



## **Cisco Nexus 3548 スイッチ NX-OS インターフェイス構成ガイド、リリース 10.3(x)**

初版：2022年8月19日

最終更新：2022年8月26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。

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS REFERENCED IN THIS DOCUMENTATION ARE SUBJECT TO CHANGE WITHOUT NOTICE. EXCEPT AS MAY OTHERWISE BE AGREED BY CISCO IN WRITING, ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS DOCUMENTATION ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED.

The Cisco End User License Agreement and any supplemental license terms govern your use of any Cisco software, including this product documentation, and are located at: <http://www.cisco.com/go/softwareterms>. Cisco product warranty information is available at <http://www.cisco.com/go/warranty>. US Federal Communications Commission Notices are found here <http://www.cisco.com/c/en/us/products/us-fcc-notice.html>.

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

Any products and features described herein as in development or available at a future date remain in varying stages of development and will be offered on a when-and-if-available basis. Any such product or feature roadmaps are subject to change at the sole discretion of Cisco and Cisco will have no liability for delay in the delivery or failure to deliver any products or feature roadmap items that may be set forth in this document.

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

The documentation set for this product strives to use bias-free language. For the purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com go trademarks](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. (1721R)

© 2022 Cisco Systems, Inc. All rights reserved.



## 目次

---

はじめに :

はじめに	xi
対象読者	xi
表記法	xi
マニュアルに関するフィードバック	xiii

---

第 1 章

新機能と変更情報	1
新機能と変更情報	1

---

第 2 章

レイヤ 2 インターフェイスの設定	3
ライセンス要件	3
イーサネット インターフェイスの概要	3
インターフェイス コマンド	3
40 Gbps インターフェイスの速度について	4
UDLD パラメータ	4
UDLD のデフォルト設定	5
UDLD アグレッシブ モードと非アグレッシブ モード	6
SVI 自動ステート	6
Cisco Discovery Protocol	7
CDP のデフォルト設定	7
errordisable ステート	8
MTU 設定	9
デバウンス タイマー パラメータについて	9
レイヤ 2 インターフェイスのガイドラインおよび制約事項	9
イーサネット インターフェイスの設定	10

UDLD モードの設定	10
インターフェイスの速度の設定	12
40 ギガビット インターフェイス速度の設定	13
リンク ネゴシエーションのディセーブル化	14
SVI 自動ステートのディセーブル化	15
CDP 特性の設定	17
CDP のイネーブル化またはディセーブル化	18
errdisable ステート検出のイネーブル化	19
error-disable ステート回復のイネーブル化	20
error-disable ステート回復間隔の設定	21
説明パラメータの設定	22
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	22
デバウンス タイマーの設定	23
レイヤ 2 インターフェイス設定の確認	24
インターフェイス情報の表示	25
物理イーサネットのデフォルト設定	27
レイヤ 2 インターフェイスの MIB	28

## 第 3 章

<b>レイヤ 3 インターフェイスの設定</b>	<b>29</b>
レイヤ 3 インターフェイスについて	29
ルーテッド インターフェイス	29
サブインターフェイス	30
VLAN インターフェイス	31
ループバック インターフェイス	32
レイヤ 3 インターフェイスの注意事項および制約事項	32
レイヤ 3 インターフェイスのデフォルト設定	32
レイヤ 3 インターフェイスの設定	33
ルーテッド インターフェイスの設定	33
サブインターフェイスの設定	34
インターフェイスでの帯域幅の設定	35
VLAN インターフェイスの設定	36

ループバック インターフェイスの設定	37
VRF へのインターフェイスの割り当て	38
レイヤ3 インターフェイス設定の確認	39
レイヤ3 インターフェイスのモニタリング	41
レイヤ3 インターフェイスの設定例	42
レイヤ3 インターフェイスの関連資料	43
レイヤ3 インターフェイスの MIB	43
レイヤ3 インターフェイスの標準	43

---

## 第 4 章

### ポート チャネルの設定 45

ポート チャネルについて	45
ポート チャネルの概要	45
互換性要件	46
ポート チャネルを使ったロード バランシング	48
LACP について	50
LACP の概要	50
LACP ID パラメータ	50
チャンネル モード	51
LACP マーカー レスポンダ	52
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	53
LACP ポート チャネルの MinLink	53
ポート チャネルの設定	53
ポート チャネルの作成	53
ポート チャネルへのポートの追加	54
ポート チャネルを使ったロード バランシングの設定	56
LACP のイネーブル化	57
ポートに対するチャンネル モードの設定	57
LACP ポートチャネルの MinLink の設定	59
LACP 高速タイマー レートの設定	60
LACP のシステム プライオリティおよびシステム ID の設定	61
LACP ポート プライオリティの設定	62

ポートチャネル設定の確認	63
ロードバランシング発信ポート ID の確認	64

## 第 5 章

## 仮想ポートチャネルの設定 67

vPC について	67
vPC の概要	67
用語	68
vPC の用語	68
vPC ドメイン	69
ピアキープアライブリンクとメッセージ	70
vPC ピアリンクの互換パラメータ	71
同じでなければならない設定パラメータ	72
同じにすべき設定パラメータ	73
タイプ 1 の不整合チェックの表示	73
VLAN ごとの整合性検査	74
vPC 自動リカバリ	74
vPC ピアリンク	75
vPC ピアリンクの概要	75
vPC 番号	76
その他の機能との vPC の相互作用	77
vPC と LACP	77
vPC ピアリンクと STP	77
CFSOE	78
vPC ピアスイッチ	78
VRF に関する注意事項と制約事項	79
vPC 設定の確認	80
グレースフルタイプ 1 検査ステータスの表示	80
グローバルタイプ 1 不整合の表示	81
インターフェイス別タイプ 1 不整合の表示	82
VLAN ごとの整合性ステータスの表示	83
vPC のデフォルト設定	85

vPC の設定	86	
vPC のイネーブル化	86	
vPC のディセーブル化	87	
vPC ドメインの作成	87	
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	89	
vPC ピア リンクの作成	92	
設定の互換性の検査	93	
vPC 自動リカバリのイネーブル化	94	
復元遅延時間の設定	95	
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	96	
VRF 名の設定	97	
他のポート チャネルの vPC への移行	98	
vPC ドメイン MAC アドレスの手動での設定	99	
システム プライオリティの手動での設定	100	
vPC ピア スイッチのロールの手動による設定	101	
レイヤ 3 vPC 経路の設定	102	
第 6 章	スタティックおよびダイナミック NAT 変換の設定	105
	ネットワーク アドレス変換の概要	105
	スタティック NAT に関する情報	106
	ダイナミック NAT の概要	108
	タイムアウトメカニズム	109
	NAT の内部アドレスおよび外部アドレス	110
	ダイナミック NAT のプール サポート	111
	スタティックおよびダイナミック Twice NAT の概要	111
	スタティック NAT の注意事項および制約事項	112
	ダイナミック NAT の制約事項	113
	ダイナミック Twice NAT の注意事項および制約事項	114
	スタティック NAT の設定	114
	スタティック NAT のイネーブル化	114
	インターフェイスでのスタティック NAT の設定	115

内部送信元アドレスのスタティック NAT のイネーブル化	116
外部送信元アドレスのスタティック NAT のイネーブル化	117
内部送信元アドレスのスタティック PAT の設定	118
外部送信元アドレスのスタティック PAT の設定	118
スタティック Twice NAT の設定	119
スタティック NAT および PAT の設定例	121
例：スタティック Twice NAT の設定	122
スタティック NAT の設定の確認	122
ダイナミック NAT の設定	123
ダイナミック変換および変換タイムアウトの設定	123
ダイナミック NAT プールの設定	126
送信元リストの設定	127
内部送信元アドレスのダイナミック Twice NAT の設定	129
外部送信元アドレスのダイナミック Twice NAT の設定	130
ダイナミック NAT 変換のクリア	132
ダイナミック NAT の設定の確認	132
NAT 統計情報の確認	134
NAT 統計情報のクリア	134
例：ダイナミック変換および変換タイムアウトの設定	135
VRF 対応 NAT に関する情報	136
VRF 対応 NAT の設定	136

## 第 7 章

<b>IP イベント減衰の設定</b>	<b>139</b>
IP イベント減衰	139
IP イベント減衰の概要	140
インターフェイス状態変化イベント	140
抑制しきい値	140
半減期	140
再使用しきい値	141
最大抑制時間	141
関連コンポーネント	141



ルートのタイプ	141
サポートされているプロトコル	142
IP イベント減衰の設定方法	142
IP イベント減衰のイネーブル化	142
IP イベント減衰の確認	143





## はじめに

---

ここでは、次の内容について説明します。

- [対象読者, on page xi](#)
- [表記法 \(xi ページ\)](#)
- [マニュアルに関するフィードバック \(xiii ページ\)](#)

## 対象読者

本書は、Cisco Nexus デバイスの設定と保守を行う、ネットワーク管理者を対象としています。

## 表記法



- (注) お客様のニーズを満たすためにドキュメントを更新するという継続的な取り組みの一環として、シスコでは設定タスクの文書化方法を変更しました。そのため、本ドキュメントには、従来とは異なるスタイルでの設定タスクが説明されている部分もあります。ドキュメントに新たに組み込まれるようになったセクションは、新しい表記法に従っています。

コマンドの説明には、次のような表記法が使用されます。

表記法	説明
<b>bold</b>	太字の文字は、表示どおりにユーザが入力するコマンドおよびキーワードです。
<i>italic</i>	イタリック体の文字は、ユーザが値を入力する引数です。
[x]	省略可能な要素（キーワードまたは引数）は、角かっこで囲んで示しています。
[x   y]	いずれか1つを選択できる省略可能なキーワードや引数は、角カッコで囲み、縦棒で区切って示しています。

表記法	説明
{x y}	必ずいずれか1つを選択しなければならない必須キーワードや引数は、波かっこで囲み、縦棒で区切って示しています。
[x {y z}]	角かっこまたは波かっこが入れ子になっている箇所は、任意または必須の要素内の任意または必須の選択肢であることを表します。角かっこ内の波かっこと縦棒は、省略可能な要素内で選択すべき必須の要素を示しています。
variable	ユーザが値を入力する変数であることを表します。イタリック体が使用できない場合に使用されます。
string	引用符を付けない一組の文字。 <b>string</b> の前後には引用符を使用しません。引用符を使用すると、その引用符も含めて <b>string</b> とみなされます。

例では、次の表記法を使用しています。

表記法	説明
screen フォント	スイッチが表示する端末セッションおよび情報は、スクリーンフォントで示しています。
太字の screen フォント	ユーザが入力しなければならない情報は、太字のスクリーンフォントで示しています。
イタリック体の screen フォント	ユーザが値を指定する引数は、イタリック体の screen フォントで示しています。
<>	パスワードのように出力されない文字は、山カッコ (<>) で囲んで示しています。
[]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!、#	コードの先頭に感嘆符 (!) またはポンド記号 (#) がある場合には、コメント行であることを示します。

このマニュアルでは、次の表記法を使用しています。



(注) 「注釈」です。役立つ情報やこのマニュアルに記載されていない参照資料を紹介しています。



注意 「要注意」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

## マニュアルに関するフィードバック

このマニュアルに関する技術的なフィードバック、または誤りや記載もれなどお気づきの点がございましたら、HTML ドキュメント内のフィードバックフォーム () よりご連絡ください。

ご協力をよろしくお願いいたします。





# 第 1 章

## 新機能と変更情報

- [新機能と変更情報 \(1 ページ\)](#)

## 新機能と変更情報

表 1: NX-OS リリース 10.3(x) の新機能および変更された機能

機能	説明	変更が行われたリリース	参照先
NA	このリリースで追加された新機能はありません。	10.3(1)F	該当なし







## 第 2 章

# レイヤ 2 インターフェイスの設定

- [ライセンス要件 \(3 ページ\)](#)
- [イーサネット インターフェイスの概要, on page 3](#)
- [レイヤ 2 インターフェイスのガイドラインおよび制約事項 \(9 ページ\)](#)
- [イーサネット インターフェイスの設定 \(10 ページ\)](#)
- [レイヤ 2 インターフェイス設定の確認 \(24 ページ\)](#)
- [インターフェイス情報の表示, on page 25](#)
- [物理イーサネットのデフォルト設定, on page 27](#)
- [レイヤ 2 インターフェイスの MIB \(28 ページ\)](#)

## ライセンス要件

Cisco NX-OS ライセンス方式の推奨の詳細と、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。

## イーサネット インターフェイスの概要

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

イーサネット インターフェイスはデフォルトでイネーブルです。

## インターフェイス コマンド

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

- インターフェイス タイプ：物理イーサネット インターフェイスには、常にキーワード **ethernet** を使用します。
- スロット番号：

- スロット1にはすべての固定ポートが含まれます。
  - スロット2には上位拡張モジュールのポートが含まれます（実装されている場合）。
  - スロット3には下位拡張モジュールのポートが含まれます（実装されている場合）。
  - スロット4には下位拡張モジュールのポートが含まれます（実装されている場合）。
- ポート番号：グループ内のポート番号。

Cisco Nexus ファブリック エクステンダ との併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。

## 40 Gbpsインターフェイスの速度について

最大12のインターフェイスで40ギガビット/秒 (Gbps) の速度を有効にできます。4つの隣接ポートのグループの最初のポートで40 Gbpsの速度をイネーブルにします。たとえば、ポートグループ1～4のポート1、ポートグループ5～8のポート5、ポートグループ9～12のポート9で40 Gbpsの速度を有効にします。40 Gbpsポート番号は、イーサネットインターフェイスの1/1、1/5、1/9、1/13、1/17、などです。

設定は、グループ内の残りの3つのポートではなく、最初のポートに適用します。残りのポートは、拡張 Small Form-Factor Pluggable (SFP+) トランシーバが挿入されていないポートと同様に機能します。設定を保存すると、すぐに有効になります。スイッチをリロードする必要はありません。

SFP+ トランシーバのセキュリティチェックは、グループの最初のポートでのみ実行されます。

## 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グループをはじめ、さまざまな問題を引き起こす可能性があります。

UDLD は、レイヤ1プロトコルと協調してリンクの物理ステータスを検出するレイヤ2プロトコルです。レイヤ1では、オートネゴシエーションは物理シグナリングと障害検出を行います。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

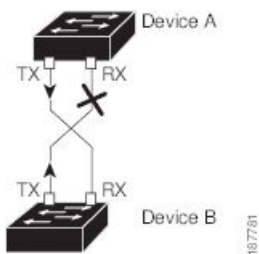
の両方をイネーブルにすると、レイヤ1とレイヤ2の検出が協調して動作して、物理的な単一方向接続と論理的な単一方向接続を防止し、その他のプロトコルの異常動作を防止できます。

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。対になったファイバケーブルのうち一方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ると、そのリンクのアップ状態は維持されなくなります。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が立てられ、その LAN ポートはシャットダウンされます。UDLD プロトコルにより単方向リンクが正しく識別されその使用が禁止されるようにするためには、リンクの両端のデバイスで UDLD がサポートされている必要があります。

次の図は、単方向リンクが発生した状態の一例を示したものです。デバイス B はこのポートでデバイス A からのトラフィックを正常に受信していますが、デバイス A は同じポート上でデバイス B からのトラフィックを受信していません。UDLD によって問題が検出され、ポートがディセーブルになります。

Figure 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。

Table 2: 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

機能	デフォルト値
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)	有効 (Enabled)

## UDLD アグレッシブ モードと非アグレッシブ モード

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

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

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

- リンク的一方にポート 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。

## 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 インターフェイスが VLAN で複数のポートを有する場合、SVI は VLAN のすべてのポートがダウンすると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、1つの VLAN の SVI がブリッジングリンクと同じデバイスに存在する場合、2つの VLAN 間のブリッジングをサポートしません。デバイスに着信し、SVI に向かうトラフィックは、IPv4 廃棄としてドロップされます。これは、BIA MAC アドレスが VLAN/SVI 間で共有され、SVI の MAC を変更するオプションがないためです。

## 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。CDP を使用すれば、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。アドバタイズには、存続可能時間（保持時間）や情報も含まれています。これは、受信側のデバイスが CDP 情報を破棄せずに保持する時間の長さです。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。

**Table 3: 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	有効
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	有効 (Enabled)

## errordisable ステート

あるインターフェイスが **errdisable** ステートであるというのは、そのインターフェイスが管理上は (**no shutdown** コマンドにより) イネーブルになっていながら、実行時に何らかのプロセスによってディセーブルになっていることを指します。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、そのインターフェイスは管理上イネーブルであるため、そのステータスは **errdisable** として表示されます。いったんインターフェイスが **errdisable** ステートになったら、手動で再イネーブル化する必要があります。あるいは、自動タイムアウト回復値を設定しておくこともできます。**errdisable** 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。

**errdisable** の特定の原因に対する **errdisable** 自動回復タイムアウトを設定する場合は、**time** 変数の値を変更します。

**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。

インターフェイスが **errdisable** からリカバリしないようにするには、**no errdisable recovery cause** コマンドを使用します。

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

- **all** : すべての原因からの回復タイマーをイネーブル化します。
- **bpduguard** : ブリッジプロトコルデータユニット (BPDU) ガードの **errdisable** ステートからの回復タイマーをイネーブル化します。
- **failed-port-state** : スパニング ツリー プロトコル (STP) のポート設定状態障害からの回復タイマーをイネーブル化します。
- **link-flap** : リンクステート フラッピングからの回復タイマーをイネーブル化します。
- **pause-rate-limit** : ポーズレートリミットの **errdisable** ステートからの回復タイマーをイネーブル化します。
- **udld** : 単方向リンク検出 (UDLD) の **errdisable** ステートからの回復タイマーをイネーブル化します。
- **loopback** : ループバック **errdisable** ステートからの回復タイマーをイネーブル化します。

特定の原因に対し、**errdisable** からの回復をイネーブルにしなかった場合、**errdisable** ステートは、**shutdown** および **no shutdown** コマンドを入力するまで続きます。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。

## MTU 設定

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。MTU を変更する場合は、クラスマップおよびポリシーマップを設定します。



**Note** 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に 1500 というデフォルトの MTU が表示されます。

## デバウンス タイマー パラメータについて

# レイヤ2 インターフェイスのガイドラインおよび制約事項

- 40 Gbpsイーサネット インターフェイスは、次の機能をサポートしていません。
  - スイッチド ポート アナライザ (SPAN)
  - Encapsulated Remote Switched Port Analyzer (ERSPAN)
  - ワープ SPAN
  - プライベート仮想ローカル エリア ネットワーク (PVLAN)
  - アクティブ バッファ モニタリング
  - 遅延モニタリング
  - リンク レベル フロー制御
  - 高精度時間プロトコル (PTP)
  - 40 Gbpsインターフェイス設定後のイメージのダウングレード
  - コンフィギュレーション ロールバック
- インターフェイスで 40 Gbps のインターフェイス速度を設定した場合、CLI は最初のポートをアップとして、残りの3つのポートをダウンとして表示します。4つのリンクのいずれかがダウンしている場合、CLIはすべてのリンクをダウンとして表示します。

# イーサネットインターフェイスの設定

ここでは、次の内容について説明します。

## 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。



**Note** 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。

### SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **feature udld**
3. switch(config)# **no feature udld**
4. switch(config)# **show udld global**
5. switch(config)# **interface type slot/port**
6. switch(config-if)# **udld {enable | disable | aggressive}**
7. switch(config-if)# **show udld interface**

### DETAILED STEPS

	Command or Action	Purpose
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 udld</b>	デバイスの UDLD をイネーブルにします。
ステップ 3	switch(config)# <b>no feature udld</b>	デバイスの UDLD をディセーブルにします。
ステップ 4	switch(config)# <b>show udld global</b>	デバイスの UDLD ステータスを表示します。
ステップ 5	switch(config)# <b>interface type 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。



	Command or Action	Purpose
ステップ 6	switch(config-if)# <b>udld</b> {enable   disable   aggressive}	ノーマルUDLDモードをイネーブルにするか、UDLDをディセーブルにするか、またはアグレッシブUDLDモードをイネーブルにします。
ステップ 7	switch(config-if)# <b>show udld interface</b>	インターフェイスの UDLD ステータスを表示します。

### Example

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
```

## インターフェイスの速度の設定



(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、**show interface ethernet slot/port** コマンドを入力すると、SFP 検証失敗メッセージが表示されます。たとえば、**speed 1000** コマンドを設定しないで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。

### 手順の概要

1. switch# **configure terminal**
2. switch(config)# **interface type slot/port**
3. switch(config-if)# **speed speed**

### 手順の詳細

	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 type slot/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>speed speed</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>• 自動</li> </ul>

### 例

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
```

## 40 ギガビット インターフェイス速度の設定

### 始める前に

40 Gbps のポート速度を実現するには、隣接するポートグループの4つのポートにそれぞれ 10 Gbps SFP を取り付ける必要があります。4つの SFP+ はすべて 10 Gbps の速度に対応し、同じタイプのポートである必要があります。デフォルトでは、すべてのポートが 10 Gbps ポートです。

### 手順の概要

1. switch# **configure terminal**
2. switch(config)# **interface** *type slot/port-range*
3. switch(config-if-rang)# **shut**
4. switch(config-if-rang)# **exit**
5. switch(config-if)# **interface** *type slot/port*
6. switch(config-if)# **speed 40000**
7. switch(config-if)# **no shut**

