



Cisco Nexus 9000 シリーズ NX-OS インターフェイス構成ガイド、リリース 10.4(x)

初版：2023年8月18日

シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

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

お問い合わせ先：シスコ コンタクトセンター
0120-092-255（フリーコール、携帯・PHS含む）

電話受付時間：平日 10:00～12:00、13:00～17:00

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

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS 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)

© 2023 Cisco Systems, Inc. All rights reserved.



目次

はじめに :

はじめに **xxi**

対象読者 **xxi**

表記法 **xxi**

Cisco Nexus 9000 シリーズ スイッチの関連資料 **xxii**

マニュアルに関するフィードバック **xxii**

通信、サービス、およびその他の情報 **xxiii**

第 1 章

新機能および変更された機能に関する情報 **1**

新機能および変更された機能に関する情報 **2**

第 2 章

概要 **9**

ライセンス要件 **9**

サポートされるプラットフォーム **9**

インターフェイスについて **9**

イーサネット インターフェイス **10**

アクセス ポート **13**

ルーテッド ポート **13**

管理インターフェイス **13**

ポートチャネル インターフェイス **13**

サブインターフェイス **14**

ループバック インターフェイス **14**

ブレイクアウト インターフェイス **14**

モジュール レベルのブレイクアウト **14**

ダイナミック ブレイクアウト (個別ポート レベルのブレイクアウト) **14**

レーンセレクトについて	16
ブレイクアウトインターフェイスの注意事項	16
Cisco NX-OS スイッチの USB ポートの無効化	24
仮想デバイス コンテキスト	24
インターフェイスのハイアベイラビリティ	25

第 3 章

基本インターフェイスパラメータの設定 27

基本インターフェイスパラメータについて	27
説明	27
ビーコン	27
エラーディセーブル化	28
MDIX	28
インターフェイスステータスエラーポリシー	28
インターフェイス MTU サイズの変更	29
帯域幅	31
スループット遅延	31
管理ステータス	31
UDLD パラメータ	32
UDLD の概要	32
UDLD のデフォルト設定	33
UDLD の通常モードとアグレッシブモード	33
ポートチャネルパラメータ	34
ポートプロファイル	35
Cisco QSFP+ to SFP+ アダプタモジュールのサポート	37
Cisco SFP+ アダプタモジュールのサポート	38
Cisco SFP-10G-T-X モジュールのサポート	38
注意事項と制約事項	39
デフォルト設定	47
基本インターフェイスパラメータの設定	47
設定するインターフェイスの指定	48
説明の設定	49

ビーコンモードの設定	52
Error-Disabled ステータスの設定	53
Error-Disable 検出のイネーブル化	53
error-disable ステータス回復のイネーブル化	55
error-disable ステータス回復間隔の設定	56
MDIX パラメータの設定	57
SFP-10G-TX のメディア タイプの設定	58
メディア タイプの確認	59
MTU サイズの設定	60
インターフェイス MTU サイズの設定	60
システム ジャンボ MTU サイズの設定	62
帯域幅の設定	63
スループット遅延の設定	65
インターフェイスのシャットダウンおよび再開	66
UDLD モードの設定	68
デバウンス タイマーの設定	72
ポートプロファイルの設定	75
ポートプロファイルの作成	76
ポートプロファイルコンフィギュレーションモードの開始およびポートプロファイルの修正	77
一定範囲のインターフェイスへのポートプロファイルの割り当て	78
特定のポートプロファイルのイネーブル化	79
ポートプロファイルの継承	80
一定範囲のインターフェイスからのポートプロファイルの削除	81
継承されたポートプロファイルの削除	82
リンク MAC アップタイマーの設定	83
25G 自動ネゴシエーションの設定	84
25G 自動ネゴシエーションの注意事項と制限事項	84
25G 自動ネゴシエーションによる FEC 選択	84
自動ネゴシエーションの有効化	85
自動ネゴシエーションのディセーブル化	86

基本インターフェイス パラメータの確認	87
インターフェイス カウンタのモニタリング	87
インターフェイス統計情報の表示	87
インターフェイス カウンタのクリア	89
DWDMの設定	89
QSA の設定例	91

第 4 章

レイヤ 2 インターフェイスの設定	93
アクセス インターフェイスとトランク インターフェイスについて	93
アクセス インターフェイスとトランク インターフェイスの概要	93
IEEE 802.1Q カプセル化	95
ドロップ適性インジケータ	96
アクセス VLAN	96
トランク ポートのネイティブ VLAN ID	96
ネイティブ VLAN トラフィックのタグging	97
Allowed VLANs	97
トランク インターフェイス上の最大 3967 の VLAN に対応するスイッチポートの分離	98
デフォルト インターフェイス	99
スイッチ仮想インターフェイスおよび自動ステート動作	99
SVI 自動ステート除外	99
SVI 自動ステートのディセーブル化	99
高可用性	100
カウンタ値	100
レイヤ 2 インターフェイスの前提条件	101
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	101
レイヤ 2 インターフェイスのデフォルト設定	107
アクセス インターフェイスとトランク インターフェイスの設定	108
アクセスおよびトランク インターフェイスの設定に関する注意事項	108
レイヤ 2 アクセス ポートとしての VLAN インターフェイスの設定	108
アクセス ホスト ポートの設定	110
トランク ポートの設定	112

802.1Q トランク ポートのネイティブ VLAN の設定	113
トランキング ポートの許可 VLAN の設定	115
ポートでの MAC アドレス制限の設定	117
スイッチポート分離の設定	119
デフォルト インターフェイスの設定	119
SVI 自動ステート除外の設定	121
システムの SVI 自動ステートのディセーブル化の設定	123
SVI 単位の SVI 自動ステートのディセーブル化の設定	124
ネイティブ VLAN トラフィックにタグを付けるためのデバイス設定	126
システムのデフォルト ポート モードをレイヤ 2 に変更	127
インターフェイス コンフィギュレーションの確認	129
レイヤ 2 インターフェイスのモニタリング	130
アクセス ポートおよびトランク ポートの設定例	130
関連資料	131

 第 5 章

レイヤ 3 インターフェイスの設定	133
レイヤ 3 インターフェイスについて	133
ルーテッド インターフェイス	133
サブインターフェイス	134
サブインターフェイスの制限事項	135
VLAN インターフェイス	135
インターフェイスの VRF メンバーシップの変更	136
インターフェイスの VRF メンバーシップの変更に関する注意事項	136
ループバック インターフェイス	137
IP アンナンバード	137
MAC 埋め込み IPv6 アドレス	138
高可用性	138
仮想化のサポート	138
DHCP クライアント	139
インターフェイスでの DHCP クライアントの使用に関する制限事項	139
レイヤ 3 スタティック MAC アドレス	140

レイヤ3 インターフェイスの前提条件	140
レイヤ3 インターフェイスの注意事項および制約事項	140
デフォルト設定	143
レイヤ3 インターフェイスの設定	143
ルーテッド インターフェイスの設定	143
ルーテッドインターフェイスでのサブインターフェイスの設定	145
ポートチャンネル インターフェイスでのサブインターフェイスの設定	147
VLAN インターフェイスの設定	148
VRF メンバーシップ変更時のレイヤ3 保持の有効化	150
レイヤ3 インターフェイス上のスタティック MAC アドレスの設定	150
ループバック インターフェイスの設定	152
イーサネット インターフェイスでの IP アンナバードの設定	153
IP アンナバード インターフェイスの OSPF の設定	154
IP アンナバード インターフェイスの ISIS の設定	156
SVI TCAM リージョンの設定	158
VRF へのインターフェイスの割り当て	160
MAC 埋め込み IPv6 アドレスの設定	161
インターフェイスでの DHCP クライアントの設定	164
SVI およびサブインターフェイスの入力/出力ユニキャストカウンタの設定	165
サブインターフェイスのマルチキャストおよびブロードキャストカウンタの設定	166
ハードウェア転送 IPv4/IPv6 インターフェイス統計情報の設定	168
レイヤ3 インターフェイス設定の確認	170
レイヤ3 インターフェイスのモニタリング	172
レイヤ3 インターフェイスの設定例	173
インターフェイスの VRF メンバーシップ変更の例	173
関連資料	175

双方向フローディング検出の設定 177

BFD について	177
非同期モード	177
BFD の障害検出	178

分散型動作	179
BFD エコー機能	179
セキュリティ	179
高可用性	179
仮想化のサポート	180
BFD の前提条件	180
注意事項と制約事項	180
デフォルト設定	185
BFD の設定	185
設定階層	185
BFD 設定のタスク フロー	185
BFD 機能のイネーブル化	186
グローバルな BFD パラメータの設定	187
インターフェイス上での BFD の設定	189
ポート チャネルの BFD の設定	190
BFD エコー機能の設定	192
メンバー単位リンク BFD セッションの設定	193
リンク単位の効率化に対処するための BFD 拡張機能	194
IETF 双方向フォワーディング検出の制限事項	194
ポート チャネルインターフェイスの設定	196
(任意) BFD スタート タイマーの設定	197
IETF リンク単位の BFD	197
BFD 宛先 IP アドレスの設定	198
マイクロ BFD セッションの設定の確認	198
例：マイクロ BFD セッションの設定	199
ルーティング プロトコルに対する BFD サポートの設定	202
BGP での BFD の設定	202
EIGRP での BFD の設定	203
OSPF での BFD の設定	205
IS-IS での BFD の設定	206
HSRP での BFD の設定	208

VRRP での BFD の設定	209
PIM (Protocol Independent Multicast) での BFD の設定	210
スタティック ルートでの BFD の設定	212
インターフェイスにおける BFD のディセーブル化	213
BFD 相互運用性の設定	214
ポイントツーポイント リンク内の Cisco NX-OS デバイスの BFD 相互運用性の設定	214
スイッチ仮想インターフェイス内の Cisco NX-OS デバイスの BFD 相互運用性の設定	215
論理モードの Cisco NX-OS デバイスの BFD 相互運用性の設定	216
Cisco Nexus 9000 シリーズ デバイスでの BFD 相互運用性の確認	217
BFD 設定の確認	218
BFD のモニタリング	218
BFD マルチホップ	219
BFD マルチホップのホップ数	219
BFD マルチホップの注意事項と制約事項	219
BFD マルチホップセッション グローバル インターバル パラメータの設定	220
マルチホップセッション単位の BFD パラメータの設定	221
BFD の設定例	223
BFDの例を表示	223
関連資料	224
RFC	224

第 7 章	ポート チャネルの設定	225
	ポート チャネルについて	225
	ポート チャネル	226
	ポートチャネル インターフェイス	227
	基本設定	228
	互換性要件	228
	ポート チャネルを使ったロード バランシング	230
	シンメトリック ハッシング	232
	ECMP の注意事項と制限事項	233
	復元力のあるハッシュ	233

GTP トンネル ロード バランシング	234
LACP	235
LACP の概要	235
ポートチャンネル モード	236
LACP ID パラメータ	238
LACP システム プライオリティ	238
LACP ポート プライオリティ	238
LACP 管理キー	239
LACP マーカー レスポンダ	239
LACP がイネーブルのポート チャンネルとスタティック ポート チャンネルの相違点	239
LACP 互換性の拡張	240
LACP ポート チャンネルの最小リンクおよび MaxBundle	241
LACP 高速タイマー	241
仮想化のサポート	242
高可用性	242
ポート チャネリングの前提条件	243
注意事項と制約事項	243
デフォルト設定	246
ポート チャンネルの設定	247
ポート チャンネルの作成	248
レイヤ 2 ポートをポート チャンネルに追加	249
レイヤ 3 ポートをポート チャンネルに追加	252
情報目的としての帯域幅および遅延の設定	254
ポート チャンネル インターフェイスのシャットダウンと再起動	255
ポート チャンネルの説明の設定	257
ポート チャンネル インターフェイスへの速度とデュプレックスの設定	258
ポート チャンネルを使ったロード バランシングの設定	259
MPLS タグ付けトラフィック用にポート チャンネルを使ったロード バランシングの構成	261
LACP のイネーブル化	263
LACP ポート チャンネル ポート モードの設定	264
LACP ポート チャンネル最少リンク数の設定	266

LACP ポートチャンネル MaxBundle の設定	267
LACP 高速タイマー レートの設定	268
LACP システム プライオリティの設定	270
LACP ポート プライオリティの設定	271
LACP システム MAC およびロールの設定	272
LACP グレースフル コンバージェンスのディセーブル化	273
LACP グレースフル コンバージェンスの再イネーブル化	275
LACP の個別一時停止のディセーブル化	276
LACP の一時停止個別 PXE のディセーブル化	277
LACP の個別一時停止の再イネーブル化	279
遅延 LACP の設定	280
ポート チャンネル ハッシュ分散の設定	282
グローバル レベルでのポート チャンネル ハッシュ分散の設定	282
ポート チャンネル レベルでのポート チャンネル ハッシュ分散の設定	283
ECMP の復元力のあるハッシュの有効化	284
ECMP の復元力のあるハッシュの無効化	285
ECMP ロード バランシングの設定	285
ECMP の復元力のあるハッシュ設定の確認	290
ポートチャンネル設定の確認	290
ポート チャンネル インターフェイス コンフィギュレーションのモニタリング	291
ポート チャンネルの設定例	291
関連資料	292

第 8 章

vPC の設定 293

vPC について	293
vPC の概要	293
vPC の用語	296
vPC ピア リンクの概要	297
プライマリおよびセカンダリ デバイス上で手動で設定する必要がある機能	300
ピアキープアライブ リンクとメッセージ	300
vPC ドメイン	302

vPC トポロジ	303
vPC インターフェイスの互換パラメータ	304
同じでなければならない設定パラメータ	305
同じにすべき設定パラメータ	306
パラメータの不一致によってもたらされる結果	307
vPC 番号	308
ヒットレス vPC ロールの変更	308
他のポート チャネルの vPC への移行	309
vPC オブジェクト トラッキング	309
その他の機能との vPC の相互作用	311
vPC と LACP	311
vPC ピア リンクと STP	311
vPC ピア スイッチ	314
vPC ピア ゲートウェイ	314
vPC および ARP または ND	315
vPC マルチキャスト : PIM、IGMP、および IGMP スヌーピング	315
マルチキャスト PIM デュアル DR (プロキシ DR)	317
IP PIM PRE-BUILD SPT	318
vPC ピア リンクとルーティング	318
vPC ピア リンクのレイヤ 3 バックアップ ルートの構成	319
CFSおE	320
vPC および孤立ポート	320
仮想化のサポート	321
停電後の vPC リカバリ	321
自動リカバリ	321
自動回復リロード遅延	321
リカバリ後の vPC ピア ロール	321
高可用性	322
vPC フォークリフト アップグレードシナリオ	322
注意事項と制約事項	325
レイヤ 3 および vPC 設定のベスト プラクティス	333

レイヤ 3 および vPC 設定の概要	333
レイヤ 3 および vPC のサポートされるトポロジ	334
レイヤ 3 リンクを使用した外部ルータとのピアリング	334
バックアップルーティングパス用 vPC デバイス間のピアリング	335
ルータ間の直接レイヤ 3 ピアリング	336
トランジットスイッチとして vPC デバイスを使用した 2 ルータの間のピアリング	337
パラレル相互接続ルーテッドポート上の外部ルータとのピアリング	337
パラレル相互接続ルーテッドポート上の vPC スイッチペア間のピアリング	338
非 vPC VLAN を使用する PC 相互接続および専用スイッチ間リンクを介したピアリング	338
vPC 接続を介した直接ピアリング	339
レイヤ 3 vPC 経由の設定	341
デフォルト設定	343
vPC の設定	343
vPC のイネーブル化	344
vPC のディセーブル化	345
vPC ドメインの作成と vpc-domain モードの開始	346
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	347
vPC ピアリンクの作成	349
他のポートチャネルの vPC への移行	351
vPC ピアリンクの構成の互換性チェック	352
グレースフル整合性検査の設定	353
vPC ピアゲートウェイの設定	354
vPC ピアスイッチの設定	356
純粋な vPC ピアスイッチトポロジの設定	356
孤立ポートの一時停止の設定	357
シングルモジュール vPC オブジェクトトラッキングでのトラッキング機能の設定	359
停電後のリカバリの設定	361
自動リカバリの設定	361
ヒットレス vPC ロール変更の設定	363
vPC ロールの変更に関する使用ケースシナリオ	364

vPC ドメイン MAC アドレスの手動での設定	365
システム プライオリティの手動での設定	366
vPC ピア デバイス ロールの手動での設定	368
Cisco MAC アドレスを使用するための STP の有効化	369
vPC 設定の確認	370
vPC のモニタリング	371
vPC の設定例	371
関連資料	373

第 9 章

IP トンネルの設定	375
IP トンネルについて	375
IP トンネルの概要	375
GRE トンネル	376
ポイントツーポイント IP-in-IP トンネルのカプセル化およびカプセル化解除	376
マルチポイント IP-in-IP トンネルのカプセル化解除	377
パス MTU ディスカバリ	377
高可用性	377
IP トンネルの前提条件	377
注意事項と制約事項	378
デフォルト設定	384
IP トンネルの設定	385
トンネリングのイネーブル化	385
トンネル インターフェイスの作成	386
ネットマスクを使用した IP-in-IP トンネルの作成	389
トンネル インターフェイスの設定	391
GRE トンネルの設定	394
Path MTU Discovery のイネーブル化	395
トンネル インターフェイスへの VRF メンバーシップの割り当て	396
IP トンネル設定の確認	397
IP トンネリングの設定例	398
関連資料	399

第 10 章	Q-in-Q VLAN トンネルの設定	401
	Q-in-Q トンネルについて	401
	Q-in-Q トンネリング	401
	ネイティブ VLAN のリスク	403
	レイヤ 2 プロトコルのトンネリングについて	404
	複数プロバイダー VLAN を使用した選択的 Q-in-Q	406
	VLAN のポート VLAN マッピングについて (着信 VLAN の変換)	407
	Q-in-Q トンネリングおよびレイヤ 2 プロトコル トンネリングの注意事項と制約事項	408
	複数プロバイダー VLAN を使用した選択的 Q-in-Q の注意事項と制約事項	410
	VLAN 上のポート VLAN マッピングに関する注意事項と制限事項	412
	Q-in-Q トンネルおよびレイヤ 2 プロトコルのトンネリングの設定	413
	802.1Q トンネル ポートの作成	413
	802.1Q トンネル ポートでの選択的 Q-in-Q の VLAN マッピングの設定	415
	複数プロバイダー VLAN で選択的 Q-in-Q を設定する	417
	Q-in-Q 用の EtherType の変更	419
	レイヤ 2 プロトコル トンネルのイネーブル化	419
	L2 プロトコル トンネル ポートに対するグローバル CoS の設定	421
	レイヤ 2 プロトコル トンネル ポートのしきい値の設定	422
	複合アクセス ポート機能セットの設定	423
	Q-in-Q 設定の確認	425
	Q-in-Q およびレイヤ 2 プロトコルのトンネリングの設定例	426
	VLAN 上のポート VLAN マッピングの構成	427
第 11 章	VLAN 上のポート VLAN マッピングの構成	431
	VLAN のポート VLAN マッピングについて (着信 VLAN の変換)	431
	VLAN 上のポート VLAN マッピングに関する注意事項と制限事項	432
	VLAN 上のポート VLAN マッピングの構成	433
第 12 章	スタティックおよびダイナミック NAT 変換の設定	437
	ネットワーク アドレス変換の概要	437

スタティック NAT に関する情報	438
ダイナミック NAT の概要	440
タイムアウトメカニズム	440
NAT の内部アドレスおよび外部アドレス	441
ダイナミック NAT のプール サポート	442
スタティックおよびダイナミック Twice NAT の概要	442
VRF 対応 NAT	443
スタティック NAT の注意事項および制約事項	445
ダイナミック NAT の制約事項	447
ダイナミック Twice NAT の注意事項および制約事項	449
TCP 認識 NAT の注意事項および制約事項	449
スタティック NAT の設定	450
スタティック NAT のイネーブル化	450
インターフェイスでのスタティック NAT の設定	450
内部送信元アドレスのスタティック NAT のイネーブル化	451
外部送信元アドレスのスタティック NAT のイネーブル化	452
内部送信元アドレスのスタティック PAT の設定	453
外部送信元アドレスのスタティック PAT の設定	454
スタティック Twice NAT の設定	455
no-alias 設定の有効化と無効化	457
スタティック NAT および PAT の設定例	459
例：スタティック Twice NAT の設定	460
スタティック NAT の設定の確認	460
ダイナミック NAT の設定	461
ダイナミック変換および変換タイムアウトの設定	461
ダイナミック NAT プールの設定	464
送信元リストの設定	466
内部送信元アドレスのダイナミック Twice NAT の設定	467
外部送信元アドレスのダイナミック Twice NAT の設定	468
FINRST および SYN タイマーの設定	470
ダイナミック NAT 変換のクリア	471

ダイナミック NAT の設定の確認	472
例：ダイナミック変換および変換タイムアウトの設定	475

第 13 章

IP イベント減衰の設定	477
IP イベント減衰の概要	477
注意事項と制約事項	478
インターフェイス状態変化イベント	478
抑制しきい値	478
半減期	479
再使用しきい値	479
最大抑制時間	479
関連コンポーネント	479
ルートタイプ	480
サポートされているプロトコル	480
IP イベント減衰の設定方法	480
IP イベント減衰のイネーブル化	480
IP イベント減衰の確認	481
IP ダンプニングパラメータのデフォルト設定	482

第 14 章

IP TCP MSS の設定	483
IP TCP MSS について	483
IP TCP MSS のデフォルト設定	483
IP TCP MSS の注意事項と制約事項	484
IP TCP MSS の設定	484
TCP 接続の MSS の設定	484
設定済み IP TCP MSS の削除	485
例：TCP 接続の MSS の設定	485
例：設定済み IP TCP MSS の削除	485
IP TCP MSS の確認	486

第 15 章

単一方向イーサネットの設定	487
----------------------	------------

単方向イーサネットの(UDE)概要	487
単一方向イーサネットの注意事項と制約事項	487
単一方向イーサネットの設定	488

第 16 章	レイヤ 2 Data Center Interconnect の設定	491
	概要	491
	レイヤ 2 Data Center Interconnect の例	492

第 17 章	Cisco NX-OS インターフェイスがサポートする IETF RFC	495
	IPv6 の RFC	495

第 18 章	Cisco NX-OS インターフェイスの設定制限	497
--------	----------------------------------	-----

第 19 章	400G デジタル コヒーレント光ファイバの構成	499
	400G デジタル コヒーレント光ファイバの概要	499
	400G デジタル コヒーレント光ファイバ パラメータ	500
	トラフィック構成パラメータ	503
	400G デジタル コヒーレント光ファイバの注意事項と制約事項	503
	ZR モジュールでの 400G デジタル コヒーレント光ファイバの構成	506
	ZRP モジュールでの 400G デジタル コヒーレント光ファイバ (DCO) の構成	508
	ブレイクアウトの設定	510
	400G デジタル コヒーレント光ファイバの確認	511
	400G コヒーレント光ファイバの構成例	511

付録 A :	ITU C-BAND テーブル	515
--------	------------------------	-----



はじめに

この前書きは、次の項で構成されています。

- [対象読者 \(xxi ページ\)](#)
- [表記法 \(xxi ページ\)](#)
- [Cisco Nexus 9000 シリーズ スイッチの関連資料 \(xxii ページ\)](#)
- [マニュアルに関するフィードバック \(xxii ページ\)](#)
- [通信、サービス、およびその他の情報 \(xxiii ページ\)](#)

対象読者

このマニュアルは、Cisco Nexus スイッチの設置、設定、および維持に携わるネットワーク管理者を対象としています。

表記法

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
bold	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、ユーザが値を指定する引数です。
[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、角かっこで囲み、縦棒で区切って示しています。
{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。

表記法	説明
[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。string の前後には引用符を使用しないでください。引用符を使用すると、その引用符も含めて string と見なされます。

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 screen 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。

Cisco Nexus 9000 シリーズ スイッチの関連資料

Cisco Nexus 9000 シリーズ スイッチ全体のマニュアルセットは、次の URL にあります。

http://www.cisco.com/en/US/products/ps13386/tsd_products_support_series_home.html

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。

通信、サービス、およびその他の情報

- シスコからタイムリーな関連情報を受け取るには、[Cisco Profile Manager](#) でサインアップしてください。
- 重要な技術によりビジネスに必要な影響を与えるには、[Cisco Services](#) [英語] にアクセスしてください。
- サービス リクエストを送信するには、[Cisco Support](#) [英語] にアクセスしてください。
- 安全で検証済みのエンタープライズクラスのアプリケーション、製品、ソリューション、およびサービスを探して参照するには、[Cisco Marketplace](#) にアクセスしてください。
- 一般的なネットワーク、トレーニング、認定関連の出版物を入手するには、[Cisco Press](#) にアクセスしてください。
- 特定の製品または製品ファミリの保証情報を探すには、[Cisco Warranty Finder](#) にアクセスしてください。

シスコバグ検索ツール

[Cisco バグ検索ツール](#) (BST) は、シスコ製品とソフトウェアの障害と脆弱性の包括的なリストを管理する Cisco バグ追跡システムへのゲートウェイとして機能する、Web ベースのツールです。BST は、製品とソフトウェアに関する詳細な障害情報を提供します。



第 1 章

新機能および変更された機能に関する情報

- [新機能および変更された機能に関する情報 \(2 ページ\)](#)

新機能および変更された機能に関する情報

表 1: 新機能および変更された機能

特長	説明	変更が行われたリリース	参照先
QDD-400G-ZR および QDD-400G-ZRP-S 光ファイバのサポート	<p>次のスイッチおよびラインカードでの QDD-400G-ZR および QDD-400G-ZRP-S 光ファイバのサポートが追加されました。</p> <ul style="list-style-type: none"> • X9624D-R2 ラインカードを搭載した Cisco Nexus 9508 スイッチ。 • Cisco Nexus 93600CD-GX、9316D-GX スイッチ、および X9716D-GX ラインカードを搭載した Cisco Nexus 9508/9504 スイッチ。 • Cisco Nexus X98900CD-A and X9836DM-A ラインカードを搭載した Cisco Nexus 9804/9808 スイッチ。 	10.4(2)F	<p>400G デジタル コヒーレント光ファイバの注意事項と制約事項 (503 ページ)</p> <p>トラフィック構成パラメータ (503 ページ)</p>
10 GB (QSA) および 25G (QSA28)	Cisco Nexus C93108TC-FX3 スイッチの QSA28 のサポートが追加されました	10.4(2)F	注意事項と制約事項 (39 ページ)

特長	説明	変更が行われたリリース	参照先
L2 転送	Cisco Nexus 93400LD-H1 プラットフォーム スイッチの L2 転送のサポートが追加されました。	10.4(2)F	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 (101 ページ)
L2 インフラ	Cisco Nexus 93400LD-H1 プラットフォーム スイッチの L2 インフラのサポートが追加されました。	10.4(2)F	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 (101 ページ)
L3 転送	Cisco Nexus 93400LD-H1 プラットフォーム スイッチの L3 転送のサポートが追加されました。	10.4(2)F	レイヤ3 インターフェイスの注意事項および制約事項 (140 ページ)
レイヤ3 物理およびサブインターフェイスの統計	Cisco Nexus C9232E-B1 プラットフォーム スイッチの L3 物理とサブインターフェイスの統計のサポートを追加	10.4(2)F	レイヤ3 インターフェイスの注意事項および制約事項 (140 ページ)
シングル ホップ BFD	Cisco Nexus C9232E-B1 スイッチのルーテッドサポート、ルーテッドサブインターフェイス、およびブレイクアウトポートでシングルホップ BFD のサポートを追加。	10.4(2)F	注意事項と制約事項 (180 ページ)
送信元/接続先 IP およびレイヤ4 ポート番号に基づくハッシュ化	Cisco Nexus C9232E-B1 スイッチの src/dst ip および src/dst L4 のポート番号ハッシュのサポートを追加。	10.4(2)F	注意事項と制約事項 (243 ページ)
ポートチャネルの機能拡張	レイヤ3 ポートチャネル Cisco Nexus C9232E-B1 スイッチのサポートを追加。	10.4(2)F	注意事項と制約事項 (243 ページ)

特長	説明	変更が行われたリリース	参照先
2x400G、8x100G、4x100G、4x25G、および2x50Gブレイクアウトオプション	Cisco Nexus C9232E-B1 スイッチのブレイクアウト (2x400G、8x100G、4x100G、4x25G、および2x50G) ポートのサポートを追加。	10.4(2)F	注意事項と制約事項 (39 ページ)
CVR-QSFP-SFP25G を介した 25G	Cisco Nexus FX3 シリーズスイッチ向け SFP28 のサポートが追加されました	10.4(1)F	注意事項と制約事項 (39 ページ)
インターフェイスカウインタのサポート	Cisco Nexus C9348GC-FX3PH のサポートと制限事項が追加された	10.4(1)F	注意事項と制約事項 (39 ページ)
管理インターフェイス	管理インターフェイスの設定手順と例を追加	10.4(1)F	説明の設定 (49 ページ)
MPLS タグ付きトラフィックの Port-channel load-balance コマンド	MPLS タグ付きトラフィックの Port-channel load-balance コマンドの構成を追加	10.4(1)F	MPLS タグ付けトラフィック用にポートチャネルを使ったロードバランシングの構成 (261 ページ)
Nexus 9800 36 ポート QSFP-DD 400G ラインカードの 4 X 25、および 4 X 10G ブレイクアウトオプション	Cisco Nexus 9808/9804 プラットフォームスイッチの N9K-X9836DM-A ラインカードのブレイクアウト (4x10G および 4x25G) ポートサポートが追加されました。	10.4(1)F	ブレイクアウト インターフェイスの注意事項 (16 ページ) 注意事項と制約事項 (39 ページ)
ネイティブ速度 AN (100G/40G)	Cisco Nexus 9332D-H2R プラットフォームスイッチの 100G/40G ポートの自動ネゴシエーションのサポートを追加。	10.4(1)F	注意事項と制約事項 (39 ページ)

特長	説明	変更が行われたリリース	参照先
L2 転送	Cisco Nexus 9332D-H2R プラットフォーム スイッチの L2 転送のサポートを追加。	10.4(1)F	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 (101 ページ)
L2 インフラ	Cisco Nexus 9332D-H2R プラットフォーム スイッチの L2 インフラのサポートを追加。	10.4(1)F	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 (101 ページ)
L3 転送	Cisco Nexus 9332D-H2R プラットフォーム スイッチの L3 転送のサポートを追加。	10.4(1)F	レイヤ3 インターフェイスの注意事項および制約事項 (140 ページ)
L3 物理およびサブインターフェイスの統計	Cisco Nexus 9804 プラットフォーム スイッチの L3 物理とサブインターフェイスの統計のサポートを追加。	10.4(1)F	レイヤ3 インターフェイスの注意事項および制約事項 (140 ページ)
ハッシュ ベース	Cisco Nexus 9804 プラットフォーム スイッチの L3、ループバックとサブインターフェイスのサポートを追加。	10.4(1)F	レイヤ3 インターフェイスの注意事項および制約事項 (140 ページ)
送信元/接続先 IP および L4 ポート番号に基づくハッシュ化	Cisco Nexus 9804 プラットフォーム スイッチの src/dst ip および src/dst L4 のポート ナンバーハッシュ サポートを追加。	10.4(1)F	注意事項と制約事項 (243 ページ)
シングル ホップ BFD	Cisco Nexus 9804 プラットフォーム スイッチのルーテッドポート、ルーテッドサブインターフェイス、およびブレイクアウトポートでシングルホップ BFD に追加のサポートをします。	10.4(1)F	注意事項と制約事項 (180 ページ)

特長	説明	変更が行われたリリース	参照先
UDLD	Cisco Nexus 9804 プラットフォームスイッチの UDLD のサポートを追加	10.4(1)F	注意事項と制約事項 (39 ページ)
シングル ホップ BFD	Cisco Nexus 9808 および 9804 スイッチを搭載した N9KX98900CD-A および N9KX9836DM-A ラインカードでのシングルホップ BFD のサポートを追加。	10.4(1)F	注意事項と制約事項 (180 ページ)
送信元 / 接続先 IP および L4 ポート番号に基づくハッシュ化	Cisco Nexus 9808 および 9804 スイッチを搭載した N9KX98900CD-A および N9KX9836DM-A で、src/dst ip および src/dst L4 ポート番号のハッシュサポートを追加。	10.4(1)F	注意事項と制約事項 (243 ページ)
L3 物理およびサブインターフェイスの統計	Cisco Nexus 9808 および 9804 スイッチを搭載した N9KX98900CD-A および N9KX9836DM-A ラインカードの L3 物理およびサブインターフェイスの統計サポートを追加。	10.4(1)F	レイヤ3 インターフェイスの注意事項および制約事項 (140 ページ)
UDLD	Cisco Nexus 9808 および 9804 スイッチを搭載した N9KX98900CD-A および N9KX9836DM-A ラインカードでの UDLD のサポートを追加。	10.4(1)F	注意事項と制約事項 (39 ページ)

特長	説明	変更が行われたリリース	参照先
CVR-QSFP-SFP10G アダプタを使用した 10G オプティクスのサポート	Cisco Nexus 9804 プラットフォームスイッチ、および Cisco Nexus X98900CD-A and X9836DM-A ラインカードの CVR-QSFP-SFP10G アダプタを使用した 10G 光ファイバサポートを追加。	10.3(1)F	注意事項と制約事項 (39 ページ)
トンネル拡張	GRE での IPv4 トンネルのサポートを追加	10.4(1)F	ポイントツーポイント IP-in-IP トンネルのカプセル化およびカプセル化解除 (376 ページ)
LACP 拡張	Nexus 9800 シリーズスイッチの LACP レイヤ 3 ポートチャネルのサポートを追加	10.4(1)F	注意事項と制約事項 (243 ページ)
400G デジタル コヒーレント光ファイバの構成	Cisco Nexus 9300-GX2 および 9408 プラットフォームスイッチでの 400G デジタル コヒーレント光ファイバのサポートを追加。	10.4(1)F	400G デジタル コヒーレント光ファイバの構成 (499 ページ)



第 2 章

概要

- [ライセンス要件 \(9 ページ\)](#)
- [サポートされるプラットフォーム \(9 ページ\)](#)
- [インターフェイスについて \(9 ページ\)](#)
- [仮想デバイス コンテキスト \(24 ページ\)](#)
- [インターフェイスのハイ アベイラビリティ \(25 ページ\)](#)

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 ライセンス ガイド](#)』および『[Cisco NX-OS ライセンス オプション ガイド](#)』を参照してください。

サポートされるプラットフォーム

Cisco NX-OS リリース 7.0(3)I7(1)以降、「[Nexus スイッチプラットフォーム サポートマトリックス](#)」に基づき、選択した機能が Cisco NX-OS のどのリリースから Cisco Nexus 9000 および 3000 スイッチでサポートされるようになったかを知ることができます。

インターフェイスについて

Cisco NX-OS は、サポート対象の各インターフェイスタイプの複数の設定パラメータをサポートします。ほとんどのパラメータはこのマニュアルで説明しますが、一部は他のマニュアルで説明します。

以下の表に、インターフェイスに設定できるパラメータの情報の入手先を示します。

表 2: インターフェイスのパラメータ

機能	パラメータ	解説場所
基本パラメータ	説明、デュプレックス、エラー ディセーブル、フロー制御、MTU、ビーコン	「基本インターフェイス パラメータの設定」
レイヤ 3	メディア、IPv4およびIPv6アドレス	「レイヤ 3 インターフェイスの設定」
レイヤ 3	帯域幅、遅延、IP ルーティング、VRF	『Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide』 『Cisco Nexus 9000 Series NX-OS Multicast Routing Configuration Guide』
ポート チャンネル	チャンネル グループ、LACP	『ポート チャンネルの設定』
セキュリティ	EOU	『Cisco Nexus 9000 Series NX-OS Security Configuration Guide』

イーサネット インターフェイス

- イーサネット インターフェイスには、ルーテッド ポートが含まれます。

Cisco NX-OS リリース 10.1(1) の場合、ポートグループサポート : GX では次のサポートを提供しています。

- N9K-C93600CD-GX には次のポイントが適用されます。
 - ポート 1 ~ 24 の場合、4 個のポート (1-4、5-8、9-12 など「クワッド」と呼ばれます) はすべて、同じ速度で動作します。
 - クワッド内のすべてのポートは、QSA を搭載した 10G、または 40G または 100G で動作します。
 - 同じクワッド内では混合速度はサポートされません。
 - QSA では、クワッド内のすべてのポートが 10G の速度で動作できます。
 - クワッドの速度は、クワッドの最初のポートに接続されているトランシーバではなく、そのクワッドに接続されている最初のトランシーバタイプによって決まります。たとえば、ポート 14 (ポート 13 ~ 16 を含むクワッドに属する) が、クワッドの最初のポートとして QSA が接続された 10G トランシーバの場合、クワッド内の他のすべてのポートの速度は 10G になります。

同様に、ポート 23（クワッド 21 - 24 に属する）がクワッドの最初のポートとして 40G トランシーバに接続されている場合、他のすべてのポートは 40G トランシーバに接続する必要があります。

- 100G トランシーバがポート 24 に接続され、ポート 21 がすでに 40G トランシーバに接続されている場合、100G インターフェイスは「XCVR 速度不一致」状態になり、リンク アップしません。
- 100G トランシーバを搭載したポート 24 をリンク アップするには、そのクワッド内の他のすべての非 100G トランシーバを接続し、ポート 24 をフラップする必要があります。
- これは、QSA + 10G トランシーバがすでにクワッドに接続されているポートに QSA + 10G を挿入した場合と同じです。
- Mismatch Transceiver をクワッドに接続すると、「Interface Ethernet1 / X is down (Reason : Inserted Transceiver Speed Mismatch with Quad Speed Y)」と syslog が生成されます。
- ポート 4 が 100G トランシーバに接続され、その後ポート 1 に 40G トランシーバが接続されている場合、100G はしてアップしますが、40G トランシーバはリンク アップせず、「XCVR 不一致速度」になります。この設定がスタートアップ コンフィギュレーションとしてコピーされ、スイッチがリロードされると、スイッチが起動した後、100G トランシーバが起動し、40G トランシーバが「XCVR 不一致速度」状態になります。
- ポート番号はクワッドの速度を決定せず、すべてのインターフェイスがクワッドの「Admin shut」状態であっても、最初に接続されたトランシーバのみが速度を決定します。「copy running-config startup-config」が実行され、スイッチがリロードされると、同じ状態が保持されます。ただし、スイッチが「Reload ascii」オプションでリロードされると、スイッチが起動した後、クワッド内の最初のポート（プラグインされたトランシーバを使用）がポート グループを決定します。その他の不一致のトランシーバは「XCVR 不一致速度」になります。
- 40G トランシーバを起動する必要がある場合は、100G トランシーバを削除する必要があります。そのクワッド内の他のすべてのポートは、そのクワッド内のすべてのトランシーバをリンクするために、空にするかまたは 40G トランシーバのみで接続できます。
- これに対する唯一の例外は、クワッドに 40G トランシーバがあり、40G 速度で設定されたデュアルレート トランシーバ（40G/100G 対応）を接続すると、40G 速度のデュアルレート トランシーバがリンク アップする場合です。ポート番号はクワッドの速度を決定せず、すべてのインターフェイスがクワッドの「Admin shut」状態であっても、最初に接続されたトランシーバだけがクワッドの速度を決定します。「copy running-config startup-config」が実行され、スイッチがリロードされたときに同じ状態が維持されますが、スイッチが「Reload ascii」オプションでリロードされると、スイッチが起動した後、最初のポート（トランシーバが差し込まれた状態）がクワッドはクワッドの速度を決定し、他の不一致のトランシーバは「XCVR 不一致速度」になります。

- 中断や不確定な状態を避けるために、クワッドでは同じ速度のトランシーバのみを使用することを強くお勧めします。クワッドポート 25～26 と他のクワッドポート 27～28 に対して同じロジックが拡張されます。

- N9K-C9316D-GX の場合：ポート 1～16 は QSA で 400G/100G/40G および 10G をサポートし、ポート グループの制限はありません。
- Cisco Nexus NX-OS Release 10.1(2) 以降では、NX-OS N9K-C93600CD-GX、N9K-C9316D-GX、および N9K-C9364C-GX の速度 40G および 100G で自動ネゴシエーションがサポートされています。
- 同じクワッド内では混合速度はサポートされません。
- QSA では、クワッド内のすべてのポートが 10G の速度で動作できます。

Cisco Nexus 9000 C9408 シャーシ、N9K-X9400-16W（16x200G ラインカード拡張モジュール（LEM））ポートには、次の注意事項と制約事項があります。

- ネイティブ ポートは、すべてのポートで 100G、40G、10G をサポートします。
- ブレークアウト ポートは 4x10G、4x25G をサポートしますが、次の制限があります。
 1. 4x10G、4x25G ブレークアウト ポートは、奇数ポートでのみサポートされます。
 2. ブレークアウト x4 が奇数ポートに構成されている場合、次に対応する偶数ポートが自動的に消去されます。
- ブレークアウト ポートは、次の制限付きで 2x50G をサポートします。
 1. 2x50G ブレークアウトは、奇数ポートと偶数ポートでサポートされます。
 2. 2x50G ブレークアウトが奇数/偶数ポートで構成されている場合、対応する偶数/奇数ポートは自動的に 2x50G にブレークアウトされます。
- QSA を使用した 10G は、次の制限付きですべてのポートでサポートされます。
 1. 10G トランシーバがリンクアップ状態の奇数/偶数ポートに存在する場合、対応する偶数/奇数ポートでは他の速度は許可されません。不一致の XCVR に関する警告/syslog が出力され、後で挿入された XCVR ポートのポート ステータスが **速度不一致**状態に変更されます。また、ポートのステータスは、**show interface brief** および **show interface status** コマンドの出力に示されます。
 2. 100G/40G トランシーバがリンクアップ状態の奇数/偶数ポートに存在し、10G トランシーバが対応する偶数/奇数ポートに挿入されると、XCVR の不一致に関する警告/syslog が出力され、後で挿入された XCVR ポートの **速度不一致**状態にポート ステータスに変更されます。また、ポートのステータスは、**show interface brief** および **show interface status** コマンドの出力に示されます。

3. 奇数ポートに40G/100Gがあり、対応する偶数ポートに10Gトランシーバがある場合、またはその逆の場合、**admin shut** ステータスではポートが **admin shut** のままである限り優先順位が決定されず、**nosshutdn** として構成されているポートが優先されます。
4. 奇数ポートに40G/100Gがあり、対応する偶数ポートに10Gトランシーバがある場合、またはその逆の場合、**admin shut** ステータスで、両方のポートが同時に **no shutdown** として構成されている場合、ソフトウェアによって最初に検出されたポートが優先され、その他は **xcvr 不一致** 状態になります。
5. 手順 4 (13 ページ) の状態に到達すると、この状態でスイッチがリロードされる場合、再度のブートアップ時にソフトウェアによって最初に検出されたポートが優先され、残りは **速度不一致** 状態になります。

アクセスポート

アクセスポートは1つのVLANのトラフィックを送受信します。このポートのタイプはレイヤ2インターフェイスだけです。

アクセスポートの詳細については、「アクセスインターフェイスとトランクインターフェイスについて」の項を参照してください。

ルーテッドポート

ルーテッドポートは、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。ルーテッドポートはレイヤ3インターフェイスだけです。

ルーテッドポートの詳細については、「ルーテッドインターフェイス」の項を参照してください。

管理インターフェイス

管理イーサネットインターフェイスを使用して、Telnetクライアント、簡易ネットワーク管理プロトコル(SNMP)、その他の管理エージェントを使用するリモート管理用ネットワークにデバイスを接続できます。管理ポート(mgmt0)は、自動検知であり、10/100/1000 Mb/sの速度の全二重モードで動作します。

管理インターフェイスの詳細については、『[Cisco Nexus 9000 Series NX-OS Fundamentals Configuration Guide](#)』を参照してください。

ポートチャネルインターフェイス

ポートチャネルは、複数の物理インターフェイスを集約した論理インターフェイスです。最大32の物理ポートへの個別リンク(1つのポートチャネルにバンドルして、帯域幅と冗長性を向上させることができます。ポートチャネルインターフェイスの詳細については、「ポートチャネルの設定」を参照してください。

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使用作成できます。親インターフェイスは物理ポートでもポート-チャンネルでもかまいません。親インターフェイスは物理ポートでもかまいません。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。

ループバック インターフェイス

ループバック インターフェイスは、常にアップ状態にある単独のエンドポイントを持つ仮想インターフェイスです。パケットが仮想ループバック インターフェイスを通じて送信されると、仮想ループバック インターフェイスですぐに受信されます。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。サブインターフェイスの詳細については、「ループバック インターフェイス」の項を参照してください。

ブレイクアウト インターフェイス

Cisco NX-OSは、モジュールレベルまたはポート単位のレベルで、1つ以上の低帯域幅インターフェイスへの高帯域幅インターフェイスのブレイクアウトをサポートします。

モジュール レベルのブレイクアウト

モジュール レベルのブレイクアウトでは、**interface breakout** コマンドにより、モジュールの高帯域幅 40G インターフェイスが4つの 10G インターフェイスに分割されます。コマンドが実行されると、モジュールがリロードされ、インターフェイスの設定は削除されます。

次に、コマンドの例を示します。

```
switch# configure terminal
switch(config)# interface breakout module 1
Module will be reloaded. Are you sure you want to continue(yes/no)? yes
```

no interface breakout module module_number コマンドはブレイクアウト設定を取り消します。モジュールのすべてのインターフェイスを 40G モードにし、前の 10G インターフェイスの設定を削除します。

ダイナミック ブレイクアウト（個別ポート レベルのブレイクアウト）

ダイナミックブレイクアウト（個別ポートレベルのブレイクアウト）の場合、**interface breakout** コマンドにより、広帯域幅の 40G ポートが4つの 10G ブレイクアウト ポートに、100G ポートが4つの 25G ブレイクアウト ポートに分割されます。ブレイクアウト ポートは、**Ethernet** <slot>/<front-panel-port>/<breakout-port> として識別されます。。たとえば、ポート単位のブレイクアウトポートは、Ethernet 1/2/1、Ethernet 1/2/2、Ethernet 1/2/3、およびEthernet 1/2/4として識別できます。

モジュールの1つ以上の40Gインターフェイスがポート単位のレベルでブレークアウトされると、コマンドの実行時にインターフェイスの設定が削除されます。



(注) ポート単位のブレークアウトでは、モジュールをリロードする必要はありません。

次に、ブレークアウトポートを設定する例を示します。

```
switch(config)# interface breakout module 1 port 1 map 10g-4x
switch(config)#
```

次に、複数のブレークアウトポートを設定する例を示します。

```
switch(config)# interface breakout module 1 port 1-4 map 10g-4x
switch(config)#
```

次に、40G インターフェイスと 10G インターフェイスを混在させて設定する例を示します。

```
switch(config-if)# show int eth1/49 transceiver
Ethernet1/49
transceiver is present
type is QSFP-40G-SR-BD
name is CISCO-AVAGO
part number is AFBR-79EBPZ-CS2
revision is 01
```

```
switch(config-if)# show int eth1/52 transceiver
Ethernet1/52
transceiver is present
type is QSFP-Cazadero
name is CISCO-DNI
part number is CAZADERO-R
revision is 03
nominal bitrate is 10000 MBit/sec per channel
```

```
switch(config-if)# show int eth1/53 transceiver
Ethernet1/53
transceiver is present
type is QSFP-Cazadero
name is CISCO-DNI
part number is CAZADERO-R
revision is 03
nominal bitrate is 10000 MBit/sec per channel
```

```
switch(config)# interface breakout module 1 port 52-53 map 10g-4x
```

```
switch(config-if)# show int br | i up
mgmt0 -- up 10.122.160.192 100 1500
Eth1/49 -- eth routed up none 40G(D) -- << Running 40G
Eth1/50 -- eth routed up none 40G(D) --
Eth1/52/1 -- eth routed up none 10G(D) -- << Broken out to 10G
Eth1/53/1 -- eth routed up none 10G(D) -- << Broken out to 10G
```

ブレークアウト ポートは **no interface breakout** コマンドで取り消すことができます。

次に、ブレークアウトポートを元に戻す例を示します。

```
switch(config)# no interface breakout module 1 port 1 map 10g-4x
switch(config)#
```

レーンセレクトタについて

レーンセレクトタは、Cisco Nexus スイッチ上にある（前面パネルの左側にあり「LS」というラベルが付いている）押しボタン式のスイッチと4つのLEDです。この押しボタン式のスイッチとLEDは、ポートのステータスを確認するために使用されます。レーンセレクトタは、Cisco Nexus 9000 シリーズ スイッチと Cisco Nexus 3164 および 3232 スイッチでサポートされています。

デフォルトでは、このLEDによって、1 x 40G 設定のリンク/アクティビティステータスが示されます。ポートが4 x 10G として設定されている場合は、このレーンセレクトタを使用して各10G ポートのリンクステータスを個別に確認できます。

レーンセレクトタの押しボタンを押すと、選択したレーンのリンク/アクティビティステータスがポートLEDに表示されます。押しボタンを押すと、1回目には最初のLEDに最初のポートのステータスが表示されます。2回目には2番目のポートのステータスが示され、以降同様です。押しボタンをこのように押すことで、4つのポートのステータスを個別に確認できます。

たとえば、ポート60が4 x 10G として設定されている場合、レーンセレクトタの押しボタンを1回押すと、60/1/1のリンクステータスが表示されます。押しボタンをもう一度押すと、60/1/2のリンクステータスが表示されます。

最後のポートのステータスが表示された後に押しボタンを押すと、4つのLEDがすべて消灯します。これは、レーンセレクトタがデフォルトの1 x 40G 設定のステータスを表示する状態に戻ったことを示します。



(注) 10Gブレイクアウトポートに対してビーコン機能が設定されている場合は、そのポートのLEDが点滅します。



(注) ポートが10Gブレイクアウトモードになるように設定されており、レーンが選択されていないときは、いずれかの10Gブレイクアウトポートだけが稼働している場合でも、40GポートのLEDが緑色で点灯します。

ブレイクアウトインターフェイスの注意事項

Cisco Nexus 9516スイッチは、モジュール8〜16のブレイクアウトをサポートしていません。

Cisco NX-OS リリース 9.2(1) 以降、N9K-9636C-R、N9K-X9636Q-R、およびN9K-X9636C-RX ラインカードは、40Gポートの4x10ギガビットへの分割をサポートします。

Cisco NX-OS リリース 9.2(2) 以降では、N9K-X9636C-R およびN9K-X9636C-RX ラインカードは、100Gポートの4x25ギガビットへの分割をサポートします。Cisco NX-OS リリース 9.3(3) 以降では、N9K-X9636C-R およびN9K-X9636C-RX のデフォルトFECモードは25Gx4 および

50Gx2 の FC-FEC です。N9K-C9636C-R は RS-FEC をサポートしておらず、N9K-X96136 YC-R ラインカードはブレイクアウトをサポートしていません。

Cisco Nexus 93600CD-GX スイッチは、28 個の 40/100 ギガビット QSFP28 ポート、8 個の 100/400 ギガビット QSFP-DD ポート、2 個の管理ポート、1 個のコンソールポート (RS-232) および 1 個の USB ポートを提供する、1 ラックユニット (RU) 固定ポートスイッチです。Cisco Nexus 93600CD-GX スイッチは、ブレイクアウト機能をサポートしています。

Cisco NX-OS リリース 9.3(3) 以降では、Cisco Nexus 9500 R シリーズスイッチは 100G ポートの 2x50 ギガビットへのブレイクアウトをサポートしています。

次の表に、サポートされているブレイクアウトモードまたはサポートされていないブレイクアウトモードの詳細情報を示します。詳細については、次の「[Cisco Nexus データシート](#)」を参照してください。

表 3: ブレイクアウトモードのサポートマトリックス

スイッチ	4x10G	4x25G	2x50G
N9K-X9636C-RX	はい	○	○
N9K-X9636C-R	はい	○	○
N9K-X9636Q-R	はい	いいえ	いいえ
N9K-X96136YC-R	いいえ	いいえ	いいえ
N9K-93108TC-EX	はい	○	○
N9K-93180YC-EX	はい	○	○
N9K-93180YC-FX	はい	○	○
N9K-9348GC-FXP	はい	○	○
N9K-93108TC-FX3P	はい	○	○
N9K-C9364D-GX2A	はい	○	○
N9K-X9836DM-A	はい	○	○



(注) N9K-X9636C-R および N9K-X9636C-RX ラインカードを搭載した Nexus 9500 R シリーズスイッチでは、限定的な光入出力 (QSFP-100G-PSM4-S、QSFP-100G-AOC、QSFP-100G-CU1M-CU3M) と、2x50G および 4x25G へのブレイクアウトがサポートされています。詳細については、『*Cisco IPICS Compatibility Matrix*』を参照してください。

不具合

- Cisco NX-OS リリース 7.0(3)I7(2) では、QSA ポートの手動ブレイクアウトはサポートされていません。

次のプラットフォームでは自動ブレイクアウトが正常に実行されないため、手動ブレイクアウトがサポートされています。N9K-C93128TX、N9K-9332、N9K-C9396PX、N9K-C9396TX、N9K-C9372PX、N9K-C9372TX、N9K-C9332PQ、N9K-C93120TX、N9K-9432PQ、N9K-9536PQ、N9K-9636PQ、N9K-X9632PC-QSFP100、N9K-X9432C-S、N3K-C3132Q-V、N3K-C3164Q、N3K-C3132C、N3K-C3232C、N3K-C3264Q、N3K-C3264C、N3K-3064Q、N3K-3016、N3K-3172。

「インターフェイス ブレイクアウト モジュール<モジュール番号> ポート<ポート範囲> マップ<ブレイクアウト マッピング>」 コマンドを使用して手動ブレイクアウトを実行する必要があります。

- ブレイクアウトポートがポートチャネルの一部として設定されている場合は、ポートチャネルの有効性を確保するために、設定を 2 回（write-erase / reload後に）適用する必要があります。
- Cisco Nexus 9000 デバイスを Cisco NX-OS リリース 7.0(3)I7(2) にアップグレードするときに、QSFP ポートが手動ブレイクアウトコマンドで設定され、QSA を使用している場合リリース、インターフェイス イーサネット 1/50/1 の設定はサポートされず、削除する必要があります。設定を復元するには、デバイスのイーサネット 1/50 を手動で設定する必要があります。

この動作は、次のプラットフォームでは手動ブレイクアウトがサポートされていません。N9K-C93128TX、N9K-9332、N9K-C9396PX、N9K-C9396TX、N9K-C9372PX、N9K-C9372TX、N9K-C9332PQ、N9K-C93120TX、N9K-9432PQ、N9K-9536PQ、N9K-9636PQ、N9K-X9632PC-QSFP100、N9K-X9432C-S、N3K-C3132Q-V、N3K-C3164Q、N3K-C3132C、N3K-C3232C、N3K-C3264Q、N3K-C3264C、N3K-3064Q、N3K-3016、N3K-3172。これらのプラットフォームでは手動ブレイクアウトがサポートされているためです。

- Cisco Nexus 9000 シリーズ スイッチには、40G ポートがあります。QSFP ブレイクアウト ケーブルを使用して 40G ポートの 1 つを 4x10G ポートに分割すると、すべてのサブインターフェイスをポート チャネルに追加できるわけではありません。次のエラー メッセージが表示されます。

```
switch# channel-group 99 mode active
command failed: port not compatible [Buffer boost]
```



- (注) 回避策として、すべてのサブインターフェイスで **no buffer-boost** を設定します。これにより、チャネルグループ設定が有効になります。

ポートチャネルで **force** キーワードを使用しても、キーワードの使用がエラーメッセージに示されている場合でも、すべてのインターフェイスをポートチャネルに追加できるわけではありません。

- Cisco NX-OS リリース 7.0(3)I7(3) 以降では、**rs-cons16** および **rs-ieee** など IEEE 標準に従って、FEC を設定するための 2 つの追加オプションが表示されます。



(注) Auto-FEC は Cisco NX-OS Release 7.0(3)I7(x) ではサポートされていません。

Cisco Nexus C92160YC スイッチ

7.0(3)I3(1) 以降、Cisco Nexus C92160YC スイッチは、2 つの異なる動作モードを提供しています。

- モード 1 : 48 X 10G/25G + 4 X 40G + 2 X 100G (デフォルト設定)
 - ハードウェア プロファイル ポートモード 48x25G + 2x100G + 4x40G
 - ブレークアウトは 2 つの 100G ポートでサポート
- モード 2 : 48 X 10G/25G + 4 X 100G
 - ハードウェア プロファイル ポートモード 48x25G + 4x100G
 - ブレークアウトは 3 * 100G ポートでサポートされています (ポート 50、51 および 52)。

現在の動作モードを表示するには、**show running-config | grep portmode** コマンドを使用します。

例 :

```
switch(config-if-range)# show running-config | grep portmode
hardware profile portmode 48x25G+2x100G+4x40G
```

詳細については、Cisco Nexus C92160YC スイッチのインストールガイドを参照してください。 ([Install and Upgrade Guides for Cisco Nexus 9000 Series Switches](#))。

Cisco Nexus C92160YC スイッチを使用している場合は、3 つのブレークアウトモードがあります。

- 40G ~ 4x10G ブレークアウトポート
 - 40G ポートから 4 X 10G ポートへのブレークアウトを有効にします。
 - **interface breakout module 1 port x map 10g-4x** コマンドを使用します。
- 100G ~ 4x25G ブレークアウトポート

- 100G ポートから 4 X 25G ポートへのブレイクアウトを有効にします。
- **interface breakout module 1 port x map 25g-4x** コマンドを使用します。

Cisco Nexus C9272Q スイッチ

7.0(3)I3(1)以降、Cisco Nexus C9272Q スイッチは、72 の 40G ポートを提供しています。ポート 37~71 は、ブレイクアウト インターフェイスをサポートしています。

ブレイクアウトインターフェイスを設定するには、**interface breakout module 1 port x map 10g-4x** コマンドを使用します。

例：

```
switch(config)# interface breakout module 1 port 38 map 10g-4x
switch(config)# show interface ethernet 1/38 capabilities | grep -i break

Breakout capable:      yes
```

Cisco Nexus C9332PQ スイッチ

7.0(3)I3(1)以降、Cisco Nexus C9332PQ スイッチは、ブレイクアウトモードをサポートし、FEX の 4 つの 10G NIF ポートに接続できる、24 の 40G ポートを提供しています。ポート 1~12 とポート 15~26 がサポートされています（ポート 13 および 14 は予約されており、ブレイクアウトモードには使用できません）。



(注) すべての FEX がサポートされています。



(注) Cisco Nexus 9332PQ スイッチだけが、FEX ファブリック インターフェイスのインターフェイスブレイクアウトサポートを提供しています（7.0(3)I3(1)以降）

Cisco Nexus 9000 C93180LC-EX スイッチ

7.0(3)I7(1)以降では、Cisco Nexus 9000 C93180LC-EX スイッチは 3 つの異なる動作モードを提供します。

- モード 1：28 x 40G + 4 x 40G/100G（デフォルト設定）
 - ハードウェア プロファイル ポートモード 4x100g + 28x40g
 - 10x4 ブレイクアウトは、1~27 の上部ポート（ポート 1、3、5、7... 27）でサポートされます。上部ポートのいずれかが故障すると、対応する下部のポートは動作しなくなります。たとえば、ポート 1 が故障すると、ポート 2 が動作しなくなります。
 - 1 ギガビットおよび 10 ギガビット QSA は、ポート 29、30、31、および 32 でサポートされます。ただし、上部および下部の前面パネルポートの QSA は同じ速度である必要があります。

- ポート 29、30、31、および 32 は、10x4、25x4、および 50x2 のブレイクアウトをサポートします。
- モード 2 : 24 x 40G + 6 x 40G/100G
 - ハードウェア プロファイル ポートモード 4x100g + 28x40g
 - 10x4 ブレイクアウトは、1~23 の上部ポート（ポート 1、3、5、7... 23）でサポートされます。上部ポートのいずれかが故障すると、対応する下部のポートは動作しなくなります。
 - ポート 25、27、29、30、31、および 32 は、10x4、25x4、および 50x2 のブレイクアウトをサポートします。
 - 1 ギガビットおよび 10 ギガビット QSA は、ポート 29、30、31、および 32 でサポートされます。ただし、上部および下部の前面パネル ポートの QSA は同じ速度である必要があります。
- モード 3 : 18 x 40G/100G
 - ハードウェア プロファイル ポートモード 18x100g
 - 10x4、25x4、および 50x2 のブレイクアウトは、1~27 のポート（ポート 1、3、5、7... 27）およびポート 29、30、31、32 でサポートされます。
 - 1 ギガビットおよび 10 ギガビット QSA は、18 ポートすべてでサポートされます。

モード 3 を他のモードに、またはその逆に変更するには、**copy running-config startup-config** コマンドの後に **reload** コマンドを実行する必要があります。ただし、モード 1 と 2 の間の移動は動的であり、**copy running-config startup-config** コマンドのみが必要です。

現在の動作モードを表示するには、**show running-config | grep portmode** コマンドを使用します。

例 :

```
switch(config-if-range)# show running-config | grep portmode
hardware profile portmode 4x100G+28x40G
```

Cisco Nexus C93180LC-EX スイッチを使用している場合は、3 つのブレイクアウト モードがあります。

- 40G~4x10Gブレイクアウトポート
 - 40G ポートから 4 X 10G ポートへのブレイクアウトを有効にします。
 - **interface breakout module 1 port x map 10g-4x** コマンドを使用します。
- 100G~4x25G ブレイクアウト ポート

- 100G ポートから 4 X 25G ポートへのブレイクアウトを有効にします。
- **interface breakout module 1 port x map 25g-4x** コマンドを使用します。
- 100G から 2x50G へのブレイクアウト ポート
 - 100G ポートから 2 X 50G ポートへのブレイクアウトを有効にします。
 - **interface breakout module 1 port x map 50g-2x** コマンドを使用します。

Cisco Nexus 9000 C9364C-GX スイッチ

Cisco Nexus N9K-C9364C-GX ブレイクアウトの考慮事項：

- ポート 1～64 については、2 x 50G、4 x 25G および 4 x 10G のブレイクアウトは、奇数番号のポートでのみサポートされます。
- クラウド内のある奇数番号のポートが分割されると、そのクラウド内の偶数ポートが削除されます。また、同じクラウド内の他の奇数ポートが自動的に同じ速度に分割されます。たとえば、ポート 1 またはポート 3 が 2 x 50、4 x 25G、または 4 x 10G に分割されている場合、そのクラウドのもう一方の奇数ポートは自動的に同じ速度に分割され、そのクラウドのポート 2 および 4 は削除されます。上記のブレイクアウト設定が削除されると、そのクラウドのすべてのポートがデフォルトに戻ります。
- QSFP28 (100G) トランシーバは、4 x 25G ブレイクアウト機能をサポートします。Cisco NX-OS Release 9.3(5) 以降では、2 x 50G ブレイクアウト機能がサポートされます。
- QSFP+ (40G) トランシーバは、4 x 10G ブレイクアウト機能をサポートします。
- 100G から 2x50G へのブレイクアウト ポート
 - すべての奇数番号ポートで、100G ポートから 2 X 50G ポートへのブレイクアウトを有効にします。
 - インターフェイスブレイクアウトモジュールの、1 ポートから 50-g2x へのマッピングコマンドを使用します。
- 40G～4x10Gブレイクアウトポート
 - 40G ポートから 4 X 10G ポートへのブレイクアウトを有効にします。
 - **interface breakout module 1 port x map 10g-4x** コマンドを使用します。

Cisco Nexus 9000 C93600CD-GX スイッチ

Cisco Nexus N9K-C93600CD-GX ブレイクアウトの考慮事項：

- Cisco Nexus N9K-C93600CD-GX では、1～24 の 4 つのポートはすべてクラウドと呼ばれます。ブレイクアウト設定と速度は、クラウド内で同じである必要があります。クラウドアウト機能は、クラウド内の速度またはブレイクアウト設定の不一致がある場合、期待どお

りに機能しないことがあります。6つのクワッドは、ポート1-4、5-8、9-12、13-16、17-20、および21-24で構成されます。

- Cisco NX-OS リリース 9.3(5) 以降では、2つの 50G ブレークアウトがポート 1-36 でサポートされます。
- 4x25G および 4x10G ブレークアウトは、ポート 1-24 の間の奇数ポートでのみサポートされます。偶数ポートはクワッド内で消去されます (4 ポート)。
- クワッド内の奇数番号のポートが分割されると、そのクワッド内の偶数ポートが削除され、クワッド内の他の奇数ポートが自動的に同じ速度に分割されます。たとえば、ポート 1 が 4x25G または 4x10G に分割されている場合、そのクワッドのもう一方のポートは自動的に同じ速度に分割されます。そのクワッドのポート 2 と 4 が削除されます。このブレークアウト設定が削除されると、そのクワッド内のすべてのポートがデフォルト設定に戻ります。
- 2x50G ブレークアウトは、1-24 のすべてのポートでサポートされます。クワッド内の 1 つのポートが 2x50G に分割されると、クワッド内のすべてのポートが自動的に同じ速度に分割されます。たとえば、ポート 2 が 2x50G に分割される場合、ポート 1、3、および 4 は自動的に 2x50G に分割されます。



(注) ポート 1-24 の 50G 速度の両方のレーンで RS-FEC のみがサポートされます。

- Cisco NX-OS リリース 9.3(3) 以降、ポート 25-28 は 4x10G、4x25G、および 2x50G のブレークアウト機能をサポートします。これらのブレークアウト機能は、ポート ペアでサポートされます。例：25-26、27-28。



(注) リンクをアップするには、2x50G のレーン 2 を RS-FEC で設定する必要があります。

- Cisco NX-OS リリース 9.3(3) 以降では、ポート 29-36 の次のブレークアウト設定を検討します。
 - QSFP-DD-400G-DR4 トランシーバは、4 x 100G ブレークアウト機能のみをサポートします。
 - QSFP-DD-400G-FR4 および QSFP-DD-400G-LR8 トランシーバは、ブレークアウト機能をサポートしていません。
 - QSFP28 (100G) トランシーバは、2 x 50G および 4 x 25G ブレークアウト機能をサポートします。
 - QSFP+ (40G) トランシーバは、4 x 10G ブレークアウト機能をサポートします。

Cisco Nexus 9000 C9316D-GX スイッチ

Cisco Nexus N9K-C9316D-GX ブレークアウトの考慮事項：

- ポート 1 ～ 16 のブレークアウトの考慮事項：
 - QSFP-DD-400G-DR4 トランシーバは、4 x 100G および 4x10G ブレークアウト機能のみをサポートします。
 - QSFP-DD-400G-FR4 および QSFP-DD-400G-LR8 トランシーバは、ブレークアウト機能をサポートしていません。
 - QSFP28 (100G) トランシーバは、2 x 50G、4 x 25G、および 4x10G ブレークアウト機能をサポートします。

Cisco NX-OS スイッチの USB ポートの無効化

Cisco NX-OS スイッチの USB ポートは、デフォルトで有効になっています。次のコマンドを使用して、すべての USB ポートを無効または有効にできます。

USB ポートを無効にするには、次のコマンドを使用します。

```
switch(config)# port usb disable
```

このコマンドでは、リロードする必要があります。 **Copy running-config startup-config** コマンドを使用して、スイッチをリロードします。

```
switch(config)#  
switch(config)# sh running-config | i usb  
port usb disable  
switch(config)#
```

以前に無効にされた USB ポートを有効にするには、次のコマンドを使用します。

```
switch(config)# no port usb disable
```

このコマンドでは、リロードする必要があります。 **Copy running-config startup-config** コマンドを使用して、スイッチをリロードします。

```
switch(config)#  
switch(config)# sh running-config | i usb  
switch(config)#
```



(注) すでに挿入されている USB で変更を有効にするには、**Copy running-config startup-config** コマンドを使用してスイッチをリロードすることをお勧めします。

仮想デバイス コンテキスト

Cisco NX-OS では、仮想デバイスをエミュレートする Virtual Device Context (VDCs) に、OS およびハードウェアリソースを分割できます。Cisco Nexus 9000 シリーズスイッチは、複数の

VDC をサポートしていません。すべてのスイッチ リソースはデフォルト VDC で管理されます。

インターフェイスのハイアベイラビリティ

インターフェイスは、ステートフル再起動とステートレス再起動をサポートします。ステートフル再起動はスーパーバイザ切り替え時に発生します。切り替え後、Cisco NX-OS は実行時の設定を適用します。



第 3 章

基本インターフェイスパラメータの設定

- [基本インターフェイスパラメータについて \(27 ページ\)](#)
- [注意事項と制約事項 \(39 ページ\)](#)
- [デフォルト設定 \(47 ページ\)](#)
- [基本インターフェイスパラメータの設定 \(47 ページ\)](#)
- [基本インターフェイスパラメータの確認 \(87 ページ\)](#)
- [インターフェイスカウンタのモニタリング \(87 ページ\)](#)
- [DWDMの設定 \(89 ページ\)](#)
- [QSA の設定例 \(91 ページ\)](#)

基本インターフェイスパラメータについて

説明

イーサネットインターフェイスおよび管理インターフェイスに説明パラメータを設定して、インターフェイスにわかりやすい名前を付けることができます。それぞれのインターフェイスに独自の名前を使用すれば、複数のインターフェイスから探す場合でも必要なインターフェイスをすぐに見つけることができます。

ポートチャンネル インターフェイスへの説明パラメータの設定については、「ポート チャンネルの説明の設定」の項を参照してください。その他のインターフェイスへのこのパラメータの設定については、「説明の設定」の項を参照してください。

ビーコン

ビーコンモードをイネーブルにするとリンク ステート LED が緑に点滅し、物理ポートを識別できます。デフォルトでは、このモードはディセーブルです。インターフェイスの物理ポートを識別するには、インターフェイスのビーコンパラメータを有効にします。

ビーコンパラメータの設定については、「ビーコンモードの設定」の項を参照してください。

エラー ディセーブル化

ポートが管理的に有効であるが (**no shutdown** コマンドを使用)、プロセスによって実行時に無効になる場合、そのポートは **error-disabled** (**err-disabled**) ステートです。たとえば、UDLD が単方向リンクを検出した場合、ポートは実行時にシャットダウンされます。ただし、ポートは管理イネーブルなので、ポートステータスは **err-disable** として表示されます。ポートが **err-disable** ステートになると、手動で再イネーブル化する必要があります。または、自動回復を提供するタイムアウト値を設定できます。自動回復はデフォルトでは設定されておらず、デフォルトでは、**err-disable** の検出はすべての原因に対してイネーブルです。

インターフェイスが **errdisable** ステートになった場合は、**errdisable detect cause** を使用します。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。

特定の **error-disabled** の原因に自動 **error-disabled** 回復タイムアウトを設定し、回復期間を設定できます。

この項で説明している **errdisable recovery cause** コマンドを使用すると、300 秒後に自動的にリカバリします。

errdisable recovery interval コマンドを使用すればコマンドを使用します。特定の **err-disable** 原因のリカバリ タイムアウトも設定できます。

原因に対する **error-disabled** 回復を有効にしない場合、そのインターフェイスは **shutdown** および **no shutdown** コマンドを開始するまでエラー無効状態です原因に対して回復をイネーブルにすると、そのインターフェイスの **errdisable** ステートは解消され、すべての原因がタイムアウトになった段階で動作を再試行できるようになります。**show interface status err-disabled** コマンドを使用し、コマンドを使用します。

MDIX

メディア依存インターフェイスクロスオーバー (MDI-X) パラメータを使用して、デバイス間のクロスオーバー接続のイネーブル/ディセーブルを切り替えます。このパラメータは銅線インターフェイスだけに適用します。デフォルトでは、このパラメータはイネーブルです。この **no mdix auto** コマンドは、N9K-C93108TC-EX、N9K-C93108TC-FX、N9K-X9788TC-FX、および N9K-C9348GC-FXP デバイスでのみサポートされます。

MDIX パラメータの設定については、「[MDIX パラメータの設定](#)」のセクションを参照してください。

インターフェイスステータス エラーポリシー

アクセスコントロールリスト (ACL) マネージャおよび Quality of Service (QoS) マネージャなどの Cisco NX-OS ポリシー サーバは、ポリシー データベースを維持します。ポリシーは、コマンドラインインターフェイスを使用して定義します。

インターフェイス上でポリシーを設定するときにポリシーをプッシュして、プッシュされるポリシーがハードウェアのポリシーと一致するようにします。エラーをクリアし、ポリシープログラミングが実行コンフィギュレーションを続行できるようにするには、**no shutdown** コマン

ドを入力します。ポリシープログラミングが成功すると、ポートのアップが許可されます。ポリシープログラミングが失敗した場合、設定はハードウェアポリシーに矛盾し、ポートは `error-disabled` ポリシー状態になります。 `error-disabled` ポリシー状態にとどまり、同じポートが今後アップされないように情報が保存されます。このプロセスにより、システムに不要な中断が生じるのを避けることができます。

インターフェイス MTU サイズの変更

最大伝送単位 (MTU) サイズは、イーサネットポートで処理できる最大フレームサイズを指定します。2つのポート間で転送するには、どちらのポートにも同じ MTU サイズを設定する必要があります。ポートの MTU サイズを超えたフレームはドロップされます。

デフォルトでは、クラウドスケール ASIC NX-OS システムは、ハードウェアでさまざまなタイプのカプセル化を完全にサポートし、受け入れるために、構成された値に加えて MTU で常に追加の 166B を許可します。

Cisco NX-OS では、プロトコルスタックの異なるレベルで設定するオプションを使用して、インターフェイスに MTU を設定できます。デフォルトではそれぞれのインターフェイスの MTU は 1500 バイトです。これはイーサネットフレームに関する IEEE 802.3 標準です。MTU サイズを大きくすると、データの処理効率が向上し、さまざまなアプリケーション要件に対応できます。このようなフレームをジャンボフレームと呼び、最大 9216 バイトまで指定できます。

MTU はインターフェイスごとに設定されます。インターフェイスは、レイヤ 2 またはレイヤ 3 インターフェイスにすることができます。レイヤ 2 インターフェイスの場合、MTU サイズは、システムのデフォルト MTU 値またはシステムジャンボ MTU 値の 2 つの値のいずれかで設定できます。システムデフォルトの MTU サイズは 1500 バイトです。すべてのレイヤ 2 インターフェイスは、デフォルトでこの値で設定されます。デフォルトのシステムジャンボ MTU 値 (9216 バイト) を使用してインターフェイスを設定できます。1500 ~ 9216 の MTU 値を許可するには、インターフェイスが同じ値で設定できる適切な値にシステムジャンボ MTU を調整する必要があります。



- (注) システムジャンボ MTU サイズを変更できます。値が変更されると、システムジャンボ MTU 値を使用するレイヤ 2 インターフェイスは新しいシステムジャンボ MTU 値に自動的に変更されます。

レイヤ 3 インターフェイスは、レイヤ 3 物理インターフェイス (スイッチポートなしで設定)、スイッチ仮想インターフェイス (SVI)、およびサブインターフェイスで、576 ~ 9216 バイトの MTU サイズを設定できます。

Cisco Nexus 9372 スイッチでは、次のことが適用されます。

- 10-G インターフェイスは、デフォルトの MTU が 1500 である特定のハードウェアポートにマッピングされます。
- 40-G インターフェイスは、デフォルトの MTU が 3FFF で、MTU 制限チェックが無効になっている HiGiG ポートとしてマッピングされます。

- 40-G インターフェイスの場合、MTU 制限チェックは無効であるため、MTU に関係なくパケットサイズとトラフィックフローを無視します。
- スイッチ上のすべてのインターフェイスの設定済み MTU が一致しない場合、スイッチの動作は、不一致の特定のポートとトラフィックフローによって異なる場合があります。次に、さまざまなシナリオでのスイッチの動作の例を示します。
 - ポートの MTU サイズを超える長さのフレームをレイヤ 3 ポートが受信すると、ポートはそのフレームをドロップします。
 - レイヤ 3 ポートが、入力ポートの MTU サイズよりも小さいが、出力レイヤ 3 ポートの MTU サイズよりも大きいフレームを受信すると、フレームはスイッチのスーパーバイザにパントされます。
 1. フレームが、Don't Fragment (DF) ビットが設定された IP パケットである場合、フレームはソフトウェアでドロップされます。それ以外の場合、フレームはソフトウェアでフラグメント化されます。
 2. それ以外の場合、フレームはソフトウェアでフラグメント化されます。
 3. これにより、コントロールプレーンポリシング (CoPP) が Cisco Nexus スイッチでデフォルトで有効になっているため、パフォーマンスの問題（影響を受けるトラフィックフローの遅延やパケット損失など）が発生する可能性があります。コントロールプレーンポリシングの詳細については、『Cisco Nexus 9000 Series NX-OS Security Configuration Guide』の「Configuring Control Plane Policing」の章を参照してください。
 - ポートの MTU サイズを超える長さのフレームをレイヤ 2 ポートが受信すると、ポートはそのフレームをドロップします。
 - レイヤ 2 ポートが、長さが入力ポートの MTU サイズよりも短く、出力レイヤ 2 ポートの MTU サイズよりも大きいフレームを受信し、フレームがスイッチによって VLAN 間でルーティングされると、フレームはスーパーバイザにパントされます。
 1. フレームが、Don't Fragment (DF) ビットが設定された IP パケットである場合、フレームはソフトウェアでドロップされます。それ以外の場合、フレームはソフトウェアでフラグメント化されます。
 2. それ以外の場合、フレームはソフトウェアでフラグメント化されます。
 3. これにより、コントロールプレーンポリシング (CoPP) が Cisco Nexus スイッチでデフォルトで有効になっているため、パフォーマンスの問題（影響を受けるトラフィックフローの遅延やパケット損失など）が発生する可能性があります。コントロールプレーンポリシングの詳細については、『Cisco Nexus 9000 Series NX-OS Security Configuration Guide』の「Configuring Control Plane Policing」の章を参照してください。
 - レイヤ 2 ポートが、入力ポートの MTU サイズよりも短く、出力レイヤ 2 ポートの MTU サイズよりも大きいフレームを受信し、フレームがスイッチによって同じ VLAN 内でスイッチングされると、スイッチはフレームをドロップします。

MTU サイズの設定については、「*MTU* サイズの設定」の項を参照してください。



- (注) Cisco Nexus 9300-FX2 および 9300-GX デバイスでは、入力インターフェイスが 9216 未満の MTU で設定されている場合、FTE は入力エラーをキャプチャせず、イベントを表示しません。ただし、入力インターフェイスが MTU 9216 で設定されている場合、FTE はすべてのイベントを表示します。

帯域幅

イーサネットポートには、物理レイヤで 1,000,000 Kb の固定帯域幅があります。レイヤ3 プロトコルでは、内部メトリックが計算できるように設定した帯域幅の値が使用されます。設定した値はレイヤ3 プロトコルで情報目的だけで使用され、物理レイヤでの固定帯域幅が変更されることはありません。たとえば、Enhanced Interior Gateway Routing Protocol (EIGRP) ではルーティングメトリックを指定するために最小パス帯域幅が使用されますが、物理レイヤの帯域幅は 1,000,000 Kb のまま変わりません。

ポートチャンネルインターフェイスへの帯域幅パラメータの設定については、「情報目的としての帯域幅および遅延の設定」の項を参照してください。その他のインターフェイスへの帯域幅パラメータの設定については、「帯域幅の設定」の項を参照してください。

スループット遅延

スループット遅延パラメータの値を指定するとレイヤ3 プロトコルで使用する値が指定できませんが、インターフェイスの実際のスループット遅延は変更されません。レイヤ3 プロトコルはこの値を使用して動作を決定します。たとえば、リンク速度などの他のパラメータが等しい場合、Enhanced Interior Gateway Routing Protocol (EIGRP) は遅延設定を使用して、他のイーサネットリンクより優先されるイーサネットリンクのプリファレンスを設定できます。設定する遅延値の単位は 10 マイクロ秒です。

ポートチャンネルインターフェイスへの帯域幅パラメータの設定については、「情報目的としての帯域幅および遅延の設定」の項を参照してください。その他のインターフェイスへのスループット遅延パラメータの設定については、「スループット遅延の設定」の項を参照してください。

管理ステータス

管理ステータスパラメータはインターフェイスのアップまたはダウンを指定します。管理ダウンしたインターフェイスはディセーブルであり、データを転送できません。管理アップしたインターフェイスはイネーブルであり、データを転送できます。

ポートチャンネルインターフェイスへの管理ステータスパラメータの設定については、「ポートチャンネルインターフェイスのシャットダウンと再起動」の項を参照してください。その他のインターフェイスへの管理ステータスパラメータの設定については、「インターフェイスのシャットダウンおよび再開」の項を参照してください。

UDLD パラメータ

UDLD の概要

シスコ独自の単方向リンク検出 (UDLD) プロトコルにより、光ファイバまたは銅線 (カテゴリ 5 ケーブルなど) イーサネットケーブルを使用して接続されたデバイスで、ケーブルの物理構成をモニタし、単方向リンクの存在を検出することができます。デバイスで単方向リンクが検出されると、UDLD が関係のある LAN ポートをシャットダウンし、ユーザに通知します。単方向リンクは、さまざまな問題を引き起こす可能性があります。

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 の検出が動作して、物理的な単方向接続と論理的な単方向接続を防止し、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限り、そのリンクはアップ状態が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 で両方のファイバが正常に動作していれば、UDLD はそれらのファイバが正しく接続しているかどうか、また、トラフィックが適切なネイバー間で双方向に流れているかどうかを判別します。自動ネゴシエーションはレイヤ 1 で動作するため、このチェックは、自動ネゴシエーションでは実行できません。

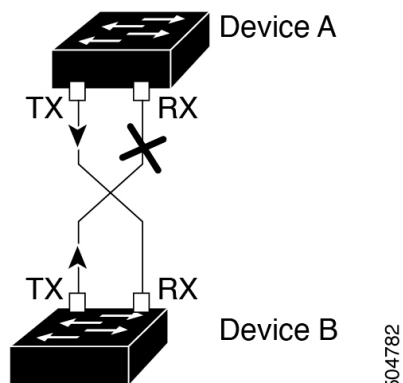
Cisco Nexus 9000 シリーズのデバイスは、UDLD をイネーブルにした LAN ポート上のネイバーデバイスに定期的に UDLD フレームを送信します。一定の時間内にフレームがエコーバックされてきて、特定の確認応答 (echo) が見つからなければ、そのリンクは単方向のフラグが立てられ、その LAN ポートはシャットダウンされます。UDLD プロトコルにより単方向リンクが正しく識別されその使用が禁止されるようにするためには、リンクの両端のデバイスで UDLD がサポートされている必要があります。UDLD フレームの送信間隔は、グローバル単位でも指定されたインターフェイスにも設定できます。



(注) UDLD は、銅線の LAN ポート上では、このタイプのメディアでの不要な制御トラフィックの送信を避けるために、ローカルでデフォルトでディセーブルになっています。

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

図 1: 単方向リンク



504782

UDLD のデフォルト設定

次の表に、UDLD のデフォルト設定を示します。

表 4: 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
ポート別の UDLD イネーブル ステート (光ファイバメディア用)	すべてのイーサネット光ファイバLANポートでイネーブル
ポート別の UDLD イネーブル ステート (ツイストペア (銅製) メディア用)	すべてのイーサネット 10/100 および 1000BASE-TX LAN ポートでディセーブル
UDLD アグレッシブ モード	ディセーブル
UDLD メッセージの間隔	15 秒

デバイスおよびそのポートへの UDLD の設定については、「UDLD モードの設定」の項を参照してください。

UDLD の通常モードとアグレッシブモード

UDLD は操作の通常およびアグレッシブモードをサポートします。デフォルトでは、通常モードが有効です。

通常モードでは、UDLD はピアポートからの着信 UDLD パケットを調べて、次のリンクエラーを検出します。

- 空のエコーパケット
- 単一方向
- TX/RX ループ

- ネイバーの不一致

デフォルトでは、UDLD アグレッシブ モードが無効になっています。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 モードを有効に設定した場合、UDLD 近接関係が設定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を再確立しようとします。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。

次のシナリオでは、UDLD アグレッシブ モードを有効にすると、トラフィックの廃棄を防ぐためにポートの 1 つが無効になります。

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



(注) UDLD アグレッシブ モードをすべてのファイバポートでイネーブルにするには、UDLD アグレッシブ モードをグローバルでイネーブルにします。指定されたインターフェイスの銅ポートで、UDLD アグレッシブ モードをイネーブルにする必要があります。



ヒント ラインカードのアップグレードが In-Service Software Upgrade (ISSU) 中に実行され、ラインカードのポートの一部がレイヤ 2 ポートチャネルのメンバーで UDLD アグレッシブ モードで設定されている場合、リモートポートの 1 つがシャットダウンされると、UDLD はローカルデバイス上の対応するポートを `errdisable` ステートにします。これは、正常な動作です。

ISSU の完了後にサービスを復元するには、ローカルポートで `shutdown` コマンドと `no shutdown` コマンドを順に入力します。

ポートチャネルパラメータ

ポートチャネルは物理インターフェイスの集合体で、論理インターフェイスを構成します。1 つのポートチャネルに最大 32 の個別インターフェイスをバンドルして、帯域幅と冗長性を向上させることができます。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。ポートチャネルの物理インターフェイスが少なくとも 1 つ動作していれば、そのポートチャネルは動作しています。

レイヤ 3 ポートチャネルに適合するレイヤ 3 インターフェイスをバンドルすれば、レイヤ 3 ポートチャネルを作成できます。

変更した設定をポートチャネルに適用すると、そのポートチャネルのインターフェイスメンバにもそれぞれ変更が適用されます。

ポートチャネルおよびポートチャネルの設定については、第6章「ポートチャネルの設定」を参照してください。

ポートプロファイル

Cisco Nexus 9300 シリーズ スイッチの場合、多くのインターフェイス コマンドを含むポートプロファイルを作成して、インターフェイスの範囲にそのポートプロファイルを適用できます。ポートプロファイルはそれぞれ特定のタイプのインターフェイスにだけ適用できます。次のインターフェイスから選択できます。

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

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

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

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

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

- ポートプロファイルに関連したデフォルト設定はありません。

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



(注) Session Manager にポートプロファイルは使用できません。Session Manager の詳細については、『Cisco Nexus 9000 Series NX-OS System Management Configuration Guide』を参照してください。

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

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

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

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

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

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

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

単独のインターフェイスまたはある範囲に属する複数のインターフェイスに対してポートプロファイルを継承した後、特定の設定値を削除すると、それらのインターフェイスではそのポートプロファイル設定が機能しなくなります。

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

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

Cisco QSFP+ to SFP+ アダプタ モジュールのサポート

Cisco QSFP+ to SFP+ アダプタ (QSA) モジュールは、特定の Cisco Nexus 9300 デバイスの Cisco Nexus M6PQ および Cisco Nexus M12PQ アップリンク モジュールの一部である 40G アップリンク ポートに 10G サポートを提供します。

M6PQ または M12PQ アップリンク モジュールの 6 つの連続するポートは、QSA/QSFP モジュールを使用するために同じ速度 (40G または 10G) で稼動している必要があります。

- Cisco Nexus 9396PX デバイスでは、2/1-6 ポートは最初のポート速度グループを形成し、残りの 2/7-12 ポートが 2 番目のポート速度グループを形成します。
- Cisco Nexus 93128PX/TX デバイスでは、2/1-6 ポートは最初のポート速度グループを形成し、残りの 2/7-8 ポートが 2 番目のポート速度グループを形成します。
- Cisco Nexus 937xPX/TX デバイスでは、1/49-54 ポートがただ 1 つのポート速度グループを形成します。
- Cisco Nexus 93120TX デバイスでは、1/97-102 ポートがただ 1 つのポート速度グループを形成します。
- Cisco Nexus 93120TX デバイスでは、1/17-32 ポートがただ 1 つのポート速度グループを形成します。

speed-group 10000 コマンドを使用し、コマンドを使用して QSA のポート速度グループの最初のポートを設定します。このコマンドは、ポートグループの管理者の速度のプリファレンスを指定します (デフォルトのポート速度は 40G です)。

- **speed-group 10000** コマンドは 10G の速度を指定します。
- **no speed-group 10000** コマンドは 40G の速度を指定します。
- Cisco NX-OS リリース 9.2(2) 以降では、CWD4M4 は 36 ポート 100 ギガビット イーサネット QSFP28 ラインカード (N9K-X9636C-R)、36 ポート 40 ギガビット イーサネット QSFP+ ラインカード (N9K-X9636Q)、36 ポート 100 ギガビット QSFP28 ラインカード (N9K-X9636C-RX) および 52 ポート 100 ギガビット QSFP28 ラインカード (N9K-X96136YC-R) でサポートされます。

速度を設定すると、互換性のあるトランシーバ モジュールがイネーブルになります。ポートグループ内の残りのトランシーバ モジュール（互換性のないトランシーバ モジュール）は「check speed-group config」として error disabled となります。



(注) Cisco QSFP+ to SFP+ アダプタ (QSA) モジュールは、Cisco Nexus 9500 デバイス用の 40G ラインカードに対して 10G のサポートを提供しません。

Cisco Nexus 9200 および 9300-EX シリーズ スイッチおよび Cisco Nexus 3232C および 3264Q シリーズ スイッチでは、QSFP-to-SFP アダプタを使用できます。

Cisco SFP+ アダプタ モジュールのサポート

Cisco Nexus 9236C スイッチの 100 ギガビットポートで 25 ギガビット光ファイバをサポートするために、CVR-2QSFP28-8SFP アダプタを使用できます。

このスイッチの 100G インターフェイスを 4 つの 25G インターフェイスに分割するには、**interface breakout module** コマンドを使用します。このコマンドを入力した後に、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する必要があります。

Cisco NX-OS リリース 9.2(3) 以降、10/25 LR は N9K-C93180YC-EX、N9K-X97160YC-EX、N9K-C93180YC-FX、N9K-C93240YC-FX2、および N3K-C34180YC スイッチでサポートされています。このデュアルスピード光トランシーバはデフォルトで 25G で動作し、他の 25G LR トランシーバとシームレスに相互運用します。このデバイスでは自動速度検出がサポートされていないため、10G トランシーバと相互運用するには、10G 速度を使用するように手動で設定する必要があります。

Cisco SFP-10G-T-X モジュールのサポート

Cisco NX-OS リリース 9.3(5) 以降、10G BASE-T SFP+ (RJ-45) は N9K-C93240YC-FX2、N9K-C93180YC-EX、N9K-C93180YC-FX、および N9K-C93360YC-FX2 デバイスでサポートされます。この銅線トランシーバは、デフォルトで 10G で動作します。



(注) SFP-10G-TX デバイスをポートに接続する場合、このデバイスのすべての隣接ポートが空であるか、パッシブ銅線リンクのみに接続されている必要があります。



(注) 管理状態が「Up」のときにメディアタイプ 10G-TX で設定されたインターフェイスは、サポートされていないメディアタイプで errdisable のままになります。この状態を解消するには、インターフェイスで次のコマンドを使用します。

- shutdown
- no shutdown

表 5: デフォルトのポート マッピング

デバイス名	ポート マップ
Cisco Nexus N9K-C93180YC-EX、 N9K-C93180YC-FX、N9K-C93180YC-FX3 および N9K-C93180YC-FX3S	PI/PE : 1、4-5、8-9、12-13、16、37、40-41、 44-45、48
Cisco Nexus N9K-C93240YC-FX2	W/PI Fan/PS : 2、6、8、12、14、18、20、24、 26、30 32、36、38、42、44、48 W/PE Fan/PS : 6、12、18、24、30、36、42、48
Cisco Nexus N9K-C93360YC-FX2	PI/PE 1、4-5、8、41、44-45、48-49、52-53、 56-57、 60-61、64-65、68-69、72-73、76-77、80-81、 84-85、 88-89、92-93、96

注意事項と制約事項

基本インターフェイスパラメータの設定には次の注意事項と制約事項があります。

- 銅線ポートでは、MDIXはデフォルトでイネーブルになっています。無効にすることはできません。
- internal** キーワードが付いている **show** コマンドはサポートされていません。
- 光ファイバーサネットポートでは、シスコがサポートするトランシーバを使用する必要があります。シスコがサポートするトランシーバをポートに使用していることを確認するには、**show interface transceivers** コマンドを使用します。シスコがサポートするトランシーバを持つインターフェイスは、機能インターフェイスとして一覧表示されます。
- ポートはレイヤ2またはレイヤ3インターフェイスのいずれかです。両方が同時に成立することはありません。

デフォルトでは、どのポートもレイヤ3インターフェイスです。

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には、**switchport** コマンドを使用します。**no switchport** コマンドを使用すれば、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ことができます。

- 通常、イーサネットポート速度およびデュプレックスモードパラメータは自動的に設定し、システムがポート間で速度およびデュプレックスモードをネゴシエートできるようにします。これらのポートのポート速度およびデュプレックスモードを手動で設定する場合は、次の点について考慮してください。

- イーサネットまたは管理インターフェイスに速度およびデュプレックスモードを設定する前に、「デフォルト設定」の項を参照して同時に設定できる速度およびデュプレックスモードの組み合わせを確認します。
- イーサネットポート速度を自動的に設定すると、デバイスは自動的にデュプレックスモードを自動的に設定します。
- **no speed** コマンドを入力すると、デバイスは自動的に速度およびデュプレックスパラメータの両方を自動的に設定します（**no speed** コマンドと **speed auto** コマンドは同じ結果になります）。
- イーサネットポート速度を自動以外の値（1G、10G、または 40G など）に設定する場合は、それに合わせて接続先ポートを設定してください。接続先ポートが速度をネゴシエーションするように設定しないでください。
- イーサネットインターフェイスの速度、デュプレックス、および自動フロー制御を設定するには、**negotiate auto** コマンドを使用します。自動ネゴシエーションをディセーブルにするには、**no negotiate auto** コマンドを使用します。
- Cisco NX-OS リリース 9.3(6) 以降、Cisco Nexus N9K-C92348GC-X スイッチは、ポート 1～48 で、10M 全二重モードをサポートします。



(注) 接続先ポートが自動以外の値に設定されている場合、デバイスはイーサネットポート速度およびデュプレックスモードを自動的にネゴシエートできません。



注意 イーサネットポート速度およびデュプレックスモードの設定を変更すると、インターフェイスがシャットダウンされてから再びイネーブルになる場合があります。

- QSFP-40G-CR4 ケーブルを使用して N9K-C9332PQ 非 ALE ポートと N9K-C9372PX ALE ポートを接続する場合は、速度を 40000 に手動で設定する必要があります。
- Base-T 銅線ポートの場合は、固定速度が設定されていても、自動ネゴシエーションがイネーブルになります。
- **regex** コマンド オプションでは、正規表現によるインターフェイスのセットの指定がサポートされています。The **regex** コマンド オプションは、すべてのインターフェイス コマンドで使用できる拡張機能です。

例：

```
switch(config-if-range)# interface ethernet regex [2]/
switch(config-if-range)# where
conf; interface Ethernet2/1-8 admin@switch%default
switch(config-if-range)# interface ethernet regex [1]/2[2-4]
```



```
switch(config-if-range)# where
conf; interface Ethernet1/22-24      admin@switch%default
```

- 管理アプリケーションの `source-interface` コマンド オプションでは、`copy` コマンドおよびその他のプロセス (`tacacs`、`ntp`、`ping/ping6`、`icmp-error`、`traceroute` など) での、IPv4 や IPv6 によるインバンドまたはアウトバンド送信元 IP アドレスの設定がサポートされています。

- コンフィギュレーション コマンド

ip services source-interface interface vrf vrf name

例 :

```
• ip ftp source-interface ethernet 8/1 vrf management
• ip http source-interface loopback 1 vrf blue
• ip ssh source-interface ethernet ethernet 5/1
  /*This command executes in the VRF context.*/
• ip ping source-interface ethernet 8/1 vrf blue
• ip traceroute source-interface ethernet 8/1 vrf red
• ip icmp-errors source-interface ethernet 8/1
  /*This command executes in the VRF context.*/
```

- show コマンド :

show ip copy services source-interface interface vrf vrf name

```
• show ip ftp source-interface ethernet 8/1 vrf management
• show ip http source-interface loopback 1 vrf blue
• show ip ssh source-interface ethernet ethernet 5/1
  /*This command executes in the VRF context.*/
• show ip ping source-interface ethernet 8/1 vrf blue
• show ip traceroute source-interface ethernet 8/1 vrf red
• show ip icmp-errors source-interface ethernet 8/1
  /*This command executes in the VRF context.*/
```

- service コマンド :

copy service://username@hostname/path file source-interface interface name

例 :

```
• copy ftp://username@hostname/usr/local/bin file source-interface ethernet
  8/1
• copy scp://username@hostname/usr/local/bin file source-interface ethernet
  8/1
```

- `copy tftp://username@hostname/usr/local/bin file source-interface ethernet 8/1`
- `copy http://username@hostname/usr/local/bin file source-interface ethernet 8/1`
- `copy sftp://username@hostname/usr/local/bin file source-interface ethernet 8/1`

- Cisco Nexus 9300 シリーズ スイッチおよび Cisco Nexus 9500 シリーズ スイッチでは、ポート プロファイルがサポートされています。
- 自動ネゴシエーションは、Cisco Nexus 9200 および 9300-EX プラットフォーム スイッチの 25 ギガビットイーサネット トランシーバモジュール、および N9K-X9700-EX ラインカードを使用する Cisco Nexus 9500 プラットフォーム スイッチではサポートされません。
- Cisco NX-OS リリース 9.2(1) 以降、Cisco Nexus N9K-X97160YC-EX、N9K-C93180YC-FX、N9K-C93240YC-FX2 および N9K-C93240YC-FX2-Z スイッチでは、ネイティブ 25G ポートでの自動ネゴシエーションがサポートされています
- 自動ネゴシエーションは、Cisco Nexus N9K-C92300YC スイッチではサポートされていません。
- 自動ネゴシエーションは、25G ブレークアウトポートではサポートされていません。
- Cisco NX-OS リリース 10.4(2)F 以降では、リンクをアクティブにするには、両方の 50Gx2 ブレークアウトポートで同じ FEC を設定する必要があります。FEC タイプは、ポートの自動ネゴシエーションではサポートされていません。デフォルト構成がポートで異なる場合は、両方のポートで同じ構成にしてください。
- N9K-C93108TC-FX3P スイッチが次のいずれかのスイッチに接続されている場合、自動ネゴシエーションはサポートされません。
 - N9K-C9236C、N9K-C92300YC、N9K-C93180YC-EX、N9K-C93180YC-EXU、N9K-C9232C、N9K-C92300YC、N9K-C93180YC-FX。
 - N3K-C3172TQ-XL、N3K-C3172TQ-10GT、N3K-C3172PQ-10GE、および N3K-C3132Q-40GE。
- Cisco NX-OS リリース 9.2(2) 以降、自動ネゴシエーション (40 G/100 G) は以下のポートでサポートされます。
 - Cisco Nexus 9336C-FX2 スイッチ：ポート 1 ～ 6 および 33 ～ 36
 - Cisco Nexus 9364C スイッチ：ポート 49 ～ 64
 - Cisco Nexus 93240YC-FX2 スイッチ：ポート 51 ～ 54
 - Cisco Nexus 9788TC ラインカード：ポート 49 ～ 52
- Cisco NX-OS リリース 9.2(2) 以降、QSA を搭載した 10 GB は以下のポートでサポートされます。

- Cisco Nexus 9336C-FX2 スイッチ：ポート1～36
 - Cisco Nexus 9364C スイッチ：ポート49～64
 - Cisco Nexus 9788TC ラインカード：ポート49～52
- Cisco NX-OS リリース 10.4(1)F 以降、Cisco Nexus C9348GC-FX3PH スイッチには以下の制限があります。
 - スイッチの前面ポート（ポート41～48）では、輻輳またはラインレートトラフィックが発生した場合に、コントロールプレーンが影響を受ける可能性があります。
 - ラインレートトラフィックの99.98%でドロップはありません。
 - 次に示すインターフェイスカウンタは、前面ポート41～48でサポートされます。
 - インターフェイスパケット：入力パケット、Rxユニキャストパケット、Rxマルチキャストパケット、Rxブロードキャストパケット、Txユニキャストパケット、出力パケット、Txマルチキャストパケット、およびTxブロードキャストパケット
 - インターフェイスエラー：入力ラントエラー、入力FCSエラー、入力エラー、シンボルエラー、入力CRC、および出力エラー
 - インターフェイスコリジョン：コリジョン、シングルコリジョン、マルチコリジョン、およびレイトコリジョン
 - インターフェイスバイト：Rxバイト、およびTxバイト
 - その他のサポートされているインターフェイスカウンタ：Tx Dropped、Short Frame、Jumbo Frames、Input Discard、Deferred、およびJabber
- Cisco NX-OS リリース 10.4(1)F 以降では、QSAを使用した10GBおよびQSA28を使用した25Gが次でサポートされます。
 - Cisco Nexus C9348GC-FX3PH スイッチ：ポート53および54のみ
 - Cisco Nexus C9348GC-FX3 スイッチ：ポート53および54のみ
- Cisco NX-OS リリース 10.4(1)F 以降、QSA28を使用した25Gは以下でサポートされます。
 - Cisco Nexus 93180YC-FX3 スイッチ：ポート49～54
 - Cisco Nexus 93108TC-FX3P スイッチ：ポート49～54
- Cisco NX-OS リリース 10.4(2)F 以降では、QSAを使用した10GBおよびQSA28を使用した25GがCisco Nexus スイッチ C93108TC-FX3 でサポートされます。
- Cisco NX-OS リリース 9.2(2) 以降、QSAを搭載した1GBは以下のポートでサポートされます。
 - Cisco Nexus 9336C-FX2 スイッチ：ポート7～32
 - Cisco Nexus 9364C スイッチ：ポート65および66のみ

- Cisco NX-OS リリース 9.3(1) 以降では、MTU 9216のみを FEX ファブリック ポートに設定できます。その他の値が渡された場合は、エラーが生成されます。スイッチを Cisco NX-OS リリース 9.3(1) にアップグレードする前に、FEX ファブリック ポートチャネルの MTU 値が 9216 に設定されていた場合、**show running config** コマンドは MTU 値を表示しませんが、**show running-config diff** コマンドは表示します。
- Cisco NX-OS リリース 9.3(1) 以降では、FEX ファブリック ポート チャネルはデフォルトで MTU 9216 のみをサポートします。
- 次のライン カードはリンク トレーニングをサポートしていません。

Nexus 9300 モジュール :

- N9K-M12PQ (C9396PX、C9396TX、C93128PX、C93128TX)

Nexus 9500 モジュール :

- X9536PQ
- X9564PX
- X9564TX

- ケーブル長が 5 m を超える場合、自動ネゴシエーションはサポートされていません。このケーブル長の制限は、銅ケーブルにのみ適用されます。光ケーブルには適用されません。
- 有効なインターフェイス記述の最後にバックスラッシュ (\) を使用すると、パーサーはバックスラッシュを継続文字として識別し、コマンド文字列に新しい行文字「\n」を追加することにより、コマンド出力に余分な改行を追加します。これは Day-1 の動作です。
- Cisco NX-OS リリース 10.2(3)F 以降、**link-flap error-disable count** コマンドはすべての物理ポートで設定できます。
- **link-flap error-disable count** コマンドは、すべての Cisco Nexus 9000 シリーズ スイッチでサポートされています。
- Cisco NX-OS リリース 10.3(1)F 以降、Cisco Nexus 9800 プラットフォームスイッチでインターフェイス整合性チェックのサポートが提供されます。
- Cisco NX-OS リリース 10.3(1)F 以降、Cisco Nexus 9800 プラットフォーム スイッチの N9K-X9836DM-A ライン カードでは、ネイティブ (400G、100G、40G) とブレイクアウト (4x100G) ポートのサポートが提供されます。
- Cisco NX-OS リリース 10.4(1)F 以降で、ブレイクアウト (4x10G および 4x25G) ポートサポートは、Cisco Nexus 9808/9804 プラットフォーム スイッチの N9K-X9836DM-A ライン カードで提供されます。
- Cisco NX-OS リリース 10.4(2)F 以降では、Cisco Nexus C9232E-B1 スイッチに以下が適用されます。
 - ブレイクアウト (2x400G、8x100G、4x100G、4x25G、および 2x50G) ポートをサポート。

- 自動ネゴシエーションはサポートされません。
- Cisco NX-OS リリース 10.3(1)F 以降、Cisco Nexus 9800 プラットフォーム スイッチの N9K-X9836DM-A ラインカード用の CVR-QSFP-SFP10G アダプタを使用する、10G オプティックスのサポートが提供されます。
- Cisco NX-OS リリース 10.3(1)F 以降、Cisco Nexus 9800 プラットフォーム スイッチの N9K-X9836DM-A ラインカード用の 40G、100G 銅線ベースのリンクでは、自動ネゴシエーションはサポートされません。
- Cisco NX-OS リリース 10.4(1)F 以降、100G/40G の自動ネゴシエーションは、Cisco Nexus 9332D-H2R プラットフォーム スイッチでサポートされます。ただし、400G はサポートされていません。
- Cisco NX-OS リリース 10.3(1)F 以降、Cisco Nexus 9808 プラットフォーム スイッチで物理インターフェイスのサポートが提供されます。
- Cisco NX-OS リリース 10.4(1)F 以降、Cisco Nexus 9804 プラットフォーム スイッチで物理インターフェイスのサポートが提供されます。
- Cisco Nexus 9808/9804 プラットフォーム スイッチには、物理インターフェイス統計のサポートに関して次の制限があります。
 - ポートチャネルはサポートされません
 - ブロードキャスト カウンタ/統計は、インターフェイス カウンタではサポートされません。
 - ローカルで生成/注入されたパケットは、ユニキャスト、マルチキャスト、またはブロードキャストに分類されません。ただし、これらは合計パケット数とバイト数に含めて計算されます。たとえば、**cdp** パケットです。
- **show interface ethernet 1/1 counters detailed snmp** コマンドの場合、Cisco Nexus 9800 プラットフォームは、次のようにさまざまなフレームサイズ範囲をサポートします：

```
This platform counter Range
=====
TX Frame octet Range
TX legal frames with 1519-2500 bytes.
TX legal frames with 2501-9000 bytes.
Nexus existing platform
=====
TX Length=1519-2047
TX Length=2048-4095
TX Length=4096-8191
TX Length=8192-9215
TX Length>=9216
Similar frame size support exists for Rx direction also.

show interface ethernet 1/1 counters detailed snmp
Ethernet1/1
Rx Packets: 4004
Rx Unicast Packets: 4000
Rx Jumbo Packets: 4000
Rx Bytes: 7031737
Rx Packets from 65 to 127 bytes: 1
```

```

Rx Packets from 128 to 255 bytes: 1
Rx Packets from 512 to 1023 bytes: 1
Rx Packets from 1024 to 1518 bytes: 1
Rx Packets from 1519 to 2500 bytes: 4000 >>>> New range supported
Tx Packets: 17
Tx Bytes: 4948
Tx Packets from 0 to 64 bytes: 2
Tx Packets from 65 to 127 bytes: 3
Tx Packets from 128 to 255 bytes: 10
Tx Packets from 512 to 1023 bytes: 1
Tx Packets from 1024 to 1518 bytes: 1
Tx Packets from 1519 to 2500 bytes: 2 >>>> New range

