



## **Cisco DCNM インターフェイス コンフィギュレーション ガイド リリース 5.x**

**Cisco DCNM Interfaces Configuration Guide, Release 5.x**

2010 年 3 月 24 日

**【注意】シスコ製品をご使用になる前に、安全上の注意  
([www.cisco.com/jp/go/safety\\_warning/](http://www.cisco.com/jp/go/safety_warning/)) をご確認ください。**

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

**また、契約等の記述については、弊社販売パートナー、または、弊  
社担当者にご確認ください。**

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

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

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

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

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

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at [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. (1005R)

このマニュアルで使用している IP アドレスは、実際のアドレスを示すものではありません。マニュアル内の例、コマンド出力、および図は、説明のみを目的として使用されています。説明の中に実際のアドレスが使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

Cisco DCNM インターフェイス コンフィギュレーション ガイド リリース 5.x  
© 2008-2009 Cisco Systems, Inc.  
All rights reserved.

Copyright © 2008–2011, シスコシステムズ合同会社.  
All rights reserved.



## CONTENTS

新機能と変更された機能	xv
-------------	----

はじめに	xvii
------	------

対象読者	xvii
------	------

マニュアルの構成	xvii
----------	------

表記法	xviii
-----	-------

関連資料	xviii
------	-------

関連資料	xix
------	-----

マニュアルの入手方法およびテクニカル サポート	xx
-------------------------	----

## CHAPTER 1

概要	1-1
----	-----

インターフェイスについて	1-1
--------------	-----

イーサネット インターフェイス	1-2
-----------------	-----

アクセス ポート	1-3
----------	-----

トランク ポート	1-3
----------	-----

PVLAN ホストと無差別モード ポート	1-3
----------------------	-----

ルーテッド ポート	1-3
-----------	-----

管理インターフェイス	1-3
------------	-----

ポート チャネル インターフェイス	1-4
-------------------	-----

vPC	1-4
-----	-----

サブインターフェイス	1-4
------------	-----

VLAN ネットワーク インターフェイス	1-4
----------------------	-----

ループバック インターフェイス	1-4
-----------------	-----

トンネル インターフェイス	1-4
---------------	-----

Fabric Extender	1-5
-----------------	-----

バーチャライゼーション インターフェイス	1-5
----------------------	-----

インターフェイスのハイ アベイラビリティ	1-5
----------------------	-----

インターフェイスのライセンス要件	1-5
------------------	-----

## CHAPTER 2

基本インターフェイス パラメータの設定	2-1
---------------------	-----

基本インターフェイス パラメータについて	2-1
----------------------	-----

説明	2-2
----	-----

ビーコン	2-2
------	-----

MDIX	2-2
------	-----

デバウンス タイマー	2-2
------------	-----

Error Disabled	2-3	
レート モード	2-3	
速度モードとデュプレックス モード	2-4	
フロー制御	2-5	
ポート MTU サイズ	2-5	
帯域幅	2-6	
スループット遅延	2-6	
管理ステータス	2-6	
UDLD パラメータ	2-7	
UDLD の概要	2-7	
UDLD のデフォルト設定	2-8	
UDLD アグレッシブ モードおよび非アグレッシブ モード	2-8	
キャリア遅延	2-9	
管理インターフェイス IP アドレス パラメータ	2-9	
ポート チャンネル パラメータ	2-9	
ライセンス要件	2-10	
注意事項および制約事項	2-10	
基本インターフェイス パラメータの設定	2-11	
設定するインターフェイスの指定	2-12	
説明の設定	2-14	
ビーコン モードの設定	2-15	
帯域幅レート モードの変更	2-15	
Error-Disabled ステートの設定	2-16	
MDIX パラメータの設定	2-16	
デバウンス タイマーの設定	2-17	
インターフェイス速度およびデュプレックス モードの設定	2-17	
フロー制御の設定	2-18	
MTU サイズの設定	2-20	
インターフェイス MTU サイズの設定	2-20	
システム ジャンボ MTU サイズの設定	2-21	
帯域幅の設定	2-22	
スループット遅延の設定	2-22	
インターフェイスのシャットダウンおよび再開	2-23	
CDP のイネーブル化またはディセーブル化	2-24	
UDLD モードの設定	2-25	
キャリア遅延タイマーの設定	2-26	
管理インターフェイスの IP アドレスの設定	2-26	
フィールドの説明	2-28	
[Device] : [Device Details] : [MTU Settings] セクション	2-28	

[Device] : [Device Details] : [Error Disable Settings] セクション	2-28
[Device] : [Device Status] タブ	2-29
[Port] : [Port Details] : [Basic Settings] セクション	2-30
[Port] : [Port Details] : [Port Mode Settings] セクション	2-31
[Port] : [Port Details] : [Advanced Settings] セクション	2-32
[Port] : [Port Status] : [Port Status] セクション	2-34
[Port] : [Port Status] : [Port Status SFP] セクション	2-35
[Port] : [Port Status] : [Port SFP Diagnostics] セクション	2-36
その他の関連資料	2-37
関連資料	2-38
標準規格	2-38
基本インターフェイス パラメータ設定の機能履歴	2-38

### CHAPTER 3

レイヤ 2 インターフェイスの設定	3-1
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	3-2
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	3-2
IEEE 802.1Q カプセル化	3-3
アクセス VLAN	3-4
トランク ポートのネイティブ VLAN ID	3-5
ネイティブ VLAN トラフィックのタギング	3-5
許容 VLAN	3-5
ハイ アベイラビリティ	3-6
バーチャライゼーションのサポート	3-6
レイヤ 2 ポート モードのライセンス要件	3-6
VLAN トランキングの前提条件	3-6
注意事項および制約事項	3-7
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	3-8
レイヤ 2 アクセス ポートとしての LAN インターフェイスの設定	3-8
トランク ポートの設定	3-9
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	3-10
統計情報の表示とクリア	3-11
フィールドの説明	3-11
その他の関連資料	3-12
関連資料	3-12
標準規格	3-12
管理情報ベース (MIB)	3-13
レイヤ 2 インターフェイス設定の機能履歴	3-13

CHAPTER 4

レイヤ 3 インターフェイスの設定 4-1

レイヤ 3 インターフェイスについて 4-1

ルーテッド インターフェイス 4-2

サブインターフェイス 4-2

VLAN インターフェイス 4-3

ループバック インターフェイス 4-4

トンネル インターフェイス 4-4

ハイ アベイラビリティ 4-4

バーチャライゼーションのサポート 4-5

レイヤ 3 インターフェイスのライセンス要件 4-5

ライセンス 3 インターフェイスの前提条件 4-5

注意事項および制約事項 4-5

レイヤ 3 インターフェイスの設定 4-6

ルーテッド インターフェイスの設定 4-7

IPv4 セカンダリ アドレスまたはヘルパー アドレスの設定 4-8

IPv6 セカンダリ アドレスの設定 4-9

サブインターフェイスの設定 4-9

サブインターフェイスの削除 4-11

ポート チャネル サブインターフェイスの作成 4-11

ポート チャネル サブインターフェイスの削除 4-12

インターフェイスでの帯域幅の設定 4-13

VLAN ネットワーク インターフェイスの設定 4-14

VLAN ネットワーク インターフェイスの削除 4-15

ループバック インターフェイスの設定 4-15

ループバック インターフェイスの削除 4-16

レイヤ 3 インターフェイス統計情報の表示 4-17

関連項目 4-17

レイヤ 3 インターフェイスのフィールドの説明 4-17

ルーテッド インターフェイス 4-17

ループバック 4-17

[Loopback] : [Details] タブ : [Basic Settings] セクション 4-18

[Loopback] : [Details] タブ : [IP Address Settings] セクション 4-18

[Loopback] : [Statistics] タブ 4-18

VLAN ネットワーク インターフェイス 4-19

[VLAN Network Interface] : [Details] タブ : [Basic Settings] セクション 4-19

[VLAN Network Interface] : [Details] タブ : [IP Address Settings] セクション 4-19

[VLAN Network Interface] : [Statistics] タブ 4-20

その他の関連資料	4-20
関連資料	4-20
管理情報ベース (MIB)	4-20
標準規格	4-20
レイヤ 3 インターフェイス設定の機能履歴	4-21

## CHAPTER 5

ポート チャネルの設定	5-1
ポート チャネルについて	5-2
ポート チャネル	5-3
ポート チャネル インターフェイス	5-4
基本設定	5-4
互換性要件	5-5
ポート チャネルを使ったロード バランシング	5-6
LACP	5-8
LACP の概要	5-8
ポート チャネル モード	5-9
LACP ID パラメータ	5-10
LACP Marker Responder	5-11
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	5-12
LACP 互換性の拡張	5-12
バーチャライゼーションのサポート	5-12
ハイ アベイラビリティ	5-13
ポート チャネリングのライセンス要件	5-13
ポート チャネリングの前提条件	5-14
注意事項および制約事項	5-14
ポート チャネルの設定	5-15
ポート チャネルの作成	5-16
ポート チャネルの削除	5-17
レイヤ 2 ポートをポート チャネルに追加	5-18
レイヤ 3 ポートをポート チャネルに追加	5-19
ポート チャネルからのポートの削除	5-20
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	5-20
ポートをポート チャネルに強制的に参加	5-21
ポート チャネルへの CDP リンクの追加	5-21
ポート チャネルへのリンクの削除	5-22
ポート チャネルの説明の設定	5-22
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	5-23

ポート チャンネルを使ったロード バランシングの設定	5-24
LACP のイネーブル化	5-24
LACP ポート チャンネル ポート モードの設定	5-25
LACP システム プライオリティの設定	5-26
LACP ポート プライオリティの設定	5-26
LACP グレースフル コンバージェンス	5-27
LACP グレースフル コンバージェンスの再イネーブル化	5-28
LACP の個別一時停止のディセーブル化	5-29
LACP の個別一時停止の再イネーブル化	5-30
統計情報の表示	5-30
ポート チャンnelingと LACP のフィールドの説明	5-31
[Device] : [Port Channel Configuration] タブ	5-31
[Device] : [vPC Configuration] タブ	5-32
[Port Channel] : [Port Channel Details] : [Common Settings] セクション	5-33
[Port Channel] : [Port Channel Details] : [Basic Settings] セクション	5-33
[Port Channel] : [Port Channel Details] : [Link Settings] セクション	5-33
[Port Channel] : [Port Channel Advanced Settings for Switched Port Channels] : [VLAN Settings] セクション	5-35
[Port Channel] : [Port Channel Advanced Settings for Routed Port Channels] : [IP Address] セクション	5-35
[Port Channel] : [Port Channel Advanced Settings] : [Advanced Settings] セクション	5-36
[Port Channel Subinterface] : [Subinterface Details] : [Basic Settings] セクション	5-36
[Port Channel Subinterface] : [Subinterface Details] : [IP Address Settings] セクション	5-37
その他の関連資料	5-37
関連資料	5-38
標準規格	5-38
管理情報ベース (MIB)	5-38
ポート チャンネル設定の機能履歴	5-38

## CHAPTER 6

## vPC の設定 6-1

vPC について	6-2
vPC の概要	6-2
vPC の用語	6-5
vPC ピア リンク	6-6
vPC ピア リンクの概要	6-6
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	6-8
レイヤ 3 接続のための VLAN インターフェイスの設定	6-9



ピアキーブアライブ リンクとメッセージ	6-9
vPC ピア ゲートウェイ	6-11
vPC ドメイン	6-11
vPC ピア リンクの互換パラメータ	6-12
同じでなければならない設定パラメータ	6-12
同じにすべき設定パラメータ	6-13
vPC 番号	6-14
他のポート チャネルの vPC への移行	6-15
単一モジュール上での vPC ピア リンクとコアへのリンクの設定	6-15
その他の機能との vPC の相互作用	6-15
vPC と LACP	6-16
vPC ピア リンクと STP	6-16
vPC マルチキャスト : PIM、IGMP、および IGMP スヌーピング	6-18
vPC ピア リンクとルーティング	6-18
CFSOE	6-19
ハイ アベイラビリティ	6-20
vPC のライセンス要件	6-20
vPC の前提条件	6-20
注意事項および制約事項	6-21
vPC の設定	6-21
vPC のイネーブル化	6-22
vPC のディセーブル化	6-23
vPC の作成と変更	6-23
vPC と vPC ピア リンクの同期化	6-28
ピアキーブアライブ リンクおよびメッセージの手動による設定	6-29
vPC のプライオリティ設定の手動による設定	6-30
vPC の削除	6-31
[Details] タブのペインを使用した vPC 設定の変更	6-32
vPC の統計情報の表示	6-33
vPC のフィールドの説明	6-34
[vPC] : [vPC Details] : [Basic Settings] セクション	6-34
[vPC] : [vPC Details] : [Layer 2 Settings] セクション	6-35
[vPC] : [vPC Details] : [Link Settings] セクション	6-36
[vPC] : [Peer-Link Details] : [vPC Global Settings] セクション	6-37
[vPC] : [Peer-Link Details] : [STP Global Settings] セクション	6-37
[vPC] : [Peer-Link Status] : [Peer Link Status] セクション	6-38
[vPC] : [Peer-Link Status] : [Peer Link Error VLANs Status] セクション	6-39
[vPC] : [Peer-Link Status] : [vPC Error VLANs Status] セクション	6-39

[Resolve Configuration Inconsistency] : [vPC]	6-39
[Resolve Configuration Inconsistency] : [Peer Link]	6-42
その他の関連資料	6-43
関連資料	6-43
標準規格	6-43
管理情報ベース (MIB)	6-43
vPC の設定機能の履歴	6-44

## CHAPTER 7

<b>IP トンネルの設定</b>	<b>7-1</b>
IP トンネルについて	7-1
IP トンネルの概要	7-2
GRE トンネル	7-2
Path MTU Discovery (PMTUD)	7-3
バーチャライゼーションのサポート	7-3
ハイ アベイラビリティ	7-3
IP トンネルのライセンス要件	7-3
IP トンネルの前提条件	7-4
注意事項および制約事項	7-4
IP トンネルの設定	7-4
トンネリングのイネーブル化	7-5
トンネル インターフェイスの作成	7-5
トンネル インターフェイスの削除	7-6
トンネル インターフェイス統計情報の表示	7-6
トンネル インターフェイスのためのフィールドの説明	7-7
[Tunnel] : [Details] タブ : [Tunnel Details] セクション	7-7
[Tunnels] : [Details] タブ : [Source] セクション	7-7
[Tunnels] : [Statistics] タブ	7-8
その他の関連資料	7-8
関連資料	7-8
標準規格	7-8
IP トンネル設定の機能履歴	7-8

## CHAPTER 8

<b>仮想イーサネット インターフェイスの設定</b>	<b>8-1</b>
vEthernet インターフェイスについて	8-1
vEthernet インターフェイスのライセンス要件	8-2
プラットフォーム サポート	8-2
vEthernet インターフェイスの設定	8-2
vEthernet インターフェイスのグローバル設定	8-3

vEthernet インターフェイスの説明の設定	8-3	
vEthernet インターフェイスの VMware DVPort ID の設定	8-4	
vEthernet インターフェイスの静的ピン接続の設定	8-5	
vEthernet アクセス インターフェイスの設定	8-6	
vEthernet トランク インターフェイスの設定	8-7	
vEthernet インターフェイスでのプライベート VLAN の設定	8-8	
vEthernet インターフェイスの IPv4 ACL の設定	8-9	
vEthernet インターフェイスでの MAC ACL の設定	8-9	
vEthernet インターフェイスでの SPAN の設定	8-10	
vEthernet インターフェイスのイネーブル化またはディセーブル化	8-11	
vEthernet インターフェイスの概要の表示	8-11	
vEthernet インターフェイス ポートのステータスの表示	8-12	
vEthernet インターフェイス統計情報の表示	8-12	
仮想イーサネット モジュールの統計情報の表示	8-12	
vEthernet インターフェイスのためのフィールドの説明	8-13	
[Virtual Ethernet] : [Device Details]	8-13	
[Virtual Ethernet] : [Device Status]	8-13	
[Virtual Ethernet] : [Port Details] : [Basic Settings] セクション	8-14	
[Virtual Ethernet] : [Port Details] : [Port Mode Settings] セクション	8-14	
[Virtual Ethernet] : [Port Details] : [Advanced Settings] セクション	8-14	
[Virtual Ethernet] : [Port Status] : [Port Status] セクション	8-15	
その他の関連資料	8-15	
関連資料	8-15	
標準規格	8-16	
vEthernet インターフェイスの機能の履歴	8-16	

## CHAPTER 9

## Fabric Extender の設定 9-1

Fabric Extender について	9-1
Fabric Extender の用語	9-2
オーバーサブスクリプション	9-2
管理モデル	9-3
Fabric Extender のイメージ管理	9-3
ホスト インターフェイス	9-3
ホスト EtherChannel	9-3
Fabric Extender のモデル	9-4
Fabric Extender のライセンス要件	9-4
Fabric Extender の前提条件	9-4
プラットフォーム サポート	9-4
Fabric Extender の設定	9-5

Fabric Extender の追加	9-6
Fabric Extender の削除	9-6
Fabric Extender の編集	9-7
リンクの再配布	9-7
リンク数の変更	9-7
ピン接続順序の維持	9-8
Fabric Extender とイーサネット インターフェイスの関連付け	9-8
Fabric Extender の関連付け	9-8
イーサネット ポート モードを Fabric Extender に設定	9-9
Fabric Extender とポート チャネルの関連付け	9-9
Fabric Extender の関連付け	9-9
ポート モードを Fabric Extender に設定	9-10
Fabric Extender のフィールドの説明	9-10
Fabric Extender の [Summary] ペイン	9-11
Fabric Extender の [Details] ペイン	9-12
その他の関連資料	9-12
Fabric Extender の機能履歴	9-12

## CHAPTER 10

## ポート プロファイルの設定 10-1

ポート プロファイルについて	10-1
ポート プロファイルのステート	10-2
ポート プロファイルの継承	10-2
システム ポート プロファイル	10-2
ポート プロファイルとポート グループ	10-2
ポート プロファイルの特性	10-3
ポート プロファイルと vPC ホスト モード	10-3
CDP または手動方式によるサブグループの作成	10-4
静的ピン接続によるインターフェイスの割り当て	10-5
ポート プロファイルと MAC ピン接続	10-5
ポート プロファイルとレイヤ 3 制御	10-6
ポート プロファイルと iSCSI マルチパス	10-7
ポート プロファイルのライセンス要件	10-7
プラットフォーム サポート	10-7
ポート プロファイルの設定	10-7
ポート プロファイルの作成	10-8
ポート プロファイルの削除	10-9
ポート プロファイルのイネーブル化とディセーブル化	10-9
ポート プロファイル継承の設定	10-10
システム ポート プロファイルの設定	10-10

仮想サービス ドメインのポート プロファイルの設定	10-11
レイヤ 3 制御のためのポート プロファイルの設定	10-11
iSCSI マルチパスのためのポート プロファイルの設定	10-13
VMware ポート グループとしてのポート プロファイルの設定	10-14
ポート チャネルの設定	10-15
vEthernet インターフェイスの静的ピン接続の設定	10-16
コントロールまたはパケット VLAN の静的ピン接続の設定	10-17
ポート管理の設定	10-17
プライベート VLAN としてのポート プロファイルの設定	10-18
DHCP スヌーピングの設定	10-19
IP ソース ガードの設定	10-20
ARP 検査の設定	10-20
レイヤ 2 インターフェイスに対するポート セキュリティのイネーブル化またはディセーブル化	10-21
スティッキ MAC アドレス学習のイネーブル化またはディセーブル化	10-22
MAC アドレスの最大数の設定	10-22
アドレス エージングのタイプと期間の設定	10-23
セキュリティ違反時の処理の設定	10-24
IPv4 ACL の設定	10-24
MAC ACL の設定	10-25
CLI の確認	10-25
複数デバイスへのポート プロファイルのコピー	10-26
ポート プロファイルのフィールドの説明	10-26
[Port Profile] : [Settings] : [Basic Settings] セクション	10-27
[Port Profile] : [Settings] : [Inherited Interfaces] セクション	10-27
[Port Profile] : [Advanced Settings] : [System, VM Settings] セクション	10-27
[Port Profile] : [Advanced Settings] : [Port Channel, Pinning] セクション	10-28
[Port Profile] : [Features] : [Interfaces] : [Ethernet]	10-29
[Port Profile] : [Features] : [Switching] : [VLAN]	10-29
[Port Profile] : [Features] : [Switching] : [DHCP Snooping]	10-30
[Port Profile] : [Features] : [Switching] : [IP Source Guard]	10-30
[Port Profile] : [Features] : [Switching] : [ARP Inspection]	10-30
[Port Profile] : [Features] : [Switching] : [Port Security]	10-31
[Port Profile] : [Features] : [Security] : [IPv4 ACL]	10-31
[Port Profile] : [Features] : [Security] : [MAC ACL]	10-31
その他の関連資料	10-32
関連資料	10-32
標準規格	10-32
ポート プロファイルの機能履歴	10-32

APPENDIX A Cisco NX-OS インターフェイスがサポートする IETF RFC A-1  
IPv6 に関する RFC の参考資料 A-1

APPENDIX B Cisco NX-OS インターフェイスの設定制限 B-1

INDEX



## 新機能と変更された機能

この章では、『Cisco DCNM Interfaces Configuration Guide, Release 4.2』に記載されている新機能および変更された機能について、リリース固有の情報を示します。このマニュアルの最新版は、シスコの次の Web サイトから入手できます。

[http://www.cisco.com/en/US/docs/switches/datacenter/sw/4\\_2/dcnm/interfaces/configuration/guide/if\\_dcnm.html](http://www.cisco.com/en/US/docs/switches/datacenter/sw/4_2/dcnm/interfaces/configuration/guide/if_dcnm.html)

Cisco DCNM Release 5.x に関する追加情報については、次のシスコ Web サイトから入手できる『Cisco DCNM Release Notes』を参照してください。

[http://www.cisco.com/en/US/docs/switches/datacenter/sw/4\\_2/dcnm/release/notes/dcnm\\_4\\_2\\_relnotes.html](http://www.cisco.com/en/US/docs/switches/datacenter/sw/4_2/dcnm/release/notes/dcnm_4_2_relnotes.html)

表 1 では、『Cisco DCNM Interfaces Configuration Guide, Release 4.2』における新機能および変更された機能を要約し、その参照先を示しています。

表 1 リリース 5.x の新機能および変更された機能

機能	説明	変更されたリリース	参照先
仮想ポート チャンネル (vPC)	ウィザードを使用して、ピアのキープアライブ メッセージ、ロールおよびシステム プライオリティを設定できます。	4.2(1)	第 6 章「vPC の設定」
仮想ポート チャンネル (vPC)	ピアのキープアライブ メッセージのホールド タイムおよび優先順位の値を設定する機能が追加されました。	4.2(1)	第 6 章「vPC の設定」
すべての VDC 内の GRE トンネル インターフェイス	すべての VDC 内のトンネル インターフェイスを作成できます。	4.2(1)	第 7 章「IP トンネルの設定」
Fabric Extender	Fabric Extender を展開および管理できます。	4.2(1)	第 9 章「Fabric Extender の設定」
SFP 診断および SOLM 統計のチャート	インターフェイスについての統計情報を収集し、表示できます。	4.2(3)	第 3 章「レイヤ 2 インターフェイスの設定」
ポート プロファイル	ポート プロファイルを 1 つ設定して複数のインターフェイスに割り当てると、これらのインターフェイスの設定を統一することができます。	5.0(2)	第 10 章「ポート プロファイルの設定」
vEthernet インターフェイス	Cisco Nexus 1000V シリーズ スイッチ で、仮想イーサネット インターフェイスを設定できます。	5.0(2)	第 8 章「仮想イーサネット インターフェイスの設定」







## はじめに

ここでは、『Cisco DCNM インターフェイス コンフィギュレーション ガイド リリース 5.x』の対象読者、構成、および表記法について説明します。また、関連マニュアルの入手方法についても説明します。

## 対象読者

このマニュアルは、Cisco DCNM の設定および維持に携わる、十分な経験を持つネットワーク管理者を対象としています。

## マニュアルの構成

このマニュアルの構成は、次のとおりです。

章	説明
第 1 章「概要」	Cisco DCNM インターフェイスの概要です。
第 2 章「基本インターフェイス パラメータの設定」	レイヤ 2 およびレイヤ 3 インターフェイスで共有する基本パラメータを設定する手順について説明します。
第 3 章「レイヤ 2 インターフェイスの設定」	レイヤ 2 スイッチング ポートをアクセス ポートまたはトランク ポートとして設定する手順について説明します。
第 4 章「レイヤ 3 インターフェイスの設定」	レイヤ 3 インターフェイスを設定する手順について説明します。
第 5 章「ポート チャネルの設定」	ポート チャネルを設定し、ポート チャネルをより有効に利用するために Link Aggregation Control Protocol (LACP) を適用して設定する手順を説明します。
第 6 章「vPC の設定」	Virtual Port Channels (vPC; 仮想ポート チャネル) の設定方法について説明します。
第 7 章「IP トンネルの設定」	装置で Generic Route Encapsulation (GRE) を使って IP トンネルを設定する手順について説明します。

章	説明
<a href="#">第 8 章「仮想イーサネット インターフェイスの設定」</a>	仮想イーサネット インターフェイスの設定方法について説明します。
<a href="#">第 9 章「Fabric Extender の設定」</a>	Cisco Nexus 2000 シリーズ Fabric Extender を Cisco Nexus デバイスと共存させて設定する方法を説明します。
<a href="#">第 10 章「ポート プロファイルの設定」</a>	ポート プロファイルの設定方法について説明します。
<a href="#">付録 A「Cisco NX-OS インターフェイスがサポートする IETF RFC」</a>	Cisco NX-OS Release 4.x でサポートするインターフェイスに関する Internet Engineering Task Force (IETF; インターネット技術特別調査委員会) Request for Comments (RFC) を示します。
<a href="#">付録 B「Cisco NX-OS インターフェイスの設定制限」</a>	NX-OS Release 4.x を実行するデバイスについてシスコが認定した制限および最大制限を示します。

## 表記法

このマニュアルでは、次の表記法を使用しています。



(注)

「注釈」を意味します。役立つ情報や、このマニュアル以外の参照資料などを紹介しています。



注意

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

## 関連資料

[Cisco NX-OS](#) には、次の資料が含まれます。

### リリース ノート

『*Cisco Nexus 7000 Series NX-OS Release Notes, Release 5.x*』

### NX-OS コンフィギュレーション ガイド

『*Cisco Nexus 7000 Series NX-OS Getting Started with Virtual Device Contexts, Release 5.x*』

『*Cisco Nexus 7000 Series NX-OS Fundamentals Configuration Guide, Release 5.x*』

『*Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 5.x*』

『*Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide, Release 5.x*』

『*Cisco Nexus 7000 Series NX-OS Quality of Service Configuration Guide, Release 5.x*』

『*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 5.x*』

『*Cisco Nexus 7000 Series NX-OS Multicast Routing Configuration Guide, Release 5.x*』

『*Cisco Nexus 7000 Series NX-OS Security Configuration Guide, Release 5.x*』

『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 5.x*』

『Cisco Nexus 7000 Series NX-OS Software Upgrade and Downgrade Guide, Release 5.x』  
『Cisco Nexus 7000 Series NX-OS Licensing Guide, Release 5.x』  
『Cisco Nexus 7000 Series NX-OS High Availability and Redundancy Guide, Release 5.x』  
『Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 5.x』  
『Cisco NX-OS XML Management Interface User Guide, Release 5.x』  
『Cisco NX-OS System Messages Reference』  
『Cisco Nexus 7000 Series NX-OS MIB Quick Reference』

## NX-OS コマンド リファレンス

『Cisco Nexus 7000 Series NX-OS Command Reference Master Index, Release 5.x』  
『Cisco Nexus 7000 Series NX-OS Fundamentals Command Reference, Release 5.x』  
『Cisco Nexus 7000 Series NX-OS Interfaces Command Reference, Release 5.x』  
『Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference, Release 5.x』  
『Cisco Nexus 7000 Series NX-OS Quality of Service Command Reference, Release 5.x』  
『Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference, Release 5.x』  
『Cisco Nexus 7000 Series NX-OS Multicast Routing Command Reference, Release 5.x』  
『Cisco Nexus 7000 Series NX-OS Security Command Reference, Release 5.x』  
『Cisco Nexus 7000 Series NX-OS Virtual Device Context Command Reference, Release 5.x』  
『Cisco Nexus 7000 Series NX-OS System Management Command Reference, Release 5.x』

## その他のソフトウェアのマニュアル

『Cisco Nexus 7000 Series NX-OS Troubleshooting Guide, Release 5.x』

## 関連資料

Cisco DCNM のマニュアルは、次の URL で入手できます。

[http://www.cisco.com/en/US/products/ps9369/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/ps9369/tsd_products_support_series_home.html)

Cisco DCNM のマニュアル セットには、次の資料が含まれます。

## リリース ノート

『Cisco DCNM Release Notes, Release 5.x』

## DCNM コンフィギュレーション ガイド

『Cisco DCNM Getting Started with Virtual Device Contexts, Release 5.x』  
『Cisco DCNM Fundamentals Configuration Guide, Release 5.x』  
『Cisco DCNM System Management Configuration Guide, Release 5.x』  
『Cisco DCNM インターフェイス コンフィギュレーション ガイド リリース 5.x』  
『Cisco DCNM Layer 2 Switching Configuration Guide, Release 5.x』

『Cisco DCNM Web Services API Guide, Release 5.x』

『Cisco DCNM Security Configuration Guide, Release 5.x』

『Cisco DCNM Unicast Routing Configuration Guide, Release 5.x』

『Cisco DCNM Virtual Device Context Configuration Guide, Release 5.x』

『Cisco DCNM Software Upgrade Guide, Release 5.x』

## マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカル サポート、その他の有用な情報について、次の URL で、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

『*What's New in Cisco Product Documentation*』は RSS フィードとして購読できます。また、リーダーアプリケーションを使用してコンテンツがデスクトップに直接配信されるように設定することもできます。RSS フィードは無料のサービスです。シスコは現在、RSS バージョン 2.0 をサポートしています。



# CHAPTER 1

## 概要

この章では、Cisco NX-OS ソフトウェアでサポートするインターフェイス タイプの概要を説明します。  
この章では、次の内容について説明します。

- 「インターフェイスについて」 (P.1-1)
- 「バーチャライゼーション インターフェイス」 (P.1-5)
- 「インターフェイスのハイ アベイラビリティ」 (P.1-5)
- 「インターフェイスのライセンス要件」 (P.1-5)

## 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。

表 1-1 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 1-1 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、デュプレクス、エラー ディセーブル、フロー制御、MTU、ビーコン	このマニュアルの第 2 章「基本インターフェイスパラメータの設定」
レイヤ 2	レイヤ 2 アクセスおよびトランク ポート設定	このマニュアルの第 3 章「レイヤ 2 インターフェイスの設定」
	レイヤ 2 MAC、VLAN、プライベート VLAN、Rapid PVST+、Multiple Spanning Tree、スパンニング ツリー拡張	『Cisco DCNM Layer 2 Switching Configuration Guide, Release 5.x』
	ポート セキュリティ	『Cisco DCNM Security Configuration Guide, Release 5.x』
レイヤ 3	メディア、IPv4 および IPv6 アドレス	このマニュアルの「レイヤ 3 インターフェイスの設定」 (P.4-1)
	帯域幅、遅延、IP ルーティング、VRF	『Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 5.x』 『Cisco Nexus 7000 Series NX-OS Multicast Routing Configuration Guide, Release 5.x』

表 1-1 インターフェイスのパラメータ (続き)

機能	パラメータ	解説場所
ポート チャンネル	チャンネル グループ、LACP	このマニュアルの第 5 章「ポート チャンネルの設定」
vPC	仮想ポート チャンネル	このマニュアルの第 6 章「vPC の設定」
トンネル	GRE トンネリング	このマニュアルの第 7 章「IP トンネルの設定」
セキュリティ	Dot1X、NAC、EOU、ポート セキュリティ	『Cisco DCNM Security Configuration Guide, Release 5.x』
仮想イーサネット インターフェイス	仮想ポートに接続されたスイッチ インターフェイスに対応する論理インターフェイス。	このマニュアルの第 8 章「仮想イーサネット インターフェイスの設定」
Fabric Extender	サーバ集約のための高密度かつ低コストの接続。	このマニュアルの第 9 章「Fabric Extender の設定」
ポート プロファイル	インターフェイスの設定を単純化するためのメカニズム。	このマニュアルの第 10 章「ポート プロファイルの設定」

ここでは、次の内容について説明します。

- 「イーサネット インターフェイス」(P.1-2)
- 「管理インターフェイス」(P.1-3)
- 「ポート チャンネル インターフェイス」(P.1-4)
- 「vPC」(P.1-4)
- 「サブインターフェイス」(P.1-4)
- 「VLAN ネットワーク インターフェイス」(P.1-4)
- 「ループバック インターフェイス」(P.1-4)
- 「トンネル インターフェイス」(P.1-4)
- 「Fabric Extender」(P.1-5)

## 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、アクセス ポート、トランク ポート、Private VLAN (PVLAN; プライベート VLAN) ホスト ポートと無差別モード ポート、ルーテッド ポートがあります。

ここでは、次の内容について説明します。

- 「アクセス ポート」(P.1-3)
- 「トランク ポート」(P.1-3)
- 「PVLAN ホストと無差別モード ポート」(P.1-3)
- 「ルーテッド ポート」(P.1-3)

## 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 インターフェイスの詳細については、[第 3 章「レイヤ 2 インターフェイスの設定」](#)を参照してください。

## トランク ポート

トランク ポートは複数の 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。トランクポート インターフェイスの詳細については、[第 3 章「レイヤ 2 インターフェイスの設定」](#)を参照してください。

