ポート チャネルに対して送信元 IP によるロード バランシングを設定する方法を示したものです。

```
switch# configure terminal
switch (config)# port-channel load-balance ethernet source-ip
```

次に、ポート チャネルの対称ハッシュを設定する例を示します。

```
switch# configure terminal
switch (config)# port-channel load-balance ethernet source-dest-ip-only symmetric
```

LACP のイネーブル化

LACP はデフォルトではディセーブルです。LACP の設定を開始するには、LACP をイネーブルにする必要があります。LACP 設定が 1 つでも存在する限り、LACP をディセーブルにはできません。

LACP は、LAN ポート グループの機能を動的に学習し、残りの LAN ポートに通知します。LACP では、適合する複数のイーサネット リンクが検出されると、これらのリンクが 1 つのポート チャネルにグループ化されます。次に、ポート チャネルは単一ブリッジ ポートとしてスパニングツリーに追加されます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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 2	switch(config)# **feature lacp**	スイッチ上で LACP をイネーブルにします。
ステップ 3	switch(config)# **show feature**	（任意） イネーブルにされた機能を表示します。

次に、LACP をイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# feature lacp
```

ポートに対するチャネル モードの設定

LACP ポート チャネルのそれぞれのリンクのチャネル モードを active または passive に設定できます。このチャネル コンフィギュレーション モードを使用すると、リンクは LACP で動作可能になります。

関連するプロトコルを使用せずにポート チャネルを設定すると、リンク両端のすべてのインターフェイスでは on チャネル モードが維持されます。

はじめる前に

LACP 機能がイネーブルになっていることを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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 2	switch(config)# **interface***typeslot*/*port*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# **channel-group** *channel-number* [**force**] [**mode** {**on** | **active** | **passive**}]	ポート チャネルのリンクのポート モードを指定します。LACP をイネーブルにしたら、各リンクまたはチャネル全体を active または passive に設定します。 **force**：LAN ポートをチャネル グループに強制的に追加することを指定します。 **mode**：インターフェイスのポート チャネル モードを指定します。 **active**：これを指定すると、LACP をイネーブルにした時点で、指定したインターフェイス上で LACP がイネーブルになります。インターフェイスはアクティブ ネゴシエーション ステートになります。この場合ポートでは、LACP パケットを送信することにより、他のポートとのネゴシエーションが開始されます。 **on**：（デフォルト モード）これを指定すると、LACP を実行していないすべてのポート チャネルに対して、このモードが維持されます。 **passive**：LACP 装置が検出された場合に限り、LACP をイネーブルにします。インターフェイスはパッシブ ネゴシエーション ステートになります。この場合ポートでは、受信した LACP パケットへの応答は行われますが、LACP ネゴシエーションは開始されません。

	コマンドまたはアクション	目的
		関連するプロトコルを使用せずにポートチャネルを実行する場合、チャネル モードは常に on です。
ステップ 4	switch(config-if)# **no channel-group***number***mode**	指定インターフェイスのポート モードを on に戻します

次に、チャネル グループ 5 のイーサネット インターフェイス 1/4 で、LACP がイネーブルなインターフェイスを active ポート チャネル モードに設定する例を示します。

```
switch# configure terminal
switch (config)# interface ethernet 1/4
switch(config-if)# channel-group 5 mode active
```

LACP ポート チャネルの MinLink の設定

MinLink 機能は、LACP ポート チャネルだけで動作します。デバイスでは非 LACP ポート チャネルでこの機能を設定できますが、機能は動作しません。

重要 LACP ポート チャネルの両側（つまり、両方のスイッチ）で LACP MinLink 機能を設定することを推奨します。ポート チャネルの片側だけで **lacp min-links** コマンドを設定すると、リンク フラッピングが発生する可能性があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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 2	switch(config)# **interface port-channel***number*	設定するインターフェイスを指定します。
ステップ 3	switch(config-if)# [**no**] **lacp min-links***number*	最小リンクの数を設定します。 *number* のデフォルト値は、1 です。指定できる範囲は 1 ～ 16 です。 （注） Release 7.0(3)I2(1) 以降でサポートされる LACP MinLink の最大数は 16 です。 この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

	コマンドまたはアクション	目的
ステップ 4	switch(config)# **show running-config interface port-channel***number*	（任意） インターフェイスのポート チャネル設定を表示します。

次に、全体として*up*とラベル付けされたバンドルに対してアップしている必要があるリンクの最小数を設定する例を示します。

```
switch#configure terminal
switch(config)#interface port-channel 3
switch(config-if)#lacp min-links 3
switch(config)#show running-config interface port-channel 3
```

LACP ポートチャネル MaxBundle の設定

LACP の maxbundle 機能を設定できます。最小リンクと maxbundles は LACP でのみ動作します。ただし、非 LACP ポート チャネルに対してこれらの機能の CLI コマンドを入力できますが、これらのコマンドは動作不能です。

（注） デフォルトのポートチャネル max-bundle 設定を復元するには、**no lacp max-bundle** コマンドを使用します。

コマンド	目的
no lacp max-bundle 例： `switch(config)# no lacp max-bundle`	デフォルトのポートチャネル max-bundle 設定を復元します。

はじめる前に

適切なポートチャネル インターフェイスであることを確認します。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		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 2	**interface port-channel***number*
	
	例：
	`switch(config)# interface port-channel 3`
	`switch(config-if)#`
		設定するインターフェイスを選択します。

ステップ 3	**lacp max-bundle***number* 例： `switch(config-if)# lacp max-bundle <number>`	ポート チャネルで許可されるアクティブなバンドル LACP ポートの最大数を設定します。 ポート チャネルの max-bundle のデフォルト値は 16 です。指定できる範囲は 1 ～ 32 です。 （注） デフォルト値は 16 ですが、ポート チャネルのアクティブ メンバー数は、ポートチャネルで許可されている *pc_max_links_config* および *pc_max_active_members* の最小数です。
ステップ 4	**show running-config interface port-channel**<*number*> 例： `switch(config-if)# show running-config interface port-channel 3`	（オプション）インターフェイスのポートチャネル設定を表示します。

次に、アクティブなバンドル LACP ポートの最大数を設定する例を示します。

```
switch# configure terminal
switch# interface port-channel 3
switch (config-if)# lacp max-bundle 3
switch (config-if)# show running-config interface port-channel 3
```

LACP 高速タイマー レートの設定

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

はじめる前に

LACP 機能がイネーブルになっていることを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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 2	switch(config)# **interface***typeslot*/*port*	設定するインターフェイスを指定します。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。 （注） Release 7.0(3)I2(1) 以降では、管理上ダウンしているポートでのみ LACP レートを設定できます。
ステップ 3	switch(config-if)# **lacp rate fast**	LACPがサポートされているインターフェイスにLACP制御パケットを送信する際のレートとして高速レート（1 秒）を設定します。

次の例は、イーサネット インターフェイス 1/4 に対して LACP 高速レートを設定する方法を示したものです。

```
switch# configure terminal
switch(config)# interface ethernet 1/4
switch(config-if)# lacp rate fast
```

次の例は、イーサネット インターフェイス 1/4 の LACP レートをデフォルトのレート（30 秒）に戻す方法を示したものです。

```
switch# configure terminal
switch(config)# interface ethernet 1/4
switch(config-if)# no lacp rate fast
```

LACP のシステム プライオリティおよびシステム ID の設定

LACP システム ID は、LACP システム プライオリティ値と MAC アドレスを組み合わせたものです。

はじめる前に

LACP 機能がイネーブルになっていることを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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 2	switch(config)# **lacp system-priority***priority*	LACP で使用するシステム プライオリティを設定します。指定できる範囲は 1 ～ 65535 で、値が大きいほどプライオリティは低くなります。デフォルト値は 32768 です。
ステップ 3	switch# **show lacp system-identifier**	（任意） LACP システム識別子を表示します。

次に、LACP システム プライオリティを 2500 に設定する例を示します。

```
switch# configure terminal
switch(config)# lacp system-priority 2500
```

LACP ポート プライオリティの設定

LACP ポート チャネルの各リンクに対して、ポート プライオリティの設定を行うことができます。

はじめる前に

LACP 機能がイネーブルになっていることを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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 2	switch(config)# **interface***typeslot*/*port*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# **lacp port-priority***priority*	LACP で使用するポート プライオリティを設定します。指定できる範囲は 1 ～ 65535 で、値が大きいほどプライオリティは低くなります。デフォルト値は 32768 です。

次に、イーサネット インターフェイス 1/4 の LACP ポート プライオリティを 40000 に設定する例を示します。

```
switch# configure terminal
switch (config)# interface ethernet 1/4
switch(config-if)# lacp port priority 40000
```

ポート チャネル設定の確認

次のコマンドを使用すると、ポート チャネルの設定情報を確認できます。

コマンド	目的
show interface port channel*chennal-number*	ポート チャネル インターフェイスのステータスを表示します。
show feature	イネーブルにされた機能を表示します。
show resource	システムで現在利用可能なリソースの数を表示します。
show lacp {**counters** | **interface***typeslot*/*port* | **neighbor** | **port-channel** | **system-identifier**}	LACP 情報を表示します。
show port-channel compatibility-parameters	ポート チャネルに追加するためにメンバ ポート間で同じにするパラメータを表示します。
show port-channel database [**interface port-channel***channel-number*]	1 つ以上のポート チャネル インターフェイスの集約状態を表示します。
show port-channel summary	ポート チャネル インターフェイスの概要を表示します。
show port-channel traffic	ポート チャネルのトラフィック統計情報を表示します。
show port-channel usage	使用済みおよび未使用のチャネル番号の範囲を表示します。
show port-channel database	現在実行中のポート チャネル機能に関する情報を表示します。
show port-channel load-balance	ポート チャネルによるロードバランシングについての情報を表示します。

ポートチャネルメンバシップ整合性チェッカのトリガー

ポート チャネル メンバシップ整合性チェッカを手動でトリガーして、ポート チャネル上のすべてのポートのハードウェア設定とソフトウェア設定を比較し、結果を表示することができます。ポートチャネルメンバシップ整合性チェッカを手動でトリガーして結果を表示するには、次のコマンドを特定のモードで使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **show consistency-checker membership port-channels**	ポート チャネルのメンバー ポートに対するポート チャネル メンバーシップ整合性検査を開始して結果を表示します。

次に、ポートチャネルメンバーシップ整合性検査をトリガーして結果を表示する例を示します。

```
switch# show consistency-checker membership port-channels
Checks: Trunk group and trunk membership table.
Consistency Check: PASSED
 No Inconsistencies found for port-channel1111:
  Module:1, Unit:0
     ['Ethernet1/4', 'Ethernet1/5', 'Ethernet1/6']
 No Inconsistencies found for port-channel2211:
  Module:1, Unit:0
     ['Ethernet1/7', 'Ethernet1/8', 'Ethernet1/9', 'Ethernet1/10']
 No Inconsistencies found for port-channel3311:
  Module:1, Unit:0
     ['Ethernet1/11', 'Ethernet1/12', 'Ethernet1/13', 'Ethernet1/14']
 No Inconsistencies found for port-channel4095:
  Module:1, Unit:0
     ['Ethernet1/33', 'Ethernet1/34', 'Ethernet1/35', 'Ethernet1/36', 'Ethernet1
/37', 'Ethernet1/38', 'Ethernet1/39', 'Ethernet1/40', 'Ethernet1/41', 'Ethernet1
/42', 'Ethernet1/43', 'Ethernet1/44', 'Ethernet1/45', 'Ethernet1/46', 'Ethernet1
/47', 'Ethernet1/48', 'Ethernet1/29', 'Ethernet1/30', 'Ethernet1/31', 'Ethernet1
/32']
```

ロードバランシング発信ポート ID の確認

コマンドに関する注意事項

show port-channel load-balance コマンドを使用すると、ポート チャネルにおいて特定のフレームがいずれのポートにハッシュされるかを確認することができます。正確な結果を取得するためには、VLAN および宛先 MAC を指定する必要があります。

（注） ポート チャネル内にポートが 1 つしかない場合などには、一部のトラフィック フローはハッシュの対象になりません。

show port-channel load-balance コマンドは、ユニキャスト トラフィック ハッシュのみをサポートします。マルチキャスト トラフィック ハッシュはサポートされません。

ロードバランシング発信ポート ID を表示する場合は、次のいずれかの操作を実行します。

コマンド	目的
switch# **show port-channel load-balance forwarding-path interface port-channel***port-channel-id***vlan** vlan-id **dst-ipsrc-ipdst-macsrc-macl4-src-port***port-id* **l4-dst-port***port-id***ether-type***ether-type***ip-proto***ip-proto*	発信ポート ID を表示します。

例

次に、ロードバランシング発信ポート ID を表示する例を示します。

```
switch# show port-channel load-balance forwarding-path interface port-channel 10 vlan 1
dst-ip 1.225.225.225 src-ip 1.1.10.10 src-mac aa:bb:cc:dd:ee:ff
l4-src-port 0 l4-dst-port 1
Missing params will be substituted by 0's. Load-balance Algorithm on switch: source-dest-port
 crc8_hash:204 Outgoing port id: Ethernet 1/1 Param(s) used to calculate load balance:
dst-port: 0
src-port: 0
dst-ip: 1.225.225.225
src-ip: 1.1.10.10
dst-mac: 0000.0000.0000
src-mac: aabb.ccdd.eeff
```

ポート チャネルの機能履歴

機能名	リリース	機能情報
最小リンク	5.0(3)U3(1)	最小リンク機能の設定および使用に関する情報を追加しました。

ポート プロファイル

7.0(3)I4(1) 以降、多くのインターフェイス コマンドを含むポート プロファイルを作成し、一定範囲のインターフェイスにそのポートプロファイルを適用できます。ポートプロファイルはそれぞれ特定のタイプのインターフェイスにだけ適用できます。次のインターフェイスから選択できます。

- イーサネット
- VLAN ネットワーク インターフェイス
- ポート チャネル

インターフェイス タイプにイーサネットまたはポート チャネルを選択する場合、ポート プロファイルはデフォルト モードになります。デフォルト モードはレイヤ 3 です。ポート プロファイルをレイヤ 2 モードに変更するには、**switchport** コマンドを入力します。

ポート プロファイルをインターフェイスまたはインターフェイスの範囲にアタッチするときにポートプロファイルを継承します。ポートプロファイルをインターフェイスまたはインターフェイスの範囲にアタッチ、または継承する場合、そのポート プロファイルのすべてのコマンドがインターフェイスに適用されます。また、ポートプロファイルには、別のポートプロファイルの設定を継承することができます。別のポートプロファイルを継承した場合、最初のポートプロファイルでは、それを継承した第 2 のポート プロファイルに含まれるすべてのコマンドは、最初のポート プロファイルとは競合していないものと見なされます。4 つのレベルの継承がサポートされています。任意の数のポート プロファイルで同じポート プロファイルを継承できます。

次の注意事項に従って、インターフェイスまたはインターフェイスの範囲で継承されたコマンドが適用されます。

- 競合が発生した場合は、インターフェイス モードで入力したコマンドがポート プロファイルのコマンドに優先します。しかし、ポートプロファイルはそのコマンドをポートプロファイルに保持します。
- ポートプロファイルのコマンドは、port-profile コマンドがデフォルト コマンドで明示的に上書きされていない限り、インターフェイスのデフォルト コマンドに優先します。
- 一定範囲のインターフェイスが 2 つ目のポート プロファイルを継承すると、矛盾がある場合、最初のポート プロファイルのコマンドが 2 つ目のポート プロファイルのコマンドを無効にします。
- ポート プロフィルをインターフェイスまたはインターフェイスの範囲に継承した後、インターフェイス コンフィギュレーション レベルで新しい値を入力して、個々の設定値を上書きできます。インターフェイス コンフィギュレーション レベルで個々の設定値を削除すると、インターフェイスではポート プロファイル内の値が再度使用されます。
- ポート プロファイルに関連したデフォルト設定はありません。

指定するインターフェイス タイプにより、コマンドのサブセットが port-profile コンフィギュレーション モードで使用できます。

ポートプロファイル設定をインターフェイスに適用するには、そのポートプロファイルをイネーブルにする必要があります。ポートプロファイルをイネーブルにする前に、そのポートプロファイルを一定範囲のインターフェイスに設定し、継承できます。その後、指定されたインターフェイスで設定が実行されるように、そのポート プロファイルをイネーブルにします。

元のポート プロファイルに 1 つ以上のポート プロファイルを継承する場合、最後に継承されたポート プロファイルだけをイネーブルにする必要があります。こうすれば、その前までのポートプロファイルがイネーブルにされたと見なされます。

ポート プロファイルをインターフェイスの範囲から削除する場合、まずインターフェイスからコンフィギュレーションを取り消して、ポートプロファイル リンク自体を削除します。また、ポートプロファイルを削除すると、インターフェイス コンフィギュレーションが確認され、直接入力された interface コマンドで無効にされた port-profile コマンドをスキップするか、それらのコマンドをデフォルト値に戻します。

他のポート プロファイルにより継承されたポート プロファイルを削除する場合は、そのポート プロファイルを削除する前に継承を無効にする必要があります。

また、ポート プロファイルを元々適用していたインターフェイスのグループの中から、そのプロファイルを削除するインターフェイスを選択することもできます。たとえば、1 つのポート プロファイルを設定した後、10個のインターフェイスに対してそのポートプロファイルを継承するよう設定した場合、その 10 個のうちいくつかのインターフェイスからのみポート プロファイルを削除することができます。ポート プロファイルは、適用されている残りのインターフェイスで引き続き動作します。

インターフェイス コンフィギュレーション モードを使用して指定したインターフェイスの範囲の特定のコンフィギュレーションを削除する場合、そのコンフィギュレーションもそのインターフェイスの範囲のポート プロファイルからのみ削除されます。たとえば、ポート プロファイル内にチャネル グループがあり、インターフェイス コンフィギュレーション モードでそのポート チャネルを削除する場合、指定したポートチャネルも同様にポートプロファイルから削除されます。

デバイスの場合と同様、オブジェクトをインターフェイスに適用せずに、そのオブジェクトのコンフィギュレーションをポート プロファイルに入力できます。たとえば、仮想ルーティングおよび転送（VRF）インスタンスをシステムに適用しなくても、設定できます。その VRF と関連するコンフィギュレーションをポート プロファイルから削除しても、システムに影響はありません。

インターフェイスまたはインターフェイスの範囲のポート プロファイルを継承し、特定の設定値を削除した後、その port-profile コンフィギュレーションは指定のインターフェイスでは動作しません。

ポート プロファイルを誤ったタイプのインターフェイスに適用しようとすると、システムによりエラーが返されます。

ポート プロファイルをイネーブル化、継承、または変更しようとすると、システムによりチェックポイントが作成されます。ポート プロファイル設定が正常に実行されなかった場合は、システムによりその前の設定までロールバックされ、エラーが返されます。ポートプロファイルは部分的にだけ適用されることはありません。

ポート プロファイルの設定

7.0(3)I4(1) 以降、いくつかの設定パラメータを一定範囲のインターフェイスに同時に適用できます。範囲内のすべてのインターフェイスが同じタイプである必要があります。また、1 つのポート プロファイルから別のポート プロファイルに設定を継承することもできます。システムは4 つのレベルの継承をサポートしています。

ポート プロファイルの作成

デバイスにポート プロファイルを作成できます。各ポート プロファイルは、タイプにかかわらず、ネットワーク上で一意の名前を持つ必要があります。

（注） ポート プロファイル名には、次の文字のみを使用できます。

- a ～ z
- A ～ Z
- 0 ～ 9
- 特殊文字は、以下を除き使用できません。
  - .
  - -
  - _

手順

	コマンドまたはアクション	目的
ステップ 1	**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 2	**port-profile** [**type** {**ethernet** | **interface-vlan** | **port-channel**}] *name*	指定されたタイプのインターフェイスのポートプロファイルを作成して命名し、ポートプロファイル 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	**exit**	ポートプロファイル コンフィギュレーション モードを終了します。
ステップ 4	**show port-profile**	（任意） ポート プロファイル設定を表示します。
ステップ 5	**copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次に、イーサネット インターフェイスに対して test という名前のポート プロファイルを作成する例を示します。

```
switch# configure terminal
switch(config)# port-profile type ethernet test
switch(config-ppm)#
```

ポートプロファイルコンフィギュレーションモードの開始およびポート プロファイルの修正

ポート プロファイル コンフィギュレーション モードを開始し、ポート プロファイルを修正できます。ポート プロファイルを修正するには、ポートプロファイル コンフィギュレーション モードを開始する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**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 2	**port-profile** [**type** {**ethernet** | **interface-vlan** | **port-channel**}] *name*	指定されたポートプロファイルのポートプロファイル コンフィギュレーション モードを開始し、プロファイルの設定を追加または削除します。
ステップ 3	**exit**	ポートプロファイルコンフィギュレーションモードを終了します。
ステップ 4	**show port-profile**	（任意） ポート プロファイル設定を表示します。
ステップ 5	**copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

次に、指定されたポート プロファイルのポート プロファイル コンフィギュレーション モードを開始し、すべてのインターフェイスを管理的にアップする例を示します。

```
switch# configure terminal
switch(config)# port-profile type ethernet test
switch(config-ppm)# no shutdown
switch(config-ppm)#
```

一定範囲のインターフェイスへのポートプロファイルの割り当て

単独のインターフェイスまたはある範囲に属する複数のインターフェイスにポート プロファイルを割り当てることができます。すべてのインターフェイスが同じタイプである必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**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 2	**interface** [**ethernet***slot/port* | **interface-vlan***vlan-id* | **port-channel***number*]	インターフェイスの範囲を選択します。
ステップ 3	**inherit port-profile***name*	指定したポート プロファイルを、選択したインターフェイスに割り当てます。
ステップ 4	**exit**	ポート プロファイル コンフィギュレーション モードを終了します。
ステップ 5	**show port-profile**	（任意） ポート プロファイル設定を表示します。
ステップ 6	**copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次に、イーサネット インターフェイス 7/3 ～ 7/5、10/2、および 11/20 ～ 11/25 に adam という名前のポート プロファイルを割り当てる例を示します。

```
switch# configure terminal
switch(config)# interface ethernet7/3-5, ethernet10/2, ethernet11/20-25
switch(config-if)# inherit port-profile adam
switch(config-if)#
```

特定のポート プロファイルのイネーブル化

ポートプロファイル設定をインターフェイスに適用するには、そのポートプロファイルをイネーブルにする必要があります。ポートプロファイルをイネーブルにする前に、そのポートプロファイルを一定範囲のインターフェイスに設定し、継承できます。その後、指定されたインターフェイスで設定が実行されるように、そのポート プロファイルをイネーブルにします。

元のポート プロファイルに 1 つ以上のポート プロファイルを継承する場合、最後に継承されたポート プロファイルだけをイネーブルにする必要があります。こうすれば、その前までのポート プロファイルがイネーブルにされたと見なされます。

ポートプロファイルをイネーブルまたはディセーブルにするには、ポートプロファイル コンフィギュレーション モードを開始する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**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 2	**port-profile** [**type** {**ethernet** | **interface-vlan** | **port-channel**}] *name*	指定されたタイプのインターフェイスのポートプロファイルを作成して命名し、ポートプロファイル 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	**state enabled**	そのポートプロファイルをイネーブルにします。
ステップ 4	**exit**	ポートプロファイルコンフィギュレーションモードを終了します。
ステップ 5	**show port-profile**	（任意） ポート プロファイル設定を表示します。
ステップ 6	**copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次の例は、ポート プロファイル コンフィギュレーション モードを開始し、ポート プロファイルをイネーブルにする方法を示したものです。

```
switch# configure terminal
switch(config)# port-profile type ethernet test
switch(config-ppm)# state enabled
switch(config-ppm)#
```

ポート プロファイルの継承

ポート プロファイルを既存のポート プロファイルに継承できます。システムは 4 つのレベルの継承をサポートしています。

手順

	コマンドまたはアクション	目的
ステップ 1	**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 2	**port-profile***name*	指定されたポートプロファイルに対して、ポートプロファイル 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	**inherit port-profile***name*	別のポートプロファイルを既存のポートプロファイルに継承します。元のポート プロファイルは、継承されたポート プロファイルのすべての設定を想定します。
ステップ 4	**exit**	ポートプロファイル コンフィギュレーション モードを終了します。
ステップ 5	**show port-profile**	（任意） ポート プロファイル設定を表示します。
ステップ 6	**copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次の例では、adam という名前のポート プロファイルを test という名前のポート プロファイルに継承する方法を示します。

```
switch# configure terminal
switch(config)# port-profile test
switch(config-ppm)# inherit port-profile adam
switch(config-ppm)#
```

一定範囲のインターフェイスからのポートプロファイルの削除

プロファイルを適用した一部またはすべてのインターフェイスから、ポート プロファイルを削除できます。この設定は、インターフェイス コンフィギュレーション モードで行います。

手順

	コマンドまたはアクション	目的
ステップ 1	**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 2	**interface** [**ethernet***slot/port* | **interface-vlan***vlan-id* | **port-channel***number*]	インターフェイスの範囲を選択します。
ステップ 3	**no inherit port-profile***name*	選択したインターフェイスへの指定したポート プロファイルの割り当てを解除します。
ステップ 4	**exit**	ポート プロファイル コンフィギュレーション モードを終了します。
ステップ 5	**show port-profile**	（任意） ポート プロファイル設定を表示します。
ステップ 6	**copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次に、イーサネット インターフェイス 7/3 ～ 7/5、10/2、および 11/20 ～ 11/25 に対する adam という名前のポート プロファイルの割り当てを解除する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 7/3-5, 10/2, 11/20-25
switch(config-if)# no inherit port-profile adam
switch(config-if)#
```

継承されたポート プロファイルの削除

継承されたポート プロファイルを削除できます。この設定は、ポート プロファイル モードで行います。

手順

	コマンドまたはアクション	目的
ステップ 1	**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 2	**port-profile***name*	指定されたポート プロファイルに対して、ポート プロファイル コンフィギュレーション モードを開始します。
ステップ 3	**no inherit port-profile***name*	このポート プロファイルから継承されたポート プロファイルを削除します。

	コマンドまたはアクション	目的
ステップ 4	**exit**	ポートプロファイルコンフィギュレーションモードを終了します。
ステップ 5	**show port-profile**	（任意） ポート プロファイル設定を表示します。
ステップ 6	**copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

次の例では、adam という名前の継承されたポート プロファイルを test という名前のポート プロファイルから削除する方法を示します。

```
switch# configure terminal
switch(config)# port-profile test
switch(config-ppm)# no inherit port-profile adam
switch(config-ppm)#
```

第 5 章

IP トンネルの設定

この章の内容は、次のとおりです。

IP トンネルについて

IP トンネルを使うと、同じレイヤまたは上位レイヤのプロトコルをカプセル化して、2 台のデバイス間で作成されたトンネルを通じて IP に結果を転送できます。

IP トンネルは次の 3 つの主要コンポーネントで構成されています。

- パッセンジャ プロトコル：カプセル化する必要があるプロトコル。パッセンジャ プロトコルの例には IPv4 があります。
- キャリア プロトコル：パッセンジャ プロトコルをカプセル化するために使用するプロトコル。Cisco NX-OS は、キャリア プロトコルとして、Generic Routing Encapsulation（GRE）と、IP-in-IP カプセル化およびカプセル化解除をサポートします。

- トランスポート プロトコル：カプセル化したプロトコルを伝送するために使用するプロトコル。トランスポート プロトコルの例には IPv4 があります。

IP トンネルは IPv4 などのパッセンジャ プロトコルを使用し、このプロトコルを GRE などのキャリア プロトコル内にカプセル化します。次に、このキャリア プロトコルは IPv4 などのトランスポート プロトコルを通じてデバイスから送信されます。

対応する特性を持つトンネル インターフェイスをトンネルの両端にそれぞれ設定します。

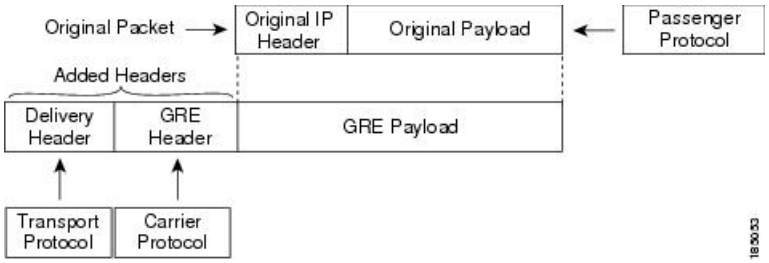
設定の前にトンネル機能をイネーブルにする必要があります。

GRE トンネル

さまざまなパッセンジャ プロトコルのキャリア プロトコルとして GRE を使用できます。トンネル インターフェイスの選択は、PBR ポリシーを基本とすることもできます。

この図は、GRE トンネルの IP トンネルのコンポーネントを示しています。オリジナルのパッセンジャ プロトコル パケットは GRE ペイロードとなり、デバイスはパケットに GRE ヘッダーを追加します。次にデバイスはトランスポート プロトコル ヘッダーをパケットに追加して送信します。

図 *5*：*GRE PDU*



ポイントツーポイント IP-in-IP トンネルのカプセル化およびカプセル化解除

ポイントツーポイント IP-in-IP の encapsulation および decapsulation は、送信元トンネル インターフェイスから宛先トンネル インターフェイスにカプセル化されたパケットを送信するために作成できるトンネルのタイプです。これらのトンネル インターフェイスの選択は、PBR ポリシーを基本とすることもできます。このタイプのトンネルは、着信トラフィックと発信トラフィックの両方を伝送します。

マルチポイント IP-in-IP トンネルのカプセル化解除

マルチポイント IP-in-IP の decapsulate-any は、任意の数の IP-in-IP トンネルから 1 つのトンネル インターフェイスにパケットのカプセル化を解除するために作成できるトンネルのタイプです。こ

のトンネルは発信トラフィックを伝送しません。ただし、任意の数のリモートトンネルエンドポイントが、このように設定されたトンネルを宛先として使用することができます。

IP トンネルのライセンス要件

製品	ライセンス要件
Cisco NX-OS	IP トンネルには Enterprise Services ライセンスが必要です。Cisco NX-OS ライセンス方式の詳細と、ライセンスの取得および適用の方法については、『*Cisco NX-OS Licensing Guide*』を参照してください。

IP トンネルの前提条件

IP トンネルには次の前提条件があります。

- IP トンネルを設定するための TCP/IP に関する基礎知識があること。
- スイッチにログインしている。
- Cisco NX-OS の Enterprise Services ライセンスをインストールしていること。
- IP トンネルを設定してイネーブルにする前にデバイスのトンネリング機能をイネーブルにしておくこと。

IP トンネルの注意事項および制約事項

IP トンネルの設定に関する注意事項と制約事項は次のとおりです。

- Cisco NX-OS ソフトウェアは、IETF RFC 2784 に定義されている GRE ヘッダーをサポートします。Cisco NX-OS ソフトウェアは、トンネル キーと IETF RFC 1701 のその他のオプションをサポートしません。
- Cisco Nexus デバイスは、次の最大数のトンネルをサポートします。
  - GRE および IP-in-IP 標準トンネル：8 トンネル
  - マルチポイント IP-in-IP トンネル：32 トンネル
- 各トンネルは、1 つの等コスト マルチパス（ECMP）隣接関係を消費します。
- Cisco Nexus デバイスは、次の機能をサポートしません。
  - パスの最大伝送単位（MTU）の検出

- トンネル インターフェイス統計情報
- アクセス コントロール リスト（ACL）
- ユニキャスト リバース パス転送（URPF）
- マルチキャスト トラフィックおよびインターネット グループ管理プロトコル（IGMP）、Protocol Independent Multicast（PIM）などの関連するマルチキャスト プロトコル