```

- インターフェイスエラーカウンタでは、Align-Err、Runts、Giants、Input Discards、および Output Discards カウンタはサポートされておらず、0 として表示されます。

次に例を示します。

```
show interface ethernet 1/1 counters errors
```

```
-----
Port Align-Err FCS-Err Xmit-Err Rcv-Err UnderSize OutDiscards
-----
```

```
Eth1/1 0 0 0 0 0 0
```

```
-----
Port Single-Col Multi-Col Late-Col Exces-Col Carri-Sen Runts
-----
```

```
Eth1/1 0 0 0 0 0 0
```

```
-----
Port Giants SQETest-Err Deferred-Tx IntMacTx-Er IntMacRx-Er Symbol-Err
-----
```

```
Eth1/1 0 -- 0 0 0 0
```

```
-----
Port InDiscards
-----
```

```
Eth1/1 0
```

```
-----
Port Stomped-CRC
-----
```

```
Eth1/1 0
```

- Cisco NX-OS リリース 10.3(1)F 以降、Cisco Nexus 9808 プラットフォームスイッチで UDLD のサポートが提供されます。
- Cisco NX-OS リリース 10.4(1)F 以降、Cisco Nexus 9804 プラットフォームスイッチで UDLD のサポートが提供されます。
- Cisco NX-OS リリース 10.4(1)F 以降、UDLD サポートは、Cisco Nexus 9808 および 9804 スイッチを搭載した N9KX98900CD-A および N9KX9836DM-A ラインカードで提供されます。

デフォルト設定

次の表に、基本インターフェイスパラメータのデフォルト設定を示します。

パラメータ	デフォルト
説明	ブランク
ビーコン	ディセーブル
帯域幅	インターフェイスのデータ レート
スループット遅延	100 マイクロ秒
管理ステータス	シャットダウン
MTU	1500 バイト
UDLD グローバル	グローバルにディセーブル
ポート別の UDLD イネーブル ステート (光ファイバメディア用)	すべてのイーサネット光ファイバLANポートでイネーブル
銅線メディア用のポート別 UDLD イネーブルステート	すべてのイーサネット 1G、10G、または 40G LAN ポートでディセーブル
UDLD メッセージの間隔	ディセーブル
UDLD アグレッシブ モード	ディセーブル
エラー ディセーブル	ディセーブル
エラー ディセーブル回復	ディセーブル
エラー ディセーブル回復間隔	300 秒
バッファ ブースト	イネーブル (注) N9K-X9564TX および N9K-X9564PX ライン カードおよび Cisco Nexus 9300 シリーズ デバイスで使用可能な機能。

基本インターフェイスパラメータの設定

インターフェイスを設定する場合、パラメータを設定する前にインターフェイスを指定する必要があります。

設定するインターフェイスの指定

始める前に

同じタイプの1つ以上のインターフェイスのパラメータを設定する前に、インターフェイスのタイプと ID を指定する必要があります。

次の表に、イーサネットインターフェイスおよび管理インターフェイスを指定するために使用するインターフェイスタイプと ID を示します。

表 6: 設定するインターフェイスの識別に必要な情報

インターフェイスタイプ	ID
イーサネット	I/O モジュールのスロット番号およびモジュールのポート番号
管理	0 (ポート 0)

インターフェイス範囲コンフィギュレーションモードを使用して、同じコンフィギュレーションパラメータを持つ複数のインターフェイスを設定できます。インターフェイス範囲コンフィギュレーションモードを開始すると、このモードを終了するまで、入力したすべてのコマンドパラメータが、その範囲内の全インターフェイスに適用されます。

ダッシュ (-) とカンマ (,) を使用して、一定範囲のインターフェイスを入力します。ダッシュは連続しているインターフェイスを区切り、カンマは不連続なインターフェイスを区切ります。不連続なインターフェイスを入力するときは、各インターフェイスのメディアタイプを入力する必要があります。

次に、連続しているインターフェイス範囲の設定例を示します。

```
switch(config)# interface ethernet 2/29-30
switch(config-if-range) #
```

次に、不連続なインターフェイス範囲の設定例を示します。

```
switch(config)# interface ethernet 2/29, ethernet 2/33, ethernet 2/35
switch(config-if-range) #
```

サブインターフェイスが同じポート上の場合にだけ、範囲でサブインターフェイスを指定できます (たとえば、2/29.1-2)。ただし、ポートの範囲でブインターフェイスを指定できません。たとえば、2/29.2-2/30.2 は入力できません。2 つのサブインターフェイスを個別に指定できます。たとえば、2/29.2、2/30.2 を入力できます。

次の例は、ブレイクアウト ケーブルを設定する方法を示しています。

```
switch(config)# interface ethernet 1/2/1
switch(config-if-range) #
```

手順の概要

1. **configure terminal**
2. **interface interface**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： <pre>switch# configure terminal switch(config)#</pre>	グローバル コンフィギュレーション モードを開始します
ステップ 2	interface interface 例： <pre>switch(config)# interface ethernet 2/1 switch(config-if)#</pre> 例： <pre>switch(config)# interface mgmt0 switch(config-if)#</pre>	<p>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 タイプと ID を指定できます。イーサネットポートの場合は、ethernet slot/port を使用します。管理インターフェイスの場合は、mgmt0 を使用します。</p> <p>例：</p> <ul style="list-style-type: none"> • 1 番目の例は、スロット 2、ポート 1 イーサネット インターフェイスを指定する方法を示します。 • 2 番目の例は、管理インターフェイスを指定する方法を示しています。 <p>(注) インターフェイス タイプと ID (ポートまたはスロット/ポート番号) の間にスペースを追加する必要はありません。たとえば、イーサネットスロット 4、ポート 5 インターフェイスの場合は、「ethernet 4/5」または「ethernet4/5」と指定できます。管理インターフェイスは「mgmt0」または「mgmt 0」となります。</p> <p>インターフェイス コンフィギュレーション モードの場合、コマンドを入力するとこのモードに指定したインターフェイスが設定されます。</p>

説明の設定

イーサネットおよび管理インターフェイスの説明を文字で設定します。

手順の概要

1. **configure terminal**
2. **interface interface**
3. **description text**
4. **show interface interface**

5. (任意) `show interface mgmt`
6. `exit`
7. `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	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	グローバル コンフィギュレーション モードを開始します
ステップ 2	interface interface 例 : <pre>switch(config)# interface ethernet 2/1 switch(config-if)#</pre> 例 : <pre>switch(config)# interface mgmt0 switch(config-if)#</pre>	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 タイプと ID を指定できます。イーサネットポートの場合は、 ethernet slot/port を使用します。管理インターフェイスには、 mgmt0 を使用します。 例 : <ul style="list-style-type: none"> • 1 番目の例は、スロット 2、ポート 1 イーサネット インターフェイスを指定する方法を示します。 • 2 番目の例は、管理インターフェイスを指定する方法を示しています。
ステップ 3	description text 例 : <pre>switch(config-if)# description Ethernet port 3 on module 1 switch(config-if)#</pre>	インターフェイスの説明を指定します。
ステップ 4	show interface interface 例 : <pre>switch(config)# show interface ethernet 2/1</pre>	(任意) インターフェイス ステータスを表示します。説明パラメータもあわせて表示します。
ステップ 5	(任意) show interface mgmt 例 : <pre>switch(config)# show interface mgmt 0</pre>	(任意) 管理インターフェイスを表示します。説明パラメータもあわせて表示します。
ステップ 6	exit 例 : <pre>switch(config-if)# exit switch(config)#</pre>	インターフェイス モードを終了します。
ステップ 7	copy running-config startup-config 例 :	(任意) 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

コマンドまたはアクション	目的
switch(config)# copy running-config startup-config	

例

次に、モジュール3のイーサネットポート24にインターフェイスの説明を設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 3/24
switch(config-if)# description server1
switch(config-if)#
```

show interface eth の出力 コマンドの出力は、次の例に示すように拡張されます。

```
Switch# show version
Software
BIOS: version 06.26
NXOS: version 6.1(2)I2(1) [build 6.1(2)I2.1]
BIOS compile time: 01/15/2014
NXOS image file is: bootflash:///n9000-dk9.6.1.2.I2.1.bin
NXOS compile time: 2/25/2014 2:00:00 [02/25/2014 10:39:03]
```

```
switch# show interface ethernet 6/36
Ethernet6/36 is up
admin state is up, Dedicated Interface
Hardware: 40000 Ethernet, address: 0022.bdf6.bf91 (bia 0022.bdf8.2bf3)
Internet Address is 192.168.100.1/24
MTU 9216 bytes, BW 40000000 Kbit, DLY 10 usec
```

show interface mgmt の出力 コマンドの出力は、次の例に示すように拡張されます。

```
switch# show interface mgmt 0mgmt0 is up
admin state is up,
Hardware: GigabitEthernet, address: d009.c863.6660 (bia d009.c863.6660)
Internet Address is 10.10.1.1
MTU 1500 bytes, BW 1000000 Kbit , DLY 10 usec
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, medium is broadcast
full-duplex, 1000 Mb/s
Auto-Negotiation is turned on
Auto-mdix is turned off
EtherType is 0x0000
1 minute input rate 208920 bits/sec, 146 packets/sec
1 minute output rate 514648 bits/sec, 144 packets/sec
Rx
 11890676 input packets 11773213 unicast packets 97704 multicast packets
 19759 broadcast packets 2089190866 bytes
Tx
 11776034 output packets 11774699 unicast packets 1323 multicast packets
 12 broadcast packets 5228573079 bytes
Management transceiver: Present
Active connector: SFP
```

RJ45 コネクタを取り外すと、アクティブなコネクタに SFP が表示されます。

ビーコンモードの設定

イーサネットポートのビーコンモードをイネーブルにしてLEDを点滅させ、物理的な位置を確認します。

手順の概要

1. **configure terminal**
2. **interface ethernet slot/port**
3. **[no] beacon**
4. **show interface ethernet slot/port**
5. **exit**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： switch# configure terminal switch(config)#	グローバル設定モードを開始します。
ステップ 2	interface ethernet slot/port 例： switch(config)# interface ethernet 3/1 switch(config-if)#	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	[no] beacon 例： switch(config)# beacon switch(config-if)#	ビーコンモードをイネーブルにします。またはビーコンモードをディセーブルにします。デフォルトモードはディセーブルです。
ステップ 4	show interface ethernet slot/port 例： switch(config)# show interface ethernet 2/1 switch(config-if)#	(任意) ビーコンモードステータスなど、インターフェイスのステータスを表示します。
ステップ 5	exit 例： switch(config-if)# exit switch(config)#	インターフェイスモードを終了します。
ステップ 6	copy running-config startup-config 例： switch(config)# copy running-config startup-config	(任意) 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

例

次に、イーサネット ポート 3/1 のビーコン モードをイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 3/1
switch(config-if)# beacon
switch(config-if)#
```

次に、イーサネット ポート 3/1 のビーコン モードをディセーブルにする例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 3/1
switch(config-if)# no beacon
switch(config-if)#
```

次に、ポート 4/17、4/19、4/21、4/23 を含むグループでイーサネット ポート 4/17 の専用モードを設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 4/17, ethernet 4/19, ethernet 4/21, ethernet 4/23
switch(config-if)# shutdown
switch(config-if)# interface ethernet 4/17
switch(config-if)# no shutdown
switch(config-if)#
```

Error-Disabled ステートの設定

インターフェイスが error-disabled ステートに移行する理由を表示し、自動回復を設定できます。

Error-Disable 検出のイネーブル化

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

手順の概要

1. **configure terminal**
2. **errdisable detect cause {acl-exception | all | link-flap | loopback}**
3. **shutdown**
4. **no shutdown**
5. **link-flap error-disable count <number_of_link_flaps> interval <time_in_seconds>**
6. **show interface status err-disabled**
7. **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	configure terminal 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	errdisable detect cause {acl-exception all link-flap loopback} 例： switch(config)# errdisable detect cause all switch(config-if)#	インターフェイスを error-disabled ステートにする条件を指定します。デフォルトではイネーブルになっています。
ステップ 3	shutdown 例： switch(config-if)# shutdown switch(config)#	インターフェイスを管理ダウンさせます。インターフェイスを error-disabled ステートから手動で回復させるには、最初にこのコマンドを入力します。
ステップ 4	no shutdown 例： switch(config-if)# no shutdown switch(config)#	インターフェイスを管理アップし、error-disabled ステートから手動で回復させるインターフェイスをイネーブルにします。
ステップ 5	link-flap error-disable count <number_of_link_flaps> interval <time_in_seconds> 例： switch(config-if)# link-flap error-disable count 10 interval 30	設定しているリンク フラップ エラー無効化数および間隔を指定します。 <ul style="list-style-type: none"> • count ポートが許容できるフラップの数を構成します。許容できるフラップの最大数は30で、最小は2です。 • interval は構成されたフラップ数が発生してからアクションが実行されるまでの時間を秒単位で構成します。最小間隔は420秒、最大間隔は30秒です。
ステップ 6	show interface status err-disabled 例： switch(config)# show interface status err-disabled	(任意) error-disabled インターフェイスに関する情報を表示します。
ステップ 7	copy running-config startup-config 例： switch(config)# copy running-config startup-config	(任意) 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

例

次の例では、すべての場合で error-disabled 検出をイネーブルにする方法を示します。

```
switch(config)# errdisable detect cause all
switch(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 error-disabled 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. `configure terminal`
2. `errdisable recovery cause {all | bpduguard | failed-port-state | link-flap | loopback | miscabling | psecure-violation | security-violation | storm-control | udld | vpc-peerlink}`
3. `show interface status err-disabled`
4. `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	configure terminal 例： <pre>switch# configure terminal switch(config)#</pre>	グローバル 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	errdisable recovery cause {all bpduguard failed-port-state link-flap loopback miscabling psecure-violation security-violation storm-control udld vpc-peerlink} 例： <pre>switch(config)# errdisable recovery cause all switch(config-if)#</pre>	インターフェイスが error-disabled ステートから自動的に回復する条件を指定すると、デバイスはインターフェイスを再びアップします。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	show interface status err-disabled 例： <pre>switch(config)# show interface status err-disabled switch(config-if)#</pre>	(任意) error-disabled インターフェイスに関する情報を表示します。
ステップ 4	copy running-config startup-config 例： <pre>switch(config)# copy running-config startup-config</pre>	(任意) 実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

例

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

```
switch(config)# errdisable recovery cause all
switch(config)#
```

error-disable ステート回復間隔の設定

error-disabled 回復タイマーの値を設定できます。

手順の概要

1. **configure terminal**
2. **errdisable recovery interval interval**
3. **show interface status err-disabled**
4. **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	configure terminal 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	errdisable recovery interval interval 例： switch(config)# errdisable recovery interval 32 switch(config-if)#	インターフェイスが error-disabled ステートから回復する間隔を指定します。有効範囲は 30 ~ 65535 秒で、デフォルトは 300 秒です。
ステップ 3	show interface status err-disabled 例： switch(config)# show interface status err-disabled switch(config-if)#	(任意) error-disabled インターフェイスに関する情報を表示します。
ステップ 4	copy running-config startup-config 例： switch(config)# copy running-config startup-config	(任意) 実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

例

次の例では、error-disabled 回復タイマーが回復の間隔を 32 秒に設定するように設定する方法を示します。


```
switch(config)# errdisable recovery interval 32
switch(config)#
```

MDIXパラメータの設定

接続のタイプ（クロスオーバーまたはストレート）を他の銅線イーサネットポート専用にするには、ローカルポートの Medium Dependent Independent Crossover（MDIX）パラメータを有効にします。デフォルトでは、このパラメータはイネーブルです。

始める前に

リモートポートの MDIX を有効にします。

手順の概要

1. **configure terminal**
2. **interface ethernet slot / port**
3. **{mdix auto | no mdix}**
4. **show interface ethernet slot / port**
5. **exit**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface ethernet slot / port 例： switch(config)# interface ethernet 3/1 switch(config-if)#	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	{mdix auto no mdix} 例： switch(config)# mdix auto switch(config-if)# switch(config)# no mdix switch(config-if)#	ポートの MDIX 検出をイネーブルまたはディセーブルにするかどうかを指定します。 (注) この no mdix auto コマンドは、N9K-C93108TC-EX、N9K-C93108TC-FX、N9K-X9788TC-FX、および N9K-C9348GC-FXP デバイスでのみサポートされます。
ステップ 4	show interface ethernet slot / port 例：	インターフェイス ステータスを表示します。MDIX ステータスもあわせて表示します。

SFP-10G-TX のメディア タイプの設定

	コマンドまたはアクション	目的
	switch(config)# show interface ethernet 3/1 switch(config-if)#	
ステップ 5	exit 例： switch(config)# exit	インターフェイス モードを終了します。
ステップ 6	copy running-config startup-config 例： switch(config)# copy running-config startup-config	(任意) 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

例

次に、イーサネット ポート 3/1 の MDIX をイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 3/1
switch(config-if)# mdix auto
switch(config-if)#
```

次に、イーサネット ポート 3/1 の MDIX をイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 3/1
switch(config-if)# no mdix
switch(config-if)#
```

SFP-10G-TX のメディア タイプの設定

インターフェイスで SFP-10G-TX デバイス接続を指定するには、インターフェイス設定モードで **media-type 10g-tx** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

手順の概要

1. `configure terminal`
2. `interface interface-id`
3. `media-type 10g-tx`

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>configure terminal</code> 例： Switch# configure terminal	グローバル設定モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	interface <i>interface-id</i> 例 : Switch (config)# interface ethernet 1/5	設定するポートを指定し、インターフェイス設定モードを開始します。
ステップ 3	media-type 10g-tx 例 : Switch (Config)# [no] media-type 10g-tx	インターフェイスで SFP-10G-TX デバイス接続を設定します。 (注) 管理状態が「Up」のときにメディアタイプ 10G-TX で設定されたインターフェイスは、サポートされていないメディアタイプで <code>errdisable</code> のままになります。この状態を解消するには、インターフェイスで次のコマンドを使用します。 <ul style="list-style-type: none"> • shutdown • no shutdown

メディアタイプの確認

次に、メディアタイプの設定を確認する例を示します。



- (注) SFP-10G-TX をサポートするポートは、デバイスによって異なります。この例では、Cisco Nexus N9K-C93240YC-FX2 スイッチの、SFP-10G-TX をサポートするポート番号を表示します。

```
switch# sh running-config interface ethernet 1/2

!Command: show running-config interface Ethernet1/2
!Running configuration last done at: Mon Jun  1 10:16:46 2020
!Time: Mon Jun  1 10:16:54 2020

version 9.3(5) Bios:version 05.41

interface Ethernet1/2
  switchport
  switchport access vlan 10
  mtu 9216
  media-type 10g-tx
  no shutdown

Supported ports in Switch 01:
switch# sh interface status | i i SFP-10
Eth1/2      --      connected 10      full    10G    SFP-10G-T-X
Eth1/6      --      connected 11      full    10G    SFP-10G-T-X
Eth1/8      --      connected 11      full    10G    SFP-10G-T-X
Eth1/12     --      connected 12      full    10G    SFP-10G-T-X
Eth1/14     --      connected 12      full    10G    SFP-10G-T-X
Eth1/18     --      connected 13      full    10G    SFP-10G-T-X
Eth1/20     --      connected 13      full    10G    SFP-10G-T-X
```

```

Eth1/24      --                connected 14      full    10G    SFP-10G-T-X
Eth1/26      --                connected 14      full    10G    SFP-10G-T-X
Eth1/30      --                connected 15      full    10G    SFP-10G-T-X
Eth1/32      --                connected 15      full    10G    SFP-10G-T-X
Eth1/36      --                connected 16      full    10G    SFP-10G-T-X
Eth1/38      --                connected 16      full    10G    SFP-10G-T-X
Eth1/42      --                connected 20      full    10G    SFP-10G-T-X
Eth1/44      Connect_to_Sw_01  connected 202     full    10G    SFP-10G-T-X
Eth1/48      Connect_to_Sw_02  connected 202     full    10G    SFP-10G-T-X

```

```

switch# sh mod
Mod Ports          Module-Type          Model              Status
-----
1      60      48x10/25G + 12x40/100G Ethernet Modul N9K-C93240YC-FX2  active *

Mod Sw              Hw      Slot
-----
1      9.3(4.104)        0.3020 NA

Mod MAC-Address(es)          Serial-Num
-----
1      b4-de-31-94-4e-c8 to b4-de-31-94-4f-0f  FDO2143306S

Mod Online Diag Status
-----
1      Pass

```

MTU サイズの設定

MTU はインターフェイスごとに設定されます。インターフェイスはレイヤ 2 またはレイヤ 3 インターフェイスにすることができます。すべてのインターフェイスのデフォルト MTU は 1500 バイトです。この値は、システムデフォルト MTU と呼ばれます。レイヤ 2 インターフェイスは、システムジャンボ MTU のデフォルト値である 9216 バイトの値で設定できます。1500 ~ 9216 の MTU 値を許可するには、インターフェイスを同じ値に設定できる適切な値にシステムジャンボ MTU を調整する必要があります。



- (注) システムジャンボ MTU サイズを変更できます。値が変更されると、システムジャンボ MTU 値を使用するレイヤ 2 インターフェイスは新しいシステムジャンボ MTU 値に自動的に変更されます。

レイヤ 3 インターフェイスは、レイヤ 3 物理インターフェイススイッチ仮想インターフェイス (SVI) にすることができます。サブインターフェイスでは、MTU サイズを 576 ~ 9216 バイトに設定できます。

インターフェイス MTU サイズの設定

レイヤ 3 インターフェイスの場合、キーワード MTU と値 (バイト単位) を使用して MTU を設定できます。値は 576 ~ 9216 バイトです。Cisco NX-OS Release 9.3(1) 以降では、すべての Cisco Nexus 9000 スイッチの管理インターフェイスで MTU サイズを最大 9216 バイトに設定で

きます。設定の変更により、エンドデバイスで一時的なリンクフラップがトリガーされることがあります。

レイヤ2インターフェイスの場合、バイト単位の値でキーワードMTUを使用してインターフェイスを設定できます。値は、システムのデフォルトMTUサイズ（1500バイト）、またはシステムジャンボMTU値（デフォルトサイズの9216バイトに調整可能）です。

レイヤ2インターフェイスに別のシステムジャンボMTUサイズを使用する必要がある場合は、「システムジャンボMTUサイズの設定」のセクションを参照してください。

手順の概要

1. **configure terminal**
2. **interface ethernet slot/port, vlan vlan-id mgmt 0**
3. **mtu size**
4. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ1	configure terminal 例： <pre>switch# configure terminal switch(config)#</pre>	グローバルコンフィギュレーションモードを開始します。
ステップ2	interface ethernet slot/port, vlan vlan-id mgmt 0 例： <pre>switch(config)# interface ethernet 3/1 switch(config-if)# switch(config)# interface vlan 100 switch(config-if)# switch(config)# interface mgmt 0 switch(config-if)#</pre>	設定するイーサネット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	mtu size 例： <pre>switch(config-if)# mtu 9216 switch(config-if)#</pre>	インターフェイスのMTU値を設定します。 レイヤ3インターフェイス、物理レイヤ3インターフェイス、SVIまたはサブインターフェイスの場合、値は576～9216バイトです。インターフェイスが物理レイヤ2インターフェイスの場合、値は1500またはシステムジャンボMTU値になります。
ステップ4	exit 例： <pre>switch(config-if)# exit switch(config)#</pre>	インターフェイスモードを終了します。

例

次に、レイヤ 2 イーサネット ポート 3/1 にデフォルト MTU サイズ (1500) を設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 3/1
switch(config-if)# switchport
switch(config-if)# mtu 1500
switch(config-if)#
```

図は、show running-config interface コマンドの出力を示しています。

```
switch# show run int mgmt0
!Command: show running-config interface mgmt0
!Running configuration last done at: Fri May 31 11:32:28 2019
!Time: Fri May 31 11:32:33 2019
version 9.3(1) Bios:version 07.65
interface mgmt0
mtu 9216
vrf member management
ip address 168.51.170.73/82
```

システムジャンボ MTU サイズの設定

レイヤ 2 インターフェイス MTU 値のシステムジャンボ MTU を設定して使用できます。システムジャンボ MTU は、1500～9216 の偶数で指定する必要があります。システムジャンボ MTU のデフォルト値は 9216 バイトです。

手順の概要

1. **configure terminal**
2. **system jumbomtu size**
3. **interface type slot/port**
4. **mtu size**
5. **exit**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	system jumbomtu size 例： switch(config)# system jumbomtu 8000 switch(config)#	システムジャンボ MTU サイズを指定します。1500～9216 の偶数を使用します。

	コマンドまたはアクション	目的
ステップ 3	interface <i>type slot/port</i> 例： switch(config)# interface ethernet 2/1 switch(config-if)#	設定するインターフェイスを指定し、インターフェイスコンフィギュレーションモードを開始します。
ステップ 4	mtu size 例： switch(config-if)# mtu 8000 switch(config-if)#	システムジャンボ MTU がレイヤ 2 インターフェイスに追加されます。
ステップ 5	exit 例： switch(config-if)# exit switch(config)#	インターフェイスモードを終了します。
ステップ 6	copy running-config startup-config 例： switch(config)# copy running-config startup-config	(任意) 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

例

次に、システムジャンボ MTU を 8000 バイトに設定し、以前ジャンボ MTU サイズに設定したインターフェイスの MTU に変更する例を示します。

```
switch# configure terminal
switch(config)# system jumbomtu 8000
switch(config)# interface ethernet 2/2
switch(config-if)# mtu 8000
```

帯域幅の設定

イーサネットインターフェイスの帯域幅を設定できます。物理層は、1G、10G、または 40G の変更されない帯域幅を使用しますが、レベル 3 プロトコルに対して 1 から 100,000,000 KB の値を設定できます。

手順の概要

1. **configure terminal**
2. **interface ethernet** *slot/port*
3. **bandwidth** *kbps*
4. **show interface ethernet** *slot/port*
5. **exit**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： switch# configure terminal switch(config)#	グローバル設定モードを開始します。
ステップ 2	interface ethernet slot/port 例： switch(config)# interface ethernet 3/1 switch(config-if)#	設定するイーサネット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	bandwidth kbps 例： switch(config-if)# bandwidth 1000000 switch(config-if)#	情報用としてのみ 1 ~ 100,000,000 の値を帯域幅に指定します。
ステップ 4	show interface ethernet slot/port 例： switch(config)# show interface ethernet 2/1	(任意) インターフェイスステータスを表示します。帯域幅の値もあわせて表示します。
ステップ 5	exit 例： switch(config-if)# exit switch(config)#	インターフェイスモードを終了します。
ステップ 6	copy running-config startup-config 例： switch(config)# copy running-config startup-config	(任意) 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

例

次に、イーサネットスロット3ポート1インターフェイス帯域幅パラメータに情報用の値 1,000,000 Kb を設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 3/1
switch(config-if)# bandwidth 1000000
switch(config-if)#
```


スループット遅延の設定

イーサネット インターフェイスのインターフェイス スループット遅延を設定できます。実際の遅延時間は変わりませんが、1 ~ 16777215 の情報値を設定できます。単位は 10 マイクロ秒です。

手順の概要

1. **configure terminal**
2. **interface ethernet slot/port**
3. **delay value**
4. **show interface ethernet slot/port**
5. **exit**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： switch# configure terminal switch(config)#	グローバル設定モードを開始します。
ステップ 2	interface ethernet slot/port 例： switch(config)# interface ethernet 3/1 switch(config-if)#	設定するイーサネット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	delay value 例： switch(config-if)# delay 10000 switch(config-if)#	遅延時間を 10 マイクロ秒単位で指定します。1 ~ 16777215 の範囲の情報値を 10 マイクロ秒単位で設定できます。
ステップ 4	show interface ethernet slot/port 例： switch(config)# show interface ethernet 3/1 switch(config-if)#	(任意) インターフェイス ステータスを表示します。スループット遅延時間もあわせて表示します。
ステップ 5	exit 例： switch(config-if)# exit switch(config)#	インターフェイス モードを終了します。
ステップ 6	copy running-config startup-config 例： switch(config)# copy running-config startup-config	(任意) 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

例

次に、あるインターフェイスが別のインターフェイスに優先するように、スループット遅延時間を設定する例を示します。低い遅延値が高い値に優先します。この例では、イーサネット 7/48 は 7/47 よりも優先されます。7/48 のデフォルトの遅延は、最大値 (16777215) に設定されている 7/47 の設定値より小さいです。

```
switch# configure terminal
switch(config)# interface ethernet 7/47
switch(config-if)# delay 16777215
switch(config-if)# ip address 192.168.10.1/24
switch(config-if)# ip router eigrp 10
switch(config-if)# no shutdown
switch(config-if)# exit
switch(config)# interface ethernet 7/48
switch(config-if)# ip address 192.168.11.1/24
switch(config-if)# ip router eigrp 10
switch(config-if)# no shutdown
switch(config-if)#
```



(注) **feature eigrp** コマンドを実行して、最初に EIGRP 機能がイネーブルであることを確認するコマンドを使用します。

インターフェイスのシャットダウンおよび再開

イーサネットまたは管理インターフェイスはシャットダウンして再起動できます。インターフェイスはシャットダウンするとディセーブルになり、すべてのモニタ画面にはダウン状態で表示されます。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。シャットダウンし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。インターフェイスを再開するには、デバイスを再起動する必要があります。

手順の概要

1. **configure terminal**
2. **interface interface**
3. **shutdown**
4. **show interface interface**
5. **no shutdown**
6. **show interface interface**
7. **exit**
8. **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	configure terminal 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します
ステップ 2	interface interface 例： switch(config)# interface ethernet 2/1 switch(config-if)# switch(config)# interface mgmt0 switch(config-if)#	設定するインターフェイスを指定します。インターフェイスタイプと ID を指定できます。イーサネットポートの場合は、 <i>ethernet slot/port</i> を使用します。管理インターフェイスの場合は、 <i>mgmt0</i> を使用します。 例： <ul style="list-style-type: none">• 1 番目の例は、スロット 2、ポート 1 イーサネット インターフェイスを指定する方法を示します。• 2 番目の例は、管理インターフェイスを指定する方法を示しています。
ステップ 3	shutdown 例： switch(config-if)# shutdown switch(config-if)#	インターフェイスをディセーブルにします。
ステップ 4	show interface interface 例： switch(config-if)# show interface ethernet 2/1 switch(config-if)#	(任意) インターフェイス ステータスを表示します。管理ステータスもあわせて表示します。
ステップ 5	no shutdown 例： switch(config-if)# no shutdown switch(config-if)#	インターフェイスを再びイネーブルにします。
ステップ 6	show interface interface 例： switch(config-if)# show interface ethernet 2/1 switch(config-if)#	(任意) インターフェイス ステータスを表示します。管理ステータスもあわせて表示します。
ステップ 7	exit 例： switch(config-if)# exit switch(config)#	インターフェイス モードを終了します。

	コマンドまたはアクション	目的
ステップ 8	copy running-config startup-config 例： <pre>switch(config)# copy running-config startup-config</pre>	(任意) 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

例

次に、イーサネットポート 3/1 の管理ステータスをディセーブルからイネーブルに変更する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 3/1
switch(config-if)# shutdown
switch(config-if)# no shutdown
switch(config-if)#
```

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、ノーマルモードの UDLD を設定できます。

インターフェイスのアグレッシブ UDLD モードをイネーブルにするには前もって、そのデバイス上でグローバルに、および指定したインターフェイスで、UDLD をイネーブルにしておく必要があります。



- (注) インターフェイスが銅線ポートの場合は、**enable UDLD** コマンドを使用して UDLD をイネーブルにする必要があります。インターフェイスがファイバポートの場合、インターフェイスで UDLD を明示的にイネーブルにする必要はありません。ただし、**enable UDLD** コマンドを使用してファイバポートで UDLD をイネーブルにしようとすると、それが有効なコマンドではないことを示すエラーメッセージが表示されることがあります。

以下の表に、異なるインターフェイスで UDLD をイネーブルおよびディセーブルにする CLI 詳細を示します。

表 7: 異なるインターフェイスで UDLD をイネーブルおよびディセーブルにする CLI 詳細

説明	ファイバポート	銅線またはファイバ以外のポート
デフォルト設定	有効	無効
enable UDLD コマンド	no udld disable	udld enable
disable UDLD コマンド	udld disable	no udld enable

始める前に

他方のリンク先ポートおよびデバイスで UDLD をイネーブルにする必要があります。

手順の概要

1. **configure terminal**
2. **[no] feature udld**
3. **udld message-time *seconds***
4. **udld aggressive**
5. **interface ethernet *slot/port***
6. **udld [enable | disable]**
7. **show udld [ethernet *slot/port* | global | neighbors]**
8. **exit**
9. **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	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	グローバル設定モードを開始します。
ステップ 2	[no] feature udld 例 : <pre>switch(config)# feature udld switch(config)# switch(config)# no feature udld switch(config)#</pre>	デバイスの UDLD をイネーブル/ディセーブルにします。
ステップ 3	udld message-time <i>seconds</i> 例 : <pre>switch(config)# udld message-time 30 switch(config)#</pre>	(任意) UDLD メッセージを送信する間隔を指定します。有効な範囲は 7 ~ 90 秒で、デフォルトは 15 秒です。
ステップ 4	udld aggressive 例 : <pre>switch(config)# udld aggressive switch(config)#</pre>	すべての光ファイバインターフェイス上で、アグレッシブモード UDLD をデフォルトで有効にします。すべてのファイバポートでアグレッシブモードの UDLD をデフォルトでディセーブルにするには、 no 形式を使用します。

	コマンドまたはアクション	目的
		<p>(注) UDLDモードを使用するようにポートを構成するには、<code>udld aggressive</code> コマンドを使用します。</p> <ul style="list-style-type: none"> • アグレッシブモードの光ファイバインターフェイスをイネーブルにするには、グローバルコマンドモードで <code>udld aggressive</code> コマンドを入力します。これにより、すべての光ファイバインターフェイスがアグレッシブUDLDモードになります。 • 銅線インターフェイスでアグレッシブモードをイネーブルにするには、インターフェイスモードで <code>udld aggressive</code> コマンドを入力し、アグレッシブUDLDモードに設定したい各インターフェイスを指定します。 <p>アグレッシブUDLDモードを使用するには、リンクの両端のインターフェイスをアグレッシブUDLDモードに構成する必要があります。</p>
ステップ 5	<p><code>interface ethernet slot/port</code></p> <p>例 :</p> <pre>switch(config)# interface ethernet 3/1 switch(config-if)#</pre>	<p>(任意) 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。</p>
ステップ 6	<p><code>udld [enable disable]</code></p> <p>例 :</p> <pre>switch(config-if)# udld enable switch(config-if)#</pre>	<p>すべての光ファイバインターフェイス上で、標準モードのUDLDをデフォルトでイネーブルにします。すべてのファイバポートで通常モードのUDLDをデフォルトでディセーブルにするには、<code>no</code>形式を使用します。</p>
ステップ 7	<p><code>show udld [ethernet slot/port global neighbors]</code></p> <p>例 :</p> <pre>switch(config)# show udld switch(config)#</pre>	<p>(任意) UDLDのステータスを表示します。</p>
ステップ 8	<p><code>exit</code></p> <p>例 :</p> <pre>switch(config-if-range)# exit switch(config)#</pre>	<p>インターフェイスモードを終了します。</p>

	コマンドまたはアクション	目的
ステップ 9	copy running-config startup-config 例 : <pre>switch(config)# copy running-config startup-config</pre>	(任意) 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

例

次に、デバイスの UDLD をイネーブルにする例を示します。

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

次の例では、UDLD メッセージの間隔を 30 秒に設定する方法を示します。

```
switch# configure terminal
switch(config)# feature udld
switch(config)# udld message-time 30
switch(config)#
```

次に、イーサネットポートの 3/1 の UDLD をディセーブルにする例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 3/1
switch(config-if-range)# no udld enable
switch(config-if-range)# exit
```

次に、デバイスの UDLD をディセーブルにする例を示します。

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

次の例は、光ファイバインターフェイスのアグレッシブ 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)# udld aggressive
```

次の例は、銅線イーサネットインターフェイス 3/1 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 3
switch(config-if)# udld aggressive
```

次の例は、アグレッシブモードがイネーブルになっているかどうかを確認する方法を示しています。

```
switch# sh udld global
```

```
UDLD global configuration mode: enabled-aggressive
UDLD global message interval: 15
switch#
```

次に、udld アグレッシブモードが特定のインターフェイスで動作可能かどうかを確認する例を示します。

```
switch# sh uddl ethernet 8/2

Interface Ethernet8/2
-----
Port enable administrative configuration setting: device-default
Port enable operational state: enabled-aggressive
Current bidirectional state: bidirectional
Current operational state: advertisement - Single neighbor detected
Message interval: 15
Timeout interval: 5
<>
```

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。



- (注) サービスプロバイダー ネットワークに接続すると、10G および 100G ポートのリンク状態が繰り返し変化することがあります。リンクリセットまたはブレイクリンク機能の一部として、リンク状態が変更された場合に、SFP の Tx 電源ライトが N/A 状態に変更されることが予想されます。

ただし、リンク状態の変更中にこの動作を防ぐには、リンク デバウンス タイマーを 500 ミリ秒から開始し、リンクが安定するまで 500 ミリ秒間隔で増加します。DWDM、UVN、および WAN ネットワークでは、可能な限り自動リンク一時停止 (ALS) を無効にすることをお勧めします。Nexus がリンクをオフにすると、ALS は WAN 上のリンクを一時停止します。



(注)

link debounce time および **link debounce link-up time** 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。

すべてのイーサネット ポートのデバウンス時間を表示するには、**show interface debounce** コマンドを使用します。

この **link debounce time** コマンドは、Cisco Nexus 9000 シリーズ スイッチの 1G、10G、40G、25G、および 100G SFP / QSFP ポートでサポートされます。

link debounce time は、Cisco Nexus N9K-C9732C-FX、N9K-C9364C、N9K-X97160YC-EX、N9K-C9336C-FX2、および N9K-C93240YC-FX2 プラットフォーム スイッチで 1G、10G、25G、40G、100G ポートがサポートされます。

link debounce time は、N9K-X97160TC-FX ライン カードを搭載した Cisco Nexus 9500 プラットフォーム スイッチの RJ-45 ポートではサポートされません。

Cisco NX-OS リリース 10.2(3)F 以降、**link debounce time** コマンドは N9K-C93180YC-FX3S、N9K-C93180YC-FX3、N9K-C93108TC-FX3P、および N9K-X9716D-GX プラットフォーム スイッチでサポートされています。

Cisco NX-OS リリース 10.2(3)F 以降、**link debounce time** コマンドは次のポートおよびプラットフォーム スイッチでサポートされています。

ポート	スイッチ
1G	Cisco Nexus N9K-C9364C、N9K-C93300YC-FX2、N9K-C93240YC-FX2、N9K-C93240YC-FX2-Z、N9K-X97160YC-EX、N9K-C9316D-GX、N9K-CCD-C9360 N9K-C9232C、N9K-C9232C、N9K-C93180YC-EX、N9K-C93180YC-EXU、N9K-C93180YC-EX-24、N9K-C93180YC-FX3S、N9K-C93180YC-FX3、N9K-C93108TC-FX3P、および N9K-X9716D-GX
10G	Cisco Nexus N9K-C9364C、N9K-C93300YC-FX2、N9K-C93240YC-FX2、N9K-C93240YC-FX2-Z、N9K-X97160YC-EX、N9K-C9316D-GX、N9K-CCD-C9360 N9K-C9232C、N9K-C9232C、N9K-C93180YC-EX、N9K-C93180YC-EXU、N9K-C93180YC-EX-24、N9K-C93180YC-FX3S、N9K-C93180YC-FX3、N9K-C93108TC-FX3P、および N9K-X9716D-GX
25 G	Cisco Nexus N9K-C93300YC-FX2、N9K-C93240YC-FX2、N9K-C93240YC-FX2-Z、N9K-X97160YC-EX、N9K-C9316D-GX、N9K-C93600CD-GX、N9K-C9、N9K-C93180YC-EX、N9K-C93180YC-EXU、N9K-C93180YC-EX-24、N9K-C93180YC-FX3S、N9K-C93180YC-FX3、N9K-C93108TC-FX3P、および N9K-X97 16D-GX
40G	Cisco Nexus N9K-C9364C、N9K-X9732C-FX、N9K-C9336C-FX2、
100G	N9K-C93300YC-FX2、N9K-C93240YC-FX2、N9K-C93240YC-FX2-Z、N9K-EX-C9716-EX、N9K-C93600CD-GX、N9K-C9364C-GX、N9K-C9232C、
400G	N9K-C93180YC-EX、N9K-C93180YC-EXU、N9K-C93180YC-EX-24、N9K-C93180YC-FX3S、N9K-C93180YC-FX3、N9K-C93108TC-FX3P、および N9K-X9716D-GX

手順の概要

1. **configure terminal**
2. **interface ethernet slot/port**
3. **link debounce time time**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： switch# configure terminal switch(config)#	グローバル設定モードを開始します。
ステップ 2	interface ethernet slot/port 例： switch(config)# interface ethernet 3/1 switch(config-if)#	設定するイーサネット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	link debounce time time 例： switch(config-if)# link debounce time 1000 switch(config-if)#	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 タイマーがディセーブルになります。

例

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

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

- 次に、イーサネットインターフェイスのデバウンス タイマーを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)# link debounce time 0
```

ポートプロファイルの設定

いくつかの設定パラメータを一定範囲のインターフェイスに同時に適用できます。範囲内のすべてのインターフェイスが同じタイプである必要があります。また、1つのポートプロファイ

ルから別のポートプロファイルに設定を継承することもできます。システムは4つのレベルの継承をサポートしています。

ポートプロファイルの作成

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



(注) ポートプロファイル名には、次の文字のみを含めることができます。

- a ~ z
- A ~ Z
- 0 ~ 9
- 次の場合を除き、特殊文字は使用できません。
 - .
 - -
 - _

手順の概要

1. **configure terminal**
2. **port-profile [type {ethernet | interface-vlan | port-channel}] name**
3. **exit**
4. (任意) **show port-profile**
5. (任意) **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	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	port-profile [type {ethernet interface-vlan port-channel}] name	指定されたタイプのインターフェイスのポートプロファイルを作成して命名し、ポートプロファイル コンフィギュレーション モードを開始します。
ステップ 3	exit	ポートプロファイル コンフィギュレーション モードを終了します。
ステップ 4	(任意) show port-profile	ポートプロファイル設定を表示します。

	コマンドまたはアクション	目的
ステップ 5	(任意) copy running-config startup-config	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、イーサネットインターフェイスに対して **test** という名前のポートプロファイルを作成する方法を示したものです。

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

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

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

手順の概要

1. **configure terminal**
2. **port-profile [type {ethernet | interface-vlan | port-channel}] name**
3. **exit**
4. (任意) **show port-profile**
5. (任意) **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	configure terminal	グローバルコンフィギュレーションモードを開始します。
ステップ 2	port-profile [type {ethernet interface-vlan port-channel}] name	指定されたポートプロファイルのポートプロファイルコンフィギュレーションモードを開始し、プロファイルの設定を追加または削除します。
ステップ 3	exit	ポートプロファイルコンフィギュレーションモードを終了します。
ステップ 4	(任意) show port-profile	ポートプロファイル設定を表示します。
ステップ 5	(任意) copy running-config startup-config	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、指定されたポートプロファイルのポートプロファイルコンフィギュレーションモードを開始し、すべてのインターフェイスを管理的にアップする例を示します。

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

一定範囲のインターフェイスへのポートプロファイルの割り当て

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

手順の概要

1. **configure terminal**
2. **interface** [ethernet *slot/port* | interface-vlan *vlan-id* | port-channel *number*]
3. **inherit port-profile** *name*
4. **exit**
5. (任意) **show port-profile**
6. (任意) **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	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface [ethernet <i>slot/port</i> interface-vlan <i>vlan-id</i> port-channel <i>number</i>]	インターフェイスの範囲を選択します。
ステップ 3	inherit port-profile <i>name</i>	指定したポートプロファイルを、選択したインターフェイスに割り当てます。
ステップ 4	exit	ポートプロファイル コンフィギュレーション モードを終了します。
ステップ 5	(任意) show port-profile	ポートプロファイル設定を表示します。
ステップ 6	(任意) copy running-config startup-config	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、イーサネット インターフェイス 7/3 ~ 7/5、10/2、および 11/20 ~ 11/25 に adam という名前のポート プロファイルを割り当てる例を示します。

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

特定のポート プロファイルのイネーブル化

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

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

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

手順の概要

1. **configure terminal**
2. **port-profile [type {ethernet | interface-vlan | port-channel}] name**
3. **state enabled**
4. **exit**
5. (任意) **show port-profile**
6. (任意) **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	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	port-profile [type {ethernet interface-vlan port-channel}] name	指定されたタイプのインターフェイスのポート プロファイルを作成して命名し、ポート プロファイル コンフィギュレーション モードを開始します。
ステップ 3	state enabled	そのポート プロファイルをイネーブルにします。
ステップ 4	exit	ポート プロファイル コンフィギュレーション モードを終了します。

	コマンドまたはアクション	目的
ステップ 5	(任意) show port-profile	ポートプロファイル設定を表示します。
ステップ 6	(任意) copy running-config startup-config	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、ポートプロファイルコンフィギュレーションモードを開始し、ポートプロファイルをイネーブルにする方法を示したものです。

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

ポートプロファイルの継承

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

手順の概要

1. **configure terminal**
2. **port-profile name**
3. **inherit port-profile name**
4. **exit**
5. (任意) **show port-profile**
6. (任意) **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	configure terminal	グローバルコンフィギュレーションモードを開始します。
ステップ 2	port-profile name	指定されたポートプロファイルに対して、ポートプロファイルコンフィギュレーションモードを開始します。
ステップ 3	inherit port-profile name	別のポートプロファイルを既存のポートプロファイルに継承します。元のポートプロファイルは、継承されたポートプロファイルのすべての設定を想定します。

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

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

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

一定範囲のインターフェイスからのポートプロファイルの削除

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

手順の概要

1. **configure terminal**
2. **interface [ethernet slot/port | interface-vlan vlan-id | port-channel number]**
3. **no inherit port-profile name**
4. **exit**
5. (任意) **show port-profile**
6. (任意) **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	configure terminal	グローバルコンフィギュレーションモードを開始します。
ステップ 2	interface [ethernet slot/port interface-vlan vlan-id port-channel number]	インターフェイスの範囲を選択します。
ステップ 3	no inherit port-profile name	指定したポートプロファイルを、選択したインターフェイスから割り当て解除します。

継承されたポートプロファイルの削除

	コマンドまたはアクション	目的
ステップ 4	exit	ポートプロファイルコンフィギュレーションモードを終了します。
ステップ 5	(任意) show port-profile	ポートプロファイル設定を表示します。
ステップ 6	(任意) copy running-config startup-config	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、イーサネットインターフェイス 7/3 ~ 7/5、10/2、および 11/20 ~ 11/25 から adam という名前のポートプロファイルを割り当て解除する例を示します。

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

継承されたポートプロファイルの削除

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

手順の概要

1. **configure terminal**
2. **port-profile name**
3. **no inherit port-profile name**
4. **exit**
5. (任意) **show port-profile**
6. (任意) **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	configure terminal	グローバルコンフィギュレーションモードを開始します。
ステップ 2	port-profile name	指定されたポートプロファイルに対して、ポートプロファイルコンフィギュレーションモードを開始します。
ステップ 3	no inherit port-profile name	このポートプロファイルから継承されたポートプロファイルを削除します。

	コマンドまたはアクション	目的
ステップ 4	exit	ポート プロファイル コンフィギュレーション モードを終了します。
ステップ 5	(任意) show port-profile	ポート プロファイル設定を表示します。
ステップ 6	(任意) copy running-config startup-config	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

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

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

リンク MAC アップタイマーの設定

この手順では、DWDM/ダーク ファイバ回線で MAC アップタイマーを設定する方法について説明します。

手順の概要

1. **configure terminal**
2. **interface type slot/port**
3. **link mac-up timer seconds**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface type slot/port 例： switch(config)# interface ethernet1/2 switch(config-if)#	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 3	link mac-up timer seconds 例： <pre>switch(config-if)# link mac-up timer 10</pre>	リンク MAC アップ タイマーの変更をイネーブルにします。リンク MAC アップ タイマーの範囲は 0 ～ 120 です。 (注) これは、DWDM リンクでのみ実行する必要があります。

25G 自動ネゴシエーションの設定

自動ネゴシエーションを使用すると、デバイスはリンクセグメントを介して所有する拡張動作モードをアダプタイズし、他のデバイスがアダプタイズする可能性がある対応する拡張動作モードを検出できます。自動ネゴシエーションは、リンクセグメントを共有する2つのデバイス間で情報を交換し、両方のデバイスの機能を最大限に活用するように自動的に設定する方法を提供します。

25G 自動ネゴシエーションの注意事項と制限事項

- Cisco NX-OS Release 9.2(1) 以降では、Cisco Nexus N9K-X97160YC-EX、N9K-C93180YC-FX、N9K-C93240YC-FX2、および N9K-C93240YC-FX2-Z で、銅ケーブルを使用したネイティブ 25G ポートでの自動ネゴシエーションがサポートされています。
- 自動ネゴシエーションは、Cisco Nexus N9K-C92300YC スイッチではサポートされていません。
- 自動ネゴシエーションは、25G ブレークアウトポートではサポートされていません。

25G 自動ネゴシエーションによる FEC 選択

表 8: 25G 自動ネゴシエーションによる FEC 選択

ハードウェア	CR 長に基づく FEC			
	1 m	2m	3m	5m
N9K-C93240YC-FX2	FEC なし	FEC なし	FC-FEC	RS-IEEE
N9K-C93180YC-FX	FEC なし	FEC なし	FC-FEC	RS-IEEE
N9K-C93180YC-EX	FEC なし	FEC なし	FC-FEC	FC-FEC
N9K-X97160YC-EX	FEC なし	FEC なし	FC-FEC	FC-FEC



(注) 25G 自動ネゴシエーションは、Cisco Nexus N9K-C92300YC スイッチではサポートされていません。

自動ネゴシエーションの有効化

`negotiate auto` を使用して自動ネゴシエーションを有効にできます。コマンドを使用する必要があります。自動ネゴシエーションを有効にするには、次の手順を実行します。

手順の概要

1. `configure terminal`
2. `interface ethernet port number`
3. `negotiate auto port 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	configure terminal 例： <code>switch# configure terminal</code> <code>switch(config)#</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	interface ethernet port number 例： <code>switch# int e1/7</code> <code>switch(config-if)#</code>	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	negotiate auto port speed 例： <code>switch(config-if)# negotiate auto 25000</code> <code>switch(config-if)#</code>	選択したインターフェイスの自動ネゴシエーションを有効にします。 (注) このコマンドは、25G ネイティブ リンクの両側のインターフェイスに適用する必要があります。

次に、指定したイーサネットインターフェイスで自動ネゴシエーションを有効にする例を示します。

例

```
switch# sh int e1/7 st
-----
Port          Name          Status      Vlan      Duplex  Speed  Type
-----
Eth1/7        --            connected   routed    full    25G    SFP-H25GB-CU1M
switch# conf
```

```
switch(config)# int e1/7
switch(config-if)# negotiate auto 25000
```

自動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、自動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。自動ネゴシエーションを設定するには、次の手順を実行します。

手順の概要

1. **configure terminal**
2. **interface ethernet *port number***
3. **no negotiate auto *port 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	configure terminal 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface ethernet <i>port number</i> 例： switch# int e1/7 switch(config-if)#	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	no negotiate auto <i>port speed</i> 例： switch(config-if)# no negotiate auto 25000 switch(config-if)#	選択したインターフェイスの自動ネゴシエーションをディセーブルにします。 (注) このコマンドは、リンクの両側のインターフェイスに適用する必要があります。

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

例

```
switch# sh int e1/7 st
-----
Port          Name          Status      Vlan      Duplex  Speed  Type
-----
Eth1/7        --            connected  routed   full    25G    SFP-H25GB-CU1M
switch# conf
switch(config)# int e1/7
switch(config-if)# no negotiate auto 25000
```

基本インターフェイスパラメータの確認

基本インターフェイスパラメータは、値を表示して確認します。パラメータ値を表示してカウンタのリストをクリアすることもできます。

基本的なインターフェイス設定情報を表示するには、次の作業のいずれかを行います。

コマンド	目的
show cdp all	CDP ステータスを表示します。
show interface interface	1つまたはすべてのインターフェイスに設定されている状態を表示します。
show interface brief	インターフェイスの状態表を表示します。
show interface status err-disabled	error-disabled インターフェイスに関する情報を表示します。
show udld interface	現在のインターフェイスまたはすべてのインターフェイスの UDLD ステータスを表示します。
show udld global	現在のデバイスの UDLD ステータスを表示します。

インターフェイスカウンタのモニタリング

Cisco NX-OS を使用して、インターフェイスカウンタを表示し、クリアできます。

インターフェイス統計情報の表示

インターフェイスでの統計情報の収集に、最大3つのサンプリング間隔を設定できます。

手順の概要

1. **configure terminal**
2. **interface ether slot/port**
3. **load-interval counters [1 | 2 | 3] seconds**
4. **show interface interface**
5. **exit**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： switch# configure terminal switch(config)#	グローバル設定モードを開始します。
ステップ 2	interface ether slot/port 例： switch(config)# interface ether 4/1 switch(config)#	インターフェイスを指定します。
ステップ 3	load-interval counters [1 2 3] seconds 例： switch(config)# load-interval counters 1 100 switch(config)#	ビットレートおよびパケットレートの統計情報を収集する最大 3 つのサンプリング間隔を設定します。各カウンタのデフォルト値は、次のとおりです。 1 : 30 秒 (VLAN の場合は 60 秒) 2 : 300 秒 3 : 未設定
ステップ 4	show interface interface 例： switch(config)# show interface ethernet 2/2 switch#	(任意) インターフェイス ステータスを表示します。カウンタもあわせて表示します。
ステップ 5	exit 例： switch(config-if-range)# exit switch(config)#	インターフェイス モードを終了します。
ステップ 6	copy running-config startup-config 例： switch(config)# copy running-config startup-config	(任意) 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

例

次に、イーサネットポート 3/1 の 3 種類のサンプリング間隔を設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 3/1
switch(config-if)# load-interval counter 1 60
switch(config-if)# load-interval counter 2 135
switch(config-if)# load-interval counter 3 225
switch(config-if)#
```


インターフェイスカウンタのクリア

clear counters interface を使用して、イーサネットおよび管理インターフェイスカウンタをクリアできます。コマンドを使用して、イーサネットおよび管理インターフェイスカウンタをクリアできます。この作業は、コンフィギュレーションモードまたはインターフェイスコンフィギュレーションモードで実行できます。

手順の概要

1. **clear counters interface** [**all** | **ethernet slot/port** | **loopback number** | **mgmt number** | **port channel channel-number**]
2. **show interface interface**
3. **show interface** [**ethernet slot/port** | **port channel channel-number**] **counters**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	clear counters interface [all ethernet slot/port loopback number mgmt number port channel channel-number] 例： switch# clear counters ethernet 2/1 switch#	インターフェイスカウンタをクリアします。
ステップ 2	show interface interface 例： switch# show interface ethernet 2/1 switch#	(任意) インターフェイスのステータスを表示します。
ステップ 3	show interface [ethernet slot/port port channel channel-number] counters 例： switch# show interface ethernet 2/1 counters switch#	(任意) インターフェイスカウンタを表示します。

例

次に、イーサネットポート 5/5 のカウンタをクリアする例を示します。

```
switch# clear counters interface ethernet 5/5
switch#
```

DWDMの設定

使用可能な96の波長のいずれかで動作するようにDWDMを設定できます。

手順の概要

1. **configure terminal**
2. **interface interface**
3. **itu channel 1-96**
4. **exit**
5. **show run interface**
6. **show itu channel all**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します
ステップ 2	interface interface 例： config)# interface <type slot/port> switch(config-if)#	インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	itu channel 1-96 例： config)# interface <type slot/port> switch(config-if)# itu channel ?	ituチャンネル値を指定し、設定を入力します。
ステップ 4	exit 例： switch(config-if)# exit switch(config)#	インターフェイス モードを終了します。
ステップ 5	show run interface 例： switch(config)# show run interface <type slot/port> switch(config)#	ituチャンネルの値を表示します。
ステップ 6	show itu channel all 例： switch(config)# show itu channel [<> all] switch# sh itu channel ?	すべてのITUチャンネル、波長、および周波数のマッピングを表示します。

QSA の設定例

Cisco Nexus 9396PX :

- ポート 2/1 のデフォルト設定を使用して、ポートグループ 2/1-6 のすべての QSFP は速度 40G になります。ポートグループ 2/1-6 に QSA モジュールがある場合は、`error disabled` になります。
- `speed-group [10000 | 40000]` コマンドを使用してポート 2/7 を設定し、ポートグループ 2/7-12 内のすべての QSA を 10G または 40G の速度にします。ポートグループ 2/7-12 に QSFP モジュールがある場合は、`error disabled` になります。

次の例は、Cisco Nexus 9396PX の速度グループの最初のポートに関して QSA を設定する方法を示したものです。

```
switch# conf t
switch(config)# interface ethernet 2/7
switch(config-if)# speed-group 10000
```




第 4 章

レイヤ 2 インターフェイスの設定

- [アクセス インターフェイスとトランク インターフェイスについて \(93 ページ\)](#)
- [レイヤ 2 インターフェイスの前提条件 \(101 ページ\)](#)
- [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 \(101 ページ\)](#)
- [レイヤ 2 インターフェイスのデフォルト設定 \(107 ページ\)](#)
- [アクセス インターフェイスとトランク インターフェイスの設定 \(108 ページ\)](#)
- [インターフェイス コンフィギュレーションの確認 \(129 ページ\)](#)
- [レイヤ 2 インターフェイスのモニタリング \(130 ページ\)](#)
- [アクセス ポートおよびトランク ポートの設定例 \(130 ページ\)](#)
- [関連資料 \(131 ページ\)](#)

アクセス インターフェイスとトランク インターフェイスについて



(注) ハイアベイラビリティ機能の詳細については、『[Cisco Nexus 9000 Series NX-OS High Availability and Redundancy Guide](#)』を参照してください。



(注) このデバイスは、IEEE 802.1Q タイプ VLAN トランク カプセル化だけをサポートします。

アクセス インターフェイスとトランク インターフェイスの概要

レイヤ 2 ポートは、アクセスまたはトランク ポートとして次のように設定できます。

- アクセス ポートでは VLAN を 1 つだけ設定でき、1 つの VLAN のトラフィックだけを伝送できます。

- トランクポートには複数のVLANを設定でき、複数のVLANのトラフィックを同時に伝送できます。

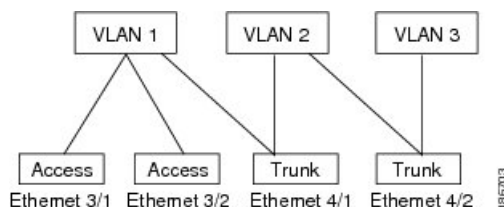
デフォルトでは、Cisco Nexus 9300-EX スイッチのすべてのポートはレイヤ3ポートであり、Cisco Nexus 9300 スイッチのすべてのポートはレイヤ2ポートです。

セットアップスクリプトを使用するか、**system default switchport** コマンドを入力して、すべてのポートをレイヤ2ポートにできます。すべてのポートをレイヤ2ポートにできます。セットアップスクリプトを使用する詳細については、『[Cisco Nexus 9000 Series NX-OS Fundamentals Configuration Guide](#)』を参照してください。CLIを使用して、ポートをレイヤ2ポートとして設定するには、**switchport** コマンドを使用します。

同じトランクのすべてのポートが同じVDCであることが必要です。トランクポートは異なるVDCのVLANのトラフィックを伝送できません。

次の図は、ネットワークにおけるトランクポートの使い方を示したものです。トランクポートは、2つ以上のVLANのトラフィックを伝送します。

図2: トランクおよびアクセスポートとVLANトラフィック



- (注) VLANについては、『[Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide](#)』を参照してください。

複数のVLANに接続するトランクポートのトラフィックを正しく伝送するために、デバイスはIEEE 802.1Qカプセル化（タギング方式）を使用します（詳細については、「IEEE 802.1Qカプセル化」の項を参照）。



- (注) レイヤ3インターフェイス上のサブインターフェイスの詳細については、『[Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide](#)』を参照してください。

アクセスポートでのパフォーマンスを最適化するには、そのポートをホストポートとして設定します。ホストポートとして設定されたポートは、自動的にアクセスポートとして設定され、チャンネルグループ化はディセーブルになります。ホストを割り当てると、割り当てたポートがパケット転送を開始する時間が短縮されます。

ホストポートとして設定できるのは端末だけです。端末以外のポートをホストとして設定しようとするとエラーになります。

アクセスポートは、アクセス VLAN 値の他に 802.1Q タグがヘッダーに設定されたパケットを受信すると、送信元の MAC アドレスを学習せずにドロップします。

レイヤ2インターフェイスはアクセスポートまたはトランクポートとして機能できますが、両方のポートタイプとして同時に機能できません。

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戻すと、このインターフェイスはレイヤ2の設定をすべて失い、デフォルト VLAN 設定に戻ります。

IEEE 802.1Q カプセル化

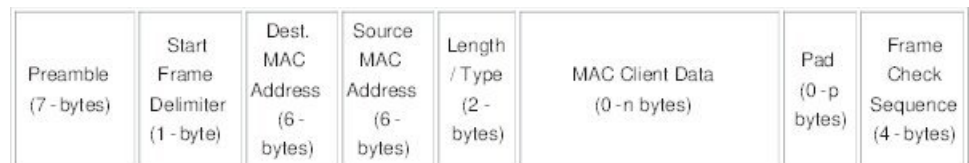


- (注) VLAN の詳細については、『[Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide](#)』を参照してください。

トランクとは、スイッチと他のネットワークデバイス間のポイントツーポイントリンクです。トランクは1つのリンクを介して複数の VLAN トラフィックを伝送するので、VLAN をネットワーク全体に拡張することができます。

複数の VLAN に接続するトランクポートのトラフィックを正しく配信するために、デバイスは IEEE 802.1Q カプセル化 (タギング方式) を使用します。この方式では、フレームヘッダーに挿入したタグが使用されます。このタグには、そのフレームおよびパケットが属する特定の VLAN に関する情報が含まれます。タグ方式を使用すると、複数の異なる VLAN 用にカプセル化されたパケットが、同じポートを通過しても、各 VLAN のトラフィックを区別することができます。また、カプセル化された VLAN タグにより、トランクは同じ VLAN 上のネットワークの端から端までトラフィックを移動させます。

図 3: 802.1Q タグなしヘッダーと 802.1Q タグ付きヘッダー



3 bits = User Priority field
1 bit = Canonical Format Identifier (CFI)
12 bits = VLAN Identifier (VLAN ID)

182779

ドロップ適性インジケータ

Nexus 9000 スイッチは DEI ビットが 1 に設定されたフレームを受信すると、そのまま次のホップに転送されます。たとえば、ネクストホップが Nexus 6000 の場合、dot1q ヘッダーで DEI ビットが 1 に設定されたパケットを受信すると、フレームがドロップされます。

Cisco Nexus NX-OS リリース 10.2(3)F 以降、DEI ビットが 1 に設定されたフレームを受信されるたびに、DEI ビットがクリアされます。

以下は DEI ビットをリセットするための構成です。

```
switch# conf t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# system default reset-dei
switch(config)
```

以下は DEI ビットを設定するための構成です。

```
switch# conf t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# no system default reset-dei
switch(config)
```

アクセス VLAN

アクセスモードでポートを設定すると、そのインターフェイスのトラフィックを伝送する VLAN を指定できます。アクセスモードのポート（アクセスポート）用に VLAN を設定しないと、そのインターフェイスはデフォルトの VLAN（VLAN1）のトラフィックだけを伝送します。

VLAN のアクセスポートメンバーシップを変更するには、新しい VLAN を指定します。VLAN をアクセスポートのアクセス VLAN として割り当てるには、まず、VLAN を作成する必要があります。アクセスポートのアクセス VLAN をまだ作成していない VLAN に変更すると、アクセスポートがシャットダウンされます。

アクセスポートは、アクセス VLAN 値の他に 802.1Q タグがヘッダーに設定されたパケットを受信すると、送信元の MAC アドレスを学習せずにドロップします。

トランクポートのネイティブ VLAN ID

トランクポートは、タグなしパケットと 802.1Q タグ付きパケットを同時に伝送できます。デフォルトのポート VLAN ID をトランクポートに割り当てると、すべてのタグなしトラフィックが、そのトランクポートのデフォルトのポート VLAN ID で伝送され、タグなしトラフィックはすべてこの VLAN に属するものと見なされます。この VLAN のことを、トランクポートのネイティブ VLAN ID といいます。つまり、トランクポートでタグなしトラフィックを伝送する VLAN がネイティブ VLAN ID となります。



(注) ネイティブ VLAN ID 番号は、トランクの両端で一致していなければなりません。

トランクポートは、デフォルトのポートVLAN IDと同じVLANが設定された出力パケットをタグなしで送信します。他のすべての出力パケットは、トランクポートによってタグ付けされます。ネイティブVLAN IDを設定しないと、トランクポートはデフォルトVLANを使用します。



(注) Fibre Channel over Ethernet (FCoE) VLANをイーサネットトランクスイッチポートのネイティブVLANとして使用できません。

ネイティブVLANトラフィックのタグging

シスコのソフトウェアは、トランクポートでIEEE 802.1Q標準をサポートします。タグなしトラフィックがトランクポートを通過するには、パケットにタグがないVLANを作成する必要があります（またはデフォルトVLANを使用することもできます）。タグなしパケットはトランクポートとアクセスポートを通過できます。

ただし、デバイスを通るすべてのパケットに802.1Qタグがあり、トランクのネイティブVLANの値と一致する場合はタグgingが取り除かれ、タグなしパケットとしてトランクポートから出力されます。トランクポートのネイティブVLANでパケットのタグgingを保持したい場合は、この点が問題になります。

トランクポートのすべてのタグなしパケットをドロップし、ネイティブVLAN IDと同じ802.1Qの値付きでデバイスに届くパケットのタグを保持するようにデバイスを設定できます。この場合も、すべての制御トラフィックはネイティブVLANを通過します。この設定はグローバルです。デバイスのトランクポートは、ネイティブVLANのタグgingを保持する場合と保持しない場合があります。

Allowed VLANs

デフォルトでは、トランクポートはすべてのVLANに対してトラフィックを送受信します。各トランク上では、すべてのVLAN IDが許可されます。この包括的なリストからVLANを削除することによって、特定のVLANからのトラフィックが、そのトランクを通過するのを禁止できます。後ほど、トラフィックを伝送するトランクのVLANを指定してリストに追加し直すこともできます。

デフォルトVLANのスパンニングツリープロトコル (STP) トポロジを区切るには、許容VLANのリストからVLAN1を削除します。この分割を行わないと、VLAN1（デフォルトでは、すべてのポートでイネーブル）が非常に大きなSTPトポロジを形成し、STPのコンバージェンス中に問題が発生する可能性があります。VLAN1を削除すると、そのポート上でVLAN1のデータトラフィックはすべてブロックされますが、制御トラフィックは通過し続けます。



(注) STPの詳細については、『[Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide](#)』を参照してください。



- (注) 内部使用に予約されている VLAN のブロックを変更できます。予約 VLAN 変更の詳細については、『Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide』を参照してください。

トランク インターフェイス上の最大 3967 の VLAN に対応するスイッチポートの分離

トランク インターフェイスは複数のVLANを伝送できます。スイッチポート独立モードで設定されたトランク インターフェイスでは、インターフェイスごとに複数のVLANを設定できます。場合によっては、ポートあたりのVLANの数を増やす必要もあるでしょう。VLAN 単位スパニングツリー (PVST) の論理ポートの規模と、複数スパニングツリー (MST) の仮想ポート数は制限される場合があります。トランク インターフェイスで分離されたスイッチポートを設定することで、Cisco Nexus 9000 ポートフォリオのスイッチ上で、ポートあたり最大 3967 の VLAN を使用して最大 48 のインターフェイスを設定できます。

分離インターフェイスのメンバー VLAN を変更すると、これらのインターフェイスのすべての VLAN が転送状態に移行します。スイッチポート分離機能はホスト インターフェイスでのみサポートされます。これは、これらのポートでスパニングツリーが実行されていないためであり (スイッチが STP BPDU を送信しないため)、他のネットワーク デバイスを接続するとネットワーク内にループが発生する可能性があるためです。スイッチポート分離機能は、物理インターフェイス、ポート チャネル、および vPC でサポートされます。スイッチポート分離機能には、次の制限事項があります。

- Per-VLAN Rapid Spanning Tree (PVRST) および分離 VLAN をサポートします。同じ VLAN で一部のポートを分離モードにし、他のポートでは Rapid Per-VLAN Spanning Tree (RPVST) を実行することができます。
- 同じ VLAN を持つ他のポートで実行される高速スパニングツリープロトコル (RSTP) がサポートされています。
- FEX HIF、FEX ファブリック インターフェイス、別のネットワーク デバイスが接続されているインターフェイスではサポートされません。
- 最大 3967 の VLAN が設定された最大 48 のポートをサポートします
- vPC 環境で使用する場合、設定に一貫性がないと、vPC タイプ 1 の不整合チェックがトリガーされます。
- ポート チャネル メンバーには、同じスイッチポート分離設定が必要です。

デフォルト インターフェイス

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



- (注) 最大8ポートがデフォルトインターフェイスに選択できます。デフォルトのインターフェイス機能は、管理インターフェイスに対しサポートされていません。それはデバイスが到達不能な状態になる可能性があるためです。

スイッチ仮想インターフェイスおよび自動ステート動作

Cisco NX-OS では、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。

このインターフェイスの動作状態は、その対応する VLAN 内のさまざまなポートの状態によって決まります。VLAN の SVI インターフェイスは、その VLAN 内の少なくとも 1 個のポートがスパンニングツリープロトコル (STP) のフォワーディングステートにある場合に稼働します。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。

SVI 自動ステート除外

一般的に、VLAN インターフェイスに複数のポートがある場合、VLAN 内のすべてのポートがダウンすると、SVI はダウン状態になります。SVI 自動ステート除外機能を使用して、SVI が同じ VLAN に属する場合でも、SVI のステータス (アップまたはダウン) を定義すると同時に特定のポートおよびポートチャネルを除外することができます。たとえば、除外されたポートまたはポートチャネルがアップ状態であり、別のポートが VLAN 内でダウン状態である場合でも、SVI 状態はダウンに変更されます。



- (注) SVI 自動ステート除外機能は、スイッチド物理イーサネット ポートおよびポートチャネルに対してのみ使用できます。

SVI 自動ステートのディセーブル化

自動ステートのディセーブル化機能を設定して、対応する VLAN 内にアップ状態のインターフェイスがない場合でも SVI をアップ状態に保持することができます。この機能は、システム (すべての SVI 向け) または個々の SVI に対し設定できます。

高可用性

ハイアベイラビリティ機能の詳細については、『[Cisco Nexus 9000 Series NX-OS High Availability and Redundancy Guide](#)』を参照してください。

カウンタ値

設定、パケットサイズ、増分カウンタ値、およびトラフィックについては、次の情報を参照してください。

設定	パケットサイズ	増分カウンタ	トラフィック
L2 ポート : MTU 設定なし	6400 および 10000	ジャンボ、ジャイアント、および入力エラー	Dropped
L2 ポート : ネットワーク QoS 設定のジャンボ MTU 9216	6400	Jumbo	Forwarded
L2 ポート : ネットワーク QoS 設定のジャンボ MTU 9216	10000	ジャンボ、ジャイアント、および入力エラー	Dropped
network-qos 設定のデフォルト レイヤ 3 MTU およびジャンボ MTU 9216 のレイヤ 3 ポート	6400	Jumbo	パケットは CPU にパントされ (CoP P 設定の対象)、フラグメント化されてから、ソフトウェアによって転送されます。
network-qos 設定のデフォルト レイヤ 3 MTU およびジャンボ MTU 9216 のレイヤ 3 ポート	6400	Jumbo	パケットは CPU にパントされ (CoP P 設定の対象)、フラグメント化されてから、ソフトウェアによって転送されます。
network-qos 設定のデフォルト レイヤ 3 MTU およびジャンボ MTU 9216 のレイヤ 3 ポート	10000	ジャンボ、ジャイアント、および入力エラー	Dropped
network-qos 設定のジャンボ レイヤ 3 MTU およびジャンボ MTU 9216 のレイヤ 3 ポート	6400	Jumbo	フラグメンテーションなしで転送されます。

設定	パケットサイズ	増分カウンタ	トラフィック
network-qos 設定のジャンボ レイヤ 3 MTU およびジャンボ MTU 9216 のレイヤ 3 ポート	10000	ジャンボ、ジャイアント、および入力エラー	Dropped
ジャンボ レイヤ 3 MTU およびデフォルト L2 MTU 設定のレイヤ 3 ポート	6400 および 10000	ジャンボ、ジャイアント、および入力エラー	Dropped



- (注)
- CRC 正常の 64 バイト未満のパケット：ショート フレームカウンタが増加します。
 - CRC 不良の 64 バイト未満のパケット：runts カウンタが増加します。
 - CRC 不良の 64 バイトを超えるパケット：CRC カウンタが増加します。

レイヤ2インターフェイスの前提条件

レイヤ2インターフェイスには次の前提条件があります。

- デフォルトでは、Cisco NX-OS はレイヤ 3 パラメータを設定します。レイヤ 2 パラメータを設定するには、ポートモードをレイヤ 2 に切り替える必要があります。switchport コマンドを使用すれば、ポートモードを変更できます。
- switchport mode コマンドを使用する前に、ポートをレイヤ 2 ポートとして設定する必要があります。デフォルトでは、デバイスのポートはすべてレイヤ 3 ポートです。デフォルトでは、Cisco Nexus 9504 および Cisco Nexus 9508 デバイスのすべてのポートはレイヤ 2 ポートです。

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

VLAN トランキングには次の設定上のガイドラインと制限事項があります。

- Cisco Nexus 9000 シリーズ スイッチには、グローバルに設定できる vlan dot1q tag native コマンドがあります。これにより、設定されたトランク ポートのネイティブ VLAN がタグ付けされます。ただし、Catalyst 6500 やサードパーティ製スイッチなどの接続されたスイッチでは、同様の設定が有効になっていない可能性があります。これにより、予期しない

い動作が発生する可能性があります。したがって、接続されたスイッチで設定されていない場合は、**vlan dot1q tag native** コマンドを無効にすることをお勧めします。

- ネイティブ VLAN を使用した SVI インターフェイスの BFD セッションは、Cisco Nexus 9300-X クラウドスケールスイッチでの **vlan dot1q tag native** コマンド構成ではサポートされていません。
- 自動ネゴシエーションは、N9K-X9636C-R、N9K-X9636C-RX、および N9K-X9636Q-R ラインカードを搭載した Cisco Nexus 9508 プラットフォームスイッチではサポートされません。
- 自動ネゴシエーションは、10/25/40/100直接接続銅ケーブルでのみサポートされます。
- BaseTポートでは自動ネゴシエーションを無効にできません。
- オートネゴシエーションは、光ファイバベースの光ファイバでは使用されません。
- Cisco NX-OS リリース9.2(1)以降では、N9K-X96136YC-R ラインカードを搭載した Cisco Nexus 9508 プラットフォームスイッチは、48ポートすべてで1ギガビットの速度をサポートします。ただし、自動ネゴシエーションはサポートされていないため、ケーブルを取り外しても 1000BASE-T SFP リンクが起動します。
- Cisco NX-OS リリース9.2(1)以降では、ネイティブ 25G ポートでの自動ネゴシエーションが、Cisco Nexus N9K-X97160YC-EX、N9K-C93180YC-FX、N9K-C93240YC-FX2、および N9K-C93240YC-FX2-Zスイッチでサポートされます。



(注) 自動ネゴシエーションは Cisco Nexus N9K-C92300YC スイッチではサポートされていません

- キーワードが付いている **show** コマンドはサポートされていません。 **internal**
- 自動ネゴシエーションは、Cisco Nexus 9200 および 9300-FX プラットフォームスイッチ、および N9K-X9700-EX ラインカードを使用する Cisco Nexus 9500 プラットフォームスイッチ上の 25-G イーサネット トランシーバ モジュールではサポートされません。
- Cisco Nexus 9364C スイッチでは、QSFP-100G-CR4 ケーブルを使用して 100G リンクを起動すると、ポート 49 ～ 64 で自動ネゴシエーションが機能しないことがあります。この問題の回避策は、ポート 49 ～ 64 で速度をハードコーディングし、自動ネゴシエーションを無効にすることです。
- Cisco NX-OS Release 10.1(1) 以降、QSA を使用した自動ネゴシエーション (40 G/100 G) および 1 GB が、次のポートでサポートされます。
 - Cisco Nexus 9336C-FX2 スイッチ：ポート 1 ～ 6 および 33 ～ 36
 - Cisco Nexus 9364C スイッチ
 - Cisco Nexus 93240YC-FX2 スイッチ：ポート 51 ～ 54
 - Cisco Nexus 9788TC ラインカード：ポート 49 ～ 52



(注) これらのポートで銅線ケーブルを使用する場合は、ピア速度を設定する必要があります。

- Cisco Nexus 9300 シリーズ スイッチでは、SVI へのユニキャスト ARP 要求は、VLAN 内の他のポートにフラッディングされます。
- Cisco Nexus 9300 シリーズ スイッチでは、SVI へのユニキャスト ARP 要求は、VLAN 内の他のポートにフラッディングされます。
- 中継スイッチとして動作する ASE2 および ASE3 ベースの Cisco Nexus 9000 シリーズ スイッチは、二重タグ付きパケットの内部タグを保持しません。

次の CLI は、LSE ベースの Cisco Nexus 9000 シリーズ スイッチでのみ必須です。Q-in-Q カプセル化またはカプセル化解除の要件を持たない、SP クラウド内の純粋な中継ボックス上ですべての VLAN タグをシームレスにパケット転送し、保持するには、CLI コマンド、**system dot1q-tunnel transit** を設定します。CLI を削除するには、**no system dot1q-tunnel transit** CLI コマンドを使用します。

スイッチで実行される CLI の注意事項は次のとおりです。

- トランク ポートから出力される L2 フレームは、ポート上のネイティブ VLAN でもタグ付けされます。
- 他のトンネリング メカニズム (VXLAN や MPLS など) は、設定された CLI では機能しません。
- ポートはレイヤ2またはレイヤ3インターフェイスのいずれかです。両方が同時に成立することはありません。
- レイヤ3ポートをレイヤ2ポートに変更する場合またはレイヤ2ポートをレイヤ3ポートに変更する場合は、レイヤに依存するすべての設定は失われます。アクセスまたはトランクポートをレイヤ3ポートに変更すると、アクセス VLAN、ネイティブ VLAN、許容 VLAN などの情報はすべて失われます。
- アクセスリンクを持つデバイスには接続しないでください。アクセスリンクにより VLAN が区分されることがあります。
- 802.1Q トランクを介してシスコ デバイスを接続するときは、802.1Q トランクのネイティブ VLAN がトランク リンクの両端で同じであることを確認してください。トランクの一端のネイティブ VLAN と反対側の端のネイティブ VLAN が異なると、スパニングツリー ループの原因になります。
- ネットワーク上のすべてのネイティブ VLAN についてスパニングツリーをディセーブルにせずに、802.1Q トランクの VLAN 上のスパニングツリーをディセーブルにすると、スパニングツリー ループが発生することがあります。802.1Q トランクのネイティブ VLAN のスパニングツリーはイネーブルのままにしておく必要があります。スパニングツリーをイネーブルにしておけない場合は、ネットワークの各 VLAN のスパニングツリーをディ

セーブルにする必要があります。スパニングツリーをディセーブルにする前に、ネットワークに物理ループがないことを確認してください。

- 802.1Q トランクを介して2台のシスコデバイスを接続すると、トランク上で許容される VLAN ごとにスパニングツリーブリッジプロトコルデータユニット (BPDU) が交換されます。トランクのネイティブ VLAN 上の BPDU は、タグなしの状態です。予約済み IEEE 802.1D スパニングツリーマルチキャスト MAC アドレス (01-80-C2-00-00-00) に送信されます。トランクの他のすべての VLAN 上の BPDU は、タグ付きの状態です。予約済み Cisco Shared Spanning Tree (SSTP) マルチキャスト MAC アドレス (01-00-0c-cc-cc-cd) に送信されます。
- 他社製の 802.1Q デバイスでは、すべての VLAN に対してスパニングツリー トポロジを定義するスパニングツリーのインスタンス (Mono Spanning Tree) が1つしか維持されません。802.1Q トランクを介してシスコ製スイッチを他社製のスイッチに接続すると、他社製のスイッチの Mono Spanning Tree とシスコ製スイッチのネイティブ VLAN スパニングツリーが組み合わされて、Common Spanning Tree (CST) と呼ばれる単一のスパニングツリー トポロジが形成されます。
- シスコ デバイスは、トランクのネイティブ VLAN 以外の VLAN にある SSTP マルチキャスト MAC アドレスに BPDU を伝送します。したがって、他社製のデバイスではこれらのフレームが BPDU として認識されず、対応する VLAN のすべてのポート上でフラッディングされます。他社製の 802.1Q クラウドに接続された他のシスコ デバイスは、フラッディングされたこれらの BPDU を受信します。BPDU を受信すると、Cisco スイッチは、他社製の 802.1Q デバイス クラウドにわたって、VLAN 別のスパニングツリー トポロジを維持できます。シスコ デバイスを隔てている他社製の 802.1Q クラウドは、802.1Q トランクを介して他社製の 802.1Q クラウドに接続されたすべてのデバイス間の単一のブロードキャストセグメントとして処理されます。
- シスコ デバイスを他社製の 802.1Q クラウドに接続するすべての 802.1Q トランク上で、ネイティブ VLAN が同じであることを確認します。
- 他社製の特定の 802.1Q クラウドに複数のシスコ デバイスを接続する場合は、すべての接続に 802.1Q トランクを使用する必要があります。シスコ デバイスを他社製の 802.1Q クラウドにアクセスポート経由で接続することはできません。この場合、シスコ製のアクセスポートはスパニングツリー「ポート不一致」状態になり、トラフィックはポートを通過しません。
- トランク ポートをポートチャネルグループに含めることができますが、そのグループのトランクはすべて同じ設定にする必要があります。グループを初めて作成したときには、そのグループに最初に追加されたポートのパラメータ設定値をすべてのポートが引き継ぎます。パラメータの設定を変更すると、許容 VLAN やトランク ステータスなど、デバイスのグループのすべてのポートにその設定を伝えます。たとえば、ポートグループのあるポートがトランクになるのを中止すると、すべてのポートがトランクになるのを中止します。
- トランク ポートで 802.1X をイネーブルにしようとする、エラーメッセージが表示され、802.1X はイネーブルになりません。802.1x 対応ポートのモードをトランクに変更しようとしても、ポートモードは変更されません。

- 入力ユニキャストパケットカウンタだけが SVI カウンタでサポートされます。
- `clear mac address-table dynamic` コマンドを使用して VLAN の MAC アドレスをクリアすると、その VLAN のダイナミック ARP (Address Resolution Protocol) エントリが更新されます。
- VLAN 上にスタティック ARP エントリが存在し、MAC アドレスからポートへのマッピングが存在しない場合、スーパーバイザは ARP 要求を生成して MAC アドレスを学習できます。MAC アドレスを学習すると、隣接エントリは正しい物理ポートをポイントします。
- Cisco NX-OS は、SVI の 1 つが BIA MAC (バーインドイン MAC アドレス) を使用して Cisco Nexus 9000 上にある場合、2 つの VLAN 間のトランスペアレントブリッジングをサポートしません。これは、BIA MAC が SVI / VLAN 間で共有される場合に発生します。BIA MAC とは異なる MAC を、トランスペアレントブリッジングが正しく動作するように SVI で設定できます。



(注) この動作は、Cisco Nexus 9300 スイッチ (ネットワーク転送エンジン) および 95xx、96xx、94xx ラインカードを搭載した Cisco Nexus 9500 スイッチに適用されます。この動作は、Cisco Nexus 9200 スイッチ、Cisco Nexus 9300-EX および 9700-EX ラインカードを搭載した Cisco Nexus 9500 スイッチには適用されません。

- ポートローカル VLAN は、ファブリックエクステンダ (FEX) をサポートしていません。
- Cisco Nexus 9364C スイッチでは、QSFP-100G-CR4 ケーブルを使用して 100G リンクを起動すると、ポート 49 ~ 64 で自動ネゴシエーションが機能しないことがあります。この問題を回避するには、ポート 49 ~ 64 の速度をハードコードし、自動ネゴシエーションを無効にする必要があります。
- インターフェイスモードをトランク VLAN とトランク VLAN に同時に設定しようとすると、エラーメッセージが表示されることがあります。Cisco NX-OS インターフェイスでは、インターフェイスモードのデフォルト値は `access` です。トランク関連の設定を実装するには、最初にインターフェイスモードを `trunk` に変更してから、トランク VLAN 範囲を設定する必要があります。
- vPC セットアップでは、VLAN が vPC VLAN の場合、VLAN およびシステムの MAC アドレス制限はサポートされません。
- インターフェイス、VLAN、システムで MAC アドレス テーブル制限が有効になっている場合は、既存のすべての MAC がフラッシュされ、再学習される可能性があります。
- vPC PO で有効になっている MAC アドレス テーブル制限は、両方のピアで一貫している必要があります。
- システム、ポート、および VLAN の MAC アドレス テーブル制限を一度に、または任意の組み合わせで設定すると、それぞれが設定されたとおりに MAC を制限します。プリファレンスは常に次の順序になります。
 - ポート

- VLAN
 - システム
-
- MAC アドレス テーブルの制限は、vPC ピア リンクではサポートされていません。
 - 設定可能な MAC アドレステーブルの最小値は 100 で、設定可能な最大値は 196000 です。
 - インターフェイスまたは VLAN がセットアップから削除されると、関連する MAC アドレス テーブル制限の設定も削除されます。
 - MAC アドレス テーブルの制限は、PVLAN インターフェイス タイプではサポートされません。
 - MAC アドレス テーブルの制限を超えると、デフォルトでトラフィックがフラッディングされます。
 - Cisco Nexus N9K-C93180YC-FX3S スイッチまたは N9K-X9716D-GX ライン カードを搭載した Cisco Nexus 9500 スイッチのポートに FET-10G ファブリックエクステンダ トランシーバを接続すると、**switchport mode fex-fabric** コマンドを使用しても、ポートはファブリック ポートに変換されません。
 - Cisco NX-OS リリース 10.1(2) 以降、レイヤ 2 インターフェイスは、Cisco Nexus N9K-X9624D-R2 ライン カードでサポートされます。
 - Cisco Nexus リリース 9.3(X) の場合、Cisco Nexus N9K-C93600CD-GX、N9K-C9364C-GX スイッチには次のガイドラインと制約事項があります。
 - Cisco Nexus NX-OS Release 10.1(2) 以降では、NX-OS N9K-C93600CD-GX、N9K-C9316D-GX、および N9K-C9364C-GX の速度 40G および 100G で自動ネゴシエーションがサポートされています。
 - Cisco Nexus 9300-GX プラットフォーム スイッチは、50Gx2 ブレークアウト ポートの 2 番目のレーンで FC-FEC をサポートしません。50Gx2 ブレークアウトが設定されている場合、2 番目のブレークアウト ポートはリンクアップしません。回避策：50Gx2 ブレークアウトで RS-FEC を設定します。
 - N9K-C9316D-GX の場合：ポート 1 ～ 16 は QSA で 400G/100G/40G および 10G をサポートします。
 - N9K-C93600CD-GX の場合：ポート 1 ～ 24 の場合、4 個のポート（1-4、5-8、9-12 など「クワッド」と呼ばれます）はすべて、同じ速度で動作します。クワッド内のすべてのポートは、10G、または 40G または 100G で動作します。同じクワッド内では混合速度はサポートされません。QSAでは、クワッド内のすべてのポートが 10G の速度で動作できます。ポート 25 ～ 26 は同じ速度で動作し、ポート 27 ～ 28 は同じ速度で動作します。ポート 25 ～ 26 または 27 ～ 28 の速度の不一致はサポートされていません。

N9K-C9364C-GXのガイドラインと制約は次のとおりです。

- ポート 1 ～ 64 の場合、4 個のポート（1-4、5-8、9-12 など「クアッド」と呼ばれます）はすべて、同じ速度で動作します。クワッド内のすべてのポートは、10G、または 40G または 100G で動作します。
- 同じクワッド内では混合速度はサポートされません。
- QSAでは、クワッド内のすべてのポートが 10G の速度で動作できます。
- Cisco NX-OS リリース 10.4(1)F 以降、L2 転送は Cisco Nexus 9332D-H2R プラットフォームスイッチでサポートされます。
- Cisco NX-OS リリース 10.4(2)F 以降、L2 転送は Cisco Nexus 93400LD-H1 プラットフォームスイッチでサポートされます。
- Cisco NX-OS リリース 10.4(1)F 以降、L2 インフラは Cisco Nexus 9332D-H2R プラットフォームスイッチでサポートされます。
- Cisco NX-OS リリース 10.4(2)F 以降、L2 インフラは Cisco Nexus 93400LD-H1 プラットフォームスイッチでサポートされます。



(注) Cisco NX-OS リリース 10.2(2)F では、N9K-C93180YC-FX3S、N9K-C93180YC-FX3 スイッチの SFP-10G-TX モジュールのリンク アップ時間は 13 秒です。

レイヤ2インターフェイスのデフォルト設定

次の表に、デバイスのアクセスおよびトランク ポート モード パラメータのデフォルト設定を示します。

表 9: デフォルトのアクセスおよびトランク ポート モード パラメータ

パラメータ	デフォルト
スイッチポート モード	アクセス
Allowed VLANs	1 ～ 3967、4048 ～ 4094
アクセス VLAN ID	VLAN1
Native VLAN ID	VLAN1
ネイティブ VLAN ID タギング	ディセーブル
管理状態	閉じる
SVI 自動ステート	有効 (Enabled)

アクセスインターフェイスとトランクインターフェイスの設定



(注) Cisco IOS の CLI に慣れている場合、この機能に対応する Cisco NX-OS コマンドは通常使用する Cisco IOS コマンドと異なる場合がありますので注意してください。

アクセスおよびトランク インターフェイスの設定に関する注意事項

トランクのすべての VLAN は同じ VDC である必要があります。

レイヤ2 アクセスポートとしての VLAN インターフェイスの設定

レイヤ2ポートをアクセスポートとして設定できます。アクセスポートは、パケットを、1つのタグなし VLAN 上だけで送信します。インターフェイスが伝送する VLAN トラフィックを指定します。これがアクセス VLAN になります。アクセスポートの VLAN を指定しない場合、そのインターフェイスはデフォルト VLAN のトラフィックだけを伝送します。デフォルトの VLAN は VLAN 1 です。

VLAN をアクセス VLAN として指定するには、その VLAN が存在しなければなりません。システムは、存在しないアクセス VLAN に割り当てられたアクセスポートをシャットダウンします。

始める前に

レイヤ2 インターフェイスを設定することを確認します。

手順の概要

1. **configure terminal**
2. **interface ethernet** *{{type slot/port} | {port-channel number}}*
3. **switchport mode** [access | trunk]
4. **switchport access vlan** *vlan-id*
5. **exit**
6. **show interface**
7. **no shutdown**
8. **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	configure terminal 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ2	interface ethernet <i>{{type slot/port}}</i> port-channel number}} 例： switch(config)# interface ethernet 3/1 switch(config-if)#	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	switchport mode [access trunk] 例： switch(config-if)# switchport mode access	インターフェイスを、非トランキング、タグなし、シングルVLANレイヤ2インターフェイスとして設定します。アクセスポートは、1つのVLANのトラフィックだけを伝送できます。デフォルトでは、アクセスポートはVLAN1のトラフィックを伝送します。異なるVLANのトラフィックを伝送するようにアクセスポートを設定するには、 switchport access vlan を使用します コマンドを使用します。
ステップ4	switchport access vlan <i>vlan-id</i> 例： switch(config-if)# switchport access vlan 5	このアクセスポートでトラフィックを伝送するVLANを指定します。このコマンドを入力しないと、アクセスポートはVLAN1だけのトラフィックを伝送します。このコマンドを使用して、アクセスポートがトラフィックを伝送するVLANを変更できます。
ステップ5	exit 例： switch(config-if)# exit switch(config)#	インターフェイス コンフィギュレーション モードを終了します。
ステップ6	show interface 例： switch# show interface	(任意) インターフェイスのステータスと内容を表示します。
ステップ7	no shutdown 例： switch# configure terminal switch(config)# int e3/1 switch(config-if)# no shutdown	(任意) ポリシーがハードウェアポリシーと一致するインターフェイスおよびVLANのエラーをクリアします。このコマンドにより、ポリシープログラミングが続き、ポートがアップできます。ポリシーが対応していない場合は、エラーはerror-disabledポリシー状態になります。

	コマンドまたはアクション	目的
ステップ 8	copy running-config startup-config 例 : <pre>switch(config)# copy running-config startup-config</pre>	(任意) 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

例

次に、イーサネット 3/1 をレイヤ2アクセスポートとして設定し、VLAN5のトラフィックだけを伝送する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 3/1
switch(config-if)# switchport mode access
switch(config-if)# switchport access vlan 5
switch(config-if)#
```

アクセス ホスト ポートの設定



(注) `switchport host` コマンドは、端末に接続するインターフェイスだけに使用します。

端末に接続されたアクセスポートでのパフォーマンスを最適化するには、そのポートをホストポートとしても設定します。アクセスホストポートはエッジポートと同様にSTPを処理し、ブロッキングステートおよびラーニングステートを通過することなくただちにフォワーディングステートに移行します。インターフェイスをアクセスホストポートとして設定すると、そのインターフェイス上でポートチャネル動作がディセーブルになります。



(注) ポートチャネルインターフェイスについては、「ポートチャネルの設定」の項および『[Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide](#)』を参照してください。

始める前に

エンドステーションのインターフェイスに接続された適切なインターフェイスを設定することを確認してください。

手順の概要

1. `configure terminal`
2. `interface ethernet type slot/port`
3. `switchport host`
4. `exit`
5. `show interface`

6. no shutdown
7. 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	configure terminal 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface ethernet type slot/port 例： switch(config)# interface ethernet 3/1 switch(config-if)#	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	switchport host 例： switch(config-if)# switchport host	インターフェイスをアクセス ホスト ポートとして設定します。このポートはただちに、スパンニング リーフォワーディング ステートに移行し、このインターフェイスのポートチャネル動作をディセーブルにします。 (注) このコマンドは端末だけに適用します。
ステップ 4	exit 例： switch(config-if-range)# exit switch(config)#	インターフェイス モードを終了します。
ステップ 5	show interface 例： switch# show interface	(任意) インターフェイスのステータスと内容を表示します。
ステップ 6	no shutdown 例： switch# configure terminal switch(config)# int e3/1 switch(config-if)# no shutdown	(任意) ポリシーがハードウェアポリシーと一致するインターフェイスおよびVLANのエラーをクリアします。このコマンドにより、ポリシープログラミングが続き、ポートがアップできます。ポリシーが対応していない場合は、エラーはerror-disabledポリシー状態になります。
ステップ 7	copy running-config startup-config 例： switch(config)# copy running-config startup-config	(任意) 実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

例

次に、イーサネット3/1をレイヤ2アクセスポートとして設定し、PortFastをイネーブルにしてポートチャンネルをディセーブルにする例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 3/1
switch(config-if)# switchport host
switch(config-if)#
```

トランクポートの設定

レイヤ2ポートをトランクポートとして設定できます。トランクポートは、1つのVLANの非タグ付きパケットと、複数のVLANのカプセル化されたタグ付きパケットを伝送します（カプセル化については、「IEEE 802.1Q カプセル化」の項を参照）。



(注) デバイスは 802.1Q カプセル化だけをサポートします。

始める前に

トランクポートを設定する前に、レイヤ2インターフェイスを設定することを確認します。

手順の概要

1. **configure terminal**
2. **interface** {type slot/port | port-channel number}
3. **switchport mode** [access | trunk]
4. **exit**
5. **show interface**
6. **no shutdown**
7. **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	configure terminal 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface {type slot/port port-channel number} 例： switch(config)# interface ethernet 3/1 switch(config-if)#	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。

	コマンドまたはアクション	目的
ステップ 3	switchport mode [access trunk] 例： switch(config-if)# switchport mode trunk	インターフェイスをレイヤ2 トランク ポートとして設定します。トランク ポートは、同じ物理リンクで1つ以上の VLAN 内のトラフィックを伝送できます（各 VLAN はトランキングが許可された VLAN リストに基づいています）。デフォルトでは、トランク インターフェイスはすべての VLAN のトラフィックを伝送できます。指定したトランクで特定の VLAN のみが許可されるように指定するには、 switchport trunk allowed vlan コマンドを使用します。
ステップ 4	exit 例： switch(config-if)# exit switch(config)#	インターフェイス モードを終了します。
ステップ 5	show interface 例： switch# show interface	(任意) インターフェイスのステータスと内容を表示します。
ステップ 6	no shutdown 例： switch# configure terminal switch(config)# int e3/1 switch(config-if)# no shutdown	(任意) ポリシーがハードウェアポリシーと一致するインターフェイスおよび VLAN のエラーをクリアします。このコマンドにより、ポリシープログラミングが続き、ポートがアップできます。ポリシーが対応していない場合は、エラーは error-disabled ポリシー状態になります。
ステップ 7	copy running-config startup-config 例： switch(config)# copy running-config startup-config	(任意) 実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

例

次に、イーサネット 3/1 をレイヤ2 トランク ポートとして設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 3/1
switch(config-if)# switchport mode trunk
switch(config-if)#
```

802.1Q トランク ポートのネイティブ VLAN の設定

ネイティブ VLAN を 802.1Q トランク ポートに設定できます。このパラメータを設定しないと、トランク ポートは、デフォルト VLAN をネイティブ VLAN ID として使用します。



(注) イーサネット インターフェイスのネイティブ VLAN として FCoE VLAN を設定できません。

手順の概要

1. **configure terminal**
2. **interface** *{{type slot/port} | {port-channel number}}*
3. **switchport trunk native vlan** *vlan-id*
4. **exit**
5. **show vlan**
6. **no shutdown**
7. **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	configure terminal 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface <i>{{type slot/port} {port-channel number}}</i> 例： switch(config)# interface ethernet 3/1 switch(config-if)#	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	switchport trunk native vlan <i>vlan-id</i> 例： switch(config-if)# switchport trunk native vlan 5	802.1Q トランクのネイティブ VLAN を設定します。指定できる範囲は 1 ~ 4094 です (ただし、内部使用に予約されている VLAN は除きます)。デフォルト値は VLAN 1 です。
ステップ 4	exit 例： switch(config-if-range)# exit switch(config)#	インターフェイス コンフィギュレーション モードを終了します。
ステップ 5	show vlan 例： switch# show vlan	(任意) VLAN のステータスと内容を表示します。
ステップ 6	no shutdown 例： switch# configure terminal switch(config)# int e3/1 switch(config-if)# no shutdown	(任意) ポリシーがハードウェアポリシーと一致するインターフェイスおよびVLANのエラーをクリアします。このコマンドにより、ポリシープログラミングが続行でき、ポートがアップできます。ポリ

	コマンドまたはアクション	目的
		シーが対応していない場合は、エラーは error-disabled ポリシー状態になります。
ステップ 7	copy running-config startup-config 例： <pre>switch(config)# copy running-config startup-config</pre>	(任意) 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

例

次に、ネイティブ VLAN をイーサネット 3/1 に設定し、レイヤ 2 トランク ポートを VLAN5 に設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 3/1
switch(config-if)# switchport trunk native vlan 5
switch(config-if)#
```

トランキングポートの許可 VLAN の設定

特定のトランク ポートで許可されている VLAN の ID を指定できます。



- (注) **switchport trunk allowed vlan *vlan-list*** コマンドは、指定されたポートの現在の VLAN リストを新しいリストに置き換えます。新しいリストが適用される前に確認を求められます。

大規模な設定のコピーアンドペーストをしている場合は、CLI が他のコマンドを受け入れる前に確認のため待機しているため障害が発生する場合があります。この問題を回避するため、**terminal dont-ask** を使用してプロンプトを無効にできます。コマンドを入力してから、設定を貼り付けます。

始める前に

指定トランク ポートの許可 VLAN を設定する前に、正しいインターフェイスを設定していること、およびそのインターフェイスがトランクであることを確認してください。



- (注) 内部使用に予約されている VLAN のブロックを変更できます。予約 VLAN 変更の詳細については、『[Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide](#)』を参照してください。

手順の概要

1. configure terminal

2. **interface** {*ethernet slot/port* | **port-channel number**}
3. **switchport trunk allowed vlan** {*vlan-list add vlan-list* | **all** | **except** *vlan-list* | **none** | **remove** *vlan-list*}
4. **exit**
5. **show vlan**
6. **no shutdown**
7. **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	configure terminal 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface { <i>ethernet slot/port</i> port-channel number }	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	switchport trunk allowed vlan { <i>vlan-list add vlan-list</i> all except <i>vlan-list</i> none remove <i>vlan-list</i> }	<p>トランク インターフェイスの許可 VLAN を設定します。デフォルトでは、トランク インターフェイス上のすべての VLAN (1 ~ 3967 および 4048 ~ 4094) が許可されます。VLAN 3968 ~ 4047 は、内部で使用するデフォルトで予約されている VLAN です。デフォルトでは、すべてのトランク インターフェイスですべての VLAN が許可されます。</p> <p>デフォルトの予約済み VLAN は 3968 ~ 4094 で、予約 VLAN のブロックを変更できます。詳細については、『Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide』を参照してください。</p> <p>(注) 内部で割り当て済みの VLAN を、トランク ポート上の許可 VLAN として追加することはできません。内部で割り当て済みの VLAN を、トランク ポートの許可 VLAN として登録しようとする、メッセージが返されます。</p>
ステップ 4	exit 例： switch(config-if)# exit switch(config)#	インターフェイス モードを終了します。
ステップ 5	show vlan 例：	(任意) VLAN のステータスと内容を表示します。

	コマンドまたはアクション	目的
	switch# show vlan	
ステップ 6	no shutdown 例 : <pre>switch# configure terminal switch(config)# int e3/1 switch(config-if)# no shutdown</pre>	(任意) ポリシーがハードウェアポリシーと一致するインターフェイスおよびVLANのエラーをクリアします。このコマンドにより、ポリシープログラミングが続き、ポートがアップできます。ポリシーが対応していない場合は、エラーはerror-disabledポリシー状態になります。
ステップ 7	copy running-config startup-config 例 : <pre>switch(config)# copy running-config startup-config</pre>	(任意) 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

例

次に、VLAN 15 ~ 20 をイーサネット 3/1、レイヤ 2 トランク ポートの許容 VLAN リストに追加する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 3/1
switch(config-if)# switchport trunk allowed vlan 15-20
switch(config-if)#
```

ポートでの MAC アドレス制限の設定

Cisco NX-OS リリース 9.2(3)以降、N9K-X9636C-RX、N3K-C3636C-R、およびN3K-C36180YC-R ラインカードを搭載した Cisco Nexus 9500 シリーズスイッチでは、各ポートが学習する MAC アドレス数の上限を設定できます。たとえば、指定された VLAN での制限が 2000 の MAC である場合、レイヤ 2 フォワーディング マネージャ (L2FM) は、受信した最初の 2000 の MAC を受け入れ、残りの MAC を拒否します。インターフェイスの MAC アドレスの制限を設定するには、次の手順を実行します。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **mac address-table limit interface port-channel value**
3. switch(config)# **show mac address-table limit interf**
4. switch(config)# **exit**

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# configure terminal	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	switch(config)# mac address-table limit interface port-channel value	ポート レベルで MAC 学習の上限を指定します。
ステップ 3	switch(config)# show mac address-table limit interf	MAC 制限が設定されているインターフェイスのリストを表示します。
ステップ 4	switch(config)# exit	コンフィグレーション モードを終了します。

例

次に、ポートレベルでの MAC 学習の上限を設定する例を示します。

```
switch# configure terminal
switch(config)# mac address-table limit interface port-channel 2 1000
Configuring Mac address limit will result in flushing existing Macs in the specified
VLAN/System.Proceed(yes/no)? [no] yes
switch(config)# exit
```

次に、MAC アドレスの制限を表示する例を示します。

```
switch# configure terminal
switch(config)# show mac address-table limit interf
Interface      Conf Limit      Curr Count      Cfg Action      Currently
-----
Vlan1          196000          0               Flood           Flooding Unknown SA
Vlan341        196000          0               Flood           Flooding Unknown SA
Vlan342        196000          0               Flood           Flooding Unknown SA
Vlan343        196000          0               Flood           Flooding Unknown SA
Vlan344        196000          0               Flood           Flooding Unknown SA
Vlan345        196000          0               Flood           Flooding Unknown SA
Vlan346        196000          0               Flood           Flooding Unknown SA
Vlan347        196000          0               Flood           Flooding Unknown SA
Vlan348        196000          0               Flood           Flooding Unknown SA
Vlan349        196000          0               Flood           Flooding Unknown SA
Vlan350        196000          0               Flood           Flooding Unknown SA
port-channel1  196000          0               Flood           Flooding Unknown SA
port-channel2  1000            0               Flood           Flooding Unknown SA
port-channel11 196000          0               Flood           Flooding Unknown SA
port-channel12 196000          0               Flood           Flooding Unknown SA
port-channel13 196000          0               Flood           Flooding Unknown SA
port-channel601 196000          0               Flood           Flooding Unknown SA
port-channel603 196000          0               Flood           Flooding Unknown SA
port-channel888 196000          0               Flood           Flooding Unknown SA
Ethernet1/6    196000          0               Flood           Flooding Unknown SA
Ethernet1/15   196000          0               Flood           Flooding Unknown SA
Ethernet1/35   196000          0               Flood           Flooding Unknown SA
BF2(config)#
switch(config)# exit
```

スイッチポート分離の設定

インターフェイス上で最大 3967 の VLAN に対応するように、インターフェイス上でスイッチポート分離を設定できます。分離されたスイッチポートで設定されたインターフェイスは、STP BPDU を送信しません。