## PVLAN ホストと無差別モード ポート

プライベート VLAN (PVLAN) は、レイヤ 2 レベルでのトラフィック分離とセキュリティを実現します。PVLAN は 1 つのプライマリ VLAN と 1 つのセカンダリ VLAN を 1 つまたは複数組み合わせたもので、プライマリ VLAN はすべて同じです。セカンダリ VLAN には 2 種類あり、独立 VLAN とコミュニティ VLAN と呼ばれます。

独立 VLAN では、PVLAN ホストはプライマリ VLAN のホストとだけ通信します。コミュニティ VLAN では、PVLAN ホストは同じコミュニティ内の PVLAN ホスト同士およびプライマリ VLAN のホストとだけ通信し、独立 VLAN や他のコミュニティの VLAN のホストとは通信しません。コミュニティ VLAN は無差別モード ポートを使って PVLAN の外部と通信します。独立およびコミュニティ セカンダリ VLAN が組み合わされているにもかかわらず、プライマリ VLAN 内のすべてのインターフェイスはレイヤ 2 ドメイン 1 つだけで構成されており、必要な IP サブネットは 1 つです。

PVLAN 無差別モード ポートにレイヤ 3 VLAN ネットワーク インターフェイスや Switched Virtual Interface (SVI; スイッチ仮想インターフェイス) を設定し、プライマリ PVLAN にルーティング機能を持たせることもできます。

PVLAN ホストおよび PVLAN 無差別モード ポートの設定や他の PVLAN の設定の詳細については、『*Cisco DCNM Layer 2 Switching Configuration Guide, Release 5.x*』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、Spanning Tree Protocol (STP; スパニング ツリー プロトコル) などのレイヤ 2 プロトコルはサポートしません。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](#)』(P.4-2) 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、Simple Network Management Protocol (SNMP; 簡易ネットワーク管理プロトコル)、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、『』を参照してください。このマニュアルにも、管理インターフェイスの IP アドレスとデフォルト IP ルーティング設定に関する情報を記載しています。

## 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 8 つの物理ポートへの個別リンクを 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 チャネリングにより、これらの物理インターフェイス チャネルのトラフィックをロード バランスさせることもできます。ポート チャネル インターフェイスの詳細については、[第 5 章「ポート チャネルの設定」](#)を参照してください。

## vPC

仮想ポート チャネル (vPC) によって、2 個の異なる Cisco Nexus 7000 シリーズ デバイスを物理的に接続し、第 3 のデバイスからは 1 つのポートとして見えるリンクが実現します。第 3 のデバイスには、スイッチ、サーバ、またはその他の任意のネットワーク デバイスが可能です。それぞれのデバイスで合計 768 個の vPC を設定できます。vPC は、レイヤ 2 マルチパスを行います。vPC の詳細については、[第 6 章「vPC 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インターフェイスを作成できます。親インターフェイスは物理ポートでもポート チャネルでもかまいません。親インターフェイスはサブインターフェイスによって複数の仮想インターフェイスに分割されます。これらの仮想インターフェイスに IP アドレスやダイナミック ルーティング プロトコルなど固有のレイヤ 3 パラメータを割り当てることができます。サブインターフェイスの詳細については、「[サブインターフェイス](#)」(P.4-2) を参照してください。

## VLAN ネットワーク インターフェイス

VLAN ネットワーク インターフェイスは仮想のルーテッドインターフェイスで、デバイスの VLAN を同じデバイスのレイヤ 3 ルータ エンジンに接続します。レイヤ 3 内部 VLAN ルーティングが実現できるように VLAN ネットワーク インターフェイス間をルーティングできます。VLAN ネットワーク インターフェイスの詳細については、「[VLAN インターフェイス](#)」(P.4-3) を参照してください。

## ループバック インターフェイス

仮想ループバック インターフェイスは、常にアップ状態にあるシングル エンドポイントを持つ仮想インターフェイスです。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](#)」(P.4-4) を参照してください。

## トンネル インターフェイス

トランスポート プロトコル内部の任意のパケットは、トンネリングによってカプセル化されます。この機能は、簡単なインターフェイスを設定する仮想インターフェイスとして実装されています。トンネル インターフェイスにより、任意の標準的な Point-To-Point (p2p; ポイントツーポイント) カプセル化スキームの実装に必要なサービスが提供されます。リンクごとに個別のトンネルを設定できます。詳細については、[第 7 章「IP トンネルの設定」](#)を参照してください。



## Fabric Extender

DCNM Release 4.2(1) 以降、Cisco Nexus 2000 シリーズ Fabric Extender を Cisco NX-OS デバイスと連携させることで、サーバ集約で高密度かつ低コストの接続を実現します。Fabric Extender は、ギガビットイーサネット、10 ギガビットイーサネット、ユニファイドファブリック、ラック、ブレードサーバなどの環境全体で拡張性を高め、データセンターのアーキテクチャと運用を簡素化するように設計されています。

Fabric Extender は、親スイッチの Cisco NX-OS スイッチに統合されることで、親スイッチから提供される設定情報を使用して、自動的にプロビジョニングおよび設定を行うことができます。この統合により、単一管理ドメインで、多くのサーバやホストが、セキュリティや Quality of Service (QoS) 設定パラメータを含め、親スイッチと同じフィーチャセットを使用してサポートされます。Fabric Extender と親スイッチを統合することにより、スパンニングツリープロトコル (STP) を使用することなく、大規模なマルチパス、ループフリー、およびアクティブ-アクティブのデータセンタートポロジが構築できます。

Cisco Nexus 2148T Fabric Extender は、すべてのトラフィックを親の Cisco NX-OS スイッチに 10 ギガビットイーサネットファブリックアップリンクを介して転送します。このため、すべてのトラフィックが Cisco NX-OS スイッチで確立されているポリシーにより検査されます。

## バーチャライゼーション インターフェイス

複数の Virtual Device Context (VDC; 仮想デバイス コンテキスト) が作成できます。各 VDC は独立した論理デバイスで、インターフェイスを割り当てることができます。VDC にインターフェイスを割り当てると、正しい VDC であればそのインターフェイスだけが設定できます。VDC の詳細については、『Cisco DCNM Virtual Device Context Configuration Guide, Release 5.x』を参照してください。

## 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。

## インターフェイスのライセンス要件

IP トンネルおよび vPC には Enterprise Services ライセンスが必要です。このライセンスは IP トンネルをイネーブルにするシステムごとにインストールする必要があります。他のインターフェイスにはライセンスが必要ありません。





## CHAPTER 2

# 基本インターフェイス パラメータの設定

この章では、Cisco DCNM で管理されるインターフェイスの基本インターフェイス パラメータを設定する方法について説明します。



(注)

管理対象デバイス上で実行される Cisco NX-OS リリースでは、この章で説明する機能や設定がすべてサポートされるとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースのマニュアルとリリース ノートを参照してください。

この章では、次の内容について説明します。

- 「基本インターフェイス パラメータについて」 (P.2-1)
- 「ライセンス要件」 (P.2-10)
- 「注意事項および制約事項」 (P.2-10)
- 「基本インターフェイス パラメータの設定」 (P.2-11)
- 「フィールドの説明」 (P.2-28)
- 「その他の関連資料」 (P.2-37)
- 「基本インターフェイス パラメータ設定の機能履歴」 (P.2-38)



(注)

レイヤ 2 インターフェイスで独自に使用するパラメータを設定するには、第 3 章「レイヤ 2 インターフェイスの設定」を参照してください（アクセス インターフェイスやトランキング インターフェイス）。レイヤ 3 インターフェイスで独自に使用するパラメータを設定するには、第 4 章「レイヤ 3 インターフェイスの設定」を参照してください（ルーテッド インターフェイス、サブインターフェイス、VLAN インターフェイス、ループバック インターフェイス、IP トンネル）。

## 基本インターフェイス パラメータについて

ここでは、次の内容について説明します。

- 「説明」 (P.2-2)
- 「ビーコン」 (P.2-2)
- 「MDIX」 (P.2-2)
- 「デバウンス タイマー」 (P.2-2)
- 「Error Disabled」 (P.2-3)

- 「レート モード」 (P.2-3)
- 「速度モードとデュプレックス モード」 (P.2-4)
- 「フロー制御」 (P.2-5)
- 「ポート MTU サイズ」 (P.2-5)
- 「帯域幅」 (P.2-6)
- 「スループット遅延」 (P.2-6)
- 「管理ステータス」 (P.2-6)
- 「UDLD パラメータ」 (P.2-7)
- 「キャリア遅延」 (P.2-9)
- 「管理インターフェイス IP アドレス パラメータ」 (P.2-9)
- 「ポート チャネル パラメータ」 (P.2-9)

## 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 チャネル インターフェイスに説明パラメータを設定する方法については、「[ポート チャネルの説明の設定](#)」 (P.5-22) を参照してください。別のインターフェイスにこのパラメータを設定する方法については、「[説明の設定](#)」 (P.2-14) 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 パラメータの設定手順については、「[ビーコン モードの設定](#)」 (P.2-15) を参照してください。

## MDIX

Medium Dependent Interface-crossover (MDI-X; メディア依存インターフェイスクロスオーバー) 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。

MDIX パラメータの設定手順については、「[MDIX パラメータの設定](#)」 (P.2-16) を参照してください。

## デバウンス タイマー

デバウンス タイマーを設定するとリンク変更の通知が遅くなり、ネットワークの再設定によるトラフィック損失が減少します。デバウンス タイマーはイーサネット ポートごとに個別に設定します。遅延時間はミリ秒単位で指定できます。デフォルトでは、このパラメータは 100 ミリ秒に設定されています。

**注意**

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

デバウンス タイマー パラメータの設定手順については、「[デバウンス タイマーの設定](#)」(P.2-17) を参照してください。

## Error Disabled

ポートが管理上 (**no shutdown** コマンドを使用しない) イネーブルであるが、プロセスによって実行時にディセーブルになる場合、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、ポートは管理上イネーブルなので、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。

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。

## レート モード

32 ポートの 10 ギガビット イーサネット モジュールでは、4 ポート単位で 10 Gbps (ギガビット/秒) の帯域幅を処理します。レートモード パラメータを使用すれば、この帯域幅を 4 ポートのうちの最初のポート専用にすることも、4 ポート全体でこの帯域幅を共有させることもできます。

表 2-1 に、10 Gbps ごとの帯域幅を共有するポートのグループと、帯域幅全体を利用するために使用するグループの専用ポートを示します。

表 2-1 共有ポートと専用ポート

帯域幅を共有する ポート グループ	10 ギガビット イー サネットの帯域幅 を専用するポート
1、3、5、7	1
2、4、6、8	2
9、11、13、15	9
10、12、14、16	10
17、19、21、23	17
18、20、22、24	18
25、27、29、31	25
26、28、30、32	26

**(注)**

各ポート グループのポートはすべて同じ Virtual Device Context (VDC) に属している必要があります。VDC の詳細については、『*Cisco DCNM Virtual Device Context Configuration Guide, Release 5.x*』を参照してください。

## 速度モードとデュプレックス モード

速度モードとデュプレックス モードはそれぞれ、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と相関関係にあります。デフォルトでは、これらのインターフェイスの速度およびデュプレックス モードは他のインターフェイスとそれぞれ自動ネゴシエートしますが、設定を変更することもできます。設定を変更する場合は、両方のインターフェイスで同じ速度とデュプレックス モード設定を使用するか、または少なくとも 1 つのインターフェイスで自動ネゴシエーションを使用します。表 2-2 は、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の各タイプで動作する設定を示します。

表 2-2 イーサネットおよび管理インターフェイスで使用する速度およびデュプレックスモード設定

モジュールのタイプ	速度モード設定	デュプレックス モード設定	動作速度 (Mb/s)	動作デュプレッ クス モード
32 ポート 10 ギガビット イーサネット	自動 <sup>1</sup>	自動 <sup>1</sup>	10,000	全二重
48 ポート 10/100/1000 イーサネット	自動 <sup>1</sup>	自動 <sup>1</sup>	1000	全二重
			10 または 100	半二重
	1000	自動 <sup>1</sup> または 全二重	1000	全二重
			100	半二重
	10	自動 <sup>1</sup> または 半二重	100	全二重
			10	半二重
		全二重	10	全二重
			10	全二重
管理	自動 <sup>1</sup>	自動 <sup>1</sup>	1000	全二重
			10 または 100	半二重
	1000	自動 <sup>1</sup> または 全二重	1000	全二重
			100	半二重
	10	自動 <sup>1</sup> または 半二重	100	全二重
			10	半二重
		全二重	10	全二重
			10	全二重

1. デフォルト設定

ポート チャネル インターフェイスに速度モードおよびデュプレックス モードを設定する方法については、「[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](#)」(P.5-23) を参照してください。他のインターフェイスに速度モードおよびデュプレックス モードを設定する方法については、「[インターフェイス速度およびデュプレックス モードの設定](#)」(P.2-17) を参照してください。

## フロー制御

1 Gbps 以上で移動するイーサネット ポートの受信バッファが満杯になると、フロー制御により、そのポートから送信ポートに IEEE 802.3x ポーズ フレームが送信され、指定した時間だけデータの送信を停止するよう要求されます。送信ポートは任意の速度で動作しており、ポーズ フレームを受信してデータの転送を停止することができます。

2 つのポート間のフロー制御を有効にするには、それぞれのポートで対応する受信および送信フロー制御パラメータをイネーブルまたはディセーブルに設定します。パラメータをイネーブルに設定すると、もう一方のポートの設定とは関係なく送信または受信フロー制御機能がアクティブになります。指定したパラメータを設定すると、もう一方のポートの対応するフロー制御状態をイネーブルまたはディセーブルに設定すれば、送信または受信フロー制御機能がアクティブになります。いずれかのフロー制御状態をディセーブルに設定すると、その送信方向のフロー制御がディセーブルになります。異なるポートフロー制御状態がリンク フロー制御状態に与える影響については、表 2-3 を参照してください。

表 2-3 リンク フロー制御上でのポート フロー制御の影響

ポート フロー制御の状態		リンク フロー制御の状態
データ受信ポート (ポーズ フレームを送信)	データ送信ポート (ポーズ フレームを受信)	
イネーブル	イネーブル	イネーブル
イネーブル	指定	イネーブル
イネーブル	ディセーブル	ディセーブル
指定	イネーブル	イネーブル
指定	指定	イネーブル
指定	ディセーブル	ディセーブル
ディセーブル	イネーブル	ディセーブル
ディセーブル	指定	ディセーブル
ディセーブル	ディセーブル	ディセーブル

フロー制御パラメータの設定手順については、「[フロー制御の設定](#)」(P.2-18) を参照してください。

## ポート MTU サイズ

Maximum Transmission Unit (MTU; 最大伝送ユニット) 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。

デフォルトではそれぞれのポートの 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。これよりも大きい MTU サイズでは、より少ないオーバーヘッドでデータをより効率的に処理できます。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。これもデフォルトのシステム ジャンボ MTU サイズです。

レイヤ 3 インターフェイスでは、576 ~ 9216 バイトの MTU サイズを設定できます。I/O モジュールごとに最大 64 MTU まで設定できます。



(注) グローバル LAN ポート MTU サイズは、非デフォルト MTU サイズを設定したレイヤ 3 イーサネット LAN ポートを通過するトラフィックに適用します。

レイヤ 2 ポートには、システム デフォルト (1500 バイト) またはシステム ジャンボ MTU サイズ (当初は 9216 バイト) のいずれかの MTU サイズを設定できます。



(注) システム ジャンボ MTU サイズを変更すると、ポートの一部または全部に新しいシステム ジャンボ MTU サイズを指定しない限り、レイヤ 2 ポートは自動的にシステム デフォルト MTU サイズ (1500 バイト) を使用します。

MTU サイズの設定手順については、「[MTU サイズの設定](#)」(P.2-20) を参照してください。

## 帯域幅

イーサネット ポートには、物理レベルで 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、物理レベル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、Interior Gateway Routing Protocol (IGRP) 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、物理レベルの帯域幅は 1,000,000 Kb のまま変わりません。

他のインターフェイスに帯域幅パラメータ設定する方法については、「[帯域幅の設定](#)」(P.2-22) 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すが、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、EIGRP は、遅延設定を使用して、あるイーサネット リンクの別のイーサネット リンクに対する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。

スループット遅延パラメータの設定手順については、「[スループット遅延の設定](#)」(P.2-22) 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。管理的に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。管理的に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 チャネル インターフェイスに管理ステータス パラメータを設定する方法については、「[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](#)」(P.5-20) を参照してください。他のインターフェイスに管理ステータス パラメータを設定する方法については、「[インターフェイスのシャットダウンおよび再開](#)」(P.2-23) を参照してください。



## UDLD パラメータ

ここでは、次の内容について説明します。

- 「UDLD の概要」(P.2-7)
- 「UDLD のデフォルト設定」(P.2-8)
- 「UDLD アグレッシブ モードおよび非アグレッシブ モード」(P.2-8)

### UDLD の概要

シスコシステムズ独自の Unidirectional Link Detection (UDLD; 単方向リンク検出) 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。単方向リンクによって、スパニング ツリー トポロジ ループなどのさまざまな問題が発生する可能性があります。

UDLD は、レイヤ 1 プロトコルと連動し、リンクの物理的ステータスを判別するレイヤ 2 プロトコルです。レイヤ 1 では、物理シグナリングおよび障害検出が自動ネゴシエーションによって処理されます。UDLD は、ネイバーの ID の検出、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できない処理を実行します。自動ネゴシエーションと UDLD の両方をイネーブルにすると、レイヤ 1 とレイヤ 2 の検知機能が連動し、物理的および論理的な単方向接続、および他のプロトコルの誤作動を防止します。

リンク上でローカル デバイスが送信したトラフィックをネイバーが受信するにもかかわらず、ネイバーから送信されたトラフィックをローカル デバイスが受信しない場合は、必ず単方向リンクが発生しています。対になっているファイバ ケーブルのどちらかの接続が切断されても、自動ネゴシエーションがアクティブである限り、リンクはアップしません。この場合、論理リンクは不確定であり、UDLD は何の処理も行いません。両方のファイバがレイヤ 1 で正常に動作していれば、レイヤ 2 の UDLD はそれらのファイバが適切に接続されているかどうか、また、適切なネイバー間でトラフィックが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 で機能するため、このチェックは自動ネゴシエーションでは実行されません。

Cisco Nexus 7000 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。このフレームが一定の時間内にエコー バックされ、かつ特定の確認応答（エコー）がない場合は、そのリンクは単方向リンクとしてマークが付けられ、LAN ポートがシャットダウンされます。プロトコルが単方向リンクを正常に識別してディセーブルにするには、リンクの両端のデバイスが UDLD をサポートする必要があります。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。

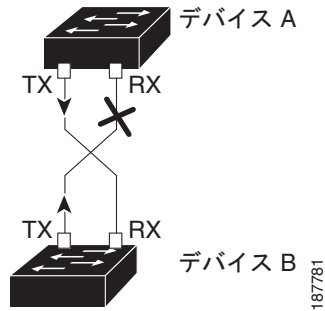


(注)

デフォルトでは、銅線の LAN ポート上の UDLD はローカルでディセーブルに設定されており、同じタイプのメディアに不要な制御トラフィックが送信されないようになっています。

図 2-1 に、単方向リンク条件の例を示します。デバイス B は、ポート上でデバイス A から正常にトラフィックを受信しますが、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されます。

図 2-1 単方向リンク



## UDLD のデフォルト設定

表 2-4 に、UDLD のデフォルト設定を示します。

表 2-4 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 ステート イネーブル (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
ツイスト ペア (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 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

デバイスとそのポートに UDLD を設定する手順については、「UDLD モードの設定」(P.2-25) を参照してください。

## UDLD アグレッシブ モードおよび非アグレッシブ モード

デフォルトでは、UDLD アグレッシブ モードはディセーブルになっています。UDLD アグレッシブ モードは、UDLD アグレッシブ モードをサポートするネットワーク デバイスの間のポイントツーポイントのリンク上に限って設定できます。UDLD アグレッシブ モードをイネーブルに設定した場合、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。

スパニング ツリー ループを防止するために、デフォルトの 15 秒間隔を使用する非アグレッシブ UDLD により、(デフォルトのスパニング ツリー パラメータを使用している場合) ブロッキング ポートがフォワーディング ステートに移行する前に、すみやかに単方向リンクをシャットダウンできます。

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

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

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



(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。

## キャリア遅延



(注)

キャリア遅延タイマーは、VLAN ネットワーク インターフェイスでだけ設定できます。このタイマーを他のインターフェイス モードで設定できません。VLAN ネットワーク インターフェイスの設定手順については、第 4 章「レイヤ 3 インターフェイスの設定」を参照してください。

リンクがダウン状態になり、キャリア遅延タイマーが期限切れになる前にアップ状態に戻った場合、ダウン状態は効果的にフィルタリングされ、デバイスの他のソフトウェアは、リンクダウン イベントが発生したことを認識しません。大きなキャリア遅延タイマーでは、検出されるリンクアップ/リンクダウン イベントが少なくなります。キャリア遅延時間を 0 に設定すると、デバイスは発生する各リンクアップ/リンクダウン イベントを検出します。

ほとんどの環境では、短い遅延時間は長い遅延時間より良好です。選択する正確な値は、リンク停止の性質およびこれらのリンクがネットワークで持続すると予想される時間によって異なります。データ リンクが短い停止の影響を受ける場合（特に、これらの停止時間が IP ルーティングの収束にかかる時間より短い場合）、長いキャリア遅延の値を設定し、これらの短い停止によってルーティング テーブルで不要な問題が発生するのを防ぐ必要があります。ただし、停止がさらに長くなる傾向がある場合、停止を早く検出し、IP ルート収束が早く始まり早く終わるように、さらに短いキャリア遅延時間を設定できます。

デフォルトのキャリア遅延時間は 2 秒または 50 ミリ秒です。

## 管理インターフェイス IP アドレス パラメータ

Cisco NX-OS デバイスの管理 (mgmt0) インターフェイスでは、複数の Telnet または SNMP のセッションを同時に実行でき、IPv4 アドレスまたは IPv6 アドレスによってデバイスを管理できます。

IPv4 および IPv6 のアドレッシングの詳細については、『Cisco DCNM Unicast Routing Configuration Guide, Release 5.x』を参照してください。

## 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 8 つ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。また、ポート チャネルでは、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。

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 チャネルの設定手順については、[第 5 章「ポート チャネルの設定」](#)を参照してください。

## ライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
DCNM	基本インターフェイス パラメータには LAN Enterprise ライセンスが必要です。
Cisco NX-OS	基本インターフェイス パラメータにライセンスは必要ありません。ライセンス パッケージに含まれていない機能はすべて Cisco NX-OS システム イメージにバンドルされており、追加費用は一切発生しません。Cisco NX-OS のライセンス スキームの詳細については、『 <i>Cisco Nexus 7000 Series NX-OS Licensing Guide, Release 5.x</i> 』を参照してください。



(注) VDC を使用する場合は Advanced Services ライセンスが必要です。

## 注意事項および制約事項

次の注意事項と制約事項に従って基本インターフェイス パラメータを設定します。

- 光ファイバイーサネット 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。
- ローカル ポートにフロー制御を設定する場合は、次の点に注意します。
  - リモート ポート送信パラメータの設定手順が不明の場合にポーズ フレームを受信するには、ローカル ポート受信パラメータを指定済みに設定します。
  - リモート ポート送信パラメータがイネーブルまたは指定済みである場合にポーズ フレームを受信するには、ローカル ポート受信パラメータをイネーブルに設定します。
  - 受信したポーズ フレームを無視するには、ローカル ポート受信パラメータをディセーブルに設定します。
  - リモート ポート受信パラメータの設定手順が不明の場合にポーズ フレームを送信するには、ローカル ポート送信パラメータを指定済みに設定します。
  - リモート ポート受信パラメータがイネーブルまたは指定済みである場合にポーズ フレームを送信するには、ローカル ポート送信パラメータをイネーブルに設定します。
  - ポーズ フレームを送信しないようにするには、ローカル ポート送信パラメータをディセーブルに設定します。

- 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、表 2-2 (P.2-4) 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 モードを自動に設定します。
  - － イーサネット ポート速度を自動以外の値 (10 Mb/s、100 Mb/s、1000 Mb/s 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トするように設定しないでください。



(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。

## 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。

ここでは、インターフェイスを指定してそれぞれの基本パラメータを設定する方法について説明します。

- 「設定するインターフェイスの指定」 (P.2-12)
- 「説明の設定」 (P.2-14)
- 「ビーコン モードの設定」 (P.2-15)
- 「帯域幅レート モードの変更」 (P.2-15)
- 「Error-Disabled ステートの設定」 (P.2-16)
- 「MDIX パラメータの設定」 (P.2-16)
- 「デバウンス タイマーの設定」 (P.2-17)
- 「インターフェイス速度およびデュプレックス モードの設定」 (P.2-17)
- 「フロー制御の設定」 (P.2-18)
- 「MTU サイズの設定」 (P.2-20)
- 「帯域幅の設定」 (P.2-22)
- 「スループット遅延の設定」 (P.2-22)
- 「インターフェイスのシャットダウンおよび再開」 (P.2-23)
- 「CDP のイネーブル化またはディセーブル化」 (P.2-24)
- 「UDLD モードの設定」 (P.2-25)
- 「キャリア遅延タイマーの設定」 (P.2-26)
- 「管理インターフェイスの IP アドレスの設定」 (P.2-26)

## 設定するインターフェイスの指定

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。

表 2-5 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 2-5 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)

SFP インターフェイスのステータスおよび診断情報を表示するには、「フィールドの説明」(P.2-28) を参照してください。

### 手順の詳細

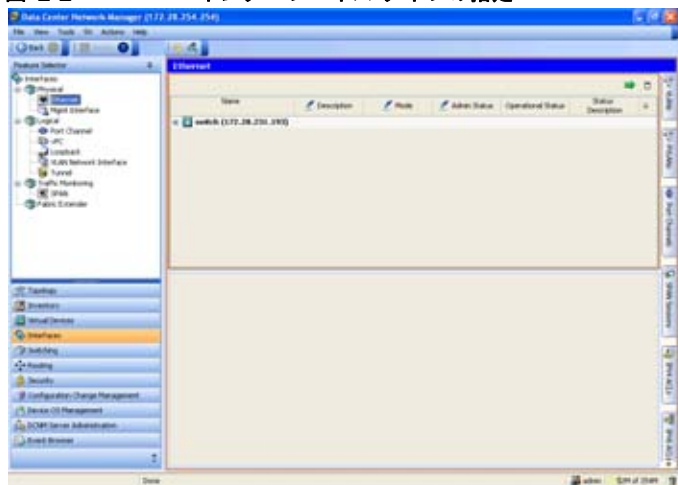
設定するインターフェイスを指定するには、次の手順を実行します。

- ステップ 1** [Feature Selector] ペインで、次の手順を実行して、設定するインターフェイスのタイプを指定します。
- a. [Interfaces] を選択します。
  - b. [Physical] または [Logical] を選択します。
    - イーサネット インターフェイスまたは管理インターフェイスを操作するには、[Physical] を選択します。
    - ポート チャネル インターフェイス、ループバック インターフェイス、VLAN ネットワーク インターフェイス、またはトンネル インターフェイスを操作するには、[Logical] を選択します。
  - c. 物理インターフェイスを操作する場合、次のインターフェイス タイプのいずれかを選択します。
    - イーサネット インターフェイス パラメータを設定するには、[Ethernet] を選択します。
    - 管理インターフェイス パラメータを設定するには、[Mgmt Interface] を選択します。
  - d. 論理インターフェイスを操作する場合、次のインターフェイス タイプのいずれかを選択します。
    - ポート チャネル
    - ループバック
    - VLAN ネットワーク インターフェイス
    - トンネル

指定されたインターフェイス タイプのデバイスが [Summary] ペインに表示されます。

図 2-2 に、インターフェイス タイプを指定する Feature Selector 項目を表示します。

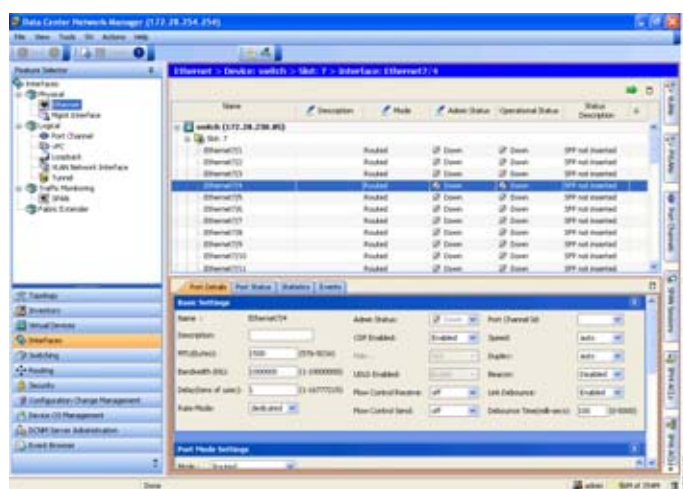
図 2-2 インターフェイス タイプの指定



**ステップ 2** [Summary] ペインで、次の方法のいずれかでデバイスと（オプションで）ポートを指定します。

- イーサネット インターフェイス タイプを指定した場合、図 2-3 に示すようにデバイスを展開し、適切な I/O モジュールのスロットを展開し、適切なポートをクリックします。

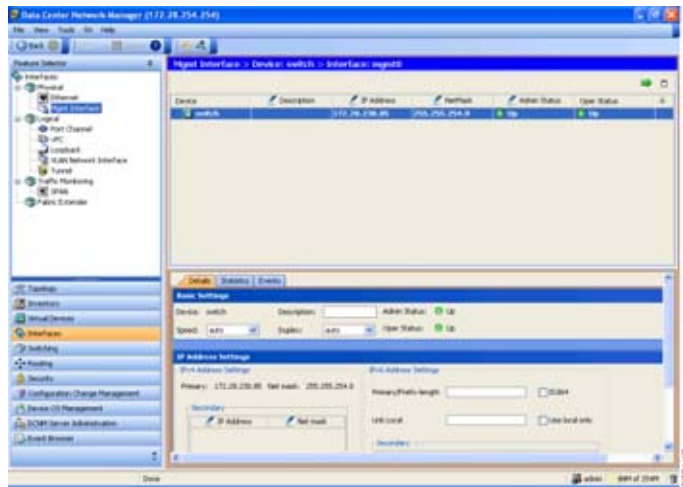
図 2-3 イーサネット インターフェイスのポートの指定



- 管理インターフェイス タイプを指定した場合、図 2-4 に示すように、デバイスをクリックします。



図 2-4 管理インターフェイスのデバイスの指定



指定したインターフェイスの詳細情報を表示するタブおよびセクションが [Details] ペインに表示されます。

## 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。使用できるのは英数字 80 字以内で、大文字と小文字は区別されます。

### 手順の詳細

説明を設定する手順は、次のとおりです。

- ステップ 1** [Feature Selector] ペインで、[Interfaces] > [Physical] を選択します。
- ステップ 2** [Ethernet] または [Mgmt Interface] を選択します。  
指定されたインターフェイス タイプのデバイスが [Summary] ペインに表示されます。
- ステップ 3** [Summary] ペインで、次のいずれかを実行して、インターフェイスを指定します。
  - イーサネット インターフェイスを設定するには、デバイスを展開し、スロットを展開して、ポートをクリックします。  
[Details] ペインにポート情報のタブが表示されます。[Port Details] タブはアクティブですが、セクションは展開されていません。
  - 管理インターフェイスを設定するには、設定するデバイスをクリックします。  
[Details] ペインにデバイス情報のタブが表示されます。[Details] タブはアクティブですが、セクションは展開されていません。
- ステップ 4** [Details] ペインの [Basic Settings] セクションを展開します。  
[Basic Settings] セクションに基本パラメータが表示されます。
- ステップ 5** [Description] フィールドで、インターフェイスの適切な説明を文字で入力します。



**ステップ 6** (任意) メニュー バーで [File] > [Deploy] を選択して変更をデバイスに適用します。

## 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。

### 手順の詳細

ビーコン モードをイネーブルまたはディセーブルにするには、次の手順を実行します。

- 
- ステップ 1** [Feature Selector] ペインで、[Interfaces] > [Physical] > [Ethernet] を選択します。  
イーサネット インターフェイスのあるデバイスが [Summary] ペインに表示されます。
- ステップ 2** [Summary] ペインで、デバイスを展開し、スロットを展開して、ポートをクリックします。  
[Details] ペインにポート情報のタブが表示されます。[Port Details] タブはアクティブですが、セクションは展開されていません。
- ステップ 3** [Details] ペインの [Basic Settings] セクションを展開します。  
[Basic Settings] セクションに基本パラメータが表示されます。
- ステップ 4** [Beacon] ドロップダウン リストで [Enabled] または [Disabled] を選択します。
- ステップ 5** (任意) メニュー バーで [File] > [Deploy] を選択して変更をデバイスに適用します。
- 

## 帯域幅レート モードの変更

32 ポートの 10 ギガビット イーサネット モジュールでは、4 ポート単位で 10 Gbps (ギガビット/秒) の帯域幅を処理します。レートモード パラメータを使用すれば、この帯域幅を 4 ポートのうちの最初のポート専用にすることも、4 ポート全体でこの帯域幅を共有させることもできます。

### 手順の詳細

専用または共有レート モードをイネーブルにするには、次の手順を実行します。

- 
- ステップ 1** [Feature Selector] ペインで、[Interfaces] > [Physical] > [Ethernet] を選択します。  
イーサネット インターフェイスのあるデバイスが [Summary] ペインに表示されます。
- ステップ 2** [Summary] ペインで、デバイスを展開し、スロットを展開して、ポートをクリックします。  
[Details] ペインにポート情報のタブが表示されます。[Port Details] タブはアクティブですが、セクションは展開されていません。
- ステップ 3** [Details] ペインの [Basic Settings] セクションを展開します。  
[Basic Settings] セクションに基本パラメータが表示されます。
- ステップ 4** 専用レート モードを使用できるポートを選択した場合、[Rate Mode] ドロップダウン リストから [dedicated] または [shared] を選択します。