### 手順の詳細

	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>type slot/port-range</i>	指定した範囲のインターフェイスで、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switch(config-if-rang)# <b>shut</b>	指定したインターフェイスの範囲をシャットダウンします。
ステップ 4	switch(config-if-rang)# <b>exit</b>	現在のコンフィギュレーション モードを終了します。
ステップ 5	switch(config-if)# <b>interface</b> <i>type slot/port</i>	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。4つの隣接ポートグループの最初のポートを指定して、そのポートを 40 Gbps の速度に設定します。たとえば、インターフェイスグループ 1/1～1/4の最初のポートであるインターフェイス 1/1 を指定すると、そのポートは 40 Gbps の速度に設定されます。

	コマンドまたはアクション	目的
		(注) 4つの隣接ポートすべてに、10 Gbps イーサネット SFP トランシーバを取り付ける必要があります。
ステップ 6	switch(config-if)# <b>speed 40000</b>	インターフェイス速度を 40 Gbps に設定します。
ステップ 7	switch(config-if)# <b>no shut</b>	インターフェイスの範囲を起動します。

### 例

次に、イーサネットインターフェイス 1/33 で速度を 40 ギガビット/秒に設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/33-36
switch(config-if-rang)# shut
switch(config-if-rang)# exit
switch(config)# interface ethernet 1/33
switch(config-if)# speed 40000
switch(config-if)# no shut
```

## リンク ネゴシエーションのディセーブル化

**no negotiate auto** コマンドを使用することにより、リンク ネゴシエーションをディセーブルにすることができます。デフォルトの場合、自動ネゴシエーションは1ギガビットポートではイネーブル、10ギガビットポートではディセーブルです。**no negotiate auto** コマンドは、全二重設定の 100M ポートでサポートされます。

このコマンドの機能は、Cisco IOS の **speed non-negotiate** コマンドと同等です。



(注) 自動ネゴシエーションの設定は、10ギガビットポートに適用されません。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
```

### 手順の概要

1. switch# **configure terminal**
2. switch(config)# **interface ethernet slot/port**
3. switch(config-if)# **no negotiate auto**
4. (任意) switch(config-if)# **negotiate auto**

## 手順の詳細

	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	(任意) switch(config-if)# <b>negotiate auto</b>	<p>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 ポートに対してはデフォルトでイネーブルです。</p> <p>(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。</p>

## 例

次の例は、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) に対して自動ネゴシエーションをイネーブルにする方法を示したものです。

```
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。

## 手順の概要

1. switch# **configure terminal**
2. switch(config)# **feature interface-vlan**
3. switch(config)# **system default interface-vlan [no] autostate**
4. (任意) switch(config)# **interface vlan interface-vlan-number**
5. (任意) switch(config-if)# **[no] autostate**
6. (任意) switch(config)# **show interface-vlan interface-vlan**
7. (任意) switch(config)# **copy running-config startup-config**

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	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	必須: 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	(任意) switch(config)# <b>interface vlan interface-vlan-number</b>	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	(任意) switch(config-if)# <b>[no] autostate</b>	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。
ステップ 6	(任意) switch(config)# <b>show interface-vlan interface-vlan</b>	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	(任意) switch(config)# <b>copy running-config startup-config</b>	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。

## 例

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.ee40.a17c
MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec
```

## CDP 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。

### SUMMARY STEPS

1. switch# **configure terminal**
2. (Optional) switch(config)# [**no**] **cdp advertise** {v1 | v2 }
3. (Optional) switch(config)# [**no**] **cdp format device-id** {mac-address | serial-number | system-name}
4. (Optional) switch(config)# [**no**] **cdp holdtime** seconds
5. (Optional) switch(config)# [**no**] **cdp timer** seconds

### DETAILED STEPS

	Command or Action	Purpose
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	(Optional) switch(config)# [ <b>no</b> ] <b>cdp advertise</b> {v1   v2 }	使用するバージョンを設定して、CDP アドバタイズメントを送信します。バージョン2がデフォルトステートです。  デフォルト設定に戻すには、このコマンドの <b>no</b> 形式を使用します。
ステップ 3	(Optional) switch(config)# [ <b>no</b> ] <b>cdp format device-id</b> {mac-address   serial-number   system-name}	CDP デバイス ID のフォーマットを設定します。デフォルトはシステム名です。完全修飾ドメイン名で表すことができます。  デフォルト設定に戻すには、このコマンドの <b>no</b> 形式を使用します。
ステップ 4	(Optional) switch(config)# [ <b>no</b> ] <b>cdp holdtime</b> seconds	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	(Optional) switch(config)# [ <b>no</b> ] <b>cdp timer</b> seconds	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。

	Command or Action	Purpose
		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。

### Example

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 のイネーブル化またはディセーブル化

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。

### SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **interface type slot/port**
3. switch(config-if)# **cdp enable**
4. switch(config-if)# **no cdp enable**

### DETAILED STEPS

	Command or Action	Purpose
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 type slot/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>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。
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。



### Example

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。これにより、インターフェイスで原因が検出されると、そのインターフェイスは errdisable ステートになります。この errdisable ステートは、リンクダウンステートに類似した動作ステートです。

### 手順の概要

1. switch# **configure terminal**
2. switch(config)# **errdisable detect cause** {all / link-flap / loopback}
3. switch(config)# **shutdown**
4. switch(config)# **no shutdown**
5. switch(config)# **show interface status err-disabled**
6. (任意) switch(config)# **copy running-config startup-config**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	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</b> {all / link-flap / loopback}	インターフェイスを errdisable 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 errdisable ステートから手動で回復させる場合は、このコマンドを最初に入力します。
ステップ 4	switch(config)# <b>no shutdown</b>	インターフェイスを管理的にアップし、errdisable 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>	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。

	コマンドまたはアクション	目的
ステップ 6	(任意) <code>switch(config)# copy running-config startup-config</code>	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。

### 例

次の例は、いずれの場合にも `errdisable` ステート検出をイネーブルにする方法を示したものです。

```
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
```

## error-disable ステート回復のイネーブル化

インターフェイスが `errdisable` ステートから回復して再びアップ状態になるようにアプリケーションを設定することができます。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)。

### 手順の概要

1. `switch# configure terminal`
2. `switch(config)# errdisable recovery cause {all | uidd | bpduguard | link-flap | failed-port-state | pause-rate-limit | loopback}`
3. `switch(config)# show interface status err-disabled`
4. (任意) `switch(config)# copy running-config startup-config`

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<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)# errdisable recovery cause {all   uidd   bpduguard   link-flap   failed-port-state   pause-rate-limit   loopback}</code>	インターフェイスが <code>errdisable</code> 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	<code>switch(config)# show interface status err-disabled</code>	<code>errdisable</code> 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 4	(任意) switch(config)# <b>copy running-config startup-config</b>	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。

### 例

次の例は、いずれの条件に対しても errdisable ステート回復をイネーブルにする方法を示したものです。

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

## error-disable 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。

### 手順の概要

1. switch# **configure terminal**
2. switch(config)# **errdisable recovery interval interval**
3. switch(config)# **show interface status err-disabled**
4. (任意) switch(config)# **copy running-config startup-config**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	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 interval</b>	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	(任意) switch(config)# <b>copy running-config startup-config</b>	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。

### 例

次の例は、いずれの条件の下でも `errdisable` ステート回復をイネーブルにする方法を示したものです。

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

## 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。

### SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **interface** *type slot/port*
3. switch(config-if)# **description** *test*

### DETAILED STEPS

	Command or Action	Purpose
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>type slot/port</i>	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</b> <i>test</i>	インターフェイスの説明を指定します。

### Example

次の例は、インターフェイスの説明を「Server 3 Interface」に設定する方法を示したものです。

```
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。この情報は、すべてのダイナ

ミック ルーティング プロトコルを通じて、他のネットワーク サーバに伝達されます。シャットダウンされたインターフェイスは、どのルーティング アップデートにも含まれません。

## SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **interface type slot/port**
3. switch(config-if)# **shutdown**
4. switch(config-if)# **no shutdown**

## DETAILED STEPS

	Command or Action	Purpose
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 type slot/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。

### Example

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
```

## デバウンス タイマーの設定

イーサネットのデバウンスタイマーは、デバウンス時間（ミリ秒単位）を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100 msに設定されており、デバウンス タイマーは動作しません。



(注) リンク デバウンス機能は、10G および 40G インターフェイスでのみ使用できます。

**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。

### 手順の概要

1. switch# **configure terminal**
2. switch(config)# **interface type slot/port**
3. switch(config-if)# **link debounce time milliseconds**

### 手順の詳細

	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 type slot/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 time milliseconds</b>	指定した時間 (1 ~ 5,000 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。

### 例

次の例は、イーサネット インターフェイスでデバウンス タイマーをイネーブルにして、デバウンス時間を 1000 ミリ秒に設定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 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
```

## レイヤ2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 ethernet slot/port brief</b>	レイヤ2インターフェイスの動作ステータスを表示します。  (注) インターフェイスに 40 Gbps のインターフェイス速度が設定されていて、リンクがアップしている場合、CLI は最初のポートをアップとして、残りの3つのポートをダウンとして表示します。4つのリンクのいずれかがダウンしている場合、CLI はすべてのリンクをダウンとして表示します。

## 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 interface type slot/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 interface type slot/port capabilities</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しか使用できません。
switch# <b>show interface type slot/port transceiver</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しか使用できません。
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。

**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します。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 100000000 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（出力の一部を割愛してあります）。

```
switch# show interface brief
```

```
-----
Ethernet      VLAN   Type Mode   Status Reason          Speed   Port
Interface                                           Ch #
-----
Eth1/1        200   eth  trunk up      none            10G(D) --
Eth1/2        1     eth  trunk up      none            10G(D) --
Eth1/3        300   eth  access down SFP not inserted 10G(D) --
Eth1/4        300   eth  access down SFP not inserted 10G(D) --
Eth1/5        300   eth  access down Link not connected 1000(D) --
Eth1/6        20    eth  access down Link not connected 10G(D) --
Eth1/7        300   eth  access down SFP not inserted 10G(D) --
...

```

次に、CDP ネイバーを表示する例を示します。

```
switch# show cdp neighbors
```

```
Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute

Device ID         Local Intrfce   Hldtme  Capability  Platform  Port ID
d13-dist-1       mgmt0          148     S I         WS-C2960-24TC Fas0/9
n5k(FLC12080012) Eth1/5         8       S I s       N5K-C5020P-BA Eth1/5

```

## 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
デュプレックス	オート（全二重）
カプセル化	ARPA
MTU <sup>1</sup>	1500 バイト
ポートモード	アクセス（Access）
スピード	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

## レイヤ2インターフェイスの MIB

MIB	MIB のリンク
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

- [レイヤ 3 インターフェイスについて \(29 ページ\)](#)
- [レイヤ 3 インターフェイスの注意事項および制約事項 \(32 ページ\)](#)
- [レイヤ 3 インターフェイスのデフォルト設定 \(32 ページ\)](#)
- [レイヤ 3 インターフェイスの設定 \(33 ページ\)](#)
- [レイヤ 3 インターフェイス設定の確認 \(39 ページ\)](#)
- [レイヤ 3 インターフェイスのモニタリング \(41 ページ\)](#)
- [レイヤ 3 インターフェイスの設定例 \(42 ページ\)](#)
- [レイヤ 3 インターフェイスの関連資料 \(43 ページ\)](#)
- [レイヤ 3 インターフェイスの MIB \(43 ページ\)](#)
- [レイヤ 3 インターフェイスの標準 \(43 ページ\)](#)

## 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、パケットを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。

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。

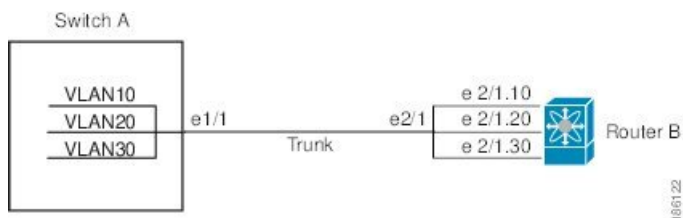
サブインターフェイスの名前は、親インターフェイスの名前（たとえば Ethernet 2/1）+ピリオド（.）+そのインターフェイス独自の番号です。たとえば、イーサネット インターフェイス 2/1 に Ethernet 2/1.1 というサブインターフェイスを作成できます。この場合、.1 はそのサブインターフェイスを表します。

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 E2/1 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有効にすると、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。

この設定では、事前に VLAN ネットワーク インターフェイス機能を有効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。

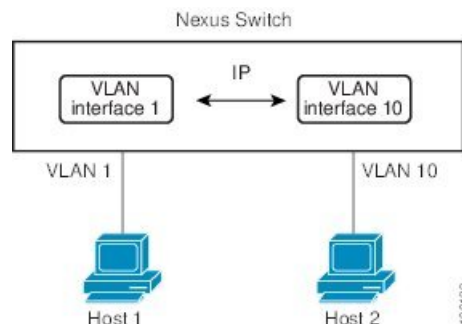


(注) VLAN 1 の VLAN インターフェイスは削除できません。

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接続した 2つの VLAN



## 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シングル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 インターフェイスを通過するパケットは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。

## 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。

- 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。

## 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。

# 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

### 手順の概要

1. switch# **configure terminal**
2. switch(config)# **interface ethernet slot/port**
3. switch(config-if)# **no switchport**
4. switch(config-if)# **ipip-address/length**
5. (任意) switch(config-if)# **medium {broadcast | p2p}**
6. (任意) switch(config-if)# **show interfaces**
7. (任意) switch(config-if)# **copy running-config startup-config**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	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。
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>ipip-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	(任意) switch(config-if)# <b>medium {broadcast   p2p}</b>	インターフェイス メディアをポイントツーポイントまたはブロードキャストのどちらかとして設定します。  (注) デフォルト設定は broadcast であり、この設定はどの <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。

	コマンドまたはアクション	目的
ステップ6	(任意) <code>switch(config-if)# show interfaces</code>	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	(任意) <code>switch(config-if)# copy running-config startup-config</code>	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。

### 例

次の例は、IPv4 ルートが設定されたレイヤ3インターフェイスの設定方法を示したものです。

```
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

### 始める前に

- 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。
- このポートチャンネル上にサブインターフェイスを作成するには、ポートチャンネルインターフェイスを作成します。

### 手順の概要

1. (任意) `switch(config-if)# copy running-config startup-config`
2. `switch(config)# interface ethernet slot/port.number`
3. `switch(config-if)# ip address ip-address/length`
4. `switch(config-if)# encapsulation dot1Q vlan-id`
5. (任意) `switch(config-if)# show interfaces`
6. (任意) `switch(config-if)# copy running-config startup-config`

### 手順の詳細

	コマンドまたはアクション	目的
ステップ1	(任意) <code>switch(config-if)# copy running-config startup-config</code>	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。



	コマンドまたはアクション	目的
ステップ 2	switch(config)# <b>interface ethernet</b> <i>slot/port.number</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。 <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>ip address</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。
ステップ 4	switch(config-if)# <b>encapsulation dot1Q</b> <i>vlan-id</i>	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。 <i>vlan-id</i> の範囲は 2 ~ 4093 です。
ステップ 5	(任意) switch(config-if)# <b>show interfaces</b>	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	(任意) switch(config-if)# <b>copy running-config startup-config</b>	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。

### 例

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。

### 手順の概要

1. switch# **configure terminal**
2. switch(config)# **interface ethernet** *slot/port*
3. switch(config-if)# **bandwidth** [*value* | **inherit** [*value*]]
4. (任意) switch(config-if)# **copy running-config startup-config**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	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 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>	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、次のよう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	(任意) switch(config-if)# <b>copy running-config startup-config</b>	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。

### 例

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

### 手順の概要

1. switch# **configure terminal**
2. switch(config)# **feature interface-vlan**
3. switch(config)# **interface vlan number**
4. switch(config-if)# **ip address ip-address/length**
5. switch(config-if)# **no shutdown**
6. (任意) switch(config-if)# **show interface vlan number**
7. (任意) switch(config-if)# **copy running-config startup-config**

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	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> の範囲は 1 ~ 4094 です。
ステップ 4	switch(config-if)# <b>ip 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	(任意) switch(config-if)# <b>show interface vlan number</b>	VLAN インターフェイスの統計情報を表示します。 <i>number</i> の範囲は 1 ~ 4094 です。
ステップ 7	(任意) switch(config-if)# <b>copy running-config startup-config</b>	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。

## 例

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

## 始める前に

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。

## 手順の概要

1. switch# **configure terminal**
2. switch(config)# **interface loopback instance**
3. switch(config-if)# **ip address ip-address/length**
4. (任意) switch(config-if)# **show interface loopback instance**
5. (任意) switch(config-if)# **copy running-config startup-config**

## VRFへのインターフェイスの割り当て

## 手順の詳細

	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 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	(任意) switch(config-if)# <b>show interface loopback instance</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。 <i>instance</i> の範囲は 0 ~ 1023 です。
ステップ 5	(任意) switch(config-if)# <b>copy running-config startup-config</b>	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。

## 例

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

## 始める前に

VRF 用のインターフェイスを設定したあとで、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。

## 手順の概要

1. switch# **configure terminal**
2. switch(config)# **interface interface-typenumber**
3. switch(config-if)# **vrf member vrf-name**
4. switch(config-if)# **ip ip-address/length**
5. (任意) switch(config-if)# **show vrf [vrf-name] interface interface-type number**
6. (任意) switch(config-if)# **show interfaces**
7. (任意) switch(config-if)# **copy running-config startup-config**

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	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 interface-typenumber</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-if)# <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-if)# <b>ipip-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。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	(任意) switch(config-if)# <b>show vrf [vrf-name] interface interface-type number</b>	VRF 情報を表示します。
ステップ 6	(任意) switch(config-if)# <b>show interfaces</b>	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	(任意) switch(config-if)# <b>copy running-config startup-config</b>	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。

## 例

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
```

## 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 ethernet slot/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の、5分間指数減少移動平均を含む）を表示します。

コマンド	目的
<b>show interface ethernet <i>slot/port</i> brief</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 ethernet <i>slot/port</i> capabilities</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 ethernet <i>slot/port</i> description</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 ethernet <i>slot/port</i> status</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 ethernet <i>slot/port.number</i></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 <i>channel-id.number</i></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の、5分間指数減少移動平均を含む）を表示します。
<b>show interface loopback <i>number</i></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 loopback <i>number</i> brief</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 loopback <i>number</i> description</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 loopback <i>number</i> status</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。
<b>show interface vlan <i>number</i></b>	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。
<b>show interface vlan <i>number</i> brief</b>	VLAN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 vlan <i>number</i> description</b>	VLANインターフェイスの説明を表示します。

コマンド	目的
<b>show interface vlan <i>number</i> status</b>	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>show interface ethernet <i>slot/port</i> 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 <i>slot/port</i> counters brief</b>	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。
<b>show interface ethernet <i>slot/port</i> counters detailed [all]</b>	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 <i>slot/port</i> 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 <i>slot/port</i> 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 <i>slot/port.number</i> counters</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 <i>channel-id.number</i> counters</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。
<b>show interface loopback <i>number</i> counters</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。

コマンド	目的
<b>show interface loopback <i>number</i> counters 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 loopback <i>number</i> counters 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 vlan <i>number</i> counters</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 vlan <i>number</i> counters 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パケットおよびバイトカウンタをすべて含めることができます（ユニキャストおよびマルチキャスト）。
<b>show interface vlan <i>counters snmp</i></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)# ip address 192.0.2.1/8
switch(config-if)# copy running-config startup-config
```