- Cisco NX-OS ソフトウェアは、トンネル インターフェイスの Web Cache Control Protocol（WCCP）をサポートしません。
- Cisco NX-OS ソフトウェアは、レイヤ 3 トラフィックのみをサポートします。
- Cisco NX-OS ソフトウェアは、トンネル間の ECMP とトンネル宛先の ECMP をサポートします。
- IPv6-in-IPv6 トンネルはサポートされません。
- GRE トンネルについては、Border Gateway Protocol（BGP）、Open Shortest Path First（OSPF）、Enhanced Interior Gateway Routing Protocol（EIGRP）などの限定された制御プロトコルがサポートされます。
- Release 6.0(2)U5(1) 以降では、トンネルが設定されていない場合、Cisco Nexus 3000 シリーズ スイッチは、すべてのパケットをドロップします。また、トンネルが設定されている場合でも、トンネルインターフェイスが設定されていないか、トンネルインターフェイスがシャットダウン状態のときは、パケットがドロップされます。

  ポイントツーポイント トンネル（送信元と宛先）：Cisco Nexus 3000 シリーズ スイッチは、**feature tunnel** コマンドが設定されており、着信パケットの外部送信元および宛先アドレスと一致するトンネル送信元および宛先アドレスによって設定されている使用可能なトンネルインターフェイスが存在する場合に、そのスイッチを宛先とするすべての IP-in-IP パケットのカプセル化を解除します。送信元および宛先パケットが一致しない場合またはインターフェイスがシャットダウン状態の場合は、パケットがドロップされます。

  トンネルのカプセル化解除（送信元のみ）：Cisco Nexus 3000 シリーズ スイッチは、**feature tunnel** コマンドが設定されており、着信パケットの外部宛先アドレスと一致するトンネル送信元アドレスによって設定されている使用可能なトンネルインターフェイスが存在する場合に、そのスイッチを宛先とするすべての IP-in-IP パケットのカプセル化を解除します。送信元パケットが一致しない場合またはインターフェイスがシャットダウン状態の場合は、パケットがドロップされます。
- Release 6.0(2)U6(1) 以降、Cisco Nexus 3000 シリーズ スイッチは、GRE ヘッダーによってのみ IPv6 in IPv4 をサポートします。トンネルでサポートされる新しい制御プロトコルは、次のとおりです。
  - BGP with v6
  - OSPFv3
  - EIGRP over v6

- GRE v4/v6 トンネル設定は、デフォルト ルーティング モードでのみサポートされます。マルチキャスト トラフィックまたはマルチキャスト プロトコル（IGMP/PIM など）はサポートされません。ACL/QoS ポリシーはサポートされません。スイッチでは最大 8 つのトンネル（すべて IPinIP、すべて GRE、またはその両方の任意の組み合わせ）がサポートされます。トンネル経由で送受信されたパケットおよびスイッチを宛先とするパケットは、トンネル統計情報ではカウントされません。
- Cisco Nexus 3000 シリーズ スイッチの ASIC は、ハードウェアでの GRE カプセル化およびカプセル化解除をサポートします。
- カプセル化側では、Cisco Nexus 3000 シリーズ スイッチは、ハードウェアでの単一検索を実行します。
- Cisco Nexus 3000 シリーズ スイッチではハードウェアで単一検索が実行されるため、ソフトウェアは、2 回目の検索に関連するすべての変更（トンネルの宛先の隣接関係など）によって常に最新のハードウェア情報を保持する必要があります。
- カプセル化解除側では、Cisco Nexus 3000 シリーズ スイッチは、外部 IP ヘッダー検索を実行するための個別のテーブルを持つため、同じ目的の ACL は不要です。

IP トンネリングのデフォルト設定

次の表に、IP トンネル パラメータのデフォルト設定を示します。

表 *6*：デフォルトの *IP* トンネル パラメータ

パラメータ	デフォルト
トンネル機能	ディセーブル

IP トンネルの設定

トンネリングのイネーブル化

はじめる前に

IP トンネルを設定する前にトンネリング機能をイネーブルにする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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 2	switch(config)# **feature tunnel**	スイッチのトンネル機能をイネーブルにします。
ステップ 3	switch(config)# **exit**	コンフィギュレーション モードに戻ります。
ステップ 4	switch(config)# **show feature**	スイッチのトンネル機能を表示します。
ステップ 5	switch# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

次に、トンネル機能をイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# feature tunnel
switch(config)# exit
switch(config)# copy running-config startup-config
```

トンネル インターフェイスの作成

トンネル インターフェイスを作成して、この論理インターフェイスを IP トンネルに設定できます。GRE モードがデフォルトのトンネル モードです。

はじめる前に

トンネルの送信元と宛先の両方が同じ Virtual Routing and Forwarding（VRF）インスタンス内にある必要があります。

トンネリング機能がイネーブルになっていることを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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 2	switch(config)# [**no**] **interface tunnel***number*	新しいトンネル インターフェイスを作成します。

	コマンドまたはアクション	目的
ステップ 3	switch(config)# **tunnel mode** {**gre ip** | **ipip** {**ip** | **decapsulate-any**}}	このトンネル モードを GRE、ipip、または ipip decapsulate-only に設定します。 **gre** キーワードおよび **ip** キーワードは、IP での GRE カプセル化の使用を指定します。 **ipip** キーワードは、IP-in-IP カプセル化の使用を指定します。オプションの **decapsulate-any** キーワードは、あるトンネル インターフェイスの IP-in-IP トンネルを終了させます。このキーワードは、発信トラフィックを伝送しないトンネルを作成します。ただし、リモート トンネル エンドポイントは、設定されたトンネルを宛先として使用できます。
ステップ 4	switch(config)# **tunnel source** {*ip address* | *interface-name*}	この IP トンネルの送信元アドレスを設定します。
ステップ 5	switch(config)# **tunnel destination** {*ip address* | *host-name*}	この IP トンネルの宛先アドレスを設定します。
ステップ 6	switch(config)# **tunnel use-vrf***vrf-name*	（任意） 設定された VRF インスタンスをトンネルの IP 宛先アドレスの検索に使用します。
ステップ 7	switch(config)# **show interface tunnel***number*	（任意） トンネル インターフェイスの統計情報を表示します。
ステップ 8	switch# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

次に、トンネル インターフェイスを作成する例を示します。

```
switch# configure terminal
switch(config)# interface tunnel 1
switch(config)# tunnel source ethernet 1/2
switch(config)# tunnel destination 192.0.2.1
switch(config)# copy running-config startup-config
```

ポリシーベース ルーティングに基づくトンネル インターフェイスの設定

トンネル インターフェイスを作成し、PBR ポリシーに基づいて、この論理インターフェイスを IP トンネルに設定できます。

はじめる前に

トンネリング機能がイネーブルになっていることを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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 2	switch(config)# [**no**] **interface tunnel***number*	新しいトンネル インターフェイスを作成します。
ステップ 3	switch(config)# **ip address***ip address*	このインターフェイスの IP アドレスを設定します。
ステップ 4	switch(config)# **route-map***map-name*	IPv4 ポリシーベース ルーティング用のルート マップをインターフェイスに割り当てます。
ステップ 5	switch(config-route-map)# **match ip address access-list-name***name*	1 つまたは複数の IP アクセス コントロール リスト（ACL）に対して IPv4 アドレスを照合します。このコマンドはポリシーベース ルーティング用であり、ルート フィルタリングまたは再配布では無視されます。
ステップ 6	switch(config-route-map)# **set ip next-hop***address*	ポリシーベース ルーティング用の IPv4 ネクストホップ アドレスを設定します。トンネル インターフェイスを選択するために、トンネル IP アドレスをネクストホップ アドレスとして指定できます。このコマンドでは、複数のアドレスが設定されている場合に、最初の有効なネクストホップ アドレスが使用されます。ネクストホップ エントリから ECMP を選択するには、**load-share** オプションを使用します。

次に、PBR に基づくトンネル インターフェイスを設定する例を示します。

```
switch# configure terminal
switch(config)# interface tunnel 1
switch(config)# ip address 1.1.1.1/24
switch(config)# route-map pbr1
switch(config-route-map)# match ip address access-list-name pbr1
switch(config-route-map)# set ip next-hop 1.1.1.1
```

GRE トンネルの設定

GRE v6 トンネルは、IPv6 トランスポートで異なるタイプのパケットを伝送するために使用されます。GREv6 トンネルは、IPv4 ペイロードのみを伝送します。トンネルの CLI は、IPv6 トンネルを選択し、v6 トンネルの送信元と宛先を設定するために拡張されました。

トンネル インターフェイスを GRE トンネル モード、ipip モード、または ipip decapsulate-only モードに設定できます。GRE モードがデフォルトのトンネル モードです。Release 6.0(2)U6(1) 以降、Cisco Nexus 3000 シリーズ スイッチは、GRE ヘッダーによってのみ IPv4 トンネルで IPv6 ペイロードをサポートします。

はじめる前に

トンネリング機能がイネーブルになっていることを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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 2	switch(config)# **interface tunnel***number*	トンネル 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 3	switch(config-if)# **tunnel mode** {**gre ip** | **ipip** {**ip** | **decapsulate-any**}}	このトンネル モードを GRE、ipip、または ipip decapsulate-only に設定します。 **gre** キーワードおよび **ip** キーワードは、IP での GRE カプセル化の使用を指定します。 ipip キーワードは、IP-in-IP カプセル化の使用を指定します。オプションの **decapsulate-any** キーワードは、あるトンネル インターフェイスの IP-in-IP トンネルを終了させます。このキーワードは、発信トラフィックを伝送しないトンネルを作成します。ただし、リモート トンネル エンドポイントは、設定されたトンネルを宛先として使用できます。
ステップ 4	switch(config-if)# **tunnel use-vrf***vrf-name*	トンネル VRF名を設定します。
ステップ 5	switch(config-if)# **ipv6 address***IPv6 address*	IPv6 アドレスを設定します。 （注） トンネルの送信元アドレスおよび宛先アドレスは同じまま（IPv4 アドレス）です。
ステップ 6	switch(config-if)# **show interface tunnel***number*	（任意） トンネル インターフェイスの統計情報を表示します。

	コマンドまたはアクション	目的
ステップ 7	switch(config-if)# **mtu***value*	インターフェイスで送信される IP パケットの最大伝送ユニット（MTU）を設定します。
ステップ 8	switch(config-if)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

次に、GRE v4 トンネル経由の IPv6 ペイロードを設定する例を示します。トンネルの送信元、宛先、IPv4 アドレス、IPv6 アドレスを設定し、**no shut** コマンドを実行します。GRE v4 トンネルが作成されると、トンネル経由の v4 または v6 ルートを設定できます。

```
switch# configure terminal
switch(config)# interface tunnel 10
switch(config)# tunnel source 11.1.1.1
switch(config)# tunnel destination 11.1.1.2
switch(config-if)# tunnel mode gre ip
switch(config-if)# tunnel use-vrf red
switch(config-if)# ip address 10.1.1.1/24
switch(config-if)# ipv6 address 2:2::2/64
switch(config-if)# no shut

switch(config)# ip route 50.1.1.0/24 tunnel 10
switch(config)# ipv6 route 2000:100::/64 tunnel 10
```

次に、GRE v4 トンネル インターフェイス 10 を表示し、IPv4 および IPv6 ルートを表示する例を示します。

```
switch(config)# show int tunnel 10
Tunnel 10 is up
    Admin State: up
    Internet address(es):
    10.1.1.1/24
    1010::1/64
    MTU 1476 bytes, BW 9 Kbit
    Tunnel protocol/transport GRE/IP
    Tunnel source 11.1.1.1, destination 11.1.1.2
    Transport protocol is in VRF "default"

switch#show ipv6 route
…
2000:100::/64, ubest/mbest: 1/0, attached
    *via Tunnel10, [1/0], 00:00:16, static

#show ip route
…
50.1.1.0/24, ubest/mbest: 1/0
    *via Tunnel10, [1/0], 00:03:33, static
```

次に、GRE v6 トンネル経由の IPv4 ペイロードを設定する例を示します。トンネル モードを GRE IPv6 に設定し、トンネルの v6 送信元および宛先、IPv4 アドレスを設定して、**no shut** コマンドを実行します。GRE v6 トンネルが作成されると、トンネル経由の v4 ルートを設定できます。

```
switch# configure terminal
switch(config)# interface tunnel 20
switch(config-if)# tunnel mode gre ipv6
switch(config)# tunnel source 1313::1
switch(config)# tunnel destination 1313::2
switch(config-if)# tunnel use-vrf red
switch(config-if)# ip address 20.1.1.1/24
```

```
switch(config-if)# no shut

switch(config)# ip route 100.1.1.0/24 tunnel 20
```

次に、GRE v6 トンネル インターフェイス 20 を表示する例を示します。

```
show interface tunnel 20
Tunnel 20 is up
    Admin State: up
    Internet address is 20.1.1.1/24
    MTU 1456 bytes, BW 9 Kbit
    Tunnel protocol/transport GRE/IPv6
    Tunnel source 1313::1, destination 1313::2
    Transport protocol is in VRF "default"

#show ip route
…
100.1.1.0/24, ubest/mbest: 1/0
    *via Tunnel20, [1/0], 00:01:00, static

red10# show interface brief | grep Tunnel
Tunnel10                up          10.1.1.1/24        GRE/IP           1476
Tunnel20                up          20.1.1.1/24        GRE/IPv6         1456
```

次に、ipip トンネルを作成する例を示します。

```
switch# configure terminal
switch(config)# interface tunnel 1
switch(config-if)# tunnel mode ipip
switch(config-if)# mtu 1400
switch(config-if)# copy running-config startup-config
switch(config-if)# no shut
```

トンネル インターフェイスへの VRF メンバーシップの割り当て

VRF にトンネル インターフェイスを追加できます。

はじめる前に

トンネリング機能がイネーブルになっていることを確認します。

VRF 用のインターフェイスを設定した後で、トンネル インターフェイスに IP アドレスを割り当てます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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 2	switch(config)# **interface tunnel** *number*	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 3	switch(config)# **vrf member** *vrf-name*	このインターフェイスを VRF に追加します。
ステップ 4	switch(config)# **ip address** *ip-prefix/length*	このインターフェイスの IP アドレスを設定します。このステップは、このインターフェイスを VRF に割り当てたあとに行う必要があります。

	コマンドまたはアクション	目的
ステップ 5	switch(config)# **show vrf** [*vrf-name*] **interface** *interface-type number*	（任意） VRF 情報を表示します。
ステップ 6	switch(config-if)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーして、変更を継続的に保存します。

次に、VRF にトンネル インターフェイスを追加する例を示します。

```
switch# configure terminal
switch(config)# interface tunnel 0
switch(config-if)# vrf member RemoteOfficeVRF
switch(config-if)# ip address 209.0.2.1/16
switch(config-if)# copy running-config startup-config
```

IP トンネル設定の確認

設定を確認するには、次のコマンドを使用します。

コマンド	目的
show interface tunnel*number*	トンネルインターフェイスの設定を表示します（MTU、プロトコル、転送、および VRF）。入力および出力パケット、バイト、およびパケット レートを表示します。
show interface tunnel*number***brief**	トンネル インターフェイスの動作状態、IP アドレス、カプセル化のタイプ、MTU を表示します。
show interface tunnel*number***description**	トンネルインターフェイスに設定された説明を表示します。
show interface tunnel*number***status**	トンネルインターフェイスの動作ステータスを表示します。
show interface tunnel*number***status err-disabled**	トンネル インターフェイスの errdisable 状態を表示します。

IP トンネリングの設定例

次に、単純な GRE トンネルを示します。イーサネット 1/2 は、ルータ A のトンネル送信元であり、ルータ B のトンネル宛先です。イーサネット インターフェイス 1/3 は、ルータ B のトンネル送信元であり、ルータ A のトンネル宛先です。

```
router A:
feature tunnel
interface tunnel 0
  ip address 209.165.20.2/8
  tunnel source ethernet 1/2
  tunnel destination 192.0.2.2
  tunnel mode gre ip
interface ethernet1/2
  ip address 192.0.2.55/8

router B:
feature tunnel
interface tunnel 0
  ip address 209.165.20.1/8
  tunnel source ethernet 1/3
  tunnel destination 192.0.2.55
  tunnel mode gre ip
interface ethernet 1/3
ip address 192.0.2.2/8
```

IP トンネルの関連資料

関連項目	マニュアル タイトル
IP トンネル コマンド	『*Cisco Nexus 3000 Series Interfaces Command Reference*』

IP トンネルの標準

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。

IP トンネル設定の機能履歴

表 *7*：*IP* トンネル設定の機能履歴

機能名	リリース	機能情報
マルチポイントおよびポイントツーポイント IP-in-IP のカプセル化とカプセル化解除	6.0(2)U2(1)	これらのトンネル モードのサポートが追加されました。

機能名	リリース	機能情報
IP トンネル	5.0(3)U4(1)	この機能が導入されました。

第 6 章

VXLAN の設定

この章の内容は、次のとおりです。

概要

VXLAN の概要

Cisco Nexus 3100 シリーズ スイッチは、ハードウェア ベースの仮想拡張 LAN（VXLAN）機能向けに設計されています。これらのスイッチは、レイヤ 3 の境界を越えてレイヤ 2 接続性を拡張し、VXLAN インフラストラクチャと非 VXLAN インフラストラクチャの間で統合することができます。仮想データセンターおよびマルチテナント データセンターの設計は、共通物理インフラストラクチャで共有できます。

VXLAN により、MAC-in-UDP のカプセル化とトンネリングを使用して、レイヤ 3 インフラストラクチャを越えてレイヤ 2 ネットワークを拡張することができます。さらに、VXLAN を使用して共有トランスポート ネットワークからテナントのレイヤ 2 セグメントを分離することによって、マルチテナント データセンターを構築することができます。

VXLAN のゲートウェイとして展開する場合、Cisco Nexus 3100 シリーズ スイッチは VXLAN および従来の VLAN セグメントと接続して共通の転送ドメインを作成し、テナントのデバイスが両方の環境に存在できるようにすることができます。

VXLAN には次の利点があります。

- データセンター全体でのマルチテナント セグメントの柔軟な配置。

VXLAN は、テナントのワークロードがデータセンター内の物理ポッド全域に配置されるように、基盤となる共有ネットワーク インフラストラクチャでレイヤ2セグメントを拡張します。

- より多くのレイヤ 2 セグメントに対応するための高度なスケーラビリティ。

  VXLAN は、24 ビットのセグメント ID、つまり VXLAN ネットワーク ID（VNID）を使用します。VNID により、最大 1600 万個の VXLAN セグメントを同じ管理ドメイン内で共存させることができます（比較すると、従来の VLAN は最大 4096個の VLAN をサポートできる 12 ビットのセグメント ID を使用します）。

- 基盤となるインフラストラクチャにおける、有効なネットワーク パスの使用率。

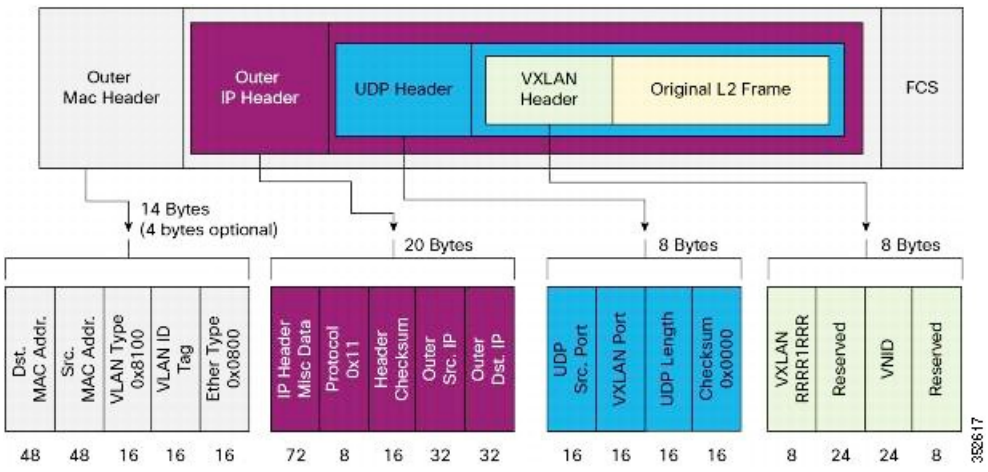
  VXLAN パケットは、レイヤ 3 ヘッダーに基づいて、基盤となるネットワークを介して転送されます。これは、等コスト マルチパス（ECMP）ルーティングおよびをリンク集約プロトコルを使用して、有効なすべてのパスを使用します。

VXLAN のカプセル化およびパケット形式

VXLAN は、レイヤ 3 ネットワーク上のレイヤ 2 オーバーレイ方式です。VXLAN は MAC-in-UDP のカプセル化を使用して、データセンター ネットワークでレイヤ 2 セグメントを拡張します。物理データセンター ネットワークでの転送プロトコルは IP と UDP です。

VXLAN は MAC-in-UDP のカプセル化方式を定義します。この方式において、元のレイヤ 2 フレームに VXLAN ヘッダーが追加され、UDP-IP パケットに置かれます。この MAC-in-UDP のカプセル化によって、VXLAN はレイヤ 3 ネットワーク上でレイヤ 2 ネットワークをトンネルします。VXLAN のパケット形式を次の図に示します。

図 *6*：*VXLAN* のパケット形式



VXLAN は、24 ビット VNID といくつかの予約ビットで構成される 8 バイト VXLAN ヘッダーを使用します。VXLAN ヘッダーと元のイーサネット フレームは、UDP ペイロードに含まれます。

24 ビット VNID はレイヤ 2 セグメントを識別し、セグメント間でレイヤ 2 の分離を維持します。VXLAN は 1600 万個の LAN セグメントをサポートできます。

VXLAN トンネル エンド ポイント

VXLAN は VXLAN トンネル エンドポイント（VTEP）デバイスを使用してテナントのエンド デバイスを VXLAN セグメントへマップし、VXLAN のカプセル化およびカプセル化解除を実行します。各 VTEP デバイスには次の 2 種類のインターフェイスがあります。

- ブリッジングを介してローカル エンドポイント通信をサポートするためのローカル LAN セグメントのスイッチ ポート インターフェイス
- VXLAN カプセル化フレームが送信されるトランスポート ネットワークへの IP インターフェイス

VTEP デバイスは、一意の IP アドレス（ループバック インターフェイス IP アドレス）を使用して IP トランスポート ネットワークで識別されます。VTEP デバイスはこの IP アドレスを使用してイーサネット フレームをカプセル化し、カプセル化されたパケットを、IP インターフェイスを介して転送ネットワークへ送信します。VTEP デバイスは、受信する VXLAN トラフィックに関して、リモート VTEP IP アドレスと、リモートの MAC アドレスから VTEP IP へのマッピングを学習します。

VXLAN セグメントは基盤となるネットワーク トポロジに依存しません。逆に、VTEP 間の基盤となる IP ネットワークは、VXLAN オーバーレイに依存しません。IP ネットワークは発信元 IP アドレスとして開始 VTEP を持ち、宛先 IP アドレスとして終端 VTEP またはマルチキャスト グループ IP アドレスを持っており、外部 IP アドレス ヘッダーに基づいて、カプセル化されたパケットをルーティングします。

VXLAN のパケット転送フロー

VXLAN は VTEP 間でステートレス トンネルを使用し、レイヤ 3 転送ネットワークを介してオーバーレイ レイヤ 2 ネットワークのトラフィックを送信します。

Cisco Nexus 3100 シリーズ スイッチでの VXLAN の導入

Cisco Nexus 3100 シリーズ スイッチは、ハードウェアベースの VXLAN 機能をサポートします。この機能により、レイヤ 2 接続がレイヤ 3 トランスポート ネットワークに拡張され、VXLAN インフラストラクチャと非 VXLAN インフラストラクチャの間の高性能ゲートウェイが実現されます。

ブロードキャスト、未知のユニキャスト、およびマルチキャストトラフィックに関するレイヤ 2 メカニズム

Cisco Nexus 3100 シリーズ スイッチ上の VXLAN は、フラッディングおよびダイナミック MAC アドレス ラーニングを使用して次のことを実行します。

- ブロードキャスト、未知のユニキャスト、およびマルチキャスト トラフィックを転送する
- リモート VTEP を検出する
- 各 VXLAN セグメントに関して、リモート ホスト MAC アドレスと、MAC から VTEP へのマッピングを学習する

VXLAN は、これらのトラフィック タイプを次のように転送できます。

- コアでのマルチキャストの使用：IP マルチキャストは、VXLAN セグメントに参加している一連のホストのフラッディングを削減します。各 VXLAN セグメント（または VNID）は、トランスポート IP ネットワークの IP マルチキャスト グループにマッピングされます。レイヤ 2 ゲートウェイは、PIM（Protocol Independent Multicast）を使用して、IP マルチキャスト グループのランデブー ポイント（RP）からのトラフィックを送受信します。このグループのマルチキャスト配信ツリーは、参加している VTEP の場所に基づき、トランスポート ネットワークを通じて構築されます。
- 入力複製の使用：各 VXLAN セグメントまたは VXLAN ネットワーク ID（VNI）は、リモート ユニキャスト ピアにマッピングされます。レイヤ 2 フレームは、リモート ユニキャスト ピア IP アドレスとして宛先 IP アドレスを使用してカプセル化された VXLAN であり、IP トランスポート ネットワークに送信され、このネットワークでリモート宛先にユニキャスト ルーティングまたは転送されます。

ユニキャスト学習されたトラフィックに関するレイヤ 2 メカニズム

Cisco Nexus 3100 シリーズ スイッチは、VXLAN のユニキャスト学習されたトラフィックに関して、MAC アドレス検索ベース転送を実行します。

アクセス側でレイヤ2トラフィックが受信されると、フレームの宛先MACアドレスに関してMACアドレス検索が実行されます。検索に成功すると、検索の結果として取得された情報に基づいて VXLAN 転送が実行されます。検索結果により、この MAC アドレスが学習されたリモート VTEP の IP アドレスが提供されます。その後、このレイヤ 2 フレームは、リモート VTEP IP アドレスとして宛先 IP アドレスを使用して UDP/IP カプセル化され、適切なネットワーク インターフェイスから転送されます。レイヤ 3 クラウドでは、この IP パケットが、ネットワークのその IP アドレスへのルートを介して、リモート VTEP に転送されます。

ユニキャスト学習されたトラフィックについては、次のことを確認する必要があります。

- リモート ピアへのルートは、ルーティング プロトコルまたはネットワークのスタティック ルートを介して認識されます。

- 隣接関係は解決されます。

マルチキャスト中継ルータとしての VXLAN レイヤ 2 ゲートウェイ

VXLAN レイヤ 2 ゲートウェイは、VNI がマッピングされているいずれかのグループを宛先とするVXLANマルチキャストトラフィックを停止させる必要があります。ネットワークでは、VXLAN レイヤ 2 ゲートウェイを、グループのトラフィックに関心を持つダウンストリーム マルチキャスト受信者のためのマルチキャスト中継ルータとして使用できます。VXLAN レイヤ 2 ゲートウェイは、受信した VXLAN マルチキャスト トラフィックを確実に停止させ、マルチキャスト ルーティングするために、いくつかの追加処理を実行する必要があります。このトラフィック処理は、次の 2 つの経路で実行されます。

1. VXLANマルチキャストトラフィックは、そのグループのトラフィックに関心を持つすべてのネットワーク受信者にマルチキャスト ルーティングされます。
2. VXLAN マルチキャスト トラフィックは停止されてカプセル化解除され、すべての VXLAN アクセス側ポートに転送されます。

VXLAN による ECMP および LACP ロード シェアリング

カプセル化された VXLAN パケットは、トランスポート ネットワークのネイティブ転送判断に基づいて VTEP 間で転送されます。ほとんどのデータセンターのトランスポート ネットワークは、使用可能なすべてのパスにトラフィック負荷を分散させるさまざまなマルチパス ロードシェアリング技術を利用した複数の冗長パスによって設計され、導入されています。

一般的な VXLAN トランスポート ネットワークは、複数のベスト パスにトラフィック負荷を分散させる標準 IP 等コスト マルチパス（ECMP）を使用する IP ルーティング ネットワークです。パケットが間違った順序で転送されることを防ぐために、一般にフローベースの ECMP が導入されます。ECMP は、送信元および宛先の IP アドレスと、オプションで、IP パケット ヘッダーの送信元および宛先の TCP または UDP ポートによって定義されます。

VTEP ペア間のすべての VXLAN パケット フローは同じ外部送信元および宛先 IP アドレスを持ちます。また、すべての VTEP デバイスは、1 つの同じ宛先 UDP ポート（Internet Assigned Numbers Authority（IANA）割り当ての UDP ポート 4789 またはカスタマー定義ポートのいずれか）を使用する必要があります。ECMP フロー定義の変数要素で、トランスポート ネットワークの観点から VXLAN フローを区別できるものは、送信元 UDP ポートだけです。ルーティングおよび ECMP 判断に基づいて解決された出力インターフェイスが Link Aggregation Control Protocol（LACP）ポート チャネルである場合は、LACP ハッシュに関して同様の状況が発生します。LACP は、リンク負荷共有ハッシュに VXLAN 外部パケット ヘッダーを使用します。このため、送信元 UDP ポートが VXLAN フローを一意に識別できる唯一の要素となります。

Cisco Nexus 3100 シリーズ スイッチの VXLAN の実装では、内部フレームのヘッダーのハッシュが VXLAN の送信元 UDP ポートとして使用されます。その結果、VXLAN フローを一意にできます。IPアドレスとUDPポートの組み合わせが外部ヘッダーに含まれていますが、パケットは、基礎となるトランスポート ネットワークを通過します。

VXLAN の注意事項と制約事項

VXLAN には、次の注意事項と制限事項があります。

- マルチキャスト グループと入力複製（IR）の設定は、同時にはサポートされません。マルチキャスト グループまたは IR のいずれかを設定して導入することにより、VXLAN を導入できます。
- **system vlan nve-overlay** CLI は、特定のタイプの BroadCom ASIC を搭載する Cisco Nexus 3000 シリーズ スイッチには必要ありません。そのため、**system vlan nve-overlay** CLI コマンドを有効にしないでください。
- vPC の VXLAN 設定では、ノース VTEP からのパケットはプライマリ vPC スイッチでカプセル化解除され、VLAN/VN セグメントのすべてのポートに送信されます。また、マルチキャストリンクでセカンダリ vPC スイッチにも転送されます。そのため、プライマリ vPC スイッチの Tx および Rx の両方で NVE VNI カウンタの増加が見られます。一方で、NVE VNI カウンタは、セカンダリ vPC スイッチの Rx のみで増加します。
- 拡張された環境で使用されるマルチキャスト グループと OIFL の合計数を 1024（マルチキャスト VXLAN VP の現在の範囲）以外にしないことを推奨します。
- IGMP スヌーピングは VXLAN VLAN ではサポートされません。
- VXLAN ルーティングはサポートされません。VXLAN VLAN のデフォルトのレイヤ 3 ゲートウェイは、別のデバイスでプロビジョニングする必要があります。

（注） リリース 7.0(3)I4(1) 以降、VXLAN ルーティングは、次の 3 つの新しい Cisco nexus 3000 シリーズ プラットフォームでサポートされます。

- C3132Q-V
- C31108TC-V
- C31108PC-V

- ネットワークが VXLAN ヘッダー用に追加の 50 バイトに対応できることを確認してください。
- スイッチでは 1 つの Network Virtualization Edge（NVE）インターフェイスだけがサポートされます。
- レイヤ 3 VXLAN アップリンクは、非デフォルトの Virtual Routing and Forwarding（VRF）インスタンスではサポートされません。
- 物理インターフェイスごとに 1 つの VXLAN IP 隣接関係のみ有効です。
- スイッチ仮想インターフェイス（SVI）は、VXLAN VLAN ではサポートされません。

（注） リリース 7.0(3)I4(1) 以降、ルーティング用の VXLAN VLAN を介した SVI は、次の 3 つの新しい Cisco nexus 3000 シリーズ プラットフォームでサポートされます。

- C3132Q-V
- C31108TC-V
- C31108PC-V

- レイヤ 3 アップリンク インターフェイスについては、VXLAN カプセル化トラフィックのスイッチド ポート アナライザ（SPAN）Tx はサポートされません。
- ディレクションにアクセスするための VXLAN トラフィックのアクセス コントロール リスト（ACL）および Quality of Service（QoS）はサポートされません。
- SNMP は NVE インターフェイスではサポートされません。
- VXLAN のネイティブ VLAN はサポートされません。
- 入力複製設定に関しては、複数の VNI が、設定済みの同じリモート ピア IPを持つことが可能になりました。
- VXLAN の送信元 UDP ポートは、VNID と送信元/宛先 IP アドレスに基づいて決定されます。
- UDP ポートの設定は、NVE インターフェイスを有効にする前に完了する必要があります。NVE インターフェイスが有効になっているときに UDP の設定を変更する必要がある場合は、NVE インターフェイスをシャットダウンし、UDP の設定を変更してから、NVE インターフェイスを再び有効にする必要があります。

（注） リリース 7.0(3)I4(1) 以降、VXLAN UDP ポートは、次の 3 つの新しい Cisco nexus 3000 シリーズ プラットフォームでは設定できません。

- C3132Q-V
- C31108TC-V
- C31108PC-V

- VN セグメントがネイティブ VLAN にマッピングされている場合、トラフィックが、VLAN でスイッチされるのではなく、そのポートの任意の標準 VLAN で送信されると、ネイティブ VLAN に関して VXLAN トンネルで転送されます。

Cisco Nexus C3132Q-V、C31108PC-V、および C31108TC-V シリーズ スイッチの検証済みスケール値

VXLAN のフラッディングおよび学習	
レイヤ 2 VNI	640
アンダーレイ マルチキャスト グループ	200
VTEP	640
MAC アドレス	64,000

VXLAN BGP eVPN	
レイヤ 2 VNI	640
レイヤ 3 VNI/VRF	320
アンダーレイ マルチキャスト グループ	200
VTEP	32
MAC アドレス	64,000
IPv4 ホスト ルート	8,000
IPv6 ホスト ルート	4,000
オーバーレイ IPv4 LPM ルート	8,000
オーバーレイ IPv6 LPM ルート	4,000

VXLAN BGP eVPN の入力複製	
レイヤ 2 VNI	640
アンダーレイ マルチキャスト グループ	320
VTEP	32
MAC アドレス	64,000

VXLAN BGP eVPN の入力複製	
IPv4 ホスト ルート	8,000
IPv6 ホスト ルート	4,000
オーバーレイ IPv4 LPM ルート	8,000
オーバーレイ IPv6 LPM ルート	4,000

VXLAN 展開の考慮事項

次に、VXLAN 展開時のいくつかの考慮事項を示します。

- ループバック インターフェイス IP は、トランスポート ネットワークで VTEP デバイスを一意に識別するために使用されます。
- コアで IP マルチキャストのルーティングを確立するには、IP マルチキャストの設定、PIM の設定、およびランデブー ポイント（RP）の設定が必要です。
- VTEP-to-VTEP ユニキャストの到達可能性は、いずれかの IGP プロトコルを介して設定できます。
- 必要に応じて、VXLAN UDP 宛先ポートを設定できます。デフォルト ポートは 4789 です。
- VXLAN VLAN のデフォルト ゲートウェイは、別のアップストリーム ルータでプロビジョニングする必要があります。
- VXLAN のマルチキャスト トラフィックは、常に RPT 共有ツリーを使用する必要があります。
- VTEP のマルチキャスト グループに対する RP は、サポート対象の設定です。ただし、マルチキャスト グループの RP は、スパイン レイヤ/アップストリーム デバイス上で設定する必要があります。すべてのマルチキャスト トラフィックはRPを通過するため、このトラフィックをスパイン レイヤ/アップストリーム デバイスへダイレクトすると、より効率的です。

VXLAN 導入に関する vPC の注意事項と制約事項

- Release 7.0(3)I2(1) 以降、VXLAN マルチキャスト カプセル化パスは、vPC ピアに vPC ピア リンクの重複メンバーを持ちます。この設計は、エニーキャスト RP およびサービス オーファン トラフィックをサポートするために採用されました。すべてのアクセス側トラフィックについて、パケットの 2 つのコピーが、マルチキャスト パスの vPC ピア リンクを介して送信されるようになっています（1 つはネイティブ パケット、1 つは VXLAN ヘッダー カプセル化パケット）。

- NVE を、レイヤ 3 プロトコルで必要な他のループバック アドレスとは別のループバック アドレスにバインドする必要があります。VXLAN に対して専用のループバック アドレスを使用します。
- 非 DF スイッチへハッシュされる vPC 上のマルチキャスト トラフィックは Multichassis EtherChannel トランク（MCT）を通過し、DF ノードでカプセル化されます。
- VXLAN vPC において、vPC ピアで NVE の設定と VN-Segment の設定が同じであることを確認するために整合性チェックが行われます。
- ユニキャスト ルーティング プロトコルのルータ ID は、VTEP に使用されるループバック IP アドレスとは異なる必要があります。
- より高いルーティング メトリックを持つルーティング プロトコルを使用して、vPC ピア間の SVI を設定し、vPC ピア間のルートをアドバタイズします。このアクションにより、1 つの vPC ノードで障害が発生しても vPC ノードの IP 接続がダウンしないことが保証されます。

さまざまなシナリオでの VXLAN vPC セットアップと想定される動作に関する設定ガイドライン

- vPC ピアは同じ設定にする必要があります。
  - VLAN から VN-segment への一貫したマッピング。
  - 同じループバック インターフェイスへの一貫した NVE1 バインディング。
  - 同じセカンダリ IP アドレスを使用する。
  - 異なるプライマリ IP アドレスを使用する。
  - グループへの一貫した VNI マッピング。
- マルチキャストでは、RP（ランデブー ポイント）から（S, G）join を受け取る vPC ノードが DF（指定フォワーダ）になります。DF のノードでは、マルチキャストに対してカプセル化のルートがインストールされます。
- カプセル化解除のルートは、vPC プライマリ ノードと vPC セカンダリ ノードの間でのカプセル化解除ノードの選択に基づいてインストールされます。カプセル化解除の選択で優先されるのは、RP へのコストが最小のノードです。
- ただし、RP へのコストが両方のノードで同じである場合は、vPC プライマリ ノードが選択されます。カプセル化解除の選択で優先されるノードに、カプセル化解除マルチキャスト ルートがインストールされます。他のノードには、カプセル化解除のルートはインストールされません。
- vPC デバイスで、ホストからの BUM トラフィック（ブロードキャスト、未知のユニキャスト、およびマルチキャスト トラフィック）がピア リンクに複製されます。各ネイティブ パケットからコピーが作成され、各ネイティブ パケットは、ピア vPC スイッチに接続された orphan ポートを提供するピア リンクを介して送信されます。
- VXLAN ネットワークでのトラフィック ループを防止するために、ピア リンクに入力されるネイティブ パケットは、アップリンクに送信できません。ただし、ピア スイッチがカプセ

ル化ノードである場合は、コピーされたパケットがピア リンクを通過してアップリンクに送信されます。

- ピア リンクが shut の場合、vPC セカンダリのループバック アドレスは停止し、ステータスはAdmin Shutになります。これは、アップストリーム上でループバックへのルートが取り消され、アップストリームがすべてのトラフィックをvPCプライマリへ転送できるようにするために行われます。

（注） MCT がシャットダウンされている場合、セカンダリ vPC に接続された orphan ポートではトラフィックの損失が発生します。この状況は、従来の vPC セットアップのセカンダリ vPC におけるレイヤ 2 の orphan ポートに類似しています。

- ピア リンクが no-shut の場合、NVE ループバック アドレスが再度提示されます。ルートはアドバタイズされたアップストリームとなり、トラフィックを誘導します。
- vPC の場合：
  - ループバック インターフェイスには、プライマリ IP アドレスとセカンダリ IP アドレスの 2 つの IP アドレスがあります。
  - プライマリ IP アドレスは一意で、レイヤ 3 プロトコルで使用されます。
  - インターフェイス NVE は VTEP IP アドレスにセカンダリ IP アドレスを使用するため、ループバック上のセカンダリ IP アドレスは必須です。
  - セカンダリ IP アドレスは、vPC の両方のピアで同じにする必要があります。
  - VPC ピアゲートウェイ機能は、両方のピアで有効にする必要があります。
- ベストプラクティスとして、vPCトポロジのコンバージェンスを改善するために、peer-switch、peer gateway、ip arp sync、ipv6 nd sync 設定を使用します。
- NVE またはループバックが vPC 設定で shut の場合：
  - プライマリ vPC スイッチでのみ NVE またはループバックが shut の場合、グローバル VXLAN vPC 整合性チェッカはエラーになります。その後、NVE、ループバック、および vPC がセカンダリ vPC スイッチでダウンになります。
  - セカンダリ vPC スイッチでのみ NVE またはループバックが shut の場合、グローバル VXLAN vPC 整合性チェッカはエラーになります。その後、NVE、ループバック、およびセカンダリ vPC がセカンダリ vPC スイッチでダウンになります。トラフィックのフローは、プライマリ vPC スイッチを介して継続されます。
- ベスト プラクティスとして、プライマリとセカンダリの両方の vPC スイッチで NVE とループバックの両方がアップの状態を維持する必要があります。
- マルチキャスト ロード バランシングおよび RP の冗長性のためにネットワークで設定される冗長エニーキャスト RP は、vPC VTEP トポロジでサポートされます。

- vPC ピア スイッチ設定の有効化は必須です。ピア スイッチ機能のために、少なくとも 1 つの SVI がピア リンクで有効にされ、PIM によって設定される必要があります。これにより、VTEP がスパインへの接続を完全に失ったときに、バックアップ パスが提供されます。この場合、リモート ピアの到達可能性は、ピア リンクを介して再ルーティングされます。

VXLAN トラフィック転送の設定

VXLAN レイヤ 2 ゲートウェイには、ブロードキャスト転送の 2 つのオプション（未知のユニキャストおよびマルチキャスト トラフィック）があります。 ブロードキャスト、未知のユニキャスト、およびマルチキャスト トラフィックに関するレイヤ 2 メカニズム, （122 ページ） には、これらの 2 つのオプションの詳細が記載されています。

VXLAN を有効にして設定する前に、次の設定が完了していることを確認してください。

- コアでの IP マルチキャストについては、IP マルチキャストの設定、PIM の設定、および RP の設定が完了していることと、ルーティング プロトコルが存在することを確認します。
- 入力複製については、ユニキャスト アドレスに到達するためのルーティング プロトコルが存在することを確認します。

（注） VXLAN レイヤ 2 ゲートウェイとして機能する Cisco Nexus 3100 シリーズ スイッチについては、アクセス側で受信されるトラフィックがネットワーク側の ARP をトリガーできないことに注意してください。ネットワーク側インターフェイスの ARP は、BGP などのルーティング プロトコルを使用するか、静的 ARP を使用して解決する必要があります。この要件は、マルチキャスト レプリケーションの場合ではなく、入力複製の場合にのみ適用されます。

PIM 機能のイネーブル化と設定

PIM コマンドにアクセスするには、PIM 機能をイネーブルにしておく必要があります。

これは、マルチキャスト複製にのみ必要です。

はじめる前に

LAN Base Services ライセンスがインストールされていることを確認してください。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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 2	switch(config)# **feature pim**	PIM をイネーブルにします。デフォルトでは PIM はディセーブルになっています。
ステップ 3	switch(config)# **show running-config pim**	（任意） **feature** コマンドを含む、PIM の実行コンフィギュレーション情報を示します。
ステップ 4	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

次に、PIM 機能をイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# feature pim
switch(config)# ip pim spt-threshold infinity group-list rp_name
switch(config)# show running-config pim

!Command: show running-config pim
!Time: Wed Mar 26 08:04:23 2014

version 6.0(2)U3(1)
feature pim

ip pim spt-threshold infinity group-list rp_name
```

