



## **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/](http://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。

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザー側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

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

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <http://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2015 Cisco Systems, Inc. All rights reserved.



## 目次

### 新機能および変更された機能に関する情報 1

このリリースの新規および変更情報 1

### レイヤ2 インターフェイスの設定 5

イーサネット インターフェイスの概要 5

インターフェイス コマンド 5

UDLD パラメータ 6

UDLD のデフォルト設定 7

UDLD アグレッシブ モードと非アグレッシブ モード 7

インターフェイス速度 8

40 ギガビット イーサネット インターフェイスの速度 8

ポート モード 9

SVI 自動ステート 11

Cisco Discovery Protocol 11

CDP のデフォルト設定 12

error-disabled ステート 12

デフォルト インターフェイス 13

デバウンス タイマー パラメータ 13

MTU 設定 14

カウンタの値 14

ダウンリンク遅延 16

物理イーサネットのデフォルト設定 16

イーサネット インターフェイスの設定 16

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

UDLD モードの設定 17

リンク ステート整合性チェッカのトリガー 18

インターフェイスのポート モードの変更 19

インターフェイス速度の設定 21

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
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	23
QSFP ポートと SFP+ ポートの切り替え	23
リンク ネゴシエーションのディセーブル化	25
SVI 自動ステートのディセーブル化	26
デフォルト インターフェイスの設定	27
CDP の特性の設定	28
CDP のイネーブル化/ディセーブル化	29
errdisable ステート検出のイネーブル化	30
errdisable ステート回復のイネーブル化	31
errdisable ステート回復間隔の設定	32
error-disabled リカバリのディセーブル化	32
デバウンス タイマーの設定	33
説明パラメータの設定	34
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	35
ダウンリンク遅延の設定	35
インターフェイス情報の表示	36
入力パケット廃棄情報の表示	38
レイヤ 2 インターフェイスの MIB	40
<b>レイヤ 3 インターフェイスの設定</b>	<b>41</b>
レイヤ 3 インターフェイスについて	42
ルーテッド インターフェイス	42
サブインターフェイス	43
VLAN インターフェイス	43
ループバック インターフェイス	44
トンネル インターフェイス	45
レイヤ 3 インターフェイスのライセンス要件	45
レイヤ 3 インターフェイスの注意事項および制約事項	45
レイヤ 3 インターフェイスのデフォルト設定	45
SVI 自動ステートのディセーブル化	45
DHCP クライアント検出	46
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	46

MAC 組み込み IPv6 アドレス	47
レイヤ 3 インターフェイスの設定	47
ルーテッド インターフェイスの設定	47
サブインターフェイスの設定	48
インターフェイスでの帯域幅の設定	49
VLAN インターフェイスの設定	51
ループバック インターフェイスの設定	51
VRF へのインターフェイスの割り当て	52
インターフェイス MAC アドレスの設定	53
MAC 組み込み IPv6 アドレスの設定	55
SVI 自動ステートのディセーブル化の設定	57
インターフェイスでの DHCP クライアントの設定	58
レイヤ 3 インターフェイス設定の確認	58
レイヤ 3 インターフェイス整合性チェッカのトリガー	60
レイヤ 3 インターフェイスのモニタリング	61
レイヤ 3 インターフェイスの設定例	62
レイヤ 3 インターフェイスの関連資料	63
レイヤ 3 インターフェイスの MIB	64
レイヤ 3 インターフェイスの標準	64
レイヤ 3 インターフェイスの機能履歴	64
ポート チャネルの設定	65
ポート チャネルについて	65
ポート チャネルの概要	66
互換性要件	67
ポート チャネルを使ったロード バランシング	68
復元力のあるハッシュ	70
NVGRE トラフィックのハッシュ	71
対称ハッシュ	71
LACP の概要	72
LACP の概要	72
LACP ID パラメータ	73
チャンネル モード	74

LACP マーカー レスポンド	75
LACP がイネーブルのポートチャンネルとスタティック ポートチャンネルの相違点	75
LACP ポート チャンネルの MinLink	76
ポート チャンネルの設定	76
ポート チャンネルの作成	76
ポート チャンネルへのポートの追加	77
ポート チャンネルを使ったロード バランシングの設定	78
LACP のイネーブル化	80
ポートに対するチャンネル モードの設定	80
LACP ポート チャンネルの MinLink の設定	82
LACP 高速タイマー レートの設定	82
LACP のシステム プライオリティおよびシステム ID の設定	83
LACP ポート プライオリティの設定	84
ポート チャンネル設定の確認	85
ポート チャンネル メンバシップ整合性チェックのトリガー	86
ロードバランシング発信ポート ID の確認	87
ポート チャンネルの機能履歴	87
<b>IP トンネルの設定</b>	<b>89</b>
IP トンネルについて	89
GRE トンネル	90
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	90
マルチポイント IP-in-IP トンネルのカプセル化解除	90
IP トンネルのライセンス要件	91
IP トンネルの前提条件	91
IP トンネルの注意事項および制約事項	91
IP トンネリングのデフォルト設定	93
IP トンネルの設定	93
トンネリングのイネーブル化	93
トンネル インターフェイスの作成	94
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	96
GRE トンネルの設定	97

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	99
IP トンネル設定の確認	100
IP トンネリングの設定例	101
IP トンネルの関連資料	101
IP トンネルの標準	101
IP トンネル設定の機能履歴	101
<b>VXLAN の設定</b>	<b>103</b>
概要	103
VXLAN の概要	103
VXLAN のカプセル化およびパケット形式	104
VXLAN トンネル エンド ポイント	105
VXLAN のパケット転送フロー	105
Cisco Nexus 3100 シリーズ スイッチでの VXLAN の導入	105
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	106
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	106
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	107
VXLAN による ECMP および LACP ロードシェアリング	107
VXLAN の注意事項と制約事項	108
VXLAN 展開の考慮事項	109
VXLAN 導入に関する vPC の注意事項と制約事項	109
VXLAN トラフィック転送の設定	112
PIM 機能のイネーブル化と設定	112
ランデブー ポイントの設定	113
VXLAN のイネーブル化	114
VLAN から VXLAN VNI へのマッピング	115
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	115
VXLAN 宛先 UDP ポートの作成	117
NVE インターフェイスの作成および設定	117
VNI の複製の設定	118
マルチキャスト複製の設定	118
入力複製の設定	119

VXLAN 設定の確認	120
仮想ポート チャネルの設定	123
vPC について	123
vPC の概要	123
用語	124
vPC の用語	124
vPC ドメイン	125
ピアキーブアライブ リンクとメッセージ	126
vPC ピア リンクの互換パラメータ	126
同じでなければならない設定パラメータ	127
同じにすべき設定パラメータ	129
VLAN ごとの整合性検査	130
vPC 自動リカバリ	130
vPC ピア リンク	130
vPC ピア リンクの概要	130
vPC 番号	132
その他の機能との vPC の相互作用	132
vPC と LACP	132
vPC ピア リンクと STP	132
CFSoSE	133
VRF に関する注意事項と制約事項	134
vPC 設定の確認	135
グレースフル タイプ 1 検査ステータスの表示	136
グローバル タイプ 1 不整合の表示	136
インターフェイス別タイプ 1 不整合の表示	137
VLAN ごとの整合性ステータスの表示	138
vPC のデフォルト設定	140
vPC の設定	141
vPC のイネーブル化	141
vPC のディセーブル化	142
vPC ドメインの作成	142
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	143



vPC ピア リンクの作成	146
設定の互換性の検査	147
vPC 自動リカバリのイネーブル化	148
復元遅延時間の設定	148
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	149
VRF 名の設定	150
他のポート チャネルの vPC への移行	151
vPC ドメイン MAC アドレスの手動での設定	152
システム プライオリティの手動での設定	153
vPC ピア スイッチのロールの手動による設定	153
<b>Q-in-Q VLAN トンネルの設定</b>	<b>155</b>
Q-in-Q トンネルについて	155
ネイティブ VLAN のリスク	157
レイヤ 2 プロトコルのトンネリングについて	159
Q-in-Q トンネルのライセンス要件	161
Q-in-Q トンネリングの注意事項および制約事項	161
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	162
802.1Q トンネル ポートの作成	162
レイヤ 2 プロトコル トンネルのイネーブル化	163
レイヤ 2 プロトコル トンネル ポートのしきい値の設定	164
Q-in-Q 設定の確認	165
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	166
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	166





## 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, 1 ページ](#)

## 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
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)	<a href="#">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)</a>
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)	<a href="#">VXLAN 導入に関する vPC の注意事項と制約事項, (109 ページ)</a>
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)	<a href="#">QSFP ポートと SFP+ ポートの切り替え, (23 ページ)</a>

機能	説明	追加または変更されたリリース	参照先
QSFP ポートでのブレイクアウトの設定に関する <code>running-config</code> の出力の更新	<code>speed 10000</code> を使用して QSFP ポートでブレイクアウトを設定すると、 <code>running-config</code> の出力に <b>interface breakout module module number port port range map 10g-4x</b> 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)
CLI コマンドの <code>sh vpc brief</code> の出力の更新	CLI コマンドの <code>sh vpc brief</code> の出力に、 <code>Delay-restore status</code> と <code>Delay-restore SVI status</code> 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、 (134 ページ) VLAN ごとの整合性ステータスの表示、 (138 ページ) グレースフル タイプ 1 検査ステータスの表示、 (136 ページ) インターフェイス別タイプ 1 不整合の表示、 (137 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 <code>MinLink</code> の設定、 (82 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)

機能	説明	追加または変更されたリリース	参照先
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)	<a href="#">レイヤ 3 インターフェイスの注意事項および制約事項、(45 ページ)</a>
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)	<a href="#">LACP 高速タイマーレートの設定、(82 ページ)</a>
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)	<a href="#">VXLAN の注意事項と制約事項、(108 ページ)</a>
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)	<a href="#">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)</a>





## 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, 5 ページ](#)
- [物理イーサネットのデフォルト設定, 16 ページ](#)
- [イーサネット インターフェイスの設定, 16 ページ](#)
- [インターフェイス情報の表示, 36 ページ](#)
- [入力パケット廃棄情報の表示, 38 ページ](#)
- [レイヤ 2 インターフェイスの MIB, 40 ページ](#)