- (注) **スイッチポート独立モード**は、FEX、スイッチ、ルータ、またはその他のネットワークデバイスに接続されたインターフェイスではサポートされません。スイッチポート分離は、FEX HIF ポートではサポートされていません。

手順の概要

1. **configure terminal**
2. **interface** {{ethernet slot/port}} | {{port-channel number}}
3. **switchport isolated**
4. **show running-config interface port-channel 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	configure terminal 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface {{ethernet slot/port}} {{port-channel number}} 例： switch(config)# interface ethernet 3/1 switch(config-if)#	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	switchport isolated 例： switch(config-if)# switchport isolated	スイッチポート分離機能を有効にします。
ステップ 4	show running-config interface port-channel port-channel-number	(任意) インターフェイスのステータスと内容を表示します。

デフォルト インターフェイスの設定

デフォルトインターフェイス機能によって、イーサネット、ループバック、VLAN ネットワーク、ポートチャネル、およびトンネルインターフェイスなどの複数インターフェイスの既存コンフィギュレーションを消去できます。特定のインターフェイスでのすべてのユーザコンフィギュレーションは削除されます。後で削除したコンフィギュレーションを復元できるように、

任意でチェックポイントを作成してからインターフェイスのコンフィギュレーションを消去できます。



(注) デフォルトのインターフェイス機能は、管理インターフェイスに対しサポートされていません。それはデバイスが到達不能な状態になる可能性があるためです。

速度グループが設定されている場合、**default interface** コマンドは次のエラーを表示します。

```
Error: default interface is not supported as speed-group is configured
```

手順の概要

1. **configure terminal**
2. **default interface** *int-if* [**checkpoint name**]
3. **exit**
4. **show interface**
5. **no shutdown**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： <pre>switch# configure terminal switch(config)#</pre>	グローバル 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	default interface <i>int-if</i> [checkpoint name] 例： <pre>switch(config)# default interface ethernet 3/1 checkpoint test8</pre>	インターフェイスの設定を削除しデフォルトの設定を復元します。 ? キーワードを使用して、サポートされるインターフェイスを表示します。 checkpoint コマンドを使用し、キーワードを使用して、設定を消し去ってしまう前にインターフェイスの実行コンフィギュレーションを保存します。
ステップ 3	exit 例： <pre>switch(config)# exit switch(config)#</pre>	グローバル コンフィギュレーション モードを終了します。
ステップ 4	show interface 例： <pre>switch# show interface</pre>	(任意) インターフェイスのステータスと内容を表示します。
ステップ 5	no shutdown 例：	(任意) ポリシーがハードウェアポリシーと一致するインターフェイスおよびVLANのエラーをクリアします。このコマンドにより、ポリシープログラミ

	コマンドまたはアクション	目的
	<pre>switch# configure terminal switch(config)# int e3/1 switch(config-if)# no shutdown</pre>	シーが実行でき、ポートがアップできます。ポリシーが対応していない場合は、エラーはerror-disabledポリシー状態になります。

例

次に、ロールバック目的で実行コンフィギュレーションのチェックポイントを保存する際にイーサネットインターフェイスの設定を削除する例を示します。

```
switch# configure terminal
switch(config)# default interface ethernet 3/1 checkpoint test8
.....Done
switch(config)#
```

SVI 自動ステート除外の設定

イーサネットインターフェイスまたはポートチャネルに SVI 自動ステート除外機能を設定できます。自動ステート除外オプションを使用して、ポートが SVI 計算を稼働または停止したり、それを選択したポートでイネーブルのすべての VLAN に適用するのをイネーブルまたはディセーブルにすることができます。また、SVI 自動ステート除外 VLAN 機能を使用して、VLAN を自動ステート除外インターフェイスから除外することができます。

手順の概要

1. **configure terminal**
2. **interface** *{{type slot/port} | {port-channel number}}*
3. **switchport**
4. **[no] switchport autostate exclude**
5. **[no] switchport autostate exclude vlan** *{vlan id | all | except}*
6. **exit**
7. **show running-config interface** *{{type slot/port} | {port-channel number}}*
8. **no shutdown**
9. **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	configure terminal 例： <pre>switch# configure terminal switch(config)#</pre>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface <i>{{type slot/port} {port-channel number}}</i> 例：	設定するインターフェイスを指定し、インターフェイスコンフィギュレーションモードを開始します。

	コマンドまたはアクション	目的
	switch(config)# interface ethernet 3/1 switch(config-if)#	
ステップ 3	switchport 例： switch(config-if)# switchport	インターフェイスをレイヤ2インターフェイスとして設定します。
ステップ 4	[no] switchport autostate exclude 例： switch(config-if)# switchport autostate exclude	VLAN に複数のポートがあるときに、VLAN インターフェイスのリンクアップ計算からポートを除外します。 デフォルト設定に戻すには、このコマンドの no 形式を使用します。
ステップ 5	[no] switchport autostate exclude vlan {vlan id all except} 例： switch(config-if)# switchport autostate exclude vlan 10	(任意) 自動ステート除外インターフェイスから vlan または vlan のセットを除外します。これにより、システムの中断を最小限に抑えることができます。 デフォルト設定に戻すには、このコマンドの no 形式を使用します。
ステップ 6	exit 例： switch(config-if)# exit switch(config)#	インターフェイス コンフィギュレーション モードを終了します。
ステップ 7	show running-config interface {{type slot/port} {port-channel number}} 例： switch(config)# show running-config interface ethernet 3/1	(任意) 指定されたインターフェイスに関する設定情報を表示します。
ステップ 8	no shutdown 例： switch# configure terminal switch(config)# int e3/1 switch(config-if)# no shutdown	(任意) ポリシーがハードウェアポリシーと一致するインターフェイスおよびVLANのエラーをクリアします。このコマンドにより、ポリシープログラミングが続行でき、ポートがアップできます。ポリシーが対応していない場合は、エラーはerror-disabledポリシー状態になります。
ステップ 9	copy running-config startup-config 例： switch(config)# copy running-config startup-config	(任意) 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

例

次に、Cisco NX-OS デバイスで VLAN インターフェイスのリンクアップ計算からポートを除外する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 3/1
switch(config-if)# switchport
switch(config-if)# switchport autostate exclude
```

次に、自動除外インターフェイスから VLAN を除外する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 3/1
switch(config-if)# switchport
switch(config-if)# switchport autostate exclude
switch(config-if)# switchport autostate exclude vlan 10
```

システムの SVI 自動ステートのディセーブル化の設定

SVI 自動ステート機能によって SVI を管理できます。SVI 自動ステートのディセーブル化機能を設定して、対応する VLAN 内にアップ状態のインターフェイスがない場合でも SVI をアップ状態に保持することができます。（同様に、SVI 自動ステートのイネーブル化機能を設定すると、対応する VLAN 内にアップ状態のインターフェイスがない場合に SVI がダウン状態になります）。システム全体にこの機能を設定するには、次の手順を使用します。



- (注) この項で説明している **system default interface-vlan autostate** コマンドが SVI 自動ステート機能をイネーブルにします。

手順の概要

1. **configure terminal**
2. **[no] system default interface-vlan autostate**
3. **no shutdown**
4. **show running-config [all]**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： switch# configure terminal switch(config)#	グローバル設定モードを開始します。
ステップ 2	[no] system default interface-vlan autostate 例：	デバイスに対するデフォルトの自動ステート動作をディセーブルにします。

	コマンドまたはアクション	目的
	<code>switch(config)# no system default interface-vlan autostate</code>	(注) system default interface-vlan autostate コマンドを使用し、コマンドを使用しません。
ステップ 3	no shutdown 例 : <pre>switch# configure terminal switch(config)# int e3/1 switch(config-if)# no shutdown</pre>	(任意) ポリシーがハードウェアポリシーと一致するインターフェイスおよびVLANのエラーをクリアします。このコマンドにより、ポリシープログラミングが続き、ポートがアップできます。ポリシーが対応していない場合は、エラーはerror-disabledポリシー状態になります。
ステップ 4	show running-config [all] 例 : <pre>switch(config)# show running-config</pre>	(任意) 実行コンフィギュレーションを表示します。 デフォルト情報および設定情報を表示するには、 all キーワードを使用します。

例

次に、Cisco NX-OS デバイス上でデフォルトの自動ステート動作をディセーブルにする例を示します。

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

SVI 単位の SVI 自動ステートのディセーブル化の設定

個々の SVI 上で SVI 自動ステートのイネーブル化またはディセーブル化を設定できます。SVI レベルの設定は、その特定の SVI に対するシステムレベルの SVI 自動ステート設定より優先されます。

手順の概要

1. **configure terminal**
2. **feature interface-vlan**
3. **interface vlan *vlan-id***
4. **[no] autostate**
5. **exit**
6. **show running-config interface vlan *vlan-id***
7. **no shutdown**
8. **show startup-config interface vlan *vlan-id***

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	feature interface-vlan 例： switch(config)# feature interface-vlan	VLAN インターフェイス モードをイネーブルにします。
ステップ 3	interface vlan vlan-id 例： switch(config-if)# interface vlan10 switch(config)#	VLAN インターフェイスを作成し、インターフェイス コンフィギュレーション モードを開始します。範囲は、1 ~ 4094 です。
ステップ 4	[no] autostate 例： switch(config-if)# no autostate	デフォルトでは、指定されたインターフェイスの SVI 自動ステート機能をイネーブルにします。 デフォルト設定をディセーブルにするには、このコマンドの no 形式を使用します。
ステップ 5	exit 例： switch(config-if)# exit switch(config)#	インターフェイス コンフィギュレーション モードを終了します。
ステップ 6	show running-config interface vlan vlan-id 例： switch(config)# show running-config interface vlan10	(任意) 特定の VLAN インターフェイスの実行コンフィギュレーションを表示します。
ステップ 7	no shutdown 例： switch# configure terminal switch(config)# int e3/1 switch(config-if)# no shutdown	(任意) ポリシーがハードウェアポリシーと一致するインターフェイスおよび VLAN のエラーをクリアします。このコマンドにより、ポリシープログラミングが続き、ポートがアップできます。ポリシーが対応していない場合は、エラーは error-disabled ポリシー状態になります。
ステップ 8	show startup-config interface vlan vlan-id 例： switch(config)# show startup-config interface vlan10	(任意) スタートアップコンフィギュレーションの VLAN 設定を表示します。

例

次に、個々の SVI 上でデフォルトの自動ステート動作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)# interface vlan10
switch(config-if)# no autostate
```

ネイティブ VLAN トラフィックにタグを付けるためのデバイス設定

802.1Q トランク インターフェイスを使用する場合、ネイティブ VLAN ID の値と一致しすべてのタグなしトラフィックをドロップするタグで開始するすべてのパケットに対するタグgingを維持できます（この場合もインターフェイスの制御トラフィックは伝送されます）。この機能はデバイス全体に当てはまります。デバイスの VLAN を指定して当てはめることはできません。

vlan dot1q tag native global グローバル コマンドを使用すると、デバイスのすべてのトランクですべてのネイティブ VLAN ID インターフェイスの動作を変更できます。



- (注) あるデバイス上で 802.1Q タグgingをイネーブルにし、別のデバイスではディセーブルにすると、デバイス上のトラフィックはすべてドロップされ、この機能はディセーブルになります。この機能はデバイスごとに独自に設定する必要があります。

手順の概要

1. **configure terminal**
2. **vlan dot1q tag native**
3. **exit**
4. **show vlan**
5. **no shutdown**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	vlan dot1q tag native 例：	802.1Q トランキング ネイティブ VLAN ID インターフェイスの動作を変更します。このインターフェイス

	コマンドまたはアクション	目的
	<code>switch(config)# vlan dot1q tag native</code>	スは、ネイティブ VLAN ID の値と一致して、すべての非タグ付きトラフィックをドロップするタグを使って入るすべてのパケットのタグリングを維持します。この場合も、制御トラフィックはネイティブ VLAN を通過します。
ステップ3	exit 例： <code>switch(config-if-range)# exit</code> <code>switch(config)#</code>	インターフェイス コンフィギュレーション モードを終了します。
ステップ4	show vlan 例： <code>switch# show vlan</code>	(任意) VLAN のステータスと内容を表示します。
ステップ5	no shutdown 例： <code>switch# configure terminal</code> <code>switch(config)# int e3/1</code> <code>switch(config-if)# no shutdown</code>	(任意) ポリシーがハードウェアポリシーと一致するインターフェイスおよびVLANのエラーをクリアします。このコマンドにより、ポリシープログラミングが続行でき、ポートがアップできます。ポリシーが対応していない場合は、エラーはerror-disabledポリシー状態になります。
ステップ6	copy running-config startup-config 例： <code>switch(config)# copy running-config startup-config</code>	(任意) 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

例

次に、802.1Q トランク インターフェイスのネイティブ VLAN の動作を変更してタグ付きパケットを維持し、すべての非タグ付きトラフィックをドロップする例を示します（制御トラフィックは除く）。

```
switch# configure terminal
switch(config)# vlan dot1q tag native
switch#
```

システムのデフォルトポートモードをレイヤ2に変更

システムのデフォルトポートモードをレイヤ2アクセスポートに設定できます。

手順の概要

1. `configure terminal`
2. `system default switchport [shutdown]`

3. **exit**
4. **show interface brief**
5. **no shutdown**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	グローバル設定モードを開始します。
ステップ 2	system default switchport [shutdown] 例 : <pre>switch(config-if)# system default switchport</pre>	<p>システムのすべてのインターフェイスに対するデフォルトのポートモードをレイヤ2アクセスポートモードに設定し、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。デフォルトでは、すべてのインターフェイスがレイヤ3です。</p> <p>(注) クライアントが system default switchport shutdown コマンドが発行されます。</p> <ul style="list-style-type: none"> • no shutdown で設定されていない FEX HIF はシャットダウンされます。シャットダウンを回避するには、no shut で FEX HIF を設定します。 • no shutdown で明示的に設定されていないレイヤ2ポートはシャットダウンされます。シャットダウンを回避するには、no shut でレイヤ2ポートを設定します。
ステップ 3	exit 例 : <pre>switch(config-if)# exit switch(config)#</pre>	インターフェイス コンフィギュレーション モードを終了します。
ステップ 4	show interface brief 例 : <pre>switch# show interface brief</pre>	(任意) インターフェイスのステータスと内容を表示します。
ステップ 5	no shutdown 例 :	(任意) ポリシーがハードウェアポリシーと一致するインターフェイスおよびVLANのエラーをクリアします。このコマンドにより、ポリシープログラミ

	コマンドまたはアクション	目的
	<pre>switch# configure terminal switch(config)# int e3/1 switch(config-if)# no shutdown</pre>	<p>ングが続行でき、ポートがアップできます。ポリシーが対応していない場合は、エラーはerror-disabledポリシー状態になります。</p>
ステップ 6	<p>copy running-config startup-config</p> <p>例 :</p> <pre>switch(config)# copy running-config startup-config</pre>	<p>(任意) 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。</p>

例

次に、システムポートをデフォルトでレイヤ2アクセスポートに設定する例を示します。

```
switch# configure terminal
switch(config-if)# system default switchport
switch(config-if)#
```

インターフェイス コンフィギュレーションの確認

アクセスおよびトランク インターフェイス設定情報を表示するには、次のタスクのいずれかを行います。

コマンド	目的
show interface ethernet slot/port [brief counters debounce description flowcontrol mac-address status transceiver]	インターフェイスの設定を表示します。
show interface brief	インターフェイス設定情報を、モードも含めて表示します。
show interface switchport	アクセスおよびトランク インターフェイスも含めて、すべてのレイヤ2インターフェイスの情報を表示します。
show interface trunk [module module-number vlan vlan-id]	トランク設定情報を表示します。
show interface capabilities	インターフェイスの機能に関する情報を表示します。
show running-config [all]	現在の設定に関する情報を表示します。 all コマンドを使用すると、デフォルトの設定と現在の設定が表示されます。

コマンド	目的
show running-config interface ethernet slot/port	指定されたインターフェイスに関する設定情報を表示します。
show running-config interface port-channel slot/port	指定されたポートチャネルインターフェイスに関するコンフィギュレーション情報を表示します。
show running-config interface vlan vlan-id	指定された VLAN インターフェイスに関するコンフィギュレーション情報を表示します。

レイヤ2インターフェイスのモニタリング

レイヤ2インターフェイスを表示するには、次のコマンドを使用します。

コマンド	目的
clear counters interface [interface]	カウンタをクリアします。
load- interval {interval seconds {1 2 3}}	Cisco Nexus 9000 シリーズ デバイスは、ビットレートおよびパケットレートの統計情報に3種類のサンプリングインターバルを設定します。
show interface counters [module module]	入力および出力オクテットユニキャストパケット、マルチキャストパケット、ブロードキャストパケットを表示します。
show interface counters detailed [all]	入力パケット、バイト、マルチキャストを、出力パケットおよびバイトとともに表示します。
show interface counters errors [module module]	エラーパケットの数を表示します。

アクセスポートおよびトランクポートの設定例

次に、レイヤ2アクセスインターフェイスを設定し、このインターフェイスにアクセスVLANモードを割り当てる例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 2/30
switch(config-if)# switchport
switch(config-if)# switchport mode access
switch(config-if)# switchport access vlan 5
switch(config-if)#
```

次に、レイヤ2 トランク インターフェイスを設定してネイティブ VLAN および許容 VLAN を割り当て、デバイスにトランク インターフェイスのネイティブ VLAN トラフィックのタグを設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 2/35
switch(config-if)# switchport
switch(config-if)# switchport mode trunk
switch(config-if)# switchport trunk native vlan 10
switch(config-if)# switchport trunk allowed vlan 5, 10
switch(config-if)# exit
switch(config)# vlan dot1q tag native
switch(config)#
```

関連資料

関連資料	マニュアル タイトル
レイヤ3 インターフェイスの設定	「レイヤ2 インターフェイスの設定」の項
ポート チャンネル	「ポート チャンネルの設定」の項
VLAN、プライベート VLAN、STP	『Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide』
システム管理	『Cisco Nexus 9000 Series NX-OS System Management Configuration Guide』
高可用性	『Cisco Nexus 9000 Series NX-OS High Availability and Redundancy Guide』
ライセンス	『Cisco NX-OS Licensing Guide』
リリース ノート	『Cisco Nexus 9000 Series NX-OS Release Notes』



第 5 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 \(133 ページ\)](#)
- [レイヤ 3 インターフェイスの前提条件 \(140 ページ\)](#)
- [レイヤ 3 インターフェイスの注意事項および制約事項 \(140 ページ\)](#)
- [デフォルト設定 \(143 ページ\)](#)
- [レイヤ 3 インターフェイスの設定 \(143 ページ\)](#)
- [レイヤ 3 インターフェイス設定の確認 \(170 ページ\)](#)
- [レイヤ 3 インターフェイスのモニタリング \(172 ページ\)](#)
- [レイヤ 3 インターフェイスの設定例 \(173 ページ\)](#)
- [関連資料 \(175 ページ\)](#)

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、IPv4 および IPv6 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。

すべてのイーサネットポートは、デフォルトでルーテッド インターフェイスです。CLI セットアップスクリプトでこのデフォルトの動作を変更できます。



- (注) デフォルトの動作は、スイッチのタイプ (Cisco Nexus 9300、Cisco Nexus 9500、または Cisco Nexus 3164) によって異なります。



- (注) Cisco Nexus 9300 シリーズ スイッチ (Cisco Nexus 9332 スイッチを除く) には、レイヤ2 のデフォルトモードがあります。

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。ポートチャネルの詳細については、「ポートチャネルの設定」を参照してください。

ルーテッドインターフェイスおよびは、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。

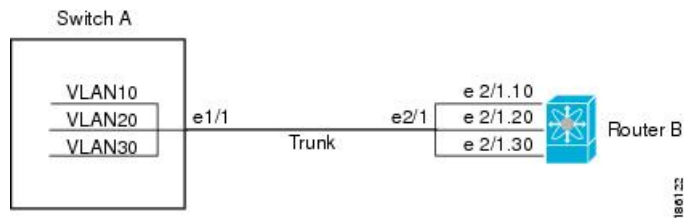
サブインターフェイスの名前は、親インターフェイスの名前 (たとえば Ethernet 2/1) + ピリオド (.) + そのインターフェイス独自の番号です。たとえば、イーサネットインターフェイス 2/1 に Ethernet 2/1.1 というサブインターフェイスを作成できます。この場合、.1 はそのサブインターフェイスを表します。

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それぞれの仮想ローカルエリアネットワーク (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 4: VLAN のサブインターフェイス



VLAN の詳細については、『[Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide](#)』を参照してください。

サブインターフェイスの制限事項

サブインターフェイスの制限事項は次のとおりです。

- 親 L3 インターフェイスをデフォルトにするには、最初にサブインターフェイスをデフォルト設定し、次に親インターフェイスをデフォルト設定する必要があります。

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 ホストに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。

設定の前に VLAN ネットワーク インターフェイス機能をイネーブルにする必要があります。システムはこの機能をディセーブルにする前のチェックポイントを自動的に取得するため、このチェックポイントにロールバックできます。ロールバックおよびチェックポイントについては、『[Cisco Nexus 9000 Series NX-OS System Management Configuration Guide](#)』を参照してください。



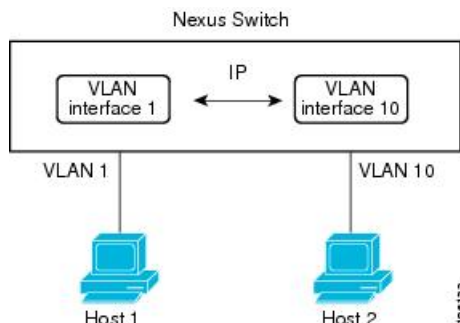
(注) VLAN 1 の VLAN インターフェイスは削除できません。

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 アドレスおよび IP ルーティングの詳細については、『[Cisco Nexus 9000 Series NX-OS 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 5: VLAN インターフェイスによる 2つの VLAN の接続



インターフェイスのVRFメンバーシップの変更

インターフェイスで **vrf member** コマンドを使用すると、インターフェイス設定の削除に関するアラートが表示されます。また、そのインターフェイスに関する設定を削除するようにクライアント/リスナー（CLI サーバなど）に通知されます。

system vrf-member-change retain-l3-config コマンドを入力すると、インターフェイスのVRFメンバーの変更時にもレイヤ3設定が保持されます。これは、既存の設定を保存（バッファ）し、古いVRFコンテキストから設定を削除し、保存された設定を新しいVRFコンテキストに再適用するために、クライアント/リスナーに通知を送信することによって行われます。



(注) **system vrf-member-change retain-l3-config** コマンドが有効になっている場合、レイヤ3設定は削除されず、保存（バッファ）されたままになります。このコマンドが有効になっていない場合（デフォルトモード）、VRFメンバーが変更されてもレイヤ3設定は保持されません。

レイヤ3設定の保持を無効にするには、**no system vrf-member-change retain-l3-config** コマンドを使用します。このモードでは、VRFメンバーが変更されてもレイヤ3設定は保持されません。

インターフェイスのVRFメンバーシップの変更に関する注意事項

- VRF名を変更すると、瞬間的なトラフィック損失が発生することがあります。
- **system vrf-member-change retain-l3-config** コマンドを有効にすると、インターフェイスレベルでの設定だけが処理されます。VRFの変更後にルーティングプロトコルに対応するには、ルータレベルで設定を手動で処理する必要があります。
- **system vrf-member-change retain-l3-config** コマンドは、次によるインターフェイスレベルの設定をサポートしています。

- CLI サーバによって保持されるレイヤ3 設定 (**ip address** および **ipv6 address** (セカンダリ) やインターフェイス設定で使用可能なすべての OSPF/ISIS/EIGRP CLI など)
 - HSRP
 - DHCP リレー エージェント CLI (**ip dhcp relay address [use-vrf]** や **ipv6 dhcp relay address [use-vrf]** など)。
- DHCP の設定
- ベストプラクティスとして、クライアントとサーバのインターフェイスVRFは一度に1つずつ変更する必要があります。そうしないと、リレーエージェントでDHCPパケットを交換できません。
 - クライアントとサーバが異なる VRF にある場合は、**ip dhcp relay address [use-vrf]** コマンドを使用して、異なる VRF 経由でリレー エージェントの DHCP パケットを交換します。

ループバック インターフェイス

ループバック インターフェイスは、常にアップ状態にある単独のエンドポイントを持つ仮想インターフェイスです。ループバック インターフェイス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。0 ~ 1023 の番号のループバック インターフェイスを最大 1024 個の設定できます。

ループバック インターフェイスを使用すると、パフォーマンスの分析、テスト、ローカル通信が実行できます。ループバック インターフェイスは、ルーティング プロトコル セッションの終端アドレスとして設定することができます。ループバックをこのように設定すると、アウトバウンドインターフェイスの一部がダウンしている場合でもルーティングプロトコルセッションはアップしたままです。

IP アンナンバード

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

ポイントツーポイントモードに準拠するインターフェイスは、IP アンナンバードインターフェイスとして使用できます。IP アンナンバード機能はイーサネット インターフェイスとサブインターフェイスでのみサポートされています。借りられるインターフェイスはループバック インターフェイスだけで、ナンバード インターフェイスと呼ばれます。

ループバック インターフェイスは、常に機能的にアップしているという点で、ナンバード インターフェイスとして理想的です。ただし、ループバック インターフェイスはスイッチ/ルータに対してローカルであるため、アンナンバードインターフェイスの到達可能性は、最初にス

タティック ルートを通じて、または OSPF や ISIS などの内部ゲートウェイ プロトコルを使用して確立する必要があります。

ポート チャネルの IP アンナナード インターフェイスの設定は、すべての Cisco Nexus 9000 シリーズ スイッチでサポートされています。

MAC 埋め込み IPv6 アドレス

BGP は、IPv4 プレフィックスを IPv6 ネクスト ホップで伝送できます。IPv6 ネクスト ホップは、ネットワークからネイバー探索 (ND) 関連のトラフィックを削除するために利用されます。これを行うために、MAC アドレスが IPv6 アドレスに組み込まれています。このようなアドレスは、MAC 埋め込み IPv6 (MEv6) アドレスと呼ばれます。ルータは、ND を通過するのではなく、MEv6 アドレスから MAC アドレスを直接抽出します。ローカル インターフェイス および ネクスト ホップ MAC アドレスは、IPv6 アドレスから抽出されます。

MEv6 対応 IPv6 インターフェイスでは、同じ MEv6 抽出 MAC アドレスが IPv4 トラフィックにも使用されます。MEv6 は、スイッチ仮想インターフェイス (SVI) を除くすべてのレイヤ 3 対応 インターフェイスでサポートされます。



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

高可用性

レイヤ3インターフェイスは、ステートフル再起動とステートレス再起動をサポートします。切り替え後、Cisco NX-OS は実行時の設定を適用します。

ハイ アベイラビリティの詳細については、『[Cisco Nexus 9000 Series NX-OS High Availability and Redundancy Guide](#)』を参照してください。

仮想化のサポート

レイヤ3インターフェイスは、仮想ルーティング/転送 (VRF) インスタンスをサポートします。VRF は仮想化デバイス コンテキスト (VDC) 内にあります。デフォルトでは、Cisco NX-OS はデフォルト VDC とデフォルト VRF に配置します。



(注) そのインターフェイスに IP アドレスを設定する前に、インターフェイスを VRF に割り当てる必要があります。

DHCP クライアント

Cisco NX-OS は、SVI、物理イーサネット、および管理インターフェイス上の IPv4 アドレスと IPv6 アドレスに関して DHCP クライアントをサポートしています。 `ip address dhcp` を使用して、DHCP クライアントの IP アドレスを設定できます。 または `ipv6 address dhcp` コマンドを使用します。これらのコマンドは、DHCPクライアントからDHCPサーバに要求を送信し、DHCPサーバからIPv4またはIPv6アドレスを要求します。Cisco Nexusスイッチ上のDHCPクライアントは、DHCPサーバに対して自身を識別します。DHCPサーバはこの ID を使用して、IP アドレスを DHCP クライアントに返します。

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

インターフェイスでの DHCP クライアントの使用に関する制限事項

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

- この機能は、物理イーサネット インターフェイス、管理インターフェイス、および SVI でのみサポートされます。
- この機能は、非デフォルトの Virtual Routing and Forwarding (VRF) インスタンスでサポートされます。
- `copy running-config startup-config` コマンドを入力すると、DNS サーバおよびデフォルトルータ オプション関連の設定がスタートアップコンフィギュレーションに保存されます。スイッチをリロードするとき、この設定が適切ではない場合は、この設定を削除しなければならない可能性があります。
- スイッチで設定できる DNS サーバは最大 6 つです。これは、スイッチの制限です。この最大数には、DHCP クライアントによって設定される DNS サーバと手動で設定される DNS サーバが含まれます。
スイッチで 7 つ以上の DNS サーバが設定されている場合、DNS オプションセットによって SVI の DHCP オファーを取得すると、IP アドレスは SVI に割り当てられません。
- Cisco Nexus 9000 シリーズスイッチは、最大 10 の IPv4 DHCP クライアントと最大 10 の IPv6 DHCP クライアントをサポートしています。
- DHCP リレーの設定と DHCP クライアントの設定には互換性がなく、同じスイッチではサポートされません。インターフェイスで DHCP クライアントを設定する前に DHCP リレーの設定を削除する必要があります。
- VLAN で DHCP スヌーピングが有効になっている場合、その VLAN の SVI が DHCP クライアントによって設定されているときは、DHCP スヌーピングが SVI DHCP クライアントで実行されません。
- IPv6 DHCP クライアントを設定する場合は、`ipv6 address use-link-local-only` コマンドで設定します。これは `ipv6 address dhcp` コマンドを使用します。

レイヤ3スタティック MAC アドレス

スタティック MAC アドレスは、次のレイヤ3 インターフェイスに設定できます。

- レイヤ3 インターフェイス
- レイヤ3 サブインターフェイス
- レイヤ3 ポート チャネル
- VLAN ネットワーク インターフェイス



(注) トンネル インターフェイスにはスタティック MAC アドレスを設定できません。

レイヤ3 インターフェイスの前提条件

レイヤ3 インターフェイスには次の前提条件があります。

- IP アドレッシングおよび基本設定を熟知している。IP アドレッシングの詳細については、『[Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide](#)』を参照してください。

レイヤ3 インターフェイスの注意事項および制約事項

レイヤ3 インターフェイスの設定には次の注意事項と制約事項があります。

- キーワードが付いている **show** コマンドはサポートされていません。 **internal**
- ポートチャネルのメンバーシップに設定されている物理インターフェイスで、サブインターフェイスを設定することはサポートされていません。ポートチャネルインターフェイス自体の下にサブインターフェイスを設定する必要があります。
- レイヤ3 インターフェイスをレイヤ2 インターフェイスに変更する場合、Cisco NX-OS はインターフェイスをシャットダウンしてインターフェイスを再度イネーブルにし、レイヤ3 固有の設定をすべて削除します。
- レイヤ2 インターフェイスをレイヤ3 インターフェイスに変更する場合、Cisco NX-OS はインターフェイスをシャットダウンしてインターフェイスを再度イネーブルにし、レイヤ2 固有の設定をすべて削除します。
- ポートチャネルインターフェイスでサブインターフェイスを設定する場合、Dynamic Host Configuration Protocol (DHCP) オプションはサポートされません。
- IP アンナンバードインターフェイスが設定されている場合、ループバックインターフェイスはIP アンナンバードインターフェイスと同じVRFにある必要があります。

- 整数 **admin-shutdown** 番号付きインターフェイスであるループバックインターフェイスでコマンドを実行しても、IPアンナンバードインターフェイスはダウンしません。これは、IPアンナンバードインターフェイス上で実行されているルーティングプロトコルが引き続き稼働していることを意味します。
- IPアンナンバードインターフェイス上で実行されるスタティックルートは、固定されたスタティックルートを使用する必要があります。



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

- IP アンナンバード インターフェイスは物理とサブインターフェイスでのみサポートされています。
- ループバックインターフェイスだけが、番号なしインターフェイスを番号付きインターフェイスとして使用できます。
- IPアンナンバードインターフェイスを介したOSPFがサポートされます。
- IPアンナンバードインターフェイスを介したISISはサポートされています。
- オーバーレイインターフェイスとしてIPアンナンバードインターフェイスを使用するループバックインターフェイス上のBGPはサポートされています。
- デフォルトおよびデフォルト以外のVRFは、IPアンナンバードインターフェイスでサポートされます。
- スイッチには、16個のユーザ定義MACアドレス (MEv6/スタティック) の制限があります。この制限を超えて設定すると、CSCux84428に記載されている問題が発生する可能性があります。 <https://tools.cisco.com/bugsearch/bug/CSCux84428>
- X9700-EX および X9700-FX ライン カードを搭載した Cisco Nexus 9500 シリーズ スイッチの SVI およびサブインターフェイスの IPv6 カウンタはサポートされていません。
- SVIとサブインターフェイスの両方のマルチキャストおよびブロードキャストカウンタはサポートされていません。
- SVIとサブインターフェイスの両方のカウンタのコントロールプレーンSVI/SIトラフィックはサポートされません。
- Cisco NX-OS リリース 9.3(6) 以降では、Cisco Nexus N9K-C9336C-FX2 および N9K-C93240YC-FX2 スイッチでサブインターフェイスマルチキャストおよびブロードキャストカウンタがサポートされています。
- サブインターフェイスのマルチキャストおよびブロードキャストカウンタを有効にすると、SVI、レイヤ2 VLAN、MPLS カウンタが機能しない場合があります。
- この統計情報では、最大 1000 個のサブインターフェイスがサポートされます。

- Cisco NX-OS リリース 10.1(2) 以降、レイヤ3 インターフェイスは Cisco Nexus N9K-X9624D-R2 ラインカードでサポートされます。
- Cisco NX-OS リリース 10.3(1)F 以降、Cisco Nexus 9808 プラットフォーム スイッチで L3、ループバック、サブインターフェイスのサポートが提供されます。
- Cisco NX-OS リリース 10.4(1)F 以降、Cisco Nexus 9804 プラットフォーム スイッチで L3、ループバック、サブインターフェイスのサポートが提供されます。
- Cisco NX-OS リリース 10.3(1)F 以降、Cisco Nexus 9808 プラットフォーム スイッチで L3 物理およびサブインターフェイスのサポートが提供されます。
- Cisco NX-OS リリース 10.4(1)F 以降、Cisco Nexus 9804 プラットフォーム スイッチで L3 物理およびサブインターフェイスのサポートが提供されます。
- Cisco NX-OS リリース 10.4(2)F 以降、Cisco Nexus C9232E-B1 プラットフォーム スイッチで以下の機能がサポートされます。
 - レイヤ3、ループバック、およびサブインターフェイスのサポート
 - 統計情報のサポートは、レイヤ3物理インターフェイスとサブインターフェイスで提供されます。
- Cisco Nexus 9800 プラットフォーム スイッチには、L3 物理およびサブインターフェイスのサポートに関して次の制限があります。
 - ブロードキャストはサポートされていません。
 - **hardware profile sub-interface flex-stats** コマンドは適用されません。
 - サブインターフェイスの統計情報は、親インターフェイスに集約されません。
- Cisco NX-OS リリース 10.4(1)F 以降、L3 転送は Cisco Nexus 9332D-H2R プラットフォーム スイッチでサポートされます。
- Cisco NX-OS リリース 10.4(2)F 以降、L3 転送は Cisco Nexus 93400LD-H1 プラットフォーム スイッチでサポートされます。
- Cisco NX-OS リリース 10.4(1)F 以降では、Cisco Nexus 9808 および 9804 スイッチを搭載した N9KX98900CD-A および N9KX9836DM-A ラインカードの L3 物理およびサブインターフェイスに対して統計情報のサポートが提供されます。



(注) Cisco IOS の CLI に慣れている場合、この機能に対応する Cisco NX-OS コマンドは通常使用する Cisco IOS コマンドと異なる場合があるので注意してください。

デフォルト設定

次の表に、レイヤ3インターフェイスパラメータのデフォルト設定を示します。

表 10: レイヤ3インターフェイスのデフォルトパラメータ

パラメータ	デフォルト
管理ステータス	閉じる

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

任意のイーサネットポートをルーテッドインターフェイスとして設定できます。

手順の概要

1. **configure terminal**
2. **interface ethernet slot/port**
3. **no switchport**
4. **[ip address ip-address/length | ipv6 address ipv6-address/length]**
5. **show interfaces**
6. **no shutdown**
7. **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	configure terminal 例： <pre>switch# configure terminal switch(config)#</pre>	グローバル設定モードを開始します。
ステップ 2	interface ethernet slot/port 例： <pre>switch(config)# interface ethernet 2/1 switch(config-if)#</pre>	インターフェイス設定モードを開始します。
ステップ 3	no switchport 例： <pre>switch(config-if)# no switchport</pre>	その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ます。

	コマンドまたはアクション	目的
ステップ4	<p>[ip address ip-address/length ipv6 address ipv6-address/length]</p> <p>例 :</p> <pre>switch(config-if)# ip address 192.0.2.1/8</pre> <p>例 :</p> <pre>switch(config-if)# ipv6 address 2001:0DB8::1/8</pre>	<ul style="list-style-type: none"> このインターフェイスのIPアドレスを設定します。IPアドレスの詳細については、『Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide』を参照してください。 このインターフェイスのIPv6アドレスを設定します。IPv6アドレスの詳細については、『Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide』を参照してください。
ステップ5	<p>show interfaces</p> <p>例 :</p> <pre>switch(config-if)# show interfaces ethernet 2/1</pre>	(任意) レイヤ3インターフェイスの統計情報を表示します。
ステップ6	<p>no shutdown</p> <p>例 :</p> <pre>switch# switch(config-if)# int e2/1 switch(config-if)# no shutdown</pre>	(任意) ポリシーがハードウェアポリシーに対応するインターフェイスのエラーをクリアします。このコマンドにより、ポリシープログラミングが続き、ポートがアップできます。ポリシーが対応していない場合は、エラーはerror-disabledポリシー状態になります。
ステップ7	<p>copy running-config startup-config</p> <p>例 :</p> <pre>switch(config)# copy running-config startup-config</pre>	(任意) この設定の変更を保存します。

例

- **medium** コマンドを使用し、コマンドを使用します。

コマンド	目的
<p>medium {broadcast p2p}</p> <p>例 :</p> <pre>switch(config-if)# medium p2p medium p2p</pre>	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** です。、およびこの設定は、**show** のいずれにも表示されません コマンドにも表示されません。ただし、設定を **p2pshow running config** を入力すると、この設定が表示されます。コマンドを使用する必要があります。

- **switchport** コマンドを使用し、コマンドを使用します。

コマンド	目的
switchport 例： switch(config-if)# switchport switchport	インターフェイスをレイヤ2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3固有の設定を削除します。

- 次に、ルーテッドインターフェイスを設定する例を示します。

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

インターフェイスのデフォルト設定がルーテッドされます。レイヤ2にインターフェイスを設定するには、**switchport**を入力しますコマンドを使用します。レイヤ2インターフェイスをルーテッドインターフェイスに変更する場合は、**no switchport** コマンドを入力します。

ルーテッドインターフェイスでのサブインターフェイスの設定

ルーテッドインターフェイスで構成されるルーテッドインターフェイスに1つまたは複数のサブインターフェイスを設定できます。

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。

「ルーテッドインターフェイスの設定」の項を参照してください。

手順の概要

- configure terminal**
- interface ethernet slot/port.number**
- [ip address ip-address/length | ipv6 address ipv6-address/length]**
- encapsulation dot1Q vlan-id**
- show interfaces**
- 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	configure terminal 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	interface ethernet slot/port.number 例： switch(config)# interface ethernet 2/1.1 switch(config-subif)#	サブインターフェイスを作成し、サブインターフェイスコンフィギュレーションモードを開始します。 number の範囲は 1 ~ 4094 です。
ステップ 3	[ip address ip-address/length ipv6 address ipv6-address/length] 例： switch(config-subif)# ip address 192.0.2.1/8 例： switch(config-subif)# ipv6 address 2001:0DB8::1/8	<ul style="list-style-type: none"> このサブインターフェイスの IP アドレスを設定します。IP アドレスの詳細については、『Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide』を参照してください。 このサブインターフェイスの IPv6 アドレスを設定します。IPv6 アドレスの詳細については、『Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide』を参照してください。
ステップ 4	encapsulation dot1Q vlan-id 例： switch(config-subif)# encapsulation dot1Q 33	サブインターフェイス上の IEEE 802.1Q VLAN カプセル化を設定します。範囲は 2 ~ 4093 です。
ステップ 5	show interfaces 例： switch(config-subif)# show interfaces ethernet 2/1.1	(任意) レイヤ 3 インターフェイスの統計情報を表示します。
ステップ 6	copy running-config startup-config 例： switch(config)# copy running-config startup-config	(任意) この設定の変更を保存します。

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 2/1.1
switch(config-if)# ip address 192.0.2.1/8
switch(config-if)# encapsulation dot1Q 33
switch(config-if)# copy running-config startup-config
```

- show interface eth** の出力 次に示すように、サブインターフェイス用に拡張されました。

```
switch# show interface ethernet 1/2.1
Ethernet1/2.1 is down (Parent Interface Admin down)
admin state is down, Dedicated Interface, [parent interface is Ethernet1/2]
Hardware: 40000 Ethernet, address: 0023.ac67.9bc1 (bia 4055.3926.61d4)
Internet Address is 10.10.10.1/24
MTU 1500 bytes, BW 40000000 Kbit, DLY 10 usec
```

```

reliability 255/255, txload 1/255, rxload 1/255
Auto-mdix is turned off
EtherType is 0x8100
L3 in Switched:
  ucast: 0 pkts, 0 bytes - mcast: 0 pkts, 0 bytes
L3 out Switched:
  ucast: 0 pkts, 0 bytes - mcast: 0 pkts, 0 bytes

```

ポートチャネルインターフェイスでのサブインターフェイスの設定

ポートチャネルインターフェイスに1つまたは複数のサブインターフェイスを設定できます。



- (注) ポートチャネルインターフェイス上のサブインターフェイスは、マルチキャストルーティング、ルータ ACL、QoS、ポリシーベースルーティング (PBR)、SPAN、または ERSPAN をサポートしません。

始める前に

親インターフェイスをポートチャネルインターフェイスとして設定します。

「ポートチャネルの設定」の章を参照してください。

手順の概要

1. **configure terminal**
2. **interface port-channel** *channel-id.number*
3. **[ip address** *ip-address/length* **| ipv6 address** *ipv6-address/length*]
4. **encapsulation dot1Q** *vlan-id*
5. **show interfaces**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface port-channel <i>channel-id.number</i> 例： switch(config)# interface port-channel 100.1 switch(config-subif)#	サブインターフェイスを作成し、サブインターフェイス コンフィギュレーション モードを開始します。
ステップ 3	[ip address <i>ip-address/length</i> ipv6 address <i>ipv6-address/length</i>]	<ul style="list-style-type: none"> • このサブインターフェイスの IP アドレスを設定します。IP アドレスの詳細については、『Cisco

	コマンドまたはアクション	目的
	例 : <pre>switch(config-subif)# ip address 192.0.2.1/8</pre> 例 : <pre>switch(config-subif)# ipv6 address 2001:0DB8::1/8</pre>	<p>Nexus 9000 Series NX-OS Unicast Routing Configuration Guide』を参照してください。</p> <ul style="list-style-type: none"> このサブインターフェイスのIPv6アドレスを設定します。IPv6アドレスの詳細については、『Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide』を参照してください。
ステップ 4	encapsulation dot1Q <i>vlan-id</i> 例 : <pre>switch(config-subif)# encapsulation dot1q 33</pre>	サブインターフェイス上の IEEE 802.1Q VLAN カプセル化を設定します。範囲は 2 ~ 4093 です。
ステップ 5	show interfaces 例 : <pre>switch(config-subif)# show interfaces ethernet 2/1.1</pre>	(任意) レイヤ 3 インターフェイスの統計情報を表示します。
ステップ 6	copy running-config startup-config 例 : <pre>switch(config)# copy running-config startup-config</pre>	(任意) この設定の変更を保存します。

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 port-channel 115.3
switch(config-subif)# ip address 141.143.101.2/24
switch(config-subif)# encapsulation dot1q 3
switch(config-subif)# copy running-config startup-config
```

VLAN インターフェイスの設定

VLAN インターフェイスを作成して内部 VLAN ルーティングを行うことができます。

手順の概要

1. **configure terminal**
2. **feature interface-vlan**
3. **interface vlan *number***
4. **[ip address *ip-address/length* | ipv6 address *ipv6-address/length*]**
5. **show interface vlan *number***
6. **no shutdown**

7. 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	configure terminal 例： switch# configure terminal switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	feature interface-vlan 例： switch(config)# feature interface-vlan	VLAN インターフェイス モードをイネーブルにします。
ステップ 3	interface vlan number 例： switch(config)# interface vlan 10 switch(config-if)#	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 4	[ip address ip-address/length ipv6 address ipv6-address/length] 例： switch(config-if)# ip address 192.0.2.1/8 例： switch(config-if)# ipv6 address 2001:0DB8::1/8	<ul style="list-style-type: none"> この VLAN インターフェイスの IP アドレスを設定します。IP アドレスの詳細については、『Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide』を参照してください。 この VLAN インターフェイスの IPv6 アドレスを設定します。IPv6 アドレスの詳細については、『Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide』を参照してください。
ステップ 5	show interface vlan number 例： switch(config-if)# show interface vlan 10	(任意) レイヤ 3 インターフェイスの統計情報を表示します。
ステップ 6	no shutdown 例： switch(config)# int e3/1 switch(config)# no shutdown	(任意) ポリシーがハードウェアポリシーに対応するインターフェイスのエラーをクリアします。このコマンドにより、ポリシープログラミングが続き、ポートがアップできます。ポリシーが対応していない場合は、エラーは error-disabled ポリシー状態になります。
ステップ 7	copy running-config startup-config 例： switch(config-if)# copy running-config startup-config	(任意) この設定の変更を保存します。

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
```

VRF メンバーシップ変更時のレイヤ3 保持の有効化

次の手順により、インターフェイスの VRF メンバーシップを変更する際にレイヤ3 設定を保持できます。

手順の概要

1. `configure terminal`
2. `system vrf-member-change retain-l3-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	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	コンフィギュレーションモードに入ります。
ステップ 2	system vrf-member-change retain-l3-config 例 : <pre>switch(config)# system vrf-member-change retain-l3-config</pre> <p>Warning: Will retain L3 configuration when vrf member change on interface.</p>	VRF メンバーシップ変更時のレイヤ3 保持を有効化します。 (注) レイヤ3 設定の保持を無効にするには、 no system vrf-member-change retain-l3-config コマンドを使用します。

レイヤ3 インターフェイス上のスタティック MAC アドレスの設定

レイヤ3 インターフェイスのスタティック MAC アドレスを設定できます。ブロードキャストまたはマルチキャストのアドレスは、スタティック MAC アドレスとして設定できません。



Note トンネル インターフェイス上には、スタティック MAC アドレスを設定できません。



Note この設定は、16のVLANインターフェイスに制限されます。追加のVLANインターフェイスに設定を適用すると、ハードウェアプログラムが失敗したインターフェイスがダウン状態になります。ステータス。

SUMMARY STEPS

1. **config t**
2. **interface** [*ethernet slot/port* | **ethernet** *slot/port.number* | **port-channel** *number* | **vlan** *vlan-id*]
3. **mac-address** *mac-address*
4. **exit**
5. (Optional) **show interface** [*ethernet slot/port* | **ethernet** *slot/port.number* | **port-channel** *number* | **vlan** *vlan-id*]
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
ステップ 1	config t Example: switch# config t switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	interface [<i>ethernet slot/port</i> ethernet <i>slot/port.number</i> port-channel <i>number</i> vlan <i>vlan-id</i>] Example: switch(config)# interface ethernet 7/3	レイヤ3 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。 Note スタティック MAC アドレスを割り当てる前に、レイヤ3 インターフェイスを作成する必要があります。
ステップ 3	mac-address <i>mac-address</i> Example: switch(config-if)# mac-address 22ab.47dd.ff89 switch(config-if)#	レイヤ3 インターフェイスに追加するスタティック MAC アドレスを指定します。
ステップ 4	exit Example: switch(config-if)# exit switch(config)#	インターフェイス モードを終了します。
ステップ 5	(Optional) show interface [<i>ethernet slot/port</i> ethernet <i>slot/port.number</i> port-channel <i>number</i> vlan <i>vlan-id</i>] Example: switch# show interface ethernet 7/3	レイヤ3 インターフェイスに関する情報を表示します。

	Command or Action	Purpose
ステップ 6	(Optional) copy running-config startup-config Example: switch# copy running-config startup-config	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、スロット7、ポート3上のレイヤ3インターフェイスにスタティック MAC アドレスを設定する例を示します。

```
switch# config t
switch(config)# interface ethernet 7/3
switch(config-if)# mac-address 22ab.47dd.ff89
switch(config-if)#
```

ループバック インターフェイスの設定

ループバック インターフェイスを設定して、常にアップ状態にある仮想インターフェイスを作成できます。

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貫であることを確認します。

手順の概要

1. **configure terminal**
2. **interface loopback instance**
3. **[ip address ip-address/length | ipv6 address ipv6-address/length]**
4. **show interface loopback instance**
5. **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	configure terminal 例： switch# configure terminal switch(config)#	コンフィギュレーションモードに入ります。
ステップ 2	interface loopback instance 例： switch(config)# interface loopback 0 switch(config-if)#	ループバック インターフェイスを作成します。範囲は 0 ~ 1023 です。

	コマンドまたはアクション	目的
ステップ 3	[ip address ip-address/length ipv6 address ipv6-address/length] 例： <pre>switch(config-if)# ip address 192.0.2.1/8</pre> 例： <pre>switch(config-if)# ipv6 address 2001:0DB8::1/8</pre>	<ul style="list-style-type: none"> このインターフェイスのIPアドレスを設定します。IPアドレスの詳細については、『Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide』を参照してください。 このインターフェイスのIPv6アドレスを設定します。IPv6アドレスの詳細については、『Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide』を参照してください。
ステップ 4	show interface loopback instance 例： <pre>switch(config-if)# show interface loopback 0</pre>	(任意) ループバックインターフェイスの統計情報を表示します。
ステップ 5	copy running-config startup-config 例： <pre>switch(config-if)# copy running-config startup-config</pre>	(任意) この設定の変更を保存します。

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 192.0.2.1/8
switch(config-if)# copy running-config startup-config
```

イーサネットインターフェイスでのIPアンナンバードの設定

イーサネットインターフェイスでIPアンナンバード機能を設定できます。

手順の概要

1. **configure terminal**
2. **interface ethernet slot/port**
3. **medium p2p**
4. **ip unnumbered type 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	configure terminal 例：	グローバル設定モードを開始します。

	コマンドまたはアクション	目的
	switch# configure terminal switch(config)#	
ステップ 2	interface ethernet slot/port 例： switch(config)# interface ethernet 1/1 switch(config-if)#	インターフェイス設定モードを開始します。
ステップ 3	medium p2p 例： switch(config-if)# medium p2p	インターフェイス メディアをポイント ツー ポイントとして設定します。
ステップ 4	ip unnumbered type number 例： switch(config-if)# ip unnumbered loopback 100	明示的な IP アドレスをインターフェイスに割り当てずにインターフェイス上の IP 処理をイネーブルにします。 <i>type</i> および <i>number</i> は、IP アドレスが割り当てられているルータ上の別のインターフェイスを指定します。指定したインターフェイスを別のアンナンバードインターフェイスに設定することはできません。 (注) <i>type</i> は loopback に制限されます。

IP アンナンバード インターフェイスの OSPF の設定

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

手順の概要

1. **configure terminal**
2. **interface ethernet slot/port**
3. **encapsulation dot1Q vlan-id**
4. **medium p2p**
5. **ip unnumbered type number**
6. (任意) **ip ospf authentication**
7. (任意) **ip ospf authentication-key password**
8. **ip router ospf instance area area-number**
9. **no shutdown**
10. **interface loopback instance**
11. **ip address ip-address/length**
12. **ip router ospf instance area area-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	configure terminal 例： switch# configure terminal switch(config)#	グローバル設定モードを開始します。
ステップ 2	interface ethernet slot/port 例： switch(config)# interface ethernet 1/20.1 switch(config-if)#	インターフェイス設定モードを開始します。
ステップ 3	encapsulation dot1Q vlan-id 例： switch(config-if)# encapsulation dot1Q 100	サブインターフェイス上の IEEE 802.1Q VLAN カプセル化を設定します。範囲は 2 ～ 4093 です。
ステップ 4	medium p2p 例： switch(config-if)# medium p2p	インターフェイスメディアをポイントツーポイントとして設定します。
ステップ 5	ip unnumbered type number 例： switch(config-if)# ip unnumbered loopback 101	明示的な IP アドレスをインターフェイスに割り当てずにインターフェイス上の IP 処理をイネーブルにします。 <i>type</i> および <i>number</i> は、IP アドレスが割り当てられているルータ上の別のインターフェイスを指定します。指定したインターフェイスを別のアンナナバードインターフェイスに設定することはできません。 (注) <i>type</i> は loopback に制限されます。
ステップ 6	(任意) ip ospf authentication 例： switch(config-if)# ip ospf authentication	インターフェイスの認証タイプを指定します。
ステップ 7	(任意) ip ospf authentication-key password 例： switch(config-if)# ip ospf authentication 3 b7bdf15f62bbd250	OSPF 認証の認証パスワードを指定します。
ステップ 8	ip router ospf instance area area-number 例： switch(config-if)# ip router ospf 100 area 0.0.0.1	インターフェイス上で IP ルーティングプロセスを設定して、エリアを指定します。 (注) アンナナバードインターフェイスとアンナナバードインターフェイスの両方に ip router ospf コマンドが必要です。

	コマンドまたはアクション	目的
ステップ 9	no shutdown 例： switch(config-if)# no shutdown	そのインターフェイスをアップします（管理的に）。
ステップ 10	interface loopback instance 例： switch(config)# interface loopback 101	ループバック インターフェイスを作成します。範囲は 0 - 1023 です。
ステップ 11	ip address ip-address/length 例： switch(config-if)# 192.168.101.1/32	インターフェイスに IP アドレスを設定します。
ステップ 12	ip router ospf instance area area-number 例： switch(config-if)# ip router ospf 100 area 0.0.0.1	インターフェイス上で IP ルーティング プロセスを設定して、エリアを指定します。 (注) アンナンバード インターフェイスとナンバード インターフェイスの両方に ip router ospf コマンドが必要です。

IP アンナンバード インターフェイスの ISIS の設定

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

手順の概要

1. **configure terminal**
2. **feature isis**
3. **router isis area-tag**
4. **net network-entity-title**
5. **end**
6. **interface ethernet slot/port**
7. **encapsulation dot1Q vlan-id**
8. **medium p2p**
9. **ip unnumbered type number**
10. **ip router isis area-tag**
11. **no shutdown**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例：	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	switch# configure terminal switch(config)#	
ステップ 2	feature isis 例： Switch(config)# feature isis	ISIS をイネーブルにします。
ステップ 3	router isis area-tag 例： Switch(config)# router isis 100	タグを IS-IS プロセスに割り当て、ルータ コンフィギュレーション モードを開始します。
ステップ 4	net network-entity-title 例： Switch(config-router)# net 49.0001.0100.0100.1001.00	デバイスでネットワーク エンティティ タイトル (NET) を設定します。
ステップ 5	end 例： Switch(config-router)# end	ルータ コンフィギュレーション モードを終了します。
ステップ 6	interface ethernet slot/port 例： switch(config)# interface ethernet 1/20.1	インターフェイス設定モードを開始します。
ステップ 7	encapsulation dot1Q vlan-id 例： switch(config-subif)# encapsulation dot1Q 100	サブインターフェイス上の IEEE 802.1Q VLAN カプセル化を設定します。範囲は 2 ～ 4093 です。
ステップ 8	medium p2p 例： switch(config-subif)# medium p2p	インターフェイスメディアをポイントツーポイントとして設定します。
ステップ 9	ip unnumbered type number 例： switch(config-if)# ip unnumbered loopback 101	明示的な IP アドレスをインターフェイスに割り当てずにインターフェイス上の IP 処理をイネーブルにします。 <i>type</i> および <i>number</i> は、IP アドレスが割り当てられているルータ上の別のインターフェイスを指定します。指定したインターフェイスを別のアンナンバードインターフェイスに設定することはできません。 (注) <i>type</i> は loopback に制限されます。
ステップ 10	ip router isis area-tag 例：	アンナンバードインターフェイスで ISIS をイネーブルにします。

	コマンドまたはアクション	目的
	<code>switch(config-subif)# ip router isis 100</code>	
ステップ 11	no shutdown 例： <code>switch(config-subif)# no shutdown</code>	インターフェイスをアップにします（管理に関して）。

SVI TCAM リージョンの設定

Cisco NX-OS リリース 9.3(3) 以降では、Cisco Nexus 3100 シリーズスイッチの SVI インターフェイスでレイヤ 3 統計情報を表示できます。ハードウェアの SVI Ternary Content Addressable Memory (TCAM) 領域のサイズを変更して、SVI インターフェイスのレイヤ 3 着信ユニキャストカウンタを表示できます。

手順の概要

1. **hardware profile tcam region {arpacl | e-racl} | ifacl | nat | qos} | qoslbl | racl} | vacl | svi } tcam_size**
2. **copy running-config startup-config**
3. `switch(config)# show hardware profile tcam region`
4. `switch(config)# reload`

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	hardware profile tcam region {arpacl e-racl} ifacl nat qos} qoslbl racl} vacl svi } tcam_size	ACL TCAM リージョン サイズを変更します。 <ul style="list-style-type: none"> • arpacl : アドレス解決プロトコル (ARP) の ACL (ARPACL) TCAM リージョンサイズを設定します。 • e-racl : 出力ルータ ACL (ERACL) TCAM リージョンサイズを設定します。 • e-vacl : 出力の VLAN ACL (EVACL) TCAM リージョンサイズを設定します。 • ifacl : インターフェイス ACL (ifacl) TCAM リージョンサイズを設定します。エントリの最大数は 1500 です。 • nat : NAT TCAM リージョンのサイズを設定します。 • qos : Quality of Service (QoS) TCAM リージョンサイズを設定します。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> • qoslbl : QoS ラベル (qoslbl) TCAM リージョン サイズを設定します。 • racl : ルータの ACL (RACL) TCAM リージョン サイズを設定します。 • vacl : VLAN ACL (VAACL) TCAM リージョン サイズを設定します。 • svi : SVI TCAM リージョン サイズを設定します。この SVI TCAM のデフォルトサイズは 0 です。 • tcam_size : TCAM サイズ。有効な範囲は 0 ~ 2,147,483,647 エントリです。 <p>(注) vacl および e-vacl TCAM リージョンを同じサイズに設定する必要があります。</p>
ステップ 2	copy running-config startup-config 例 : <pre>switch(config)# copy running-config startup-config</pre>	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーして、変更を継続的に保存します。
ステップ 3	<pre>switch(config)# show hardware profile tcam region</pre> 例 : <pre>switch(config)# show hardware profile tcam region</pre>	スイッチの次回のリロード時に適用される TCAM サイズを表示します。
ステップ 4	<pre>switch(config)# reload</pre> 例 : <pre>switch(config)# reload</pre>	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。 (注) copy running-config to startup-config を保存した後、次回のリロード時に新しいサイズ値が有効になります。

例

次に、SVI TCAM リージョンのサイズを変更する例を示します。

```
switch(config)# hardware profile tcam region svi 256
[SUCCESS] New tcam size will be applicable only at boot time.
You need to 'copy run start' and 'reload'
```

```
switch(config)# copy running-config startup-config
switch(config)# reload
WARNING: This command will reboot the system
Do you want to continue? (y/n) [n] y
```

VRFへのインターフェイスの割り当て

VRFにレイヤ3インターフェイスを追加できます。

手順の概要

1. **configure terminal**
2. **interface** *interface-type number*
3. **vrf member** *vrf-name*
4. **ip address** *ip-prefix/length*
5. **show vrf** [*vrf-name*] **interface** *interface-type number*
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： switch# configure terminal switch(config)#	コンフィギュレーションモードに入ります。
ステップ 2	interface <i>interface-type number</i> 例： switch(config)# interface loopback 0 switch(config-if)#	インターフェイス設定モードを開始します。
ステップ 3	vrf member <i>vrf-name</i> 例： switch(config-if)# vrf member RemoteOfficeVRF	このインターフェイスを VRF に追加します。
ステップ 4	ip address <i>ip-prefix/length</i> 例： switch(config-if)# ip address 192.0.2.1/16	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	show vrf [<i>vrf-name</i>] interface <i>interface-type number</i> 例： switch(config-vrf)# show vrf Enterprise interface loopback 0	(任意) VRF 情報を表示します。
ステップ 6	copy running-config startup-config 例： switch(config-if)# copy running-config startup-config	(任意) この設定の変更を保存します。

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
```

MAC 埋め込み IPv6 アドレスの設定

MAC 埋め込み IPv6 (MEv6) アドレスを設定できます。

手順の概要

1. **configure terminal**
2. **interface type slot/port**
3. **no switchport**
4. **mac-address ipv6-extract**
5. **ipv6 address ip-address/length**
6. **ipv6 nd mac-extract [exclude nud-phase]**
7. (任意) **show ipv6 icmp interface type slot/port**
8. (任意) **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	configure terminal 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface type slot/port 例： switch(config)# interface ethernet 1/3 switch(config-if)#	指定したインターフェイスのインターフェイス コンフィギュレーション モードを開始します。
ステップ 3	no switchport 例： switch(config-if)# no switchport	インターフェイスをレイヤ3 インターフェイスとして設定し、このインターフェイス上のレイヤ2 固有の設定を削除します。 (注) レイヤ3 インターフェイスを元のレイヤ2 インターフェイスに変換するには、 switchport コマンドを使用します。

	コマンドまたはアクション	目的
ステップ 4	mac-address ipv6-extract 例： switch(config-if)# mac-address ipv6-extract	インターフェイスに設定されている IPv6 アドレスに埋め込まれている MAC アドレスを抽出します。 (注) 現在、MEv6 設定は IPv6 アドレスの EUI-64 形式ではサポートされていません。
ステップ 5	ipv6 address ip-address/length 例： switch(config-if)# ipv6 address 2002:1::10/64	このインターフェイスの IPv6 アドレスを設定します。
ステップ 6	ipv6 nd mac-extract [exclude nud-phase] 例： switch(config-if)# ipv6 nd mac-extract	ネクストホップIPv6アドレスに埋め込まれているネクストホップMACアドレスを抽出します。 exclude nud-phase フェーズオプションにより、ND フェーズでのみパケットがブロックされます。 exclude nud-phase (NUD) フェーズオプションが指定されていない場合は、ND フェーズと近隣到達不能検出 (NUD) フェーズの両方でパケットがブロックされます。
ステップ 7	(任意) show ipv6 icmp interface type slot/port 例： switch(config-if)# show ipv6 icmp interface ethernet 1/3	IPv6 Internet Control Message Protocolバージョン6 (ICMPv6) インターフェイス情報を表示します。
ステップ 8	(任意) copy running-config startup-config 例： switch(config-if)# copy running-config startup-config	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、ND MAC抽出をイネーブルにしてMAC組み込みIPv6アドレスを設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/3
switch(config-if)# no switchport
switch(config-if)# mac-address ipv6-extract
switch(config-if)# ipv6 address 2002:1::10/64
switch(config-if)# ipv6 nd mac-extract
switch(config-if)# show ipv6 icmp interface ethernet 1/3
ICMPv6 Interfaces for VRF "default"
Ethernet1/3, Interface status: protocol-up/link-up/admin-up
  IPv6 address: 2002:1::10
  IPv6 subnet: 2002:1::/64
  IPv6 interface DAD state: VALID
```

```

ND mac-extract : Enabled
ICMPv6 active timers:
  Last Neighbor-Solicitation sent: 00:01:39
  Last Neighbor-Advertisement sent: 00:01:40
  Last Router-Advertisement sent: 00:01:41
  Next Router-Advertisement sent in: 00:03:34
Router-Advertisement parameters:
  Periodic interval: 200 to 600 seconds
  Send "Managed Address Configuration" flag: false
  Send "Other Stateful Configuration" flag: false
  Send "Current Hop Limit" field: 64
  Send "MTU" option value: 1500
  Send "Router Lifetime" field: 1800 secs
  Send "Reachable Time" field: 0 ms
  Send "Retrans Timer" field: 0 ms
  Suppress RA: Disabled
  Suppress MTU in RA: Disabled
Neighbor-Solicitation parameters:
  NS retransmit interval: 1000 ms
ICMPv6 error message parameters:
  Send redirects: true
  Send unreachable: false
ICMPv6-nd Statistics (sent/received):
  RAs: 3/0, RSs: 0/0, NAs: 2/0, NSs: 7/0, RDs: 0/0
  Interface statistics last reset: never

```

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

```

switch# configure terminal
switch(config)# interface ethernet 1/5
switch(config-if)# no switchport
switch(config-if)# mac-address ipv6-extract
switch(config-if)# ipv6 address 2002:2::10/64
switch(config-if)# ipv6 nd mac-extract exclude nud-phase
switch(config-if)# show ipv6 icmp interface ethernet 1/5
ICMPv6 Interfaces for VRF "default"
Ethernet1/5, Interface status: protocol-up/link-up/admin-up
  IPv6 address: 2002:2::10
  IPv6 subnet: 2002:2::/64
  IPv6 interface DAD state: VALID
  ND mac-extract : Enabled (Excluding NUD Phase)
  ICMPv6 active timers:
    Last Neighbor-Solicitation sent: 00:06:45
    Last Neighbor-Advertisement sent: 00:06:46
    Last Router-Advertisement sent: 00:02:18
    Next Router-Advertisement sent in: 00:02:24
  Router-Advertisement parameters:
    Periodic interval: 200 to 600 seconds
    Send "Managed Address Configuration" flag: false
    Send "Other Stateful Configuration" flag: false
    Send "Current Hop Limit" field: 64
    Send "MTU" option value: 1500
    Send "Router Lifetime" field: 1800 secs
    Send "Reachable Time" field: 0 ms
    Send "Retrans Timer" field: 0 ms
    Suppress RA: Disabled
    Suppress MTU in RA: Disabled
  Neighbor-Solicitation parameters:
    NS retransmit interval: 1000 ms
  ICMPv6 error message parameters:
    Send redirects: true
    Send unreachable: false

```

```
ICMPv6-nd Statistics (sent/received):
  RAs: 6/0, RSs: 0/0, NAs: 2/0, NSs: 7/0, RDs: 0/0
Interface statistics last reset: never
```

インターフェイスでの DHCP クライアントの設定

SVI、管理インターフェイス、または物理イーサネットインターフェイスで DHCP クライアントの IPv4 または IPv6 アドレスを設定できます。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **interface ethernet type slot/port | mgmt mgmt-interface-number | vlan vlan id**
3. switch(config-if)# **[no] ipv6 address use-link-local-only**
4. switch(config-if)# **[no] [ip | ipv6] address dhcp**
5. (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# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# interface ethernet type slot/port mgmt mgmt-interface-number vlan vlan id	物理イーサネットインターフェイス、管理インターフェイス、または VLAN インターフェイスを作成します。 vlan id の範囲は 1 ~ 4094 です。
ステップ 3	switch(config-if)# [no] ipv6 address use-link-local-only	DHCP サーバへの要求を準備します。 (注) このコマンドは、IPv6 アドレスの場合にのみ必要です。
ステップ 4	switch(config-if)# [no] [ip ipv6] address dhcp	DHCP サーバに IPv4 または IPv6 アドレスを要求します。 取得されたいずれかのアドレスを削除するには、このコマンドの no 形式を使用します。
ステップ 5	(任意) switch(config)# copy running-config startup-config	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーして、変更を継続的に保存します。

例

次に、SVIでDHCPクライアントのIPアドレスを設定する例を示します。

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

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

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

SVI およびサブインターフェイスの入力/出力ユニキャストカウンタの設定

Cisco NX-OS リリース 9.3(3) 以降では、SVI およびサブインターフェイスユニキャストカウンタが Cisco Nexus 9300-EX、9300-FX/FX2 スイッチ、および X9700-EX および X9700-FX ラインカードを搭載した Cisco Nexus 9500 シリーズ スイッチでサポートされています。Cisco NX-OS リリース 9.3(5) 以降では、SVI およびサブインターフェイスユニキャストカウンタが Cisco Nexus N9K-C9316D-GX、N9K-C93600CD-GX、N9K-C9364C-GX スイッチでサポートされています。



- (注) この機能を有効にすると、VxLAN、MPLS、トンネル、マルチキャスト、およびERSPANカウンターが無効になります。変更を有効にするために、スイッチをリロードしてください。



- (注) vPC セットアップでは、両方の vPC ピアの **vpc ドメイン** で **ピアゲートウェイ** 機能を有効にする必要があります。そうしないと、SVI カウンタが不整合になる可能性があります。

デバイスで SVI およびサブインターフェイスの入力/出力ユニキャストカウンタを設定するには、次の手順を実行します。

手順の概要

1. **configure terminal**
2. **[no] hardware profile svi-and-si flex-stats-enable**
3. **copy running-config startup-config**
4. **reload**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	[no] hardware profile svi-and-si flex-stats-enable 例： switch(config)# hardware profile svi-and-si flex-stats-enable switch(config-if)#	SVI およびサブインターフェイスの入力/出力ユニキャストカウンタを設定します。 (注) このコマンドを機能させるには、設定を保存し、スイッチをリロードする必要があります。
ステップ 3	copy running-config startup-config 例： switch(config-if)# copy running-config startup-config	この設定を保存します。
ステップ 4	reload 例： switch(config-if)# reload	スイッチをリロードします。

サブインターフェイスのマルチキャストおよびブロードキャストカウンタの設定

Cisco NX-OS リリース 9.3(6) 以降では、Cisco Nexus N9K-C9336C-FX2 および N9K-C93240YC-FX2 スイッチでサブインターフェイス マルチキャストおよびブロードキャストカウンタがサポートされています。

デバイスでマルチキャストおよびブロードキャストカウンタを設定するには、次の手順を実行します。

手順の概要

1. **configure terminal**
2. **[no] hardware profile sub-interface flex-stats**
3. **copy running-config startup-config**
4. **reload**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	[no] hardware profile sub-interface flex-stats 例： switch(config)# hardware profile sub-interface flex-stats switch(config-if)#	マルチキャストおよびブロードキャストカウンタのサブインターフェイスのフレックス統計情報を有効にします。
ステップ 3	copy running-config startup-config 例： switch(config-if)# copy running-config startup-config	この設定を保存します。
ステップ 4	reload 例： switch(config-if)# reload	スイッチをリロードします。

例

次に、show interface counters コマンドの結果として、サブインターフェイスのマルチキャストカウンタとブロードキャストカウンタを表示する例を示します。

```
switch(config)# show int ethernet 1/31/4.1 counters
```

```
-----
Port                               InOctets                               InUcastPkts
-----
Eth1/31/4.1                         0                                       0
```

```
-----
Port                               InMcastPkts                             InBcastPkts
-----
Eth1/31/4.1                         0                                       0
```

```
-----
Port                               InIPv4Octets                             InIPv4UcastPkts
-----
Eth1/31/4.1                         0                                       0
```

```
-----
Port                               InIPv4McastPkts                         InIPv4BcastPkts
-----
Eth1/31/4.1                         0                                       0
```

```
-----
Port                               InIPv6Octets                             InIPv6UcastPkts
-----
Eth1/31/4.1                         0                                       0
```

Port	InIPv6McastPkts	InIPv6BcastPkts
Eth1/31/4.1	0	0

Port	OutOctets	OutUcastPkts
Eth1/31/4.1	0	0

Port	OutMcastPkts	OutBcastPkts
Eth1/31/4.1	0	0

Port	OutIPv4Octets	OutIPv4UcastPkts
Eth1/31/4.1	0	0

Port	OutIPv4McastPkts	OutIPv4BcastPkts
Eth1/31/4.1	0	0

Port	OutIPv6Octets	OutIPv6UcastPkts
Eth1/31/4.1	0	0

Port	OutIPv6McastPkts	OutIPv6BcastPkts
Eth1/31/4.1	0	0

ハードウェア転送 IPv4/IPv6 インターフェイス統計情報の設定

Cisco NX-OS リリース 10.1(1) 以降では、**ipIfStatsTable** が SNMP を通じてポーリングされるときに、ハードウェア転送された IPv4/IPv6 インターフェイス統計情報（インターフェイス IPv4 および IPv6 Rx および Tx パケットとバイトカウンタ）をデバイスがエクスポートできるように、**hardware forwarding ip statistics** コマンドを使用できます。デフォルトでは、Cisco NX-OS は、SUP CPU で実行されている IPv4/IPv6 Netstack ソフトウェアによって転送されるパケットの IPv4/IPv6 インターフェイスカウンタのみをエクスポートします。

Cisco NX-OS リリース 10.1(1) 以降では、IPv4/IPv6 MIB サポートは、N9K-X9736C-FX、N9K-X9736Q-FX、N9K-X9788TC-FX、N9K-X9788TC2-FX、N9K-X97284YC-FX、N9K-C93180YC-FX、N9K-C93180YC2-FX、N9K-C93108TC-FX、N9K-C93108TC2-FX、N9K-X9732C-FX、N9K-C92348GC のプラットフォーム/ラインカードで利用できます。

サポートされているオブジェクト識別子（OID）は次のとおりです。

- ipIfStatsInReceives
- ipIfStatsOutTransmits
- ipIfStatsOutOctets

- ipIfStatsInOctets
- ipIfStatsHCInReceives
- ipIfStatsHCOutTransmits
- ipIfStatsHCOutOctets
- ipIfStatsHCInOctets

ハードウェア転送 IP インターフェイス統計情報機能には、次の制約事項があります。

- この機能は、サブインターフェイスが7つ以上ある物理インターフェイスでは機能しません。
- 指定された **ipIfStatsTable** カウンタは、前面パネルのイーサネットインターフェイスでのみサポートされます。
- サポートされている OID 以外のすべてのオブジェクト識別子 (OID) は、**ipIfStatsTable** でゼロに設定されます。
- カウンタをクリアまたはリセットするオプションはありません。
- スライスごとにサポートされる L3 物理インターフェイスの最大数は 62 です。

デバイスで **hardware forwarding ip statistics** を設定するには、次の手順を実行します。

手順の概要

1. **configure terminal**
2. **[no] hardware forwarding ip statistics**
3. **hardware access-list tcam region ing-ctacl 512**
4. **hardware access-list tcam region egr-ctacl 512**
5. **hardware access-list tcam region ing-racl 512**
6. **hardware access-list tcam region egr-racl 512**
7. **copy running-config startup-config**
8. **reload**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	グローバル 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	[no] hardware forwarding ip statistics 例 : <pre>switch(config)# hardware forwarding ip statistics</pre>	ハードウェア転送 IPv4/IPv6 インターフェイス統計情報を設定します。

	コマンドまたはアクション	目的
ステップ 3	hardware access-list tcam region ing-cntacl 512 例： switch(config)# hardware access-list tcam region ing-cntacl 512	ACL TCAM カービングと入力 IP または MAC ポート TCAM リージョンのサイズを設定します。
ステップ 4	hardware access-list tcam region egr-cntacl 512 例： switch(config)# hardware access-list tcam region egr-cntacl 512	ACL TCAM カービングと出力 IP または MAC ポート TCAM リージョンのサイズを設定します。
ステップ 5	hardware access-list tcam region ing-racl 512 例： switch(config)# hardware access-list tcam region ing-racl 512	入力 IP ルータの ACL (RACL) TCAM リージョンのサイズを設定します。
ステップ 6	hardware access-list tcam region egr-racl 512 例： switch(config)# hardware access-list tcam region egr-racl 512	出力 IP ルータの ACL (RACL) TCAM リージョンのサイズを設定します。
ステップ 7	copy running-config startup-config 例： switch(config)# copy running-config startup-config	この設定を保存します。
ステップ 8	reload 例： switch(config)# reload	スイッチをリロードします。

レイヤ3インターフェイス設定の確認

レイヤ3の設定を表示するには、次のいずれかの作業を行います。

コマンド	目的
show interface ethernet <i>slot/port</i>	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。
show interface ethernet <i>slot/port</i> brief	レイヤ3インターフェイスの動作ステータスを表示します。

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

コマンド	目的
show ip interface brief	インターフェイス アドレスとインターフェイスステータス (ナンバード/アンナンバード) を表示します。
show ip route	OSPF または ISIS を介して取得されたルートを表示します (最適なユニキャストおよびマルチキャスト ネクストホップのアドレスが含まれる)。

レイヤ3インターフェイスのモニタリング

レイヤ3 統計情報を表示するには、次のコマンドを使用します。

コマンド	目的
load- interval {interval seconds {1 2 3}}	Cisco Nexus 9000 シリーズ デバイスは、ビットレートおよびパケットレートの統計情報に3種類のサンプリング インターバルを設定します。 VLAN ネットワーク インターフェイスでの範囲は60～300秒であり、レイヤインターフェイスでの範囲は30～300秒です。
show interface ethernet slot/port counters	レイヤ3インターフェイスの統計情報を表示します (ユニキャスト、マルチキャスト、ブロードキャスト)。
show interface ethernet slot/port counters brief	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。
show interface ethernet errors slot/port detailed [all]	レイヤ3インターフェイスの統計情報を表示します。オプションとして、32ビットと64ビットのパケットおよびバイト カウンタ (エラーを含む) をすべて含めることができます。
show interface ethernet errors slot/port counters errors	レイヤ3インターフェイスの入力および出力エラーを表示します。
show interface ethernet errors slot/port counters snmp	SNMP MIB から報告されたレイヤ3インターフェイス カウンタを表示します。
show interface ethernet slot/port.number counters	サブインターフェイスの統計情報 (ユニキャスト、マルチキャスト、およびブロードキャスト) を表示します。

コマンド	目的
show interface port-channel <i>channel-id.number</i> counters	ポートチャネルサブインターフェイスの統計情報（ユニキャスト、マルチキャスト、およびブロードキャスト）を表示します。
show interface loopback <i>number</i> counters	ループバック インターフェイスの入力および出力カウンタ（ユニキャスト、マルチキャスト、およびブロードキャスト）を表示します。
show interface loopback <i>number</i> detailed [all]	ループバック インターフェイスの統計情報を表示します。オプションとして、32 ビットと 64 ビットの 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。
show interface loopback <i>number</i> counters errors	ループバック インターフェイスの入力および出力エラーを表示します。
show interface vlan <i>number</i> counters	VLAN インターフェイスの入力および出力カウンタ（ユニキャスト、マルチキャスト、およびブロードキャスト）を表示します。
show interface vlan <i>number</i> counters detailed [all]	VLAN インターフェイスの統計情報を表示します。オプションとして、レイヤ3 パケット およびバイト カウンタをすべて含めることができます（ユニキャストおよびマルチキャスト）。
show interface vlan <i>number</i> counters snmp	SNMP MIB から報告された VLAN インターフェイス カウンタを表示します。

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。

```
interface ethernet 2/1.10
description Layer 3
ip address 192.0.2.1/8
```

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。

```
interface loopback 3
ip address 192.0.2.2/32
```

インターフェイスの VRF メンバーシップ変更の例

- VRF メンバーシップを変更する場合はレイヤ3 設定の保持を有効にします。

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

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

- レイヤ3の保持を確認します。

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

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

- レイヤ3設定によってSVIインターフェイスをVRFの「blue」として設定します。

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

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

- SVIインターフェイスのVRFを「red」に変更します。

```
switch# configure terminal

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

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

- VRFの変更後にSVIインターフェイスを確認します。

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

```
interface Vlan2002
description TESTSVI
no shutdown
mtu 9192
vrf member red
no ip redirects
ip address 192.168.211.2/27
```

```

ipv6 address 2620:10d:c041:12::2/64
ipv6 link-local fe80::1
ip router ospf 1 area 0.0.0.0
ipv6 router ospfv3 1 area 0.0.0.0
hsrp version 2
hsrp 2002
preempt delay minimum 300 reload 600
priority 110 forwarding-threshold lower 1 upper 110
ip 192.168.211.1
hsrp 2002 ipv6
preempt delay minimum 300 reload 600
priority 110 forwarding-threshold lower 1 upper 110
ip 2620:10d:c041:12::1

```



(注)

• VRF を変更する場合、レイヤ3 設定の保持は次に影響します。

- 物理インターフェイス
- ループバック インターフェイス
- SVI インターフェイス
- サブインターフェイス
- トンネル インターフェイス
- ポート チャネル

• VRF を変更する場合、既存のレイヤ3 設定が削除され、再適用されます。すべてのルーティングプロトコル (OSPF/ISIS/EIGRP/HSRP) が古い VRF でダウンし、新しい VRF でアップします。

• ダイレクトおよびローカル IPv4/IPv6 アドレスが古い VRF から削除され、新しい VRF にインストールされます。

• VRF 変更時にトラフィック損失が発生する可能性があります。

関連資料

関連資料	マニュアル タイトル
IP	『Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide』
VLANs	『Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide』



第 6 章

双方向フォワーディング検出の設定

- [BFD について \(177 ページ\)](#)
- [BFD の前提条件 \(180 ページ\)](#)
- [注意事項と制約事項 \(180 ページ\)](#)
- [デフォルト設定 \(185 ページ\)](#)
- [BFD の設定 \(185 ページ\)](#)
- [ルーティングプロトコルに対する BFD サポートの設定 \(202 ページ\)](#)
- [BFD 相互運用性 \(214 ページ\)](#)
- [BFD 設定の確認 \(218 ページ\)](#)
- [BFD のモニタリング \(218 ページ\)](#)
- [BFD マルチホップ \(219 ページ\)](#)
- [BFD の設定例 \(223 ページ\)](#)
- [関連資料 \(224 ページ\)](#)
- [RFC \(224 ページ\)](#)

BFD について

BFD は、メディア タイプ、カプセル化、トポロジ、およびルーティングプロトコルの転送パス障害を高速で検出するように設計された検出プロトコルです。BFD を使用することで、さまざまなプロトコルの Hello メカニズムにより、変動速度ではなく一定速度で転送パス障害を検出できます。BFD はプロファイリングおよびプランニングを簡単にし、再コンバージェンス時間の一貫性を保ち、予測可能にします。

BFD は 2 台の隣接デバイス間のサブセカンド障害を検出し、BFD の負荷の一部を、サポートされるモジュール上のデータプレーンに分散できるため、プロトコル hello メッセージよりも CPU を使いません。

非同期モード

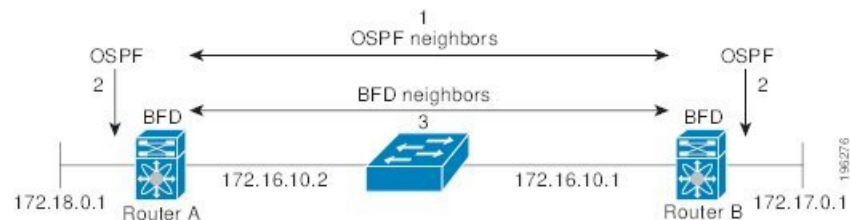
Cisco NX-OS は、BFD 非同期モードをサポートします。BFD 非同期モードでは、2 個の隣接するデバイス間で BFD 制御パケットが送信され、デバイス間の BFD ネイバーセッションがアクティベートされ、維持されます。両方のデバイス (または BFD ネイバー) で BFD を設定でき

まず、インターフェイスおよび適切なプロトコルで一度 BFD がイネーブルになると、Cisco NX-OS は BFD セッションを作成し、BFD セッション パラメータをネゴシエートし、BFD 制御パケットをネゴシエートされた間隔で各 BFD ネイバーに送信し始めます。BFD セッション パラメータは、次のとおりです。

- 目的の最小送信間隔：このデバイスが BFD Hello メッセージを送信する間隔。
- 必要最小受信間隔：このデバイスが別の BFD デバイスからの BFD Hello メッセージを受け付ける最小間隔。
- 検出乗数：転送パスの障害を検出するまでに喪失した、別の BFD デバイスからの BFD Hello メッセージの数。

次の図は、BFDセッションがどのように確立されているかを示します。この図は、Open Shortest Path First (OSPF) と BFD を実行する 2 台のルータがある単純なネットワークを示します。OSPF がネイバーを検出すると (1)、OSPF 隣接ルータで BFD ネイバー セッションを開始する要求が、ローカル BFD プロセスに送信されます (2)。OSPF ネイバー ルータとの BFD ネイバー セッションが確立されました (3)。

図 6: BFD ネイバー関係の確立



BFD の障害検出

一度 BFD セッションが確立され、タイマー ネゴシエーションが終了すると、BFD ネイバーは、より速い速度の場合を除き IGP Hello プロトコルと同じ動作をする BFD 制御パケットを送信し、活性度を検出します。BFD は障害を検出しますが、プロトコルが障害の発生したピアをバイパスするための処置を行う必要があります。

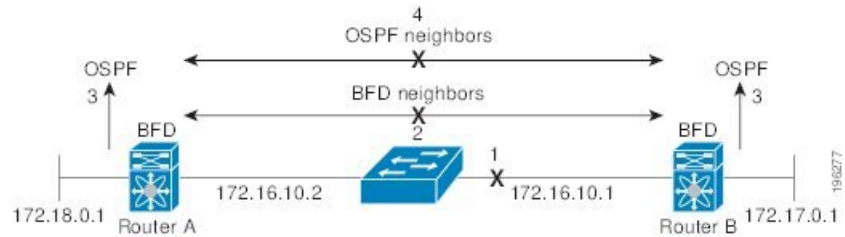
BFD は転送パスに障害を検出したとき、障害検出通知を BFD 対応プロトコルに送信します。ローカルデバイスは、プロトコル再計算プロセスを開始してネットワーク全体の収束時間を削減できます。

次の図は、ネットワークで障害が発生した場合を示します (1)。OSPF ネイバー ルータでの BFD ネイバー セッションが停止されます (2)。BFD はローカル OSPF プロセスに BFD ネイバーに接続できなくなったことを通知します (3)。ローカル OSPF プロセスは OSPF ネイバー関係を解除します (4)。代替パスが使用可能な場合、ルータはただちにそのパスでコンバージェンスを開始します。



(注) 注意: BFD 障害検出は 1 秒未満で行われます。これは OSPF Hello メッセージが同じ障害を検出するより速い必要があります。

図 7: OSPF ネイバー関係の解除



分散型動作

Cisco NX-OS は、BFD をサポートする互換性のあるモジュールへ BFD 動作を配布できます。このプロセスで、BFD パケット処理の CPU の負荷を、BFD ネイバーに接続された各モジュールへオフロードします。すべての BFD セッションはモジュール CPU 上で行われます。BFD 障害が検出されたときに、モジュールはスーパーバイザに通知します。

BFD エコー機能

エコー パケットは、送信側システムによってのみ定義および処理されます。IPv4 および IPv6 の場合、エコー パケットの宛先アドレスは送信側デバイスの宛先アドレスです。これは、リモートシステムがパケットをローカルシステムに転送するように選択されます。これにより、リモートシステムでのルーティング ルックアップはバイパスされ、代わりに転送情報ベース (FIB) が利用されます。BFD はエコー機能がイネーブルになっている場合に非同期セッションの速度を低下させ、2 台の BFD ネイバー間で送信される BFD 制御パケット数を減らすために、slow timer を使用できます。エコー機能は、リモート (ネイバー) システムにループバックさせることにより、リモートシステムの転送パスのみをテストします。パケット間遅延の変動が少なくなり、障害検出時間が短縮されます。

セキュリティ

Cisco NX-OS は BFD パケットを隣接する BFD ピアから受信したことを確認するためにパケットの存続可能時間 (TTL) 値を使用します。すべての非同期およびエコー要求パケットの場合、BFD ネイバーは TTL 値を 255 に設定し、ローカル BFD プロセスは着信パケットを処理する前に TTL 値を 255 として確認します。エコー応答パケットの場合、BFD は TTL 値を 254 に設定します。

BFD パケットの SHA-1 認証を設定できます。

高可用性

BFD は、ステートレス リスタートをサポートします。リブートまたはスーパーバイザ スイッチオーバー後に、Cisco NX-OS が実行コンフィギュレーションを適用し、BFD がただちに制御パケットを BFD ピアに送信します。

仮想化のサポート

BFD は、仮想ルーティングおよび転送 (VRF) インスタンスをサポートしています。VRF は仮想化デバイスコンテキスト (VDC) 内にあります。デフォルトでは、Cisco NX-OS はデフォルト VDC とデフォルト VRF に配置します。

BFD の前提条件

BFD には、次の前提条件があります。

- BFD機能をイネーブルにする必要があります。
- BFD 対応インターフェイスでインターネット制御メッセージプロトコル (ICMP) リダイレクトメッセージをディセーブルにします。
- 同一の IP 送信元アドレスおよび宛先アドレスを調べる IP パケット検証チェックをディセーブルにします。
- 設定作業とともに一覧表示されているその他の詳細な前提条件を参照してください。

注意事項と制約事項

BFD 設定時のガイドラインと制約事項は次のとおりです。

- QSFP 40/100-G BiDi は、ポートで使用可能な最高速度で起動します。たとえば、Cisco Nexus 93180LC-EX スイッチでは、最初の 28 ポートで 40 G、最後の 4 ポートで 100 G として起動します。40-G SR4 BiDi に接続する必要がある場合は、40/100-G BiDi の速度を 40 G に設定する必要があります。
- 孤立ポートを介した vPC VLAN での BFD ネイバーの形成は、Cisco Nexus 9000 スイッチではサポートされていません。
- Cisco NX-OS リリース 9.2 (1) 以降、QSFP-40 / 100-SRBD は 100-G の速度で起動し、N9K-X9636C-RX ラインカードを搭載した Cisco Nexus 9500 スイッチで 40-G または 100-G のいずれかの速度で他の QSFP-40 / 100-SRBD と相互運用します。QSFP-40 / 100-SRBD は、40G の速度で QSFP-40G-SR-BD と相互運用することもできます。ただし、40G の速度で動作するには、速度を 40G に設定する必要があります。
- キーワードが付いている **show** コマンドはサポートされていません。 **internal**
- Cisco Nexus 9000 シリーズ スイッチは、メンバー単位の BFD リンクをサポートします。
- メンバー単位の BFD リンクのサポートが Cisco Nexus 9000 シリーズ スイッチに追加されました。
- Cisco NX-OS リリース 9.3(3) BFD 以降では、次の Cisco Nexus スイッチでサポートされません。

- 9364C-GX
 - 9316D-GX
 - 93600CD-GX
- BFD は BFD バージョン 1 をサポートします。
 - BFD は IPv4 と IPv6 をサポートします。
 - BFD は OSPFv3 をサポートします。
 - BFD は IS-ISv6 をサポートします。
 - BFD は BGPv6 をサポートします。
 - BFD は EIGRPv6 をサポートします。
 - BFD は、レイヤ 3 インターフェイスごとのアドレス ファミリ 1 つにつき 1 セッションだけサポートします。
 - BFD は、一意の (src_ip、dst_ip、interface/vrf) の組み合わせを持つセッションのみをサポートします。
 - BFD は、シングルホップ BFD をサポートします。
 - シングルホップ静的 BFD のみがサポートされます。
 - ボーダー ゲートウェイ プロトコル (BGP) の BFD は、シングルホップ External BGP (EBGP) および Internal BGP (iBGP) ピアをサポートしています。
 - BFD は、キー付き SHA-1 認証をサポートします。
 - BFD は、レイヤ 3 インターフェイスとして、物理インターフェイス、ポート チャネル、サブインターフェイス、および VLAN インターフェイスをサポートします。
 - BFD はレイヤ 3 隣接情報に応じて、レイヤ 2 のトポロジ変更を含むトポロジ変更を検出します。レイヤ 3 隣接情報が使用できない場合、VLAN インターフェイス (SVI) の BFD セッションはレイヤ 2 トポロジのコンバージェンス後に稼働しない可能性があります。
 - 2 台のデバイス間のスタティックルート上の BFD については、両方のデバイスが BFD をサポートする必要があります。デバイスの一方または両方が BFD をサポートしていない場合、スタティックルートはルーティング情報ベース (RIB) でプログラミングされません。
 - シングルホップとマルチホップの両方の BFD 機能は、特定の制限付きでサポートされます。マルチホップ BFD 機能の制限については、セクションを参照してください。
 - ポート チャネル設定の制限事項
 - BFD で使用されるレイヤ 3 ポート チャネルでは、ポート チャネルの LACP をイネーブルにする必要があります。

- SVI のセッションで使用されるレイヤ 2 ポート チャネルでは、ポート チャネルの LACP をイネーブルにする必要があります。
 - SVI の制限事項
 - ASIC のリセットにより、他のポートのトラフィックが中断され、他のポートでの SVI セッションがフラップする可能性があります。たとえば、キャリアインターフェイスが仮想ポートチャネル (vPC) の場合、BFD は SVI インターフェイスではサポートされず、ASIC のトリガーをリセットする可能性があります。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。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。
- Cisco Nexus シリーズ スイッチの SVI は、vPC を介して接続されたデバイスとの BFD ネイバー隣接関係を確立するように設定しないでください。これは、ネイバーからの BFD キープアライブが、vPC ピア スイッチに接続された vPC メンバーリンクを介して送信された場合、この SVI に到達せず、BFD 隣接関係が機能不全になるためです。
- トポロジを変更すると (たとえば、VLAN へのリンクの追加または削除、レイヤ 2 ポートチャネルからのメンバの削除など)、SVI セッションが影響を受ける場合があります。SVI セッションはダウンした後、トポロジディスカバリの終了後に起動する場合があります。
 - BEX over FEX HIF インターフェイスはサポートされていません。
 - 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 (BCM または GEM いずれかのベースのポート)、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** コマンドを使用して、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。



ヒント SVI のセッションがフラップしないようにし、トポロジを変更する必要がある場合は、変更を加える前に BFD 機能を無効にし、変更後、BFD を再度有効にすることができます。また、大きな値 (たとえば、5 秒) になるように BFD タイマーを設定し、上記のイベントの完了後に高速なタイマーに戻すこともできます。

- 分散レイヤ 3 ポートチャネルで BFD エコー機能を設定した場合、メンバーモジュールをリロードすると、そのモジュールでホストされた BFD セッションがフラップされ、そのためパケット損失が発生します。

レイヤ 2 スイッチを間に入れずに BFD ピアを直接接続する場合、代替策として BFD per-link を使用できます。



(注) BFD per-link モードとサブインターフェイス最適化をレイヤ3ポートチャンネルで同時に使用することはサポートされていません。

- **clear {ip | ipv6} route prefix** コマンドで BFD ネイバーにプレフィックスを指定すると、BFD エコーセッションがフラップします。
- **clear {ip | ipv6} route *** コマンドにより、BFD エコーセッションがフラップします。
- IPv4 に対する HSRP は、BFD でサポートされます。
- Cisco NX-OS デバイスのラインカードによって生成される BFD パケットは COS 6/DSCP CS6 とともに送信されます。BFD パケットの DSCP/COS 値は、ユーザが設定可能な値ではありません。
- no-bfd-echo モードで BFDv6 を設定する場合は、乗数3のタイマー150ms で実行することを推奨します。
- BFDv6 は、v6 の VRRPv3 および HSRP ではサポートされません。
- インターフェイスで IPv6 **igrp bfd** を無効にすることはできません。
- IETF BFD は、N9K-X96136YC-R、N9K-X9636C-R、N9K-X9636C-RX、および N9K-X9636Q-R ラインカードではサポートされません。
- ポートチャンネル設定の注意事項：
 - BFD per-link モードが設定されている場合、BFD エコー機能はサポートされません。コマンドを設定する前に、**no bfd echo** コマンドを使用して BFD エコー機能をディセーブルにする必要があります。**bfd per-link**
 - BFD リンクごとに設定する前に、BFD セッションがポートチャンネルで実行されていないことを確認します。すでに実行中の BFD セッションがある場合は、それを削除してから bfd リンクごとの設定に進みます。
 - リンクローカルでのリンクごとの BFD の設定はサポートされていません。
 - サポートされているプラットフォームには、N9K-X9636C-R、N9K-X9636Q-R、N9K-X9636C-RX ラインカードを搭載した Cisco Nexus 9500 シリーズスイッチがあります。
- Cisco NX-OS リリース 9.3(7) 以降では、アンナンバードインターフェイスで BFD がサポートされます。



(注) アンナンバード スイッチド 仮想インターフェイス (SVI) を介した BFD はサポートされていません。

アンナンバード インターフェイス サポートでの BFD のダウングレードの互換性は、**show incompatibility nxos bootflash:filename** コマンドを使用して確認することはできません。**install all** コマンドの実行中に互換性がチェックされます。

- OSPF とともに番号付きインターフェイスで BFD を設定し、インターフェイスを番号なしインターフェイスに変換すると、OSPF および BFD コマンドは実行コンフィギュレーションに残りますが、BFD 機能が動作しない場合があります。
- 次の BFD コマンド設定は、設定の置換ではサポートされていません。
 - **port-channel bfd track-member-link**
 - **port-channel bfd destination destination-ip-address**
- 1024 を超えるセッションを設定する場合は、BFD ハードウェア レトリミッタ (25000 kbps) 、および BFD スタートアップ タイマーの範囲を 0~60 秒に設定することを推奨します。この機能は、Cisco Nexus 9300-EX、9300-FX、9300-FX2、9300-FX3 および 9300-GX プラットフォーム スイッチでサポートされます。
- Cisco Nexus 9800 プラットフォーム スイッチには、BFD IPv6 セッションに対して次の制限があります。
 - ラインカードのスーパーバイザ スイッチ モードの各 ASIC ユニットの、最大 256 の BFD IPv6 セッションをサポートします。より多くの BFD IPv6 セッションが必要な場合は、セッションを ASIC ユニットの全体に分散させる必要があります。
- Cisco NX-OS リリース 10.3(1)F 以降、BFD は Cisco Nexus 9808 プラットフォーム スイッチのルーテッドポート、ルーテッドサブインターフェイス、およびブレイクアウトポートでシングルホップ BFD をサポートします。
- Cisco NX-OS リリース 10.4(1)F 以降、BFD は Cisco Nexus 9804 プラットフォーム スイッチのルーテッドポート、ルーテッドサブインターフェイス、およびブレイクアウトポートでシングルホップ BFD をサポートします。
- Cisco NX-OS リリース 10.4(2)F 以降では、Cisco Nexus C9232E-B1 スイッチに以下が適用されます。
 - ルーテッドポート、ルーテッドサブインターフェイス、およびブレイクアウトポートでのシングルホップ BFD がサポートされます。
 - BFD 認証はサポートされていません。
- BFD 認証は、Cisco Nexus 9800 プラットフォーム スイッチではサポートされません。

- Cisco NX-OS リリース 10.4(1)F 以降、BFD は、Cisco Nexus 9808 および 9804 スイッチに搭載されている N9KX98900CD-A および N9KX9836DM-A ライン カードでシングルホップ BFD をサポートします。

デフォルト設定

次の表に、BFD パラメータのデフォルト設定を示します。

表 11: デフォルトの BFD パラメータ

パラメータ	デフォルト
BFD 機能	ディセーブル
必要最小受信間隔	50 ミリ秒
目的の最小送信間隔	50 ミリ秒
検出乗数	3
エコー機能	イネーブル
モード	非同期
ポート チャネル	論理モード (送信元/宛先ペアのアドレスごとに 1 セッション)
slow timer	2000 ミリ秒
起動タイマー	5 秒

BFD の設定

設定階層

グローバル レベルおよびインターフェイス レベルで BFD を設定できます。インターフェイス設定はグローバル設定よりも優先されます。

ポート チャネルのメンバである物理ポートについては、メンバポートはプライマリポートチャネルの BFD 設定を継承します。

BFD 設定のタスク フロー

BFD を設定するには、以下の項にある次の手順に従います。

- BFD 機能のイネーブル化
- グローバルな BFD パラメータを設定またはインターフェイスでの BFD の設定

BFD 機能のイネーブル化

インターフェイスとプロトコルの BFD を設定する前に、BFD 機能をイネーブルにする必要があります。



(注) **no feature bfd** コマンドを使用して、BFD 機能をディセーブルにし、関連するコンフィギュレーションをすべて削除します。

コマンド	目的
no feature bfd 例： switch(config)# no feature bfd	BFD 機能をディセーブルにして、関連するすべての設定を削除します。

手順の概要

1. **configure terminal**
2. **feature bfd**
3. **show feature | include bfd**
4. **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	configure terminal 例： switch# configure terminal switch(config)#	コンフィギュレーションモードに入ります。
ステップ 2	feature bfd 例： switch(config)# feature bfd	BFD 機能をイネーブルにします。
ステップ 3	show feature include bfd 例： switch(config)# show feature include bfd	(任意) イネーブルおよびディセーブルにされた機能を表示します。

	コマンドまたはアクション	目的
ステップ 4	copy running-config startup-config 例： <pre>switch(config)# copy running-config startup-config</pre>	(任意) この設定の変更を保存します。

グローバルな BFD パラメータの設定

デバイスのすべての BFD セッションの BFD セッションパラメータを設定できます。BFD セッションパラメータは、スリーウェイ ハンドシェイクの BFD ピア間でネゴシエートされます。

インターフェイスでこれらのグローバルなセッションパラメータを上書きするには、「インターフェイスでの BFD の設定」の項を参照してください。

始める前に

BFD 機能をイネーブルにします。

手順の概要

1. **configure terminal**
2. **bfd interval *mintx* *min_rx* *msec* *multiplier* *value***
3. **bfd slow-timer [*interval*]**
4. **[no] bfd startup-timer [*seconds*]**
5. **bfd echo-interface loopback *interface number***
6. **show running-config bfd**
7. **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	configure terminal 例： <pre>switch# configure terminal switch(config)#</pre>	コンフィギュレーション モードに入ります。
ステップ 2	bfd interval <i>mintx</i> <i>min_rx</i> <i>msec</i> <i>multiplier</i> <i>value</i> 例： <pre>switch(config)# bfd interval 50 min_rx 50 multiplier 3</pre>	デバイスのすべての BFD セッションの BFD セッションパラメータを設定します。インターフェイスで BFD セッションパラメータを設定することにより、このコマンドでこれらの値を無効にすることができます。 <i>mintx</i> および <i>msec</i> の範囲は 50 ~ 999 ミリ秒で、デフォルトは 50 です。乗数の範囲は 1 ~ 50 です。乗数のデフォルトは 3 です。

	コマンドまたはアクション	目的
ステップ 3	bfd slow-timer [<i>interval</i>] 例： <pre>switch(config)# bfd slow-timer 2000</pre>	エコー機能で使用される slow timer を設定します。この値はエコー機能がイネーブルの場合、BFD が新しいセッションを開始する速度および非同期セッションが BFD 制御パケットに使用する速度を決定します。 slow-timer 値は新しい制御パケット間隔として使用されますが、エコーパケットは設定された BFD 間隔を使用します。エコーパケットはリンク障害検出に使用されますが、低速の制御パケットは BFD セッションを維持します。指定できる範囲は 1000 ~ 30000 ミリ秒です。デフォルトは 2000 です。
ステップ 4	[no] bfd startup-timer [<i>seconds</i>] 例： <pre>switch(config)# bfd startup-timer 20</pre>	BFD 起動タイマーを設定します。BFD 起動タイマーは、BFD セッションの起動時間を遅らせることにより、ローカルおよびリモートルータで使用されているルートがハードウェアに固定されるまでの時間を作ります。この機能を使用すると、より大規模なシナリオで BFD のフラップを防止できます。範囲は 0 ~ 30 秒です。デフォルトは 5 秒です。 bfd startup-timer 0 コマンドは、BFD 起動タイマーをディセーブルにします。 no bfd startup-timer コマンドは、BFD 起動タイマーを 5 秒（デフォルト値）に設定します。
ステップ 5	bfd echo-interface loopback <i>interface number</i> 例： <pre>switch(config)# bfd echo-interface loopback 1 3</pre>	双方向フォワーディング検出（BFD）のエコーフレームに使用するインターフェイスを設定します。このコマンドは、指定されたループバックインターフェイスで設定されるアドレスに、エコーパケットの送信元アドレスを変更します。指定できるインターフェイス番号の範囲は 0 ~ 1023 です。
ステップ 6	show running-config bfd 例： <pre>switch(config)# show running-config bfd</pre>	（任意）BFD 実行コンフィギュレーションを表示します。
ステップ 7	copy running-config startup-config 例： <pre>switch(config)# copy running-config startup-config</pre>	（任意）この設定の変更を保存します。

インターフェイス上での BFD の設定

インターフェイスのすべての BFD セッションの BFD セッションパラメータを設定できます。BFD セッションパラメータは、スリーウェイ ハンドシェイクの BFD ピア間でネゴシエートされます。

この設定は、設定されたインターフェイスのグローバルセッションパラメータより優先されます。

始める前に

インターネット制御メッセージプロトコル (ICMP) のリダイレクトメッセージが BFD 対応インターフェイスでディセーブルであることを確認します。インターフェイスで **no ip redirects** コマンドまたは **no ipv6 redirects** コマンドを使用します。

BFD 機能をイネーブルにします。「BFD 機能のイネーブル化」を参照してください。

手順の概要

1. **configure terminal**
2. **interface int-if**
3. **bfd interval mintx min_rx msec multiplier value**
4. **bfd authentication keyed-sha1 keyid id key ascii_key**
5. **show running-config bfd**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	コンフィギュレーション モードに入ります。
ステップ 2	interface int-if 例 : <pre>switch(config)# interface ethernet 2/1 switch(config-if)#</pre>	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。? キーワードを使用して、サポートされるインターフェイスを表示します。
ステップ 3	bfd interval mintx min_rx msec multiplier value 例 : <pre>switch(config-if)# bfd interval 50 min_rx 50 multiplier 3</pre>	デバイスのすべての BFD セッションの BFD セッションパラメータを設定します。インターフェイスで BFD セッションパラメータを設定することにより、このコマンドでこれらの値を無効にすることができます。mintx および msec の範囲は 50 ~ 999 ミリ秒で、デフォルトは 50 です。乗数の範囲は 1 ~ 50 です。乗数のデフォルトは 3 です。