ランデブー ポイントの設定

ランデブー ポイント（RP）を設定するには、PIM ドメインに参加するルータのそれぞれに RP アドレスを設定します。

これは、マルチキャスト複製にのみ必要です。

はじめる前に

LAN Base Services ライセンスがインストールされていること、および PIM がイネーブル化されていることを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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 2	switch(config)# **ip pim rp-address***rp-address* [**group-list***ip-prefix* | **route-map** *policy-name*]	マルチキャスト グループ範囲に、PIM RP アドレスを設定します。**match ip multicast** コマンドで、使用するグループ プレフィックスを示すルートマップ ポリシー名を指定できます。デフォルトモードは ASM です。デフォルトのグループ範囲は 224.0.0.0 ～ 239.255.255.255 です。
ステップ 3	switch(config)# **show ip pim group-range** [*ip-prefix*] [**vrf** {*vrf-name* | **all** | **default** | **management**}]	（任意） PIM モードおよびグループ範囲を表示します。
ステップ 4	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

次に、RP を設定する例を示します。

```
switch# configure terminal
switch(config)# ip pim rp-address 111.1.1.1 group-list 224.0.0.0/4
```

VXLAN のイネーブル化

VXLAN をイネーブルにするには、次の手順を実行します。

- VXLAN 機能をイネーブルにする。
- VN-Segment への VLAN のマッピングをイネーブルにする。

はじめる前に

VXLAN Enterprise ライセンスをインストールしていることを確認してください。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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 2	switch(config)# **[no] feature nv overlay**	VXLAN 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 3	switch (config)# **[no] feature vn-segment-vlan-based**	すべての VXLAN ブリッジドメインにグローバルモードを設定します。 VN-Segment への VLAN のマッピングをイネーブルにします。VN-Segment への VLAN のマッピングは常に 1 対 1 です。
ステップ 4	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

次に、VXLAN をイネーブルにして、VN-Segment への VLAN のマッピングを設定する例を示します。

```
switch# configure terminal
switch(config)# feature nv overlay
switch(config)# feature vn-segment-vlan-based
switch(config)# copy running-config startup-config
```

VLAN から VXLAN VNI へのマッピング

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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 2	switch(config)# **vlan***vlan-id*	VLAN を指定します。
ステップ 3	switch(config-vlan)# **vn-segment***vnid*	VXLAN 仮想ネットワーク ID（VNID）を指定します。

次に、VLAN から VXLAN VNI にマッピングする例を示します。

```
switch# configure terminal
switch(config)# vlan 3100
switch(config-vlan)# vn-segment 5000
```

NVE ユニキャスト アドレスのルーティング プロトコルの設定

ユニキャスト アドレスのルーティング プロトコルの設定には、次の作業が含まれます。

- NVE 到達可能性に関する専用ループバック インターフェイスを設定する。
- ルーティング プロトコルのネットワーク タイプを設定する。
- インターフェイスのルーティング プロトコル インスタンスおよびエリアを指定する。
- マルチキャスト複製の場合は PIM スパース モードを有効にする。

（注） 例では、Open Shortest Path First（OSPF）がルーティング プロトコルとして使用されます。

これは、マルチキャストと入力複製の両方の前提条件です。

ユニキャストアドレスのルーティングプロトコルの設定に関するガイドラインは、次のとおりです。

- 入力複製の場合、隣接関係を解決できるルーティングプロトコル（BGP など）を使用できます。
- vPC トポロジでユニキャスト ルーティング プロトコルを使用する場合は、VTEP ループバック IP アドレス（vPC ピア上のものと同じ）がルータ ID として使用されることを防ぐために、vPC ピアの一意のルータ ID を明示的に設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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 2	switch(config)# **interface loopback***instance*	NVE インターフェイスの専用ループバック インターフェイスを作成します。instance の範囲は 0 ～ 1023 です。
ステップ 3	switch(config-if)# **ip address***ip-address/length*	このインターフェイスの IP アドレスを設定します。
ステップ 4	switch(config-if)# **ip ospf network** {**broadcast** | **point-to-point**}	OSPF ネットワーク タイプをインターフェイスのデフォルト以外のタイプに設定します。
ステップ 5	switch(config-if)# **ip router ospf***instance-tag***area***area-id*	インターフェイスの OSPF インスタンスおよびエリアを指定します。
ステップ 6	switch(config-if)# **ip pim sparse-mode**	現在のインターフェイスで PIM スパース モードをイネーブルにします。デフォルトではディセーブルになっています。 マルチキャスト複製の場合は PIM スパース モードを有効にします。

次に、NVE ユニキャスト アドレスのルーティング プロトコルを設定する例を示します。

```
switch# configure terminal
switch(config)# interface loopback 10
switch(config-if)# ip address 222.2.2.1/32
switch(config-if)# ip ospf network point-to-point
switch(config-if)# ip router ospf 1 area 0.0.0.0
switch(config-if)# ip pim sparse-mode
```

VXLAN 宛先 UDP ポートの作成

UDP ポートの設定は、NVE インターフェイスを有効にする前に完了する必要があります。

（注） NVE インターフェイスが有効になっているときに設定を変更する必要がある場合は、必ず、NVE インターフェイスをシャットダウンし、UDP の設定を変更してから、NVE インターフェイスを再び有効にしてください。

ネットワークで NVE インターフェイスを有効にする前に、UDP ポートの設定がネットワーク全体で完了していることを確認してください。

VXLAN UDP 送信元ポートは、VNID および送信元と宛先の IP アドレスに基づいて決定されます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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 2	switch(config)# **vxlan udp port***number*	VXLAN カプセル化パケットの宛先 UDP ポート番号を指定します。デフォルトの宛先 UDP ポート番号は 4789 です。

次に、VXLAN 宛先 UDP ポートを作成する例を示します。

```
switch# configure terminal
switch(config)# vxlan udp port 4789
```

NVE インターフェイスの作成および設定

NVE インターフェイスは、VXLAN トンネルを開始または停止させるオーバーレイ インターフェイスです。NVE（オーバーレイ）インターフェイスを作成および設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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 2	switch(config)# **interfacenve***instance*	VXLAN トンネルを開始および停止させる VXLAN オーバーレイ インターフェイスを作成します。 （注） スイッチでは 1 つの NVE インターフェイスのみ使用できます。
ステップ 3	switch(config-if-nve)# **source-interface loopback***instance*	送信元インターフェイスを指定します。 送信元インターフェイスは、有効な /32 IP アドレスを持つスイッチ上に設定されているループバック インターフェイスにする必要があります。この /32 IP アドレスは、トランスポート ネットワークの中継ルータおよびリモート VTEP によって認識される必要があります。

次に、NVE インターフェイスを作成および設定する例を示します。

```
switch# configure terminal
switch(config)# interface nve 1
switch(config-if-nve)# source-interface loopback 10
```

VNI の複製の設定

VXLAN ネットワーク ID（VNI）の複製は、次の 2 つの方法のいずれかで設定できます。

- マルチキャスト複製
- 入力複製

マルチキャスト複製の設定

はじめる前に

- NVE インターフェイスが作成され、設定されていることを確認します。
- 送信元インターフェイスが指定されていることを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch(config-if-nve)# **member vni** {*vnid***mcast-group***multicast-group-addr* | *vnid-range***mcast-group***start-addr* [*end-addr*]}	VXLAN VNI を NVE インターフェイスにマッピングし、マルチキャスト グループを VNI に割り当てます。

次に、VNI を NVE インターフェイスにマッピングし、VNI をマルチキャスト グループに割り当てる例を示します。

```
switch(config-if-nve)# member vni 5000 mcast-group 225.1.1.1
```

入力複製の設定

はじめる前に

- NVE インターフェイスが作成され、設定されていることを確認します。
- 送信元インターフェイスが指定されていることを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch(config-if-nve)# **member vni***vnid*	VXLAN VNI を NVE インターフェイスにマッピングします。
ステップ 2	switch(config-if-nve-vni)# **ingress-replication protocol static**	VNI の静的入力複製を有効にします。
ステップ 3	switch(config-if-nve-vni)# **peer-ip***ip-address*	ピア IP を有効にします。 （注） • VNI は単一の IP アドレスにのみ関連付けることができます。 • IP アドレスは単一の VNI にのみ関連付けることができます。

次に、VNI を NVE インターフェイスにマッピングし、ユニキャスト トンネルを作成する例を示します。

```
switch(config-if-nve)# member vni 5001
switch(config-if-nve-vni)# ingress-replication protocol static
switch(config-if-nve-vni)# peer-ip 111.1.1.1
```

VXLAN 設定の確認

VXLAN 設定を確認し、MAC アドレスを表示し、MAC アドレスを消去するには、次のいずれかのコマンドを使用します。

コマンド	目的
show nve interface nve*id*	NVE インターフェイスの設定を表示します。
show nve vni	NVE インターフェイスにマッピングされた VNI を表示します。
show nve peers	NVE インターフェイスのピアを表示します。
show interface nve*id***counters**	NVE インターフェイスのすべてのカウンタを表示します。
show nve vxlan-params	設定されている VXLAN UDP ポートを表示します。
show mac address-table	VLAN と VXLAN の両方の MAC アドレスを表示します。
clear mac address-table dynamic	MAC アドレス テーブルのすべての MAC アドレス エントリを消去します。

次に、NVE インターフェイスの設定を表示する例を示します。

```
switch# show nve interface nve 1
Interface: nve1, State: up, encapsulation: VXLAN
Source-interface: loopback10 (primary: 111.1.1.1, secondary: 0.0.0.0)
```

次に、マルチキャスト複製のために NVE インターフェイスにマッピングされている VNI を表示する例を示します。

```
switch# show nve vni
Interface          VNI        Multicast-group   VNI State
-----------------  --------   ---------------   ---------
nve1               5000       225.1.1.1          Up
```

次に、入力複製のために NVE インターフェイスにマッピングされている VNI を表示する例を示します。

```
switch# show nve vni
Interface          VNI        Multicast-group   VNI State
-----------------  --------   ---------------   ---------
nve1               5000       0.0.0.0           Up
```

次に、NVE インターフェイスのピアを表示する例を示します。

```
switch# show nve peers
Interface          Peer-IP           Peer-State
-----------------  ----------------  -------------
```

```
nve1              111.1.1.1          Up
```

次に、NVE インターフェイスのカウンタを表示する例を示します。

```
switch# show interface nv 1 counter

--------------------------------------------------------------------------------
Port                                InOctets                    InUcastPkts
--------------------------------------------------------------------------------
nve1                                       0                              0

--------------------------------------------------------------------------------
Port                              InMcastPkts                    InBcastPkts
--------------------------------------------------------------------------------
nve1                                       0                              0

--------------------------------------------------------------------------------
Port                               OutOctets                   OutUcastPkts
--------------------------------------------------------------------------------
nve1                                       0                              0

--------------------------------------------------------------------------------
Port                             OutMcastPkts                   OutBcastPkts
--------------------------------------------------------------------------------
nve1                                       0                              0
```

次に、設定されている VXLAN UDP ポートを表示する例を示します。

```
switch# show nve vxlan-params
VxLAN Dest. UDP Port: 4789
```

次に、VLAN と VXLAN の両方の MAC アドレスを表示する例を示します。

```
switch# show mac address-table
Legend:
        * - primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC
        age - seconds since first seen,+ - primary entry using vPC Peer-Link
   VLAN     MAC Address      Type      age     Secure NTFY   Ports/SWID.SSID.LID
---------+-----------------+--------+---------+------+----+------------------
* 109      0000.0410.0902    dynamic   470        F    F  Po2233
* 109      0000.0410.0912    dynamic   470        F    F  Po2233
* 109      0000.0410.0912    dynamic   470        F    F  nve1(1.1.1.200)
* 108      0000.0410.0802    dynamic   470        F    F  Po2233
* 108      0000.0410.0812    dynamic   470        F    F  Po2233
* 107      0000.0410.0702    dynamic   470        F    F  Po2233
* 107      0000.0410.0712    dynamic   470        F    F  Po2233
* 107      0000.0410.0712    dynamic   470        F    F  nve1(1.1.1.200)
* 106      0000.0410.0602    dynamic   470        F    F  Po2233
* 106      0000.0410.0612    dynamic   470        F    F  Po2233
* 105      0000.0410.0502    dynamic   470        F    F  Po2233
* 105      0000.0410.0512    dynamic   470        F    F  Po2233
* 105      0000.0410.0512    dynamic   470        F    F  nve1(1.1.1.200)
* 104      0000.0410.0402    dynamic   470        F    F  Po2233
* 104      0000.0410.0412    dynamic   470        F    F  Po2233
```

次に、MAC アドレス テーブルのすべての MAC アドレス エントリを消去する例を示します。

```
switch# clear mac address-table dynamic
switch#
```

第 7 章

VXLAN BGP EVPN の設定

この章の内容は、次のとおりです。

VXLAN BGP EVPN に関する情報

VXLAN BGP EVPN の注意事項と制約事項

VXLAN BGP EVPN には、次の注意事項と制約事項があります。

- **internal** キーワードを指定した **show** コマンドはサポートされません。
- レイヤ 3 EVPN は、Broadcom ASIC に基づいた Cisco Nexus 3000 シリーズ スイッチで設定され、これらのスイッチはレイヤ 2 EVPN を持つトポロジに追加されます。このシナリオのルーティングはサポートされません。エニーキャスト ゲートウェイを持つ Broadcom ASIC に基づく Cisco Nexus 3000 シリーズ スイッチで SVI およびレイヤ 3 EVPN を設定する場合、およびレイヤ 2 EVPN デバイス（Broadcom ASIC に基づく Cisco Nexus 3000 シリーズ スイッチなど）から ARP 要求を送信する場合、Cisco Nexus 3000 シリーズ スイッチをネットワーク ポートで受信される ARP 要求のゲートウェイとして使用することはできません。
- IGMP スヌーピングは VXLAN VLAN ではサポートされません。
- DHCP スヌーピング（Dynamic Host Configuration Protocol スヌーピング）は、VXLAN VLAN ではサポートされません。

- VXLAN に対する SPAN TX のカプセル化されたトラフィックは、レイヤ 3 アップリンク インターフェイスではサポートされません。
- RACL は VXLAN トラフィックのレイヤ 3 のアップリンクでサポートされません。出力 VACL のサポートは、ネットワークのカプセル化解除されたパケットが内部ペイロードでディレクションにアクセスするためには使用できません。

  ベスト プラクティスとして、ネットワーク ディレクションへのアクセスに対して、PACL/VACL を使用します。
- QoS 分類は、レイヤ 3 アップリンク インターフェイス上でディレクションにアクセスするための、ネットワーク内の VXLAN トラフィックではサポートされません。
- QoS バッファ ブースト機能は、VXLAN トラフィックには適用できません。
- ポイント ツー マルチポイント レイヤ 3 アップリンクおよび SVI アップリンクは、サポートされません。両方のアップリンク タイプはポイントツーポイントでのみ有効にできるため、2 台以上のスイッチにまたがることはできません。
- EBGP では、ループバック間で単一のオーバーレイ EBGP EVPN セッションを使用することを推奨します。
- NVE を、レイヤ 3 プロトコルで必要な他のループバック アドレスとは別のループバック アドレスにバインドします。VXLAN に対して専用のループバック アドレスを使用することがベスト プラクティスです。
- VXLAN BGP EVPN は、非デフォルト VRF の NVE インターフェイスをサポートしません。
- オーバーレイ BGP セッションのループバックを介して単一の BGP セッションを設定することを推奨します。
- VXLAN UDP ポート番号は、VXLAN のカプセル化に使用されます。Cisco Nexus NX-OS では、UDP ポート番号は 4789 です。これは IETF 標準に準拠しており、設定することはできません。
- ベスト プラクティスとして、対応する VLAN の SVI インターフェイスを持たないレイヤ 2 のみの VNI に対しての ARP 抑制を有効にしないでください。
- 7.0(3)I4(1) 以降、VXLAN は In Service Software Upgrade（ISSU）をサポートします。
- VXLAN は、ネットワーク転送エンジン（NFE）を搭載した Cisco Nexus 9000 シリーズ スイッチでの GRE トンネル機能または MPLS（スタティックまたはセグメントルーティング）機能との共存をサポートしません。
- FEX ホスト インターフェイス ポートに接続された VTEP はサポートされません（7.0(3)I2(1) 以降）。
- Cisco NX-OS リリース 7.0(3)I4(1) では、復元力のあるハッシュ（ポートチャネルのロードバランシング復元力）および VXLAN 設定は、ALE アップリンク ポートを使用する VTEP と互換性がありません。

（注） 復元力のあるハッシュは、デフォルトでは無効になっています。

EVPN コンバージェンスの注意事項

次に、EVPN コンバージェンスに関する注意事項（7.0(3)I3(1) 以降）を示します。

- ベスト プラクティスとしては、必要に応じて NVE がループバックをアップおよびダウンすることができるように、NVE ソース ルックバックを NVE 専用にします。
- vPC が設定されている場合、ループバックは MCT リンクがアップするまでダウンのままになります。

（注） **feature vpc** が有効で VPC が設定されていない場合、NVE ソース ループバックはアップグレード後に「シャットダウン」ステートになります。この場合、**feature vpc** を削除すると、インターフェイスが「アップ」ステートに復元されます。

- NVE アンダーレイ（ソース ループバックを介した）は、オーバーレイが収束するまでダウンのままになります。
  - MCT がアップになると、ソース ループバックは、設定可能な期間中ダウンのままになります。このアプローチでは、オーバーレイが収束するまでノースサウストラフィックは着信できません。
  - MCT がダウンすると、ダウンしていない vPC レッグからノースサウス トラフィックがある場合、NVE は 30 秒間アップのままになります。
- BGP は、vPC ピアからのルートを無視します。これによって、BGP のルート数が削減されます。

VXLAN BGP EVPN 展開に対する考慮事項

- **source-interface config** コマンドを使用する場合は、ループバック アドレスが必要です。 コマンドを使用します。ループバック アドレスは、ローカル VTEP IP を表します。
- スイッチ（7.0(3)I2(2) 以降）のブートアップ時に、**source-interface hold-down-time***hold-down-time* コマンドを使用して、オーバーレイが収束するまで NVE ループバック アドレスのアドバタイズメントを抑制することができます。*hold-down-time* の範囲は、0 ～ 2147483647 秒です。デフォルトは 300 秒です。
- コアで IP マルチキャストのルーティングを確立するには、IP マルチキャストの設定、PIM の設定、および RP の設定が必要です。

- VTEP to VTEP ユニキャストの到達可能性は、いずれかの IGP/BGP プロトコルを介して設定できます。
- 特定の VNI に対してエニーキャスト ゲートウェイ機能が有効になっている場合、ゲートウェイ機能は、その VNI が設定されているすべての VTEP で有効にする必要があります。特定の VNI に対して有効化された一部の VTEP にのみエニーキャスト ゲートウェイ機能を設定することはできません。
- VTEP デバイスの IP アドレスを変更する際のベスト プラクティスとして、IP アドレスを変更する前に NVE インターフェイスを停止/NVE インターフェイスのループバックを停止します。
- ベスト プラクティスとして、マルチキャスト グループの RP は、スパイン レイヤでのみ設定される必要があります。RP のロード バランシングおよび冗長性のために、エニーキャスト RP を使用します。
- すべてのテナント VRF には、VRF オーバーレイ VLAN および VXLAN ルーティング用の SVI が必要です。
- BGP-EVPN で ARP の抑制を設定する場合、**hardware access-list tcam region arp-ether***size***double-wide** コマンドを使用して、この領域の ARP に対応します。（このコマンドを使用する前に、既存の TCAM 領域のサイズを削減する必要があります。）