**ステップ 5** (任意) メニュー バーで [File] > [Deploy] を選択して変更をデバイスに適用します。

## 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。

### 手順の詳細

error-disabled 状態のインターフェイスの検出および自動回復を設定するには、次の手順を実行します。

- 
- ステップ 1** [Feature Selector] ペインで、[Interfaces] > [Physical] > [Ethernet] を選択します。  
イーサネット インターフェイスのあるデバイスが [Summary] ペインに表示されます。
- ステップ 2** [Summary] ペインで、デバイスをクリックします。  
[Details] ペインにデバイス情報のタブが表示されます。
- ステップ 3** [Error Disable Settings] セクションをクリックします。  
セクションが展開され、[Detection] フィールドと [Recovery] フィールドが表示されます。
- ステップ 4** [Detection] セクションで、error-disable 状態のすべてのインターフェイスを検出する理由をクリックします。
- ステップ 5** [Recovery] セクションの [Recovery Interval] フィールドで、自動検出の間隔を秒単位で入力します。  
指定できる範囲は 30 ～ 65535 秒です。
- ステップ 6** [Recovery] セクションで、自動的に回復させるインターフェイスの error-disabled 状態の原因をクリックします。
- ステップ 7** (任意) メニュー バーで [File] > [Deploy] を選択して変更をデバイスに適用します。
- 

## 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 ポート専用にする必要がある場合は、ローカル ポートの Medium Dependent Independent Crossover (MDIX) パラメータをイネーブルにします。デフォルトでは、このパラメータはイネーブルです。

### 作業を開始する前に

リモート ポートの MDIX をイネーブルにする必要があります。

### 手順の詳細

MDIX 接続をイネーブルまたはディセーブルにするには、次の手順を実行します。

- 
- ステップ 1** [Feature Selector] ペインで、[Interfaces] > [Physical] > [Ethernet] を選択します。  
イーサネット インターフェイスのあるデバイスが [Summary] ペインに表示されます。
- ステップ 2** [Summary] ペインで、デバイスを展開し、スロットを展開して、ポートをクリックします。

[Details] ペインにポート情報のタブが表示されます。[Port Details] タブはアクティブですが、セクションは展開されていません。

**ステップ 3** [Details] ペインの [Basic Settings] セクションを展開します。

[Basic Settings] セクションに基本パラメータが表示されます。

**ステップ 4** [Mdix] ドロップダウン リストで [enabled] または [disabled] を選択します。

**ステップ 5** (任意) メニュー バーで [File] > [Deploy] を選択して変更をデバイスに適用します。

## デバウンス タイマーの設定

[Link Debounce] フィールドと [Debounce Time] フィールドを使用して、デバウンス タイマーをイネーブルまたはディセーブルにできます。[Link Debounce] フィールドで、タイマーをイネーブルまたはディセーブルにします。[Debounce Time] フィールドで、時間をミリ秒 (ms) 単位で指定します。



(注)

時間を 0 ms に指定した場合、[Link Debounce] フィールドでタイマーをイネーブルにした場合でも、タイマーがディセーブルになります。

### 手順の詳細

デバウンス タイマーをイネーブルまたはディセーブルにするには、次の手順を実行します。

**ステップ 1** [Feature Selector] ペインで、[Interfaces] > [Physical] > [Ethernet] を選択します。

イーサネット インターフェイスのあるデバイスが [Summary] ペインに表示されます。

**ステップ 2** [Summary] ペインで、デバイスを展開し、スロットを展開して、ポートをクリックします。

[Details] ペインにポート情報のタブが表示されます。[Port Details] タブはアクティブですが、セクションは展開されていません。

**ステップ 3** [Details] ペインの [Basic Settings] セクションを展開します。

[Basic Settings] セクションに基本パラメータが表示されます。

**ステップ 4** [Link Debounce] ドロップダウン リストで [Enabled] または [Disabled] を選択します。

**ステップ 5** [Debounce Time] フィールドで、デバウンス時間をミリ秒単位で入力します (0 ~ 5000)。

時間を 0 ミリ秒にすると、デバウンス タイマーはディセーブルになります。1 ~ 5000 ミリ秒の時間が使用されるのは、タイマーをイネーブルにした場合だけです。

**ステップ 6** メニュー バーの [File] > [Deploy] を選択して、変更をデバイスに適用します。

## インターフェイス速度およびデュプレックス モードの設定

インターフェイス速度とデュプレックス モードは相関関係にあります。このため、両方のパラメータを同時に設定する必要があります。

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同時に設定できる速度およびデュプレックス モードについては、[表 2-2 \(P.2-4\)](#) を参照してください。



(注)

指定するインターフェイス速度はインターフェイスで使用するデュプレックス モードに影響を与えます。このため、デュプレックス モードを設定する前に速度を設定する必要があります。自動ネゴシエーションの速度を設定する場合、デュプレックス モードは自動的に自動ネゴシエーションに設定されます。速度を 10 または 100 Mb/s に指定すると、ポートでは半二重モードを使用するように自動的に設定されますが、全二重モードを指定することもできます。1000 Mb/s (1 Gb/s) 以上の速度に設定すると、自動的に全二重モードが使用されます。

### 作業を開始する前に

リモート ポートの速度設定はローカル ポートへの変更をサポートします。ローカル ポートを固有の速度で使用するには、リモート ポートにも同じ速度を設定するか、ローカル ポートがその速度を自動ネゴシエートするように設定する必要があります。

### 手順の詳細

インターフェイス速度とデュプレックス モードを設定するには、次の手順を実行します。

- ステップ 1** [Feature Selector] ペインで、[Interfaces] > [Physical] を選択します。
- ステップ 2** [Ethernet] または [Mgmt Interface] を選択します。  
指定されたインターフェイス タイプのデバイスが [Summary] ペインに表示されます。
- ステップ 3** [Summary] ペインで、次のいずれかを実行して、インターフェイスを指定します。
  - イーサネット インターフェイスを設定するには、デバイスを展開し、スロットを展開して、ポートをクリックします。  
[Details] ペインにポート情報のタブが表示されます。[Port Details] タブはアクティブですが、セクションは展開されていません。
  - 管理インターフェイスを設定するには、設定するデバイスをクリックします。  
[Details] ペインにデバイス情報のタブが表示されます。[Details] タブはアクティブですが、セクションは展開されていません。
- ステップ 4** [Details] ペインの [Basic Settings] セクションを展開します。  
[Basic Settings] セクションに基本パラメータが表示されます。
- ステップ 5** [Speed] フィールドで、ポートに適切な速度を選択します。
- ステップ 6** [Duplex] フィールドで、[full]、[half] または [auto] を選択します。  
これらのオプションのいずれかが使用できない場合、インターフェイス速度を変更します（前の手順を参照）。
- ステップ 7** (任意) メニュー バーで [File] > [Deploy] を選択して変更をデバイスに適用します。

## フロー制御の設定

1 Gb/s 以上で動作するイーサネット ポートの場合、フロー制御ポーズ フレームを送受信するポートをイネーブルまたはディセーブルにできます。1 Gb/s 未満で動作するイーサネット ポートの場合、ポーズ フレームを受信するポートの機能だけをイネーブルまたはディセーブルにできます。

ローカル ポートのフロー制御をイネーブルにすると、リモート ポートでのフロー制御設定にかかわらずローカル ポートでのフレームの送受信を完全にイネーブルにするか、リモート ポートで指定して使用する設定をローカルポートで使用するよう設定します。ローカルおよびリモート ポートのフロー制御をどちらもイネーブルにする、一方のポートのフロー制御を指定して設定する、あるいはこの2つの状態を組み合わせて設定する場合、それらのポートではフロー制御がイネーブルです。



(注)

10 Gb/s で動作するポートの場合、状態を指定してパラメータを送受信できません。

## 作業を開始する前に

必要なフロー制御に対応する設定がリモート ポートにあることを確認します。ローカル ポートからフロー制御ポーズ フレームを送信するには、リモート ポートの受信パラメータがオンまたは指定になっていることを確認します。ローカル ポートでフロー制御ポーズ フレームを受信するには、リモート ポートの送信パラメータがオンまたは指定になっていることを確認します。フロー制御を使用しない場合は、リモート ポートの送信パラメータおよび受信パラメータをオフにします。

## 手順の詳細

インターフェイス フロー制御を設定するには、次の手順を実行します。

- 
- |               |  |
|---------------|--|
| <b>ステップ 1</b> | [Feature Selector] で、[Interfaces] > [Physical] > [Ethernet] を選択します。<br>[Summary] ペインに、イーサネット インターフェイスのあるデバイスの一覧が表示されます。  |
| <b>ステップ 2</b> | [Summary] ペインで、スイッチを展開し、スロットを展開して、ポートを選択します。<br>[Details] ペインに、ポートのタブと展開されていない [Basic Settings] セクションが表示されます。  |
| <b>ステップ 3</b> | [Details] ペインで、[Port Details] をクリックし、[Basic Settings] をクリックします。<br>[Basic Settings] セクションが展開され、複数の機能に使用される基本パラメータが表示されます。  |
| <b>ステップ 4</b> | [Flow Control Receive] ドロップダウン リストで、次のようにフロー制御フレームを受信する方法を選択します。 <ul style="list-style-type: none"><li>• ポーズ フレームの受信をディセーブルにするには、[off] を選択します。</li><li>• 受信フロー制御設定のために送信フロー制御設定を使用するには、[desired] を選択します。</li><li>• その他のポートの送信設定に関係なくポーズ フレームの受信をイネーブルにするには、[on] を選択します。</li></ul>  |
| <b>ステップ 5</b> | [Flow Control Send] ドロップダウン リストで、[desired]、[on] または [off] を選択します。 <ul style="list-style-type: none"><li>• ポーズ フレームの送信をディセーブルにするには、[off] を選択します。</li><li>• 送信フロー制御設定のために受信フロー制御設定を使用するには、[desired] を選択します。</li><li>• その他のポートの受信設定に関係なくポーズ フレームの送信をイネーブルにするには、[on] を選択します。</li></ul> |
| <b>ステップ 6</b> | (任意) メニュー バーで [File] > [Deploy] を選択して変更をデバイスに適用します。  |
-

## MTU サイズの設定

レイヤ 2 およびレイヤ 3 イーサネット インターフェイスの最大伝送ユニット (MTU) サイズを設定できます。レイヤ 3 インターフェイスでは、576 ～ 9216 バイトの MTU を設定できます (偶数値にする必要があります)。レイヤ 2 インターフェイスでは、システム デフォルト MTU (1500 バイト) またはシステム ジャンボ MTU サイズ (デフォルト サイズは 9216 バイト) の MTU を設定できます。



(注)

システム ジャンボ MTU サイズは変更できますが、この値を変更した場合は、値を使用するレイヤ 2 インターフェイスもアップデートして、新しいシステム ジャンボ MTU 値を使用する必要があります。レイヤ 2 インターフェイスの MTU 値をアップデートしない場合、これらのインターフェイスはシステム デフォルト MTU (1500 バイト) を使用します。

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。

[Details] ペインの [Port Details] および [Port Mode Settings] をクリックし、レイヤ 2 モード ([Access]、[Trunk]、[PVLAN Host]、または [PVLAN Promiscuous]) を選択して、ポート モードを変更します。

ポート モードをレイヤ 2 に変更した後、ポート モードを再び変更し、[Port Details] および [Port Mode Settings] をクリックし、レイヤ 3 モード ([Routed]) を選択すると、レイヤ 3 インターフェイスの設定に戻ることができます。

ここでは、次の内容について説明します。

- 「[インターフェイス MTU サイズの設定](#)」 (P.2-20)
- 「[システム ジャンボ MTU サイズの設定](#)」 (P.2-21)

## インターフェイス MTU サイズの設定

レイヤ 3 インターフェイスでは、576 ～ 9216 バイトの MTU サイズを設定できます。

レイヤ 2 インターフェイスでは、すべてのレイヤ 2 インターフェイスをデフォルト MTU サイズ (1500 バイト) またはシステム ジャンボ MTU サイズ (デフォルト サイズは 9216 バイト) を使用するように設定できます。

レイヤ 2 インターフェイスとは異なるシステム ジャンボ MTU サイズを使用する場合は、「[システム ジャンボ MTU サイズの設定](#)」 (P.2-21) を参照してください。

### 手順の詳細

インターフェイスの MTU サイズを変更するには、次の手順を実行します。

- ステップ 1** [Feature Selector] ペインで、[Interfaces] > [Physical] > [Ethernet] を選択します。  
イーサネット インターフェイスのあるデバイスが [Summary] ペインに表示されます。
- ステップ 2** [Summary] ペインで、デバイスを展開し、スロットを展開して、ポートをクリックします。  
[Details] ペインにポート情報のタブが表示されます。[Port Details] タブはアクティブですが、セクションは展開されていません。
- ステップ 3** レイヤ 2 インターフェイスを設定する場合、[Summary] ペインで [Mode settings] をダブルクリックし、[Mode] ドロップダウンリストから [Access]、[Trunk]、[PVLAN Host] または [PVLAN Promiscuous] を選択します。



(注) レイヤ 3 インターフェイスでの作業にスイッチ バックする必要がある場合、[Mode] ドロップダウン リストから [Routed] を選択します。

**ステップ 4** [Details] ペインの [Basic Settings] セクションを展開します。

[Basic Settings] セクションに基本パラメータが表示されます。

**ステップ 5** [MTU] フィールドで、次のように目的の MTU サイズを入力します。

- レイヤ 2 インターフェイスの場合、デフォルトの MTU サイズ (1500) またはシステム ジャンボ MTU サイズを入力します (デフォルト サイズは 9216)。システム ジャンボ MTU サイズを変更した場合、システム ジャンボ MTU サイズに新しいサイズを使用できます。
- レイヤ 3 インターフェイスの場合、576 ~ 9216 の MTU サイズを入力します。

**ステップ 6** (任意) メニュー バーで [File] > [Deploy] を選択して変更をデバイスに適用します。

## システム ジャンボ MTU サイズの設定

システム ジャンボ MTU サイズを設定するとレイヤ 2 インターフェイスの MTU サイズを指定できます。1500 ~ 9216 の偶数を指定できます。システム ジャンボ MTU サイズを設定しない場合、デフォルトは 1500 バイトです。

### 手順の詳細

システム ジャンボ MTU サイズを設定するには、次の手順を実行します。

**ステップ 1** [Feature Selector] で、[Interfaces] > [Physical] > [Ethernet] を選択します。

指定したタイプのデバイスが [Summary] ペインに表示されます。

**ステップ 2** [Summary] ペインで、デバイスをクリックします。

[Details] ペインにデバイス情報のタブが表示されます。[Details] タブはアクティブですが、セクションは展開されていません。

**ステップ 3** [Details] ペインの [MTU Settings] セクションを展開します。

**ステップ 4** [MTU Settings] セクションにシステム ジャンボ MTU 情報が表示されます。

**ステップ 5** [Jumbo MTU] フィールドで、1500 ~ 9216 の範囲の偶数でサイズを入力します。

**ステップ 6** (任意) メニュー バーで [File] > [Deploy] を選択して変更をデバイスに適用します。

## 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。物理レベルでは 1 GB の変更不可能な帯域幅を使用しますが、レベル 3 プロトコルには 1 ～ 10,000,000 Kb の値を設定できます。

### 手順の詳細

インターフェイス帯域幅を変更するには、次の手順を実行します。

- 
- |               |   |
|---------------|---|
| <b>ステップ 1</b> | [Feature Selector] ペインで、[Interfaces] > [Physical] > [Ethernet] を選択します。<br>イーサネット インターフェイスのあるデバイスが [Summary] ペインに表示されます。     |
| <b>ステップ 2</b> | [Summary] ペインで、デバイスを展開し、スロットを展開して、ポートをクリックします。<br>[Details] ペインにポート情報のタブが表示されます。[Port Details] タブはアクティブですが、セクションは展開されていません。 |
| <b>ステップ 3</b> | [Details] ペインの [Basic Settings] セクションを展開します。<br>[Basic Settings] セクションに基本パラメータが表示されます。                                      |
| <b>ステップ 4</b> | [Bandwidth] フィールドに、帯域幅をキロビット単位で入力します（1 ～ 10,000,000（カンマは省略する））。   |
| <b>ステップ 5</b> | （任意）メニュー バーで [File] > [Deploy] を選択して変更をデバイスに適用します。  |
- 

## 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。

### 手順の詳細

インターフェイス スループット遅延の情報用の値を変更するには、次の手順を実行します。

- 
- |               |   |
|---------------|---|
| <b>ステップ 1</b> | [Feature Selector] ペインで、[Interfaces] > [Physical] > [Ethernet] を選択します。<br>イーサネット インターフェイスのあるデバイスが [Summary] ペインに表示されます。     |
| <b>ステップ 2</b> | [Summary] ペインで、デバイスを展開し、スロットを展開して、ポートをクリックします。<br>[Details] ペインにポート情報のタブが表示されます。[Port Details] タブはアクティブですが、セクションは展開されていません。 |
| <b>ステップ 3</b> | [Details] ペインの [Basic Settings] セクションを展開します。<br>[Basic Settings] セクションに基本パラメータが表示されます。                                      |
| <b>ステップ 4</b> | [Delay] フィールドに、遅延時間に使用する数値を 10 マイクロ秒単位で入力します。<br>たとえば、遅延が 10,000 マイクロ秒の場合、1000 と入力します。                                      |
| <b>ステップ 5</b> | （任意）メニュー バーで [File] > [Deploy] を選択して変更をデバイスに適用します。  |
-



## 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 プロトコルによってその他のネットワーク 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。

### 手順の詳細

インターフェイスの管理ステータスを変更するには、次の手順を実行します。

- 
- |               |   |
|---------------|---|
| <b>ステップ 1</b> | [Feature Selector] ペインで、[Interfaces] > [Physical] を選択します。   |
| <b>ステップ 2</b> | [Ethernet] または [Mgmt Interface] を選択します。<br>指定されたインターフェイス タイプのデバイスが [Summary] ペインに表示されます。  |
| <b>ステップ 3</b> | [Summary] ペインで、次のいずれかを実行して、インターフェイスを指定します。 <ul style="list-style-type: none"><li>• イーサネット インターフェイスを設定するには、デバイスを展開し、スロットを展開して、ポートをクリックします。<br/>[Details] ペインにポート情報のタブが表示されます。[Port Details] タブはアクティブですが、セクションは展開されていません。</li><li>• 管理インターフェイスを設定するには、設定するデバイスをクリックします。<br/>[Details] ペインにデバイス情報のタブが表示されます。[Details] タブはアクティブですが、セクションは展開されていません。</li></ul> |
| <b>ステップ 4</b> | [Details] ペインの [Basic Settings] セクションを展開します。<br>[Basic Settings] セクションに基本パラメータが表示されます。  |
| <b>ステップ 5</b> | [Admin Status] ドロップダウン リストで [Down] を選択します。  |
| <b>ステップ 6</b> | [Admin Status] ドロップダウン リストで [Up] を選択します。  |
| <b>ステップ 7</b> | (任意) メニュー バーで [File] > [Deploy] を選択して変更をデバイスに適用します。   |
-

## CDP のイネーブル化またはディセーブル化



(注)

Command-Line Interface (CLI; コマンドライン インターフェイス) を使用する Cisco Discovery Protocol (CDP) の設定の詳細については、『*Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 5.x*』を参照してください。

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で CDP をイネーブルまたはディセーブルにできます。このプロトコルは、同じリンクの両方のインターフェイスでイネーブルにした場合だけ動作します。

### 作業を開始する前に

リモート ポートでもこのプロトコルがイネーブルになっていることを確認します。

### 手順の詳細

インターフェイスの CDP をイネーブルまたはディセーブルにするには、次の手順を実行します。

- ステップ 1** [Interfaces] > [Physical] を選択します。
  - ステップ 2** [Ethernet] または [Mgmt Interface] を選択します。  
指定されたインターフェイス タイプのデバイスが [Summary] ペインに表示されます。
  - ステップ 3** [Summary] ペインで、次のいずれかを実行して、インターフェイスを指定します。
    - イーサネット インターフェイスを設定するには、デバイスを展開し、スロットを展開して、ポートをクリックします。  
[Details] ペインにポート情報のタブが表示されます。[Port Details] タブはアクティブですが、セクションは展開されていません。
    - 管理インターフェイスを設定するには、デバイスを展開し、設定するポートをクリックします。  
[Details] ペインにデバイス情報のタブが表示されます。[Details] タブはアクティブですが、セクションは展開されていません。
  - ステップ 4** [Details] ペインの [Basic Settings] セクションを展開します。  
[Basic Settings] セクションに基本パラメータが表示されます。
  - ステップ 5** [CDP Enabled] ドロップダウン リストで [Enabled] または [Disabled] を選択します。
- (注) CDP を機能させる場合、同じリンクの両方のインターフェイスを [Enabled] に設定する必要があります。インターフェイスのいずれかまたは両方の [CDP Enabled] パラメータが [Disabled] に設定されている場合、CDP が機能できません。
- ステップ 6** (任意) メニュー バーで [File] > [Deploy] を選択して変更をデバイスに適用します。

## UDLD モードの設定

UDLD を実行するように設定されたデバイスのイーサネット インターフェイスに、ノーマルまたはアグレッシブ単方向リンク検出 (UDLD) モードを設定できます。インターフェイスの UDLD モードをイネーブルにする前に、インターフェイスを含むデバイスの UDLD がイネーブルになっていることを確認する必要があります。UDLD は他方のリンク先のインターフェイスおよびそのデバイスでもイネーブルになっている必要があります。

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

デフォルトでは、48 ポート 10/100/1000 イーサネット モジュール ポートでは UDLD がディセーブルですが、32 ポート 10 ギガビット イーサネット モジュール ポートではノーマル UDLD モードがイネーブルです。

### 作業を開始する前に

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。

### 手順の詳細

ビーコン モードをイネーブルまたはディセーブルにするには、次の手順を実行します。

- 
- ステップ 1 [Feature Selector] ペインで、[Interfaces] > [Physical] > [Ethernet] を選択します。
  - ステップ 2 イーサネット インターフェイスのあるデバイスが [Summary] ペインに表示されます。
  - ステップ 3 [Summary] ペインで、UDLD を使用するインターフェイスがあるデバイスをクリックします。
  - ステップ 4 [Actions] > [Enable UDLD] を選択します。
  - ステップ 5 [Summary] ペインで、スイッチを展開し、スロットを展開して、ポートをクリックします。  
ポートのタブと展開されていないセクションが [Details] ペインに表示されます。
  - ステップ 6 [Details] ペインの [Basic Settings] セクションを展開します。  
[Basic Settings] セクションに基本パラメータが表示されます。
  - ステップ 7 [UDLD Enabled] ドロップダウン リストで [Enabled]、[Disabled]、[Aggressive]、または [Global] を選択します。



- 
- (注) UDLD メッセージの間隔を設定するには、コマンドライン インターフェイスを使用します。  
このパラメータの設定については、『Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 5.x』を参照してください。
- 

- ステップ 8 (任意) メニュー バーで [File] > [Deploy] を選択して変更をデバイスに適用します。
-

## キャリア遅延タイマーの設定

キャリア遅延タイマーは、すべてのリンクダウン/リンクアップ イベントがデバイスの他のソフトウェアによって検出されない時間を設定します。長いキャリア遅延時間を設定すると、記録されるリンクダウン/リンクアップ イベントは少なくなります。キャリア遅延時間を 0 に設定すると、デバイスは各リンクダウン/リンクアップ イベントを検出します。



(注)

キャリア遅延タイマーは、VLAN ネットワーク インターフェイスでだけ設定できます。このタイマーを他のインターフェイス モードで設定できません。

[VLAN Network Interface] ペインを使用して、キャリア遅延タイマーを設定します。

### 手順の詳細

キャリア遅延タイマーを設定するには、次の手順を実行します。

- ステップ 1** [Feature Selector] ペインで、[Interfaces] > [Logical] > [VLAN Network Interface] を選択します。
- ステップ 2** [Contents] ペインの [Summary] ペインで、目的のデバイスをダブルクリックします。
- ステップ 3** キャリア遅延タイマーを設定する VLAN ネットワーク インターフェイスをクリックします。  
選択した VLAN ネットワーク インターフェイスが強調表示され、[Details] ペインにタブが表示されます。
- ステップ 4** [Details] ペインの [Details] タブをクリックします。
- ステップ 5** [Basic Settings] セクションをクリックします。
- ステップ 6** [Carrier Delay] フィールドで、このタイマーの値を入力します。
- ステップ 7** [Carrier Delay] フィールドで、プルダウン メニューをクリックし、[secs] または [msecs] を選択します。  
デフォルト値は 2 秒です。
- ステップ 8** (任意) メニュー バーで [File] > [Deploy] を選択して変更をデバイスに適用します。

## 管理インターフェイスの IP アドレスの設定

IPv4 アドレスまたは IPv6 アドレスを使用して、管理 (mgmt0) イーサネット インターフェイスを設定して IP 上で接続できます。

### 作業を開始する前に

管理インターフェイスに IPv4 アドレスを使用する場合は、次の情報が必要です。

- スイッチの管理インターフェイスの IPv4 サブネット マスク
- デフォルト ゲートウェイの IPv4 アドレス (任意)

コンソール ケーブルがコンソール ポートに接続されていることを確認します。

## 手順の詳細

- ステップ 1** [Feature Selector] ペインで、[Interfaces] > [Physical] > [Mgmt Interface] を選択します。
- ステップ 2** [Contents] ペインの [Summary] ペインで、目的のデバイスをダブルクリックします。
- ステップ 3** 設定するポートをクリックします。
- ステップ 4** [Details] ペインの [Details] タブをクリックします。
- ステップ 5** [IP Address Settings] セクションをクリックします。
- ステップ 6** 次のいずれかを行います。

**IPv4 アドレスを設定する場合：**

- a. [IPv4 Address settings] フィールドで、[Primary] フィールドに IP アドレスを入力し、[Net Mask] フィールドにネットワーク マスクをドット付き 10 進表記で入力します。
- b. (任意) [Secondary] フィールドで右クリックし、[Add secondary IP] を選択し、セカンダリ IP アドレスとネットワーク マスクを入力します。

**IPv6 アドレスを設定する場合：**

- a. [Primary/Prefix-length] フィールドに、セカンダリ IPv6 プレフィクスを x:x:x::x/length 形式で入力します。
- b. アドレスが Extended Universal Identifier (EUI) -64 形式の IPv6 アドレスであることを示すには、[EUI64] チェックボックスをオンにします。
- c. [Link Local] フィールドに、IPv6 リンク ローカル アドレスを x:x:x::x 形式で入力します。
- d. 自動的に生成された IPv6 アドレスよりリンク ローカル アドレスを優先するには、[Use local only] チェックボックスをオンにします。
- e. (任意) [Secondary] フィールドで右クリックし、[Add IPv6 address] を選択し、セカンダリ IPv6 アドレスを設定します。

- ステップ 7** (任意) メニュー バーで [File] > [Deploy] を選択して変更をデバイスに適用します。

表 2-6 基本インターフェイス パラメータのデフォルト設定

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
デバウンス タイマー	100 ミリ秒
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 ステート イネーブル (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 10/100 および 1000BASE-TX 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

表 2-6 基本インターフェイス パラメータのデフォルト設定 (続き)

パラメータ	デフォルト
UDLD アグレッシブ モード	ディセーブル
キャリア遅延	2 秒または 50 ミリ秒
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
リンクのデバウンス	イネーブル
ポート プロファイル	ディセーブル

## フィールドの説明

ここでは、[Ethernet] ペインに表示される次のフィールドについて説明します。

- 「[Device] : [Device Details] : [MTU Settings] セクション」 (P.2-28)
- 「[Device] : [Device Details] : [Error Disable Settings] セクション」 (P.2-28)
- 「[Device] : [Device Status] タブ」 (P.2-29)
- 「[Port] : [Port Details] : [Basic Settings] セクション」 (P.2-30)
- 「[Port] : [Port Details] : [Port Mode Settings] セクション」 (P.2-31)
- 「[Port] : [Port Details] : [Advanced Settings] セクション」 (P.2-32)
- 「[Port] : [Port Status] : [Port Status] セクション」 (P.2-34)
- 「[Port] : [Port Status] : [Port Status SFP] セクション」 (P.2-35)
- 「[Port] : [Port Status] : [Port SFP Diagnostics] セクション」 (P.2-36)

## [Device] : [Device Details] : [MTU Settings] セクション

表 2-7 [Device] : [Device Details] : [MTU Settings] セクション

フィールド	説明
Jumbo MTU	システム ジャンボ最大伝送ユニット (MTU) サイズ (バイト単位)。指定できる範囲は 1500 ~ 9216 です。デフォルト値は 1500 です。

## [Device] : [Device Details] : [Error Disable Settings] セクション

表 2-8 [Device] : [Device Details] : [Error Disable Settings] セクション

フィールド	説明
<b>Discovery</b>	
Select cause	error-disabled 状態のインターフェイスのすべての原因または特定の原因を入力します。
Acl exception	ACL インストールの失敗が error-disabled ステートの原因です。

表 2-8 [Device] : [Device Details] : [Error Disable Settings] セクション (続き)

フィールド	説明
Link state flapping	停止したり稼動したりしているリンクの error-disabled ステータス。
Loopback	ループバック インターフェイスは error-disabled になります。
<b>Recovery</b>	
Recovery Interval (sec)	インターフェイスが error-disabled ステートから回復する間隔。
Select cause	インターフェイスですべての原因または次の特定の原因のいずれかによる error-disable の回復をイネーブルにするように指定されています。
Link State Flapping	インターフェイスが停止したり稼動したりしています。
BPDU Guard	BPDU ガード機能。
Psecure Violation	Psecure 違反。
Storm Control	ストーム制御違反。
Security Violation	ポートのセキュリティ違反。
UDLD	UDLD 障害。

## [Device] : [Device Status] タブ

表 2-9 [Device] : [Device Status] タブ

フィールド	説明
Port Mode	表示のみ。インターフェイスの動作モード。次のいずれかのタイプになります。 <ul style="list-style-type: none"> <li>Access</li> <li>Trunk</li> <li>PVLAN Host</li> <li>PVLAN Promiscuous</li> <li>Routed</li> </ul>
Total	表示のみ。デバイスで使用できる各ポート モードの合計数。
Active	表示のみ。各ポート モードのアクティブ ポート数。
Admin Down	表示のみ。各ポート モードで管理的にダウンしているポート数。
Operationally Down	表示のみ。各ポート モードで動作的にダウンしているポート数。

## [Port] : [Port Details] : [Basic Settings] セクション

表 2-10 [Port] : [Port Details] : [Basic Settings] タブ

フィールド	説明
Name	表示のみ。インターフェイス名。
Description	インターフェイスの説明文（最大 80 文字）。
MTU	最大伝送ユニット サイズ（バイト単位）。指定できる範囲は 576 ～ 9216 です。デフォルト値は 1500 です。
Bandwidth	レイヤ 3 プロトコルで使用される帯域幅の情報用の値（この値では、インターフェイスの実際の帯域幅は変更されない）。指定できる範囲は 1 ～ 10,000,000 です。デフォルトは 10,000,000 です。
Delay	レイヤ 3 プロトコルで使用されるスループット遅延の情報用の値（この値では、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ない）。指定できる範囲は 1 ～ 16,777,215 です。デフォルトは 1 です。
Rate Mode	共有または専用レート モードを使用できるモジュールおよびポートで選択されたポートのレート モード。
Admin status	インターフェイスの管理ステータス。選択肢は [Up] と [Down] です。デフォルトは [Down] です。
CDP Enabled	他の接続デバイスを学習するために使用される Cisco Discovery Protocol。選択肢は [Enabled] と [Disabled] です。デフォルトは [Enabled] です。
Mdix	メディア依存インターフェイス クロスオーバー（MDIX）は、インターフェイス間のクロスオーバー接続を検出します。選択肢は [Enabled] と [Disabled] です。デフォルトは [Enabled] です。
UDLD Enabled	単方向リンク検出では、インターフェイス間の物理的な接続をモニタし、単方向リンクを検出してディセーブルにします。選択肢は [Enabled] と [Disabled] です。デフォルトは [Enabled] です。
Flow Control Receive	一定の時間のデータ伝送で一時停止を要求する受信したポーズ フレーム。この機能はオン、オフ、または目的の状態にすることができます（他のインターフェイスの Flow Control Send パラメータがイネーブルになっているか、または [desired] に設定されている場合にイネーブルになる）。選択肢は [off]、[desired]、[on] です。デフォルトは [desired] です。
Flow Control Send	一定の時間の他のインターフェイスに対するデータ伝送で一時停止を要求する送信したポーズ フレーム。この機能はオン、オフ、または目的の状態にすることができます（他のインターフェイスの Flow Control Receive パラメータがイネーブルになっているか、または [desired] に設定されている場合にイネーブルになる）。選択肢は [off]、[desired]、[on] です。デフォルトは [desired] です。
Port Channel Id	インターフェイスが属しているポート チャネル（存在している場合）。デフォルトは空白です。
Speed	メガビット/秒単位のインターフェイス速度（Mb/s）。選択肢は [10]、[100]、[1000]、[auto] です。デフォルトの設定は [auto] です。 このパラメータの設定は、デュプレックス モードに使用できる値を指定します。
Duplex mode	インターフェイスのデュプレックス モード。選択肢は [full]、[half]、[auto] です。デフォルトの設定は [auto] です。



表 2-10 [Port] : [Port Details] : [Basic Settings] タブ (続き)