	コマンドまたはアクション	目的
		<p>Cisco NX-OS Release 9.3(5) 以降では、bfd interval 50 min_rx 50 multiplier 3 コマンドを使用してデフォルトのタイマー値を使用してインターフェイスで BFD セッションパラメータを設定することは、no bfd interval コマンドと機能的に同等です。</p> <p>インターフェイスの BFD セッションパラメータがデフォルト値に設定されると、そのインターフェイスで実行されている BFD セッションは、グローバルセッションパラメータを継承します（存在する場合）。</p>
<p>ステップ 4</p>	<p>bfd authentication keyed-sha1 keyid id key ascii_key</p> <p>例 :</p> <pre>switch(config-if)# bfd authentication keyed-sha1 keyid 1 ascii_key cisco123</pre>	<p>（任意）インターフェイス上のすべての BFD セッションの SHA-1 認証を設定します。<i>ascii_key</i> 文字列は BFD ピア間で共有される秘密キーです。0 ~ 255 の数値の <i>id</i> 値が、この特定の <i>ascii_key</i> に割り当てられます。BFD パケットは <i>id</i> でキーを指定し、複数のアクティブキーが使用できます。</p> <p>インターフェイスの SHA-1 認証を無効にするには、コマンドの no 形式を使用します。</p>
<p>ステップ 5</p>	<p>show running-config bfd</p> <p>例 :</p> <pre>switch(config-if)# show running-config bfd</pre>	<p>（任意）BFD 実行コンフィギュレーションを表示します。</p>
<p>ステップ 6</p>	<p>copy running-config startup-config</p> <p>例 :</p> <pre>switch(config-if)# copy running-config startup-config</pre>	<p>（任意）この設定の変更を保存します。</p>

ポートチャネルの BFD の設定

ポートチャネルのすべての BFD セッションの BFD セッションパラメータを設定できます。パーリンクモードがレイヤ 3 ポートチャネルに使用される場合、BFD により、ポートチャネルの各リンクのセッションが作成され、集約結果がクライアントプロトコルへ提供されます。たとえば、ポートチャネルの 1 つのリンクの BFD セッションが稼働している場合、OSPF などのクライアントプロトコルにポートチャネルが稼働していることが通知されます。BFD セッションパラメータは、スリーウェイハンドシェイクの BFD ピア間でネゴシエートされます。

この設定は、設定されたポートチャネルのグローバルセッションパラメータより優先されます。ポートチャネルのメンバポートは、ポートチャネルの BFD セッションパラメータを継承します。

始める前に

BFD をイネーブルにする前に、ポートチャネルの Link Aggregation Control Protocol (LACP) がイネーブルにされていることを確認します。

インターネット制御メッセージプロトコル (ICMP) のリダイレクトメッセージが BFD 対応インターフェイスでディセーブルであることを確認します。インターフェイスで **no ip redirects** コマンドを使用します。

BFD 機能をイネーブルにします。「BFD 機能のイネーブル化」を参照してください。

手順の概要

1. **configure terminal**
2. **interface port-channel *number***
3. **bfd per-link**
4. **bfd interval *mintx min_rx msec multiplier value***
5. **bfd authentication keyed-sha1 keyid *id key ascii_key***
6. **show running-config bfd**
7. **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	configure terminal 例： <pre>switch# configure terminal switch(config)#</pre>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface port-channel <i>number</i> 例： <pre>switch(config)# interface port-channel 2 switch(config-if)#</pre>	ポートチャネル コンフィギュレーション モードを開始します。? キーワードを使用して、サポートされる数値の範囲を表示します。
ステップ 3	bfd per-link 例： <pre>switch(config-if)# bfd per-link</pre>	ポートチャネルのリンクごとに BFD セッションを設定します。
ステップ 4	bfd interval <i>mintx min_rx msec multiplier value</i> 例： <pre>switch(config-if)# bfd interval 50 min_rx 50 multiplier 3</pre>	(任意) ポートチャネルのすべての BFD セッションの BFD セッションパラメータを設定します。BFD セッションパラメータを設定することにより、このコマンドでこれらの値を無効にすることができます。 <i>mintx</i> および <i>msec</i> の範囲は 50 ~ 999 ミリ秒で、デフォルトは 50 です。乗数の範囲は 1 ~ 50 です。乗数のデフォルトは 3 です。
ステップ 5	bfd authentication keyed-sha1 keyid <i>id key ascii_key</i> 例：	(任意) インターフェイス上のすべての BFD セッションの SHA-1 認証を設定します。 <i>ascii_key</i> 文字列

	コマンドまたはアクション	目的
	<code>switch(config-if)# bfd authentication keyed-sha1 keyid 1 ascii_key cisco123</code>	は BFD ピア間で共有される秘密キーです。0 ~ 255 の数値の <i>id</i> 値が、この特定の <i>ascii_key</i> に割り当てられます。BFD パケットは <i>id</i> でキーを指定し、複数のアクティブ キーが使用できます。 インターフェイスの SHA-1 認証を無効にするには、コマンドの no 形式を使用します。
ステップ 6	show running-config bfd 例： <code>switch(config-if)# show running-config bfd</code>	(任意) BFD 実行コンフィギュレーションを表示します。
ステップ 7	copy running-config startup-config 例： <code>switch(config-if)# copy running-config startup-config</code>	(任意) この設定の変更を保存します。

BFD エコー機能の設定

BFD モニタ対象リンクの一端または両端で BFD エコー機能を設定できます。エコー機能は設定された *slow timer* に基づいて必要最小受信間隔を遅くします。RequiredMinEchoRx BFD セッションパラメータは、エコー機能が RFC 5880 に準拠して無効の場合、ゼロに設定されます。*slow timer* は、エコー機能がイネーブルの場合、必要最小受信間隔になります。

始める前に

BFD 機能をイネーブルにします。「BFD 機能のイネーブル化」を参照してください。

BFD セッションパラメータを設定します。「グローバルな BFD パラメータの設定」の項または「インターフェイスでの BFD の設定」の項を参照してください。

インターネット制御メッセージプロトコル (ICMP) のリダイレクトメッセージが BFD 対応インターフェイスでディセーブルであることを確認します。インターフェイスで **no ip redirects** コマンドを使用します。

同一の送信元アドレスおよび宛先アドレスを調べる IP パケット検証チェックがディセーブルになっていることを確認します。 **no hardware ip verify address identical** コマンドを使用します。このコマンドの詳細については、『Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide』を参照してください。

手順の概要

1. **configure terminal**
2. **bfd slow-timer echo-interval**
3. **interface int-if**
4. **bfd echo**

- 5. `show running-config bfd`
- 6. `copy running-config startup-config`

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： <pre>switch# configure terminal switch(config)#</pre>	コンフィギュレーション モードに入ります。
ステップ 2	bfd slow-timer echo-interval 例： <pre>switch(config)# bfd slow-timer 2000</pre>	エコー機能で使用する <code>slow timer</code> を設定します。この値は BFD が新しいセッションを開始する速度を決定し、BFD エコー機能がイネーブルの場合に非同期セッションの速度を低下させるために使用されます。この値は、エコー機能がイネーブルの場合、必要最小受信間隔より優先されます。指定できる範囲は 1000 ~ 30000 ミリ秒です。デフォルトは 2000 です。
ステップ 3	interface int-if 例： <pre>switch(config)# interface ethernet 2/1 switch(config-if)#</pre>	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。? キーワードを使用して、サポートされるインターフェイスを表示します。
ステップ 4	bfd echo 例： <pre>switch(config-if)# bfd echo</pre>	エコー機能をイネーブルにします。デフォルトではイネーブルになっています。
ステップ 5	show running-config bfd 例： <pre>switch(config-if)# show running-config bfd</pre>	(任意) BFD 実行コンフィギュレーションを表示します。
ステップ 6	copy running-config startup-config 例： <pre>switch(config-if)# copy running-config startup-config</pre>	(任意) この設定の変更を保存します。

メンバー単位リンク BFD セッションの設定

メンバー単位の BFD リンクのサポートが Cisco Nexus 9000 シリーズ スイッチに追加されました。詳細については、次の項を参照してください。

リンク単位の効率化に対処するための BFD 拡張機能

IETF Micro BFD と呼ばれるリンク単位の効率化機能に対処するための双方向転送 (BFD) 拡張機能を使用すれば、すべてのリンク集約グループ (LAG) メンバー インターフェイス (RFC 7130 で規定されている) 上で個別の BFD セッションを設定することができます。

この拡張機能により、BFD セッションはポートチャネルの各メンバーリンク上で動作します。BFD がリンク障害を検出すると、そのメンバーリンクが転送テーブルから削除されます。BFD セッションは個別のポートチャネルインターフェイス上で作成されるため、このメカニズムが迅速な障害検出を可能にします。

ポートチャネルのメンバーリンクで実行されている BFD セッションは、マイクロ BFD セッションと呼ばれます。ユーザは、メインポートチャネルインターフェイス経由で RFC 7130 BFD を設定できます。このインターフェイスでは、メンバーごとに 1 つずつのマイクロ BFD セッションを使用することにより LAG 経由の帯域幅モニタリングが実行されます。メンバーポートのいずれかがダウンすると、そのポートが転送テーブルから削除されます。これにより、そのメンバー上のトラフィックの破損が回避されます。

マイクロ BFD セッションは、LACP ベースポートチャネルと非 LACP ベースポートチャネルの両方でサポートされます。マイクロ BFD セッションの設定方法の詳細については、「マイクロ BFD セッションの設定」のトピックを参照してください。

IETF 双方向フォワーディング検出の制限事項

IETF 双方向フォワーディング検出の次の制限事項を確認してください。

- BFD の制限事項
 - 論理ポートチャネルまたは独自の BFD メンバ単位リンクを介して BFD と共存することはできません。PC で BFD IETF IPv4 が設定されている場合、BFD IPv6 の論理/独自リンク単位セッションもサポートされません。
 - いずれかのルーティングプロトコルで論理 BFD セッションを設定する場合は、どの IETF ポートチャネルにも適用されないようにしてください。同じポートチャネルに論理設定と IETF 設定の両方を設定すると、ISSU/リロード時に未定義の動作が発生します。
 - IETF BFD IPv6 はサポートされていません。
 - エコー機能は、マイクロ BFD セッションではサポートされません。
 - ポートチャネルインターフェイスは、BFD セッションを実行している 2 台のスイッチ (ピアデバイス) 間で直接接続されるべきです。中間のレイヤ 2 スイッチは想定されていません。
- EthPCM/LACP の制限事項
 - LACP ポートチャネルのメンバーがホットスタンバイ状態で、アクティブリンクの 1 つで BFD 障害が発生した場合は、ホットスタンバイリンクが直接起動しない可能性があります。BFD 障害が発生したアクティブリンクがダウンすると、ホットスタ

ンバイメンバーがアクティブになります。ただし、ポートチャネルの最小リンク条件がヒットした場合、ホットスタンバイリンクが起動する前にポートチャネルがダウンするのを防ぐことはできません。

- 一般的な制限事項
 - レイヤ 3 ポートチャネルでのみサポートされます。
 - 以下ではサポートされていません。
 - vPC
 - レイヤ 3 サブインターフェイス
 - レイヤ 2 ポートチャネル/レイヤ 2 ファブリックパス
 - FPC/HIF PC
 - レイヤ 3 サブインターフェイス
 - ポートチャネル上の SVI

IETF メンバー単位セッションの移行/設定のガイドライン：

IETF メンバー単位セッションの移行/設定については、次のガイドラインを確認してください。

- ポートチャネル サブインターフェイス (RFC 7130 を実行できない) 上でルーティングプロトコルを使用して作成された論理 BFD セッションは引き続きサポートされます。ただし、メイン ポートチャネル インターフェイスは、共存する論理セッションと RFC 7130 セッションの両方をサポートしません。いずれかのみをサポートできます。
- ユーザは、メイン ポートチャネル インターフェイス経由で RFC 7130 BFD を設定できます。このインターフェイスでは、メンバーごとに 1 つずつのマイクロ BFD セッションを使用することにより LAG 経由の帯域幅モニタリングが実行されます。いずれかのメンバーポートがダウンすると、BFD はポートチャネル マネージャにそのポートを通知し、ポートチャネル マネージャは LTL からポートを削除することで、そのメンバーのトラフィックのブラックホール化を防止します。
- ポートチャネルをアップにするために必要なリンクの最小数が満たされていない場合は、ポートチャネル マネージャがポートチャネルをダウンにします。これにより、ポートチャネル サブインターフェイスが設定されている場合にポートチャネル サブインターフェイスがダウンし、ルーティングプロトコルを通知する論理 BFD セッションもダウンします。
- メイン ポートチャネル インターフェイス上で設定された RFC 7130 を使用している場合、論理 BFD セッションは、アグレッシブ タイマーを RFC 7130 BFD セッションより弱くして実行する必要があります。ポートチャネル インターフェイスに RFC 7130 を設定することも、ポートチャネル サブインターフェイスの論理 BFD セッションと組み合わせて設定することもできます。

- 独自のリンク単位が設定されている場合、ポートチャネルで IETF Micro-BFD セッションを有効にすることはできません。その逆も同様です。独自のリンク単位の設定を削除する必要があります。独自のリンク単位の現在の実装では、アプリケーションによってブートストラップされる（リンクごとではない）BFDセッションがある場合、設定を変更できません。各アプリケーションの BFD トラッキングを削除し、リンクごとの設定を削除する必要があります。独自のリンク単位から IETF Micro-BFD への移行パスは次のとおりです。

- アプリケーションの BFD 設定を削除します。
- リンク単位の設定を削除します。
- IETF Micro-BFD コマンドを有効にします。
- アプリケーションで BFD を有効にします。

メインのポートチャネルインターフェイスでは、独自の BFD から IETF Micro-BFD に移行するのに、同じパスをたどることができます。

ポートチャネルインターフェイスの設定

始める前に

BFD 機能が有効になっていることを確認します。

手順の概要

1. `switch(config)# interface port-channel port-number`
2. `switch(config-if)# no switchport`

手順の詳細

ステップ 1 `switch(config)# interface port-channel port-number`

インターフェイスのポートチャネルを設定します。

ステップ 2 `switch(config-if)# no switchport`

インターフェイスをレイヤ 3 ポートチャネルとして設定します。

次のタスク

- BFD スタートタイマーの設定
- IETF リンク単位の BFD

(任意) BFD スタート タイマーの設定

BFD 開始タイマーを設定するには、次の手順を実行します。

手順の概要

1. `switch(config-if)# port-channel bfd start 60`

手順の詳細

```
switch(config-if)# port-channel bfd start 60
```

ポート チャネルの BFD 開始タイマーを設定します。

- (注) デフォルト値は無限です (つまり、タイマーは動作していません)。ポート チャネルの BFD 開始タイマー値の範囲は 60 ~ 3600 秒です。開始タイマーを動作させるためには、開始タイマーの値を、ポート チャネル BFD 設定を完了する前 (つまり、`port-channel bfd track-member-link` と `port-channel bfd destination` をアクティブ メンバーとのレイヤ 3 ポート チャネル インターフェイス用に設定する前) に設定します。

次のタスク

- IETF リンク単位の BFD
- BFD 宛先 IP アドレスの設定

IETF リンク単位の BFD

手順の概要

1. `switch(config-if)# port-channel bfd track-member-link`

手順の詳細

```
switch(config-if)# port-channel bfd track-member-link
```

ポート チャネル インターフェイス上で IETF BFD を有効にします。

次のタスク

- BFD 宛先 IP アドレスの設定
- マイクロ BFD セッションの設定の確認

BFD 宛先 IP アドレスの設定

次の手順を実行して、BFD 宛先 IP アドレスを設定します。

手順の概要

1. `switch(config-if)# port-channel bfd destinationip-address`

手順の詳細

```
switch(config-if)# port-channel bfd destinationip-address
```

メンバー リンク上の BFD セッションに使用される IPv4 アドレスを設定します。

次のタスク

- マイクロ BFD セッションの設定の確認

マイクロ BFD セッションの設定の確認

マイクロ BFD セッション設定を確認するには、次のコマンドを使用します。

手順の概要

1. ポート チャネルとポート チャネル メンバーの動作状態を表示します。
2. `switch# show bfd neighbors`
3. `switch# show bfd neighbors details`
4. `switch# show tech-support bfd`
5. `switch# show tech-support lacp all`
6. `switch# show running-config interface port-channel port-channel-number`

手順の詳細

ステップ 1 ポート チャネルとポート チャネル メンバーの動作状態を表示します。

```
switch# show port-channel summary
```

ステップ 2 `switch# show bfd neighbors`

ポート チャネル メンバー上のマイクロ BFD セッションを表示します。

ステップ 3 `switch# show bfd neighbors details`

ポート チャネル インターフェイスの BFD セッションと、メンバーの関連するマイクロ BFD セッションを表示します。

ステップ 4 `switch# show tech-support bfd`

BFD のテクニカル サポート情報を表示します。

ステップ 5 switch# **show tech-support lacp all**

イーサネット ポート マネージャ、イーサネット ポートチャネル マネージャ、および LACP のテクニカル サポート情報を表示します。

ステップ 6 switch# **show running-config interface port-channel port-channel-number**

ポート チャネル インターフェイスの実行コンフィギュレーション情報を表示します。

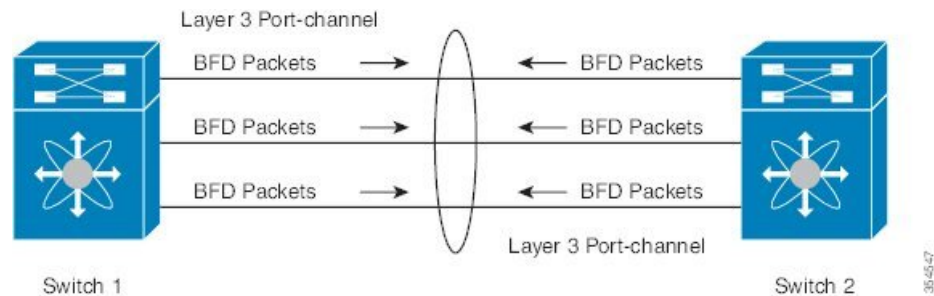
例：マイクロ BFD セッションの設定

マイクロ BFD セッションの設定については、次の例を参照してください。

マイクロ BFD セッションの設定

この例では、次のトポロジが使用されます。

図 8: マイクロ BFD セッションの設定



スイッチ 1 の設定例は次のとおりです。

```
feature bfd
configure terminal
interface port-channel 10
port-channel bfd track-member-link
port-channel bfd destination 10.1.1.2
port-channel bfd start 60
ip address 10.1.1.1/24
```

スイッチ 2 の設定例は次のとおりです。

```
feature bfd
configure terminal
interface port-channel 10
port-channel bfd track-member-link
port-channel bfd destination 10.1.1.1
port-channel bfd start 60
ip address 10.1.1.2/24
```

マイクロBFDセッションの設定の確認

次に、**show running-config interface port-channel**<port-channel>、**show port-channel summary**、**show bfd neighbors vrf internet_routes**、および **show bfd neighbors interface port-channel** <port-channel> **vrf internet_routes details** コマンドの出力結果を示します。

```
switch# show running-config interface port-channel 1001

!Command: show running-config interface port-channel1001
!Time: Fri Oct 21 09:08:00 2016

version 7.0(3)I5(1)

interface port-channel1001
  no switchport
  vrf member internet_routes
  port-channel bfd track-member-link
  port-channel bfd destination 40.4.1.2
  ip address 40.4.1.1/24
  ipv6 address 2001:40:4:1::1/64

switch# show por
port-channel port-profile
switch# show port-channel summary
Flags:  D - Down          P - Up in port-channel (members)
        I - Individual    H - Hot-standby (LACP only)
        s - Suspended     r - Module-removed
        b - BFD Session Wait
        S - Switched      R - Routed
        U - Up (port-channel)
        p - Up in delay-lacp mode (member)
        M - Not in use. Min-links not met
-----
Group Port-      Type      Protocol  Member Ports
Channel
-----
1001 Po1001(RU) Eth      LACP      Eth1/11/1(P) Eth1/11/2(P) Eth1/12/1(P)
                               Eth1/12/2(P)
switch# show bfd neighbors vrf internet_routes

OurAddr      NeighAddr      LD/RD          RH/RS          Holdown(mult)
State        Int             Vrf
40.4.1.1     40.4.1.2       1090519041/0   Up             N/A (3)
Up           Po1001          internet_routes
40.4.1.1     40.4.1.2       1090519042/1090519051 Up             819 (3)
Up           Eth1/12/1       internet_routes
40.4.1.1     40.4.1.2       1090519043/1090519052 Up             819 (3)
Up           Eth1/12/2       internet_routes
40.4.1.1     40.4.1.2       1090519044/1090519053 Up             819 (3)
Up           Eth1/11/1       internet_routes
40.4.1.1     40.4.1.2       1090519045/1090519054 Up             819 (3)
Up           Eth1/11/2       internet_routes
switch#

switch# show bfd neighbors interface port-channel 1001 vrf internet_routes details

OurAddr      NeighAddr      LD/RD          RH/RS          Holdown(mult)
State        Int             Vrf
40.4.1.1     40.4.1.2       1090519041/0   Up             N/A (3)
Up           Po1001          internet_routes

Session state is Up
```



```

Local Diag: 0
Registered protocols: eth_port_channel
Uptime: 1 days 11 hrs 4 mins 8 secs
Hosting LC: 0, Down reason: None, Reason not-hosted: None
Parent session, please check port channel config for member info
switch#

switch# show bfd neighbors interface ethernet 1/12/1 vrf internet_routes details

OurAddr      NeighAddr      LD/RD              RH/RS              Holddown(mult)
State        Int             Vrf
40.4.1.1     40.4.1.2       1090519042/1090519051 Up                  604(3)
Up           Eth1/12/1      internet_routes

Session state is Up and not using echo function
Local Diag: 0, Demand mode: 0, Poll bit: 0, Authentication: None
MinTxInt: 100000 us, MinRxInt: 100000 us, Multiplier: 3
Received MinRxInt: 300000 us, Received Multiplier: 3
Holddown (hits): 900 ms (0), Hello (hits): 300 ms (458317)
Rx Count: 427188, Rx Interval (ms) min/max/avg: 19/1801/295 last: 295 ms ago
Tx Count: 458317, Tx Interval (ms) min/max/avg: 275/275/275 last: 64 ms ago
Registered protocols: eth_port_channel
Uptime: 1 days 11 hrs 4 mins 24 secs
Last packet: Version: 1                - Diagnostic: 0
              State bit: Up            - Demand bit: 0
              Poll bit: 0              - Final bit: 0
              Multiplier: 3            - Length: 24
              My Discr.: 1090519051    - Your Discr.: 1090519042
              Min tx interval: 300000  - Min rx interval: 300000
              Min Echo interval: 300000 - Authentication bit: 0
Hosting LC: 1, Down reason: None, Reason not-hosted: None
Member session under parent interface Po1001

switch# show bfd neighbors interface ethernet 1/12/2 vrf internet_routes details

OurAddr      NeighAddr      LD/RD              RH/RS              Holddown(mult)
State        Int             Vrf
40.4.1.1     40.4.1.2       1090519043/1090519052 Up                  799(3)
Up           Eth1/12/2      internet_routes

Session state is Up and not using echo function
Local Diag: 0, Demand mode: 0, Poll bit: 0, Authentication: None
MinTxInt: 100000 us, MinRxInt: 100000 us, Multiplier: 3
Received MinRxInt: 300000 us, Received Multiplier: 3
Holddown (hits): 900 ms (0), Hello (hits): 300 ms (458336)
Rx Count: 427207, Rx Interval (ms) min/max/avg: 19/1668/295 last: 100 ms ago
Tx Count: 458336, Tx Interval (ms) min/max/avg: 275/275/275 last: 251 ms ago
Registered protocols: eth_port_channel
Uptime: 1 days 11 hrs 4 mins 30 secs
Last packet: Version: 1                - Diagnostic: 0
              State bit: Up            - Demand bit: 0
              Poll bit: 0              - Final bit: 0
              Multiplier: 3            - Length: 24
              My Discr.: 1090519052    - Your Discr.: 1090519043
              Min tx interval: 300000  - Min rx interval: 300000
              Min Echo interval: 300000 - Authentication bit: 0
Hosting LC: 1, Down reason: None, Reason not-hosted: None
Member session under parent interface Po1001
switch#
    
```

ルーティングプロトコルに対する BFD サポートの設定

BGP での BFD の設定

ボーダー ゲートウェイ プロトコル (BGP) の BFD を設定できます。

始める前に

BFD 機能をイネーブルにします。「BFD 機能のイネーブル化」を参照してください。

BFD セッション パラメータを設定します。「グローバルな BFD パラメータの設定」の項または「インターフェイスでの BFD の」の項を参照してください。

BGP 機能をイネーブルにします。詳細については、『[Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide](#)』を参照してください。

手順の概要

1. **configure terminal**
2. **router bgp as-number**
3. **neighbor (ip-address | ipv6-address) remote-as as-number**
4. **bfd [multihop | singlehop]**
5. **update-source interface**
6. **show running-config bgp**
7. **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	configure terminal 例 : switch# configure terminal switch(config)#	コンフィギュレーションモードに入ります。
ステップ 2	router bgp as-number 例 : switch(config)# router bgp 64496 switch(config-router)#	BGP を有効にして、ローカル BGP スピーカに AS 番号を割り当てます。AS 番号は 16 ビット整数または 32 ビット整数にできます。上位 16 ビット 10 進数と下位 16 ビット 10 進数による xx.xx という形式です。
ステップ 3	neighbor (ip-address ipv6-address) remote-as as-number 例 : switch(config-router)# neighbor 209.165.201.1 remote-as 64497 switch(config-router-neighbor)#	リモート BGP ピアの IPv4 アドレスまたは IPv6 アドレスおよび AS 番号を設定します。The <i>ip-address</i> 形式は x.x.x.x です。 <i>ipv6-address</i> の形式は A:B::C:D です。

	コマンドまたはアクション	目的
ステップ 4	bfd [multihop singlehop] 例： <pre>switch(config-router-neighbor)# bfd multiihop</pre>	デバイスで BFD マルチ ホップまたはシングル ホップセッションを設定します。デフォルトでは、キーワードは指定されていません。キーワードを指定せず、ピアが直接接続されている場合はシングルホップセッションが選択され、ピアが接続されていない場合はマルチ ホップセッションタイプが選択されます。「multihop」または「singlehop」オプションを指定すると、セッションタイプは CLI オプションに従ってデバイスで強制されます。
ステップ 5	update-source interface 例： <pre>switch(config-router-neighbor)# update-source ethernet 2/1</pre>	ネイバーで BGP セッションを形成し、BFD とともにクライアントとして登録するために BGP を有効にするとき、特定のインターフェイスからのプライマリ IP アドレスをローカルアドレスとして BGP セッションで使用できます。
ステップ 6	show running-config bgp 例： <pre>switch(config-router-neighbor)# show running-config bgp</pre>	(任意) BGP 実行コンフィギュレーションを表示します。
ステップ 7	copy running-config startup-config 例： <pre>switch(config-router-neighbor)# copy running-config startup-config</pre>	(任意) この設定の変更を保存します。

EIGRP での BFD の設定

Enhanced Interior Gateway Routing Protocol (EIGRP) の BFD を設定できます。

始める前に

BFD 機能をイネーブルにします。「BFD 機能のイネーブル化」を参照してください。

BFD セッションパラメータを設定します。「グローバルな BFD パラメータの設定」の項または「インターフェイスでの BFD の」の項を参照してください。

EIGRP 機能をイネーブルにします。詳細については、『[Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide](#)』を参照してください。

手順の概要

1. **configure terminal**
2. **router eigrp instance-tag**
3. **bfd [ipv4 | ipv6]**

4. **interface int-if**
5. **ip eigrp instance-tag bfd**
6. **show ip eigrp [vrf vrf-name] [interfaces if]**
7. **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	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	コンフィギュレーションモードに入ります。
ステップ 2	router eigrp instance-tag 例 : <pre>switch(config)# router eigrp Test1 switch(config-router)#</pre>	インスタンス タグを設定して、新しい EIGRP プロセスを作成します。インスタンス タグには最大 20 文字の英数字を使用できます。大文字と小文字を区別します。 AS 番号であると認められていないインスタンス タグを設定する場合は、 autonomous-system を使用しますして AS 番号を明示的に設定する必要があります。そうしないと、この EIGRP インスタンスはシャットダウン状態のままになります。
ステップ 3	bfd [ipv4 ipv6] 例 : <pre>switch(config-router-neighbor)# bfd ipv4</pre>	(任意) すべての EIGRP インターフェイスの BFD をイネーブルにします。
ステップ 4	interface int-if 例 : <pre>switch(config-router-neighbor)# interface ethernet 2/1 switch(config-if)#</pre>	インターフェイス設定モードを開始します。? キーワードを使用して、サポートされるインターフェイスを表示します。
ステップ 5	ip eigrp instance-tag bfd 例 : <pre>switch(config-if)# ip eigrp Test1 bfd</pre>	(任意) EIGRP インターフェイスの BFD をイネーブルまたはディセーブルにします。インスタンス タグには最大 20 文字の英数字を使用できます。大文字と小文字を区別します。 デフォルトではディセーブルになっています。
ステップ 6	show ip eigrp [vrf vrf-name] [interfaces if] 例 : <pre>switch(config-if)# show ip eigrp</pre>	(任意) EIGRP に関する情報を表示します。vrf-name には最大 32 文字の英数字文字列を指定します。大文字と小文字は区別されます。
ステップ 7	copy running-config startup-config 例 :	(任意) この設定の変更を保存します。

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

OSPF での BFD の設定

Open Shortest Path First で BFD を設定できます。

始める前に

BFD 機能をイネーブルにします。「BFD 機能のイネーブル化」を参照してください。

BFD セッションパラメータを設定します。「グローバルな BFD パラメータの設定」の項または「インターフェイスでの BFD の」の項を参照してください。

OSPF 機能をイネーブルにします。詳細については、『[Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide](#)』を参照してください。

手順の概要

1. **configure terminal**
2. **router ospf instance-tag**
3. **bfd [ipv4 | ipv6]**
4. **interface int-if**
5. **ip ospf bfd**
6. **show ip ospf [vrf vrf-name] [interfaces if]**
7. **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	configure terminal 例： <code>switch# configure terminal</code> <code>switch(config)#</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	router ospf instance-tag 例： <code>switch(config)# router ospf 200</code> <code>switch(config-router)#</code>	インスタンス タグを設定して、新しい OSPF インスタンスを作成します。インスタンス タグには最大 20 文字の英数字を使用できます。大文字と小文字を区別します。
ステップ 3	bfd [ipv4 ipv6] 例： <code>switch(config-router)# bfd</code>	(任意) すべての OSPF インターフェイスの BFD をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 4	interface <i>int-if</i> 例： switch(config-router)# interface ethernet 2/1 switch(config-if)#	インターフェイス設定モードを開始します。? キーワードを使用して、サポートされるインターフェイスを表示します。
ステップ 5	ip ospf bfd 例： switch(config-if)# ip ospf bfd	(任意) OSPF インターフェイスの BFD をイネーブルまたはディセーブルにします。デフォルトではディセーブルになっています。
ステップ 6	show ip ospf [vrf vrf-name] [interfaces if] 例： switch(config-if)# show ip ospf	(任意) OSPF に関する情報を表示します。vrf-name には最大 32 文字の英数字文字列を指定します。大文字と小文字は区別されます。
ステップ 7	copy running-config startup-config 例： switch(config-if)# copy running-config startup-config	(任意) この設定の変更を保存します。

OSPF での BFD の設定例

非デフォルト VRF (vrf3 の OSPFv3 ネイバー) で BFD が有効になる設定例

```
configure terminal
router ospfv3 10
vrf vrf3
bfd
```

IS-IS での BFD の設定

Intermediate System-to-Intermediate System (IS-IS) プロトコルで BFD を設定できます。

始める前に

BFD 機能をイネーブルにします。「BFD 機能のイネーブル化」を参照してください。

BFD セッションパラメータを設定します。「グローバルな BFD パラメータの設定」の項または「インターフェイスでの BFD の」の項を参照してください。

IS-IS 機能をイネーブルにします。詳細については、『[Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide](#)』を参照してください。

手順の概要

1. **configure terminal**
2. **router isis instance-tag**

3. **bfd [ipv4 | ipv6]**
4. **interface int-if**
5. **isis bfd**
6. **show isis [vrf vrf-name] [interface if]**
7. **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	configure terminal 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	router isis instance-tag 例： switch(config)# router isis 100 switch(config-router)# net 49.0001.1720.1600.1001.00 switch(config-router)# address-family ipv6 unicast	<i>instance tag</i> を設定して、新しい IS-IS インスタンスを作成します。
ステップ 3	bfd [ipv4 ipv6] 例： switch(config-router)# bfd	(任意) すべての OSPF インターフェイスの BFD をイネーブルにします。
ステップ 4	interface int-if 例： switch(config-router)# interface ethernet 2/1 switch(config-if)#	インターフェイス設定モードを開始します。? キーワードを使用して、サポートされるインターフェイスを表示します。
ステップ 5	isis bfd 例： switch(config-if)# isis bfd	(任意) IS-IS インターフェイスの BFD をイネーブルまたはディセーブルにします。デフォルトではディセーブルになっています。
ステップ 6	show isis [vrf vrf-name] [interface if] 例： switch(config-if)# show isis	(任意) IS-IS に関する情報を表示します。vrf-name には最大 32 文字の英数字文字列を指定します。大文字と小文字は区別されます。
ステップ 7	copy running-config startup-config 例： switch(config-if)# copy running-config startup-config	(任意) この設定の変更を保存します。

IS-IS での BFD の設定例

IPv4およびIPv6アドレスファミリでBFDが有効になっているIS-ISの設定例。

```
configure terminal
  router isis isis-1
    bfd
    address-family ipv6 unicast
  bfd
```

HSRP での BFD の設定

Hot Standby Router Protocol (HSRP) の BFD を設定できます。アクティブおよびスタンバイの HSRP ルータは BFD を介して相互に追跡しています。スタンバイ HSRP ルータ上の BFD がアクティブ HSRP ルータが動作していないことを検知すると、スタンバイ HSRP はこのイベントをアクティブ タイマー失効として取り扱いアクティブ HSRP ルータとして役割を引き継ぎます。

この項で説明している **show hsrp detail** コマンドでは、このイベントが BFD@Act-down または BFD@Sby-down として表示されます。

始める前に

BFD 機能をイネーブルにします。「BFD 機能のイネーブル化」を参照してください。

BFD セッションパラメータを設定します。「グローバルな BFD パラメータの設定」の項または「インターフェイスでの BFD の」の項を参照してください。

HSRP 機能をイネーブルにします。詳細については、『Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide』を参照してください。

手順の概要

1. **configure terminal**
2. **hsrp bfd all-interfaces**
3. **interface int-if**
4. **hsrp bfd**
5. **show running-config hsrp**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	グローバル 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	hsrp bfd all-interfaces 例： switch# hsrp bfd all-interfaces	(任意) すべての HSRP インターフェイスで BFD をイネーブルまたはディセーブルにします。デフォルトではディセーブルになっています。
ステップ 3	interface int-if 例： switch(config-router)# interface ethernet 2/1 switch(config-if)#	インターフェイス設定モードを開始します。? キーワードを使用して、サポートされるインターフェイスを表示します。
ステップ 4	hsrp bfd 例： switch(config-if)# hsrp bfd	(任意) HSRP インターフェイスの BFD をイネーブルまたはディセーブルにします。デフォルトではディセーブルになっています。
ステップ 5	show running-config hsrp 例： switch(config-if)# show running-config hsrp	(任意) HSRP 実行コンフィギュレーションを表示します。
ステップ 6	copy running-config startup-config 例： switch(config-if)# copy running-config startup-config	(任意) この設定の変更を保存します。

VRRP での BFD の設定

仮想ルータ冗長プロトコル (VRRP) の BFD を設定できます。アクティブおよびスタンバイの VRRP ルータは BFD を介して相互に追跡しています。スタンバイ VRRP ルータ上の BFD がアクティブ VRRP ルータが動作していないことを検知すると、スタンバイ VRRP はこのイベントをアクティブ タイマー失効として取り扱いアクティブ VRRP ルータとして役割を引き継ぎます。

この項で説明している **show vrrp detail** コマンドでは、このイベントが BFD@Act-down または BFD@Sby-down として表示されます。

始める前に

BFD 機能をイネーブルにします。「BFD 機能のイネーブル化」を参照してください。

BFD セッションパラメータを設定します。「グローバルな BFD パラメータの設定」の項または「インターフェイスでの BFD の」の項を参照してください。

VRRP 機能をイネーブルにします。詳細については、『[Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide](#)』を参照してください。

PIM (Protocol Independent Multicast) での BFD の設定

手順の概要

1. **configure terminal**
2. **interface int-if**
3. **vrrp group-no**
4. **vrrp bfd address**
5. **show running-config vrrp**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface int-if 例： switch(config)# interface ethernet 2/1 switch(config-if)#	インターフェイス設定モードを開始します。? キーワードを使用して、サポートされるインターフェイスを表示します。
ステップ 3	vrrp group-no 例： switch(config-if)# vrrp 2	VRRP グループ番号を指定します。
ステップ 4	vrrp bfd address 例： switch(config-if)# vrrp bfd	VRRP インターフェイスで BFD をイネーブルまたはディセーブルにします。デフォルトではディセーブルになっています。
ステップ 5	show running-config vrrp 例： switch(config-if)# show running-config vrrp	(任意) VRRP 実行コンフィギュレーションを表示します。
ステップ 6	copy running-config startup-config 例： switch(config-if)# copy running-config startup-config	(任意) この設定の変更を保存します。

PIM (Protocol Independent Multicast) での BFD の設定

PIM (Protocol Independent Multicast) プロトコルの BFD を設定できます。

始める前に

BFD 機能をイネーブルにします。「BFD 機能のイネーブル化」を参照してください。

PIM 機能をイネーブルにします。詳細については、『Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide』を参照してください。

手順の概要

1. **configure terminal**
2. **ip pim bfd**
3. **interface *int-if***
4. **ip pim bfd-instance [disable]**
5. **show running-config pim**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ip pim bfd 例： switch(config)# ip pim bfd	PIM の BFD をイネーブルにします。
ステップ 3	interface <i>int-if</i> 例： switch(config)# interface ethernet 2/1 switch(config-if)#	インターフェイス設定モードを開始します。? キーワードを使用して、サポートされるインターフェイスを表示します。
ステップ 4	ip pim bfd-instance [disable] 例： switch(config-if)# ip pim bfd-instance	(任意) PIM インターフェイスの BFD をイネーブルまたはディセーブルにします。デフォルトではディセーブルになっています。
ステップ 5	show running-config pim 例： switch(config)# show running-config pim	(任意) PIM 実行コンフィギュレーションを表示します。
ステップ 6	copy running-config startup-config 例： switch(config)# copy running-config startup-config	(任意) この設定の変更を保存します。

スタティックルートでの BFD の設定

インターフェイスのスタティックルートの BFD を設定できます。Virtual Routing and Forwarding (VRF) インスタンス内のスタティックルートでの BFD を任意で設定できます。

始める前に

BFD 機能をイネーブルにします。「BFD 機能のイネーブル化」を参照してください。

手順の概要

1. **configure terminal**
2. **vrf context** *vrf-name*
3. **ip route** *route interface {nh-address | nh-prefix}*
4. **ip route static bfd** *interface {nh-address | nh-prefix}*
5. **show ip route static** [*vrf vrf-name*]
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： <pre>switch# configure terminal switch(config)#</pre>	グローバル 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	vrf context <i>vrf-name</i> 例： <pre>switch(config)# vrf context Red switch(config-vrf)#</pre>	(任意) VRF コンフィギュレーションモードを開始します。
ステップ 3	ip route <i>route interface {nh-address nh-prefix}</i> 例： <pre>switch(config-vrf)# ip route 192.0.2.1 ethernet 2/1 192.0.2.4</pre>	スタティック ルートを作成します。? キーワードを使用して、サポートされているインターフェイスを表示します。
ステップ 4	ip route static bfd <i>interface {nh-address nh-prefix}</i> 例： <pre>switch(config-vrf)# ip route static bfd ethernet 2/1 192.0.2.4</pre>	インターフェイスのすべてのスタティックルートの BFD をイネーブルにします。? キーワードを使用して、サポートされるインターフェイスを表示します。
ステップ 5	show ip route static [<i>vrf vrf-name</i>] 例： <pre>switch(config-vrf)# show ip route static vrf Red</pre>	(任意) スタティック ルートを表示します。

	コマンドまたはアクション	目的
ステップ 6	copy running-config startup-config 例 : <pre>switch(config-vrf)# copy running-config startup-config</pre>	(任意) この設定の変更を保存します。

インターフェイスにおける BFD のディセーブル化

グローバルまたは VRF レベルでイネーブルにされた BFD のあるルーティングプロトコルに対するインターフェイス上の BFD を選択的にディセーブルにできます。

インターフェイス上の BFD をディセーブルにするには、インターフェイス コンフィギュレーション モードで次のコマンドのいずれかを使用します。

コマンド	目的
ip eigrp instance-tag bfd disable 例 : <pre>switch(config-if)# ip eigrp Test1 bfd disable</pre>	EIGRP インターフェイスで BFD をディセーブルにします。インスタンスタグには最大 20 文字の英数字を使用できます。大文字と小文字を区別します。
ip ospf bfd disable 例 : <pre>switch(config-if)# ip ospf bfd disable</pre>	OSPFv2 インターフェイスで BFD をディセーブルにします。
isis bfd disable 例 : <pre>switch(config-if)# isis bfd disable</pre>	IS-IS インターフェイスで BFD をディセーブルにします。

インターフェイスにおける BFD のディセーブル化

インターフェイスごとに BFD が無効になっている設定例。

```
configure terminal
interface port-channel 10
no ip redirects
ip address 22.1.10.1/30
ipv6 address 22:1:10::1/120
no ipv6 redirects
ip router ospf 10 area 0.0.0.0
ip ospf bfd disable          /*** disables IPv4 BFD session for OSPF
ospfv3 bfd disable          /*** disables IPv6 BFD session for OSPFv3
```

BFD 相互運用性の設定

ポイントツーポイントリンク内の Cisco NX-OS デバイスの BFD 相互運用性

手順の概要

1. `configure terminal`
2. `interface port-channel int-if`
3. `ip ospf bfd`
4. `no ip redirects`
5. `bfd interval mintx min_rx msec multiplier value`
6. `exit`

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： <code>switch# configure terminal</code> <code>switch(config)#</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	interface port-channel int-if 例： <code>switch(config-if)# interface ethernet 2/1</code>	インターフェイス設定モードを開始します。? キーワードを使用して、サポートされるインターフェイスを表示します。
ステップ 3	ip ospf bfd 例： <code>switch(config-if)# ip ospf bfd</code>	OSPFv2 インターフェイスで BFD をイネーブルにします。デフォルトではディセーブルになっています。 OSPF は例として使用されています。サポートされている任意のプロトコルの BFD をイネーブルにできます。
ステップ 4	no ip redirects 例： <code>switch(config-if)# no ip redirects</code>	デバイスがリダイレクトを送信しないようにします。
ステップ 5	bfd interval mintx min_rx msec multiplier value 例： <code>switch(config-if)# bfd interval 50</code> <code>min_rx 50 multiplier 3</code>	ポートチャネルのすべての BFD セッションの BFD セッションパラメータを設定します。BFD セッションパラメータを設定することにより、このコマンドでこれらの値を無効にすることができます。 <i>mintx</i> および <i>msec</i> の範囲は 50 ~ 999 ミリ秒で、デフォル

	コマンドまたはアクション	目的
		トは 50 です。乗数の範囲は 1 ~ 50 です。乗数のデフォルトは 3 です。
ステップ 6	exit 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、EXEC モードに戻ります。

スイッチ仮想インターフェイス内の Cisco NX-OS デバイスの BFD 相互運用性の設定

手順の概要

1. **configure terminal**
2. **interface port-channel vlan vlan-id**
3. **bfd interval mintx min_rx msec multiplier value**
4. **no ip redirects**
5. **ip address ip-address/length**
6. **ip ospf bfd**
7. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface port-channel vlan vlan-id 例 : switch(config)# interface vlan 998 switch(config-if)#	ダイナミック スイッチ仮想インターフェイス (SVI) を作成します。
ステップ 3	bfd interval mintx min_rx msec multiplier value 例 : switch(config-if) # bfd interval 50 min_rx 50 multiplier 3	デバイスのすべての BFD セッションの BFD セッション パラメータを設定します。mintx および msec の範囲は 50 ~ 999 ミリ秒で、デフォルトは 50 です。乗数の範囲は 1 ~ 50 です。乗数のデフォルトは 3 です。
ステップ 4	no ip redirects 例 : switch(config-if) # no ip redirects	デバイスがリダイレクトを送信しないようにします。

	コマンドまたはアクション	目的
ステップ 5	ip address <i>ip-address/length</i> 例： switch(config-if)# ip address 10.1.0.253/24	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 6	ip ospf bfd 例： switch(config-if)# ip ospf bfd	OSPFv2 インターフェイスで BFD をイネーブルにします。デフォルトではディセーブルになっています。
ステップ 7	exit 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、EXEC モードに戻ります。

論理モードの Cisco NX-OS デバイスの BFD 相互運用性の設定

手順の概要

1. **configure terminal**
2. **interface port-channel** *type number.subinterface-id*
3. **bfd interval** *mintx min_rx msec multiplier value*
4. **no ip redirects**
5. **ip ospf bfd**
6. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface port-channel <i>type number.subinterface-id</i> 例： switch(config-if)# interface port-channel 50.2	ポート チャネル コンフィギュレーション モードを開始します。? キーワードを使用して、サポートされる数値の範囲を表示します。
ステップ 3	bfd interval <i>mintx min_rx msec multiplier value</i> 例： switch(config-if)# bfd interval 50 min_rx 50 multiplier 3	ポート チャネルのすべての BFD セッションの BFD セッション パラメータを設定します。 <i>mintx</i> および <i>msec</i> の範囲は 50 ~ 999 ミリ秒で、デフォルトは 50 です。乗数の範囲は 1 ~ 50 です。乗数のデフォルトは 3 です。

	コマンドまたはアクション	目的
ステップ 4	no ip redirects 例： switch(config-if)# no ip redirects	デバイスがリダイレクトを送信しないようにします。
ステップ 5	ip ospf bfd 例： switch(config-if)# ip ospf bfd	OSPFv2 インターフェイスで BFD をイネーブルにします。デフォルトではディセーブルになっています。 OSPF は例として使用されています。サポートされている任意のプロトコルの BFD をイネーブルにできます。
ステップ 6	exit 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、EXEC モードに戻ります。

Cisco Nexus 9000 シリーズ デバイスでの BFD 相互運用性の確認

次に、Cisco Nexus 9000 シリーズ デバイス上で BFD 相互運用性を確認する例を示します。

```
switch# show bfd neighbors details
OurAddr NeighAddr LD/RD RH/RS Holddown(mult) State Int
Vrf
10.1.1.1 10.1.1.2 1140850707/2147418093 Up 6393(4) Up Vlan2121
default
Session state is Up and using echo function with 50 ms interval
Local Diag: 0, Demand mode: 0, Poll bit: 0, Authentication: None
MinTxInt: 50000 us, MinRxInt: 2000000 us, Multiplier: 3
Received MinRxInt: 2000000 us, Received Multiplier: 4
Holddown (hits): 8000 ms (0), Hello (hits): 2000 ms (108)
Rx Count: 92, Rx Interval (ms) min/max/avg: 347/1996/1776 last: 1606 ms ago
Tx Count: 108, Tx Interval (ms) min/max/avg: 1515/1515/1515 last: 1233 ms ago
Registered protocols: ospf
Uptime: 0 days 0 hrs 2 mins 44 secs
Last packet: Version: 1 - Diagnostic: 0
State bit: Up - Demand bit: 0
Poll bit: 0 - Final bit: 0
Multiplier: 4 - Length: 24
My Discr.: 2147418093 - Your Discr.: 1140850707
Min tx interval: 2000000 - Min rx interval: 2000000
Min Echo interval: 1000 - Authentication bit: 0
Hosting LC: 10, Down reason: None, Reason not-hosted: None
```

```
switch# show bfd neighbors details
OurAddr NeighAddr LD/RD RH/RS Holddown(mult) State Int
Vrf
10.0.2.1 10.0.2.2 1140850695/131083 Up 270(3) Up Po14.121
default
Session state is Up and not using echo function
Local Diag: 0, Demand mode: 0, Poll bit: 0, Authentication: None
MinTxInt: 50000 us, MinRxInt: 50000 us, Multiplier: 3
```

```

Received MinRxInt: 100000 us, Received Multiplier: 3
Holdown (hits): 300 ms (0), Hello (hits): 100 ms (3136283)
Rx Count: 2669290, Rx Interval (ms) min/max/avg: 12/1999/93 last: 29 ms ago
Tx Count: 3136283, Tx Interval (ms) min/max/avg: 77/77/77 last: 76 ms ago
Registered protocols: ospf
Uptime: 2 days 21 hrs 41 mins 45 secs
Last packet: Version: 1 - Diagnostic: 0
State bit: Up - Demand bit: 0
Poll bit: 0 - Final bit: 0
Multiplier: 3 - Length: 24
My Discr.: 131083 - Your Discr.: 1140850695
Min tx interval: 100000 - Min rx interval: 100000
Min Echo interval: 0 - Authentication bit: 0
Hosting LC: 8, Down reason: None, Reason not-hosted: None
    
```

BFD 設定の確認

BFD 設定情報を表示するには、次のいずれかを行います。

コマンド	目的
<code>show running-config bfd</code>	実行 BFD コンフィギュレーションを表示します。
<code>show startup-config bfd</code>	次のシステム起動時に適用される BFD コンフィギュレーションを表示します。

BFD のモニタリング

BFD を表示するには、次のコマンドを使用します。

コマンド	目的
<code>show bfd neighbors [application name] [details]</code>	BGP や OSPFv2 などのサポートされるアプリケーションの BFD に関する情報を表示します。
<code>show bfd neighbors [interface int-if] [details]</code>	インターフェイスの BGP セッションに関する情報を表示します。
<code>show bfd neighbors [dest-ip ip-address] [src-ip ip-address][details]</code>	インターフェイス上の指定された BGP セッションに関する情報を表示します。
<code>show bfd neighbors [vrf vrf-name] [details]</code>	VRF の BFD に関する情報を表示します。
<code>show bfd [ipv4 ipv6] [neighbors]</code>	IPv4 ネイバーまたは IPv6 ネイバーに関する情報を表示します。

BFD マルチホップ

IPv4 の BFD マルチホップおよび IPv6 の BFD マルチホップは、RFC5883 に準拠してサポートされます。BFD マルチホップセッションは、固有のソースと宛先アドレス ペア間で設定されます。マルチホップ BFD セッションは、シングルホップ BFD セッションの場合のように、インターフェイスではなく、送信元と宛先間のリンクに関連付けられます。

BFD マルチホップのホップ数

BFD マルチホップは TTL フィールドを最大制限に設定し、受信時に値をチェックしません。BFD コードは、BFD マルチホップパケットが通過できるホップ数には影響しません。ただし、ほとんどのシステムでは、ホップ数が 255 に制限されています。

BFD マルチホップの注意事項と制約事項

BFD マルチホップ設定時の注意事項と制約事項は次のとおりです。

- VXLAN を介した BFD マルチホップは、Cisco Nexus 9200、9364C、9300-EX、9300-FX/FX2、9300-GX、9300-FX/FX、X9716D-GX、9600-R、および 9600-RX スイッチでサポートされます。
- Cisco NX-OS リリース 9.3(6) から、BFD マルチホップは、BGP IPv4 でのみ Cisco Nexus 9200、9300-EX/FX/GX プラットフォーム スイッチおよび Cisco Nexus 9500 プラットフォーム スイッチでサポートされています (N9K-X9700-EX ライン カード搭載のもの)。
- ダイナミック BGP コンフィギュレーションでは、シングル BGP ピアとマルチホップ BGP ピアの両方が BFD マルチホップ設定を受け入れます。
- BFD マルチホップは BGP でのみサポートされています。
- BFD マルチホップは、次のデバイスの BGP IPv6 マルチホップ ネイバーでサポートされません。
 - Cisco Nexus 9200YC-X、9300-EX、9300-FX および 9300-GX スイッチ
 - N9K-X9736C-EX、N9K-X97160YC-EX、N9K-X9732C-EX、N9K-X9732C-EXM、または N9K-X9736C-FX ライン カードを搭載した Cisco Nexus 9500 プラットフォーム スイッチ



(注) -EX および -FX ライン カードを使用した Cisco Nexus 9500 プラットフォーム スイッチで BGP IPv6 の BFD マルチホップを使用するには、**system routing template-mpls-heavy** コマンドを有効にする必要があります。

- マルチホップ BFD は、UDP 宛先ポート 4784 で識別されます。
- マルチホップ BFD のデフォルトのインターバル タイマーは、乗数 3 で 250 ms です。
- サポートされるマルチホップ BFD セッションの最大数は 100 です。
- 既存の BFD 認証サポートは、マルチホップセッション用に拡張されています。
- エコー モードはマルチホップ BFD ではサポートされません。
- セグメントルーティングアンダーレイによるマルチホップはサポートされていません。
- サポートされていないプラットフォームでは、BGPv6 マルチホップ ネイバーを設定するときに BFD コマンドが受け入れられません。ただし、セッションは作成またはインストールされません。
- マルチホップ BFD セッションがポート チャネルにインストールされている場合、次の点に注意する必要があります。
 - すべてのセッションが Cisco Nexus 9500 スイッチファミリの単一のラインカードでホストされている場合、ホストされたラインカードのリロード中に、すべてのセッションが別のラインカードでホストされます。この場合、BFD および BGP セッションがフラップすることがあります。
 - モジュール間ポートチャネルを介した BGP のマルチホップ BFD セッションは、完全な冗長性を提供しません。

BFD マルチホップセッショングローバルインターバルパラメータの設定

デバイスのすべての BFD セッションの BFD セッションパラメータを設定できます。セッションごとに異なる BFD セッションパラメータを設定するには、セッション単位の設定コマンドを使用します。

始める前に

BFD 機能をイネーブルにします。

手順の概要

1. **configure terminal**
2. **[no] bfd multihop interval *milliseconds* min_rx *milliseconds* multiplier *interval-multiplier***
3. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： switch# configure terminal switch(config)#	コンフィギュレーションモードに入ります。
ステップ 2	[no] bfd multihop interval milliseconds min_rx milliseconds multiplier interval-multiplier 例： switch(config)# bfd multihop interval 250 min_rx 250 multiplier 3	デバイスのすべての BFD セッションの BFD セッションパラメータを設定します。このコマンドは、デフォルトの動作を上書きします。 <i>Required Minimum Receive Interval</i> と <i>Desired Minimum Transmit Interval</i> は 250 です。乗数のデフォルトは 3 です。
ステップ 3	end 例： switch(config)# end	設定の変更を保存し、設定セッションを終了します。

マルチホップセッション単位の BFD パラメータの設定

マルチホップセッション単位の BFD パラメータを設定できます。

始める前に

BFD 機能をイネーブルにします。「BFD 機能のイネーブル化」を参照してください。

手順の概要

1. **configure terminal**
2. **router bgp as-number**
3. **neighbor (ip-address | ipv6-address) remote-as as-number**
4. **update-source interface**
5. **bfd**
6. **bfd multihop interval mintx min_rx msec multiplier value**
7. **bfd multihop authentication keyed-sha1 keyid id key ascii_key**
8. **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	configure terminal 例： switch# configure terminal switch(config)#	コンフィギュレーションモードに入ります。

	コマンドまたはアクション	目的
ステップ 2	router bgp as-number 例： switch(config)# router bgp 64496 switch(config-router)#	BGP を有効にして、ローカル BGP スピーカに AS 番号を割り当てます。AS 番号は 16 ビット整数または 32 ビット整数にできます。上位 16 ビット 10 進数と下位 16 ビット 10 進数による xx.xx という形式です。
ステップ 3	neighbor (ip-address ipv6-address) remote-as as-number 例： switch(config-router)# neighbor 209.165.201.1 remote-as 64497 switch(config-router-neighbor)#	リモート BGP ピアの IPv4 アドレスまたは IPv6 アドレスおよび AS 番号を設定します。The <i>ip-address</i> 形式は x.x.x.x です。 <i>ipv6-address</i> の形式は A:B::C:D です。
ステップ 4	update-source interface 例： switch(config-router-neighbor)# update-source Ethernet1/4 switch(config-router-neighbor)#	インターフェイスから BFD セッションの送信元 IP アドレスを取得します。
ステップ 5	bfd 例： switch(config-router-neighbor)# bfd multihop	この BGP ピアの BFD をイネーブルにします。
ステップ 6	bfd multihop interval mintx min_rx msec multiplier value 例： switch(config-router-neighbor)# bfd multihop interval 250 min_rx 250 multiplier 3	このネイバーのマルチホップ BFD 間隔値を設定します。 <i>mintx</i> および <i>msec</i> の範囲は 250 ~ 999 ミリ秒で、デフォルトは 250 です。乗数の範囲は 1 ~ 50 です。乗数のデフォルトは 3 です。
ステップ 7	bfd multihop authentication keyed-sha1 keyid id key ascii_key 例： switch(config-router-neighbor)# bfd multihop authentication keyed-sha1 keyid 1 ascii_key cisco123	(オプション) このネイバー上のマルチホップ BFD セッションで BFD の SHA-1 認証を設定します。 <i>ascii_key</i> 文字列は BFD ピア間で共有される秘密キーです。0 ~ 255 の数値の <i>id</i> 値が、この特定の <i>ascii_key</i> に割り当てられます。BFD パケットは <i>id</i> でキーを指定し、複数のアクティブ キーが使用できます。 インターフェイスの SHA-1 認証を無効にするには、コマンドの no 形式を使用します。
ステップ 8	copy running-config startup-config 例： switch(config-router-neighbor)# copy running-config startup-config	(任意) この設定の変更を保存します。

BFD の設定例

次に、デフォルト BFD セッションパラメータを使用した、Ethernet 2/1 上の OSPFv2 の BFD 設定例を示します。

```
feature bfd
feature ospf
router ospf Test1
interface ethernet 2/1
ip ospf bfd
no shutdown
```

次に、デフォルト BFD セッションパラメータを使用した、EIGRP インターフェイスの BFD 設定例を示します。

```
feature bfd
feature eigrp
bfd interval 100 min_rx 100 multiplier 4
router eigrp Test2
bfd
```

次に、BFDv6を設定する例を示します。

```
feature bfd
feature ospfv3
router ospfv3 Test1
interface Ethernet2/7
  ipv6 router ospfv3 Test1 area 0.0.0.0
  ospfv3 bfd
  no shutdown
```

BFDの例を表示

show bfd ipv6 neighbors details コマンドの実行結果の例を次に示します。

```
#show bfd ipv6 neighbors details

OurAddr          NeighAddr
LD/RD            RH/RS           Holdown(mult)   State          Int
Vrf
cc:10::2         cc:10::1
1090519335/1090519260 Up              5692 (3)       Up             Po1
default

Session state is Up and using echo function with 250 ms interval
Local Diag: 0, Demand mode: 0, Poll bit: 0, Authentication: None
MinTxInt: 250000 us, MinRxInt: 2000000 us, Multiplier: 3
Received MinRxInt: 2000000 us, Received Multiplier: 3
Holdown (hits): 6000 ms (4), Hello (hits): 2000 ms (205229)
Rx Count: 227965, Rx Interval (ms) min/max/avg: 124/1520/1510 last: 307 ms ago
Tx Count: 205229, Tx Interval (ms) min/max/avg: 1677/1677/1677 last: 587 ms ago
```

```

Registered protocols: bgp
Uptime: 3 days 23 hrs 31 mins 13 secs
Last packet: Version: 1          - Diagnostic: 0
                  State bit: Up    - Demand bit: 0
                  Poll bit: 0      - Final bit: 0
                  Multiplier: 3    - Length: 24
                  My Discr.: 1090519260 - Your Discr.: 1090519335
                  Min tx interval: 250000 - Min rx interval: 2000000
                  Min Echo interval: 250000 - Authentication bit: 0
Hosting LC: 1, Down reason: None, Reason not-hosted: None

```

関連資料

関連項目	マニュアルタイトル
BFD コマンド	『Cisco Nexus 9000 シリーズ NX-OS ユニキャストルーティング設定ガイド』

RFC

RFC	タイトル
RFC 5880	<i>Bidirectional Forwarding Detection (BFD)</i>
RFC 5881	<i>BFD for IPv4 and IPv6 (Single Hop)</i>
RFC 7130	<i>Link Aggregation Group (LAG) インターフェイスでの Bidirectional Forwarding Detection (BFD)</i>



第 7 章

ポートチャネルの設定

- [ポートチャネルについて \(225 ページ\)](#)
- [ポートチャネル \(226 ページ\)](#)
- [ポートチャネルインターフェイス \(227 ページ\)](#)
- [基本設定 \(228 ページ\)](#)
- [互換性要件 \(228 ページ\)](#)
- [ポートチャネルを使ったロードバランシング \(230 ページ\)](#)
- [シンメトリックハッシング \(232 ページ\)](#)
- [ECMP の注意事項と制限事項 \(233 ページ\)](#)
- [復元力のあるハッシュ \(233 ページ\)](#)
- [GTP トンネルロードバランシング \(234 ページ\)](#)
- [LACP \(235 ページ\)](#)
- [ポートチャネリングの前提条件 \(243 ページ\)](#)
- [注意事項と制約事項 \(243 ページ\)](#)
- [デフォルト設定 \(246 ページ\)](#)
- [ポートチャネルの設定 \(247 ページ\)](#)

ポートチャネルについて

ポートチャネルは複数の物理インターフェイスの集合体で、論理インターフェイスを作成します。1つのポートチャネルに最大32つの個別アクティブリンクをバンドルして、帯域幅と冗長性を向上させることができます。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。ポートチャネルの物理インターフェイスが少なくとも1つ動作していれば、そのポートチャネルは動作しています。

レイヤ2ポートチャネルに適合するレイヤ2インターフェイスをバンドルすれば、レイヤ2ポートチャネルを作成できます。レイヤ3ポートチャネルに適合するレイヤ3インターフェイスをバンドルすれば、レイヤ3ポートチャネルを作成できます。レイヤ2インターフェイスとレイヤ3インターフェイスを同一のポートチャネルで組み合わせることはできません。

ポートチャネルをレイヤ3からレイヤ2に変更することもできます。レイヤ2インターフェイスの作成については、「レイヤ2インターフェイスの設定」の章を参照してください。

レイヤ2ポートチャネルインターフェイスとそのメンバーポートは、異なるSTPパラメータを持つことができます。ポートチャネルのSTPパラメータを変更しても、メンバーポートがバンドルされている場合はポートチャネルインターフェイスが優先されるため、メンバーポートのSTPパラメータには影響しません。



- (注) レイヤ2ポートがポートチャネルの一部になった後に、すべてのスイッチポートの設定をポートチャネルで実行する必要があります。スイッチポートの設定を各ポートチャネルメンバに適用できません。レイヤ3の設定を各ポートチャネルメンバに適用できません。設定をポートチャネル全体に適用する必要があります。

集約プロトコルが関連付けられていない場合でもスタティックポートチャネルを使用して設定を簡略化できます。

柔軟性を高めたい場合はLACPを使用できます。Link Aggregation Control Protocol (LACP) はIEEE 802.3adで定義されています。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。共有インターフェイスではLACPを設定できません。

LACPについては、「LACPの概要」の項を参照してください。

ポートチャネル

ポートチャネルは、物理リンクをまとめて1つのチャンネルグループに入れ、最大32の物理リンクの帯域幅を集約した単一の論理リンクを作ります。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。

ただし、LACPをイネーブルにすればポートチャネルをより柔軟に使用できます。LACPを使ってポートチャネルを設定する場合とスタティックポートチャネルを使って設定する場合は、手順が多少異なります（「ポートチャネルの設定」の項を参照）。



- (注) デバイスはポートチャネルに対するポート集約プロトコル (PAgP) をサポートしません。

各ポートにはポートチャネルが1つだけあります。ポートチャネルのすべてのポートには互換性があり、同じ速度とデュプレックスモードを使用します（「互換性要件」の項を参照）。集約プロトコルを使わずにスタティックポートチャネルを実行する場合、物理リンクはすべてonチャンネルモードです。このモードは、LACPをイネーブルにしない限り変更できません（「ポートチャネルモード」の項を参照）。

ポートチャネルインターフェイスを作成すると、ポートチャネルを直接作成できます。またはチャンネルグループを作成して個別ポートをバンドルに集約させることができます。インターフェイスをチャンネルグループに関連付けると、ポートチャネルがない場合は対応するポートチャネルが自動的に作成されます。この場合、ポートチャネルは最初のインターフェイスのレイヤ2またはレイヤ3設定を行います。最初にポートチャネルを作成することもできます。こ

の場合は、Cisco NX-OS ソフトウェアがポートチャネルと同じチャンネル番号の空のチャンネルグループを作成してデフォルトレイヤ2またはレイヤ3設定を行い、互換性も設定します（「互換性要件」の項を参照）。

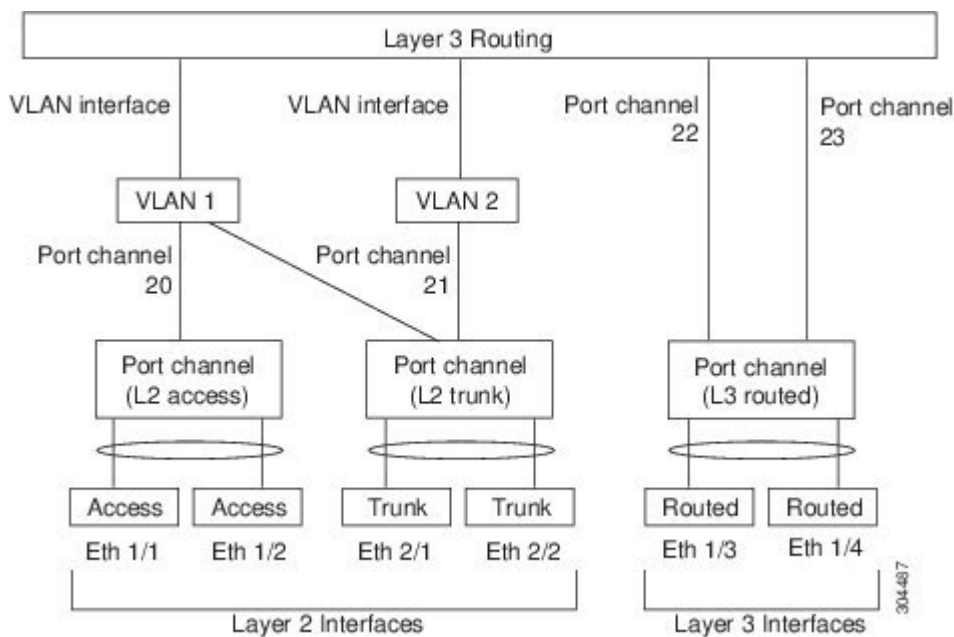


- (注) 少なくともメンバポートの1つがアップしており、かつそのポートのチャンネルが有効であれば、ポートチャネルは動作上アップ状態にあります。メンバーポートがすべてダウンしていれば、ポートチャネルはダウンしています。

ポートチャネルインターフェイス

次に、ポートチャネルインターフェイスを示します。

図 9: ポートチャネルインターフェイス



ポートチャネルインターフェイスは、レイヤ2またはレイヤ3インターフェイスとして分類できます。さらに、レイヤ2ポートチャネルはアクセスモードまたはトランクモードに設定できます。レイヤ3ポートチャネルインターフェイスのチャンネルメンバにはルーテッドポートがあります。

レイヤ3ポートチャネルにスタティックMACアドレスを設定できます。この値を設定しない場合、レイヤ3ポートチャネルは、最初にアップになるチャンネルメンバのルータMACを使用します。レイヤ3ポートでスタティックMACアドレスを設定する情報については、『[Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide](#)』を参照してください。

アクセスモードまたはトランクモードでのレイヤ2ポートの設定については、「レイヤ2 インターフェイスの設定」の章を、レイヤ3インターフェイスおよびサブインターフェイスの設定については、「レイヤ3 インターフェイスの設定」の章を参照してください。

基本設定

ポートチャネルインターフェイスには次の基本設定ができます。

- 帯域幅：この設定は情報目的で使用します。上位レベルプロトコルで使用されます。
- 遅延：この設定は情報目的で使用します。上位レベルプロトコルで使用されます。
- 説明
- デュプレックス
- IP アドレス
- 最大伝送単位 (MTU)
- シャットダウン
- 速度

互換性要件

チャネルグループにインターフェイスを追加する場合、そのインターフェイスにチャネルグループとの互換性があるかどうかを確認するために、特定のインターフェイス属性がチェックされます。たとえば、レイヤ2チャネルグループにレイヤ3インターフェイスを追加できません。また Cisco NX-OS ソフトウェアは、インターフェイスがポートチャネル集約に参加することを許可する前に、そのインターフェイスの多数の動作属性もチェックします。

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。

- ネットワーク層
- (リンク) 速度性能
- 速度設定
- デュプレックス性能
- デュプレックス設定
- ポートモード
- アクセス VLAN
- トランクネイティブ VLAN
- タグ付きまたは非タグ付き

- 許可 VLAN リスト
- MTU サイズ
- SPAN : SPAN の始点または宛先ポートは不可
- ストーム制御
- フロー制御性能
- フロー制御設定
- メディア タイプ、銅線またはファイバ

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

チャンネルモードが **on** に設定されているインターフェイスは、スタティックなポートチャネルにだけ追加できます。また、チャンネルモードが **active** または **passive** に設定されているインターフェイスは、LACP が実行されているポートチャネルにだけ追加できます。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。設定するメンバポートの属性に互換性がない場合、ソフトウェアはこのポートをポートチャネルで一時停止させます。

または、次のパラメータが同じ場合、パラメータに互換性がないポートを強制的にポートチャネルに参加させることもできます。

- (リンク) 速度性能
- 速度設定
- デュプレックス性能
- デュプレックス設定
- フロー制御性能
- フロー制御設定

インターフェイスがポートチャネルに参加すると、一部のパラメータが削除され、ポートチャネルの値が次のように置き換わります。

- 帯域幅
- 遅延
- UDP の拡張認証プロトコル
- VRF
- IP アドレス
- MAC アドレス
- スパニングツリー プロトコル
- NAC

- サービス ポリシー
- アクセス コントロール リスト (ACL)

インターフェイスがポートチャネルに参加または脱退しても、次に示す多くのインターフェイスパラメータは影響を受けません。

- ビーコン
- 説明
- CDP
- LACP ポート プライオリティ
- Debounce
- UDLD
- MDIX
- レート モード
- シャットダウン
- SNMP トラップ



(注) ポートチャネルを削除すると、すべてのメンバインターフェイスはポートチャネルから削除されたかのように設定されます。



(注) ポートチャネル上のすべてのQoSサービスポリシーは、ポートチャネルに加入すると、暗黙的にメンバーポートに適用されます。メンバーポートの実行コンフィギュレーションにQoSサービスポリシーは表示されません。show policy-map interface ethernet <slot/port> コマンドを使用すると、メンバーポートに適用されているポリシーが表示されます。

ポートチャネルモードについては、「LACPマーカーレスポнда」の項を参照してください。

ポートチャネルを使ったロードバランシング

Cisco NX-OS ソフトウェアは、ポートチャネルにおけるすべての動作インターフェイス間のトラフィックをロードバランシングします。その際、フレーム内のアドレスをハッシュして、チャネル内の1つのリンクを選択する数値にします。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。ポートチャネルロードバランシングでは、MACアドレス、IPアドレス、またはレイヤ4ポート番号を使用してリンクを選択します。ポートチャネルロードバランシングは、送信元または宛先アドレスおよびポートの両方またはどちらか一方を使用します。

ロードバランシングモードを設定して、デバイス全体に設定したすべてのポートチャネルに適用することができます。デバイス全体で1つのロードバランシングモードを設定できます。ポートチャネルごとにロードバランシング方式を設定することはできません。

使用するロードバランシングアルゴリズムのタイプを設定できます。ロードバランシングアルゴリズムを指定し、フレームのフィールドを見て出力トラフィックに選択するメンバーポートを決定します。

レイヤ3インターフェースのデフォルトロードバランシングモードは、発信元および宛先 IP L4 ポートです。非 IP トラフィックのデフォルトロードバランシングモードは、送信元および宛先 MAC アドレスです。**port-channel load-balance** コマンドを使用し、して、チャネルグループバンドルのインターフェース間のロードバランシング方式を設定します。レイヤ2パケットのデフォルト方式は **src-dst-mac** です。レイヤ3パケットのデフォルトの方式は **src-dst-ip-l4** です。

次のいずれかの方式を使用するデバイスを設定し、ポートチャネル全体をロードバランシングできます。

- 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
- 送信元 TCP/UDP ポート番号
- 宛先 TCP/UDP ポート番号
- 送信元および宛先 TCP/UDP ポート番号
- 送信元、宛先、および送信元と宛先の GRE 内部 IP ヘッダー

非 IP およびレイヤ3ポートチャネルはどちらも設定したロードバランシング方式に従い、発信元、宛先、または発信元および宛先パラメータを使用します。たとえば、発信元 IP アドレスを使用するロードバランシングを設定すると、すべての非 IP トラフィックは発信元 MAC アドレスを使用してトラフィックをロードバランシングしますが、レイヤ3トラフィックは発信元 IP アドレスを使用してトラフィックをロードバランシングします。同様に、宛先 MAC アドレスをロードバランシング方式として設定すると、すべてのレイヤ3トラフィックは宛先 IP アドレスを使用しますが、非 IP トラフィックは宛先 MAC アドレスを使用してロードバランシングします。



(注) ハッシュロードバランシングの設定は、Cisco Nexus 9200、9300-EX、および9300-GX シリーズスイッチのユニキャストおよびマルチキャストトラフィックに適用されます。

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。

マルチキャストトラフィックは、次の方式を使用してポートチャネルのロードバランシングを行います。

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



(注) Cisco IOS を実行するデバイスは、**port-channel hash-distribution** コマンドによって単一のメンバーに障害が発生した場合、メンバーポートASICの動作を最適化できます。Cisco Nexus 9000 シリーズのデバイスはこの最適化をデフォルトで実行し、このコマンドを必要とせず、またサポートしません。Cisco NX-OS は、デバイス全体に対して、**port-channel load-balance** コマンドによるポートチャネル上のロードバランシング基準のカスタマイズをサポートします。

シンメトリックハッシング

ポートチャネル上のトラフィックを効果的にモニタできるようにするには、ポートチャネルに接続された各インターフェイスが、順方向と逆方向の両方のトラフィックフローを受信することが不可欠です。通常、順方向および逆方向のトラフィックフローが同じ物理インターフェイスを使用する保証はありません。ただし、ポートチャネルで対称ハッシュを有効にすると、双方向トラフィックは同じ物理インターフェイスを使用するように強制され、ポートチャネルの各物理インターフェイスは一連のフローに効果的にマッピングされます。

対称ハッシュを有効にすると、送信元および宛先IPアドレスなどのハッシュに使用されるパラメータは、ハッシュアルゴリズムに入力される前に正規化されます。このプロセスにより、パラメータが逆になった場合（順方向トラフィックの送信元が逆方向トラフィックの宛先になる）、ハッシュ出力は同じになります。したがって、同じインターフェイスが選択されます。

次のロードバランシングアルゴリズムがシンメトリックハッシングをサポートします。

- `src-dst ip`
- `src-dst ip-l4port`

ECMPの注意事項と制限事項

レイヤ2/レイヤ3 GWフローでのロードバランシングは、リロード後にスイッチが最初に起動したときに、すべてのリンク間で均等にロードバランシングされないことがあります。ハードウェアのECMPハッシュ設定を変更するには、2つのCLIがあります。これらのコマンドは相互に排他的です。

- MAC ベースのみのハッシュの **port-channel load-balance [src | src-dst | dst] mac** コマンドを入力します。
- IP/レイヤ4ポートに基づくハッシュの場合は、**ip load-share** または **port-channel load-balance** コマンドを入力します。
- **port-channel load-balance** コマンドは **ip load-share** コマンドを上書きできます。IPパラメータとMACパラメータの両方を設定するのに役立つ **port-channel load-balance** コマンドを入力することをお勧めします。
- IP/レイヤ4ポートに基づいてハッシュアルゴリズムを強制するオプションはありません。デフォルトのMAC設定は、常にポートチャネル設定の一部としてプログラムされます。
- トンネル上のトラフィックフローでは、ECMPの復元力のあるハッシュはサポートされません。

復元力のあるハッシュ

データセンターで使用される物理リンクの数が急増すると、障害物理リンクの数も増加する可能性があります。ポートチャネルまたは等コストマルチパス (ECMP) グループのメンバー間でフローをロードバランシングするために使用されるスタティックハッシュシステムでは、各フローがリンクにハッシュされます。あるリンクで機能不全が発生すると、残った実行リンクでは、すべてのフローが再ハッシュされます。リンクへのフローのこの再ハッシュにより、障害が発生したリンクにハッシュされなかったフローであっても、一部の packets が順序どおりに配信されなくなります。

の再ハッシュは、リンクがポートチャネルまたは等コストマルチパス (ECMP) グループに追加された場合にも発生します。すべてのフローが新しいリンク数で再ハッシュされるため、一部の packets は順序どおりに配信されません。

復元力のあるハッシュは、物理ポートにフローをマッピングし、ECMPグループとポートチャネルインターフェイスの両方でサポートされます。

物理的リンクに障害が発生すると、障害リンクに割り当てられているフローは、残りの動作中のリンク間で均等に再分配されます。動作中のリンクを流れる既存のフローは再ハッシュされないため、影響を受けません。

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

復元力のあるハッシュは、すべての Cisco Nexus 9000 シリーズプラットフォームでサポートされます。。 Cisco NX-OS リリース 9.3(3) 以降、復元力のあるハッシュは、Cisco Nexus 92160YC-X、92304QC、9272Q、9232C、9236C、92300YC スイッチでサポートされます。

GTP トンネル ロード バランシング

GPRS トンネリング プロトコル (GTP) は、コア ルータとして Cisco Nexus 9000 シリーズ スイッチを介してワイヤレス ネットワーク上のモバイル データを配信するために使用されます。GTP トラフィックを伝送する 2 つのルータがリンク バンドリングで接続されている場合、トラフィックはすべてのバンドル メンバー間で均等に分散される必要があります。

ロード バランシングを実現するために、Cisco Nexus 9000 シリーズ スイッチは 5 タプルのロード バランシング メカニズムを使用します。ロード バランシング メカニズムでは、パケットの送信元 IP、宛先 IP、プロトコル、レイヤ 4 リソース、および宛先ポート (トラフィックが TCP または UDP の場合) フィールドが考慮されます。GTP トラフィックの場合は、これらのフィールドへの一意の値の数が限られていると、トンネルでのトラフィック ロードの均等分散が制限されます。

ロード バランシングにおける GTP トラフィックの偏波を回避するために、GTP ヘッダーのトンネル エンドポイント ID (TEID) が UDP ポート番号の代わりに使用されます。TEID がトンネルごとに異なるため、トラフィックをバンドルの複数のリンク間で均等にロード バランシングすることができます。

Cisco Nexus リリース 9.3(3) GTP トンネル ロード バランシングの開始は、9700-EX および 9700-FX ラインカードを搭載した Cisco Nexus 9500 プラットフォーム スイッチでサポートされます。ただし、IPv6 フローの GTP トンネル ロード バランシングは、FM-E2 ファブリック モジュールを搭載した Cisco Nexus 9500 プラットフォーム スイッチでのみサポートされます。それは、FM-E ファブリック モジュールをもつ Cisco Nexus 9500 プラットフォーム スイッチではサポートされません。ハードウェア制御はポートチャネルと ECMP の両方で同じであるため、GTP オプションを使用して `port-channel load-balance` または `ip load-sharing` を有効にすると、両方のケースで GTP TEID ベースのロード バランシングが有効になります。マルチカプセル化パケットでは、GTP ヘッダーが外部ヘッダーの一部である場合、ハッシュのために外部レイヤから GTP TEID を取得します。GTP ヘッダーが内部ヘッダーの一部である場合、内部レイヤから GTP TEID を取得してハッシュします。

GTP トンネル ロード バランシングは、Cisco Nexus 9300-EX、9300-FX、9300-FX2、9394C、および 9300-GX プラットフォーム スイッチでサポートされます。

この機能は、GTPU パケットに存在する 32 ビット TEID 値で送信元および宛先ポート情報を上書きします。

GTP トンネルのロード バランシング機能により、次のサポートが追加されます。

- 物理インターフェイスでの IPv4/IPv6 トランスポート ヘッダーによる GTP
- TE トンネルを介した GTP トラフィック
- UDP ポート 2152 を使用した GTPU

ip load-sharing address source-destination gtpu コマンドは、GTP トンネル ロード バランシングをイネーブルにします。

ロードバランシング後の GTP トラフィックの出力インターフェイスを確認するには、L4 プロトコルの送信元および宛先ポート番号の代わりに TEID を指定して **show cef {ipv4 | ipv6} exact-route** コマンドを使用します。送信元ポートで TEID の 16MSBist、宛先ポートで TEID の 16LSBits を使用します。

port-channel load-balance src-dst gtpu コマンドは、UDP 宛先ポート番号 2152 の GTP パケットをイネーブルにして、GTP TEID 値に基づいてロードバランシングを行います。このコマンドは、外側の 5 つのタプル (*src-ip*、*dst-ip*、*ip proto*、*L4 sport*、*L4 dport*) が同じであっても、スイッチが GTP パケットのロードバランシングを行えるようにします。ハードウェア制御はポートチャネルと ECMP の両方で同じであるため、GTP オプションを使用して **port-channel load-balance** または **ip load-sharing** を有効にすると、GTP TEID ベースのロードバランシングが有効になります。

- **port-channel load-balance src-dst gtpu** コマンドは、VXLAN カプセル化の有無にかかわらず、両方の GTP パケットに適用できます。
- GTP ヘッダーが外部レイヤの一部である場合、**port-channel load-balance src-dst gtpu** コマンドはハッシュのために外部レイヤから GTP TEID を取得します。
- GTP ヘッダーが内部レイヤの一部である場合、**port-channel load-balance src-dst gtpu** コマンドはハッシュのために内部レイヤから GTP TEID を取得します。

show port-channel load-balance forwarding-path コマンドを使用する場合は、プロトコルフィールドを 17 に設定し、他のパラメータの値を設定する必要があります。次に例を示します。

```
switch(config)# show port-channel load-balance forwarding-path interface port-channel 2
src-ip 1.1.1.1 dst-ip 2.2.2.2 gtpteid
0x3 protocol 17
```

LACP

LACP では、最大 16 のインターフェイスを 1 つのポートチャネルに設定できます。

LACP の概要

イーサネットのリンクアグリゲーション制御プロトコル (LACP) は、IEEE 802.1AX および IEEE 802.3ad で定義されています。このプロトコルは、物理ポートをまとめて 1 つの論理チャネルを形成する方法を制御します。

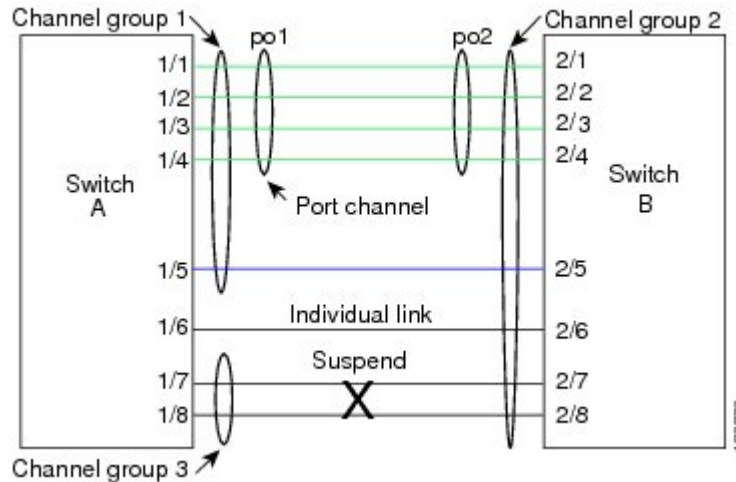


- (注) LACP は、使用する前にイネーブルにする必要があります。デフォルトでは、LACP はディセーブルです。LACP のイネーブル化については、「LACP のイネーブル化」の項を参照してください。

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。ロールバックおよびチェックポイントについては、『Cisco Nexus 9000 Series NX-OS System Management Configuration Guide』を参照してください。

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

図 10: 個々のリンクをポートチャネルに組み込む



LACP では、最大 16 のインターフェイスを 1 つのチャネルグループにまとめることができます。



(注) ポートチャネルを削除すると、ソフトウェアは関連付けられたチャネルグループを自動的に削除します。すべてのメンバインターフェイスはオリジナルの設定に戻ります。

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。

ポートチャネルモード

ポートチャネルの個別インターフェイスは、チャネルモードで設定します。スタティックポートチャネルを集約プロトコルを使用せずに実行すると、チャネルモードは常に **on** に設定されます。デバイス上で LACP をグローバルにイネーブルにした後、各チャネルの LACP をイネーブルにします。それには、各インターフェイスのチャネルモードを **active** または **passive** に設定します。チャネルグループにリンクを追加すると、LACP チャネルグループの個別リンクにチャネルモードを設定できます。



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

次の図は、チャネルモードをまとめたものです。

表 12: 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	LACPはこのポートチャネルでイネーブルになっており、ポートはパッシブネゴシエーション状態になっています。ポートは受信したLACPパケットに応答しますが、LACPネゴシエーションは開始しません。
active	LACPはこのポートチャネルでイネーブルになっており、ポートはアクティブネゴシエーション状態です。アクティブモードでは、ポートはLACPパケットを送信することによって他のポートとのネゴシエーションを開始します。
on	LACPはこのポートチャネルでディセーブルであり、ポートは非ネゴシエーション状態です。ポートチャネルが on 状態であることは、スタティックモードであることを表します。 ポートはポートチャネルメンバーシップの確認またはネゴシエートを行いません。LACPをイネーブルにする前にチャネルモードをアクティブまたはパッシブにしようとする、デバイス表示はエラーメッセージを表示します。LACPは、 on 状態のインターフェイスとネゴシエートする場合、LACPパケットを受信しないため、そのインターフェイスと個別のリンクを形成します。つまり、LACPチャネルグループには参加しません。 on 状態が、デフォルトポートチャネルモードです。

LACPは、パッシブおよびアクティブモードの両方でポート間をネゴシエートして、ポート速度やランキングステートなどを基準にしてポートチャネルを形成できるかどうかを決定します。パッシブモードは、リモートシステムやパートナーがLACPをサポートするかどうか不明の場合に役に立ちます。

次の例のようにモードに互換性がある場合、ポートのLACPモードが異なれば、2つのデバイスはLACPポートチャネルを形成できます。

表 13: チャネルモードの互換性

デバイス 1 > ポート-1	デバイス 2 > ポート-2	結果
アクティブ	アクティブ	ポートチャネルを形成できます。
Active	Passive	ポートチャネルを形成できます。
パッシブ	パッシブ	ネゴシエーションを開始できるポートがないため、ポートチャネルを形成できません。
点灯	アクティブ	LACP が片側でのみ有効になっているため、ポートチャネルを形成できません。
点灯	パッシブ	LACP が有効になっていないため、ポートチャネルを形成できません。

LACP ID パラメータ

ここでは、LACP パラメータについて説明します。

LACP システム プライオリティ

LACP を実行するどのシステムにも LACP システム プライオリティ値があります。このパラメータのデフォルト値である 32768 をそのまま使用するか、1 ~ 65535 の範囲で値を設定できます。LACP は、このシステム プライオリティと MAC アドレスを組み合わせることでシステム ID を生成します。また、システム プライオリティを他のデバイスとのネゴシエーションにも使用します。システム プライオリティ値が大きいほど、プライオリティは低くなります。



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

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ポートにはそれぞれ LACP ポート プライオリティがあります。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ポートごとに、チャンネルグループ番号と同じ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 レートやデュプレックス性能などです。
- ユーザが作成した設定に関する制約事項

LACP マーカー レスポンド

ポートチャネルを使用すればデータトラフィックを動的に再配布できます。この再配布により、リンクが削除または追加されたり、ロードバランシングスキームが変更されることもあります。トラフィックフローの途中でトラフィックが再配布されると、フレームの順序が乱れる可能性があります。

LACP は Marker Protocol を使って、再配布によってフレームが重複したり順番が入れ替わらないようにします。Marker Protocol は、所定のトラフィックフローのすべてのフレームがリモートエンドで正しく受信すると検出します。LACP はポートチャネルリンクごとに Marker PDU を送信します。リモートシステムは、Marker PDU よりも先にこのリンクで受信されたすべてのフレームを受信すると、Marker PDU に応答します。リモートシステムは次に Marker Responder を送信します。ポートチャネルのすべてのメンバリンクの Marker Responder を受信したローカルシステムは、トラフィックフローのフレームを正しい順序で再配分します。ソフトウェアは Marker Responder だけをサポートします。

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

次の表に、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主な相違点を示します。

表 14: 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	N/A
リンクのチャンネルモード	次のいずれか <ul style="list-style-type: none"> • Active • Passive 	On だけ

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
チャネルを構成する最大リンク数	32	32

LACP 互換性の拡張

Cisco Nexus 9000 シリーズのデバイスが非 Nexus ピアに接続されている場合、そのグレースフルフェールオーバーのデフォルトが、無効にされたポートがダウンになるための時間を遅らせる可能性があります。また、ピアからのトラフィックを喪失する原因にもなります。これらの条件に対処するため、**lacp graceful-convergence** コマンドが追加されました。

デフォルトで、ピアから LACP PDU を受信しない場合、ポートは一時停止状態に設定されます。**lacp suspend-individual** は Cisco Nexus 9000 シリーズ スイッチではデフォルト設定です。このコマンドは、LACP PDU を受信しない場合、ポートを中断状態にします。場合によっては、この機能は誤設定によって作成されるループの防止に役立ちますが、サーバが LACP にポートを論理的アップにするように要求するため、サーバの起動に失敗する原因になることがあります。**no lacp suspend-individual** コマンドを使用して、ポートを個別の状態に設定できます。個々に設定されているポートは、ポート設定に基づいて個々のポートの属性を取得します。

LACP ポートチャネルは、サーバとスイッチを接続すると、リンクの迅速なバンドルのために LACP PDU を交換します。ただし、PDU が受信されない場合は、リンクが中断状態になります。

delayed LACP 機能により、LACP PDU の受信前に 1 つのポートチャネルメンバー（遅延 LACP ポート）がまず通常のポートチャネルのメンバーとしてアップできます。このメンバーが LACP モードで接続した後に、他のメンバー（補助 LACP ポート）がアップします。これにより、PDU が受信されない場合にリンクが中断状態になることが回避されます。

ポートチャネルのどのポートが最初に起動するかは、ポートのポートプライオリティ値によって決まります。プライオリティ値が最も低いポートチャネルのメンバーリンクが、LACP 遅延ポートとして最初に起動します。リンクの動作ステータスに関係なく、LACP ポートに設定されたプライオリティが使用され、遅延 lacp ポートが選択されます。

この機能は、レイヤ 2 ポートチャネル、トランク モード スパニング ツリー、および vPC をサポートします。

- 同じポートチャネルで **no lacp suspend-individual lacp mode delay** を使用することは、非 lacp 遅延ポートを個別の状態にする可能性があるため、推奨されません。ベストプラクティスとして、これら 2 つの設定を組み合わせないようにする必要があります。
- レイヤ 3 ポートチャネルではサポートされません。
- Cisco Nexus 9500 スイッチおよび FEX HIF および FEX ファブリック ポートではサポートされません。

LACP ポートチャネルの最小リンクおよび MaxBundle

ポートチャネルは、同様のポートを集約し、単一の管理可能なインターフェイスの帯域幅を増加させます。

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

LACP ポートチャネルの最小リンク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アップし、バンドルする必要があるポートの最小数を設定します。
- 低帯域幅の LACP ポートチャネルがアクティブにならないようにします。
- 必要な最小帯域幅を提供するアクティブメンバーポートが少数の場合、LACP ポートチャネルが非アクティブになります。

LACP MaxBundle は、LACP ポートチャネルで許可されるバンドルポートの最大数を定義します。

LACP MaxBundle 機能では、次の処理が行われます。

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



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

LACP 高速タイマー

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。LACP 高速タイマーレートを設定するには、「LACP 高速タイマーレートの設定」の項を参照してください。

ポートチャネルメンバーポートで LACP 高速タイマーレートが設定されている場合、LACP PDU は毎秒交換されます。3つの連続した LACP PDU が失われると、タイムアウトが発生します。システムのスイッチオーバーおよび ISSU 中に、LACP PDU が 1 秒間隔で送信されないことがあります。これにより、タイムアウトが発生し、ピアポートが再初期化されることがあります。Cisco NX-OS リリース 9.3(1) 以降、次の Cisco Nexus 9500 シリーズスイッチは、ユーザが開始したシステムスイッチオーバー中に LACP 高速タイマーをサポートします。

- N9K-C9504-FM-E、N9K-C9508-FM-E、N9K-C9506-FM-E2、またはN9K-C9516-FM-E2 ファブリック モジュールを搭載した Cisco Nexus 9500 シリーズ スイッチ
- Cisco Nexus 9500 シリーズ スイッチ (N9K-X9736C-EX、N9K-X9732C-EX、N9K-X9732C-FX、N9K-X97160YC-EX、N9K-X9732C-EXM、N9K-X9736C-FX、N9K-X9788TC-FX、または N9K-X97284YC-FX ライン カード搭載)

ISSU および非グレースフル スイッチオーバーは、LACP 高速タイマーではサポートされません。

仮想化のサポート

メンバポートと他のポートチャネルに関連する設定は、ポートチャネルとメンバポートを持つ仮想デバイス コンテキスト (VDC) で設定します。各 VDC で 1 ~ 4096 の番号を使用してポートチャネルに番号を付けることができます。

1つのポートチャネルのすべてのポートは同じ VDC に置く必要があります。LACP を使用する場合、8つすべてのアクティブポートと8つすべてのスタンバイポートは同じ VDC である必要があります。



-
- (注) デフォルト VDC のポートチャネルを使用するロードバランシングを設定する必要があります。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用したロードバランシング」の項を参照してください。
-

高可用性

ポートチャネルは、複数のポートのトラフィックをロードバランシングすることでハイアベイラビリティを実現します。物理ポートが故障した場合、ポートチャネルのメンバがアクティブであればポートチャネルは引き続き動作します。モジュール間の設定が共通しているため、異なるモジュールのポートをバンドルして、モジュール故障時にも動作するポートチャネルを作成できます。

ポートチャネルは、ステートフル再起動とステートレス再起動をサポートします。ステートフル再起動はスーパーバイザ切り替え時に発生します。切り替え後、Cisco NX-OS ソフトウェアは実行時の設定を適用します。

動作しているポート数が設定された最小リンク数を下回った場合、ポートチャネルはダウンします。



-
- (注) ハイアベイラビリティ機能の詳細については、『Cisco Nexus 9000 Series NX-OS High Availability and Redundancy Guide』を参照してください。
-

ポートチャネリングの前提条件

ポートチャネリングには次の前提条件があります。

- デバイスにログインしていること。
- シングルポートチャネルのすべてのポートは、レイヤ2またはレイヤ3ポートであること。
- シングルポートチャネルのすべてのポートが、互換性の要件を満たしていること。互換性要件の詳細については、「互換性要件」の項を参照してください。
- デフォルトVDCのロードバランシングを設定すること。

注意事項と制約事項

ポートチャネル設定時のガイドラインおよび制約事項は、次のとおりです。

- Gen 1 ラインカードを備えた Cisco Nexus 9516 スイッチでの拡張ポートチャネルの導入では、コマンドの後にコマンドとコマンドを使用する必要があります。**port-channel scale-fanout copy run start reload**
- キーワードが付いている **show** コマンド **internal** はサポートされていません。
- LACP ポートチャネルの最小リンクおよび **maxbundle** 機能は、ホストインターフェイスポートチャネルではサポートされていません。
- この機能を使用する前に LACP をイネーブルにする必要があります。
- デバイスに複数のポートチャネルを設定できます。
- 共有および専用ポートは同じポートチャネルに設定できません（共有ポートおよび専用ポートについては、「基本インターフェイスパラメータ章の設定」を参照してください）。
- レイヤ2ポートチャネルでは、ポートに互換性が設定されていれば、STP ポートパスコストが異なる場合でもポートチャネルを形成できます。互換性要件の詳細については、「互換性要件」の項を参照してください。
- L3 ポートチャネルインターフェイス間に L2 ePBR が構成されている場合、LACP パケットが ePBR デバイスでドロップされるため、ポートチャネルは起動しません。
- カプセル化された NVGRE パケットで IPv6 トラフィックを送信する場合、トラフィックは使用可能なすべてのアップリンクでロードシェアリングされるわけではありません。1つのアップリンクのみが使用されます。ただし、IPv4 カプセル化 NVGRE トラフィックでは、トラフィックはすべてのアップリンクに送信されます。これは、Cisco NXOS リリース 10.1(1) の Cisco Nexus 9300-FX3 スイッチプラットフォームに適用されます。
- STP では、ポートチャネルのコストはポートメンバーの集約帯域幅に基づきます。

- ポートチャネルを設定した場合、ポートチャネルインターフェイスに適用した設定はポートチャネルメンバポートに影響を与えます。メンバポートに適用した設定は、設定を適用したメンバポートにだけ影響します。
- LACPは半二重モードをサポートしません。LACPポートチャネルの半二重ポートは中断ステートになります。
- ポートチャネルグループに属するポートはプライベートVLANポートとして設定しないでください。ポートがプライベートVLANの設定に含まれている間は、そのポートチャネルの設定は非アクティブになります。
- チャネルメンバポートを発信元または宛先SPANポートにできません。
- ポートチャネルは、第1世代100Gラインカード（N9K-X9408PC-CFP2）または汎用拡張モジュール（N9K-M4PC-CFP2）ではサポートされていません。
- ポートチャネルは、第2世代（以降）の100Gインターフェイスを備えたデバイスでサポートされます。
- ポートチャネルは、Cisco Nexus 9300 および 9500 シリーズデバイスのアプリケーションリーフエンジン（ALE）アップリンクポートに関する制約事項の影響を受ける可能性があります（「[ALE アップリンクポートに関する制約事項](#)」）。
- ポートチャネルの復元ハッシュは、Cisco Nexus 9200、Cisco Nexus 9300-EX、および9700-EXラインカードを搭載したCisco Nexus 9500 スイッチではサポートされません。
- 復元力のあるハッシュ（ポートチャネルロードバランシング復元力）およびVXLAN設定は、ALEアップリンクポートを使用したVTEPと互換性がありません。



(注) 復元力のあるハッシュはデフォルトではディセーブルになっています。

- サテライト/FEXポートのサブインターフェイスの最大数は63です。
- Cisco Nexus 92300YC スイッチでは、同じクワドラントの一部である最初の24個のポート。同じクワドラントのすべてのポートは同じ速度である必要があります。クワドラント内のポートで異なる速度を使用することはサポートされていません。次に、同じクワドラントを共有するCisco Nexus 92300YCスイッチの最初の24個のポートを示します。
 - 1,4,7,10
 - 2,5,8,11
 - 3,6,9,12
 - 13,16,19,22
 - 14,17,20,23
 - 15,18,21,24

- X96136YC-R ラインカードを搭載した Cisco Nexus 9500 スイッチでは、ポート 17 ~ 48 は同じクワドラントの一部です。同じクワドラントのポートは、すべてのポートで同じ速度 (1/10G または 25G) である必要があります。クワドラント内のポートで異なる速度を使用することはサポートされていません。クワドラントのいずれかのポートに異なる速度を設定すると、ポートはエラーディセーブル状態になります。同じクワドラントのインターフェイスは次のとおりです。
 - 17 ~ 20
 - 21 ~ 24
 - 25 ~ 28
 - 29 ~ 32
 - 33 ~ 36
 - 37 ~ 40
 - 41 ~ 44
 - 45 ~ 48
- レジリエント ハッシュは、N9K-X9636C-R、N9K-X9636Q-R、N9K-X9636C-RX、および N9K-X96136YC-R ラインカードを搭載した Cisco Nexus 9500 Series スイッチでサポートされています。
- ポートチャネル対称ハッシュは、Cisco Nexus 9200、9300-EX、9300-FX/FX2、および 9300-GX プラットフォーム スイッチと、N9K-X9732C-EX、N9K-X9736C-EX、N9K-X9736C-FX、および N9K-X9732C-FX ラインカードを搭載した Cisco Nexus 9500 プラットフォーム スイッチでサポートされています。
- ECMP 対称ハッシュは、Cisco Nexus 9200、9300-EX、および 9300-FX/FX2/FX3 プラットフォーム スイッチと、N9K-X9732C-EX、N9K-X9736C-EX、N9K-X9736C-FX、および N9K-X9732C-FX ラインカードを搭載した Cisco Nexus 9500 プラットフォーム スイッチでサポートされています。
- GRE 内部ヘッダーは、次のスイッチでサポートされます。
 - Cisco Nexus 9364C プラットフォーム スイッチ
 - Cisco Nexus 9336C-FX2、9348GC-FXP、93108TC-FX、93180YC-FX、および 93240YC-FX2 プラットフォーム スイッチ
 - Cisco Nexus 9300-GX プラットフォーム スイッチ
 - Cisco Nexus 9300-FX3 プラットフォーム スイッチ
 - N9K-X9736C-FX ラインカードを搭載した Cisco Nexus 9500 プラットフォーム スイッチ

- Cisco NX-OS リリース 9.3(6) 以降では、Cisco Nexus 9300-FX2 プラットフォーム スイッチは VXLAN および IP-in-IP トンネリングの共存をサポートします。制限事項を含む詳細については、「**VXLAN and IP-in-IP Tunneling**」の項（『Cisco Nexus 9000 Series NX-OS VXLAN Configuration Guide, Release 9.3(x)』）を参照してください。
- Cisco Nexus 9000 NX-OS リリース 10.2 (1) 以降、admin up 状態のポートチャネルで設定が許可されます。**[no] lacp suspend-individual** この機能は、すべての Cisco Nexus 9000 シリーズ プラットフォーム スイッチでサポートされています。
- Cisco Nexus 9000 NX-OS リリース 10.2 (1) 以降、この設定は PXE ブートをサポートし、サーバの設定ミスによる L2 ループを防止します。**[no] lacp suspend-individual pxe** この設定では、通常のポートチャネルと vPC ピアの両方で 1 つのポートチャネルメンバーのみを個別 (I) 状態にすることができます。とは同じ設定で、show lacp suspend-individual として実行されている show に表示されます。**lacp suspend-individual lacp suspend-individual pxe** vPC サブシステムの場合、この設定は両方の vPC レッグに適用する必要があります。そうでない場合は、vPC セカンダリがダウンします。この機能は、すべての Cisco Nexus 9000 シリーズ プラットフォーム スイッチでサポートされています。ただし、FEX はサポートされていません。
- LACP を使用する FEX インターフェイスの場合、FEX インターフェイスのすべての DME 操作/ランタイム プロパティは更新されません。FEX ポートのすべてのランタイムアップデートは、FEX LACP プロセス コンテキストから発生し、親スイッチに通信されません。これは、1 日目の動作です。
- Cisco NX-OS リリース 10.3(1)F 以降、src/dst ip および src/dst L4 ポート番号に基づくハッシュは、Cisco Nexus 9808 プラットフォーム スイッチでサポートされます。
- Cisco NX-OS リリース 10.4(1) 以降、LACP レイヤ 3 ポートチャネルは Nexus 9800 シリーズ スイッチでサポートされます。
- Cisco NX-OS リリース 10.4(1)F 以降、src/dst ip および src/dst L4 ポート番号に基づくハッシュは、Cisco Nexus 9804 プラットフォーム スイッチでサポートされます。
- Cisco NX-OS リリース 10.4(1)F 以降、Cisco Nexus 9808 および 9804 スイッチを搭載した N9KX98900CD-A および N9KX9836DM-A ラインカードに基づくハッシュ。
- Cisco NX-OS リリース 10.4(1)F 以降、src/dst ip および src/dst L4 ポート番号に基づくハッシュは、Cisco Nexus 9808 および 9804 スイッチを搭載した N9KX98900CD-A および N9KX9836DM-A ラインカードでサポートされます。

デフォルト設定

次の表に、ポートチャネルパラメータのデフォルト設定を示します。

表 15: デフォルトポートチャネルパラメータ

パラメータ	デフォルト
ポートチャネル	管理アップ
レイヤ3 インターフェイスのロードバランシング方式	送信元および宛先 IP アドレス
レイヤ2 インターフェイスのロードバランシング方式	送信元および宛先 MAC アドレス
モジュールごとのロードバランシング	ディセーブル
LACP	ディセーブル
チャンネルモード	on
LACP システムプライオリティ	32768
LACP ポートプライオリティ	32768
LACP 用最少リンク数	1
Maxbundle	32
FEX ファブリックポートチャネル用最少リンク数	1

ポートチャネルの設定



- (注) ポートチャネルインターフェイスに最大伝送単位 (MTU) を設定する手順については、「基本インターフェイスパラメータの設定」の章を参照してください。ポートチャネルインターフェイスに IPv4 および IPv6 アドレスを設定する手順については、「レイヤ3 インターフェイスの設定」の章を参照してください。



- (注) Cisco IOS の CLI に慣れている場合、この機能に対応する Cisco NX-OS コマンドは通常使用する Cisco IOS コマンドと異なる場合がありますので注意してください。

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。関連するチャネルグループは自動的に作成されます。



- (注) ポートチャネルがチャネルグループの前に作成されると、ポートチャネルは、メンバーインターフェイスが設定されるインターフェイス属性のすべてを使用して設定される必要があります。 **switchport mode trunk** {*allowed vlan vlan-id* | *native vlan-id*} コマンドを使用して、メンバーを設定します。

これは、チャネルグループのメンバがレイヤ2ポート (switchport) およびトランク (switchport mode trunk) の場合にのみ必要です。



- (注) **no interface port-channel** コマンドを使用して、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。

コマンド	目的
no interface port-channel <i>channel-number</i> 例 : switch(config)# no interface port-channel 1	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。

始める前に

LACP ベースのポートチャネルにする場合は LACP をイネーブルにします。

手順の概要

1. **configure terminal**
2. **interface port-channel** *channel-number*
3. **show port-channel summary**
4. **no shutdown**
5. **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	configure terminal 例 : switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します

	コマンドまたはアクション	目的
ステップ 2	interface port-channel <i>channel-number</i> 例： <pre>switch(config)# interface port-channel 1 switch(config-if)</pre>	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。Cisco NX-OS ソフトウェアは、チャンネルグループがない場合はそれを自動的に作成します。
ステップ 3	show port-channel summary 例： <pre>switch(config-router)# show port-channel summary</pre>	(任意) ポートチャネルに関する情報を表示します。
ステップ 4	no shutdown 例： <pre>switch# configure terminal switch(config)# int e3/1 switch(config-if)# no shutdown</pre>	(任意) ポリシーがハードウェアポリシーと一致するインターフェイスおよびVLANのエラーをクリアします。このコマンドにより、ポリシープログラミングが続き、ポートがアップできます。ポリシーが対応していない場合は、エラーはerror-disabledポリシー状態になります。
ステップ 5	copy running-config startup-config 例： <pre>switch(config)# copy running-config startup-config</pre>	(任意) 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