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
```

## 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 3548 Switch NX-OS Interfaces Command Reference
IP	<i>Cisco Nexus 3548 NX-OS Unicast Routing Configuration Guide</i> の「Configuring IP」の章
VLAN	<i>Cisco Nexus 3548 NX-OS Layer 2 Switching Configuration Guide</i> の「Configuring VLANs」の章

## レイヤ3インターフェイスの MIB

MIB	MIB のリンク
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。 <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>
CISCO-IF-EXTENSION-MIB	
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。





## 第 4 章

# ポート チャンネルの設定

- [ポート チャンネルについて, on page 45](#)
- [ポート チャンネルの設定 \(53 ページ\)](#)
- [ポート チャンネル設定の確認, on page 63](#)
- [ロードバランシング発信ポート ID の確認 \(64 ページ\)](#)

## ポート チャンネルについて

ポートチャンネルは、複数のインターフェイスを1つのグループにバンドルしたもので、帯域幅を広げ冗長性を高めることができます。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。ポートチャン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、そのポートチャンネルは動作しています。

ポートチャンネルは、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 ポートチャンネルのほか、Link Aggregation Control Protocol (LACP) を実行するポートチャン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ンネルに適用すると、そのポートチャン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ンネルに設定すると、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ン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 ポートチャンネルを使用すれば、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、ポートチャン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。

### Related Topics

[LACP の概要 \(50 ページ\)](#)

## ポート チャンネルの概要

Cisco NX-OS は、ポートチャンネルを使用することにより、広い帯域幅、冗長性、チャン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ことができるほか、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, on page 48](#)を参照してください。



**Note** 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、かつ全二重方式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。



**Note** 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。



**Note** 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。メンバー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
- スピード
- 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

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。

チャンネル 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、チャンネル 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
- Debounce

**channel-group force** コマンドを使用して、ポートをチャン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追加されると、次のパラメータは削除され、代わってポートチャネルに関する値が指定されます。ただしこの変更は、インターフェイスに関する実行中の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
  - Debounce
  - 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。

すべてのレイヤ2、レイヤ3、およびレイヤ4フレームのデフォルトのポートチャネルロードバランスのパラメータは、送信元と宛先の IP アドレスだけです。この基準は、**port-channel load-balance ethernet** コマンドを使用して変更できます。MACアドレスにのみ起因するロードバランシングは、レイヤ2パケットヘッダーで Ethertype が 0800 に設定されていないときのみ行われます。Ethertype が 0800 の場合、コマンドラインに定義されているポートチャネルのロードバランシングパラメータに関係なく IP パケットヘッダー内の IP アドレスに基づいてロードバランシングが引き継がれます。さらに、パケットが Ethertype 0800 であり有効な IP アドレスがない場合は、このパケットは解析エラーのフラグが付けられた後でドロップされます。

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

**Table 4:** ポートチャネルにおけるロードバランシングの基準

設定 (Configuration)	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
宛先 IP (Destination IP)	宛先 MAC	宛先 MAC、宛先 IP	宛先 MAC、宛先 IP
Source IP	送信元 MAC	送信元 MAC、送信元 IP	送信元 MAC、送信元 IP
送信元/宛先 IP	送信元/宛先 MAC	送信元/宛先 MAC、送信元/宛先 IP	送信元/宛先 MAC、送信元/宛先 IP
宛先 TCP/UDP ポート	宛先 MAC	宛先 MAC、宛先 IP	宛先 MAC、宛先 IP、宛先ポート
送信元 TCP/UDP ポート	送信元 MAC	送信元 MAC、送信元 IP	送信元 MAC、送信元 IP、送信元ポート
送信元/宛先 TCP/UDP ポート	送信元/宛先 MAC	送信元/宛先 MAC、送信元/宛先 IP	送信元/宛先 MAC、送信元/宛先 IP、送信元/宛先ポート

使用している設定で最も多様なバランス基準を提供するオプションを使用してください。たとえば、ポートチャネルのトラフィックが1つのMACアドレスにだけ送られ、ポートチャネルでのロードバランシングの基準としてその宛先MACアドレスが使用されている場合、ポー

トチャネルでは常にそのポートチャネル内の同じリンクが選択されます。したがって、送信元アドレスまたはIPアドレスを使用すると、結果的により優れたロードバランシングが行われることになります。

ユニキャストおよびマルチキャストトラフィックは、**show port-channel load-balancing** コマンド出力に表示される設定済みのロードバランシングアルゴリズムに基づいて、ポートチャネルリンク間でロードバランシングが行われます。

## LACP について

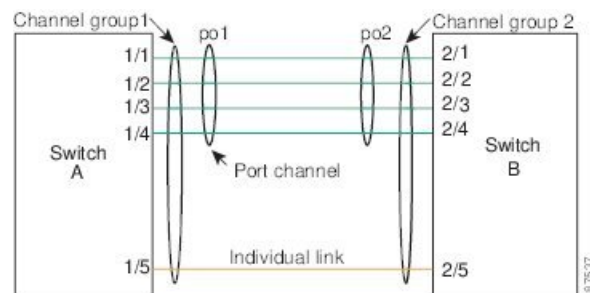
### LACP の概要



**Note** LACP 機能を設定して使用する場合は、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。

**Figure 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。



**Note** 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。



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

- **LACP ポートプライオリティ** : LACP を使用するように設定された各ポートには、LACP ポートプライオリティが割り当てられます。デフォルト値である 32768 をそのまま使用するか、1 ~ 65535 の範囲で値を設定できます。LACP では、ポートプライオリティおよびポート番号によりポート ID が構成されます。また、互換性のあるポートのうち一部を束ねることができない場合に、どのポートをスタンバイモードにし、どのポートをアクティブモードにするかを決定するのに、ポートプライオリティを使用します。LACP では、ポートプライオリティ値が大きいほど、プライオリティは低くなります。指定ポートが、より低い LACP プライオリティを持ち、ホットスタンバイリンクではなくアクティブリンクとして選択される可能性が最も高くなるように、ポートプライオリティを設定できます。
- **LACP 管理キー** : LACP は、LACP を使用するように設定された各ポート上のチャン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

## チャンネルモード

ポートチャネルの個別インターフェイスは、チャン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、そのチャンネルモードは常に 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、各チャンネルの 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ンネルモードを active または passive に設定します。LACP チャンネルグループを構成する個々のリンクについて、どちらかのチャンネルモードを設定できます。



**Note** active または passive のチャンネルモードで、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化する必要があります。

次の図は、チャンネルモードをまとめたものです。

Table 5: 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 によって on 状態のインターフェイスとネゴシエートする場合、LACP パケットを受信しないため、そのインターフェイスと個別のリンクを形成します。つまり、LACP チャネルグループには参加しません。

passive と active のどちらのモードでも、ポート速度やトランキングステートなどの基準に基づいてポートチャネルを構成可能かどうかを判定するため、LACP によるポート間のネゴシエーションが行われます。passive モードは、リモートシステム、つまり、パートナーが、LACP をサポートしているかどうか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正常にポートチャネルを形成できます。
- 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нда

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нда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。

**Table 6: 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	該当なし
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 ポートチャネルでだけ動作します。デバイスでは非 LACP ポートチャネルでも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。



**Note** 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。

## SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **interface port-channel** *channel-number*
3. switch(config)# **no interface port-channel** *channel-number*

## DETAILED STEPS

	Command or Action	Purpose
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-channel</b> <i>channel-number</i>	設定するポートチャネルインターフェイスを指定し、インターフェイスコンフィギュレーションモードを開始します。範囲は 1 ~ 4096 です。チャネルグループがまだ存在していなければ、Cisco NX-OS によって自動的に作成されます。
ステップ 3	switch(config)# <b>no interface port-channel</b> <i>channel-number</i>	ポートチャネルを削除し、関連するチャネルグループを削除します。

### Example

次の例は、ポートチャネルの作成方法を示しています。

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

## ポートチャネルへのポートの追加

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



**Note** 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。

## SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **interface** *type slot/port*
3. (Optional) switch(config-if)# **switchport mode trunk**
4. (Optional) switch(config-if)# **switchport trunk** {**allowed vlan** *vlan-id* | **native vlan** *vlan-id*}
5. switch(config-if)# **channel-group** *channel-number*
6. (Optional) switch(config-if)# **no channel-group**

## DETAILED STEPS

	Command or Action	Purpose
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>type slot/port</i>	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	(Optional) switch(config-if)# <b>switchport mode trunk</b>	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	(Optional) switch(config-if)# <b>switchport trunk</b> { <b>allowed vlan</b> <i>vlan-id</i>   <b>native vlan</b> <i>vlan-id</i> }	トランクポートに必要なパラメータを設定します。
ステップ 5	switch(config-if)# <b>channel-group</b> <i>channel-number</i>	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。ポートチャンネルがない場合は、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ンネルが作成されます。これを、暗黙的なポートチャンネル作成と言います。
ステップ 6	(Optional) switch(config-if)# <b>no channel-group</b>	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。

## Example

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。



**Note** 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。



**Note** Nexus 5672UP-16G スイッチの SAN PO メンバー間で FC トラフィックをロードバランシングする場合、**port-channel load-balance ethernet** コマンドは必要ありません。ロードバランシングはデフォルトで実行されます。

### SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **port-channel load-balance ethernet** {[**destination-ip** | **destination-mac** | **destination-port** | **source-dest-ip** | **source-dest-mac** | **source-dest-port** | **source-ip** | **source-mac** | **source-port**] | **crc-poly**}
3. (Optional) switch(config)# **no port-channel load-balance ethernet**
4. (Optional) switch# **show port-channel load-balance**

### DETAILED STEPS

	Command or Action	Purpose
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>port-channel load-balance ethernet</b> {[ <b>destination-ip</b>   <b>destination-mac</b>   <b>destination-port</b>   <b>source-dest-ip</b>   <b>source-dest-mac</b>   <b>source-dest-port</b>   <b>source-ip</b>   <b>source-mac</b>   <b>source-port</b> ]   <b>crc-poly</b> }	デバイスのロードバランシングアルゴリズムを指定します。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 <b>source-dest-mac</b> です。
ステップ 3	(Optional) switch(config)# <b>no port-channel load-balance ethernet</b>	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。
ステップ 4	(Optional) switch# <b>show port-channel load-balance</b>	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。

### Example

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
```

## 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。その後、ポートチャネルは単一のブリッジポートとしてスパニングツリーに追加されます。

### SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **feature lacp**
3. (Optional) switch(config)# **show feature**

### DETAILED STEPS

	Command or Action	Purpose
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	(Optional) switch(config)# <b>show feature</b>	イネーブルにされた機能を表示します。

### Example

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。

**Before you begin**

LACP 機能がイネーブルになっていることを確認します。

**SUMMARY STEPS**

1. switch# **configure terminal**
2. switch(config)# **interface** *type slot/port*
3. switch(config-if)# **channel-group** *channel-number* [**force**] [**mode** {**on** | **active** | **passive**}]
4. switch(config-if)# **no channel-group** *number mode*

**DETAILED STEPS**

	Command or Action	Purpose
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>type slot/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> : これを指定すると、チャネルグループに LAN ポートが強制的に追加されます。</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) すべてのポートチャネル (LACP を稼働していないポートチャネル) に対して、このモードが維持されます。</p> <p><b>passive</b> : LACP デバイスが検出された場合にのみ、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>



	Command or Action	Purpose
		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、チャンネルモードは常に on です。
ステップ 4	switch(config-if)# <b>no channel-group number mode</b>	指定インターフェイスのポートモードを on に戻します

### Example

次に、チャンネルグループ 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
```

次の例は、チャンネルグループ 5 にインターフェイスを強制的に追加する方法を示したものです。

```
switch(config)# interface ethernet 1/1
switch(config-if)# channel-group 5 force
switch(config-if)#
```

## LACP ポートチャネルの MinLink の設定

MinLink 機能は、LACP ポートチャネルでだけ動作します。デバイスでは非 LACP ポートチャネルでも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端、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でだけ **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。

### 手順の概要

1. switch# **configure terminal**
2. switch(config)# **interface port-channel number**
3. switch(config-if)# **[no] lacp min-links number**
4. (任意) switch(config)# **show running-config interface port-channel number**

### 手順の詳細

	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 port-channel number</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>no</b> ] <b>lacp min-links number</b>	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。  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	(任意) switch(config)# <b>show running-config interface port-channel number</b>	ポートチャネルの MinLink 設定を表示します。

### 例

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。

### 始める前に

LACP 機能がイネーブルになっていることを確認します。

### 手順の概要

1. switch# **configure terminal**
2. switch(config)# **interface type slot/port**
3. switch(config-if)# **lacp rate fast**

## 手順の詳細

	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 type slot/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。
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。

## 例

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。

### Before you begin

LACP 機能がイネーブルになっていることを確認します。

### SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **lacp system-priority priority**
3. (Optional) switch# **show lacp system-identifier**

## DETAILED STEPS

	Command or Action	Purpose
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	(Optional) switch# <b>show lACP system-identifier</b>	LACP システム識別子を表示します。

## Example

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。

## Before you begin

LACP 機能がイネーブルになっていることを確認します。

## SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **interface** *type slot/port*
3. switch(config-if)# **lACP port-priority** *priority*

## DETAILED STEPS

	Command or Action	Purpose
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>type slot/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、値が大きいほど

	Command or Action	Purpose
		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。

### Example

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、ポートチャネル設定情報を確認することができます。

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>interface type slot/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ー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ン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。

## 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。



(注) ワープモードでは、出力には2つの宛先ポートがあります。1つはワープテーブルに一致がない場合で、もう1つはワープテーブルに一致がある場合です。レイヤ2ポートの一致は、送信元および宛先 MAC アドレスが MAC テーブルで学習されることを意味し、レイヤ3ポートの一致は、IP アドレスが解決されたことを意味しています。

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
<b>switch# show port-channel load-balance forwarding-path interface port-channel <i>port-channel-id</i> src-interface <i>source-interface</i> vlan <i>vlan-id</i> dst-ip <i>src-ip</i> dst-mac <i>src-mac</i> l4-src-port <i>port-id</i> l4-dst-port <i>port-id</i> ether-type <i>ether-type</i> ip-proto <i>ip-proto</i></b>	発信ポート ID を表示します。

### 例

次に、ロードバランシングの発信ポート 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
```

### 例

次に、デバイスでワーブモードになっている間の **port-channel load-balance** コマンドの出力例を示します。

```
switch# show port-channel load-balance forwarding-path interface port-channel 1  
src-interface ethernet 1/6 vlan 1 src-ip 1.1.1.1 dst-ip 2.2.2.2  
Missing params will be substituted by 0's.  
Load-balance Algorithm on switch: source-dest-ip  
    Outgoing port id (no cache hit): Ethernet1/29  
    Outgoing port id (cache hit): Ethernet1/32  
Param(s) used to calculate load-balance:  
    dst-ip: 2.2.2.2  
    src-ip: 1.1.1.1  
    dst-mac: 0000.0000.0000  
    src-mac: 0000.0000.0000  
    VLAN: 1
```







## 第 5 章

# 仮想ポート チャンネルの設定

- vPC について (67 ページ)
- VRF に関する注意事項と制約事項 (79 ページ)
- vPC 設定の確認, on page 80
- vPC のデフォルト設定, on page 85
- vPC の設定 (86 ページ)

## vPC について

### vPC の概要

仮想ポートチャンネル (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ン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 デバイスを含み、Cisco Nexus ファブリック エクステンダに接続されたトポロジ内に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 チャンネルなど、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。



**Note** 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ブアライブ 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。



**Note** 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 ピアキーブアライブ リンク、vPC ピア リンク、および vPC ドメイン内にあってダウンストリーム デバイスに接続されているすべての EtherChannel チャンネルが含まれます。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。



**Note** 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 には次のような利点があります。

- 単独のデバイスが、2 つのアップストリーム デバイスを介して EtherChannel を使用できるようになります。
- スパニングツリー プロトコル (STP) のブロック ポートが不要になります。
- ループフリーなトポロジが実現されます。
- 利用可能なすべてのアップリンク帯域幅を使用します。
- リンクまたはスイッチに障害が発生した場合、高速コンバージェンスが実行されます。
- リンクレベルの復元力を提供します。
- ハイ アベイラビリティが保証されます。

## 用語

### vPC の用語

vPC で使用される用語は、次のとおりです。

- vPC : vPC ピア デバイスとダウンストリーム デバイスの間の結合された EtherChannel。
- vPC ピア デバイス : vPC ピア リンクと呼ばれる特殊な EtherChannel により接続されることで対をなす個々のデバイス。
- vPC ピアリンク : vPC ピア デバイス間の状態を同期するために使用されるリンク。
- vPC メンバ ポート : vPC に属するインターフェイス。

- vPC ドメイン：両方の vPC ピア デバイス、vPC ピア キープアライブ リンク、vPC 内にあってダウンストリーム デバイスに接続されているすべてのポートチャネルが含まれるドメイン。また、このドメインは、vPC グローバルパラメータを割り当てるために使用する必要があるコンフィギュレーション モードに関連付けられています。vPC ドメイン ID は、両スイッチで同じである必要があります。
- 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、さまざまな 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必要があります。

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。

どちらのピアにも同じ vPC ドメイン ID を設定することが推奨されます。またドメイン ID はネットワーク内で一意である必要があります。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。



**Note** 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。

ホールドタイムアウトとタイムアウト値を同時に設定できます。

**ホールドタイムアウト値**：ホールドタイムアウト値は、3 ～ 10 秒の範囲内で設定可能で、デフォルトのホールドタイムアウト値は3秒です。このタイマーは、vPC ピアリンクが停止した時点で開始します。ホールドタイムアウト期間の目的は、誤ったポジティブケースを防ぐことです。

タイムアウト値よりも小さいホールドタイムアウト値を設定すると、vPC システムは、ホールドタイムアウト期間の vPC ピアキープアライブメッセージを無視し、タイムアウト期間のリマインダに関するメッセージを考慮します。この期間にキープアライブメッセージが受信されない場合、vPC セカンダリ デバイスがプライマリ デバイスの役割を引き継ぎます。たとえば、ホールドタイムアウト値が3秒で、タイムアウト値が5秒の場合、最初の3秒間は vPC キープアライブメッセージが無視されます（ピアリンク障害後の数秒間にスーパーバイザ障害に対応する場合など）。メッセージは、残りのタイムアウト期間である2秒間は考慮されます。この期間が経過し、キープアライブメッセージがなかった場合、vPC セカンダリ デバイスがプライマリ デバイスの役割を引き継ぎます。

**タイムアウト値**：タイムアウト値の範囲は3～20秒で、デフォルト値は5秒です。このタイマーは、ホールドタイムアウト間隔が終了した時点で開始します。ホールドタイムアウト値以下のタイムアウト値を設定すると、タイムアウト期間はホールドタイムアウト期間の後に開始されます。たとえば、タイムアウト値が3秒で、ホールドタイムアウト値が5秒の場合、タイムアウト期間は5秒後に開始されます。



**Note** Cisco Nexus デバイスの vPC ピアキープアライブリンクは、管理 VRF で mgmt 0 インターフェイスを使用して実行されるように設定することが推奨されます。デフォルトの VRF を設定する場合は、vPC ピアキープアライブメッセージの伝送に vPC ピア リンクが使用されないようにしてください。

## vPC ピアリンクの互換パラメータ

多くの設定パラメータおよび動作パラメータが、vPC内のすべてのインターフェイスで同じでなければなりません。vPC機能をイネーブルにし、さらに両方のvPCピアスイッチ上でピアリンクを設定すると、シスコファブリックサービス (CFS) メッセージにより、ローカルvPCピアスイッチに関する設定のコピーがリモートvPCピアスイッチへ送信されます。これによりシステムでは、2つのスイッチ間で重要な設定パラメータに違いがないかどうか判定が行われます。

vPC内のすべてのインターフェイスで設定されている値を表示するには、**show vpc consistency-parameters** コマンドを入力します。表示される設定は、vPCピアリンクおよびvPCの稼働を制限する可能性のある設定だけです。

vPCに関する互換性チェックのプロセスは、正規のEtherChannelに関する互換性チェックとは異なります。

### vPCポートチャネルでの新しいタイプ2整合性チェック

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整合性チェックが追加されました。**show vpc consistency-check vPC <vpc no.>** のCLIは、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、ローカル値とピア値の間に不一致がある場合でもvPCは動作しますが、CLI出力から不一致が表示されることがあります。

```
switch# sh vpc consistency-parameters vpc 1112
```

Legend:

Type 1 : vPC will be suspended in case of mismatch

Name Value	Type	Local Value	Peer
----- -----	----	-----	
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, 0-23-4-ee-be-64, 8458, (8000, f4-4e-5-84-5e-3c, 457, 0, 0)], (8000, 0, 0), f4-4e-5-84-5e-3c, 457, 0, 0)]	[(fa0, 0-23-4-ee-be-64, 8458, 0-23-4-ee-be-64, 8458, (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

## 同じでなければならない設定パラメータ

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。



**Note** 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 トラフィックのタグging
- 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。



**Note** 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で、両側の vPC ピア スイッチ上の設定が一致しないと、誤設定に伴ってトラフィックフローに望ましくない動作が発生する可能性があります。

- MAC エージング タイマー
- スタティック MAC エントリ
- VLAN インターフェイス：vPC ピアリンクの両端にある各スイッチの VLAN インターフェイスは同じ VLAN 用に設定されている必要があり、さらにそれらの管理モードおよび動作モードも同じであることが必要です。ピアリンクの一方のスイッチでのみ設定されている VLAN では、vPC またはピアリンクを使用したトラフィックの転送は行われません。VLAN はすべて、プライマリ vPC スイッチとセカンダリ vPC スイッチの両方で作成する必要があります。両方で作成されていない場合、VLAN は停止することになります。
- 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 フィルタ
  - 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。

## タイプ1の不整合チェックの表示



(注) 両方の vPC ピアが同じ転送モードであることを確認する必要があります。転送モードが一致しない場合、vPC は一時停止されます。

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, 0)	(1538, 0, 0, 0, 0, 0, 0, 0)
Network QoS (Pause)	2	(F, F, F, F, F, F, F, F)	(F, F, F, F, F, F, F, F)
Network QoS (WRED)	2	(F, F, F, F, F, F, F, F)	(F, F, F, F, F, F, F, F)
Network QoS (ECN)	2	(F, F, F, F, F, F, F, F)	(F, F, F, F, F, F, F, F)
Output Queuing (Bandwidth)	2	(100, 0, 0, 0, 0, 0, 0, 0)	(100, 0, 0, 0, 0, 0, 0, 0)
Output Queuing (Absolute Priority)	2	(F, F, F, F, F, F, F, F)	(F, F, F, F, F, F, F, F)
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	1		
STP Loopguard	1	Disabled	Disabled
STP Bridge Assurance	1	Enabled	Enabled
STP Port Type, Edge BPDUGuard	1	Normal, Disabled, Disabled	Normal, Disabled, Disabled
STP MST Simulate PVST	1	Enabled	Enabled
HW profile Forwarding Mode	1	warp	warp
<<<<<<<<< Both Local and remote VPC have same forwarding mode.			
IGMP Snooping Group-Limit	2	8190	8190
Interface-vlan admin up capability	2	10	10
Interface-vlan routing capability	2	10	10
Allowed VLANs	-	10	10
Local suspended VLANs	-	-	-

## VLAN ごとの整合性検査

VLAN 上でスパニングツリーのイネーブル/ディセーブルが切り替わるたびに、いくつかのタイプ 1 整合性検査が VLAN 単位で実行されます。この整合性検査に合格しない VLAN は、プライマリスイッチおよびセカンダリスイッチでダウン状態になりますが、その他の VLAN は影響を受けません。