フィールド	説明
Beacon	シャーシのモジュール上のインターフェイスを識別する LED。選択肢は [Enabled] と [Disabled] です。デフォルトは [Disabled] です。
Link Debounce	遅延したリンク変更の通知。選択肢は [Enabled] と [Disabled] です。デフォルトは [Enabled] です。
Debounce Time	デバウンス遅延時間 (ミリ秒単位)。指定できる範囲は 0 ~ 5000 です。デフォルトは 100 です。

## [Port] : [Port Details] : [Port Mode Settings] セクション

表 2-11 [Port] : [Port Details] : [Port Mode Settings] セクション

フィールド	説明
Mode	有効な値は次のとおりです。 <ul style="list-style-type: none"> <li>Access</li> <li>Trunk</li> <li>PVLAN Host</li> <li>PVLAN Promiscuous</li> <li>Routed</li> </ul>
<b>Access</b>	
Access VLAN	このアクセス ポートのアクセス VLAN。デフォルトのアクセス VLAN はデフォルト VLAN、または VLAN1 です。
<b>Trunk</b>	
Encapsulation	使用できないフィールド。IEEE 802.1Q は、サポートされている唯一のカプセル化方法です。
Allowed VLANs	このポートでデータを伝送できる VLAN。有効範囲は 1 ~ 4094。デフォルトは 1。 <b>(注)</b> VLAN 3968 ~ 4047 および 4094 は、デバイス内部使用のために割り当てられており、データトラフィックは伝送しません。
Native VLAN	このトランクポートのネイティブ VLAN。デフォルトのネイティブ VLAN はデフォルト VLAN、または VLAN1 です。
<b>PVLAN Host</b>	
Primary Vlan	表示のみ。このポートが属している VLAN に関連付けられたプライマリ VLAN。 <b>(注)</b> この値は、[Secondary VLAN] フィールドを使用してセカンダリ VLAN を選択した後に表示されます。
Secondary VLAN	プライマリ VLAN とペアになるセカンダリ VLAN。セカンダリ VLAN のタイプはコミュニティまたは独立です。
<b>PVLAN Promiscuous</b>	

表 2-11 [Port] : [Port Details] : [Port Mode Settings] セクション (続き)

フィールド	説明
Primary Vlan	表示のみ。このポートが属している VLAN に関連付けられたプライマリ VLAN。 (注) この値は、[Secondary VLAN] フィールドを使用してセカンダリ VLAN を選択した後に表示されます。
Secondary VLAN	プライマリ VLAN とペアになるセカンダリ VLAN。セカンダリ VLAN のタイプはコミュニティまたは独立です。 (注) 複数のセカンダリ VLAN を選択でき、そのすべてのプライマリ VLAN が同じで、それぞれにプライベート VLAN 無差別モード ポートを用意できます。
<b>Routed</b>	
IPv4 Address Settings	
Primary	ドット付き 10 進表記の IPv4 アドレス。
Net mask	ドット付き 10 進表記の IPv4 アドレスのネットワーク マスク。
Secondary: IP Address	ドット付き 10 進表記のセカンダリ IPv4 アドレス。1 つのインターフェイスに対して複数のセカンダリ アドレスを設定できます。
Secondary: Net mask	ドット付き 10 進表記のセカンダリ IPv4 アドレスのネットワーク マスク。
Helper: IP Address	User Datagram Protocol (UDP; ユーザ データグラム プロトコル) ブロードキャストの転送をイネーブルにするために使用されるヘルパー アドレス。
IPv6 Address Settings	
Primary/Prefix-length	x::x::x/length 形式の IPv6 プレフィクス。
EUI64	Extended Universal Identifier (EUI) -64 形式の IPv6 アドレス。
Link Local	x::x::x 形式の IPv6 リンク ローカル アドレス。
Use local only	リンク ローカル アドレスは、自動的に生成された IPv6 アドレスより優先されます。
Secondary: IP Address	x::x::x/length 形式のセカンダリ IPv6 プレフィクス。1 つのインターフェイスに対して複数のセカンダリ アドレスを設定できます。
Secondary: EUI64	Extended Universal Identifier (EUI) -64 形式のセカンダリ IPv6 アドレス。

## [Port] : [Port Details] : [Advanced Settings] セクション

表 2-12 [Port] : [Port Details] : [Advance Settings] セクション

フィールド	説明
<b>IPv4 ACL</b>	
Incoming Ipv4 Traffic	インターフェイス上の入力トラフィックをフィルタリングする IPv4 ACL。デフォルトでは、このリストは空白です。
Outgoing Ipv4 Traffic	インターフェイス上の出力トラフィックをフィルタリングする IPv4 ACL。デフォルトでは、このリストは空白です。
<b>IPv6 ACL</b>	
Incoming Ipv6 Traffic	インターフェイス上の入力トラフィックをフィルタリングする IPv6 ACL。デフォルトでは、このリストは空白です。

表 2-12 [Port] : [Port Details] : [Advance Settings] セクション (続き)

フィールド	説明
Outgoing Ipv6 Traffic	インターフェイス上の出力トラフィックをフィルタリングする IPv6 ACL。 デフォルトでは、このリストは空白です。
<b>MAC ACL</b>	
Incoming Traffic	インターフェイス上の入力トラフィックをフィルタリングする MAC ACL。 デフォルトでは、このリストは空白です。
<b>Security</b>	
Dot1x	表示のみ。dot1x がイネーブルまたはディセーブルです。
Traffic Storm Control	表示のみ。トラフィック ストーム制御がイネーブルまたはディセーブルです。
IP Source Guard	表示のみ。IP ソース ガードがイネーブルまたはディセーブルです。
Port Security	表示のみ。ポート セキュリティがイネーブルまたはディセーブルです。
<b>SPAN</b>	
Use Interface as SPAN	このインターフェイスの送信元または宛先。
Session ID	インターフェイスが適用される SPAN セッション ID。
Type	表示のみ。セッションのタイプ。
Direction: Ingress	入力パケットをモニタします。
Direction: Egress	出力パケットをモニタします。

## [Port] : [Port Status] : [Port Status] セクション

表 2-13 [Port] : [Port Status] : [Port Status] セクション

フィールド	説明
Operational Status	<p>表示のみ。インターフェイスの動作ステータス。デフォルトは <b>down</b> です。有効な値は次のとおりです。</p> <ul style="list-style-type: none"> <li>Up</li> <li>Down</li> </ul>
Status Description	<p>表示のみ。次のような動作ステータスの説明。</p> <ul style="list-style-type: none"> <li>Connected : ケーブルがインターフェイスに接続され、アップしています。</li> <li>Admin down : インターフェイスが管理的にダウンしていると設定されます。</li> <li>Channel down : インターフェイスが、動作的にダウンしているポートチャネルのメンバです。</li> <li>Disabled : インターフェイスが管理的にダウンしていると設定されます。</li> <li>Error disabled : インターフェイスが <b>error-disabled</b> ステートです。</li> <li>Hardware failure : インターフェイスでハードウェア障害が発生しています。</li> <li>Inactive : インターフェイスが非アクティブです。</li> <li>Initializing : 起動プロセスでインターフェイスを初期化しています。</li> <li>Not connected : インターフェイスにケーブルが接続されていません。</li> <li>SFP not inserted : インターフェイスに SFP コネクタが接続されていません。</li> <li>Link failure : インターフェイスの別のインターフェイスへのケーブル接続に失敗しました。</li> <li>Interface removed : 物理ポートが壊れているか、またはインターフェイスから物理的に接続されていません。</li> <li>Incompatible admin mode : このインターフェイスの管理モードに、接続されたインターフェイスで設定されている管理モードとの互換性がありません。</li> <li>Incompatible admin speed : このインターフェイスの速度に、接続されたインターフェイスで設定されている速度との互換性がありません。</li> <li>Suspended by mode : モード設定の問題によって、物理的接続が停止されました。</li> <li>Suspended by speed : 速度設定の問題によって、物理的接続が停止されました。</li> <li>Upgrade in progress : 物理ポートでソフトウェアのアップグレードが進行中です。</li> <li>Port channel member down : ポートがダウンしていて、ポートチャネルのメンバです。</li> <li>Module removed : ポートのモジュールがシャーシ内にありません。</li> <li>Unsupported transceiver : シスコが認定していないトランシーバがポートに挿入されています。</li> <li>Unknown : 不明な理由により、ポートが動作的にダウンしています。</li> </ul>

表 2-13 [Port] : [Port Status] : [Port Status] セクション (続き)

フィールド	説明
Speed	表示のみ。インターフェイスの伝送速度。デフォルトの設定は auto です。
Duplex	表示のみ。インターフェイスのデュプレックス動作。デフォルトの設定は auto です。
UDLD	表示のみ。UDLD のステータス。デフォルトはディセーブルです。有効な値は次のとおりです。 <ul style="list-style-type: none"> <li>• Enabled</li> <li>• Disabled</li> </ul>
Flow Control Send	表示のみ。ポーズ フレームの送信ステータス。デフォルトは off です。有効な値は次のとおりです。 <ul style="list-style-type: none"> <li>• off</li> <li>• desired</li> <li>• on</li> </ul>
Flow Control Receive	表示のみ。ポーズ フレームの受信ステータス。デフォルトは off です。有効な値は次のとおりです。 <ul style="list-style-type: none"> <li>• off</li> <li>• desired</li> <li>• on</li> </ul>
Hardware Type	表示のみ。ポートのハードウェア タイプ。

## [Port] : [Port Status] : [Port Status SFP] セクション

表 2-14 [Port] : [Port Status] : [Port Status SFP] セクション

フィールド	説明
Name	表示のみ。SFP デバイス名。
Part Number	表示のみ。SFP デバイスの部品番号。
Revision	表示のみ。SFP デバイスのリビジョン番号。
Serial Number	表示のみ。SFP デバイスのシリアル番号。
Nominal Bitrate	表示のみ。SFP デバイスのビットレート。
Link Length for 9/125um	表示のみ。SFP デバイスの 9/125um の長さ。
Link Length for 50/125um	表示のみ。SFP デバイスの 50/125um の長さ。
Link Length for 62.5/125um	表示のみ。SFP デバイスの 62.5/125um の長さ。
Cisco Id	表示のみ。SFP デバイスの Cisco ID。
Extended Cisco Id	表示のみ。SFP デバイスの拡張 Cisco ID。

## [Port] : [Port Status] : [Port SFP Diagnostics] セクション

表 2-15 [Port] : [Port Status] : [Port SFP Diagnostics] セクション

フィールド	説明
Refresh Frequency	情報が更新される頻度。範囲は 30 秒～ 5 分で、30 秒間隔です。
Temperature (celsius)	表示のみ。次の値の SFP デバイスの温度。 <ul style="list-style-type: none"> <li>• Current Diagnostic Value</li> <li>• High Alarm</li> <li>• Low Alarm</li> <li>• High Warning</li> <li>• Low Warning</li> <li>• Status</li> </ul>
Voltage (volts)	表示のみ。次の値の SFP デバイスの電圧。 <ul style="list-style-type: none"> <li>• Current Diagnostic Value</li> <li>• High Alarm</li> <li>• Low Alarm</li> <li>• High Warning</li> <li>• Low Warning</li> <li>• Status</li> </ul>
Current (milli amps)	表示のみ。次の値の SFP デバイスの電流。 <ul style="list-style-type: none"> <li>• Current Diagnostic Value</li> <li>• High Alarm</li> <li>• Low Alarm</li> <li>• High Warning</li> <li>• Low Warning</li> <li>• Status</li> </ul>

表 2-15 [Port] : [Port Status] : [Port SFP Diagnostics] セクション (続き)

フィールド	説明
Tx Power (decibels)	表示のみ。次の値の SFP デバイスの伝送電力。 <ul style="list-style-type: none"><li>• Current Diagnostic Value</li><li>• High Alarm</li><li>• Low Alarm</li><li>• High Warning</li><li>• Low Warning</li><li>• Status</li></ul>
Rx Power (decibels)	表示のみ。次の値の SFP デバイスの受信電力。 <ul style="list-style-type: none"><li>• Current Diagnostic Value</li><li>• High Alarm</li><li>• Low Alarm</li><li>• High Warning</li><li>• Low Warning</li><li>• Status</li></ul>

## その他の関連資料

機能 1 の実装に関連した情報については、次を参照してください。

- 「関連資料」 (P.2-38)
- 「標準規格」 (P.2-38)
- 「基本インターフェイス パラメータ設定の機能履歴」 (P.2-38)

## 関連資料

関連項目	参照先
コマンド リファレンス	『Cisco Nexus 7000 Series NX-OS Interfaces Command Reference, Release 5.x』
レイヤ 2 スイッチング	『Cisco DCNM Layer 2 Switching Configuration Guide, Release 5.x』
CDP	『Cisco Nexus 7000 Series NX-OS System Management Command Reference, Release 5.x』

## 標準規格

標準規格	タイトル
この機能でサポートされる新規または改訂された標準規格はありません。また、この機能による既存の標準規格サポートの変更はありません。	—

# 基本インターフェイス パラメータ設定の機能履歴

表 2-16 は、この機能のリリースの履歴です。

表 2-16 基本インターフェイス パラメータ設定の機能履歴

機能名	リリース	機能情報
基本インターフェイスの設定	4.0(1)	これらの機能が導入されました。
SFP 情報	4.1(2)	SFP インターフェイスに関する表示情報が追加されました。
キャリア遅延	4.1(2)	インターフェイスのアップ/ダウンが急激に変更されないようにするためのタイマーを設定します。





## CHAPTER 3

# レイヤ 2 インターフェイスの設定

この章では、レイヤ 2 スイッチング ポートをアクセス ポートまたはトランク ポートとして設定する手順について説明します。



(注)

管理対象デバイス上で実行される Cisco NX-OS リリースでは、この章で説明する機能や設定がすべてサポートされるとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースのマニュアルとリリース ノートを参照してください。



(注)

レイヤ 2 ポートは、トランク ポート、アクセス ポート、またはプライベート VLAN ポートとして機能させることができます。プライベート VLAN の詳細については、『*Cisco DCNM Layer 2 Switching Configuration Guide, Release 5.x*』を参照してください。

この章では、次の内容について説明します。

- 「アクセス インターフェイスとトランク インターフェイスについて」 (P.3-2)
- 「レイヤ 2 ポート モードのライセンス要件」 (P.3-6)
- 「VLAN トランッキングの前提条件」 (P.3-6)
- 「注意事項および制約事項」 (P.3-7)
- 「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」 (P.3-8)
- 「統計情報の表示とクリア」 (P.3-11)
- 「フィールドの説明」 (P.3-11)
- 「その他の関連資料」 (P.3-12)
- 「レイヤ 2 インターフェイス設定の機能履歴」 (P.3-13)



(注)

SPAN 宛先インターフェイスについては、『*Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 5.x*』を参照してください。

Data Center Network Manager の機能の詳細については、『*Cisco DCNM Fundamentals Configuration Guide, Release 5.x*』を参照してください。

レイヤ 2 スイッチング ポートをアクセス ポートまたはトランク ポートとして設定できます。トランクは単一のリンクを介して複数の VLAN トラフィックを伝送します。これにより、ネットワーク全体に VLAN を拡張できます。すべてのレイヤ 2 スイッチング ポートは、Media Access Control (MAC; メディア アクセス制御) アドレス テーブルを維持します。



(注)

VLAN、プライベート VLAN、およびスパンニング ツリー プロトコルの詳細については、『*Cisco DCNM Layer 2 Switching Configuration Guide, Release 5.x*』を参照してください。



(注)

レイヤ 2 ポートは、トランク ポート、アクセス ポート、またはプライベート VLAN ポートとして機能させることができます。プライベート VLAN の詳細については、『*Cisco DCNM Layer 2 Switching Configuration Guide, Release 5.x*』を参照してください。

## 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 7000 Series NX-OS High Availability and Redundancy Guide, Release 5.x*』を参照してください。

ここでは、次の内容について説明します。

- 「アクセス インターフェイスとトランク インターフェイスについて」 (P.3-2)
- 「IEEE 802.1Q カプセル化」 (P.3-3)
- 「アクセス VLAN」 (P.3-4)
- 「トランク ポートのネイティブ VLAN ID」 (P.3-5)
- 「ネイティブ VLAN トラフィックのタグging」 (P.3-5)
- 「許容 VLAN」 (P.3-5)
- 「ハイ アベイラビリティ」 (P.3-6)
- 「バーチャライゼーションのサポート」 (P.3-6)



(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 インターフェイスについて

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 ポートには 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。

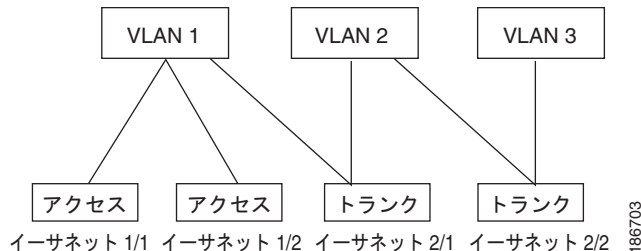
デフォルトでは、デバイスのポートはすべてレイヤ 3 ポートです。

デフォルト ポート設定をレイヤ 2 に変更するには、Command-Line Interface (CLI; コマンドライン インターフェイス) を使用します。システムのデフォルト ポート設定をレイヤ 2 に変更する方法については、『*Cisco DCNM Layer 2 Switching Configuration Guide, Release 5.x*』を参照してください。

同じトランクのポートはすべて同じデバイス内にある必要があります。複数のデバイスからの VLAN のトラフィックをトランク ポートで伝送できません。

図 3-1 に、ネットワーク内でのトランク ポートの使用例を示します。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 3-1 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 DCNM Layer 2 Switching Configuration Guide, Release 5.x』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」(P.3-3) を参照してください）。



(注) レイヤ 3 インターフェイスのサブインターフェイスの詳細については、『Cisco DCNM Unicast Routing Configuration Guide, Release 5.x』を参照してください。

アクセス ポートのパフォーマンスを最適化するには、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メッセージが表示されます。

アクセスポートで受信するパケットのヘッダーにアクセス VLAN 値以外の 802.1Q タグがある場合、このポートは MAC 送信元アドレスを学習せずにパケットをドロップします。

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 の情報については、『Cisco DCNM Layer 2 Switching Configuration Guide, Release 5.x』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キングデバイス間の Point-To-Point (p2p; ポイントツーポイント) リンクです。トランクは単一のリンクを介して複数の VLAN トラフィックを伝送します。これにより、ネットワーク全体に VLAN を拡張できます。

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（図 3-2 を参照）。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 間でトラフィック分離を維持できます。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 3-2 802.1Q タグなしヘッダーと 802.1Q タグ付きヘッダー

プリアンブル (7 バイト)	開始 フレーム デリミタ (1 バイト)	宛先 MAC アドレス (6 - バイト)	送信元 MAC アドレス (6 - バイト)	長さ /タイプ (2 - バイト)	MAC クライアント データ (0 ~ n バイト)	パッド (0 ~ p バイト)	フレーム チェック シーケンス (4 バイト)
-------------------	-------------------------------	-----------------------------------	------------------------------------	----------------------------	-------------------------------	-----------------------	----------------------------------

プリアンブル (7 バイト)	開始 フレーム デリミタ (1 バイト)	宛先 MAC アドレス (6 バイト)	送信元 MAC アドレス (6 バイト)	長さ/タイプ = 802.1Q タグ タイプ (2 バイト)	タグ 制御 情報 (2 バイト)	長さ /タイプ (2- バイト)	MAC クライアント データ (0 ~ n バイト)	パッド (0 ~ p バイト)	フレーム チェック シーケンス (4 バイト)
-------------------	-------------------------------	------------------------------	-------------------------------	---	---------------------------	---------------------------	----------------------------------	-----------------------	----------------------------------

3 ビット = ユーザ プライオリティ フィールド  
1 ビット = Canonical Format Identifier (CFI)  
12 ビット = VLAN 識別子 (VLAN ID)

182779

## アクセス VLAN



(注)

アクセス VLAN を割り当て、プライベート VLAN のプライマリ VLAN としても動作させると、そのアクセス VLAN に対応するすべてのアクセス ポートも、プライベート VLAN モードのプライマリ VLAN 向けのすべてのブロードキャスト トラフィックを受信するようになります。



(注)

プライベート VLAN の詳細については、『Cisco DCNM Layer 2 Switching Configuration Guide, Release 5.x』を参照してください。

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 モードのポート用またはアクセス 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) のトラフィックを伝送します。

VLAN のアクセス ポート メンバ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 値のほかに 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 MAC アドレスを学習せずに、そのパケットをドロップします。

## 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 は、トランク ポートのネイティブ VLAN ID と呼ばれます。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る必要があります。

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。

## 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。

## 許容 VLAN

デフォルトでは、トランク ポートは、すべての VLAN へのトラフィックを送信し、すべての VLAN からのトラフィックを受信します。各トランク上では、すべての VLAN ID が許可されます。ただし、この包括的なリストから VLAN を削除すれば、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 の収束時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)

パーティションの詳細については、『Cisco DCNM Layer 2 Switching Configuration Guide, Release 5.x』を参照してください。

## ハイ アベイラビリティ

ソフトウェアは、レイヤ 2 ポートのハイ アベイラビリティをサポートします。



(注)

ハイ アベイラビリティの詳細については、『*Cisco Nexus 7000 Series NX-OS High Availability and Redundancy Guide, Release 5.x*』を参照してください。

## バーチャライゼーションのサポート

デバイスは仮想デバイス コンテキスト (VDC) をサポートします。

同じトランクのポートはすべて同じデバイス内にある必要があります。また、複数のデバイスからの VLAN のトラフィックをトランク ポートで伝送できません。



(注)

VDC およびリソースの割り当ての詳細については、『*Cisco DCNM Virtual Device Context Configuration Guide, Release 5.x*』を参照してください。

## レイヤ 2 ポート モードのライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
DCNM	レイヤ 2 ポート モードにライセンスは必要ありません。ライセンス パッケージに含まれていない機能は Cisco DCNM にバンドルされており、無料で使用できます。
NX-OS	レイヤ 2 ポート モードにライセンスは必要ありません。ライセンス パッケージに含まれていない機能はすべて Cisco NX-OS システム イメージにバンドルされており、追加費用は一切発生しません。NX-OS のライセンス スキームの詳細については、『 <i>Cisco Nexus 7000 Series NX-OS Licensing Guide, Release 5.x</i> 』を参照してください。



(注)

VDC を使用する場合は Advanced Services ライセンスが必要です。

## VLAN トランキングの前提条件

アクセスまたはトランク スイッチポート モードでポートを設定するには、次の前提条件が必要です。

- デバイスにログインしていること。

## 注意事項および制約事項

次に示す設定時の注意事項および制約事項は、802.1Q トランクを使用するときに適用され、ネットワークのトランッキングの構築方法が多少制限されます。802.1Q トランクを使用するときは、これらの制約事項に注意してください。

- 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 と他端のネイティブ 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。
- ネットワーク上の各 VLAN のスパニング ツリーをディセーブルにせずに 802.1Q トランクのネイティブ VLAN 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 Bridge Protocol Data Unit (BPDU; ブリッジ プロトコル データ ユニット) 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。トランク上の他の全 VLAN 上の BPDU は、タグ付きの状態で、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の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 とシスコ製の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グディングされます。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、フラグ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する場合、すべてのポートはグループに追加する最初のポートのパラメータ セットのとおりになります。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と、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 をイネーブルにしたポートをトランク モードに変更しようとしても、ポートのモードは変更されません。

## 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

ここでは、次の内容について説明します。

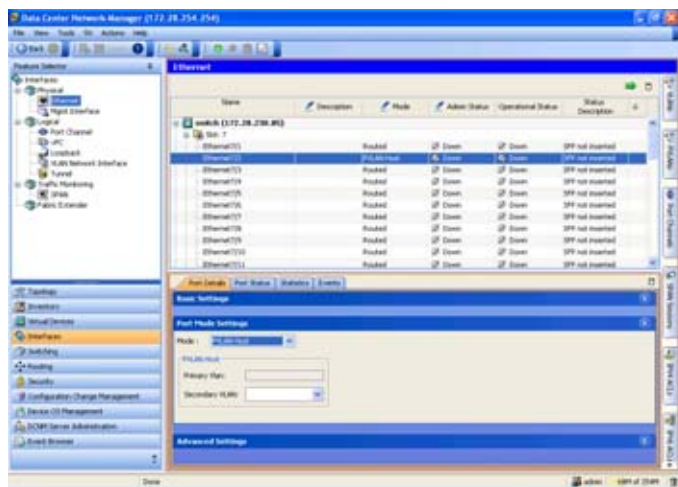
- ・ 「レイヤ2 アクセス ポートとしての LAN インターフェイスの設定」 (P.3-8)
- ・ 「トランク ポートの設定」 (P.3-9)
- ・ 「ネイティブ VLAN トラフィックにタグを付けるためのデバイス設定」 (P.3-10)

## レイヤ2 アクセス ポートとしての LAN 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、タグなしの1つのVLANだけのパケットを伝送します。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VLAN1です。

レイヤ2 アクセスポートを設定するには、[Ethernet] ペインを使用します (図 3-3 を参照)。

図 3-3 [Ethernet] ペイン、[Port Mode Settings]



### 手順の詳細

レイヤ2 アクセスポートを設定するには、次の手順を実行します。

- ステップ 1** [Feature Selector] ペインで [Interfaces] > [Physical] > [Ethernet] を選択して [Ethernet] ペインを開きます。
- ステップ 2** [Summary] ペインの [Contents] ペインで、デバイスをダブルクリックしてインターフェイスを表示します。
- ステップ 3** スロットをクリックすると、インターフェイスのリストが表示されます。
- ステップ 4** インターフェイスをクリックします。

そのインターフェイスが [Summary] ペイン内で強調表示され、一連のタブが [Details] ペインに表示されます。



- ステップ 5** [Details] ペインの [Port Details] タブをクリックします。
- ステップ 6** [Port Mode Settings] セクションをクリックします。
- ステップ 7** ポートをアクセス ポートとして設定するには、[Mode] ドロップダウン リストで [Access] を選択します。  
[Routed] がデフォルトのポート モードです。
- ステップ 8** [Access VLAN] フィールドでアクセス VLAN を指定します。指定するには、既知の VLAN を使用するか、このデバイス上の VLAN の 1 つを割り当てるか、新しい VLAN を作成します。  
デフォルトのアクセス VLAN は VLAN1 です。有効範囲は VLAN 1 ~ 4094 です。ただし、内部的に割り当てられている VLAN 3968 ~ 4047 と 4094 を除きます。
- ステップ 9** メニュー バーで [File] > [Deploy] を選択して変更をデバイスに適用します。

## トランク ポートの設定



(注)

実際のポートがまだアクセス モードであるときに、トランク ポートをプレプロビジョニングすることができます。メイン メニューで [Tools] > [Global Preferences] > [Pre Provisioning] を選択すると、この機能を設定する画面の表示と非表示が切り替わります。プレプロビジョニングの詳細については、『Cisco DCNM Fundamentals Configuration Guide, Release 5.x』を参照してください。

レイヤ 2 ポートをトランク ポートとして設定することができます。このポートは、1 つの VLAN のタグなしパケットを送信するのに加えて、複数の VLAN のカプセル化されたタグ付きパケットを送信します。



(注)

デバイスは 802.1Q カプセル化だけをサポートします。

レイヤ 2 トランク ポートを設定するには、[Ethernet] ペインを使用します (図 3-3 を参照)。

### 手順の詳細

レイヤ 2 トランク ポートを設定する手順は次のとおりです。

- ステップ 1** [Feature Selector] ペインで [Interfaces] > [Physical] > [Ethernet] を選択して [Ethernet] ペインを開きます。
- ステップ 2** [Summary] ペインの [Contents] ペインで、デバイスをダブルクリックしてインターフェイスを表示します。
- ステップ 3** スロットをクリックすると、インターフェイスのリストが表示されます。
- ステップ 4** インターフェイスをクリックします。  
そのインターフェイスが [Summary] ペイン内で強調表示され、一連のタブが [Details] ペインに表示されます。
- ステップ 5** [Details] ペインの [Port Details] タブをクリックします。
- ステップ 6** [Port Mode Settings] セクションをクリックします。
- ステップ 7** ポートをトランク ポートとして設定するには、[Mode] ドロップダウン リストで [Trunk] を選択します。



(注)

[Encapsulation] の行の淡色表示されている dot1q からの値は変更しないでください。IEEE 802.1Q カプセル化法は、サポートされている唯一のカプセル化方法です。

VLAN 1 ～ 4094 がデフォルトです。VLAN 3968 ～ 4047 および 4094 は、デバイス使用のために内部的に割り当てられています。

デフォルトのネイティブ VLAN は VLAN1 です。有効範囲は VLAN 1 ～ 4094 です。ただし、内部的に割り当てられている VLAN 3968 ～ 4047 と 4094 を除きます。

**ステップ 10** メニュー バーで [File] > [Deploy] を選択して変更をデバイスに適用します。

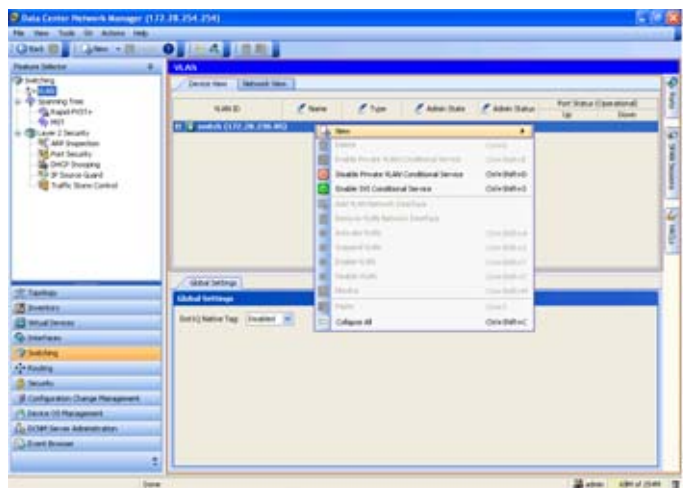
**802.1Q** トランク インターフェイスを使用する場合、ネイティブ **VLAN ID** の値と一致しすべてのタグなしトラフィックをドロップするタグで開始するすべてのパケットに対するタグgingを維持できます（この場合もインターフェイスの制御トラフィックは伝送されます）。この機能はデバイス全体に当てはまります。デバイスの **VLAN** を指定して当てはめることはできません。



(注) あるデバイスの 802.1Q タギングでディセーブルにし、別のデバイスではディセーブルにすると、この機能をディセーブルにしたデバイスのトラフィックはすべてドロップされます。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。

すべてのトランク ポートのすべてのネイティブ **VLAN** に対してタグgingを維持するように設定するには、**[VLAN]** ペインを使用します (図 3-4 を参照)。

**図 3-4 [VLAN] ペイン、[Global Settings]**



トランク ポートのネイティブ VLAN に対してタギングを維持するようにデバイスを設定する手順は次のとおりです。

- 
- ステップ 1** [Feature Selector] ペインで [Switching] > [VLAN] を選択して [VLAN] ペインを開きます。
- ステップ 2** [Summary] ペインの [Device View] タブをクリックします。
- ステップ 3** 設定するデバイスをクリックします。  
そのデバイスが [Summary] ペイン内で強調表示され、一連のタブが [Details] ペインに表示されます。
- ステップ 4** [Details] ペインの [Global Settings] タブをクリックします。
- ステップ 5** [Dot1Q Native Tag] ドロップダウン リストから [Enabled] を選択します。これで、すべてのトランクポートのネイティブ VLAN 上で常に 802.1q タグを維持するようにデバイスが設定されます。  
デフォルトはディセーブルです。
- ステップ 6** メニュー バーで [File] > [Deploy] を選択して変更をデバイスに適用します。
- 

## 統計情報の表示とクリア

統計情報を表示するために作成できるチャートには、次のものがあります。これらは [Statistics] タブに表示されます。

- Traffic Statistics Chart : ポートに関する情報（ユニキャスト、マルチキャスト、廃棄など）が表示されます。
- Error Counters Chart : アクセスまたはトランク インターフェイスに関するエラーが表示されます（アラインメント、コリジョン、ラント、ジャイアントなど）。
- SFP Diagnostic Chart : このデバイスに接続されている SFP トランシーバに関する診断情報が表示されます。
- Trunk Statistics Chart : 特定のトランク ポートを選択したときにトランクの情報が表示されます（ユニキャスト、マルチキャストなど）。
- SOLM Statistics Chart : ユニキャストおよびマルチキャストの受信/送信トラフィックに関するデータが表示されます。



**(注)** SOLM Statistics Chart を作成できるのは、Cisco Nexus 4000 プラットフォーム、Cisco DCNM 4.2(3) リリース以降のみです。

- FIP Statistics Chart : 選択されているイーサネット インターフェイスの FIP 統計情報が表示されます。

この機能のための統計情報収集の詳細については、『Cisco DCNM Fundamentals Configuration Guide, Release 5.x』を参照してください。

## フィールドの説明

この章で説明したフィールドの説明は、第2章「基本インターフェイス パラメータの設定」を参照してください。

## その他の関連資料

アクセスおよびトランク ポート モードの実装に関する追加情報については、次の項を参照してください。

- 「関連資料」(P.3-12)
- 「標準規格」(P.3-12)
- 「管理情報ベース (MIB)」(P.3-13)

## 関連資料

関連項目	参照先
レイヤ 3 インターフェイスの設定	<a href="#">第 4 章「レイヤ 3 インターフェイスの設定」</a>
ポート チャンネル	<a href="#">第 5 章「ポート チャンネルの設定」</a>
VLAN、プライベート VLAN、STP	『Cisco DCNM Layer 2 Switching Configuration Guide, Release 5.x』
インターフェイス	『Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 5.x』
システム管理	『Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 5.x』
ハイ アベイラビリティ	『Cisco Nexus 7000 Series NX-OS High Availability and Redundancy Guide, Release 5.x』
仮想デバイス コンテキスト (VDC)	『Cisco DCNM Virtual Device Context Configuration Guide, Release 5.x』
ライセンス	『Cisco DCNM Fundamentals Configuration Guide, Release 5.x』
リリース ノート	『Cisco DCNM Release Notes, Release 5.x』