VXLAN BGP EVPN 展開に対する VPC の考慮事項

- NVE で使用されるループバック アドレスは、プライマリ IP アドレスとセカンダリ IP アドレスを持つように設定する必要があります。

  セカンダリ IP アドレスは、マルチキャストおよびユニキャストのカプセル化されたトラフィックを含むすべての VxLAN トラフィックに使用されます。
- VPC ピアごとに、スパインへの異なる BGP セッションが必要です。
- VPC ピアは同じ設定にする必要があります。
  - VLAN から VN-segment への一貫したマッピング。
  - 同じループバック インターフェイスへの一貫した NVE1 バインディング
    - 同じセカンダリ IP アドレスを使用する。
    - 異なるプライマリ IP アドレスを使用する。
  - グループへの一貫した VNI マッピング。
  - VRF オーバーレイ VLAN は、ピア リンク ポートチャネルのメンバーである必要があります。
- マルチキャストでは、RP（ランデブー ポイント）から（S, G）join を受け取る VPC ノードが DF（指定フォワーダ）になります。DF ノードでは、マルチキャストに対してカプセル化のルートがインストールされます。

カプセル化解除のルートは、VPC プライマリ ノードと VPC セカンダリ ノードの間でのカプセル化解除ノードの選択に基づいてインストールされます。カプセル化解除の選択で優先されるのは、RP へのコストが最小のノードです。ただし、RP へのコストが両方のノードで同じである場合は、vPC プライマリ ノードが選択されます。

カプセル化解除の選択で優先されるノードに、カプセル化解除マルチキャスト ルートがインストールされます。他のノードには、カプセル化解除のルートはインストールされません。

- VPC デバイスで、ホストからの BUM トラフィック（ブロードキャスト、未知のユニキャスト、およびマルチキャスト トラフィック）がピア リンクに複製されます。各ネイティブ パケットからコピーが作成されます。各ネイティブ パケットは、ピア VPC スイッチに接続された orphan ポートを提供するピア リンクを介して送信されます。

  VXLAN ネットワークでのトラフィック ループを防止するために、ピア リンクに入力されるネイティブ パケットは、アップリンクに送信できません。ただし、ピア スイッチがカプセル化ノードである場合は、コピーされたパケットがピア リンクを通過してアップリンクに送信されます。

  （注） それぞれのコピーされたパケットは、特別な内部 VLAN（VLAN 4041）で送信されます。

- ピア リンクが停止している場合、VPC セカンダリの NVE によって使用されるループバック インターフェイスはダウンし、ステータスは **Admin Shut** になります。これは、アップストリーム上でループバックへのルートが取り消され、アップストリームがすべてのトラフィックを VPC プライマリへ転送できるようにするために行われます。

  （注） VPC セカンダリに接続されている orphan ポートでは、ピア リンクが停止している間にトラフィックの損失が発生します。これは、従来の VPC セットアップのセカンダリ VPC におけるレイヤ 2 の orphan ポートに類似しています。

- ピア リンクが停止していない場合、NVE ループバック アドレスが再度提示されます。ルートはアドバタイズされたアップストリームとなり、トラフィックを誘導します。

- VPC の場合、ループバック インターフェイスには、プライマリ IP アドレスとセカンダリ IP アドレスの 2 つの IP アドレスがあります。

  プライマリ IP アドレスは一意で、レイヤ 3 プロトコルで使用されます。

  インターフェイス NVE は VTEP IP アドレスにセカンダリ IP アドレスを使用するため、ループバック上のセカンダリ IP アドレスは必須です。セカンダリ IP アドレスは、vPC の両方のピアで同じにする必要があります。

- VPC ピアゲートウェイ機能は、両方のピアで有効にする必要があります。

  ベストプラクティスとして、vPC トポロジのコンバージェンスを改善するために、peer-switch、peer gateway、ip arp sync、ipv6 nd sync 設定を使用します。

さらに STP Hello タイマーを 4 秒に増やして、VPC ロールの変更が発生したときに不要な TCN が生成されないようにします。

次に、VPC 設定の例（ベスト プラクティス）を示します。

```
switch# sh ru vpc

version 6.1(2)I3(1)
feature vpc
vpc domain 2
  peer-switch
  peer-keepalive destination 172.29.206.65 source 172.29.206.64
  peer-gateway
  ipv6 nd synchronize
  ip arp synchronize
```

- VPC ペアで、片方の VPC ノードの NVE または NVE ループバックをシャットダウンすることはサポートされていない設定です。これは、片方の NVE の停止または片方のループバックの停止でのトラフィック フェールオーバーはサポートされないことを意味します。
- マルチキャスト ロード バランシングおよび RP の冗長性のためにネットワークで設定される冗長エニーキャスト RP は、vPC VTEP トポロジでサポートされます。
- VPC ピアゲートウェイ設定を有効にする必要があります。ピアゲートウェイ機能のために、少なくとも 1 つのバックアップ ルーティング SVI をピア リンクで有効にして、PIM でも設定する必要があります。これにより、VTEPがスパインへの接続を完全に失ったときに、バックアップ ルーティング パスが提供されます。この場合、リモート ピアの到達可能性は、ピア リンクを介して再ルーティングされます。

  次に、PIM が有効な SVI の例を示します。

```
swithch# sh ru int vlan 2

interface Vlan2
  description special_svi_over_peer-link
  no shutdown
  ip address 30.2.1.1/30
  ip pim sparse-mode
```

（注） SVI は、両方の VPC ピアで設定する必要があり、PIM を有効にする必要があります。

- ベスト プラクティスとして、エニーキャスト VPC VTEP のセカンダリ IP アドレスを変更する場合、VPC プライマリおよび VPC セカンダリの両方の NVE インターフェイスを停止してから IP を変更する必要があります。
- VTEP がスパインへのアップリンクをすべて失ったときに、VXLAN トラフィックの冗長性とフェールオーバーを実現するために、VPC ピア間のピア リンクを介してレイヤ 3 リンクまたは SVI リンクを実行することを推奨します。

- DHCP リレーが DHCP クライアントの VRF で必要な場合や、VRF のループバックが VPC ペアの到達可能性テストに必要な場合、PIM が有効な VRF ごとにバックアップ SVI を作成する必要があります。

```
switch# sh ru int vlan 20

interface Vlan20
description backup routing svi for VRF Green
vrf member GREEN
no shutdown
ip address 30.2.10.1/30
```

VXLAN 展開に対するネットワークの考慮事項

- 転送ネットワークの MTU サイズ

  MAC-to-UDP のカプセル化に起因して、VXLAN は元のフレームに 50 バイトのオーバーヘッドを導入しています。このため、転送ネットワークの最大転送単位（MTU）は 50 バイト増やす必要があります。オーバーレイで 1500 バイトの MTU を使用する場合、転送ネットワークは、最低でも 1550 バイトのパケットに対応できるように設定する必要があります。オーバーレイ アプリケーションで 1500 バイトを超える フレーム サイズを頻繁に使用する場合は、転送ネットワークでジャンボ フレームのサポートが必要になります。

- 転送ネットワークの ECMP および LACP ハッシュ アルゴリズム

  前のセクションで説明したように、Cisco Nexus 3000 シリーズ スイッチは、転送ネットワークの ECMP および LACP ハッシュに対する送信元 UDP ポートのエントロピー レベルを導入しています。この実装を強化する方法として、転送ネットワークは ECMP または LACP のハッシュ アルゴリズムを使用します。これらのアルゴリズムはハッシュの入力として UDP 送信元ポートを使用し、これにより VXLAN のカプセル化されたトラフィックに対して最適なロード シェアリングを実現します。

- マルチキャスト グループの拡張

  Cisco Nexus 3000 シリーズ スイッチの VXLAN の実装では、ブロードキャスト、未知のユニキャスト、およびマルチキャスト トラフィックの転送に対してマルチキャスト トンネルを使用します。マルチキャスト転送を提供するには、1 つの VXLAN セグメントを 1 つの IP マルチキャスト グループにマッピングする方法が理想的です。ただし、複数の VXLAN セグメントは、コア ネットワーク内で 1 つの IP マルチキャスト グループを共有することが可能です。VXLAN は、ヘッダーの 24 ビット VNID フィールドを使用して最大 1600 万個の論理レイヤ 2 セグメントをサポートできます。VXLAN セグメントと IP マルチキャスト グループ間の 1 対 1 マッピングにより、VXLAN のセグメント数の増加に起因して、必要なマルチキャスト アドレス空間とコア ネットワーク デバイスのフォワーディング ステートの量がパラレルに増加します。ある時点で、転送ネットワークにおけるマルチキャスト スケーラビリティが問題になることがあります。この場合には、複数の VXLAN セグメントを 1 つのマルチキャスト グループにマッピングすると、コア デバイス上のマルチキャスト コントロール プレーンのリソースが節約され、目的の VXLAN のスケーラビリティを実現できるようになります。ただしこのマッピングは、次善のマルチキャスト転送を犠牲にして実現されます。1 つのテナントのマルチキャスト グループに転送されたパケットは、同じマルチキャスト グループを共有する他のテナントの VTEP に送信されます。このため、マルチキャスト データ

のプレーン リソースの使用が非効率的になります。したがってこのソリューションは、コントロールプレーンのスケーラビリティとデータ プレーンの効率性との二者択一になります。

次善のマルチキャスト複製と転送を実現しているにも関わらず、複数テナントの VXLAN ネットワークで 1 つのマルチキャスト グループを共有することで、テナント ネットワーク間のレイヤ 2 分離に影響をもたらすことはありません。マルチキャスト グループからカプセル化されたパケットを受信すると、VTEP はパケットの VXLAN ヘッダー内の VNID をチェックし、検証します。VTEP は、不明な VNID が見つかるとパケットを廃棄します。VNID が VTEP のローカル VXLAN VNID のいずれかに一致する場合のみ、パケットを VXLAN セグメントに転送します。別のテナントのネットワークはパケットを受信しません。したがって、VXLAN セグメント間の分離は低下しません。

転送ネットワークの考慮事項

転送ネットワークの設定に関する考慮事項は次のとおりです。

- VTEP デバイス：
  - IP マルチキャストを有効にして、設定します。*
  - /32 IP アドレスで、ループバック インターフェイスを作成および設定します。

    （vPC VTEP では、プライマリおよびセカンダリの /32 IP アドレスを設定する必要があります）
  - ループバック インターフェイスで IP マルチキャストを有効にします。*
  - 転送ネットワークで実行されるルーティング プロトコル（スタティック ルート）を通じて、ループバック インターフェイス/32 アドレスをアドバタイズします。
  - アップリンクの出力物理インターフェイスで IP マルチキャストを有効にします。*
- 転送ネットワーク全体：
  - IP マルチキャストを有効にして、設定します。*
- Cisco Nexus 9200 シリーズ スイッチでは、**system nve infra-vlans** コマンドを使用して、インフラ VLAN として使用される VLAN を設定します。VN-Segment を使用せずに設定された VLAN は、インフラ VLAN と見なされます。

（注） * 静的な入力複製または BGP EVPN の入力複製には必要ありません。

VXLAN 展開に対する BGP EVPN の考慮事項

BGP EVPN のコマンド

次に、BGP EVPN VXLAN コントロール プレーンをサポートするコマンドについて説明します。

コマンド	説明
member vni*range* [**associate-vrf**]	VXLAN VNI（仮想ネットワーク識別子）を NVE インターフェイスに関連付けます。 属性 **associate- vrf** は、VRF に関連付けられた処理 VNI を識別および分離したり、ルーティングのために使用されます。 （注） このコマンドで指定される VRF および VNI は、VRF 下の VNI の設定と一致している必要があります。
show nve vni **show nve vni summary**	コントロール プレーンまたはデータ プレーン経由で VNI がピアおよびホスト学習用に設定されているかどうかを特定する情報を表示します。
show bgp l2vpn evpn **show bgp l2vpn evpn summary**	レイヤ 2 VPN EVPN アドレス ファミリを表示します。
host-reachability protocol bgp	BGP をホストの到達可能性アドバタイズメントのメカニズムとして指定します。
suppress-arp	レイヤ 2 VNI の ARP を抑制します。
fabric forwardinganycast-gateway-mac	スイッチのエニーキャスト ゲートウェイ MAC を設定します。
vrf context	VRF を作成して、VRF モードを開始します。
nv overlay evpn	イーサネット VPN（EVPN）を有効/無効にします。
router bgp	ボーダー ゲートウェイ プロトコル（BGP）を設定します。

コマンド	説明
suppress mac-route	BGP がホストの MAC/IP ルートのみを送信するように、BGP MAC ルートを抑制します。 NVE 下では、すべての VNI の MAC の更新が抑制されます。 （注） • 受信側：MAC ルートの抑制は、MAC/IP ルートから MAC ルートを得るためのリモート EVPN ピアの能力に依存します（7.0(3)I2(2) 以降）。ネットワーク内のデバイスが以前の NX-OS リリースで実行されている場合、suppress mac-route コマンドは使用しないでください。 • 送信側：MAC ルートの抑制は、送信元に MAC/IP ルートがあることを意味します。設定に完全なレイヤ 2 VNI（対応する VRF またはレイヤ 3 VNI がない）が含まれている場合、対応する MAC/IP はありません。suppress mac-route コマンドは使用しないでください。

VXLAN BGP EVPN の設定

VXLAN のイネーブル化

VXLAN および EVPN を有効にします。

手順

	コマンドまたはアクション	目的
ステップ 1	**feature vn-segment**	VLAN ベースの VXLAN を有効にします。
ステップ 2	**feature nv overlay**	VXLAN を有効にします。

	コマンドまたはアクション	目的
ステップ 3	**nv overlay evpn**	VXLAN の EVPN コントロールプレーンを有効にします。

VLAN および VXLAN VNI の設定

手順

	コマンドまたはアクション	目的
ステップ 1	**vlan***number*	VLAN を指定します。
ステップ 2	**vn-segment***number*	VXLAN VNI に VLAN をマッピングして、VXLAN VLAN でレイヤ 2 VNI を設定します。

VXLAN ルーティング用の VRF の設定

テナント VRF を設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	**vrf context***vxlan*	VRF を設定します。
ステップ 2	**vni***number*	VNI を指定します。
ステップ 3	**rd auto**	VRF RD（ルート識別子）を指定します。
ステップ 4	**address-family ipv4 unicast**	IPv4 のアドレス ファミリを設定します。
ステップ 5	**route-target both auto**	（注） **auto** オプションの指定は、IBGP にのみ適用可能です。 EBGP では、ルート ターゲットを手動で設定する必要があります。

	コマンドまたはアクション	目的
ステップ 6	**route-target both auto evpn**	（注） **auto** オプションの指定は、IBGP にのみ適用可能です。 EBGP では、ルート ターゲットを手動で設定する必要があります。
ステップ 7	**address-family ipv6 unicast**	IPv6 のアドレス ファミリを設定します。
ステップ 8	**route-target both auto**	（注） **auto** オプションの指定は、IBGP にのみ適用可能です。 EBGP では、ルート ターゲットを手動で設定する必要があります。
ステップ 9	**route-target both auto evpn**	（注） **auto** オプションの指定は、IBGP にのみ適用可能です。 EBGP では、ルート ターゲットを手動で設定する必要があります。

VXLAN ルーティング用のホストの SVI の設定

ホストの SVI を設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	**vlan***number*	VLAN を指定します。
ステップ 2	**interface***vlan-number*	VLAN インターフェイスを指定します。
ステップ 3	**vrf member***vxlan-number*	ホストの SVI を設定します。
ステップ 4	**ip address***address*	IP アドレスを指定します。

VXLAN ルーティング用の VRF オーバレイ VLAN の設定

手順

	コマンドまたはアクション	目的
ステップ 1	**vlan***number*	VLAN を指定します。
ステップ 2	**vn-segment***number*	vn-segment を指定します。

VXLAN ルーティング用の VRF の VNI の設定

VRF オーバーレイ VLAN でレイヤ 3 VNI を設定します。（VRF オーバーレイ VLAN は、ポートに直面するサーバに関連付けられていない VLAN です。VRF にマッピングされるすべての VXLAN VNI には、独自の内部 VLAN を割り当てる必要があります。）

手順

	コマンドまたはアクション	目的
ステップ 1	**vrf context***vxlan*	VXLAN のテナント VRF を作成します。
ステップ 2	**vni***number*	VRF でレイヤ 3 VNI を設定します。

VXLAN ルーティング用のエニーキャスト ゲートウェイの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**fabric forwarding anycast-gateway-mac***address*	分散型ゲートウェイの仮想 MAC アドレスを設定します。 （注） VTEP ごとに 1 つの仮想 MAC を設定します。 （注） すべての VTEP に同じ仮想 MAC アドレスが必要です。

	コマンドまたはアクション	目的
ステップ 2	**fabric forwarding mode anycast-gateway**	VLAN コンフィギュレーション モードで、SVI をエニーキャスト ゲートウェイと関連付けます。

NVE インターフェイスおよび VNI の設定

手順

	コマンドまたはアクション	目的
ステップ 1	**interface***nve-interface*	NVE インターフェイスを設定します。
ステップ 2	**host-reachability protocol bgp**	BGP をホストの到達可能性アドバタイズメントのメカニズムとして定義します。
ステップ 3	**member vni***vni***associate-vrf**	テナント VRF ごとに、オーバーレイに 1 つのレイヤ 3 VNI を追加します。 （注） VXLAN ルーティングに対してのみ必要です。
ステップ 4	**member vni***vni*	レイヤ 2 VNI をトンネル インターフェイスに追加します。
ステップ 5	**mcast-group***address*	VNI 単位で mcast グループを設定します。

VTEP での BGP の設定

手順

	コマンドまたはアクション	目的
ステップ 1	**router bgp***number*	BGP を設定します。
ステップ 2	**router-id***address*	ルータ アドレスを指定します。
ステップ 3	**neighbor***address***remote-as***number*	MP-BGP ネイバーを定義します。各ネイバーで l2vpn evpn を定義します。
ステップ 4	**address-family ipv4 unicast**	IPv4 のアドレス ファミリを設定します。

	コマンドまたはアクション	目的
ステップ 5	**address-family l2vpn evpn**	BGP ネイバーでレイヤ 2 VPN EVPN アドレス ファミリを設定します。 （注） vxlan ホストベース ルーティングでは、Address-family ipv4 evpn です。
ステップ 6	**Allowas-in**	（任意） AS パスで AS 番号の重複を許可します。すべてのリーフが同じ AS を使用しているけれどもスパインがリーフとは異なる AS を持つ場合、eBGP のリーフでこのパラメータを設定します。
ステップ 7	**send-community extended**	BGP ネイバーのコミュニティを設定します。
ステップ 8	**vrf***vrf-name*	VRF を指定します。
ステップ 9	**address-family ipv4 unicast**	IPv4 のアドレス ファミリを設定します。
ステップ 10	**advertise***l2vpn***evpn**	EVPN ルートのアドバタイジングを有効にします。
ステップ 11	**address-family ipv6 unicast**	IPv6 のアドレス ファミリを設定します。
ステップ 12	**advertise***l2vpn***evpn**	EVPN ルートのアドバタイジングを有効にします。

VXLAN ブリッジング用の RD およびルート ターゲットの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**evpn**	VRF を設定します。
ステップ 2	**vni***number***l2**	（注） レイヤ 2 VNI のみ指定する必要があります。
ステップ 3	**rd auto**	VRF RD（ルート識別子）を定義して、VRF コンテキストを設定します。

	コマンドまたはアクション	目的
ステップ 4	**route-target import auto**	VRF ルート ターゲットとインポート ポリシーを定義します。
ステップ 5	**route-target export auto**	VRF ルート ターゲットとエクスポート ポリシーを定義します。

スパインでの EVPN の BGP の設定

手順

	コマンドまたはアクション	目的
ステップ 1	**route-map permitall permit 10**	ルート マップを設定します。 （注） ルートマップは、EVPN ルート用にネクストホップを変更せずに保持します。 • eBGP では必須です。 • iBGP ではオプションです。
ステップ 2	**set ip next-hop unchanged**	ネクストホップ アドレスを設定します。 （注） ルートマップは、EVPN ルート用にネクストホップを変更せずに保持します。 • eBGP では必須です。 • iBGP ではオプションです。
ステップ 3	**router bgp***autonomous system number*	BGP を指定します。
ステップ 4	**address-family l2vpn evpn**	BGP ネイバーでレイヤ 2 VPN EVPN アドレスファミリを設定します。
ステップ 5	**retain route-target all**	レイヤ 2 VPN EVPN アドレスファミリ（グローバル）で retain route-target all を設定します。

	コマンドまたはアクション	目的
		（注） eBGP では必須です。インポート ルート ターゲットと一致するように設定されたローカル VNI がない場合、スパインはすべての EVPN ルートを保持してアドバタイズできます。
ステップ 6	**neighbor***address***remote-as***number*	ネイバーを定義します。
ステップ 7	**address-family l2vpn evpn**	BGP ネイバーでレイヤ 2 VPN EVPN アドレス ファミリを設定します。
ステップ 8	**disable-peer-as-check**	ルート アドバタイズメント時のピア AS 番号のチェックを無効にします。すべてのリーフが同じ AS を使用しているけれどもスパインがリーフとは異なる AS を持つ場合、eBGP のスパインでこのパラメータを設定します。 （注） eBGP では必須です。
ステップ 9	**send-community extended**	BGP ネイバーのコミュニティを設定します。
ステップ 10	**route-map permitall out**	ネクストホップを変更せずに保持するためにルートマップを適用します。 （注） eBGP では必須です。

ARP の抑制

ARP の抑制には、ハードウェアの ACL Ternary Content Addressable Memory（TCAM）領域のサイズ変更が含まれます。

手順

	コマンドまたはアクション	目的
ステップ 1	**hardware access-list tcam region arp-ether***size***double-wide**	ARP を抑制するように TCAM 領域を設定します。 *tcam-size*：TCAM サイズ。サイズは、256 の倍数にする必要があります。サイズが 256 より大きい場合は、512 の倍数でなければなりません。 （注） TCAM 設定を有効にするために、リロードが必要です。

	コマンドまたはアクション	目的
ステップ 2	**interface nve 1**	ネットワーク仮想エンドポイント（NVE）インターフェイスを作成します。
ステップ 3	**member vni***vni-id*	VNI ID を指定します。
ステップ 4	**suppress-arp**	レイヤ 2 VNI で ARP を抑制するように設定します。
ステップ 5	**copy running-config start-up-config**	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

VXLANs のディセーブル化

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	コンフィギュレーション モードに入ります。
ステップ 2	**no nv overlay evpn**	EVPN コントロール プレーンを無効にします。
ステップ 3	**no feature vn-segment-vlan-based**	すべての VXLAN ブリッジ ドメインのグローバル モードをディセーブルにします。
ステップ 4	**no feature nv overlay**	VXLAN 機能をディセーブルにします。
ステップ 5	**copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

IP および MAC アドレスの重複データ検出

Cisco NX-OS では、IP および MAC アドレスの重複データ検出をサポートします。これにより、指定された時間間隔（秒）での移動数に基づいて、IP または MAC アドレスの重複を検出できます。

デフォルトは 180 秒で 5 移動です。（デフォルトの移動回数は 5 です。デフォルトの時間間隔は 180 秒です。）

- IP アドレスの場合：
  - 180 秒以内の 5 番目の移動の後、スイッチで 30 秒間のロック（ホールド ダウン タイマー）が開始され、重複がまだ存在するかどうかが確認されます（シーケンス ビットの増加を防ぐための取り組みです）。この 30 秒間のロックは 5 回発生する可能性があり（180 秒以内に 5 移動を 5 回の意味）、その後スイッチは永続的に重複エントリをロックまたは凍結します。
- MAC アドレスの場合：
  - 180 秒以内の 5 番目の移動の後、スイッチで 30 秒間のロック（ホールド ダウン タイマー）が開始され、重複がまだ存在するかどうかが確認されます（シーケンス ビットの増加を防ぐための取り組みです）。この 30 秒間のロックは 3 回発生する可能性があり（180 秒以内に 5 移動を 3 回の意味）、その後スイッチは永続的に重複エントリをロックまたは凍結します。

次に、重複 IP 検出について特定の時間間隔（秒）での VM の移動数を設定するのに役立つコマンドの例を示します。

コマンド	説明

`switch(config)# fabric forwarding ?`
`anycast-gateway-mac`
`dup-host-ip-addr-detection`
	使用可能なサブコマンド：
	• スイッチのエニーキャストゲートウェイ MAC。
	• n 秒で重複ホスト アドレスを検出します。

`switch(config)# fabric forwarding dup-host-ip-addr-detection ?` `<1-1000>`	n 秒に許可されるホスト移動回数。指定できる範囲は 1 ～ 1000 移動です。デフォルトは 5 移動です。
`switch(config)# fabric forwarding dup-host-ip-addr-detection 100 ?` `<2-36000>`	ホスト移動数に対する重複データ検出のタイムアウト（秒）。指定できる範囲は 2 ～ 36000 秒です。デフォルトは 180 秒です。
`switch(config)# fabric forwarding dup-host-ip-addr-detection 100 10`	10 秒間で重複ホスト アドレスを検出します（100 移動まで）。

次に、重複 MAC 検出について特定の時間間隔（秒）での VM の移動数を設定するのに役立つコマンドの例を示します。

コマンド	説明

`switch(config)# l2rib dup-host-mac-detection ?`
`<1-1000>`
`default`
	L2RIB の使用可能なサブコマンド：
	• n秒に許可されるホスト移動回数。指定できる範囲は 1 ～ 1000 移動です。
	• デフォルト設定（180 秒で 5 移動）。

`switch(config)# l2rib dup-host-mac-detection 100 ?` `<2-36000>`	ホスト移動数に対する重複データ検出のタイムアウト（秒）。指定できる範囲は 2 ～ 36000 秒です。デフォルトは 180 秒です。
`switch(config)# l2rib dup-host-mac-detection 100 10`	10 秒間で重複ホスト アドレスを検出します（100 移動まで）。

VXLAN BGP EVPN 設定の確認

VXLAN BGP EVPN の設定情報を表示するには、次のいずれかのコマンドを入力します。

コマンド	目的
show nve vrf	VRF および関連する VNI を表示します。
show bgp l2vpn evpn	ルーティング テーブルの情報を表示します。
show ip arp suppression-cache [**detail** | **summary** | **vlan***vlan* | **statistics***vlan*]	ARP 抑制の情報を表示します。
show vxlan interface	VXLAN インターフェイスのステータスを表示します。

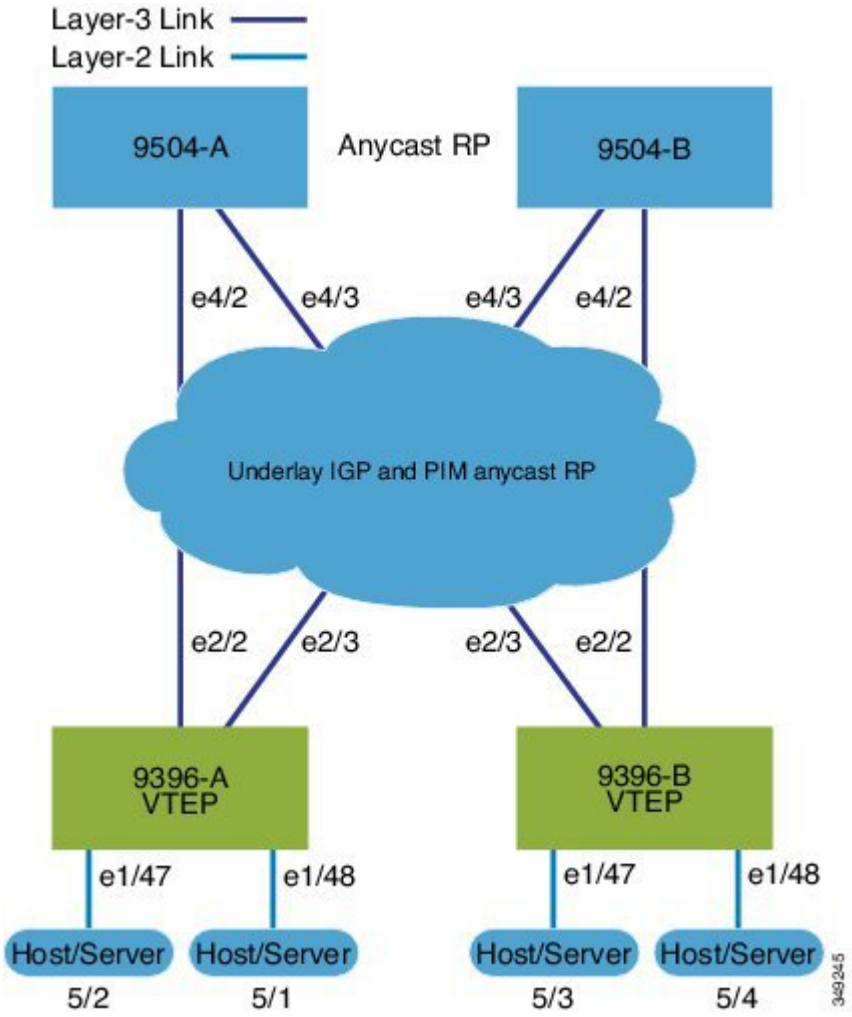
コマンド	目的
show vxlan interface | count	VXLAN VLAN の論理ポートの VP カウントを表示します。 （注） VP は、ポート単位 VLAN 単位で割り当てられます。すべての VXLAN 対応レイヤ 2 ポートのすべての VP の合計が、論理ポートの VP カウントの総数になります。たとえば、レイヤ2 トランク インターフェイスが 10 個あり、それぞれに VXLAN VLAN が 10 個ある場合、VXLAN VLAN の論理ポートの VP カウント総数は 10*10 = 100 になります。
show l2route evpn mac [**all** | **evi***evi* [**bgp** | **local** | **static** | **vxlan** | **arp**]]	レイヤ 2 ルート情報を表示します。
show l2route evpn fl all	すべての fl ルートを表示します。
show l2route evpn imet all	すべての imet ルートを表示します。
show l2route evpn mac-ip all **show l2route evpn mac-ip all detail**	すべての MAC IP ルートを表示します。
show l2route topology	レイヤ 2 ルート トポロジを表示します。

（注） **show ip bgp** コマンドは BGP 設定の確認に使用できますが、ベスト プラクティスとして、代わりに **show bgp** コマンドを使用することが好まれます。

VXLAN BGP EVPN（EBGP）の例

VXLAN BGP EVPN（EBGP）の例：

図 *7*：***VXLAN BGP EVPN*** トポロジ（***EBGP***）



スパインとリーフの間の EBGP

- スパイン（9504-A）
  - EVPN コントロール プレーンの有効化

```
nv overlay evpn
```

  - 関連プロトコルの有効化

```
feature bgp
feature pim
```

- ローカル VTEP IP のループバック、および BGP の設定

```
interface loopback0
  ip address 10.1.1.1/32
  ip pim sparse-mode
```

- エニーキャスト RP のループバックの設定

```
interface loopback1
  ip address 100.1.1.1/32
  ip pim sparse-mode
```

- エニーキャスト RP の設定

```
ip pim rp-address 100.1.1.1 group-list 225.0.0.0/8
ip pim rp-candidate loopback1 group-list 225.0.0.0/8
ip pim log-neighbor-changes
ip pim ssm range 232.0.0.0/8
ip pim anycast-rp 100.1.1.1 10.1.1.1
ip pim anycast-rp 100.1.1.1 20.1.1.1
```

- スパイン用に EBGP で使用されるルートマップの設定

```
route-map permitall permit 10
  set ip next-hop unchanged
```

- スパインリーフ相互接続用インターフェイスの設定

```
interface Ethernet4/2
  ip address 192.168.1.42/24
  ip pim sparse-mode
  no shutdown

interface Ethernet4/3
  ip address 192.168.2.43/24
  ip pim sparse-mode
  no shutdown
```

- EVPN アドレス ファミリの BGP オーバーレイの設定

```
router bgp 100
  router-id 10.1.1.1
  address-family l2vpn evpn
    nexthop route-map permitall
    retain route-target all
  neighbor 30.1.1.1 remote-as 200
    update-source loopback0
    ebgp-multihop 3
    address-family l2vpn evpn
      disable-peer-as-check
      send-community extended
      route-map permitall out
  neighbor 40.1.1.1 remote-as 200
    update-source loopback0
    ebgp-multihop 3
    address-family l2vpn evpn
      disable-peer-as-check
      send-community extended
      route-map permitall out
```