## vPC 自動リカバリ

次のようなシナリオでは、vPC 自動リカバリ機能によって vPC リンクは再イネーブル化されます。

両側の vPC ピアスイッチでリロードが実行され、かつ一方のスイッチのみリブートした場合、自動リカバリによってそのスイッチがプライマリスイッチとして機能し、一定時間が経過した後に vPC リンクがアップ状態になります。このシナリオにおけるリロード遅延時間は、240 ～ 3600 秒の範囲で設定できます。



ピアリンクの障害に伴ってセカンダリ vPC スイッチ上の vPC がディセーブルになり、さらにプライマリ vPC スイッチで障害が発生するか、またはトラフィックが転送できなくなると、セカンダリ スイッチでは vPC が再イネーブル化されます。このシナリオの場合、vPC ではキーブアライブが 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 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。



**Note** vPC ピア リンクを設定する場合は、あらかじめ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。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。



**Note** 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 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。



**Note** 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

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ピアリンクを作成すると、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を作成することができます。ダウンストリームスイッチ上でEtherChannelを1つだけ作成し、そのポートの半分をプライマリvPCピアスイッチ用、残りの半分をセカンダリvPCピアスイッチ用として使用します。

各vPCピアスイッチ上では、ダウンとリームスイッチに接続されたEtherChannelに同じvPC番号を割り当てます。vPCの作成時にトラフィックが中断されることはほとんどありません。設定を簡素化するため、各EtherChannelに対してそのEtherChannelと同じ番号のvPCID番号を割り当てることもできます(EtherChannel 10に対してはvPCID 10を割り当てるなど)。



**Note** 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チャンネルに割り当てる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。

## その他の機能との vPC の相互作用

### vPC と LACP

Link Aggregation Control Protocol (LACP) では、vPC ドメインのシステム MAC アドレスに基づいて、その vPC に対する LACP Aggregation Group (LAG) ID が構成されます。

LACP は、ダウンストリームスイッチからのチャネルも含め、すべての vPC EtherChannel 上で使用できます。vPC ピアスイッチの各 EtherChannel のインターフェイスに対しては、LACP をアクティブモードで設定することが推奨されます。この設定により、スイッチ、単方向リンク、およびマルチホップ接続の間の互換性をより簡単に検出できるようになり、実行時の変更およびリンク障害に対してダイナミックな応答が可能になります。

vPC ピアリンクは、16 個の EtherChannel インターフェイスをサポートしています。



**Note** 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。

### 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 over E) 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。



**Note** vPC ピア リンクの両側での設定を表示して、設定が同じであることを確認してください。vPC に関する情報を表示する場合は、**show spanning-tree** コマンドを使用します。

## CFSOE

Cisco Fabric Services over Ethernet (CFSOE) は、vPC ピア デバイスの動作を同期化するために使用される信頼性の高い状態転送メカニズムです。CFSOE は、vPC にリンクされている、STP、IGMP などの多くの機能のメッセージとパケットを伝送します。情報は、CFS/CFSOE プロトコル データ ユニット (PDU) に入れて伝送されます。

CFSOE は、vPC 機能をイネーブルにすると、デバイスによって自動的にイネーブルになります。何も設定する必要はありません。vPC の CFSOE 分散には、IP を介してまたは CFS リージョンに分散する機能は必要ありません。CFSOE 機能が vPC 上で正常に機能するために必要な設定は一切ありません。

**show mac address-table** コマンドを使用すれば、CFSOE が vPC ピア リンクのために同期する MAC アドレスを表示できます。



**Note** **no cfs eth distribute** または **no cfs distribute** コマンドは入力しないでください。vPC 機能に対しては CFSOE をイネーブルにする必要があります。vPC がイネーブルの場合にこれらのコマンドのいずれかを入力すると、エラーメッセージが表示されます。

**show cfs application** コマンドを入力すると、出力に「Physical-eth」と表示されます。これは、CFSOE を使用しているアプリケーションを表します。

## vPC ピア スイッチ

vPC ピア スイッチ機能は、STP コンバージェンスに関連するパフォーマンス上の問題を解決するために追加されました。この機能は、一対の Cisco Nexus 3500 シリーズ スイッチがレイヤ 2 トポロジ内で 1 つの STP ルートとして現れることを可能にします。この機能は、STP ルートを vPC プライマリ スイッチに固定する必要性をなくし、vPC プライマリ スイッチに障害が発生した場合の vPC コンバージェンスを向上させます。

ループを回避するために、vPC ピア リンクは STP 計算からは除外されます。vPC ピア スイッチ モードでは、ダウストリーム スイッチでの STP BPDU タイムアウトに関連した問題（この問題は、トラフィックの中断につながります）を避けるために、STP BPDU が両方の vPC ピア デバイスから送信されます。

vPC ピア スイッチは、すべてのデバイスが vPC に属する純粋なピア スイッチ トポロジと組み合わせて使用できます。



- (注) ピアスイッチは、vPCを使用するネットワークでサポートされ、STPベースの冗長性はサポートされません。ハイブリッドピアスイッチ設定でvPCピアリンクに障害が発生すると、トラフィックが失われる場合があります。このシナリオでは、vPCピアは同じSTPルートIDや同じブリッジIDを使用します。アクセススイッチのトラフィックは2つに別れ、その半分が最初のvPCピアに、残りの半分が2番目のvPCピアに転送されます。ピアリンク障害は、南北のトラフィックには影響がありませんが、東西のトラフィックが失われます。

## VRFに関する注意事項と制約事項

vPC設定時の注意事項と制限事項は次のとおりです。

- vPCはIPv6で修飾されていません。
- Cisco Nexus 3500 シリーズプラットフォームでは、VPCがWarpモードでサポートされるようになりました。
- 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。
- どちらのピアにも同じvPCドメインIDを設定することが推奨されます。またドメインIDはネットワーク内で一意であることが必要です。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。
- vPC内のLACPを使用するポートチャネルはすべて、アクティブモードのインターフェイスで設定することが推奨されます。
- 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。

- SVI の制限 : 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。

## 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# <b>show feature</b>	vPC がイネーブルかどうかを表示します。
switch# <b>show port-channel capacity</b>	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# <b>show running-config vpc</b>	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# <b>show vpc brief</b>	vPC に関する簡単な情報を表示します。
switch# <b>show vpc consistency-parameters</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。
switch# <b>show vpc peer-keepalive</b>	ピアキープアライブメッセージの情報を表示します。
switch# <b>show vpc role</b>	ピアステータス、ローカルスイッチのロール、vPC システムの MAC アドレスとシステムプライオリティ、およびローカル vPC スイッチの MAC アドレスとプライオリティを表示します。
switch# <b>show vpc statistics</b>	vPC に関する統計情報を表示します。  <b>Note</b> 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。

スイッチの出力に関する詳細については、ご使用の Cisco Nexus シリーズスイッチに関する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

```

```
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    Po1   up     1-10
-----

```

```
vPC status
```

```

-----
id   Port   Status Consistency Reason                               Active vlans
-----
20   Po20   down*  failed   Global compat check failed -
30   Po30   down*  failed   Global compat check failed -
-----

```

次に、プライマリスイッチ上の不整合ステータス（プライマリvPC上のVLANは一時停止されていない）を表示する例を示します。

```
switch(config)# show vpc
```

```
Legend:
```

```

(*) - local vPC is down, forwarding via vPC peer-link

vPC domain id          : 10
Peer status            : peer adjacency formed ok
vPC keep-alive status  : peer is alive
Configuration consistency status: failed
Per-vlan consistency status : success
Configuration consistency reason: vPC type-1 configuration incompatible - STP 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    Po1    up     1-10

vPC status
-----
id   Port   Status Consistency Reason Active vlans
--   -
20   Po20   up     failed Global compat check failed 1-10
30   Po30   up     failed Global compat check failed 1-10

```

## インターフェイス別タイプ1不整合の表示

インターフェイス別タイプ1不整合が発生すると、セカンダリスイッチのvPCポートはダウンしますが、プライマリスイッチのvPCポートはアップ状態が維持されます。次の例は、スイッチポートモードでの不一致に伴って生じたこのタイプの不整合を示したものです。

次に、セカンダリスイッチ上の一時停止されたvPC VLANのステータスを表示する例を示します。

```

switch(config-if)# show vpc brief
Legend:
(*) - local vPC is down, forwarding via vPC peer-link

vPC domain id          : 10
Peer status            : peer adjacency formed ok
vPC keep-alive status  : peer is alive
Configuration consistency status: success
Per-vlan consistency status : success
Type-2 consistency status : success
vPC role                : secondary
Number of vPCs configured : 2
Peer Gateway           : Disabled
Dual-active excluded VLANs : -
Graceful Consistency Check : Enabled

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
```

```
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。

### 例

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
```

## VLAN ごとの整合性ステータスの表示

```
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
```

```
vPC Peer-link status
```

```
-----
id  Port  Status Active vlans
--  ---  -
1   Po1   up    1-10
-----
```

```
vPC status
```

```
-----
id  Port      Status Consistency Reason          Active vlans
-----
20  Po20      up    success    success    1-10
30  Po30      up    success    success    1-10
-----
```

**no spanning-tree vlan 5** コマンドを実行することにより、プライマリ VLAN とセカンダリ VLAN との間に不整合が生じます。

```
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
```

```
vPC Peer-link status
```

```
-----
id  Port  Status Active vlans
--  ---  -
1   Po1   up    1-4,6-10
-----
```

```
vPC status
```

```
-----
id  Port      Status Consistency Reason          Active vlans
-----
20  Po20      up    success    success    1-4,6-10
30  Po30      up    success    success    1-4,6-10
-----
```

次に、プライマリスイッチ上の VLAN ごとの整合ステータスを Failed として表示する例を示します。

```
switch(config)# show vpc brief
Legend:
          (*) - local vPC is down, forwarding via vPC peer-link

vPC domain id          : 10
Peer status            : peer adjacency formed ok
vPC keep-alive status  : peer is alive
Configuration consistency status: success
Per-vlan consistency status : failed
Type-2 consistency status : success
vPC role                : primary
Number of vPCs configured : 2
Peer Gateway           : Disabled
Dual-active excluded VLANs : -
Graceful Consistency Check : Enabled

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
```

次の例では、STP Disabled という不整合が表示されています。

```
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                      1    success                0-4095
BPDUFilter, Edge BPDUGuard              1    success                0-4095
STP MST Simulate PVST                    1    success                0-4095
Pass Vlans                               -    -                      0-4,6-4095
```

## vPC のデフォルト設定

次の表は、vPC パラメータのデフォルト設定をまとめたものです。

Table 7: デフォルト vPC パラメータ

パラメータ	デフォルト
vPC システム プライオリティ	32667
vPC ピアキープアライブ メッセージ	ディセーブル
vPC ピアキープアライブ間隔	1 秒
vPC ピアキープアライブ タイムアウト	5 秒
vPC ピアキープアライブ UDP ポート	3200

## vPC の設定

### vPC のイネーブル化

vPC を設定して使用する場合は、事前に vPC 機能をイネーブルにしておく必要があります。

#### SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **feature vpc**
3. (Optional) switch# **show feature**
4. (Optional) switch# **copy running-config startup-config**

#### DETAILED STEPS

	Command or Action	Purpose
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	(Optional) switch# <b>show feature</b>	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	(Optional) switch# <b>copy running-config startup-config</b>	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。

#### Example

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。



**Note** vPC 機能をディセーブルにすると、Cisco Nexus デバイス はすべての vPC 設定をクリアします。

### SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **no feature vpc**
3. (Optional) switch# **show feature**
4. (Optional) switch# **copy running-config startup-config**

### DETAILED STEPS

	Command or Action	Purpose
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	(Optional) switch# <b>show feature</b>	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	(Optional) switch# <b>copy running-config startup-config</b>	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。

### Example

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。

**Before you begin**

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。

**SUMMARY STEPS**

1. switch# **configure terminal**
2. switch(config)# **vpc domain domain-id**
3. switch(config-vpc-domain)# **fast-convergence**
4. (Optional) switch# **show vpc brief**
5. (Optional) switch# **copy running-config startup-config**

**DETAILED STEPS**

	Command or Action	Purpose
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。  <b>Note</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(config-vpc-domain)# <b>fast-convergence</b>	vPC 最適化機能をイネーブルにします。vPC 最適化機能を無効にするには、 <b>[no] fast-convergence</b> コマンドを使用します。高速コンバージェンスを実現するには、両方の vPC ピアで CLI を有効にする必要があります。
ステップ 4	(Optional) switch# <b>show vpc brief</b>	各 vPC ドメインに関する要約情報を表示します。
ステップ 5	(Optional) switch# <b>copy running-config startup-config</b>	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。

**Example**

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
```

次に、高速コンバージェンス設定のグローバルレベルタイプ2整合性チェックを適用する例を示します。

```
switch# show vpc consistency-parameters global
```

Legend:

Type 1 : vPC will be suspended in case of mismatch

Name	Type	Local Value	Peer Value
Vlan to Vn-segment Map	1	No Relevant Maps	No Relevant Maps
QoS	2	([], [], [], [], [], [], [], [])	([], [], [], [], [], [], [], [])
Network QoS (MTU)	2	(1538, 0, 0, 0, 0, 0, 0, 0, 0, 0)	(1538, 0, 0, 0, 0, 0, 0, 0, 0, 0)
VTP pruning status	2	Disabled	Disabled
IGMP Snooping Group-Limit	2	8000	8000
Fast Convergence	2	Enable	Enable
Interface-vlan admin up	2	101-120	
Interface-vlan routing capability	2	1,101-120	1
Allowed VLANs	-	-	-
Local suspended VLANs	-	-	-

## 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 IP アドレスと宛先の 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仮想ルーティングおよび転送 (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。



**Note** vPC ピアキープアライブリンクを使用する際は、個別の VRF インスタンスを設定して、各 vPC ピアスイッチからその VRF インスタンスにレイヤ3ポートを接続することが推奨されます。ピアリンク自体を使用してvPCピアキープアライブメッセージを送信しないでください。

### Before you begin

vPC 機能が有効なことを確認します。

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。

## SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **vpc domain** *domain-id*
3. switch(config-vpc-domain)# **peer-keepalive destination** *ipaddress* [**hold-timeout** *secs* | **interval** *msecs* {**timeout** *secs*} | **precedence** {*prec-value* | **network** | **internet** | **critical** | **flash-override** | **flash** | **immediate** | **priority** | **routine**} | **tos** {*tos-value* | **max-reliability** | **max-throughput** | **min-delay** | **min-monetary-cost** | **normal**} | **tos-byte** *tos-byte-value*} | **source** *ipaddress* | **vrf** {*name* | **management** | **vpc-keepalive**}]
4. (Optional) switch(config-vpc-domain)# **vpc peer-keepalive destination** *ipaddress* **source** *ipaddress*
5. (Optional) switch# **show vpc peer-keepalive**
6. (Optional) switch# **copy running-config startup-config**

## DETAILED STEPS

	Command or Action	Purpose
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-timeout</b> <i>secs</i>   <b>interval</b> <i>msecs</i> { <b>timeout</b> <i>secs</i> }   <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>source</b> <i>ipaddress</i>   <b>vrf</b> { <i>name</i>   <b>management</b>   <b>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。  <b>Note</b> 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	(Optional) switch(config-vpc-domain)# <b>vpc peer-keepalive destination</b> <i>ipaddress</i> <b>source</b> <i>ipaddress</i>	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	(Optional) switch# <b>show vpc peer-keepalive</b>	キープアライブメッセージのコンフィギュレーションに関する情報を表示します。
ステップ 6	(Optional) switch# <b>copy running-config startup-config</b>	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。



## Example

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。

### Before you begin

vPC 機能が有効なことを確認します。

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。

### SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **interface port-channel** *channel-number*
3. switch(config-if)# **vpc peer-link**
4. (Optional) switch# **show vpc brief**
5. (Optional) switch# **copy running-config startup-config**

### DETAILED STEPS

	Command or Action	Purpose
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-channel</b> <i>channel-number</i>	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	(Optional) switch# <b>show vpc brief</b>	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	(Optional) switch# <b>copy running-config startup-config</b>	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。

### Example

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 パラメータでタイプ 2 整合性検査がサポートされています。

- 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。

### 手順の概要

1. switch# show vpc consistency-parameters {global|interface port-channel channel-number}

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# show vpc consistency-parameters {global interface port-channel channel-number}	すべての vPC インターフェイス全体で一貫している必要があるパラメータのステータスを表示します。

### 例

次の例は、すべての vPC インターフェイスの間で必須設定の互換性が保たれているかチェックする方法を示します。

```
switch# show vpc consistency-parameters global
Legend:
      Type 1 : vPC will be suspended in case of mismatch
Name           Type  Local Value           Peer Value
-----
QoS                2      ([], [], [], [], [],  ([], [], [], [], [],
                    [])
Network QoS (MTU)  2      (1538, 0, 0, 0, 0, 0)  (1538, 0, 0, 0, 0, 0)
Network QoS (Pause)  2      (F, F, F, F, F, F)    (1538, 0, 0, 0, 0, 0)
Input Queuing (Bandwidth)  2      (100, 0, 0, 0, 0, 0)  (100, 0, 0, 0, 0, 0)
```

```

Input Queuing (Absolute Priority) 2 (F, F, F, F, F, F) (100, 0, 0, 0, 0, 0)
Output Queuing (Bandwidth) 2 (100, 0, 0, 0, 0, 0) (100, 0, 0, 0, 0, 0)
Output Queuing (Absolute Priority) 2 (F, F, F, F, F, F) (100, 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 1
STP Loopguard 1 Disabled Disabled
STP Bridge Assurance 1 Enabled Enabled
STP Port Type, Edge BPDUGuard 1 Normal, Disabled, Disabled Normal, 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

### 手順の概要

1. switch# **configure terminal**
2. switch(config)# **vpc domain domain-id**
3. switch(config-vpc-domain)# **auto-recovery reload-delay delay**

### 手順の詳細

	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。

### 例

次の例は、vPC ドメイン 10 で自動リカバリ機能をイネーブルにし、遅延時間を 240 秒に設定する方法を示したものです。

```

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
```

次の例は、vPC ドメイン 10 における自動リカバリ機能のステータスを表示する方法を示したものです。

```
switch(config-vpc-domain)# show running-config vpc
!Command: show running-config vpc
!Time: Tue Dec 7 02:38:44 2010

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、バックアップからの vPC の回復を遅らせるようにリストア 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始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。

### 始める前に

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。

### 手順の概要

1. switch# **configure terminal**
2. switch(config)# **vpc domain domain-id**
3. switch(config-vpc-domain)# **delay restore time**
4. (任意) switch# **copy running-config startup-config**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	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。

	コマンドまたはアクション	目的
		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。値の範囲は 1 ～ 3600 です。デフォルトは 30 秒です。
ステップ 4	(任意) switch# <b>copy running-config startup-config</b>	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。

### 例

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) が一時停止されます。また、vPC セカンダリ スイッチのすべての VLAN に対して、レイヤ 3 転送はすべてディセーブルになります。ただし、特定の SVI インターフェイスを一時停止の対象から除外することができます。

### 始める前に

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。

### 手順の概要

1. switch# **configure terminal**
2. switch(config)# **vpc domain domain-id**
3. switch(config-vpc-domain)# **dual-active exclude interface-vlan range**

### 手順の詳細

	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。

	コマンドまたはアクション	目的
ステップ 3	switch(config-vpc-domain)# <b>dual-active exclude interface-vlan range</b>	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。値の範囲は 1 ~ 4094 です。

### 例

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。

### 手順の概要

1. switch# **ping ipaddress vrf vrf-name**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# <b>ping ipaddress vrf vrf-name</b>	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。

### 例

次の例は、vpc\_keepalive という名前の VRF を指定する方法を示したものです。

```
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
```

## 他のポートチャンネルの vPC への移行

### Before you begin

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。

### SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **interface port-channel** *channel-number*
3. switch(config-if)# **vpc** *number*
4. (Optional) switch# **show vpc brief**
5. (Optional) switch# **copy running-config startup-config**

### DETAILED STEPS

	Command or Action	Purpose
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-channel</b> <i>channel-number</i>	vPC に配置してダウンストリームスイッチに接続するポートチャンネルを選択し、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。  <b>Note</b> vPC は、通常のポートチャンネル上（物理 vPC トポロジ）およびポートチャンネルのホストインターフェイス上（ホストインターフェイスの vPC トポロジ）で設定できます。
ステップ 3	switch(config-if)# <b>vpc</b> <i>number</i>	選択したポートチャンネルを 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ンネルに割り当てる 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。



	Command or Action	Purpose
ステップ 4	(Optional) switch# <b>show vpc brief</b>	各 vPC に関する情報を表示します。
ステップ 5	(Optional) switch# <b>copy running-config startup-config</b>	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。

### Example

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



**Note** システム アドレスの設定を行うかどうかは任意です。

### Before you begin

vPC 機能が有効なことを確認します。

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。

### SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **vpc domain domain-id**
3. switch(config-vpc-domain)# **system-mac mac-address**
4. (Optional) switch# **show vpc role**
5. (Optional) switch# **copy running-config startup-config**

### DETAILED STEPS

	Command or Action	Purpose
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>	スイッチ上にある既存の vPC ドメインを選択するか、または新規の vPC ドメインを作成して、vpc-domain コンフィギュレーションモードを開始し

	Command or Action	Purpose
		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	(Optional) switch# <b>show vpc role</b>	vPC システムの MAC アドレスを表示します。
ステップ 5	(Optional) switch# <b>copy running-config startup-config</b>	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。

### Example

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。

### Before you begin

vPC 機能が有効なことを確認します。

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。

### SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **vpc domain** *domain-id*
3. switch(config-vpc-domain)# **system-priority** *priority*
4. (Optional) switch# **show vpc brief**
5. (Optional) switch# **copy running-config startup-config**