例

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
```

ポートチャネルを削除したときにインターフェイス設定がどのように変わるかの詳細については、「互換性要件」の項を参照してください。

レイヤ2ポートをポートチャネルに追加

新しいチャンネルグループまたはすでにレイヤ2ポートを含むチャンネルグループにレイヤ2ポートを追加できます。ポートチャネルがない場合は、このチャンネルグループに関連付けられたポートチャネルが作成されます。



(注) **no channel-group** コマンドを使用して、チャンネルグループからポートを削除します。

コマンド	目的
no channel-group 例 : <pre>switch(config)# no channel-group</pre>	チャンネルグループからポートを削除します。

始める前に

LACP ベースのポートチャネルにする場合は LACP をイネーブルにします。

すべてのレイヤ2メンバポートは、全二重モードで同じ速度で実行されている必要があります。

手順の概要

1. **configure terminal**
2. **interface** *type slot/port*
3. **switchport**
4. **switchport mode trunk**
5. **switchport trunk** {**allowed vlan** *vlan-id* | **native** *vlan-id*}
6. **channel-group** *channel-number* [**force**] [**mode** {**on** | **active** | **passive**}]
7. **show interface** *type slot/port*
8. **no shutdown**
9. **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	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface <i>type slot/port</i> 例 : <pre>switch(config)# interface ethernet 1/4 switch(config-if)#</pre>	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	switchport 例 : <pre>switch(config)# switchport</pre>	インターフェイスをレイヤ2アクセスポートとして設定します。

	コマンドまたはアクション	目的
ステップ 4	switchport mode trunk 例： switch(config)# switchport mode trunk	(任意) インターフェイスをレイヤ2 トランク ポートとして設定します。
ステップ 5	switchport trunk {allowed vlan vlan-id native vlan-id} 例： switch(config)# switchport trunk native 3 switch(config-if)#	(任意) レイヤ2 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 6	channel-group channel-number [force] [mode {on active passive}] 例： <ul style="list-style-type: none"> • switch(config-if)# channel-group 5 • switch(config-if)# channel-group 5 force 	チャンネルグループ内にポートを設定し、モードを設定します。channel-number の指定できる範囲は 1 ~ 4096 です。ポートチャネルがない場合は、このチャンネルグループに関連付けられたポートチャネルが作成されます。すべてのスタティックポートチャネルインターフェイスは、 on モードに設定されます。すべての LACP 対応ポートチャネルインターフェイスを active または passive に設定する必要があります。デフォルトモードは on です。 (任意) 一部の設定に互換性がないインターフェイスをチャンネルに追加します。強制されるインターフェイスは、チャンネルグループと同じ速度、デュプレックス、およびフロー制御設定を持っている必要があります。 (注) force オプションは、ポートにポートチャネルの他のメンバーとの QoS ポリシーの不一致がある場合に失敗します。
ステップ 7	show interface type slot/port 例： switch# show interface port channel 5	(任意) インターフェイスの内容を表示します。
ステップ 8	no shutdown 例： switch# configure terminal switch(config)# int e3/1 switch(config-if)# no shutdown	(任意) ポリシーがハードウェアポリシーと一致するインターフェイスおよびVLANのエラーをクリアします。このコマンドにより、ポリシープログラミングが続行でき、ポートがアップできます。ポリシーが対応していない場合は、エラーはerror-disabledポリシー状態になります。
ステップ 9	copy running-config startup-config 例： switch(config)# copy running-config startup-config	(任意) 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

例

次に、レイヤ2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 5 に追加する例を示します。

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

レイヤ3ポートをポートチャネルに追加

新しいチャンネルグループまたはすでにレイヤ3ポートが設定されているチャンネルグループにレイヤ3ポートを追加できます。ポートチャネルがない場合は、このチャンネルグループに関連付けられたポートチャネルが作成されます。

追加するレイヤ3ポートにIPアドレスが設定されている場合、ポートがポートチャネルに追加される前にそのIPアドレスは削除されます。レイヤ3ポートチャネルを作成したら、ポートチャネルインターフェイスにIPアドレスを割り当てることができます。



(注) **no channel-group** コマンドを使用して、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。このポートのIPアドレスを再設定する必要があります。

コマンド	目的
no channel-group 例 : <pre>switch(config)# no channel-group</pre>	チャンネルグループからポートを削除します。

始める前に

LACP ベースのポートチャネルにする場合は LACP をイネーブルにします。

レイヤ3 インターフェイスに設定した IP アドレスがあれば、この IP アドレスを削除します。

手順の概要

1. **configure terminal**
2. **interface type slot/port**
3. **no switchport**
4. **channel-group channel-number [force] [mode {on | active | passive}]**
5. **show interface type slot/port**
6. **no shutdown**
7. **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	configure terminal 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface type slot/port 例： switch(config)# interface ethernet 1/4 switch(config-if)#	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	no switchport 例： switch(config-if)# no switchport	インターフェイスをレイヤ3ポートとして設定します。
ステップ 4	channel-group channel-number [force] [mode {on active passive}] 例： <ul style="list-style-type: none"> • switch(config-if)# channel-group 5 • switch(config-if)# channel-group 5 force 	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、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。 (任意) 一部の設定に互換性がないインターフェイスをチャンネルに追加します。強制されるインターフェイスは、チャンネルグループと同じ速度、デュープレックス、およびフロー制御設定を持っている必要があります。
ステップ 5	show interface type slot/port 例： switch# show interface ethernet 1/4	(任意) インターフェイスの内容を表示します。
ステップ 6	no shutdown 例： switch# configure terminal switch(config)# int e3/1 switch(config-if)# no shutdown	(任意) ポリシーがハードウェアポリシーと一致するインターフェイスおよびVLANのエラーをクリアします。このコマンドにより、ポリシープログラミングが続き、ポートがアップできます。ポリシーが対応していない場合は、エラーはerror-disabledポリシー状態になります。
ステップ 7	copy running-config startup-config 例： switch(config)# copy running-config startup-config	(任意) 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

例

次に、レイヤ3イーサネットインターフェイス 1/5 を on モードのチャネルグループ 6 に追加する例を示します。

```
switch# configure terminal
switch (config)# interface ethernet 1/5
switch(config-if)# switchport
switch(config-if)# channel-group 6
```

次の例では、レイヤ3ポートチャネルインターフェイスを作成し、IPアドレスを割り当てる方法を示します。

```
switch# configure terminal
switch (config)# interface port-channel 4
switch(config-if)# ip address 192.0.2.1/8
```

情報目的としての帯域幅および遅延の設定

ポートチャネルの帯域幅は、チャネル内のアクティブリンクの合計数によって決定されます。

情報目的でポートチャネルインターフェイスに帯域幅および遅延を設定します。

手順の概要

1. **configure terminal**
2. **interface port-channel** *channel-number*
3. **bandwidth** *value*
4. **delay** *value*
5. **exit**
6. **show interface port-channel** *channel-number*
7. **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	configure terminal 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します
ステップ 2	interface port-channel <i>channel-number</i> 例： switch(config)# interface port-channel 2 switch(config-if)#	設定するポートチャネルインターフェイスを指定し、インターフェイスコンフィギュレーションモードを開始します。

	コマンドまたはアクション	目的
ステップ 3	bandwidth value 例： switch(config-if)# bandwidth 60000000 switch(config-if)#	情報目的で使用される帯域幅を指定します。有効な範囲は 1 ~ 3,200,000,000 kbs です。デフォルト値はチャンネルグループのアクティブインターフェイスの合計によって異なります。
ステップ 4	delay value 例： switch(config-if)# delay 10000 switch(config-if)#	情報目的で使用されるスループット遅延を指定します。範囲は、1 ~ 16,777,215 (10 マイクロ秒単位) です。デフォルト値は 10 マイクロ秒です。
ステップ 5	exit 例： switch(config-if)# exit switch(config)#	インターフェイスモードを終了し、コンフィギュレーションモードに戻ります。
ステップ 6	show interface port-channel channel-number 例： switch# show interface port-channel 2	(任意) 指定したポートチャネルのインターフェイス情報を表示します。
ステップ 7	copy running-config startup-config 例： switch(config)# copy running-config startup-config	(任意) 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

例

次に、ポートチャネル 5 の帯域幅および遅延の情報パラメータを設定する例を示します。

```
switch# configure terminal
switch (config)# interface port-channel 5
switch(config-if)# bandwidth 60000000
switch(config-if)# delay 10000
switch(config-if)#
```

ポートチャネルインターフェイスのシャットダウンと再起動

ポートチャネルインターフェイスをシャットダウンして再起動できます。ポートチャネルインターフェイスをシャットダウンすると、トラフィックは通過しなくなりインターフェイスは管理ダウンします。

手順の概要

1. **configure terminal**
2. **interface port-channel channel-number**

3. **shutdown**
4. **exit**
5. **show interface port-channel *channel-number***
6. **no shutdown**
7. **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	configure terminal 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します
ステップ 2	interface port-channel <i>channel-number</i> 例： switch(config)# interface port-channel 2 switch(config-if)#	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。
ステップ 3	shutdown 例： switch(config-if)# shutdown switch(config-if)#	インターフェイスをシャットダウンします。トラフィックは通過せず、インターフェイスは管理ダウン状態になります。デフォルトはシャットダウンなしです。 (注) インターフェイスを開くには、 no shutdown コマンドを使用します。 インターフェイスは管理アップとなります。操作上の問題がなければ、トラフィックが通過します。デフォルトはシャットダウンなしです。
ステップ 4	exit 例： switch(config-if)# exit switch(config)#	インターフェイス モードを終了し、コンフィギュレーション モードに戻ります。
ステップ 5	show interface port-channel <i>channel-number</i> 例： switch(config-router)# show interface port-channel 2	(任意) 指定したポートチャネルのインターフェイス情報を表示します。
ステップ 6	no shutdown 例： switch# configure terminal switch(config)# int e3/1 switch(config-if)# no shutdown	(任意) ポリシーがハードウェアポリシーと一致するインターフェイスおよびVLANのエラーをクリアします。このコマンドにより、ポリシープログラミングが続行でき、ポートがアップできます。ポリ

	コマンドまたはアクション	目的
		シーが対応していない場合は、エラーはerror-disabledポリシー状態になります。
ステップ 7	copy running-config startup-config 例： <pre>switch(config)# copy running-config startup-config</pre>	(任意) 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

例

次に、ポートチャネル2のインターフェイスをアップする例を示します。

```
switch# configure terminal
switch (config)# interface port-channel 2
switch(config-if)# no shutdown
```

ポートチャネルの説明の設定

ポートチャネルの説明を設定できます。

手順の概要

1. **configure terminal**
2. **interface port-channel** *channel-number*
3. **description**
4. **exit**
5. **show interface port-channel** *channel-number*
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： <pre>switch# configure terminal switch(config)#</pre>	グローバルコンフィギュレーションモードを開始します
ステップ 2	interface port-channel <i>channel-number</i> 例： <pre>switch(config)# interface port-channel 2 switch(config-if)#</pre>	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。
ステップ 3	description 例： <pre>switch(config-if)# description</pre>	ポートチャネルインターフェイスに説明を追加できます。説明に80文字まで使用できます。デフォルトでは、説明は表示されません。このパラメータ

	コマンドまたはアクション	目的
	<code>switch(config-if)# description engineering</code> <code>switch(config-if)#</code>	を設定してから、出力に説明を表示する必要があります。
ステップ 4	exit 例： <code>switch(config-if)# exit</code> <code>switch(config)#</code>	インターフェイスモードを終了し、コンフィギュレーションモードに戻ります。
ステップ 5	show interface port-channel <i>channel-number</i> 例： <code>switch# show interface port-channel 2</code>	(任意) 指定したポートチャネルのインターフェイス情報を表示します。
ステップ 6	copy running-config startup-config 例： <code>switch(config)# copy running-config startup-config</code>	(任意) 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

例

次に、ポートチャネル 2 に説明を追加する例を示します。

```
switch# configure terminal
switch (config)# interface port-channel 2
switch(config-if)# description engineering
```

ポートチャネルインターフェイスへの速度とデュプレックスの設定

ポートチャネルインターフェイスに速度とデュプレックスを設定できます。

手順の概要

1. **configure terminal**
2. **interface port-channel *channel-number***
3. **speed {10 | 100 | 1000 | auto}**
4. **duplex {auto | full | half}**
5. **exit**
6. **show interface port-channel *channel-number***
7. **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	configure terminal 例：	グローバルコンフィギュレーションモードを開始します

	コマンドまたはアクション	目的
	<code>switch# configure terminal</code> <code>switch(config)#</code>	
ステップ 2	interface port-channel <i>channel-number</i> 例： <code>switch(config)# interface port-channel 2</code> <code>switch(config-if)#</code>	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。
ステップ 3	speed {10 100 1000 auto} 例： <code>switch(config-if)# speed auto</code> <code>switch(config-if)#</code>	ポートチャネルインターフェイスの速度を設定します。デフォルトの自動ネゴシエーションは自動です。
ステップ 4	duplex {auto full half} 例： <code>switch(config-if)# speed auto</code> <code>switch(config-if)#</code>	ポートチャネルインターフェイスのデュプレックスを設定します。デフォルトの自動ネゴシエーションは自動です。
ステップ 5	exit 例： <code>switch(config-if)# exit</code> <code>switch(config)#</code>	インターフェイスモードを終了し、コンフィギュレーションモードに戻ります。
ステップ 6	show interface port-channel <i>channel-number</i> 例： <code>switch# show interface port-channel 2</code>	(任意) 指定したポートチャネルのインターフェイス情報を表示します。
ステップ 7	copy running-config startup-config 例： <code>switch(config)# copy running-config startup-config</code>	(任意) 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

例

次に、ポートチャネル 2 に 100 Mb/s を設定する例を示します。

```
switch# configure terminal
switch (config)# interface port-channel 2
switch(config-if)# speed 100
```

ポートチャネルを使ったロードバランシングの設定

VDC アソシエーションにかかわらず、ポートチャネルのロードバランシングアルゴリズムを設定し、デバイス全体または 1 つのモジュールだけに適用できます。



- (注) デフォルトのロードバランシングアルゴリズムである、非IPトラフィック用の `source-dest-mac`、および IP トラフィック用の `source-dest-ip` を復元するには、**no port-channel load-balance** コマンドを使用します。

コマンド	目的
no port-channel load-balance 例： <pre>switch(config)# no port-channel load-balance</pre>	デフォルトのロードバランシングアルゴリズムを復元します。

始める前に

LACP ベースのポートチャネルにする場合は LACP をイネーブルにします。

手順の概要

1. **configure terminal**
2. **port-channel load-balance** *method* {**dst ip** | **dst ip-gre** | **dst ip-l4port** | **dst ip-l4port-vlan** | **dst ip-vlan** | **dst l4port** | **dst mac** | **src ip** | **src ip-gre** | **src ip-l4port** | **src ip-l4port-vlan** | **src ip-vlan** | **src l4port** | **src mac** | **src-dst ip** | **src-dst ip-gre** | **src-dst ip-l4port** [symmetric] | **src-dst ip-l4port-vlan** | **src-dst ip-vlan** | **src-dst l4port** | **src-dst mac**} [*fex {fex-range | all}*] [**dst inner-header**] | **src inner-header** | **src-dst inner-header**] [*rotate rotate*]
3. **show port-channel load-balance**
4. **show port-channel load-balance** [**forwarding-path interface port-channel** *channel-number* |**src-ip** *src-ip* |**dst-ip** *dst-ip* |**protocol** *protocol* |**gtp-teid** *gtp-teid* |**module** *module_if*]
5. **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	configure terminal 例： <pre>switch# configure terminal switch(config)#</pre>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	port-channel load-balance <i>method</i> { dst ip dst ip-gre dst ip-l4port dst ip-l4port-vlan dst ip-vlan dst l4port dst mac src ip src ip-gre src ip-l4port src ip-l4port-vlan src ip-vlan src l4port src mac src-dst ip src-dst ip-gre src-dst ip-l4port [symmetric] src-dst ip-l4port-vlan src-dst ip-vlan src-dst l4port src-dst mac } [<i>fex {fex-range all}</i>] [dst inner-header] src inner-header src-dst inner-header] [<i>rotate rotate</i>] 例：	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。レイヤ3のデフォルトはIPv4とIPv6の両方で src-dst ip-l4port で、非IPのデフォルトは src-dst mac です。 (注) GRE 内部 IP ヘッダーは、送信元、宛先、および送信元と宛先をサポートします。

	コマンドまたはアクション	目的
	<ul style="list-style-type: none"> • switch(config)# port-channel load-balance src-dst mac switch(config)# • switch(config)# no port-channel load-balance src-dst mac switch(config)# • switch(config)# port-channel load-balance dst inner-header switch(config)# • switch(config)# port-channel load-balance src inner-header switch(config)# • switch(config)# port-channel load-balance src-dst inner-header switch(config)# 	<p>(注) 次のロードバランシングアルゴリズムがシンメトリックハッシングをサポートします。</p> <ul style="list-style-type: none"> • src-dst ip • src-dst ip-l4port
ステップ 3	<p>show port-channel load-balance</p> <p>例 :</p> <pre>switch(config-router)# show port-channel load-balance</pre>	<p>(任意) ポートチャネルロードバランシングアルゴリズムを表示します。</p>
ステップ 4	<p>show port-channel load-balance [forwarding-path interface port-channel channel-number src-ip src-ip dst-ip dst-ip protocol protocol gtp-teid gtp-teid module module_if]</p> <p>例 :</p> <pre>switch# show port-channel load-balance forwarding-path load-balance</pre>	<p>(任意) パケットを転送する EtherChannel インターフェイスのポートを識別します。</p>
ステップ 5	<p>copy running-config startup-config</p> <p>例 :</p> <pre>switch(config)# copy running-config startup-config</pre>	<p>(任意) 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。</p>

MPLS タグ付けトラフィック用にポートチャネルを使ったロードバランシングの構成

始める前に

- mpls の構成 port-channel load-balance と mpls load-sharing オプションは共存できません。
- MPLS タグ付き L2 トラフィックの場合は、mpls オプションを指定してポートチャネルロードバランシング構成を使用できます。

- mpls オプションを使用した feature-set mpls および port-channel load-balance の構成は、相互に排他的です。
- mpls オプション機能を使用したポートチャネルのロードバランシング機能は、vxlan 機能と共存できません。
- 以下は、mpls label-ip が設定された <non-mpls options> を使用したポートチャネルロードバランスの注意事項および制限事項です。
 - SRC と DST L2 アドレスフィールドの両方が、ASIC の MPLS の 4 つのラベルスタックすべてでオーバーロードされます。SRC-MAC は上位 3 つのラベルでオーバーロードされ、DST-MAC は残った 4 番目のラベルでオーバーロードされます。この機能をイネーブルにすると、ハッシュ用の MPLS IP パケットの SRC および DST L2 MAC フィールドが省略される可能性があります。
 - SRC または DST L2 アドレスフィールドに影響を与える非 mpls オプションの場合ラベルスタックハッシュの計算に影響します。
- 以下は、mpls label-only が設定された <non-mpls options> を使用したポートチャネルロードバランスの注意事項および制限事項です。
 - SRC と DST IP アドレスフィールドの両方が、ASIC の MPLS ラベルスタック（9 ラベル）でオーバーロードされます（SRC-IP は上位 5 つのラベルでオーバーロードされ、DST-IP は下位 4 つのラベルでオーバーロードされます）。したがって、このバリエーションをオンにすると、一般に、ハッシュ用の MPLS パケットの SRC および DST IP フィールドが無視される可能性があります。
 - <non-mpls options> に「SRC IP」のみのバリエーションが含まれている場合、上位 5 つの MPLS ラベルのみがハッシュの対象と見なされます（ラベルスタックサイズが 9 の場合）。
 - <non-mpls options> に DST IP のみのバリエーションが含まれている場合、下位 4 つの MPLS ラベルのみがハッシュ用に考慮されます（スタックサイズ 9 の MPLS ラベルの場合）。たとえば、ラベルが 5 つしかない MPLS パケットの場合、これらのラベルはいずれもハッシュの対象とは見なされません。7 つのラベルを持つ MPLS パケットの場合、ハッシュの対象となるのは下位 2 ラベルだけです。
 - <non-mpls options> に SRC と DST IP フィールドの両方が含まれていない場合、いずれのラベルもハッシュの対象と見なされません。
 - L4 SRC および DST ポートはハッシュの対象になりません。

手順の概要

1. **configure terminal**
2. **port-channel load-balance src-dst ip-l4port mpls {label-ip|label-only}**
3. (任意) **show port-channel load-balance**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	port-channel load-balance src-dst ip-l4port mpls {label-ip label-only} 例： switch(config)# port-channel load-balance src-dst ip-l4port mpls label-ip	ポートチャネルを使用して MPLS のロードバランシングを指定します。 label-ip : MPLS ラベルと IP に基づいてロードシェアリングを指定します。 label-only : MPLS ラベルのみに基づいてロードシェアリングを指定します。
ステップ 3	(任意) show port-channel load-balance 例： switch(config)# show port-channel load-balance	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。

例

次の例は、mpls オプションを使用したロードバランス構成です。

```
switch# show port-channel load-balance
System config:
Non-IP: src-dst mac
IP: src-dst ip-l4port mpls label-ip rotate 0
Port Channel Load-Balancing Configuration for all modules:
Module 1:
Non-IP: src-dst mac
IP: src-dst ip-l4port mpls label-ip rotate 0
```

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 は、正確に一致しているイーサネットリンクを識別すると、リンクを 1 つのポートチャネルとしてまとめます。次に、ポートチャネルは単一ブリッジポートとしてスパンニングツリーに追加されます。

LACP を設定する手順は次のとおりです。

- LACP をグローバルにイネーブルにするには、**feature lacp** コマンドを使用します。

- LACP をイネーブルにした同一ポートチャネルでは、異なるインターフェイスに異なるモードを使用できます。指定したチャンネルグループに割り当てられた唯一のインターフェイスである場合に限り、モードを **active** と **passive** で切り替えることができます。

手順の概要

1. **configure terminal**
2. **feature lacp**
3. **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	configure terminal 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	feature lacp 例： switch(config)# feature lacp	デバイスの LACP をイネーブルにします。
ステップ 3	copy running-config startup-config 例： switch(config)# copy running-config startup-config	(任意) 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

例

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
```

LACP ポートチャネルポートモードの設定

LACP をイネーブルにしたら、LACP ポートチャネルのそれぞれのリンクのチャンネルモードを **active** または **passive** に設定できます。このチャンネル 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。

関連する集約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は **on** チャンネルモードを維持します。

手順の概要

1. **configure terminal**
2. **interface type slot/port**

3. **channel-group** *number* **mode** {**active** | **on** | **passive**}
4. **show port-channel summary**
5. **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	configure terminal 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface type slot/port 例： switch(config)# interface ethernet 1/4 switch(config-if)#	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	channel-group number mode { active on passive } 例： switch(config-if)# channel-group 5 mode active	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ンネル全体を active または passive に設定します。 関連する集約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、ポートチャネルモードは常に on です。 デフォルト ポートチャネルモードは on です。
ステップ 4	show port-channel summary 例： switch(config-if)# show port-channel summary	(任意) ポートチャネルの概要を表示します。
ステップ 5	copy running-config startup-config 例： switch(config)# copy running-config startup-config	(任意) 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

例

次に、LACP をイネーブルにしたインターフェイスを、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 のアクティブポートチャネルモードに設定する例を示します。

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

LACP ポートチャネル最少リンク数の設定

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



(注) `no lacp min-links` コマンドを使用して、デフォルトポートチャネル最少リンクの設定を復元します。

コマンド	目的
no lacp min-links 例 : <pre>switch(config)# no lacp min-links</pre>	デフォルトのポートチャネル最少リンク設定を復元します。

始める前に

正しいポートチャネルインターフェイスであることを確認します。

手順の概要

1. `configure terminal`
2. `interface port-channel number`
3. `lacp min-links number`
4. `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	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface port-channel number 例 : <pre>switch(config)# interface port-channel 3 switch(config-if)#</pre>	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	lacp min-links number 例 : <pre>switch(config-if)# lacp min-links 3</pre>	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ます。指定できる範囲は 1 ~ 16 です。

	コマンドまたはアクション	目的
ステップ 4	show running-config interface port-channel <i>number</i> 例 : <pre>switch(config-if)# show running-config interface port-channel 3</pre>	(任意) ポートチャネル最小リンク設定を表示します。

例

次に、アップ/アクティブにするポートチャネルに関して、アップ/アクティブにするポートチャネルメンバー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
```

LACP ポートチャネル MaxBundle の設定

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



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

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

始める前に

正しいポートチャネルインターフェイスを使用していることを確認します。

手順の概要

1. **configure terminal**
2. **interface port-channel *number***
3. **lacp max-bundle *number***
4. **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	configure terminal 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface port-channel number 例： switch(config)# interface port-channel 3 switch(config-if)#	設定するインターフェイスを指定し、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	lacp max-bundle number 例： switch(config-if)# lacp max-bundle	max-bundle を設定するポートチャネルインターフェイスを指定します。 ポートチャネルの max-bundle のデフォルト値は 16 です。指定できる範囲は 1 ~ 32 です。 (注) デフォルト値は 16 ですが、ポートチャネルのアクティブメンバ数は、 pc_max_links_config およびポートチャネルで許可されている pc_max_active_members の最小数です。
ステップ 4	show running-config interface port-channel number 例： switch(config-if)# show running-config interface port-channel 3	(任意) ポートチャネル max-bundle 設定を表示します。

例

次に、ポートチャネルインターフェイスの max-bundle を設定する例を示します。

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

LACP 高速タイマー レートの設定

LACP タイマー レートを変更することにより、LACP タイムアウトの時間を変更することができます。lacp rate コマンドを使用し、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。



(注) LACP タイマー レートの変更は推奨しません。HA および SSO は、LACP 高速レートのタイマーが設定されている場合はサポートされません。



(注) vPC ピア リンクでの **lacp rate fast** の構成は推奨されません。**lacp rate fast** が vPC ピア リンク メンバー インターフェイスで設定されている場合、LACP ロギング レベルが 5 に設定されている場合にのみ、syslog メッセージにアラートが表示されます。

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. **configure terminal**
2. **interface type slot/port**
3. **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	configure terminal 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface type slot/port 例： switch(config)# interface ethernet 1/4 switch(config-if)#	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	lacp rate fast 例： switch(config-if)# lacp rate fast	LACP がサポートされているインターフェイスに LACP 制御パケットを送信する際のレートとして高速レート (1 秒) を設定します。 タイムアウトレートをデフォルトにリセットするには、コマンドの no 形式を使用します。

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 システム プライオリティの設定

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。

始める前に

LACP をイネーブルにします。

手順の概要

1. **configure terminal**
2. **lacp system-priority *priority***
3. **show lacp system-identifier**
4. **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	configure terminal 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	lacp system-priority <i>priority</i> 例： switch(config)# lacp system-priority 40000	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。 (注) VDC ごとに LACP システム ID が異なります。これは、この設定値に MAC アドレスが追加されるためです。
ステップ 3	show lacp system-identifier 例： switch(config-if)# show lacp system-identifier	(任意) LACP システム識別子を表示します。

	コマンドまたはアクション	目的
ステップ 4	copy running-config startup-config 例 : switch(config)# copy running-config startup-config	(任意) 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

例

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 をイネーブルにしたら、ポート プライオリティの LACP ポート チャネルにそれぞれのリンクを設定できます。

始める前に

LACP をイネーブルにします。

手順の概要

1. **configure terminal**
2. **interface type slot/port**
3. **lACP port-priority priority**
4. **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	configure terminal 例 : switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface type slot/port 例 : switch(config)# interface ethernet 1/4 switch(config-if)#	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	lACP port-priority priority 例 : switch(config-if)# lACP port-priority 40000	LACP で使用するポート プライオリティを設定します。指定できる範囲は 1 ~ 65535 で、値が大きいほどプライオリティは低くなります。デフォルト値は 32768 です。

	コマンドまたはアクション	目的
ステップ 4	copy running-config startup-config 例： <pre>switch(config-if)# copy running-config startup-config</pre>	(任意) 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

例

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
```

LACP システム MAC およびロールの設定

プロトコル交換用の LACP で使用される MAC アドレスとオプションのロールを設定できます。デフォルトでは、LACP は VDC MAC アドレスを使用します。デフォルトでは、ロールはプライマリです。

LACP でデフォルト (VDC) MAC アドレスとデフォルト ロールを使用するには、**no lacp system-mac** コマンドを使用します。

この手順は、Cisco Nexus 9336C-FX2、93300YC-FX2、および 93240YC-FX2-Z スイッチでサポートされています。

始める前に

LACP を有効にする必要があります。

手順の概要

1. **configure terminal**
2. **lacp system-mac mac-address role role-value**
3. (任意) **show lacp system-identifier**
4. **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	configure terminal 例： <pre>switch# configure terminal</pre>	グローバル 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	lacp system-mac mac-address role role-value 例 : <pre>switch(config)# lacp system-mac 000a.000b.000c role primary switch(config)# lacp system-mac 000a.000b.000c role secondary</pre>	LACP プロトコル交換で使用する MAC アドレスを指定します。ロールはオプションです。プライマリがデフォルトです。
ステップ 3	(任意) show lacp system-identifier 例 : <pre>switch(config)# show lacp system-identifier</pre>	設定されている MAC アドレスを表示します。
ステップ 4	copy running-config startup-config 例 : <pre>switch(config)# copy running-config startup-config</pre>	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、スイッチのロールをプライマリとして設定する例を示します。

```
Switch1# sh lacp system-identifier
32768,0-b-0-b-0-b
Switch1# sh run | grep lacp
feature lacp
lacp system-mac 000b.000b.000b role primary
```

セカンダリとしてスイッチのロールを設定する例を示します。

```
Switch2# sh lacp system-identifier
32768,0-b-0-b-0-b
Switch2# sh run | grep lacp
feature lacp
lacp system-mac 000b.000b.000b role secondary
```

LACP グレースフル コンバージェンスのディセーブル化

デフォルトで、LACP グレースフル コンバージェンスはイネーブルになっています。あるデバイスとの LACP 相互運用性をサポートする必要がある場合、コンバージェンスをディセーブルにできます。そのデバイスとは、グレースフルフェールオーバーのデフォルトが、ディセーブルにされたポートがダウンになるための時間を遅らせる可能性がある、または、ピアからのトラフィックを喪失する原因にもなるデバイスです。ダウンストリーム アクセス スイッチが Cisco Nexus デバイスでない場合は、LACP グレースフル コンバージェンス オプションをディセーブルにします。



(注) このコマンドを使用する前に、ポートチャネルが管理ダウン状態である必要があります。

始める前に

LACP をイネーブルにします。

手順の概要

1. **configure terminal**
2. **interface port-channel *number***
3. **shutdown**
4. **no lacp graceful-convergence**
5. **no shutdown**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface port-channel <i>number</i> 例： switch(config)# interface port-channel 1 switch(config-if)#	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。
ステップ 3	shutdown 例： switch(config-if) shutdown	ポート チャネルを管理シャットダウンします。
ステップ 4	no lacp graceful-convergence 例： switch(config-if)# no lacp graceful-convergence	ポートチャネルの LACP グレースフル コンバージェンスをディセーブルにします。
ステップ 5	no shutdown 例： switch(config-if) no shutdown	ポート チャネルを管理アップします。
ステップ 6	copy running-config startup-config 例： switch(config)# copy running-config startup-config	(任意) 実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

例

次に、ポートチャネルのLACP グレースフル コンバージェンスをディセーブルにする方法を示します。

```
switch# configure terminal
switch (config)# interface port-channel 1
switch(config-if)# shutdown
switch(config-if)# no lacp graceful-convergence
switch(config-if)# no shutdown
```

LACP グレースフル コンバージェンスの再イネーブル化

デフォルトの LACP グレースフル コンバージェンスが再度必要になった場合、コンバージェンスを再度イネーブルにできます。

手順の概要

1. **configure terminal**
2. **interface port-channel** *number*
3. **shutdown**
4. **lacp graceful-convergence**
5. **no shutdown**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface port-channel <i>number</i> 例： switch(config)# interface port-channel 1 switch(config-if)#	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。
ステップ 3	shutdown 例： switch(config-if) shutdown	ポートチャネルを管理シャットダウンします。
ステップ 4	lacp graceful-convergence 例： switch(config-if) lacp graceful-convergence	ポートチャネルの LACP グレースフル コンバージェンスをイネーブルにします。

	コマンドまたはアクション	目的
ステップ 5	no shutdown 例： switch(config-if) no shutdown	ポートチャネルを管理アップします。
ステップ 6	copy running-config startup-config 例： switch(config)# copy running-config startup-config	(任意) 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

例

次に、ポートチャネルの LACP グレースフルコンバージェンスをイネーブルにする方法を示します。

```
switch# configure terminal
switch (config)# interface port-channel 1
switch(config-if)# shutdown
switch(config-if)# lACP graceful-convergence
switch(config-if)# no shutdown
```

LACP の個別一時停止のディセーブル化

ポートがピアから LACP PDU を受信しない場合、LACP はポートを中断ステートに設定します。このプロセスは、サーバが LACP にポートを論理的アップにするように要求するときに、サーバの起動に失敗する原因になることがあります。



(注) **lACP suspend-individual** のみを入力する必要がありますエッジポートのコマンド。

始める前に

LACP をイネーブルにします。

手順の概要

1. **configure terminal**
2. **interface port-channel** *number*
3. **no lACP suspend-individual**
4. **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	configure terminal 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface port-channel number 例： switch(config)# interface port-channel 1 switch(config-if)#	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。
ステップ 3	no lacp suspend-individual 例： switch(config-if)# no lacp suspend-individual	ポートチャネルでLACP個別ポートの一時停止動作をディセーブルにします。 (注) この設定と、同じポートチャネルインターフェイスの一部として設定された複数のメンバーがある場合、メンバーがパートナーからLACP PDUを受信しない場合、すべてのメンバーが個別 (I) 状態に移行します。
ステップ 4	copy running-config startup-config 例： switch(config)# copy running-config startup-config	(任意) 実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

例

次に、ポートチャネルでLACP個別ポートの一時停止をディセーブルにする方法を示します。

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

switch(config-if)# no lacp suspend-individual
```

LACPの一時停止個別PXEのディセーブル化

ポートがピアからLACP PDUを受信しない場合、LACPはポートを中断ステータスに設定します。このプロセスは、サーバがLACPにポートを論理的アップにするように要求するときに、サーバの起動に失敗する原因になることがあります。



(注) **lacp suspend-individual pxe** のみを入力する必要があります エッジポートのコマンド。

始める前に

LACPをイネーブルにします。

手順の概要

1. **configure terminal**
2. **interface port-channel *number***
3. **no lacp suspend-individual pxe**
4. **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	configure terminal 例： <pre>switch# configure terminal switch(config)#</pre>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface port-channel <i>number</i> 例： <pre>switch(config)# interface port-channel 1 switch(config-if)#</pre>	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。
ステップ 3	no lacp suspend-individual pxe 例： <pre>switch(config-if)# no lacp suspend-individual pxe</pre>	ポートチャネルでLACP個別ポートの一時停止動作をディセーブルにします。 (注) <ul style="list-style-type: none"> • この設定と、同じポートチャネルインターフェイスの一部として設定された複数のメンバーがある場合、メンバーがパートナーからLACPPDUを受信しない場合、1つのポートのみが個別 (I) 状態に遷移し、残りはポートは一時停止 (S) 状態になります。ポートがP状態で起動した場合、I状態のポートはありません。vPCピア間では、I状態のポートが1つ存在することに注意してください。 • ピア デバイスが一時停止ポートにトラフィックをハッシュすると、トラフィックはドロップされます。
ステップ 4	copy running-config startup-config 例： <pre>switch(config)# copy running-config startup-config</pre>	(任意) 実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

例

次に、ポートチャネルでLACP個別ポートの一時停止をディセーブルにする方法を示します。

```
switch# configure terminal
switch (config)# interface port-channel 1
switch(config-if)# no lacp suspend-individual pxe
```

LACPの個別一時停止の再イネーブル化

デフォルトのLACP個別ポートの一時停止を再度イネーブルにできます。

手順の概要

1. **configure terminal**
2. **interface port-channel *number***
3. **lacp suspend-individual pxe**
4. **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	configure terminal 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface port-channel <i>number</i> 例： switch(config)# interface port-channel 1 switch(config-if)#	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。
ステップ 3	lacp suspend-individual pxe 例： switch(config-if)# lacp suspend-individual	ポートチャネルでLACP個別ポートの一時停止動作をイネーブルにします。 (注) lacp suspend-individual pxeを設定しても、show runningコマンドはlacp suspend-individualのみを表示し、個々のpxeを停止しません。
ステップ 4	copy running-config startup-config 例： switch(config)# copy running-config startup-config	(任意) 実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

例

次に、ポートチャネルで LACP 個別ポートの一時停止を再度イネーブルにする方法を示します。

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

switch(config-if)# lacp suspend-individualpxe
```

遅延 LACP の設定

遅延 LACP 機能により、LACP PDU の受信前に 1 つのポートチャネルメンバー（遅延 LACP ポート）がまず通常のポートチャネルのメンバーとしてアップできます。遅延 LACP 機能を設定するには、ポートチャネルでコマンドを使用してから、ポートチャネルの 1 つのメンバーポートで LACP ポートプライオリティを設定します。 **lacp mode delay**



(注) vPC の場合は、両方の vPC スイッチで遅延 LACP を有効にする必要があります。



(注) vPC の場合、プライマリ スイッチに遅延 LACP ポートがあり、プライマリ スイッチが起動できないときは、動作上のプライマリ スイッチの遅延 LACP ポートチャネルで vPC 設定を削除し、新しいポートのポートチャネルをフラップして既存のポートチャネルの遅延 LACP ポートとして選択されるようにする必要があります。

手順の概要

1. **configure terminal**
2. **interface port-channel** *number*
3. **lacp mode 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	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface port-channel <i>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。
ステップ 3	lacp mode delay	遅延 LACP を有効化します。

	コマンドまたはアクション	目的
		<p>(注) 遅延 LACP を無効にするには、no lacp mode delay コマンドを使用します。</p> <p>LACP ポートプライオリティを設定して、遅延 LACP の設定を完了します。詳細については、「LACP ポートプライオリティの設定」を参照してください。</p> <p>LACP ポートのプライオリティによって、遅延 LACP ポートの選択が決まります。プライオリティの数値が最小のポートが選択されます。</p> <p>複数のポートの優先順位が同じ場合、VDC システム MAC を使用して、使用する vPC が決定されます。次に、非 vPC スイッチまたは選択された vPC スイッチ内で、最も小さいイーサネットポート名が使用されます。</p> <p>遅延 LACP 機能を設定し、ポートチャネルフラップで有効にすると、遅延 LACP ポートは通常のポートチャネルのメンバーとして動作し、サーバとスイッチ間でデータを交換できるようになります。最初の LACP PDU を受信すると、遅延 LACP ポートは通常のポートメンバーから LACP ポートメンバーに移行します。</p> <p>(注) 遅延 LACP ポートの選択は、ポートチャネルがスイッチまたはリモートサーバでフラップするまで完了または有効になりません。</p>

例

次に、遅延 LACP を設定する例を示します。

```
switch# config terminal
switch(config)# interface po 1
switch(config-if)# lacp mode delay
```

```
switch# config terminal
switch(config)# interface ethernet 1/1
switch(config-if)# lacp port-priority 1
switch(config-if)# channel-group 1 mode active
```

次に、遅延 LACP をディセーブルにする例を示します。

```
switch# config terminal
```

```
switch(config)# interface po 1
switch(config-if)# no lacp mode delay
```

ポートチャネルハッシュ分散の設定

Cisco NX-OS は、グローバルレベルとポートチャネルレベルの両方でアダプティブおよび固定のハッシュ分散の設定をサポートしています。このオプションは、メンバがアップまたはダウンしたときに Result Bundle Hash (RBH) 分散の変化を最小限に抑えることにより、トラフィックの中断を最小限に抑えます。このため、変化のない RBH 値にマッピングされているフローが同じリンクを流れ続けるようになります。ポートチャネルレベルの設定はグローバル設定よりも優先されます。デフォルト設定はグローバルに適応し、各ポートチャネルの設定がないので、ISSU 中に変更はありません。コマンドが適用されたときにポートはフラップされず、設定は次のメンバーリンクの変更イベントで有効になります。どちらのモードも RBH モジュールまたは非モジュールスキームで動作します。

この機能がサポートされない下位バージョンへの ISSU 時には、固定モードコマンドがグローバルに使用されている場合や、ポートチャネルレベルの設定がある場合は、この機能を無効にする必要があります。

グローバルレベルでのポートチャネルハッシュ分散の設定

手順の概要

1. **configure terminal**
2. **no port-channel hash-distribution {adaptive | fixed}**
3. **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	configure terminal 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	no port-channel hash-distribution {adaptive fixed} 例： switch(config)# port-channel hash-distribution adaptive switch(config)#	グローバルレベルでポートチャネルハッシュ分散を指定します。 デフォルトはアダプティブモードです。 コマンドは、次のメンバーリンクイベント (link down/up/no shutdown/shutdown) まで有効になりません。 ([まだ続けますか (はい / いいえ) ? [はい] (Do you still want to continue (y/n)? [yes])])
ステップ 3	copy running-config startup-config 例：	(任意) 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

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

例

次に、グローバルレベルでハッシュ分散を設定する例を示します。

```
switch# configure terminal
switch(config)# no port-channel hash-distribution fixed
```

ポートチャネルレベルでのポートチャネルハッシュ分散の設定

手順の概要

1. **configure terminal**
2. **interface port-channel {channel-number | range}**
3. **no port-channel port hash-distribution {adaptive | fixed}**
4. **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	configure terminal 例： <code>switch# configure terminal</code> <code>switch(config)#</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	interface port-channel {channel-number range} 例： <code>switch# interface port-channel 4</code> <code>switch(config-if)#</code>	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	no port-channel port hash-distribution {adaptive fixed} 例： <code>switch(config-if)# port-channel port</code> <code>hash-distribution adaptive</code> <code>switch(config-if)</code>	ポートチャネルレベルでポートチャネルハッシュ分散を指定します。 デフォルトはありません。 コマンドは、次のメンバー リンク イベント (link down/up/no shutdown/shutdown) まで有効になります。 ([まだ続けますか (はい / いいえ) ? [はい] (Do you still want to continue(y/n)? [yes])])
ステップ 4	copy running-config startup-config 例： <code>switch(config)# copy running-config startup-config</code>	(任意) 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

例

次に、グローバル レベル コマンドとしてハッシュ分散を設定する例を示します。

```
switch# configure terminal
switch(config)# no port-channel hash-distribution fixed
```

ECMP の復元力のあるハッシュの有効化

復元力のある ECMP では、ECMP グループからメンバーが削除されたときでも、既存のフローへの影響が最小限に抑えられます。これは、削除されたメンバーが以前占有していたインデックスにおいて、ラウンドロビン方式で既存のメンバーを複製することによって実現されます。

手順の概要

1. **configure terminal**
2. **hardware profile ecmp resilient**
3. **copy running-config startup-config**
4. **reload**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： switch# configure terminal	グローバル設定モードを開始します。
ステップ 2	hardware profile ecmp resilient 例： switch(config)# hardware profile ecmp resilient	ECMP の復元力のあるハッシュを有効にすると、次のメッセージが表示されます。警告：コマンドは次のリロード後に有効になります。 (注) このコマンドは、Cisco Nexus 9808/9804 プラットフォーム スイッチではサポートされていません。
ステップ 3	copy running-config startup-config 例： switch(config)# copy running-config startup-config	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。
ステップ 4	reload 例： switch(config)# reload	スイッチをリブートします。

ECMP の復元力のあるハッシュの無効化

始める前に

ECMP の復元力のあるハッシュが有効になっています。

手順の概要

1. **configure terminal**
2. **no hardware profile ecmp resilient**
3. **copy running-config startup-config**
4. **reload**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： <code>switch# configure terminal</code>	グローバル設定モードを開始します。
ステップ 2	no hardware profile ecmp resilient 例： <code>switch(config)# no hardware profile ecmp resilient</code>	ECMP の復元力のあるハッシュを無効にし、次のメッセージを表示します。警告：コマンドは次のリロード後に有効になります。
ステップ 3	copy running-config startup-config 例： <code>switch(config)# copy running-config startup-config</code>	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。
ステップ 4	reload 例： <code>switch(config)# reload</code>	スイッチをリブートします。

ECMP ロード バランシングの設定

ECMP ロード シェアリング アルゴリズムを設定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

始める前に

手順の概要

1. **ip load-sharing address {destination port destination | source-destination [port source-destination | gre | gtpu | ipv6-flowlabel | ttl | udf offset offset length length | symmetricinner allgreheader]} [universal-id seed] [rotate rotate] [concatenation]**
2. (任意) **show ip load-sharing**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<p>ip load-sharing address {destination port destination source-destination [port source-destination gre gtpu ipv6-flowlabel ttl udf offset <i>offset</i> length <i>length</i> symmetric inner <i>allgreheader</i>]} [universal-id <i>seed</i>] [rotate <i>rotate</i>] [concatenation]</p> <p>例 :</p> <pre>ip load-sharing address source-destination</pre> <p>例 :</p> <pre>switch(config)# ip load-sharing address source-destination ipv6-flowlabel</pre> <p>例 :</p> <pre>switch(config)# ip load-sharing address source-destination ttl</pre> <p>例 :</p> <pre>switch(config)# ip load-sharing address source-destination udf offset 8 length 8</pre> <p>例 :</p> <pre>switch(config)# [no] ip load-sharing address source-destination port source-destination symmetric</pre> <p>例 :</p> <pre>switch(config)# ip load-sharing address source-destination port source-destination inner [all greheader]</pre>	<p>データトラフィックに対する ECMP ロードシェアリングアルゴリズムを設定します。</p> <ul style="list-style-type: none"> • gre オプションは、Generic Routing Encapsulation (GRE) キーの送信元と宛先の値を指定します。 • gtpu オプションは、ポートの送信元/宛先の GPRS トンネリングプロトコル (GTP) トンネルエンドポイント識別子 (TEID) 値を指定します。 • ipv6-flowlabel オプションには、ECMP ハッシュを計算するための IPv6 フローラベルが含まれます。これにより、異なるフローラベル値に基づいてすべてのリンクにトラフィックフローが分散されます。port-channel load-balance コマンドを使用してレイヤ 4 パラメータが有効になっている場合、このオプションを有効または無効にすると、ポートチャネルのロードバランシングも有効または無効になります。このオプションを使用できるのは、以下のデバイスのみです。 <ul style="list-style-type: none"> • Cisco Nexus 9332C および 9364C プラットフォームスイッチ • X9700-EX/FX ラインカードおよび FM-E2 ファブリックモジュールを搭載して、Cisco Nexus 9500 プラットフォームスイッチ (すべてのルーティングモードで) • X9700-EX / FX ラインカードおよび FM-E ファブリックモジュールを搭載した Cisco Nexus 9500 プラットフォームスイッチ (ラインカードで IPv6 ルートがプログラムされている、非階層型ルーティングモードで) • Cisco NX-OS リリース 9.3(5) 以降では、Cisco Nexus N9K-C9316D-GX、N9K-C93600CD-GX、N9K-C9364C-GX スイッチがこのオプションをサポートしています。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> <p>• ttl オプションには、ECMP ハッシュを計算するための存続可能時間情報が含まれています。これにより、異なる TTL 値に基づいてすべてのリンクにトラフィックフローが分散されます。IPv4 フローの場合は、ttl 値に基づきます。IPv6 フローの場合は、ホップ制限に基づきます。</p> <p>port-channel load-balance コマンドを使用してレイヤ 4 パラメータが有効になっている場合、このオプションを有効または無効にすると、ポートチャネルのロードバランシングも有効または無効になります。Cisco Nexus 9364C および 9300-EX/FX/FX2 プラットフォームスイッチだけがこのオプションをサポートします。Cisco NX-OS リリース 9.3(5) 以降では、Cisco Nexus N9K-C9316D-GX、N9K-C93600CD-GX、N9K-C9364C-GX スイッチがこのオプションをサポートしています。</p> <p>• udf オプションには、ECMP ハッシュを計算するためのユーザ定義フィールドが含まれます。UDF フィールドのオフセットベースと長さ（ビット単位）は設定できます。オフセットベースの範囲は 0 ～ 127 バイトです。UDF フィールドの長さの範囲は 1 ～ 32 ビットです。</p> <p>port-channel load-balance コマンドを使用してレイヤ 4 パラメータが有効になっている場合、このオプションを有効または無効にすると、ポートチャネルのロードバランシングも有効または無効になります。Cisco Nexus 9364C および 9300-EX/FX/FX2 プラットフォームスイッチだけがこのオプションをサポートします。Cisco NX-OS リリース 9.3(5) 以降では、Cisco Nexus N9K-C9316D-GX、N9K-C93600CD-GX、N9K-C9364C-GX スイッチがこのオプションをサポートしています。</p> <p>• symmetric オプションは、対称ハッシュをグローバルに有効にします。ECMP 対称ハッシュを無効にするには、コマンドで no キーワードを使用します。このコマンドは、グローバルコンフィギュレーションモードで実行する必要があります。</p>

	コマンドまたはアクション	目的
		<p>(注) 対称ハッシュが効果的に機能するために、構成された universal-id シード値が ECMP 対称ハッシュのパス内のノード間で一貫していることを確認します。</p> <ul style="list-style-type: none"> • inner オプションは、GRE トラフィックの内部ヘッダーベースのハッシュをグローバルに有効にします。内部ヘッダーベースのハッシュを無効にするには、コマンドで no キーワードを使用します。このコマンドは、グローバル コンフィギュレーションモードで実行する必要があります。 • all : GRE カプセル化パケットにこのオプションを設定すると、内部ヘッダーを使用する ECMP のパスのハッシュ化を開始します。これは、他のカプセル化タイプにも影響を与える可能性があります。これは、Cisco Nexus 9364C および 9300-EX/FX/FX2 プラットフォームスイッチ、および X9700-EX/FX ラインカードを搭載した Cisco Nexus 9500 プラットフォームスイッチでサポートされています。 • greheader : このオプションは、GRE カプセル化パケットに対してのみ設定できるもので、内部ヘッダーを使用する ECMP のパスのハッシュ化を開始します。これは、Cisco Nexus 9364C および 9300-FX/FX2 プラットフォームスイッチ、および X9700-FX ラインカードを搭載した Cisco Nexus 9500 プラットフォームスイッチでサポートされています。 <p>次のオプションは、すべての IP ロードシェアリング設定で使用できます。</p> <ul style="list-style-type: none"> • universal-id オプションは、ハッシュアルゴリズムのランダムシードを設定することにより、フローをあるリンクから別のリンクにシフトします。 <p>汎用 ID を設定する必要はありません。ユーザが設定しなかった場合は、Cisco NX-OS が汎用</p>

	コマンドまたはアクション	目的
		<p>ID を選択します。 <i>universal-id</i> の範囲は 1 ～ 4294967295 です。</p> <ul style="list-style-type: none"> rotate オプションを使用すると、ハッシュアルゴリズムは、リンク ピッキングの選択をローテーションさせます。これは、ネットワーク内のすべてのノードが同じリンクを継続的に選択しないようにするためです。これは、ハッシュアルゴリズムのビットパターンに影響を与えることによって機能します。このオプションは、あるリンクから別のリンクにフローをシフトし、最初の ECMP レベルからすでにロードバランシング（極性化）されているトラフィックのロードバランシングを複数のリンク間で行います。 <p><i>rotate</i> 値を指定すると、64 ビットのストリームが、循環回転でのそのビット位置から解釈されます。 <i>rotate</i> 値の範囲は 1 ～ 63 で、デフォルトは 32 です。</p> <p>(注) 多層レイヤ3 トポロジでは、極性が発生する可能性があります。極性を回避するには、トポロジの各層で異なる循環ビットを使用します。</p> <p>(注) ポートチャネルの <i>rotation</i> 値を設定するには、 port-channel load-balance src-dst ip-l4port rotate rotate コマンドを使用します。</p> <ul style="list-style-type: none"> concatenation オプションを使用すると、ECMP のハッシュタグ値とポートチャネルのハッシュタグ値がひとつに結合され、より強力な 64 ビットのハッシュを使用できるようになります。このオプションを使用しない場合、ECMP のロードバランシングおよびポートチャネルのロードバランシングを個別に制御できます。デフォルトではディセーブルになっています。
<p>ステップ 2</p>	<p>(任意) show ip load-sharing</p> <p>例 :</p> <pre>switch(config)# show ip load-sharing address source-destination</pre>	<p>データトラフィックに対する ECMP のロードシェアリングアルゴリズムを表示します。</p>

ECMP の復元力のあるハッシュ設定の確認

ECMP の復元力のあるハッシュ設定情報を表示するには、次の作業を行います。

コマンド	目的
<pre>switch(config)# show running-config grep "hardware profile ecmp resilient hardware profile ecmp resilient switch(config)#</pre>	機能が有効になったステータスを表示します。
<pre>switch(config)# show running-config grep "hardware profile ecmp resilient switch(config)#</pre>	機能が無効になったステータスを表示します。

ポートチャネル設定の確認

ポートチャネルの設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show interface port-channel <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。
show feature	イネーブルにされた機能を表示します。
load-interval { <i>interval seconds</i> { 1 2 3 }}	ビットレートとパケットレートの統計情報に対して3つの異なるサンプリング間隔を設定します。
show port-channel compatibility-parameters	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。
show port-channel database [<i>interface port-channel 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。
show port-channel load-balance	ポートチャネルで使用するロードバランシングのタイプを表示します。
show port-channel summary	ポートチャネルインターフェイスのサマリーを表示します。
show port-channel traffic	ポートチャネルのトラフィック統計情報を表示します。
show port-channel usage	使用済みおよび未使用のチャンネル番号の範囲を表示します。

コマンド	目的
show lacp {counters [interface port-channel channel-number] [interface type/slot] neighbor [interface port-channel channel-number] port-channel [interface port-channel channel-number] system-identifier]}	LACPに関する情報を表示します。
show running-config interface port-channel channel-number	ポートチャネルの実行コンフィギュレーションに関する情報を表示します。

ポートチャネルインターフェイスコンフィギュレーションのモニタリング

次のコマンドを使用すると、ポートチャネルインターフェイス構成情報を表示することができます。

コマンド	目的
clear counters interface port-channel channel-number	カウンタをクリアします。
clear lacp counters [interface port-channel channel-number]	LACPカウンタをクリアします。
load-interval {interval seconds {1 2 3}}	ビットレートとパケットレートの統計情報に対して3つの異なるサンプリング間隔を設定します。
show interface counters [module module]	入力および出力オクテットユニキャストパケット、マルチキャストパケット、ブロードキャストパケットを表示します。
show interface counters detailed [all]	入力パケット、バイト、マルチキャストおよび出力パケット、バイトを表示します。
show interface counters errors [module module]	エラーパケットの数を表示します。
show lacp counters	LACPの統計情報を表示します。

ポートチャネルの設定例

次に、LACPポートチャネルを作成し、そのポートチャネルに2つのレイヤ2インターフェイスを追加する例を示します。

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

```

switch (config)# interface port-channel 5
switch (config-if)# interface ethernet 1/4
switch(config-if)# switchport
switch(config-if)# channel-group 5 mode active
switch(config-if)# lacp port priority 40000
switch(config-if)# interface ethernet 1/7
switch(config-if)# switchport
switch(config-if)# channel-group 5 mode

```

次に、チャネルグループに2つのレイヤ3インターフェイスを追加する例を示します。Cisco NX-OS ソフトウェアはポートチャネルを自動的に作成します。

```

switch# configure terminal
switch (config)# interface ethernet 1/5
switch(config-if)# no switchport
switch(config-if)# no ip address
switch(config-if)# channel-group 6 mode active
switch (config)# interface ethernet 2/5
switch(config-if)# no switchport
switch(config-if)# no ip address
switch(config-if)# channel-group 6 mode active
switch (config)# interface port-channel 6
switch(config-if)# ip address 192.0.2.1/8

```

関連資料

関連項目	マニュアルタイトル
システム管理	『Cisco Nexus 9000 Series NX-OS System Management Configuration Guide』
高可用性	『Cisco Nexus 9000 Series NX-OS High Availability and Redundancy Guide』
ライセンス	『Cisco NX-OS Licensing Guide』



第 8 章

vPC の設定

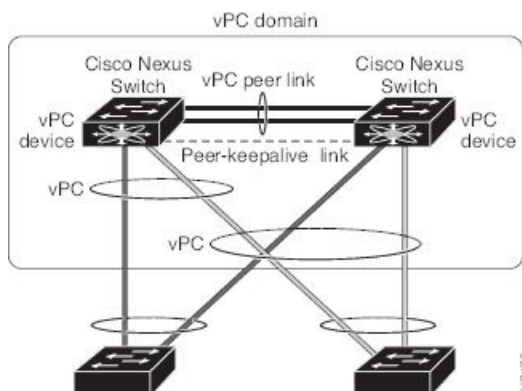
- [vPC について \(293 ページ\)](#)
- [注意事項と制約事項 \(325 ページ\)](#)
- [レイヤ 3 および vPC 設定のベストプラクティス \(333 ページ\)](#)
- [デフォルト設定 \(343 ページ\)](#)
- [vPC の設定 \(343 ページ\)](#)
- [vPC 設定の確認 \(370 ページ\)](#)
- [vPC のモニタリング \(371 ページ\)](#)
- [vPC の設定例 \(371 ページ\)](#)
- [関連資料 \(373 ページ\)](#)

vPC について

vPC の概要

仮想ポートチャネル (vPC) は、物理的には 2 台の異なる Cisco Nexus 9000 シリーズ デバイスに接続されているリンクを、第 3 のデバイスには単一のポートに見えるようにします (図を参照)。第 3 のデバイスは、スイッチ、サーバ、ポートチャネルをサポートするその他の任意のネットワークングデバイスのいずれでもかまいません。vPC は、ノード間の複数の並列パスを可能にし、トラフィックのロードバランシングを可能にすることによって、冗長性を作り、バイセクショナルな帯域幅を増やすレイヤ 2 マルチパスを提供できます。

図 11: vPC のアーキテクチャ



vPC で使用できるのは、レイヤ 2 ポート チャンネルだけです。ポート チャンネルの設定は、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)

LACP を使用せずに vPC (vPC ピア リンク チャンネルも含めて) のポート チャンネルを設定する場合は、各デバイスが、単一のポート チャンネル内に最大 8 つのアクティブリンクを持てます。LACP を使用して vPC (vPC ピア リンク チャンネルも含めて) のポート チャンネルを設定する場合は、各デバイスが、単一のポート チャンネル内に 32 個のアクティブリンクと 8 つのスタンバイリンクを持つことができます。(LACP と vPC の使用の詳細については、「その他の機能との vPC の相互作用」の項を参照)。



(注) vPC の機能を設定したり実行したりするには、まず vPC 機能をイネーブルにする必要があります。

vPC 機能をイネーブルにしたら、ピアキープアライブリンクを作成します。このリンクは、2 つの vPC ピア デバイス間でのハートビート メッセージの送信を行います。

1 ギガビットイーサネット以上の速度のイーサネットポートを 2 つ以上使用することにより、1 台の Cisco Nexus 9000 シリーズ シャーシでポート チャンネルを設定して vPC ピア リンクを作成できます。vPC を有効にして実行するための正しいハードウェアが揃っていることを確認するには、**show hardware feature-capability** と入力します コマンドを入力します。コマンド出力で vPC の向かいに X が表示されている場合、そのハードウェアでは vPC 機能をイネーブルにできません。

vPC ピア リンク レイヤ 2 ポート チャンネルは、トランクとして設定することを推奨します。もう 1 つの Cisco Nexus 9000 シリーズ シャーシで、再度専用ポート モードで 1 ギガビット以上の速度の 2 つ以上のイーサネットポートを使用して、もう 1 つのポート チャンネルを設定します。これらの 2 つのポート チャンネルを接続すると、リンクされた 2 つの Cisco Nexus デバイスが第 3 のデバイスには 1 つのデバイスとして見える vPC ピア リンクが作成されます。第 3 のデバイス、またはダウンストリームデバイスは、スイッチ、サーバ、vPC に接続された正規の

ポート チャンネルを使用するその他の任意のネットワーキング デバイスのいずれでもかまいません。

モジュラ Cisco Nexus 9500 スイッチの場合、異なるモジュールの専用ポート上で vPC ピア リンクを設定して、障害発生の可能性を下げることをお勧めします。復元力を最適にしたい環境では、少なくとも 2 つのモジュールを使用してください。

vPC ピア リンクに Nexus 9000 デバイスの任意のインターフェイスを使用できます。すべての vPC ピア リンクおよびコアに面したインターフェイスを 1 つのモジュール上で設定しなければならない場合、コアへのレイヤ 3 リンクに関連付けられているトラック オブジェクトおよび両方の vPC ピア デバイス上の vPC ピア リンク上のすべてのリンクを設定してください。

vPC ドメインには、両方の vPC ピア デバイス、vPC ピア キープ アライブ リンク、vPC ピア リンク、および vPC ドメイン内においてダウンストリーム デバイスに接続されているすべてのポート チャンネルが含まれます。各デバイスに設定できる vPC ドメイン ID は、1 つだけです。

このバージョンでは、各ダウンストリーム デバイスを、単一のポート チャンネルを使用して単一の vPC ドメイン ID に接続できます。

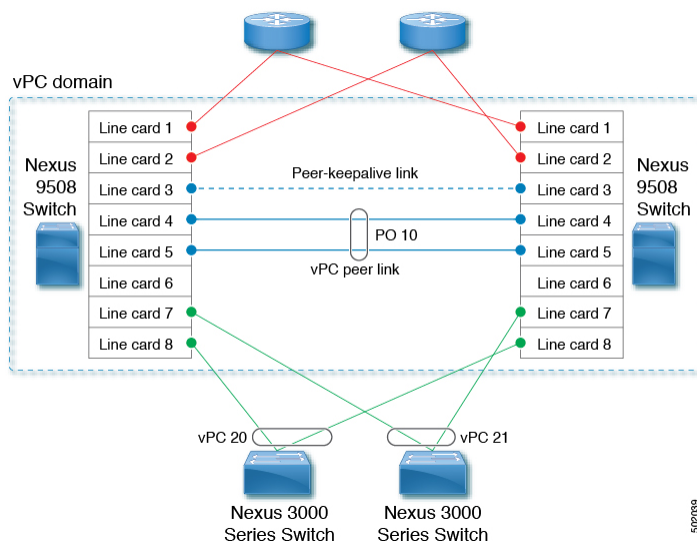


(注) ポート チャンネルを使用して vPC ドメインに接続されたデバイスは、両方の vPC ピアに接続する必要があります。

vPC (図を参照) には、次の利点があります。

- 単一のデバイスが 2 つのアップストリーム デバイスを介して 1 つのポート チャンネルを使用することを可能にします。
- 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。
- リンクまたはデバイスに障害が発生した場合に、ファーストコンバージェンスを提供します。
- 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。

図 12: vPC インターフェイス



vPC の用語

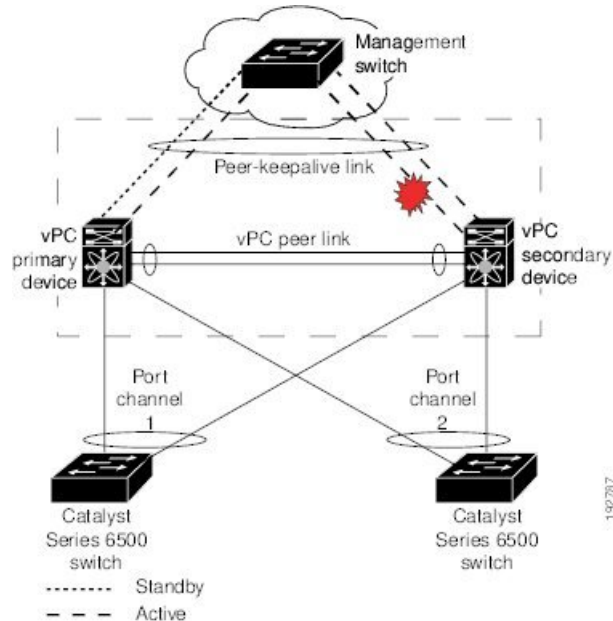
vPC で使用される用語は、次のとおりです。

- 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ポート チャネル。
- vPC ピア デバイス : vPC ピア リンクと呼ばれる特殊なポート チャネルで接続されている一対のデバイスの 1 つ。
- 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。このリンクは、少なくとも 10 ギガビットイーサネット インターフェイスを使用する必要があります。より広い帯域幅のインターフェイス (25 ギガビットイーサネット、40 ギガビットイーサネット、100 ギガビットイーサネットなど) も使用できます。
- vPC メンバ ポート : vPC に属するインターフェイス。
- ホスト vPC ポート : vPC に属するファブリック エクステンダのホスト インターフェイス。
- vPC ドメイン : このドメインには、両方の vPC ピア デバイス、vPC ピア キープアライブ リンク、vPC 内においてダウンストリーム デバイスに接続されているすべてのポート チャネルが含まれます。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 ピア キープアライブ リンク : ピア キープアライブ リンクは、さまざまな vPC ピア Cisco Nexus 9000 シリーズのデバイスをモニタします。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。

ピア キープアライブ リンクを、各 vPC ピア デバイス内のレイヤ 3 インターフェイスにマッピングされている独立した仮想ルーティングおよび転送 (VRF) インスタンスに関連付けることを推奨します。独立した VRF を設定しなかった場合は、デフォルトで管理 VRF が使用されます。ただし、ピア キープアライブ リンクに管理 インターフェイスを使用する場

合は、各 vPC ピア デバイスのアクティブ管理ポートとスタンバイ管理ポートの両方に接続した管理スイッチを置く必要があります（図を参照）。

図 13: vPC ピアキープアライブリンクの管理ポートを接続するための独立したスイッチが必要



vPC 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。

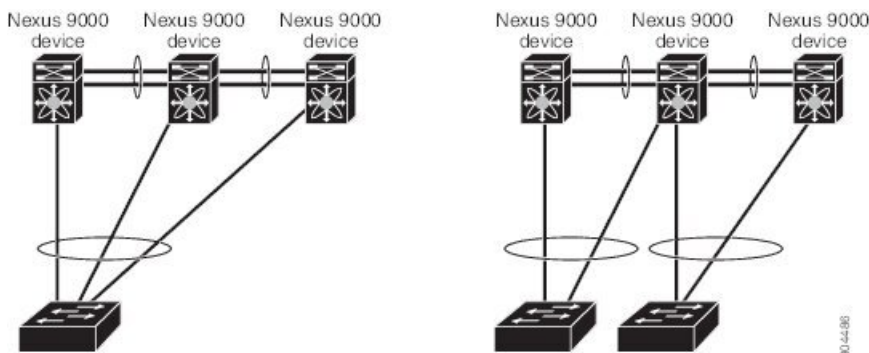
- vPC メンバ ポート：vPC に属するインターフェイス。
- デュアルアクティブ：プライマリとして動作する両方の vPC ピア。この状況は、両方のピアがまだアクティブなときに vPC ピアキープアライブとピアリンクがダウンした場合に発生します。この場合、セカンダリ vPC はプライマリ vPC が動作しないと想定し、プライマリ vPC として機能します。
- リカバリ：ピアキープアライブと vPC ピアリンクが起動すると、1 台のスイッチがセカンダリ vPC になります。セカンダリ vPC になるスイッチで、vPC リンクが停止してから復帰します。

vPC ピア リンクの概要

vPC ピアとして持てるのは 2 台のデバイスだけです。各デバイスが、他方の 1 つの vPC ピアに対してだけ vPC ピアとして機能します。vPC ピア デバイスは、他のデバイスに対する非 vPC リンクも持つことができます。

無効な vPC ピア設定については、次の図を参照してください。

図 14: 許可されていない vPC ピア 設定



有効な設定を作成するには、まず各デバイス上でポートチャネルを設定してから、vPC ドメインを設定します。ポートチャネルを各デバイスに、同じ vPC ドメイン ID を使用して vPC ピアリンクとして割り当てます。vPC ピアリンクのインターフェイスの片方に障害が発生した場合に、デバイスが自動的に vPC ピアリンク内の他方のインターフェイスを使用するようにフォールバックするため、冗長性のために少なくとも 2 つの専用ポートをポートチャネルに設定することを推奨します。



(注) レイヤ 2 ポートチャネルをトランク モードで設定することを推奨します。

多くの動作パラメータおよび設定パラメータが、vPC ピアリンクによって接続されている各デバイスで同じでなければなりません（「vPC インターフェイスの互換パラメータ」の項を参照）。各デバイス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デバイス同士に互換性があることを確認する必要があります。vPC ピアデバイスは、個別のコントロールプレーンを持ちます。vPC ピアリンクを設定し終わったら、各 vPC ピアデバイスの設定を表示して、設定に互換性があることを確認してください。



(注) vPC ピアリンクによって接続されている 2 つのデバイスが、特定の同じ動作パラメータおよび設定パラメータを持っていることを確認する必要があります。必要な設定の一貫性の詳細については、「vPC インターフェイスの互換パラメータ」の項を参照してください。

vPC ピアリンクを設定すると、vPC ピアデバイスは接続されたデバイスの一方がプライマリデバイスで、もう一方の接続デバイスがセカンダリデバイスであると交渉します（「vPC の設定」の項を参照）。Cisco NX-OS ソフトウェアは、最小の MAC アドレスを使用してプライマリデバイスを選択します。特定のフェールオーバー条件の下でだけ、ソフトウェアが各デバイス（つまり、プライマリデバイスおよびセカンダリデバイス）に対して異なるアクションを取ります。プライマリデバイスに障害が発生すると、システムの回復時にセカンダリデバイスが新しいプライマリデバイスになり、以前のプライマリデバイスがセカンダリデバイスになります。

どちらの vPC デバイスをプライマリデバイスにするか設定することもできます。vPC ピアデバイスのプライオリティを変更すると、ネットワークでインターフェイスがアップしたりダウン

ンしたりする可能性があります。1 台の vPC デバイスをプライマリ デバイスにするよう再度
ロールプライオリティを設定する場合は、プライオリティ値が低いプライマリ vPC デバイス
と値が高いセカンダリ vPC デバイスの両方でロールプライオリティを設定します。次に、
shutdown コマンドを入力して、両方のデバイスで vPC ピア リンクであるポート チャネルを
シャットダウンし、最後に **no shutdown** コマンドを入力して、両方のデバイスでポート チャ
ネルを再度イネーブルにします。



- (注) 各 vPC ピア リンクの各 vPC ピア デバイスの冗長性のために、2 つの異なるモジュールを使用
することを推奨します。

ソフトウェアは、vPC ピアを介して転送されたすべてのトラフィックをローカルトラフィック
としてキープします。ポート チャネルから入ってきたパケットは、vPC ピア リンクを介して
移動するのではなく、ローカルリンクの1つを使用します。不明なユニキャスト、マルチキャ
スト、およびブロードキャストトラフィック (STP BPDU を含む) は、vPC ピア リンクでフ
ラッディングされます。ソフトウェアが、マルチキャストフォワーディングを両方の vPC ピ
ア デバイス上で同期された状態に保ちます。

両方の vPC ピア リンク デバイスおよびダウンストリームデバイスで、任意の標準ロードバラ
ンシングスキームを設定できます (ロード バランシングについては、「ポート チャネルの設
定」の章を参照)。

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。(CFSoE の詳細については、「[CFSoE \(320 ページ\)](#)」の項を参照)。

両方のデバイス上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 デ
バイス間で同期されています。この同期に、CFSoE が使用されます (CFSoE の詳細につい
ては、「[CFSoE \(320 ページ\)](#)」の項を参照)

vPC ピア リンクに障害が発生した場合は、ソフトウェアが、両方のデバイスが稼働している
ことを確認するための vPC ピア デバイス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 デバイスのステータスをチェックします。vPC ピア デバイスが稼働し
ている場合は、セカンダリ vPC デバイスは、ループやトラフィックの消失あるいはフラッディ
ングを防ぐために、そのデバイス上のすべての vPC ポートをディセーブルにします。したがっ
て、データは、ポート チャネルの残っているアクティブな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たキープアライブメッセージが返されな
い場合に、vPC ピア デバイスに障害が発生したことを学習します。

vPC ピア デバイス間の設定可能なキープアライブメッセージの送信には、独立したリンク
(vPC ピアキープアライブリンク) を使用します。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から、障害が vPC ピア リンク上でだけ発生したのか、vPC ピア デバ
イス上で発生したのかがわかります。キープアライブメッセージは、vPC 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。キープアライブメッセージについ
ては、「ピアキープアライブリンクとメッセージ」の項を参照してください。

プライマリおよびセカンダリ デバイス上で手動で設定する必要がある機能

各 vPC ピア デバイスのプライマリ/セカンダリ マッピングに従うために、次の機能を手動で設定する必要があります。

- **STP ルート**：プライマリ vPC ピア デバイスを STP プライマリ ルート デバイスとして設定し、vPC セカンダリ デバイスを STP セカンダリ ルート デバイスとして設定します。vPC および STP の詳細については、「vPC ピア リンクと STP」の項を参照してください。
- **Bridge Assurance** がすべての vPC ピア リンク上でイネーブルになるように、vPC ピア リンク インターフェイスを STP ネットワーク ポートとして設定することを推奨します。
- **VLAN 単位の高速スパンニングツリー (PVST+)** を設定してプライマリ デバイスがすべての VLAN のルートになるようにし、**マルチ スパンニングツリー (MST)** を設定してプライマリ デバイスがすべてのインスタンスのルートになるようにすることを推奨します。
- **レイヤ3 VLAN ネットワーク インターフェイス**：両方のデバイスから同じ VLAN の VLAN ネットワーク インターフェイスを設定することにより、各 vPC ピア デバイスのレイヤ3 接続を設定します。
- **HSRP アクティブ**：vPC ピア デバイス上でホットスタンバイ ルータ プロトコル (HSRP) と VLAN インターフェイスを使用する場合は、プライマリ vPC ピア デバイスを HSRP アクティブの最も高いプライオリティで設定します。セカンダリ デバイスを HSRP スタンバイになるように設定し、各 vPC デバイスの VLAN インターフェイスが同じ管理/動作モードにあることを確認します (vPC および HSRP の詳細については、「vPC ピア リンクとルーティング」の項を参照)。

単方向リンク検出 (UDLD) の設定では、次の留意点に注意してください。

- LACP がポート チャネル集約プロトコルとして使用されている場合は、vPC ドメイン内に UDLD は必要ありません。
- LACP がポート チャネル集約プロトコル (静的なポート チャネル) として使用されていない場合は、vPC メンバー ポートの通常モードで UDLD を使用します。
- STP が Bridge Assurance なしで使用されている場合と LACP が使用されていない場合は、vPC 孤立ポートの通常モードで UDLD を使用します。

ピアキーブアライブ リンクとメッセージ

Cisco NX-OS ソフトウェアは、vPC ピア間でピアキーブアライブ リンクを使用して、設定可能なキーブ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接続がなくはなりません。ピアキーブアライブリンクが有効になつて稼働していないと、システムは vPC ピア リンクを稼働させることができません。



- (注) vPC ピアキーブアライブリンクを、各vPCピアデバイス内のレイヤ3インターフェイスにマッピングされている独立した VRF に関連付けることを推奨します。独立した VRF を設定しなかった場合は、デフォルトで管理 VRF と管理ポートが使用されます。vPC ピア キープアライブ メッセージの送受信に vPC ピア リンク自体を使用することはしないでください。

片方の vPC ピア デバイスに障害が発生したら、vPC ピア リンクの他方の側にある vPC ピア デバイスは、ピアキーブアライブメッセージを受信しなくなることによってその障害を感知します。vPC ピアキーブアライブ メッセージのデフォルトの間隔は、1 秒です。この間隔は、400 ミリ秒～ 10 秒の範囲内で設定可能です。

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 ピアリンクがダウンすると開始します。セカンダリ vPC ピア デバイスは、ネットワークの収束が確実に発生してから vPC アクションが発生するようにするために、このホールドタイムアウト期間の間は vPC ピアキーブアライブ メッセージを無視します。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。

タイムアウト値は、3～20秒の範囲内で設定可能で、デフォルトのタイムアウト値は5秒です。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。このタイムアウト期間の間は、セカンダリ vPC ピア デバイスは、プライマリ vPC ピア デバイスから vPC ピアキーブアライブ hello メッセージが送信されてこないかチェックします。セカンダリ vPC ピア デバイスが1つの hello メッセージを受信したら、そのデバイスは、セカンダリ vPC ピア デバイス上のすべての vPC インターフェイスをディセーブルにします。

ホールドタイムアウトパラメータとタイムアウトパラメータの相違点は、次のとおりです。

- ホールドタイムアウトの間は、vPCセカンダリ デバイスは、受信したキーブアライブメッセージに基づいてアクションを起こしません。それにより、たとえばスーパーバイザがピアリンクがダウンした数秒後に失敗した場合などに、キーブアライブが一時的に受信される可能性がある場合に、システムがアクションを起こすのを回避できます。
- タイムアウト中は、vPCセカンダリ デバイスは、設定された間隔が終了するまでにキーブアライブメッセージを受信できないと、vPCプライマリ デバイスになるというアクションを取ります。

キーブアライブメッセージへのタイマーの設定については、「vPC キープアライブリンクとメッセージの設定」の項を参照してください。



- (注) ピアキーブアライブメッセージに使用される送信元 IP アドレスと宛先 IP アドレスがどちらもネットワーク上で一意であり、かつそれらの IP アドレスがその vPC ピアキーブアライブリンクに関連付けられている VRF から到達可能であることを確認してください。

ピアキーブアライブ IP アドレスは、グローバルユニキャストアドレスである必要があります。リンクローカルアドレスはサポートされていません。

コマンドラインインターフェイス (CLI) を使用して、vPC ピアキープアライブメッセージを使用するインターフェイスを信頼できるポートとして設定してください。優先順位をデフォルト (6) のままにしておくか、またはもっと高い値に設定します。

vPC ドメイン

vPC ドメイン ID を使用すれば、vPC ダウンストリーム デバイスに接続されている vPC ピアリンクとポートを識別できます。

vPC ドメインは、キープアライブメッセージや他の vPC ピアリンク パラメータを、デフォルト値をそのまま使用するのではなく値を設定する場合に使用する構成モードでもあります。これらのパラメータの設定の詳細については、「vPC の設定」の項を参照してください。

vPC ドメインを作成するには、まず各 vPC ピア デバイス上で、1 ~ 1000 の値を使用して vPC ドメイン ID を作成しなければなりません。vPC ピアごとに設定できる vPC ドメイン ID は 1 つだけです。

各デバイス上で、vPC ピアリンクとして機能させるポートチャネルを明示的に構成する必要があります。各デバイス上で vPC ピアリンクにしたポートチャネルを、1 つの vPC ドメインからの同じ vPC ドメイン ID に関連付けます。このドメイン内で、システムはループフリートポロジとレイヤ 2 マルチパスを提供します。

これらのポートチャネルと vPC ピアリンクは、静的にしか構成できません。ポートチャネルおよび 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構成できます。各 vPC でポートチャネルを設定するにはアクティブモードのインターフェイスで LACP を使用することを推奨します。それにより、ポートチャネルのフェールオーバーシナリオの最適でグレースフルなリカバリが保証され、ポートチャネル間の設定不一致に対する設定検査が行われます。

vPC ピア デバイスは、設定された vPC ドメイン ID を使用して、一意の vPC システム MAC アドレスを自動的に割り当てます。各 vPC ドメインが、具体的な vPC 関連操作に ID として使用される一意の MAC アドレスを持ちます。ただし、デバイスは vPC システム MAC アドレスを LACP などのリンクスコープでの操作にしか使用しません。連続したレイヤ 2 ネットワーク内の各 vPC ドメインを、一意のドメイン ID で作成することを推奨します。Cisco NX-OS ソフトウェアにアドレスを割り当てさせるのではなく、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 MAC テーブルを表示する詳細については、「vPC および孤立ポート」の項を参照してください。

vPC ドメインを作成した後は、Cisco NX-OS ソフトウェアによって vPC ドメインのシステムプライオリティが作成されます。vPC ドメインに特定のシステムプライオリティを設定することもできます。

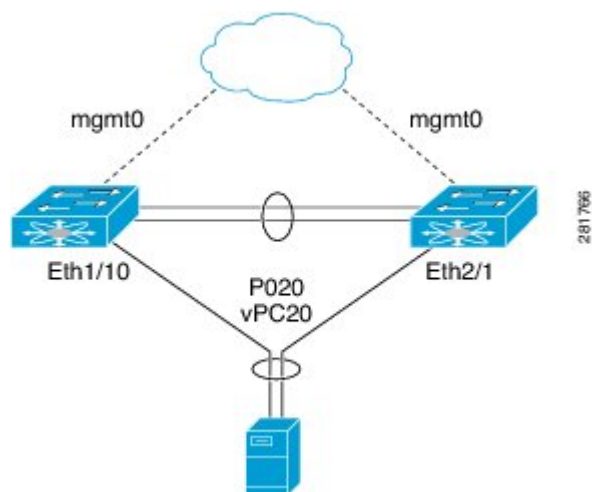


(注) システムプライオリティを手動で設定する場合は、必ず両方の vPC ピア デバイス上で同じプライオリティ値を割り当てる必要があります。vPC ピア デバイス同士が異なるシステムプライオリティ値を持っていると、vPC は稼働しません。

vPC トポロジ

次の図は、Cisco Nexus 9000 シリーズ デバイス ポートが別のスイッチまたはホストに直接接続され、vPC の一部となるポート チャンネルの一部として設定される基本設定を示しています。

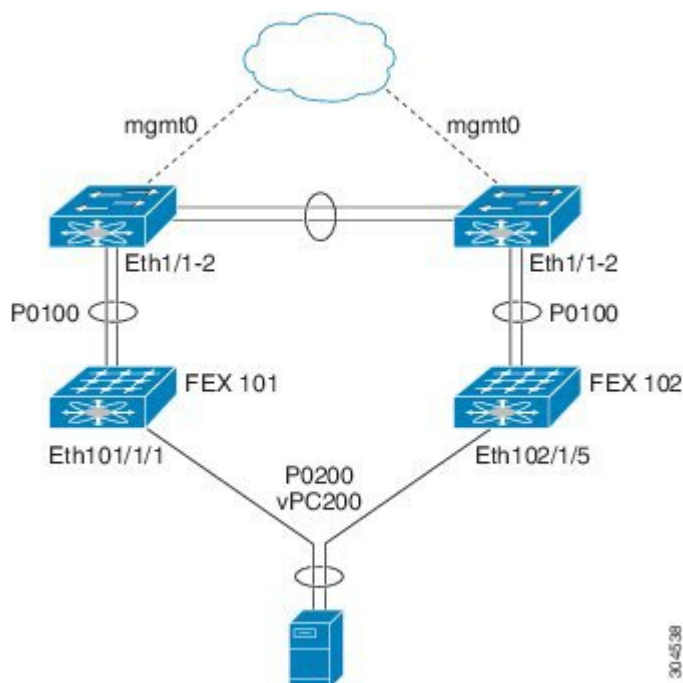
図 15: vPC トポロジのスイッチ



この図では、vPC 20 がポート チャンネル 20 で設定され、最初のデバイスには Eth1/10 が、2 番目のデバイスには Eth2/1 がメンバポートとしてあります。

図で示されるように、ファブリック エクステンダ (FEX) を通してピア デバイスから vPC を設定できます。

図 16: FEX Straight-Through トポロジ (ホスト vPC)



この図では、各 FEX は Cisco Nexus 9000 シリーズ デバイスがあるシングル ホーム接続 (Straight-Through FEX トポロジ) です。この FEX 上のホストインターフェイスはポートチャネルとして設定され、それらのポートチャネルは vPC として設定されています。Eth101/1/1 および Eth102/1/5 は、PO200 のメンバーとして設定され、PO200 は vPC 200 に対し設定されます。

どちらのトポロジでも、ポートチャネル P020 および P0200 をピアスイッチ上でまったく同じように設定する必要があります。その後、設定の同期を使用して vPC スイッチの設定を同期します。

FEX ポートの設定に関する詳細は、『[Cisco Nexus 2000 Series NX-OS Fabric Extender Configuration Guide for Cisco Nexus 9000 Series Switches](#)』を参照してください。

vPC インターフェイスの互換パラメータ

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 ピアリンクに使用するレイヤ 2 ポートチャネルはトランクモードに設定することを推奨します。

vPC 機能をイネーブルにし、さらに両方の vPC ピアデバイス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 ピアデバイスに関する設定のコピーがリモート vPC ピアデバイスへ送信されます。これにより、システムが 2 つのデバイス上で異なっている重要な設定パラメータがないか調べます (CFS の詳細については、「vPC および孤立ポート」の項を参照)。



- (注) **show vpc consistency-parameters** を入力します。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。



- (注) ポート チャネルの互換性パラメータは、物理スイッチのすべてのポート チャネル メンバーで同じである必要があります。vPC の一部になるように共有インターフェイスを設定できません。

vPC の互換性チェックプロセスは、正規のポートチャネルの互換性チェックとは異なります。
正規のポート チャネルについては、「ポート チャネルの設定」の章を参照してください。

同じでなければならない設定パラメータ

このセクションの設定パラメータは、vPC ピア リンクの両方のデバイスで同じに設定する必要があります。そうしないと、vPC は一時停止モードに完全にまたは部分的に移動します。



- (注) ここで説明する動作パラメータおよび設定パラメータは、vPC 内のすべてのインターフェイスで一致している必要があります。



- (注) **show vpc consistency-parameters** を入力します。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 インターフェイスでのこれらのパラメータの一部は、デバイスによって自動的に互換性がチェックされます。インターフェイスごとのパラメータは、インターフェイスごとに一貫性を保っていなければならない、グローバルパラメータはグローバルに一貫性を保っていなければならない。

- ポートチャネル モード：オン、オフ、またはアクティブ（ただし、ポートチャネル モードは vPC ピアの各サイドでアクティブ/パッシブにできます）
- []設定は、vPC の両側で同じである必要があります。 **no lacp suspend-individual pxe**
- チャネル単位のリンク速度
- チャネル単位のデュプレックス モード
- チャネルごとのトランク モード：
 - ネイティブ VLAN

- トランク上で許可される VLAN
- ネイティブ VLAN トラフィックのタギング
- スパニング ツリー プロトコル (STP) モード
- Multiple Spanning Tree 用の STP リージョン コンフィギュレーション
- 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
 - 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
- 最大伝送単位 (MTU)

これらのパラメータのいずれかがイネーブルになっていなかったり、片方のデバイスでしか定義されていないと、vPC の一貫性チェックではそのパラメータは無視されます。



(注) どの vPC インターフェイスもサスペンドモードになっていないことを確認するには、**show vpc brief** および **show vpc consistency-parameters** コマンドを実行し、syslogメッセージを確認します。

show vpc または **show vpc brief** コマンドの出力では、vPC ポートチャネルが 50 回構成されるたびに、次のメッセージが表示されます。

「show vpc consistency-parameters vpc <vpc-num>」を実行して、ダウンした vpc の整合性の理由および任意の vpc のタイプ 2 の整合性の理由を確認してください。

同じにすべき設定パラメータ

次の挙げるパラメータのいずれかが両方の vPC ピア デバイス上で同じように設定されていないと、誤設定が原因でトラフィックフローに望ましくない動作が発生する可能性があります。

- MAC エージング タイマー
- スタティック MAC エントリ

- VLAN インターフェイス：vPC ピア リンク エンドにある各デバイスの VLAN インターフェイスが両エンドで同じ VLAN 用に設定されていなければならない、さらに同じ管理モードで同じ動作モードになっていなければなりません。vPC ピア リンクの 1 個のデバイスだけで設定されている VLAN は、vPC または vPC ピア リンクを使用してトラフィックを通過させません。すべての VLAN をプライマリ vPC デバイスとセカンダリ vPC デバイスの両方で作成する必要があります。そうっていない VLAN は、停止します。
- ACL のすべての設定とパラメータ
- Quality of Service (QoS) の設定とパラメータ
- 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+)
- ポート セキュリティ
- Cisco Trusted Security (CTS)
- ダイナミック ホスト コンフィギュレーション プロトコル (DHCP) スヌーピング
- ネットワーク アクセス コントロール (NAC)
- ダイナミック ARP インスペクション (DAI)
- IP ソース ガード (IPSG)
- インターネット グループ管理プロトコル (IGMP) スヌーピング
- ホット スタンバイ ルーティング プロトコル (HSRP)
- プロトコルに依存しないマルチキャスト (PIM)
- すべてのルーティング プロトコル設定

すべての設定パラメータで互換性が取れていることを確認するために、vPC の設定が終わったら、各 vPC ピア デバイスの設定を表示してみることを推奨します。

パラメータの不一致によってもたらされる結果

稼働中の vPC で不一致が発生した場合にセカンダリ ピア デバイス上のリンクのみを一時停止する、グレースフル整合性検査機能を設定できます。この機能は CLI のみで設定可能で、デフォルトでイネーブルになっています。

graceful consistency-check コマンドはデフォルトで設定されます。

一致しなければならないパラメータのリストのすべてのパラメータに関する整合性検査の一部として、システムはすべての VLAN の一貫性をチェックします。

vPC は稼動を継続し、矛盾した VLAN のみがダウンします。この VLAN 単位の整合性検査機能はディセーブルにできず、マルチ スパニングツリー (MST) VLAN には適用されません。

vPC 番号

vPC ドメイン ID と vPC ピア リンクを作成し終わったら、ダウンストリーム デバイスを各 vPC ピア デバイスに接続するためのポート チャネルを作成します。つまり、プライマリ vPC ピア デバイスからダウンストリーム デバイスへのポート チャネルを 1 つ作成し、もう 1 つ、セカンダリ ピア デバイスからダウンストリーム デバイスへのポート チャネルも作成します。



-
- (注) スイッチとしてもブリッジとしても機能しないホストまたはネットワーク デバイスに接続されているダウンストリーム デバイス上のポートは、STP エッジ ポートとして設定することを推奨します。
-

各 vPC ピア デバイス上で、ダウンストリーム デバイスに接続するポート チャネルに 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。すべてのポート番号に、ポート チャネル自体と同じ vPC ID 番号を割り当てると (つまり、ポート チャネル 10 には vPC ID 10) 、設定が簡単になります。



-
- (注) vPC ピア デバイスからダウンストリーム デバイスに接続するためにポート チャネルに割り当てられる vPC 番号は、両方の vPC ピア デバイスで同じである必要があります。
-

ヒットレス vPC ロールの変更

仮想ポート チャネル (vPC) は、2 つの異なる Cisco Nexus 9000 シリーズ デバイスに物理的に接続されたリンクを、単一のポート チャネルとして扱えるようにします。vPC ロールの変更機能は、トラフィック フローに影響を与えることなく、vPC ピア間で vPC ロールを切り替えることができるようにします。vPC ロールの切り替えは、vPC ドメインに属しているデバイスのロール優先順位の値に基づいて行われます。vPC ロールの切り替え中にロール優先順位が低い vPC ピア デバイスがプライマリ vPC デバイスとして選択されます。vpc role preempt コマンドを使用して、ピア間で vPC ロールを切り替えることができます。

ヒットレス vPC ロール変更の設定方法については、[ヒットレス vPC ロール変更の設定 \(363 ページ\)](#) を参照してください。

他のポート チャネルの vPC への移行



- (注) ダウンストリーム デバイスは、ポート チャネルを使用して両方の vPC ピア デバイスに接続する必要があります。

ダウンストリーム デバイスを接続するために、プライマリ vPC ピア デバイスからダウンストリーム デバイスへのポート チャネルを作成し、セカンダリ ピア デバイスからダウンストリーム デバイスへのもう 1 つのポート チャネルを作成します。各 vPC ピア デバイス上で、ダウンストリーム デバイスに接続するポート チャネルに 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。

vPC オブジェクト トラッキング



- (注) Cisco Nexus 9500 デバイスの異なるモジュールの専用ポート上で vPC ピア リンクを設定して、障害発生の可能性を下げることをお勧めします。これは、障害の可能性を減らすために推奨されます。復元力を最適にしたい環境では、少なくとも 2 つのモジュールを使用してください。

vPC オブジェクト トラッキングは、vPC ピア リンクとコアへのアップリンクの両方が存在するモジュールで障害が発生した場合、トラフィックのブラックホールになってしまうことを防止するために使用されます。トラッキングインターフェイス機能により、影響を受けるスイッチで vPC を一時停止し、トラフィックのブラックホールとなるのを防ぐことができます。

すべての vPC ピア リンクとコアに面するインターフェイスを単一モジュール上で設定しなければならない場合は、両方の vPC ピア デバイス上のすべての vPC ピア リンク上にあり、コアへのレイヤ 3 リンクに関連付けられているトラック オブジェクトとトラック リストをコマンドラインインターフェイスを使用して設定してください。トラック リスト上のすべてのトラッキング対象オブジェクトが停止した場合、システムは次のように動作するため、この設定を使用すれば、その特定のモジュールが停止した場合のトラフィックのドロップを避けることができます。

- vPC プライマリ ピア デバイスによるピアキープアライブメッセージの送信を停止します。これにより、vPC セカンダリ ピア デバイスが強制的に引き継がされます。
- その vPC ピア デバイス上のすべてのダウンストリーム vPC を停止させます。これにより、すべてのトラフィックが強制的に他の vPC ピア デバイスに向けてそのアクセス スイッチでルーティングされます。

いったんこの機能を設定したら、モジュールに障害が発生した場合には、システムが自動的にプライマリ vPC ピア デバイス上のすべての vPC リンクを停止させ、ピアキープアライブメッセージを停止します。このアクションにより、vPC セカンダリ デバイスが強制的にプライマリ ロールを引き継がされ、システムが安定するまで、すべての vPC トラフィックがこの新しい vPC プライマリ デバイスに送られます。

コアに対するすべてのリンクおよびすべての vPC ピア リnkを含むトラック リストを、そのオブジェクトとして作成する必要があります。このトラック リストの指定した vPC ドメインに対して、トラッキングをイネーブルにします。この同じ設定を他方の vPC ピア デバイスにも適用します。オブジェクト トラッキングおよびトラック リストの詳細については、『[Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide](#)』を参照してください。



- (注) 次の例では、Boolean OR を追跡リストで使用し、完全なモジュール障害の場合にのみすべてのトラフィックが vPC ピア デバイスへ流れるよう強制します。コア インターフェイスまたは vPC ピア リンクがダウンしたときにスイッチオーバーをトリガーする場合は、次の追跡リストでブール AND を使用します。

単一モジュール上の関連するすべてのインターフェイスが故障したときに vPC をリモートピアに切替えるように追跡リストを設定するには、次の手順に従います。

1. インターフェイス上（コアへのレイヤ3）およびポートチャネル上（vPC ピア リンク）でトラック オブジェクトを設定します。

```
switch(config-if)# track 35 interface ethernet 8/35 line-protocol
switch(config-track)# track 23 interface ethernet 8/33 line-protocol
switch(config)# track 55 interface port-channel 100 line-protocol
```

2. ブール OR を使って追跡リスト内のすべてのインターフェイスを含むトラック リストを作成して、すべてのオブジェクトに障害が発生したときにトリガーします。

```
switch(config)# track 44 list boolean OR
switch(config-track)# object 23
switch(config-track)# object 35
switch(config-track)# object 55
switch(config-track)# end
```

3. このトラック オブジェクトを vPC ドメインに追加します。

```
switch(config)# vpc domain 1
switch(config-vpc-domain)# track 44
```

4. トラック オブジェクトを表示します。

```
switch# show vpc brief
Legend:
(*) - local vPC is down, forwarding via vPC peer-link
vPC domain id : 1
Peer status : peer adjacency formed ok
vPC keep-alive status : peer is alive
Configuration consistency status: success
vPC role : secondary
Number of vPCs configured : 52
Track object : 44
vPC Peer-link status
-----
```

```

id Port Status Active vlans
-----
1 Po100 up 1-5,140
vPC status
-----
id Port Status Consistency Reason Active vlans
-----
1 Po1 up success success 1-5,140

```

次に、オブジェクト トラッキングに関する情報を表示する例を示します。

```

switch# show track brief
Track Type Instance Parameter State Last
Change
23 Interface Ethernet8/33 Line Protocol UP 00:03:05
35 Interface Ethernet8/35 Line Protocol UP 00:03:15
44 List ----- Boolean
or UP 00:01:19
55 Interface port-channel100 Line Protocol UP 00:00:34

```

その他の機能との vPC の相互作用

vPC と LACP

LACP は、vPC ドメインのシステム MAC アドレスを使用して、vPC の LACP Aggregation Group (LAG) ID を形成します (LAG-ID および LACP については、「ポート チャンネルの設定」の章を参照)。

ダウンストリームデバイスからのチャンネルも含めて、すべての vPC ポートチャンネル上の LACP を使用できます。LACP は、vPC ピア デバイスの各ポート チャンネル上のインターフェイスのアクティブモードで設定することを推奨します。この設定により、デバイス、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 デバイスのシステム プライオリティを手動で設定して、vPC ピア リンク デバイスが、接続されているダウンストリーム デバイスより確実に高い LACP プライオリティを持つようにすることを推奨します。システム プライオリティの値が低いほど、高い LACP プライオリティを意味します。



- (注) システム プライオリティを手動で設定する場合は、必ず両方の vPC ピア デバイス上で同じプライオリティ値を割り当てる必要があります。vPC ピア デバイス同士が異なるシステム プライオリティ値を持っていると、vPC は稼働しません。

vPC ピア リンクと STP

vPC はループフリーなレイヤ 2 トポロジを提供しますが、それでもやはり、誤った配線やケーブルの欠陥、誤設定などから保護するためのフェールセーフ メカニズムを STP が提供する必

必要があります。vPC を初めて稼働させたときに、STP による再コンバージェンスが発生します。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 リンク上でブリッジアシュアランスが自動的に有効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 拡張機能も有効にしないことも推奨します。STP 拡張がすでに設定されている場合、その拡張が vPC ピアリンクの問題の原因となることはありません。

MST と Rapid PVST+ の両方を実行している場合は、必ず PVST シミュレーション機能を正しく設定してください。

STP 拡張機能および PVST シミュレーションについては、『[Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide](#)』を参照してください。



-
- (注) パラメータのリストは、vPC ピアリンクの両サイドの vPC ピアデバイス上で同じになるように設定する必要があります。このような一致が必要な設定については、「vPC インターフェイスの互換パラメータ」の項を参照してください。
-

STP は分散しています。つまり、このプロトコルは、両方の vPC ピアデバイス上で実行され続けます。ただし、プライマリデバイスとして選択されている vPC ピアデバイス上での設定が、セカンダリ vPC ピアデバイス上の vPC インターフェイスの STP プロセスを制御します。

プライマリ vPC デバイスは、Cisco Fabric Services over Ethernet (CFS over E) を使用して、vPC セカンダリピアデバイス上の STP の状態を同期させます。CFS over E の詳細については、「vPC および孤立ポート」の項を参照してください。

vPC の STP プロセスも、ピアリンク上で接続されているデバイスの 1 つに障害が発生したときにそれを検出するために、定期的なキープアライブメッセージに依存しています。これらのメッセージについては、「ピアキープアライブリンクとメッセージ」の項を参照してください。

vPC マネージャが、vPC ピアデバイス間で、プライマリデバイスとセカンダリデバイスを設定して 2 つのデバイスを STP 用に調整する提案/ハンドシェイク合意を実行します。その後、プライマリ vPC ピアデバイスが、プライマリデバイスとセカンダリデバイス両方での STP プロトコルの制御を行います。プライマリ vPC ピアデバイスを STP プライマリルートデバイスとして設定し、セカンダリ vPC デバイスを STP セカンダリルートデバイスになるように設定することを推奨します。

プライマリ vPC ピアデバイスがセカンダリ vPC ピアデバイスにフェールオーバーした場合、STP トポロジには何の変化も発生しません。

BPDU は、代表ブリッジ ID フィールドで、STP ブリッジ ID の vPC に設定されている MAC アドレスを使用します。vPC プライマリデバイスが、vPC インターフェイス上でこれらの BPDU を送信します。

次のパラメータについて同じ STP 設定を使用して、vPC ピアリンクの両エンドを設定する必要があります。

- STP グローバル設定：
 - STP モード
 - MST のための STP リージョン設定
 - VLAN ごとのイネーブル/ディセーブル状態
 - ブリッジ保証設定
 - ポート タイプ設定
 - 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



(注) これらのパラメータのいずれかに誤設定があった場合、Cisco NX-OS ソフトウェアが vPC 内のすべてのインターフェイスを停止します。syslog をチェックし、**show vpc brief** を開始します。コマンドを入力して、vPC インターフェイスが停止していないか確認してください。

次の STP インターフェイス設定が、vPC ピアリンクの両側で同じになっていることを確認します。そうならないと、トラフィックフローに予測不能な動作が発生する可能性があります。

- 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 (PVRST+)



(注) vPC ピアリンクの両側での設定を表示して、設定が同じであることを確認してください。

show spanning-tree コマンドを使用すればコマンドで vPC に関する情報を表示できます。例については、『[Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide](#)』を参照してください。



- (注) ダウンストリームデバイスのポートは、STP エッジポートとして設定することを推奨します。スイッチに接続されているすべてのホストポートを STP エッジポートとして設定してください。STP ポート タイプの詳細については、『[Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide](#)』を参照してください。

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、Cisco NX-OS に追加されました。この機能により、一対の Cisco Nexus 9000 シリーズ デバイスをレイヤ 2 トポロジ内に 1 つの STP ルートとして表示できます。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、ダウンストリーム 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。

この機能は、すべてのデバイス vPC に属する純粋なピア スイッチ トポロジで使用できます。



- (注) ピア スイッチ機能は、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。vPC 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。

STP 拡張機能および Rapid PVST+ については、『[Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide](#)』を参照してください。

vPC ピア ゲートウェイ

vPC ピア デバイスを、vPC ピア デバイスの MAC アドレスに送信されるパケットに対してもゲートウェイとして機能するように設定できます。

peer-gateway コマンドを使用し、**peer-gateway** コマンドを使用します。



- (注) この項で説明している **peer-gateway exclude-vlan** コマンド (vPC ピア デバイスでレイヤ 3 バックアップルーティングの VLAN インターフェイスを構成する際に使用) は、サポートされていません。

一部のネットワーク接続ストレージ (NAS) デバイスまたはロードバランサは、特定のアプリケーションのパフォーマンスを最適化するのに役立つ機能を備えている場合があります。これらの機能により、同じサブネットにローカルに接続されていないホストから送信された要求に応答するときに、デバイスはルーティングテーブルのルックアップを回避できます。このようなデバイスは、一般的な HSRP ゲートウェイではなく、送信元 Cisco Nexus 9000 シリーズデバイスの MAC アドレスを使用して、トラフィックに応答する場合があります。この動作は、一部の基本的なイーサネット RFC 基準に準拠していません。ローカルではないルータ MAC アドレスの vPC デバイスに到達するパケットは、vPC ピア リンクを介して送信され、最終的な宛先が他の vPC の背後にある場合には、組み込みの vPC ループ回避メカニズムによってドロップされる場合があります。

vPC ピアゲートウェイ機能は、vPC スイッチが、vPC ピアのルータ MAC アドレスを宛先とするパケットに対して、アクティブなゲートウェイとして機能することを可能にします。この機能は、このようなパケットが vPC ピア リンクを通過する必要なしにローカルに転送されることを可能にします。このシナリオでは、この機能によって vPC ピア リンクの使用が最適化され、トラフィック損失が回避されます。

ピアゲートウェイ機能の設定は、プライマリ vPC ピアとセカンダリ vPC ピアの両方で行う必要がありますが、デバイスの稼働も vPC トラフィックも中断しません。vPC ピアゲートウェイ機能は、vPC ドメイン サブモードの下でグローバルに設定できます。

この機能をイネーブルにすると、ピアゲートウェイルータを介してスイッチングされたパケットの IP リダイレクトメッセージの発生を避けるために、Cisco NX-OS は vPC VLAN を介してマッピングされるすべてのインターフェイス VLAN 上で IP リダイレクトを自動的にディセーブルにします。

TTL が 1 のパケットが TTL の有効期限が原因で伝送中にドロップされるように、ピアゲートウェイ vPC デバイスに到達するパケットは、デクリメントされたパケット存続時間 (TTL) を有しています。ピアゲートウェイ機能がイネーブルで、TTL が 1 のパケットを送信する特定のネットワーク プロトコルが vPC VLAN で動作する場合は、この状況を考慮する必要があります。

vPC および ARP または ND

Cisco Fabric Service over Ethernet (CFSoS) プロトコルの信頼性が高いトランスポートメカニズムを使用した、vPC ピア間のテーブル同期に対応する機能が Cisco NX-OS に追加されました。**ip arp synchronize** を有効にする必要があります および **ipv6 nd synchronize** コマンドをイネーブルにし、vPC ピア間のアドレステーブルのコンバージェンスの高速化をサポートする必要があります。このコンバージェンスにより、vPC ピアリンクポートチャネルがフラップしたり、vPC ピアがオンラインに戻るときに、IPv4 の場合は ARP テーブルの復元でまたは IPv6 の場合は ND テーブルの復元で発生する遅延を解消できます。

vPC マルチキャスト : PIM、IGMP、および IGMP スヌーピング

Nexus 9000 シリーズデバイス用の Cisco NX-OS ソフトウェアは、vPC で次をサポートします。

- PIM Any Source Multicast (ASM)。
- PIM Source-Specific Multicast (SSM)。



(注) Cisco NX-OS ソフトウェアは、vPC での双方向 (BIDR) をサポートしません。

ソフトウェアが、マルチキャストフォワーディングを両方の vPC ピア デバイス上で同期された状態に保ちます。vPC ピア デバイス上の IGMP スヌーピング プロセスは、学習したグループ情報を vPC ピア リンクを通じて他の vPC ピア デバイスと共有します。マルチキャスト状態は、常に両方の vPC ピア デバイス上で同期されます。vPC モードでの PIM プロセスは、1 つの vPC ピア デバイスだけが受信者に向けてマルチキャストトラフィックを転送する状態を確保します。

各 vPC ピアは、レイヤ 2 またはレイヤ 3 デバイスです。マルチキャストトラフィックは 1 つの vPC ピア デバイスだけから伝送されます。次のシナリオで、重複したパケットが観察される場合があります。

- 孤立ホスト
- 送信元と受信者が、マルチキャストルーティングのイネーブルになった異なる VLAN 内のレイヤ 2 vPC クラウド内にあり、vPC メンバリンクが停止している場合。