- BGP アンダーレイの設定

```
neighbor 192.168.1.43 remote-as 200
    address-family ipv4 unicast
      allowas-in
```

```
      disable-peer-as-check
```

- スパイン（9504-B）
  - EVPN コントロール プレーンおよび関連プロトコルの有効化

```
feature telnet
feature nxapi
feature bash-shell
feature scp-server
nv overlay evpn
feature bgp
feature pim
feature lldp
```

  - エニーキャスト RP の設定

```
ip pim rp-address 100.1.1.1 group-list 225.0.0.0/8
ip pim rp-candidate loopback1 group-list 225.0.0.0/8
ip pim log-neighbor-changes
ip pim ssm range 232.0.0.0/8
ip pim anycast-rp 100.1.1.1 10.1.1.1
ip pim anycast-rp 100.1.1.1 20.1.1.1
vlan 1-1002
route-map permitall permit 10
  set ip next-hop unchanged
```

  - スパインリーフ相互接続用インターフェイスの設定

```
interface Ethernet4/2
  ip address 192.168.4.42/24
  ip pim sparse-mode
  no shutdown

interface Ethernet4/3
  ip address 192.168.3.43/24
  ip pim sparse-mode
  no shutdown
```

  - ローカル VTEP IP のループバック、および BGP の設定

```
interface loopback0
  ip address 20.1.1.1/32
  ip pim sparse-mode
```

  - エニーキャスト RP のループバックの設定

```
interface loopback1
  ip address 100.1.1.1/32
  ip pim sparse-mode
```

  - EVPN アドレス ファミリの BGP オーバーレイの設定

```
router bgp 100
  router-id 20.1.1.1
  address-family l2vpn evpn
    retain route-target all
  neighbor 30.1.1.1 remote-as 200
    update-source loopback0
    ebgp-multihop 3
    address-family l2vpn evpn
      disable-peer-as-check
      send-community extended
      route-map permitall out
```

```
  neighbor 40.1.1.1 remote-as 200
    ebgp-multihop 3
    address-family l2vpn evpn
      disable-peer-as-check
      send-community extended
      route-map permitall out
```

◦BGP アンダーレイの設定

```
neighbor 192.168.1.43 remote-as 200
    address-family ipv4 unicast
      allowas-in
      disable-peer-as-check
```

- リーフ（9396-A）

◦EVPN コントロール プレーンの有効化

```
nv overlay evpn
```

◦関連プロトコルの有効化

```
feature bgp
feature pim
feature interface-vlan
feature dhcp
```

◦テナント VRF の DHCP リレーの設定

```
service dhcp
ip dhcp relay
ip dhcp relay information option
ip dhcp relay sub-option type cisco
ip dhcp relay information option vpn
```

◦BGP EVPN を使用した分散型エニーキャストゲートウェイがある VXLAN の有効化

```
feature vn-segment-vlan-based
feature nv overlay
fabric forwarding anycast-gateway-mac 0000.2222.3333
```

◦PIM RP の有効化

```
ip pim rp-address 100.1.1.1 group-list 225.0.0.0/8
```

◦BGP のループバックの設定

```
interface loopback0
  ip address 30.1.1.1/32
  ip pim sparse-mode
```

◦ローカル VTEP IP のループバックの設定

```
interface loopback1
  ip address 50.1.1.1/32
  ip pim sparse-mode
```

◦スパインリーフ相互接続用インターフェイスの設定

```
interface Ethernet2/2
  no switchport
  load-interval counter 1 5
```

```
  ip address 192.168.1.22/24
  ip pim sparse-mode
  no shutdown

interface Ethernet2/3
  no switchport
  load-interval counter 1 5
  ip address 192.168.3.23/24
  ip pim sparse-mode
  no shutdown
```

- VRF オーバーレイ VLAN の作成および VN-Segment の設定

```
vlan 101
  vn-segment 900001
```

- VRF の VRF オーバーレイ VLAN/SVI の設定

```
interface Vlan101
  no shutdown
  vrf member vxlan-900001
```

- VLAN の作成および VXLAN へのマッピングの提供

```
vlan 1001
  vn-segment 2001001
vlan 1002
  vn-segment 2001002
```

- VRF の作成および VNI の設定

```
vrf context vxlan-900001
  vni 900001
  rd auto
  address-family ipv4 unicast
    route-target import 65535:101 evpn
    route-target export 65535:101 evpn
    route-target import 65535:101
    route-target export 65535:101
  address-family ipv6 unicast
    route-target import 65535:101 evpn
    route-target export 65535:101 evpn
    route-target import 65535:101
    route-target export 65535:101
```

- SVI に直面するサーバの作成および分散型エニーキャストゲートウェイの有効化

```
interface Vlan1001
  no shutdown
  vrf member vxlan-900001
  ip address 4.1.1.1/24
  ipv6 address 4:1:0:1::1/64
  fabric forwarding mode anycast-gateway
  ip dhcp relay address 192.168.100.1 use-vrf default

interface Vlan1002
  no shutdown
  vrf member vxlan-900001
  ip address 4.2.2.1/24
  ipv6 address 4:2:0:1::1/64
  fabric forwarding mode anycast-gateway
```

- ARP 抑制用の ACL TCAM 領域の設定

```
hardware access-list tcam region arp-ether 256 double-wide
```

- ネットワーク仮想エンドポイント（NVE）インターフェイスの作成

```
interface nve1
  no shutdown
  source-interface loopback1
  host-reachability protocol bgp
  member vni 900001 associate-vrf
  member vni 2001001
    suppress-arp
    mcast-group 225.4.0.1
  member vni 2001002
    suppress-arp
    mcast-group 225.4.0.1
```

- ホスト/サーバのインターフェイスの設定

```
interface Ethernet1/47
  switchport access vlan 1002
interface Ethernet1/48
  switchport access vlan 1001
```

- BGP の設定

```
router bgp 200
router-id 30.1.1.1
  neighbor 10.1.1.1 remote-as 100
    update-source loopback0
    ebgp-multihop 3
      allowas-in
      send-community extended
    address-family l2vpn evpn
      allowas-in
      send-community extended
  neighbor 20.1.1.1 remote-as 100
    update-source loopback0
    ebgp-multihop 3
      allowas-in
      send-community extended
    address-family l2vpn evpn
      allowas-in
      send-community extended
  vrf vxlan-900001

      advertise l2vpn evpn
evpn
  vni 2001001 l2
    rd auto
    route-target import auto
    route-target export auto
  vni 2001002 l2
    rd auto
    route-target import auto
    route-target export auto
```

- リーフ（9396-B）

- EVPN コントロール プレーン機能および関連プロトコルの有効化

```
feature telnet
feature nxapi
feature bash-shell
feature scp-server
nv overlay evpn
feature bgp
feature pim
feature interface-vlan
feature vn-segment-vlan-based
```

```
feature lldp
feature nv overlay
```

- BGP EVPN を使用した分散型エニーキャストゲートウェイがある VXLAN の有効化

```
fabric forwarding anycast-gateway-mac 0000.2222.3333
```

- VRF オーバーレイ VLAN の作成および VN-Segment の設定

```
vlan 1-1002
vlan 101
  vn-segment 900001
```

- VLAN の作成および VXLAN へのマッピングの提供

```
vlan 1001
  vn-segment 2001001
vlan 1002
  vn-segment 2001002
```

- VRF の作成および VNI の設定

```
vrf context vxlan-900001
  vni 900001
  rd auto
  address-family ipv4 unicast
    route-target import 65535:101 evpn
    route-target export 65535:101 evpn
    route-target import 65535:101
    route-target export 65535:101
  address-family ipv6 unicast
    route-target import 65535:101 evpn
    route-target export 65535:101 evpn
    route-target import 65535:101 evpn
    route-target export 65535:101 evpn
```

- ARP 抑制用の ACL TCAM 領域の設定

```
hardware access-list tcam region arp-ether 256 double-wide
```

- VRF の内部制御 VLAN/SVI の設定

```
interface Vlan1

interface Vlan101
  no shutdown
  vrf member vxlan-900001
```

- SVI に直面するサーバの作成および分散型エニーキャストゲートウェイの有効化

```
interface Vlan1001
  no shutdown
  vrf member vxlan-900001
  ip address 4.1.1.1/24
  ipv6 address 4:1:0:1::1/64
  fabric forwarding mode anycast-gateway

interface Vlan1002
  no shutdown
  vrf member vxlan-900001
  ip address 4.2.2.1/24
  ipv6 address 4:2:0:1::1/64
  fabric forwarding mode anycast-gateway
```

- ネットワーク仮想エンドポイント（NVE）インターフェイスの作成

```
interface nve1
  no shutdown
  source-interface loopback1
  host-reachability protocol bgp
  member vni 900001 associate-vrf
  member vni 2001001
    suppress-arp
    mcast-group 225.4.0.1
  member vni 2001002
    suppress-arp
    mcast-group 225.4.0.1
```

- ホスト/サーバのインターフェイスの設定

```
interface Ethernet1/47
  switchport access vlan 1002

interface Ethernet1/48
  switchport access vlan 1001
```

- スパインリーフ相互接続用インターフェイスの設定

```
interface Ethernet2/1

interface Ethernet2/2
  no switchport
  load-interval counter 1 5
  ip address 192.168.4.22/24
  ip pim sparse-mode
  no shutdown

interface Ethernet2/3
  no switchport
  load-interval counter 1 5
  ip address 192.168.2.23/24
  ip pim sparse-mode
  no shutdown
```

- BGP のループバックの設定

```
interface loopback0
  ip address 40.1.1.1/32
  ip pim sparse-mode
```

- ローカル VTEP IP のループバックの設定

```
interface loopback1
  ip address 51.1.1.1/32
  ip pim sparse-mode
```

- BGP の設定

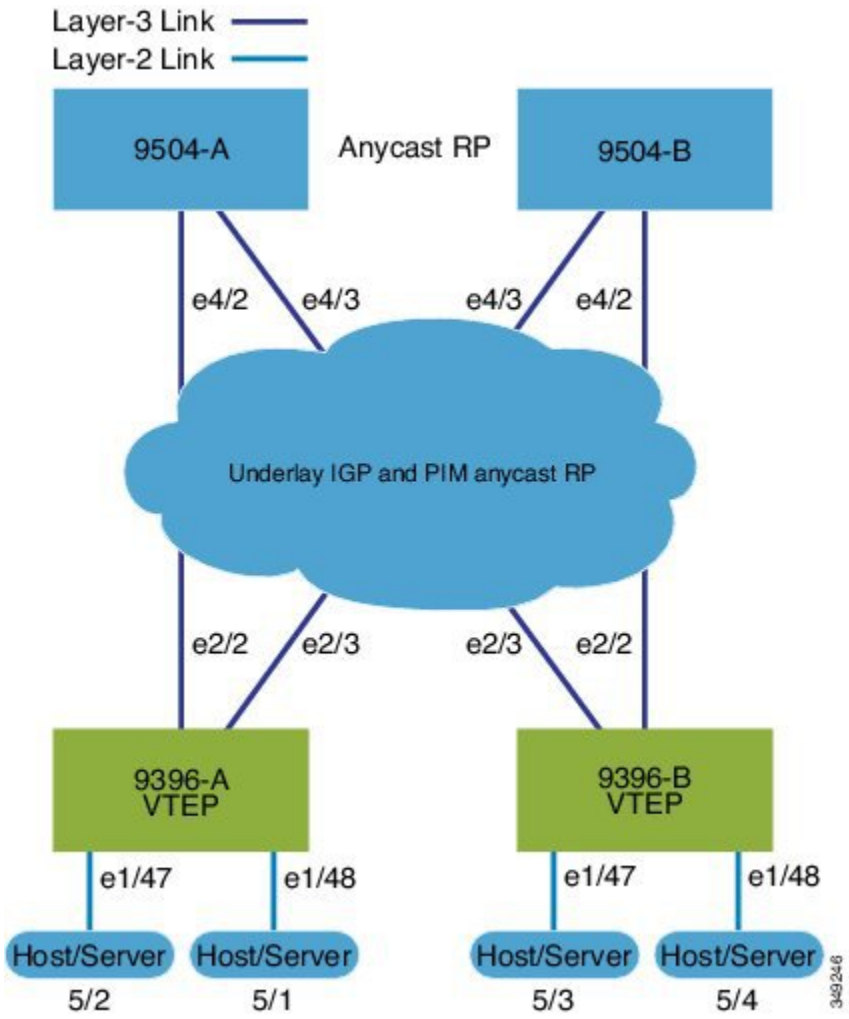
```
router bgp 200
router-id 40.1.1.1
  neighbor 10.1.1.1 remote-as 100
    update-source loopback0
    ebgp-multihop 3
      allowas-in
      send-community extended
    address-family l2vpn evpn
      allowas-in
      send-community extended
  neighbor 20.1.1.1 remote-as 100
    update-source loopback0
```

```
    ebgp-multihop 3
      allowas-in
      send-community extended
    address-family l2vpn evpn
      allowas-in
      send-community extended
  vrf vxlan-900001
      advertise l2vpn evpn
evpn
  vni 2001001 l2
    rd auto
    route-target import auto
    route-target export auto
  vni 2001002 l2
    rd auto
    route-target import auto
    route-target export auto
```

VXLAN BGP EVPN（IBGP）の例

VXLAN BGP EVPN（IBGP）の例：

図 *8*：*VXLAN BGP EVPN* トポロジ（*IBGP*）



スパインとリーフの間の IBGP

- スパイン（9504-A）
  - EVPN コントロール プレーンの有効化

```
nv overlay evpn
```

  - 関連プロトコルの有効化

```
feature ospf
feature bgp
feature pim
```

- ローカル VTEP IP のループバック、および BGP の設定

```
interface loopback0
  ip address 10.1.1.1/32
  ip router ospf 1 area 0.0.0.0
  ip pim sparse-mode
```

- エニーキャスト RP のループバックの設定

```
interface loopback1
  ip address 100.1.1.1/32
  ip router ospf 1 area 0.0.0.0
  ip pim sparse-mode
```

- エニーキャスト RP の設定

```
ip pim rp-address 100.1.1.1 group-list 225.0.0.0/8
ip pim rp-candidate loopback1 group-list 225.0.0.0/8
ip pim ssm range 232.0.0.0/8
ip pim anycast-rp 100.1.1.1 10.1.1.1
ip pim anycast-rp 100.1.1.1 20.1.1.1
```

- アンダーレイ ルーティングの OSPF の有効化

```
router ospf 1
```

- スパインリーフ相互接続用インターフェイスの設定

```
interface Ethernet4/2
  ip address 192.168.1.42/24
  ip router ospf 1 area 0.0.0.0
  ip pim sparse-mode
  no shutdown

interface Ethernet4/3
  ip address 192.168.2.43/24
  ip router ospf 1 area 0.0.0.0
  ip pim sparse-mode
  no shutdown
```

- BGP の設定

```
router bgp 65535
router-id 10.1.1.1
  neighbor 30.1.1.1 remote-as 65535
    update-source loopback0
    address-family l2vpn evpn
      send-community both
      route-reflector-client
  neighbor 40.1.1.1 remote-as 65535
    update-source loopback0
    address-family l2vpn evpn
      send-community both
      route-reflector-client
```

- スパイン（9504-B）

- EVPN コントロール プレーンおよび関連プロトコルの有効化

```
feature telnet
feature nxapi
feature bash-shell
feature scp-server
nv overlay evpn
```

```
feature ospf
feature bgp
feature pim
feature lldp
```

◦エニーキャスト RP の設定

```
ip pim rp-address 100.1.1.1 group-list 225.0.0.0/8
ip pim rp-candidate loopback1 group-list 225.0.0.0/8
ip pim ssm range 232.0.0.0/8
ip pim anycast-rp 100.1.1.1 10.1.1.1
ip pim anycast-rp 100.1.1.1 20.1.1.1
vlan 1-1002
```

◦スパインリーフ相互接続用インターフェイスの設定

```
interface Ethernet4/2
  ip address 192.168.4.42/24
  ip router ospf 1 area 0.0.0.0
  ip pim sparse-mode
  no shutdown

interface Ethernet4/3
  ip address 192.168.3.43/24
  ip router ospf 1 area 0.0.0.0
  ip pim sparse-mode
  no shutdown
```

◦ローカル VTEP IP のループバック、および BGP の設定

```
interface loopback0
  ip address 20.1.1.1/32
  ip router ospf 1 area 0.0.0.0
  ip pim sparse-mode
```

◦エニーキャスト RP のループバックの設定

```
interface loopback1
  ip address 100.1.1.1/32
  ip router ospf 1 area 0.0.0.0
  ip pim sparse-mode
```

◦アンダーレイ ルーティングの OSPF の有効化

```
router ospf 1
```

◦BGP の設定

```
router bgp 65535
router-id 20.1.1.1
  neighbor 30.1.1.1 remote-as 65535
    update-source loopback0
    address-family l2vpn evpn
      send-community both
      route-reflector-client
  neighbor 40.1.1.1 remote-as 65535
    update-source loopback0
     address-family l2vpn evpn
      send-community both
      route-reflector-client
```

• リーフ（9396-A）

- EVPN コントロール プレーンの有効化

```
nv overlay evpn
```

- 関連プロトコルの有効化

```
feature ospf
feature bgp
feature pim
feature interface-vlan
```

- BGP EVPN を使用した分散型エニーキャストゲートウェイがある VXLAN の有効化

```
feature vn-segment-vlan-based
feature nv overlay
fabric forwarding anycast-gateway-mac 0000.2222.3333
```

- アンダーレイ ルーティングの OSPF の有効化

```
router ospf 1
```

- ローカル VTEP IP のループバック、および BGP の設定

```
interface loopback0
  ip address 30.1.1.1/32
  ip router ospf 1 area 0.0.0.0
  ip pim sparse-mode
```

- スパインリーフ相互接続用インターフェイスの設定

```
interface Ethernet2/2
  no switchport
  ip address 192.168.1.22/24
  ip router ospf 1 area 0.0.0.0
  ip pim sparse-mode
  no shutdown

interface Ethernet2/3
  no switchport
  ip address 192.168.3.23/24
  ip router ospf 1 area 0.0.0.0
  ip pim sparse-mode
  no shutdown
```

- PIM RP の設定

```
ip pim rp-address 100.1.1.1 group-list 225.0.0.0/8
ip pim ssm range 232.0.0.0/8
```

- オーバーレイ VRF VLAN の作成および VN-Segment の設定

```
vlan 101
  vn-segment 900001
```

- VRF の VRF オーバーレイ VLAN/SVI の設定

```
interface Vlan101
  no shutdown
  vrf member vxlan-900001
```

- VLAN の作成および VXLAN へのマッピングの提供

```
vlan 1001
  vn-segment 2001001
vlan 1002
  vn-segment 2001002
```

- VRF の作成および VNI の設定

```
vrf context vxlan-900001
  vni 900001
  rd auto
  address-family ipv4 unicast
    route-target both auto
    route-target both auto evpn
  address-family ipv6 unicast
    route-target both auto
    route-target both auto evpn
```

- SVI に直面するサーバの作成および分散型エニーキャストゲートウェイの有効化

```
interface Vlan1001
  no shutdown
  vrf member vxlan-900001
  ip address 4.1.1.1/24
  ipv6 address 4:1:0:1::1/64
  fabric forwarding mode anycast-gateway

interface Vlan1002
  no shutdown
  vrf member vxlan-900001
  ip address 4.2.2.1/24
  ipv6 address 4:2:0:1::1/64
  fabric forwarding mode anycast-gateway
```

- ARP 抑制用の ACL TCAM 領域の設定

```
hardware access-list tcam region arp-ether 256 double-wide
```

- ネットワーク仮想エンドポイント（NVE）インターフェイスの作成

```
interface nve1
  no shutdown
  source-interface loopback0
  host-reachability protocol bgp
  member vni 900001 associate-vrf
  member vni 2001001
    suppress-arp
    mcast-group 225.4.0.1
  member vni 2001002
    suppress-arp
    mcast-group 225.4.0.1
```

- ホスト/サーバのインターフェイスの設定

```
interface Ethernet1/47
  switchport access vlan 1002

interface Ethernet1/48
  switchport access vlan 1001
```

- BGP の設定

```
router bgp 65535
router-id 30.1.1.1
```

```
  neighbor 10.1.1.1 remote-as 65535
    update-source loopback0
    address-family l2vpn evpn
      send-community both
  neighbor 20.1.1.1 remote-as 65535
    update-source loopback0
    address-family l2vpn evpn
      send-community both
  vrf vxlan-900001
    address-family ipv4 unicast
      advertise l2vpn evpn
evpn
  vni 2001001 l2
    rd auto
    route-target import auto
    route-target export auto
  vni 2001002 l2
    rd auto
    route-target import auto
    route-target export auto
```

- リーフ（9396-B）
  - EVPN コントロール プレーン機能および関連プロトコルの有効化

```
feature telnet
feature nxapi
feature bash-shell
feature scp-server
nv overlay evpn
feature ospf
feature bgp
feature pim
feature interface-vlan
feature vn-segment-vlan-based
feature lldp
feature nv overlay
```

  - BGP EVPN を使用した分散型エニーキャストゲートウェイがある VXLAN の有効化

```
fabric forwarding anycast-gateway-mac 0000.2222.3333
```

  - PIM RP の設定

```
ip pim rp-address 100.1.1.1 group-list 225.0.0.0/8
ip pim ssm range 232.0.0.0/8
```

  - オーバーレイ VRF VLAN の作成および VN-Segment の設定

```
vlan 1-1002
vlan 101
  vn-segment 900001
```

  - VLAN の作成および VXLAN へのマッピングの提供

```
vlan 1001
  vn-segment 2001001
vlan 1002
  vn-segment 2001002
```

  - VRF の作成および VNI の設定

```
vrf context vxlan-900001
  vni 900001
  rd auto
```

```
  address-family ipv4 unicast
    route-target both auto
    route-target both auto evpn
  address-family ipv6 unicast
    route-target both auto
    route-target both auto evpn
```

- ARP 抑制用の ACL TCAM 領域の設定

```
hardware access-list tcam region arp-ether 256 double-wide
```

- VRF の内部制御 VLAN/SVI の設定

```
interface Vlan101
  no shutdown
  vrf member vxlan-900001
```

- SVI に直面するサーバの作成および分散型エニーキャストゲートウェイの有効化

```
interface Vlan1001
  no shutdown
  vrf member vxlan-900001
  ip address 4.1.1.1/24
  ipv6 address 4:1:0:1::1/64
  fabric forwarding mode anycast-gateway

interface Vlan1002
  no shutdown
  vrf member vxlan-900001
  ip address 4.2.2.1/24
  ipv6 address 4:2:0:1::1/64
  fabric forwarding mode anycast-gateway
```

- ネットワーク仮想エンドポイント（NVE）インターフェイスの作成

```
interface nve1
  no shutdown
  source-interface loopback0
  host-reachability protocol bgp
  member vni 900001 associate-vrf
  member vni 2001001
    suppress-arp
    mcast-group 225.4.0.1
  member vni 2001002
    suppress-arp
    mcast-group 225.4.0.1
```

- ホスト/サーバのインターフェイスの設定

```
interface Ethernet1/47
  switchport access vlan 1002

interface Ethernet1/48
  switchport access vlan 1001
```

- スパインリーフ相互接続用インターフェイスの設定

```
interface Ethernet2/1

interface Ethernet2/2
  no switchport
  ip address 192.168.4.22/24
  ip router ospf 1 area 0.0.0.0
  ip pim sparse-mode
  no shutdown
```

```
interface Ethernet2/3
  no switchport
  ip address 192.168.2.23/24
  ip router ospf 1 area 0.0.0.0
  ip pim sparse-mode
  no shutdown
```

- ローカル VTEP IP のループバック、および BGP の設定

```
interface loopback0
  ip address 40.1.1.1/32
  ip router ospf 1 area 0.0.0.0
  ip pim sparse-mode
```

- アンダーレイ ルーティングの OSPF の有効化

```
router ospf 1
```

- BGP の設定

```
router bgp 65535
router-id 40.1.1.1
  neighbor 10.1.1.1 remote-as 65535
    update-source loopback0
    address-family l2vpn evpn
      send-community both
  neighbor 20.1.1.1 remote-as 65535
    update-source loopback0
    address-family l2vpn evpn
      send-community both
  vrf vxlan-900001
    address-family ipv4 unicast
      advertise l2vpn evpn
evpn
  vni 2001001 l2
    rd auto
    route-target import auto
    route-target export auto
  vni 2001002 l2
    rd auto
    route-target import auto
    route-target export auto
```

Show コマンドの例

- **show nve peers**

```
9396-B# show nve peers
Interface Peer-IP          Peer-State
--------- ---------------  ----------
nve1      30.1.1.1         Up
```

- **show nve vni**

```
9396-B# show nve vni
Codes: CP - Control Plane        DP - Data Plane
       UC - Unconfigured         SA - Suppress ARP

Interface VNI      Multicast-group   State Mode Type [BD/VRF]      Flags
--------- -------- ----------------- ----- ---- ------------------ -----
```

```
nve1      900001   n/a               Up    CP   L3 [vxlan-900001]
nve1      2001001  225.4.0.1         Up    CP   L2 [1001]          SA
nve1      2001002  225.4.0.1         Up    CP   L2 [1002]          SA
```

- **show ip arp suppression-cache detail**

```
9396-B# show ip arp suppression-cache detail

Flags: + - Adjacencies synced via CFSoE
       L - Local Adjacency
       R - Remote Adjacency
       L2 - Learnt over L2 interface

Ip Address      Age      Mac Address    Vlan Physical-ifindex    Flags

4.1.1.54        00:06:41 0054.0000.0000 1001 Ethernet1/48        L
4.1.1.51        00:20:33 0051.0000.0000 1001 (null)              R
4.2.2.53        00:06:41 0053.0000.0000 1002 Ethernet1/47        L
4.2.2.52        00:20:33 0052.0000.0000 1002 (null)              R
```

- **show vxlan interface**

```
9396-B# show vxlan interface
Interface       Vlan    VPL Ifindex     LTL             HW VP
=========       ====    ===========     ===             =====
Eth1/47         1002    0x4c07d22e      0x10000         5697
Eth1/48         1001    0x4c07d02f      0x10001         5698
```

- **show bgp l2vpn evpn summary**

```
leaf3# show bgp l2vpn evpn summary
BGP summary information for VRF default, address family L2VPN EVPN
BGP router identifier 40.0.0.4, local AS number 10
BGP table version is 60, L2VPN EVPN config peers 1, capable peers 1
21 network entries and 21 paths using 2088 bytes of memory
BGP attribute entries [8/1152], BGP AS path entries [0/0]
BGP community entries [0/0], BGP clusterlist entries [1/4]

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down
State/PfxRcd
40.0.0.1        4    10    8570    8565       60    0    0    5d22h 6
```

- **show bgp l2vpn evpn**

```
leaf3# show bgp l2vpn evpn
BGP routing table information for VRF default, address family L2VPN EVPN
BGP table version is 60, local router ID is 40.0.0.4
Status: s-suppressed, x-deleted, S-stale, d-dampened, h-history, *-valid,
>-best
Path type: i-internal, e-external, c-confed, l-local, a-aggregate, r-redist,
I-injected
Origin codes: i - IGP, e - EGP, ? - incomplete, | - multipath, & - backup

   Network            Next Hop            Metric     LocPrf     Weight Path
Route Distinguisher: 40.0.0.2:32868
*>i[2]:[0]:[10001]:[48]:[0000.8816.b645]:[0]:[0.0.0.0]/216
                      40.0.0.2                          100          0 i
*>i[2]:[0]:[10001]:[48]:[0011.0000.0034]:[0]:[0.0.0.0]/216
                      40.0.0.2                          100          0 i
```

- **show l2route evpn mac all**

```
leaf3# show l2route evpn mac all
Topology    Mac Address    Prod   Next Hop (s)
```

```
----------- -------------- ------ ---------------
101         0000.8816.b645 BGP    40.0.0.2
101         0001.0000.0033 Local  Ifindex 4362086
101         0001.0000.0035 Local  Ifindex 4362086
101         0011.0000.0034 BGP    40.0.0.2
```

- **show l2route evpn mac-ip all**

```
leaf3# show l2route evpn mac-ip all
Topology ID Mac Address    Prod Host IP                 Next Hop (s)
----------- -------------- ---- ------------------------------------------------------------
101         0011.0000.0034 BGP  5.1.3.2                      40.0.0.2
102         0011.0000.0034 BGP  5.1.3.2                      40.0.0.2
```

第 8 章

VXLAN EVPN ファブリックでの IPv6

VXLAN EVPN ファブリックでの IPv6 の概要

この項では、VXLAN EVPN ファブリックのオーバーレイで IPv6 を有効にする設定の例を示します。

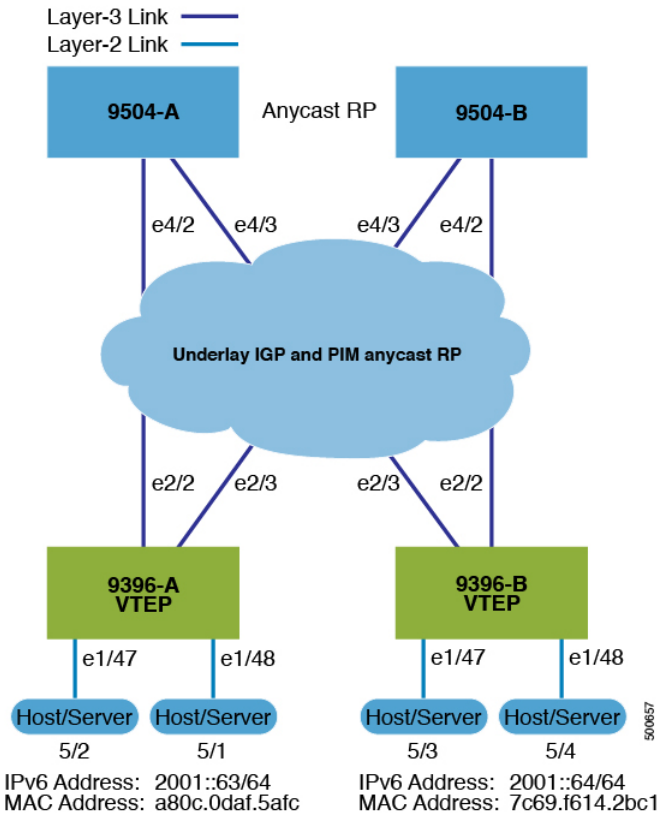
VXLAN のカプセル化メカニズムでは、オーバーレイの IPv6 パケットを IPv4 UDP パケットとしてカプセル化し、IPv4 ルーティングを使用して VXLAN のカプセル化トラフィックを転送します。

VXLAN EVPN ファブリック全体で IPv6 を有効にするには、IPv6 アドレス ファミリを VRF、BGP、および EVPN に含めます。IPv6 ルートは、VTEP のテナント VRF IPv6 ユニキャスト アドレスファミリで開始され、L2VPN EVPN アドレス ファミリを介して EVPN ルートタイプ 2 または 5 として VXLAN ファブリックでアドバタイズされます。

（注） これらのルートは、スパインの EVPN ルートとしてアドバタイズされます。

VXLAN EVPN ファブリックでの IPv6 の設定例

例のトポロジ：



（注） この例では次の動作になります。

- VLAN 10 のホストの設定は、VN-Segment 10010 にマッピングされます。
- VRF RED は、この VLAN に関連付けられた VRF です。
- 20010 は、VRF RED の L3 VNI です。
- VLAN 100 は、L3 VNI 20010 にマッピングされます。

- レイヤ 2 VLAN を設定します。

```
vlan 10
  name RED
  vn-segment 10010
```

- L3 VNI の VLAN を設定します。

```
vlan 100
 name RED_L3_VNI_VLAN
 vn-segment 20010
```