### DETAILED STEPS

	Command or Action	Purpose
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。

	Command or Action	Purpose
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、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。
ステップ 3	switch(config-vpc-domain)# <b>system-priority</b> <i>priority</i>	指定した vPC ドメインに割り当てるシステム優先度を入力します。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	(Optional) switch# <b>show vpc brief</b>	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	(Optional) switch# <b>copy running-config startup-config</b>	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。

### Example

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ブ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 が再び稼働しても、機能のロールは元に戻りません。

### Before you begin

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。

## SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **vpc domain domain-id**
3. switch(config-vpc-domain)# **role priority priority**
4. (Optional) switch# **show vpc brief**
5. (Optional) switch# **copy running-config startup-config**

## DETAILED STEPS

	Command or Action	Purpose
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>	スイッチ上にある既存の vPC ドメインを選択するか、または新規の vPC ドメインを作成して、vpc-domain コンフィギュレーションモードを開始します。 <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 priority</b>	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	(Optional) switch# <b>show vpc brief</b>	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	(Optional) switch# <b>copy running-config startup-config</b>	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。

## Example

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
```

## レイヤ 3 vPC 経路の設定

始める前に

- vPC 機能をイネーブルにしていることを確認します。
- 正しい VDC を使用していることを確認します（または `switchto vdc` コマンドを使用します）。

- 両方のピアでvPC経由のレイヤ3でのピアゲートウェイとピアルーティングを有効にします。
- ピアリンクがアップしていることを確認します

vPC ピア デバイスおよび汎用レイヤ3 デバイスの間でルーティングプロトコルの隣接関係が必要な場合は、相互接続に物理的にルーティングされたインターフェイスを使用する必要があります。vPC ピアゲートウェイ機能の使用では、この要件は変わりません。

- vPC 機能をイネーブルにしていることを確認します。
- 正しい VDC を使用していることを確認します（または `switchto vdc` コマンドを使用します）。
- vPC を介したレイヤ3のピアゲートウェイとピアルーティングは、両方のピアで有効になります。
- ピアリンクがアップし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)#vpc domain domain-id</code>	デバイス上に vPC ドメインを作成し、設定目的で <code>vpc-domain</code> コンフィギュレーションモードを開始します。デフォルトはありません。指定できる範囲は 1 ~ 1000 です。
ステップ 3	<code>switch(config-vpc-domain)# peer-gateway</code>	ピアのゲートウェイ MAC アドレスを宛先とするパケットのレイヤ3 フォワーディングをイネーブルにします。
ステップ 4	<code>switch(config-vpc-domain)# layer3 peer-router</code>	両方のピアとのピアリング隣接関係を形成するためレイヤ3 デバイスを有効にします。  (注) 両方のピアでこのコマンドを設定します。
ステップ 5	<code>switch(config-vpc-domain)#exit</code>	vpc-domain 設定モードを終了します。
ステップ 6	(任意) <code>switch# show vpc brief</code>	各 vPC ドメインに関する要約情報を表示します。  (注) [Operational Layer3 Peer-router] フィールドは、レイヤ3 ピアルータが両方の vPC ノードで設定されている場合にのみ有効と表示されます。

	コマンドまたはアクション	目的
ステップ7	(任意) switch# <b>copy running-config startup-config</b>	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。

### 例

次に、Layer 3 over vPC を設定する例を示します。

```
switch# configure terminal
switch(config)# vpc domain 2
switch(config-vpc-domain)# peer-gateway
switch(config-vpc-domain)# layer3 peer-router
switch(config-vpc-domain)# exit
switch(config)#
```

次に、Layer 3 over vPC が設定されているかどうかを確認する例を示します。

```
switch(config)# show vpc brief
vPC domain id : 2
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 : 7
Peer Gateway : Enabled
Peer gateway excluded VLANs : -
Dual-active excluded VLANs : 502
Graceful Consistency Check : Enabled
Operational Layer3 Peer-router : Enabled
Auto-recovery status : Disabled

vPC Peer-link status
-----
id Port Status Active vlans
-----
1 Po300 up 1,300,400-403,500-503

vPC Status
-----
id Port Status Consistency Reason Active vlans
-----
1 Po400 up success success 400
2 Po500 up success success 500
3 Po401 up success success 401
4 Po402 up success success 402
5 Po403 up success success 1
6 Po501 up success success 501
7 Po502 up success success 502

switch(config)#
```



## 第 6 章

# スタティックおよびダイナミック NAT 変換の設定

- [ネットワーク アドレス変換の概要 \(105 ページ\)](#)
- [スタティック NAT に関する情報 \(106 ページ\)](#)
- [ダイナミック NAT の概要 \(108 ページ\)](#)
- [タイムアウトメカニズム \(109 ページ\)](#)
- [NAT の内部アドレスおよび外部アドレス \(110 ページ\)](#)
- [ダイナミック NAT のプール サポート \(111 ページ\)](#)
- [スタティックおよびダイナミック Twice NAT の概要 \(111 ページ\)](#)
- [スタティック NAT の注意事項および制約事項 \(112 ページ\)](#)
- [ダイナミック NAT の制約事項 \(113 ページ\)](#)
- [ダイナミック Twice NAT の注意事項および制約事項 \(114 ページ\)](#)
- [スタティック NAT の設定 \(114 ページ\)](#)
- [ダイナミック NAT の設定 \(123 ページ\)](#)
- [VRF 対応 NAT に関する情報 \(136 ページ\)](#)
- [VRF 対応 NAT の設定 \(136 ページ\)](#)

## ネットワーク アドレス変換の概要

ネットワークアドレス変換 (NAT) は、登録されていない IP アドレスを使用してインターネットへ接続するプライベート IP インターネットワークをイネーブルにします。NAT はデバイス (通常、2 つのネットワークを接続するもの) で動作し、パケットを別のネットワークに転送する前に、社内ネットワークの (グローバルに一意のアドレスではなく) プライベート IP アドレスを正規の IP アドレスに変換します。NAT は、ネットワーク全体に対して 1 つの IP アドレスだけを外部にアドバタイズするように設定できます。この機能により、1 つの IP アドレスの後ろに内部ネットワーク全体を効果的に隠すことで、セキュリティが強化されます。

NAT が設定されたデバイスには、内部ネットワークと外部ネットワークのそれぞれに接続するインターフェイスが少なくとも 1 つずつあります。標準的な環境では、NAT はスタブ ドメインとバックボーンの間の出ルータに設定されます。パケットがドメインから出て行くと、NAT はローカルで意味のある送信元 アドレスをグローバルで一意のアドレスに変換しま

す。パケットがドメインに入ってくる際は、NAT はグローバルに一意的な宛先アドレスをローカルアドレスに変換します。出口点が複数存在する場合、個々の NAT は同じ変換テーブルを持っている必要があります。

NAT は RFC 1631 に記述されています。

## スタティック NAT に関する情報

スタティック ネットワーク アドレス変換 (NAT) を使用すると、ユーザは内部ローカルアドレスから外部グローバルアドレスへの 1 対 1 変換を設定することができます。これにより、内部から外部トラフィックおよび外部から内部トラフィックへの IP アドレスとポート番号の両方の変換が可能になります。Cisco Nexus デバイスはヒットレス NAT をサポートします。これは、既存の NAT トラフィック フローに影響を与えずに NAT 設定で NAT 変換を追加または削除できることを意味します。

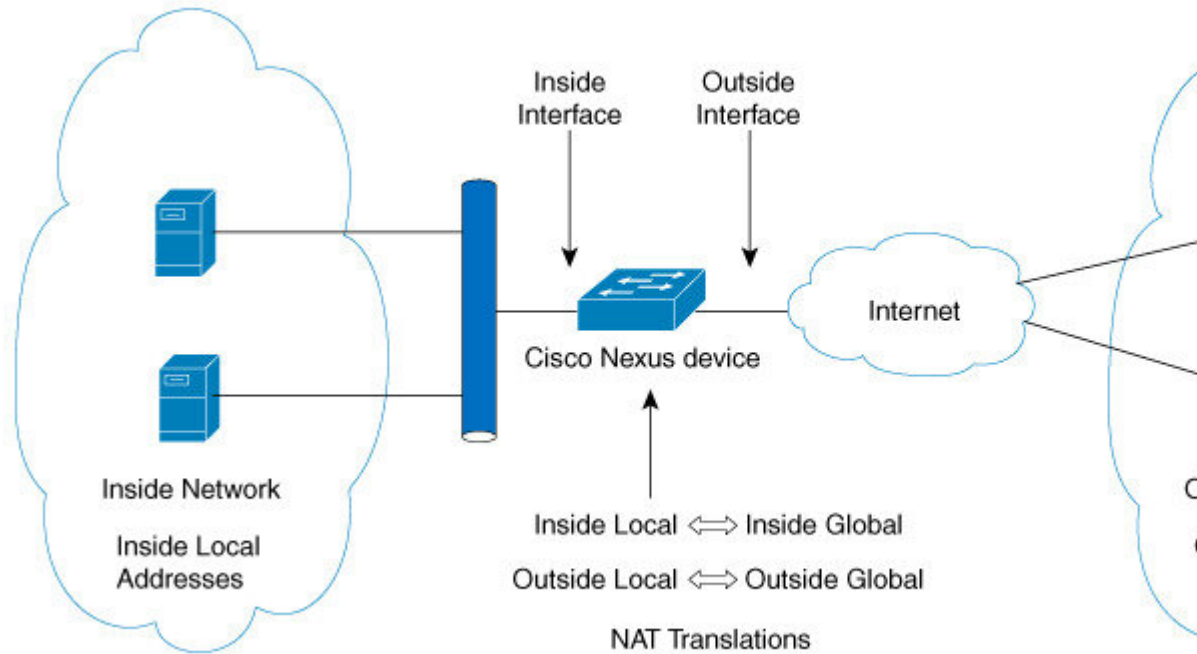
スタティック NAT では、プライベートアドレスからパブリックアドレスへの固定変換が作成されます。スタティック NAT では 1 対 1 ベースでアドレスが割り当てられるため、プライベートアドレスと同じ数のパブリックアドレスが必要です。スタティック NAT では、パブリックアドレスは連続する各接続で同じであり、永続的な変換規則が存在するため、宛先ネットワークのホストは変換済みのホストへのトラフィックを開始できます (そのトラフィックを許可するアクセスリストがある場合)。

ダイナミック NAT およびポートアドレス変換 (PAT) では、各ホストは後続する変換ごとに異なるアドレスまたはポートを使用します。ダイナミック NAT とスタティック NAT の主な違いは、スタティック NAT ではリモートホストが変換済みのホストへの接続を開始でき (それを許可するアクセスリストがある場合)、ダイナミック NAT では開始できないという点です。

次の図に、一般的なスタティック NAT のシナリオを示します。変換は常にアクティブであるため、変換対象ホストとリモートホストの両方で接続を生成でき、マップアドレスは **static** コマンドによって静的に割り当てられます。



図 5:スタティック NAT



次に、スタティック NAT を理解するのに役立つ主な用語を示します。

- NAT の内部インターフェイス：プライベートネットワークに面するレイヤ3インターフェイス。
- NAT の外部インターフェイス：パブリック ネットワークに面するレイヤ3インターフェイス。
- ローカルアドレス：ネットワークの内部（プライベート）部分に表示される任意のアドレス。
- グローバルアドレス：ネットワークの外部（パブリック）部分に表示される任意のアドレス。
- 正規の IP アドレス：Network Information Center（NIC）やサービス プロバイダーにより割り当てられたアドレス。
- 内部ローカルアドレス：内部ネットワーク上のホストに割り当てられた IP アドレス。このアドレスは正規の IP アドレスである必要はありません。
- 外部ローカルアドレス：内部ネットワークから見た外部ホストの IP アドレス。これは、内部ネットワークのルーティング可能なアドレス空間から割り当てられるため、正規のアドレスである必要はありません。
- 内部グローバルアドレス：1つ以上の内部ローカル IP アドレスを外部に対して表すために使用できる正規の IP アドレス。

- 外部グローバルアドレス：ホスト所有者が外部ネットワーク上のホストに割り当てる IP アドレス。このアドレスは、ルート可能なアドレスまたはネットワーク空間から割り当てられた正規のアドレスです。

## ダイナミック NAT の概要

ダイナミック Network Address Translation (NAT) では、実際の IP アドレスのグループは、宛先ネットワーク上でルーティング可能なマッピング IP アドレスのプールに変換されます。ダイナミック NAT は、未登録の IP アドレスと登録済みの IP アドレスの間に 1 対 1 のマッピングを確立します。ただし、マッピングは、通信時に使用可能な登録済み IP アドレスによって異なります。

ダイナミック NAT を設定自動 A すると、使用している内部ネットワークと外部ネットワークまたはインターネット間に、ファイウォールが構築されます。ダイナミック NAT は、スタブドメイン内で発信された接続のみを許可します。外部ネットワーク上のデバイスは、接続を開始していない限り、ネットワーク内のデバイスに接続できません。

ダイナミック NAT の場合、変換対象のトラフィックデバイスに受信するまでは、NAT 変換テーブルには変換エントリが存在しません。ダイナミック変換は、新しいエントリ用のスペースを確保するために使用されていない場合、クリアまたはタイムアウトされます。通常、NAT 変換エントリは、Ternary Content Addressable Memory (TCAM) エントリが制限されるとクリアされます。ダイナミック NAT 変換のデフォルトの最小タイムアウトは 30 分です。 **ip nat translation sampling-timeout** コマンドのサンプリングタイムアウトの最小値は、30 分から 15 分に短縮されました。

ダイナミック NAT 変換のタイムアウトには、サンプリングタイムアウト値と TCP または UDP タイムアウト値の両方が含まれます。サンプリングタイムアウトは、デバイスが動的変換アクティビティをチェックするまでの時間を指定します。デフォルト値は 12 時間です。他のすべてのタイムアウトは、**sample-timeout** がタイムアウトした後にのみ開始されます。サンプリングタイムアウト後、デバイスはこの変換にヒットしているパケットを検査します。このチェックは、TCP または UDP のタイムアウト期間に行われます。TCP または UDP タイムアウト期間のパケットがない場合、変換はクリアされます。変換でアクティビティが検出されると、チェックはすぐに停止され、サンプリングタイムアウト期間が開始されます。

この新しいサンプリングタイムアウト期間を待機した後、デバイスはダイナミック変換アクティビティを再度チェックします。アクティビティチェック中に、TCAM はダイナミック NAT 変換に一致するパケットのコピーを CPU に送信します。コントロールプレーンポリシング (CoPP) が低しきい値に設定されている場合、TCP または UDP パケットが CPU に到達しない可能性があり、CPU はこれを NAT 変換の非アクティブと見なします。

ダイナミック NAT は、ポートアドレス変換 (PAT) およびアクセスコントロールリスト (ACL) をサポートします。PAT (暗号化ともいう)、オーバーロードは未登録の複数の IP アドレスを、さまざまなポートを使うことによって、登録済みの単一の IP アドレスにマッピングするダイナミック NAT の 1 形態です。NAT 設定には、同じまたは異なる ACL を持つ複数のダイナミック NAT 変換を含めることができます。ただし、特定の ACL に対して指定できるインターフェイスは 1 つだけです。

## タイムアウトメカニズム

ダイナミック NAT 変換を作成した後は、特に TCAM エントリの数が制限されている場合、新しい変換を作成できるように、使用していないものをクリアする必要があります。Cisco NX-OS リリース 7.x は **syn-timeout** および **finrst-timeout** をサポートします。スイッチでは、次の NAT 変換タイムアウト タイマーがサポートされています。

- **syn-timeout** : TCP データのパケットタイムアウト値。SYN リクエストを送信後、SYN-ACK 応答を受信するまでの最大待ち時間です。

タイムアウト値の範囲は、1 ~ 172800 秒です。デフォルト値は 60 秒です。

- **finrst-timeout** : RST または FIN パケットの受信によって接続が終了したときのフロー エントリのタイムアウト値。RST パケットと FIN パケットの両方の動作を設定するには、同じキーワードを使用します。
  - 接続が確立された後に RST パケットが受信されると (SYN-> SYN-ACK-> RST)、フローは設定されたタイムアウト値の後に期限切れになります。
  - 接続が確立された後に SYN パケット (SYN-> SYN-ACK-> FIN) が受信されると、**finrst** タイマーが開始されます。
  - 相手側から FIN-ACK を受信すると、変換エントリはすぐにクリアされます。それ以外の場合は、タイムアウト値の完了後にクリアされます。



---

(注) ダイナミックプールベースの設定を使用し、FIN-ACK を受信した場合、変換エントリはクリアされません。

---

タイムアウト値の範囲は、1 ~ 172800 秒です。デフォルト値は 60 秒です。

- **tcp-timeout** : TCP 変換のタイムアウト値。3 ウェイ ハンドシェイク (SYN、SYN-ACK、ACK) の後に確立した接続の最大待ち時間です。接続が確立された後にアクティブフローが発生しない場合、変換は設定されたタイムアウト値に従って期限切れになります。このタイムアウト値は、サンプリング タイムアウト値の完了後に開始されます。

タイムアウト値の範囲は、1 ~ 172800 秒です。これにはサンプリングタイムアウトも含まれます。

- **udp-timeout** : すべての NAT UDP パケットのタイムアウト値。

タイムアウト値の範囲は、1 ~ 172800 秒です。これにはサンプリングタイムアウトも含まれます。

- **timeout** : ダイナミック NAT 変換のタイムアウト値。

タイムアウト値の範囲は、1 ~ 172800 秒です。これにはサンプリングタイムアウトも含まれます。

- **sampling-timeout** : デバイスがダイナミック変換アクティビティをチェックするまでの時間。

タイムアウト値の範囲は、1 ~ 172800 秒です。

**tcp-timeout**、**udp-timeout**、および **timeout** 値のタイマーは、**ip nat translation sampling-timeout** コマンドで設定されているタイムアウトの期限が切れた後にトリガーされます。



(注) 上記のタイマーはすべて、期限が切れるまでさらに時間がかかります (1 ~ 30 秒)。この追加時間は、パフォーマンスと最適化のためにタイマー期限切れイベントをランダム化するためのものです。

## NAT の内部アドレスおよび外部アドレス

NAT 内部とは、変換を必要とする組織が所有するネットワークを指します。NAT が設定されている場合、このネットワーク内のホストは、別の空間 (グローバルアドレス空間として知られている) にあるものとしてネットワークの外側に現れる 1 つ空間 (ローカルアドレス空間として知られている) 内のアドレスを持つこととなります。

同様に、NAT 外部とは、スタブ ネットワークが接続するネットワークを指します。通常、組織の管理下にはありません。外部ネットワーク内のホストを変換の対象にすることもできるため、これらのホストもローカルアドレスとグローバルアドレスを持つことができます。

NAT では、次の定義が使用されます。

- ローカルアドレス : ネットワークの内側部分に表示されるローカルな IP アドレスです。
- グローバルアドレス : ネットワークの外側部分に表示されるグローバルな IP アドレスです。
- 内部ローカルアドレス : 内部ネットワーク上のホストに割り当てられた IP アドレス。このアドレスは、多くの場合、インターネット ネットワーク 情報センター (InterNIC) や サービス プロバイダーにより割り当てられた正規の IP アドレスではありません。
- 内部グローバルアドレス : 外部に向けて、1 つ以上の内部ローカル IP アドレスを表現した正規の IP アドレス (InterNIC または サービス プロバイダーにより割り当てられたもの)。
- 外部ローカルアドレス : 内部ネットワークから見た外部ホストの IP アドレス。必ずしも正規のアドレスではありません。内部でルート可能なアドレス空間から割り当てられたものです。
- 外部グローバルアドレス : 外部ネットワークに存在するホストに対して、ホストの所有者により割り当てられた IP アドレス。このアドレスは、グローバルにルート可能なアドレス、またはネットワーク空間から割り当てられたものです。

## ダイナミック NAT のプール サポート

ダイナミック NAT を使用すると、グローバルアドレスのプールを設定して、新しい変換ごとにプールからグローバルアドレスを動的に割り当てることができます。アドレスは、セッションが期限切れになるか、閉じられた後にプールに戻されます。これにより、要件に基づいてアドレスをより効率的に使用できます。

PAT のサポートには、グローバルアドレス プールの使用が含まれます。これにより、IP アドレスの使用率がさらに最適化されます。PAT は、ポート番号を使用して、一度に 1 つの IP アドレスを使い果たします。ポートが該当グループで見つけられなかった場合や、複数の IP アドレスが設定されている場合、はユーザー定義プールに基づいて、（ソースポートを無視するか、それを保存しようと試みて）割り当てを取得します。

ダイナミック NAT および PAT では、各ホストは変換するたびに異なるアドレスまたはポートを使用します。ダイナミック NAT とスタティック NAT の主な違いは、スタティック NAT ではリモート ホストが変換済みのホストへの接続を開始でき（それを許可するアクセスリストがある場合）、ダイナミック NAT では開始できないという点です。

## スタティックおよびダイナミック Twice NAT の概要

送信元 IP アドレスと宛先 IP アドレスの両方が、ネットワークアドレス変換 (NAT) デバイスを通過する単一のパケットとして変換される場合、Twice NAT と呼ばれます。Twice NAT は、スタティックおよびダイナミック変換でサポートされます。

Twice NAT では、2 つの NAT 変換（1 つは内部、もう 1 つは変換）を変換グループの一部として設定できます。これらの変換は、NAT デバイスを通過する単一のパケットに適用できます。グループの一部として 2 つの変換を追加すると、個々の変換と結合された変換の両方が有効になります。

NAT 内部変換は、パケットが内部から外部に流れるときに送信元 IP アドレスとポート番号を変更します。パケットが外部から内部に戻るときに、宛先 IP アドレスとポート番号を変更します。NAT 外部変換は、パケットが外部から内部に流れるときに送信元 IP アドレスとポート番号を変更し、パケットが内部から外部に戻るときに宛先 IP アドレスとポート番号を変更します。

Twice NAT を使用しない場合、送信元 IP アドレスとポート番号、または宛先 IP アドレスとポート番号のいずれか 1 つの変換ルールのみがパケットに適用されます。

同じグループに属するスタティック NAT 変換は、Twice NAT 設定の対象となります。スタティック設定にグループ ID が設定されていない場合、Twice NAT 設定は機能しません。グループ ID で識別される単一のグループに属するすべての内部および外部 NAT 変換は、ペアになって Twice NAT 変換を形成します。

ダイナミック双方向 NAT 変換は、事前定義された **ip nat pool** または **インターフェイス オーバーロード** 設定から、送信元 IP アドレスとポート番号の情報を動的に選択します。パケットフィルタリングは ACL の設定によって行われ、トラフィックはダイナミック NAT 変換ルール

の方向から発信される必要があります。そのため、送信元変換はダイナミック NAT ルールを使用して行われます。

ダイナミック Twice NAT では、2つの NAT 変換（内部と外部）を変換グループの一部として設定できます。1つの変換はダイナミックで、他の変換はスタティックである必要があります。これらの2つの変換が変換のグループの一部である場合、内部から外部または外部から内部のいずれかで NAT デバイスを通過するときに、両方の変換を1つのパケットに適用できます。

## スタティック NAT の注意事項および制約事項

スタティック NAT 設定時の注意事項および制約事項は、次のとおりです。

- NAT は、スタティック NAT とダイナミック NAT の両方を含む最大 1024 の変換をサポートします。
- Cisco Nexus 3500 シリーズ スイッチは、vPC トポロジでの NAT をサポートしていません。
- Cisco Nexus デバイスは、次のインターフェイス タイプ上の NAT をサポートします。
  - スイッチ仮想インターフェイス (SVI)
  - ルーテッド ポート
  - レイヤ 3 ポート チャネル
- NAT は、IPv4 ユニキャストだけでサポートされています。
- Cisco Nexus デバイスは、次をサポートしません。
  - アプリケーション層の変換。レイヤ 4 およびその他の組み込み IP は変換されません (FTP、ICMP の障害、IPSec、HTTPS など)。
  - インターフェイス上で同時に設定された NAT および VLAN アクセス コントロール リスト (VACL)。
  - フラグメント化された IP パケットの PAT 変換。
  - ソフトウェア転送パケットの NAT 変換。たとえば、IP オプションを持つパケットは NAT 変換されません。
- 出力 ACL は元のパケットに適用され、NAT 変換済みパケットには適用されません。
- デフォルトでは、NAT は 256 TCAM エントリで最大 127 の変換まで実行できます。より多くの NAT 変換が必要な場合は、他のエリア内の TCAM リージョン割り当てを減らしてから、**hardware profile tcam region nat** コマンドを使用して、NAT TCAM リージョンを増やします。
- HSRP および VRRP は NAT 内部アドレスではサポートされますが、NAT 外部アドレスではサポートされません。

- ワープ モード遅延パフォーマンスは、外部から内部ドメインに着信するパケットではサポートされません。
- IP アドレスがスタティック NAT 変換または PAT 変換に使用される場合、他の目的には使用できません。たとえば、インターフェイスに割り当てることはできません。
- スタティック NAT の場合は、外部グローバル IP アドレスが外部インターフェイス IP アドレスと異なる必要があります。
- 変換された IP が、外部インターフェイス サブネットの一部である場合、NAT の外部インターフェイスで **ip local-proxy-arp** コマンドを使用します。
- NAT 統計情報は利用できません。
- (100 を超える) 多数の変換を設定する場合、変換を設定してから NAT インターフェイスを設定する方が迅速に設定できます。
- インターフェイスで一度に有効にできるのは、次の機能のいずれか1つだけです。これらの機能の1つ以上がインターフェイスで有効になっている場合、最後に有効になっている機能のみが機能します。
  - NAT
  - DHCP リレー
  - VACL
- 127 を超える PD NAT スタティック エントリは、一貫性のない CoPP ハードウェア カウンタの増分を行うハードウェアの制限によりサポートされません。

## ダイナミック NAT の制約事項

ダイナミックネットワークアドレス変換 (NAT) には、次の制約事項が適用されます。

- フラグメント化されたパケットはサポートされません。
- アプリケーション層ゲートウェイ (ALG) 変換はサポートされていません。ALG、またはアプリケーションレベルゲートウェイは、アプリケーションパケットのペイロード内の IP アドレス情報を変換するアプリケーションです。
- NAT および VLAN アクセス コントロール リスト (VACL) は、インターフェイスで一緒にサポートされません。インターフェイスで NAT または VACL を設定できます。
- 出力 ACL は、変換されたパケットには適用されません。
- MIB はサポートされていません。
- Cisco Data Center Network Manager (DCNM) はサポートされていません。
- ダイナミック NAT 変換は、アクティブデバイスおよびスタンバイデバイスと同期されません。

- ステートフル NAT はサポートされていません。ただし、NAT と Hot Standby Router Protocol (HSRP) は共存できます。
- 通常、ICMP NAT フローは、設定されたサンプリングタイムアウトおよび変換タイムアウトの満了後にタイムアウトします。ただし、スイッチに存在する ICMP NAT フローがアイドル状態になると、設定されたサンプリングタイムアウトの期限が切れた直後にタイムアウトします。
- 変換された IP が、外部インターフェイス サブネットの一部である場合、NAT の外部インターフェイスで `ip local-proxy-arp` コマンドを使用します。
- Cisco Nexus 3548 シリーズ スイッチで新しい変換を作成する場合、変換がハードウェアでプログラムされるまでフローがソフトウェア転送されます。これには数秒かかることがあります。この期間中、内部グローバルアドレスの変換エントリはありません。したがって、リターントラフィックはドロップされます。この制限を克服するには、ループバックインターフェイスを作成し、NAT プールに属する IP アドレスを割り当てます。

## ダイナミック Twice NAT の注意事項および制約事項

ダイナミック双方向 NAT の設定については、次の注意事項を参照してください。

- ダイナミック双方向 NAT では、スタティック NAT フローを作成する前にダイナミック NAT フローを作成しないと、ダイナミック双方向 NAT フローが正しく作成されません。
- 空の ACL が作成されると、`permit ip any any` のデフォルトルールが設定されます。最初の ACL が空白の場合、NAT-ACL はそれ以上の ACL エントリに一致しません。
- TCAM スペースを最適に使用するためにサポートされる ICMP 変換またはフローエントリの最大数は 176 です。
- NAT は ECMP 対応であり、最大 24 の ECMP パスをサポートします。
- Cisco NX-OS リリース 9.x は、Cisco Nexus 3548 スイッチのネットワーク アドレス変換 (NAT) 統計情報をサポートします。
- `traceroute` は、スタティックおよびダイナミック NAT ではサポートされていません。

## スタティック NAT の設定

### スタティック NAT のイネーブル化

手順の概要

1. `switch# configure terminal`
2. `switch(config)# feature nat`



3. (任意) switch(config)# copy running-config startup-config

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	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 nat</b>	デバイス上でスタティック NAT 機能をイネーブルにします。
ステップ 3	(任意) switch(config)# <b>copy running-config startup-config</b>	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。

## インターフェイスでのスタティック NAT の設定

手順の概要

1. switch# **configure terminal**
2. switch(config)# **interface type slot/port**
3. switch(config-if)# **ip nat {inside | outside}**
4. (任意) switch(config)# **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	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 type 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>ip nat {inside   outside}</b>	内部または外部としてインターフェイスを指定します。  (注) マーク付きインターフェイスに到着したパケットだけが変換できます。
ステップ 4	(任意) switch(config)# <b>copy running-config startup-config</b>	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。

例

次に、スタティック NAT を使用して内部の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 1/4
switch(config-if)# ip nat inside
```