## 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 インターフェイスでは、Fibre Channel over Ethernet (FCoE) もサポートされます。FCoE により、イーサネット トラフィックとファイバ チャネル トラフィックの両方を物理イーサネット リンクで伝送できるようになります。

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)# interface ethernet [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、これらの光ファイバ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。

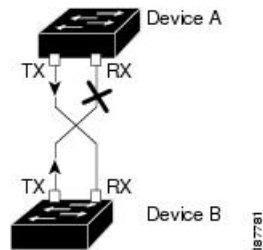
Cisco Nexus デバイスは、UDLD がイネーブルになっている LAN ポート上のネイバー デバイスに定期的に UDLD フレームを送信します。一定の時間内にフレームがエコーバックされてきて、特定の確認応答 (echo) が見つからなければ、そのリンクは単一方向のフラグを立てられ、その LAN ポートはシャットダウンされます。UDLD プロトコルにより単方向リンクが正しく識別されその



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。

スパンニングツリー 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、（デフォルトのスパンニングツリー 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せん。

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。

- リンク的一方にポート スタックが生じる（送受信どちらも）
- リンク的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。

## インターフェイス速度

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。ブレイクアウト 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。

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	<p>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。</p> <ul style="list-style-type: none"> <li>• <b>32x40G</b> : これはオーバーサブスクリプ ポートモードです。32 個のポートはすべて、オーバーサブスクリプされており、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 <b>speed 10000</b> 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。</li> <li>• <b>26x40G</b> : これはオーバーサブスクリプ 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リプされていません (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リプされています。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。</li> <li>• <b>24x40G</b> : これは、非オーバーサブスクリプ (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。</li> </ul> <p>Fixed32x40G ポートモードはブレイクアウトをサポートしません。</p>
Cisco Nexus 3172PQ	6 個の QSFP ポートおよび 48 個の SFP+ ポート	<p>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。</p> <ul style="list-style-type: none"> <li>• <b>48x10G+breakout6x40G</b></li> </ul> <p>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。</p> <ul style="list-style-type: none"> <li>• <b>48x10G+6x40G</b></li> <li>• <b>72x10G</b></li> </ul>

## 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。

ポートデバウンス時間は、リンクがダウンしたことをスーパーバイザに通知するためにインターフェイスが待機する時間です。この時間、インターフェイスはリンクがアップ状態に戻ったかどうかを確認するために待機します。待機時間は、トラフィックが停止している時間です。

デバウンス タイマーは各インターフェイスに対してイネーブルにでき、ミリ秒単位で遅延時間を指定できます。



注意

ポートデバウンスタイマーをイネーブルにすると、リンクアップ検出とリンクダウン検出に遅延が発生するため、デバウンス期間中にトラフィックが一部損失します。トラフィックが損失することにより、一部のプロトコルのコンバージェンスおよび再コンバージェンスに影響を及ぼす場合があります。

## 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、ファイバチャネルインターフェイスの受信データフィールドサイズは 2112 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	トラフィック
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	ドロップされる。
L2 ポート : ネットワーク QoS 設定にジャンボ MTU 9216 あり	6400	Jumbo	転送される。
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	ドロップされる。
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	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	トラフィック
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	ドロップされる。
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	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	ドロップされる。
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	ドロップされる。



(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)
Encapsulation	ARPA
MTU <sup>1</sup>	1500 バイト
Port Mode	アクセス
Speed	オート (10000)

<sup>1</sup> 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	<code>switch# configure terminal</code>	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	<code>switch(config)# feature udld</code>	デバイスのUDLDをイネーブルにします。
ステップ 3	<code>switch(config)# no feature udld</code>	デバイスのUDLDをディセーブルにします。
ステップ 4	<code>switch(config)# show udld global</code>	デバイスのUDLDステータスを表示します。
ステップ 5	<code>switch(config)# interfacetypeslot/port</code>	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	<code>switch(config-if)# udld {enable   disable   aggressive}</code>	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	<code>switch(config-if)# show udldinterface</code>	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# <b>show consistency-checker link-state moduleslot</b>	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# <b>configure terminal</b>	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)# <b>copy running-config bootflash: my-config.cfg</b>	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)# <b>write erase</b>	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)# <b>reload</b>	Cisco NX-OS ソフトウェアをリロードします。
ステップ 5	switch(config)# [ <b>no</b> ] <b>hardware profile portmode portmode</b>	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)# <b>hardware profile portmode portmode 2-tuple</b>	(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)# <b>copy running-config startup-config</b>	(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)# <b>reload</b>	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
```

次に、QSFP+ ポートのポートモードを 48x10g+4x40g 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+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
```

次に、QSFP+ ポートのポートモードを 48x10g+4x40g に変更し、その変更を確認する例を示します。

```
switch# configure terminal
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)# 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$0OV4MdOM$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#
```

次に、QSFP+ ポートのデフォルトのポートモードに戻す例を示します。

```
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 ethernetslot/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# <b>configure terminal</b>	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)# <b>interfacetypeslot/port</b>	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)# <b>speedspeed</b>	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。 <i>speed</i> 引数には次のいずれかを設定できます。 <ul style="list-style-type: none"> <li>• 10 Mbps</li> <li>• 100 Mbps</li> <li>• 1 Gbps</li> <li>• 10 Gbps</li> <li>• automatic</li> </ul>

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# <b>configure terminal</b>	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)# <b>interfacetypeslot/port-range</b>	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)# <b>speed 10000</b>	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) <b>speed 10000</b> 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 <b>interface breakout module &lt;module number&gt; port &lt;port range&gt; map 10g-4x</b> 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# <b>configure terminal</b>	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)# <b>interfacetypeslot/port</b>	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)# <b>speed 40000</b>	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# <b>configure terminal</b>	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)# <b>[no] hardware profile front portmode qsf   sfp-plus</b>	<p>指定されたポート モードをアクティブにします。</p> <ul style="list-style-type: none"> <li>• <b>qsfp</b> : 前面パネルの QSFP ポートがアクティブです。</li> <li>• <b>sfp-plus</b> : 前面パネルの SFP+ ポート 1 ~ 4 がアクティブです。</li> </ul> <p>このコマンドの <b>no</b> 形式を使用すると、QSFP ポートがアクティブになります。</p> <p>(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。</p>
ステップ 3	switch(config)# <b>interface breakout module module number port port range map 10g-4x</b>	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、 <b>hardware profile front portmode</b> 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)# <b>copy running-config startup-config</b>	(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 transceiver
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# <b>configure terminal</b>	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)# <b>interface ethernet slot/port</b>	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)# <b>no negotiate auto</b>	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)# <b>negotiate auto</b>	(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イネーブルまたはディセーブルにすると、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# <b>configure terminal</b>	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)# <b>feature interface-vlan</b>	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)# <b>system default interface-vlan [no] autostate</b>	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)# <b>interface vlan interface-vlan-number</b>	(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)# <b>[no] autostate</b>	(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)# <b>show interface-vlan interface-vlan</b>	(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)# <b>copy running-config startup-config</b>	(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イネーブル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.0040.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# <b>configure terminal</b>	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)# <b>default interfacetypeinterface number</b>	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。 <ul style="list-style-type: none"> <li>• <b>ethernet</b></li> <li>• <b>loopback</b></li> </ul>

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> <li>• <b>mgmt</b></li> <li>• <b>port-channel</b></li> <li>• <b>vlan</b></li> </ul>
ステップ 3	switch(config)# <b>exit</b>	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# <b>configure terminal</b>	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)# [ <b>no</b> ] <b>cdp advertise {v1   v2 }</b>	<p>(任意)</p> <p>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。</p> <p>デフォルト設定に戻すには、このコマンドの<b>no</b>形式を使用します。</p>
ステップ 3	switch(config)# [ <b>no</b> ] <b>cdp format device-id {mac-address   serial-number   system-name}</b>	<p>(任意)</p> <p>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。</p> <p>デフォルト設定に戻すには、このコマンドの<b>no</b>形式を使用します。</p>

	コマンドまたはアクション	目的
ステップ 4	switch(config)# [no] <b>cdp holdtime</b> 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 <b>no</b> 形式を使用します。
ステップ 5	switch(config)# [no] <b>cdp timer</b> 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 <b>no</b> 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# <b>configure terminal</b>	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)# <b>interfacetype</b> slot/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)# <b>cdp enable</b>	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)# <b>no cdp enable</b>	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# <b>configure terminal</b>	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)# <b>errdisable detect cause {all   link-flap   loopback}</b>	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)# <b>shutdown</b>	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)# <b>no shutdown</b>	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)# <b>show interface status err-disabled</b>	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)# <b>copy running-config startup-config</b>	(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# <b>configure terminal</b>	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)# <b>errdisable recovery cause</b> {all   uddl   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)# <b>show interface status err-disabled</b>	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)# <b>copy running-config startup-config</b>	(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# <b>configure terminal</b>	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)# <b>errdisable recovery interval</b> <i>interval</i>	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)# <b>show interface status err-disabled</b>	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)# <b>copy running-config startup-config</b>	(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ディセーブルにできます。

## 手順

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configure terminal</b>	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)# <b>no errdisable recovery cause {all   udld   bpduguard   link-flap   failed-port-state   pause-rate-limit   loopback}</b>	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)# <b>show interface status err-disabled</b>	(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)# <b>copy running-config startup-config</b>	(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# <b>configure terminal</b>	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)# <b>interfacetypeslot/port</b>	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)# <b>link debounce timemilliseconds</b>	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# <b>configure terminal</b>	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)# <b>interfacetypeslot/port</b>	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)# <b>description test</b>	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# <b>configure terminal</b>	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)# <b>interfacetypeslot/port</b>	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)# <b>shutdown</b>	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)# <b>no shutdown</b>	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# <b>configure terminal</b>	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)# <b>downlink delayenable</b>   <b>disable [timeouttime-out]</b>	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# <b>show interfacetypeslot/port</b>	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# <b>show interfacetypeslot/portcapabilities</b>	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# <b>show interfacetypeslot/porttransceiver</b>	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# <b>show interface brief</b>	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# <b>show interface flowcontrol</b>	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。
<b>show port--profile</b>	ポート プロファイルに関する情報を表示します。

**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。



(注) 上記の例のとおり、CDP アドバタイズメントのデバイス ID フィールドには、デフォルトでホスト名とシリアル番号が表示されます。