## 標準規格

標準規格	タイトル
この機能でサポートされる新規または改訂された標準規格はありません。また、この機能による既存の標準規格サポートの変更はありません。	—

## 管理情報ベース（MIB）

管理情報ベース（MIB）	MIB リンク
<ul style="list-style-type: none"><li>BRIDGE-MIB</li><li>IF-MIB</li><li>CISCO-IF-EXTENSION-MIB</li><li>ETHERLIKE-MIB</li></ul>	Management Information Base（MIB; 管理情報ベース）を検索およびダウンロードするには、次の URL にアクセスしてください。 <a href="http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml">http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</a>

## レイヤ 2 インターフェイス設定の機能履歴

表 3-1 は、この機能のリリースの履歴です。

表 3-1 レイヤ 2 インターフェイス設定の機能履歴

機能名	リリース	機能情報
レイヤ 2 インターフェイス	4.0(1)	この機能が導入されました。
SFP 診断および SOLM 統計のチャート	4.2(3)	この機能が導入されました。





# CHAPTER 4

## レイヤ 3 インターフェイスの設定

この章では、Cisco Nexus 7000 シリーズ デバイスのレイヤ 3 インターフェイスを設定する手順について説明します。

この章では、次の内容について説明します。

- 「レイヤ 3 インターフェイスについて」 (P.4-1)
- 「レイヤ 3 インターフェイスのライセンス要件」 (P.4-5)
- 「注意事項および制約事項」 (P.4-5)
- 「ライセンス 3 インターフェイスの前提条件」 (P.4-5)
- 「レイヤ 3 インターフェイスの設定」 (P.4-6)
- 「レイヤ 3 インターフェイス統計情報の表示」 (P.4-17)
- 「関連項目」 (P.4-17)
- 「レイヤ 3 インターフェイスのフィールドの説明」 (P.4-17)
- 「その他の関連資料」 (P.4-20)
- 「レイヤ 3 インターフェイス設定の機能履歴」 (P.4-21)

## レイヤ 3 インターフェイスについて



(注)

管理対象デバイス上で実行される Cisco NX-OS リリースでは、この章で説明する機能や設定がすべてサポートされるとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースのマニュアルとリリース ノートを参照してください。

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。

ここでは、次の内容について説明します。

- 「ルーテッド インターフェイス」 (P.4-2)
- 「サブインターフェイス」 (P.4-2)
- 「VLAN インターフェイス」 (P.4-3)
- 「ループバック インターフェイス」 (P.4-4)
- 「トンネル インターフェイス」 (P.4-4)

- 「ハイ アベイラビリティ」 (P.4-4)
- 「バーチャライゼーションのサポート」 (P.4-5)

## 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、Spanning Tree Protocol (STP; スパニング ツリー プロトコル) 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。

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 チャンネルも作成できます。ポート チャンネルの詳細については、第 5 章「ポート チャンネルの設定」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サブインターフェイスは、指数関数的に減少するレート カウンタをサポートします。Cisco NX-OS はこれらの平均カウンタを用いて次の統計情報を追跡します。

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

## サブインターフェイス

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

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

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

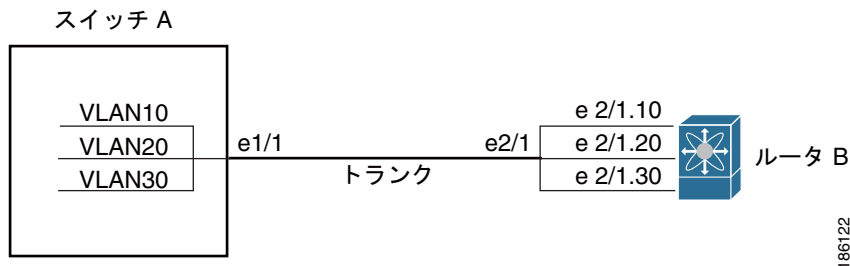
Cisco NX-OS では、親インターフェイスがイネーブルの場合にサブインターフェイスがイネーブルになります。サブインターフェイスは、親インターフェイスには関係なくシャットダウンできます。親インターフェイスをシャットダウンすると、関連するサブインターフェイスもすべてシャットダウンされます。

サブインターフェイスを使用すると、親インターフェイスがサポートするそれぞれの Virtual Local Area Network (VLAN; 仮想ローカル エリア ネットワーク) 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。



図 4-1 に、インターフェイス E 2/1 のルータ B に接続するスイッチのトランキング ポートを示します。このインターフェイスには 3 つのサブインターフェイスがあり、トランキング ポートに接続する 3 つの VLAN にそれぞれ関連付けられています。

図 4-1 VLAN のサブインターフェイス



VLAN の詳細については、『Cisco DCNM Layer 2 Switching Configuration Guide, Release 5.x』を参照してください。

## VLAN インターフェイス

VLAN ネットワーク インターフェイスは仮想のルーテッドインターフェイスで、デバイスの VLAN を同じデバイスのレイヤ 3 ルータ エンジンに接続します。1 つの VLAN には 1 つの VLAN ネットワーク インターフェイスだけを関連付けできます。ただし、VLAN 同士をルーティングする場合や管理 Virtual Routing and Forwarding (VRF; 仮想ルーティング/転送) 以外の VRF インスタンスを経由してデバイスを IP ホスト接続する場合だけ、VLAN に VLAN ネットワーク インターフェイスを設定する必要があります。VLAN ネットワーク インターフェイスの作成をイネーブルにすると、NX-OS によってデフォルト VLAN (VLAN 1) に VLAN ネットワーク 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。リリース 4.2 から、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ようになったため、このチェックポイントにロールバックすれば機能をイネーブルにできます。ロールバックとチェックポイントについては、『Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 5.x』を参照してください。

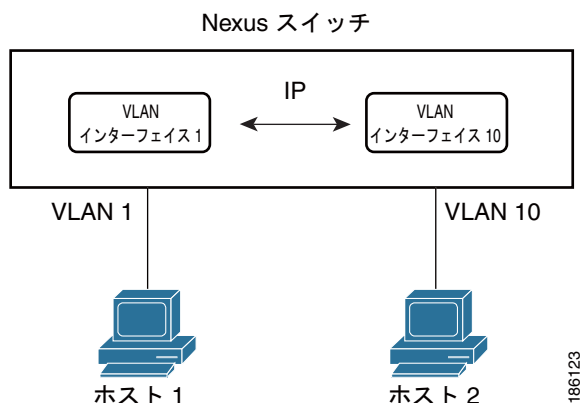


(注) VLAN 1 の VLAN インターフェイスは削除できません。

VLAN インターフェイスをルーティングするには、トラフィックをルーティングする VLAN ごとに VLAN インターフェイスを作成し、その VLAN インターフェイスに IP アドレスを割り当ててレイヤ 3 内部 VLAN ルーティングを実現します。IP アドレスと IP ルーティングの詳細については、『Cisco DCNM Unicast Routing Configuration Guide, Release 5.x』を参照してください。

図 4-2 に、2 つの VLAN に 2 つのホストが接続しているデバイスを示します。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 4-2 VLAN インターフェイスに接続した 2 つの VLAN



## ループバック インターフェイス

ループバック インターフェイスは、常にアップ状態にある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。VDC ごとに最大 1024 のループバック インターフェイスが設定できます。VDC には 0 ～ 1023 の番号が付いています。

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

## トンネル インターフェイス

Cisco DCNM は、IP トンネルとしてトンネル インターフェイスをサポートします。IP トンネルを使うと、同じレイヤまたは上位レイヤ プロトコルをカプセル化して、2 台のルータ間で作成されたトンネルを通じて IP の結果を転送できます。IP トンネルの詳細については、第 7 章「IP トンネルの設定」を参照してください。

## ハイ アベイラビリティ

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 7000 Series NX-OS High Availability and Redundancy Guide, Release 5.x』を参照してください。

## バーチャライゼーションのサポート

レイヤ3 インターフェイスは、Virtual Routing and Forwarding (VRF; 仮想ルーティング/転送) インスタンスをサポートします。VRF は Virtual Device Context (VDC; 仮想デバイス コンテキスト) 内に存在します。特に別の VDC や VRF を設定しない限り、デフォルトでは、Cisco NX-OS のデフォルトの VDC およびデフォルトの VRF が使用されます。ある VDC に設定されたレイヤ3 論理インターフェイス (VLAN インターフェイス、ループバック) は、同じ番号を持つ別の VDC に設定されたレイヤ3 論理インターフェイスとは区別されます。たとえば、VDC 1 のループバック 0 は VDC 2 のループバック 0 とは異なります。

VDC ごとに最大 1024 のループバック インターフェイスを設定できます。

このインターフェイスは VRF に関連付けることができます。VLAN インターフェイスの場合、VLAN と同じ VDC に設定する必要があります。

VDC については『Cisco DCNM Virtual Device Context Configuration Guide, Release 5.x』を、VRF でのインターフェイスの設定については『Cisco DCNM Unicast Routing Configuration Guide, Release 5.x』を参照してください。



(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。

## レイヤ3 インターフェイスのライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
DCNM	レイヤ3 インターフェイスにライセンスは必要ありません。
Cisco NX-OS	レイヤ3 インターフェイスにライセンスは必要ありません。ライセンス パッケージに含まれていない機能はすべて Cisco NX-OS システム イメージにバンドルされており、追加費用は一切発生しません。Cisco NX-OS のライセンス スキームの詳細については、『Cisco Nexus 7000 Series NX-OS Licensing Guide, Release 5.x』を参照してください。

## ライセンス3 インターフェイスの前提条件

ライセンス3 インターフェイスには次の前提条件があります。

- Advanced Services ライセンスをインストールしており、該当する VDC を開始している (VDC を設定する場合は、『Cisco DCNM Virtual Device Context Configuration Guide, Release 5.x』を参照してください)。
- 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 DCNM Unicast Routing Configuration Guide, Release 5.x』を参照してください。

## 注意事項および制約事項

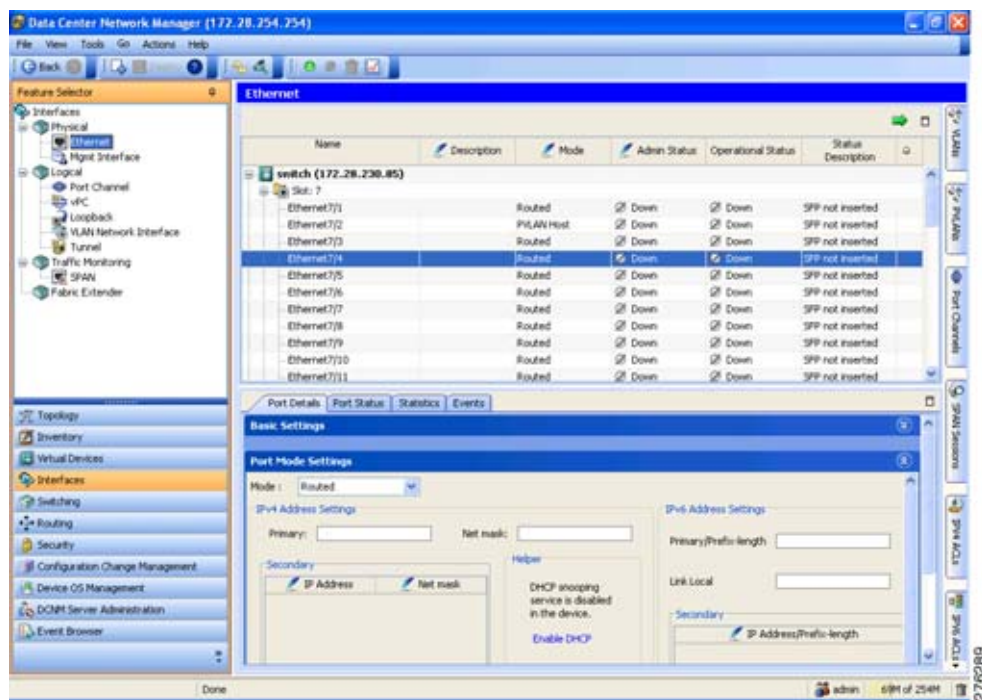
レイヤ3 インターフェイスの設定には次の注意事項と制約事項があります。

- レイヤ3 インターフェイスをレイヤ2 インターフェイスに変更する場合、Cisco NX-OS はインターフェイスをシャットダウンしてインターフェイスを再度イネーブルにし、レイヤ3 固有の設定をすべて削除します。
- レイヤ2 インターフェイスをレイヤ3 インターフェイスに変更する場合、Cisco NX-OS はインターフェイスをシャットダウンしてインターフェイスを再度イネーブルにし、レイヤ2 固有の設定をすべて削除します。

## レイヤ3 インターフェイスの設定

インターフェイス機能を選択すると、レイヤ3 インターフェイスにアクセスできます。図 4-3 に、レイヤ3 インターフェイスを示します。

図 4-3 レイヤ3 インターフェイスの設定



Data Center Network Manager の機能の詳細については、『Cisco DCNM Fundamentals Configuration Guide, Release 5.x』を参照してください。

ここでは、次の内容について説明します。

- 「ルーテッドインターフェイスの設定」 (P.4-7)
- 「IPv4 セカンダリ アドレスまたはヘルパー アドレスの設定」 (P.4-8)
- 「IPv6 セカンダリ アドレスの設定」 (P.4-9)
- 「サブインターフェイスの設定」 (P.4-9)
- 「サブインターフェイスの削除」 (P.4-11)
- 「ポート チャネル サブインターフェイスの作成」 (P.4-11)
- 「ポート チャネル サブインターフェイスの削除」 (P.4-12)
- 「インターフェイスでの帯域幅の設定」 (P.4-13)
- 「VLAN ネットワーク インターフェイスの設定」 (P.4-14)
- 「VLAN ネットワーク インターフェイスの削除」 (P.4-15)
- 「ループバック インターフェイスの設定」 (P.4-15)
- 「ループバック インターフェイスの削除」 (P.4-16)

## 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。

### 手順の詳細

ルーテッド インターフェイスを設定する手順は、次のとおりです。

- 
- |                |   |
|----------------|---|
| <b>ステップ 1</b>  | [Feature Selector] ペインで、[Interfaces] > [Physical] > [Ethernet] を選択します。<br>[Summary] ペインに使用可能なデバイスが表示されます (図 4-3 を参照)。               |
| <b>ステップ 2</b>  | [Summary] ペインで、スロットのリストに表示するデバイスをダブルクリックします。  |
| <b>ステップ 3</b>  | スロットをダブルクリックすると、インターフェイスのリストが表示されます。  |
| <b>ステップ 4</b>  | ルーテッド インターフェイスとして設定するインターフェイスをクリックします。<br>そのインターフェイスが [Summary] ペイン内で強調表示され、一連のタブが [Details] ペインに表示されます。                            |
| <b>ステップ 5</b>  | [Details] ペインの [Port Details] タブをクリックします。<br>[Port Details] タブが表示されます。  |
| <b>ステップ 6</b>  | [Port Details] タブの [Port Mode Settings] セクションを展開します。<br>ポート モードが表示されます。   |
| <b>ステップ 7</b>  | [Mode] ドロップダウン リストから [Routed] を選択します。<br>[Details] ペインに IP アドレス情報が表示され、NX-OS によってレイヤ 2 の設定が削除されます。                                  |
| <b>ステップ 8</b>  | (任意) [IPv4 Address Settings] の [Primary] フィールドで、このルーテッド インターフェイスの IPv4 アドレスを設定します。  |
| <b>ステップ 9</b>  | (任意) [Net mask] フィールドで、この IPv4 アドレスのネットワーク マスクをドット付き 10 進表記で設定します。  |
| <b>ステップ 10</b> | (任意) [IPv6 Address Settings] 領域の [Primary/Prefix-length] フィールドで、このルーテッド インターフェイスの IPv6 アドレスとプレフィックスの長さを設定します。<br>長さの範囲は 1 ~ 128 です。 |
| <b>ステップ 11</b> | (任意) EUI64 を設定するには、[EUI64] をオンにします。   |
| <b>ステップ 12</b> | (任意) [Link Local] フィールドで、リンクローカル IPv6 アドレスを入力します。   |
| <b>ステップ 13</b> | (任意) リンクローカル ルーティングのみに対してこのルーテッド インターフェイスを設定するには、[Use local only] をオンにします。  |
| <b>ステップ 14</b> | メニュー バーの [File] > [Deploy] を選択して、変更をデバイスに適用します。   |
-

## IPv4 セカンダリ アドレスまたはヘルパー アドレスの設定

インターフェイスのセカンダリ アドレスまたはヘルパー アドレスを設定できます。

### 手順の詳細

ルーテッド インターフェイスの IPv4 セカンダリ アドレスまたはヘルパー アドレスを設定するには、次の手順を実行します。

- 
- ステップ 1** [Feature Selector] ペインで、[Interfaces] > [Physical] > [Ethernet] を選択します。  
[Summary] ペインに使用可能なデバイスが表示されます (図 4-3 を参照)。
- ステップ 2** [Summary] ペインで、スロットのリストに表示するデバイスをダブルクリックします。
- ステップ 3** スロットをダブルクリックすると、インターフェイスのリストが表示されます。
- ステップ 4** ルーテッド インターフェイスとして設定するインターフェイスをクリックします。  
そのインターフェイスが [Summary] ペイン内で強調表示され、一連のタブが [Details] ペインに表示されます。
- ステップ 5** [Details] ペインの [Port Details] タブをクリックします。  
[Port Details] タブが表示されます。
- ステップ 6** [Port Details] タブの [Port Mode Settings] セクションを展開します。  
ポート モードが表示されます。
- ステップ 7** (任意) [IPv4 Address settings] セクションの [Secondary] 領域で、右クリックして [Add Secondary IP] を選択し、セカンダリ IP アドレスを追加します。
- ステップ 8** [Secondary] 領域の [IP address] フィールドで、IPv4 アドレスを入力します。
- ステップ 9** [Net mask] フィールドで、この IPv4 アドレスのネットワーク マスクをドット付き 10 進表記で入力します。
- ステップ 10** (任意) [IPv4 Address settings] セクションの [Helper] 領域で、右クリックして [Add Helper IP] を選択し、DHCP ヘルパー IP アドレスを追加します。
- ステップ 11** [Helper] 領域の [IP address] フィールドで、IPv4 アドレスを入力します。
- ステップ 12** メニュー バーの [File] > [Deploy] を選択して、変更をデバイスに適用します。
-

## IPv6 セカンダリ アドレスの設定

インターフェイスのセカンダリ アドレスまたはヘルパー アドレスを設定できます。

### 手順の詳細

ルーテッド インターフェイスの IPv6 セカンダリ アドレスを設定するには、次の手順を実行します。

- 
- |                |  |
|----------------|--|
| <b>ステップ 1</b>  | [Feature Selector] ペインで、[Interfaces] > [Physical] > [Ethernet] を選択します。<br>[Summary] ペインに使用可能なデバイスが表示されます（図 4-3 を参照）。 |
| <b>ステップ 2</b>  | [Summary] ペインで、スロットのリストに表示するデバイスをダブルクリックします。   |
| <b>ステップ 3</b>  | スロットをダブルクリックすると、インターフェイスのリストが表示されます。   |
| <b>ステップ 4</b>  | ルーテッド インターフェイスとして設定するインターフェイスをクリックします。<br>そのインターフェイスが [Summary] ペイン内で強調表示され、一連のタブが [Details] ペインに表示されます。             |
| <b>ステップ 5</b>  | [Details] ペインの [Port Details] タブをクリックします。<br>[Port Details] タブが表示されます。   |
| <b>ステップ 6</b>  | [Port Details] タブの [Port Mode Settings] セクションを展開します。<br>ポート モードが表示されます。  |
| <b>ステップ 7</b>  | [IPv6 Address settings] セクションの [Secondary] 領域で、右クリックして [Add IPv6 Address] を選択し、セカンダリ IPv6 アドレスを追加します。                |
| <b>ステップ 8</b>  | [IP Address/Prefix-length] フィールドで、このセカンダリ IPv6 アドレスの IPv6 アドレスとプレフィックスの長さを入力します。                                     |
| <b>ステップ 9</b>  | （任意）EUI64 を設定するには、[EUI64] をオンにします。   |
| <b>ステップ 10</b> | メニュー バーの [File] > [Deploy] を選択して、変更をデバイスに適用します。  |
- 

## サブインターフェイスの設定

ルーテッド インターフェイスまたはルーテッド インターフェイスで作成したポート チャネルに 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。

### 作業を開始する前に

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](#)」(P.4-7) を参照してください。

このポート チャネル上にサブインターフェイスを作成するには、ポート チャネル インターフェイスを作成します（「[ポート チャネルの設定](#)」(P.5-15) を参照）。

### 手順の詳細

ルーテッド インターフェイスでサブインターフェイスを作成するには、次の手順を実行します。

- 
- |               |  |
|---------------|--|
| <b>ステップ 1</b> | [Feature Selector] ペインで、[Interfaces] > [Physical] > [Ethernet] を選択します。 |
|---------------|--|

- [Summary] ペインに使用可能なデバイスが表示されます。
- ステップ 2** [Summary] ペインで、スロットのリストに表示するデバイスをダブルクリックします。
- ステップ 3** スロットをダブルクリックすると、インターフェイスのリストが表示されます。
- ステップ 4** サブインターフェイスを設定するインターフェイスをクリックします。  
そのインターフェイスが [Summary] ペイン内で強調表示され、一連のタブが [Details] ペインに表示されます。
- ステップ 5** メニュー バーの [Actions] > [Add Subinterface] を選択し、サブインターフェイスを作成します。  
[Summary] ペインでサブインターフェイスが強調表示され、[Details] ペインでタブが更新されます。
- ステップ 6** 強調表示されたサブインターフェイスのフィールドで、サブインターフェイス番号を入力します。  
有効な範囲は 1 ～ 4093 です。
- ステップ 7** [Details] ペインの [Port Details] タブをクリックします。  
[Port Details] タブが表示されます。
- ステップ 8** [Port Details] タブの [Basic Settings] セクションを展開します。  
[Details] ペインに基本インターフェイスの情報が表示されます。
- ステップ 9** (任意) [encapsulation] 領域の [Vlan Id] ドロップダウン リストで、このサブインターフェイスに関連付ける VLAN ID を選択します。
- ステップ 10** [Port Details] タブの [IP Address Settings] セクションを展開します。  
[Details] ペインに IP アドレスの情報が表示されます。
- ステップ 11** (任意) [IPv4 Address Settings] の [Primary] フィールドで、このサブインターフェイスの IPv4 アドレスを設定します。
- ステップ 12** (任意) [Net mask] フィールドで、この IPv4 アドレスのネットワーク マスクをドット付き 10 進表記で設定します。
- ステップ 13** (任意) [IPv6 Address Settings] 領域の [Primary/Prefix-length] フィールドで、このサブインターフェイスの IPv6 アドレスとプレフィックスの長さを設定します。  
長さの範囲は 1 ～ 128 です。
- ステップ 14** (任意) EUI64 を設定するには、[EUI64] をオンにします。
- ステップ 15** (任意) [Link Local] フィールドで、リンクローカル IPv6 アドレスを入力します。
- ステップ 16** (任意) リンクローカル ルーティングのみに対してこのサブインターフェイスを設定するには、[Use local only] をオンにします。
- ステップ 17** メニュー バーの [File] > [Deploy] を選択して、変更をデバイスに適用します。
-



## サブインターフェイスの削除

サブインターフェイスは削除できます。

### 手順の詳細

ルーテッド インターフェイスでサブインターフェイスを削除するには、次の手順を実行します。

- 
- |               |   |
|---------------|---|
| <b>ステップ 1</b> | [Feature Selector] ペインで、[Interfaces] > [Physical] > [Ethernet] を選択します。<br>[Summary] ペインに使用可能なデバイスが表示されます。 |
| <b>ステップ 2</b> | [Summary] ペインで、スロットのリストに表示するデバイスをダブルクリックします。  |
| <b>ステップ 3</b> | スロットをダブルクリックすると、インターフェイスのリストが表示されます。  |
| <b>ステップ 4</b> | サブインターフェイスを削除するインターフェイスをクリックします。<br>そのインターフェイスが [Summary] ペイン内で強調表示され、一連のタブが [Details] ペインに表示されます。        |
| <b>ステップ 5</b> | 削除するサブインターフェイスをクリックします。<br>[Summary] ペインでサブインターフェイスが強調表示されます。   |
| <b>ステップ 6</b> | メニュー バーの [Actions] > [Delete Subinterface] を選択し、サブインターフェイスを削除します。   |
| <b>ステップ 7</b> | メニュー バーの [File] > [Deploy] を選択して、変更をデバイスに適用します。   |
- 

## ポート チャネル サブインターフェイスの作成

ポート チャネル サブインターフェイスを作成できます。

### 手順の詳細

ポート チャネルでサブインターフェイスを作成するには、次の手順を実行します。

- 
- |               |  |
|---------------|--|
| <b>ステップ 1</b> | [Feature Selector] ペインで、[Interfaces] > [Logical] > [Port Channel] を選択します。<br>[Summary] ペインに使用可能なデバイスが表示されます。                             |
| <b>ステップ 2</b> | [Summary] ペインで、既存のポート チャネルのリストに表示するデバイスをダブルクリックします。  |
| <b>ステップ 3</b> | サブインターフェイスを設定するポート チャネルを右クリックし、[New] > [Subinterface] を選択します。<br>ポート チャネルのサブインターフェイスが [Summary] ペイン内で強調表示され、一連のタブが [Details] ペインに表示されます。 |
| <b>ステップ 4</b> | 強調表示されたチャネル ID のフィールドで、サブインターフェイス番号を入力します。<br>有効な範囲は 1 ～ 4093 です。  |
| <b>ステップ 5</b> | [Details] ペインの [Port Channels Details] タブをクリックします。<br>[Details] タブが表示されます。   |
| <b>ステップ 6</b> | [Details] タブの [Basic Settings] セクションを展開します。<br>[Details] ペインに基本インターフェイスの情報が表示されます。   |

- ステップ 7** (任意) [VLAN ID] ドロップダウン リストで、このサブインターフェイスに関連付ける VLAN ID を選択します。
- ステップ 8** [Details] タブの [IP Address Settings] セクションを展開します。  
[Details] ペインに IP アドレスの情報が表示されます。
- ステップ 9** (任意) [IPv4 Address Settings] の [IP Address] フィールドで、このサブインターフェイスの IPv4 アドレスを設定します。
- ステップ 10** (任意) [Net Mask] フィールドで、この IPv4 アドレスのネットワーク マスクをドット付き 10 進表記で設定します。
- ステップ 11** (任意) [IPv6 Address Settings] 領域の [Primary/Prefix-length] フィールドで、このサブインターフェイスの IPv6 アドレスとプレフィックスの長さを設定します。  
長さの範囲は 1 ~ 128 です。
- ステップ 12** (任意) EUI64 を設定するには、[EUI64] をオンにします。
- ステップ 13** (任意) [Link Local] フィールドで、リンクローカル IPv6 アドレスを入力します。
- ステップ 14** (任意) リンクローカル ルーティングのみに対してこのサブインターフェイスを設定するには、[Use local only] をオンにします。
- ステップ 15** メニュー バーの [File] > [Deploy] を選択して、変更をデバイスに適用します。

## ポート チャネル サブインターフェイスの削除

ポート チャネル サブインターフェイスを削除できます。

### 手順の詳細

ポート チャネルでサブインターフェイスを削除するには、次の手順を実行します。

- ステップ 1** [Feature Selector] ペインで、[Interfaces] > [Logical] > [Port Channel] を選択します。  
[Summary] ペインに使用可能なデバイスが表示されます。
- ステップ 2** [Summary] ペインで、ポート チャネルのリストに表示するデバイスをダブルクリックします。
- ステップ 3** サブインターフェイスを削除するポート チャネルをクリックします。  
そのインターフェイスが [Summary] ペイン内で強調表示され、一連のタブが [Details] ペインに表示されます。
- ステップ 4** 削除するサブインターフェイスをクリックします。  
[Summary] ペインでサブインターフェイスが強調表示されます。
- ステップ 5** メニュー バーの [Actions] > [Delete] を選択し、サブインターフェイスを削除します。
- ステップ 6** メニュー バーの [File] > [Deploy] を選択して、変更をデバイスに適用します。

## インターフェイスでの帯域幅の設定

ルーテッド インターフェイス、ポート チャネル、またはサブインターフェイスに帯域幅を設定できます。上位レイヤ プロトコルは帯域幅パラメータを使用してパス コストを計算します。サブインターフェイスの帯域幅は、次のいずれかの方法で設定できます。

- 明示的：サブインターフェイスの帯域幅を直接設定します。
- 継承：サブインターフェイスが固有の値として、つまり親インターフェイスの帯域幅を親インターフェイスから継承するように帯域幅を設定します。

サブインターフェイスの帯域幅を設定しない場合、または親インターフェイスの帯域幅を継承しない場合、サブインターフェイスの帯域幅は次の方法で決定されます。

- 親インターフェイスがアップしている場合、サブインターフェイスの帯域幅は親インターフェイスの動作速度と同じです。ポートの場合、サブインターフェイスの帯域幅は設定されているリンク速度またはネゴシエート対象のリンク速度です。ポート チャネルの場合、サブインターフェイスの帯域幅は、ポート チャネルの各メンバのリンク速度の集合です。
- 親インターフェイスがダウンしている場合、サブインターフェイスの帯域幅は親インターフェイスのタイプによって異なります。
  - ポート チャネル サブインターフェイスの場合、サブインターフェイスの帯域幅は 100 Mb/s です。
  - 1 Gb/s イーサネット ポートの場合、サブインターフェイスの帯域幅は 1 Gb/s です。
  - 10 Gb/s イーサネット ポートの場合、サブインターフェイスの帯域幅は 10 Gb/s です。

### 手順の詳細

インターフェイスの帯域幅を設定するには、次の手順を実行します。

- 
- ステップ 1** [Feature Selector] ペインで、[Interfaces] > [Physical] > [Ethernet] を選択します。  
[Summary] ペインに使用可能なデバイスが表示されます（図 4-3 を参照）。
  - ステップ 2** [Summary] ペインで、スロットのリストに表示するデバイスをダブルクリックします。
  - ステップ 3** スロットをダブルクリックすると、インターフェイスのリストが表示されます。
  - ステップ 4** 帯域幅を設定するインターフェイスをクリックします。  
そのインターフェイスが [Summary] ペイン内で強調表示され、一連のタブが [Details] ペインに表示されます。
  - ステップ 5** [Details] ペインの [Port Details] タブをクリックします。  
[Port Details] タブが表示されます。
  - ステップ 6** [Port Details] タブの [Basic Settings] セクションを展開します。  
基本設定が表示されます。
  - ステップ 7** [Bandwidth (kb)] フィールドで、帯域幅の値を入力します。
  - ステップ 8** メニュー バーの [File] > [Deploy] を選択して、変更をデバイスに適用します。
-

## VLAN ネットワーク 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。

### 手順の詳細

VLAN ネットワーク インターフェイスを作成するには、次の手順を実行します。

- 
- |                |   |
|----------------|---|
| <b>ステップ 1</b>  | [Feature Selector] ペインで、[Interfaces] > [Logical] > [VLAN Network Interface] を選択します。<br>[Summary] ペインに使用可能なデバイスが表示されます。                            |
| <b>ステップ 2</b>  | [Summary] ペインで、既存の VLAN ネットワーク インターフェイスのリストを表示するデバイスをダブルクリックします。  |
| <b>ステップ 3</b>  | [Details] ペインに [Enable VLAN Network Interface Service] リンクが表示されている場合、これをクリックします。  |
| <b>ステップ 4</b>  | メニュー バーの、[Actions] > [New] > [Add VLAN Network Interface] を選択します。<br>新しい VLAN ネットワーク インターフェイスが [Summary] ペイン内で強調表示され、一連のタブが [Details] ペインに表示されます。 |
| <b>ステップ 5</b>  | 強調表示された VLAN ネットワーク インターフェイスのフィールドで、VLAN ネットワーク インターフェイス番号を入力します。<br>number の範囲は 1 ～ 4094 です。   |
| <b>ステップ 6</b>  | [Details] ペインの [Details] タブをクリックします。<br>[Details] タブが表示されます。  |
| <b>ステップ 7</b>  | [Details] タブの [IP Address Settings] セクションを展開します。<br>[Details] ペインに IP アドレスの情報が表示されます。   |
| <b>ステップ 8</b>  | (任意) [IPv4 Address Settings] の [Primary] フィールドで、この VLAN ネットワーク インターフェイスの IPv4 アドレスを設定します。   |
| <b>ステップ 9</b>  | (任意) [Net Mask] フィールドで、この IPv4 アドレスのネットワーク マスクをドット付き 10 進表記で設定します。  |
| <b>ステップ 10</b> | (任意) [IPv6 Address Settings] 領域の [Primary/Prefix-length] フィールドで、この VLAN ネットワーク インターフェイスの IPv6 アドレスとプレフィックスの長さを設定します。<br>長さの範囲は 1 ～ 128 です。        |
| <b>ステップ 11</b> | (任意) EUI64 を設定するには、[EUI64] をオンにします。   |
| <b>ステップ 12</b> | (任意) [Link Local] フィールドで、リンクローカル IPv6 アドレスを入力します。   |
| <b>ステップ 13</b> | (任意) リンクローカル ルーティングのみに対してこの VLAN ネットワーク インターフェイスを設定するには、[Use local only] をオンにします。   |
| <b>ステップ 14</b> | メニュー バーの [File] > [Deploy] を選択して、変更をデバイスに適用します。   |
-