次のシナリオで、ごくわずかなトラフィック損失が観察される場合があります。

- トラフィックを転送している vPC ピア デバイスをリロードした場合。
- トラフィックを転送している vPC ピア デバイスの PIM を再起動した場合。

全体的なマルチキャストコンバージェンス時間は、スケールと vPC ロールの変更 / PIM 再起動期間に依存します。

必ずすべてのレイヤ 3 デバイスを両方の vPC ピア デバイスにデュアル接続してください。片方の vPC ピア デバイスが停止した場合、他方の vPC ピア デバイスが、通常どおりにすべてのマルチキャストトラフィックを転送し続けます。

次に、vPC PIM および vPC IGMP/IGMP スヌーピングについて説明します。

- vPC PIM : vPC モードの PIM プロセスは、1 台の vPC ピア デバイスのみがマルチキャストトラフィックを転送する状態を確保します。vPC モードの PIM プロセスは、送信元の状態を両方の vPC ピア デバイスと同期させ、トラフィックを転送する vPC ピア デバイスを選択します。
- vPC IGMP/IGMP スヌーピング : vPC モードの IGMP プロセスは、両方の vPC ピア デバイスで指定ルータ (DR) 情報を同期させます。デュアル DR は、vPC モードのときに IGMP で利用可能です。デュアル DR は、vPC モードでない場合は利用できません。これは、両方の vPC ピア デバイスがピア間のマルチキャストグループ情報を保持するためです。



- (注) vPC VLAN (vPC ピアリンクで伝送される VLAN) 上のスイッチ仮想インターフェイス (SVI) とダウンストリーム デバイス間の PIM 隣接関係はサポートされません。この設定により、マルチキャストパケットがドロップされる可能性があります。ダウンストリームデバイスと PIM ネイバー関係が必要な場合は、vPC SVI ではなく、物理レイヤ 3 インターフェイスを Nexus スイッチで使用する必要があります。

vPC VLAN 上の SVI では、vPC ピアスイッチとの PIM 隣接関係が 1 つだけサポートされます。vPC-SVI の vPC ピアスイッチ以外のデバイスとの vPC ピアリンク上の PIM 隣接関係はサポートされていません。

IGMP スヌーピングは、両方の vPC ピアデバイス上で同じようにイネーブルにしたりディセーブルにしたりする必要があり、すべての機能設定を同じにする必要があります。IGMP スヌーピングは、デフォルトで有効になっています。



- (注) 次のコマンドは、vPC モードでサポートされていません。

- **ip pim spt-threshold infinity**
- **ip pim use-shared-tree-only**

マルチキャストの詳細については、『Cisco Nexus 9000 Series NX-OS Multicast Routing Configuration Guide』を参照してください。

マルチキャスト PIM デュアル DR (プロキシ DR)

デフォルトでは、マルチキャスト ルータは該当する受信先が存在する場合のみ PIM ジョインをアップストリームに送信します。これらの該当する受信先は、IGMP ホスト (IGMP レポートを通じて通信します) または他のマルチキャスト ルータ (PIM ジョインを通じて通信します) のどちらかの場合があります。

Cisco NX-OS vPC 実装では、PIM はデュアル指定ルータ (DR) モードで動作します。つまり、vPC デバイスが vPC SVI の発信インターフェイス (OIF) 上の DR である場合、そのピアは自動的にプロキシ DR ロールを引き継ぎます。IGMP は、OIF が DR である場合、OIF (レポートはその OIF で学習されます) をフォワーディングに追加します。デュアル DR では、両方の vPC デバイスには、次の例に示すように、vPC SVI OIF に対して同一のエントリ (*,G) があります。

```
VPC Device1:
-----
(*,G)
oif1 (igmp)
VPC Device2:
-----
(*,G)
oif1 (igmp)
```

IP PIM PRE-BUILD SPT

マルチキャストソースがレイヤ3クラウド (vPC ドメイン外) にある場合、1つの vPC ピアが送信元のフォワーダとして選定されます。このフォワーダの選択は、送信元に到達するためのメトリックに基づきます。関係がある場合、vPC プライマリはフォワーダとして選択されます。フォワーダのみがその関連する (S,G) 内に vPC OIF を持っており、非フォワーダ (S,G) は 0 OIF を持っています。したがって、フォワーダのみがこの例に示すように、送信元へ PIM (S,G) ジョインを送信します。

```
VPC Device1 (say this is Forwarder for Source 'S'):
-----
(*,G)
oif1 (igmp)
(S,G)
oif1 (mrib)
VPC Device2:
-----
(*,G)
oif1 (igmp)
(S,G)
NULL
```

障害が発生した場合 (たとえば、フォワーダのレイヤ3リバースパス転送 (RPF) リンクが動作しない、またはフォワーダがリロードされるなど)、現在の非フォワーダが最終的にフォワーダになる場合は、トラフィック取得するために送信元への (S,G) に対する PIM ジョインの送信を開始をする必要があります。送信元に到達するホップ数によって、この操作には時間がかかる場合があります (PIM はホップバイホッププロトコルです)。

この問題を排除し、より優れたコンバージェンスを取得するには、**ip pim pre-build-spt** を使用します コマンドを使用します。このコマンドにより、マルチキャストルートに 0 OIF があっても PIM はジョインを送信できます。vPC デバイスでは、非フォワーダは送信元へ PIM (S,G) ジョインをアップストリームに送信します。欠点は、非フォワーダからのリンク帯域幅のアップストリームが最終的にそれによってドロップされるトラフィックに使用されることです。コンバージェンスの向上によるメリットは、リンク使用帯域幅をはるかに上回っていることです。したがって、vPC を使用する場合は、このコマンドを使用することを推奨します。

vPC ピア リンクとルーティング

ファーストホップ冗長性プロトコル (FHRP) は、vPC と相互運用します。Hot Standby Routing Protocol (HSRP)、および Virtual Router Redundancy Protocol (VRRP) のすべてが、vPC と相互運用できます。すべてのレイヤ3 デバイスを両方の vPC ピア デバイスにデュアル接続することを推奨します。

プライマリ FHRP デバイスは、たとえセカンダリ vPC デバイスがデータトラフィックを転送したとしても、ARP 要求に応答します。

プライマリ vPC ピア デバイスを FHRP アクティブルータの最も高いプライオリティで設定しておくと、初期の設定確認と vPC/HSRP のトラブルシューティングを簡単にできます。

さらに、if-hsrp コンフィギュレーションモードで **priority** コマンドを使用して、vPC ピアリンク上でイネーブルになっているグループの状態がスタンバイになっているか、またはリッスン

状態になっている場合のフェールオーバーのしきい値を設定できます。インターフェイスがアップまたはダウンするのを防ぐために下限および上限しきい値を設定できます。

VRRP は、vPC ピア デバイス上で実行されている場合に HSRP とよく似た動作を示します。VRRP は、HSRP を設定したのと同じ方法で設定してください。

プライマリ vPC ピア デバイスに障害が発生した場合は、セカンダリ vPC ピア デバイスにフェールオーバーされ、FHRP トラフィックはシームレスに流れ続けます。

バックアップルーティングパスとして機能するように2台のvPCピアデバイス間にルーティング隣接を設定することを推奨します。1台のvPCピアデバイスがレイヤ3アップリンクを失うと、そのvPCはルーテッドトラフィックを他のvPCピアデバイスにリダイレクトでき、そのアクティブレイヤ3アップリンクを活用できます。

次の方法で、バックアップのルーティングパス用のスイッチ間リンクを設定できます。

- 2台のvPCピアデバイス間でレイヤ3リンクを作成します。
- 専用のVLANインターフェイスを持つ非VPC VLAN トランクを使用します。
- 専用のVLANインターフェイスを持つvPCピアリンクを使用します。

vPC 環境での HSRP の焼き付け MAC アドレス オプション (use-bia) の設定、および任意の FHRP プロトコルのための仮想 MAC アドレスの手動での設定は、推奨できません。これらの設定は、vPC ロード バランシングに不利な影響を与えるためです。HSRP use-bia オプションは、vPC ではサポートされていません。カスタム MAC アドレスを設定する際には、両方の vPC ピア デバイスに同じ MAC アドレスを設定する必要があります。

delay restore コマンドを使用すればコマンドを使用して、ピアの隣接が形成され、VLAN インターフェイスがバックアップされるまで、vPC+ の回復を遅らせるようにリストア タイマーを設定します。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。**delay restore** コマンドを使用して、この機能を設定します。

復元した vPC ピア デバイス上の VLAN インターフェイスが起動するのを遅延するには、**interfaces-vlan** オプションを **delay restore** のオプション コマンドを使用します。

FHRP およびルーティングに関する詳細情報については、『[Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide](#)』を参照してください。

vPC ピアリンクのレイヤ3バックアップルートの構成

HSRP や PIM などのアプリケーションを使用するネットワークのレイヤ3にリンクするために、vPC ピア デバイス上の VLAN ネットワーク インターフェイスを使用できます。各ピア デバイス上で VLAN ネットワーク インターフェイスが設定されており、そのインターフェイスが各デバイス上で同じ VLAN に接続されていることを確認してください。また、各 VLAN インターフェイスが、同じ管理/動作モードになっていなければなりません。VLAN ネットワーク インターフェイスの設定の詳細については、「レイヤ3インターフェイスの設定」の章を参照してください。

vPC ピア リンクでフェールオーバーが発生すると、vPC ピア デバイス上の VLAN インターフェイスも影響を受けます。vPC ピア リンクに障害が発生すると、セカンダリ vPC ピア デバイス上の関連付けられている VLAN インターフェイスがシステムによって停止されます。

vPC ピア リンクに障害が発生したときに特定の VLAN インターフェイスが vPC セカンダリ デバイス上で停止しないようにできます。

CFSoE

Cisco Fabric Services over Ethernet (CFSoE) は、vPC ピア デバイスのアクションを同期化するために使用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。

CFSoE 転送は、各 VDC にローカルです。

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



- (注) **no cfs eth distribute** または **no cfs distribute** コマンドは入力しないでください。CFSoE for vPC 機能のための CFSoE をイネーブルにしなければなりません。vPC をイネーブルにして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。

引数を使用せずに **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。

CFS は、TCP/IP を介したデータも転送します。IP 経由の CFS の詳細については、『[Cisco Nexus 9000 Series NX-OS System Management Configuration Guide](#)』を参照してください。



- (注) CFS リージョンはサポートされていません。

vPC および孤立ポート

vPC 対応でないデバイスが各ピアに接続するとき、接続されたポートはvPCのメンバではないため、孤立ポートと称されます。一方のピアへのデバイスのリンクがアクティブ（フォワーディング）になり、他方のリンクは STP のためスタンバイ（ブロッキング）になります。

vPC ピア リンク障害またはリストアが発生すると、孤立ポートの接続は vPC 障害または復元プロセスにバインドされる可能性があります。たとえば、デバイスのアクティブな孤立ポートがセカンダリ vPC ピアに接続する場合、vPC ピア リンク障害が発生し、vPC ポートがセカンダリ ピアによって一時停止されると、そのデバイスはプライマリ ピアを経由する接続を失い

ます。セカンダリ ピアがアクティブな孤立ポートも一時停止した場合は、デバイスのスタンバイポートがアクティブになり、プライマリピアへの接続が提供され、接続が復元されます。セカンダリピアがvPCポートを一時停止するときに特定の孤立ポートがそのピアによって一時停止され、vPCが復元されるとそのポートが復元されるようにCLIで設定できます。

仮想化のサポート

1つのvPC内のすべてのポートが、同じVDC内にはなりません。このバージョンのソフトウェアは、VDCごとに1つのvPCドメインしかサポートしません。各VDCで1～4096の番号を使用してvPCに番号を付けることができます。

停電後のvPCリカバリ

データセンターが停止すると、vPCドメインの両方のvPCピアがリロードされます。場合によっては、1つのピアのみが復元される場合があります。機能するピアキープアライブまたはvPCピアリンクがないと、vPCは正常に機能することができません。vPCサービスが機能するピアのローカルポートのみを使用するようにする方法が利用可能です。

自動リカバリ

Cisco Nexus 9000 シリーズ デバイスは、そのピアがオンラインになるのに失敗した場合に、**auto-recovery** コマンドを使用して、vPC サービスを復元するように設定できます。この設定は、スタートアップ コンフィギュレーションに保存しなければなりません。リロード時に、vPC ピア リンクがダウンし、3 回連続してピア キープアライブ メッセージが失われた場合、セカンダリ デバイスはプライマリ STP ロールとプライマリ LACP ロールを引き継ぎます。ソフトウェアがvPCを初期化し、そのローカルポートを稼働させ始めます。ピアがないため、ローカルvPCポートの一貫性チェックはバイパスされます。デバイスは、自身をそのロールプライオリティに関係なくSTPプライマリに選出し、LACPポートロールのプライマリデバイスとしても機能します。

自動回復リロード遅延

vPCピアの自動回復は、**auto-recovery reload-delay** コマンドを使用して遅延させることができます。自動回復リロード遅延時間は、最初にアップしたピアで使用されます。**reload-delay time** コマンドは、両方のピアが回復するのを待機し、既存のロールを保持してから自動回復を開始するために使用します。デバイスは、回復したスイッチに対してプライマリロールを再開します。

リカバリ後のvPCピアロール

ピアデバイスのリロードが完了し、隣接が形成されたら、次のプロセスが発生します。

1. 最初のvPCピアがその現在のロールを維持して、その他のプロトコルへの任意の移行リセットを回避します。ピアが、他の可能なロールを受け入れます。
2. 隣接が形成されたら、整合性検査が実行され、適切なアクションが取られます。

高可用性

In-Service Software Upgrade (ISSU) では、最初の vPC デバイス上のソフトウェア リロード プロセスが、vPC 通信チャンネルを介した CFS メッセージングを使用して、その vPC ピア デバイスをロックします。1 度に 1 つのデバイスだけアップグレードできます。最初のデバイスは、そのアップグレードが完了したら、そのピアデバイスのロックを解除します。次に、2 つ目のデバイスが、最初のデバイスが行ったのと同じように最初のデバイスをロックして、アップグレードプロセスを実行します。アップグレード中は、2 つの vPC デバイスが一時的に異なるリリースの Cisco NX-OS を実行することになりますが、その下位互換性サポートにより、システムは正常に機能します。



(注) ハイアベイラビリティ機能の詳細については、『[Cisco Nexus 9000 Series NX-OS High Availability and Redundancy Guide](#)』を参照してください。

vPC フォークリフト アップグレードシナリオ

次の手順では、vPC ドメイン内の Cisco Nexus 9500 スイッチのペアを、同じタイプのラインカードを使用する、Cisco Nexus 9500 スイッチの別のペアに移行するためのシナリオについて説明します。このような移行の一般的な例としては、より多くのインターフェイスが必要な場合に、Cisco Nexus 9504 スイッチから Cisco Nexus 9508 スイッチに移行するケースがあります。次の移行シナリオはサポートされていません。

- 異なるラインカードセットを使用する Cisco Nexus 9500 スイッチへの移行。例えば、N9K-X94xx ラインカードを搭載した Cisco Nexus 9500 スイッチから、N9K-X97xx ラインカードを搭載した Cisco Nexus 9500 スイッチへの移行です。
- 異なる世代の Cisco Nexus 9300 スイッチ間の移行。例えば、Cisco Nexus N9K-C9372PX から Cisco Nexus N9K-93180YC-EX スイッチへの移行です。
- vPC ドメインでの、異なる世代の Cisco Nexus 9000 スイッチの使用はサポートされていません

vPCフォークリフトアップグレードの考慮事項：

- vPCロール選択とスティッキビット

2つのvPCシステムを結合してvPCドメインを形成する場合、優先順位によって、どのデバイスがvPCプライマリで、どのデバイスがvPCセカンダリであるかが決まります。プライマリデバイスがリロードされると、システムがオンラインに戻り、vPCセカンダリデバイス（現在動作可能なプライマリ）への接続が復元されます。セカンダリデバイス（動作プライマリ）の動作ロールは変更されません（不要な中断を回避するため）。この動作は、スティッキ情報がスタートアップコンフィギュレーションに保存されないスティッキビットで実現されます。この方法では、稼働中のデバイスがリロードされたデバイスに勝ちます。したがって、vPCプライマリはvPCの動作セカンダリになります。スティッキビット

は、vPCノードがvPCピアリンクおよびピアキープアライブダウンで起動し、自動回復期間後にプライマリになるときにも設定されます。

- vPC の遅延復元

遅延復元タイマーは、ピア隣接が既に確立されている場合、リロードの後で復元済みのvPCピアデバイスで起動するvPCの遅延のために使用されます。

復元したvPCピアデバイス上のVLANインターフェイスが起動するのを遅延するには、**interfaces-vlan** オプションを **delay restore** のオプションコマンドを使用します。

- vPC 自動リカバリ

両方のvPCピアスイッチがダウンしたデータセンターの停電中に、1つのスイッチのみが復元された場合、自動回復機能により、そのスイッチがプライマリスイッチの役割を引き継ぎ、自動回復期間後にvPCリンクが起動します。デフォルトの自動回復期間は240秒です。

次の例は、vPCピアノードNode1とNode2をNew_Node1とNew_Node2に置き換える移行シナリオです。

	移行ステップ	予想される動作	Node1 Configured role (Ex : role priority 100)	Node1 動作のロール	Node2 Configured role (Ex : role priority 200)	Node2 動作のロール
1	初期状態です。	トラフィックはvPCピア (Node1とNode2) の両方によって転送されます。 Node1はプライマリで、Node2はセカンダリです。	プライマリ	プライマリ ステイキービット : False	セカンダリ	セカンダリ ステイキービット : False
2	Node2 の交換 – Node2 のすべてのvPCとアップリンクをシャットダウンします。vPCピアリンクおよびvPCピアキープアライブは、管理上のアップ状態です。	プライマリvPCピアNode1でトラフィックが収束しました。	プライマリ	プライマリ ステイキービット : False	セカンダリ	セカンダリ ステイキービット : False

	移行ステップ	予想される動作	Node1 Configured role (Ex : role priority 100)	Node1 動作のロール	Node2 Configured role (Ex : role priority 200)	Node2 動作のロール
3	Node2を削除します。	Node1は引き続きトラフィックを転送します。	プライマリ	プライマリ スティッキービット : False	適用対象外	適用対象外
4	New_Node2を設定します。構成を管理アップ状態のvPCピアリンクおよびピアキーブアライブでスタートアップ構成にコピーします。 New_Node2の電源をオフにします。 すべての接続を確立します。 New_Node2の電源をオンにします。	New_Node2がセカンダリとして起動します。 Node1は引き続きプライマリです。 トラフィックはNode01で引き続き転送されます。	プライマリ	プライマリ スティッキービット : False	セカンダリ	セカンダリ スティッキービット : False
5	New_Node2のすべてのvPCとアップリンクポートを起動します。	トラフィックは、ノード1とNew_Node2の両方によって転送されます。	プライマリ	プライマリ スティッキービット : False	セカンダリ	セカンダリ スティッキービット : False
6	Node1の交換 : Node1でvPCとアップリンクをシャットダウンします。	トラフィックはNew_Node2に収束します。	プライマリ	プライマリ スティッキービット : False	セカンダリ	セカンダリ スティッキービット : False

	移行ステップ	予想される動作	Node1 Configured role (Ex : role priority 100)	Node1 動作のロール	Node2 Configured role (Ex : role priority 200)	Node2 動作のロール
7	Node1を削除します。	New_Node2がセカンダリになり、プライマリが動作し、スティッキービットがTrueに設定されます。	適用対象外	適用対象外	セカンダリ	プライマリ スティッキービット : True
8	New_Node1を設定します。スタートアップ実行をコピーします。 新しいNode1の電源をオフにします。すべての接続を確立します。New_Node1の電源をオンにします。	New_Node1がプライマリ、運用セカンダリとして起動します。	プライマリ	セカンダリ スティッキービット : False	セカンダリ	プライマリ スティッキービット : True
9	New_Node1のすべてのvPCとアップリンクポートを起動します。	トラフィックは、新しいノード1と新しいノード2の両方によって転送されます。	プライマリ	セカンダリ スティッキービット : False	セカンダリ	プライマリ スティッキービット : True



(注) 設定済みのセカンダリノードを動作可能なセカンダリとして設定し、設定済みのプライマリを動作可能なプライマリとして使用する場合は、移行の最後にNode2をリロードできます。これオプションであり、機能上の影響はありません。

注意事項と制約事項

vPC 設定時のガイドラインと制限事項は次のとおりです。

- 2つの Cisco Nexus 9300 シリーズ スイッチ間で vPC ドメインを形成する場合、サポートされる vPC ドメインを形成するには、両方のスイッチがまったく同じモデルである必要があ

ります。2つの Cisco Nexus 9500 シリーズ スイッチ間で vPC ドメインを形成する場合、両方のスイッチは、サポートされる vPC ドメインを形成するために、シャーシの同じスロットに挿入された同じモデルのラインカード、ファブリック モジュール、スーパーバイザ モジュール、およびシステム コントローラで構成されている必要があります。

- ピアキープアライブ リンクを設定し、システムが vPC ピア リンクを確立する前に、ピア間の隣接関係を形成する必要があります。
- 両方の vPC ピア デバイスを設定しなければなりません。設定が片方のデバイスから他方へ送信されることはありません。
- vPC に入れられるのは、レイヤ 2 ポート チャンネルだけです。
- vPC 内の LACP を使用するすべてのポート チャンネルを、アクティブモードのインターフェイスで設定することを推奨します。
- vPC ドメインに接続されているすべてのデバイスは、デュアルホームである必要があります。
- 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確認する必要があります。互換性の推奨については、「vPC インターフェイスの互換パラメータ」の項を参照してください。
- 既存のポート チャンネルで 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。
- CFS リージョンはサポートされていません。
- vPC ピアリンクでは、デフォルトで MTU が 9216 に設定されています。
- STP ポート コストは、vPC 環境で 200 に固定されています。
- マルチレイヤ (バックツーバック) vPC を設定するには、それぞれの vPC に一意の vPC ドメイン ID を割り当てる必要があります。
- vPC がダウンし、トラフィックが vPC ピア リンクを通過する必要があるときに、増加するトラフィックに対応するためのベスト プラクティスは、vPC ピア リンクのラインカードを横断して複数の高帯域幅インターフェイス (Cisco Nexus 9000 スイッチの 40G インターフェイスなど) を使用することです。
- 次の場合、L3 リンクとバックツーバック vPC でマルチキャストストリームが重複する可能性があります。
 - SVI は、バックツーバック vPC の一部である 4 つすべてのスイッチで設定されます。
 - vPC の一部である 4 つのスイッチを接続する追加の L3 リンクがあります。
 - PIM は、すべての SVI およびスイッチ間の L3 リンクでイネーブルです。

ストリームの重複を防ぐには、vPC スイッチペアの 1 つから SVI または PIM 設定を削除します。

- Cisco NX-OS リリース 7.0(3)I5(1) 以降では、vPC を介したレイヤ 3 は、レイヤ 3 ユニキャスト通信の Cisco Nexus 9000 シリーズ スイッチでのみサポートされます。vPC 上のレイヤ 3 は、レイヤ 3 マルチキャストトラフィックではサポートされません。詳細については、「レイヤ 3 および vPC 設定のベストプラクティス」セクションを参照してください。
- デフォルトでは、レイヤ 3 vPC は、ピア vPC ノード宛てのすべてのパケット (TTL=1) を転送します。OSPF/BGP は、この転送が原因でフラップする可能性があります。スイッチハードウェアを前進させるには、ing-sup TCAM をサイズ 768 に切り分ける必要があります。TCAM カービング後にスイッチをリロードしてください。次に例を示します。

```
show hardware access-list tcam region | gr ing-sup
Ingress SUP [ing-sup] size = 768
```

- Cisco Nexus 9000 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。
- vPC ピアは同じ Cisco NX-OS リリースを実行する必要があります。ソフトウェアアップグレード中は、最初にプライマリ vPC ピアをアップグレードする必要があります。
- 無停止アップグレードを実行する前に、vPC の両方のピアが同じモード (通常 ISSU モードまたは拡張 ISSU モード) であることを確認します。



(注) 拡張 ISSU モード (ブートモード lxc) が設定されたスイッチと非拡張 ISSU モードスイッチ間の vPC ピアリングはサポートされていません。

- **vpc orphan-ports suspend** コマンドは、vPC VLAN を持つインターフェイスでを使用することを推奨します。コマンドは、非 vPC VLAN のポートおよびレイヤ 3 ポートにも適用可能です。
- このソフトウェアでは、vPC 上での BIDR PIM はサポートされていません。
- vPC 環境での DHCP スヌーピング、DAI、IPSG はサポートされていません。DHCP リレーはサポートされています。
- 2 つの Cisco Nexus 9000 シリーズ スイッチで **vpc domain** 構成モードでピアスイッチ機能を設定すると、vPC ピアリンクで有効になっていない VLAN のスパニングツリールートも変更されます。両方のスイッチは、ブリッジアドレスとして 1 つの MAC アドレスを持つ 1 つのシステムとして機能します。これは、non-vPC mst-instance または VLAN でも true です。したがって、2 つのスイッチ間の非 vPC ピアリンクはバックアップリンクとしてブロックされます。これは予期された動作です。
- ダブルサイド vPC 上のすべてのノードで同じ Hot Standby Router Protocol (HSRP) /Virtual Router Redundancy Protocol (VRRP) グループを持つことは、Cisco NX-OS 7.0(3)I2(1) 以降のリリースでサポートされています。
- スパインノードのペアから Cisco Nexus 9000 デバイスのペアに移行する場合、Cisco Nexus 9000 vPC ピアがアクティブ/スタンバイ状態になるように HSRP プライオリティを設定する

必要があります。HSRP 状態の Cisco Nexus 9000 vPC をアクティブ/リッスン状態またはスタンバイ/リッスン状態にすることはサポートされていません (7.0(I2(2) 以降)。

- NX-OS リリース 7.0(3)I2(2) 以降では、以前に **ip pim pre-build-spt** コマンドによって提供されていた動作がデフォルトで自動的に有効になっており、無効にはできません。
- Cisco NX-OS リリース NX-OS 7.0(3)I2(2) 以降では、個別の状態で作動する vPC ポートチャネルメンバー リンクが、VLAN の不整合の検査時にフラップされます。サーバのプロビジョニング時にリンクがフラップされることを回避するには、**no graceful consistency-check** コマンドによって vPC グレースフル整合性検査を無効にします。
- vPC を使用する場合は、FHRP (HSRP、VRRP) にデフォルトのタイマーを使用し、PIM 設定を行うことを推奨します。アグレッシブタイマーを vPC 設定で使用すると、コンバージェンス時間のメリットがありません。
- vPC 環境で open shortest path first (OSPF) を設定する場合は、コア スイッチ上でルータ コンフィギュレーション モードで次のタイマー コマンドを使用することにより、vPC ピア リンクがシャットダウンしたときに OSPF の高速コンバージェンスを実現します。

```
switch (config-router)# timers throttle spf 1 50 50
switch (config-router)# timers lsa-arrival 10
```

OSPF の詳細については、「Cisco Nexus 9000 シリーズ NX-OS ユニキャストルーティング設定ガイド」を参照してください。

- VRRP/HSRP の BFD は、vPC 環境ではサポートされていません。
- Cisco Nexus 9000 リリース 7.0(3)I7(1) 以降では、vPC STP ヒットレス ロール変更機能がサポートされています。
- vPC ロール変更はいずれかのピア デバイスで実行できます。
- 元のセカンダリ デバイスに高プライオリティ値がある場合、元のプライオリティ デバイスはロール スワッピングは実行できません。vPC デバイスのいずれかでロールプライオリティを変更すると、元のセカンダリ デバイスの値は元のプライマリ デバイスの値よりも低くなります。デバイスの既存のロールを確認するには、ローカルおよびピアスイッチで **show vpc role** コマンドを使用します。
- vPC ドメインで vPC ヒットレス ロール変更機能を設定する前に、既存の設定済みロールプライオリティをチェックし、**peer-switch** コマンドを有効にします。これにより、両方の vPC ピアが同じ STP プライオリティになり、ロールの変更を発行する前にピアが稼働可能になることが保証されます。**peer-switch** コマンドを有効にできない場合、コンバージェンスの問題が発生する可能性があります。**show spanning-tree summary | grep peer** コマンドを使用して、ピア vPC スイッチが動作しているかどうかを確認します。
- Cisco NX-OS リリース 7.0(3)I5(2) 以降では、FEX-AA (デュアルホーム FEX) および FEX-ST (FEX ストレートスルー) トポロジ (FEX-AA および FEX-ST) がサポートされています。次の親スイッチの組み合わせはサポートされていません。
 - Cisco Nexus 9300-EX および 9300 スイッチ。

- Cisco Nexus 9300 および 9500 スイッチ。
- Cisco Nexus 9300-EX および 9500 スイッチ。
- 第 1 世代の Broadcom ベースの Nexus 9300 シリーズ スイッチおよび Nexus 9500 シリーズ ラインカードは、vPC コンバージェンス TCAM リージョンが割り当てられている間に、出力インターフェイスが vPC ピア リンクである ip ネクスト ホップ ステートメントを設定しているポリシー ベースのルーティング ルート マップをサポートしていません。この制限は、This limitation does not apply to cloud scale based EX/FX/FX2 ラインカードを搭載した Nexus 9000 シリーズ デバイスや、9700-EX/FX ラインカードを搭載した Nexus 9500 プラットフォーム スイッチなど Nexus 9000 シリーズ デバイスに基づきクラウドスケールには適用されません。
- **show** コマンドで **internal** キーワードを指定することはサポートされていません
- vPC を介したレイヤ 3 は、レイヤ 3 ユニキャスト通信の Cisco Nexus 9000 シリーズ スイッチでのみサポートされます。vPC 上のレイヤ 3 は、レイヤ 3 マルチキャスト トラフィックではサポートされません。詳細については、「レイヤ 3 および vPC 設定のベストプラクティス」を参照してください。
- vPC ピアの IP を宛先としたレイヤ 3 ピア ルータ および TTL=1 パケットのデフォルトの動作では、パケットを CPU にパントし、ソフトウェアを vPC ピアに転送します。これは、クラウドスケールベースの EOR スイッチに適用されます。
- Cisco NX-OS リリース 7.0(3)I7(9) および Cisco NX-OS リリース 9.3(5)以降、クラウドスケールベースの TOR スイッチは、ハードウェア/データプレーンの vPC ピア宛での TTL=1 パケットを転送できます。機能のシームレスな動作のために、これらのリリースまたはそれ以降のリリースのいずれかを使用することを推奨します。
 - Cisco NX-OS リリース 9.3(4)にはこのデフォルトの動作がありますが、クラウドスケールベースの TOR スイッチに対する vPC ピアへのパケットのハードウェアリダイレクトには TCAM 再分割オプションを使用できます。これには、ing-sup リージョンに少なくとも 768 スペースを割り当てる必要があり、リロードが必要であり、操作上のオーバーヘッドがあります。
- STP プライオリティの vPC ペアを設定する場合は、両方の vPC ピアを STP ルートとして機能させるために、両方の vPC ピア スイッチに同じプライオリティ レベルを設定する必要があります。
- クラウドスケール ASIC ベースのスイッチでレイヤ 3 ピア ルータを設定すると、ユニキャスト パケットで次の動作が発生することがあります。
 - vPC ピア ノード宛での TTL=0 のユニキャスト パケットは、ピアに転送されます。
 - TTL=0 のユニキャスト パケットはピアによってドロップされず、代わりに SUP にパントされます。
 - vPC ピア ノード宛での TTL=1 および TTL=0 のユニキャスト パケットは、ソフトウェア転送およびハードウェア転送が可能です。そのため、ピア ノードで重複パケットが確認されます。

- vPC ポート チャンネルの LACP 設定は、vPC ピア リンク上の両方の Cisco Nexus スイッチで一貫している必要があります。
- VPCの両方のピアが同じモード（通常モードまたは拡張モード）であることを確認してから、無停止アップグレードを実行してください。



(注) 拡張 ISSU モード（ブートモード `lxc`）が設定されたスイッチと非拡張 ISSU モードスイッチ間の vPC ピアリングはサポートされていません。

- キーワードが付いている **show** コマンドはサポートされていません。 **internal**
- Cisco Nexus 9000 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 NX-OS リリース 9.2(1) 以降の Cisco Nexus 9000 スイッチでは、**show vpc consistency-checker** コマンドは使用できません。
- Cisco NX-OS リリース 9.2(1) 以降の Cisco Nexus 9500-R プラットフォーム スイッチでは、**delay restore interface-bridge-domain** および **peer-gateway exclude-bridge-domain** コマンドは使用できません。
- vPC ピアは同じ Cisco NX-OS リリースを実行する必要があります。ソフトウェアのアップグレード中は、必ずプライマリ vPC ピアをアップグレードしてください。
- 1 つの vPC のすべてのポートが、同じ VDC 内になくてもなりません。
- vPC を設定するには、まず vPC をイネーブルにする必要があります。
- システムが vPC ピア リンクを形成する前に、ピア キープアライブ リンクとメッセージを設定する必要があります。
- vPC に入れられるのは、レイヤ 2 ポート チャンネルだけです。
- 両方の vPC ピア デバイスを設定しなければなりません。設定が片方のデバイスから他方へ送信されることはありません。
- マルチレイヤ（バックツーバック）vPC を設定するには、それぞれの vPC に一意の vPC ドメイン ID を割り当てる必要があります。
- 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。互換性の推奨については、「vPC インターフェイスの互換パラメータ」の項を参照してください。
- 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 上での BIDR PIM はサポートされていません。
- CFS リージョンはサポートされていません。

- 2つの Cisco Nexus 9000 シリーズ スイッチで **vpc domain** 構成モードの下にある **peer-switch** 機能を設定すると、vPC ピアリンクで有効になっていない VLAN に対してもスパンニングツリー ルートが変更されます。両方のスイッチは、ブリッジアドレスとして 1つの MAC アドレスを持つ 1つのシステムとして機能します。これは、**non-vPC mst-instance** または **VLAN** でも **true** です。したがって、2つのスイッチ間の非 vPC ピア リンクはバックアップリンクとしてブロックされます。これは予期された動作です。
- vPC 内の LACP を使用するすべてのポートチャネルを、アクティブモードのインターフェイスで設定することを推奨します。
- バックツーバックのマルチレイヤ vPC トポロジでは、それぞれの vPC に一意のドメイン ID が必要です。
- ダブルサイド vPC 上のすべてのノードで同じ Hot Standby Router Protocol (HSRP) /Virtual Router Redundancy Protocol (VRRP) グループを持つことはサポートされています。
- スパイン ノードのペアから Cisco Nexus 9000 デバイスへ移行するとき、HSRP プライオリティが設定される必要があります。これにより Cisco Nexus 9000 vPC ピアはアクティブ/スタンバイ状態になります。HSRP 状態をアクティブ/リッスン状態、またはスタンバイ/リッスン状態にすることは Cisco Nexus 9000 vPC ピアでサポートされていません。
- vPC を使用する場合は、FHRP (HSRP、VRRP、) にデフォルトのタイマーを使用し、PIM 設定を行うことを推奨します。アグレッシブタイマーを vPC 設定で使用すると、コンバージェンス時間のメリットがありません。
- vPC 環境で **open shortest path first (OSPF)** を設定する場合は、コア スイッチ上でルータ コンフィギュレーション モードで次のタイマー コマンドを使用することにより、vPC ピア リンクがシャットダウンしたときに OSPF の高速コンバージェンスを実現します。

```
switch (config-router)# timers throttle spf 1 50 50
switch (config-router)# timers lsa-arrival 10
```

OSPF に関する詳細については、『*Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide*』を参照してください。

- VRRP/HSRP の BFD は、vPC 環境ではサポートされていません。
- STP ポート コストは、vPC 環境で 200 に固定されています。
- ジャンボ フレームは、vPC ピア リンクではデフォルトで有効に設定されます。
- vPC がダウンし、トラフィックが vPC ピア リンクを通過する必要があるときに、増加するトラフィックに対応するためはのベスト プラクティス、vPC ピア リンクのラインカードを横断して複数の高帯域幅インターフェイス (Cisco Nexus 9000 の 40G インターフェイスなど) を使用することです。
- この項で説明している **vpc orphan-ports suspend** コマンドは、非 vPC VLAN のポートおよびレイヤ 3 ポートにも適用可能です。ただし、VPC VLAN のポートで使用することをお勧めします。

- FEX-AA (デュアルホーム FEX) および FEX-ST (FEX ストレート) トポロジ (FEX-AA および FEX-ST) がサポートされています。次の混合は、親スイッチとしてサポートされていません。
 - Cisco Nexus 9300-EX および 9300 スイッチ
 - Cisco Nexus 9300 および 9500 スイッチ
 - Cisco Nexus 9300-EX および 9500 スイッチ

- 以前に `ip pim pre-build-spt` コマンドによって提供されていた動作がデフォルトで自動的に有効になっており、無効にはできません。
- 個別の状態で作動する vPC ポートチャネル メンバー リンクが、VLAN の不整合の検査時にフラップされます。サーバのプロビジョニング時にリンクがフラップされることを回避するには、**no graceful consistency-check** コマンドによって vPC グレースフル整合性検査を無効にします。

次の例では、vPC グレースフル整合性チェックを無効にします。

```
switch# conf t
Enter configuration commands, one per line. End with CNTL/Z.

switch(config)# vpc domain 1
switch(config-vpc-domain)# no graceful consistency-check
```

- vPC STP ヒットレス ロール変更機能がサポートされています。
- vPC ロール変更はいずれかのピア デバイスで実行できます。
- 元のセカンダリ デバイスに高プライオリティ値がある場合、元のプライオリティ デバイスはロール スワッピングは実行できません。vPC デバイスのいずれかでロール プライオリティを変更すると、元のセカンダリ デバイスの値は元のプライマリ デバイスの値よりも低くなります。デバイスの既存のロールを確認するには、ローカルおよびピアスイッチで `show vpc role` コマンドを使用します。
- サポートされている vPC ドメインを形成するには、次の点に注意してください。
 - Cisco Nexus 9300 シリーズ スイッチの場合、両方のスイッチがまったく同じモデルである必要があります。
 - 2つの Cisco Nexus 9500 シリーズ スイッチ間で vPC ドメインを形成する場合、両方のスイッチは、サポートされる vPC ドメインを形成するために、シャーシの同じスロットに挿入された同じモデルのラインカード、ファブリック モジュール、スーパーバイザ モジュール、およびシステム コントローラで構成されている必要があります。
- vPC ヒットレス ロールの変更機能を設定する前に、必ず、既存の設定されたロール プライオリティをチェックしてください
- vPC ドメインで `peer-switch` コマンドを有効にします。これにより、両方の vPC ピアが同じ STP プライオリティになり、ロールの変更を発行する前にピアが稼働可能になることが保証されます。peer-switch コマンドを有効にできない場合、コンバージェンスの問題が発

生ずる可能性があります。 **show spanning-tree summary | grep peer** コマンドを使用して、ピア vPC スイッチが操作可能かどうか確認します。

- vPC ドメインに接続されているすべてのデバイスは、デュアルホームである必要があります。
- 第 1 世代の Broadcom ベースの Nexus 9300 シリーズ スイッチおよび Nexus 9500 シリーズ ライン カードは、vPC コンバージェンス TCAM リージョンが割り当てられている間に、出カインターフェイスが vPC ピア リンクである ip ネクスト ホップ ステートメントを設定しているポリシー ベースのルーティング ルート マップをサポートしていません。この制限は、**This limitation does not apply to cloud scale based EX/FX/FX2** ラインカードを搭載した Nexus 9000 シリーズ デバイスや、9700-EX/FX ラインカードを搭載した Nexus 9500 プラットフォーム スイッチなど Nexus 9000 シリーズ デバイスに基づきクラウドスケールには適用されません。
- **lACP suspend-individual** および **lACP mode delay** を実行して、PXE で vPC 経由で Cisco Nexus 9000 スイッチに接続しているサーバを起動する必要があります。

レイヤ 3 および vPC 設定のベスト プラクティス

ここでは、vPC でレイヤ 3 を使用し、設定するためのベスト プラクティスについて説明します。

レイヤ 3 および vPC 設定の概要

レイヤ 3 デバイスが vPC を介して vPC ドメインに接続されている場合、次のビューがあります。

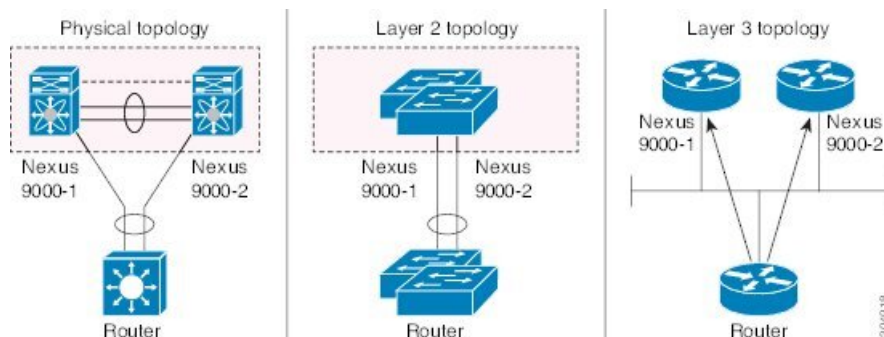
- レイヤ 2 では、レイヤ 3 デバイスは vPC ピア デバイスによって提供される一意のレイヤ 2 スイッチを認識します。
- レイヤ 3 では、レイヤ 3 デバイスは 2 台の異なるレイヤ 3 デバイス (vPC ピア デバイスごとに 1 台) を認識します。

vPC はレイヤ 2 仮想化テクノロジーであるため、レイヤ 2 では、両方の vPC ピア デバイスがネットワークの他の部分に対して固有の論理デバイスとして表示されます。

レイヤ 3 には仮想化テクノロジーがないため、各 vPC ピア デバイスは、ネットワークの他の部分では別個のレイヤ 3 デバイスと見なされます。

次の図は、vPC を使用した 2 つの異なるレイヤ 2 およびレイヤ 3 ビューを示しています。

図 17: vPCピアデバイスのさまざまなビュー

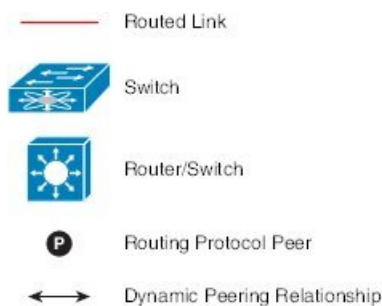


レイヤ 3 および vPC のサポートされるトポロジ

ここでは、レイヤ 3 および vPC のネットワーク トポロジの例を示します。

レイヤ 3 と vPC のインタラクションには 2 つのアプローチがあります。1 つ目は、専用のレイヤ 3 リンクを使用してレイヤ 3 デバイスを各 vPC ピア デバイスに接続する方法です。2 つ目は、vPC 接続で伝送される専用 VLAN 上で、レイヤ 3 デバイスが各 vPC ピア デバイスで定義された SVI とピアリングできるようにすることです。次のセクションでは、次の図の凡例に記載されている要素を利用して、サポートされているすべてのトポロジについて説明します。

図 18: 凡例



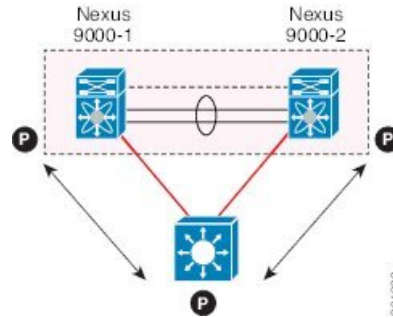
レイヤ 3 リンクを使用した外部ルータとのピアリング

この例は、レイヤ 3 リンクを使用してレイヤ 3 デバイスを vPC ドメインの一部である Cisco Nexus 9000 スイッチに接続するトポロジを示しています。



(注) この方法で 2 つのエンティティを相互接続すると、レイヤ 3 ユニキャストおよびマルチキャスト通信をサポートできます。

図 19: レイヤ 3 リンクを使用した外部ルータとのピアリング



レイヤ 3 デバイスは、両方の vPC ピア デバイスとのレイヤ 3 ルーティングプロトコルの隣接関係を開始できます。

1 つまたは複数のレイヤ 3 リンクを、各 vPC ピア デバイスにレイヤ 3 デバイスを接続するために使用できます。Cisco Nexus 9000 シリーズ デバイスは、プレフィックスごとに最大 16 のハードウェア ロードシェアリングパスでレイヤ 3 Equal Cost Multipathing (ECMP) をサポートします。vPC ピア デバイスからレイヤ 3 デバイスへのトラフィックを、2 台のデバイスを相互接続するすべてのレイヤ 3 リンクにロードバランスできます。

レイヤ 3 デバイスでレイヤ 3 ECMP を使用すると、このデバイスから vPC ドメインへのすべてのレイヤ 3 リンクを効果的に使用できます。レイヤ 3 デバイスから vPC ドメインへのトラフィックを、2 つのエンティティを相互接続するすべてのレイヤ 3 リンクにロードバランスできます。

レイヤ 3 デバイスをレイヤ 3 リンクを使用している vPC ドメインに接続する際は、次の注意事項に従ってください。

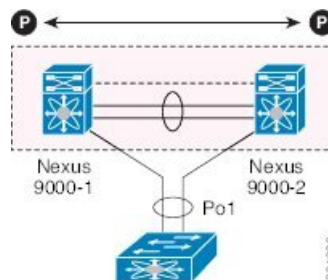
- レイヤ 3 デバイスを vPC ドメインに接続するには、独立したレイヤ 3 リンクを使用します。各リンクはポイントツーポイントレイヤ 3 接続を表し、小さな IP サブネット (/30 または /31) から取得された IP アドレスが割り当てられます。
- 複数の VRF にレイヤ 3 ピアリングが必要な場合は、それぞれが個別の VRF にマッピングされる複数のサブインターフェイスを定義することを推奨します。

バックアップルーティングパス用 vPC デバイス間のピアリング

この例では、レイヤ 3 バックアップルーテッドパスを持つ 2 つの vPC ピア デバイス間のピアリングを示します。vPC ピア デバイス 1 または vPC ピア デバイス 2 のレイヤ 3 アップリンクに障害が発生した場合、2 つのピア デバイス間のパスを使用して、レイヤ 3 アップリンクがアップ状態のスイッチにトラフィックがリダイレクトされます。

レイヤ 3 バックアップルーティングパスは、vPC ピアリンク上で専用インターフェイス VLAN (SVI など) を使用するか、2 つの vPC ピア デバイス間で専用のレイヤ 2 またはレイヤ 3 リンクを使用して実装できます。

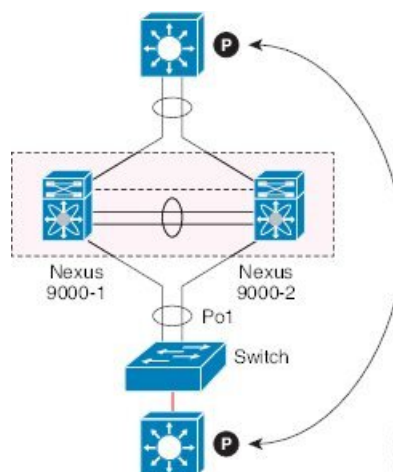
図 20: バックアップルーティングパス用 vPC デバイス間のピアリング



ルータ間の直接レイヤ3 ピアリング

このシナリオでは、vPC ドメインの Nexus 9000 デバイスの部分が単にレイヤ2 中継パスとして使用され、接続されたルータがレイヤ3 ピアリングおよび通信を確立できるようにします。

図 21: ルータ間ピアリング



レイヤ3 デバイスは、次の2つの方法で相互のピアとなることが出来ます。また、ピアリングの方法は、このロールにどのようなデバイスが展開されるかによっても変わります。

- 中間の Cisco Nexus 9000 vPC ピアスイッチを介してレイヤ3 デバイス間で拡張される VLAN の VLAN ネットワーク インターフェイス (SVI) を定義します。
- 各レイヤ3 デバイスでレイヤ3 ポートチャンネルインターフェイスを定義し、ポイントツーポイントレイヤ3 ピアリングを確立します。

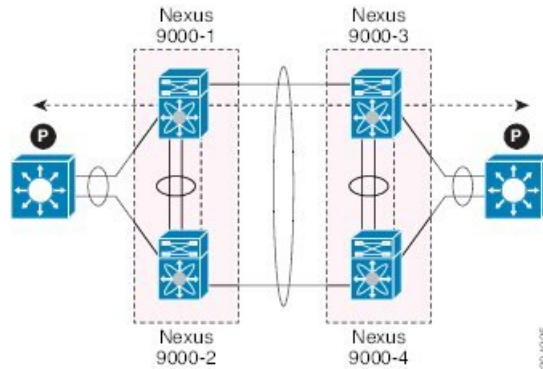


(注) 複数の VRF に対してレイヤ3 ピアリングを確立する必要がある展開の場合、最初の方法では、VRF ごとに VLAN (および SVI) のレイヤ3 デバイスで定義する必要があります。2 番目の方法では、VRF ごとにレイヤ3 ポートチャンネルサブインターフェイスを作成できます。

トランジットスイッチとして vPC デバイスを使用した 2 ルータの間のピアリング

この例は、「ルータ間のピアリング」トポロジと似ています。この場合も、同じ vPC ドメインの一部である Cisco Nexus 9000 デバイスは、レイヤ 2 中継パスとしてのみ使用されます。ここでの違いは、Cisco Nexus 9000 スイッチのペアが 2 つあることです。vPC 接続を使用してレイヤ 3 デバイスに接続されている各スイッチは、それらの間のバックツーバック vPC 接続も確立します。異なる点は、vPC ドメインがレイヤ 2 中継パスとしてのみ使用されていることです。

図 22: トランジットスイッチとして vPC デバイスを使用した 2 ルータの間のピアリング



このトポロジは、直接リンク（ダークファイバまたは DWDM 回線）で相互接続された個別のデータセンター間の接続を確立する場合によく使用されます。この場合、Cisco Nexus 9000 スイッチの 2 つのペアはレイヤ 2 拡張サービスのみを提供し、レイヤ 3 デバイスがレイヤ 3 で相互にピアリングできるようにします。

パラレル相互接続ルーテッドポート上の外部ルーターとのピアリング

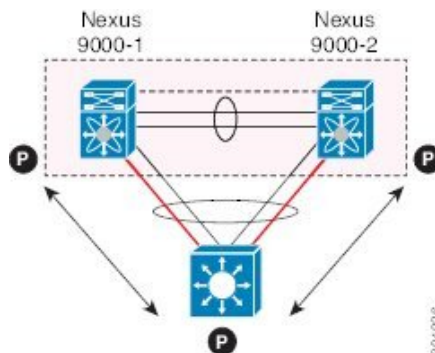
次の図に示すように、ルーテッドトラフィックとブリッジトラフィックの両方が必要な場合は、ルーテッドトラフィックに個別のレイヤ 3 リンクを使用し、ブリッジトラフィックに個別のレイヤ 2 ポートチャネルを使用します。

レイヤ 2 リンクは、ブリッジドトラフィック（同じ VLAN に保持されるトラフィック）または VLAN 間トラフィック（vPC ドメインがインターフェイス VLAN と関連 HSRP コンフィギュレーションをホストすることが前提）に使用されます。

レイヤ 3 リンクは、各 vPC ピアデバイスとのルーティングプロトコルピアリング隣接に使用されます。

このトポロジの目的は、レイヤ 3 デバイスを通る特定のトラフィックを引き付けることです。レイヤ 3 リンクは、レイヤ 3 デバイスから vPC ドメインにルーティングされたトラフィックを伝送するためにも使用されます。

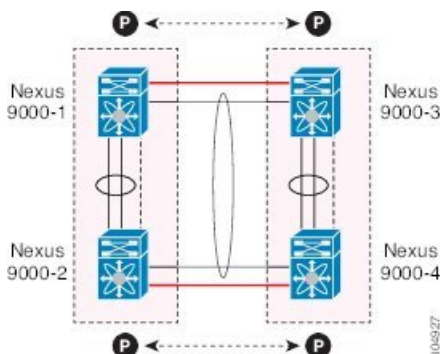
図 23: パラレル相互接続ルーテッドポート上の 外部ルーターとのピアリング



パラレル相互接続ルーテッドポート上の vPC スイッチペア間のピアリング

前の項（中継スイッチとして vPC デバイスを使用した 2 台のルーター間のピアリング）で示したものに代わる設計では、レイヤ 2 とレイヤ 3 の両方の拡張サービスを提供するために、各データセンターに導入された 2 ペアの Cisco Nexus 9000 スイッチを使用します。ルーティングプロトコルピアリング隣接を 2 ペアの Cisco Nexus 9000 デバイス間で確立する必要がある場合、ベストプラクティスは、次の例に示すように 2 サイト間に専用のレイヤ 3 リンクを追加することです。

図 24: パラレル相互接続ルーテッドポートでの vPC 相互接続を介したピアリング



2 つのデータセンター間のバックツーバック vPC 接続は、ブリッジドトラフィックまたは VLAN 間トラフィックを伝送し、専用レイヤ 3 リンクは 2 サイト間でルーテッドトラフィックを伝送します。

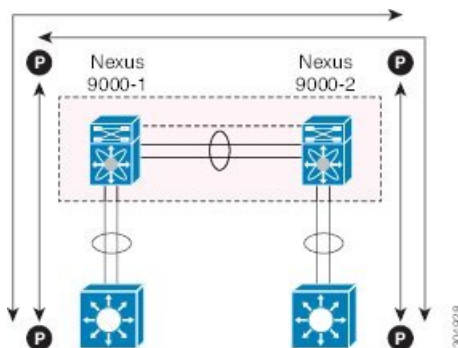
非 vPC VLAN を使用する PC 相互接続および専用スイッチ間リンクを介したピアリング

この例は、レイヤ 3 デバイスが vPC ドメインにシングル接続されている場合に、専用スイッチ間リンクで非 vPC VLAN を使用して、レイヤ 3 デバイスと各 vPC ピア デバイスとの間でルーティングプロトコルピアリング隣接を確立できることを示しています。ただし、非 vPC VLAN は、vPC VLAN とは異なるスタティック MAC を使用するよう設定する必要があります。



- (注) この目的のために vPC VLAN (および vPC ピア リンク) を設定することはサポートされていません。

図 25: 非 vPC VLAN を使用する PC 相互接続および専用スイッチ間リンクを介したピアリング



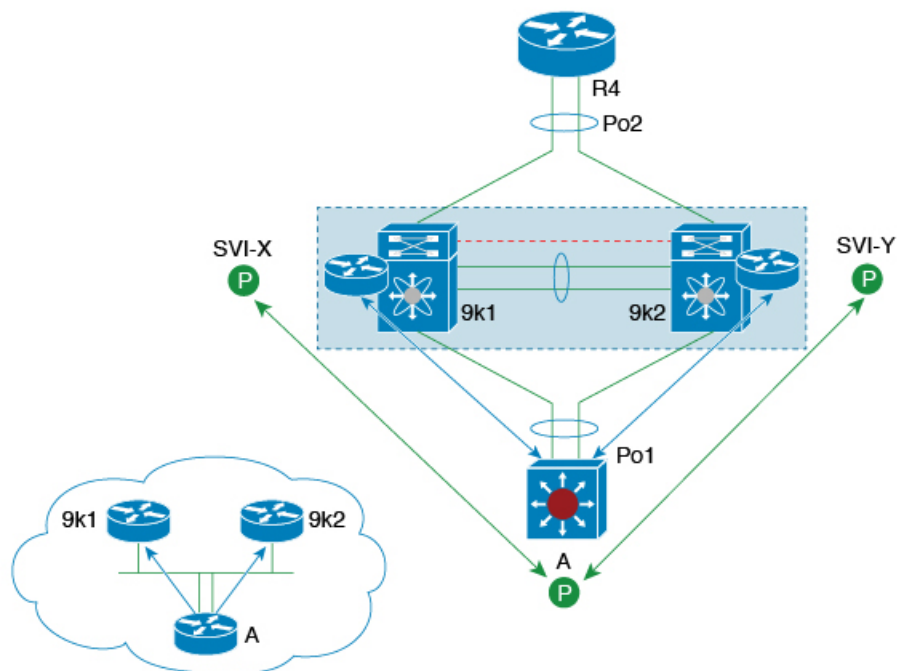
vPC 接続を介した直接ピアリング

Cisco NX-OS リリース 7.0(3)I5(1) 以降では、レイヤ 3 ルータと Cisco Nexus 9000 vPC スイッチのペア間にレイヤ 3 ピアリングを確立するための代替方法が導入されています。



- (注) vPC 接続を介した直接ピアリングは、レイヤ 3 ユニキャスト通信でのみサポートされ、レイヤ 3 マルチキャストトラフィックではサポートされません。レイヤ 3 マルチキャストが必要な場合は、専用のレイヤ 3 リンクでピアリングを確立する必要があります。

図 26: サポート : ルータが両方の vPC ピアとピアリングする vPC 相互接続を介するピアリング。

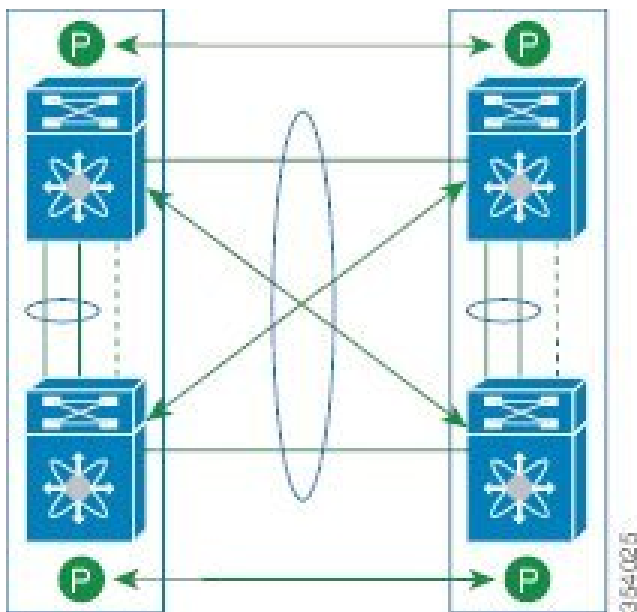


501182

このシナリオでは、同じ vPC ドメインの一部である外部ルータと Cisco Nexus 9000 スイッチ間のレイヤ 3 ピアリングは、vPC 接続で伝送される VLAN 上で直接確立されます。この場合の外部ルータは、各 vPC デバイスで定義された SVI インターフェイスとピアリングします。前の図 12 のシナリオでは、外部ルータは SVI またはレイヤ 3 ポートチャネルを使用して vPC デバイスとピアリングできます（複数の SVI またはポートチャネルサブインターフェイスをマルチ VRF 展開に使用できます）。

この展開モデルでは、vPC ドメインの一部として **layer3 peer-router** コマンドを設定する必要があります。vPC スイッチの 2 つの個別のペア間で確立された vPC バックツーバック接続でレイヤ 2 およびレイヤ 3 接続を確立するために、同じアプローチを採用できます。

図 27: サポート : 各 Nexus デバイスが 2 つの vPC ピアとピアリングする vPC 相互接続を介したピアリング。



この展開モデルでは、4 つの Cisco Nexus 9000 スイッチすべてに同じ VLAN 内の SVI インターフェイスが設定され、これらの中でルーティング ピアリングと接続が確立されます。

レイヤ 3 vPC 経路の設定

始める前に

ピア ゲートウェイ機能が両方のピアで有効かつ設定済みで、両方のピアが vPC 経路のレイヤ 3 に対応したイメージを実行していることを確認します。ピアゲートウェイ機能を有効にせずに **layer3 peer-router** コマンドを入力した場合は、ピアゲートウェイ機能を有効にするように勧める syslog メッセージが表示されます。

vPC ピアリンクがアップしてい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)#**layer3 peer-router**
4. switch(config-vpc-domain)# **exit**
5. (任意) switch# **show vpc brief**
6. (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# configure terminal 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# vpc domain domain-id 例： switch(config)# vpc domain 5 switch(config-vpc-domain)#	vPC ドメインがまだ存在しなかった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。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	switch(config-vpc-domain)# layer3 peer-router	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。このコマンドをピアのうち1つでのみ設定するか、1つのピアで無効にすると、レイヤ3 ピアルータの動作状態が無効になります。動作状態に変更があると、通知が表示されます。
ステップ 4	switch(config-vpc-domain)# exit	vpc-domain 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	(任意) switch# show vpc brief	各 vPC ドメインに関する要約情報を表示します。
ステップ 6	(任意) switch# copy running-config startup-config	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、vPC 機能経由でレイヤ 3 を設定する例を示します。

```
switch# configure terminal
switch(config)# vpc domain 5
switch(config-vpc-domain)# layer3 peer-router

switch(config-vpc-domain)# exit

switch(config)#
```

次に、vPC 経由でレイヤ 3 機能が設定されているかどうかを確認する例を示します。
動作レイヤ 3 ピアは、vPC 経由のレイヤ 3 の動作状態の設定に応じて有効または無効になります。

```
switch# show vpc brief

vPC domain id : 5
```

```

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 : Enabled
Peer gateway excluded VLANs : -
Dual-active excluded VLANs : -
Graceful Consistency Check : Enabled
Auto-recovery status : Enabled (timeout = 240 seconds)
Operational Layer3 Peer : Enabled

```

デフォルト設定

次の表は、vPC パラメータのデフォルト設定をまとめたものです。

表 16: 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



- (注) vPC ピアリンクの両側のデバイス両方でこれらの手順を使用する必要があります。両方の vPC ピア デバイスをこの手順で設定します。

ここでは、コマンドラインインターフェイス (CLI) を使用して vPC を設定する方法を説明します。



- (注) Cisco IOS の CLI に慣れている場合、この機能に対応する Cisco NX-OS コマンドは通常使用する Cisco IOS コマンドと異なる場合がありますので注意してください。

vPC のイネーブル化

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

手順の概要

1. **configure terminal**
2. **feature vpc**
3. **exit**
4. **show feature**
5. **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	configure terminal 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	feature vpc 例： switch(config)# feature vpc	デバイス上で vPC をイネーブルにします。
ステップ 3	exit 例： switch(config)# exit switch#	グローバル コンフィギュレーション モードを終了します。
ステップ 4	show feature 例： switch# show feature	(任意) デバイス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 5	copy running-config startup-config 例： switch# copy running-config startup-config	(任意) 実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

例

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
switch(config)# exit
switch(config)#
```


vPC のディセーブル化



(注) vPC 機能をディセーブルにすると、デバイス上のすべての vPC 設定がクリアされます。

手順の概要

1. **configure terminal**
2. **no feature vpc**
3. **exit**
4. **show feature**
5. **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	configure terminal 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	no feature vpc 例： switch(config)# no feature vpc	デバイスの vPC をディセーブルにします。
ステップ 3	exit 例： switch(config)# exit switch#	グローバル コンフィギュレーション モードを終了します。
ステップ 4	show feature 例： switch# show feature	(任意) デバイス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 5	copy running-config startup-config 例： switch# copy running-config startup-config	(任意) 実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

例

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
```

```
switch(config)# exit
switch#
```

vPC ドメインの作成と vpc-domain モードの開始

vPC ドメインを作成し、両方の vPC ピア デバイス上で vPC ピア リンク ポート チャネルを同じ vPC ドメイン内に置くことができます。1 つの VDC 全体を通じて一意の vPC ドメイン番号を使用するこのドメイン ID は、vPC システム MAC アドレスを自動的に形成するのに使用されます。

このコマンドを使用して、vpc-domain コマンドモードを開始することもできます。

手順の概要

1. **configure terminal**
2. **vpc domain *domain-id* [shut | no shut]**
3. **exit**
4. **show vpc brief**
5. **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	configure terminal 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	vpc domain <i>domain-id</i> [shut no shut] 例： switch(config)# vpc domain 5 switch(config-vpc-domain)#	デバイス上に vPC ドメインを作成し、設定目的で vpc-domain 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	exit 例： switch(config)# exit switch#	vpc-domain 設定モードを終了します。
ステップ 4	show vpc brief 例： switch# show vpc brief	(任意) 各 vPC ドメインに関する簡単な情報を表示します。
ステップ 5	copy running-config startup-config 例： switch# copy running-config startup-config	(任意) 実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

例

次に、vpc-domain コマンドモードを開始して、既存の vPC ドメインを設定する例を示します。

```
switch# configure terminal
switch(config)# vpc domain 5
switch(config-vpc-domain)# exit
switch(config)#
```

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。



- (注) 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。



- (注) vPC ピアキープアライブリンクを使用する際は、個別の VRF インスタンスを設定して、各 vPC ピアデバイスからその VRF にレイヤ 3 ポートを接続することを推奨します。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。VRF の作成および設定方法については、『[Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide](#)』を参照してください。ピアキープアライブメッセージに使用される送信元と宛先の両方の IP アドレス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。管理ポートと管理 VRF が、これらのキープアライブメッセージのデフォルトです。

始める前に

vPC 機能が有効なことを確認します。

手順の概要

1. **configure terminal**
2. **vpc domain domain-id [shut | no shut]**
3. **peer-keepalive destination ipaddress [hold-timeout secs | interval msec {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. **exit**
5. **show vpc statistics**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	グローバル 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	vpc domain domain-id [shut no shut] 例 : <pre>switch(config)# vpc domain 5 switch(config-vpc-domain)#</pre>	デバイスで 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。
ステップ 3	peer-keepalive destination ipaddress [hold-timeout secs interval msec {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}] 例 : <pre>switch(config-vpc-domain)# peer-keepalive destination 172.28.230.85 switch(config-vpc-domain)#</pre>	<p>vPC ピアキープアライブリンクのリモートエンドの IPv4 および IPv6 アドレスを設定します。</p> <p>(注) vPC ピアキープアライブリンクを設定するまで、vPC ピアリンクは構成されません。</p> <p>(注) vPC ピアキープアライブリンクのリモートエンドに IPv6 アドレスを設定するときに送信元 IP アドレスを指定しないと、次のエラーメッセージが表示されることがあります。</p> <pre>Cannot configure IPV6 peer-keepalive without source IPV6 address</pre> <p>管理ポートと VRF がデフォルトです。</p> <p>(注) 独立した VRF を設定し、vPC ピアキープアライブリンクのための VRF 内の各 vPC ピア デバイスからのレイヤ 3 ポートを使用することを推奨します。VRF の作成および設定の詳細については、『Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide』を参照してください。</p>
ステップ 4	exit 例 : <pre>switch(config)# exit switch#</pre>	グローバル コンフィギュレーション モードを終了します。
ステップ 5	show vpc statistics 例 : <pre>switch# show vpc statistics</pre>	(任意) キープアライブメッセージの設定に関する情報を表示します。

	コマンドまたはアクション	目的
ステップ 6	copy running-config startup-config 例 : switch# copy running-config startup-config	(任意) 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

例

VRF の設定方法については、『[Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide](#)』を参照してください。

次の例は、vPC ピアキーブアライブ リンクの宛先と送信元の IP アドレスおよび VRF を設定する方法を示します。

```
switch# configure terminal
switch(config)# vpc domain 100
switch(config-vpc-domain)# peer-keepalive destination 172.168.1.2 source 172.168.1.1 vrf vpc-keepalive
switch(config-vpc-domain)# exit
switch#
```

vPC ピア リンクの作成

指定した vPC ドメインの vPC ピア リンクとして設定するポートチャネルを各デバイス上で指定して、vPC ピア リンクを作成します。冗長性を確保するため、トランクモードで vPC ピア リンクとして指定したレイヤ 2 ポートチャネルを設定し、各 vPC ピア デバイス上の個別のモジュールで 2 つのポートを使用することを推奨します。

始める前に

vPC 機能が有効なことを確認します。

手順の概要

1. **configure terminal**
2. **interface port-channel *channel-number***
3. **switchport mode trunk**
4. **switchport trunk allowed vlan *vlan-list***
5. **vpc peer-link**
6. **exit**
7. **show vpc brief**
8. **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	configure terminal 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します
ステップ 2	interface port-channel channel-number 例： switch(config)# interface port-channel 20 switch(config-if)#	このデバイスの vPC ピアリンクとして使用するポート 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。
ステップ 3	switchport mode trunk 例： switch(config-if)# switchport mode trunk	(任意) このインターフェイスをトランク モードで設定します。
ステップ 4	switchport trunk allowed vlan vlan-list 例： switch(config-if)# switchport trunk allowed vlan 1-120,201-3967	(任意) 許容 VLAN リストを設定します。
ステップ 5	vpc peer-link 例： switch(config-if)# vpc peer-link switch(config-vpc-domain)#	選択したポート チャンネルを 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 6	exit 例： switch(config)# exit switch#	vpc-domain 設定モードを終了します。
ステップ 7	show vpc brief 例： switch# show vpc brief	(任意) 各 vPC に関する情報を表示します。vPC ピアリンクに関する情報も表示されます。
ステップ 8	copy running-config startup-config 例： switch# copy running-config startup-config	(任意) 実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

例

次の例は、vPC ピアリンクを設定する方法を示しています。

```
switch# configure terminal
switch(config)# interface port-channel 20
switch(config-if)# switchport mode
```

```
switch(config-if)# switchport mode trunk
switch(config-if)# switchport trunk allowed vlan 1-120,201-3967
switch(config-if)# vpc peer-link
switch(config-vpc-domain)# exit
switch(config)#
```

他のポート チャネルの vPC への移行

冗長性を確保するために、vPC ドメイン ダウンストリーム ポート チャネルを 2 つのデバイスに接続することを推奨します。

ダウンストリーム デバイスに接続するには、ダウンストリーム デバイスからプライマリ vPC ピア デバイスへのポート チャネルを作成し、ダウンストリーム デバイスからセカンダリ ピア デバイスへのもう 1 つのポート チャネルを作成します。各 vPC ピア デバイス上で、ダウンストリーム デバイスに接続するポート チャネルに 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。

始める前に

vPC 機能が有効なことを確認します。

レイヤ 2 ポート チャネルを使用していることを確認します。

手順の概要

1. **configure terminal**
2. **interface port-channel *channel-number***
3. **vpc *number***
4. **exit**
5. **show vpc brief**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します
ステップ 2	interface port-channel <i>channel-number</i> 例： switch(config)# interface port-channel 20 switch(config-if)#	ダウンストリーム デバイスに接続するために vPC に入れるポートチャネルを選択し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	vpc <i>number</i> 例：	選択したポート チャネルを vPC に入れてダウンストリーム デバイスに接続するように設定します。こ

	コマンドまたはアクション	目的
	<pre>switch(config-if)# vpc 5 switch(config-vpc-domain)#</pre>	<p>これらのポートチャネルには、デバイス内の任意のモジュールを使用できます。範囲は、1～4096です。</p> <p>(注) vPC ピア デバイスからダウンストリームデバイスに接続されているポートチャネルに割り当てる vPC 番号は、両方の vPC デバイスで同じでなければなりません。</p>
ステップ 4	<p>exit</p> <p>例 :</p> <pre>switch(config)# exit switch#</pre>	vpc-domain 設定モードを終了します。
ステップ 5	<p>show vpc brief</p> <p>例 :</p> <pre>switch# show vpc brief</pre>	(任意) vPC に関する情報を表示します。
ステップ 6	<p>copy running-config startup-config</p> <p>例 :</p> <pre>switch# copy running-config startup-config</pre>	(任意) 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

例

次に、ダウンストリーム デバイスに接続するポート チャネルを設定する例を示します。

```
switch# configure terminal
switch(config)# interface port-channel 20
switch(config-if)# vpc 5
switch(config-if)# exit
switch(config)#
```

vPC ピア リンクの構成の互換性チェック

両方の vPC ピア デバイス上の 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が一貫していることをチェックします。vPC での一貫した設定については、「vPC インターフェイスの互換パラメータ」の項を参照してください。

手順の概要

1. **configure terminal**
2. **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	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	グローバル 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	show vpc consistency-parameters {global interface port-channel channel-number} 例 : <pre>switch(config)# show vpc consistency-parameters global switch(config)#</pre>	(任意) 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# configure terminal
switch(config)# show vpc consistency-parameters global
switch(config)#
```



(注) vPC インターフェイス設定の互換性に関するメッセージが syslog にも記録されます。

グレースフル整合性検査の設定

デフォルトでイネーブルになるグレースフル整合性検査機能を設定できます。この機能がイネーブルでない場合、必須互換性パラメータの不一致が動作中の vPC で導入されると、vPC は完全に一時停止します。この機能がイネーブルの場合、セカンダリ ピア デバイスのリンクだけが一時停止します。vPC での一貫した設定については、「vPC インターフェイスの互換パラメータ」の項を参照してください。

手順の概要

1. **configure terminal**
2. **vpc domain domain-id [shut | no shut]**
3. **graceful consistency-check**
4. **exit**
5. **show vpc brief**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	vpc domain domain-id [shut no shut] 例： switch(config-if)# vpc domain 5 switch(config-vpc-domain)#	vPC ドメインがまだ存在してい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	graceful consistency-check 例： switch(config-vpc-domain)# graceful consistency-check	必須互換性パラメータで不一致が検出された場合に、セカンダリ ピア デバイスのリンクのみが一時停止するということを指定します。 この機能を無効にするには、このコマンドの no 形式を使用します。
ステップ 4	exit 例： switch(config)# exit switch#	vpc-domain 設定モードを終了します。
ステップ 5	show vpc brief 例： switch# show vpc brief	(任意) vPC に関する情報を表示します。

例

次に、グレースフル整合性検査機能をイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# vpc domain 5
switch(config-vpc-domain)# graceful consistency-check
switch(config-vpc-domain)# exit
switch(config)#
```

vPC ピアゲートウェイの設定

vPC ピア デバイスを、vPC ピア デバイスの MAC アドレスに送信されるパケットに対してゲートウェイとして機能するように設定できます。

始める前に

vPC 機能が有効なことを確認します。

手順の概要

1. **configure terminal**
2. **vpc domain *domain-id* [shut | no shut]**
3. **peer-gateway**
4. **exit**
5. **show vpc brief**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	グローバル 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	vpc domain <i>domain-id</i> [shut no shut] 例 : <pre>switch(config-if)# vpc domain 5 switch(config-vpc-domain)#</pre>	vPC ドメインがまだ存在してい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	peer-gateway 例 : <pre>switch(config-vpc-domain)# peer-gateway</pre> (注) この機能を正常に動作させるために、このvPCドメインのすべてのインターフェイス VLAN 上で IP リダイレクトをディセーブルにします。	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	exit 例 : <pre>switch(config)# exit switch#</pre>	vpc-domain 設定モードを終了します。
ステップ 5	show vpc brief 例 : <pre>switch# show vpc brief</pre>	(任意) 各 vPC に関する情報を表示します。vPC ピアリンクに関する情報も表示されます。
ステップ 6	copy running-config startup-config 例 : <pre>switch# copy running-config startup-config</pre>	(任意) 実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

vPC ピアスイッチの設定

Cisco Nexus 9000 シリーズ デバイスは、一対の vPC デバイスがレイヤ 2 トポロジ内で 1 つの STP ルートとして現れるように設定することができます。

純粋な vPC ピアスイッチ トポロジの設定

純粋な vPC ピアスイッチ トポロジを設定するには、`peer-switch` コマンドを使用し、次に可能な範囲内で最高の（最も小さい）スパンニングツリーブリッジプライオリティ値を設定します。

始める前に

vPC 機能が有効なことを確認します。



(注) VPC ピア間の非 VPC 専用トランク リンクを使用する場合は、STP が VLAN をブロックするのを防ぐために、非 VPC VLAN はピアによって異なるグローバルプライオリティが必要です。

手順の概要

1. `configure terminal`
2. `vpc domain domain-id [shut | no shut]`
3. `peer-switch`
4. `spanning-tree vlan vlan-range priority value`
5. `exit`
6. `show spanning-tree summary`
7. `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	configure terminal 例： <code>switch# configure terminal</code> <code>switch(config)#</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	vpc domain domain-id [shut no shut] 例： <code>switch(config)# vpc domain 5</code> <code>switch(config-vpc-domain)#</code>	設定する vPC ドメインの番号を入力し、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	peer-switch 例： <code>switch(config-vpc-domain)# peer-switch</code>	vPC スイッチ ペアがレイヤ 2 トポロジ内で 1 つの STP ルートとして現れるようにします。 ピア スイッチ vPC トポロジをディセーブルにするには、このコマンドの no 形式を使用します。

	コマンドまたはアクション	目的
ステップ 4	spanning-tree vlan <i>vlan-range</i> priority <i>value</i> 例： switch(config)# spanning-tree vlan 1 priority 8192	VLAN のブリッジプライオリティを設定します。有効な値は、4096 の倍数です。デフォルト値は 32768 です。
ステップ 5	exit 例： switch(config-vpc-domain)# exit switch#	vpc-domain 設定モードを終了します。
ステップ 6	show spanning-tree summary 例： switch# show spanning-tree summary	(任意) スパニングツリーポートの状態の概要を表示します。これに、vPC ピア スイッチも含まれます。
ステップ 7	copy running-config startup-config 例： switch# copy running-config startup-config	(任意) 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

例

次の例は、純粋な vPC ピア スイッチ トポロジを設定する方法を示します。

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# vpc domain 5
switch(config-vpc-domain)# peer-switch

2010 Apr 28 14:44:44 switch %STP-2-VPC_PEERSWITCH_CONFIG_ENABLED: vPC peer-switch
configuration is enabled. Please make sure to configure spanning tree "bridge" priority
as
per recommended guidelines to make vPC peer-switch operational.

switch(config-vpc-domain)# spanning-tree vlan 1 priority 8192
switch(config-vpc-domain)# exit
switch(config)#
```

孤立ポートの一時停止の設定

vPC 対応でないデバイスが各ピアに接続するとき、接続されたポートは vPC のメンバではないため、孤立ポートと称されます。vPC ピア リンクまたはピア キープアライブ障害に応じてセカンダリピアが vPC ポートを一時停止するときに、セカンダリピアによって一時停止（シャットダウン）される孤立ポートとして物理インターフェイスを明示的に宣言できます。孤立ポートは vPC が復元されたときに復元されます。



(注) vPC 孤立ポートの一時停止は、物理ポート、ポート チャネルでのみ設定できます。ただし、個々のポート チャネル メンバー ポートで同じ設定はできません。

始める前に

vPC 機能が有効なことを確認します。

手順の概要

1. **configure terminal**
2. **show vpc orphan-ports**
3. **interface type slot/port**
4. **vpc orphan-port suspend**
5. **exit**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	show vpc orphan-ports 例： switch# show vpc orphan-ports	(任意) 孤立ポートのリストを表示します。
ステップ 3	interface type slot/port 例： switch(config)# interface ethernet 3/1 switch(config-if)#	設定するインターフェイスを指定し、インターフェイス コンフィギュレーションモードを開始します。
ステップ 4	vpc orphan-port suspend 例： switch(config-if)# vpc orphan-ports suspend	選択したインターフェイスを vPC 障害時にセカンダリ ピアにより一時停止される vPC 孤立ポートとして設定します。
ステップ 5	exit 例： switch(config-if)# exit switch#	インターフェイス コンフィギュレーション モードを終了します。
ステップ 6	copy running-config startup-config 例：	(任意) 実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

コマンドまたはアクション	目的
switch# copy running-config startup-config	

例

次に、インターフェイスを vPC 障害時にセカンダリ ピアにより一時停止される vPC 孤立ポートとして設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 3/1
switch(config-if)# vpc orphan-ports suspend
switch(config-if)# exit
switch(config)#
```

Cisco NX-OS リリース 9.2(1) 以降では、**show vpc orphan-ports** コマンドの出力が以前のリリースの出力と若干異なります。次に、**show vpc orphan-ports** コマンドの出力例を示します。

```
switch# show vpc orphan-ports
-----::Going through port database. Please be patient.::-----
VLAN          Orphan Ports
-----
1              Eth1/18, Eth3/23
2              Eth3/23
3              Eth3/23
4              Eth3/23
5              Eth3/23
```

シングルモジュール vPC オブジェクト トラッキングでのトラッキング機能の設定

すべての vPC ピア リンクとコアに面するインターフェイスを単一モジュール上で設定しなければならない場合は、両方のプライマリ vPC ピア デバイス上の vPC ピア リンクのすべてのリンク上にあり、コアへのレイヤ 3 リンクに関連付けられているトラックオブジェクトとトラックリストを設定しなければなりません。いったんこの機能を設定したら、プライマリ vPC ピア デバイスに障害が発生した場合には、プライマリ vPC ピア デバイス上のすべての vPC リンクを、システムが自動的に停止します。システムが安定するまでは、このアクションにより、すべての vPC トラフィックが強制的にセカンダリ vPC ピア デバイスに送られます。

この設定は、両方の vPC ピア デバイスに置かなければなりません。さらに、いずれの vPC ピア デバイスも機能上のプライマリ vPC ピア デバイスになる場合があるため、両方の vPC ピア デバイスに同じ設定を置いておく必要があります。

始める前に

vPC 機能が有効なことを確認します。

トラックオブジェクトとトラックリストが設定済みであることを確認します。コアおよびvPCピアリンクに接続されているすべてのインターフェイスが両方のvPCピアデバイス上のトラックオブジェクトに割り当てられていることを確認します。

手順の概要

1. **configure terminal**
2. **vpc domain** *domain-id* [**shut** | **no shut**]
3. **track** *track-object-id*
4. **exit**
5. **show vpc brief**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	vpc domain <i>domain-id</i> [shut no shut] 例： switch(config)# vpc domain 5 switch(config-vpc-domain)#	設定する vPC ドメインの番号を入力し、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	track <i>track-object-id</i> 例： switch(config-vpc-domain)# track object 23 switch(config-vpc-domain)#	以前に関連するインターフェイスで設定されたトラックリストオブジェクトをvPCドメインに追加します。オブジェクトトラッキングおよびトラックリストの詳細については、『 Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide 』を参照してください。
ステップ 4	exit 例： switch(config-vpc-domain)# exit switch#	vpc-domain 設定モードを終了します。
ステップ 5	show vpc brief 例： switch# show vpc brief	(任意) 追跡対象オブジェクトに関する情報を表示します。
ステップ 6	copy running-config startup-config 例： switch# copy running-config startup-config	(任意) 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

例

次に、以前に設定されたトラックリストオブジェクトを、vPC ピアデバイス上の vPC ドメインに配置する例を示します。

```
switch# configure terminal
switch(config)# vpc domain 5
switch(config-vpc-domain)# track object 5
switch(config-vpc-domain)# exit
switch(config)#
```

停電後のリカバリの設定

停電が発生すると、vPC はピア隣接がスイッチリロード時に形成するのを待ちます。この状況は、許容範囲内に収まらないほど長いサービスの中断に至る場合があります。Cisco Nexus 9000 シリーズ デバイスは、そのピアがオンラインになるのに失敗した場合に vPC サービスを復元するように設定できます。

自動リカバリの設定

Cisco Nexus 9000 シリーズ デバイスは、**auto-recovery** コマンドを使用して、そのピアがオンラインになるのに失敗した場合に vPC サービスを復元するように設定できます。

Cisco Nexus 9000 シリーズ デバイスは、**auto-recovery** コマンドを使用して、vPC プライマリ ピアが失敗し、ピア キープアライブと vPC ピア リンクを停止するとき、セカンダリ vPC ピアの vPC サービスを復元するように構成できます。ピア キープアライブと vPC ピア リンクの両方がダウンしているプライマリ スイッチに障害が発生すると、セカンダリ スイッチは vPC メンバーを一時停止します。ただし、キープアライブ ハートビートが 3 回失われると、セカンダリ スイッチはプライマリ スイッチの役割を再開し、vPC メンバーポートを起動します。

auto-recovery reload restore コマンドは、vPC プライマリ スイッチがリロードするシナリオで使用できます。この場合、セカンダリ スイッチは vPC プライマリの役割を再開し、IP VPC メンバー ポートを持ち込みます。



- (注) Cisco Nexus 9000 スイッチでは、自動回復機能はデフォルトで有効になっていません。オブジェクト トラッキングがトリガーされると、vPC セカンダリ ピア デバイスはそのプライマリ デバイスへのロールを変更せず、vPC レッグを再初期化します。プライマリ ロールを引き継いで vPC レッグを再初期化できるように、vPC セカンダリ ピア デバイスで自動回復を手動で設定する必要があります。

始める前に

vPC 機能が有効なことを確認します。

手順の概要

1. configure terminal

2. `vpc domain domain-id [shut | no shut]`
3. `auto-recovery [reload-delay time]`
4. `exit`
5. `show running-config vpc`
6. `show vpc consistency-parameters interface port-channel number`
7. `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	configure terminal 例： <code>switch# configure terminal</code> <code>switch(config)#</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	vpc domain domain-id [shut no shut] 例： <code>switch(config)# vpc domain 5</code> <code>switch(config-vpc-domain)#</code>	設定する vPC ドメインの番号を入力し、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	auto-recovery [reload-delay time] 例： <code>switch(config-vpc-domain)# auto-recovery</code>	vPC がそのピアが機能しないことを前提として vPC を稼働させ始めるように設定し、vPC を復元するためのリロード後に待機する時間を指定します。デフォルト遅延値は 240 秒です。240 ~ 3600 秒の遅延を設定できます。 vPC をデフォルト設定にリセットするには、このコマンドの no 形式を使用します。
ステップ 4	exit 例： <code>switch(config-vpc-domain)# exit</code> <code>switch#</code>	vpc-domain 設定モードを終了します。
ステップ 5	show running-config vpc 例： <code>switch# show running-config vpc</code>	(任意) vPC に関する情報、特にリロードステータスを表示します。
ステップ 6	show vpc consistency-parameters interface port-channel number 例： <code>switch# show vpc consistency-parameters interface port-channel 1</code>	(任意) 指定したインターフェイスの vPC の一貫性パラメータに関する情報を表示します。
ステップ 7	copy running-config startup-config 例：	(任意) 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

	コマンドまたはアクション	目的
	switch# copy running-config startup-config	(注) 自動リカバリ機能がイネーブルになっていることを確認するには、この手順を実行します。

例

次に、vPC 自動リカバリ機能を設定し、それをスイッチのスタートアップ コンフィギュレーションに保存する例を示します。

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# vpc domain 5
switch(config-vpc-domain)# auto-recovery
switch(config-vpc-domain)# auto-recovery auto-recovery reload-delay 100

Warning:
Enables restoring of vPCs in a peer-detached state after reload, will wait for 240
seconds to determine if peer is un-reachable

switch(config-vpc-domain)# exit
switch(config)# exit
switch# copy running-config startup-config
```

ヒットレス vPC ロール変更の設定

ヒットレス vPC ロールの変更を有効にするには、次の手順を実行します。

始める前に

- vPC 機能がイネーブルになっていることを確認します。
- vPC ピア リンクがアップしていることを確認します
- デバイスのロール プライオリティを検証します

手順の概要

1. **vpc role preempt**
2. **show vpc role**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	vpc role preempt 例 : switch# vpc role preempt switch(config)#	ヒットレス vPC ロールの変更を有効にします。

	コマンドまたはアクション	目的
ステップ 2	show vpc role 例 : switch(config)# show vpc role	(任意) ヒットレスvPCロール変更機能を確認します。

例

次に、ヒットレス vPC ロールの変更を設定する例を示します。

```
switch# show vpc role
vPC Role status
-----
vPC role                : secondary
vPC system-mac          : 00:23:04:ee:be:01
vPC system-priority     : 32667
vPC local system-mac    : 8c:60:4f:03:84:41
vPC local role-priority : 32668
vPC peer system-mac     : 8c:60:4f:03:84:43
vPC peer role-priority  : 32667

! Configure vPC hitless role change on the device!

switch(config)# vpc role preempt
! The following is an output from the show vpc role command after the
vPC hitless feature is configured
switch(config)# show vpc role
vPC Role status
-----
vPC role                : primary
vPC system-mac          : 00:00:00:00:00:00
vPC system-priority     : 32667
vPC local system-mac    : 8c:60:4f:03:84:41
vPC local role-priority : 32666
vPC peer system-mac     : 8c:60:4f:03:84:43
vPC peer role-priority  : 32667

switch(config)#
```

vPC ロールの変更に関する使用ケース シナリオ

ヒットレス vPC ロール変更機能は、次のシナリオで使用できます。

- ロール変更要求 : vPC ドメインのピアデバイスのロールを変更する場合。
- プライマリ スイッチのリロード : リロード後にロールが定義され、ロールが定義されると、ヒットレス vPC ロール変更機能を使用してロールを復元できます。たとえば、リロード後にプライマリデバイスが動作可能なセカンダリの役割を果たし、セカンダリデバイスがプライマリの動作の役割を担う場合、**vpc role preempt** コマンドを使用してvPCピアの役割を元の定義済みの役割に変更できます。



(注) vPC ロールを切り替える前に、必ず、既存のデバイスロールプライオリティをチェックしてください。

- デュアルアクティブリカバリ：デュアルアクティブリカバリシナリオでは、vPCプライマリスイッチが引き続き（動作中）プライマリになりますが、vPCセカンダリスイッチがターゲットプライマリスイッチになり、vPCメンバーポートがアップ状態になります。vPCヒットレス機能を使用して、デバイスロールを復元できます。デュアルアクティブリカバリ後は、一方が稼働可能なプライマリで、もう一方が稼働可能なセカンダリの場合に、**vpc role preempt** コマンドを使用して、プライマリにするデバイスロールとセカンダリにするデバイスロールを復元できます。

vPC ドメイン MAC アドレスの手動での設定

vPC ドメインを作成すると、Cisco NX-OS ソフトウェアが自動的に vPC システム MAC アドレスを作成します。このアドレスは、LACP など、リンクスコープに制限される操作に使用されます。ただし、vPC ドメインの MAC アドレスを手動で設定するように選択することもできます。

始める前に

vPC 機能が有効なことを確認します。

手順の概要

1. **configure terminal**
2. **vpc domain *domain-id* [shut | no shut]**
3. **system-mac *mac-address***
4. **exit**
5. **show vpc role**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： <pre>switch# configure terminal switch(config)#</pre>	グローバル 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	vpc domain <i>domain-id</i> [shut no shut] 例： <pre>switch(config)# vpc domain 5 switch(config-vpc-domain)#</pre>	設定する vPC ドメインの番号を入力します。システムは、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	system-mac <i>mac-address</i> 例： <pre>switch(config-vpc-domain)# system-mac 23fb.4ab5.4c4e switch(config-vpc-domain)#</pre>	指定した vPC ドメインに割り当てる MAC アドレスを <code>aaaa.bbbb.cccc</code> の形式で入力します。

	コマンドまたはアクション	目的
ステップ 4	exit 例： switch(config-vpc-domain)# exit switch#	vpc-domain 設定モードを終了します。
ステップ 5	show vpc role 例： switch# show vpc brief	(任意) vPC システム MAC アドレスを表示します。
ステップ 6	copy running-config startup-config 例： switch# copy running-config startup-config	(任意) 実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

例

次の例は、vPC ドメイン MAC アドレスを手動で設定する方法を示します。

```
switch# configure terminal
switch(config)# vpc domain 5
switch(config-vpc-domain)# system-mac 13gb.4ab5.4c4e
switch(config-vpc-domain)# exit
switch(config)#
```

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。



- (注) LACP の実行時には、vPC ピア デバイスが LACP のプライマリ デバイスになるように、vPC システム プライオリティを手動で設定することを推奨します。システム プライオリティを手動で設定する場合には、必ず同じプライオリティ値を両方のvPC ピアデバイスに設定します。これらの値が一致しないと、vPC は起動しません。

始める前に

vPC 機能が有効なことを確認します。

手順の概要

1. **configure terminal**
2. **vpc domain domain-id [shut | no shut]**
3. **system-priority priority**
4. **exit**

5. **show vpc role**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	vpc domain domain-id [shut no shut] 例： switch(config)# vpc domain 5 switch(config-vpc-domain)#	設定する vPC ドメインの番号を入力します。システムは、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	system-priority priority 例： switch(config-vpc-domain)# system-priority 4000 switch(config-vpc-domain)#	指定した vPC ドメインに割り当てるシステム プライオリティを入力します。指定できる値の範囲は、1 ~ 65535 です。デフォルト値は 32667 です。
ステップ 4	exit 例： switch(config-vpc-domain)# exit switch#	vpc-domain 設定モードを終了します。
ステップ 5	show vpc role 例： switch# show vpc role	(任意) vPC システム プライオリティを表示します。
ステップ 6	copy running-config startup-config 例： switch# copy running-config startup-config	(任意) 実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

例

次の例は、vPC ドメインのシステム プライオリティを手動で設定する方法を示します。

```
switch# configure terminal
switch(config)# vpc domain 5
switch(config-vpc-domain)# system-priority 4000
switch(config-vpc-domain)# exit
switch(config)#
```

vPC ピア デバイス ロールの手動での設定

デフォルトでは、vPC ドメインと、vPC ピア リンクの両端を設定すると、Cisco NX-OS ソフトウェアはプライマリとセカンダリの vPC ピア デバイスを選択します。ただし、vPC のプライマリ デバイスとして、特定の vPC ピア デバイスを選択することもできます。選択したら、プライマリ デバイスにする vPC ピア デバイスに、他の vPC ピア デバイス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ません。プライマリ vPC ピア デバイスに障害が発生すると、セカンダリ vPC ピア デバイスが、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 が再起動しても、機能のロールは元に戻りません。

始める前に

vPC 機能が有効なことを確認します。

手順の概要

1. **configure terminal**
2. **vpc domain *domain-id* [shut | no shut]**
3. **role priority *priority***
4. **exit**
5. **show vpc role**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	vpc domain <i>domain-id</i> [shut no shut] 例： switch(config)# vpc domain 5 switch(config-vpc-domain)#	設定する vPC ドメインの番号を入力します。システムは、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	role priority <i>priority</i> 例： switch(config-vpc-domain)# role priority 4 switch(config-vpc-domain)#	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。値の範囲は1～65636で、デフォルト値は32667です。低い値は、このスイッチがプライマリ vPC になる可能性が高いということを意味します。
ステップ 4	exit 例：	vpc-domain 設定モードを終了します。

	コマンドまたはアクション	目的
	switch(config)# exit switch#	
ステップ 5	show vpc role 例： switch# show vpc role	(任意) vPC システム プライオリティを表示します。
ステップ 6	copy running-config startup-config 例： switch# copy running-config startup-config	(任意) 実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

例

次の例は、vPC ピアデバイスのロールプライオリティを手動で設定する方法を示します。

```
switch# configure terminal
switch(config)# vpc domain 5
switch(config-vpc-domain)# role priority 4
switch(config-vpc-domain)# exit
switch(config)#
```

Cisco MAC アドレスを使用するための STP の有効化

この手順により、STP が Cisco MAC アドレス (00 : 26 : 0b : xx : xx : xx) を使用できるようになります。

始める前に

vPC 機能が有効なことを確認します。

手順の概要

1. **configure terminal**
2. **vpc domain domain-id**
3. **[no] mac-address bpdu source version 2**
4. **exit**
5. (任意) **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	configure terminal 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 2	vpc domain <i>domain-id</i> 例： switch(config)# vpc domain 5	vPC ドメインがまだ存在してい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	[no] mac-address bpd source version 2 例： switch(config-vpc-domain)# mac-address bpd source version 2	STP がシスコの MAC アドレス (00:26:0b:xx:xx:xx) を、vPC ポートで生成される BDPU の発信元アドレスとして使用できるようになります。
ステップ 4	exit 例： switch(config-vpc-domain)# exit	vpc-domain 設定モードを終了します。
ステップ 5	(任意) copy running-config startup-config 例： switch(config)# copy running-config startup-config	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。

vPC 設定の確認

vPC 設定情報を表示するには、次の作業のいずれかを行います。

コマンド	目的
show feature	vPC がイネーブルになっているかどうかを表示します。
show vpc brief	vPC に関する要約情報を表示します。
show vpc consistency-parameters	すべての vPC インターフェイス全体で一貫している必要があるパラメータのステータスを表示します。
show running-config vpc	vPC の実行コンフィギュレーションの情報を表示します。
show port-channel capacity	設定されているポート チャンネルの数、およびデバイス上でまだ使用可能なポート チャンネル数を表示します。
show vpc statistics	vPC に関する統計情報を表示します。
show vpc peer-keepalive	ピアキープアライブ メッセージに関する情報を表示します。

コマンド	目的
<code>show vpc role</code>	ピア ステータス、ローカル デバイスのロール、vPC システム 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 デバイスの MAC アドレスとプライオリティを表示します。

vPC のモニタリング

`show vpc statistics` コマンドを使用し、vPC 統計情報を表示します。

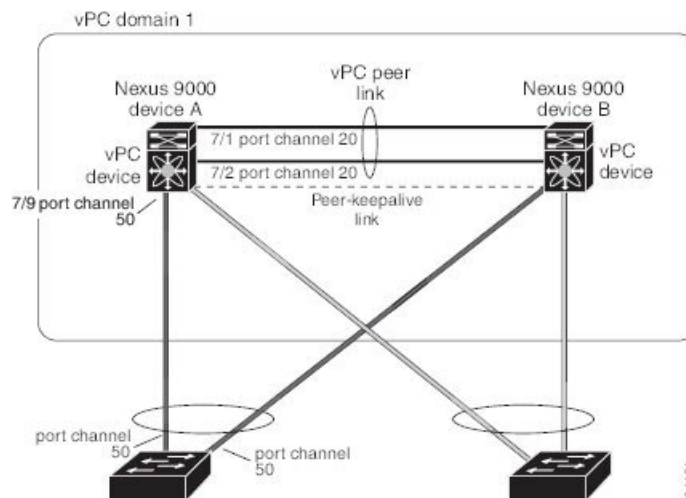


(注) このコマンドは、現在作業している vPC ピア デバイスの vPC 統計情報しか表示しません。

vPC の設定例

次の例は、の図に示すように、デバイス A 上で vPC を設定する方法を示します。

図 28: vPC の設定例



- vPC および LACP をイネーブルにします。


```
switch# configure terminal
switch(config)# feature vpc
switch(config)# feature lacp
```
- (任意) vPC ピア リンクにするインターフェイスの 1 つを専用モードに構成します。


```
switch(config)# interface ethernet 7/1,
ethernet 7/3, ethernet 7/5. ethernet 7/7
```

```
switch(config-if)# shutdown
switch(config-if)# exit
switch(config)# interface ethernet 7/1
```

```
switch(config-if)# no shutdown
switch(config-if)# exit
switch(config)#
```

3. (任意) vPC ピア リンクにする 2 つ目の冗長インターフェイスを専用ポートモードに構成します。

```
switch(config)# interface ethernet 7/2, ethernet 7/4,
ethernet 7/6. ethernet 7/8
switch(config-if)# shutdown
switch(config-if)# exit
switch(config)# interface ethernet 7/2
```

```
switch(config-if)# no shutdown
switch(config-if)# exit
switch(config)#
```

4. vPC ピア リンクに入れる 2 つのインターフェイス (冗長性のために) をアクティブ レイヤ 2 LACP ポート チャネルに構成します。

```
switch(config)# interface ethernet 7/1-2
switch(config-if)# switchport
switch(config-if)# switchport mode trunk
switch(config-if)# switchport trunk allowed vlan 1-50
switch(config-if)# switchport trunk native vlan 20
switch(config-if)# channel-group 20 mode active
switch(config-if)# exit
```

5. VLAN を作成し、イネーブルにします。

```
switch(config)# vlan 1-50
switch(config-vlan)# no shutdown
switch(config-vlan)# exit
```

6. vPC ピアキープアライブ リンク用の独立した VEF を作成し、レイヤ 3 インターフェイスをその VRF に追加します。

```
switch(config)# vrf context pkal
switch(config-vrf)# exit
switch(config)# interface ethernet 8/1
switch(config-if)# vrf member pkal
switch(config-if)# ip address 172.23.145.218/24
switch(config-if)# no shutdown
switch(config-if)# exit
```

7. vPC ドメインを作成し、vPC ピアキープアライブ リンクを追加します。

```
switch(config)# vpc domain 1
switch(config-vpc-domain)# peer-keepalive
destination 172.23.145.217 source 172.23.145.218 vrf pkal
switch(config-vpc-domain)# exit
```

8. vPC vPC ピア リンクを構成します。

```
switch(config)# interface port-channel 20
switch(config-if)# switchport mode trunk
switch(config-if)# switchport trunk allowed vlan 1-50
switch(config-if)# vpc peer-link
```

```
switch(config-if)# exit
switch(config)#
```

9. vPC のダウンストリーム デバイスへのポート チャネルのインターフェイスを設定します。

```
switch(config)# interface ethernet 7/9
switch(config-if)# switchport mode trunk
switch(config-if)# allowed vlan 1-50
switch(config-if)# native vlan 20
switch(config-if)# channel-group 50 mode active
switch(config-if)# exit
switch(config)# interface port-channel 50
switch(config-if)# vpc 50
switch(config-if)# exit
switch(config)#
```

10. 設定を保存します。