```
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

```

## 入力パケット廃棄情報の表示

Cisco NX-OS Release 5.0(3)U2(1) 以降では、特定のインターフェイスで入力廃棄が発生する原因となった具体的な状況について、詳細な情報を取得することができます。 **show hardware internal interface indiscard-stats front-port x** コマンドを使用すると、ポート eth1/x で入力廃棄が発生する原因となった可能性がある状況を特定することができます。スイッチの出力には、IPv4、STP、および入力ポリシーに関する廃棄数のほか、ACL に基づく廃棄数、汎用受信ドロップ数、VLAN 関連の廃棄数が表示されます。

次の例は、入力廃棄が発生する原因となった可能性がある状況を特定する方法を示したものです。

```
switch# show hardware internal interface indiscard-stats front-port 1
```

```
-----+-----+-----+
| Counter Description | Count |
+-----+-----+-----+
| IPv4 Discards      | 0     |
| STP Discards       | 0     |
| Policy Discards    | 100   |
| ACL Drops          | 0     |
| Receive Drops      | 0     |
| Vlan Discards      | 33    |
+-----+-----+-----+

```

カウンタの情報:



- **IPv4 Discards** : IPv4 Discards は IP レイヤでのエラー (IP チェックサム エラーなど) を表します。
- **STP Discards** : STP Discards は、受信インターフェイス STP の状態が、受信したパケットを転送していない場合に増分されます。
- **Policy Discards** : Policy Discards は、インターフェイス上の入力ポリシーのために廃棄が発生した場合に増分されます。
- **ACL Drops** : ACL Drops は、着信パケットがドロップ動作を含む ACL エントリに一致していることを示します。
- **Receive Drops** : このドロップの増分は、入力パケットの出力ポートが決定されていない状態を表します。Receive Drops は、IPv4、STP、およびポリシー廃棄を含むさまざまな理由によって発生します。このドロップカウンタは、上のいずれかのカウンタとともに、または個別に増分します。
- **VLAN Discard** : VLAN Discard は VLAN ベースの廃棄を示します。たとえば、VLAN のメンバではないポートに入力される VLAN タグ付きパケットなどがあります。

次に、すべての入力廃棄カウンタをクリアする例を示します。

```
switch# show hardware internal interface indiscard-stats front-port 1 clear
```

Counter	Description	Count	Last Increment	Last Increment Time
Discard Stats have been reset				

## 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。
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。 <ul style="list-style-type: none"> <li>• ifMauType (読み取り専用) GET</li> <li>• ifMauAutoNegSupported (読み取り専用) GET</li> <li>• ifMauTypeListBits (読み取り専用) GET</li> <li>• ifMauDefaultType (読み取りと書き込み) GET-SET</li> <li>• ifMauAutoNegAdminStatus (読み取りと書き込み) GET-SET</li> <li>• ifMauAutoNegCapabilityBits (読み取り専用) GET</li> <li>• ifMauAutoNegAdvertisedBits (読み取りと書き込み) GET-SET</li> </ul>	



## 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, 42 ページ](#)
- [レイヤ 3 インターフェイスのライセンス要件, 45 ページ](#)
- [レイヤ 3 インターフェイスの注意事項および制約事項, 45 ページ](#)
- [レイヤ 3 インターフェイスのデフォルト設定, 45 ページ](#)
- [SVI 自動ステートのディセーブル化, 45 ページ](#)
- [DHCP クライアント検出, 46 ページ](#)
- [MAC 組み込み IPv6 アドレス, 47 ページ](#)
- [レイヤ 3 インターフェイスの設定, 47 ページ](#)
- [レイヤ 3 インターフェイス設定の確認, 58 ページ](#)
- [レイヤ 3 インターフェイス整合性チェッカのトリガー, 60 ページ](#)
- [レイヤ 3 インターフェイスのモニタリング, 61 ページ](#)
- [レイヤ 3 インターフェイスの設定例, 62 ページ](#)
- [レイヤ 3 インターフェイスの関連資料, 63 ページ](#)
- [レイヤ 3 インターフェイスの MIB, 64 ページ](#)
- [レイヤ 3 インターフェイスの標準, 64 ページ](#)
- [レイヤ 3 インターフェイスの機能履歴, 64 ページ](#)

## 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、スパン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。

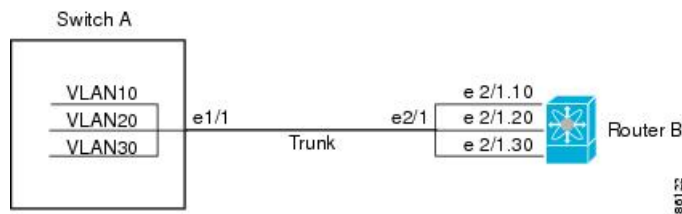
サブインターフェイスの名前は、親インターフェイスの名前（たとえば Ethernet 2/1）+ピリオド（.）+そのインターフェイス独自の番号です。たとえば、イーサネットインターフェイス 2/1 に Ethernet 2/1.1 というサブインターフェイスを作成できます。この場合、.1はそのサブインターフェイスを表します。

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 トランッ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 トランッキングを使って 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ッ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、トランッ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。

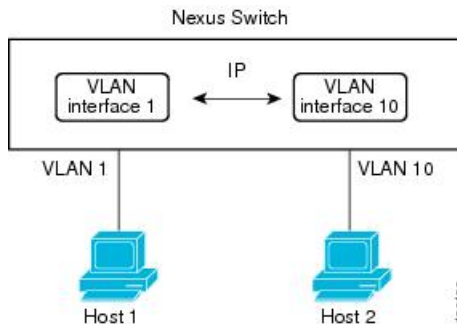


(注) VLAN 1 の VLAN インターフェイスは削除できません。

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



## 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。

## 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。

- 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 3016 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 個のポートがスパン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



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# <b>configure terminal</b>	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)# <b>interface ethernet slot/port</b>	インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	<code>switch(config-if)# no switchport</code>	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、 <b>switchport</b> コマンドを使用します。
ステップ 4	<code>switch(config-if)# [ip ipv6]ip-address/length</code>	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	<code>switch(config-if)# medium {broadcast   p2p}</code>	(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 <b>broadcast</b> であり、この設定はどの <b>show</b> コマンドにも表示されません。ただし、 <b>p2p</b> に設定を変更した場合、 <b>show running config</b> 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	<code>switch(config-if)# show interfaces</code>	(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	<code>switch(config-if)# copy running-config startup-config</code>	(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	<code>switch(config-if)# copy running-config startup-config</code>	(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	<code>switch(config)# interface ethernet slot/port.number</code>	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	<code>switch(config-if)# [ip   ipv6] address ip-address/length</code>	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	<code>switch(config-if)# encapsulation dot1Q vlan-id</code>	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	<code>switch(config-if)# show interfaces</code>	(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	<code>switch(config-if)# copy running-config startup-config</code>	(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# <b>configure terminal</b>	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)# <b>interface ethernet slot/port</b>	インターフェイス コンフィギュレーション モードを開始します。 <i>slot</i> の範囲は 1 ~ 255 です。 <i>port</i> の範囲は 1 ~ 128 です。
ステップ 3	switch(config-if)# <b>bandwidth [value   inherit [value]]</b>	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。 <ul style="list-style-type: none"> <li>• <b>value</b> : 帯域幅のサイズ (KB 単位)。指定できる範囲は 1 ~ 10000000 です。</li> <li>• <b>inherit</b> : 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。</li> </ul>
ステップ 4	switch(config-if)# <b>copy running-config startup-config</b>	(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# <b>configure terminal</b>	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)# <b>feature interface-vlan</b>	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)# <b>interface vlan number</b>	VLAN インターフェイスを作成します。 <i>number</i> の有効範囲は 1 ~ 4094 です。
ステップ 4	switch(config-if)# <b>[ip   ipv6] address ip-address/length</b>	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)# <b>no shutdown</b>	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)# <b>show interface vlan number</b>	(任意) VLAN インターフェイスの統計情報を表示します。 <i>number</i> の有効範囲は 1 ~ 4094 です。
ステップ 7	switch(config-if)# <b>copy running-config startup-config</b>	(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
```

## 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# <b>configure terminal</b>	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)# <b>interface loopback instance</b>	ループバック インターフェイスを作成します。 <i>instance</i> の範囲は 0 ~ 1023 です。
ステップ 3	switch(config-if)# [ <b>ip   ipv6</b> ] <b>address ip-address/length</b>	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)# <b>show interface loopback instance</b>	(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。 <i>instance</i> の範囲は 0 ~ 1023 です。
ステップ 5	switch(config-if)# <b>copy running-config startup-config</b>	(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、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
```

## 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# <b>configure terminal</b>	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)# <b>interface</b> <i>interface-typenumber</i>	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)# <b>vrf member</b> <i>vrf-name</i>	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)# [ <b>ip   ipv6</b> ] <i>ip-address/length</i>	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。
ステップ 5	switch(config-if)# <b>show vrf</b> [ <i>vrf-name</i> ] <b>interface</b> <i>interface-typenumber</i>	(任意) VRF 情報を表示します。
ステップ 6	switch(config-if)# <b>show interfaces</b>	(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)# <b>copy running-config startup-config</b>	(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# <b>configure terminal</b>	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)# <b>interface ethernet</b> 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)# [ <b>no</b> ] <b>mac-address</b> static router MAC address	<p>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、<b>no</b> 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。</p> <ul style="list-style-type: none"> <li>• E.E.E</li> <li>• EE-EE-EE-EE-EE-EE</li> <li>• EE:EE:EE:EE:EE:EE</li> <li>• EEEE.EEEE.EEEE</li> </ul> <p>次の無効な MAC アドレスを入力しないでください。</p> <ul style="list-style-type: none"> <li>• ヌル MAC アドレス : 0000.0000.0000</li> <li>• ブロードキャスト MAC アドレス : FFFF.FFFF.FFFF</li> <li>• マルチキャスト MAC アドレス : 0100.DAAA.ADDD</li> </ul>
ステップ 4	switch(config-if)# <b>show interface</b> 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# <b>configure terminal</b>	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)# <b>interfacetype slot/port</b>	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)# <b>no switchport</b>	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、 <b>switchport</b> コマンドを使用します。
ステップ 4	switch(config-if)# <b>mac-address ipv6-extract</b>	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)# <b>ipv6 address ip-address/length</b>	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)# <b>ipv6 nd mac-extract [exclude nud-phase]</b>	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。  <b>exclude nud-phase</b> 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。 <b>exclude nud-phase</b> 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)# <b>show ipv6 icmp interfacetype slot/port</b>	(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 unreachable: false
  ICMPv6-nd Statistics (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 unreachable: false