- エニーキャスト ゲートウェイ MAC を定義します。

```
fabric forwarding anycast-gateway-mac 0000.2222.3333
```

- NVE インターフェイスを定義します。

```
interface nve1
  no shutdown
  source-interface loopback1
  host-reachability protocol bgp
  member vni 20010 associate-vrf
  member vni 10010
    suppress-arp
    mcast-group 225.4.0.1

evpn
  vni 10010 l2
    rd auto
    route-target import auto
    route-target export auto
```

- VLAN 10 および L3 VNI VLAN 100 の SVI 定義に設定を追加します。

```
interface Vlan10
  description RED
  no shutdown
  vrf member RED
  no ip redirects
  ip address 10.1.1.1/24
  ipv6 address 2001::1/64
  fabric forwarding mode anycast-gateway
```

- VLAN 100 の SVI 定義を設定します。

```
interface Vlan100
 description RED_L3_VNI_VLAN
 no shutdown
 vrf member RED
 ip forward
 ipv6 address use-link-local-only
```

（注） IPv6 address use-link-local-only は、IPv4 の IP FORWARD と同じ役割を果たします。これによって、インターフェイス VLAN に定義済みの IP アドレスがなくても、スイッチは IP ベースのルックアップを実行できます。

- VRF 定義に設定を追加します。

```
vrf context RED
  vni 20010
  rd auto
  address-family ipv4 unicast
    route-target both auto
    route-target both auto evpn
  address-family ipv6 unicast
    route-target both auto
    route-target both auto evpn

evpn
  vni 10010 l2
    rd auto
    route-target import auto
    route-target export auto
```

- BGP の VRF 定義に設定を追加します。

```
router bgp 65000
  vrf RED
```

```
    address-family ipv4 unicast
      advertise l2vpn evpn
    address-family ipv6 unicast
      advertise l2vpn evpn
```

（注） VTEP が VPC ピアとして動作するように設定されている場合、次の設定が両方のスイッチの VPC ドメインの下に含める必要があるベスト プラクティスです。

```
vpc domain 1
   ipv6 nd synchronize
```

show コマンドの例

次に、VXLAN EVPN を介して IPv6 アドバタイズメントを確認する例を示します。

- 接続されたサーバの ND 情報を表示します。

```
9396-B_VTEP# show ipv6 neighbor vrf RED

Flags: # - Adjacencies Throttled for Glean
       G - Adjacencies of vPC peer with G/W bit
       R - Adjacencies learnt remotely

IPv6 Adjacency Table for VRF RED
Total number of entries: 2
Address         Age       MAC Address     Pref Source     Interface
2001::64        00:00:26  7c69.f614.2bc1  50   icmpv6     Vlan10
fe80::7e69:f6ff:fe14:2bc1
                00:01:13  7c69.f614.2bc1  50   icmpv6     Vlan10
```

- L2ROUTE をチェックして、MAC-IP が学習されたことを確認します。

```
9396-B_VTEP# show l2route evpn mac-ip evi 10 host-ip 2001::64
Mac Address    Prod Host IP                                 Next Hop (s)
-------------- ---- --------------------------------------- --------------
7c69.f614.2bc1 HMM  2001::64                                N/A
```

（注） MAC-IP テーブルは、エンド サーバがネイバー要請メッセージ（IPv4 の場合は ARP）を送信するときにのみ移入されます。

- ルートが BGP テーブルにローカルに存在することを確認します。

```
9396-B_VTEP# show bgp l2vpn evpn 2001::64
BGP routing table information for VRF default, address family L2VPN EVPN
Route Distinguisher: 198.19.0.15:34180    (L2VNI 10010)
BGP routing table entry for [2]:[0]:[0]:[48]:[7c69.f614.2bc1]:[128]:[2001::64]/368,
version 678
Paths: (1 available, best #1)
Flags: (0x00010a) on xmit-list, is not in l2rib/evpn

  Advertised path-id 1
  Path type: local, path is valid, is best path, no labeled nexthop
  AS-Path: NONE, path locally originated
    198.19.0.15 (metric 0) from 0.0.0.0 (198.19.0.15)
      Origin IGP, MED not set, localpref 100, weight 32768
```

```
      Received label 10010 20010
      Extcommunity:  RT:64567:10010 RT:64567:20010

    Path-id 1 advertised to peers:
    198.19.0.3
    198.19.0.4
```

- ルートがリモートの VTEP 9396-A-VTEP BGP テーブルに存在することを確認します。

```
9396-A-VTEP# show bgp l2vpn evpn 2001::64
BGP routing table information for VRF default, address family L2VPN EVPN
Route Distinguisher: 198.19.0.14:34180    (L2VNI 10010)
BGP routing table entry for [2]:[0]:[0]:[48]:[7c69.f614.2bc1]:[128]:[2001::64]/368,
version 305
Paths: (1 available, best #1)
Flags: (0x00021a) on xmit-list, is in l2rib/evpn, is not in HW,

  Advertised path-id 1
  Path type: internal, path is valid, is best path, no labeled nexthop
             Imported from
198.19.0.15:34180:[2]:[0]:[0]:[48]:[7c69.f614.2bc1]:[128]:[2001::64]/240
  AS-Path: NONE, path sourced internal to AS
    198.19.0.15 (metric 81) from 198.19.0.3 (198.19.0.3)
      Origin IGP, MED not set, localpref 100, weight 0
      Received label 10010 20010
      Extcommunity:  RT:64567:10010 RT:64567:20010 ENCAP:8 Router MAC:5087.89a1.a52f
      Originator: 198.19.0.15 Cluster list: 198.19.0.3
```

- L2ROUTE をチェックして、リモート VTEP - 9396-A-VTEP で MAC-IP が学習されたことを確認します。

```
rswV1leaf14# show l2route evpn mac-ip evi 1413 host-ip 2001::64
Mac Address    Prod Host IP                                 Next Hop (s)
-------------- ---- --------------------------------------- --------------
7c69.f614.2bc1 BGP  2001::64                                198.19.0.15
```

第 9 章

仮想ポート チャネルの設定

この章の内容は、次のとおりです。

vPC について

vPC の概要

仮想ポート チャネル（vPC）を使用すると、物理的には 2 台の異なる Cisco Nexus デバイスまたは Cisco Nexus ファブリック エクステンダに接続されている複数のリンクを、第 3 のデバイスからは単一のポート チャネルとして認識されるようにすることができます（次の図を参照）。第 3 のデバイスには、スイッチやサーバなどあらゆるネットワーキング デバイスが該当します。Cisco Nexus ファブリック エクステンダに接続された Cisco Nexus デバイスを含むトポロジ内に vPC を設定できます。vPC では、マルチパス機能を使用することができます。この機能では、ノード間の複数のパラレル パスをイネーブルにし、さらには存在する代替パスでトラフィックのロードバランシングを行うことにより、冗長性が確保されます。

EtherChannel の設定は、次のいずれかを使用して行います。

- プロトコルなし
- リンク集約制御プロトコル（LACP）

vPC ピア リンク チャネルなど、vPC で EtherChannel を設定した場合、それぞれのスイッチでは 1 つの EtherChannel に最大 16 個のアクティブ リンクをまとめることができます。

（注） vPC の機能を設定したり実行したりするには、まず vPC 機能をイネーブルにする必要があります。

vPC 機能をイネーブルにするためには、vPC 機能を実現する 2 つの vPC ピア スイッチの vPC ドメインにピアキープアライブ リンクおよびピアリンクを作成する必要があります。

vPC ピア リンクを作成する場合は、まず一方の Cisco Nexus デバイス上で、2 つ以上の Ethernet ポートを使用して EtherChannel を設定します。さらに他方のスイッチ上で、2 つ以上の Ethernet ポートを使用して別の EtherChannel を設定します。これら 2 つの EtherChannel を接続することにより、vPC ピア リンクが作成されます。

（注） vPC ピアリンク EtherChannel はトランクとして設定することが推奨されます。

vPC ドメインには、両方の vPC ピア デバイス、vPC ピアキープアライブ リンク、vPC ピア リンク、および vPC ドメイン内にあってダウンストリーム デバイスに接続されているすべての EtherChannel が含まれます。各 vPC ピア デバイスに設定できる vPC ドメイン ID は 1 つだけです。

（注） EtherChannel を使用する vPC デバイスはすべて、両方の vPC ピア デバイスに接続する必要があります。

vPC には次のような特長があります。

- 単独のデバイスが、2 つのアップストリーム デバイスを介して EtherChannel を使用できるようになります。
- スパニングツリー プロトコル（STP）のブロック ポートが不要になります。
- ループフリーなトポロジが実現されます。
- 利用可能なすべてのアップリンク帯域幅を使用します。
- リンクまたはスイッチに障害が発生した場合、高速コンバージェンスが実行されます。
- リンクレベルの復元力を提供します。
- ハイ アベイラビリティが保証されます。

用語

vPC の用語

vPC で使用される用語は、次のとおりです。

- vPC：vPC ピア デバイスとダウンストリーム デバイスの間の結合された EtherChannel。

- vPC ピア デバイス：vPC ピア リンクと呼ばれる特殊な EtherChannel により接続されることで対をなす個々のデバイス。
- vPC ピア リンク：vPC ピア デバイス間の状態を同期するために使用されるリンク。
- vPC メンバ ポート：vPC に属するインターフェイス。
- vPC ドメイン：両方の vPC ピア デバイス、vPC ピアキープアライブ リンク、vPC 内にあってダウンストリーム デバイスに接続されているすべてのポート チャネルが含まれるドメイン。また、このドメインは、vPC グローバル パラメータを割り当てるために使用する必要があるコンフィギュレーション モードに関連付けられています。vPC ドメイン ID は、両スイッチで同じであることが必要です。
- vPC ピアキープアライブ リンク：ピアキープアライブ リンクでは、vPC ピア Cisco Nexus デバイスの稼働力のモニタリングが行われます。ピアキープアライブ リンクは、vPC ピア デバイス間での設定可能なキープアライブ メッセージの定期的な送信を行います。

  vPCs ピアキープアライブ リンク上を移動するデータまたは同期トラフィックはありません。このリンクを流れるトラフィックは、送信元スイッチが稼働しており、vPC を実行していることを知らせるメッセージだけです。

vPC ドメイン

vPC ドメインを作成するには、まず各 vPC ピア スイッチに対し、1 ～ 1000 の範囲にある値を使用して vPC ドメイン ID を作成する必要があります。この ID は、対象となるすべての vPC ピア デバイス上で同じであることが必要です。

EtherChannel および vPC ピア リンクは、LACP を使用するかまたはプロトコルなしのいずれかで設定できます。可能な場合、ピア リンクで LACP を使用することを推奨します。これは、LACP が EtherChannel の設定の不一致に対する設定チェックを提供するためです。

vPC ピア スイッチでは、設定した vPC ドメイン ID に基づいて、一意の vPC システム MAC アドレスが自動的に割り当てられます。各 vPC ドメインには一意の MAC アドレスがあり、vPC に関連する特定の処理の際に固有識別子として使用されます。ただしスイッチで vPC システム MAC アドレスが使用されるのは、LACP などリンク関連の処理に限ります。連続したネットワーク内の vPC ドメインはそれぞれ、一意のドメイン ID を使用して作成することが推奨されます。ただし、Cisco NX-OS ソフトウェアでアドレスを割り当てる代わりに、vPC ドメインに特定の MAC アドレスを設定することもできます。

vPC ピア スイッチでは、設定した vPC ドメイン ID に基づいて、一意の vPC システム MAC アドレスが自動的に割り当てられます。スイッチで vPC システム MAC アドレスが使用されるのは、LACP や BPDU などリンク関連の処理に限ります。vPC ドメインに特定の MAC アドレスを設定することもできます。

両方のピアに同じ vPC ドメイン ID を設定し、ドメイン ID をネットワークで一意にすることを推奨します。たとえば、2 つの異なる vPC（一方がアクセス スイッチ、もう一方が集約スイッチ）がある場合は、それぞれの vPC に固有のドメイン ID を割り当ててください。

vPC ドメインを作成すると、その vPC ドメインのシステム プライオリティが Cisco NX-OS ソフトウェアによって自動的に作成されます。vPC ドメインに特定のシステム プライオリティを手動で設定することもできます。

（注） システム プライオリティを手動で設定する場合は、必ず両方の vPC ピア スイッチ上に同じプライオリティ値を割り当てるようにしてください。両側の vPC ピア スイッチに異なるシステム プライオリティ値が割り当てられている場合、vPC は稼働しません。

ピアキープアライブ リンクとメッセージ

Cisco NX-OS ソフトウェアでは、vPC ピア間のピアキープアライブ リンクを使用して、設定可能なキープアライブ メッセージが定期的に送信されます。これらのメッセージを送信するためには、ピア スイッチ間にレイヤ 3 接続が必要です。ピアキープアライブ リンクがアップ状態で稼働していなければ、システムでは vPC ピア リンクをアップすることができません。

一方の vPC ピア スイッチに障害が発生すると、vPC ピア リンクのもう一方の側にある vPC ピア スイッチでは、ピアキープアライブ メッセージを受信しなくなることによってその障害を検知します。vPC ピアキープアライブ メッセージのデフォルトの時間間隔は 1 秒です。この時間間隔は、400 ミリ秒～ 10 秒の範囲で設定することができます。タイムアウト値は、3 ～ 20 秒の範囲内で設定可能で、デフォルトのタイムアウト値は 5 秒です。ピアキープアライブのステータスの確認は、ピアリンクがダウンした場合にのみ行われます。

vPC ピアキープアライブは、Cisco Nexus デバイス上の管理 VRF でもデフォルトの VRF でも伝送できます。管理 VRF を使用するようスイッチを設定した場合は、mgmt 0 インターフェイスの IP アドレスがキープアライブ メッセージの送信元および宛先となります。デフォルトの VRF を使用するようスイッチを設定した場合は、vPC キープアライブ メッセージの送信元アドレスおよび宛先アドレスとしての役割を果たす SVI を作成する必要があります。ピアキープアライブ メッセージに使用される送信元 IP アドレスと宛先 IP アドレスがどちらもネットワーク上で一意であり、かつそれらの IP アドレスがその vPC ピアキープアライブ リンクに関連付けられている VRF から到達可能であることを確認してください。

（注） Cisco Nexus デバイスの vPC ピアキープアライブ リンクは、管理 VRF で mgmt 0 インターフェイスを使用して実行されるように設定することが推奨されます。デフォルトの VRF を設定する場合は、vPC ピアキープアライブ メッセージの伝送に vPC ピア リンクが使用されないようにしてください。

vPC ピア リンクの互換パラメータ

多くの設定パラメータおよび動作パラメータが、vPC 内のすべてのインターフェイスで同じでなければなりません。vPC 機能をイネーブルにし、さらに両方の vPC ピア スイッチ上でピア リンクを設定すると、シスコ ファブリック サービス（CFS）メッセージにより、ローカル vPC ピア ス

イッチに関する設定のコピーがリモート vPC ピア スイッチへ送信されます。これによりシステムでは、2 つのスイッチ間で重要な設定パラメータに違いがないかどうか判定が行われます。

vPC 内のすべてのインターフェイスで設定されている値を表示するには、**show vpc consistency-parameters** コマンドを入力します。表示される設定は、vPC ピア リンクおよび vPC の稼働を制限する可能性のある設定だけです。

vPC に関する互換性チェックのプロセスは、正規の EtherChannel に関する互換性チェックとは異なります。

vPC ポート チャネルでの新しいタイプ 2 整合性検査

vPC ポート チャネルのスイッチポート MAC 学習設定を検証するために、新しいタイプ 2 整合性検査が追加されました。CLI の **show vpc consistency-check vPC <vpc no.>** は、スイッチポート MAC 学習設定のローカル値とピア値を表示するように拡張されました。これはタイプ 2 チェックであるため、vPC は、ローカル値とピア値の間に不一致がある場合でも動作上アップ状態になりますが、この不一致は CLI 出力から表示できます。

```
switch# sh vpc consistency-parameters vpc 1112

    Legend:
        Type 1 : vPC will be suspended in case of mismatch

Name                                  Type            Local Value                Peer Value
-------------                          ----            -----------------------
-----------------------
Shut Lan                              1               No                         No
STP Port Type                         1               Default                     Default
STP Port Guard                        1               None                        None
STP MST Simulate PVST                 1               Default                     Default
nve configuration                     1               nve                        nve
lag-id                                1               [(fa0,                      [(fa0,
                                                      0-23-4-ee-be-64, 8458,
0-23-4-ee-be-64, 8458,
                                                      0, 0), (8000,              0, 0),
(8000,
                                                      f4-4e-5-84-5e-3c, 457,
f4-4e-5-84-5e-3c, 457,
                                                      0, 0)]                     0, 0)]
mode                                  1               active                      active
Speed                                 1               10 Gb/s                    10 Gb/s
Duplex                                1               full                        full
Port Mode                             1               trunk                       trunk
Native Vlan                           1               1                          1
MTU                                   1               1500                        1500
Admin port mode                       1
Switchport MAC Learn                  2               Enable                     Disable>
Newly added consistency parameter
vPC card type                         1               Empty                      Empty
Allowed VLANs                         -               311-400                     311-400
Local suspended VLANs                 -               -
```

同じでなければならない設定パラメータ

ここで説明する設定パラメータは、vPC ピア リンクの両側のスイッチ上で設定が同じであることが必要です。

（注） ここで説明する動作パラメータおよび設定パラメータは、vPC内のすべてのインターフェイスで一致している必要があります。

vPC 内のすべてのインターフェイスで設定されている値を表示するには、**show vpc consistency-parameters** コマンドを入力します。表示される設定は、vPC ピア リンクおよびvPCの稼働を制限する可能性のある設定だけです。

スイッチでは、vPC インターフェイス上でこれらのパラメータに関する互換性チェックが自動的に行われます。インターフェイス別のパラメータはインターフェイスごとに整合性を保っていることが必要であり、グローバル パラメータはグローバルに整合性を保っていることが必要です。

- ポートチャネル モード：オン、オフ、またはアクティブ
- チャネル単位のリンク速度
- チャネル単位のデュプレックス モード
- チャネルごとのトランク モード：
  - ネイティブ VLAN
  - トランク上で許可される VLAN
  - ネイティブ VLAN トラフィックのタギング
- スパニング ツリー プロトコル（STP）モード
- マルチ スパニングツリーの STP 領域コンフィギュレーション（MST）
- VLAN ごとのイネーブル/ディセーブル状態
- STP グローバル設定：
  - ブリッジ保証設定
  - ポート タイプ設定：vPCインターフェイスはすべて標準ポートとして設定することが推奨されます
  - ループ ガード設定
- STP インターフェイス設定：
  - ポート タイプ設定
  - ループ ガード
  - ルート ガード

これらのうち、イネーブルでないパラメータや一方のスイッチでしか定義されていないパラメータは、vPC の整合性検査では無視されます。

（注） どの vPC インターフェイスもサスペンド モードになっていないことを確認するには、**show vpc brief** コマンドおよび **show vpc consistency-parameters** コマンドを入力して、syslog メッセージをチェックします。

同じにすべき設定パラメータ

次に挙げるパラメータのいずれかが両方の vPC ピア スイッチ上で同じように設定されていないと、誤設定が原因でトラフィック フローに望ましくない動作が発生する可能性があります。

- MAC エージング タイマー
- スタティック MAC エントリ
- VLAN インターフェイス：vPC ピア リンクの両端にある各スイッチの VLAN インターフェイスは同じ VLAN 用に設定されている必要があり、さらにそれらの管理モードおよび動作モードも同じであることが必要です。ピア リンクの一方のスイッチでのみ設定されている VLAN では、vPC またはピア リンクを使用したトラフィックの転送は行われません。VLAN はすべて、プライマリ vPC スイッチとセカンダリ vPC スイッチの両方で作成する必要があります。両方で作成されていない場合、VLAN は停止することになります。
- プライベート VLAN 設定
- ACL のすべての設定とパラメータ
- Quality of Service（QoS）の設定およびパラメータ：ローカル パラメータです。グローバル パラメータは同じであることが必要です
- STP インターフェイス設定：
  - BPDU Filter
  - BPDU ガード
  - コスト
  - リンク タイプ
  - プライオリティ
  - VLAN（Rapid PVST+）

すべての設定パラメータについて互換性があることを確認するためにも、vPC の設定後は各 vPC ピア スイッチの設定を表示することが推奨されます。

VLAN ごとの整合性検査

タイプ 1 整合性検査が VLAN ごとに実行されます。この整合性検査に合格しない VLAN は、プライマリ スイッチおよびセカンダリ スイッチでダウン状態になりますが、その他の VLAN は影響を受けません。

vPC 自動リカバリ

両側の vPC ピア スイッチでリロードが実行され、かつ一方のスイッチのみリブートした場合、自動リカバリによってそのスイッチがプライマリ スイッチとして機能し、一定時間が経過した後に vPC リンクがアップ状態になります。このシナリオにおけるリロード遅延時間は、240 ～ 3600 秒の範囲で設定できます。

ピア リンクの障害に伴ってセカンダリ vPC スイッチ上の vPC がディセーブルになり、さらにプライマリ vPC スイッチで障害が発生するか、またはトラフィックが転送できなくなると、セカンダリ スイッチでは vPC が再イネーブル化されます。このシナリオの場合、vPC ではキープアライブが 3 回連続して検出されないのを待ってから vPC リンクが回復します。

vPC 自動リカバリ機能は、デフォルトではディセーブルです。

vPC ピア リンク

vPC ピア リンクは、vPC ピア デバイス間の状態を同期するために使用されるリンクです。

（注） vPC ピア リンクを設定する場合は、あらかじめピアキープアライブ リンクを設定しておく必要があります。設定しておかないと、ピア リンクは機能しません

vPC ピア リンクの概要

vPC ピアとして設定できるのは、対をなす 2 台のスイッチです。それぞれのスイッチは互いに、他方の vPC ピアに対してのみ vPC ピアとして機能します。vPC ピア スイッチには、他のスイッチへの非 vPC リンクを設定することもできます。

適正な設定を行うため、各スイッチに EtherChannel を設定し、さらに vPC ドメインを設定します。各スイッチの EtherChannel をピア リンクとして割り当てます。冗長性を確保できるよう、EtherChannel には少なくとも 2 つの専用ポートを設定することが推奨されます。これにより、vPC ピア リンクのインターフェイスの 1 つに障害が発生すると、スイッチは自動的にフォールバックし、そのピア リンクの別のインターフェイスが使用されます。

（注） EtherChannel はトランク モードで設定することが推奨されます。

多くの動作パラメータおよび設定パラメータは、vPC ピア リンクにより接続されている各スイッチ上で同じ値であることが必要です。各スイッチは管理プレーンから完全に独立しているため、重要なパラメータについてスイッチ同士に互換性があることを確認する必要があります。vPC ピア スイッチは、個別のコントロールプレーンを持ちます。vPC ピア リンクの設定が完了したら、各 vPC ピア スイッチの設定を表示し、それらの設定に互換性があることを確認してください。

（注） vPC ピア リンクによって接続されている 2 つのスイッチでは必ず、同一の動作パラメータおよび設定パラメータが設定されている必要があります。

vPC ピア リンクを設定する際、vPC ピア スイッチでは、接続されたスイッチの一方がプライマリ スイッチ、もう一方がセカンダリ スイッチとなるようにネゴシエーションが行われます。デフォルトの場合、Cisco NX-OS ソフトウェアでは、最小の MAC アドレスを基にプライマリ スイッチが選択されます。特定のフェールオーバー条件の下でのみ、このソフトウェアは各スイッチ（つまり、プライマリ スイッチとセカンダリ スイッチ）に対して別々の処理を行います。プライマリ スイッチに障害が発生した場合、システムが回復した時点でセカンダリ スイッチがプライマリ スイッチとして動作し、元々のプライマリ スイッチがセカンダリ スイッチとなります。

ただし、どちらの vPC スイッチをプライマリ スイッチにするか設定することもできます。一方の vPC スイッチをプライマリ スイッチにするためロール プライオリティを再設定する場合は、まずプライマリ vPC スイッチとセカンダリ vPC スイッチのそれぞれに対してロール プライオリティを適切な値に設定し、**shutdown** コマンドを入力して両スイッチの vPC ピア リンクである EtherChannel をシャットダウンした後、**no shutdown** コマンドを入力して両スイッチの EtherChannel を再度イネーブルにします。

ピア間では、vPC リンクを介して認識された MAC アドレスの同期も行われます。

設定情報は、Cisco Fabric Service over Ethernet（CFSoE）プロトコルを使用して vPC ピア リンクを転送されます。両方のスイッチで設定されているこれらの VLAN の MAC アドレスはすべて、vPC ピア スイッチ間で同期されています。この同期に、CFSoE が使用されます

vPC ピア リンクに障害が発生すると、ソフトウェアでは、両方のスイッチが稼働していることを確認するため、vPC ピア スイッチ間のリンクであるピアキープアライブ リンクを使用してリモート vPC ピア スイッチのステータス確認が行われます、vPC ピア スイッチが稼働している場合は、セカンダリ vPC スイッチにあるすべて vPC ポートがディセーブルになります。さらにデータは、EtherChannel において依然アクティブ状態にあるリンクに転送されます。

ソフトウェアは、ピアキープアライブ リンクを介してキープアライブ メッセージが返されない場合、vPC ピア スイッチに障害が発生したと認識します。

vPC ピア スイッチ間では、別途用意されたリンク（vPC ピアキープアライブ リンク）を使用して、設定可能なキープアライブ メッセージが送信されます。vPC ピアキープアライブ リンク上のキープアライブ メッセージにより、障害が vPC ピア リンク上でだけ発生したのか、vPC ピア スイッチ上で発生したのかが判断されます。キープアライブ メッセージは、ピア リンク内のすべてのリンクで障害が発生した場合にだけ使用されます。

vPC 番号

vPC ドメイン ID と vPC ピア リンクを作成し終えたら、ダウンストリーム スイッチを各 vPC ピア スイッチに接続するための EtherChannel を作成します。つまり、ダウンストリーム スイッチ上に単一の EtherChannel を作成し、プライマリ vPC ピア スイッチにポートの半分を、セカンダリ ピア スイッチにポートの残り半分を使用します。

各 vPC ピア スイッチ上では、ダウンとリーム スイッチに接続された EtherChannel に同じ vPC 番号を割り当てます。vPC の作成時にトラフィックが中断されることはほとんどありません。設定を簡素化するため、各 EtherChannel に対してその EtherChannel と同じ番号の vPC ID 番号を割り当てることもできます（EtherChannel 10 に対しては vPC ID 10 を割り当てるなど）。

（注） vPC ピア スイッチからダウンストリーム スイッチに接続されている EtherChannel に割り当てる vPC 番号は、両方の vPC スイッチで同じでなければなりません。

その他の機能との vPC の相互作用

vPC と LACP

Link Aggregation Control Protocol（LACP）では、vPC ドメインのシステム MAC アドレスに基づいて、その vPC に対する LACP Aggregation Group（LAG）ID が構成されます。

LACP は、ダウンストリーム スイッチからのチャネルも含め、すべての vPC EtherChannel 上で使用できます。vPC ピア スイッチの各 EtherChannel のインターフェイスに対しては、LACP をアクティブ モードで設定することが推奨されます。この設定により、スイッチ、単方向リンク、およびマルチホップ接続の間の互換性をより簡単に検出できるようになり、実行時の変更およびリンク障害に対してダイナミックな応答が可能になります。

vPC ピア リンクは、16 個の EtherChannel インターフェイスをサポートしています。

（注） システム プライオリティを手動で設定する場合は、必ず両方の vPC ピア スイッチ上に同じプライオリティ値を割り当てるようにしてください。vPC ピア スイッチ同士が異なるシステム プライオリティ値を持っていると、vPC は稼働しません。

vPC ピア リンクと STP

vPC 機能の初回起動時には、STP は再コンバージェンスします。STP は、vPC ピア リンクを特殊なリンクとして扱い、常に vPC ピア リンクを STP のアクティブ トポロジに含めます。

すべての vPC ピア リンク インターフェイスを STP ネットワーク ポート タイプに設定して、すべての vPC リンク上で Bridge Assurance が自動的にイネーブルになるようにすることを推奨します。また、vPC ピア リンク上ではどの STP 拡張機能もイネーブルにしないことが推奨されます。

一連のパラメータは、vPC ピア リンクの両端の vPC ピア スイッチ上で設定を同じにする必要があります。

STP は分散型です。つまり、このプロトコルは、両端の vPC ピア スイッチ上で継続的に実行されます。ただし、セカンダリ vPC ピア スイッチ上の vPC インターフェイスの STP プロセスは、プライマリ スイッチとして選択されている vPC ピア スイッチ上での設定により制御されます。

プライマリ vPC スイッチでは、Cisco Fabric Services over Ethernet（CFSoE）を使用して、vPC セカンダリ ピア スイッチ上の STP 状態の同期化が行われます。

vPC ピア スイッチ間では、プライマリ スイッチとセカンダリ スイッチを設定して 2 つのスイッチを STP 用に調整する提案/ハンドシェイク合意が vPC マネージャによって実行されます。さらにプライマリ vPC ピア スイッチにより、プライマリ スイッチおよびセカンダリ スイッチの vPC インターフェイスに対する STP プロトコルの制御が行われます。

ブリッジ プロトコル データ ユニット（BPDU）では、代表ブリッジ ID フィールドの STP ブリッジ ID として、vPC に対して設定された MAC アドレスが使用されます。これら vPC インターフェイスの BPDU は vPC プライマリ スイッチにより送信されます。

（注） vPC ピア リンクの両側での設定を表示して、設定が同じであることを確認してください。vPC に関する情報を表示する場合は、**show spanning-tree** コマンドを使用します。

CFSoE

Cisco Fabric Services over Ethernet（CFSoE）は、vPC ピア デバイスのアクションを同期化するために使用する信頼性の高い状態転送メカニズムです。CFSoE は、vPC にリンクされている、STP、IGMP などの多くの機能のメッセージとパケットを伝送します。情報は、CFS/CFSoE プロトコル データ ユニット（PDU）に入れて伝送されます。

CFSoE は、vPC 機能をイネーブルにすると、デバイスによって自動的にイネーブルになります。何も設定する必要はありません。vPC の CFSoE 分散には、IP を介してまたは CFS リージョンに分散する機能は必要ありません。CFSoE 機能が vPC 上で正常に機能するために必要な設定は一切ありません。

show mac address-table コマンドを使用すれば、CFSoE が vPC ピア リンクのために同期する MAC アドレスを表示できます。

（注） **no cfs eth distribute** コマンドと **no cfs distribute** コマンドは入力しないでください。vPC 機能に対しては CFSoE をイネーブルにする必要があります。vPC がイネーブルの場合にこれらのコマンドのいずれかを入力すると、エラー メッセージが表示されます。

show cfs application コマンドを入力すると、出力に「Physical-eth」と表示されます。これは、CFSoE を使用しているアプリケーションを表します。