```
switch(config)# copy running-config startup-config
```



(注) まずポート チャネルを設定する場合は、それがレイヤ 2 ポート チャネルであることを確認してください。

関連資料

関連項目	関連項目
システム管理	システム管理
高可用性	高可用性
リリース ノート	リリース ノート



第 9 章

IP トンネルの設定

- [IP トンネルについて \(375 ページ\)](#)
- [IP トンネルの前提条件 \(377 ページ\)](#)
- [注意事項と制約事項 \(378 ページ\)](#)
- [デフォルト設定 \(384 ページ\)](#)
- [IP トンネルの設定 \(385 ページ\)](#)
- [IP トンネル設定の確認 \(397 ページ\)](#)
- [IP トンネリングの設定例 \(398 ページ\)](#)
- [関連資料 \(399 ページ\)](#)

IP トンネルについて

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

IP トンネルの概要

IP トンネルは次の 3 つの主要コンポーネントで構成されています。

- **パッセンジャ プロトコル**：カプセル化する必要があるプロトコル。パッセンジャ プロトコルの例には IPv4 があります。
- **キャリア プロトコル**：パッセンジャ プロトコルをカプセル化するために使用するプロトコル。Cisco NX-OS はキャリア プロトコルとして GRE をサポートします。
- **トランスポート プロトコル**：カプセル化したプロトコルを伝送するために使用するプロトコル。トランスポート プロトコルの例には IPv4 があります。IP トンネルは IPv4 などのパッセンジャ プロトコルを使用し、このプロトコルを GRE などのキャリア プロトコル内にカプセル化します。次に、このキャリア プロトコルは IPv4 などのトランスポート プロトコルを通じてデバイスから送信されます。

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

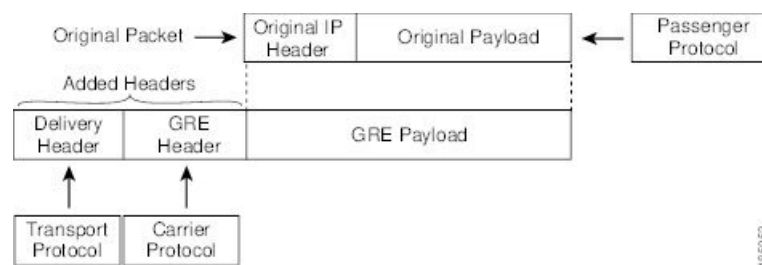
設定の前にトンネル機能をイネーブルにする必要があります。システムはこの機能をディセーブルにする前のチェックポイントを自動的に取得するため、このチェックポイントにロールバックできます。ロールバックおよびチェックポイントについては、『[Cisco Nexus 9000 Series NX-OS System Management Configuration Guide](#)』を参照してください。

GRE トンネル

Generic Routing Encapsulation (GRE) をさまざまなパッセンジャプロトコルのキャリアプロトコルとして使用できます。

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

図 29: GRE PDU



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

ポイントツーポイント IP-in-IP のカプセル化およびカプセル化解除は、送信元トンネルインターフェイスから宛先トンネルインターフェイスにカプセル化されたパケットを送信するために作成できる一種のトンネルです。このタイプのトンネルは、着信トラフィックと発信トラフィックの両方を伝送します。

Cisco NX-OS リリース 10.4(1)F 以降、IPv4 トンネルは GRE でサポートされ、IPv6 トラフィックは GRE IPv4 内でカプセル化できます。



(注) Cisco NX-OS リリース 10.3(3)F 以降、PBR ポリシーに基づいて GRE または IP-in-IP トンネル宛先の選択がサポートされます。



(注) IP-in-IP トンネル カプセル化とカプセル化解除は、N9K-X9636C-R、N9K-X9636Q-R、N9K-X9636C-RX ラインカードを搭載した Cisco Nexus 9500 シリーズスイッチではサポートされません。



- (注) IP-in-IP トンネルのカプセル化とカプセル化解除は、Cisco Nexus 9300-EX、9300-FX、9300-GX および Nexus 9500 プラットフォーム スイッチの vPC 設定ではサポートされません。

マルチポイント IP-in-IP トンネルのカプセル化解除

マルチポイント IP-in-IP の decapsulate-any は、任意の数の IP-in-IP トンネルから 1 つのトンネル インターフェイスにパケットのカプセル化を解除するために作成できるトンネルのタイプです。このトンネルは発信トラフィックを伝送しません。ただし、任意の数のリモートトンネル エンドポイントが、このように設定されたトンネルを宛先として使用することができます。

パス MTU ディスカバリ

パス最大伝送単位 (MTU) ディスカバリ (PMTUD) は、パケットの発信元から宛先へのパスに沿って最小 MTU を動的に決定することで、2 つのエンドポイント間のパスのフラグメンテーションを防ぎます。PMTUD は、パケットにフラグメンテーションが必要であるという情報がインターフェイスに届くと、接続に対する送信 MTU 値を減らします。

PMTUD をイネーブルにすると、インターフェイスはトンネルを通過するすべてのパケットに Don't Fragment (DF) ビットを設定します。トンネルに入ったパケットがそのパケットの MTU 値よりも小さい MTU 値を持つリンクを検出すると、リモートリンクはそのパケットをドロップし、パケットの送信元にインターネット制御メッセージプロトコル (ICMP) メッセージを返します。このメッセージには、フラグメンテーションが要求されたこと (しかし許可されなかったこと) と、パケットをドロップしたリンクの MTU が含まれています。



- (注) トンネル インターフェイスの PMTUD は、トンネル エンドポイントがトンネルのパスでデバイスによって生成される ICMP メッセージを受信することを要求します。ファイアウォール接続を通じて PMTUD を使用する前に、ICMP メッセージを受信できることを確認してください。

高可用性

IP トンネルはステートフル再起動をサポートします。ステートフル再起動はスーパーバイザ切り替え時に発生します。切り替え後、Cisco NX-OS は実行時の設定を適用します。

IP トンネルの前提条件

IP トンネルには次の前提条件があります。

- IP トンネルを設定するための TCP/IP に関する基礎知識があること。
- スイッチにログインしている。

- IP トンネルを設定してイネーブルにする前にデバイスのトンネリング機能をイネーブルにしておくこと。

注意事項と制約事項

IP トンネルの設定に関する注意事項と制約事項は次のとおりです。

- Cisco NX-OS リリース 9.3(3) 以降：
 - 合計 16 個の GRE/IPIP トンネルが、Cisco Nexus 9200、9300-EX/FX/FX2 スイッチ、および 9700-EX/FX ラインカードを搭載した 9500 スイッチでサポートされます。
 - 同じ Cisco Nexus デバイス上の複数の IP-in-IP/GRE トンネルインターフェイスは、異なる VRF 間で、同じ IP アドレスを送信元とすること、または同じ IP アドレスを宛先とすることができます。これは、Cisco Nexus 9200 および 9300-EX/FX/FX2 プラットフォームでサポートされています。これは、9300-GX ラインカードを搭載した Cisco Nexus 9500 プラットフォーム スイッチではサポートされていません。
 - 複数の、最大で 16 の IPIP Decap-any トンネルがサポートされています。VRF ごとに 1 つの decap-any トンネルです。これは、Cisco Nexus 9200 および 9300-EX/FX/FX2 プラットフォームでサポートされています。
 - IPIP/GRE カプセル化パケットが終端ノードで入力されるインターフェイスの VRF メンバーシップは、トンネルのパケットを正しく終端するために、トンネル転送 VRF と一致している必要があります。
 - パケットの外部ヘッダーがトンネルの送信元およびトンネルの宛先と一致する場合、デフォルト以外の VRF に着信する IPIP/GRE パケットは、デフォルトの VRF トンネルによって終端されることがあります。
- Cisco NX-OS リリース 9.3(5) 以降では、次の機能が N9K-C9316D-GX、N9K-C93600CD-GX、および N9K-C9364C-GX スイッチでサポートされています。
 - 合計 16 の GRE/IPIP トンネル。
 - 同じ Cisco Nexus デバイス上の複数の IP-in-IP/GRE トンネルインターフェイスは、異なる VRF 間で、同じ IP アドレスを送信元とすること、または同じ IP アドレスを宛先とすることができます。
 - 複数の、最大で 16 の IPIP Decap-any トンネルがサポートされています。VRF ごとに 1 つの decap-any トンネルです。
- GRE ストリッピングは、N9K-C9364C および N9K-C9332C ファミリ スイッチ、および N9K-C9508-FM-E2、N9K-C9516-FM-E2 モジュールではサポートされていません。
- トンネルの **source-direct** および **ipv6ipv6-decapsulate-any** オプションについてのガイドラインは、以下のとおりです：

- IP トンネルは、インターフェイス、IPv4 アドレス、IPv6 アドレス、または IPv4 プレフィックスを使用した **tunnel source** CLI コマンドをサポートします。新しい **tunnel source direct** CLI コマンドを使用すれば、直接接続された IP アドレス（物理インターフェイス、ポートチャネル、ループバック、SVI など）で IP-in-IP トンネルのカプセル化解除を設定できます。2つのスイッチ間に複数の IP リンクがある場合は、IPECMP リンクを選択できます。単一のトンネルインターフェイスは、外部宛先 IP がローカルで設定された IPv4 または IPv6 アドレスのいずれかであり、スイッチで動作的にアップ状態になっているようなトンネルパケットを、カプセル化解除できます。
 - 現在、**tunnel mode ipip decapsulate-any** は、IPv4 トランスポート（IPv4inIPv4 パケット）を介して IPv4 ペイロードをカプセル化解除するためにサポートされています。**tunnel mode ipv6ipv6 decapsulate-any** コマンドは、IPv6 トランスポートを介した IPv6 ペイロード（IPv6inIPv6 パケット）をサポートするために導入されました。
 - ネットワーク形成エンジン（NFE）を搭載した Cisco Nexus 9500 プラットフォームスイッチでは、**tunnel source direct** および **tunnel mode ipv6ipv6 decapsulate-any** CLI コマンドはサポートされていません。
 - **tunnel source direct** CLI コマンドがサポートされるのは、管理者が IP-in-IP カプセル化解除を使用して、パケットをネットワーク経由でソースルーティングする場合だけです。source-direct トンネルは、管理上シャットダウンされない限り、常に動作的にアップ状態です。直接接続されたインターフェイスは、**show ip route direct** CLI コマンドを使用して識別されます。
 - CLI コマンドは、カプセル化解除トンネルモード（and など）でのみサポートされます。**tunnel source direct tunnel mode ipip decapsulate-any tunnel mode ipv6ipv6 decapsulate-any**
 - source-direct の自動回復はサポートされていません。
 - ipv6ipv6 decapsulate-any の場合、inter-VRF はサポートされません。トンネルインターフェイス VRF（iVRF）と、トンネルトランスポートまたはフォワーディング VRF（fVRF）は、同じである必要があります。Cisco Nexus 9200、9300-EX、および 9300-FX プラットフォームスイッチと、EX および FX ラインカードを備えた Cisco Nexus 9500 プラットフォーム モジュラ スイッチには、VRF に関係なくカプセル化解除トンネルが 1 つだけ存在します。
 - ipv6ipv6 decap-any トンネルインターフェイスで IPv6 を有効にするには、有効な IPv6 アドレスを設定するか、トンネルインターフェイスで **ipv6 address use-link-local-only** を設定します。
- Cisco NX-OS リリース 10.4(1)F 以降では、ループバック インターフェイスで tunnel source CLI コマンドを使用して、ループバック IP アドレスをトンネル送信元 IP アドレスとして構成できます。
 - 送信元ダイレクトトンネルで対応可能な送信元の最大数と関連動作については、次のハードウェア制限を参照してください。

- 送信元直接トンネルは、ネットワーク転送エンジン (NFE)、アプリケーションスパインエンジン (ASE)、およびリーフスパインエンジン (LSE) を搭載した Cisco Nexus 9000 シリーズスイッチでサポートされるようになりましたほとんどの制限は、スケーリングされた SIP の場合に限り、インターフェイス上の IP/IPv6 アドレスの合計数にのみ適用されます。この場合のインターフェイスとは、L3、サブインターフェイス、PC、PC-サブインターフェイス、ループバック、SVI、および任意のセカンダリ IP/IPv6 アドレスを指します。

次の使用例を参照してください。

- 使用例 1：IP / IPv6 インターフェイス スケール数がより多い場合に SIP がインストールされたときの非決定的動作への対応。

両方のスイッチにトンネル SIP が 512 エントリがあります。トンネル送信元を使用する場合は、任意の IP または IPv6 アドレスを、**ipip or ipv6ipv6 decap any** により、上記のテーブルにインストールされたトンネル送信元にダイレクトします。

これらのエントリの挿入は、どのインターフェイス IP アドレスをインストールするかを制御する CLI コマンドを使用せずに、先着順に行われますシステムにインストールする IP/IPv6 インターフェイスの数が多い場合、動作は非決定的です (動作はインターフェイス フラップを使用して変更できます)。

- 使用例 2：両方のスイッチでスケール数が異なる場合。それぞれに長所と短所があります。

NFE を備えたスイッチの場合、IPv4 の個別のスケールはより大きくすることができますが (最大 512)、IPv6 と共有されます。ASE および LSE を備えたスイッチでは、IPv4 の個別のスケールは 256 までですが、IPv6 とは共有されません。

トンネル decap テーブルがいっぱいになると、TABLE_FULL エラーが表示されます。テーブルがいっぱいになった後でも、一部のエントリが削除されると、テーブルフルエラーはクリアされます。

表 17: スケール番号

コマンド	NFE を使用したスイッチ： テーブルサイズ 512、v4 は 1 エントリ、v6 は 4 エント リ	ASE および LSE を使用した スイッチ：テーブルサイ ズ 512、v4 は 1 エントリ、 v6 は 2 エントリ (ペアイン デックス)
トンネルソースダイレク トによる IPIP カプセル化 解除	v4 と v6 の間で共有、v6 は 4 エントリを取得 v4 + 4 * v6 = 512 最大エントリ数は 512 で、v6 エントリなし	専用で 256

コマンド	NFE を使用したスイッチ： テーブルサイズ 512 、 v4 は 1 エントリ、 v6 は 4 エントリ	ASE および LSE を使用した スイッチ：テーブルサイ ズ 512 、 v4 は 1 エントリ、 v6 は 2 エントリ（ペアイ ンデックス）
トンネルソースダイレク トによる IPv6IPv6 カプセル 化解除	v4 と v6 の間で共有、v6 は 4 エントリを取得 $v4 + 4 * v6 = 512$ 最大エントリ数は 128 で、v4 エントリなし	専用で 128

- 使用例 3：自動リカバリはサポートされていません。

上記のテーブルが使い果たされたためにハードウェアにエントリがインストールされない場合、すでにインストールされている IP/IPv6 をインターフェイスから削除すると、テーブルにスペースが生じますが、前に失敗した SIP がテーブルに自動的に追加されることはありません。トンネルインターフェイスまたは IP インターフェイスをフラップしてインストールする必要があります。

ただし、エントリが重複しているためにエントリがハードウェアにインストールされない場合（すでに 1 つのソースで **decap-any** が存在していて、**source direct tunnel CLI** コマンドを設定した場合、以前に設定されたソースのエントリは重複します）両方のトンネルが削除された場合にのみエントリを削除するように注意してください。

- Network Forwarding Engine (NFE) と Application Spine Engine (ASE) を備えた Cisco Nexus 9000 シリーズスイッチでは、専用の IPv4 および IPv6 のカプセル化解除が syslog に記録されるため、syslog は異なります。**tunnel-decap-table** がいっぱいの場合、ユーザは次のように syslog を取得します。

```
2017 Apr 6 12:18:04 switch %$ VDC-1 %$
%IPFIB-2-FIB_HW_IPV4_TUNNEL_DECAP_TABLE_FULL: IPv4 tunnel decap hardware table
full.
IP tunnel decapsulation may not work for some GRE/IPinIP traffic
```

```
2017 Apr 6 12:18:11 switch %$ VDC-1 %$
%IPFIB-2-FIB_HW_IPV6_TUNNEL_DECAP_TABLE_FULL: IPv6 tunnel decap hardware table
full.
IP tunnel decapsulation may not work for some GRE/IPinIP traffic
```

テーブルがいっぱいで、一部のエントリがテーブルから削除されるようになった場合（インターフェイスが動作上ダウンしているか、IP アドレスが削除されているため）、テーブルがクリアされたとの syslog が表示されます。トンネルを削除すると、そのトンネルの一部として追加されたすべてのエントリが削除されることに注意してください。

```
2017 Apr 5 13:29:25 switch %$ VDC-1 %$
%IPFIB-2-FIB_HW_IPV4_TUNNEL_DECAP_TABLE_FULL_CLRD: IPv4 tunnel decap hardware
```

```

table full exception cleared

2017 Apr 4 19:41:22 switch %$ VDC-1 %$
%IPFIB-2-FIB_HW_IPV6_TUNNEL_DECAP_TABLE_FULL_CLRD: IPv6 tunnel decap hardware
table full exception cleared

```

- IP-in-IP トンネルのカプセル化解除は、IPv6 対応ネットワークでサポートされます。

```

!
interface tunnel 1
  ipv6 address use-link-local-only          <<< enable IPv6
  tunnel mode ipv6ipv6 decapsulate-any
  tunnel source direct
  description IPinIP Decapsulation Interface
  mtu 1476
  no shutdown

```

- **internal** キーワードが付いている **show** マンドはサポートされていません。
- Cisco NX-OS は、次のプロトコルだけをサポートします。
 - IPv4 パッセンジャー プロトコル
 - GRE キャリア プロトコル
- Cisco NX-OS は、Cisco NX-OS リリース 9.3(3) よりも前のトンネルについては、次の最大数をサポートします。
 - IP トンネル : 8 トンネル
 - GRE および IP-in-IP 標準トンネル : 8 トンネル
- Cisco NX-OS リリース9.3(3) 以降、サポートされる GRE および IP-in-IP の通常トンネルの最大数は 16 です。
- アクセス コントロール リスト (ACL) または QoS ポリシーは IP トンネルでサポートされません。
- Cisco NX-OS は、IETF RFC 2784 に定義されている GRE ヘッダーをサポートします。Cisco NX-OS は、トンネル キーと IETF RFC 1701 のその他のオプションをサポートしません。
- Cisco NX-OS は、GRE トンネル キープアライブをサポートしません。
- すべてのユニキャストルーティング プロトコルが IP トンネルでサポートされます。
- IP トンネル インターフェイスは、SPAN 送信元または宛先には設定できません。
- IP トンネルは、PIM またはその他のマルチキャスト機能およびプロトコルをサポートしません
- Cisco NX-OS リリース 10.3(3)F 以降、PBR ポリシーに基づいて GRE または IP-in-IP トンネル宛先の選択がサポートされます。
- IP トンネルは、デフォルトの **system routing** モードでのみサポートされ、その他のモードではサポートされません

- トンネルインターフェイスを **ipip mode** に構成する場合、最大の mtu 値は 9196 です。
NX-OS 9.2(1) 以降のリリースから以前のリリースにダウングレードする場合、MTU 値が 9196 の **ipip mode** のトンネルインターフェイスを使用していると、ダウングレード操作の結果として MTU 構成が失われます。ベストプラクティスとしては、MTU 設定が失われることを回避するために、ダウングレードを開始する前に MTU 値を 9192 に調整します。
- トンネルインターフェイスを **ipip mode** に構成する場合、デフォルトの mtu 値は 1480 です。
NX-OS 9.2(1) 以降のリリースから以前のリリースにダウングレードする場合、明示的な MTU 構成のない **ipip mode** のトンネルインターフェイスを使用していると、ダウングレード操作の結果として MTU 値が 1480 から 1476 に変更されます。ベストプラクティスとしては、MTU 値が変更されることを回避するために、ダウングレードを開始する前に MTU 値を 1476 に調整します。
から NX-OS 9.2(1) 以降のリリースにアップグレードする場合、で、明示的な mtu 構成のない **ipip mode** のトンネルインターフェイスがあると、アップグレード操作の結果として MTU 値が 1476 から 1480 に変更されます。ベストプラクティスとしては、MTU 値が変更されることを回避するために、アップグレードを開始する前に MTU 値を 1480 に調整します。
- Cisco Nexus 9200 シリーズ スイッチでは、IP-in-IP トンネルで受信される GRE パケットが予想通りにドロップされず、パケット宛先に転送されます。
- スイッチから送信される Tx パケット（制御パケットなど）は、Tx 統計には含まれません。
- 別のトンネル経由で到達可能なトンネル宛先は、サポートされません。
- トンネル経由のルートについては整合性チェッカがサポートされません。
- 非 IP ルーティングプロトコル（isis など）は、IP-in-IP トンネル経由ではサポートされません。
- RFC5549 は、トンネル経由ではサポートされません。
- トンネル経由の BGP 隣接関係は、トンネルインターフェイスとトンネル入口が同じ VRF にあり（例：VRF-A）、トンネル出口が反対側からのルートリーク（例：VRF-B経由）で到達可能なシナリオでは、サポートされません。
- デバイスごとに設定できる GRE トンネルは 8 つだけです。
- GRE トンネルは RAACL をサポートしません。
- GRE トンネルは、基盤となるルーティングインフラストラクチャと同じ VRF に属している必要があります。つまり、*tunnel use-vrf* および *vrf member* の値は、同じ GRE トンネルで常に一致する必要があります。
- GRE トンネルは、限定されたトラフィック（入力または出力）カウンタのみをサポートします。

- レイヤ 3 FEX インターフェイスは、トンネルの入口または出口として許可されません。
- GRE トンネルでは二重カプセル化は許可されません。
- BFD は GRE トンネルではサポートされていません。
- Cisco Nexus N9K-C9300-GX プラットフォームでは、GRE/IPinIP トンネル インターフェイスは、Dot1Q タグ付き L2 bcast または 1Q タグ付き L2/L3 mcast 中継トラフィックと共存できません。Cisco Nexus N9300-GX プラットフォームで **feature tunnel** を設定すると、次の警告が表示され、syslog メッセージにも警告が記録されます。デバイスに Dot1Q タグ付き L2 bcast または 1Q タグ付き L2/L3 mcast 中継トラフィックがある場合は、**feature tunnel** を設定しないでください。

```
N9300-GX(config)# feature tunnel
WARN:GRE/IPinIP cannot coexist with 1Q tagged L2 bcast or 1Q tagged L2/L3 mcast
transit packets on this
platform
N9300-GX(config)#
N9300-GX(config)# show logging logfile
2019 Dec 12 00:41:08 N9300-GX %TUNNEL-2-TRAFFIC_WARNING: GRE/IPinIP cannot coexist
with 1Q
tagged L2 bcast or 1Q tagged L2/L3 mcast transit packets on this platform
N9300-GX(config)#
```

- Cisco Nexus 9000 スイッチの機能トンネル機能は、VXLAN 機能である機能 **nv オーバーレイ** と共存できません。
- Cisco Nexus 9200、9300-EX、9300-FX、9300-FX2 シリーズ スイッチ、および 9700-EX/FX ラインカードを搭載した Cisco Nexus 9500 プラットフォーム スイッチでは、複数のトンネル インターフェイスを、同じ IP アドレスを送信元または宛先とする単一の VRF に含めることはできません。たとえば、デバイスは、トンネル 0 およびトンネル 1 のインターフェイスを、同じ IP アドレスまたはインターフェイスを送信元とするデフォルト VRF に含めることはできません。
- vPC の Cisco Nexus 9300-EX、9300-FX、9300-GX、および Nexus 9500 プラットフォーム スイッチは、それぞれのトンネルの GRE トンネル エンドポイントとして機能できます。ただし、トンネルの宛先を vPC 経由にすることはできません。
- Cisco NX-OS リリース 10.3(3)F 以降、トンネル インターフェイスの PBR ポリシーは、Cisco Nexus 9300-FX2/FX3/GX/GX2 プラットフォーム スイッチの **gre ip**、**ipip ip**、および **ipip decapsulate-any ip** モードでのみサポートされます。

デフォルト設定

次の表に、IP トンネル パラメータのデフォルト設定を示します。

表 18: デフォルトの IP トンネル パラメータ

パラメータ	デフォルト
パス MTU ディスカバリ経過時間タイマー	10 分

パラメータ	デフォルト
パス MTU ディスカバリの最小 MTU	64
トンネル機能	ディセーブル

IP トンネルの設定



(注) Cisco IOS の CLI に慣れている場合、この機能に対応する Cisco NX-OS コマンドは通常使用する Cisco IOS コマンドと異なる場合がありますので注意してください。

トンネリングのイネーブル化

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

手順の概要

1. **configure terminal**
2. **feature tunnel**
3. **exit**
4. **show feature**
5. **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	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	feature tunnel 例 : <pre>switch(config)# feature tunnel switch(config-if)#</pre>	新しいトンネルインターフェイスを作成できます。 トンネルインターフェイス機能を無効にするには、このコマンドの no 形式を使用します。 (注) マルチキャストの重いテンプレートが適用されている場合、 feature tunnel コマンドはマルチキャスト機能を中断する可能性があります。

	コマンドまたはアクション	目的
ステップ 3	exit 例： switch(config-if)# exit switch#	インターフェイス モードを終了し、コンフィギュレーション モードに戻ります。
ステップ 4	show feature 例： switch(config-if)# show feature	(任意) デバイス上でイネーブルされている機能に関する情報を表示します。
ステップ 5	copy running-config startup-config 例： switch(config-if)# copy running-config startup-config	(任意) この設定の変更を保存します。

トンネル インターフェイスの作成

トンネル インターフェイスを作成して、この論理インターフェイスを IP トンネルに設定できます。



(注) Cisco NX-OS は、最大 8 つの IP トンネルをサポートしています。



- (注) トンネル インターフェイスおよび関連するすべての設定を削除するには、**no interface tunnel** コマンドを使用します。

コマンド	目的
no interface tunnel <i>number</i> 例： switch(config)# no interface tunnel 1	トンネル インターフェイスおよび関連する設定を削除します。
description <i>string</i> 例： switch(config-if)# description GRE tunnel	トンネルの説明を設定します。
mtu <i>value</i> 例： switch(config-if)# mtu 1400	インターフェイスで送信される IP パケットの MTU を設定します。
tunnel ttl <i>value</i> 例： switch(config-if)# tunnel ttl 100	トンネルの存続可能時間を設定します。範囲は 1 ～ 255 です。



- (注) トンネルの宛先の **use-vrf** とは異なるトンネル インターフェイス VRF を使用する GREv6 トンネルまたは IP-in-IP トンネルを設定することは、サポートされていません。トンネル インターフェイスとトンネルの宛先で同じ VRF を使用する必要があります。GREv4 では、トンネルの **use-vrf** とは異なるトンネル インターフェイス VRF の設定がサポートされています。

始める前に

異なる VRF でトンネル送信元およびトンネル宛先を設定できます。トンネリング機能がイネーブルになっていることを確認します。

手順の概要

1. **configure terminal**
2. **interface tunnel** *number*
3. **tunnel mode** {gre ip | ipip {ip | decapsulate-any}}
4. **tunnel source** {ip-address | interface-name}
5. **tunnel destination** ip {address | hostname} >
6. **tunnel use-vrf** *vrf-name*
7. **show interfaces tunnel** *number*
8. **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	configure terminal 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface tunnel number 例： switch(config)# interface tunnel 1 switch(config-if)#	新しいトンネル インターフェイスを作成します。
ステップ 3	tunnel mode {gre ip ipip {ip decapsulate-any}}	このトンネルモードを GRE、ipip、または ipip decapsulate-only に設定します。 IP での GRE カプセル化の使用を指定するには、 gre キーワードおよび ip キーワードを指定します。 ipip キーワードは、IP-in-IP カプセル化の使用を指定します。オプションの decapsulate-any キーワードは、トンネル インターフェイスの IP-in-IP トンネルを終了させます。このキーワードは、発信トラフィックを伝送しないトンネルを作成します。ただし、リモート トンネル エンド ポイントは、宛先として設定されたトンネルを使用できます。
ステップ 4	tunnel source {ip-address interface-name} 例： switch(config-if)# tunnel source ethernet 1/2	この IP トンネルの送信元アドレスを設定します。送信元は、IP アドレスまたは論理インターフェイス名によって指定できます。
ステップ 5	tunnel destination ip {address hostname} > 例： switch(config-if)# tunnel destination 192.0.2.1	この IP トンネルの宛先アドレスを設定します。宛先は、IP アドレスまたは論理ホスト名によって指定できます。
ステップ 6	tunnel use-vrf vrf-name 例： switch(config-if)# tunnel use-vrf blue	(任意) 設定された VRF をトンネルの IP 宛先アドレスの検索に使用します。
ステップ 7	show interfaces tunnel number 例： switch# show interfaces tunnel 1	(任意) トンネル インターフェイス 統計情報を表示します。
ステップ 8	copy running-config startup-config 例：	(任意) この設定の変更を保存します。

コマンドまたはアクション	目的
switch(config-if) # copy running-config startup-config	

例

次に、トンネル インターフェイスを作成する例を示します。

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

ネットマスクを使用した IP-in-IP トンネルの作成

ネットマスクを使用して IP-in-IP トンネルを作成すると、トンネル送信元サブネットおよびトンネル宛先サブネットを指定することと、一致するパケットのカプセル化を解除することが可能になります。

- IP-in-IP decap-any トンネルは、任意の数の IP-in-IP トンネルからカプセル化されたパケットを受信します。
- ネットマスク機能により、スイッチは、ネットマスクに適合する IP アドレスからのパケットを受信します。

ネットマスク機能に関する注意事項

- ルーティングプロトコルは、ネットマスクを使用して作成された IP-in-IP トンネルではサポートされません。
- カプセル化はネットマスク機能ではサポートされていません。同じサブネットの一連の送信元からのカプセル化解除だけがサポートされています。

手順の概要

1. **configure terminal**
2. **interface tunnel *number***
3. **tunnel mode ipip [*ip*]**
4. **tunnel source *ip-address / mask_length***
5. **tunnel destination *ip-address / mask_length***
6. (任意) **no shut**
7. **ip address *ip-prefix/length***

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface tunnel number 例： switch(config)# interface tunnel 5 switch(config-if)#	新しいトンネル インターフェイスを作成します。
ステップ 3	tunnel mode ipip [ip]	このトンネル モードを ipip に設定します。 ipip キーワードは、IP-in-IP カプセル化の使用を指定します。
ステップ 4	tunnel source ip-address / mask_length 例： switch(config-if)# tunnel source 33.1.1.1 255.255.255.0	この IP トンネルの送信元アドレスを設定します。送信元は、IP アドレスとマスクの長さによって指定されます。
ステップ 5	tunnel destination ip-address / mask_length 例： switch(config-if)# tunnel destination 33.1.1.2 255.255.255.0	この IP トンネルの宛先アドレスを設定します。宛先は、IP アドレスとマスクの長さによって指定されます。
ステップ 6	(任意) no shut	インターフェイスを消去します。
ステップ 7	ip address ip-prefix/length 例： switch(config-if)# ip address 50.1.1.1/24	このインターフェイスの IP アドレスを設定します。

例

次に、ネットマスクを使用して IP-in-IP トンネルを作成する例を示します。

```
switch(config)# interface tunnel 10
switch(config-if)# tunnel mode ipip
switch(config-if)# tunnel source 33.1.1.2/24
switch(config-if)# tunnel destination 33.1.1.1/24
switch(config-if)# no shut
switch(config-if)# ip address 10.10.10.10/24
switch(config-if)# end
switch# show interface tunnel 10
Tunnel10 is up
  Admin State: up
  Internet address is 10.10.10.10/24
  MTU 1476 bytes, BW 9 Kbit
```

```
Tunnel protocol/transport IPIP/IP
Tunnel source 33.1.1.2, destination 33.1.1.1
Transport protocol is in VRF "default"
Last clearing of "show interface" counters never
Tx
0 packets output, 0 bytes
Rx
0 packets input, 0 bytes

switch# show run interface tunnel 10

!Command: show running-config interface Tunnell10
!Time: Wed Aug 26 13:50:01 2015

version 7.0(3)I2(1)

interface Tunnell10
 ip address 10.10.10.10/24
 tunnel mode ipip ip
 tunnel source 33.1.1.2 255.255.255.0
 tunnel destination 33.1.1.1 255.255.255.0
 no shutdown
```

トンネルインターフェイスの設定

トンネルインターフェイスを GRE トンネルモード、**ipip** モード、または **ipip** カプセル化解除モードに設定できます。GRE モードはデフォルトのトンネルモードです。

Cisco NX-OS Release 7.0(3)I6(1) 以降、**tunnel source direct** および **tunnel mode ipv6ipv6 decapsulate-any** CLI コマンドが Cisco Nexus 9000 シリーズスイッチでサポートされています。

tunnel source direct および **tunnel mode ipv6ipv6 decapsulate-any** CLI コマンドは、Cisco Nexus 9000 シリーズスイッチでサポートされています。



- (注) Network Forwarding Engine (NFE) を搭載した Cisco Nexus 9500 プラットフォームスイッチでは、**tunnel source direct** および **tunnel mode ipv6ipv6 decapsulate-any** CLI コマンドはサポートされていません。

IPv6 トランスポート (IPv6inIPv6 パケット) を介した IPv6 ペイロードをサポートするために、新しい CLI **tunnel mode ipv6ipv6 decapsulate-any** コマンドが導入されました。新しい CLI **tunnel source direct** コマンドを使用すれば、直接接続された IP アドレス (物理インターフェイス、ポートチャネル、ループバック、SVI など) で IP-in-IP トンネルのカプセル化解除を設定できます。

始める前に

トンネリング機能がイネーブルになっていることを確認します。

手順の概要

1. configure terminal

2. **interface tunnel** *number*
3. **tunnel mode** {gre ip | ipip | {ip | decapsulate-any}}
4. (任意) **tunnel mode ipv6ipv6 decapsulate-any**
5. **tunnel source direct**
6. **show interfaces tunnel** *number*
7. **mtu** *value*
8. **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	configure terminal 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface tunnel <i>number</i> 例： switch(config)# interface tunnel 1 switch(config-if)#	新しいトンネル インターフェイスを作成します。
ステップ 3	tunnel mode {gre ip ipip {ip decapsulate-any}}	このトンネルモードを GRE、ipip、または ipip decapsulate-only に設定します。 IP での GRE カプセル化の使用を指定するには、 gre キーワードおよび ip キーワードを指定します。 ipip キーワードは、IP-in-IP カプセル化の使用を指定します。オプションの decapsulate-any キーワードは、トンネル インターフェイスの IP-in-IP トンネルを終了させます。このキーワードは、発信トラフィックを伝送しないトンネルを作成します。ただし、リモート トンネル エンド ポイントは、宛先として設定されたトンネルを使用できます。
ステップ 4	(任意) tunnel mode ipv6ipv6 decapsulate-any	IPv6 トランスポートを介した IPv6 ペイロード (IPv6 パケット) をサポートします (7.0(3)I6(1) 以降)。この手順は、IPv6 ネットワークにのみ適用されます。 (注) このコマンドは、Cisco Nexus 9500-GX プラットフォーム スイッチではサポートされていません。
ステップ 5	tunnel source direct	直接接続されている IP アドレスで IP-in-IP トンネルのカプセル化解除を設定します。このオプションは、IP-in-IP カプセル化解除を使用してネットワー

	コマンドまたはアクション	目的
		<p>ク経由でパケットを送信する場合にのみサポートされるようになりました。</p> <p>(注) このコマンドは、Network Forwarding Engine (NFE) を備えた Cisco Nexus 9500 プラットフォームスイッチではサポートされません。</p>
ステップ 6	show interfaces tunnel number 例 : <pre>switch(config-if)# show interfaces tunnel 1</pre>	(任意) トンネルインターフェイス統計情報を表示します。
ステップ 7	mtu value	<p>インターフェイスで送信される IP パケットの Maximum Transmission Unit (MTU; 最大伝送単位) を設定します。</p> <p>有効な範囲は 64 ~ 9192 ユニットです。</p> <p>(注) tunnel mode ipip を設定する場合、その範囲は NX-OS のリリースによって異なります。</p> <ul style="list-style-type: none"> • 64 ~ 9192 ユニット • 64 ~ 9196 ユニット
ステップ 8	copy running-config startup-config 例 : <pre>switch(config-if)# copy running-config startup-config</pre>	(任意) この設定の変更を保存します。

例

次に、GRE へのトンネルインターフェイスを作成する例を示します。

```
switch# configure terminal
switch(config)# interface tunnel 1
switch(config-if)# tunnel mode gre ip
switch(config-if)# copy running-config startup-config
```

次に、ipip トンネルを作成する例を示します。

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

次に、直接接続された IP アドレスで IP-in-IP トンネルのカプセル化解除を設定する例を示します。

```
switch# configure terminal
switch(config)# interface tunnel 0
switch(config-if)# tunnel mode ipip ip
switch(config-if)# tunnel source direct
switch(config-if)# description IPinIP Decapsulation Interface
switch(config-if)# no shut
```

次に、IPv6 対応ネットワークで IP-in-IP トンネルのカプセル化解除を設定する例を示します。

```
!
interface tunnel 1
  ipv6 address use-link-local-only          <<< enable IPv6
  tunnel mode ipv6ip6 decapsulate-any
  tunnel source direct
  description IPinIP Decapsulation Interface
  mtu 1476
  no shutdown

show running-config interface tunnel 1
interface Tunnell
  tunnel mode ipv6ip6 decapsulate-any
  tunnel source direct
  no shutdown

show interface tunnel 1
Tunnell is up    Admin State: up
MTU 1460 bytes, BW 9 Kbit
Tunnel protocol/transport IPv6/DECAPANY/IPv6
Tunnel source - direct
Transport protocol is in VRF "default"
Tunnel interface is in VRF "default"
Last clearing of "show interface" counters never
Tx    0 packets output, 0 bytes    Rx    0 packets input, 0 bytes
```

GRE トンネルの設定

トンネル インターフェイスを GRE トンネル モードに設定できます。



(注) Cisco NX-OSは、IPV4 over IPV4のGREプロトコルのみをサポートします。

始める前に

トンネリング機能がイネーブルになっていることを確認します。

手順の概要

1. **configure terminal**
2. **interface tunnel *number***

3. **tunnel mode gre ip**
4. **show interfaces tunnel number**
5. **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	configure terminal 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface tunnel number 例： switch(config)# interface tunnel 1 switch(config-if)#	新しいトンネル インターフェイスを作成します。
ステップ 3	tunnel mode gre ip 例： switch(config-if)# tunnel mode gre ip	このトンネル モードを GRE に設定します。
ステップ 4	show interfaces tunnel number 例： switch(config-if)# show interfaces tunnel 1	(任意) トンネルインターフェイス統計情報を表示します。
ステップ 5	copy running-config startup-config 例： switch(config-if)# copy running-config startup-config	(任意) この設定の変更を保存します。

Path MTU Discovery のイネーブル化

tunnel path-mtu discovery コマンドを使用し、トンネルのパスMTUディスカバリをイネーブルにします。

手順の概要

1. **tunnel path-mtu-discovery age-timer min**
2. **tunnel path-mtu-discovery min-mtu bytes**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	tunnel path-mtu-discovery age-timer min 例：	トンネル インターフェイスで Path MTU Discovery (PMTUD) をイネーブルにします。

	コマンドまたはアクション	目的
	<code>switch(config-if)# tunnel path-mtu-discovery age-timer 25</code>	<ul style="list-style-type: none"> • min : 分数。指定できる範囲は 10 ~ 30 です。デフォルトは 10 です。
ステップ 2	tunnel path-mtu-discovery min-mtu bytes 例 : <code>switch(config-if)# tunnel path-mtu-discovery min-mtu 1500</code>	トンネルインターフェイスで Path MTU Discovery (PMTUD) をイネーブルにします。 <ul style="list-style-type: none"> • bytes : 認識された最小 MTU。範囲は 64~9192 です。デフォルトは 64 です。

トンネルインターフェイスへの VRF メンバーシップの割り当て

VRF にトンネルインターフェイスを追加できます。

始める前に

トンネリング機能がイネーブルになっていることを確認します。

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

手順の概要

1. **configure terminal**
2. **interface tunnel number**
3. **vrf member vrf-name**
4. **ip address ip-prefix/length**
5. **show vrf [vrf-name] interface interface-type number**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <code>switch# configure terminal</code> <code>switch(config)#</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	interface tunnel number 例 : <code>switch(config)# interface tunnel 0</code> <code>switch(config-if)#</code>	インターフェイス設定モードを開始します。
ステップ 3	vrf member vrf-name 例 :	このインターフェイスを VRF に追加します。

	コマンドまたはアクション	目的
	<code>switch(config-if)# vrf member RemoteOfficeVRF</code>	
ステップ 4	ip address <i>ip-prefix/length</i> 例： <code>switch(config-if)# ip address 192.0.2.1/16</code>	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	show vrf [<i>vrf-name</i>] interface <i>interface-type number</i> 例： <code>switch(config-vrf)# show vrf Enterprise interface tunnel 0</code>	(任意) VRF 情報を表示します。
ステップ 6	copy running-config startup-config 例： <code>switch# copy running-config startup-config</code>	(任意) この設定の変更を保存します。

例

次に、VRF にトンネルインターフェイスを追加する例を示します。

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

IP トンネル設定の確認

IP トンネルの設定情報を確認するには、次のいずれかの作業を行います。

コマンド	目的
show interface tunnel <i>number</i>	トンネルインターフェイスの設定を表示します (MTU、プロトコル、転送、および VRF)。入力および出力パケット、バイト、およびパケット レートを表示します。
show interface tunnel <i>number brief</i>	トンネルインターフェイスの動作状態、IP アドレス、カプセル化のタイプ、MTU を表示します。

コマンド	目的
show interface tunnel number counters	入出力パケットのインターフェイス カウンタを表示します。 (注) インターフェイスカウンタとともに表示されるバイトカウントには、内部ヘッダーサイズが含まれます。
show interface tunnel number description	トンネル インターフェイスに設定された説明を表示します。
show interface tunnel number status	トンネル インターフェイスの動作ステータスを表示します。
show interface tunnel number status err-disabled	トンネル インターフェイスの errdisable 状態を表示します。

IP トンネリングの設定例

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

ルータ A :

```
feature tunnel
interface tunnel 0
ip address 209.165.20.2/8
tunnel source ethernet 1/2
tunnel destination 192.0.2.2
tunnel mode gre ip
tunnel path-mtu-discovery 25 1500

interface ethernet 1/2
ip address 192.0.2.55/8
```

ルータ B :

```
feature tunnel
interface tunnel 0
ip address 209.165.20.1/8
tunnel source ethernet 2/1
tunnel destination 192.0.2.55
tunnel mode gre ip

interface ethernet 2/1
ip address 192.0.2.2/8
```

関連資料

関連項目	マニュアルタイトル
IP トンネル コマンド	『Cisco Nexus 9000 Series NX-OS Interfaces Command Reference』



第 10 章

Q-in-Q VLAN トンネルの設定

- [Q-in-Q トンネルについて \(401 ページ\)](#)
- [Q-in-Q トンネリングおよびレイヤ2プロトコルトンネリングの注意事項と制約事項 \(408 ページ\)](#)
- [複数プロバイダー VLAN を使用した選択的 Q-in-Q の注意事項と制約事項 \(410 ページ\)](#)
- [VLAN 上のポート VLAN マッピングに関する注意事項と制限事項 \(412 ページ\)](#)
- [Q-in-Q トンネルおよびレイヤ2プロトコルトンネリングの設定 \(413 ページ\)](#)
- [複合アクセス ポート機能セットの設定 \(423 ページ\)](#)
- [Q-in-Q 設定の確認 \(425 ページ\)](#)
- [Q-in-Q およびレイヤ2プロトコルトンネリングの設定例 \(426 ページ\)](#)
- [VLAN 上のポート VLAN マッピングの構成 \(427 ページ\)](#)

Q-in-Q トンネルについて

この章では、Cisco NX-OS デバイス上で IEEE 802.1Q-in-Q VLAN トンネルおよびレイヤ2 プロトコルトンネリングを設定する方法について説明します。

Q-in-Q VLAN トンネルを使用することで、サービスプロバイダーは第2の 802.1Q タグをすでにタグ付けされたフレームに追加して、カスタマーに内部使用の VLAN をすべて提供しながら、インフラストラクチャ内で異なるカスタマーのトラフィックを分離することができます。

Q-in-Q トンネリング

サービスプロバイダーのビジネスカスタマーには、多くの場合、サポートする VLAN ID および VLAN の数に固有の要件があります。同一サービスプロバイダネットワークのさまざまなカスタマーが必要とする VLAN 範囲は重複し、インフラストラクチャを通るカスタマーのトラフィックは混合してしまふことがあります。カスタマーごとに一意の VLAN ID 範囲を割り当てると、カスタマーの設定が制限され、802.1Q 仕様の VLAN に関する上限 (4096 個) を容易に超えてしまいます。

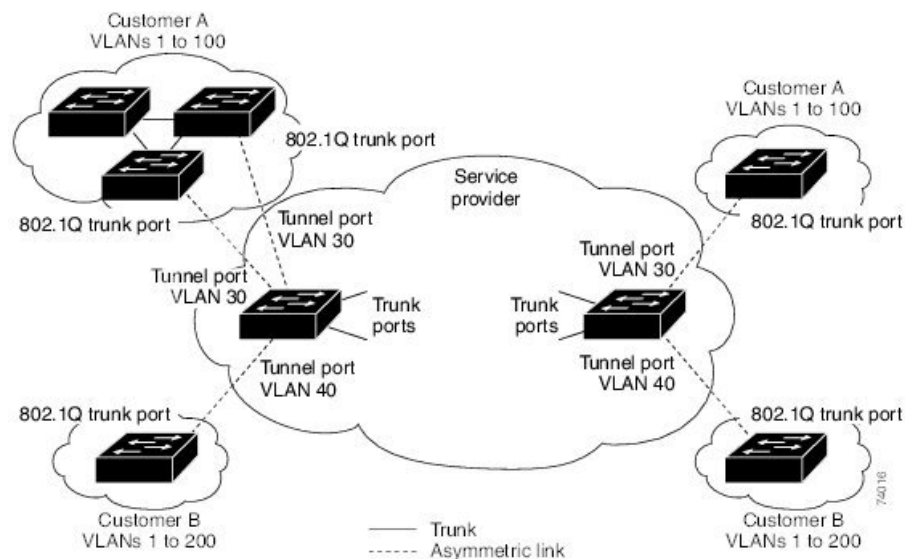


- (注) Q-in-Q は、ポート チャンネルでサポートされています。非対称リンクとしてポート チャンネルを設定するには、ポートチャンネル内のすべてのポートが同じトンネリング設定でなければなりません。

サービス プロバイダは、802.1Q トンネリング機能を使用すると、単一の VLAN を使用して、複数の VLAN を含む顧客をサポートできます。サービスプロバイダーのインフラストラクチャ上で顧客 VLAN ID が保持され、同じ VLAN 上に存在するように見えても、異なる顧客からのトラフィックが分離されます。IEEE 802.1Q トンネリングは、VLAN-in-VLAN 階層構造およびタグ付きパケットへのタグgingによって、VLAN スペースを拡張します。802.1Q トンネリングをサポートするように設定されたポートは、トンネルポートといます。トンネリングを設定する場合、トンネリング専用の VLAN にトンネルポートを割り当てます。顧客ごとに個別の VLAN が必要ですが、その VLAN は顧客の VLAN をすべてサポートします。

適切な VLAN ID で通常どおりにタグ付けされた顧客のトラフィックは、顧客デバイス の 802.1Q トランク ポートからサービス プロバイダー側のエッジスイッチのトンネルポートに発信されます。顧客 デバイスとエッジスイッチの間のリンクは、一方の端が 802.1Q トランク ポート、反対側がトンネルポートとして設定されているので、非対称リンクです。それぞれの顧客に固有のアクセス VLAN ID には、トンネルポートインターフェイスを割り当てます。以下の図を参照してください。

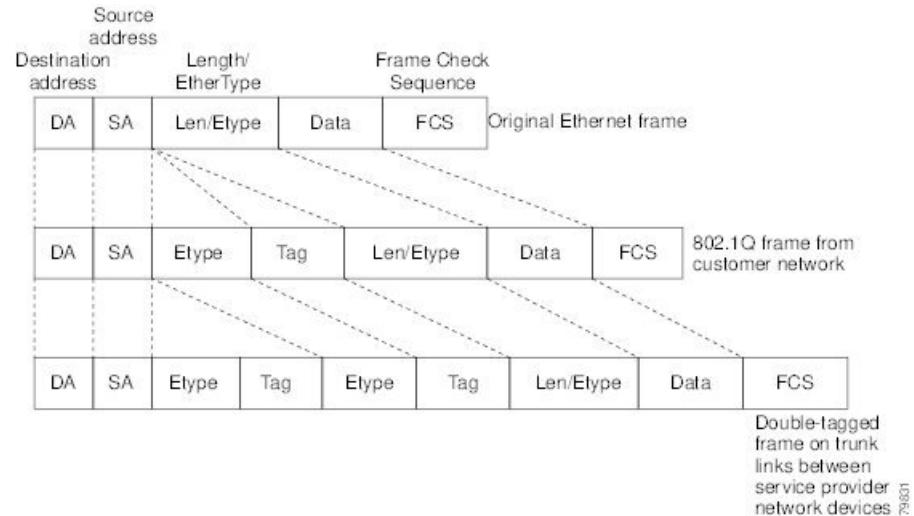
図 30: 802.1Q-in-Q トンネルポート



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

外部タグには、カスタマーの（サービスプロバイダーによって割り当てられた）アクセス VLAN ID が含まれます。（カスタマーによって割り当てられた）内部タグの VLAN ID は、受信トラフィックの VLAN です。この二重タグgingは、以下の図に示すようにタグスタック構成 Double-Q または Q-in-Q と呼ばれます。

図 31: タグなし、802.1Q タグ付き、および二重タグ付きイーサネットフレーム



この方法で、外部タグの VLAN ID スペースは内部タグの VLAN ID スペースに依存しません。単一の外部 VLAN ID は、個々のカスタマーの全体の VLAN ID スペースを表すことができます。この方法により、カスタマーのレイヤ2ネットワークをサービスプロバイダーネットワーク全体に拡張して、複数のサイトに仮想 LAN インフラストラクチャを作成することも可能になります。



(注) 階層型タグging、すなわちマルチレベルの dot1q タグging Q-in-Q はサポートされていません。

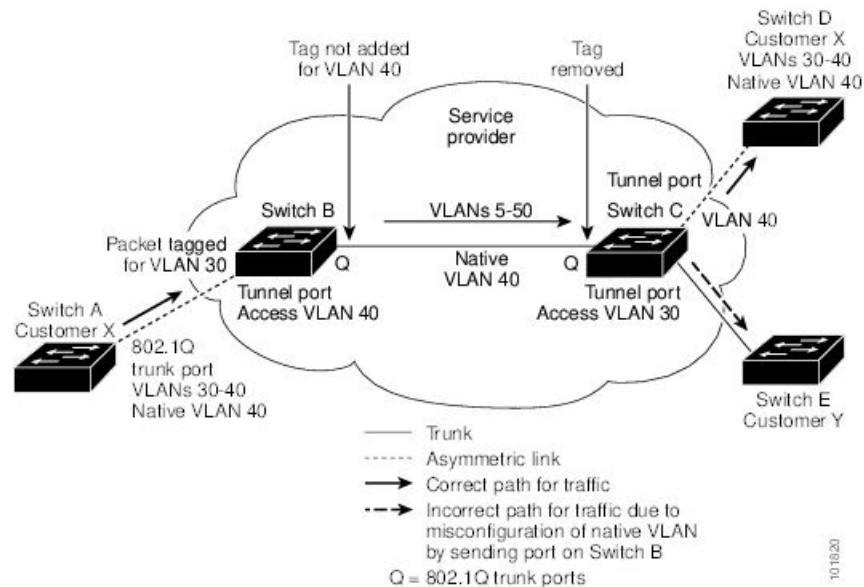
ネイティブ VLAN のリスク

エッジスイッチで 802.1Q トンネリングを設定する場合は、サービスプロバイダーネットワークにパケットを送信するために、802.1Q トランクポートを使用する必要があります。ただし、サービスプロバイダーネットワークのコアを通過するパケットは、802.1Q トランク、ISL トランク、または非トランッキングリンクで伝送される場合があります。802.1Q トランクをこれらのコアスイッチで使用する場合には、802.1Q トランクのネイティブ VLAN を、同じスイッチ上の dot1q トンネルポートのどのネイティブ VLAN にも一致させないでください。ネイティブ VLAN 上のトラフィックが 802.1Q 送信トランクポートでタグ付けされなくなるためです。

下の図の VLAN 40 は、サービスプロバイダーネットワークの入力エッジスイッチ（スイッチ B）において、カスタマー X からの 802.1Q トランクポートのネイティブ VLAN として設定されています。カスタマー X のスイッチ A は、VLAN 30 のタグ付きパケットを、アクセス VLAN 40 に属する、サービスプロバイダネットワークのスイッチ B の入力トンネルポートに

送信します。トンネル ポートのアクセス VLAN (VLAN 40) は、エッジスイッチのトランクポートのネイティブ VLAN (VLAN 40) と同じなので、トンネルポートから受信したタグ付きパケットに 802.1Q タグは追加されません。パケットには VLAN 30 タグだけが付いて、サービスプロバイダー ネットワークで出力エッジスイッチ (スイッチ C) のトランクポートに送信され、出力スイッチ トンネルによってカスタマー Y に間違えて送信されます。

図 32: ネイティブ VLAN のリスク



ネイティブ VLAN の問題を解決する方法は2つあります。

- 802.1Q トランクから出るすべてのパケット (ネイティブ VLAN を含む) が、`vlan dot1q tag native` コマンドを使用してタグ付けされるように、エッジスイッチを設定します。すべての 802.1Q トランクでネイティブ VLAN パケットにタグを付けるようにスイッチを設定した場合、スイッチはタグなしパケットを受信しますが、タグ付きパケットだけを送信します。



(注) `vlan dot1q tag native` コマンドは、すべてのトランクポート上のタグリング動作に影響を与えるグローバルコマンドです。

- エッジスイッチのトランクポートのネイティブ VLAN ID が、カスタマー VLAN 範囲に属さないようにします。たとえばトランクポートが VLAN100 ~ 200 のトラフィックを運ぶ場合は、この範囲以外の番号をネイティブ VLAN に割り当てます。

レイヤ2 プロトコルのトンネリングについて

サービスプロバイダーネットワーク経由で接続される複数のサイトのカスタマーは、さまざまなレイヤ2 プロトコルを実行して、すべてのリモートサイトおよびローカルサイトを含むようにトポロジを拡大する必要があります。スパンニングツリープロトコル (STP) が適切に稼働

している必要があります。すべての VLAN で、ローカル サイトおよびサービスプロバイダー インフラストラクチャ経由のすべてのリモート サイトを含む、適切なスパニングツリーを構築する必要があります。Cisco Discovery Protocol (CDP) は、ローカルおよびリモート サイトから隣接するシスコ デバイスを検出することができる必要があります。VLAN トランッキング プロトコル (VTP) は、カスタマー ネットワークのすべてのサイトを通して一貫した VLAN 設定を提供する必要があります。

トンネルポートでマルチタグ付き BPDU を許可するようにスイッチを設定できます。`l2protocol tunnel allow-double-tag` コマンドをイネーブルにすると、複数のタグが付けられたカスタマー BPDU がトンネルポートに入ると、カスタマー トラフィックからの元の 802.1Q タグが保持され、外部 VLAN タグ (サービス プロバイダーによって割り当てられたカスタマー アクセス VLAN ID) が追加されます。カプセル化されたパケットに含まれています。したがって、サービス プロバイダー インフラストラクチャに着信するパケットは複数のタグが付けられます。BPDU がサービス プロバイダー ネットワークを離れると、外部タグが削除され、元の複数のタグが付けられた BPDU がカスタマー ネットワークに送信されます。

プロトコルトンネリングがイネーブルになると、サービスプロバイダーインフラストラクチャの受信側にあるエッジスイッチが、レイヤ2プロトコルを特別の MAC アドレスでカプセル化し、サービスプロバイダー ネットワークの端まで送信します。ネットワークのコアスイッチでは、このパケットが処理されずに通常のパケットとして転送されます。CDP、STP、または VTP のブリッジプロトコル データ ユニット (BPDU) は、サービスプロバイダー インフラストラクチャを通過し、サービスプロバイダー ネットワークの発信側にあるカスタマー スイッチまで配信されます。同一パケットは同じ VLAN のすべてのカスタマー ポートで受信されます。

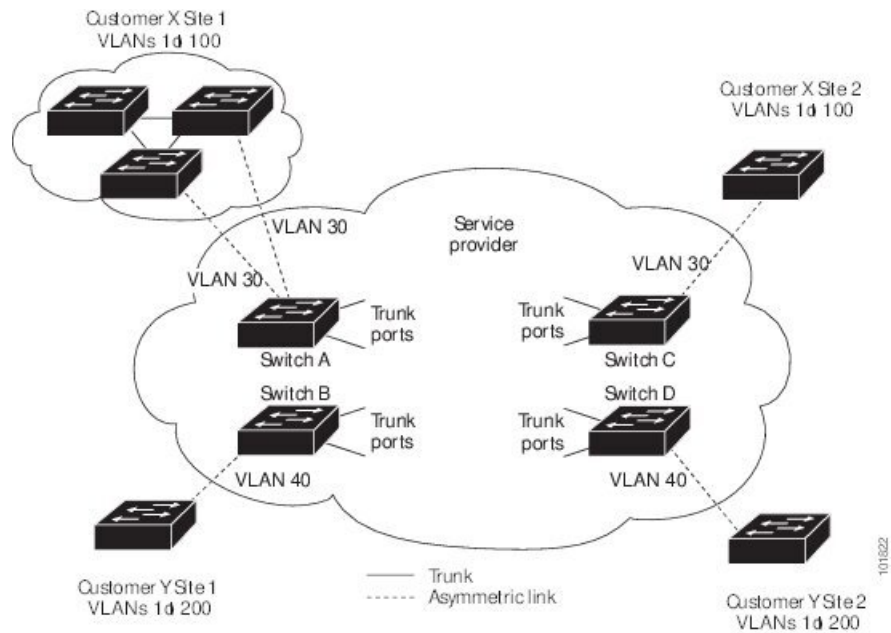
802.1Q トンネリングポートでプロトコルのトンネリングをイネーブルにしていない場合、サービスプロバイダー ネットワークの受信側のリモート スイッチでは BPDU を受信せず、STP、CDP、802.1X、および VTP を適切に実行できません。プロトコルのトンネリングがイネーブルである場合、それぞれのカスタマーネットワークのレイヤ2プロトコルは、サービスプロバイダー ネットワーク内で動作しているものから完全に区別されます。802.1Q トンネリングでサービスプロバイダーネットワークを通してトラフィックを送信する、さまざまなサイトのカスタマー スイッチでは、カスタマー VLAN が完全に認識されます。



- (注) レイヤ2プロトコルのトンネリングは、ソフトウェアでBPDUをトンネリングすることで動作します。スーパーバイザが受信する多数のBPDUによりCPUの負荷が大きくなります。スーパーバイザCPUの負荷を軽減するために、Software レートリミッタを使用する必要がある場合があります。[レイヤ2プロトコルトンネルポートのしきい値の設定 \(422ページ\)](#) を参照してください。

たとえば、以下の図で、カスタマー X には、サービスプロバイダー ネットワークを介して接続された同じ VLAN に 4 台のスイッチがあります。ネットワークが BPDU をトンネリングしないと、ネットワークの遠端のスイッチは STP、CDP、802.1X、および VTP プロトコルを正しく実行できません。

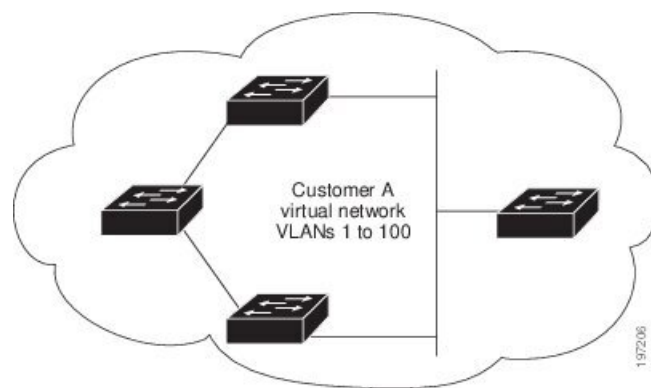
図 33: レイヤ 2 プロトコル トンネリング



前の例では、カスタマー X、サイト 1 のスイッチ上の VLAN で動作する STP は、カスタマー X、サイト 2 のスイッチに基づくコンバージェンスパラメータを考慮せずに、このサイトのスイッチのスパニングツリーを構築します。

以下の図は、BPDU トンネリングがイネーブルになっていない場合の、カスタマーのネットワークでの結果トポロジを示します。

図 34: BPDU トンネリングを使用しない仮想ネットワーク トポロジ



複数プロバイダー VLAN を使用した選択的 Q-in-Q

複数プロバイダー VLAN を使用する選択的 Q-in-Q は、ポート上のユーザ固有の範囲のカスタマー VLAN を 1 つの特定のプロバイダー VLAN に関連付けることができるトンネリング機能であり、ポート上で複数のカスタマー VLAN をプロバイダー VLAN にマッピングできます。ポートに設定されたカスタマー VLAN のいずれかに一致する VLAN タグが付いたパケットは、

サービスプロバイダー VLAN のプロパティを使用して VLAN ファブリック全体でトンネリングされます。カプセル化パケットは、内部パケットのレイヤ 2 ヘッダーの一部としてカスタマー VLAN タグを伝送します。

VLAN のポート VLAN マッピングについて (着信 VLAN の変換)

サービスプロバイダーに、同じ VLAN カプセル化を使用して同じ物理スイッチに接続している複数の顧客があるものの、それらが同じ Layer 2 セグメント上に存在しない場合には、着信 VLAN を一意の VLAN/VNI に変換することが、セグメントを拡張する正しい方法です。

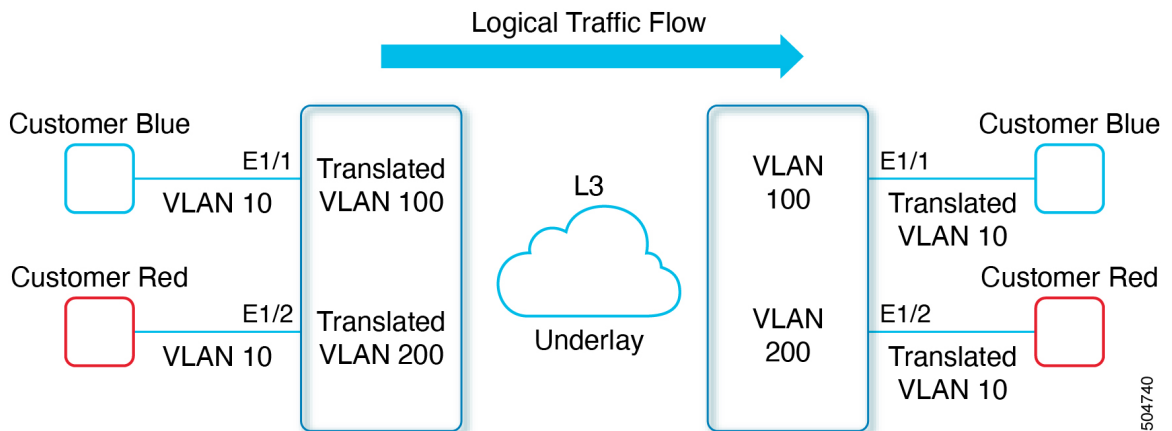
Cisco NX-OS リリース 10.3(3)F 以降、VXLAN VLAN 以外のポート VLAN マッピングは、Cisco Nexus 9300-EX/FX/FX2/FX3/GX/GX2、C9408 プラットフォームスイッチ、および 9700-EX/FX/GX ラインカードを搭載した Cisco Nexus 9500 スイッチでサポートされます。

次の図では、Blue と Red がカプセル化として VLAN 10 を使用してリーフに接続しています。

この例では、Customer Blue の VLAN 10 (インターフェイス E1/1) が VLAN 100 にマッピング/変換され、Customer Red の VLAN 10 (インターフェイス E1/2) が VLAN 200 にマッピングされます。

もう一方のリーフでは、このマッピングが逆に適用されます。着信 VLAN 100 はインターフェイス E1/1 の VLAN 10 にマッピングされ、VLAN 200 はインターフェイス E1/2 の VLAN 10 にマッピングされます。

図 35: 論理的トラフィックフロー



504740

入力 (着信) VLAN とポートにあるローカル (変換先) VLAN との間での VLAN 変換を設定できます。VLAN 変換が有効にされたインターフェイスに到着するトラフィックにおいて、着信 VLAN は変換された VLAN にマッピングされます。

アンダーレイ上で、内部 dot1q が削除され、VXLAN ネットワーク以外に切り替えられます。VLAN 変換が設定された発信インターフェイスで、トラフィックは元の VLAN に変換されてから出力されます。トラフィックカウンタについては、入力 VLAN ではなく、変換先 VLAN にある VLAN カウンタを参照してください。

Q-in-Q トンネリングおよびレイヤ2 プロトコル トンネリングの注意事項と制約事項

Q-in-Q トンネリングおよびレイヤ2 トンネリングには、次の設定に関するガイドラインと制約事項があります。

- Q-in-Q は、サービス プロバイダーのエッジデバイスのカスタマー側インターフェイスで設定する必要があります。イーサネットフレームが Cisco Nexus 9000 シリーズ スイッチに入力されると、スイッチは 1 つの転送決定内で 2 つの 802.1Q ヘッダーを持つフレームをカプセル化できません。同様に、Q-in-Q カプセル化イーサネットフレームが 802.1Q ヘッダーのない Cisco Nexus 9000 シリーズ スイッチを出力する必要がある場合、スイッチは単一の転送決定内でイーサネット フレームから 2 つの 802.1Q ヘッダーをカプセル化解除できません。
- 複数の VLAN のマッピングがサポートされています。
- マルチタグ付き BPDU は、Cisco Nexus 93108TC-EX および 93180YC-EX スイッチでサポートされています。最大 3 つのタグをサポートしています。
- マルチタグ付きの BPDU では選択的 Q-in-Q トンネリングはサポートされません。
- マルチタグ付き CDP および STP BPDU のみがサポートされます。
- 最も内側のタグは常に 0x8100 である必要があります。
- 複数の選択的 Q-in-Q タグはサポートされていません。つまり、Q-in-Q は単一のインターフェイスで複数の SP タグをサポートしません。
- サービスプロバイダー ネットワーク内のスイッチは、Q-in-Q タギングによる MTU サイズの増加に対応するように設定する必要があります。
- Q-in-Q タグ付きパケットの MAC アドレス ラーニングは、外部 VLAN (サービス プロバイダー VLAN) タグに基づいています。単一の MAC アドレスが複数の内部 (カスタマー) VLAN で使用される配置においては、パケット転送の問題が発生する場合があります。
- レイヤ3 以上のパラメータは、トンネルトラフィックでは識別できません (レイヤ3宛先や送信元アドレスなど)。トンネル型トラフィックはルーティングできません。
- または **system dot1q-tunnel transit** または **system dot1q-tunnel transit vlan provider_vlan_list** コマンドには、次の制限があります。
 - MPLS、GRE、および IP-in-IP 機能は、これらのコマンドがスイッチで構成されている場合、Q-in-Q トンネリング機能と組み合わせて効果的に機能しません。
 - vPC スイッチで Q-in-Q トンネリング機能が有効になっている場合は、これらのコマンドを構成する必要があります。
 - これらのコマンドは、デバイスが Q-in-Q、選択的 Q-in-Q、および複数のプロバイダ VLAN 機能を備えた選択的 Q-in-Q で構成される場合、Cisco Nexus

9300-EX/FX/FX2/FX3/GX/GX2 スイッチおよび9700-EX/FX/GX ラインカードを備えた9500 でサポートされます。

- これらのコマンドが構成されている場合、ポートのネイティブVLANであっても、トランクポートを出るレイヤ2 フレームは常にタグ付けされます。
- Cisco Nexus 9000 シリーズのデバイスは、トンネルトラフィックに対するMAC レイヤ ACL/QoS (VLAN ID および送信元/宛先 MAC アドレス) のみを提供できます。
- MAC アドレスに基づくフレーム配布を使用する必要があります。
- 非対称リンクでは1つのポートだけがトラッキングするため、Dynamic Trunking Protocol (DTP) をサポートしません。無条件でトランクになるように、非対称リンクの802.1Q トランクポートを設定する必要があります。
- プライベートVLANをサポートするように設定されたポートに802.1Q トンネリング機能を設定することはできません。プライベートVLANは、これらの導入には必要ではありません。
- トンネルVLANのIGMP スヌーピングをディセーブルにする必要があります。
- ネイティブVLANでのタグgingを維持し、タグなしトラフィックを廃棄するには、`vlan dot1q tag native` コマンドを入力する必要があります。このコマンドにより、ネイティブVLANの設定ミスを防止できます。
- 802.1Q インターフェイスをエッジポートにするように手動で設定する必要があります。
- IGMP スヌーピングは内部VLANではサポートされません。
- Q-in-Q は、Cisco Nexus 9332PQ、9372PX、9372TX、および93120TX スイッチのアップリンクポートと、N9K-M6PQ または N9K-M12PQ の汎用拡張モジュール (GEM) を搭載したCisco Nexus 9396PX、9396TX、および93128TX スイッチではサポートされていません。
- Q-in-Q トンネルは、Cisco Nexus 9300 および9500 シリーズ デバイスのアプリケーションリーフ エンジン (ALE) アップリンクポートに関する制約事項の影響を受ける可能性があります (「ALE アップリンクポートに関する制約事項」)。
- Q-in-Q トンネリングは、次の Application Spine Engine 2 (ASE2) および Application Spine Engine 3 (ASE3) ベースの Cisco Nexus スイッチではサポートされていません。
 - ASE2 - N9236C、N9272Q、N92304QC、および N92300Y
 - ASE3 - N92160YC-X
- Q-in-Q タグgingはサポートされていません。
- Layer 2 プロトコル トンネリングは、N9K-X9636C-R、N9K-X9636Q-R、N9K-X9636C-RX ラインカードを搭載したCisco Nexus 9500 シリーズ スイッチではサポートされません。
- N9K-X9636C-R、N9K-X9636Q-R、N9K-X9636C-RX ラインカードを搭載したCisco Nexus 9500 シリーズ スイッチでは、Q-in-Q はポートまたはポートチャネルのレイヤ2 アクセスVLAN エッジデバイスでのみサポートされます。

- FEX 設定は Q-in-Q ポートではサポートされません。
- コマンド `l2protocol tunnel stp` がトンネルインターフェイスで設定されている場合、サービスプロバイダーで設定する VLAN はカスタマーネットワークの VLAN とは異なる必要があります。
- LACP の L2PT トンネリングを使用するエッジデバイスでフォールバック ISSU をトリガすると、エッジデバイスはソフトウェアでトンネリング（カプセル化および送信）を行います。ISSU 中のエッジデバイスのコントロールプレーンのダウンタイムが 90 秒を超える場合、エッジデバイスのいずれかに接続されている LACP 対応ピアは、いずれかの LACP 対応ピアの LACP PDU タイムアウトが原因でフラップする可能性があります。90 秒の制限の期間は、次の理由によるものです。
 - ISSU が原因でコントロールプレーンがダウンする直前に LACP PDU を送信するために、L2PT トンネリングを使用するエッジデバイスで実行される特別なスクリプトはありません。
 - エッジデバイスで確認された最後の LACP PDU は、ISSU がトリガされる前の最後の 90 秒間である可能性があります。これは、デフォルトの LACP PDU 送信レートが 30 秒で、タイムアウトが 90 秒であるためです。

複数プロバイダー VLAN を使用した選択的 Q-in-Q の注意事項と制約事項

- 複数のプロバイダー VLAN を使用する選択的 Q-in-Q には、選択的 Q-in-Q に関する既存の制限事項とガイドラインがすべて適用されます。
- Cisco NX-OS リリース 9.3(5) 以降、複数プロバイダー VLAN を使用した選択的 Q-in-Q 機能は、Cisco Nexus N9K-C9316D-GX、N9K-C93600CD-GX、N9K-C9364C-GX スイッチでサポートされます。
- 複数プロバイダー VLAN を使用した選択的 Q-in-Q 機能は、Nexus 9300-EX、9300-FX、および 9300-FX2 プラットフォームでサポートされます。
- vPC ポートチャネルで複数のプロバイダー VLAN をイネーブルにする場合は、vPC ピア間で設定が一貫している必要があります。
- 通常のトランクではプロバイダー VLAN を許可しないことを推奨します。
- 複数のプロバイダー VLAN インターフェイスの VLAN リストを許可しているトランクインターフェイスで、ネイティブ VLAN およびプロバイダー VLAN のみを許可します。
- ポートから VLAN へのマッピング（例：`switchport vlan mapping 10 20`）は、複数のプロバイダー VLAN で選択的 Q-in-Q 用に設定されたポートではサポートされません。
- プライベート VLAN は、複数のプロバイダー VLAN で選択的 Q-in-Q 用に設定されたポートではサポートされません。

- レイヤ 2 スイッチングのみがサポートされます。
- プロバイダー VLAN でのルーティングはサポートされていません。
- FEX は、複数のプロバイダー VLAN を使用する選択的 Q-in-Q ではサポートされません。
- 複数プロバイダー VLAN を使用した選択的 Q-in-Q
- VLAN1 が複数のプロバイダー タグを使用して選択的 Q-in-VNI を使用してネイティブ VLAN として設定されている場合、ネイティブ VLAN 上のトラフィックはドロップされます。ポートが選択的 Q-in-Q で設定されている場合は、VLAN1 をネイティブ VLAN として設定しないでください。VLAN1 がカスタマー VLAN として設定されている場合、VLAN1 のトラフィックはドロップされます。

複合アクセス ポート機能セットに関する注意事項と制限事項

- Cisco NX-OS リリース 9.3(3) 以降では、IPv4 アンダーレイを搭載した Cisco Nexus C9348GC-FXP スイッチで複合アクセス ポート機能セットがサポートされています。
- 複合アクセス ポート機能セットは、次の機能で構成されます。
 - プライベート VLAN (セカンダリ隔離あり)
 - 選択的 Q-in-Q
 - ポートセキュリティ
- PVLAN および選択的 Q-in-Q に関するすべてのガイドラインと制限は、複合アクセス ポート機能セットにも適用されます。
- ポートモードの **private-vlan trunk secondary** は、複合アクセス ポート機能セットでサポートされます。
- vPC ポート チャンネルで複合アクセス ポート機能セットを有効にする場合は、設定が vPC ピア全体で一貫していることを確認する必要があります。
- 複合アクセス ポート機能セットを実行する場合は、**system dot1q-tunnel transit** と入力することを推奨します。
- ポート VLAN マッピング (例 : **switchport vlan mapping 10 20**) はサポートされていません。
- 選択的 Q-in-Q ではレイヤ 2 スイッチングのみがサポートされます。
- 複合アクセス ポート機能のネイティブ VLAN では、ルーティングのみがサポートされます。

VLAN 上のポート VLAN マッピングに関する注意事項と制限事項

次に、ポート VLAN マッピングに関する注意事項と制限事項を示します。

- Cisco NX-OS リリース 10.3(3)F 以降、VLAN のポート VLAN マッピングは、Cisco Nexus 9300-EX/FX/FX2/FX3/GX/GX2、C9408 プラットフォームスイッチ、および 9700-EX/FX/GX ラインカードを搭載した Cisco Nexus 9500 スイッチでサポートされます。
- 入力（着信）VLAN は、スイッチで VLAN として設定する必要はありません。変換された VLAN を構成する必要があります。
- すべてのレイヤ 2 送信元アドレスの学習およびレイヤ 2 MAC 宛先のルックアップは、変換先 VLAN で行われます。入力（着信）VLAN ではなく、変換先 VLAN にある VLAN カウンタを参照してください。
- ポート VLAN マッピングルーティングは、変換された VLAN での SVI の設定をサポートします。
- 次に、ローカル VLAN 100 にマッピングされる着信 VLAN 10 の例を示します。

```
interface ethernet1/1
switchport vlan mapping 10 100
```

- 次に、PV 変換用のオーバーラップ VLAN の例を示します。最初のステートメントでは、VLAN-102 は変換された VLAN です。2 番目のステートメントでは、VLAN-102 は VLAN-103 に変換される VLAN です。

```
interface ethernet1/1
switchport vlan mapping 101 102
switchport vlan mapping 102 103
```

- force コマンドを使用して既存のポートチャネルにメンバーを追加する場合、「mapping enable」設定は一貫している必要があります。次に例を示します。

```
Int po 101
switchport vlan mapping enable
switchport vlan mapping 101 10
switchport trunk allowed vlan 10
```

```
int eth 1/8
/****No configuration****/
```



- (注) switchport VLAN mapping enable コマンドは、ポートモードがトランクの場合にのみサポートされます。

- VLAN マッピングは、ポートごとに VLAN をスコーピングすることで、ポートへの VLAN のローカリゼーションに役立ちます。一般的な使用例は、サービスプロバイダーのリーフスイッチに、重複する VLAN を持つ異なる顧客があり、異なるポートに着信する

サービス プロバイダー環境です。たとえば、顧客 A には Eth 1/1 に着信する VLAN 10 があり、顧客 B には Eth 2/2 に着信する VLAN 10 があります。

- ポート VLAN マッピングは PVLAN と共存しません。
- **inherit port-profile** コマンドが PV インターフェイスで構成されている場合は、**no inherit port-profile <profile name>** コマンドを使用してデタッチしてから、**no switchport vlan mapping all** コマンドを実行します。
- **system dot1q-tunnel transit vlan provider_vlan_list** コマンドがスイッチ上でグローバルに構成されている場合は、プロバイダ VLAN をシステム上の他のトランクまたはアクセスポートのネイティブまたはアクセスポート VLAN として設定しないでください。システム上のネイティブ VLAN 以外のプロバイダ VLAN を選択する必要があります。

Q-in-Q トンネルおよびレイヤ2 プロトコルのトンネリングの設定

802.1Q トンネル ポートの作成

dot1q トンネルポートを作成するには、コマンドを使用します。 **switchport mode**



- (注) コマンドを使用して、802.1Q トンネルポートをエッジポートに設定する必要があります。**spanning-tree port type edge** ポートのプロバイダ VLAN メンバーシップは、**switchport access vlan vlan-id** コマンドを使用して変更します。

dot1q-tunnel ポートに割り当てられたアクセス VLAN の IGMP スヌーピングをディセーブルにして、マルチキャストパケットが Q-in-Q トンネルを通過できるようにする必要があります。

Q-in-Q カプセル化またはカプセル化解除の要件を持たない SP クラウド内の純粋な中継ボックス上で、すべての VLAN タグのシームレスなパケット転送と保存を行うには、システム全体の **system dot1q-tunnel transit** を構成するか、**system dot1q-tunnel transit vlan provider_vlan_list** コマンドを使用します。構成を削除するには、**no system dot1q-tunnel transit** または **system dot1q-tunnel transit vlan provider_vlan_list** コマンドを使用します。

system dot1q-tunnel transit または **system dot1q-tunnel transit vlan provider_vlan_list** コマンドのサポートされているプラットフォームと制限については、「[Q-in-Q トンネリングおよびレイヤ2 プロトコル トンネリングの注意事項と制約事項 \(408 ページ\)](#)」セクションを参照してください。

始める前に

はじめに、スイッチポートとしてインターフェイスを設定する必要があります。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **interface ethernet slot/port**
3. switch(config-if)# **switchport**
4. switch(config-if)# **switchport mode dot1q-tunnel**
5. switch(config-if)# **spanning-tree port type edge**
6. switch(config-if)# **switchport access vlan vlan-id**
7. (任意) switch(config-if)# **no switchport mode dot1q-tunnel**
8. switch(config-if)# **exit**
9. (任意) switch(config)# **show dot1q-tunnel [interface if-range]**
10. (任意) switch(config)# **no shutdown**
11. (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# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# interface ethernet slot/port	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# switchport	インターフェイスをレイヤ 2 スイッチング ポートとして設定します。
ステップ 4	switch(config-if)# switchport mode dot1q-tunnel	ポートに 802.1Q トンネルを作成します。インターフェイスモードを変更すると、ポートはダウンし、再初期化 (ポートフラップ) されます。トンネルインターフェイスでは BPDU フィルタリングがイネーブルになり、CDP がディセーブルになります。
ステップ 5	switch(config-if)# spanning-tree port type edge	ポートをスパンニングツリー エッジ ポートとして指定します。
ステップ 6	switch(config-if)# switchport access vlan vlan-id	プロバイダー アクセス VLAN 値を設定します。
ステップ 7	(任意) switch(config-if)# no switchport mode dot1q-tunnel	ポートで 802.1Q トンネルをディセーブルにします。
ステップ 8	switch(config-if)# exit	コンフィギュレーション モードを終了します。
ステップ 9	(任意) switch(config)# show dot1q-tunnel [interface if-range]	dot1q-tunnel モードにあるすべてのポートを表示します。必要に応じて、表示するインターフェイスまたはインターフェイスの範囲を指定できます。
ステップ 10	(任意) switch(config)# no shutdown	ポリシーがハードウェア ポリシーと一致するインターフェイスおよび VLAN のエラーをクリアしま

	コマンドまたはアクション	目的
		す。このコマンドにより、ポリシープログラミングが続行でき、ポートがアップできます。ポリシーが対応していない場合は、エラーは <code>error-disabled</code> ポリシー状態になります。
ステップ 11	(任意) <code>switch(config)# copy running-config startup-config</code>	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、802.1Q トンネル ポートを作成する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 7/1
switch(config-if)# switchport
switch(config-if)# switchport mode dot1q-tunnel
switch(config-if)# spanning-tree port type edge
switch(config-if)# switchport access vlan vlan 10
switch(config-if)# exit
switch(config)# exit
switch# show dot1q-tunnel
```

802.1Q トンネル ポートでの選択的 Q-in-Q の VLAN マッピングの設定

802.1Q トンネル ポートで選択的 Q-in-Q の VLAN マッピングを設定するには、次の手順を実行します。



(注) 同じインターフェイスでは、1対1のマッピングと選択的 Q-in-Q を設定できません。

コマンドを使用して、802.1Q トンネルポートをエッジポートに設定する必要があります。

spanning-tree port type edge ポートのプロバイダー VLAN メンバーシップは、**switchport access vlan *vlan-id*** コマンドを使用して変更します。

`dot1q-tunnel` ポートに割り当てられたアクセス VLAN の IGMP スヌーピングをディセーブルにして、マルチキャストパケットが Q-in-Q トンネルを通過できるようにする必要があります。

手順の概要

1. `switch# configure terminal`
2. `switch(config)# interface interface-id`
3. `switch(config-if)# switchport mode dot1q-tunnel`
4. `switch(config-if)# spanning-tree port type edge`
5. `switch(config-if)# switchport access vlan vlan-id`
6. `switch(config-if)# switchport vlan mapping vlan-id-range dot1q-tunnel outer vlan-id`

802.1Q トンネル ポートでの選択的 Q-in-Q の VLAN マッピングの設定

7. switch(config-if)# **exit**
8. switch# **show interfaces interface-id vlan mapping**
9. 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# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# interface interface-id	サービス プロバイダ ネットワークに接続されるインターフェイスのインターフェイス コンフィギュレーションモードを開始します。物理インターフェイスまたは EtherChannel ポートチャネルを入力できます。
ステップ 3	switch(config-if)# switchport mode dot1q-tunnel	トンネルポートとしてインターフェイスを構成します。
ステップ 4	switch(config-if)# spanning-tree port type edge	ポートをスパンニングツリー エッジポートとして指定します。
ステップ 5	switch(config-if)# switchport access vlan vlan-id	プロバイダー アクセス VLAN 値を設定します。
ステップ 6	switch(config-if)# switchport vlan mapping vlan-id-range dot1q-tunnel outer vlan-id	マッピングする VLAN ID を入力します。 <ul style="list-style-type: none"> • vlan-id-range1 : カスタマー ネットワークからスイッチに入るカスタマー VLAN ID (C-VLAN) の範囲。指定できる範囲は 1 ~ 4094 です。VLAN-ID のストリングを入力できます。 • outer vlan-id : サービスプロバイダー ネットワークの外部 VLAN ID (S-VLAN) を入力します。指定できる範囲は 1 ~ 4094 です。
ステップ 7	switch(config-if)# exit	コンフィギュレーション モードを終了します。
ステップ 8	switch# show interfaces interface-id vlan mapping	設定を確認します。
ステップ 9	switch# copy running-config startup-config	(任意) コンフィギュレーションファイルに設定を保存します。

VLAN マッピング設定を削除するには、**no switchport vlan mapping vlan-id-range dot1q-tunnel outer vlan-id** コマンドを使用します。

次の例では、ポートに選択した QinQ マッピングを設定して、C-VLAN ID が 1~5 のトラフィックが、S-VLAN ID が 100 であるスイッチに入るようにする方法を示します。その他の VLAN ID のトラフィックはドロップされます。

例

```
switch(config)# interface gigabitethernet0/1
switch(config-if)# switchport vlan mapping 1-5 dot1q-tunnel 100
switch(config-if)# spanning-tree port type edge
switch(config-if)# switchport access vlan 10
Switch(config-if)# exit
```

複数プロバイダー VLAN で選択的 Q-in-Q を設定する

始める前に

プロバイダー VLAN を設定する必要があります。

spanning-tree bpdudfilter enable コマンドを使用して、トランクポートでスパンニングツリーを無効にする必要があります。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **interface** *interface-id*
3. switch(config-if)# **switchport**
4. switch(config-if)# **switchport mode trunk**
5. switch(config-if)# **spanning-tree bpdudfilter enable**
6. switch(config-if)# **switchport trunk native vlan** *vlan-id*
7. switch(config-if)# **switchport vlan mapping** *vlan-id-range* **dot1q-tunnel** *outer vlan-id*
8. switch(config-if)# **switchport trunk allowed vlan** *vlan_list*
9. switch(config-if)# **exit**
10. switch(config-if)# **show interfaces** *interface-id* **vlan mapping**

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# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# interface <i>interface-id</i>	サービス プロバイダ ネットワークに接続されるインターフェイスのインターフェイス コンフィギュレーションモードを開始します。物理インターフェイスまたは EtherChannel ポート チャンネルを入力できます。
ステップ 3	switch(config-if)# switchport	インターフェイスをレイヤ 2 スイッチング ポートとして設定します。

複数プロバイダー VLAN で選択的 Q-in-Q を設定する

	コマンドまたはアクション	目的
ステップ 4	switch(config-if)# switchport mode trunk	インターフェイスをレイヤ 2 トランク ポートとして設定します。
ステップ 5	switch(config-if)# spanning-tree bpdupfilter enable	このインターフェイスでのスパンニングツリー BPDU の送信と処理を無効にします。
ステップ 6	switch(config-if)# switchport trunk native vlan <i>vlan-id</i>	802.1Q トランクのネイティブ VLAN を設定します。有効な値は 1 ~ 4094 です。デフォルト値は VLAN 1 です。
ステップ 7	switch(config-if)# switchport vlan mapping <i>vlan-id-range dot1q-tunnel outer vlan-id</i>	マッピングする VLAN ID を入力します。 <ul style="list-style-type: none"> • <i>vlan-id-range1</i> : カスタマー ネットワークからスイッチに入るカスタマー VLAN ID (C-VLAN) の範囲。指定できる範囲は 1 ~ 4094 です。VLAN-ID のストリングを入力できます。 • <i>outer vlan-id</i> : サービス プロバイダー ネットワークの外部 VLAN ID (S-VLAN) を入力します。指定できる範囲は 1 ~ 4094 です。
ステップ 8	switch(config-if)# switchport trunk allowed vlan <i>vlan_list</i>	トランク インターフェイスの許可 VLAN を設定します。
ステップ 9	switch(config-if)# exit	コンフィギュレーション モードを終了します。
ステップ 10	switch(config-if)# show interfaces <i>interface-id</i> vlan mapping	マッピングの設定の確認

次の例では、複数のプロバイダー VLAN で選択的 Q-in-Q を設定する方法を示します。

例

```
switch# sh run int e1/1

interface Ethernet1/1
  switchport
  switchport mode trunk
  switchport trunk native vlan 2
  switchport vlan mapping 3-400 dot1q-tunnel 400
  switchport vlan mapping 401-800 dot1q-tunnel 401
  switchport vlan mapping 801-1200 dot1q-tunnel 10
  switchport vlan mapping 1201-1600 dot1q-tunnel 1400
  switchport vlan mapping 1601-2000 dot1q-tunnel 9
  switchport vlan mapping 2001-2400 dot1q-tunnel 3000
  switchport vlan mapping 2401-2800 dot1q-tunnel 2099
  switchport vlan mapping 2801-3200 dot1q-tunnel 2800
  switchport vlan mapping 3201-3600 dot1q-tunnel 3967
  switchport vlan mapping 3601-4000 dot1q-tunnel 600
  spanning-tree bpdupfilter enable
```

```

switchport trunk allowed vlan 2,9-10,400-401,600,1400,2099,2800,3000,3967

switch# show interface e1/1 vlan mapping
Interface Eth1/1:
Original VLAN                               Translated VLAN
-----
3                                               400
4                                               400
5                                               400
6                                               400
7                                               400
8                                               400
9                                               400
10                                              400
11                                              400
12                                              400
13                                              400
14                                              400
15                                              400
16                                              400
17                                              400
18                                              400
19                                              400
20                                              400

switch# show consistency-checker selective-qinq interface e1/1
Fetching ingressVlanXlate entries from slice:0 HW
Fetching ingressVlanXlate entries from slice:1 HW
Performing port specific checks for intf Eth1/1
Port specific selective QinQ checks for interface Eth1/1 : PASS

Switch#

```

Q-in-Q 用の EtherType の変更

スイッチは、802.1Q および Q-in-Q カプセル化に 0x8100 のデフォルトの EtherType を使用します。EtherType は、スイッチポートインターフェイスで 0x9100、0x9200、および 0x88a8 に設定できません。

レイヤ 2 プロトコル トンネルのイネーブル化

802.1Q トンネル ポートでプロトコルのトンネリングをイネーブルにできます。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **interface ethernet slot/port**
3. switch(config-if)# **switchport**
4. switch(config-if)# **switchport mode dot1q-tunnel**
5. switch(config-if)# **l2protocol tunnel [cdp | stp | lacp | lldp | vtp]**
6. (任意) switch(config-if)# **no l2protocol tunnel [cdp | stp | lacp | lldp | vtp]**
7. switch(config-if)# **exit**
8. (任意) switch(config)# **no shutdown**

9. (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# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# interface ethernet slot/port	設定するインターフェイスを指定し、インターフェイス コンフィギュレーションモードを開始します。
ステップ 3	switch(config-if)# switchport	インターフェイスをレイヤ2 スイッチング ポートとして設定します。
ステップ 4	switch(config-if)# switchport mode dot1q-tunnel	ポートに 802.1Q トンネルを作成します。インターフェイスモードを変更すると、ポートはダウンし、再初期化 (ポートフラップ) されます。トンネル インターフェイスでは BPDU フィルタリングがイネーブルになり、CDP がディセーブルになります。
ステップ 5	switch(config-if)# l2protocol tunnel [cdp stp lacp lldp vtp]	レイヤ2 プロトコルのトンネリングをイネーブルにします。必要に応じて、CDP、STP、LACP、LLDP または VTP トンネリングを有効にできます。
ステップ 6	(任意) switch(config-if)# no l2protocol tunnel [cdp stp lacp lldp vtp]	プロトコルのトンネリングをディセーブルにします。
ステップ 7	switch(config-if)# exit	コンフィギュレーション モードを終了します。
ステップ 8	(任意) switch(config)# no shutdown	ポリシーがハードウェア ポリシーと一致するインターフェイスおよび VLAN のエラーをクリアします。このコマンドにより、ポリシープログラミングが続き、ポートがアップできます。ポリシーが対応していない場合は、エラーは error-disabled ポリシー状態になります。
ステップ 9	(任意) switch(config)# copy running-config startup-config	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、802.1Q トンネルポートでプロトコルのトンネリングをイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 7/1
switch(config-if)# switchport
```

```
switch(config-if)# switchport mode dot1q-tunnel
switch(config-if)# l2protocol tunnel stp
switch(config-if)# exit
switch(config)# exit
```

L2 プロトコル トンネル ポートに対するグローバル CoS の設定

トンネル ポートの入力 BPDU が指定されたクラスでカプセル化されるように、サービス クラス (CoS) の値をグローバルに指定できます。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **l2protocol tunnel cos value**
3. (任意) switch(config)# **no l2protocol tunnel cos**
4. switch(config)# **exit**
5. (任意) switch# **no shutdown**
6. (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# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# l2protocol tunnel cos value	すべてのレイヤ2プロトコルのトンネリングポートでグローバル CoS 値を指定します。デフォルト CoS 値は 5 です。
ステップ 3	(任意) switch(config)# no l2protocol tunnel cos	グローバル CoS 値をデフォルト値に設定します。
ステップ 4	switch(config)# exit	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	(任意) switch# no shutdown	ポリシーがハードウェア ポリシーと一致するインターフェイスおよび VLAN のエラーをクリアします。このコマンドにより、ポリシープログラミングが続行でき、ポートがアップできます。ポリシーが対応していない場合は、エラーは error-disabled ポリシー状態になります。
ステップ 6	(任意) switch# copy running-config startup-config	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、レイヤ2 プロトコルのトンネリングのためのグローバル CoS 値を指定する例を示します。

```
switch# configure terminal
switch(config)# l2protocol tunnel cos 6
switch(config)# exit
```

レイヤ2 プロトコル トンネル ポートのしきい値の設定

レイヤ2 プロトコルのトンネリング ポートに対するポート ドロップおよびシャットダウン値を指定できます。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **interface ethernet slot/port**
3. switch(config-if)# **switchport**
4. switch(config-if)# **switchport mode dot1q-tunnel**
5. switch(config-if)# **l2protocol tunnel drop-threshold [cdp | stp | vtp] packets-per-sec**
6. (任意) switch(config-if)# **no l2protocol tunnel drop-threshold [cdp | stp | vtp]**
7. switch(config-if)# **l2protocol tunnel shutdown-threshold [cdp | stp | vtp] packets-per-sec**
8. (任意) switch(config-if)# **no l2protocol tunnel shutdown-threshold [cdp | stp | vtp]**
9. switch(config-if)# **exit**
10. (任意) switch(config)# **no shutdown**
11. (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# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# interface ethernet slot/port	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# switchport	インターフェイスをレイヤ2 スイッチング ポートとして設定します。
ステップ 4	switch(config-if)# switchport mode dot1q-tunnel	ポートに 802.1Q トンネルを作成します。
ステップ 5	switch(config-if)# l2protocol tunnel drop-threshold [cdp stp vtp] packets-per-sec	廃棄される前にインターフェイスで処理できる最大パケット数を指定します。必要に応じて、CDP、

	コマンドまたはアクション	目的
		STP、または VTP を指定できます。パケットの有効な値は 1 ~ 4096 です。
ステップ 6	(任意) <code>switch(config-if)# no l2protocol tunnel drop-threshold [cdp stp vtp]</code>	しきい値を 0 にリセットし、ドロップしきい値をディセーブルにします。
ステップ 7	<code>switch(config-if)# l2protocol tunnel shutdown-threshold [cdp stp vtp] packets-per-sec</code>	インターフェイスで処理できる最大パケット数を指定します。パケット数が超過すると、ポートは <code>error-disabled</code> ステートになります。必要に応じて、CDP、STP、または VTP を指定できます。パケットの有効な値は 1 ~ 4096 です。
ステップ 8	(任意) <code>switch(config-if)# no l2protocol tunnel shutdown-threshold [cdp stp vtp]</code>	しきい値を 0 にリセットし、シャットダウンしきい値をディセーブルにします。
ステップ 9	<code>switch(config-if)# exit</code>	コンフィグレーション モードを終了します。
ステップ 10	(任意) <code>switch(config)# no shutdown</code>	ポリシーがハードウェア ポリシーと一致するインターフェイスおよび VLAN のエラーをクリアします。このコマンドにより、ポリシープログラミングが続行でき、ポートがアップできます。ポリシーが対応していない場合は、エラーは <code>error-disabled</code> ポリシー状態になります。
ステップ 11	(任意) <code>switch(config)# copy running-config startup-config</code>	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。

複合アクセス ポート機能セットの設定

混合アクセス ポートを設定するには、次の手順を実行します。

手順の概要

1. `interface interface [port | port-channel | vPC]`
2. `switchport mode private-vlan trunk secondary`
3. `switchport private-vlan trunk native vlan vlan_id`
4. `switchport private-vlan trunk allowed vlan vlan list`
5. `switchport private-vlan association trunk primary_vlan_ID secondary_vlan_ID`
6. `switchport vlan mapping [vlan-id-range | all] dot1q-tunnel outer vlan-id`
7. `storm-control broadcast level [high level] [lower level]`
8. `storm-control multicast level [high level] [lower level]`
9. `storm-control action [shutdown | trap]`
10. `load-interval counter {1 | 2 | 3 }`
11. `switchport port-security maximum [max-addr]`

12. `switchport port-security action [restrict | shutdown | protect]`
13. `switchport port-security`
14. `service-policy {input | type {qos input | queuing {input | output}}}` `policy-map-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	<code>interface interface [port port-channel vPC]</code> 例： <code>switch# interface port-channel 202</code>	指定されたポート チャンネルをインターフェイス コンフィギュレーションモードにします。範囲は 1 ~ 4096 です。
ステップ 2	<code>switchport mode private-vlan trunk secondary</code> 例： <code>switch(config)# switchport mode private-vlan trunk secondary</code>	プライベート VLAN のセカンダリ トランク ポートとしてポートを設定します。
ステップ 3	<code>switchport private-vlan trunk native vlan vlan_id</code> 例： <code>switch(config)# switchport private-vlan trunk native vlan 4002</code>	PVLAN トランク ポートに割り当てるネイティブ VLAN を設定します。
ステップ 4	<code>switchport private-vlan trunk allowed vlan vlan list</code> 例： <code>switch(config)# switchport private-vlan trunk allowed vlan 1002,4002</code>	PVLAN トランク ポートで許容される通常の VLAN のリストを設定します。
ステップ 5	<code>switchport private-vlan association trunk primary_vlan_ID secondary_vlan_ID</code> 例： <code>switch(config)# switchport private-vlan association trunk 4050 4049</code>	PVLAN トランク ポートでプライマリ VLAN およびセカンダリ VLAN 間の関連付けを設定します。
ステップ 6	<code>switchport vlan mapping [vlan-id-range all] dot1q-tunnel outer_vlan-id</code> 例： <code>switch(config-if)# switchport vlan mapping all dot1q-tunnel 1002</code>	すべての 4K VLAN を含むカスタマー範囲 VLAN またはキーワード <code>all</code> を入力します。
ステップ 7	<code>storm-control broadcast level [high level] [lower level]</code> 例： <code>switch(config-if)# storm-control broadcast level 1.00</code>	ブロードキャスト ストーム制御を設定します。ブロードキャスト トラフィックの上限しきい値レベルを指定します。
ステップ 8	<code>storm-control multicast level [high level] [lower level]</code> 例：	インターフェイス上のマルチキャスト トラフィック ストーム制御をイネーブルにし、トラフィック ストーム制御レベルを設定し、そのトラフィック

	コマンドまたはアクション	目的
	<code>switch(config-if)# storm-control multicast level 1.00</code>	ストーム制御レベルを、インターフェイス上でイネーブルにされているすべてのトラフィックストーム制御モードに適用します。
ステップ 9	storm-control action [shutdown trap] 例 : <code>switch(config-if)# storm-control action shutdown</code>	トラフィック ストームの発生時にトラップを生成するか、ポートをエラー無効にするようにトラフィック ストーム制御を設定します。
ステップ 10	load-interval counter {1 2 3 } 例 : <code>switch(config-if)# load-interval counter 1 5</code>	インターフェイスで統計情報をサンプリングする間隔を指定します。
ステップ 11	switchport port-security maximum [max-addr] 例 : <code>switch(config-if)# switchport port-security maximum 3</code>	ポートでセキュア MAC アドレスの最大数を設定します。
ステップ 12	switchport port-security action [restrict shutdown protect] 例 : <code>switch(config-if)# switchport port-security violation restrict</code>	インターフェイスのセキュリティ違反モードを制限します。
ステップ 13	switchport port-security 例 : <code>switch(config-if)# switchport port-security</code>	ポートセキュリティのコンフィギュレーション情報を表示します。
ステップ 14	service-policy {input type {qos input queuing {input output}} } policy-map-name 例 : <code>switch(config-if)# service-policy type qos input ovh_qos</code>	ポリシーマップをインターフェイスに付加します。

Q-in-Q 設定の確認

コマンド	目的
clear l2protocol tunnel counters [interface if-range]	すべての統計情報カウンタをクリアします。インターフェイスが指定されていない場合、すべてのインターフェイスのレイヤ 2 プロトコル トンネル統計情報がクリアされます。

コマンド	目的
show dot1q-tunnel [interface <i>if-range</i>]	dot1q トンネルモードのインターフェイス範囲またはすべてのインターフェイスが表示されます。
show l2protocol tunnel [interface <i>if-range</i> vlan <i>vlan-id</i>]	一定範囲のインターフェイス（特定の VLAN の一部であるすべての dot1q-tunnel インターフェイスまたはすべてのインターフェイス）のレイヤ2 プロトコル トンネル情報を表示します。
show l2protocol tunnel summary	レイヤ2 プロトコル トンネルが設定されているすべてのポートのサマリーを表示します。
show running-config l2pt	現在のレイヤ2 プロトコル トンネルの実行コンフィギュレーションを表示します。

Q-in-Q およびレイヤ2 プロトコルのトンネリングの設定例

次に、イーサネット 7/1 に着信するトラフィックに対し Q-in-Q を処理するように設定されているサービス プロバイダーのスイッチを示します。レイヤ2 プロトコル トンネルが STP BPDU に対してイネーブルにされます。このカスタマーは VLAN 10（外部 VLAN タグ）に割り当てられます。

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# vlan 10
switch(config-vlan)# no shutdown
switch(config-vlan)# no ip igmp snooping
switch(config-vlan)# exit
switch(config)# interface ethernet 7/1
switch(config-if)# switchport
switch(config-if)# switchport mode dot1q-tunnel
switch(config-if)# switchport access vlan 10
switch(config-if)# spanning-tree port type edge
switch(config-if)# l2protocol tunnel stp
switch(config-if)# no shutdown
switch(config-if)# exit
switch(config)# exit
switch#
```

VLAN 上のポート VLAN マッピングの構成

始める前に

- VLAN 変換を実装する物理またはポート チャンネルがレイヤ 2 トランク ポートとして設定されていることを確認します。
- 変換先 VLAN がスイッチで作成されており、レイヤ 2 トランク ポートのトランク許可 VLAN の `vlan-list` にも追加されていることを確認します。



(注) ベストプラクティスとして、入力 VLAN ID をインターフェイスのスイッチポート許可 `vlan-list` に追加しないでください。

手順の概要

1. `configure terminal`
2. `interface type/port`
3. `[no] switchport vlan mapping enable`
4. `[no] switchport vlan mapping vlan-id translated-vlan-id`
5. `[no] switchport vlan mapping all`
6. `copy running-config startup-config`
7. `show interface [if-identifier] vlan mapping`

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： <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	interface type/port 例： <code>switch(config)# interface Ethernet1/1</code>	設定するインターフェイスを指定します。
ステップ 3	[no] switchport vlan mapping enable 例： <code>switch(config-if)# [no] switchport vlan mapping enable</code>	スイッチ ポートでの VLAN 変換をイネーブルにします。VLAN 変換はデフォルトでディセーブルです。 (注) VLAN 変換を無効にするには、このコマンドの no 形式を使用します。

	コマンドまたはアクション	目的
ステップ 4	<p>[no] switchport vlan mapping <i>vlan-id translated-vlan-id</i></p> <p>例 :</p> <pre>switch(config-if)# switchport vlan mapping 10 100</pre>	<p>VLAN を他の VLAN に変換します。</p> <ul style="list-style-type: none"> • <i>vlan-id</i> 引数と <i>translated-vlan-id</i> 引数の範囲は 1 ~ 4094 です。 • 入力（着信）VLAN とポートにあるローカル（変換先）VLAN との間での VLAN 変換を設定できます。VLAN 変換が有効にされたインターフェイスに到着するトラフィックにおいて、着信 VLAN は変換された VLAN にマッピングされます。 <p>トラフィックのルーティングは、変換された VLAN の SVI のコンテキストで行われます。VLAN 変換が設定された発信インターフェイスで、トラフィックは元の VLAN に変換されてから出力されます。</p> <p>(注) このコマンドの no 形式を使用すると、VLAN ペア間のマッピングがクリアされます。</p>
ステップ 5	<p>[no] switchport vlan mapping all</p> <p>例 :</p> <pre>switch(config-if)# no switchport vlan mapping all</pre>	<p>インターフェイスに設定されたすべての VLAN のマッピングを削除します。</p>
ステップ 6	<p>copy running-config startup-config</p> <p>例 :</p> <pre>switch(config-if)# copy running-config startup-config</pre>	<p>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。</p> <p>(注) VLAN 変換の設定は、スイッチポートが動作トランクポートになるまで有効になりません。</p>
ステップ 7	<p>show interface [<i>if-identifier</i>] vlan mapping</p> <p>例 :</p> <pre>switch# show interface ethernet1/1 vlan mapping</pre>	<p>インターフェイスの範囲または特定のインターフェイスについて、VLAN マッピング情報を表示します。</p>

例

次に、（入力）VLAN 10 と（ローカル）VLAN 100 間で VLAN 変換を設定する例を示します。show vlan counters コマンド出力は、カスタマー VLAN ではなく変換先 VLAN として統計情報カウンタを表示します。

```
switch# configure terminal
switch(config)# interface ethernet1/1
switch(config-if)# switchport vlan mapping enable
switch(config-if)# switchport vlan mapping 10 100
```

```
switch(config-if)# switchport trunk allowed vlan 100
switch(config-if)# show interface ethernet1/1 vlan mapping
Interface eth1/1:
Original VLAN          Translated VLAN
-----
10                     100

switch(config-if)# show vlan counters
Vlan Id                :100
Unicast Octets In      :292442462
Unicast Packets In     :1950525
Multicast Octets In    :14619624
Multicast Packets In   :91088
Broadcast Octets In    :14619624
Broadcast Packets In   :91088
Unicast Octets Out     :304012656
Unicast Packets Out    :2061976
L3 Unicast Octets In   :0
L3 Unicast Packets In :0
```




第 11 章

VLAN 上のポート VLAN マッピングの構成

この章は、次の内容で構成されています。

- [VLAN のポート VLAN マッピングについて（着信 VLAN の変換）](#)（431 ページ）
- [VLAN 上のポート VLAN マッピングに関する注意事項と制限事項](#)（432 ページ）
- [VLAN 上のポート VLAN マッピングの構成](#)（433 ページ）

VLAN のポート VLAN マッピングについて（着信 VLAN の変換）

サービス プロバイダーに、同じ VLAN カプセル化を使用して同じ物理スイッチに接続している複数の顧客があるものの、それらが同じ Layer 2 セグメント上に存在しない場合には、着信 VLAN を一意の VLAN/VNI に変換することが、セグメントを拡張する正しい方法です。

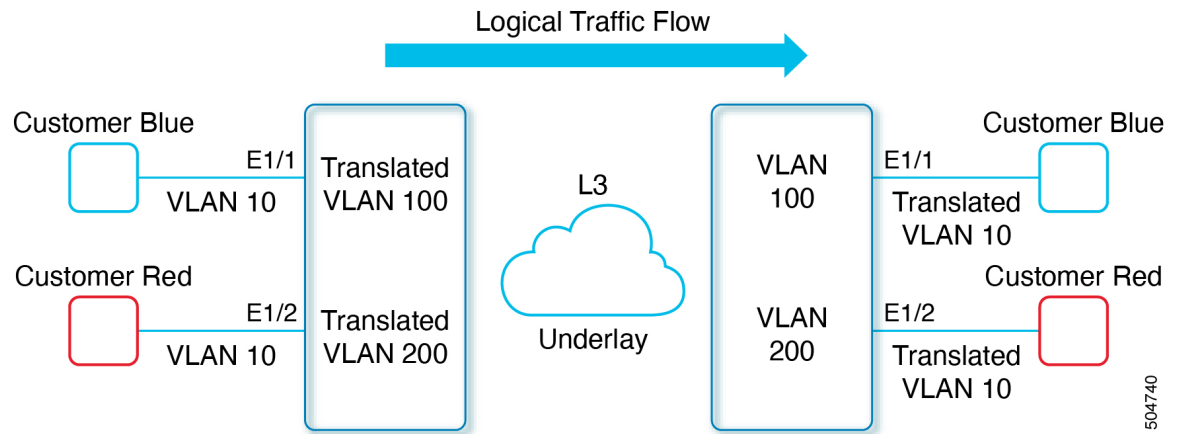
Cisco NX-OS リリース 10.3(3)F 以降、VXLAN VLAN 以外のポート VLAN マッピングは、Cisco Nexus 9300-EX/FX/FX2/FX3/GX/GX2、C9408 プラットフォームスイッチ、および 9700-EX/FX/GX ラインカードを搭載した Cisco Nexus 9500 スイッチでサポートされます。

次の図では、Blue と Red がカプセル化として VLAN 10 を使用してリーフに接続しています。

この例では、Customer Blue の VLAN 10（インターフェイス E1/1）が VLAN 100 にマッピング/変換され、Customer Red の VLAN 10（インターフェイス E1/2）が VLAN 200 にマッピングされます。

もう一方のリーフでは、このマッピングが逆に適用されます。着信 VLAN 100 はインターフェイス E1/1 の VLAN 10 にマッピングされ、VLAN 200 はインターフェイス E1/2 の VLAN 10 にマッピングされます。

図 36: 論理的トラフィックフロー



入力（着信）VLAN とポートにあるローカル（変換先）VLAN との間での VLAN 変換を設定できます。VLAN 変換が有効にされたインターフェイスに到着するトラフィックにおいて、着信 VLAN は変換された VLAN にマッピングされます。

アンダーレイ上で、内部 dot1q が削除され、VXLAN ネットワーク以外に切り替えられます。VLAN 変換が設定された発信インターフェイスで、トラフィックは元の VLAN に変換されてから出力されます。トラフィック カウンタについては、入力 VLAN ではなく、変換先 VLAN にある VLAN カウンタを参照してください。

VLAN 上のポート VLAN マッピングに関する注意事項と制限事項

次に、ポート VLAN マッピングに関する注意事項と制限事項を示します。

- Cisco NX-OS リリース 10.3(3)F 以降、VLAN のポート VLAN マッピングは、Cisco Nexus 9300-EX/FX/FX2/FX3/GX/GX2、C9408 プラットフォーム スイッチ、および 9700-EX/FX/GX ラインカードを搭載した Cisco Nexus 9500 スイッチでサポートされます。
- 入力（着信）VLAN は、スイッチで VLAN として設定する必要はありません。変換された VLAN を構成する必要があります。
- すべてのレイヤ 2 送信元アドレスの学習およびレイヤ 2 MAC 宛先のルックアップは、変換先 VLAN で行われます。入力（着信）VLAN ではなく、変換先 VLAN にある VLAN カウンタを参照してください。
- ポート VLAN マッピング ルーティングは、変換された VLAN での SVI の設定をサポートします。
- 次に、ローカル VLAN 100 にマッピングされる着信 VLAN 10 の例を示します。

```
interface ethernet1/1
switchport vlan mapping 10 100
```


- 次に、PV 変換用のオーバーラップ VLAN の例を示します。最初のステートメントでは、VLAN-102は変換された VLAN です。2 番目のステートメントでは、VLAN-102は VLAN-103 に変換される VLAN です。

```
interface ethernet1/1
switchport vlan mapping 101 102
switchport vlan mapping 102 103
```

- force** コマンドを使用して既存のポート チャンネルにメンバーを追加する場合、「mapping enable」設定は一貫している必要があります。次に例を示します。

```
Int po 101
switchport vlan mapping enable
switchport vlan mapping 101 10
switchport trunk allowed vlan 10
```

```
int eth 1/8
/***No configuration***/
```



- (注) **switchport VLAN mapping enable** コマンドは、ポートモードがトランクの場合にのみサポートされます。

- VLAN マッピングは、ポートごとに VLAN をスコーピングすることで、ポートへの VLAN のローカリゼーションに役立ちます。一般的な使用例は、サービスプロバイダーのリーフスイッチに、重複する VLAN を持つ異なるカスタマーがあり、異なるポートに着信するサービスプロバイダー環境です。たとえば、顧客 A には Eth 1/1 に着信する VLAN 10 があり、顧客 B には Eth 2/2 に着信する VLAN 10 があります。
- ポート VLAN マッピングは PVLAN と共存しません。
- inherit port-profile** コマンドが PV インターフェイスで構成されている場合は、**no inherit port-profile <profile name>** コマンドを使用してデタッチしてから、**no switchport vlan mapping all** コマンドを実行します。
- system dot1q-tunnel transit vlan provider_vlan_list** コマンドがスイッチ上でグローバルに構成されている場合は、プロバイダ VLAN をシステム上の他のトランクまたはアクセスポートのネイティブまたはアクセスポート VLAN として設定しないでください。システム上のネイティブ VLAN 以外のプロバイダ VLAN を選択する必要があります。