```

```
ICMPv6-nd Statistics (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# <b>configure terminal</b>	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)# <b>system default interface-vlan autostate</b>	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 <b>no</b> 形式を使用します。
ステップ 3	switch(config)# <b>feature interface-vlan</b>	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)# <b>interface vlanvlan id</b>	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)# <b>[no] autostate</b>	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)# <b>end</b>	特権 EXEC モードに戻ります。
ステップ 7	<b>show running-config interface vlanvlan id</b>	(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# <b>configure terminal</b>	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)# <b>interface ethernet type slot/port   mgmt mgmt-interface-number   vlan vlan id</b>	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)# <b>[no] ip   ipv6 address dhcp</b>	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 <b>no</b> 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)# <b>copy running-config startup-config</b>	(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
<b>show interface ethernetslot/port</b>	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。
<b>show interface ethernetslot/portbrief</b>	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。
<b>show interface ethernetslot/portcapabilities</b>	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。
<b>show interface ethernetslot/portdescription</b>	レイヤ3インターフェイスの説明を表示します。
<b>show interface ethernetslot/portstatus</b>	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。
<b>show interface ethernetslot/port.number</b>	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。
<b>show interface port-channel channel-id.number</b>	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。
<b>show interface loopbacknumber</b>	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。
<b>show interface loopbacknumberbrief</b>	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。
<b>show interface loopbacknumberdescription</b>	ループバック インターフェイスの説明を表示します。
<b>show interface loopbacknumberstatus</b>	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。

コマンド	目的
<code>show interface vlannumber</code>	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。
<code>show interface vlannumberbrief</code>	VLANインターフェイスの動作ステータスを表示します。
<code>show interface vlannumberdescription</code>	VLANインターフェイスの説明を表示します。
<code>show interface vlannumberprivate-vlan mapping</code>	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。
<code>show interface vlannumberstatus</code>	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クのトリガー

レイヤ3インターフェイス整合性チェック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ク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	<code>show consistency-checker l3-interface moduleslot</code>	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
<b>load-interval</b> <i>seconds</i>   <b>counter</b> { <b>1</b>   <b>2</b>   <b>3</b> } <i>seconds</i>	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。
<b>show interface ethernet</b> <i>slot/port</i> <b>counters</b>	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）。
<b>show interface ethernet</b> <i>slot/port</i> <b>counters brief</b> <i>load-interval-id</i>	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。  <i>load-interval-id</i> 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。
<b>show interface ethernet</b> <i>slot/port</i> <b>counters detailed</b> [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 packets 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。
<b>show interface ethernet</b> <i>slot/port</i> <b>counters error</b>	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。
<b>show interface ethernet</b> <i>slot/port</i> <b>counters snmp</b>	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。
<b>show interface ethernet</b> <i>slot/port</i> <b>numbercounters</b>	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。
<b>show interface port-channel</b> <i>channel-id</i> <b>numbercounters</b>	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。

コマンド	目的
<b>show interface loopbacknumbercounters</b>	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。
<b>show interface loopbacknumbercounters detailed [all]</b>	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 packets 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。
<b>show interface loopbacknumbercounters errors</b>	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。
<b>show interface vlannumbercounters</b>	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。
<b>show interface vlannumbercounters detailed [all]</b>	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 packets 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）。
<b>show interface vlangcounterssnmp</b>	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)#
```

## 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』 コマンド構文の詳細については、ご使用のデバイスのコマンドリファレンスを参照してください。
IP	『Cisco Nexus 3000 Series NX-OS Unicast Routing Configuration Guide』 ご使用のデバイスの『Unicast Routing Configuration Guide』の「Configuring IP」の章
VLAN	『Cisco Nexus 3000 Series NX-OS Layer 2 Switching Configuration Guide』 『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。 <a href="http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml">http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</a>
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
<b>show interface vlan <i>vlan-id</i> counters</b> command	5.0(3)U3(1)	<b>show interface vlan <i>vlan-id</i> counters</b> 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, 65 ページ](#)
- [ポートチャネルの設定, 76 ページ](#)
- [ポートチャネル設定の確認, 85 ページ](#)
- [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, 86 ページ](#)
- [ロードバランシング発信ポート ID の確認, 87 ページ](#)
- [ポートチャネルの機能履歴, 87 ページ](#)

## 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、スパン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, \(72 ページ\)](#)

## 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, \(68 ページ\)](#)」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 アドレス
- 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

設定	レイヤ2基準	レイヤ3基準	レイヤ4基準
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となります。

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。



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 packets が間違っただ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 packets が間違っただ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 packets は間違っただ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 Encapsulation (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) 経路で転送される際に 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

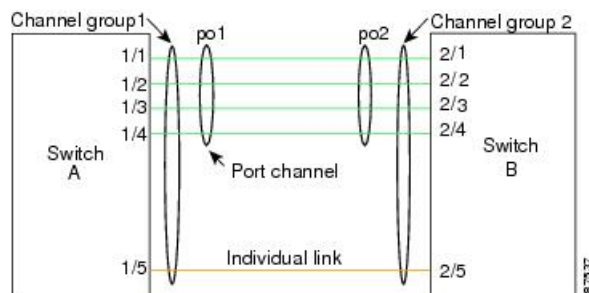
### LACP の概要



(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ることでシステム 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られたものです。

- **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。
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、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せん。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、ポート速度やトラッ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。 <ul style="list-style-type: none"> <li>• Active</li> <li>• Passive</li> </ul>	on モードのみ

## LACP ポートチャネルの MinLink

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。MinLink 機能を使用すると、ポートチャネルがダウンする前に停止する必要がある LACP バンドルからのインターフェイスの最小数を定義できます。

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。



(注) 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。

# 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# <b>configure terminal</b>	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)# <b>interface port-channelchannel-number</b>	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。

	コマンドまたはアクション	目的
ステップ 3	<code>switch(config)# no interface port-channel channel-number</code>	ポートチャネルを削除し、関連するチャン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

新規のチャンネルグループ、または他のポートがすでに属しているチャン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 によってこのチャン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	<code>switch# configure terminal</code>	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	<code>switch(config)# interface typeslot/port</code>	チャン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	<code>switch(config-if)# switchport mode trunk</code>	(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	<code>switch(config-if)# switchport trunk {allowed vlan vlan-id   native vlan vlan-id}</code>	(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	<code>switch(config-if)# channel-group channel-number</code>	チャン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 によってこのチャン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。

	コマンドまたはアクション	目的
ステップ 6	<code>switch(config-if)# no channel-group</code>	(任意) チャンネルグループからポートを削除します。チャン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 をチャンネルグループ 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	<code>switch# configure terminal</code>	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	<code>switch(config)# port-channel load-balance ethernet {[destination-ip  </code>	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 <code>source-dest-mac</code> です。



	コマンドまたはアクション	目的
	<pre>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}</pre>	<p>(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 <b>destination-ip-gre</b>、<b>source-dest-ip-gre</b>、および <b>source-ip-gre</b> 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。</p> <p>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 <b>symmetric</b> 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。</p> <ul style="list-style-type: none"> <li>• source-dest-ip-only</li> <li>• source-dest-port-only</li> <li>• source-dest-ip</li> <li>• source-dest-port</li> <li>• source-dest-ip-gre</li> </ul>
ステップ 3	<pre>switch(config)# no port-channel load-balance ethernet</pre>	<p>(任意) ロードバランシングアルゴリズムをデフォルトの <b>source-dest-mac</b> に戻します。</p>
ステップ 4	<pre>switch# show port-channel load-balance</pre>	<p>(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。</p>

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ン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# <b>configure terminal</b>	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)# <b>feature lacp</b>	スイッチ上で LACP をイネーブルにします。
ステップ 3	switch(config)# <b>show feature</b>	(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# <b>configure terminal</b>	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)# <b>interface</b> <i>typeslot/port</i>	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)# <b>channel-group</b> <i>channel-number</i> [ <b>force</b> ] [ <b>mode</b> { <b>on</b>   <b>active</b>   <b>passive</b> }]	<p>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 <b>active</b> または <b>passive</b> に設定します。</p> <p><b>force</b> : 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。</p> <p><b>mode</b> : 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。</p> <p><b>active</b> : 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。</p> <p><b>on</b> : (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。</p> <p><b>passive</b> : 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。</p> <p>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 <b>on</b> です。</p>
ステップ 4	switch(config-if)# <b>no</b> <b>channel-group</b> <i>numbermode</i>	指定インターフェイスのポートモードを <b>on</b> 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	<code>switch# configure terminal</code>	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	<code>switch(config)# interface port-channelnumber</code>	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	<code>switch(config-if)# [no] lACP min-linksnumber</code>	ポートチャネルインターフェイスを指定して、最小リンクの数を設定し、インターフェイスコンフィギュレーションモードを開始します。  <i>number</i> 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 <b>no</b> 形式を使用します。
ステップ 4	<code>switch(config)# show running-config interface port-channelnumber</code>	(任意) ポートチャネルの MinLink 設定を表示します。