## VLAN ネットワーク インターフェイスの削除

VLAN ネットワーク インターフェイスは削除できます。

### 手順の詳細

VLAN ネットワーク インターフェイスを削除するには、次の手順を実行します。

- 
- |               |  |
|---------------|--|
| <b>ステップ 1</b> | [Feature Selector] ペインで、[Interfaces] > [Logical] > [VLAN Network Interface] を選択します。<br>[Summary] ペインに使用可能なデバイスが表示されます。 |
| <b>ステップ 2</b> | [Summary] ペインで、既存の VLAN ネットワーク インターフェイスのリストを表示するデバイスをダブルクリックします。   |
| <b>ステップ 3</b> | 削除する VLAN ネットワーク インターフェイスをクリックします。<br>VLAN ネットワーク インターフェイスが [Summary] ペイン内で強調表示され、一連のタブが [Details] ペインに表示されます。         |
| <b>ステップ 4</b> | メニュー バーの [Actions] > [Delete VLAN Network Interface] を選択して、この VLAN ネットワーク インターフェイスを削除します。                              |
| <b>ステップ 5</b> | メニュー バーの [File] > [Deploy] を選択して、変更をデバイスに適用します。  |
- 

## 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。

### 作業を開始する前に

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

### 手順の詳細

ループバック インターフェイスを作成するには、次の手順を実行します。

- 
- |               |   |
|---------------|---|
| <b>ステップ 1</b> | [Feature Selector] ペインで、[Interfaces] > [Logical] > [Loopback] を選択します。<br>[Summary] ペインに使用可能なデバイスが表示されます。                                |
| <b>ステップ 2</b> | [Summary] ペインで、既存のループバック インターフェイスのリストに表示するデバイスをダブルクリックします。  |
| <b>ステップ 3</b> | メニュー バーの、[Actions] > [New] > [Add Loopback Interface] を選択します。<br>新しいループバック インターフェイスが [Summary] ペイン内で強調表示され、一連のタブが [Details] ペインに表示されます。 |
| <b>ステップ 4</b> | 強調表示されたループバックのフィールドで、ループバック番号を入力します。<br>number の範囲は 1 ～ 4094 です。  |
| <b>ステップ 5</b> | [Details] ペインの [Details] タブをクリックします。<br>[Details] タブが表示されます。  |

- ステップ 6** [Details] タブの [IP Address Settings] セクションを展開します。  
[Details] ペインに IP アドレスの情報が表示されます。
- ステップ 7** (任意) [IPv4 Address Settings] の [Primary] フィールドで、このループバック インターフェイスの IPv4 アドレスを設定します。
- ステップ 8** (任意) [Net Mask] フィールドで、この IPv4 アドレスのネットワーク マスクをドット付き 10 進表記で設定します。
- ステップ 9** (任意) [IPv6 Address Settings] 領域の [Primary/Prefix-length] フィールドで、このループバック インターフェイスの IPv6 アドレスとプレフィックスの長さを設定します。  
長さの範囲は 1 ～ 128 です。
- ステップ 10** (任意) EUI64 を設定するには、[EUI64] をオンにします。
- ステップ 11** (任意) [Link Local] フィールドで、リンクローカル IPv6 アドレスを入力します。
- ステップ 12** (任意) リンクローカル ルーティングのみに対してこのループバック インターフェイスを設定するには、[Use local only] をオンにします。
- ステップ 13** メニュー バーの [File] > [Deploy] を選択して、変更をデバイスに適用します。

## ループバック インターフェイスの削除

ループバック インターフェイスは削除できます。

### 手順の詳細

ループバック インターフェイスを削除するには、次の手順を実行します。

- ステップ 1** [Feature Selector] ペインで、[Interfaces] > [Logical] > [Loopback] を選択します。  
[Summary] ペインに使用可能なデバイスが表示されます。
- ステップ 2** [Summary] ペインで、既存のループバック インターフェイスのリストに表示するデバイスをダブルクリックします。
- ステップ 3** 削除するループバック インターフェイスをクリックします。  
ループバック インターフェイスが [Summary] ペイン内で強調表示され、一連のタブが [Details] ペインに表示されます。
- ステップ 4** メニュー バーの [Actions] > [Delete Loopback Interface] を選択して、このループバック インターフェイスを削除します。
- ステップ 5** メニュー バーの [File] > [Deploy] を選択して、変更をデバイスに適用します。

## レイヤ3 インターフェイス統計情報の表示

レイヤ3 インターフェイス統計情報を収集するように DCNM を設定できます。[Feature Selector] ページで、[Interfaces] を選択し、統計情報を収集するインターフェイスに移動します。

[Statistics] タブに次のウィンドウが表示されます。

- Port Traffic Statistics : 入力および出力（パケットおよびバイト）カウンタ、ブロードキャスト、マルチキャスト、およびユニキャスト トラフィックを収集します。
- Port Error Statistics : (物理ポートのみ) インターフェイスのさまざまなエラー統計情報を収集します。

レイヤ3 インターフェイスの統計情報収集の詳細については、『Cisco DCNM Fundamentals Configuration Guide, Release 5.x』を参照してください。

## 関連項目

レイヤ3 インターフェイスの詳細については、次の項目を参照してください。

- [第5章「ポート チャネルの設定」](#)
- 『Cisco DCNM Unicast Routing Configuration Guide, Release 5.x』

## レイヤ3 インターフェイスのフィールドの説明

ここでは、レイヤ3 インターフェイスの次のフィールドについて説明します。

- 「[ルーテッド インターフェイス](#)」(P.4-17)
- 「[ループバック](#)」(P.4-17)
- 「[VLAN ネットワーク インターフェイス](#)」(P.4-19)

### ルーテッド インターフェイス

ルーテッド インターフェイスのフィールドの説明については、[第2章「基本インターフェイス パラメータの設定」](#)に記載されています。

### ループバック

ここでは、ループバック インターフェイスの次のフィールドについて説明します。

- 「[\[Loopback\] : \[Details\] タブ : \[Basic Settings\] セクション](#)」(P.4-18)
- 「[\[Loopback\] : \[Details\] タブ : \[IP Address Settings\] セクション](#)」(P.4-18)
- 「[\[Loopback\] : \[Statistics\] タブ](#)」(P.4-18)
- 「[VLAN ネットワーク インターフェイス](#)」(P.4-19)

## [Loopback] : [Details] タブ : [Basic Settings] セクション

表 4-1 [Loopback] : [Details] : [Basic Settings]

フィールド	説明
Name	表示のみ。ループバック インターフェイスの名前。
Description	ループバック インターフェイスを説明する文字列。
Admin Status	ループバック インターフェイスの管理ステータス。デフォルトは up です。

## [Loopback] : [Details] タブ : [IP Address Settings] セクション

表 4-2 [Loopback] : [Details] : [IP Address Settings]

フィールド	説明
<b>IPv4 Address Settings</b>	
Primary	ドット付き 10 進表記の IPv4 アドレス。
Net Mask	ドット付き 10 進表記の IPv4 アドレスのネットワーク マスク。
Secondary IP Address	ドット付き 10 進表記のセカンダリ IPv4 アドレス。1 つのインターフェイスに対して複数のセカンダリ アドレスを設定できます。
Secondary NetMask	ドット付き 10 進表記のセカンダリ IPv4 アドレスのネットワーク マスク。
Helper IP Address	User Datagram Protocol (UDP; ユーザ データグラム プロトコル) ブロードキャストの転送をイネーブルにするために使用される DHCP ヘルパー アドレス。
<b>IPv6 Address Settings</b>	
Primary/Prefix-length	x:x:x::x/length 形式の IPv6 プレフィクス。
EUI64	Extended Universal Identifier (EUI) -64 形式の IPv6 アドレス。
Link Local	x:x:x::x 形式の IPv6 リンク ローカル アドレス。
Use local only	リンク ローカル アドレスは、自動的に生成された IPv6 アドレスより優先されます。
Secondary IP Address/Prefix Length	x:x:x::x/length 形式のセカンダリ IPv6 プレフィクス。1 つのインターフェイスに対して複数のセカンダリ アドレスを設定できます。
EUI64	Extended Universal Identifier (EUI) -64 形式のセカンダリ IPv6 アドレス。

## [Loopback] : [Statistics] タブ

表 4-3 [Loopback] : [Statistics] タブ

フィールド	説明
Status	統計情報の収集のステータス。[Status] にマウスのカーソルを合わせると、ポップアップのヒントが表示されます。
Select Parameters	ループバック インターフェイスで収集できる統計情報のリスト。
Show Overview Chart	統計情報の概要のポップアップ。



## VLAN ネットワーク インターフェイス

- ここでは、VLAN ネットワーク インターフェイスの次のフィールドについて説明します。
- 「[VLAN Network Interface] : [Details] タブ : [Basic Settings] セクション」 (P.4-19)
- 「[VLAN Network Interface] : [Details] タブ : [IP Address Settings] セクション」 (P.4-19)
- 「[VLAN Network Interface] : [Statistics] タブ」 (P.4-20)

### [VLAN Network Interface] : [Details] タブ : [Basic Settings] セクション

表 4-4 [VLAN Network Interface] : [Details] : [Basic Settings]

フィールド	説明
Name	表示のみ。VLAN ネットワーク インターフェイスの名前。
Admin Status	VLAN ネットワーク インターフェイスの管理ステータス。デフォルトは up です。
MTU (bytes)	最大伝送ユニット。デフォルト値は 1500 です。
Description	VLAN ネットワーク インターフェイスを説明する文字列。
Delay (tens of usecs)	インターフェイス スループット遅延で、単位は 10 マイクロ秒です。デフォルト値は 1 (単位は 10 マイクロ秒) です。
Oper Status	キャリア遅延タイマーで、単位は秒またはミリ秒です。デフォルト値は 2 秒です。
Carrier Delay	VLAN ネットワーク インターフェイスの動作ステータス。
Bandwidth (kb)	VLAN ネットワーク インターフェイスのインターフェイス帯域幅で、単位はキロバイトです。デフォルト値は 100000 です。

### [VLAN Network Interface] : [Details] タブ : [IP Address Settings] セクション

表 4-5 [VLAN Network Interface] : [Details] : [IP Address Settings]

フィールド	説明
<b>IPv4 Address Settings</b>	
Primary	ドット付き 10 進表記の IPv4 アドレス。
Net mask	ドット付き 10 進表記の IPv4 アドレスのネットワーク マスク。
Secondary IP Address	ドット付き 10 進表記のセカンダリ IPv4 アドレス。1 つのインターフェイスに対して複数のセカンダリ アドレスを設定できます。
Secondary NetMask	ドット付き 10 進表記のセカンダリ IPv4 アドレスのネットワーク マスク。
Helper IP Address	User Datagram Protocol (UDP; ユーザ データグラム プロトコル) ブロードキャストの転送をイネーブルにするために使用されるヘルパー アドレス。
<b>IPv6Address 設定</b>	
Primary/Prefix-length	x::x::x/length 形式の IPv6 プレフィクス。
EUI64	Extended Universal Identifier (EUI) -64 形式の IPv6 アドレス。
Link Local	x::x::x 形式の IPv6 リンク ローカル アドレス。
Use local only	リンク ローカルアドレスは、自動的に生成された IPv6 アドレスより優先されます。
Secondary IP Address/Prefix Length	x::x::x/length 形式のセカンダリ IPv6 プレフィクス。1 つのインターフェイスに対して複数のセカンダリ アドレスを設定できます。
EUI64	Extended Universal Identifier (EUI) -64 形式のセカンダリ IPv6 アドレス。

## [VLAN Network Interface] : [Statistics] タブ

表 4-6 [VLAN Network Interface] : [Statistics] タブ

フィールド	説明
Status	統計情報の収集のステータス。[Status] にマウスのカーソルを合わせると、ポップアップのヒントが表示されます。
Select Parameters	VLAN ネットワーク インターフェイスで収集できる統計情報のリスト。
Show Overview Chart	統計情報の概要のポップアップ。

## その他の関連資料

レイヤ 3 インターフェイスの実装に関する追加情報については、次の項を参照してください。

- 「関連資料」(P.4-20)
- 「管理情報ベース (MIB)」(P.4-20)
- 「標準規格」(P.4-20)

## 関連資料

関連項目	参照先
コマンド構文	『Cisco Nexus 7000 Series NX-OS Interfaces Command Reference, Release 5.x』
IP	『Cisco DCNM Unicast Routing Configuration Guide, Release 5.x』の「Configuring IP」の章
VLAN	『Cisco DCNM Layer 2 Switching Configuration Guide, Release 5.x』の「Configuring VLANs」の章

## 管理情報ベース (MIB)

管理情報ベース (MIB)	MIB リンク
<ul style="list-style-type: none"> <li>• IF-MIB</li> <li>• CISCO-IF-EXTENSION-MIB</li> <li>• ETHERLIKE-MIB</li> </ul>	Management Information Base (MIB; 管理情報ベース) を検索およびダウンロードするには、次の URL にアクセスしてください。 <a href="http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml">http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</a>

## 標準規格

標準規格	タイトル
この機能でサポートされる新規または改訂された標準規格はありません。また、この機能による既存の標準規格サポートの変更はありません。	—

## レイヤ 3 インターフェイス設定の機能履歴

表 4-7 は、この機能のリリースの履歴です。

表 4-7 レイヤ 3 インターフェイス設定の機能履歴

機能名	リリース	機能情報
レイヤ 3 インターフェイス	4.0(1)	この機能が導入されました。
SVI	4.0(3)	DCNM 全体およびすべてのマニュアルで VLAN ネットワーク インターフェイスに変更されました。





## CHAPTER 5

# ポート チャネルの設定

この章では、ポート チャネルを設定し、Cisco Nexus 7000 シリーズ NX-OS でポート チャネルをより有効に利用するために Link Aggregation Control Protocol (LACP) を適用して設定する手順を説明します。

Data Center Network Manager の機能とポート チャネルでの [Topology] タブの使用の詳細については、『Cisco DCNM Fundamentals Configuration Guide, Release 5.x』を参照してください。



(注)

管理対象デバイス上で実行される Cisco NX-OS リリースでは、この章で説明する機能や設定がすべてサポートされるとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースのマニュアルとリリース ノートを参照してください。



(注)

ポート チャネル機能に対するシステム メッセージのログ レベルは、Cisco DCNM の要件以上でなければなりません。デバイス検出時に、ログ レベルが不十分であることが検出された場合は、最低限必要なレベルまで Cisco DCNM によって引き上げられます。ただし、Cisco Nexus 7000 シリーズ スイッチで Cisco NX-OS Release 4.0 を実行する場合は例外です。Cisco NX-OS Release 4.0 の場合は、デバイス検出の前に、コマンドライン インターフェイスを使用してログ レベルを Cisco DCNM の要件以上となるように設定してください。詳細については、『Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 5.x』を参照してください。

この章では、次の内容について説明します。

- 「ポート チャネルについて」 (P.5-2)
- 「ポート チャネリングのライセンス要件」 (P.5-13)
- 「ポート チャネリングの前提条件」 (P.5-14)
- 「注意事項および制約事項」 (P.5-14)
- 「ポート チャネルの設定」 (P.5-15)
- 「統計情報の表示」 (P.5-30)
- 「ポート チャネリングと LACP のフィールドの説明」 (P.5-31)
- 「その他の関連資料」 (P.5-37)
- 「ポート チャネル設定の機能履歴」 (P.5-38)

## ポート チャンネルについて

ポート チャン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 チャンネルに最大 8 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。また、ポート チャンネルでは、これらの集約された各物理インターフェイス間でトラフィックのロード バランシングも行います。ポート チャンネルの物理インターフェイスが少なくとも 1 つ動作していれば、そのポート チャンネルは動作しています。

レイヤ 2 ポート チャン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 チャンネルを作成できます。レイヤ 3 ポート チャン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 チャンネルを作成できます。レイヤ 3 ポート チャンネルを作成したら、ポート チャンネル インターフェイスに IP アドレスを追加してレイヤ 3 ポート チャンネルにサブインターフェイスを作成できます。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 チャンネルで組み合わせることはできません。

Cisco NX-OS Release 4.2 から、ポート セキュリティをポート チャンネルに適用できます（ポート セキュリティの詳細については、『Cisco DCNM Security Configuration Guide, Release 5.x』を参照してください）。

ポート チャンネル内のすべてのポートは同じデバイス内にある必要があり、複数のデバイスにまたがってポート チャンネルを設定することはできません。

ポート チャンネルをレイヤ 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手順については、[第 3 章「レイヤ 2 インターフェイスの設定」](#)を参照してください。

変更した設定をポート チャンネルに適用すると、そのポート チャンネルのメンバ インターフェイスにもそれぞれ変更が適用されます。たとえば、Spanning Tree Protocol (STP; スパニング ツリー プロトコル) パラメータをポート チャンネルに設定すると、Cisco DC-OS ソフトウェアはこれらのパラメータをポート チャンネルのそれぞれのインターフェイスに適用します。



(注)

レイヤ 2 ポートがポート チャン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 チャン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 チャンネル メンバに適用できません。レイヤ 3 の設定を各ポート チャンネル メンバに適用できません。設定をポート チャンネル全体に適用する必要があります。

サブインターフェイスが論理ポート チャンネル インターフェイスの一部であっても、レイヤ 3 ポート チャンネルにサブインターフェイスを作成できます。ポート チャンネル サブインターフェイスの詳細については、[「サブインターフェイス」\(P.4-2\)](#)を参照してください。

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 チャン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。

LACP については、[を参照してください](#)。

ここでは、次の内容について説明します。

- [「ポート チャンネル」\(P.5-3\)](#)
- [「ポート チャンネル インターフェイス」\(P.5-4\)](#)
- [「基本設定」\(P.5-4\)](#)
- [「互換性要件」\(P.5-5\)](#)
- [「ポート チャンネルを使ったロード バランシング」\(P.5-6\)](#)
- [「LACP」\(P.5-8\)](#)
- [「バーチャライゼーションのサポート」\(P.5-12\)](#)
- [「ハイ アベイラビリティ」\(P.5-13\)](#)

## ポート チャンネル

ポート チャンネルは物理リンクをチャンネル グループにバンドルして単一の論理リンクを作成し、最大 8 つの物理リンクからなる集約帯域幅を実現します。ポート チャンネルのメンバ ポートが故障すると、それまでに故障したリンクで伝送されたトラフィックはポート チャンネルに残っている他のメンバ ポートに切り替えます。

最大 8 つのポートをスタティック ポート チャンネルにバンドルできます。集約プロトコルは使用しません。ただし、LACP をイネーブルにすればポート チャンネルをより柔軟に使用できます。LACP を使ってポート チャンネルを設定する場合とスタティック ポート チャンネルを使って設定する場合では、手順が多少異なります（「[ポート チャンネルの設定](#)」(P.5-15) を参照）。



(注) デバイスのポート チャンネルは Port Aggregation Protocol (PAgP) をサポートしません。

各ポートにはポート チャンネルが 1 つだけあります。ポート チャン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](#)」(P.5-5) を参照）。集約プロトコルを使わずにスタティック ポート チャン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 チャンネル モード](#)」(P.5-9) を参照）。

ポート チャンネル インターフェイスを作成すると、ポート チャン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 チャンネルがない場合は対応するポート チャンネルが自動的に作成されます。この場合、ポート チャン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 チャンネルを作成することもできます。この場合は、Cisco DC-OS ソフトウェアがポート チャン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](#)」(P.5-5) を参照）。ポート チャンネル サブインターフェイスの作成と削除の詳細については、[第 4 章「レイヤ 3 インターフェイスの設定](#)」を参照してください。

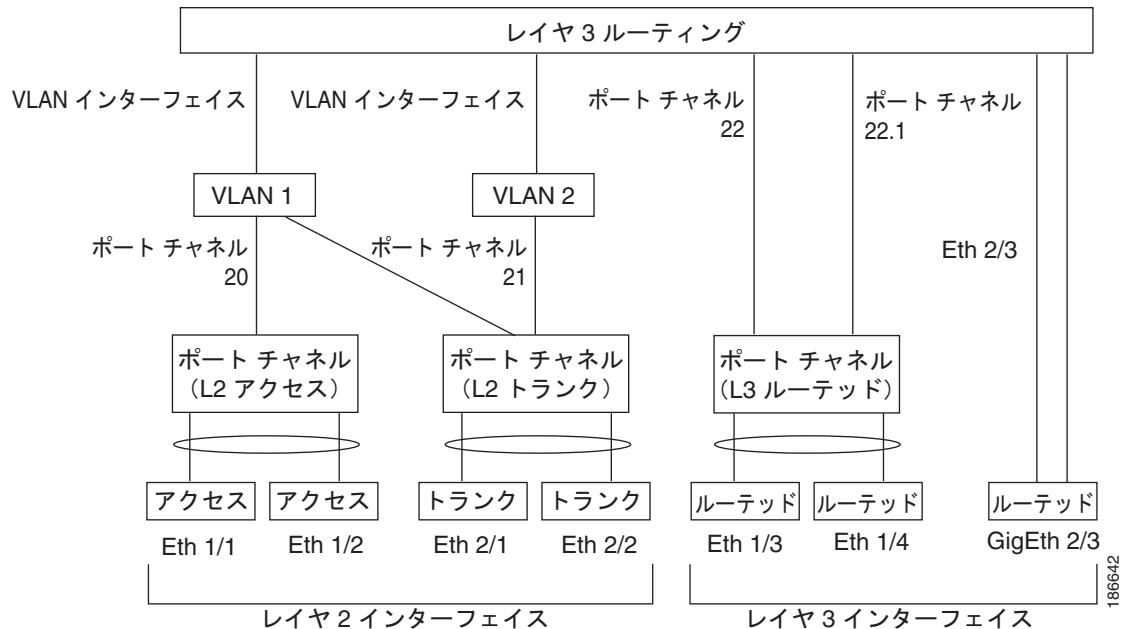


(注) 少なくともメンバ ポートの 1 つがアップしており、そのポートのチャンネルが有効であれば、ポート チャンネルはアップしています。メンバ ポートがすべてダウンしていれば、ポート チャンネルはダウンしています。

## ポート チャンネル インターフェイス

図 5-1 に、ポート チャンネル インターフェイスを示します。

図 5-1 ポート チャンネル インターフェイス



ポート チャンネル 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 チャンネルはアクセス 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 チャンネル 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、場合によってはサブインターフェイスもあります。

Cisco NX-OS Release 4.2(1) から、スタティック Media Access Control (MAC; メディア アクセス制御) アドレスを使用してレイヤ 3 ポート チャンネルを設定できます。この値を設定しない場合、レイヤ 3 ポート チャンネルは、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 チャンネルでのスタティック MAC アドレス設定については、『Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide, Release 5.x』を参照してください。

レイヤ 2 ポートにアクセスまたはトランク モードを設定する手順については、第 3 章「レイヤ 2 インターフェイスの設定」を参照してください。レイヤ 3 インターフェイスとサブインターフェイスを設定する手順については、第 4 章「レイヤ 3 インターフェイスの設定」を参照してください。

## 基本設定

ポート チャンネル インターフェイスには次の基本設定ができます。

- 説明
- デュプレックス
- IP アドレス : IPv4 および IPv6
- 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、ソフトウェアは特定のインターフェイス属性をチェックし、インターフェイスがチャネル グループと互換性があることを確認します。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 DC-OS ソフトウェアはインターフェイスの多数の動作属性をチェックしてから、その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容します。

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 レイヤ
- (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
- タグ付きまたはタグなし
- 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
- レイヤ 3 ポート : サブインターフェイスは不可
- ストーム制御
- フロー制御性能
- フロー制御設定

チャネル モード セットを **on** に設定したインターフェイスだけをスタティック ポート チャネルに追加できます。また、チャネル モードを **active** または **passive** に設定したインターフェイスだけを、LACP を実行するポート チャネルに追加できます (ポート チャネル モードの詳細については、「[LACP Marker Responder](#)」(P.5-11) を参照してください)。これらの属性は、個々のメンバ 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 (v4 および v6)
- 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
- Quality of Service (QoS)
- Access Control List (ACL; アクセス コントロール リスト)

インターフェイスがポート チャン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
- デバウンス
- UDLD
- MDIX
- レート モード
- シャットダウン
- SNMP トラップ

ポート チャンネル インターフェイスにサブインターフェイスを設定し、ポート チャンネルのメンバ ポートを削除すると、ポート チャンネル サブインターフェイスの設定はメンバ ポートに伝わりません。



(注)

ポート チャンネルを削除すると、すべてのメンバ インターフェイスはポート チャンネルから削除されたかのように設定されます。

## ポート チャンネルを使ったロード バランシング

Cisco DC-OS ソフトウェアは、フレームのアドレスを数値にハッシュしてチャンネルのリンクを 1 つ選択することで、ポート チャンネルの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。ポート チャン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 チャンネル ロード バランシングは、MAC アドレス、IP アドレスを使用します。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 チャンネル 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、デバイス全体または指定したモジュールに設定したすべてのポート チャンネルに適用することができます。モジュールごとの設定はデバイス全体のロード バランシング設定に優先されます。デバイス全体に 1 つのロード バランシング モードを、指定したモジュールに別のモードを、さらに別の指定したモジュールに別のモードを設定できます。ポート チャンネルごとにロード 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 ポートを決めます。



(注)

レイヤ 3 インターフェイスのデフォルト ロード バランシング モードは、発信元および宛先 IP アドレスです。非 IP インターフェイスのデフォルト 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。

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 チャンネル全体をロード 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

非 IP およびレイヤ 3 ポート チャン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。

ロード バランシングは、VDC とは無関係に、システム全体または特定のモジュールによって設定できます。ポート チャンネルのロード バランシングは、すべての VDC にわたるグローバル設定です。

入トラフィックが Multiprotocol Label Switching (MPLS; マルチプロトコル ラベル スイッチング) の場合、ソフトウェアはパケットの IP アドレスのラベルの下位部分を参照します。

ポート チャンネルを使用するロード バランシング アルゴリズムは、マルチキャスト トラフィックには適用されません。設定したロード バランシング アルゴリズムにかかわらず、マルチキャスト トラフィックは次の方式を使用してポート チャンネルのロード 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、単一メンバの障害時に、**port-channel hash-distribution** コマンドを実行することで、メンバ ポートの ASIC の動作を最適化できました。Cisco Nexus 7000 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であれ、モジュール単位であれ、**port-channel load-balance ethernet** コマンドによるポート チャンネル上のロード バランシング基準のカスタマイズをサポートしません。

# LACP

LACP では、最大 16 のインターフェイスを 1 つのポート チャンネルに設定できます。最大 8 つのインターフェイスをアクティブに、最大 8 つのインターフェイスをスタンバイ ステートにできます。

ここでは、次の内容について説明します。

- 「[LACP の概要](#)」 (P.5-8)
- 「[ポート チャンネル モード](#)」 (P.5-9)
- 「[LACP ID パラメータ](#)」 (P.5-10)
- 「[LACP Marker Responder](#)」 (P.5-11)
- 「[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](#)」 (P.5-12)
- 「[LACP 互換性の拡張](#)」 (P.5-12)

## LACP の概要



(注)

---

LCAP 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。

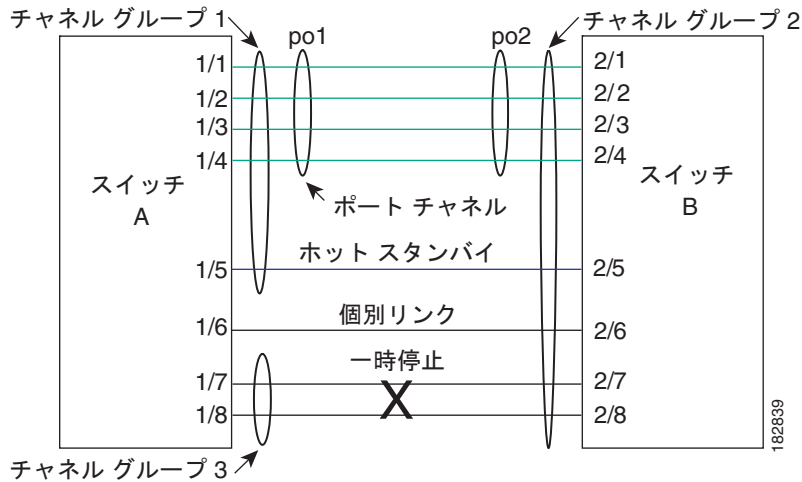
---

LACP をイネーブルにする手順については「[LACP のイネーブル化](#)」 (P.5-24) を参照してください。

Cisco NX-OS Release 4.2 から、システムは機能のディセーブル化の前に自動的にチェックポイントを作成するため、このチェックポイントにロールバックできます。ロールバックとチェックポイントについては、『*Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 5.x*』を参照してください。

図 5-2 に、個別リンクを LACP ポート チャンネルおよびチャンネル グループに組み込み、個別リンクとして機能させる方法を示します。

図 5-2 個別リンクをポート チャンネルに組み込む



LACP では、最大 16 のインターフェイスを 1 つのチャンネル グループにバンドルできます。チャンネル グループのインターフェイスが 8 つよりも多い場合、残りのインターフェイスは、このチャンネル グループに関連付けられたポート チャンネルのホットスタンバイとなります。



(注)

ポート チャンネルを削除すると、ソフトウェアは関連付けられたチャンネル 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 設定が有効な場合は LACP をディセーブルにできません。

## ポート チャンネル モード

ポート チャンネルの個別インターフェイスは、チャンネル モードで設定します。スタティック ポート チャンネルを集約プロトコルを使用せずに実行すると、チャンネル モードは常に **on** に設定されます。

デバイス上で LACP をグローバルにイネーブルにした後、各インターフェイスのチャンネル モードを **active** または **passive** に設定して、各チャンネルの LACP をイネーブルにします。チャンネル グループにリンクを追加すると、LACP チャンネル グループの個別リンクにいずれかのチャンネル モードを設定できます。



(注)

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

表 5-1 で、各チャネル モードについて説明します。

表 5-1 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
<b>passive</b>	LACP モード。ポートをパッシブ ネゴシエーション ステートにします。ポートは受信した LACP パケットには応答しますが、LACP ネゴシエーションは開始しません。
<b>active</b>	LACP モード。ポートをアクティブ ネゴシエーション ステートにします。ポートは LACP パケットを送信して、他のポートとのネゴシエーションを開始します。
<b>on</b>	すべてのスタティック ポート チャネル（LACP を実行していない）がこのモードです。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と、デバイス表示はエラー メッセージを表示します。  各チャネルで LACP をイネーブルにするには、そのチャネルのインターフェイスでチャネル モードを <b>active</b> または <b>passive</b> に設定します。LACP は、 <b>on</b> 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。そのため、LACP チャネル グループには参加しません。  デフォルト ポート チャネル モードは <b>on</b> 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、ポート速度やトラッキング 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、ポートは LACP ポート チャネルを形成できます。

- **active** モードのポートは、**active** モードの別のポートとともにポート チャネルを正しく形成できます。
- **active** モードのポートは、**passive** モードの別のポートとともにポート チャネルを形成できます。
- **passive** モードのポートは、どちらのポートもネゴシエーションを開始しないため、**passive** モードの別のポートとともにポート チャネルを形成できません。
- **on** モードのポートは LACP を実行しておらず、**active** または **passive** モードの別のポートとともにポート チャネルを形成できません。

## LACP ID パラメータ

ここでは、LACP パラメータについて次の内容を説明します。

- 「LACP システム プライオリティ」(P.5-10)
- 「LCAP ポート プライオリティ」(P.5-11)
- 「LACP 管理キー」(P.5-11)

## 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の値である 32768 を適用することも、1 ～ 65535 の値を設定することもできます。LACP はシステム プライオリティに MAC アドレスを使用してシステム ID を形成します。また、他のデバイスとのネゴシエーション中にもシステム プライオリティを使用します。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。

システム ID は VDC ごとに異なります。



(注) LACP のシステム 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。

## LCAP 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。LACP ポート プライオリティに、デフォルト値である 32768 を適用することも、1 ~ 65535 の値を設定することもできます。LACP はポート番号とともにポート プライオリティを使用して、ポート ID を形成します。

互換性のあるすべてのポートを集約できない制限がある場合、LACP はポート プライオリティを使用して、スタンバイ モードにする必要があるポートを決定し、アクティブ モードにすべきポートを指定します。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。管理キーは、他のポートと集約されるポートの機能を定義します。他のポートと集約されるポート機能は、次の要因によって決まります。

- ポートの物理特性。データ レートやデブ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 Marker Responder

ポート チャン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、フレームの秩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 チャンネル リンクごとに Marker PDUS 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 チャン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 チャンネルとスタティック ポート チャンネルの相違点

表 5-2 に、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 チャンネルの主な相違点を示します。

表 5-2 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

設定	LACP がイネーブルのポート チャンネル	スタティック ポート チャンネル
適用されるプロトコル	グローバルにイネーブル	適用不可
リンクのチャンネルモード	次のいずれかです。 <ul style="list-style-type: none"> <li>Active</li> <li>Passive</li> </ul>	On だけ
チャンネルの最大リンク数	16	8

## LACP 互換性の拡張

相互運用性の解決、および LACP プロトコル収束の高速化のために複数の新しいコマンドがリリース 4.2(3) に追加されました。

Cisco Nexus 7000 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、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。これらの状況を解決するために、**lacp graceful-convergence** コマンドが追加されました。

デフォルトで、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。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。**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。

## バーチャライゼーションのサポート

メンバ ポートと他のポート チャンネルに関連する設定は、ポート チャンネルとメンバ ポートを持つ Virtual Device Context (VDC; 仮想デバイス コンテキスト) で設定します。すべての VDC 間に最大 256 のポート チャンネルを設定できます。各 VDC で 1 ~ 4096 の番号を使ってポート チャンネルに番号を設定できます。異なる VDC に同じポート チャンネル番号を使用できます。たとえば、VDC1 にポート チャンネル 100 を設定し、VDC2 の別のポート チャンネルにも 100 を設定できます。

ただし、LACP システム ID は VDC ごとに異なります。LACP の詳細については、「[LACP の概要 \(P.5-8\)](#)」を参照してください。



(注)