## 内部送信元アドレスのスタティック NAT のイネーブル化

内部送信元変換の場合、トラフィックは内部インターフェイスから外部インターフェイスに流れます。NAT は、内部ローカル IP アドレスを内部グローバル IP アドレスに変換します。リターントラフィックでは、宛先の内部グローバル IP アドレスが内部ローカル IP アドレスに変換されて戻されます。



(注) Cisco Nexus デバイスが、内部送信元 IP アドレス (Src:ip1) を外部送信元 IP アドレス (newSrc:ip2) に変換するように設定されている場合、Cisco Nexus デバイスは外部宛先 IP アドレス (Dst: ip2) の内部宛先 IP アドレス (newDst: ip1) への変換を暗黙的に追加します。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **ip nat inside source static local-ip-address global-ip-address [group group-id]**
3. (任意) switch(config)# **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	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 nat inside source static local-ip-address global-ip-address [group group-id]</b>	内部グローバルアドレスを内部ローカルアドレスに、またはその逆に（内部ローカルトラフィックを内部グローバルトラフィックに）変換するようにスタティック NAT を設定します。
ステップ 3	(任意) switch(config)# <b>copy running-config startup-config</b>	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。

例

次に、内部送信元アドレスのスタティック NAT を設定する例を示します。

```
switch# configure terminal
switch(config)# ip nat inside source static 1.1.1.1 5.5.5.5
switch(config)# copy running-config startup-config
```

## 外部送信元アドレスのスタティック NAT のイネーブル化

外部送信元変換の場合、トラフィックは外部インターフェイスから内部インターフェイスに流れます。NAT は、外部グローバル IP アドレスを外部ローカル IP アドレスに変換します。リターントラフィックでは、宛先の外部ローカル IP アドレスが外部グローバル IP アドレスに変換されて戻されます。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **ip nat outside source static** *global-ip-address local-ip-address* [**group group-id**] [**add-route**]
3. (任意) switch(config)# **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	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 nat outside source static</b> <i>global-ip-address local-ip-address</i> [ <b>group group-id</b> ] [ <b>add-route</b> ]	外部グローバル アドレスを外部ローカル アドレスに、またはその逆に外部ローカルトラフィックを外部グローバルトラフィックに変換するようにスタティック NAT を設定します。
ステップ 3	(任意) switch(config)# <b>copy running-config startup-config</b>	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。

例

次に、外部送信元アドレスのスタティック NAT を設定する例を示します。

```
switch# configure terminal
switch(config)# ip nat outside source static 2.2.2.2 6.6.6.6
switch(config)# copy running-config startup-config
```

## 内部送信元アドレスのスタティック PAT の設定

ポートアドレス変換 (PAT) を使用して、特定の内部ホストにサービスをマッピングできます。

### 手順の概要

1. switch# **configure terminal**
2. switch(config)# **ip nat inside source static** {inside-local-address outside-local-address | {tcp|udp} inside-local-address {local-tcp-port | local-udp-port} inside-global-address {global-tcp-port | global-udp-port}} **group group-id**
3. (任意) switch(config)# **copy running-config startup-config**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	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 nat inside source static</b> {inside-local-address outside-local-address   {tcp udp} inside-local-address {local-tcp-port   local-udp-port} inside-global-address {global-tcp-port   global-udp-port}} <b>group group-id</b>	スタティック NAT を内部ローカル ポート、内部グローバル ポートにマッピングします。
ステップ 3	(任意) switch(config)# <b>copy running-config startup-config</b>	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。

### 例

次に、UDP サービスを特定の内部送信元アドレスおよび UDP ポートにマッピングする例を示します。

```
switch# configure terminal
switch(config)# ip nat inside source static udp 20.1.9.2 63 35.48.35.48 130
switch(config)# copy running-config startup-config
```

## 外部送信元アドレスのスタティック PAT の設定

ポートアドレス変換 (PAT) を使用して、特定の外部ホストにサービスをマッピングできます。

### 手順の概要

1. switch# **configure terminal**

2. switch(config)# **ip nat outside source static** {*outside-global-address outside-local-address* | {**tcp** | **udp**} *outside-global-address {global-tcp-port | global-udp-port} outside-local-address {global-tcp-port | global-udp-port}*} **group group-id add-route**
3. (任意) switch(config)# **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	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 nat outside source static</b> { <i>outside-global-address outside-local-address</i>   { <b>tcp</b>   <b>udp</b> } <i>outside-global-address {global-tcp-port   global-udp-port} outside-local-address {global-tcp-port   global-udp-port}</i> } <b>group group-id add-route</b>	スタティック NAT を、外部グローバル ポート、外部ローカル ポートにマッピングします。
ステップ 3	(任意) switch(config)# <b>copy running-config startup-config</b>	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。

例

次に、TCP サービスを特定の外部送信元アドレスおよび TCP ポートにマッピングする例を示します。

```
switch# configure terminal
switch(config)# ip nat outside source static tcp 20.1.9.2 63 35.48.35.48 130
switch(config)# copy running-config startup-config
```

## スタティック Twice NAT の設定

同じグループ内のすべての変換は、スタティック Twice Network Address Translation (NAT) ルールを作成するために考慮されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip nat inside source static** *inside-local-ip-address inside-global-ip-address* [**group group-id**]
4. **ip nat outside source static** *outside-global-ip-address outside-local-ip-address* [**group group-id**] [**add-route**]
5. **interface** *type number*
6. **ip address** *ip-address mask*
7. **ip nat inside**
8. **exit**
9. **interface** *type number*

10. **ip address** *ip-address mask*
11. **ip nat outside**
12. **end**

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： switch> enable	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"><li>• プロンプトが表示されたら、パスワードを入力します。</li></ul>
ステップ 2	<b>configure terminal</b> 例： switch# configure terminal	特権 EXEC モードを開始します。
ステップ 3	<b>ip nat inside source static</b> <i>inside-local-ip-address inside-global-ip-address</i> [ <b>group</b> <i>group-id</i> ] 例： switch(config)# ip nat inside source static 10.1.1.1 192.168.34.4 group 4	内部ローカルIPアドレスを対応する内部グローバルIPアドレスに変換するようにスタティック Twice NATを設定します。 <ul style="list-style-type: none"><li>• <b>group</b> キーワードは、変換が属するグループを決定します。</li></ul>
ステップ 4	<b>ip nat outside source static</b> <i>outside-global-ip-address outside-local-ip-address</i> [ <b>group</b> <i>group-id</i> ] [ <b>add-route</b> ] 例： switch(config)# ip nat outside source static 209.165.201.1 10.3.2.42 group 4 add-route	スタティック Twice NATを設定して、外部グローバルIPアドレスを対応する外部ローカルIPアドレスに変換します。 <ul style="list-style-type: none"><li>• <b>group</b> キーワードは、変換が属するグループを決定します。</li></ul>
ステップ 5	<b>interface</b> <i>type number</i> 例： switch(config)# interface ethernet 1/2	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 6	<b>ip address</b> <i>ip-address mask</i> 例： switch(config-if)# ip address 10.2.4.1 255.255.255.0	インターフェイスのプライマリ IP アドレスを設定します。
ステップ 7	<b>ip nat inside</b> 例： switch(config-if)# ip nat inside	NATの対象である内部ネットワークにインターフェイスを接続します。
ステップ 8	<b>exit</b> 例： switch(config-if)# exit	インターフェイス コンフィギュレーション モードを終了し、グローバルコンフィギュレーションモードに戻ります。

	コマンドまたはアクション	目的
ステップ 9	<b>interface</b> <i>type number</i> 例： switch(config)# interface ethernet 1/1	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 10	<b>ip address</b> <i>ip-address mask</i> 例： switch(config-if)# ip address 10.5.7.9 255.255.255.0	インターフェイスのプライマリ IP アドレスを設定します。
ステップ 11	<b>ip nat outside</b> 例： switch(config-if)# ip nat outside	NATの対象である外部ネットワークにインターフェイスを接続します。
ステップ 12	<b>end</b> 例： switch(config-if)# end	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

## スタティック NAT および PAT の設定例

次に、スタティック NAT の設定例を示します。

```
ip nat inside source static 103.1.1.1 11.3.1.1
ip nat inside source static 139.1.1.1 11.39.1.1
ip nat inside source static 141.1.1.1 11.41.1.1
ip nat inside source static 149.1.1.1 95.1.1.1
ip nat inside source static 149.2.1.1 96.1.1.1
ip nat outside source static 95.3.1.1 95.4.1.1
ip nat outside source static 96.3.1.1 96.4.1.1
ip nat outside source static 102.1.2.1 51.1.2.1
ip nat outside source static 104.1.1.1 51.3.1.1
ip nat outside source static 140.1.1.1 51.40.1.1
```

次に、スタティック PAT の設定例を示します。

```
ip nat inside source static tcp 10.11.1.1 1 210.11.1.1 101
ip nat inside source static tcp 10.11.1.1 2 210.11.1.1 201
ip nat inside source static tcp 10.11.1.1 3 210.11.1.1 301
ip nat inside source static tcp 10.11.1.1 4 210.11.1.1 401
ip nat inside source static tcp 10.11.1.1 5 210.11.1.1 501
ip nat inside source static tcp 10.11.1.1 6 210.11.1.1 601
ip nat inside source static tcp 10.11.1.1 7 210.11.1.1 701
ip nat inside source static tcp 10.11.1.1 8 210.11.1.1 801
ip nat inside source static tcp 10.11.1.1 9 210.11.1.1 901
ip nat inside source static tcp 10.11.1.1 10 210.11.1.1 1001
ip nat inside source static tcp 10.11.1.1 11 210.11.1.1 1101
ip nat inside source static tcp 10.11.1.1 12 210.11.1.1 1201
```

## 例：スタティック Twice NAT の設定

次に、内部送信元および外部送信元のスタティック双方向NATを設定する例を示します。

```
Switch> enable
Switch# configure terminal
Switch(config)# ip nat inside source static 10.1.1.1 192.168.34.4 group 4
Switch(config)# ip nat outside source static 209.165.201.1 10.3.2.42 group 4
Switch(config)# interface ethernet 1/2
Switch(config-if)# ip address 10.2.4.1 255.255.255.0
Switch(config-if)# ip nat inside
switch(config-if)# exit
switch(config)# interface ethernet 1/1
switch(config-if)# ip address 10.5.7.9 255.255.255.0
switch(config-if)# ip nat outside
Switch(config-if)# end
```

## スタティック NAT の設定の確認

スタティック NAT の設定を表示するには、次の作業を行います。

### 手順の概要

1. switch# show ip nat translations

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# show ip nat translations	内部グローバル、内部ローカル、外部ローカル、および外部グローバルの各 IP アドレスを示します。

### 例

次に、スタティック NAT の設定を表示する例を示します。

```
switch# show ip nat translations
Pro Inside global      Inside local      Outside local     Outside global
any ---               ---               20.4.4.40         220.2.2.20
tcp ---               ---               23.1.1.133:333   210.3.3.33:555
any 160.200.1.140     10.1.1.40        ---               ---
any 160.200.1.140     10.1.1.40        20.4.4.40         220.2.2.20
tcp 172.9.9.142:777   12.2.2.42:444    ---               ---
tcp 172.9.9.142:777   12.2.2.42:444    23.1.1.133:333   210.3.3.33:555
```



# ダイナミック NAT の設定

## ダイナミック変換および変換タイムアウトの設定

### 手順の概要

1. **enable**
2. **configure terminal**
3. **ip access-list** *access-list-name*
4. **permit** *protocol source source-wildcard any*
5. **deny** *protocol source source-wildcard any*
6. **exit**
7. **ip nat inside source list** *access-list-name interface type number overload*
8. **interface** *type number*
9. **ip address** *ip-address mask*
10. **ip nat inside**
11. **exit**
12. **interface** *type number*
13. **ip address** *ip-address mask*
14. **ip nat outside**
15. **exit**
16. **ip nat translation tcp-timeout** *seconds*
17. **ip nat translation max-entries** [**all-host**] *number-of-entries*
18. **ip nat translation udp-timeout** *seconds*
19. **ip nat translation timeout** *seconds*
20. **ip nat translation syn-timeout** {*seconds* | **never**}
21. **ip nat translation finrst-timeout** {*seconds* | **never**}
22. **end**

### 手順の詳細

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

	コマンドまたはアクション	目的
ステップ 3	<b>ip access-list</b> <i>access-list-name</i> 例： Switch(config)# ip access-list acl1	アクセスリストを定義し、アクセスリスト 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	<b>permit</b> <i>protocol source source-wildcard any</i> 例： Switch(config-acl)# permit ip 10.111.11.0/24 any	条件に一致するトラフィックを許可する条件をIPアクセスリストに設定します。
ステップ 5	<b>deny</b> <i>protocol source source-wildcard any</i> 例： Switch(config-acl)# deny udp 10.111.11.100/32 any	ネットワークにパケットが入るのを拒否する IP アクセスリストの条件を設定します。 <b>deny</b> ルールは <b>permit</b> として扱われ、拒否ルールに記載された条件に一致するパケットは NAT 変換されずに転送されます。
ステップ 6	<b>exit</b> 例： Switch(config-acl)# exit	アクセスリスト コンフィギュレーションモードを終了し、グローバル コンフィギュレーションモードに戻ります。
ステップ 7	<b>ip nat inside source list</b> <i>access-list-name interface type number overload</i> 例： Switch(config)# ip nat inside source list acl1 interface ethernet 1/1 overload	ステップ3で定義したアクセスリストを指定して、ダイナミック送信元変換を設定します。
ステップ 8	<b>interface</b> <i>type number</i> 例： Switch(config)# interface ethernet 1/4	インターフェイスを設定し、インターフェイス コンフィギュレーションモードを開始します。
ステップ 9	<b>ip address</b> <i>ip-address mask</i> 例： Switch(config-if)# ip address 10.111.11.39 255.255.255.0	インターフェイスのプライマリ IP アドレスを設定します。
ステップ 10	<b>ip nat inside</b> 例： Switch(config-if)# ip nat inside	NATの対象である内部ネットワークにインターフェイスを接続します。
ステップ 11	<b>exit</b> 例： Switch(config-if)# exit	インターフェイス コンフィギュレーションモードを終了し、グローバルコンフィギュレーションモードに戻ります。
ステップ 12	<b>interface</b> <i>type number</i> 例： Switch(config)# interface ethernet 1/1	インターフェイスを設定し、インターフェイス コンフィギュレーションモードを開始します。