次に、モジュール 3 のポートチャネルインターフェイス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-if) #
```

## 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# <b>configure terminal</b>	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)# <b>interface typeslot/port</b>	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)# <b>lacp rate fast</b>	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# <b>configure terminal</b>	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)# <b>lACP system-priority</b> <i>priority</i>	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# <b>show lACP system-identifier</b>	(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# <b>configure terminal</b>	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)# <b>interface</b> <i>typeslot/port</i>	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)# <b>lACP port-priority</b> <i>priority</i>	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

	コマンドまたはアクション	目的
		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
<b>show interface port channel</b> <i>channel-number</i>	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。
<b>show feature</b>	イネーブルにされた機能を表示します。
<b>show resource</b>	システムで現在利用可能なリソースの数を表示します。
<b>show lacp</b> { <b>counters</b>   <b>interfacetypeslot/port</b>   <b>neighbor</b>   <b>port-channel</b>   <b>system-identifier</b> }	LACP 情報を表示します。
<b>show port-channel compatibility-parameters</b>	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。
<b>show port-channel database</b> [ <b>interface port-channel</b> <i>channel-number</i> ]	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。
<b>show port-channel summary</b>	ポートチャネルインターフェイスの概要を表示します。
<b>show port-channel traffic</b>	ポートチャネルのトラフィック統計情報を表示します。
<b>show port-channel usage</b>	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。
<b>show port-channel database</b>	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。

コマンド	目的
<b>show port-channel load-balance</b>	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
<b>ステップ 1</b>	<b>switch# show consistency-checker membership port-channels</b>	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
<pre>switch# show port-channel load-balance forwarding-path interface port-channel port-channel-idvlan vlan-id dst-ipsrc-ipdst-macsrc-macl4-src-portport-id l4-dst-portport-idether-typeether-typeip-protoip-proto</pre>	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。





## 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, 89 ページ](#)
- [IP トンネルのライセンス要件, 91 ページ](#)
- [IP トンネルの前提条件, 91 ページ](#)
- [IP トンネルの注意事項および制約事項, 91 ページ](#)
- [IP トンネリングのデフォルト設定, 93 ページ](#)
- [IP トンネルの設定, 93 ページ](#)
- [IP トンネル設定の確認, 100 ページ](#)
- [IP トンネリングの設定例, 101 ページ](#)
- [IP トンネルの関連資料, 101 ページ](#)
- [IP トンネルの標準, 101 ページ](#)
- [IP トンネル設定の機能履歴, 101 ページ](#)

## 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。

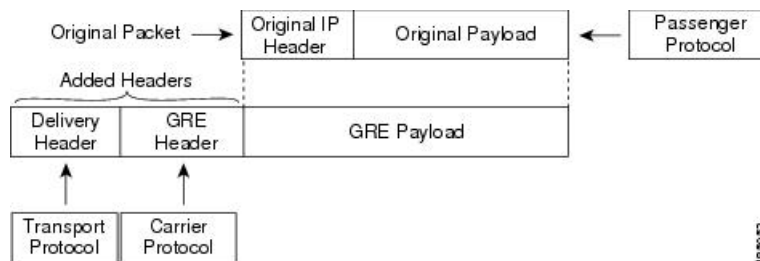
設定の前にトンネル機能をイネーブルにする必要があります。

## 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 をサポートしません。
- 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 ヘッダーによるのみ 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 (Parameters)	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# <b>configure terminal</b>	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)# <b>feature tunnel</b>	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)# <b>exit</b>	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)# <b>show feature</b>	スイッチのトンネル機能を表示します。
ステップ 5	switch# <b>copy running-config startup-config</b>	(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# <b>configure terminal</b>	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)# <b>[no] interface tunnelnumber</b>	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)# <b>tunnel mode</b> {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。  <b>gre</b> キーワードおよび <b>ip</b> キーワードは、IP での GRE カプセル化の使用を指定します。  <b>ipip</b> 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 <b>decapsulate-any</b> 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)# <b>tunnel source</b> {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)# <b>tunnel destination</b> {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)# <b>tunnel use-vrf</b> 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)# <b>show interface tunnel</b> 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# <b>copy running-config startup-config</b>	(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# <b>configure terminal</b>	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)# <b>[no] interface tunnelnumber</b>	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)# <b>ip addressip address</b>	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)# <b>route-mapmap-name</b>	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)# <b>match ip address access-list-namename</b>	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)# <b>set ip next-hopaddress</b>	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ず、ネクストホップ エントリから ECMP を選択するには、 <b>load-share</b> 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。GRE v6 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	<code>switch# configure terminal</code>	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	<code>switch(config)# interface tunnel number</code>	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	<code>switch(config-if)# tunnel mode {gre ip   ipip {ip   decapsulate-any}}</code>	このトンネル モードを GRE、 <code>ipip</code> 、または <code>ipip decapsulate-only</code> に設定します。  <b>gre</b> キーワードおよび <b>ip</b> キーワードは、IP での GRE カプセル化の使用を指定します。  <b>ipip</b> 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 <b>decapsulate-any</b> 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	<code>switch(config-if)# tunnel use-vrf vrf-name</code>	トンネル VRF 名を設定します。
ステップ 5	<code>switch(config-if)# ipv6 address IPv6 address</code>	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	<code>switch(config-if)# show interface tunnel number</code>	(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)# <i>mtu value</i>	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)# <b>copy running-config startup-config</b>	(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# <b>configure terminal</b>	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)# <b>interface tunnel number</b>	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)# <b>vrf member vrf-name</b>	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)# <b>ip address ip-prefix/length</b>	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)# <b>show vrf</b> [vrf-name] <b>interface interface-type</b> <i>number</i>	(任意) VRF 情報を表示します。
ステップ 6	switch(config-if)# <b>copy</b> <b>running-config startup-config</b>	(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
<b>show interface tunnel</b> <i>number</i>	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。
<b>show interface tunnel</b> <i>number</i> <b>brief</b>	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。
<b>show interface tunnel</b> <i>number</i> <b>description</b>	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。
<b>show interface tunnel</b> <i>number</i> <b>status</b>	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。
<b>show interface tunnel</b> <i>number</i> <b>status err-disabled</b>	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, 103 ページ](#)
- [VXLAN トラフィック転送の設定, 112 ページ](#)
- [VXLAN 設定の確認, 120 ページ](#)

## 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。

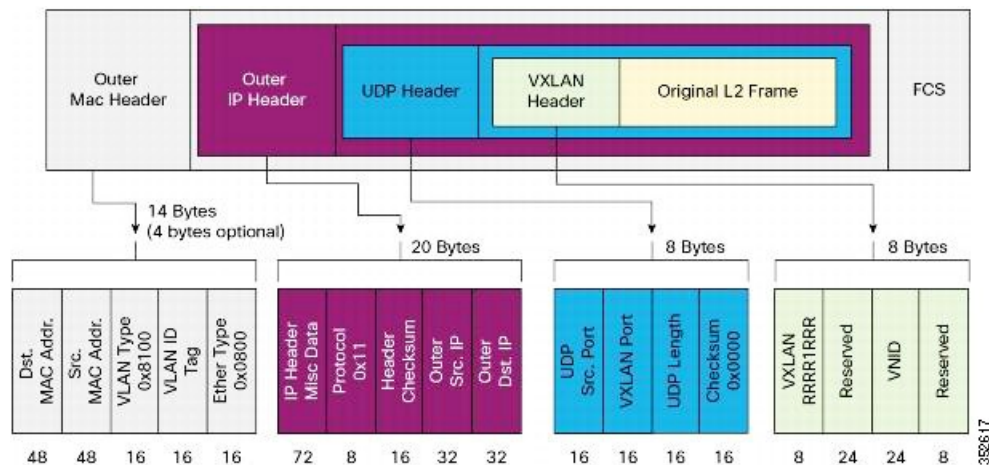
## VXLAN のカプセル化およびパケット形式

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、フラッドイ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ドイングを削減します。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パッケージが、ネットワークのそのIPアドレスへのルートを紹介して、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紹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) ポートチャンネルである場合は、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せん。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。

- Cisco Nexus 3000 Release 7.0(3)I2(1) は、マルチキャスト グループと入力複製 (IR) の同時設定をサポートしません。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。
- VXLAN については、バドモードはサポートされません。
- 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。
- 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。
- 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。

- 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。

## 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、ユニキャスト RP およびサービス オーフア 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オーファン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 に接続されたオーファン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 オーファンに類似しています。

- 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 整合性チェック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 整合性チェック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、\(106ページ\)](#)」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# <b>configure terminal</b>	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)# <b>feature pim</b>	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。

	コマンドまたはアクション	目的
ステップ 3	switch(config)# <b>show running-config pim</b>	(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)# <b>copy running-config startup-config</b>	(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# <b>configure terminal</b>	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)# <b>ip pim rp-address rp-address [group-list ip-prefix   route-map policy-name]</b>	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。 <b>match ip multicast</b> 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

	コマンドまたはアクション	目的
		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	<code>switch(config)# show ip pim group-range [ip-prefix] [vrf {vrf-name   all   default   management}]</code>	(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	<code>switch(config)# copy running-config startup-config</code>	(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	<code>switch# configure terminal</code>	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	<code>switch(config)# [no] feature vn overlay</code>	VXLAN 機能をイネーブルにします。
ステップ 3	<code>switch (config)# [no] feature vn-segment-vlan-based</code>	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。

	コマンドまたはアクション	目的
		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	<code>switch(config)# copy running-config startup-config</code>	(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	<code>switch# configure terminal</code>	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	<code>switch(config)# vlan vlan-id</code>	VLAN を指定します。
ステップ 3	<code>switch(config-vlan)# vn-segment vniid</code>	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) を使用できません。
- 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# <b>configure terminal</b>	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)# <b>interface loopbackinstance</b>	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)# <b>ip addressip-address/length</b>	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)# <b>ip ospf network {broadcast   point-to-point}</b>	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)# <b>ip router ospfinstance-tagareaarea-id</b>	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)# <b>ip pim sparse-mode</b>	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# <b>configure terminal</b>	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)# <b>vxlan udp portnumber</b>	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# <b>configure terminal</b>	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)# <b>interface nve instance</b>	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)# <b>source-interface loopback instance</b>	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	<code>switch(config-if-nve)# member vni {vni} mcast-group {multicast-group-addr   vni-range} mcast-group {start-addr [end-addr]}</code>	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	<code>switch(config-if-nve)# member vni vni</code>	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	<code>switch(config-if-nve-vni)# ingress-replication protocol static</code>	VNI の静的入力複製を有効にします。
ステップ 3	<code>switch(config-if-nve-vni)# peer-ip ip-address</code>	ピア IP を有効にします。 (注) <ul style="list-style-type: none"> <li>• 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。</li> <li>• 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。</li> </ul>

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
<code>show nve interface nveid</code>	NVE インターフェイスの設定を表示します。
<code>show nve vni</code>	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。
<code>show nve peers</code>	NVE インターフェイスのピアを表示します。
<code>show interface nveidcounters</code>	NVE インターフェイスのすべてのカウンタを表示します。
<code>show nve vxlan-params</code>	設定されている VXLAN UDP ポートを表示します。
<code>show mac address-table</code>	VLAN と VXLAN の両方の MAC アドレスを表示します。
<code>clear mac address-table dynamic</code>	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.LIID
-----+-----+-----+-----+-----+-----+-----
* 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

## 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, 123 ページ](#)
- [VRF に関する注意事項と制約事項, 134 ページ](#)
- [vPC 設定の確認, 135 ページ](#)
- [vPC のデフォルト設定, 140 ページ](#)
- [vPC の設定, 141 ページ](#)

### 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ク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ドメイン内におい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 VRF を設定するときは、vPC ピアキープアライブメッセージを伝送するために vPC ピアリンクが使用されていないことを確認してください。

## 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



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, 0-23-4-ee-be-64, 8458, 0, 0), (8000, (8000, f4-4e-5-84-5e-3c, 457, 0, 0)]	[(fa0, 0-23-4-ee-be-64, 8458, 0, 0), (8000, (8000, f4-4e-5-84-5e-3c, 457, 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ます、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 整合性検査は、スパニングツリーが VLAN でイネーブルまたはディセーブルにされるときに VLAN ごとに行われます。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

両方の vPC ピア スイッチをリロードし、スイッチを 1 つだけリブートすると、自動リカバリによってスイッチがプライマリ スイッチのロールを負い、vPC リンクが所定の期間後に稼働できるようになります。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ンネルも含め、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 (CFS/eE) 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。

---

## CFS/eE

Cisco Fabric Services over Ethernet (CFS/eE) 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。CFS/eE 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/CFS/eE プロトコルデータユニット (PDU) に入れて伝送されます。

CFS/eE 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 CFS/eE 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。CFS/eE 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、CFS/eE 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 CFS/eE 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。

- 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、その前にピアキーブ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。
- ピアキーブ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 ピアキーブアラ



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witchの MAC アドレスとプライオリティを表示します。
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、スパン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    Pol    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 Mode 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    Pol    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