VDC およびリソースの割り当ての詳細については、『*Cisco DCNM Virtual Device Context Configuration Guide, Release 5.x*』を参照してください。

1 つのポート チャンネルのすべてのポートと VLAN は同じ VDC である必要があります。LACP を使用する場合、最大 8 つのアクティブ ポートと最大 8 つのスタンバイ ポートは同じ VDC である必要があります。ポート チャンネルはグローバルに作成されるので、ポート チャンネルにメンバ ポートを設定する



前に、それぞれの VDC に割り当てるメンバ ポートを確認する必要があります。ポート チャンネルは 1 つの VDC から始まり（そのチャンネルのすべてのポートが同じ VDC）、別の VDC のポート チャンネルに対応します（この場合もそのチャンネルのすべてのポートは同じ VDC）。



(注)

ポートチャネリング ロード バランシング モードは、単一のモジュールまたはモジュール全体で動作します。デフォルト VDC のポート チャン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。指定した VDC のポート チャンネルを使用してロード バランシングを設定することはできません。ロード バランシングの詳細については、「[ポート チャンネルを使ったロード バランシング](#)」(P.5-6) を参照してください。

## ハイ アベイラビリティ

ポート チャンネルは、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 チャンネルのメンバがアクティブであればポート チャン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 チャンネルを作成できます。

ポート チャンネルは、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 DC-OS ソフトウェアは実行時の設定を適用します。



(注)

ハイ アベイラビリティ機能の詳細については、『*Cisco Nexus 7000 Series NX-OS High Availability and Redundancy Guide, Release 5.x*』を参照してください。

## ポート チャネリングのライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
DCNM	ポート チャネリングにライセンスは必要ありません。ライセンス パッケージに含まれていない機能は Cisco DCNM にバンドルされており、無料で使用できます。
Cisco NX-OS	ポート チャネリングにライセンスは必要ありません。ライセンス パッケージに含まれていない機能はすべて Cisco NX-OS システム イメージにバンドルされており、追加費用は一切発生しません。NX-OS のライセンス スキームの詳細については、『 <i>Cisco Nexus 7000 Series NX-OS Licensing Guide, Release 5.x</i> 』を参照してください。

ただし、VDC を使用する場合は Advanced Services ライセンスが必要です。

## 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。
- DCNM を使用してポート チャネルを設定する前に、デバイスのコマンドラインで NX-OS グローバル コマンド **logging-level port-channel 6** を入力して、ログ レベルを設定する必要があります。ログ レベルの詳細については、『*Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 5.x*』を参照してください。
- 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。互換性の要件の詳細については、「[互換性要件](#)」(P.5-5) 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。

## 注意事項および制約事項

ポート チャネリングには次の注意事項と制約事項があります。

- 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。
- 冗長スーパーバイザ エンジン上のポートも含め、すべてのモジュール上のすべてのイーサネットポートは、ポート チャネル（最大 8 つのアクティブ ポートを持つ）をサポートします。これらのポートは、物理的に隣接しているポートでなくても、また同じモジュール上のポートでなくてもかまいません。
- 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（共有および専用ポートについては、[第 2 章「基本インターフェイス パラメータの設定」](#)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。
- STP では、ポート チャネル バンドルはシングル ポートと見なされます。この場合のポート コストは、そのチャネルに割り当てられているすべての設定されたポート コストの合計です。
- 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 チャネルにポートを追加する前に、ポートセキュリティ情報をそのポートから削除しておく必要があります。同様に、チャネル グループのメンバであるポートにポートセキュリティ情報を追加できません。
- 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 チャンネルの設定



(注)

ポート チャンネルでの Topology 機能の使用方法の詳細については、『*Cisco DCNM Fundamentals Configuration Guide, Release 5.x*』を参照してください。

ここでは、次の内容について説明します。

- 「ポート チャンネルの作成」 (P.5-16)
- 「ポート チャンネルの削除」 (P.5-17)
- 「レイヤ 2 ポートをポート チャンネルに追加」 (P.5-18)
- 「レイヤ 3 ポートをポート チャンネルに追加」 (P.5-19)
- 「ポート チャンネルからのポートの削除」 (P.5-20)
- 「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」 (P.5-20)
- 「ポートをポート チャンネルに強制的に参加」 (P.5-21)
- 「ポート チャンネルへの CDP リンクの追加」 (P.5-21)
- 「ポート チャンネルへのリンクの削除」 (P.5-22)
- 「ポート チャンネルの説明の設定」 (P.5-22)
- 「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」 (P.5-23)
- 「ポート チャンネルを使ったロード バランシングの設定」 (P.5-24)
- 「LACP のイネーブル化」 (P.5-24)
- 「LACP ポート チャンネル ポート モードの設定」 (P.5-25)
- 「LACP システム プライオリティの設定」 (P.5-26)
- 「LACP ポート プライオリティの設定」 (P.5-26)
- 「LACP グレースフル コンバージェンス」 (P.5-27)
- 「LACP の個別一時停止のディセーブル化」 (P.5-29)

## ポート チャンネルの作成

チャンネル グループを作成する前に、ポート チャンネルを作成します。関連するチャンネル グループは自動的に作成されます。

### 作業を開始する前に

LACP ベースのポート チャンネルにする場合は LACP をイネーブルにします。

正しいデバイスで操作していることを確認します（または [Feature Selector] ペインから [Virtual Devices] を選択）。

[Port Channel] パネルを使用して、ポート チャンネルを作成します。またはレイヤ 3 のポート チャンネルとは別に、スイッチド、またはレイヤ 2 のポート チャンネルを作成します。

### 手順の詳細

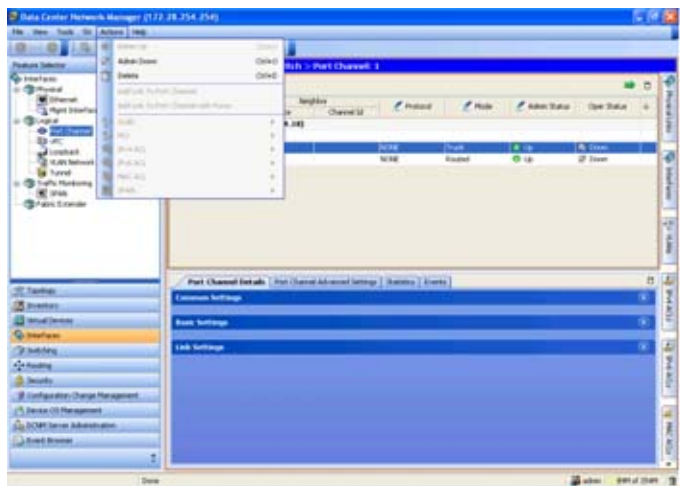
ポート チャンネルを作成するには、次の手順を実行します。

- 
- |               |   |
|---------------|---|
| <b>ステップ 1</b> | [Feature Selector] ペインで、[Interfaces] > [Logical] > [Port Channel] を選択し、[Port Channel] ペインを開きます。     |
| <b>ステップ 2</b> | [Contents] ペインの [Summary] ペインで、ポート チャンネルを作成するデバイスをクリックします。<br>該当するデバイスが強調表示されます。                    |
| <b>ステップ 3</b> | メニュー バーで [New] > [Switched Port Channel] を選択し、レイヤ 2 ポート チャンネルを作成します。<br>新しく作成されたポート チャンネルの行が追加されます。 |
| <b>ステップ 4</b> | メニュー バーで [New] > [Routed Port Channel] を選択し、レイヤ 3 ポート チャンネルを作成します。<br>新しく作成されたポート チャンネルの行が追加されます。   |
| <b>ステップ 5</b> | [Channel ID] に数値を入力します。   |
| <b>ステップ 6</b> | (任意) メニュー バーで [File] > [Deploy] を選択して変更をデバイスに適用します。   |
-

## ポート チャネルの削除

[Port Channel] ペインを使用して、ポート チャネルを削除します（図 5-3 を参照）。

図 5-3 ポート チャネルの削除



### 手順の詳細

ポート チャネルを削除するには、次の手順を実行します。

- ステップ 1** [Feature Selector] ペインで、[Interfaces] > [Logical] > [Port Channel] を選択し、[Port Channel] ペインを開きます。
- ステップ 2** [Contents] ペインの [Summary] ペインで、ポート チャネルを削除するデバイスをダブルクリックします。  
該当するデバイスが強調表示されます。
- ステップ 3** 削除するポート チャネルをクリックします。  
該当するポート チャネルが強調表示されます。
- ステップ 4** メニュー バーで [Actions] > [Delete] を選択します。
- ステップ 5** (任意) メニュー バーで [File] > [Deploy] を選択して変更をデバイスに適用します。

## レイヤ 2 ポートをポート チャンネルに追加

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。

### 作業を開始する前に

LACP ベースのポート チャンネルにする場合は 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。

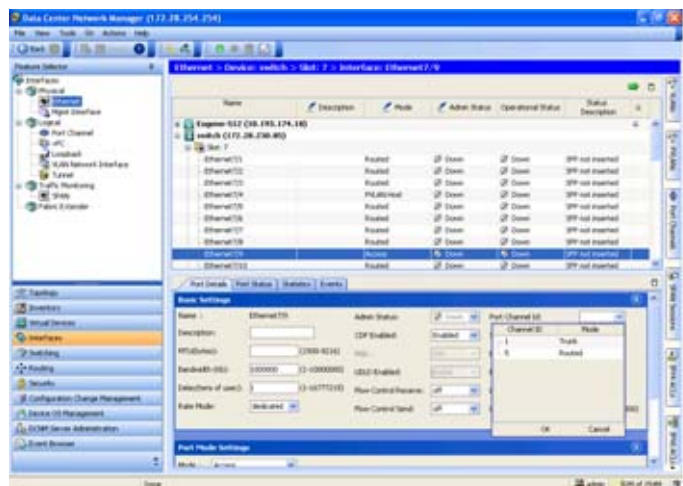


(注)

特定のポート チャンネルに特定のインターフェイスを追加できない場合、互換性の問題を示すエラー メッセージが表示されます。

[Ethernet] ペインを使用して、レイヤ 2 ポートをスイッチドポート チャンネルに追加します (図 5-4 を参照)。

図 5-4 ポートの追加



### 手順の詳細

レイヤ 2 インターフェイスをスイッチドポート チャンネルに追加するには、次の手順を実行します。

- ステップ 1** [Feature Selector] ペインで [Interfaces] > [Physical] > [Ethernet] を選択して [Ethernet] ペインを開きます。
- ステップ 2** [Summary] ペインの [Contents] ペインで、デバイスをダブルクリックしてインターフェイスを表示します。
- ステップ 3** スロットをクリックすると、インターフェイスのリストが表示されます。
- ステップ 4** インターフェイスをクリックします。  
そのインターフェイスが [Summary] ペイン内で強調表示され、一連のタブが [Details] ペインに表示されます。
- ステップ 5** [Details] ペインの [Port Details] タブをクリックします。
- ステップ 6** [Basic Settings] セクションをクリックします。
- ステップ 7** [Port Channel Id] ドロップダウン リストで、レイヤ 2 ポートを追加するスイッチドポート チャンネルを選択します。
- ステップ 8** [OK] をクリックします。
- ステップ 9** (任意) メニュー バーで [File] > [Deploy] を選択して変更をデバイスに適用します。

## レイヤ 3 ポートをポート チャンネルに追加

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。

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 チャン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 チャンネルを作成したら、ポート チャンネル 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。また、既存のレイヤ 3 ポート チャンネルにサブインターフェイスを追加できます。

### 作業を開始する前に

LACP ベースのポート チャンネルにする場合は 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。

[Ethernet] ペインを使用して、レイヤ 3 ポートをルーテッド ポート チャンネルに追加します (図 5-4 を参照)。

### 手順の詳細

ルーテッド ポートをルーテッド ポート チャンネルに追加するには、次の手順を実行します。

- 
- ステップ 1** [Feature Selector] ペインで [Interfaces] > [Physical] > [Ethernet] を選択して [Ethernet] ペインを開きます。
  - ステップ 2** [Summary] ペインの [Contents] ペインで、デバイスをダブルクリックしてインターフェイスを表示します。
  - ステップ 3** スロットをクリックすると、インターフェイスのリストが表示されます。
  - ステップ 4** インターフェイスをクリックします。  
そのインターフェイスが [Summary] ペイン内で強調表示され、一連のタブが [Details] ペインに表示されます。
  - ステップ 5** [Details] ペインの [Port Details] タブをクリックします。
  - ステップ 6** [Port Mode Settings] セクションをクリックします。
  - ステップ 7** IP アドレス情報を削除します。
  - ステップ 8** [Basic Settings] セクションをクリックします。
  - ステップ 9** [Port Channel Id] ドロップダウン リストで、ルーテッド ポートを追加するルーテッド ポート チャンネルを選択します。
  - ステップ 10** [OK] をクリックします。
  - ステップ 11** (任意) メニュー バーで [File] > [Deploy] を選択して変更をデバイスに適用します。
- 

(IP アドレスの割り当てとサブインターフェイスの追加の詳細については、第 4 章「レイヤ 3 インターフェイスの設定」を参照してください)。

## ポート チャネルからのポートの削除

[Port Channel] ペインを使用して、ポート チャネルからポートを削除します（図 5-3 を参照）。

### 手順の詳細

ポート チャネルからポートを削除するには、次の手順を実行します。

- 
- |               |   |
|---------------|---|
| <b>ステップ 1</b> | [Feature Selector] ペインで、[Interfaces] > [Logical] > [Port Channel] を選択し、[Port Channel] ペインを開きます。 |
| <b>ステップ 2</b> | [Contents] ペインの [Summary] ペインで、ポート チャネルを表示するデバイスをダブルクリックします。                                    |
| <b>ステップ 3</b> | ポートを削除するポート チャネルをクリックします。<br>ポート チャネルが [Summary] ペイン内で強調表示され、一連のタブが [Details] ペインに表示されます。       |
| <b>ステップ 4</b> | [Details] ペインの [Port Channel Details] タブをクリックします。   |
| <b>ステップ 5</b> | [Link Settings] セクションをクリックします。  |
| <b>ステップ 6</b> | 削除するポートをクリックします。  |
| <b>ステップ 7</b> | メニュー バーで [Actions] > [Delete] を選択し、ポート チャネルからポートを削除します。   |
| <b>ステップ 8</b> | (任意) メニュー バーで [File] > [Deploy] を選択して変更をデバイスに適用します。   |
- 

## 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上ダウンします。

[Port Channel] ペインを使用して、ポート チャネル インターフェイスを管理的にアップまたはダウンするように設定します（図 5-3 を参照）。

### 手順の詳細

ポート チャネル インターフェイスを管理的にアップまたはダウンするように設定するには、次の手順を実行します。

- 
- |               |   |
|---------------|---|
| <b>ステップ 1</b> | [Feature Selector] ペインで、[Interfaces] > [Logical] > [Port Channel] を選択し、[Port Channel] ペインを開きます。 |
| <b>ステップ 2</b> | [Contents] ペインの [Summary] ペインで、ポート チャネルを表示するデバイスをダブルクリックします。                                    |
| <b>ステップ 3</b> | 操作するポート チャネルをクリックします。<br>ポート チャネルが [Summary] ペイン内で強調表示され、一連のタブが [Details] ペインに表示されます。           |
| <b>ステップ 4</b> | [Details] ペインの [Port Channel Details] タブをクリックします。   |
| <b>ステップ 5</b> | [Common Settings] セクションをクリックします。  |
| <b>ステップ 6</b> | [Admin Status] ドロップダウン リストで [Up] または [Down] を選択します。<br>デフォルトの設定は [Up] です。                       |
| <b>ステップ 7</b> | (任意) メニュー バーで [File] > [Deploy] を選択して変更をデバイスに適用します。   |
-



## ポートをポート チャネルに強制的に参加

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

### 手順の詳細

ポート チャネルにポートを強制的に参加させるように設定するには、次の手順を実行します。

- 
- |               |   |
|---------------|---|
| <b>ステップ 1</b> | [Feature Selector] ペインで、[Interfaces] > [Logical] > [Port Channel] を選択し、[Port Channel] ペインを開きます。 |
| <b>ステップ 2</b> | [Contents] ペインの [Summary] ペインで、ポート チャネルを表示するデバイスをダブルクリックします。                                    |
| <b>ステップ 3</b> | 操作するポート チャネルをクリックします。<br>ポート チャネルが [Summary] ペイン内で強調表示され、一連のタブが [Details] ペインに表示されます。           |
| <b>ステップ 4</b> | [Associated Panes] の [Interfaces] タブを選択します。<br>タブが開かれ、デバイスとインターフェイスが表示されます。                     |
| <b>ステップ 5</b> | ポート チャネルへの参加を強制するポートを選択します。   |
| <b>ステップ 6</b> | メニュー バーで [Actions] > [Add Port to Port Channel with Force] を選択します。                              |
| <b>ステップ 7</b> | (任意) メニュー バーで [File] > [Deploy] を選択して変更をデバイスに適用します。   |
- 

## ポート チャネルへの CDP リンクの追加

Cisco Discovery Protocol (CDP) リンクを強制または強制せずにポート チャネルに追加できます。

### 作業を開始する前に

CDP リンクが存在している必要があります。

### 手順の詳細

ポート チャネルにポートを強制的に参加させるように設定するには、次の手順を実行します。

- 
- |               |   |
|---------------|---|
| <b>ステップ 1</b> | [Feature Selector] ペインで、[Interfaces] > [Logical] > [Port Channel] を選択し、[Port Channel] ペインを開きます。 |
| <b>ステップ 2</b> | [Contents] ペインの [Summary] ペインで、ポート チャネルを表示するデバイスをダブルクリックします。                                    |
| <b>ステップ 3</b> | 操作するポート チャネルをクリックします。<br>ポート チャネルが [Summary] ペイン内で強調表示され、一連のタブが [Details] ペインに表示されます。           |

- ステップ 4** [Associated Panes] の [Physical Links] タブを選択します。  
タブが開かれ、ポート チャネルへの物理リンクが表示されます。
- ステップ 5** ポート チャネルに追加する 1 つまたは複数のリンクを選択します。
- ステップ 6** メニュー バーで [Actions] > [Add Link Port Channel] を選択します。  
DCNM ソフトウェアによって、[Port Channel Details] タブの [Link Settings] セクションで、ローカルポートまたはネイバー ポートとして物理リンクのいずれかの側にポートが追加されます。
- ステップ 7** (任意) メニュー バーで [Actions] > [Add Link Port Channel with Force] を選択します。
- ステップ 8** (任意) メニュー バーで [File] > [Deploy] を選択して変更をデバイスに適用します。

## ポート チャネルへのリンクの削除

ポート チャネルへのリンクを削除できます。

### 手順の詳細

ポート チャネルへのリンクを削除するには、次の手順を実行します。

- ステップ 1** [Feature Selector] ペインで、[Interfaces] > [Logical] > [Port Channel] を選択し、[Port Channel] ペインを開きます。
- ステップ 2** [Contents] ペインの [Summary] ペインで、ポート チャネルを表示するデバイスをダブルクリックします。
- ステップ 3** 操作するポート チャネルをクリックします。  
ポート チャネルが [Summary] ペイン内で強調表示され、一連のタブが [Details] ペインに表示されます。
- ステップ 4** [Port Channels Details] タブをクリックします。
- ステップ 5** [Link Settings] セクションをクリックします。  
セクションが展開され、選択したポート チャネルへのすべてのリンクが表示されます。
- ステップ 6** 削除するリンクをクリックします。
- ステップ 7** 右クリックし、[Delete] を選択します。
- ステップ 8** (任意) メニュー バーで [File] > [Deploy] を選択して変更をデバイスに適用します。

## 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。

[Port Channel] ペインを使用して、ポート チャネル インターフェイスの説明を追加または変更します (図 5-3 を参照)。

### 手順の詳細

ポート チャネル インターフェイスの説明を設定するには、次の手順を実行します。

- 
- ステップ 1** [Feature Selector] ペインで、[Interfaces] > [Logical] > [Port Channel] を選択し、[Port Channel] ペインを開きます。
- ステップ 2** [Contents] ペインの [Summary] ペインで、ポートチャネルを表示するデバイスをダブルクリックします。
- ステップ 3** 操作するポートチャネルをクリックします。  
ポートチャネルが [Summary] ペイン内で強調表示され、一連のタブが [Details] ペインに表示されます。
- ステップ 4** [Details] ペインの [Port Channel Details] タブをクリックします。
- ステップ 5** [Basic Settings] セクションをクリックします。
- ステップ 6** [Local Device:switch] 領域で、[Description] 行をダブルクリックし、説明を追加または変更します。  
デフォルトは空白です。
- ステップ 7** (任意) メニューバーで [File] > [Deploy] を選択して変更をデバイスに適用します。
- 

## 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。

[Port Channel] ペインを使用して、ポートチャネルインターフェイスの速度とデュプレックスの設定を行います (図 5-3 を参照)。

### 手順の詳細

ポートチャネルインターフェイスの速度とデュプレックスを設定するには、次の手順を実行します。

- 
- ステップ 1** [Feature Selector] ペインで、[Interfaces] > [Logical] > [Port Channel] を選択し、[Port Channel] ペインを開きます。
- ステップ 2** [Contents] ペインの [Summary] ペインで、ポートチャネルを表示するデバイスをダブルクリックします。
- ステップ 3** 操作するポートチャネルをクリックします。  
ポートチャネルが [Summary] ペイン内で強調表示され、一連のタブが [Details] ペインに表示されます。
- ステップ 4** [Details] ペインの [Port Channel Details] タブをクリックします。
- ステップ 5** [Basic Settings] セクションをクリックします。
- ステップ 6** [Local Device:switch] 領域で、[Speed setting] をダブルクリックして、速度を設定します。
- ステップ 7** ドロップダウンリストから必要な速度を選択します。
- ステップ 8** [Local Device:switch] 領域で、[Duplex setting] をダブルクリックして、デュプレックスを設定します。
- ステップ 9** ドロップダウンリストから必要なデュプレックス設定を選択します。
- ステップ 10** (任意) メニューバーで [File] > [Deploy] を選択して変更をデバイスに適用します。
-

## ポート チャンネルを使ったロード バランシングの設定

ポート チャンネルのロード 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 のモジュールだけに適用します。モジュールベースのロード バランシングは、デバイスベースのロード バランシングに優先します。

[Port Channel] ペインを使用して、ポート チャンネルを使用したロード バランシングを設定します。

### 手順の詳細

ポート チャンネルを使用したロード バランシングを設定するには、次の手順を実行します。

- 
- |               |  |
|---------------|--|
| <b>ステップ 1</b> | [Feature Selector] ペインで、[Interfaces] > [Logical] > [Port Channel] を選択し、[Port Channel] ペインを開きます。<br><br>そのデバイスが [Contents] ペイン内で表示され、一連のタブが [Details] ペインに表示されます。           |
| <b>ステップ 2</b> | [Contents] ペインの [Summary] ペインで、目的のデバイスをクリックします。<br><br>[Details] ペインにタブが表示されます。  |
| <b>ステップ 3</b> | [Details] ペインの [Configuration] タブをクリックします。   |
| <b>ステップ 4</b> | [Load Balancing Algorithm] ドロップダウン リストから目的のロード バランシング方式を選択します。<br><br>レイヤ 2 ポート チャンネルのデフォルトは [Source Destination MAC] で、レイヤ 3 ポート チャンネルのデフォルトは [Source Destination IP] です。 |
| <b>ステップ 5</b> | (任意) [Network Card Loadbalance Settings] 領域で、ロード バランシングを設定するシャーシ内の他のモジュールの行をクリックします。   |
| <b>ステップ 6</b> | (任意) [Load Balancing Algorithm] フィールドで、他のモジュールのロード バランシング方式を選択します。<br><br>ステップ 5 と 6 を繰り返して、シャーシ内の他のモジュールのロード バランシング方式を設定します。  |
| <b>ステップ 7</b> | (任意) メニュー バーで [File] > [Deploy] を選択して変更をデバイスに適用します。  |
- 

## LACP のイネーブル化

LACP はデフォルトでディセーブルです。LACP 設定を開始する前に 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 チャンネルとしてまとめます。次に、ポート チャン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。

[Port Channel] ペインを使用して、LACP 機能をイネーブルにします。

### 手順の詳細

LACP をイネーブルにするには、次の手順を実行します。

- 
- |               |   |
|---------------|---|
| <b>ステップ 1</b> | [Feature Selector] ペインで、[Interfaces] > [Logical] > [Port Channel] を選択し、[Port Channel] ペインを開きます。 |
| <b>ステップ 2</b> | [Contents] ペインの [Summary] ペインで、デバイスをクリックします。  |

- ステップ 3** メニュー バーで [Actions] > [Enable LACP Service] を選択します。  
デフォルトはディセーブルです。
- ステップ 4** (任意) LACP をディセーブルにするには、メニュー バーで [Actions] > [Enable LACP Service] を選択します。
- ステップ 5** (任意) メニュー バーで [File] > [Deploy] を選択して変更をデバイスに適用します。
- 

## 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ネル モードを **active** または **passive** に設定できます。このチャネル コンフィギュレーション モードを使えば、LACP でリンクを許容できます。

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** チャネル モードを維持します。

[Port Channel] ペインを使用して LACP チャネル モードを設定します (図 5-3 を参照)。

### 手順の詳細

LACP チャネル モードを設定するには、次の手順を実行します。

- 
- ステップ 1** [Feature Selector] ペインで、[Interfaces] > [Logical] > [Port Channel] を選択し、[Port Channel] ペインを開きます。
- ステップ 2** [Contents] ペインの [Summary] ペインで、ポート チャネルを表示するデバイスをダブルクリックします。  
そのデバイスが [Summary] ペイン内で強調表示され、一連のタブが [Details] ペインに表示されます。
- ステップ 3** ポート チャネルをクリックします。  
ポート チャネルが [Summary] ペイン内で強調表示され、一連のタブが [Details] ペインに表示されます。
- ステップ 4** [Port Channel Details] タブをクリックします。
- ステップ 5** [Link Settings] セクションをクリックします。  
ポート チャネルに個々のリンクが表示されます。
- ステップ 6** 設定するリンクをクリックします。
- ステップ 7** [Ports (switch)] 領域の [Mode] フィールドをクリックし、ドロップダウン リストから [Active] または [Passive] を選択します。
- ステップ 8** (任意) メニュー バーで [File] > [Deploy] を選択して変更をデバイスに適用します。
-

## LACP システム プライオリティの設定

LACP のシステム 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。

### 作業を開始する前に

LACP をイネーブルにします。

[Port Channel] ペインを使用して、LACP システム プライオリティを設定します。

### 手順の詳細

LACP システム プライオリティを設定するには、次の手順を実行します。

- 
- |               |   |
|---------------|---|
| <b>ステップ 1</b> | [Feature Selector] ペインで、[Interfaces] > [Logical] > [Port Channel] を選択し、[Port Channel] ペインを開きます。 |
| <b>ステップ 2</b> | [Contents] ペインの [Summary] ペインで、デバイスをクリックします。  |
| <b>ステップ 3</b> | [Details] ペインの [Configuration] タブをクリックします。  |
| <b>ステップ 4</b> | [LACP System Priority] フィールドで、システム ID の値を入力します。<br>デフォルト値は 32768 です。                            |
| <b>ステップ 5</b> | (任意) メニュー バーで [File] > [Deploy] を選択して変更をデバイスに適用します。   |
- 

## 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 チャンネルにそれぞれのリンクを設定できます。

### 作業を開始する前に

LACP をイネーブルにします。

[Port Channel] ペインを使用して、LACP ポート プライオリティを設定します (図 5-3 を参照)。

### 手順の詳細

LACP ポート プライオリティを設定するには、次の手順を実行します。

- 
- |               |   |
|---------------|---|
| <b>ステップ 1</b> | [Feature Selector] ペインで、[Interfaces] > [Logical] > [Port Channel] を選択し、[Port Channel] ペインを開きます。                             |
| <b>ステップ 2</b> | [Contents] ペインの [Summary] ペインで、ポート チャンネルを表示するデバイスをダブルクリックします。<br>そのデバイスが [Summary] ペイン内で強調表示され、一連のタブが [Details] ペインに表示されます。 |
| <b>ステップ 3</b> | ポート チャンネルをクリックします。<br>ポート チャンネルが [Summary] ペイン内で強調表示され、一連のタブが [Details] ペインに表示されます。   |
| <b>ステップ 4</b> | [Port Channel Details] タブをクリックします。  |

- ステップ 5** [Link Settings] セクションをクリックします。  
ポート チャネルに個々のリンクが表示されます。
- ステップ 6** 設定するリンクをクリックします。
- ステップ 7** [Ports (switch)] 領域で、[Priority] フィールドをダブルクリックし、ポートのプライオリティの値を入力します。  
デフォルト値は 32768 です。
- ステップ 8** (任意) メニュー バーで [File] > [Deploy] を選択して変更をデバイスに適用します。

## LACP グレースフル コンバージョン

デフォルトで、LACP グレースフル コンバージョン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、コンバージョン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。



(注)

コマンドが実行される前に、ポート チャネルが管理上のダウン状態である必要があります。

### 作業を開始する前に

LACP をイネーブルにします。

[Port Channel] ペインを使用して、LACP ポート プライオリティを設定します (図 5-3 を参照)。

### 手順の詳細

LACP ポート プライオリティを設定するには、次の手順を実行します。

- ステップ 1** [Feature Selector] ペインで、[Interfaces] > [Logical] > [Port Channel] を選択し、[Port Channel] ペインを開きます。
- ステップ 2** [Contents] ペインの [Summary] ペインで、ポート チャネルを表示するデバイスをダブルクリックします。  
そのデバイスが [Summary] ペイン内で強調表示され、一連のタブが [Details] ペインに表示されます。
- ステップ 3** ポート チャネルをクリックします。  
ポート チャネルが [Summary] ペイン内で強調表示され、一連のタブが [Details] ペインに表示されます。
- ステップ 4** [Port Channel Details] タブをクリックします。
- ステップ 5** [Link Settings] セクションをクリックします。  
ポート チャネルに個々のリンクが表示されます。
- ステップ 6** 設定するリンクをクリックします。
- ステップ 7** [Ports (switch)] 領域で、[Priority] フィールドをダブルクリックし、ポートのプライオリティの値を入力します。  
デフォルト値は 32768 です。
- ステップ 8** (任意) メニュー バーで [File] > [Deploy] を選択して変更をデバイスに適用します。

## 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。

[Port Channel] ペインを使用して、LACP ポート プライオリティを設定します (図 5-3 を参照)。

### 手順の詳細

LACP ポート プライオリティを設定するには、次の手順を実行します。

- 
- |               |   |
|---------------|---|
| <b>ステップ 1</b> | [Feature Selector] ペインで、[Interfaces] > [Logical] > [Port Channel] を選択し、[Port Channel] ペインを開きます。                             |
| <b>ステップ 2</b> | [Contents] ペインの [Summary] ペインで、ポート チャンネルを表示するデバイスをダブルクリックします。<br>そのデバイスが [Summary] ペイン内で強調表示され、一連のタブが [Details] ペインに表示されます。 |
| <b>ステップ 3</b> | ポート チャンネルをクリックします。<br>ポート チャンネルが [Summary] ペイン内で強調表示され、一連のタブが [Details] ペインに表示されます。   |
| <b>ステップ 4</b> | [Port Channel Details] タブをクリックします。  |
| <b>ステップ 5</b> | [Link Settings] セクションをクリックします。<br>ポート チャンネルに個々のリンクが表示されます。  |
| <b>ステップ 6</b> | 設定するリンクをクリックします。  |
| <b>ステップ 7</b> | [Ports (switch)] 領域で、[Priority] フィールドをダブルクリックし、ポートのプライオリティの値を入力します。<br>デフォルト値は 32768 です。                                    |
| <b>ステップ 8</b> | (任意) メニュー バーで [File] > [Deploy] を選択して変更をデバイスに適用します。   |
-



## 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。これが、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。個別の利用のために動作を調整できます。



(注)

エッジ ポートで **lacp suspend-individual** コマンドを実行するだけです。コマンドが実行される前に、ポート チャンネルが管理上のダウン状態である必要があります。

### 作業を開始する前に

LACP をイネーブルにします。

[Port Channel] ペインを使用して、LACP ポート プライオリティを設定します (図 5-3 を参照)。

### 手順の詳細

LACP ポート プライオリティを設定するには、次の手順を実行します。

- ステップ 1** [Feature Selector] ペインで、[Interfaces] > [Logical] > [Port Channel] を選択し、[Port Channel] ペインを開きます。
- ステップ 2** [Contents] ペインの [Summary] ペインで、ポート チャンネルを表示するデバイスをダブルクリックします。そのデバイスが [Summary] ペイン内で強調表示され、一連のタブが [Details] ペインに表示されます。
- ステップ 3** ポート チャンネルをクリックします。ポート チャンネルが [Summary] ペイン内で強調表示され、一連のタブが [Details] ペインに表示されます。
- ステップ 4** [Port Channel Details] タブをクリックします。
- ステップ 5** [Link Settings] セクションをクリックします。ポート チャンネルに個々のリンクが表示されます。
- ステップ 6** 設定するリンクをクリックします。
- ステップ 7** [Ports (switch)] 領域で、[Priority] フィールドをダブルクリックし、ポートのプライオリティの値を入力します。デフォルト値は 32768 です。
- ステップ 8** (任意) メニュー バーで [File] > [Deploy] を選択して変更をデバイスに適用します。