VRF に関する注意事項と制約事項

vPC 設定時の注意事項と制限事項は次のとおりです。

- vPC は、異なるタイプの Cisco Nexus 3000 シリーズ スイッチ間ではサポートされません。
- VPC ピアには、VXLAN 用に予約した同一の VLAN が必要です。ピアで予約した VLAN が異なると、VXLAN によって望ましくない動作が発生する可能性があります。
- Release 7.0(3)I2(1) 以降では、CLI コマンドの **sh vpc brief** の出力に、Delay-restore status と Delay-restore SVI status の 2 つの追加のフィールドが表示されます。
- vPC は、IPv6 では動作確認されていません。
- vPC ピアリンクおよび vPC インターフェイスを設定する場合は、あらかじめ vPC 機能をイネーブルにしておく必要があります。
- システムにおいて vPC ピア リンクを構成するためには、その前にピアキープアライブ リンクを設定しておく必要があります。
- vPC ピアリンクは、少なくとも 2 つの 10 ギガビット イーサネット インターフェイスを使用して構成する必要があります。
- 両方のピアに同じ vPC ドメイン ID を設定し、ドメイン ID をネットワークで一意にすることを推奨します。たとえば、2 つの異なる vPC（1 つがアクセスで 1 つが集約）がある場合は、各 vPC には、一意のドメイン ID がある必要があります。
- vPC に使用できるのは、ポート チャネルのみです。vPC は標準ポート チャネル（スイッチ間の vPC トポロジ）およびポート チャネル ホスト インターフェイス（ホスト インターフェイスの vPC トポロジ）で設定できます。
- 両側の vPC ピア スイッチを設定する必要があります。ただし vPC ピア デバイス間で設定が自動的に同期化されることはありません。
- 必要な設定パラメータが、vPC ピア リンクの両側で互換性を保っているかチェックしてください。
- vPC の設定中に、最小限のトラフィックの中断が発生する可能性があります。
- アクティブ モードのインターフェイスで LACP を使用して vPC のすべてのポート チャネルを設定する必要があります。
- vPC の最初のメンバが起動すると、トラフィックが中断する可能性があります。
- OSPF over vPC および BFD with OSPF は、Cisco Nexus 3000 および 3100 シリーズ スイッチでサポートされます。

  SVI の制約：BFD セッションが仮想ポート チャネル（vPC）ピア リンクを使用して SVI 経由で行われる場合、BFD エコー機能はサポートされません。SVI 設定レベルで **no bfd echo** を

使用して、vPC ピア ノード間で行われる SVI 経由のすべてのセッションに関して BFD エコー機能を無効にする必要があります。

- ピアキープアライブに管理インターフェイスではなくレイヤ 3 リンクが使用されている場合、CPU キューがコントロール プレーン トラフィックと輻輳すると、vPC ピアキープアライブ パケットがドロップする可能性があります。CPU トラフィックには、ルーティング プロトコル、ARP、Glean、および IPMC ミス パケットが含まれます。ピアキープアライブ インターフェイスが管理インターフェイスではなくレイヤ 3 リンクである場合、vPC ピアキープアライブ パケットは、ロープライオリティ キューで CPU に送信されます。

  vPC ピアキープアライブにレイヤ 3 リンクが使用されている場合は、次の ACL を設定して vPC ピアキープアライブを優先させます。

  ```
  ip access-list copp-system-acl-routingproto2
  30 permit udp any any eq 3200
  ```

  ここで、「3200」は、キープアライブ パケットのデフォルトの UDP ポートです。デフォルト ポートが変更されている場合は、この ACL を、設定されている UDP ポートに一致させる必要があります。

vPC 設定の確認

vPC の設定情報を表示する場合は、次のコマンドを使用します。

コマンド	目的
switch# **show feature**	vPC がイネーブルかどうかを表示します。
switch# **show port-channel capacity**	設定されている EtherChannel の数、およびスイッチ上でまだ使用可能な EtherChannel の数を表示します。
switch# **show running-config vpc**	vPC の実行コンフィギュレーションの情報を表示します。
switch# **show vpc brief**	vPC に関する簡単な情報を表示します。
switch# **show vpc consistency-parameters**	すべての vPC インターフェイス全体で一貫している必要があるパラメータのステータスを表示します。
switch# **show vpc peer-keepalive**	ピアキープアライブ メッセージの情報を表示します。
switch# **show vpc role**	ピア ステータス、ローカル スイッチのロール、vPC システムの MAC アドレスとシステム プライオリティ、およびローカル vPC スイッチの MAC アドレスとプライオリティを表示します。

コマンド	目的
switch# **show vpc statistics**	vPC に関する統計情報を表示します。 （注） このコマンドは、現在作業している vPC ピア デバイスの vPC 統計情報しか表示しません。

スイッチの出力の詳細については、使用する Cisco Nexus シリーズ スイッチのコマンド リファレンスを参照してください。

グレースフル タイプ 1 検査ステータスの表示

次に、グレースフル タイプ 1 整合性検査の現在のステータスを表示する例を示します。

```
switch# show vpc brief
Legend:
                (*) - local vPC is down, forwarding via vPC peer-link

vPC domain id                     : 10
Peer status                       : peer adjacency formed ok
vPC keep-alive status             : peer is alive
Configuration consistency status: success
Per-vlan consistency status     : success
Type-2 consistency status       : success
vPC role                          : secondary
Number of vPCs configured       : 34
Peer Gateway                      : Disabled
Dual-active excluded VLANs      : -
Graceful Consistency Check      : Enabled
Auto-recovery status              : Disabled
Delay-restore status              : Timer is off.(timeout = 30s)
Delay-restore SVI status          : Timer is off.(timeout = 10s)

vPC Peer-link status
---------------------------------------------------------------------
id   Port   Status Active vlans
--   ----   ------ --------------------------------------------------
1    Po1    up     1
```

グローバル タイプ 1 不整合の表示

グローバル タイプ 1 不整合が発生すると、セカンダリ スイッチの vPC はダウンします。次の例は、スパニングツリー モードでの不一致に伴って生じたこのタイプの不整合を示したものです。

次に、セカンダリ スイッチ上の一時停止された vPC VLAN のステータスを表示する例を示します。

```
switch(config)# show vpc
Legend:
                (*) - local vPC is down, forwarding via vPC peer-link

vPC domain id                     : 10
Peer status                       : peer adjacency formed ok
vPC keep-alive status             : peer is alive
Configuration consistency status: failed
Per-vlan consistency status     : success
Configuration consistency reason: vPC type-1 configuration incompatible - STP
```

```
                                  Mode inconsistent
Type-2 consistency status       : success
vPC role                        : secondary
Number of vPCs configured       : 2
Peer Gateway                    : Disabled
Dual-active excluded VLANs      : -
Graceful Consistency Check      : Enabled

vPC Peer-link status
---------------------------------------------------------------------
id   Port   Status Active vlans
--   ----   ------ -----------------------------------------------------
1    Po1    up     1-10

vPC status
----------------------------------------------------------------------------
id     Port        Status Consistency Reason                     Active vlans
------ ----------- ------ ----------- -------------------------- -----------
20     Po20        down*  failed      Global compat check failed -
30     Po30        down*  failed      Global compat check failed -
```

次に、プライマリ スイッチ上の不整合ステータス（プライマリ vPC 上の VLAN は一時停止されていない）を表示する例を示します。

```
switch(config)# show vpc
Legend:
                (*) - local vPC is down, forwarding via vPC peer-link

vPC domain id                   : 10
Peer status                     : peer adjacency formed ok
vPC keep-alive status           : peer is alive
Configuration consistency status: failed
Per-vlan consistency status     : success
Configuration consistency reason: vPC type-1 configuration incompatible - STP Mo
de inconsistent
Type-2 consistency status       : success
vPC role                        : primary
Number of vPCs configured       : 2
Peer Gateway                    : Disabled
Dual-active excluded VLANs      : -
Graceful Consistency Check      : Enabled

vPC Peer-link status
---------------------------------------------------------------------
id   Port   Status Active vlans
--   ----   ------ -----------------------------------------------------
1    Po1    up     1-10

vPC status
----------------------------------------------------------------------------
id     Port        Status Consistency Reason                     Active vlans
------ ----------- ------ ----------- -------------------------- -----------
20     Po20        up     failed      Global compat check failed 1-10
30     Po30        up     failed      Global compat check failed 1-10
```

インターフェイス別タイプ 1 不整合の表示

インターフェイス別タイプ 1 不整合が発生すると、セカンダリ スイッチの vPC ポートはダウンしますが、プライマリ スイッチの vPC ポートはアップ状態が維持されます。次の例は、スイッチポート モードでの不一致に伴って生じたこのタイプの不整合を示したものです。

次に、セカンダリ スイッチ上の一時停止された vPC VLAN のステータスを表示する例を示します。

```
switch(config-if)# show vpc brief
Legend:
                (*) - local vPC is down, forwarding via vPC peer-link

vPC domain id                     : 10
Peer status                       : peer adjacency formed ok
vPC keep-alive status             : peer is alive
Configuration consistency status: success
Per-vlan consistency status       : success
Type-2 consistency status         : success
vPC role                          : secondary
Number of vPCs configured         : 2
Peer Gateway                      : Disabled
Dual-active excluded VLANs        : -
Graceful Consistency Check        : Enabled
Auto-recovery status                : Disabled
Delay-restore status                : Timer is off.(timeout = 30s)
Delay-restore SVI status            : Timer is off.(timeout = 10s)

vPC Peer-link status
---------------------------------------------------------------------
id   Port   Status Active vlans
--   ----   ------ --------------------------------------------------
1    Po1    up     1

vPC status
----------------------------------------------------------------------------
id     Port        Status Consistency Reason                     Active vlans
------ ----------- ------ ----------- -------------------------- -----------
20     Po20        up     success     success                    1
30     Po30        down*  failed      Compatibility check failed -
                                       for port mode
```

次に、プライマリ スイッチ上の不整合ステータス（プライマリ vPC 上の VLAN は一時停止されていない）を表示する例を示します。

```
switch(config-if)# show vpc brief
Legend:
                (*) - local vPC is down, forwarding via vPC peer-link

vPC domain id                     : 10
Peer status                       : peer adjacency formed ok
vPC keep-alive status             : peer is alive
Configuration consistency status: success
Per-vlan consistency status       : success
Type-2 consistency status         : success
vPC role                          : primary
Number of vPCs configured         : 2
Peer Gateway                      : Disabled
Dual-active excluded VLANs        : -
Graceful Consistency Check        : Enabled
Auto-recovery status                : Disabled
Delay-restore status                : Timer is off.(timeout = 30s)
Delay-restore SVI status            : Timer is off.(timeout = 10s)

vPC Peer-link status
---------------------------------------------------------------------
id   Port   Status Active vlans
--   ----   ------ --------------------------------------------------
1    Po1    up     1

vPC status
----------------------------------------------------------------------------
id     Port        Status Consistency Reason                     Active vlans
------ ----------- ------ ----------- -------------------------- -----------
20     Po20        up     success     success                    1
30     Po30        up     failed      Compatibility check failed 1
```

for port mode

VLAN ごとの整合性ステータスの表示

VLAN ごとの整合性ステータスまたは不整合のステータスを表示する場合は、**show vpc consistency-parameters vlans** コマンドを入力します。

次に、プライマリおよびセカンダリ スイッチ上の VLAN の整合ステータスを表示する例を示します。

```
switch(config-if)# show vpc brief
Legend:
                (*) - local vPC is down, forwarding via vPC peer-link

vPC domain id                     : 10
Peer status                       : peer adjacency formed ok
vPC keep-alive status             : peer is alive
Configuration consistency status: success
Per-vlan consistency status     : success
Type-2 consistency status       : success
vPC role                          : secondary
Number of vPCs configured       : 2
Peer Gateway                      : Disabled
Dual-active excluded VLANs      : -
Graceful Consistency Check      : Enabled
Auto-recovery status              : Disabled
Delay-restore status              : Timer is off.(timeout = 30s)
Delay-restore SVI status          : Timer is off.(timeout = 10s)

vPC Peer-link status
---------------------------------------------------------------------
id   Port   Status Active vlans
--   ----   ------ --------------------------------------------------
1    Po1    up     1-10

vPC status
----------------------------------------------------------------------------
id     Port        Status Consistency Reason                     Active vlans
------ ----------- ------ ----------- -------------------------- -----------
20     Po20        up     success     success                    1-10
30     Po30        up     success     success                    1-10
```

no spanning-tree vlan 5 コマンドを入力すると、プライマリおよびセカンダリ VLAN で不整合が引き起こされます。

```
switch(config)# no spanning-tree vlan 5
```

次に、セカンダリ スイッチ上の VLAN ごとの整合ステータスを Failed として表示する例を示します。

```
switch(config)# show vpc brief
Legend:
                (*) - local vPC is down, forwarding via vPC peer-link

vPC domain id                     : 10
Peer status                       : peer adjacency formed ok
vPC keep-alive status             : peer is alive
Configuration consistency status: success
Per-vlan consistency status     : failed
Type-2 consistency status       : success
vPC role                          : secondary
Number of vPCs configured       : 2
Peer Gateway                      : Disabled
Dual-active excluded VLANs      : -
Graceful Consistency Check      : Enabled
```

```
Auto-recovery status             : Disabled
Delay-restore status             : Timer is off.(timeout = 30s)
Delay-restore SVI status         : Timer is off.(timeout = 10s)

vPC Peer-link status
---------------------------------------------------------------------
id   Port   Status Active vlans
--   ----   ------ --------------------------------------------------
1    Po1    up     1-4,6-10

vPC status
----------------------------------------------------------------------------
id     Port        Status Consistency Reason                     Active vlans
------ ----------- ------ ----------- -------------------------- -----------
20     Po20        up     success     success                    1-4,6-10
30     Po30        up     success     success                    1-4,6-10
```

次に、プライマリ スイッチ上の VLAN ごとの整合ステータスを Failed として表示する例を示します。

```
switch(config)# show vpc brief
Legend:
                (*) - local vPC is down, forwarding via vPC peer-link

vPC domain id                   : 10
Peer status                     : peer adjacency formed ok
vPC keep-alive status           : peer is alive
Configuration consistency status: success
Per-vlan consistency status     : failed
Type-2 consistency status       : success
vPC role                        : primary
Number of vPCs configured       : 2
Peer Gateway                    : Disabled
Dual-active excluded VLANs      : -
Graceful Consistency Check      : Enabled
Auto-recovery status              : Disabled
Delay-restore status              : Timer is off.(timeout = 30s)
Delay-restore SVI status          : Timer is off.(timeout = 10s)

vPC Peer-link status
---------------------------------------------------------------------
id   Port   Status Active vlans
--   ----   ------ --------------------------------------------------
1    Po1    up     1-4,6-10

vPC status
----------------------------------------------------------------------------
id     Port        Status Consistency Reason                     Active vlans
------ ----------- ------ ----------- -------------------------- -----------
20     Po20        up     success     success                    1-4,6-10
30     Po30        up     success     success                    1-4,6-10
```

次に、STP Disabled としての不整合の例を示します。

```
switch(config)# show vpc consistency-parameters vlans

Name                        Type  Reason Code             Pass Vlans

-------------               ----  --------------------- ------------------------
STP Mode                    1     success               0-4095
STP Disabled                1     vPC type-1            0-4,6-4095
                                  configuration
                                  incompatible - STP is
                                  enabled or disabled on
                                   some or all vlans
STP MST Region Name         1     success               0-4095
STP MST Region Revision     1     success               0-4095
STP MST Region Instance to  1     success               0-4095
 VLAN Mapping
STP Loopguard               1     success               0-4095
STP Bridge Assurance        1     success               0-4095
```

```
STP Port Type, Edge          1     success                0-4095
BPDUFilter, Edge BPDUGuard
STP MST Simulate PVST        1     success                0-4095
Pass Vlans                   -                            0-4,6-4095
```

vPC のデフォルト設定

次の表は、vPC パラメータのデフォルト設定をまとめたものです。

表 *8*：デフォルト *vPC* パラメータ

パラメータ	デフォルト
vPC システム プライオリティ	32667
vPC ピアキープアライブ メッセージ	ディセーブル
vPC ピアキープアライブ間隔	1 秒
vPC ピアキープアライブ タイムアウト	5 秒
vPC ピアキープアライブ UDP ポート	3200

vPC の設定

vPC のイネーブル化

vPC を設定して使用する場合は、事前に vPC 機能をイネーブルにしておく必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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 2	switch(config)# **feature vpc**	スイッチで vPC をイネーブルにします。
ステップ 3	switch# **show feature**	（任意） スイッチ上でイネーブルになっている機能を表示します。

	コマンドまたはアクション	目的
ステップ 4	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次の例は、vPC 機能をイネーブルにする方法を示します。

```
switch# configure terminal
switch(config)# feature vpc
```

vPC のディセーブル化

vPC 機能をディセーブルにできます。

（注） vPC 機能をディセーブルにすると、Cisco Nexus デバイスがすべての vPC 設定をクリアします。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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 2	switch(config)# **no feature vpc**	スイッチで vPC をディセーブルにします。
ステップ 3	switch# **show feature**	（任意） スイッチ上でイネーブルになっている機能を表示します。
ステップ 4	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次の例は、vPC 機能をディセーブルにする方法を示します。

```
switch# configure terminal
switch(config)# no feature vpc
```

vPC ドメインの作成

両側の vPC ピア スイッチに対して、同じ vPC ドメイン ID を作成する必要があります。このドメイン ID を基に、vPC システムの MAC アドレスが自動的に構成されます。

はじめる前に

vPC 機能をイネーブルにしていることを確認します。

vPC ピア リンクの両側に両方のスイッチを設定する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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 2	switch(config)# **vpc domain***domain-id*	スイッチに対して vPC ドメインを作成し、vpc-domain コンフィギュレーション モードを開始します。 *domain-id* のデフォルト値はありません。指定できる値の範囲は 1 ～ 1000 です。 （注） 既存の vPC ドメインに対して vpc-domain コンフィギュレーション モードを開始する場合は、**vpc domain** コマンドを使用することもできます。
ステップ 3	switch# **show vpc brief**	（任意） 各 vPC ドメインに関する要約情報を表示します。
ステップ 4	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次に、vPC ドメインを作成する例を示します。

```
switch# configure terminal
switch(config)# vpc domain 5
```

vPC キープアライブ リンクと vPC キープアライブ メッセージの設定

キープアライブ メッセージを伝送するピアキープアライブ リンクの宛先 IP を設定できます。必要に応じて、キープアライブ メッセージのその他のパラメータも設定できます。

Cisco NX-OS ソフトウェアは、vPC ピア間でピアキープアライブ リンクを使用して、設定可能なキープアライブ メッセージを定期的に送信します。これらのメッセージを送信するには、ピアデバイス間にレイヤ 3 接続が必要です。ピアキープアライブ リンクが起動および動作していないと、システムは vPC ピア リンクを開始できません。

ピアキープアライブ メッセージに使用される送信元と宛先の IP アドレスの両方が、ネットワーク内で一意であることを確認してください。また、vPC ピアキープアライブ リンクに関連付けられ

ている Virtual Routing and Forwarding（VRF）インスタンスから、これらの IP アドレスが到達可能であることを確認してください。

（注） vPC ピアキープアライブ リンクを使用する際は、個別の VRF インスタンスを設定して、各 vPC ピア スイッチからその VRF インスタンスにレイヤ 3 ポートを接続することが推奨されます。ピア リンク自体を使用して vPC ピアキープアライブ メッセージを送信しないでください。

はじめる前に

vPC 機能をイネーブルにしていることを確認します。

システムで vPC ピア リンクを形成できるようにするには、まず vPC ピアキープアライブ リンクを設定する必要があります。

vPC ピア リンクの両側に両方のスイッチを設定する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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 2	switch(config)# **vpc domain***domain-id*	スイッチ上に vPC ドメインが存在しない場合はそれを作成し、vpc-domain 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	switch(config-vpc-domain)# **peer-keepalive destination***ipaddress* [**hold-timeout***secs* | **interval***msecs* {**timeout***secs*} | **precedence** {*prec-value* | **network** | **internet** | **critical** | **flash-override** | **flash** | **immediate** **priority** | **routine**} | **tos** {*tos-value* | **max-reliability** | **max-throughput** | **min-delay** | **min-monetary-cost** | **normal**} | **tos-byte***tos-byte-value*} | **source***ipaddress* | **vrf** {*name* | **management vpc-keepalive**}]	vPC ピアキープアライブ リンクのリモート エンドの IPv4 アドレスを設定します。 （注） vPC ピアキープアライブ リンクを設定するまで、vPC ピア リンクは構成されません。 管理ポートと VRF がデフォルトです。
ステップ 4	switch(config-vpc-domain)# **vpc peer-keepalive destination** *ipaddress* **source***ipaddress*	（任意） vPC ピアキープアライブ リンクに対し、個別の VRF インスタンスを設定して、各 vPC ピア デバイスからその VRF にレイヤ 3 ポートを接続します。

	コマンドまたはアクション	目的
ステップ 5	switch# **show vpc peer-keepalive**	（任意） キープアライブ メッセージのコンフィギュレーションに関する情報を表示します。
ステップ 6	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次の例は、vPC ピアキープアライブ リンクの宛先 IP アドレスを設定する方法を示したものです。

```
switch# configure terminal
switch(config)# vpc domain 5
switch(config-vpc-domain)# peer-keepalive destination 10.10.10.42
```

次に、プライマリとセカンダリの vPC デバイス間でピア キープアライブ リンク接続を設定する例を示します。

```
switch(config)# vpc domain 100
switch(config-vpc-domain)# peer-keepalive destination 192.168.2.2 source 192.168.2.1
Note:--------:: Management VRF will be used as the default VRF ::--------
switch(config-vpc-domain)#
```

次の例は、vPC ピアキープアライブ リンクに対して、vpc_keepalive という名前の VRF インスタンスを別途設定する方法、およびその新しい VRF を検査する方法を示したものです。

```
vrf context vpc_keepalive
interface Ethernet1/31
  switchport access vlan 123
interface Vlan123
  vrf member vpc_keepalive
  ip address 123.1.1.2/30
  no shutdown
vpc domain 1
  peer-keepalive destination 123.1.1.1 source 123.1.1.2 vrf
vpc_keepalive

L3-NEXUS-2# show vpc peer-keepalive

vPC keep-alive status           : peer is alive
--Peer is alive for             : (154477) seconds, (908) msec
--Send status                   : Success
--Last send at                  : 2011.01.14 19:02:50 100 ms
--Sent on interface             : Vlan123
--Receive status                : Success
--Last receive at               : 2011.01.14 19:02:50 103 ms
--Received on interface         : Vlan123
--Last update from peer         : (0) seconds, (524) msec

vPC Keep-alive parameters
--Destination                   : 123.1.1.1
--Keepalive interval            : 1000 msec
--Keepalive timeout             : 5 seconds
--Keepalive hold timeout        : 3 seconds
--Keepalive vrf                 : vpc_keepalive
--Keepalive udp port            : 3200
--Keepalive tos                 : 192
```

```
The services provided by the switch , such as ping, ssh, telnet,
radius, are VRF aware. The VRF name need to be configured or
specified in order for the correct routing table to be used.
L3-NEXUS-2# ping 123.1.1.1 vrf vpc_keepalive
PING 123.1.1.1 (123.1.1.1): 56 data bytes
64 bytes from 123.1.1.1: icmp_seq=0 ttl=254 time=3.234 ms
64 bytes from 123.1.1.1: icmp_seq=1 ttl=254 time=4.931 ms
64 bytes from 123.1.1.1: icmp_seq=2 ttl=254 time=4.965 ms
64 bytes from 123.1.1.1: icmp_seq=3 ttl=254 time=4.971 ms
64 bytes from 123.1.1.1: icmp_seq=4 ttl=254 time=4.915 ms

--- 123.1.1.1 ping statistics ---
5 packets transmitted, 5 packets received, 0.00% packet loss
round-trip min/avg/max = 3.234/4.603/4.971 ms
```

vPC ピア リンクの作成

vPC ピア リンクを作成する場合は、指定した vPC ドメインのピア リンクとする EtherChannel を各スイッチ上で指定します。冗長性を確保するため、トランク モードで vPC ピア リンクとして指定する EtherChannel を設定し、各 vPC ピア スイッチで個別のモジュールの 2 つのポートを使用することを推奨します。

はじめる前に

vPC 機能をイネーブルにしていることを確認します。

vPC ピア リンクの両側に両方のスイッチを設定する必要があります

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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 2	switch(config)# **interface port-channel***channel-number*	このスイッチの vPC ピア リンクとして使用する EtherChannel を選択し、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 3	switch(config-if)# **vpc peer-link**	選択した EtherChannel を vPC ピア リンクとして設定し、vpc-domain 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	switch# **show vpc brief**	（任意） vPC ピア リンクに関する情報など、各 vPC の情報を表示します。
ステップ 5	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次の例は、vPC ピア リンクを設定する方法を示します。

```
switch# configure terminal
switch(config)# interface port-channel 20
switch(config-if)# vpc peer-link
```

設定の互換性の検査

両側の vPC ピア スイッチに vPC ピア リンクを設定した後に、すべての vPC インターフェイスで設定に整合性があるかどうかの検査を行います。

次の QoS パラメータは、タイプ 2 整合性検査をサポートします。

- Network QoS：MTU および Pause
- Input Queuing：Bandwidth および Absolute Priority
- Output Queuing：Bandwidth および Absolute Priority

タイプ 2 の不一致の場合、vPC は停止しません。タイプ 1 の不一致が検出されると vPC は停止します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **show vpc consistency-parameters**{**global**|**interface port-channel***channel-number*}	すべての vPC インターフェイス全体で一貫している必要があるパラメータのステータスを表示します。

次の例は、すべての vPC インターフェイスの間で必須設定の互換性が保たれているかチェックする方法を示します。

```
switch# show vpc consistency-parameters global
Legend:
        Type 1 : vPC will be suspended in case of mismatch
Name                        Type  Local Value            Peer Value

------------- ----  ---------------------- -----------------------
QoS                         2     ([], [], [], [], [],   ([], [], [], [], [],
                                   [])                    [])

Network QoS (MTU)           2     (1538, 0, 0, 0, 0, 0)  (1538, 0, 0, 0, 0, 0)
Network Qos (Pause)         2     (F, F, F, F, F, F)     (1538, 0, 0, 0, 0, 0)
Input Queuing (Bandwidth)   2     (100, 0, 0, 0, 0, 0)   (100, 0, 0, 0, 0, 0)
Input Queuing (Absolute     2     (F, F, F, F, F, F)     (100, 0, 0, 0, 0, 0)
Priority)
Output Queuing (Bandwidth)  2     (100, 0, 0, 0, 0, 0)   (100, 0, 0, 0, 0, 0)
Output Queuing (Absolute    2     (F, F, F, F, F, F)     (100, 0, 0, 0, 0, 0)
Priority)
STP Mode                    1     Rapid-PVST             Rapid-PVST
STP Disabled                1     None                   None
STP MST Region Name         1     ""                     ""
STP MST Region Revision     1     0                      0
STP MST Region Instance to  1
  VLAN Mapping
```

```
STP Loopguard               1     Disabled              Disabled
STP Bridge Assurance        1     Enabled               Enabled
STP Port Type, Edge         1     Normal, Disabled,     Normal, Disabled,
BPDUFilter, Edge BPDUGuard        Disabled              Disabled
STP MST Simulate PVST       1     Enabled               Enabled
Allowed VLANs               -     1,624                 1
Local suspended VLANs       -     624                   -
switch#
```

vPC 自動リカバリのイネーブル化

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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 2	switch(config)# **vpc domain***domain-id*	既存の vPC ドメインに対して vpc-domain 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	switch(config-vpc-domain)# **auto-recovery reload-delay***delay*	自動リカバリ機能をイネーブルにし、リロード遅延時間を設定します。デフォルトではディセーブルになっています。

次に、vPC ドメイン 10 の自動リカバリ機能をイネーブルにし、240 秒の遅延期間を設定する例を示します。

```
switch(config)# vpc domain 10
switch(config-vpc-domain)# auto-recovery reload-delay 240
Warning:
 Enables restoring of vPCs in a peer-detached state after reload, will wait for 240 seconds
  (by default) to determine if peer is un-reachable
```

次に、vPC ドメイン 10 の自動リカバリ機能のステータスを表示する例を示します。

```
switch(config-vpc-domain)# show running-config vpc
!Command: show running-config vpc
!Time: Tue Dec  7 02:38:44 2010


version 5.0(3)U2(1)
feature vpc
vpc domain 10
  peer-keepalive destination 10.193.51.170
  auto-recovery
```

復元遅延時間の設定

ピアの隣接が形成され、VLAN インターフェイスがバックアップされるまで、vPC の再稼働を遅らせるように復元タイマーを設定できます。この機能により、vPC が再びトラフィックの受け渡

しをしはじめる前にルーティング テーブルが収束できなかった場合のパケットのドロップを回避できます。

はじめる前に

vPC 機能をイネーブルにしていることを確認します。

vPC ピア リンクの両端にあるそれぞれのスイッチで設定を行う必要があります。手順は次のとおりです。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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 2	switch(config)# **vpc domain***domain-id*	スイッチ上に vPC ドメインが存在しない場合はそれを作成し、vpc-domain 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	switch(config-vpc-domain)# **delay restore***time*	vPC が復元されるまでの遅延時間を設定します。 復元時間は、復元された vPC ピア デバイスが稼働するまで遅延時間（単位は秒）です。有効な範囲は 1 ～ 3600 です。デフォルトは 30 秒です。
ステップ 4	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次の例は、vPC リンクに対する復元遅延時間の設定方法を示したものです。

```
switch(config)# vpc domain 1
switch(config-vpc-domain)# delay restore 10
switch(config-vpc-domain)#
```

vPC ピア リンク障害発生時における VLAN インターフェイスのシャットダウン回避

vPC ピア リンクが失われると、vPC セカンダリ スイッチによりその vPC メンバ ポートおよびスイッチ仮想インターフェイス（SVI）インターフェイスが一時停止します。また、vPCセカンダリ スイッチのすべての VLAN に対して、レイヤ 3 転送はすべてディセーブルになります。ただし、特定の SVI インターフェイスを一時停止の対象から除外することができます。

はじめる前に

VLAN インターフェイスが設定済みであることを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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 2	switch(config)# **vpc domain***domain-id*	スイッチ上に vPC ドメインが存在しない場合はそれを作成し、vpc-domain 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	switch(config-vpc-domain))# **dual-active exclude interface-vlan***range*	vPC ピアリンクが失われた場合でもアップ状態を維持する必要がある VLAN インターフェイスを指定します。 range：シャットダウンしないようにする VLAN インターフェイスの範囲を指定します。指定できる範囲は 1 ～ 4094 です。

次の例は、vPC ピア リンクに障害が発生した場合でも vPC ピア スイッチの VLAN 10 に対してインターフェイスのアップ状態を維持する方法を示したものです。

```
switch# configure terminal
switch(config)# vpc domain 5
switch(config-vpc-domain)# dual-active exclude interface-vlan 10
switch(config-vpc-domain)#
```

VRF 名の設定

ping、ssh、telnet、radius などのスイッチ サービスは VRF 対応です。適切なルーティング テーブルを使用するためには、VRF 名を設定する必要があります。

VRF 名を指定することができます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **ping***ipaddress* **vrf** *vrf-name*	使用する Virtual Routing and Forwarding（VRF）名を指定します。VRF 名は、長さが最大 32 文字で、大文字と小文字は区別されます。

次に、vpc_keepalive という名前の VRF を指定する例を示します。

```
switch# ping 123.1.1.1 vrf vpc_keepalive
PING 123.1.1.1 (123.1.1.1): 56 data bytes
64 bytes from 123.1.1.1: icmp_seq=0 ttl=254 time=3.234 ms
```

```
64 bytes from 123.1.1.1: icmp_seq=1 ttl=254 time=4.931 ms
64 bytes from 123.1.1.1: icmp_seq=2 ttl=254 time=4.965 ms
64 bytes from 123.1.1.1: icmp_seq=3 ttl=254 time=4.971 ms
64 bytes from 123.1.1.1: icmp_seq=4 ttl=254 time=4.915 ms

--- 123.1.1.1 ping statistics ---
5 packets transmitted, 5 packets received, 0.00% packet loss
round-trip min/avg/max = 3.234/4.603/4.971 ms
```