```

## VLAN ごとの整合性ステータスの表示

```

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   Pol  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   Pol  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 VLAN Mapping 1    success                    0-4095
STP Loopguard                       1    success                    0-4095
STP Bridge Assurance                 1    success                    0-4095
STP Port Type, Edge BPDUGuard       1    success                    0-4095
STP MST Simulate PVST                1    success                    0-4095
Pass Vlans                           -

```

## 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 (Parameters)	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# <b>configure terminal</b>	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)# <b>feature vpc</b>	スイッチで vPC をイネーブルにします。
ステップ 3	switch# <b>show feature</b>	(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# <b>copy running-config startup-config</b>	(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# <b>configure terminal</b>	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)# <b>no feature vpc</b>	スイッチで vPC をディセーブルにします。
ステップ 3	switch# <b>show feature</b>	(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# <b>copy running-config startup-config</b>	(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# <b>configure terminal</b>	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)# <b>vpc domain</b> <i>domain-id</i>	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。 <i>domain-id</i> 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、 <b>vpc domain</b> コマンドを使用することもできます。
ステップ 3	switch# <b>show vpc brief</b>	(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# <b>copy running-config startup-config</b>	(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せん。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# <b>configure terminal</b>	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)# <b>vpc domain</b> <i>domain-id</i>	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)# <b>peer-keepalive destination</b> <i>ipaddress</i> [ <b>hold-timeoutsecs</b>   <b>interval</b> <i>msecs</i> { <b>timeoutsecs</b> }   <b>precedence</b> { <i>prec-value</i>   <b>network</b>   <b>internet</b>   <b>critical</b>   <b>flash-override</b>   <b>flash</b>   <b>immediate</b> <b>priority</b>   <b>routine</b> }   <b>tos</b> { <i>tos-value</i>   <b>max-reliability</b>   <b>max-throughput</b>   <b>min-delay</b>   <b>min-monetary-cost</b>   <b>normal</b> }   <b>tos-byte</b> <i>tos-byte-value</i> }   <b>sourceipaddress</b>   <b>vrf</b> { <i>name</i>   <b>management vpc-keepalive</b> }]	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)# <b>vpc peer-keepalive destination</b> <i>ipaddress</i> <b>sourceipaddress</b>	(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。
ステップ 5	switch# <b>show vpc peer-keepalive</b>	(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。

	コマンドまたはアクション	目的
ステップ 6	switch# <b>copy running-config startup-config</b>	(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# <b>configure terminal</b>	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)# <b>interface port-channelchannel-number</b>	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)# <b>vpc peer-link</b>	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# <b>show vpc brief</b>	(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# <b>copy running-config startup-config</b>	(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# <b>show vpc consistency-parameters {global interface port-channelchannel-number}</b>	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, 0) (1538, 0, 0, 0, 0, 0, 0)
Network QoS (Pause)                 2      (F, F, F, F, F, F)      (1538, 0, 0, 0, 0, 0, 0)
Input Queuing (Bandwidth)           2      (100, 0, 0, 0, 0, 0, 0) (100, 0, 0, 0, 0, 0, 0)
Input Queuing (Absolute Priority)    2      (F, F, F, F, F, F)      (100, 0, 0, 0, 0, 0, 0)
Output Queuing (Bandwidth)           2      (100, 0, 0, 0, 0, 0, 0) (100, 0, 0, 0, 0, 0, 0)
Output Queuing (Absolute Priority)   2      (F, F, F, F, F, F)      (100, 0, 0, 0, 0, 0, 0)
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 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           1      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# <b>configure terminal</b>	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)# <b>vpc domain domain-id</b>	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)# <b>auto-recovery reload-delay delay</b>	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(2)N2(1)
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# <b>configure terminal</b>	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)# <b>vpc domain domain-id</b>	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)# <b>delay restore time</b>	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# <b>copy running-config startup-config</b>	(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。すべてのレイヤ 3 転送は vPC セカンダリ スイッチ上のすべての VLAN で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# <b>configure terminal</b>	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)# <b>vpc domain</b> <i>domain-id</i>	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)# <b>dual-active exclude interface-vlan</b> <i>range</i>	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# <b>pingipaddress vrf</b> <i>vrf-name</i>	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# <b>configure terminal</b>	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)# <b>interface port-channelchannel-number</b>	ダウンストリームスイッチに接続するためにvPCに入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)# <b>vpcnumber</b>	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# <b>show vpc brief</b>	(任意) 各vPCに関する情報を表示します。
ステップ 5	switch# <b>copy running-config startup-config</b>	(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# <b>configure terminal</b>	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)# <b>vpc domain</b> <i>domain-id</i>	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、 <b>vpc-domain</b> コンフィギュレーション モードを開始します。 <i>domain-id</i> 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)# <b>system-mac</b> <i>mac-address</i>	指定した vPC ドメインに割り当てる MAC アドレスを <i>aaaa.bbbb.cccc</i> の形式で入力します。
ステップ 4	switch# <b>show vpc role</b>	(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# <b>copy running-config startup-config</b>	(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	<code>switch# configure terminal</code>	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	<code>switch(config)# vpc domain domain-id</code>	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、 <code>vpc-domain</code> コンフィギュレーションモードを開始します。 <code>domain-id</code> 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	<code>switch(config-vpc-domain)# system-priority priority</code>	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	<code>switch# show vpc brief</code>	(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	<code>switch# copy running-config startup-config</code>	(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# <b>configure terminal</b>	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)# <b>vpc domain</b> <i>domain-id</i>	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、 <b>vpc-domain</b> コンフィギュレーションモードを開始します。 <i>domain-id</i> 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)# <b>role priority</b> <i>priority</i>	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# <b>show vpc brief</b>	(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# <b>copy running-config startup-config</b>	(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 8 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, 155 ページ](#)
- [レイヤ 2 プロトコルのトンネリングについて, 159 ページ](#)
- [Q-in-Q トンネルのライセンス要件, 161 ページ](#)
- [Q-in-Q トンネリングの注意事項および制約事項, 161 ページ](#)
- [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, 162 ページ](#)
- [Q-in-Q 設定の確認, 165 ページ](#)
- [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, 166 ページ](#)
- [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, 166 ページ](#)

## 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 チャンネルでサポートされます。非対称リンクとしてポート チャンネルを設定するには、ポート チャン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。