VLAN 上のポート VLAN マッピングの構成

始める前に

- VLAN 変換を実装する物理またはポート チャンネルがレイヤ 2 トランク ポートとして設定されていることを確認します。
- 変換先 VLAN がスイッチで作成されており、レイヤ 2 トランク ポートのトランク許可 VLAN の **vlan-list** にも追加されていることを確認します。



(注) ベストプラクティスとして、入力 VLAN ID をインターフェイスのスイッチポート許可 `vlan-list` に追加しないでください。

手順の概要

1. **configure terminal**
2. **interface *type/port***
3. **[no] switchport vlan mapping enable**
4. **[no] switchport vlan mapping *vlan-id translated-vlan-id***
5. **[no] switchport vlan mapping all**
6. **copy running-config startup-config**
7. **show interface [*if-identifier*] vlan mapping**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： <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	interface <i>type/port</i> 例： <code>switch(config)# interface Ethernet1/1</code>	設定するインターフェイスを指定します。
ステップ 3	[no] switchport vlan mapping enable 例： <code>switch(config-if)# [no] switchport vlan mapping enable</code>	スイッチ ポートでの VLAN 変換をイネーブルにします。VLAN 変換はデフォルトでディセーブルです。 (注) VLAN 変換を無効にするには、このコマンドの no 形式を使用します。
ステップ 4	[no] switchport vlan mapping <i>vlan-id translated-vlan-id</i> 例： <code>switch(config-if)# switchport vlan mapping 10 100</code>	VLAN を他の VLAN に変換します。 <ul style="list-style-type: none"> • <code>vlan-id</code> 引数と <code>translated-vlan-id</code> 引数の範囲は 1 ~ 4094 です。 • 入力 (着信) VLAN とポートにあるローカル (変換先) VLAN との間での VLAN 変換を設定できます。VLAN 変換が有効にされたインターフェイスに到着するトラフィックにおいて、着信 VLAN は変換された VLAN にマッピングされます。

	コマンドまたはアクション	目的
		<p>トラフィックのルーティングは、変換された VLAN の SVI のコンテキストで行われます。VLAN 変換が設定された発信インターフェイスで、トラフィックは元の VLAN に変換されてから出力されます。</p> <p>(注) このコマンドの no 形式を使用すると、VLAN ペア間のマッピングがクリアされます。</p>
ステップ 5	<p>[no] switchport vlan mapping all</p> <p>例 :</p> <pre>switch(config-if)# no switchport vlan mapping all</pre>	<p>インターフェイスに設定されたすべての VLAN のマッピングを削除します。</p>
ステップ 6	<p>copy running-config startup-config</p> <p>例 :</p> <pre>switch(config-if)# copy running-config startup-config</pre>	<p>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。</p> <p>(注) VLAN 変換の設定は、スイッチポートが動作トランクポートになるまで有効になりません。</p>
ステップ 7	<p>show interface [if-identifier] vlan mapping</p> <p>例 :</p> <pre>switch# show interface ethernet1/1 vlan mapping</pre>	<p>インターフェイスの範囲または特定のインターフェイスについて、VLAN マッピング情報を表示します。</p>

例

次に、(入力) VLAN 10 と (ローカル) VLAN 100 間で VLAN 変換を設定する例を示します。show vlan counters コマンド出力は、カスタマー VLAN ではなく変換先 VLAN として統計情報カウンタを表示します。

```
switch# configure terminal
switch(config)# interface ethernet1/1
switch(config-if)# switchport vlan mapping enable
switch(config-if)# switchport vlan mapping 10 100
switch(config-if)# switchport trunk allowed vlan 100
switch(config-if)# show interface ethernet1/1 vlan mapping
Interface eth1/1:
Original VLAN          Translated VLAN
-----
10                      100

switch(config-if)# show vlan counters
Vlan Id                :100
Unicast Octets In      :292442462
Unicast Packets In     :1950525
Multicast Octets In    :14619624
Multicast Packets In   :91088
Broadcast Octets In    :14619624
Broadcast Packets In   :91088
Unicast Octets Out     :304012656
```

```
Unicast Packets Out           :2061976
L3 Unicast Octets In          :0
L3 Unicast Packets In         :0
```



第 12 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 \(437 ページ\)](#)
- [スタティック NAT に関する情報 \(438 ページ\)](#)
- [ダイナミック NAT の概要 \(440 ページ\)](#)
- [タイムアウトメカニズム \(440 ページ\)](#)
- [NAT の内部アドレスおよび外部アドレス \(441 ページ\)](#)
- [ダイナミック NAT のプール サポート \(442 ページ\)](#)
- [スタティックおよびダイナミック Twice NAT の概要 \(442 ページ\)](#)
- [VRF 対応 NAT \(443 ページ\)](#)
- [スタティック NAT の注意事項および制約事項 \(445 ページ\)](#)
- [ダイナミック NAT の制約事項 \(447 ページ\)](#)
- [ダイナミック Twice NAT の注意事項および制約事項 \(449 ページ\)](#)
- [TCP 認識 NAT の注意事項および制約事項 \(449 ページ\)](#)
- [スタティック NAT の設定 \(450 ページ\)](#)
- [ダイナミック NAT の設定 \(461 ページ\)](#)

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で出口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き、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

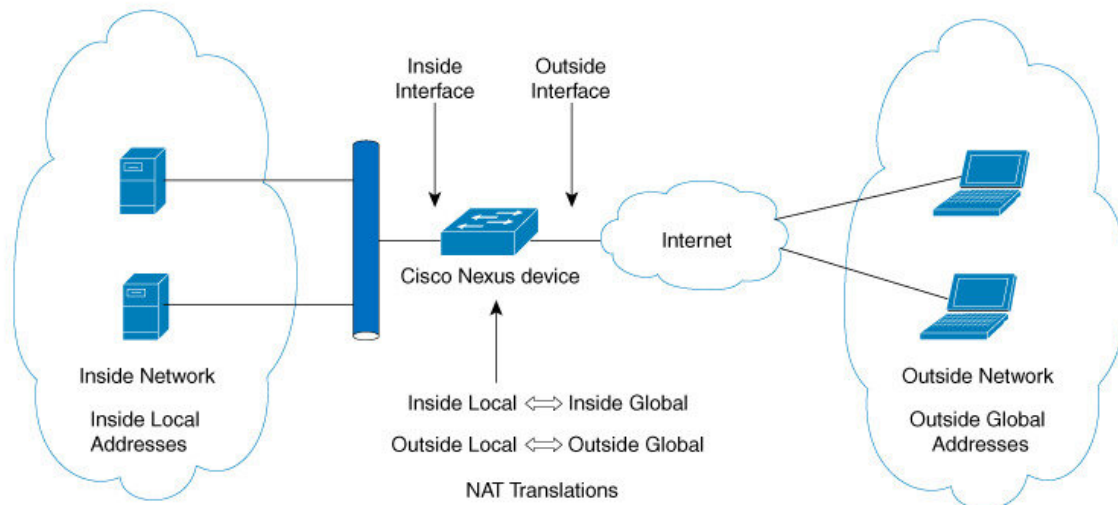
スタティック ネットワーク アドレス変換 (NAT) を使用すると、ユーザは内部ローカルアドレスから外部グローバルアドレスへの 1 対 1 変換を設定することができます。これにより、内部から外部トラフィックおよび外部から内部トラフィックへの IP アドレスとポート番号の両方の変換が可能になります。Cisco Nexus デバイスはヒットレス NAT をサポートします。これは、既存の NAT トラフィック フローに影響を与えずに NAT 設定で NAT 変換を追加または削除できることを意味します。

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 37: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 ネットワーク アドレス変換 (NAT) では、実際の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アドレスのプールに変換されます。またダイナミック NAT では、未登録の IP アドレスと登録済み IP アドレス間で一対一のマッピング確立しますが、通信時にプール内で利用可能な登録済みアドレスによって、マッピングは変化します。

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。



- (注) この項で説明している **ip nat translation sampling-timeout** コマンドはサポートされていません。統計情報はインストール済みの NAT ポリシーに 60 秒ごとに収集されます。これらの統計情報はフローがアクティブかまたはアクティブでないかを決定するために使用されます。

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

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。

- **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。

udp-timeout および **timeout** 値のタイマーは、**ip nat translation sampling-timeout** に設定されたタイムアウト後トリガーされます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) エージングに関して設定可能な次の 3 つの異なるオプションがあります。
- タイムアウト: すべてのタイプのフロー (TCP および UDP 両方) に適用可能です。
 - TCP TIME-OUT: TCP フローにのみ適用可能です。
 - UDP TIME-OUT: UDP フローにのみ適用可能です。



- (注) 設定されたタイムアウトのないダイナミック エントリを作成すると、1 時間のデフォルトのタイムアウトが使用されます (60 秒後)。タイムアウトを設定した後、**clear ip nat translations all** コマンドを入力すると、設定されたタイムアウトが有効になります。タイムアウトは、60 ~ 172800 秒まで設定することができます。

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

Cisco NX-OS は、ダイナミック NAT のプールをサポートします。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返されます。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、PAT は次の IP アドレスに移動して、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。

ダイナミック NAT が、ローカルで使用できない、またはローカルに設定されていない IP アドレスのプールを使用するように設定されている場合、アウトツライントラフィックは DEST MISS と見なされます。この動作により、`show system internal access-list dest-miss stats` コマンドの出力に DEST MISS カウンタの増分が表示されます。DEST MISS 統計情報は、Cisco NX-OS リリース 9.3(5) 以降でサポートされます。Cisco NX-OS リリース 10.1(1) 以降、この機能は Cisco Nexus 9300-FX3 プラットフォーム スイッチでサポートされます。

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 Twice NAT 変換は、事前定義された **ip nat pool** または **インターフェイス過負荷** 設定から動的に送信元 IP アドレスとポート番号の情報を選択します。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。

VRF 対応 NAT

VRF 対応 NAT 機能により、スイッチは VRF（仮想ルーティングおよび転送インスタンス）のアドレス空間を認識し、パケットを変換できます。これにより、NAT 機能は 2 つの VRF 間で使用される重複アドレス空間のトラフィックを変換できます。

VRF 対応 NAT に関する注意事項：

- VRF 対応の NAT 機能は、N9K-9408PC-CFP2、N9K-X9564PX、N9K-C9272Q、N9K-C9272Q、N9K-X9464TX、N9K-X9464TX2、N9K-X9564TX、N9K-X9464PX、N9K-X9536PQ、N9K-X6963 でサポートされています。N9K-X9432PQ、N9K-C9332PQ、N9K-C9372PX、N9K-C9372PX-E、N9K-C9372TX、N9K-C9372TX-E、N9K-C93120TX
- VRF 対応 NAT 機能は Cisco Nexus 9300-EX、9300-FX、9300-FX2、および 9300-GX プラットフォーム スイッチではサポートされていません。



(注) これは、Cisco Nexus 9300-EX および 9300-FX プラットフォーム スイッチの NAT TCAM の制限です。NAT TCAM は VRF 対応ではありません。NAT は、Cisco Nexus 9300-EX、9300-FX、9300-FX2、および 9300-GX プラットフォーム スイッチで重複する IP アドレスでは動作しません。

- Cisco NX-OS リリース 10.2(3)F 以降、VRF 対応 NAT は Cisco Nexus 9300-FX、FX2、GX と GX2 プラットフォーム スイッチでサポートされます。Cisco Nexus 9346C スイッチではサポートされません。
- 1つのnon-default-vrfから別のnon-default-vrfに流れるトラフィックは変換されません。（たとえば、vrfAからvrfB）。
- VRFからグローバルVRFに流れるトラフィックの場合、nat-outside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。
- 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、**match-in-vrf** オプション（**ip nat**）の コマンドは指定できません。
 - 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、**match-in-vrf** オプション（**ip nat**）の コマンドを指定する必要があります。

次に設定例を示します。

```
Switch(config)# ip nat inside source {list <acl-name>} {pool <pool-name> [vrf
<vrf-name> [match-in-vrf]] [overload] | interface <globalAddrInterface> [vrf
<vrf-name> [match-in-vrf]] overload} [group <group-id> dynamic]
```

```
Switch(config)#ip nat outside source list <acl-name> pool <pool-name> [vrf
<vrf-name> [match-in-vrf]] [group <group-id> dynamic]
```

- VRF 対応 NATは、フラグメント化されたパケットをサポートしていません。
- VRF 対応 NATは、アプリケーション層の変換をサポートしていません。
したがって、レイヤ4およびその他の組み込みIPは変換されず、次のエラーが発生します。
 - FTP
 - ICMP障害
 - IPSec
 - HTTPS
- VRF対応NATは、インターフェイス上でNATまたはVACLをサポートします。（ただし、インターフェイスで両方の機能を同時にサポートすることはできません）。
- VRF対応NATは、NAT変換パケットではなく、元のパケットに適用される出力ACLをサポートします。
- VRF対応NATは、デフォルトのVRFのみをサポートします。
- VRF対応NATはMIBサポートを提供しません。
- VRF対応NATはDCNMサポートを提供しません。

- VRF対応NATは、単一のグローバルVDCのみをサポートします。
- VRF対応NATは、アクティブ/スタンバイスーパーバイザモデルをサポートしません。
- サブネットが重複する VRF は、NAT なしで共通の宛先に移動できません。ただし、ダイナミック NAT ルール設定で VRF 間 NAT を使用すると、この機能を実現できます。スタティック NAT 設定は、重複アドレスではサポートされません。

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。

- Broadcom ベースの Cisco Nexus 9000 シリーズ スイッチでは、変換デバイス上の内部グローバルアドレスへのルートが外部インターフェイスを介して到達可能な場合、外部から内部へのネットワーク アドレス変換フローの packets は、ネットワークでソフトウェアで転送、複製、およびループされます。この状況では、このフローの NAT 設定の最後に **add-route** CLI 引数を入力する必要があります。例えば、**ip nat inside source static 192.168.1.1 172.16.1.1 add-route** のようになります。
- vPC を介したスタティック NAT 機能は、Cisco Nexus 9300 プラットフォーム スイッチでサポートされます。
- キーワードが付いている **show** コマンドはサポートされていません。 **internal**
- スタティック NAT 機能は Cisco Nexus 9300 プラットフォーム スイッチでサポートされています。
- スタティック NAT 機能は Cisco Nexus 9200 プラットフォーム スイッチでサポートされています。
- Cisco Nexus 9200 および 9300-EX、-FX、-FX2、-FX3、-FXP、-GX プラットフォーム スイッチ、 **add-route** オプションはポリシーの内部と外部の両方に必要です。



(注) NAT のサポートは、Cisco Nexus 9500 プラットフォーム スイッチでは使用されません。

- 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。
- 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 proxy-arp** コマンドを使用します。 **add-route** キーワードを使用する場合は、**ip proxy-arp** を有効にする必要があります。
- NAT と Flow は同じポートではサポートされません。

- Cisco NX-OS リリース 10.2(1)F 以降では、VXLAN NAT および分散型 Elastic NAT 機能が Cisco Nexus 9300-FX2 プラットフォーム シリーズ スイッチでサポートされます。分散型 Elastic NAT 機能は、VXLAN トポロジのリーフとスパインで NAT を有効にします。
- VXLAN NAT および分散型 Elastic NAT は次をサポートします。
 - Upto 8000 NAT 変換
 - VRF
 - スタティック内部設定のアドルルート
 - IP アドレス設定なしの SVI
- VXLAN および分散型 Elastic NAT は次をサポートしません。
 - IPv6
 - NAT は vPC を認識しません。すべての設定を両方の vPC ピアに適用する必要があります。
- Cisco Nexus デバイスは、次のインターフェイスタイプで 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 とレイヤ 3 サブインターフェイス
- NAT はデフォルトの仮想ルーティングおよびフォワーディング (VRF) テーブルのみでサポートされます。
- 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ていません。
 - ソフトウェアの変換。すべての変換はハードウェアで行われます。
 - 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。
- デフォルトでは、NAT 機能に TCAM エントリは割り当てられません。NAT 機能に TCAM サイズを割り当てるには、他の機能の TCAM サイズを調整します。TCAM は **hardware access-list tcam region nat tcam-size** コマンドで割り当て可能です。
- HSRP および VRRP は NAT インターフェイス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。
- (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。
- NAT は (無中断の) In Service Software Upgrade (ISSU) をサポートしています。
- NAT TCAM が切り分けられている場合、UDF ベースの機能が動作しないことがあります。
- ECMP NAT は Cisco Nexus 9000 スイッチではサポートされません。
- [**ip nat 内部 (ip nat inside)**] または [**ip nat 外部 (ip nat outside)**] などの NAT 構成は、ループバック インターフェイスではサポートされていません。

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。

- Broadcom ベースの Cisco Nexus 9000 シリーズ スイッチでは、変換デバイス上の内部グローバルアドレスへのルートが外部インターフェイスを介して到達可能な場合、外部から内部へのネットワーク アドレス変換フローの packets は、ネットワークでソフトウェアで転送、複製、およびループされます。この状況では、このフローの NAT 設定の最後に **add-route** CLI 引数を入力する必要があります。例えば、**ip nat inside source static 192.168.1.1 172.16.1.1 add-route** のようになります。
- VRF 対応 NAT は、Cisco Nexus 9200 および 9300-EX プラットフォーム スイッチでの内部/外部 IP サブネット アドレスの重複に対してはサポートされません。
- キーワードが付いている **show** コマンドはサポートされていません。 **internal**
- ダイナミック NAT 機能は Cisco Nexus 9300 プラットフォーム スイッチでサポートされています。
- ダイナミック NAT 機能は Cisco Nexus 9200 プラットフォーム スイッチでサポートされています。
- Cisco Nexus 9200 および 9300-EX、-FX、-FX2、-FX3、-FXP、-GX プラットフォーム スイッチ、 **add-route** オプションはポリシーの内部と外部の両方に必要です。
- **interface overload option for inside policies** オプションは、外部および内部ポリシー両方の Cisco Nexus 9200、9300-EX、9300-FX、9300-FX2、9300-FX3、9300-FXP、および 9300-GX プラットフォーム スイッチではサポートされていません。
- VXLAN ルーティングは Cisco Nexus デバイスではサポートされません。
- フラグメント化された packets 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。
- 出力 ACL は、変換されたパケットには適用されません。
- デフォルト以外の仮想ルーティングおよび転送 (VRF) インスタンスはサポートされません。
- 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。
- Cisco Nexus デバイスでは、複数のグローバル仮想デバイスコンテキスト (VDC) 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。
- のタイムアウト値は、設定されたタイムアウト + 119 秒までかかります。
- 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。
- Cisco Nexus 9300 プラットフォームスイッチの ICMP にハードウェアプログラミングが導入されました。したがって、ICMP エントリはハードウェアの TCAM リソースを消費します。ICMP はハードウェア内にあるため、Cisco Nexus プラットフォーム シリーズ スイッチの NAT 変換の最大制限は 1024 に変更されます。リソースを最大限に活用するには、最大 100 ICMP エントリが許可されます。
- Cisco Nexus 9000 シリーズ スイッチで新しい変換を作成すると、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 NAT では、プールのオーバーロードとインターフェイスのオーバーロードは外部 NAT ではサポートされません。
- NAT オーバーロードは PBR (ポリシーベースルーティング) を使用するため、PBR テーブル内の使用可能なネクストホップエントリの最大数によって NAT の規模が決まります。NAT 内部インターフェイスの数が PBR テーブルで使用可能なネクストホップエントリの範囲内にある場合、最大 NAT 変換スケールは変わりません。そうしないと、サポートされる変換の最大数が減少する可能性があります。PBR と NAT オーバーロードは相互に排他的ではありません。相互に制限されています。

- Cisco Nexus デバイスは、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)。
- [**ip nat 内部 (ip nat inside)**] または [**ip nat 外部 (ip nat outside)**] などの NAT 構成は、ループバック インターフェイスではサポートされていません。
- vPC を介したダイナミック NAT 機能はサポートされていません。

ダイナミック Twice NAT の注意事項および制約事項

Broadcom ベースの Cisco Nexus 9000 シリーズ スイッチでは、変換デバイス上の内部グローバルアドレスへのルートが外部インターフェイスを介して到達可能な場合、外部から内部へのネットワークアドレス変換フローの packets は、ネットワークでソフトウェアで転送、複製、およびループされます。この状況では、このフローの NAT 設定の最後に **add-route CLI** 引数を入力する必要があります。例えば、**ip nat inside source static 192.168.1.1 172.16.1.1 add-route** のようになります。

TCP/UDP/ICMP ヘッダーのない IP パケットは、ダイナミック NAT では変換されません。

ダイナミック Twice NAT では、スタティック NAT のフローを作成する前にダイナミック NAT のフローが作成されない場合、ダイナミック Twice NAT のフローは正しく作成されません。

空の ACL が作成されると、**permit ip any any** のデフォルトのルールが設定されます。最初の ACL が空白な場合、NAT-ACL は、さらに ACL エントリと一致しません。

TCP 認識 NAT の注意事項および制約事項

TCP 対応 NAT には次の制限があります。

- TCP 対応 NAT は、Cisco Nexus 9500 および Cisco Nexus 9300-EX、FX、および FX2 シリーズ スイッチでサポートされます。
- Cisco NX-OS リリース 9.3(5) 以降、TCP 対応 NAT は Cisco Nexus N9K-C9316D-GX、N9K-C93600CD-GX、N9K-C9364C-GX スイッチでサポートされます。
- 1 つの範囲のアドレス プールに関連付けることができる一致 ACL は 1 つだけです。プールを一致 ACL に関連付けると、インターフェイス IP を変更したり、プール範囲を変更したりできなくなります。
- ダイナミック NAT 設定で設定または使用する前に、プールを定義する必要があります。
- インターフェイスの過負荷の場合にプール範囲またはインターフェイスアドレスが変更されるたびに、ダイナミック NAT ルールを再設定する必要があります。

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. 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# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# feature nat	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	switch(config)# copy running-config startup-config	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーして、変更を継続的に保存します。

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# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# interface type slot/port	設定するインターフェイスを指定し、インターフェイス コンフィギュレーションモードを開始します。
ステップ 3	switch(config-if)# ip nat {inside outside}	内部または外部としてインターフェイスを指定します。

	コマンドまたはアクション	目的
		(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。 ループバック インターフェイスではこの構成がサポートされていません。
ステップ 4	(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) 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、は内部宛先 IP アドレス (newDst: ip1) への外部宛先 IP アドレス (Dst: ip2) の変換を Cisco Nexus デバイス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 [vrf vrf-name] [match-in-vrf] [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# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# ip nat inside source static <i>local-ip-address global-ip-address [vrf vrf-name]</i> [match-in-vrf] [group group-id]	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ローカル（local）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。 group を指定することにより、スタティック Twice NAT でこの変換が属するグループが指定されます。 (注) Cisco Nexus 9000 シリーズ スイッチで Twice NAT 設定を実行している間は、異なる VRF 間で同じグループ ID を使用できません。一意の Twice NAT ルールには、一意のグループ ID を使用する必要があります。
ステップ 3	(任意) switch(config)# copy running-config startup-config	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーして、変更を継続的に保存します。

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** *outsideGlobalIP outsideLocalIP [vrf vrf-name [match-in-vrf] [group group-id] [dynamic] [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# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# ip nat outside source static <i>outsideGlobalIP outsideLocalIP</i> [vrf vrf-name [match-in-vrf] [group group-id] [dynamic] [add-route]]	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。group を指定することにより、スタティック Twice NAT でこの変換が属するグループが指定されます。ポートなしで内部変換が設定されると、暗黙的な追加ルートが実行されます。外部変換の設定中、最初の追加ルート機能はオプションです。
ステップ 3	(任意) switch(config)# copy running-config startup-config	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーして、変更を継続的に保存します。

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 inside-global-address | {tcp|udp} inside-local-address {local-tcp-port | local-udp-port} inside-global-address {global-tcp-port | global-udp-port}} {vrf vrf-name {match-in-vrf} {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# configure terminal	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	switch(config)# ip nat inside source static { <i>inside-local-address</i> <i>inside-global-address</i> { tcp udp } <i>inside-local-address</i> { <i>local-tcp-port</i> <i>local-udp-port</i> } <i>inside-global-address</i> { <i>global-tcp-port</i> <i>global-udp-port</i> }} { vrf <i>vrf-name</i> { match-in-vrf } { group <i>group-id</i> }}	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)# copy running-config startup-config	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーして、変更を継続的に保存します。

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、サービスを特定の外部ホストに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**} {**vrf** *vrf-name* {**match-in-vrf**}}
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# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# ip nat outside source static { <i>outside-global-address</i> <i>outside-local-address</i> { tcp udp } <i>outside-global-address</i> { <i>global-tcp-port</i> <i>global-udp-port</i> } <i>outside-local-address</i> { <i>global-tcp-port</i> <i>global-udp-port</i> }} { group <i>group-id</i> } { add-route } { vrf <i>vrf-name</i> { match-in-vrf }}	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。 group を指定することにより、スタティック Twice NAT でこの変換が属するグループが指定されます。ポートなしで内部変換が設定されると、暗黙的な追加ルートが実行されます。外部変換の設定中、最初の追加ルート機能はオプションです。

	コマンドまたはアクション	目的
ステップ 3	(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**] [**add-route**]
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	enable 例： <code>switch> enable</code>	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。

	コマンドまたはアクション	目的
ステップ 2	configure terminal 例： switch# configure terminal	特権 EXEC モードを開始します。
ステップ 3	ip nat inside source static <i>inside-local-ip-address</i> <i>inside-global-ip-address</i> [group <i>group-id</i>] [add-route] 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。 • group 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	ip nat outside source static <i>outside-global-ip-address</i> <i>outside-local-ip-address</i> [group <i>group-id</i>] [add-route] 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。 • group 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 5	interface <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	ip address <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	ip nat inside 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。 (注) ループバック インターフェイスでは構成がサポートされていません。
ステップ 8	exit 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 9	interface <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	ip address <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。

	コマンドまたはアクション	目的
ステップ 11	ip nat outside 例： <pre>switch(config-if)# ip nat outside</pre>	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。 (注) ループバック インターフェイスでは構成がサポートされていません。
ステップ 12	end 例： <pre>switch(config-if)# end</pre>	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。

no-alias 設定の有効化と無効化

NAT デバイスは内部グローバル (IG) アドレスと外部ローカル (OL) アドレスを所有し、これらのアドレス宛での ARP 要求に応答します。IG/OL アドレス サブネットがローカル インターフェイス サブネットと一致すると、NAT は IP エイリアスと ARP エントリをインストールします。この場合、デバイスは `local-proxy-arp` を使用して ARP 要求に応答します。

`no-alias` 機能は、アドレス範囲が外部インターフェイスの同じサブネットにある場合、特定の NAT プール アドレス範囲からのすべての変換された IP の ARP 要求に応答します。

NAT が設定されたインターフェイスで `no-alias` が有効になっている場合、外部インターフェイスはサブネット内の ARP 要求に応答しません。`no-alias` を無効にすると、外部インターフェイスと同じサブネット内の IP に対する ARP 要求が処理されます。



(注) この機能をサポートしていない古いリリースにダウングレードすると、`no-alias` オプションの設定が削除されることがあります。

手順の概要

1. `switch# configure terminal`
2. `switch(config)# feature nat`
3. `switch(config)# show run nat`
4. `switch(config)# show ip nat-alias`
5. `switch(config)# clear ip nat-alias ip address/all`

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。

	コマンドまたはアクション	目的
ステップ 2	switch(config)# feature nat	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	switch(config)# show run nat	NAT の設定を表示します。
ステップ 4	switch(config)# show ip nat-alias	エイリアスが作成されたかどうかの情報を表示します。 (注) デフォルトでは、エイリアスが作成されます。エイリアスを無効にするには、 no-alias キーワードをコマンドに追加する必要があります。
ステップ 5	switch(config)# clear ip nat-alias ip address/all	エイリアスリストからエントリを削除します。特定のエントリを削除するには、削除する IP アドレスを指定する必要があります。すべてのエントリを削除するには、すべてのキーワードを使用します。

例

次に、すべてのインターフェイスの情報を表示する例を示します。

```
switch# configure terminal
switch(config)# show ip int b
IP Interface Status for VRF "default"(1)
Interface          IP Address      Interface Status
Lo0                 100.1.1.1      protocol-up/link-up/admin-up
Eth1/1             7.7.7.1        protocol-up/link-up/admin-up
Eth1/3             8.8.8.1        protocol-up/link-up/admin-up
```

次に、実行コンフィギュレーションの例を示します。

```
switch# configure terminal
switch(config)# show running-config nat
!Command: show running-config nat
!Running configuration last done at: Thu Aug 23 11:57:01 2018
!Time: Thu Aug 23 11:58:13 2018

version 9.2(2) Bios:version 07.64
feature nat
interface Ethernet1/1
 ip nat inside
interface Ethernet1/3
 ip nat outside
switch(config)#
```

この例は、エイリアスを設定する例を示します。

```
switch# configure terminal
switch(config)# ip nat pool p1 7.7.7.2 7.7.7.20 prefix-length 24
switch(config)# ip nat inside source static 1.1.1.2 8.8.8.3
switch(config)# ip nat outside source static 2.2.2.1 7.7.7.3
switch(config)# show ip nat-alias
Alias Information for Context: default
```

```

Address      Interface
7.7.7.2      Ethernet1/1
8.8.8.2      Ethernet1/3
switch(config)#

```

次に、`show ip nat-alias` の出力例を示します。デフォルトでは、エイリアスが作成されます。

```

switch# configure terminal
switch(config)# show ip nat-alias
Alias Information for Context: default
Address      Interface
7.7.7.2      Ethernet1/1
8.8.8.2      Ethernet1/3
switch(config)#

```

この例は、エイリアスを無効にする方法を示します。

```

switch# configure terminal
switch(config)# ip nat pool p1 7.7.7.2 7.7.7.20 prefix-length 24 no-alias
switch(config)# ip nat inside source static 1.1.1.2 8.8.8.3 no-alias
switch(config)# ip nat outside source static 2.2.2.1 7.7.7.3 no-alias
switch(config)# show ip nat-alias
Alias Information for Context: default
Address      Interface
7.7.7.2      Ethernet1/1
8.8.8.2      Ethernet1/3
switch(config)#

```

```

** None of the entry got appended as alias is disabled for above CLIs.
switch(config)#

```

この例は、エイリアスをクリアする方法を示します。エイリアスリストからエントリを削除するには、`clear ip nat-alias` を使用します。IP アドレスを指定して 1 つのエントリを削除することも、すべてのエイリアス エントリを削除することもできます。

```

switch# configure terminal
switch(config)# clear ip nat-alias address 7.7.7.2
switch(config)# show ip nat-alias
Alias Information for Context: default
Address      Interface
8.8.8.2      Ethernet1/3
switch(config)#
switch(config)# clear ip nat-alias all
switch(config)# show ip nat-alias
switch(config)#

```

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

```

例：スタティック Twice NAT の設定

```
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# sh ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
--- ---              ---              51.3.1.1          104.1.1.1
--- ---              ---              95.4.1.1          95.3.1.1
--- ---              ---              96.4.1.1          96.3.1.1
--- ---              ---              51.40.1.1         140.1.1.1
--- ---              ---              51.42.1.1         142.1.2.1
--- ---              ---              51.1.2.1          102.1.2.1
--- 11.1.1.1          101.1.1.1        ---              ---
--- 11.3.1.1          103.1.1.1        ---              ---
--- 11.39.1.1         139.1.1.1        ---              ---
--- 11.41.1.1         141.1.1.1        ---              ---
--- 95.1.1.1          149.1.1.1        ---              ---
--- 96.1.1.1          149.2.1.1        ---              ---
--- 130.1.1.1:590     30.1.1.100:5000  ---              ---
--- 130.2.1.1:590     30.2.1.100:5000  ---              ---
--- 130.3.1.1:590     30.3.1.100:5000  ---              ---
--- 130.4.1.1:590     30.4.1.100:5000  ---              ---
--- 130.1.1.1:591     30.1.1.101:5000  ---              ---

switch# sh ip nat translations verbose
Pro Inside global      Inside local      Outside local      Outside global
any ---              ---              22.1.1.3          22.1.1.2
  Flags:0x200009 time-left(secs):-1 id:0 state:0x0 grp_id:10
any 11.1.1.130        11.1.1.3         ---              ---
  Flags:0x1 time-left(secs):-1 id:0 state:0x0 grp_id:0
any 11.1.1.133        11.1.1.33        ---              ---
  Flags:0x1 time-left(secs):-1 id:0 state:0x0 grp_id:10
any 11.1.1.133        11.1.1.33        22.1.1.3         22.1.1.2
  Flags:0x200009 time-left(secs):-1 id:0 state:0x0 grp_id:0
tcp 10.1.1.100:64490   10.1.1.2:0       20.1.1.2:0       20.1.1.2:0
  Flags:0x82 time-left(secs):43192 id:31 state:0x3 grp_id:0 vrf: default
N9300-1#
```

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* [**vrf** *vrf-name* [**match-in-vrf** **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 max-entries** *number-of-entries*
17. **ip nat translation timeout** *seconds*
18. **ip nat translation creation-delay** *seconds*
19. **ip nat translation icmp-timeout** *seconds*
20. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例： 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	configure terminal 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。
ステップ 3	ip access-list <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	permit <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	deny <i>protocol source source-wildcard any</i> 例： Switch(config-acl)# deny udp 10.111.11.100/32 any	ネットワークに入る時に拒否されるパケットの条件を IP アクセスリストに設定します。
ステップ 6	exit 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。

	コマンドまたはアクション	目的
ステップ 7	<p>ip nat inside source list <i>access-list-name</i> interface type number [vrf vrf-name [match-in-vrf] overload]</p> <p>例 :</p> <pre>Switch(config)# ip nat inside source list acl1 interface ethernet 1/1 overload</pre>	<p>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。</p>
ステップ 8	<p>interface type number</p> <p>例 :</p> <pre>Switch(config)# interface ethernet 1/4</pre>	<p>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。</p>
ステップ 9	<p>ip address ip-address mask</p> <p>例 :</p> <pre>Switch(config-if)# ip address 10.111.11.39 255.255.255.0</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 10	<p>ip nat inside</p> <p>例 :</p> <pre>Switch(config-if)# ip nat inside</pre>	<p>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。</p> <p>(注) ループバック インターフェイスでは構成がサポートされていません。</p>
ステップ 11	<p>exit</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 12	<p>interface type number</p> <p>例 :</p> <pre>Switch(config)# interface ethernet 1/1</pre>	<p>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。</p>
ステップ 13	<p>ip address ip-address mask</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>ip nat outside</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> <p>(注) ループバック インターフェイスでは構成がサポートされていません。</p>
ステップ 15	<p>exit</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>

	コマンドまたはアクション	目的
ステップ 16	ip nat translation max-entries <i>number-of-entries</i> 例： Switch(config)# ip nat translation max-entries 300	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。
ステップ 17	ip nat translation timeout <i>seconds</i> 例： switch(config)# ip nat translation timeout 13000	ダイナミック NAT 変換のタイムアウト値を指定します。
ステップ 18	ip nat translation creation-delay <i>seconds</i> 例： switch(config)# ip nat translation creation-delay 250	ダイナミック NAT 変換の ICMP タイムアウト値を指定します。 (注) ハードウェアでの NAT エントリのプログラミング頻度を減らすために、NAT は変換を 1 秒間バッチ処理してプログラミングします。ハードウェアのプログラミングを頻繁に行うと CPU に負荷がかかりますが、プログラミングを遅らせるとセッションの確立が遅れます。このコマンドを使用して、バッチ処理を無効にしたり、作成遅延を短縮したりできます。作成遅延を 0 に設定することは推奨されません。
ステップ 19	ip nat translation icmp-timeout <i>seconds</i> 例： switch(config)# ip nat translation icmp-timeout 100	ダイナミック NAT 変換の ICMP タイムアウト値を指定します。
ステップ 20	end 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

単一の **ip nat pool** コマンドで IP アドレスの範囲を定義することにより、コマンドを使用するか、**ip nat pool** を使用します および **address** コマンドを使用することにより NAT プールを作成できます。

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# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# feature nat	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)# ip nat pool <i>pool-name</i> [<i>startip endip</i>] { prefix <i>prefix-length</i> netmask <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)# address <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)# no ip nat pool <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 pool15 20.1.1.1 20.1.1.5 netmask 255.0.255.0
switch(config)#
```

この例では、NAT プールを作成し、**ip nat pool** を使用してグローバル IP アドレスの範囲を定義します。および **address** コマンドを使用した NAT プールの作成およびグローバル IP アドレスの範囲の定義方法を示します。

```
switch# configure terminal
switch(config)# ip nat pool pool17 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# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	(任意) switch# ip nat inside source list list-name pool pool-name [overload]	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# ip nat outside source list list-name pool pool-name [add-route]	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*] [**dynamic**] [**add-route**]
3. switch(config)# **ip nat inside source list** *access-list-name* [**interface** *type slot/port overload* | **pool** *pool-name overload*] [**group** *group-id*] [**dynamic**] [**add-route**]
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# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# ip nat outside source static <i>outside-global-ip-address outside-local-ip-address</i> [tcp udp] <i>outside-global-ip-address outside-global-port outside-local-ip-address outside-local-port</i> [group <i>group-id</i>] [dynamic] [add-route]	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。 group キーワードは、変換が属するグループを決定します。

	コマンドまたはアクション	目的
ステップ 3	switch(config)# ip nat inside source list <i>access-list-name</i> [interface <i>type slot/port overload</i> pool <i>pool-name</i> overload] [group <i>group-id</i>] [dynamic] [add-route]	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。 group 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)# ip nat pool <i>pool-name</i> [<i>startip endip</i>] { prefix <i>prefix-length</i> netmask <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 5	switch(config)# interface <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)# ip nat outside	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)# 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 8	switch(config)# interface <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)# 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。

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**] [**add-route**]
3. switch(config)# **ip nat outside source list** *access-list-name pool pool-name* [**group** *group-id*] **dynamic** [**add-route**]
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# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# ip nat inside source static <i>inside-local-ip-address inside-global-ip-address</i> [tcp udp] <i>inside-local-ip-address local-port inside-global-ip-address global-port</i> [group <i>group-id</i>] [dynamic] [add-route]	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。 group 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)# ip nat outside source list <i>access-list-name pool pool-name</i> [group <i>group-id</i>] dynamic [add-route]	オーバーロードの有無にかかわらずプールを使用した NAT 外部送信元リストを作成することにより、ダイナミック送信元変換を確立します。
ステップ 4	switch(config)# ip nat pool <i>pool-name</i> [<i>startip endip</i>] { prefix <i>prefix-length</i> netmask <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 5	switch(config)# interface <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)# ip nat outside	インターフェイスを外部ネットワークに接続します。

	コマンドまたはアクション	目的
ステップ 7	switch(config-if)# 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 8	switch(config)# interface type slot/port	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)# 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。

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_1 pool pool_1 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
```

FINRST および SYN タイマーの設定

ここでは、FINRST および SYN タイマー値の設定方法について説明します。スイッチをリロードする場合、設定された FINRST や SYN タイマー値の復元または消去は、TCP TCAM が切り分けられるかどうかによって異なります。TCAM が切り分けられると、スイッチは現在設定されている値を復元します。タイマー値が設定されていない場合、デフォルト値の 60 が設定されます。TCAM が切り分けられていない場合、スイッチは現在設定されている値をすべて削除し、デフォルト値を **never** に設定します。これは、TCP TCAM が切り分けられていない場合、TCP AWARE 機能がディセーブルになるためです。

始める前に

手順の概要

1. switch# **configure terminal**
2. switch(config-if)# **ip nat translation syn-timeout {seconds | never}**
3. switch(config-if)# **ip nat translation finrst-timeout {seconds | never}**

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# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config-if)# ip nat translation syn-timeout {seconds never}	SYN 要求を送信するが SYN-ACK 応答を受信しない TCP データのパケット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。TCP TCAM が切り分けられる場合、デフォルト値は 60 秒です。TCP TCAM が切り分けられていない場合、デフォルト値は <i>never</i> です。 <i>never</i> キーワードは、SYN タイマーを非アクティブにします。 (注) TCP TCAM が切り分けられていない場合は、SYN タイマーを設定できません。
ステップ 3	switch(config-if)# ip nat translation finrst-timeout {seconds never}	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 と FIN の両方の動作を設定する必要があります。タイムアウト値の範囲は、1～172800 秒です。TCP TCAM が切り分けられる場合、デフォルト値は 60 秒です。TCP TCAM が切り分けられていない場合、デフォルト値は <i>never</i> です。 <i>never</i> キーワードは、FIN または RST タイマーを非アクティブにします。 (注) TCP TCAM が切り分けられていない場合は、FINRST タイマーを設定できません。

例

次の例は、TCP TCAM が切り分けられるタイミングを示しています。

```
switch(config)# ip nat translation syn-timeout 20
```

次の例は、TCP TCAM が切り分けられていない場合を示しています。

```
switch(config)# ip nat translation syn-timeout 20
Error: SYN TIMER CONFIG FAILED.TCP TCAM NOT CONFIGURED
```

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
clear ip nat translation [all inside <i>global-ip-address local-ip-address</i> [outside <i>local-ip-address global-ip-address</i>] outside <i>local-ip-address global-ip-address</i>]	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
show ip nat translations	アクティブなネットワーク アドレス変換 (NAT) 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。
show run nat	NAT の設定を表示します。
show ip nat max	アクティブなネットワーク アドレス変換 (NAT) の最大値を表示します。
show ip nat statistics	NAT 統計情報をモニタします。

例

次に、IP NAT 最大値を表示する例を示します。

```
switch# show ip nat max

IP NAT Max values
=====
Max Dyn Translations:80
Max all-host:0
No.Static:0
No.Dyn:1
No.Dyn-ICMP:1
=====
```


Switch(config)#

次に、NAT 統計情報を表示する例を示します。

```
switch# show ip nat statistics

IP NAT Statistics
=====
Stats Collected since: Mon Feb 24 18:27:34 2020
-----
Total active translations: 1
No.Static: 0
No.Dyn: 1
No.Dyn-ICMP: 1
-----
Total expired Translations: 0
SYN timer expired: 0
FIN-RST timer expired: 0
Inactive timer expired: 0
-----
Total Hits: 2                Total Misses: 2
In-Out Hits: 0              In-Out Misses: 2
Out-In Hits: 2              Out-In Misses: 0
-----
Total SW Translated Packets: 2
In-Out SW Translated: 2
Out-In SW Translated: 0
-----
Total SW Dropped Packets: 0
In-Out SW Dropped: 0
Out-In 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
-----
Total TCP session established: 0
Total TCP session closed: 0
-----
NAT Inside Interfaces: 1
Ethernet1/34

NAT Outside Interfaces: 1
Ethernet1/32
-----
Inside source list:
+++++

Access list: T2
RefCount: 1
Pool: T2 Overload
Total addresses: 10
Allocated: 1 percentage: 10%
Missed: 0

Outside source list:
+++++
=====
Switch(config)#
```

```
Switch(config)#
```

```
**No.Dyn-ICMP field is to display the no of icmp dynamic translations , its a subset
of "No.Dyn" field.
```



(注) Cisco NX-OS リリース 9.3(5) 以降では、**No.Dyn-ICMP** フィールドは **No.Dyn** フィールドのサブセットであり、**ICMP** ダイナミック変換の数が表示されます。

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
```

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
```

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 max-entries 300
Switch(config)# ip nat translation timeout 13000
Switch(config)# end
```

例: ダイナミック変換および変換タイムアウトの設定



第 13 章

IP イベント減衰の設定

- [IP イベント減衰の概要 \(477 ページ\)](#)
- [注意事項と制約事項 \(478 ページ\)](#)
- [インターフェイス状態変化イベント \(478 ページ\)](#)
- [関連コンポーネント \(479 ページ\)](#)
- [IP イベント減衰の設定方法 \(480 ページ\)](#)

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ドバ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。

注意事項と制約事項

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。IP イベント ダンプニング機能を設定する前に、次のガイドラインと制限事項を参照してください。

- Cisco NX-OS リリース 9.2(1) 以降、IP イベント ダンプニングは Cisco Nexus 9300-EX、9300-FX、9300-FX2、9300-FXP、9700-EX、および9700-FX プラットフォーム スイッチでサポートされます。
- 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。
- ペナルティが抑制しきい値を超えると、インターフェイスはダンプニングされます。ペナルティが Reuse しきい値を下回ると抑制されません。
- 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、ポートチャネル、および SVI がこの機能をサポートしています。

インターフェイス状態変化イベント

IP イベント ダンプ機能は、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衰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。

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します。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。

IP イベント ダンプニング コンフィギュレーション コマンドは、IP と CLNS の両方のルーティング プロトコルにダンプニングを適用します。

パラメータの最初のセット ([half-life|restart|suppress max-suppress]) は、ダンプニングアルゴリズムのさまざまなパラメータを設定します。2 番目のセット ([restart [penalty]]) は、インターフェイスがリブート後に最初に起動したときにダンプニングペナルティを適用できるようにします。デフォルトの再起動ペナルティは、restart パラメータを指定した場合のみ適用されます。どちらのパラメータセットもオプションです。

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。

ルートのタイプ

- 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. **no dampening**
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface <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	dampening [<i>half-life-period reuse-threshold</i>] [<i>suppress-threshold max-suppress</i> [<i>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"> • 引数なしで dampening 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。 • 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。
ステップ 4	no dampening	インターフェイス減衰をディスエーブル化します。
ステップ 5	end	インターフェイス コンフィギュレーション モードを終了します。

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 イベント減衰機能の設定を確認します。

手順の概要

1. **show ip interface** [*interface*]
2. **show dampening interface**
3. **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	show ip interface [interface]	ペナルティ情報を含む、設定されているすべての衰退パラメータを表示します。インターフェイスで IP が有効になっている場合にのみ出力が表示されます。
ステップ 2	show dampening interface	減衰されたインターフェイスを表示します。
ステップ 3	show interface dampening	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。

IP ダンプニングパラメータのデフォルト設定

表 19: IP ダンプニングパラメータのデフォルト値

パラメータ	範囲	デフォルト
Half-life	1～30	5
再使用しきい値	1～20000	800
抑制しきい値	1～20000	2000
最大抑制時間	1～255 秒	20 秒
再起動ペナルティの適用		False
再起動ペナルティ	true / false	false



第 14 章

IP TCP MSS の設定

- [IP TCP MSS について \(483 ページ\)](#)
- [IP TCP MSS のデフォルト設定 \(483 ページ\)](#)
- [IP TCP MSS の注意事項と制約事項 \(484 ページ\)](#)
- [IP TCP MSS の設定 \(484 ページ\)](#)
- [IP TCP MSS の確認 \(486 ページ\)](#)

IP TCP MSS について

IP TCP 最大セグメントサイズ (MSS) 機能を使用すると、スイッチは Cisco Nexus 9000 シリーズスイッチで発信または終端するすべての TCP 接続の最大セグメントサイズを設定できます。TCP ヘッダーフィールドの MSS は、ホストが単一のセグメントで送受信できる最大データサイズまたはペイロードです。デフォルトでは、Cisco Nexus 9000 シリーズスイッチは、IPv4 TCP 接続の場合は 536 バイト、IPv6 TCP 接続の場合は 1240 バイトに設定します。このデフォルト値は、最初の TCP 接続の確立時にスイッチによって設定されます。

TCP 接続の発信元であるスイッチは、MSS を常にユーザ設定の MSS に設定するか、またはルートインターフェイス MTU とプロトコルヘッダーの差のいずれか小さい方に設定します。したがって、ホスト A は 1460 バイトの提案された MSS を持つ SYN パケットをホスト B に送信します。提案された MSS を持つ SYN パケットを受信した後、ホスト B はホスト A に SYN-ACK パケットを送信し、TCP 接続の提案された MSS 値を受け入れます。ホスト A はホスト B に ACK パケットを送信し、TCP 接続の MSS 値を 1460 に設定します。

IP TCP MSS のデフォルト設定

表 20: IP TCP MSS のデフォルト設定

パラメータ	デフォルト設定
IP TCP MSS	IPv4 TCP 接続の場合は 536 バイト IPv6 TCP 接続の場合は 1240 バイト

IP TCP MSS の注意事項と制約事項

IPv4 TCP 接続で MSS を 1460 バイトを超える値に設定する必要がある場合、対応する MTU 値は、必要な MSS 値に 40 バイトを加えた値に設定する必要があります。IPv6 TCP 接続で MSS を 1440 バイトを超える値に設定する必要がある場合、対応する MTU 値は、必要な MSS 値に 60 バイトを加えた値に設定する必要があります。

IP TCP MSS の設定

[TCP 接続の MSS の設定 \(484 ページ\)](#)

[設定済み IP TCP MSS の削除 \(485 ページ\)](#)

TCP 接続の MSS の設定

始める前に

手順の概要

1. switch# **configure terminal**
2. switch(config)# **ip tcp mss** <bytes>
3. switch# **show ip tcp mss**

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# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# ip tcp mss <bytes>	最大セグメント サイズを設定します。
ステップ 3	switch# show ip tcp mss	設定された IP TCP MSS を表示します。

例: 実行コンフィギュレーション

例

この例では、実行コンフィギュレーションと、設定された IP TCP MSS を表示する確認コマンドを示します。

```
configure terminal
ip tcp mss 5000
Setting TCP MSS to 5000 bytes
```

```
switch# show ip tcp mss
TCP MSS value 5000 bytes
```

設定済み IP TCP MSS の削除

手順の概要

1. switch# **configure terminal**
2. switch(config)# **no ip tcp mss**
3. switch# **show ip tcp mss**

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# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# no ip tcp mss	設定された IP TCP MSS を削除し、IP TCP MSS をデフォルト値に設定します。
ステップ 3	switch# show ip tcp mss	設定された IP TCP MSS を表示します。

例: 実行コンフィギュレーション

例

この例では、実行コンフィギュレーションと、設定された IP TCP MSS を表示する確認コマンドを示します。

```
configure terminal
no ip tcp mss 5000
Setting default MSS value is 536 bytes
```

```
switch# show ip tcp mss
TCP MSS value 536 bytes
```

例 : TCP 接続の MSS の設定

次に、TCP 接続の MSS を設定する例を示します。

```
configure terminal
ip tcp mss 2000
```

例 : 設定済み IP TCP MSS の削除

次に、MSS を削除する例を示します。

```
configure terminal  
no ip tcp mss
```

IP TCP MSS の確認

表 21: IP TCP MSS の確認

コマンド	目的
<code>show ip tcp mss</code>	設定されている IP TCP MSS を表示します。



第 15 章

単方向イーサネットの設定

この章では、Cisco Nexus 9000 シリーズ スイッチで双方向イーサネットを設定する方法を説明します。

- [単方向イーサネットの\(UDE\)概要 \(487 ページ\)](#)
- [単方向イーサネットの注意事項と制約事項 \(487 ページ\)](#)
- [単方向イーサネットの設定 \(488 ページ\)](#)

単方向イーサネットの(UDE)概要

単方向イーサネットでは、一方向トラフィックの送信または受信に、2本の光ファイバではなく、光ファイバを1本だけ使用します。

単方向リンクでは、ビデオストリーミングなどのアプリケーションのトラフィックを送信または受信します。送信されるほとんどのトラフィックは確認されません。双方向トランシーバを装備したポートを単方向で送受信するように設定することで、単方向リンクを作成できます。適切な単方向トランシーバが使用できない場合は、UDEを使用できます。たとえば、サポートされる送信専用トランシーバがない場合は、ソフトウェアベース UDE で送信専用リンクを設定する必要があります。

単方向イーサネットの注意事項と制約事項

- UDE 送信専用がサポートされます。
- UDE 受信専用は、Cisco NX-OS リリース 10.1(1) までサポートされていません。
- Cisco NX-OS リリース 10.1(2) 以降では、UDE 受信専用もサポートされています。
- Cisco NX-OS リリース 10.1(2) 以降、UDE は N9K-X9624D-R2、N9K-X9636Q-R、N9K-X9636C-RX、N9K-X96136YC-R、N9K-X9624D-R2、N9K-X9636C-R、Cisco Nexus 3636C-R、および Cisco Nexus 36180YC-R モジュールでサポートされます。
- UDE は、すべてのポートで同時に有効にできます。

- ブレークアウトの UDE は、Cisco NX-OS リリース 10.1(1) 以降のリリースからサポートされます。
- ハードウェア レベルの UDE は、X97160YC-EX ラインカードを搭載した Cisco Nexus 9500 スイッチでのみサポートされます。
- UDE はネイティブ 10G-LR/10G-LRS トランシーバでのみサポートされ、QSA またはブレークアウト ケーブルでは使用できません。
- Cisco NX-OS リリース 10.1(1) 以降、UDE は N9K-C9336C-FX2、N9KC93240YC-FX2、N9K-C93180YC-FX、N9K-C93360YC-FX2 TOR、および N9K-X97160YC-EX ラインカードでサポートされています。
- Cisco NX-OS リリース 10.1(1) 以降、UDE は 10G-SR、10G-AOC、40G-SR、40G-LR、40G-AOC、100G-SR、100G-LR、および 100G-AOC の各トランシーバをサポートしています。
- ポートで UDE を設定すると、ポートフラップが発生することがあります。
- UDE 設定の有無にかかわらず、物理インターフェイスをポートチャンネルに追加できます。ただし、ポートチャンネルに送信専用インターフェイスだけが追加されていることを確認する必要があります。送信専用設定を他のインターフェイスと混在させると、UDE が期待どおりに動作しないことがあります。
- すべてのメンバーが UDE 送信専用として設定されている場合、ポートチャンネルはパケットを受信できません。
- すべてのメンバーが UDE 送信専用として設定されている場合、ポートチャンネルはパケットを受信できません。これにより LCAP ベースのポートチャンネルが作動しないようにすることが可能です。
- 特別なコントロールプレーントラフィック プルーニングは、送信専用ポートでは設定されません。
- 単一方向ポートでは、次のようにリンクの反対側の終端にあるポートとのネゴシエーションが必要になる機能またはプロトコルがサポートされません。双方向通信を必要とするすべての機能を無効にする必要があります。

単一方向イーサネットの設定

単一方向イーサネットを設定するには、次の手順を実行します。

手順の概要

1. **configure terminal**
2. **interface ethernet {type slot /port}**
3. **unidirectional send-only**
4. **unidirectional receive-only**
5. **exit**

- 6. **show running-config interface {type slot /port}**
- 7. **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	configure terminal 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface ethernet {type slot /port} 例： switch(config)# interface ethernet 3/1	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	unidirectional send-only 例： switch(config)# unidirectional send-only	単方向送信（送信のみ）モードを設定します。
ステップ 4	unidirectional receive-only 例： switch(config)# unidirectional receive-only	単方向送信（受信のみ）モードを設定します。
ステップ 5	exit 例： switch(config)# exit	インターフェイス モードを終了します。
ステップ 6	show running-config interface {type slot /port} 例： switch(config)# show running-config interface ethernet 3/1	指定されたインターフェイスに関する設定情報を表示します。
ステップ 7	copy running-config startup-config 例： switch(config)# copy running-config startup-config	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。



第 16 章

レイヤ 2 Data Center Interconnect の設定

このセクションでは、仮想ポートチャンネル (vPC) を使用したレイヤ 2 データセンター相互接続 (DCI) を設定する方法について説明します。

- [概要 \(491 ページ\)](#)
- [レイヤ 2 Data Center Interconnect の例 \(492 ページ\)](#)

概要

データセンターインターコネクト (DCI) の目的は、異なるデータセンター間で特定の VLAN を拡張することです。DCIは、長距離で分離されたサーバおよびネットワーク接続ストレージ (NAS) デバイスにレイヤ 2 隣接関係を提供します。

Cisco NX-OS リリース 7.0(3)I2(2) 以降の Cisco Nexus 9000 シリーズ スイッチは、FHRP 分離を使用した DCI をサポートします。ただし、N9K-X9636C-R および N9K-X9636Q-R ラインカードを搭載した Cisco Nexus 9500 スイッチでは、FHRP 分離を使用した DCI はサポートされていません。vPC を使用して複数のサイト間に単一の論理リンクを作成すると、DCI vPC ポートチャンネル全体で BPDU フィルタリングを使用した STP 分離の利点を活用できます。この設定では、ブリッジプロトコルデータユニット (BPDU) はデータセンター間を通過せず、サイト間の STP 障害ドメインを効果的に分離します。

Cisco Nexus 9000 シリーズスイッチは、FHRP 分離を使用した DCI をサポートします。ただし、N9K-X9636C-R および N9K-X9636Q-R ラインカードを搭載した Cisco Nexus 9500 スイッチでは、FHRP 分離を使用した DCI はサポートされていません。vPC を使用して複数のサイト間に単一の論理リンクを作成すると、DCI vPC ポートチャンネル全体で BPDU フィルタリングを使用した STP 分離の利点を活用できます。この設定では、ブリッジプロトコルデータユニット (BPDU) はデータセンター間を通過せず、サイト間の STP 障害ドメインを効果的に分離します。



(注) 最大 2 つのデータセンターを相互接続するには、vPC を使用してください。



- (注) サポートされているプラットフォームには、N9K-X9636C-R、N9K-X9636Q-R、N9K-X9636C-RX ラインカードを搭載した Cisco Nexus 9500 シリーズ スイッチがあります。

レイヤ 2 Data Center Interconnect の例

次に、vPCを使用したレイヤ2データセンターインターコネクト (DCI) の設定例を示します。次の例は、ファースト ホップ冗長性プロトコル (FHRP) 分離を可能にします。

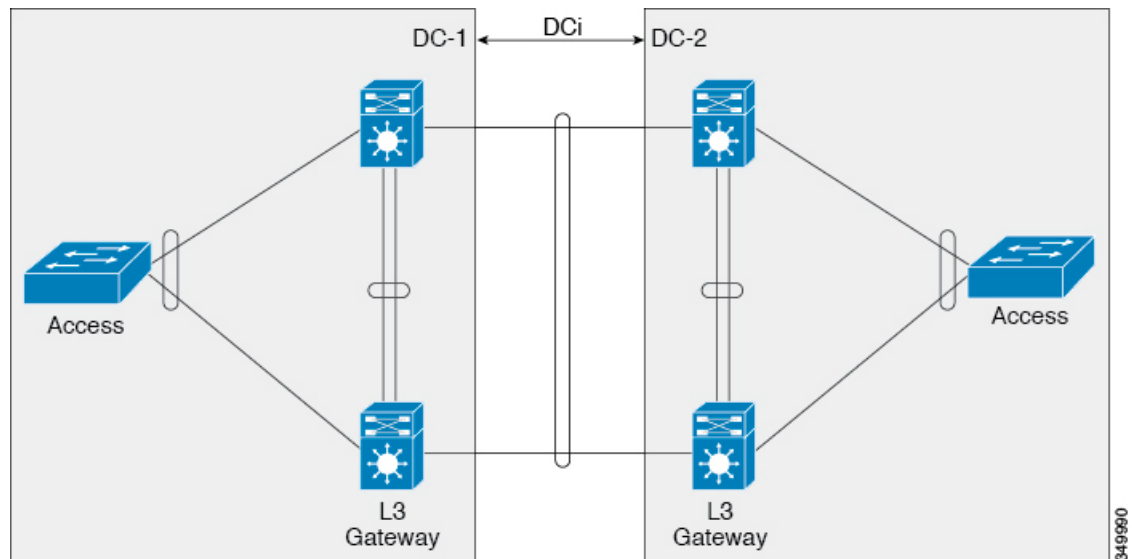


- (注) vPCおよびホットスタンバイルーティングプロトコル (HSRP) はすでに設定されています。



- (注) DCI として機能する Link Aggregation Control Protocol (LACP) を vPC リンク で使用する必要があります。

図 38: デュアル レイヤ 2/レイヤ 3 の POD 相互接続



この例では、同じ vPC のペアでレイヤ 3 (L3) ゲートウェイが設定され、DCI として機能します。Hot Standby Routing Protocol (HSRP) を分離するには、DCI ポート チャンネルでポート アクセス コントロール リスト (PACL) を設定し、DCI を横断して移動する VLAN 用のスイッチ 仮想 インターフェイス (SVI) 上で HSRP Gratuitous Address Resolution Protocol (ARP) (GARP) を無効にする必要があります。

```
ip access-list DENY_HSRP_IP
 10 deny udp any 224.0.0.2/32 eq 1985
```

```
20 deny udp any 224.0.0.102/32 eq 1985
30 permit ip any any

interface <DCI-Port-Channel>
 ip port access-group DENY_HSRP_IP in

interface Vlan <x>
 no ip arp gratuitous hsrp duplicate
```




第 17 章

Cisco NX-OS インターフェイスがサポートする IETF RFC

ここでは、Cisco NX-OS でサポートされているインターフェイスの IETF RFC を示します。

- [IPv6 の RFC \(495 ページ\)](#)

IPv6 の RFC

RFC	タイトル
RFC 1981 (7.0(3)I1(1)以降)	『 <i>Path MTU Discovery for IP version 6</i> 』
RFC 2373	『 <i>IP Version 6 Addressing Architecture</i> 』
RFC 2374	集約可能なグローバルユニキャスト形式
RFC 2460	『 <i>Internet Protocol, Version 6 (IPv6) Specification</i> 』
RFC 2462	『 <i>IPv6 Stateless Address Autoconfiguration</i> 』
RFC 2464	イーサネット ネットワーク上での IPv6 パケットの送信
RFC 2467	『 <i>Transmission of IPv6 Packets over FDDI Networks</i> 』
RFC 2472	『 <i>IP Version 6 over PPP</i> 』
RFC 2492	『 <i>IPv6 over ATM Networks</i> 』
RFC 2590	『 <i>Transmission of IPv6 Packets over Frame Relay Networks Specification</i> 』
RFC 3021	IPv4 Point-to-Point リンクでの 31 ビットプレフィックスの使用
RFC 3152	IP6.ARPA の委任

RFC	タイトル
RFC 3162	<i>RADIUS</i> および <i>IPv6</i>
RFC 3513	インターネットプロトコルバージョン6 (<i>IPv6</i>) アドレス指定アーキテクチャ
RFC 3596	<i>IP</i> バージョン6 への <i>DNS</i> 拡張
RFC 4193	固有ローカル <i>IPv6</i> ユニキャストアドレス



第 18 章

Cisco NX-OS インターフェイスの設定制限

設定制限は『Cisco Nexus 9000 シリーズ NX-OS 検証済みスケラビリティガイド』にまとめられています。



第 19 章

400G デジタル コヒーレント 光ファイバの構成

この章では、400G デジタル コヒーレント QSFP-DD 光モジュールとサポートされる構成について説明します。

- [400G デジタル コヒーレント 光ファイバの概要 \(499 ページ\)](#)
- [400G デジタル コヒーレント 光ファイバ パラメータ \(500 ページ\)](#)
- [トラフィック 構成 パラメータ \(503 ページ\)](#)
- [400G デジタル コヒーレント 光ファイバ の注意事項と制約事項 \(503 ページ\)](#)
- [ZR モジュールでの 400G デジタル コヒーレント 光ファイバ の構成 \(506 ページ\)](#)
- [ZRP モジュールでの 400G デジタル コヒーレント 光ファイバ \(DCO\) の構成 \(508 ページ\)](#)
- [ブレイクアウトの設定 \(510 ページ\)](#)
- [400G デジタル コヒーレント 光ファイバ の確認 \(511 ページ\)](#)
- [400G コヒーレント 光ファイバ の構成例 \(511 ページ\)](#)

400G デジタル コヒーレント 光ファイバの概要

振幅のみを使用する PAM4 光ファイバ (パルス振幅変調) とは異なり、コヒーレント 光ファイバは位相と振幅を使用してデータをエンコードします。これにより、コヒーレント 光ファイバのノイズに対する耐性が向上し、長距離伝送がサポートされます。

Cisco 400G デジタル コヒーレント 光ファイバの詳細については、『[Cisco 400G デジタル コヒーレント 光ファイバ QSFP-DD 光ファイバ モジュール データ シート](#)』を参照してください。

400G デジタル コヒーレント 光ファイバには 2 つのバリエーションがあります。

- **ZR バリエント** : QSFP-DD ZR バリエントは OIF MSA に準拠しており、同じ MSA 標準に準拠した同等のコンポーネントとの互換性を提供できます。ZR 標準の主な用途は、ポイントツーポイント トポロジで 400G 波長を最大 120 km の距離まで伝送できるようにすることです。

- **ZR Plus バリエント** : QSFP-DD OpenZR+ モジュールは、OpenZR+ MSA に準拠しています。ZR+ プラガブル コヒーレント 光ファイバは、エンドポイント間の複数の増幅サイトで、波長の地域から長距離伝送をサポートします。ZR+ は、さまざまなネットワーク トポロジをサポートするために、変調方式、シェーピング、およびボーレートに関して複数の構成オプションをサポートし、最長伝送距離 (120 km 超) を可能にします。

400G デジタル コヒーレント 光ファイバ パラメータ

400G デジタル コヒーレント 光ファイバは構成可能で、光ファイバに関する次のパラメータを構成できます。構成値の詳細については、[表 22 : 400G デジタル コヒーレント QSFP-DD トラフィックの構成値 \(501 ページ\)](#) を参照してください。

- **[トランスポンダ/マックスポンダ モード (Transponder/Muxponder mode)]** : このパラメータは、メディア回線を 400G で構成し、ホスト側に最大 4 つのクライアントを構成するために使用されます。
- **[DAC レート (DAC rate)]** : デジタル アナログ変換 (DAC) パラメータは、オーバーサンプリング (パルス整形の有効化または無効化) とメディア回線モデムを標準 (S) または拡張 (E) に設定するために使用されます。
- **[FEC モード (FEC mode)]** : 前方誤り訂正 (FEC) は、メディア回線で cFEC または oFEC モードをサポートし、データ伝送中のエラーを制御するために使用されます。
- **[変調 (Modulation)]** : このパラメータは、光波を制御して、搬送光波の情報をエンコードするために使用されます。サポートされる変調は、16 QAM、8 QAM、および QPSK です。
- **[CD 最小/最大 (CD min/max)]** : 波長分散 (CD) は、光ファイバ通信において重要な要素となる現象です。光線が接続先に到達する時間がわずかに異なることで、その色(波長)に違いが生じることによって発生します。このパラメータは、デバイスが良好な光信号と周波数を取得する範囲を設定するために使用されます。

マックスポンダ-FEC-変調	CD デフォルト高 (ps/nm)	CD デフォルト低 (ps/nm)	最大プロビ ジョニング可 能 CD 高 (ps/nm)	最小プロビ ジョニング可 能な CD 低 (ps/nm)
400G-400GZR-cFEC-16QAM	2400	-2400	2400	-2400
400G-400GZR-oFEC-16QAM	13,000	-13000	52000	-52000
200G-200GZR-oFEC-QPSK	50000	-50000	100000	-100000
200G-200GZR-oFEC-8QAM	26000	-26000	100000	-100000
200G-200GZR-oFEC-16QAM	21000	-21000	85000	-85000
100G-100GZR-oFEC-QPSK	80000	-80000	160000	-160000

- **[Tx パワー (Tx power)]** : 送信光ファイバパワーは、光ファイバ モジュールの送信端にある光源の出力光ファイバパワーを指し、受信光パワーは、光ファイバ モジュールの受信端にある光源の入力光ファイバパワーを指します。

各光モジュールには、独自の送信 (TX) 電力範囲があります。モジュールの機能に基づいて、送信 (TX) 電力値を変更できます。

光ファイバ モジュール	トランク速 度 ^{1, 3}	光ファイバ 送信パワー (Tx) シェ イピング	インターバ ル (Interval)	光ファイバ送信電力 (Tx) 値のサポー トされる範囲 (0.1 dBm 単位) ²		
				最小値 (Minimum Value)	最大標準値	最大最悪 ケース値
QDD400GZR-S	400G	いいえ	1	-150	-100	-100
QDD400GZR-PS	400G	はい	1	-150	-110	-130
QDD400GZR-PS	200G	はい	1	-150	-90	-105
QDD400GZR-PS	100 G	はい	1	-150	-59	-75

- **[周波数 (Frequency)]** : 光ファイバ通信では、波長分割多重 (WDM) は、異なる波長 (つまり色) のレーザー光を使用して、複数の光キャリア信号を単一の光ファイバに多重化する技術です。この技術により、波長分割デュプレックスとも呼ばれる1本の光ファイバを介した双方向通信と、キャパシティの増加が可能になります。このパラメータは、ITU C-BAND テーブルの任意の周波数を設定するために使用されます。値の詳細については、「[ITU C-BAND テーブル \(515 ページ\)](#)」セクションを参照してください。

構成の詳細については、「[ZR モジュールでの 400G デジタルコヒーレント光ファイバの構成 \(506 ページ\)](#)」セクションを参照してください。

次の表に、トランスポンダ (TXP) およびマックスポンダ (MXP) モードでの 400G デジタルコヒーレント QSFP-DD 光ファイバ モジュールの可能なトラフィック構成値を示します。

表 22: 400G デジタルコヒーレント QSFP-DD トラフィックの構成値

クライアント 速度	トランク速度	周波数	FEC	変調	DAC レート
QDD-400G-ZR-S トランスポンダおよびマックスポンダの構成値					
1 クライアン ト、速度 400G	1 トランク、 400G	C バンド、 196.1 ~ 191.3 THz	cFEC	16 QAM	1 x 1
QDD-400G-ZRP-S トランスポンダおよびマックスポンダの構成値					

クライアント速度	トランク速度	周波数	FEC	変調	DAC レート
1X400GA UI-8	1 トランク、 速度 400G	C バンド、 196.1 ~ 191.3 THz	cFEC	16 QAM	1 x 1
4X100GA UI-2					
1X400GA UI-8	1 トランク、 速度 400G	C バンド、 196.1 ~ 191.3 THz	cFEC	16 QAM	1x1.5
4X100GA UI-2					
1X400GA UI-8	1 トランク、 速度 400G	C バンド、 196.1 ~ 191.3 THz	oFEC	16 QAM	1x1.25
4X100GA UI-2					
1X400GA UI-8	1 トランク、 速度 400G	C バンド、 196.1 ~ 191.3 THz	oFEC	16 QAM	1x2
4X100GA UI-2					
1X400GA UI-8	1 トランク、 速度 400G	C バンド、 196.1 ~ 191.3 THz	oFEC	16 QAM	1 x 1
4X100GA UI-2					
1X400GA UI-8	1 トランク、 速度 400G	C バンド、 196.1 ~ 191.3 THz	oFEC	16 QAM	1x1.5
4X100GA UI-2					
2X100GA UI-2	1 トランク、 速度 200G	C バンド、 196.1 ~ 191.3 THz	oFEC	QPSK	1x1.5
				QPSK	1
100 G	1 トランク、 速度 100G	C バンド、 196.1 ~ 191.3 THz	oFEC	QPSK	1x1.5

トラフィック構成パラメータ

次の表に、サポートされているさまざまなトラフィック構成を示します。

TXP/MXP	クライアント (Client)	トランク	変調	FEC	DAC レート
400G-TXP	1 クライアント、速度 400G	1 トランク、速度 400G	16 QAM	oFEC	1x1、1x1.25、1x1.5 および 1x2
400G-TXP	1 クライアント、速度 400G	1 トランク、速度 400G	16 QAM	cFEC	1x1、および 1x1.5
4x100G-MXP	4 クライアント、速度 100G	1 トランク、速度 400G	16 QAM	oFEC	1x1、1x1.25、1x1.5、および 1x2
4x100G-MXP	4 クライアント、速度 100G	1 トランク、速度 400G	16 QAM	cFEC	1x1、および 1x1.5
2x100G-MXP	2 クライアント、速度 100G	1 トランク、速度 200G	QPSK	oFEC	1x1、および 1x1.5
			8 QAM		1x1.25
			16 QAM		1x1.25
1x100G-MXP	1 クライアント、速度 100G	1 トランク、速度 100G	QPSK	oFEC	1x1.5



- (注)
- ZR は 1x400G トランスポンダのみをサポートします。
 - ZR は 1x1 DAC レートのみをサポートします。
 - 4x100 および 2x100 マックスポンダを構成するには、ZRP を構成する前にインターフェイスブレイクアウトを実行する必要があります。詳細については、[ブレイクアウトの設定 \(510 ページ\)](#) の項を参照してください。

400G デジタルコヒーレント光ファイバの注意事項と制約事項

400G デジタルコヒーレント光ファイバには、次の注意事項と制約事項があります。

- Cisco NX-OS リリース 10.4(1)F 以降、400G デジタル コヒーレント光ファイバ (DCO) サポートは、Cisco Nexus 9300-GX2 および 9408 プラットフォーム スイッチで提供されます。
- Cisco NX-OS リリース 10.4(2)F 以降、QDD-400G-ZR-S および QDD-400G-ZRP-S 光ファイバサポートは、次のスイッチおよびラインカードで提供されます。
 - X9624D-R2 ラインカードを搭載した Cisco Nexus 9508 スイッチ。
 - Cisco Nexus 93600CD-GX、9316D-GX スイッチ、および X9716D-GX ラインカードを搭載した Cisco Nexus 9508/9504 スイッチ。
 - Cisco Nexus X98900CD-A and X9836DM-A ラインカードを搭載した Cisco Nexus 9804/9808 スイッチ。
- 1x100G トランスポンダおよび 2x100G マックスポンダモードは、Cisco Nexus 93600CD-GX、9316D-GX スイッチ、および Cisco Nexus X98900CD-A および X9836DM-A ラインカードではサポートされません。
- QDD-400G-ZR-S 光ファイバは、インターフェイスのブレイクアウトをサポートしていません。
- QDD-400G-ZRP-S 光ファイバは、インターフェイスのブレイクアウトをサポートします。ZRP 光ファイバでは、複数のブレイクアウト マップがサポートされています。
- 2x100 ブレイクアウト インターフェイスには、ブレイクアウト マップ **100g-2x-pam4** オプションを使用します。



(注) 2x100G ブレイクアウトは、Cisco Nexus X9624D-R2 ラインカードではサポートされません。

- システムの安定性と効率を向上させるために、DCO の頻繁な挿入と取り外しを避けることをお勧めします。OIR の場合、バックツーバック トランシーバの挿入と取り外しの間に少なくとも 1 分間待つ必要があります。
- ZR/ZRP モジュールの光ファイバの最大リンクアップ時間は最大 180 秒です。
- 電力制限のために影響を受けたコヒーレント光ファイバ ポートまたは MACsec ポートを回復するには、アクティブな ZR/ZRP ポートをディセーブルにするか、既存の MACsec セッションを構成解除して、影響を受けるポートをフラップする必要があります。
- 一部のプラットフォームでは、ハードウェアの電力制限があり、多数の 400Gig-ZR/ZRP トランシーバと MACsec 構成を同時に使用することが制限されています。
- Cisco NX-OS リリース 10.4(2)F 以降、2X100 マックスポンダは 8QAM および 16QAM 変調をサポートします。
- 1X100 マックスポンダは、Cisco Nexus X9624D-R2 ラインカードではサポートされません。
- 制約事項の概要は次のとおりです。

• Cisco Nexus 9364D-GX2A の場合 :

- システムに9つ以上の MACsec セッションが構成されていて、ZR/ZRP トランシーバが存在しない場合、ZR/ZRP トランシーバを挿入すると対応するポートが無効になります。ZR/ZRP トランシーバが存在しない場合、許可される MACsec セッションの最大数は 16 です。
- システムにアクティブ状態の ZR/ZRP トランシーバが9つ以上あり、MACsec セッションが存在しない場合、新しい MACsec セッションの起動は失敗します。MACsec セッションがシステムに存在しない場合、アクティブな ZR/ZRP トランシーバの最大数は 13 です。14 番目の ZR/ZRP トランシーバを挿入すると、対応するポートが無効になります。
- MACsec セッションとアクティブな ZR/ZRP トランシーバの両方が共存する場合、合計の制限は MACsec セッションが最大 8 つ、ZR/ZRP トランシーバが最大 8 つです。9 番目の MACsec セッションを構成するか、9 番目のアクティブ ZR/ZRP を追加すると、対応するポートが無効になります。
- ZR/ZRP トランシーバは、このプラットフォームの奇数番号の前面ポートでのみサポートされます。偶数番号の前面ポートに ZR/ZRP トランシーバを挿入すると、ポートはエラー状態になります。

• Cisco Nexus 9332D-GX2B の場合 :

- システムに5つ以上の MACsec セッションが構成されていて、アクティブな ZR/ZRP トランシーバが存在しない場合、ZR/ZRP トランシーバを追加すると対応するポートが無効になります。アクティブな ZR/ZRP トランシーバが存在しない場合、許可される MACsec セッションの最大数は 8 です。9 番目の MACsec セッションを設定すると、対応するポートが無効になります。
- システムに5つ以上のアクティブな ZR/ZRP トランシーバが挿入されていて、MACsec セッションが存在しない場合、新しい MACsec セッションの起動は失敗します。システムに MACsec セッションが存在しない場合、アクティブな ZR/ZRP トランシーバの最大数は 8 です。9 番目の ZR/ZRP トランシーバを挿入すると、対応するポートが無効になります。
- MACsec セッションとアクティブな ZR/ZRP トランシーバの両方が共存する場合、組み合わせでの制限は最大 4 つの MACsec セッションと最大 4 つのアクティブな ZR/ZRP トランシーバです。5 番目の MACsec セッションを構成するか、5 番目の ZR/ZRP を挿入すると、対応するポートが無効になります。
- ZR/ZRP トランシーバは、このプラットフォームの前面ポートのいずれかでサポートされます。

• Cisco Nexus 9348D-GX2A の場合 :

- ZR/ZRP トランシーバは、このプラットフォームの次の 24 個の前面ポートでサポートされます。

- 3、6、9、12、15、18、21、24、27、30、33、36、39、42、45、48、26、29、32、35、38、41、44、47



(注) 上記のリストにない他の前面ポートに ZR/ZRP トランシーバを挿入すると、ポートがエラー状態になります。

• Cisco Nexus 9408 の場合 :

- システムは、MACsec 構成が存在するかどうかに関係なく、最大 32 のアクティブな ZR/ZRP トランシーバをサポートできます。
- ZR/ZRP トランシーバは、Cisco Nexus X9400-8D モジュールでのみサポートされます。

ZR モジュールでの 400G デジタル コヒーレント 光ファイバの構成

DAC レート、マックスポンダ モード、変調、および FEC パラメータについて、ZR モジュールのコヒーレント 光ファイバを構成できます。

始める前に

DCO の構成時に次の点に注意してください。

- ZR 光ファイバを挿入しないと、コヒーレント 光ファイバ構成は機能しません。
- ZRP モジュールで特定の zr 光ファイバを構成すると、コヒーレント構成は機能しません。
- ZR モジュールで特定の zrp 光ファイバを構成すると、コヒーレント構成は機能しません。

手順の概要

1. **configure terminal**
2. **interface ethernet** {type slot/port}
3. **[no] zr-optics fec** *fec_val* **muxponder** *mxp_val* **modulation** *mod_val* **dac-rate** *dr_val*
4. (任意) **zr-optics cd-min** *cd_min* **cd-max** *cd_max*
5. (任意) **zr-optics transmit-power** *tx_pwr*
6. (任意) **zr-optics dwdm-carrier** [**100MHz-grid** *frequency freq_100mhz_val* | **100GHz-grid** *frequency freq_100ghz_val* | **50GHz-grid** { **frequency** *freq* | **itu-channel** *itu-chan* | **wavelength** *wavelen* }]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： <pre>switch# configure terminal switch(config)#</pre>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface ethernet {type slot/port} 例： <pre>switch(config)# interface ethernet 1/3 switch(config-if)#</pre>	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	[no] zr-optics fec fec_val muxponder mxp_val modulation mod_val dac-rate dr_val 例： <pre>switch(config-if)# zr-optics fec cFEC muxponder 1x400 modulation 16QAM dac-rate 1x1</pre>	ZR 光ファイバで次のパラメータを構成します。詳細については、 400G デジタルコヒーレント光ファイバパラメータ (500ページ) セクションを参照してください。 <ul style="list-style-type: none"> • FEC • マックスポンダ • 変調 • DAC
ステップ 4	(任意) zr-optics cd-min cd_min cd-max cd_max 例： <pre>switch(config-if)# zr-optics cd-min -2300 cd-max 2300</pre>	設定された最小値と最大値を使用して、コヒーレント光ファイバの波長分散を構成します。詳細については、 400G デジタルコヒーレント光ファイバパラメータ (500 ページ) の項を参照してください。 <p>(注) 任意のデータ レートの CD の最大値と最小値を構成する場合は、構成された値の最小差が 1000 ps/nm 以上であることを確認します。</p>
ステップ 5	(任意) zr-optics transmit-power tx_pwr 例： <pre>switch(config-if)# zr-optics transmit-power -190</pre>	光信号の送信電力を設定します。詳細については、 400G デジタルコヒーレント光ファイバパラメータ (500 ページ) の項を参照してください。 <p>(注) Tx 電力パラメータは、ユーザー設定をハードウェアにプログラムするベストエフォート設定です。しかし、ZR/ZRP トランシーバファームウェアはこれを参照としてのみ使用し、実行時に実際の最適な Tx 電力値を計算します。これはユーザー構成と同じである場合とそうでない場合があります。</p>

	コマンドまたはアクション	目的
ステップ 6	<p>(任意) zr-optics dwdm-carrier [100MHz-grid frequency <i>freq_100mhz_val</i> 100GHz-grid frequency <i>freq_100ghz_val</i> 50GHz-grid { frequency <i>freq</i> itu-channel <i>itu-chan</i> wavelength <i>wavelen</i> }]</p> <p>例 :</p> <pre>switch(config-if)# zr-optics dwdm-carrier 100MHz-grid frequency 1913000</pre>	<p>構成された周波数 (100MHz グリッド、100GHz グリッド、または 50GHz グリッド) に基づいて周波数を構成します。50GHz グリッドは、追加の ITU チャンネルまたは波長パラメータを提供します。詳細については、400G デジタルコヒーレント光ファイバパラメータ (500 ページ) の項を参照してください。</p> <p>(注) 周波数が [50Ghz グリッド波長 (50Ghz-grid wavelength)] または [50 Ghz グリッド ITU チャンネル (50Ghz-grid itu-channel)] オプションを使用して構成されている場合、システムは特定の波長または ITU チャンネルの周波数を計算し、それを使用してハードウェアをプログラムします。</p>

ZRP モジュールでの 400G デジタルコヒーレント光ファイバ (DCO) の構成

DAC レート、マックスポンダモード、変調、および FEC パラメータについて、ZRP モジュールのコヒーレント光ファイバを構成できます。

始める前に

DCO の構成時には、次の点に注意してください。

- ZRP 光ファイバを挿入しないと、コヒーレント光ファイバ構成は機能しません。
- ZRP モジュールで特定の zr 光ファイバを構成すると、コヒーレント構成は機能しません。
- ZR モジュールで特定の zrp 光ファイバを構成すると、コヒーレント構成は機能しません。

手順の概要

1. **configure terminal**
2. **interface ethernet** {*type slot/port*}
3. [no] **zrp-optics fec** *fec_val* **muxponder** *mzp_val* **modulation** *mod_val* **dac-rate** *dr_val*
4. (任意) **zrp-optics cd-min** *cd_min* **cd-max** *cd_max*
5. (任意) **zrp-optics transmit-power** *tx_pwr*
6. (任意) **zrp-optics dwdm-carrier** [**100MHz-grid frequency** *freq_100mhz_val* | **100GHz-grid frequency** *freq_100ghz_val* | **50GHz-grid** { **frequency** *freq* | **itu-channel** *itu-chan* | **wavelength** *wavelen* }]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : <pre>switch# configure terminal switch(config)#</pre>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	interface ethernet {type slot/port} 例 : <pre>switch(config)# interface ethernet 1/3 switch(config-if)#</pre>	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	[no] zrp-optics fec fec_val muxponder mxp_val modulation mod_val dac-rate dr_val 例 : <pre>switch(config-if)# zrp-optics fec cFEC muxponder 1x400 modulation 16QAM dac-rate 1x1</pre>	ZRP 光ファイバで次のパラメータを構成します。詳細については、 400G デジタルコヒーレント光ファイバパラメータ (500ページ) セクションを参照してください。 <ul style="list-style-type: none"> • FEC • マックスポンダ • 変調 • DAC
ステップ 4	(任意) zrp-optics cd-min cd_min cd-max cd_max 例 : <pre>switch(config-if)# zrp-optics cd-min -2400 cd-max 2400</pre>	設定された最小値と最大値を使用して、コヒーレント光ファイバの波長分散を構成します。詳細については、 400G デジタルコヒーレント光ファイバパラメータ (500ページ) の項を参照してください。 (注) 任意のデータ レートの波長分散の最大値と最小値を構成する場合は、構成された値の最小差が 1000 ps/nm 以上であることを確認します。
ステップ 5	(任意) zrp-optics transmit-power tx_pwr 例 : <pre>switch(config-if)# zrp-optics transmit-power -190</pre>	光信号の送信電力を設定します。詳細については、 400G デジタルコヒーレント光ファイバパラメータ (500ページ) の項を参照してください。 (注) Tx 電力パラメータは、ユーザー設定をハードウェアにプログラムするベストエフォート設定です。しかし、ZR/ZRP トランシーバファームウェアはこれを参照としてのみ使用し、実行時に実際の最適な Tx 電力値を計算します。これはユーザー構成と同じである場合とそうでない場合があります。

	コマンドまたはアクション	目的
ステップ 6	<p>(任意) zrp-optics dwdm-carrier [100MHz-grid frequency <i>freq_100mhz_val</i> 100GHz-grid frequency <i>freq_100ghz_val</i> 50GHz-grid { frequency <i>freq</i> itu-channel <i>itu-chan</i> wavelength <i>wavelen</i> }]</p> <p>例 :</p> <pre>switch(config-if)# zrp-optics dwdm-carrier 100MHz-grid frequency 1913000</pre>	<p>構成された周波数 (100MHz グリッド、100GHz グリッド、または 50GHz グリッド) に基づいて周波数を構成します。50GHz グリッドは、追加の ITU チャンネルまたは波長パラメータを提供します。詳細については、400G デジタル コヒーレント光ファイバパラメータ (500 ページ) の項を参照してください。</p> <p>(注) 周波数が [50Ghz グリッド波長 (50Ghz-grid wavelength)] または [50Ghz グリッド ITU チャンネル (50Ghz-grid itu-channel)] オプションを使用して構成されている場合、システムは特定の波長または ITU チャンネルの周波数を計算し、それを使用してハードウェアをプログラムします。</p>

ブレイクアウトの設定

ZRP 光ファイバのインターフェイスでブレイクアウトを構成できます。

手順の概要

1. **configure terminal**
2. **interface breakout module** {*slot*} **port** {*port_num*} **map** {*breakoutmap*}
3. **interface ethernet** {*type slot/port/sub-port*}
4. [no] **zrp-optics fec** *fec_val* **muxponder** *mxp_val* **modulation** *mod_val* **dac-rate** *dr_val*
5. (任意) **show running interface ethernet** {*type slot/port*}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<p>configure terminal</p> <p>例 :</p> <pre>switch# configure terminal switch(config)#</pre>	グローバル 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	<p>interface breakout module {<i>slot</i>} port {<i>port_num</i>} map {<i>breakoutmap</i>}</p> <p>例 :</p> <pre>switch(config)# interface breakout module 1 port 3 map 100g-2x-pam4</pre>	インターフェイス ブレイクアウトを構成します

	コマンドまたはアクション	目的
ステップ 3	interface ethernet {type slot/port/sub-port} 例 : switch(config)# interface ethernet 1/3/1 switch(config-if)#	設定するインターフェイスを指定し、インターフェイスコンフィギュレーションモードを開始します。
ステップ 4	[no] zrp-optics fec fec_val muxponder mxp_val modulation mod_val dac-rate dr_val 例 : switch(config-if)# zrp-optics fec oFEC muxponder 2x100 modulation QPSK dac-rate 1x1	ブレイクアウト インターフェイスで ZRP を構成します。
ステップ 5	(任意) show running interface ethernet {type slot/port} 例 : switch(config-if)# show running interface ethernet1/3/1	ブレイクアウトインターフェイスに設定されている構成情報を表示します。

400G デジタル コヒーレント光ファイバの確認

400G デジタル コヒーレント光ファイバ構成情報を確認するには、次のいずれかの作業を行います。

コマンド	目的
show running interface ethernet {type slot/port}	コヒーレント ZR/ZRP 光ファイバを検証するように設定されたインターフェイスの実行コンフィギュレーション情報を表示します。
show interface ethernet {type slot/port} transceiver details	インターフェイスのコヒーレント ZR/ZRP 光ファイバ構成情報を表示します。

400G コヒーレント光ファイバの構成例

次に、ZR/ZRP 光ファイバを使用した実行構成の例を示します。

```
switch(config-if)# show running interface ethernet1/3

!Command: show running-config interface Ethernet1/3
!Running configuration last done at: Mon Aug 28 12:16:40 2023
!Time: Mon Aug 17 12:17:40 2023

version 10.3(2) Bios:version 01.10

interface Ethernet1/3
  zr-optics fec cFEC muxponder 1x400 modulation 16QAM dac-rate 1x1
```

```

zr-optics cd-min -2400 cd-max 2400
zr-optics transmit-power -190
zr-optics dwdm-carrier 100MHz-grid frequency 1931000
no shutdown

```

次に、コヒーレント構成を確認する例を示します。

```

switch# show interface ethernet1/3 transceiver details
Ethernet1/3
  transceiver is present
  type is QSFP-DD-400G-ZR-S
  name is CISCO-ACACIA
  part number is DP04QSDD-E20-190
  revision is A
  serial number is ACA254700F0
  nominal bitrate is 425000 MBit/sec per channel
  cisco id is 0x18
  cisco extended id number is 21
  cisco part number is 10-3495-01
  cisco product id is QDD-400G-ZR-S
  cisco version id is V01
  firmware version is 61.10
  Link length SMF is 12 km
  Nominal transmitter wavelength is 1547.70 nm
  Wavelength tolerance is 166.550 nm
  host lane count is 8
  media lane count is 1
  max module temperature is 80 deg C
  min module temperature is 0 deg C
  min operational voltage is 3.12 V
  vendor OUI is 0x7cb25c
  date code is 211125
  clei code is INUIANYEAA
  power class is 8 (>14 W maximum)
  max power is 20.00 W
  near-end lanes used none
  far-end lane code for 8 lanes Undefined
  media interface is unknown value 0x10
  Advertising code is Optical Interfaces: SMF
  Host electrical interface code is 400GAUI-8 C2M (Annex 120E)

```

FEC State: FEC cFEC

Optics Status

Optics Type: QSFP-DD-400G-ZR-S
DWDM carrier Info: Frequency: 193.10 THz

Alarm Status

DAC Rate: 1x1

THRESHOLD VALUES

Configured Tx Power: -400 dBm
Modulation Type: 16QAM
Muxponder Type: 1x400
Configured CD-MIN: -2400 ps/nm CD-MAX: 2400 ps/nm

Lane Number:1 Network Lane

	Current Measurement	Alarms		Warnings	
		High	Low	High	Low
Temperature	36.00 C	80.00 C	-5.00 C	75.00 C	15.00 C
Voltage	3.36 V	3.46 V	3.13 V	3.43 V	3.16 V
Current	N/A	N/A	N/A	N/A	N/A


```
Tx Power          N/A          0.00 dBm -18.23 dBm  -2.00 dBm  -16.02 dBm
Rx Power          N/A          1.99 dBm -23.01 dBm   0.00 dBm  -20.00 dBm
Transmit Fault Count = 0
```

```
-----
Note: ++ high-alarm; + high-warning; -- low-alarm; - low-warning
```

次の例は、ブレイクアウトインターフェイスでブレイクアウト構成を構成する方法を示しています。

```
switch(config)# interface ethernet 1/3/1
switch(config-if)# zrp-optics fec ofec muxponder 2x100 modulation QPSK dac-rate 1x1
```

```
switch (config-if)# show running interface ethernet1/3/1
```

```
interface Ethernet1/3/1
  zrp-optics fec ofEC muxponder 2x100 modulation QPSK dac-rate 1x1
  zrp-optics cd-min -50000 cd-max 50000
  zrp-optics transmit-power -190
  zrp-optics dwdm-carrier 100MHz-grid frequency 1913000
  no shutdown
```




付録 **A**

ITU C-BAND テーブル

ITU チャンネル	周波数 (GHz)	波長
1	19610	1528773
2	19605	1529163
3	19600	1529553
4	19595	1529944
5	19590	1530334
6	19585	1530725
7	19580	1531116
8	19575	1531507
9	19570	1531898
10	19565	1532290
11	19560	1532681
12	19555	1533073
13	19550	1533465
14	19545	1533858
15	19540	1534250
16	19535	1534643
17	19530	1535036
18	19525	1535429
19	19520	1535822
20	19515	1536216
21	19510	1536609
22	19505	1537003
23	19500	1537397

ITU チャンネル	周波数 (GHz)	波長
24	19495	1537792
25	19490	1538186
26	19485	1538581
27	19480	1538976
36	19475	1539371
29	19470	1539766
30	19465	1540162
31	19460	1540557
32	19455	1540953
33	19450	1541349
34	19445	1541746
35	19440	1542142
36	19435	1542539
37	19430	1542936
38	19425	1543333
39	19420	1543730
40	19415	1544128
41	19410	1544526
42	19405	1544924
43	19400	1545322
44	19395	1545720
45	19390	1546119
46	19385	1546518
47	19380	1546917
48	19375	1547316
49	19370	1547715
50	19365	1548115
51	19360	1548515
52	19355	1548915
53	19350	1549315
54	19345	1549715
55	19340	1550116

ITU チャンネル	周波数 (GHz)	波長
56	19335	1550517
57	19330	1550918
58	19325	1551319
59	19320	1551721
60	19315	1552122
61	19310	1552524
62	19305	1552926
63	19300	1553329
64	19295	1553731
65	19290	1554134
66	19285	1554537
67	19280	1554940
68	19275	1555343
69	19270	1555747
70	19265	1556151
71	19260	1556555
72	19255	1556959
73	19250	1557363
74	19245	1557768
75	19240	1558173
76	19235	1558578
77	19230	1558983
78	19225	1559389
79	19220	1559794
80	19215	1560200
81	19210	1560606
82	19205	1561013
83	19200	1561419
84	19195	1561826
85	19190	1562233
86	19185	1562640
87	19180	1563047

ITU チャンネル	周波数 (GHz)	波長
88	19175	1563455
89	19170	1563863
90	19165	1564271
91	19160	1564679
92	19155	1565087
93	19150	1565496
94	19145	1565905
95	19140	1566314
96	19135	1566723
97	19130	1567133



索引

A

admin-shutdown [141](#)
auto-recovery [321, 362](#)
autonomous-system [204](#)

B

bfd authentication keyed-sha1 keyid [189–191, 221–222](#)
bfd echo [192–193](#)
bfd echo-interface loopback [187–188](#)
bfd interval [187, 189, 191, 214–216, 221–222](#)
bfd multihop interval [220–221](#)
bfd per-link [191](#)
bfd slow-timer [187–188, 192–193](#)
bfd [203–205, 207, 221–222](#)

C

channel-group [250–253, 265](#)
checkpoint [120](#)
clear counters interface port-channel [291](#)
clear counters interface [89, 130](#)
clear ip nat translation [472](#)
clear ip route [183](#)
clear lacp counters [291](#)
clear ipv6 route [183](#)
clear l2protocol tunnel counters [425](#)
config t [151](#)
copy [41, 48–49](#)

D

default interface [120](#)
delay [65, 254–255](#)
delay restore [319, 323](#)
deny [461–462](#)
duplex [258–259](#)
duplex auto [258–259](#)
duplex full [258–259](#)
duplex half [258–259](#)

E

encapsulation dot1Q [145–148, 154–157](#)
errdisable detect cause acl-exception [53–54](#)
errdisable detect causeall [53–54](#)
errdisable detect cause link-flap [53–54](#)
errdisable detect cause loopback [53–54](#)
errdisable detect cause [28, 53–54](#)
errdisable recovery cause [28, 55](#)
errdisable recovery cause all [55](#)
errdisable recovery cause bpduguard [55](#)
errdisable recovery cause failed-port-state [55](#)
errdisable recovery cause link-flap [55](#)
errdisable recovery cause loopback [55](#)
errdisable recovery cause miscabling [55](#)
errdisable recovery cause psecure-violation [55](#)
errdisable recovery cause security-violation [55](#)
errdisable recovery cause storm-control [55](#)
errdisable recovery cause udld [55](#)
errdisable recovery cause vpc-peerlink [55](#)
errdisable recovery interval [28, 56](#)
ethernet [50](#)

F

feature bfd [186](#)
feature eigrp [66](#)
feature interface-vlan [124–125, 148–149](#)
feature isis [156–157](#)
feature lacp [263–264](#)
feature nat [450, 464–465](#)
feature tunnel [385](#)
feature vpc [344](#)

H

hardware access-list team region nat [446](#)
show l2protocol tunnel summary [426](#)
hsrp bfd [208–209](#)
hsrp bfd all-interfaces [208–209](#)

I

include bfd [186](#)

interface ether **87–88**
 interface ethernet **52, 61, 63–65, 69–70, 75, 108–111, 116, 119, 143, 145–146, 151, 153–157, 164, 414, 419–420, 422**
 interface loopback **152, 154, 156**
 interface port-channel **116, 119, 121, 147, 151, 191, 214–216, 248–249, 254–259, 266–268, 274–280, 283, 349–351**
 interface tunnel **387–390, 392, 394–396**
 interface vlan **124–125, 148–149, 151**
 インターフェイス **49–50, 62–63, 66–67, 121, 151, 160–161, 189, 358, 450, 455–456, 462–463, 467–470**
 interfaces-vlan **319, 323**
 ip **41**
 ip access-list **461–462**
 ip address dhcp **139**
 ip arp synchronize **315**
 ip eigrp **204, 213**
 ip load-sharing address **285–286**
 ip nat inside source list **462–463, 466–468**
 ip nat inside source static **451–456, 469**
 ip nat inside **450, 455–456, 462–463, 467–470**
 ip nat outside source list **466, 469**
 ip nat outside source static **452–456, 467**
 ip nat outside **450, 455, 457, 462–463, 467–469**
 ip nat pool **443, 464–465, 467–469**
 ip nat translation creation-delay **462, 464**
 ip nat translation icmp-timeout **462, 464**
 ip nat translation mas-entries **462, 464**
 ip nat translation sampling-timeout **440**
 ip nat translation timeout **462, 464**
 ip nat **444**
 ip ospf authentication **154–155**
 ip ospf authentication-key **154–155**
 ip ospf bfd disable **213**
 ip ospf bfd **205–206, 214–217**
 ip pim bfd **211**
 ip pim bfd-instance **211**
 ip pim pre-build-spt **318**
 ip pim spt-threshold infinity **317**
 ip route static bfd **212**
 router eigrp **203–204**
 ip router isis **156–157**
 ip router ospf **154–156**
 ip unnumbered **153–157**
 ip address **143–149, 152–154, 156, 160, 215–216, 389–390, 396–397, 455–456, 462–463**
 ip name-server **139**
 ip pim use-shared-tree-only **317**
 ip route **139, 212**
 ipv6 address dhcp **139**
 ipv6 address use-link-local-only **139**
 ipv6 nd mac-extract **161–162**
 ipv6 nd synchronize **315**
 ipv6 アドレス **143–149, 152–153, 161–162**
 isis bfd **207**
 isis bfd disable **213**

L

l2protocol tunnel **419–420**
 l2protocol tunnel cos **421**
 l2protocol tunnel drop-threshold **422**
 l2protocol tunnel shutdown-threshold **422–423**
 lacp graceful-convergence **240, 275**
 lacp max-bundle **267–268**
 lacp min-links **266**
 lacp mode delay **280**
 lacp port-priority **271**
 lacp rate **268**
 lacp rate fast **269**
 lacp suspend-individual **276–277, 279**
 lacp system-priority **270**
 link debounce time **75**
 load- interval **130, 172, 290–291**
 load-interval counters **87–88**

M

mac-address **151**
 mac-address ipv6-extract **161–162**
 match-in-vrf **444**
 medium **144**
 medium broadcast **144**
 medium p2p **144, 153–157**
 mgmt0 **50**
 mtu **61–63, 387, 392–393**

N

negotiate auto **40, 85–86**
 negotiate auto 25000 **85**
 neighbor **202, 221–222**

P

p2p **144**
 peer-gateway **314, 355**
 peer-gateway exclude-vlan **314**
 peer-keepalive destination **347–348**
 peer-switch **356**
 permit **461–462**
 permit ip any any **449**
 port-channel load-balance **231, 260**

R

regex **40**
 role priority **368**
 router bgp **202, 221–222**
 router isis **156–157, 206–207**
 router ospf **205**

- S**
- show 144
 - show bfd 218
 - show bfd neighbors 218
 - show cdp all 87
 - show cfs application 320
 - show feature 186, 290, 344–345, 370, 385–386
 - show hardware feature-capability 294
 - show hsrp detail 208
 - show interface 49–50, 66–67, 87–90, 108–113, 120, 151, 250–253
 - show interface brief 87, 128–129
 - show interface capabilities 129
 - show interface counters 130, 291
 - show interface counters detailed 130, 291
 - show interface counters errors 130, 291
 - show interface eth 51, 146
 - show interface ethernet errors 172
 - show interface ethernet 52, 63–65, 129, 151, 170, 172
 - show interface loopback 152–153, 171, 173
 - show interface port-channel 151, 171, 173, 254–259, 290
 - show interface status err-disabled 28, 53–56, 87
 - show interface switchport 129
 - show interface transceivers 39
 - show interface trunk 129
 - show interface tunnel 397–398
 - show interface vlan 148–149, 151, 171, 173
 - show interfaces 145–146
 - show interfaces tunnel 387–388, 392–393, 395
 - show ip nat statistics 472
 - show ip copy 41
 - show ip eigrp 204
 - show ip interface brief 172
 - show ip load-sharing 285, 289
 - show ip nat max 472
 - show ip nat translations 460, 472
 - show ip route static 212
 - show ip route 172
 - show ipv6 ICMP interface 161–162
 - show isis 207
 - show l2protocol tunnel 426
 - show lacp 291
 - show lacp counters 291
 - show lacp system-identifier 270
 - show ip ospf 205–206
 - show port-channel capacity 370
 - show port-channel compatibility-parameters 229, 290
 - show port-channel database 290
 - show port-channel load-balance 260–261, 290
 - show port-channel summary 248–249, 265, 290
 - show port-channel traffic 290
 - show port-channel usage 290
 - show run nat 472
 - show running-config 123–124, 129
 - show running-config bfd 187–193, 218
 - show running-config bgp 202–203
 - show running-config hsrp 208–209
 - show running-config interface ethernet 130
 - show running-config interface port-channel 119, 121–122, 130, 267–268
 - show running-config interface vlan 124–125, 130
 - show running-config pim 211
 - show running-config vpc 362, 370
 - show running-config vrrp 210
 - show spanning-tree summary 356–357
 - show spanning-tree 313
 - show startup-config bfd 218
 - show startup-config interface vlan 124–125
 - show udd 69–70, 87
 - show udd global 87
 - show vlan 114, 116
 - show vpc brief 306, 313, 346, 349–355, 360, 370
 - show vpc consistency-parameters global 352–353
 - show vpc consistency-parameters interface port-channel 352–353, 362
 - show vpc consistency-parameters 305–306, 352–353, 370
 - show vpc orphan-ports 358
 - show vpc peer-keepalive 370
 - show vpc role 365–369, 371
 - show vpc statistics 347–348, 370–371
 - show vrf 160, 396–397
 - show vrrp detail 209
 - show dot1q-tunnel 414, 426
 - show interface mgmt 51
 - show mac address-table 320
 - show running-config l2pt 426
 - show running config 144
 - shutdown 28, 53–54, 66–67, 256, 274–275, 299
 - spanning-tree vlan 356–357
 - speed 10 258–259
 - speed 100 258–259
 - speed 1000 258–259
 - speed auto 40, 258–259
 - speed-group 91
 - speed-group 10000 37
 - switchport 39, 94, 121–122, 144–145, 250, 414, 419–420, 422
 - switchport access vlan 108–109
 - switchport host 110–111
 - switchport isolated 119
 - switchport mode dot1q-tunnel 414, 419–420, 422
 - switchport mode trunk 248, 250–251, 349–350
 - switchport mode 101, 108–109, 112–113
 - switchport trunk 250–251
 - switchport trunk allowed vlan 113, 115–116, 250–251, 349–350
 - switchport trunk native 250–251
 - switchport trunk native vlan 114
 - system default interface-vlan autostate 123–124
 - system default switchport 94, 127–128
 - system default switchport shutdown 128
 - system jumbomtu 62
 - system-mac 365
 - system-priority 366–367

T

terminal dont-ask [115](#)
 track [360](#)
 tunnel destination [387–390](#)
 トンネル モード [387–388, 392](#)
 tunnel mode gre ip [387–388, 395](#)
 tunnel mode ipip [387–390, 392](#)
 tunnel mode ipv6ipv6 decapsulate-any [392](#)
 tunnel path-mtu discovery [395](#)
 tunnel path-mtu discovery age-timer [395](#)
 tunnel path-mtu discovery min-mtu [395–396](#)
 tunnel source [387–390](#)
 tunnel ttl [387](#)
 tunnel use-vrf [387–388](#)

U

udld [69–70](#)
 udld aggressive [69](#)
 udld message-time [69](#)
 update-source [202–203, 221–222](#)

V

vlan dot1q tag native [404](#)
 vpc domain [346–348, 353–356, 360, 362, 365–368](#)
 vpc orphan-ports suspend [331, 358](#)
 vpc peer-link [349–350](#)
 vpc [351](#)
 vrf context [212](#)
 vrf member [160, 396](#)
 vrrp bfd [210](#)
 vrrp [210](#)

あ

address [464–465](#)

い

イーサネット [14](#)

イネーブル化 [455, 461–462](#)
 インターフェイス過負荷 [443](#)
 インターフェイスブレイクアウト [14](#)

<

graceful consistency-check [353–354](#)

し

end [156–157, 462, 464](#)

す

スタティック [438](#)

せ

説明 [49–50, 257, 387](#)

そ

速度 [258–259](#)

た

bandwidth [63–64, 254–255](#)
 タイムアウト [440](#)

ね

net [156–157](#)

ふ

broadcast [144](#)

る

loopback [154–155, 157](#)

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。