	コマンドまたはアクション	目的
ステップ 13	<p><b>ip address</b> <i>ip-address mask</i></p> <p>例 :</p> <pre>Switch(config-if)# ip address 172.16.232.182 255.255.255.240</pre>	<p>インターフェイスのプライマリ IP アドレスを設定します。</p>
ステップ 14	<p><b>ip nat outside</b></p> <p>例 :</p> <pre>Switch(config-if)# ip nat outside</pre>	<p>インターフェイスを外部ネットワークに接続します。</p>
ステップ 15	<p><b>exit</b></p> <p>例 :</p> <pre>Switch(config-if)# exit</pre>	<p>インターフェイス コンフィギュレーション モードを終了し、グローバルコンフィギュレーションモードに戻ります。</p>
ステップ 16	<p><b>ip nat translation tcp-timeout</b> <i>seconds</i></p> <p>例 :</p> <pre>Switch(config)# ip nat translation tcp-timeout 50000</pre>	<p>TCP ベースのダイナミック NAT エントリのタイムアウト値を指定します。</p> <ul style="list-style-type: none"> <li>ダイナミックに作成された NAT 変換は、設定されたタイムアウト制限に達するとクリアされます。すべての設定されたタイムアウトは、<b>ip nat translation sampling-timeout</b> コマンドのために設定されたタイムアウトが終了すると、トリガされます。</li> </ul>
ステップ 17	<p><b>ip nat translation max-entries</b> [<b>all-host</b>] <i>number-of-entries</i></p> <p>例 :</p> <pre>Switch(config)# ip nat translation max-entries 300</pre>	<p>ダイナミック NAT 変換の最大数を指定します。エントリの数は 1~1023 です。</p> <p><b>all-host</b> キーワードは、この変換制限をすべてのホストに適用します。ホストあたりのエントリ数は 1~1023 です。</p>
ステップ 18	<p><b>ip nat translation udp-timeout</b> <i>seconds</i></p> <p>例 :</p> <pre>Switch(config)# ip nat translation udp-timeout 45000</pre>	<p>UDP ベースのダイナミック NAT エントリのタイムアウト値を指定します。</p> <ul style="list-style-type: none"> <li>ダイナミックに作成された NAT 変換は、設定されたタイムアウト制限に達するとクリアされます。すべての設定されたタイムアウトは、<b>ip nat translation sampling-timeout</b> コマンドのために設定されたタイムアウトが終了すると、トリガされます。</li> </ul>
ステップ 19	<p><b>ip nat translation timeout</b> <i>seconds</i></p> <p>例 :</p> <pre>switch(config)# ip nat translation timeout 13000</pre>	<p>ダイナミック NAT 変換のタイムアウト値を指定します。</p>

	コマンドまたはアクション	目的
ステップ 20	<b>ip nat translation syn-timeout</b> {seconds   never} 例： switch(config)# ip nat translation syn-timeout 20	SYN 要求を送信するが SYN-ACK 応答を受信しない TCP データの packets タイムアウト値を指定します。 タイムアウト値の範囲は、1 ~ 172800 秒です。デフォルト値は 60 秒です。 <b>never</b> キーワードは、SYN タイマーが実行されないことを指定します。
ステップ 21	<b>ip nat translation finrst-timeout</b> {seconds   never} 例： switch(config)# ip nat translation finrst-timeout 30	終了 (FIN) パケットまたはリセット (RST) パケットを受信して接続が終了したときのフローエントリのタイムアウト値を指定します。RST パケットと FIN パケットの両方の動作を設定するには、同じキーワードを使用します。 タイムアウト値の範囲は、1 ~ 172800 秒です。デフォルト値は 60 秒です。 <b>never</b> キーワードは、FIN または RST タイマーが実行されないことを指定します。
ステップ 22	<b>end</b> 例： Switch(config)# end	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

## ダイナミック NAT プールの設定

NAT プールは、単一の **ip nat pool** コマンドか、または **ip nat pool** と **address** コマンドを使用して、IP アドレスの範囲を定義することで作成できます。

### 手順の概要

1. switch# **configure terminal**
2. switch(config)# **feature nat**
3. switch(config)# **ip nat pool** pool-name [startip endip] {**prefix** prefix-length | **netmask** network-mask}
4. (任意) switch(config-ipnat-pool)# **address** startip endip
5. (任意) switch(config)# **no ip nat pool** pool-name

### 手順の詳細

	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>feature nat</b>	デバイスの NAT 機能をイネーブルにします。
ステップ 3	switch(config)# <b>ip nat pool</b> <i>pool-name</i> [ <i>startip endip</i> ] { <b>prefix</b> <i>prefix-length</i>   <b>netmask</b> <i>network-mask</i> }	グローバル IP アドレスの範囲で NAT プールを作成します。IP アドレスは、プレフィックス長またはネットワークマスクを使用してフィルタリングされます。
ステップ 4	(任意) switch(config-ipnat-pool)# <b>address</b> <i>startip endip</i>	グローバル IP アドレスの範囲を指定します (プールの作成時に指定していなかった場合)。
ステップ 5	(任意) switch(config)# <b>no ip nat pool</b> <i>pool-name</i>	指定した NAT プールを削除します。

### 例

次に、プレフィックス長を使用して NAT プールを作成する例を示します。

```
switch# configure terminal
switch(config)# ip nat pool pool1 30.1.1.1 30.1.1.2 prefix-length 24
switch(config)#
```

次に、ネットワークマスクを使用して NAT プールを作成する例を示します。

```
switch# configure terminal
switch(config)# ip nat pool pool5 20.1.1.1 20.1.1.5 netmask 255.0.255.0
switch(config)#
```

この例では **ip nat pool** と **address** コマンドを使用して NAT プールを作成し、グローバル IP アドレスの範囲を定義します。

```
switch# configure terminal
switch(config)# ip nat pool pool7 netmask 255.255.0.0
switch(config-ipnat-pool)# address 40.1.1.1 40.1.1.5
switch(config-ipnat-pool)#
```

次の例は、NAT プールの削除方法を示します。

```
switch# configure terminal
switch(config)# no ip nat pool pool4
switch(config)#
```

## 送信元リストの設定

内部インターフェイスと外部インターフェイスの IP アドレスの送信元リストを設定できます。

## 始める前に

プールの送信元リストを設定する前に、必ずプールを設定してください。

## 手順の概要

1. switch# **configure terminal**
2. (任意) switch# **ip nat inside source list list-name pool pool-name [overload]**
3. (任意) switch# **ip nat outside source list list-name pool pool-name [add-route]**

## 手順の詳細

	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	(任意) switch# <b>ip nat inside source list list-name pool pool-name [overload]</b>	オーバーロードの有無にかかわらず、プールを使用して NAT 内部送信元リストを作成します。
ステップ 3	(任意) switch# <b>ip nat outside source list list-name pool pool-name [add-route]</b>	オーバーロードなしでプールを使用して NAT 外部送信元リストを作成します。

## 例

次に、オーバーロードのないプールを使用して NAT 内部送信元リストを作成する例を示します。

```
switch# configure terminal
switch(config)# ip nat inside source list list1 pool pool1
switch(config)#
```

次に、オーバーロードのあるプールを使用して NAT 内部送信元リストを作成する例を示します。

```
switch# configure terminal
switch(config)# ip nat inside source list list2 pool pool2 overload
switch(config)#
```

次に、オーバーロードのないプールを使用して NAT 外部送信元リストを作成する例を示します。

```
switch# configure terminal
switch(config)# ip nat outside source list list3 pool pool3
switch(config)#
```

## 内部送信元アドレスのダイナミック Twice NAT の設定

内部送信元変換の場合、トラフィックは内部インターフェイスから外部インターフェイスに流れます。内部送信元アドレスにはダイナミック双方向 NAT を設定できます。

### 始める前に

スイッチで NAT がイネーブルになっていることを確認します。

### 手順の概要

1. switch# **configure terminal**
2. switch(config)# **ip nat outside source static** *outside-global-ip-address outside-local-ip-address* [**tcp** | **udp**] *outside-global-ip-address outside-global-port outside-local-ip-address outside-local-port* [**group** *group-id*] [**add-route**] [**dynamic**]
3. switch(config)# **ip nat inside source list** *access-list-name* [**interface** *type slot/port overload* | **pool** *pool-name* ] [**group** *group-id*] [**dynamic** ]
4. switch(config)# **ip nat pool** *pool-name* [*startip endip*] {**prefix** *prefix-length* | **netmask** *network-mask*}
5. switch(config)# **interface** *type slot/port*
6. switch(config-if)# **ip nat outside**
7. switch(config-if)# **exit**
8. switch(config)# **interface** *type slot/port*
9. switch(config-if)# **ip nat inside**

### 手順の詳細

	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 nat outside source static</b> <i>outside-global-ip-address outside-local-ip-address</i> [ <b>tcp</b>   <b>udp</b> ] <i>outside-global-ip-address outside-global-port outside-local-ip-address outside-local-port</i> [ <b>group</b> <i>group-id</i> ] [ <b>add-route</b> ] [ <b>dynamic</b> ]	外部グローバルアドレスを内部ローカルアドレスに変換するか、または内部ローカルトラフィックを内部グローバルトラフィックに変換するようにスタティック NAT を設定します。  <b>group</b> キーワードは、変換が属するグループを決定します。
ステップ 3	switch(config)# <b>ip nat inside source list</b> <i>access-list-name</i> [ <b>interface</b> <i>type slot/port overload</i>   <b>pool</b> <i>pool-name</i> ] [ <b>group</b> <i>group-id</i> ] [ <b>dynamic</b> ]	オーバーロードの有無にかかわらず、プールを使用して NAT 内部ソースリストを作成することによって、ダイナミック ソース変換を確立します。  <b>group</b> キーワードは、変換が属するグループを決定します。
ステップ 4	switch(config)# <b>ip nat pool</b> <i>pool-name</i> [ <i>startip endip</i> ] { <b>prefix</b> <i>prefix-length</i>   <b>netmask</b> <i>network-mask</i> }	グローバル IP アドレスの範囲で NAT プールを作成します。IP アドレスは、プレフィックス長または

	コマンドまたはアクション	目的
		ネットワークマスクを使用してフィルタリングされます。
ステップ 5	switch(config)# <b>interface</b> <i>type slot/port</i>	インターフェイスを設定し、インターフェイスコンフィギュレーションモードを開始します。
ステップ 6	switch(config-if)# <b>ip nat outside</b>	インターフェイスを外部ネットワークに接続します。
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、グローバルコンフィギュレーションモードに戻ります。
ステップ 8	switch(config)# <b>interface</b> <i>type slot/port</i>	インターフェイスを設定し、インターフェイスコンフィギュレーションモードを開始します。
ステップ 9	switch(config-if)# <b>ip nat inside</b>	NATの対象である内部ネットワークにインターフェイスを接続します。

### 例

次に、内部送信元アドレスのダイナミック双方向 NAT 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)# ip nat outside source static 2.2.2.2 4.4.4.4 group 20 dynamic
switch(config)# ip nat inside source list acl_1 pool pool_1 overload group 20 dynamic
switch(config)# ip nat pool pool_1 3.3.3.3 3.3.3.10 prefix-length 24
switch(config)# interface Ethernet1/8
switch(config-if)# ip nat outside
switch(config-if)# exit
switch(config)# interface Ethernet1/15
switch(config-if)# ip nat inside
```

## 外部送信元アドレスのダイナミック Twice NAT の設定

内部送信元変換の場合、トラフィックは外部インターフェイスから内部インターフェイスに流れます。外部送信元アドレスにダイナミック双方向 NATを設定できます。

### 始める前に

スイッチで NAT がイネーブルになっていることを確認します。

### 手順の概要

#### 1. switch# **configure terminal**



2. switch(config)# **ip nat inside source static** *inside-local-ip-address inside-global-ip-address* | [**tcp** | **udp**] *inside-local-ip-address local-port inside-global-ip-address global-port* [**group group-id**] [**dynamic**]
3. switch(config)# **ip nat outside source list** *access-list-name* [**interface type slot/port pool pool-name** ] [**group group-id**] [**add-route**] [**dynamic**]
4. switch(config)# **ip nat pool** *pool-name* [*startip endip*] {**prefix prefix-length** | **netmask network-mask**}
5. switch(config)# **interface type slot/port**
6. switch(config-if)# **ip nat outside**
7. switch(config-if)# **exit**
8. switch(config)# **interface type slot/port**
9. switch(config-if)# **ip nat inside**

手順の詳細

	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 nat inside source static</b> <i>inside-local-ip-address inside-global-ip-address</i>   [ <b>tcp</b>   <b>udp</b> ] <i>inside-local-ip-address local-port inside-global-ip-address global-port</i> [ <b>group group-id</b> ] [ <b>dynamic</b> ]	内部グローバルアドレスを内部ローカルアドレスに変換するか、または内部ローカルトラフィックを内部グローバルトラフィックに変換するようにスタティック NAT を設定します。  <b>group</b> キーワードは、変換が属するグループを決定します。
ステップ 3	switch(config)# <b>ip nat outside source list</b> <i>access-list-name</i> [ <b>interface type slot/port pool pool-name</b> ] [ <b>group group-id</b> ] [ <b>add-route</b> ] [ <b>dynamic</b> ]	プールを使用して NAT 外部送信元リストを作成することによって、ダイナミック送信元変換を確立します。
ステップ 4	switch(config)# <b>ip nat pool</b> <i>pool-name</i> [ <i>startip endip</i> ] { <b>prefix prefix-length</b>   <b>netmask network-mask</b> }	グローバル IP アドレスの範囲で NAT プールを作成します。IP アドレスは、プレフィックス長またはネットワークマスクを使用してフィルタリングされます。
ステップ 5	switch(config)# <b>interface type slot/port</b>	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 6	switch(config-if)# <b>ip nat outside</b>	インターフェイスを外部ネットワークに接続します。
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、グローバルコンフィギュレーションモードに戻ります。
ステップ 8	switch(config)# <b>interface type slot/port</b>	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 9	switch(config-if)# <b>ip nat inside</b>	NATの対象である内部ネットワークにインターフェイスを接続します。

例

次に、外部送信元アドレスにダイナミック双方向 NAT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)# ip nat inside source static 7.7.7.7 5.5.5.5 group 30 dynamic
switch(config)# ip nat outside source list acl_2 pool pool_2 group 30 dynamic
switch(config)# ip nat pool pool_2 4.4.4.4 4.4.4.10 prefix-length 24
switch(config)# interface Ethernet1/6
switch(config-if)# ip nat outside
switch(config-if)# exit
switch(config)# interface Ethernet1/11
switch(config-if)# ip nat inside
```

## ダイナミック NAT 変換のクリア

ダイナミック変換をクリアするには、次の作業を実行します。

コマンド	目的
<b>clear ip nat translation [ all   inside global-ip-address local-ip-address [outside local-ip-address global-ip-address]   outside local-ip-address global-ip-address ]</b>	すべてまたは特定のダイナミック NAT変換を削除します。

例

次に、すべてのダイナミック変換をクリアする例を示します。

```
switch# clear ip nat translation all
```

次に、内部アドレスと外部アドレスのダイナミック変換をクリアする例を示します。

```
switch# clear ip nat translation inside 2.2.2.2 4.4.4.4 outside 5.5.5.5 7.7.7.7
```

## ダイナミック NAT の設定の確認

ダイナミック NAT の設定を表示するには、次の作業を行います。

コマンド	目的
<b>show ip nat translations</b>	ダイナミック変換を含むアクティブなネットワーク アドレス変換 (NAT) 変換を表示します。  エントリが作成および使用された日時など、各変換テーブル エントリの追加情報を表示します。
<b>show ip nat translations verbose</b>	ダイナミック変換を含むアクティブなネットワークアドレス変換 (NAT) 変換を読みやすい形式で表示します。
<b>show run nat</b>	NAT の設定を表示します。

**例**

次に、NAT の実行コンフィギュレーションを表示する例を示します。

```
switch# show run nat

!Command: show running-config nat
!Time: Wed Apr 23 11:17:43 2014

version 6.0(2)A3(1)
feature nat

ip nat inside source list list1 pool pool1
ip nat inside source list list2 pool pool2 overload
ip nat inside source list list7 pool pool7 overload
ip nat outside source list list3 pool pool3
ip nat pool pool1 30.1.1.1 30.1.1.2 prefix-length 24
ip nat pool pool2 10.1.1.1 10.1.1.2 netmask 255.0.255.0
ip nat pool pool3 30.1.1.1 30.1.1.8 prefix-length 24
ip nat pool pool5 20.1.1.1 20.1.1.5 netmask 255.0.255.0
ip nat pool pool7 netmask 255.255.0.0
    address 40.1.1.1 40.1.1.5
```

次に、アクティブな NAT 変換を表示する例を示します。

オーバーロードのある内部プール

```
switch# show ip nat translation
Pro  Inside global      Inside local          Outside local         Outside global
icmp 20.1.1.3:64762     10.1.1.2:133         20.1.1.1:0           20.1.1.1:0
icmp 20.1.1.3:64763     10.1.1.2:134         20.1.1.1:0           20.1.1.1:0
```

```
switch# sh ip nat translations verbose
Pro Inside global      Inside local          Outside local         Outside global
any  1.1.1.1           10.1.1.2             ---                  ---
    Flags:0x1  Entry-id:0  State:0x0  Group_id:0  Format(H:M:S)  Time-left:0:0:-1
icmp 101.1.0.1:65351  101.0.0.1:0          102.1.0.1:231        102.1.0.1:231
    Flags:0x82  Entry-id:101  State:0x3  Group_id:0  VRF: red  Format(H:M:S)  Time-left:12:0:9
udp  101.1.0.1:65383  101.0.0.1:63         102.1.0.1:63         102.1.0.1:63
```

```

Flags:0x82 Entry-id:103 State:0x3 Group_id:0 VRF: red Format(H:M:S) Time-left:12:0:9
tcp 101.1.0.1:64549 101.0.0.1:8809 102.1.0.1:9087 102.1.0.1:9087
Flags:0x82 Entry-id:102 State:0x1 Group_id:0 VRF: red Format(H:M:S) Time-left:12:0:9

syn:0:1:9 fin-rst:12:0:9

```

オーバーロードのない外部プール

```

switch# show ip nat translation
Pro Inside global      Inside local      Outside local      Outside global
any ---                ---                177.7.1.1:0        77.7.1.64:0
any ---                ---                40.146.1.1:0        40.46.1.64:0
any ---                ---                10.4.146.1:0        10.4.46.64:0

switch# show ip nat translations verbose
Pro Inside global      Inside local      Outside local      Outside global
any 1.1.1.1            10.1.1.2         ---                ---
Flags:0x1 Entry-id:0 State:0x0 Group_id:0 Format(H:M:S) Time-left:0:0:-1
any 101.1.0.1         101.0.0.1        ---                ---
Flags:0x0 Entry-id:92 State:0x3 Group_id:0 VRF: red Format(H:M:S) Time-left:12:0:11

```

## NAT 統計情報の確認

ネットワーク アドレス変換 (NAT) 統計情報を表示するには、次の作業を実行します。

コマンド	目的
<b>show ip nat statistics</b>	ネットワーク アドレス変換 (NAT) 統計を表示します。

例

次に、**show ip nat statistics** コマンドのサンプル出力例を示します。

## NAT 統計情報のクリア

ネットワーク アドレス変換 (NAT) 統計情報をクリアするには、次のタスクを実行します。

コマンド	目的
<b>clear ip nat Statistics</b>	ネットワーク アドレス変換 (NAT) 統計情報 エントリをクリアします。

## 例

**clear ip nat statistics** コマンドは、ネットワーク アドレス変換 (NAT) 統計エントリをクリアします。

```
switch# clear ip nat statistics

-----
Total expired Translations: 0
SYN timer expired:
FIN-RST timer expired:
Inactive timer expired:
-----
Total Hits: 0
In-Out Hits: 0
Out-In Hits: 0
-----
Total Misses: 0
In-Out Misses: 0
Out-In Misses: 0
-----
Total SW Translated Packets: 0
In-Out SW Translated: 0
Out-In SW Translated: 0
-----
Total SW Dropped Packets: 0
In-Out SW Dropped: 0
-----
Address alloc. failure drop: 0
Port alloc. failure drop: 0
Dyn. Translation max limit drop: 0
ICMP max limit drop: 0
Allhost max limit drop: 0
-----
Inside / Outside source list:
Missed: 0
-----
```