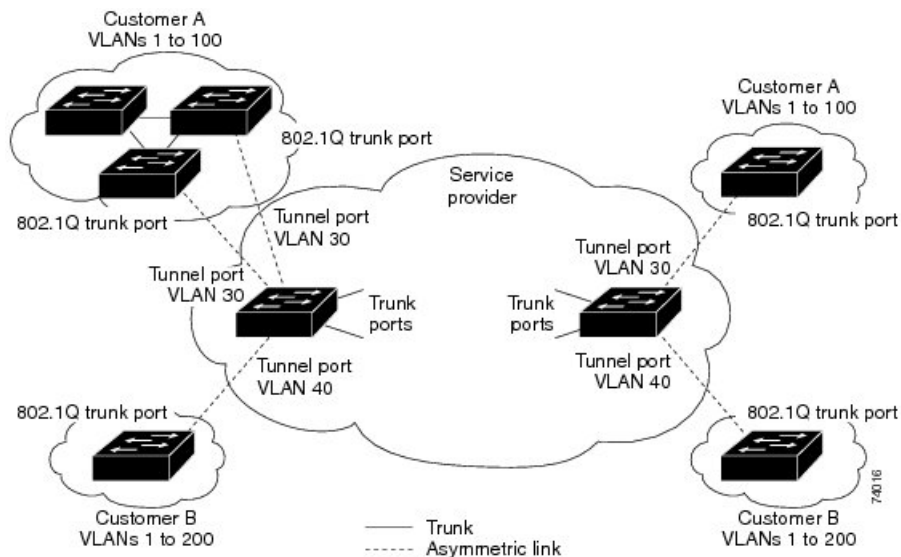
サービス プロバイダーは、802.1Q トンネリング機能を使用すると、単一の VLAN を使用して、複数の VLAN を含む顧客をサポートできます。同一の VLAN 上にあるように見えるときでも、サービス プロバイダー インフラストラクチャ内の顧客の VLAN ID を保護したり、異なる顧客の VLAN トラフィックを分離しておくことができます。IEEE 802.1Q トンネリングは、VLAN-in-VLAN 階層構造およびタグ付きパケットへのタグgingによって、VLAN スペースを拡張します。802.1Q トンネリングをサポートするように設定されたポートは、トンネルポートといいます。トンネ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。顧客ごとに個別の VLAN が必要ですが、その VLAN は顧客の 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顧客のトラフィックは、顧客 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。顧客 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。それぞれの顧客に固有のアクセス VLAN ID には、トンネルポート インターフェイスを割り当てます。



(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 タグgingの対象となります。

図 7: 802.1Q-in-Q トンネル ポート

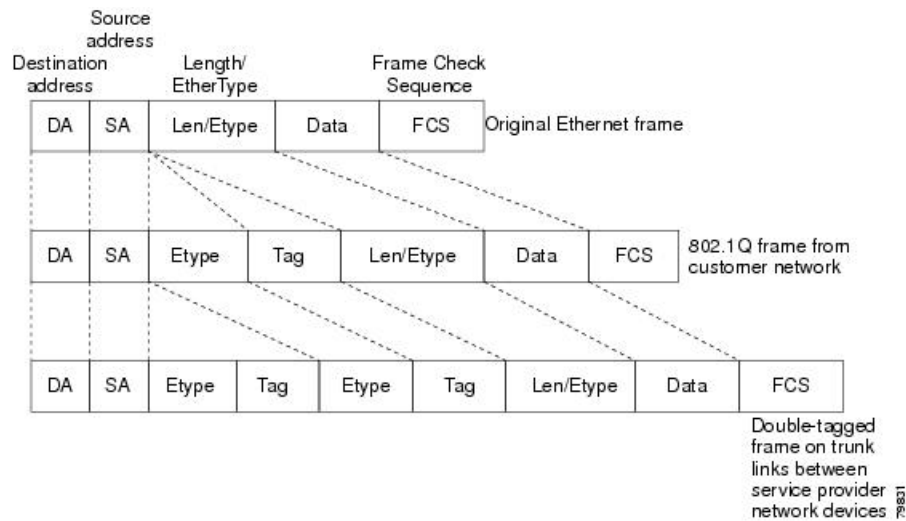


サービスプロバイダー エッジスイッチのトンネルポートに着信するパケット（適切な VLAN ID ですでに 802.1Q タグ付けされている）は、カスタマーに一意である VLAN ID を含む 802.1Q タグの別のレイヤでカプセル化されます。元々のカスタマーの 802.1Q タグは、カプセル化されたパケットの中に維持されます。したがって、サービスプロバイダー インフラストラクチャに着信するパケットは二重にタグ付けされます。

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イーサネットフレーム間の相違点を示します。

図 8 : 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

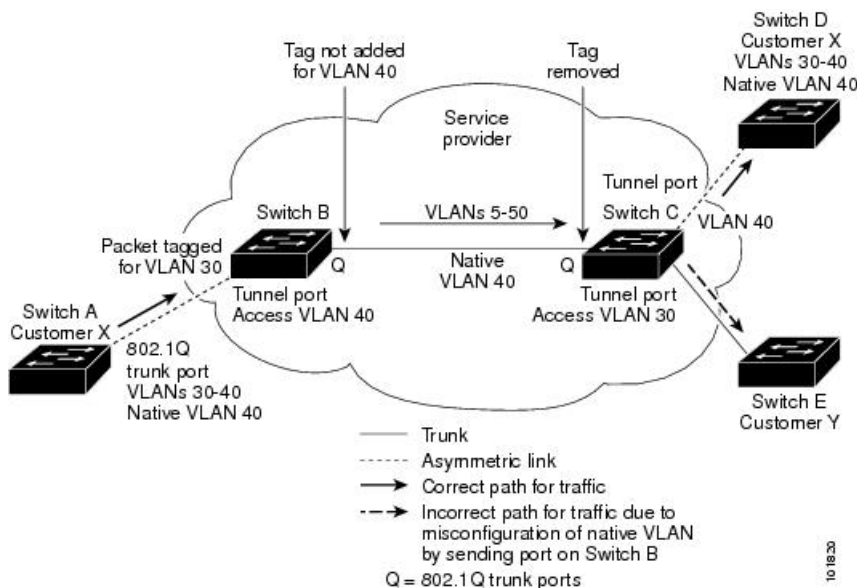
エッジスイッチで 802.1Q トンネリングを設定する場合は、サービスプロバイダー ネットワークにパケットを送信するために、802.1Q トランクポートを使用する必要があります。ただし、サービスプロバイダー ネットワークのコアを通過するパケットは、IEEE 802.1Q トランク、ISL トランク、または非トランッキングリンクで伝送される場合があります。802.1Q トランクをこれらのコア

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 9：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ます。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ます。VLAN トランッキングプロトコル (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プロトコルを特別な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。

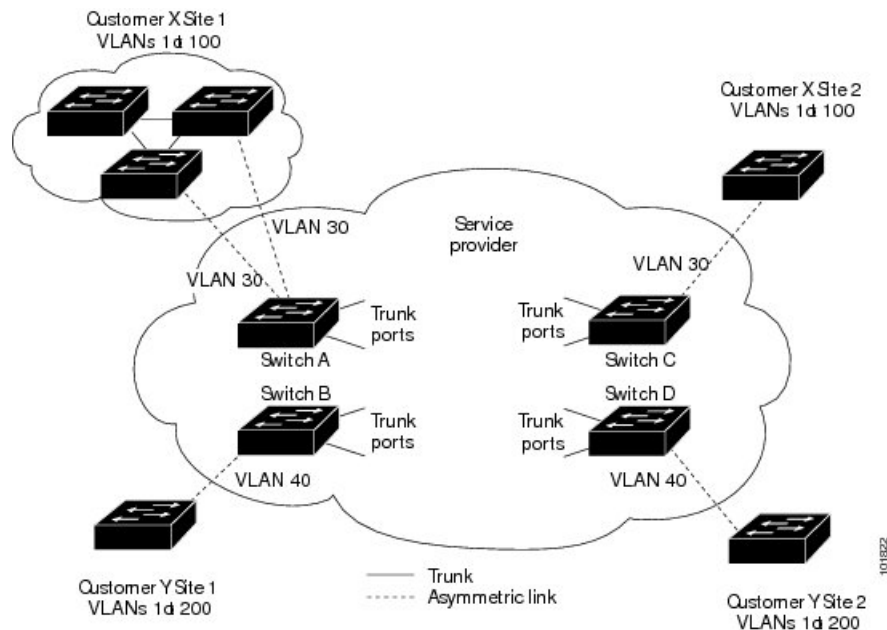


(注) レイヤ2プロトコルのトンネリングは、ソフトウェアでBPDUをトンネリングすることで動作します。スーパーバイザモジュールが受信する多数のBPDUによりCPUの負荷が大きくなります。この負荷は、BPDUとしてマークされたパケットに関して設定されるコントロールプレーンポリシング (CoPP) によって制御されます。

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。

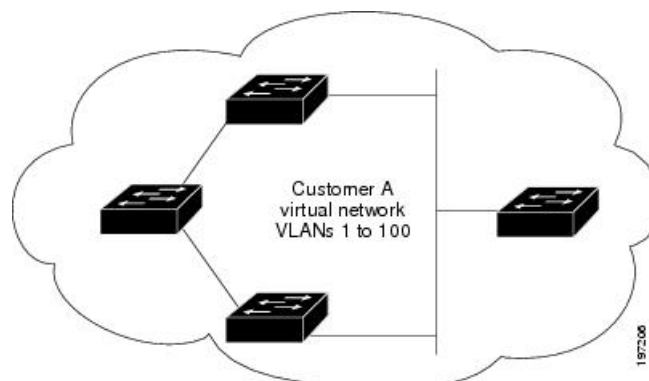
図 10: レイヤ2 プロトコル トンネリング



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 11: 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# <b>configure terminal</b>	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)# <b>interface ethernet slot/port</b>	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)# <b>switchport</b>	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)# <b>[no] switchport mode dot1q-tunnel</b>	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)# <b>exit</b>	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)# <b>exit</b>	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)# <b>copy running-config startup-config</b>	(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# <b>configure terminal</b>	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)# <b>interface ethernet slot/port</b>	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)# <b>switchport</b>	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)# <b>switchport mode dot1q-tunnel</b>	ポートに 802.1Q トンネルを作成します。
ステップ 5	switch(config-if)# [ <b>no</b> ] <b>l2protocol tunnel drop-threshold [cdp   stp   vtp]</b>	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 <b>no</b> 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] <b>l2protocol tunnel</b> <b>shutdown-threshold [cdp   stp   vtp]</b>	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 トランッキングプロトコル (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)# <b>exit</b>	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)# <b>copy</b> <b>running-config startup-config</b>	(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
<b>clear l2protocol tunnel counters [interface if-range]</b>	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。
<b>show dot1q-tunnel [interface if-range]</b>	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
<code>show l2protocol tunnel [interface if-range   vlan vlan-id]</code>	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。
<code>show l2protocol tunnel summary</code>	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。
<code>show running-config l2pt</code>	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