他のポート チャネルの vPC への移行

はじめる前に

vPC 機能をイネーブルにしていることを確認します。

vPC ピア リンクの両端にあるそれぞれのスイッチで設定を行う必要があります。手順は次のとおりです。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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 2	switch(config)# **interface port-channel***channel-number*	ダウンストリーム スイッチに接続するために vPC に入れるポート チャネルを選択し、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。 （注） 通常のポート チャネル（物理的な vPC トポロジ）およびポート チャネル ホスト インターフェイス（ホスト インターフェイス vPC トポロジ）で vPC を設定できます。
ステップ 3	switch(config-if)# **vpc***number*	選択したポート チャネルを vPC に配置してダウンストリーム スイッチに接続するように設定します。範囲は 1 ～ 4096 です。 vPC ピア スイッチからダウンストリーム スイッチに接続されているポート チャネルに割り当てる vPC 番号は、両方の vPC スイッチで同じでなければなりません。
ステップ 4	switch# **show vpc brief**	（任意） 各 vPC に関する情報を表示します。
ステップ 5	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次の例は、ダウンストリームデバイスに接続されるポートチャネルを設定する方法を示します。

```
switch# configure terminal
switch(config)# interface port-channel 20
switch(config-if)# vpc 5
```

vPC ドメイン MAC アドレスの手動での設定

（注） システム アドレスの設定は、オプションの設定手順です。

はじめる前に

vPC 機能をイネーブルにしていることを確認します。

vPC ピア リンクの両側に両方のスイッチを設定する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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 2	switch(config)# **vpc domain***domain-id*	スイッチ上にある既存の vPC ドメインを選択するか、または新規の vPC ドメインを作成して、vpc-domain コンフィギュレーション モードを開始します。*domain-id* のデフォルト値はありません。指定できる値の範囲は 1 ～ 1000 です。
ステップ 3	switch(config-vpc-domain)# **system-mac***mac-address*	指定した vPC ドメインに割り当てる MAC アドレスを aaaa.bbbb.cccc の形式で入力します。
ステップ 4	switch# **show vpc role**	（任意） vPC システムの MAC アドレスを表示します。
ステップ 5	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次の例は、vPC ドメインの MAC アドレスを設定する方法を示したものです。

```
switch# configure terminal
switch(config)# vpc domain 5
switch(config-if)# system-mac 23fb.4ab5.4c4e
```

システム プライオリティの手動での設定

vPC ドメインを作成すると、vPC システム プライオリティが自動的に作成されます。ただし、vPC ドメインのシステム プライオリティは手動で設定することもできます。

はじめる前に

vPC 機能をイネーブルにしていることを確認します。

vPC ピア リンクの両側に両方のスイッチを設定する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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 2	switch(config)# **vpc domain***domain-id*	スイッチ上にある既存の vPC ドメインを選択するか、または新規の vPC ドメインを作成して、vpc-domain コンフィギュレーション モードを開始します。*domain-id* のデフォルト値はありません。指定できる値の範囲は 1 ～ 1000 です。
ステップ 3	switch(config-vpc-domain)# **system-priority***priority*	指定した vPC ドメインに割り当てるシステム プライオリティを入力します。指定できる値の範囲は、1 ～ 65535 です。デフォルト値は 32667 です。
ステップ 4	switch# **show vpc brief**	（任意） vPC ピア リンクに関する情報など、各 vPC の情報を表示します。
ステップ 5	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次の例は、vPC ピア リンクを設定する方法を示します。

```
switch# configure terminal
switch(config)# vpc domain 5
switch(config-if)# system-priority 4000
```

vPC ピア スイッチのロールの手動による設定

デフォルトの場合、Cisco NX-OS では、vPC ドメインおよび vPC ピア リンクの両側を設定した後、プライマリおよびセカンダリの vPC ピア スイッチが選択されます。ただし、vPC のプライマ

リ スイッチとして、特定の vPC ピア スイッチを選択することもできます。選択したら、プライマリ スイッチにする vPC ピア スイッチに、他の vPC ピア スイッチより小さいロール値を手動で設定します。

vPC はロールのプリエンプションをサポートしていません。プライマリ vPC ピア スイッチに障害が発生すると、セカンダリ vPC ピア スイッチが、vPC プライマリ デバイスの機能を引き継ぎます。ただし、以前のプライマリ vPC が再稼働しても、機能のロールは元に戻りません。

はじめる前に

vPC 機能をイネーブルにしていることを確認します。

vPC ピア リンクの両側に両方のスイッチを設定する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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 2	switch(config)# **vpc domain***domain-id*	スイッチ上にある既存の vPC ドメインを選択するか、または新規の vPC ドメインを作成して、vpc-domain コンフィギュレーション モードを開始します。*domain-id* のデフォルト値はありません。指定できる値の範囲は 1 ～ 1000 です。
ステップ 3	switch(config-vpc-domain)# **role priority***priority*	vPC システム プライオリティとして使用するロール プライオリティを指定します。指定できる値の範囲は、1 ～ 65535 です。デフォルト値は 32667 です。
ステップ 4	switch# **show vpc brief**	（任意） vPC ピア リンクに関する情報など、各 vPC の情報を表示します。
ステップ 5	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次の例は、vPC ピア リンクを設定する方法を示します。

```
switch# configure terminal
switch(config)# vpc domain 5
switch(config-if)# role priority 4000
```

第 10 章

Q-in-Q VLAN トンネルの設定

この章の内容は、次のとおりです。

Q-in-Q トンネルについて

Q-in-Q VLAN トンネルを使用することで、サービス プロバイダーは第 2 の 802.1Q タグをすでにタグ付けされたフレームに追加して、カスタマーに内部使用の VLAN をすべて提供しながら、インフラストラクチャ内で異なるカスタマーのトラフィックを分離することができます。

サービス プロバイダーのビジネス カスタマーには、多くの場合、サポートする VLAN ID および VLAN の数に固有の要件があります。同一サービスプロバイダー ネットワークのさまざまなカスタマーが必要とする VLAN 範囲は重複し、インフラストラクチャを通るカスタマーのトラフィックは混合してしまうことがあります。カスタマーごとに一意の VLAN ID 範囲を割り当てると、カスタマーの設定が制限され、802.1Q 仕様の 4096 の VLAN に関する上限を容易に超えてしまいます。

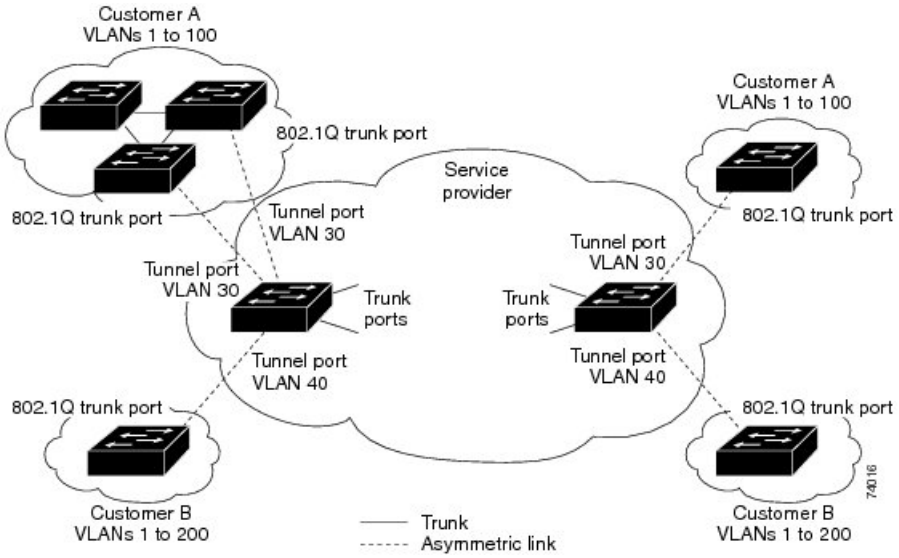
（注） Q-in-Q は、ポート チャネルでサポートされます。非対称リンクとしてポート チャネルを設定するには、ポート チャネル内のすべてのポートが同じトンネリング設定でなければなりません。

サービス プロバイダーは、802.1Q トンネリング機能を使用すると、単一の VLAN を使用して、複数の VLAN を含むカスタマーをサポートできます。同一の VLAN 上にあるように見えるときでも、サービス プロバイダー インフラストラクチャ内のカスタマーの VLAN ID を保護したり、異なるカスタマーの VLAN トラフィックを分離しておくことができます。IEEE 802.1Q トンネリングは、VLAN-in-VLAN 階層構造およびタグ付きパケットへのタギングによって、VLAN スペースを拡張します。802.1Q トンネリングをサポートするように設定されたポートは、トンネル ポートといいます。トンネリングを設定する場合、トンネリング専用の VLAN にトンネル ポートを割り当てます。カスタマーごとに個別の VLAN が必要ですが、その VLAN はカスタマーの VLAN をすべてサポートします。

適切な VLAN ID で通常どおりにタグ付けされたカスタマーのトラフィックは、カスタマー デバイスの 802.1Q トランク ポートからサービス プロバイダー側のエッジ スイッチのトンネル ポートに発信されます。カスタマー デバイスとエッジ スイッチの間のリンクは、一方の端が 802.1Q トランク ポート、反対側がトンネル ポートとして設定されているので、非対称リンクです。それぞれのカスタマーに固有のアクセス VLAN ID には、トンネル ポート インターフェイスを割り当てます。

（注） 選択的 Q-in-Q トンネリングはサポートされません。トンネル ポートに着信するすべてのフレームは、Q-in-Q タギングの対象となります。

図 *9*：*802.1Q-in-Q* トンネル ポート

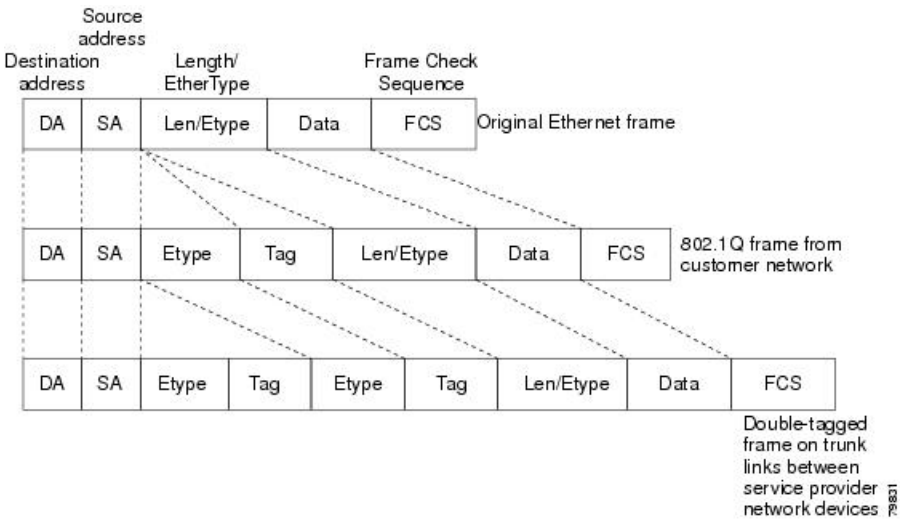


サービスプロバイダー エッジ スイッチのトンネル ポートに着信するパケット（適切な VLAN ID ですでに 802.1Q タグ付けされている）は、カスタマーに一意である VLAN ID を含む 802.1Q タグの別のレイヤでカプセル化されます。元々のカスタマーの 802.1Q タグは、カプセル化されたパケットの中に維持されます。したがって、サービスプロバイダー インフラストラクチャに着信するパケットは二重にタグ付けされます。

外部タグには、カスタマーの（サービス プロバイダーによって割り当てられた）アクセス VLAN ID が含まれます。（カスタマーによって割り当てられた）内部タグの VLAN ID は、受信トラフィックの VLAN です。この二重タギングは、タグ スタック構成 Double-Q または Q-in-Q と呼ばれます。

次の図に、タグなし、タグ付き、および二重タグ付きのイーサネット フレーム間の相違点を示します。

図 *10*：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



この方法で、外部タグの VLAN ID スペースは内部タグの VLAN ID スペースに依存しません。単一の外部 VLAN ID は、個々のカスタマーの全体の VLAN ID スペースを表すことができます。この方法により、カスタマーのレイヤ 2 ネットワークをサービス プロバイダー ネットワーク全体に拡張して、複数のサイトに仮想 LAN インフラストラクチャを作成することも可能になります。

（注） 階層型タギング、すなわちマルチレベルの dot1q タギング Q-in-Q はサポートされていません。

ネイティブ VLAN のリスク

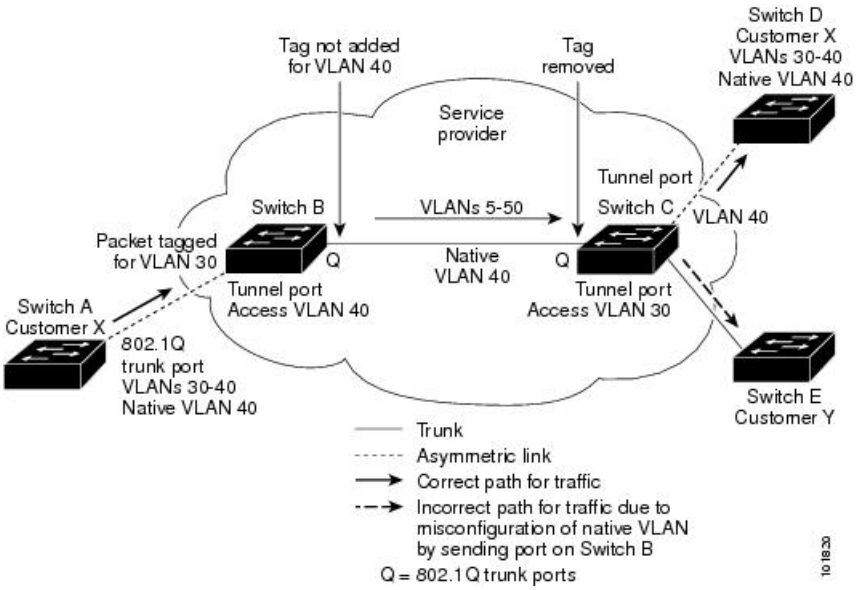
エッジ スイッチで 802.1Q トンネリングを設定する場合は、サービス プロバイダー ネットワークにパケットを送信するために、802.1Q トランク ポートを使用する必要があります。ただし、サービスプロバイダー ネットワークのコアを通過するパケットは、IEEE 802.1Q トランク、ISL トランク、または非トランキング リンクで伝送される場合があります。802.1Q トランクをこれらのコア

スイッチで使用する場合には、802.1Q トランクのネイティブ VLAN を、同じスイッチ上の dot1q トンネル ポートのどのネイティブ VLAN にも一致させないでください。ネイティブ VLAN 上のトラフィックが 802.1Q 送信トランク ポートでタグ付けされなくなるためです。

VLAN 40 は、サービス プロバイダー ネットワークの入力エッジ スイッチ（スイッチ B）において、カスタマー X からの 802.1Q トランク ポートのネイティブ VLAN として設定されています。カスタマー X のスイッチ A は、VLAN 30 のタグ付きパケットを、アクセス VLAN 40 に属する、サービスプロバイダー ネットワークのスイッチ B の入力トンネル ポートに送信します。トンネル ポートのアクセス VLAN（VLAN 40）は、エッジ スイッチのトランク ポートのネイティブ VLAN（VLAN 40）と同じなので、トンネル ポートから受信したタグ付きパケットに 802.1Q タグは追加されません。パケットには VLAN 30 タグだけが付いて、サービスプロバイダー ネットワークで出力エッジ スイッチ（スイッチ C）のトランク ポートに送信され、出力スイッチ トンネルによってカスタマー Y に間違えて送信されます。

次の図は、ネイティブ VLAN のリスクを示します。

図 *11*：ネイティブ *VLAN* のリスク



ネイティブ VLAN の問題は、次のようないくつかの方法で解決できます。

- 802.1Q トランクから出るすべてのパケット（ネイティブ VLAN を含む）が、**vlan dot1q tag native** コマンドを使用してタグ付けされるように、エッジ スイッチを設定します。すべての 802.1Q トランクでネイティブ VLAN パケットにタグを付けるようにスイッチを設定した場合、スイッチはタグなしパケットを受信しますが、タグ付きパケットだけを送信します。

（注） **vlan dot1q tag native** コマンドは、すべてのトランク ポート上のタギング動作に影響を与えるグローバル コマンドです。

- エッジ スイッチのトランク ポートのネイティブ VLAN ID が、カスタマー VLAN 範囲に属さないようにします。たとえばトランク ポートが VLAN100 ～ 200 のトラフィックを運ぶ場合は、この範囲以外の番号をネイティブ VLAN に割り当てます。

レイヤ2 プロトコルのトンネリングについて

サービスプロバイダー ネットワーク経由で接続される複数のサイトのカスタマーは、さまざまなレイヤ2プロトコルを実行して、すべてのリモート サイトおよびローカル サイトを含むようにトポロジを拡大する必要があります。スパニングツリー プロトコル（STP）が適切に稼働している必要があり、すべての VLAN で、ローカル サイトおよびサービスプロバイダー インフラストラクチャ経由のすべてのリモート サイトを含む、適切なスパニングツリーを構築する必要があります。Cisco Discovery Protocol（CDP）は、ローカルおよびリモート サイトから隣接するシスコ デバイスを検出することができる必要があり、VLAN トランキング プロトコル（VTP）は、カスタマー ネットワークのすべてのサイトを通して一貫した VLAN 設定を提供する必要があります。

プロトコル トンネリングがイネーブルになると、サービス プロバイダー インフラストラクチャの受信側にあるエッジ スイッチが、レイヤ2プロトコルを特別の MAC アドレスでカプセル化し、サービス プロバイダー ネットワークの端まで送信します。ネットワークのコア スイッチでは、このパケットが処理されずに通常のパケットとして転送されます。CDP、STP、または VTP のブリッジプロトコルデータ ユニット（BPDU）は、サービスプロバイダーインフラストラクチャを通過し、サービスプロバイダーネットワークの発信側にあるカスタマースイッチまで配信されます。同一パケットは同じ VLAN のすべてのカスタマー ポートで受信されます。

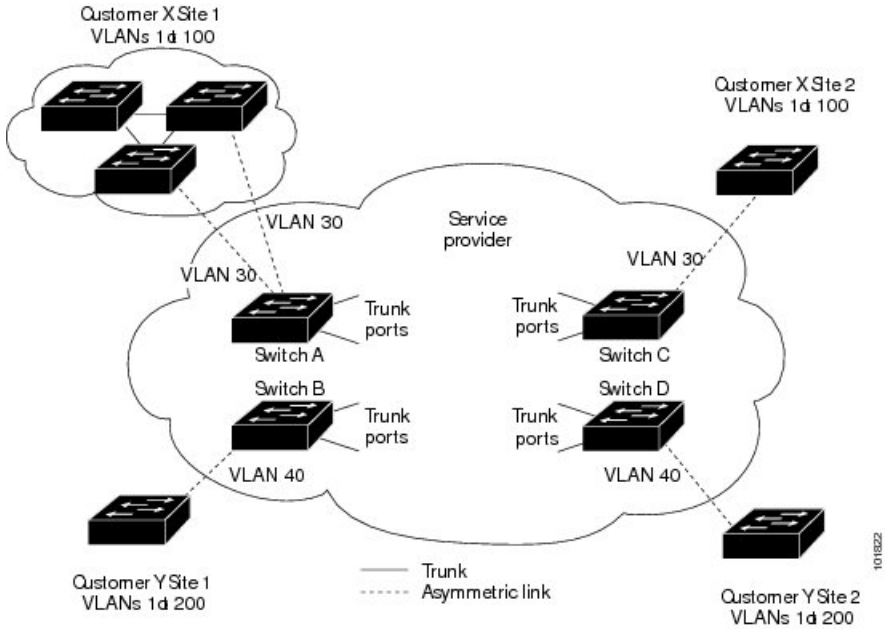
802.1Q トンネリング ポートでプロトコルのトンネリングをイネーブルにしていない場合、サービスプロバイダー ネットワークの受信側のリモート スイッチでは BPDU を受信せず、STP、CDP、802.1X、および VTP を適切に実行できません。プロトコルのトンネリングがイネーブルである場合、それぞれのカスタマー ネットワークのレイヤ2プロトコルは、サービスプロバイダー ネットワーク内で動作しているものから完全に区別されます。802.1Q トンネリングでサービスプロバイダーネットワークを通してトラフィックを送信する、さまざまなサイトのカスタマースイッチでは、カスタマー VLAN が完全に認識されます。

（注） レイヤ2プロトコルのトンネリングは、ソフトウェアで BPDU をトンネリングすることで動作します。スーパーバイザ モジュールが受信する多数の BPDU により CPU の負荷が大きくなります。この負荷は、BPDU としてマークされたパケットに関して設定されるコントロール プレーン ポリシング（CoPP）によって制御されます。

たとえば、以下の図で、カスタマー X には、サービス プロバイダー ネットワークを介して接続された同じ VLAN に 4 台のスイッチがあります。ネットワークが BPDU をトンネリングしない

と、ネットワークの遠端のスイッチは STP、CDP、802.1X、および VTP プロトコルを正しく実行できません。

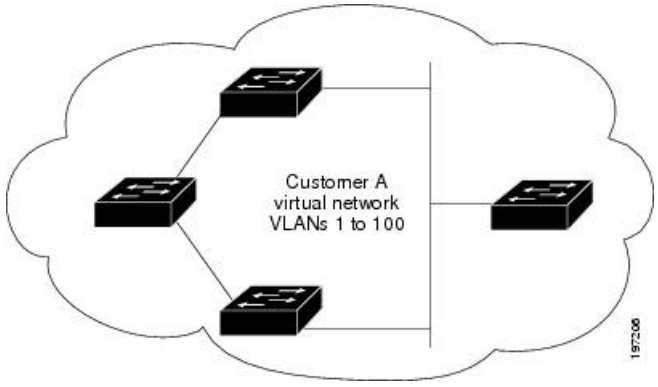
図 *12*：レイヤ *2* プロトコル トンネリング



前の例では、カスタマー X、サイト 1 のスイッチ上の VLAN で動作する STP は、カスタマー X、サイト 2 のスイッチに基づくコンバージェンス パラメータを考慮せずに、このサイトのスイッチのスパニング ツリーを構築します。

以下の図は、BPDU トンネリングがイネーブルになっていない場合の、カスタマーのネットワークでの結果トポロジを示します。

図 *13*：*BPDU* トンネリングを使用しない仮想ネットワーク トポロジ



Q-in-Q トンネルのライセンス要件

製品	ライセンス要件
Cisco NX-OS	802.1Q-in-Q VLAN トンネリングおよびL2プロトコルのトンネリングにライセンスは必要ありません。ライセンスパッケージに含まれていない機能はすべてCisco NX-OSシステムイメージにバンドルされており、追加費用は一切発生しません。NX-OSライセンス方式の詳細については、『*Cisco NX-OS Licensing Guide*』を参照してください。

Q-in-Q トンネリングの注意事項および制約事項

Q-in-Q トンネリングおよびレイヤ 2 トンネリングには、次の設定に関する注意事項と制約事項があります。

- サービスプロバイダー ネットワーク内のスイッチは、Q-in-Q タギングによる MTU サイズの増加に対応するように設定する必要があります。
- 選択的 Q-in-Q トンネリングはサポートされません。トンネル ポートに着信するすべてのフレームは、Q-in-Q タギングの対象となります。
- Q-in-Q タグ付きパケットの MAC アドレス ラーニングは、外部 VLAN（サービス プロバイダー VLAN）タグに基づいています。単一の MAC アドレスが複数の内部（カスタマー）VLAN で使用される配置においては、パケット転送の問題が発生する場合があります。
- レイヤ 3 以上のパラメータは、トンネル トラフィックでは識別できません（レイヤ 3 宛先や送信元アドレスなど）。トンネル型トラフィックはルーティングできません。
- MAC アドレスに基づくフレーム配布を使用する必要があります。
- プライベート VLAN をサポートするように設定されたポートに 802.1Q トンネリング機能を設定することはできません。プライベート VLAN は、これらの導入には必要ではありません。
- CDP は、必要に応じて、dot1Q トンネル ポートで明示的にディセーブルにする必要があります。
- トンネル VLAN の IGMP スヌーピングをディセーブルにする必要があります。
- ネイティブVLANでのタギングを維持し、タグなしトラフィックをドロップしてネイティブVLANの誤設定を防止するには、**vlan dot1Q tag native** コマンドを実行する必要があります。
- 802.1Q インターフェイスをエッジ ポートにするように手動で設定する必要があります。

- Dot1x トンネリングはサポートされていません。

Q-in-Q トンネルおよびレイヤ 2 プロトコルのトンネリングの設定

802.1Q トンネル ポートの作成

switchport mode コマンドを使用して dot1q-tunnel ポートを作成します。

（注） **spanning-tree port type edge** コマンドを使用して、エッジ ポートに 802.1Q トンネル ポートを設定する必要があります。**switchport access vlan vlan-id** コマンドを入力すると、ポートの VLAN メンバーシップが変更されます。

dot1q-tunnel ポートに割り当てられたアクセス VLAN の IGMP スヌーピングをディセーブルにして、マルチキャスト パケットが Q-in-Q トンネルを通過できるようにする必要があります。

はじめる前に

はじめに、スイッチ ポートとしてインターフェイスを設定する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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 2	switch(config)# **interface ethernet** *slot*/*port*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# **switchport**	インターフェイスをレイヤ 2 スイッチング ポートとして設定します。
ステップ 4	switch(config-if)# [**no**] **switchport mode dot1q-tunnel**	ポートに 802.1Q トンネルを作成します。インターフェイス モードを変更すると、ポートはダウンし、再初期化（ポート フラップ）されます。トンネル インターフェイスでは BPDU フィルタリングがイネーブルになり、CDP がディセーブルになります。
ステップ 5	switch(config-if)# **exit**	インターフェイス コンフィギュレーション モードを終了します。

	コマンドまたはアクション	目的
ステップ 6	switch(config)# **show dot1q-tunnel** [**interface** *if-range*]	（任意） dot1q-tunnel モードにあるすべてのポートを表示します。オプションで、表示するインターフェイスまたはインターフェイスの範囲を指定できます。
ステップ 7	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

次に、802.1Q トンネル ポートを作成する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 7/1
switch(config-if)# switchport
switch(config-if)# switchport mode dot1q-tunnel
switch(config-if)# exit
switch(config)# exit
switch# show dot1q-tunnel
```

レイヤ 2 プロトコル トンネルのイネーブル化

802.1Q トンネル ポートでプロトコルのトンネリングをイネーブルにできます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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 2	switch(config)# **interface ethernet** *slot*/*port*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switch(config)# **switchport**	インターフェイスをレイヤ 2 スイッチング ポートとして設定します。
ステップ 4	switch(config-if)# **switchport mode dot1q-tunnel**	ポートに 802.1Q トンネルを作成します。
ステップ 5	switch(config-if)# [**no**] **l2protocol tunnel** [**cdp** | **stp** | **vtp**]	レイヤ 2 プロトコルのトンネリングをイネーブルにします。必要に応じて、CDP、STP、または VTP トンネリングをイネーブルにできます。

	コマンドまたはアクション	目的
ステップ 6	switch(config-if)# **exit**	インターフェイス コンフィギュレーション モードを終了します。
ステップ 7	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

次に、802.1Q トンネル ポートでプロトコルのトンネリングをイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 7/1
switch(config-if)# switchport
switch(config-if)# switchport mode dot1q-tunnel
switch(config-if)# l2protocol tunnel stp
switch(config-if)# exit
switch(config)# exit
```

レイヤ 2 プロトコル トンネル ポートのしきい値の設定

レイヤ 2 プロトコルのトンネリング ポートに対するポート ドロップおよびシャットダウン値を指定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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 2	switch(config)# **interface ethernet** *slot*/*port*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# **switchport**	インターフェイスをレイヤ 2 スイッチング ポートとして設定します。
ステップ 4	switch(config-if)# **switchport mode dot1q-tunnel**	ポートに 802.1Q トンネルを作成します。
ステップ 5	switch(config-if)# [**no**] **l2protocol tunnel drop-threshold** [**cdp** | **stp** | **vtp**]	廃棄される前にインターフェイスで処理できる最大パケット数を指定します。必要に応じて、CDP、STP、または VTP を指定できます。パケットの有効な値は 1 ～ 4096 です。 このコマンドの **no** 形式は、しきい値を 0 にリセットし、ドロップしきい値をディセーブルにします。

	コマンドまたはアクション	目的
ステップ 6	switch(config-if)# [**no**] **l2protocol tunnel shutdown-threshold** [**cdp** | **stp** | **vtp**]	インターフェイスで処理できる最大パケット数を指定します。パケット数が超過すると、ポートは error-disabled ステートになります。オプションで、Cisco Discovery Protocol（CDP）、スパニングツリープロトコル（STP）、または VLAN トランキングプロトコル（VTP）を指定できます。パケットの有効な値は 1 ～ 4096 です。
ステップ 7	switch(config-if)# **exit**	インターフェイス コンフィギュレーション モードを終了します。
ステップ 8	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

次に、レイヤ 2 プロトコル トンネル ポートのしきい値を設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 7/1
switch(config-if)# switchport
switch(config-if)# switchport mode dot1q-tunnel
switch(config)# l2protocol tunnel drop-threshold 3000
switch(config)# l2protocol tunnel shutdown-threshold 3000
switch(config)# exit
switch# copy running-config startup-config
```

Q-in-Q 設定の確認

Q-in-Q トンネルおよびレイヤ 2 プロトコルのトンネリングの設定情報を確認するには、次のコマンドを使用します。

コマンド	目的
clear l2protocol tunnel counters [**interface** *if-range*]	すべての統計情報カウンタをクリアします。インターフェイスが指定されていない場合、すべてのインターフェイスのレイヤ2プロトコル トンネル統計情報がクリアされます。
show dot1q-tunnel [**interface** *if-range*]	dot1q トンネル モードのインターフェイス範囲またはすべてのインターフェイスが表示されます。

コマンド	目的
show l2protocol tunnel [**interface** *if-range* | **vlan** *vlan-id*]	一定範囲のインターフェイスや、特定のVLANの一部であるすべてのdot1q-tunnelインターフェイスまたはすべてのインターフェイスの、レイヤ 2 プロトコル トンネル情報を表示します。
show l2protocol tunnel summary	レイヤ2プロトコルトンネルが設定されているすべてのポートのサマリーを表示します。
show running-config l2pt	現在のレイヤ2プロトコルトンネルの実行コンフィギュレーションを表示します。

Q-in-Q およびレイヤ 2 プロトコルのトンネリングの設定例

次に、イーサネット 7/1 に着信するトラフィックに対し Q-in-Q を処理するよう設定されたサービス プロバイダーのスイッチを示します。レイヤ 2 プロトコル トンネルが STP BPDU に対してイネーブルにされます。このカスタマーは VLAN 10（外部 VLAN タグ）に割り当てられます。

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# vlan 10
switch(config-vlan)# no shutdown
switch(config-vlan)# vlan configuration 8
switch(config-vlan-config)# no ip igmp snooping
switch(config-vlan-config)# exit
switch(config-vlan)# exit
switch(config)# interface ethernet 7/1
switch(config-if)# switchport
switch(config-if)# switchport mode dot1q-tunnel
switch(config-if)# switchport access vlan 10
switch(config-if)# spanning-tree port type edge
switch(config-if)# l2protocol tunnel stp
switch(config-if)# no shutdown
switch(config-if)# exit
switch(config)# exit
switch#
```

Q-in-Q トンネルおよびレイヤ 2 プロトコルのトンネリングの機能履歴

表 *9* : *Q-in-Q* トンネルおよびレイヤ *2* プロトコルのトンネリングの機能履歴

機能名	リリース	機能情報
Q-in-Q VLAN トンネル	6.0(2)U1(1)	この機能が導入されました。

機能名	リリース	機能情報
L2 プロトコルのトンネリング	6.0(2)U1(1)	この機能が導入されました。

索 引

数字

A

D

E

F

G

H

I

L

M

N

P

Q

R

S

U

V

い

さ

た

ち

て

と

は

ふ

ほ

ま

も

ゆ

ら

る

れ

ろ