## 例：ダイナミック変換および変換タイムアウトの設定

次に、アクセスリストを指定してダイナミックオーバーロードネットワークアドレス変換 (NAT) を設定する例を示します。

```
Switch> enable
Switch# configure terminal
Switch(config)# ip access-list acl1
Switch(config-acl)# permit ip 10.111.11.0/24 any
Switch(config-acl)# deny udp 10.111.11.100/32 any
Switch(config-acl)# exit
Switch(config)# ip nat inside source list acl1 interface ethernet 1/1 overload
Switch(config)# interface ethernet 1/4
Switch(config-if)# ip address 10.111.11.39 255.255.255.0
Switch(config-if)# ip nat inside
Switch(config-if)# exit
Switch(config)# interface ethernet 1/1
```

```
Switch(config-if)# ip address 172.16.232.182 255.255.255.240
Switch(config-if)# ip nat outside
Switch(config-if)# exit
Switch(config)# ip nat translation tcp-timeout 50000
Switch(config)# ip nat translation max-entries 300
Switch(config)# ip nat translation udp-timeout 45000
Switch(config)# ip nat translation timeout 13000
Switch(config)# end
```

## VRF 対応 NAT に関する情報

VRF 対応 NAT は、スタティックおよびダイナミック NAT 設定でサポートされます。トラフィックが、デフォルト以外の VRF（内部）から同じデフォルト以外の VRF（外部）に流れるように設定されている場合、IP NAT コマンドの `match-in-vrf` オプションを指定する必要があります。

トラフィックが、デフォルト以外の VRF（内部）からデフォルトの VRF（外部）に流れるように設定されている場合、IP NAT コマンドの `match-in-vrf` オプションを指定することはできません。NAT の内部設定がデフォルトの VRF インターフェイスで設定されている場合、NAT の外部設定はデフォルト以外の VRF インターフェイスではサポートされません。

NAT 内部インターフェイスの異なる VRF 間で重複したアドレスが設定されている場合、NAT 外部インターフェイスをデフォルトの VRF インターフェイスにすることはできませんたとえば、`vrfA` と `vrfB` が同じ送信元サブネットを持つ NAT 内部インターフェイスとして設定され、NAT 外部インターフェイスはデフォルト VRF として設定されていたとします。このような設定では、NAT 外部インターフェイスから NAT 内部インターフェイスへのパケットのルーティングがあいまいであるため、NAT はサポートされません。

## VRF 対応 NAT の設定

始める前に

スイッチで NAT がイネーブルになっていることを確認します。

手順の概要

1. `switch# configure terminal`
2. `switch(config)# [no] ip nat inside | outside source list ACL_NAME [interface INTERFACE NAME overload ][pool POOL NAME overload ] [group group-id] [dynamic] [ vrf <vrf-name> [match-in-vrf] ]`
3. `switch(config)# [no] ip nat inside | outside source static LOCAL IP GLOBAL IP | [tcp | udp LOCAL IP LOCAL PORT GLOBAL IP GLOBAL PORT ] [group group-id] [dynamic] [ vrf <vrf-name> [match-in-vrf] ]`
4. `switch(config)# interface type slot/port [ vrf <vrf-name ip nat inside | outside`

手順の詳細

	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] ip nat inside   outside source list ACL_NAME [interface INTERFACE NAME overload ] [pool POOL NAME overload ] [group group-id] [dynamic] [ vrf &lt;vrf-name&gt; [match-in-vrf] ]</b>	VRF 固有のダイナミック NAT を作成または削除します。  <b>group</b> キーワードは、変換が属するグループを決定します。
ステップ 3	switch(config)# <b>[no] ip nat inside   outside source static LOCAL IP GLOBAL IP   [tcp   udp LOCAL IP LOCAL PORT GLOBAL IP GLOBAL PORT ] [group group-id] [dynamic] [ vrf &lt;vrf-name&gt; [match-in-vrf] ]</b>	VRF 固有のスタティック NAT を作成または削除します。  <b>group</b> キーワードは、変換が属するグループを決定します。
ステップ 4	switch(config)# <b>interface type slot/port [ vrf &lt;vrf-name&gt; ip nat inside   outside</b>	VRF 対応インターフェイスで NAT をイネーブルにします。

**show run nat** コマンドの出力を参照してください。

```
#show run nat
...
feature nat
ip nat inside source static 1.1.1.1 1.1.1.100 vrf red match-in-vrf
ip nat outside source static 2.2.2.200 2.2.2.2 vrf red match-in-vrf add-route
ip nat inside source list nat-acl-in1 pool pool-in1 vrf red match-in-vrf overload
ip nat outside source list nat-acl-out1 pool pool-out1 vrf red match-in-vrf add-route
interface Ethernet1/3
 ip nat outside
interface Ethernet1/5
 ip nat inside

N3548#show ip nat translation verbose
Pro Inside global      Inside local          Outside local         Outside global
any 1.1.1.1            10.1.1.2              ---                   ---
  Flags:0x1  Entry-id:0  State:0x0  Group_id:0  Format(H:M:S)  Time-left:0:0:-1
icmp 101.1.0.1:65351  101.0.0.1:0          102.1.0.1:231        102.1.0.1:231
  Flags:0x82  Entry-id:101  State:0x3  Group_id:0  VRF: red  Format(H:M:S)  Time-left:12:0:9
udp 101.1.0.1:65383   101.0.0.1:63         102.1.0.1:63         102.1.0.1:63
  Flags:0x82  Entry-id:103  State:0x3  Group_id:0  VRF: red  Format(H:M:S)  Time-left:12:0:9
tcp 101.1.0.1:64549   101.0.0.1:8809       102.1.0.1:9087       102.1.0.1:9087
  Flags:0x82  Entry-id:102  State:0x1  Group_id:0  VRF: red  Format(H:M:S)  Time-left:12:0:9

syn:0:1:9  fin-rst:12:0:9
```







## 第 7 章

# IP イベント減衰の設定

- [IP イベント減衰 \(139 ページ\)](#)

## IP イベント減衰

IP イベント減衰機能は、設定可能な指数関数的減少メカニズムを導入し、過剰なインターフェイスフラッピングイベントによるネットワーク内のルーティングプロトコルおよびルーティングテーブルに対する影響を抑制します。ネットワークオペレータはこの機能を使用し、フラップが発生しているローカルインターフェイスをルータが自動的に特定して、選択的に減衰するように設定できます。

### 注意事項と制約事項

IP イベントダンプニング機能を設定する前に、次の注意事項と制約事項を参照してください。

- netstack-IP コンポーネントの変更により、すべての IP クライアントはダンプニングまたはインターフェイスの影響を観察します。
- インターフェイスのフラップごとに、一定のペナルティが追加されます。パラメータが設定されているペナルティは指数関数的に減衰します。
- ペナルティが特定の高レベルを超えると、インターフェイスは減衰されます。ペナルティが低レベルを下回っている間は、抑制されません。
- インターフェイスがダンプニングされると、IP アドレスとスタティックルートがインターフェイスから削除されます。IP のすべてのクライアントが IP 削除通知を受信します。
- インターフェイスの抑制が解除されると、IP アドレスと関連するルートが再び追加されます。IP のすべてのクライアントは、インターフェイスのすべての IP アドレスの IP アドレス追加通知を取得します。
- イーサネットインターフェイスに設定されたすべてのレイヤ3インターフェイス、ポートの変更、および SVI がこの機能をサポートしています。

## IP イベント減衰の概要

インターフェイス状態変化は、インターフェイスが管理上アップまたはダウンした場合や、インターフェイスで状態が変化した場合に発生します。インターフェイスで状態が変化したりフラップが発生すると、状態の変化に影響されるルートの状態がルーティングプロトコルに通知されます。インターフェイスの状態が変化するたびに、ネットワーク内のすべての影響を受けるデバイスで、最良パスを再計算し、ルーティングテーブルでルートをインストールまたは削除し、有効なルートをピアルータにアダプタイズする必要があります。過剰なフラップが発生する不安定なインターフェイスは、ネットワークの他のデバイスに大量のシステム処理リソースを消費させ、ルーティングプロトコルでフラップが発生しているインターフェイスとの同期が失われる原因になる可能性があります。

IP イベント減衰機能は、設定可能な指数関数的減少メカニズムを導入し、過剰なインターフェイスフラッピングイベントによるネットワーク内のルーティングプロトコルおよびルーティングテーブルに対する影響を抑制します。ネットワークオペレータはこの機能を使用し、フラップが発生しているローカルインターフェイスをルータが自動的に特定して、選択的に減衰するように設定できます。インターフェイスの減衰により、インターフェイスでフラップが発生せず安定するまで、ネットワークからインターフェイスが除外されます。IP イベント減衰機能を設定すると、悪影響が広がらないように障害を分離することで、コンバージェンス時間とネットワーク全体の安定性を向上します。これにより、ネットワークの他のデバイスのシステム処理リソースの使用率が減少し、ネットワーク全体の安定性が向上します。

## インターフェイス状態変化イベント

この項では、IP イベント減衰機能のインターフェイス状態変化イベントについて説明します。この機能は、過剰なインターフェイスのフラップや状態変化の影響を抑制するために使用される、設定可能な指数関数的減少メカニズムを採用しています。IP イベント減衰機能がイネーブルになっている場合、過剰なルート更新情報をフィルタリングすることによって、フラップが発生しているインターフェイスは、ルーティングプロトコルの観点から減衰されます。フラップが発生しているインターフェイスが特定され、ペナルティを割り当てられ、必要に応じて抑制され、インターフェイスが安定すればネットワークで利用可能になります。図1は、ルーティングプロトコルによってインターフェイス状態イベントが認識された場合を示しています。

### 抑制しきい値

抑制しきい値は、フラップが発生しているインターフェイスをルータが減衰するトリガーとなる、累積ペナルティの値です。フラップが発生しているインターフェイスはルータによって特定され、アップおよびダウン状態変化ごとにペナルティを割り当てられますが、インターフェイスは自動的に減衰されません。ルータは、フラップが発生しているインターフェイスの累積ペナルティをトラッキングします。累積ペナルティがデフォルトまたは設定済みの抑制しきい値に到達すると、インターフェイスが減衰状態になります。

### 半減期

半減期は、累積ペナルティの指数関数的な減少の速さを指定します。インターフェイスが減衰状態になると、ルータは、インターフェイスの以後のアップおよびダウン状態変化をモニタリ

ます。インターフェイスでペナルティの累積が続き、抑制しきい値の範囲内に留まっている間は、インターフェイスは減衰されたままです。インターフェイスが安定しフラップが発生しなくなると、半減期が終了するごとに、ペナルティが半分に減らされます。ペナルティが再使用しきい値に低下するまで、累積ペナルティが減らされていきます。半減期タイマーの設定可能な範囲は 1 ～ 30 秒です。デフォルトの半減期タイマーは 5 秒です。

## 再使用しきい値

累積ペナルティが減らされて再使用しきい値まで低下すると、ルートの抑制がなくなり、ネットワーク上の他のデバイスに対して使用可能になります。再使用値の範囲は 1 ～ 20000 ペナルティです。デフォルト値は 1000 ペナルティです。

## 最大抑制時間

最大抑制時間は、インターフェイスにペナルティが割り当てられている場合に、インターフェイスの抑制状態を維持できる時間の上限を表します。最大抑制時間は 1 ～ 255 秒で設定できます。最大ペナルティは、最大 20000 単位に切り捨てられます。累積ペナルティの最大値は、最大抑制時間、再使用しきい値、および半減期に基づいて算出されます。

## 関連コンポーネント

インターフェイスで減衰が設定されていない場合や、減衰が設定されていても抑制されていない場合、インターフェイス状態が移行しても IP イベント減衰機能によってルーティングプロトコルの動作が変更されることはありません。ただし、インターフェイスが抑制されている場合、インターフェイスの抑制がなくなるまで、ルーティングプロトコルとルーティングテーブルは、インターフェイスの状態移行の以降の影響を受けません。

## ルートタイプ

次のインターフェイスは、この機能の設定の影響を受けます。

- 接続ルート：
  - 減衰されたインターフェイスの接続ルートは、ルーティングテーブルにインストールされません。
  - 減衰されたインターフェイスの抑制がなくなり、インターフェイスがアップしていれば、接続ルートはルーティングテーブルにインストールされます。
- スタティック ルート：
  - 減衰されたインターフェイスに割り当てられているスタティック ルートは、ルーティングテーブルにインストールされません。
  - 減衰されたインターフェイスの抑制がなくなり、インターフェイスがアップしていれば、スタティック ルートはルーティングテーブルにインストールされます。



- (注) この機能を設定できるのはプライマリ インターフェイスのみです。また、すべてのサブインターフェイスには、プライマリ インターフェイスと同じ減衰設定が適用されます。IP イベント減衰は、インターフェイス上の個々のサブインターフェイスのフラップはトラッキングしません。

## サポートされているプロトコル

使用されるすべてのプロトコルは、IP イベント減衰機能の影響を受けます。IP イベント減衰機能は、Border Gateway Protocol (BGP)、Enhanced Interior Gateway Routing Protocol (EIGRP)、Hot Standby Routing Protocol (HSRP)、Open Shortest Path First (OSPF)、Routing Information Protocol (RIP)、および VRRP をサポートします。該当するインターフェイス IP アドレスへの ping および SSH は機能しません。



- (注) IP イベント減衰機能がイネーブルになっていない場合や、インターフェイスが減衰されていない場合は、ルーティングプロトコルへの影響はありません。

## IP イベント減衰の設定方法

### IP イベント減衰のイネーブル化

IP イベント減衰機能をイネーブルにするには、インターフェイス設定モードで **dampening** コマンドを入力します。すでに減衰が設定されているインターフェイスに対してこのコマンドを適用すると、減衰状態はすべてリセットされ、累積ペナルティが 0 に設定されます。インターフェイスが減衰されている場合、累積ペナルティは再使用しきい値まで低下し、減衰しているインターフェイスはネットワークに対して使用可能になります。ただし、フラップカウントは保持されます。

#### 手順の概要

1. **configure terminal**
2. **interface** *type number*
3. **dampening** [*half-life-period reuse-threshold*] [*suppress-threshold max-suppress [restart-penalty]*]
4. **end**

#### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<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	<b>interface</b> <i>type number</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、特定のインターフェイスを設定します。
ステップ 3	<b>dampening</b> [ <i>half-life-period reuse-threshold</i> ] [ <i>suppress-threshold max-suppress [restart-penalty]</i> ]	インターフェイス減衰をイネーブル化します。 <ul style="list-style-type: none"> <li>引数なしで <b>dampening</b> コマンドを入力すると、デフォルトの設定パラメータでインターフェイス減衰がイネーブルになります。</li> <li>手動で <i>restart-penalty</i> 引数のタイマーを設定する場合、すべての引数に対して手動で値を入力する必要があります。</li> </ul>
ステップ 4	<b>end</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。

## IP イベント減衰の確認

**show dampening interface** または **show interface dampening** コマンドを使用して、IP イベント衰退機能の設定を確認します。

### 手順の概要

1. **show dampening interface**
2. **show interface dampening**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>show dampening interface</b>	減衰されたインターフェイスを表示します。
ステップ 2	<b>show interface dampening</b>	減衰されたローカルルータ上のインターフェイスを表示します。





## 索引

### L

- LACP [45, 50, 52–53, 57, 59](#)
  - システム ID [50](#)
  - 設定 [57](#)
  - ポートチャンネル [50](#)
  - ポートチャンネル、MinLink [53, 59](#)
  - マーカー レスポンダ [52](#)
- LACP がイネーブルとスタティック [53](#)
  - ポートチャンネル [53](#)
- LACP 高速タイマー レート [60](#)
  - 設定 [60](#)
- LACP の設定 [57](#)
- LACP ポートプライオリティ [62](#)
  - 設定 [62](#)
- Link Aggregation Control Protocol [45](#)

### M

- MIB [28, 43](#)
  - レイヤ 2 インターフェイス [28](#)
  - レイヤ 3 インターフェイス [43](#)

### N

- NAT [122](#)
  - 確認 [122](#)

### P

- PAT [121](#)
  - 設定例 [121](#)

### S

- STP [45](#)
  - ポートチャンネル [45](#)
- SVI 自動ステート [6](#)
  - レイヤ 2 [6](#)
- SVI 自動ステート、ディセーブル化 [15](#)
  - レイヤ 2 [15](#)

### U

- UDLD [4, 6](#)
  - アグレッシブモード [6](#)
  - 定義 [4](#)
  - 非アグレッシブモード [6](#)
- UDLD モード A [10](#)
  - 設定 [10](#)

### V

- VLAN [31](#)
  - インターフェイス [31](#)
- VLAN インターフェイス [36](#)
  - 設定 [36](#)
- vPC [98](#)
  - ポートチャンネルの移行 [98](#)
- vPC の用語 [68](#)
- VRF [38](#)
  - インターフェイスの割り当て [38](#)

### い

- イーサネット インターフェイス [23](#)
  - デバウンス タイマー、設定 [23](#)
- インターフェイス [3–4, 29, 31–32, 35–38, 41–42](#)
  - UDLD [4](#)
  - VLAN [31, 36](#)
    - 設定 [36](#)
  - VRF への割り当て [38](#)
  - オプション [3](#)
  - シャーシ ID [3](#)
  - 帯域幅の設定 [35](#)
  - ルーテッド [29](#)
  - loopback [32, 37](#)
  - レイヤ 3 [29, 41–42](#)
    - 設定例 [42](#)
    - モニタリング [41](#)
- インターフェイス情報、表示 [25](#)
  - レイヤ 2 [25](#)

インターフェイス、設定 **115**  
 スタティック NAT **115**  
 インターフェイスの速度 **12**  
 設定 **12**

## か

外部アドレス **117**  
 スタティック NAT、設定 **117**  
 確認 **39**  
 レイヤ3 インターフェイス設定 **39**  
 関連資料 **43**  
 レイヤ3 インターフェイス **43**

## さ

再起動 **22**  
 イーサネット インターフェイス **22**  
 サブインターフェイス **30, 34–35**  
 設定 **34**  
 帯域幅の設定 **35**

## す

スタティック NAT **106, 114–115, 121–122**  
 インターフェイス、設定 **115**  
 確認 **122**  
 セキュリティ **106**  
 設定例 **121**  
 イネーブル化 **114**  
 スタティック NAT、設定 **116–117**  
 外部アドレス **117**  
 内部送信元アドレス **116**  
 スタティック PAT **121**  
 設定例 **121**  
 スタティック PAT、設定 **118**  
 ポート **118**

## せ

セキュリティ **106**  
 スタティック NAT **106**  
 設定 **21–22, 33–37, 39, 60, 62**  
 error-disabled ステート回復間隔 **21**  
 LACP 高速タイマー レート **60**  
 LACP ポートプライオリティ **62**  
 VLAN インターフェイス **36**  
 インターフェイス帯域幅 **35**  
 サブインターフェイス **34**  
 説明パラメータ **22**

設定 (続き)  
 ルーテッド インターフェイス **33**  
 ループバック インターフェイス **37**  
 レイヤ3 インターフェイス **39**  
 確認 **39**  
 設定例 **42, 121**  
 スタティック NAT **121**  
 レイヤ3 インターフェイス **42**

## た

bandwidth **35**  
 設定 **35**  
 ダイナミック NAT の設定の確認 **132**  
 ダイナミックプールの設定 **126**  
 単方向リンク検出 **4**

## ち

チャンネルモード **51, 57**  
 ポートチャンネル **51, 57**

## て

デバウンスタイマー **9**  
 パラメータ **9**  
 デバウンス タイマー、設定 **23**  
 イーサネット インターフェイス **23**  
 デフォルト設定 **32**  
 レイヤ3 インターフェイス **32**

## な

内部送信元アドレス **116**  
 スタティック NAT、設定 **116**

## は

パラメータ、概要 **9**  
 デバウンスタイマー **9**

## ひ

規格 **43**  
 レイヤ3 インターフェイス **43**

## ふ

物理イーサネットの設定 **27**



## ほ

- ポート **118**
  - スタティック PAT、設定 **118**
- ポートチャネリング **45**
- ポートチャンネル **35, 45–46, 48, 50, 53–54, 56–57, 63, 98**
  - LACP **50**
  - LACP がイネーブルとスタティック **53**
  - STP **45**
  - vPC への移行 **98**
  - 互換性要件 **46**
  - 作成 **53**
  - 設定の確認 **63**
  - 帯域幅の設定 **35**
  - チャンネルモード **57**
  - ポートの追加 **54**
  - ロードバランシング **48, 56**
    - ポートチャンネル **48**
- ポートチャンネル、MinLink **53, 59**
  - LACP **53, 59**
- ポートの追加 **54**
  - ポートチャンネル **54**

## む

- 無効化 **18, 22, 87**
  - CDP **18**
  - vPC **87**
  - イーサネット インターフェイス **22**

## も

- モニタリング **41**
  - レイヤ3 インターフェイス **41**

## ゆ

- イネーブル化 **18–20**
  - CDP **18**

イネーブル化 (続き)

- error-disabled の検出 **19**
- error-disable リカバリ **20**

## る

- ルーテッドインターフェイス **29, 33, 35**
  - 設定 **33**
  - 帯域幅の設定 **35**
- ループバック インターフェイス **32, 37**
  - 設定 **37**

## れ

- レイヤ2 **6, 15, 25**
  - SVI 自動ステート **6**
  - SVI 自動ステート、ディセーブル化 **15**
  - インターフェイス情報、表示 **25**
- レイヤ3 インターフェイス **29, 32–33, 39, 41–43**
  - MIB **43**
  - インターフェイス **43**
    - レイヤ3 **43**
    - MIB **43**
    - 関連資料 **43**
    - 規格 **43**
  - 確認 **39**
  - 関連資料 **43**
  - 設定例 **42**
  - デフォルト設定 **32**
  - 規格 **43**
  - モニタリング **41**
  - ルーテッドインターフェイスの設定 **33**

## ろ

- ロードバランシング **56**
  - ポートチャンネル **56**
  - 設定 **56**



## 翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。