- 10 GbE インターフェイス速度の設定 [22](#)
- 40 GbE インターフェイス速度の設定 [23](#)
- 40 ギガビットイーサネット インターフェイスの速度 [8](#)
- 40 ギガビットイーサネット モード [8](#)
- 802.1Q トンネル ポート、作成 [162](#)
  - インターフェイス [162](#)

### D

- DHCP クライアント検出 [46](#)
- DHCP クライアント設定 [46](#)
- DHCP クライアント設定の制限事項 [46](#)

### G

- GRE トンネル [90](#)
  - インターフェイス [90](#)
- GRE トンネル、設定 [97](#)
  - インターフェイス [97](#)

### I

- IP トンネリング [101](#)
  - 設定例 [101](#)
- IP トンネル [89, 91, 93, 101](#)
  - インターフェイス [89](#)
  - ガイドライン [91](#)
  - デフォルト設定 [93](#)
  - ライセンス要件 [91](#)
  - 機能の履歴 [101](#)
  - 規格 [101](#)
  - 前提条件 [91](#)

- IP トンネル設定、確認 [100](#)
  - インターフェイス [100](#)
- ipip decapsulate-only [90](#)

### L

- LACP [66, 72, 73, 75, 76, 80, 82](#)
  - システム ID [73](#)
  - ポートチャネル [72](#)
  - ポートチャネル、MinLink [76, 82](#)
  - マーカーレスボンダ [75](#)
    - 設定 [80](#)
- LACP がイネーブルとスタティック [75](#)
  - ポートチャネル [75](#)
- LACP の設定 [80](#)
- LACP ポートプライオリティ [84](#)
  - 設定 [84](#)
- LACP 高速タイマー レート [82](#)
  - 設定 [82](#)
- Link Aggregation Control Protocol [66](#)

### M

- MIB [40, 64](#)
  - レイヤ2 インターフェイス [40](#)
  - レイヤ3 インターフェイス [64](#)

### N

- NV オーバーレイ機能のイネーブル化 [114](#)
- NVE インターフェイスの設定 [117](#)
- NVGRE トラフィック [71](#)

**P**

PIM のイネーブル化 [112](#)

**Q**

Q-in-Q トンネリング、注意事項 [161](#)

    インターフェイス [161](#)

Q-in-Q トンネル [155](#)

    インターフェイス [155](#)

Q-in-Q トンネル、ライセンス [161](#)

    インターフェイス [161](#)

Q-in-Q トンネル、レイヤ 2 プロトコル [166](#)

    機能の履歴 [166](#)

Q-in-Q 設定、確認 [165](#)

    インターフェイス [165](#)

**R**

RP の設定 [113](#)

**S**

SFP+ トランシーバ [8](#)

Small Form-Factor Pluggable (プラス) トランシーバ [8](#)

STP [65](#)

    ポート チャンネル [65](#)

SVI 自動ステート [11](#)

    レイヤ 2 [11](#)

SVI 自動ステート、ディセーブル化 [26](#)

    レイヤ 2 [26](#)

SVI 自動ステートのディセーブル化 [45](#)

SVI 自動ステートのディセーブル化、設定 [57](#)

**U**

UDLD [6, 7](#)

    アグレッシブ モード [7](#)

    定義 [6](#)

    非アグレッシブ モード [7](#)

UDLD モード A [17](#)

    設定 [17](#)

**V**

VLAN [43](#)

    インターフェイス [43](#)

VLAN インターフェイス [51](#)

    設定 [51](#)

VLAN インターフェイスの作成 [117](#)

VLAN から VXLAN VNI へのマッピング [115](#)

VN-Segment への VLAN のマッピングのイネーブル化 [114](#)

vPC [134, 151](#)

    ポート チャンネルの移行 [151](#)

    注意事項と制約事項 [134](#)

vPC の用語 [124](#)

VRF [52](#)

    インターフェイスの割り当て [52](#)

VRF メンバーシップ、割り当て [99](#)

    トンネル インターフェイス [99](#)

VXLAN UDP ポートの作成 [117](#)

VXLAN UDP ポートの設定 [117](#)

VXLAN の注意事項と制約事項 [108](#)

**い**

イーサネット インターフェイス [8, 33](#)

    インターフェイスの速度 [8](#)

    デバウンス タイマー、設定 [33](#)

イネーブル化 [29, 30, 31](#)

    CDP [29](#)

    error-disabled の検出 [30](#)

    error-disabled リカバリ [31](#)

    インターフェイス [5, 6, 42, 43, 44, 45, 49, 51, 52, 61, 62, 89, 90, 94, 97,](#)

[100, 155, 159, 161, 162, 163, 164, 165](#)

    802.1Q トンネル ポート、作成 [162](#)

    GRE トンネル [90](#)

    GRE トンネル、設定 [97](#)

    IP トンネル [89](#)

    IP トンネル設定、確認 [100](#)

    ipip トンネル decapsulation-only、設定 [97](#)

    ipip トンネル、設定 [97](#)

    loopback [44, 51](#)

    options [5](#)

    Q-in-Q トンネリング、注意事項 [161](#)

    Q-in-Q トンネル [155](#)

    Q-in-Q トンネル、ライセンス [161](#)

    Q-in-Q 設定、確認 [165](#)

    tunnel [45](#)

    UDLD [6](#)

## インターフェイス (続き)

- VLAN [43, 51](#)
  - 設定 [51](#)
- VRF への割り当て [52](#)
- シャーシ ID [5](#)
- トンネル インターフェイス、作成 [94](#)
- ルーテッド [42](#)
- レイヤ 2 プロトコル トンネル [163](#)
- レイヤ 2 プロトコル トンネル ポート、しきい値の設定 [164](#)
- レイヤ 2 プロトコルのトンネリング [159](#)
- レイヤ 3 [42, 61, 62](#)
  - モニタリング [61](#)
  - 設定例 [62](#)
- 帯域幅の設定 [49](#)
- インターフェイス MAC アドレス、設定 [53](#)
- インターフェイスでの DHCP クライアントの設定 [58](#)
- インターフェイスの速度 [8, 21](#)
  - イーサネット インターフェイス [8](#)
  - 設定 [21](#)
- インターフェイス情報、表示 [36](#)
  - レイヤ 2 [36](#)

## か

- ガイドライン [91](#)
  - IP トンネル [91](#)

## さ

- サブインターフェイス [43, 48, 49](#)
  - 設定 [48](#)
  - 帯域幅の設定 [49](#)

## た

- ダウンリンク遅延 [16](#)

## ち

- チャンネル モード [74, 80](#)
  - ポート チャンネル [74, 80](#)

## て

- ディセーブル化 [25, 29, 32, 35, 142](#)
  - CDP [29](#)
  - error-disabled リカバリ [32](#)
  - vPC [142](#)
  - イーサネット インターフェイス [35](#)
  - リンク ネゴシエーション [25](#)
- デバウンス タイマー [13](#)
  - パラメータ [13](#)
- デバウンス タイマー、設定 [33](#)
  - イーサネット インターフェイス [33](#)
- デフォルト インターフェイス [13](#)
- デフォルト設定 [45, 93](#)
  - IP トンネル [93](#)
  - レイヤ 3 インターフェイス [45](#)

## と

- トンネル インターフェイス [45, 96, 99](#)
  - PBR に基づく設定 [96](#)
  - VRF メンバーシップ、割り当て [99](#)
- トンネル インターフェイス、作成 [94](#)
  - インターフェイス [94](#)

## は

- バド ノード [107](#)
- パラメータ、概要 [13](#)
  - デバウンス タイマー [13](#)

## ふ

- 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 [106](#)

## ほ

- ポイントツーポイント IP-in-IP のカプセル化およびカプセル化解除 [90](#)
- ポート チャネリング [66](#)
- ポート チャンネル [49, 65, 67, 68, 72, 75, 76, 77, 78, 80, 85, 87, 151](#)
  - LACP [72](#)
  - LACP がイネーブルとスタティック [75](#)
  - STP [65](#)

## ポートチャネル (続き)

- vPC への移行 [151](#)
- チャネルモード [80](#)
- ポートの追加 [77](#)
- ロードバランシング [68, 78](#)
  - ポートチャネル [68](#)
- 機能の履歴 [87](#)
- 互換性要件 [67](#)
- 作成 [76](#)
- 設定の確認 [85](#)
- 帯域幅の設定 [49](#)

ポートチャネル、MinLink [76, 82](#)LACP [76, 82](#)ポートモード [9, 19](#)interface [19](#)ポートの追加 [77](#)ポートチャネル [77](#)

## ま

マルチキャストグループへの VNI のマッピング [118](#)マルチポイント IP-in-IP のカプセル化解除 [90](#)

## も

モニタリング [61](#)レイヤ3 インターフェイス [61](#)

## ゆ

ユニキャストルーティングプロトコルの設定 [115](#)

## ら

ライセンス要件 [45, 91](#)IP トンネル [91](#)レイヤ3 インターフェイス [45](#)ランデブーポイントの設定 [113](#)

## る

ルーテッドインターフェイス [42, 47, 49](#)設定 [47](#)帯域幅の設定 [49](#)ループバック インターフェイス [44, 51](#)設定 [51](#)

## れ

レイヤ2 [11, 26, 36](#)SVI 自動ステート [11](#)SVI 自動ステート、ディセーブル化 [26](#)インターフェイス情報、表示 [36](#)レイヤ2 プロトコルトンネル [163](#)インターフェイス [163](#)レイヤ2 プロトコルのトンネリング [159](#)インターフェイス [159](#)レイヤ3 インターフェイス [42, 45, 47, 58, 61, 62, 63, 64](#)MIB [64](#)インターフェイス [63, 64](#)レイヤ3 [63, 64](#)MIB [64](#)関連資料 [63](#)機能の履歴 [64](#)規格 [64](#)デフォルト設定 [45](#)モニタリング [61](#)ライセンス要件 [45](#)ルーテッドインターフェイスの設定 [47](#)確認 [58](#)関連資料 [63](#)機能の履歴 [64](#)規格 [64](#)設定例 [62](#)注意事項と制約事項 [45](#)

## ろ

ロードバランシング [78](#)ポートチャネル [78](#)設定 [78](#)