## 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動作を再度イネーブルにできます。

[Port Channel] ペインを使用して、LACP ポート プライオリティを設定します (図 5-3 を参照)。

### 手順の詳細

LACP ポート プライオリティを設定するには、次の手順を実行します。

- 
- |               |   |
|---------------|---|
| <b>ステップ 1</b> | [Feature Selector] ペインで、[Interfaces] > [Logical] > [Port Channel] を選択し、[Port Channel] ペインを開きます。                             |
| <b>ステップ 2</b> | [Contents] ペインの [Summary] ペインで、ポート チャンネルを表示するデバイスをダブルクリックします。<br>そのデバイスが [Summary] ペイン内で強調表示され、一連のタブが [Details] ペインに表示されます。 |
| <b>ステップ 3</b> | ポート チャンネルをクリックします。<br>ポート チャンネルが [Summary] ペイン内で強調表示され、一連のタブが [Details] ペインに表示されます。   |
| <b>ステップ 4</b> | [Port Channel Details] タブをクリックします。  |
| <b>ステップ 5</b> | [Link Settings] セクションをクリックします。<br>ポート チャンネルに個々のリンクが表示されます。  |
| <b>ステップ 6</b> | 設定するリンクをクリックします。  |
| <b>ステップ 7</b> | [Ports (switch)] 領域で、[Priority] フィールドをダブルクリックし、ポートのプライオリティの値を入力します。<br>デフォルト値は 32768 です。                                    |
| <b>ステップ 8</b> | (任意) メニュー バーで [File] > [Deploy] を選択して変更をデバイスに適用します。   |
- 

## 統計情報の表示

[Statistics] タブに次のウィンドウが表示されます。

- Port Traffic Statistics : ロード バランシングのトラフィック速度、および使用率を表示します。
- Port Error Counters : ポート チャンネルでのエラーを表示します。
- FIP Traffic Statistics : 選択したポート チャンネルの FIP トラフィックの統計情報を表示します。

この機能のための統計情報収集の詳細については、『Cisco DCNM Fundamentals Configuration Guide, Release 5.x』を参照してください。

## ポート チャネリングと LACP のフィールドの説明

これらのフィールドの説明は、ポート チャネリングと LACP の設定に使用されます。ここでは、次の内容について説明します。

- 「[Device] : [Port Channel Configuration] タブ」 (P.5-31)
- 「[Device] : [vPC Configuration] タブ」 (P.5-32)
- 「[Port Channel] : [Port Channel Details] : [Common Settings] セクション」 (P.5-33)
- 「[Port Channel] : [Port Channel Details] : [Basic Settings] セクション」 (P.5-33)
- 「[Port Channel] : [Port Channel Details] : [Link Settings] セクション」 (P.5-33)
- 「[Port Channel] : [Port Channel Advanced Settings for Switched Port Channels] : [VLAN Settings] セクション」 (P.5-35)
- 「[Port Channel] : [Port Channel Advanced Settings for Routed Port Channels] : [IP Address] セクション」 (P.5-35)
- 「[Port Channel] : [Port Channel Advanced Settings] : [Advanced Settings] セクション」 (P.5-36)

### [Device] : [Port Channel Configuration] タブ

表 5-3 [Device] : [Port Channel Configuration] タブ

フィールド	説明
LACP System Priority	LACP のシステム プライオリティ。デフォルト値は 32768 です。
Load Balancing Algorithm	ポート チャネル内のインターフェイス間でトラフィックを分散させるために使用されるアルゴリズム。レイヤ 3 ポート チャネルのデフォルトは [Source Destination IP] で、レイヤ 2 ポート チャネルのデフォルトは [Source Destination MAC] です。
<b>Network Card Loadbalance Settings</b>	
Module Number	モジュールの番号。
Module Name	表示のみ。該当するスロット内のモジュール名。
Load Balancing Algorithm	該当するモジュールに現在設定されているロード バランシング アルゴリズム。

## [Device] : [vPC Configuration] タブ



- (注) デバイスで vPC がイネーブルになっていない場合、この画面に次の 2 つのフィールドが表示されます。
- 表示のみ。デバイスで VPC がディセーブルになっています。
  - [Enable vPC]。このフィールドをクリックすると、デバイスで vPC がイネーブルになります。

表 5-4 [Device] : [vPC Channel Configuration] タブ

フィールド	説明
Domain Id	vPC ドメイン ID。
<b>Peer-Keepalive Settings</b>	
Source IP	ピア キープアライブのステータスを確認するためのプライマリ vPC ピア デバイス フォールトトレラント リンクの送信元 IP アドレス。
Destination IP	ピア キープアライブのステータスを確認するためのセカンダリ vPC ピア デバイス フォールトトレラント リンクの宛先 IP アドレス。
VRF	宛先 IP アドレスが属している VRF。デフォルトは管理 VRF です。
UDP port	ピア キープアライブのステータスを確認するためのフォールトトレラント リンクの UDP ポート。デフォルト ポートは 3200 です。
Interval	キープアライブ メッセージの送信間隔 (ミリ秒単位)。間隔のデフォルト値は 1000 ミリ秒です。
Timeout	デバイスでキープアライブ メッセージへの応答を待機する時間。このタイムアウトのデフォルト値は 5 秒です。
Hold Timeout	セカンダリ vPC デバイスでキープアライブ リンクがダウンした後で待機する時間。タイムアウトのデフォルト値は 3 秒です。
<b>Priority Settings</b>	
Role Priority	プライマリ vPC ピア デバイスを手動で選出する値。プライオリティ値が大きい方が、プライマリ vPC ピア デバイスを意味します。デフォルトは vPC の作成時に自動的に設定されます。
System Priority	LACP で使用される vPC のシステム プライオリティを手動で設定する値。デフォルトの vPC システムのプライオリティは、vPC の作成時に自動的に設定されます。
System MAC Address	vPC のシステム MAC アドレスを手動で設定する値。デフォルトのシステム MAC アドレスは、vPC の作成時に自動的に設定されます。
<b>Packet Settings</b>	
Precedence	キープアライブ メッセージの優先順位の値。デフォルトは [internet] です。
Type of Service	キープアライブ メッセージの TOS の優先順位の値。
TOS Byte	キープアライブ メッセージの 8 ビットの TOS の値。

## [Port Channel] : [Port Channel Details] : [Common Settings] セクション

表 5-5 [Port Channel] : [Port Channel Details] : [Common Settings] セクション

フィールド	説明
Protocol	ポートチャネリング プロトコル。デフォルトは [None] です。
Mode	設定したポート チャネルのモード。 スイッチド ポート チャネルの場合、デフォルトはスイッチド ポート チャネルの最初のチャネルのモードになります。スイッチド ポート チャネルのアクセス モードとトランク モードで切り替えることができます。
Admin Status	ポート チャネルの管理ステータス。デフォルトは [Up] です。
Oper Status	表示のみ。ポート チャネルのインターフェイスのステータス。

## [Port Channel] : [Port Channel Details] : [Basic Settings] セクション

表 5-6 [Port Channel] : [Port Channel Details] : [Basic Settings] セクション

フィールド	説明
Channel ID	表示のみ。ポート チャネルに割り当てられたチャネル番号。
Description	ポート チャネルの名前。デフォルトは空白です。
Speed	ポート チャネルの送信速度。デフォルトの自動ネゴシエーションは自動です。
Duplex	ポート チャネルのデュプレックス動作。デフォルトの自動ネゴシエーションは自動です。

## [Port Channel] : [Port Channel Details] : [Link Settings] セクション

表 5-7 [Port Channel] : [Port Channel Details] : [Link Settings] セクション

フィールド	説明
<b>Ports (switch)</b>	
(注) ここでは、ローカル デバイスのリンクについて詳しく説明します。	
Name	表示のみ。ポート チャネル インターフェイスのポートの名前。
Mode	表示のみ。インターフェイスのポート チャネル モード。有効なモードは次のとおりです。 <ul style="list-style-type: none"> <li>Active</li> <li>Passive</li> <li>On</li> </ul> LACP を実行していない場合のデフォルトは [On] です。 LACP を実行している場合、デフォルトは [Active] です。
Priority	LACP のインターフェイスのプライオリティ。1 ～ 65535 の値を入力します。デフォルト値は 32768 です。

表 5-7 [Port Channel] : [Port Channel Details] : [Link Settings] セクション (続き)

フィールド	説明
Status	<p>表示のみ。ポート チャンネルのインターフェイスのステータスは次のいずれかです。</p> <ul style="list-style-type: none"> <li>• Down</li> <li>• Bundled</li> <li>• Standalone</li> <li>• Suspended</li> <li>• Hot Standby</li> </ul>
<b>Neighbor Devices</b>	
(注) ここでは、ネイバー デバイス上の物理リンクについて詳しく説明します。	
Device	表示のみ。ネイバー デバイスで設定されたホスト名。
Name	表示のみ。ポート チャンネル インターフェイスの一部であるネイバー デバイスのポート名。
Mode	<p>表示のみ。インターフェイスのポート チャンネル モード。有効なモードは次のとおりです。</p> <ul style="list-style-type: none"> <li>• Active</li> <li>• Passive</li> <li>• On</li> </ul> <p>LACP を実行していない場合のデフォルトは [On] です。</p> <p>LACP を実行している場合、デフォルトは [Active] です。</p>
Priority	表示のみ。LACP のインターフェイスのプライオリティ。有効範囲は 1 ～ 65535 番です。デフォルト値は 32768 です。
Status	<p>表示のみ。ポート チャンネルのインターフェイスのステータスは次のいずれかです。</p> <ul style="list-style-type: none"> <li>• Down</li> <li>• Bundled</li> <li>• Standalone</li> <li>• Suspended</li> <li>• Hot Standby</li> </ul>

## [Port Channel] : [Port Channel Advanced Settings for Switched Port Channels] : [VLAN Settings] セクション

表 5-8 [Port Channel] : [Port Channel Advanced Settings] : [VLAN Settings] セクション

フィールド	説明
<b>Access</b>	
Access VLAN	このアクセス ポート チャンネルのアクセス VLAN。デフォルトのアクセス VLAN はデフォルト VLAN または VLAN1 です。
<b>Trunk</b>	
Encapsulation	使用できないフィールド。IEEE 802.1Q は、サポートされている唯一のカプセル化方法です。
Allowed VLANs	このポート チャンネルでデータを伝送できる VLAN。指定できる範囲は 1 ～ 4094 です。デフォルトは 1 です。  (注) VLAN 3968 ～ 4047 および 4094 は、デバイス内部使用のために割り当てられており、データ トラフィックは伝送しません。
Native VLAN	このトランク ポート チャンネルのネイティブ VLAN。デフォルトのネイティブ VLAN はデフォルト VLAN または VLAN1 です。

## [Port Channel] : [Port Channel Advanced Settings for Routed Port Channels] : [IP Address] セクション

表 5-9 [Port Channel] : [Port Channel Advanced Settings] : [IP Address Settings] セクション

フィールド	説明
<b>IPv4 Address Settings</b>	
IP Address	ドット付き 10 進表記の IPv4 アドレス。
Net Mask	ドット付き 10 進表記の IPv4 アドレスのネットワーク マスク。
Secondary IP Address	ドット付き 10 進表記のセカンダリ IPv4 アドレス。1 つのインターフェイスに対して複数のセカンダリ アドレスを設定できます。
Secondary NetMask	ドット付き 10 進表記のセカンダリ IPv4 アドレスのネットワーク マスク。
Helper IP Address	User Datagram Protocol (UDP; ユーザ データグラム プロトコル) ブロードキャストの転送をイネーブルにするために使用されるヘルパー アドレス。この機能を使用する場合は、DHCP をイネーブルにする必要があります。
<b>IPv6 Address Settings</b>	
Primary/Prefix-length	x:x:x::x/length 形式の IPv6 プレフィクス。
EUI64	Extended Universal Identifier (EUI) -64 形式の IPv6 アドレス。
Link Local	x:x:x::x 形式の IPv6 リンク ローカル アドレス。
Use local only	リンク ローカル アドレスは、自動的に生成された IPv6 アドレスより優先されます。
IPv6 Addresses	IPv6 アドレスと、このアドレスが EUI-64 形式であるかどうかのリスト。インターフェイスに複数のセカンダリ アドレスを設定できます。

## [Port Channel] : [Port Channel Advanced Settings] : [Advanced Settings] セクション

表 5-10 [Port Channel] : [Port Channel Advanced Settings] : [Advanced Settings] セクション

フィールド	説明
<b>IPv4 ACL</b>	
Incoming Traffic	ポート チャンネル上の入力トラフィックをフィルタリングする IPv4 ACL。
Outgoing Traffic	ポート チャンネル上の出力トラフィックをフィルタリングする IPv4 ACL。
<b>IPv6 ACL</b>	
Incoming Traffic	ポート チャンネル上の入力トラフィックをフィルタリングする IPv6 ACL。
Outgoing Traffic	ポート チャンネル上の出力トラフィックをフィルタリングする IPv6 ACL。
<b>SPAN</b>	
Use Interface as SPAN	このインターフェイスの送信元または宛先。
Session ID	表示のみ。インターフェイスが適用される SPAN セッション ID。
Type	表示のみ。セッションのタイプ。
Direction: Ingress	モニタされる入力パケット。
Direction: Egress	モニタされる出力パケット。
<b>Security</b>	
Traffic Storm Control	表示のみ。トラフィック ストーム制御がイネーブルまたはディセーブルです。
IP Source Guard	表示のみ。IP ソース ガードがイネーブルまたはディセーブルです。
Port Security	表示のみ。ポート セキュリティがイネーブルまたはディセーブルです。

## [Port Channel Subinterface] : [Subinterface Details] : [Basic Settings] セクション

表 5-11 [Port Channel Subinterface] : [Subinterface Details] : [Basic Settings] セクション

フィールド	説明
Name	表示のみ。ポート チャンネル サブインターフェイスの名前。
Description	ポート チャンネル サブインターフェイスを説明する文字列。デフォルトは空白です。
Admin State	ポート チャンネル サブインターフェイスの管理ステータス。デフォルトは up です。
Oper Status	表示のみ。ポート チャンネルのサブインターフェイスのステータス。
Bandwidth	設定されたデータ レート (kbps 単位)。デフォルトは 1,000,000 です。
Delay	ポート チャンネル サブインターフェイスのスループット (10 秒単位)。デフォルトは 1 です。
VLAN ID	このポート チャンネル サブインターフェイスで動作する VLAN を割り当てるために使用されます。



## [Port Channel Subinterface] : [Subinterface Details] : [IP Address Settings] セクション

表 5-12 [Port Channel Subinterface] : [Subinterface Details] : [IP Address Settings] セクション

フィールド	説明
<b>IPv4 Address Settings</b>	
IP Address	ドット付き 10 進表記の IPv4 アドレス。
Net Mask	ドット付き 10 進表記の IPv4 アドレスのネットワーク マスク。
Secondary IP Address	ドット付き 10 進表記のセカンダリ IPv4 アドレス。1 つのインターフェイスに対して複数のセカンダリ アドレスを設定できます。
Secondary NetMask	ドット付き 10 進表記のセカンダリ IPv4 アドレスのネットワーク マスク。
Helper IP Address	User Datagram Protocol (UDP; ユーザ データグラム プロトコル) ブロードキャストの転送をイネーブルにするために使用されるヘルパー アドレス。この機能を使用する場合は、DHCP をイネーブルにする必要があります。
<b>IPv6 Address Settings</b>	
Primary/Prefix-length	x:x:x::x/length 形式の IPv6 プレフィクス。
EUI64	Extended Universal Identifier (EUI) -64 形式の IPv6 アドレス。
Link Local	x:x:x::x 形式の IPv6 リンク ローカル アドレス。
Use local only	リンク ローカル アドレスは、自動的に生成された IPv6 アドレスより優先されます。
IPv6 Addresses	IPv6 アドレスと、このアドレスが EUI-64 形式であるかどうかのリスト。インターフェイスに複数のセカンダリ アドレスを設定できます。

## その他の関連資料

ポート チャネルの実装に関する追加情報については、次の項を参照してください。

- 「関連資料」 (P.5-38)
- 「管理情報ベース (MIB)」 (P.5-38)

## 関連資料

関連項目	参照先
レイヤ 2 インターフェイスの設定	<a href="#">第 3 章「レイヤ 2 インターフェイスの設定」</a>
レイヤ 3 インターフェイスの設定	<a href="#">第 4 章「レイヤ 3 インターフェイスの設定」</a>
共有および専用ポート	<a href="#">第 2 章「基本インターフェイス パラメータの設定」</a>
インターフェイス	『Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 5.x』
システム管理	『Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 5.x』
ハイ アベイラビリティ	『Cisco Nexus 7000 Series NX-OS High Availability and Redundancy Guide, Release 5.x』
VDC	『Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 5.x』
ライセンス	『Cisco DCNM Fundamentals Configuration Guide, Release 5.x』
リリース ノート	『Cisco DCNM Release Notes, Release 5.x』

## 標準規格

標準規格	タイトル
IEEE 802.3ad	—

## 管理情報ベース（MIB）

管理情報ベース（MIB）	MIB リンク
<ul style="list-style-type: none"> <li>IEEE8023-LAG-CAPABILITY</li> <li>CISCO-LAG-MIB</li> </ul>	Management Information Base（MIB; 管理情報ベース）を検索およびダウンロードするには、次の URL にアクセスしてください。 <a href="http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml">http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</a>

## ポート チャネル設定の機能履歴

表 5-13 は、この機能のリリースの履歴です。

表 5-13 ポート チャネル設定の機能履歴

機能名	リリース	機能情報
ポート チャネル	4.0(1)	この機能が導入されました。
ポート チャネル	4.2(1)	サポートが 256 ポート チャネルに増加されました。



## CHAPTER 6

# vPC の設定

この章では、Cisco Nexus 7000 シリーズ NX-OS デバイス上で仮想ポート チャンネル (vPC) を設定する方法を説明します。

ポート チャンネルと Link Aggregation Control Protocol (LACP) の設定の詳細については、[第 5 章「ポート チャンネルの設定」](#)を参照してください。

Data Center Network Manager の機能の詳細については、『*Cisco DCNM Fundamentals Configuration Guide, Release 5.x*』を参照してください。



(注)

管理対象デバイス上で実行される Cisco NX-OS リリースでは、この章で説明する機能や設定がすべてサポートされるとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースのマニュアルとリリース ノートを参照してください。



(注)

vPC 機能に対するシステム メッセージのログ レベルは、Cisco DCNM の要件以上でなければなりません。デバイス検出時に、ログ レベルが不十分であることが検出された場合は、最低限必要なレベルまで Cisco DCNM によって引き上げられます。ただし、Cisco Nexus 7000 シリーズ スイッチで Cisco NX-OS Release 4.0 を実行する場合は例外です。Cisco NX-OS Release 4.0 の場合は、デバイス検出の前に、コマンドライン インターフェイスを使用してログ レベルを Cisco DCNM の要件以上となるように設定してください。詳細については、『*Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 5.x*』を参照してください。

この章では、次の内容について説明します。

- [「vPC について」 \(P.6-2\)](#)
- [「vPC のライセンス要件」 \(P.6-20\)](#)
- [「vPC の前提条件」 \(P.6-20\)](#)
- [「注意事項および制約事項」 \(P.6-21\)](#)
- [「vPC の設定」 \(P.6-21\)](#)
- [「vPC の統計情報の表示」 \(P.6-33\)](#)
- [「vPC のフィールドの説明」 \(P.6-34\)](#)
- [「その他の関連資料」 \(P.6-43\)](#)
- [「vPC の設定機能の履歴」 \(P.6-44\)](#)

## vPC について

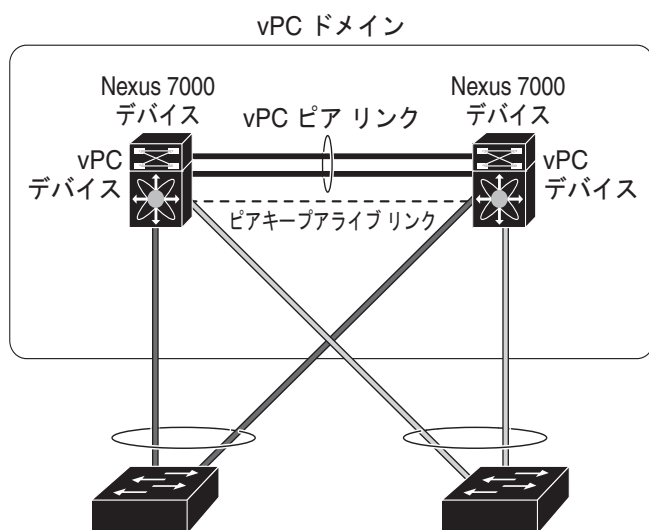
ここで説明する内容は、次のとおりです。

- 「vPC の概要」 (P.6-2)
- 「vPC の用語」 (P.6-5)
- 「vPC ピア リンク」 (P.6-6)
- 「ピアキーブアライブ リンクとメッセージ」 (P.6-9)
- 「vPC ピア ゲートウェイ」 (P.6-11)
- 「vPC ドメイン」 (P.6-11)
- 「vPC ピア リンクの互換パラメータ」 (P.6-12)
- 「vPC 番号」 (P.6-14)
- 「他のポート チャネルの vPC への移行」 (P.6-15)
- 「単一モジュール上での vPC ピア リンクとコアへのリンクの設定」 (P.6-15)
- 「その他の機能との vPC の相互作用」 (P.6-15)
- 「ハイ アベイラビリティ」 (P.6-20)

## 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 7000 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 6-1 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キング デバイスのいずれでもかまいません。Cisco NX-OS Release 4.1(4) から、デバイスごとに最大 256 個の vPC を設定できます。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 6-1 vPC のアーキテクチャ



273225

vPC で使用できるのは、レイヤ 2 ポート チャネルだけです。vPC ドメインは単一の VDC に関連付けられるため、同じ 1 つの vPC ドメインに所属するすべての vPC インターフェイスが同一 VDC 内で定義されていなければなりません。配置した各 VDC に、独立した vPC ピアリンクとピアキープアライブリンクのインフラストラクチャがなくはありません。vPC ピア（ドメインが同じ 2 台の vPC ピアデバイス）を同じ物理デバイスの 2 つの VDC 内に統合することは、サポートされていません。vPC ピアリンクは、リンクの両エンドに 10 ギガバイト イーサネット ポートを使用しなければならず、そうならないとリンクが形成されません。

ポート チャネルの設定は、次のいずれかを使用して行います。

- プロトコルなし
- Link Aggregation Control Protocol (LACP)

LACP を使用せずに vPC (vPC ピア リンク チャネルも含めて) のポート チャネルを設定する場合は、各デバイスが、単一のポート チャネル内に最大 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 チャネルも含めて) のポート チャネルを設定する場合は、各デバイスが、単一のポート チャネル内に 8 つのアクティブ 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 の使用方法の詳細については、「[その他の機能との vPC の相互作用](#)」(P.6-15) を参照してください)。



(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。

リリース 4.2 から、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ようになったため、このチェックポイントにロールバックすれば機能をイネーブルにできます。ロールバックとチェックポイントについては、『*Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 5.x*』を参照してください。

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 つの Cisco Nexus 7000 シリーズシャーシ上のポート チャネルを、N7K-M132XP-12 モジュールおよび 2 つ以上の 10 ギガビット イーサネット ポートを専用モードで使用して設定することにより、vPC ピア リンクを作成できます。正しいハードウェアをイネーブルにしておき、Cisco NX-OS Release 4.1(5) で始まった vPC を実行していることを確認するには、**show hardware feature-capability** コマンドを入力します。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 チャネルは、トランクとして設定することを推奨します。次に、もう 1 つの Cisco Nexus 7000 シリーズシャーシで N7K-M132XP-12 モジュールと一緒に 2 つ以上の 10 ギガビット イーサネット ポートを専用モードで使用して、もう 1 つのポート チャネルを設定します。これらの 2 つのポート チャネルを接続すると、リンクされた 2 つの 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 チャネルを使用するその他の任意のネットワーク デバイスのいずれでもかまいません。正しいモジュールを使用していないと、システムからエラー メッセージが表示されます。



(注) 異なる N7K-M132XP-12 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推奨します。復元力を最適にしたい環境では、少なくとも 2 つの N7K-M132XP-12 モジュールを使用してください。

Cisco Release NX-OS 4.2 から、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 N7K-M132XP-12 モジュール上で設定する必要がある場合、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。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。

**track interface** コマンドの詳細については、『Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 5.x』を、このトラッキング機能の設定の詳細については、『Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 5.x』を参照してください。

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 ドメイン内にあってダウンストリーム デバイスに接続されているすべてのポート チャンネルが含まれます。各デバイス上で持てる 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。



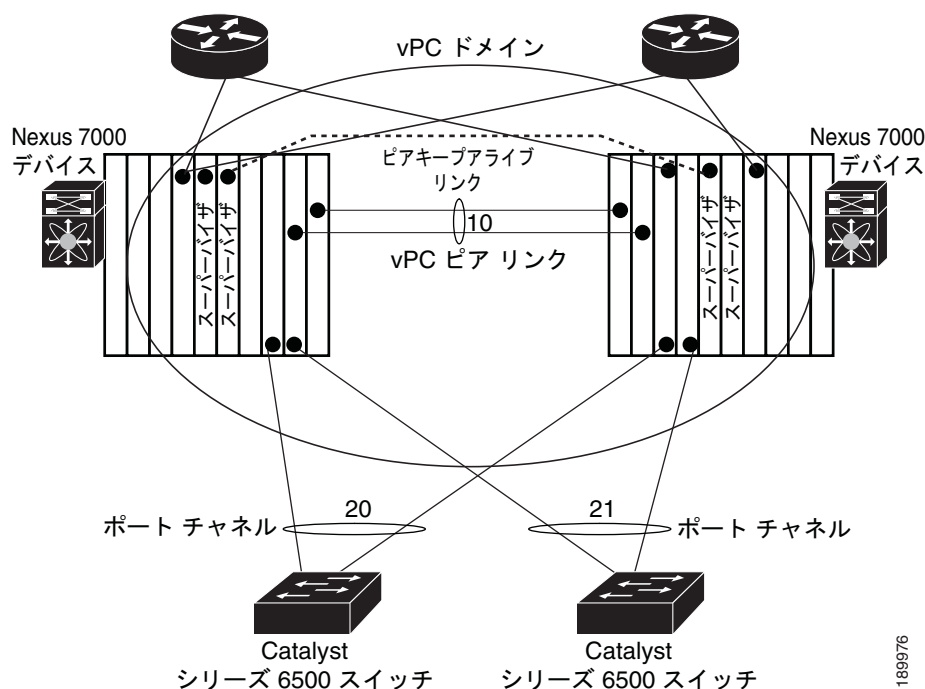
(注)

常にすべての vPC デバイスを両方の vPC ピア デバイスに、ポート チャンネルを使用して接続してください。

vPC (図 6-2 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 ポートをなくします。
- ループフリーなトポロジを提供します。
- 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 アベイラビリティを保証します。

図 6-2 1 つの VDC 内の vPC インターフェイス



VDC の詳細については、『Cisco DCNM Virtual Device Context Configuration Guide, Release 5.x』を参照してください。

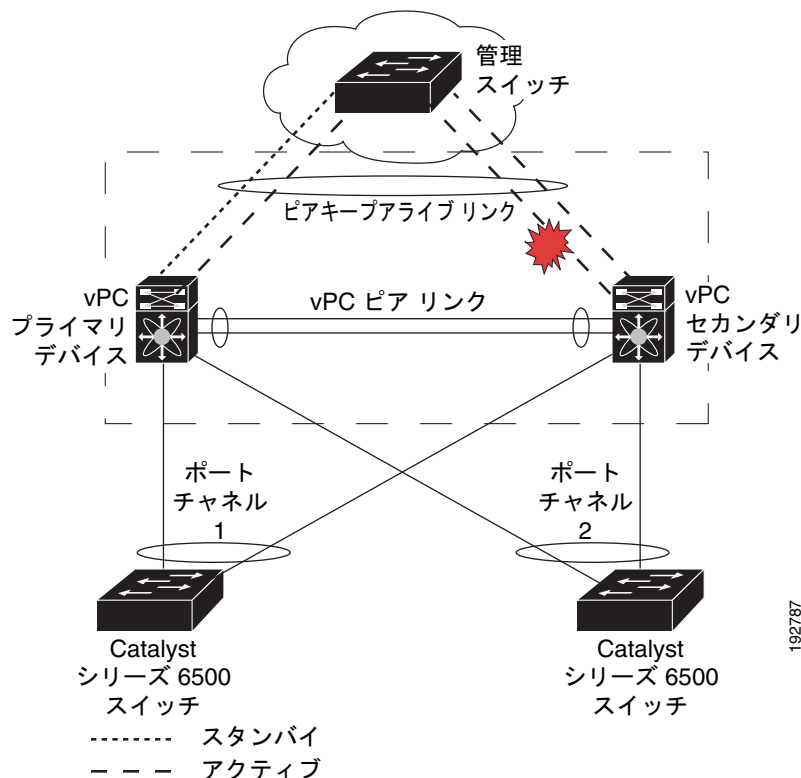
## vPC の用語

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 チャンネル。
- **vPC ピア デバイス** : vPC ピア リンクと呼ばれる特殊なポート チャン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。両エンドが 10 ギガバイト イーサネット インターフェイス上になくてもなりません。
- **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 内にあってダウンストリーム デバイスに接続されているすべてのポート チャンネルが含まれます。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 7000 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 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 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 6-3 を参照)。

図 6-3 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動しており、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。

## vPC ピア リンク

vPC ピア リンクは、vPC ピア デバイス間の状態を同期するために使用されるリンクです。リンクの両エンドが、10 ギガビット イーサネット インターフェイス上になくてもなりません。

ここでは、vPC ピア リンクについて説明します。内容は次のとおりです。

- 「vPC ピア リンクの概要」 (P.6-6)
- 「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」 (P.6-8)
- 「レイヤ 3 接続のための VLAN インターフェイスの設定」 (P.6-9)



(注)

vPC ピア リンクを設定するよりも前にピアキーブアライブ リンクを設定する必要があります。そうしないと、ピアリンクは機能しません (vPC のピアキーブアライブ リンクとメッセージの詳細については、「ピアキーブアライブ リンクとメッセージ」 (P.6-9) を参照してください)。

vPC ピア リンクは、2 つのデバイスを vPC ピアとして設定するように設定できます。vPC ピア リンクを設定するためには、N7K-M132XP-12 モジュールを使用する必要があります。



(注)

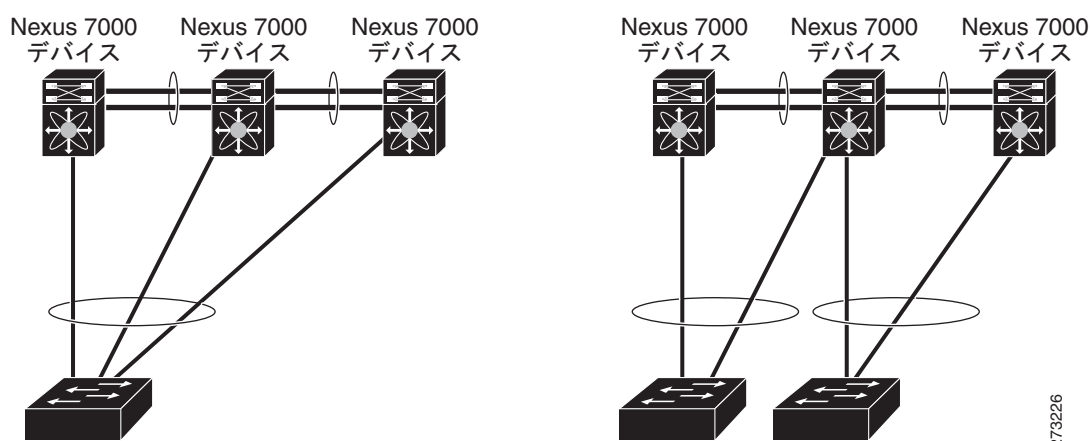
vPC ピア リンクを設定する場合は、専用ポート モードを使用することを推奨します。専用ポート モードの詳細については、第 2 章「基本インターフェイス パラメータの設定」を参照してください。

## 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 リンクを持つことができます。

無効な vPC ピア設定については、図 6-4 を参照してください。

図 6-4 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 チャンネルを設定してから、vPC ドメインを設定します。ポート チャンネルを各デバイスに、同じ vPC ドメイン ID を使用してピア 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 チャンネルに設定することを推奨します。



(注)

レイヤ 2 ポート チャンネルをトランク 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 ピア リンクの互換パラメータ](#)」(P.6-12) を参照）。各デバイスが管理プレーンから完全に独立しているため、デバイスが重要なパラメータについて互換性があることを管理者が確認する必要があります。vPC ピア デバイスは、独立したコントロール プレーンを持っています。vPC ピア リンクを設定し終えたら、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。一貫性が必要な設定の詳細については、「[vPC ピア リンクの互換パラメータ](#)」(P.6-12) を参照してください。

vPC を設定する場合、接続されているデバイスのどちらがプライマリ デバイスで、どちらがセカンダリ デバイスであるかを選択します（「[vPC の設定](#)」(P.6-21) を参照）。ピア リンクのパラメータを設定する場合、vPC ピア リンクのプライマリ側で設定すると、vPC ピア リンクのセカンダリ側のインターフェイスに自動的に適用されます。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、以前プライマリ デバイスだったデバイスがセカンダリ デバイスになります。



(注)

各 vPC ピア デバイスの vPC ピア リンクに対して、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 チャン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 バランシングの詳細については、[第 5 章「ポート チャンネルの設定](#)」を参照してください)。

設定情報は、Cisco Fabric Service over Ethernet (CFSSoE) プロトコルを使用して vPC ピア リンクを流れます (CFSSoE の詳細については、「[CFSSoE](#)」(P.6-19) を参照してください)。

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、CFSSoE が使用されます (CFSSoE については、「[CFSSoE](#)」(P.6-19) を参照してください)。

Cisco NX-OS 4.2(1) から、vPC ピア デバイスを、vPC ピア デバイスの MAC アドレスを送信先とす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るようになりました。

この機能の設定の詳細については、『Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 5.x』を参照してください。

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動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ブアライブ 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 デバイスが稼動している場合は、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 チャネルに残っているアクティブなリンクに転送されます。



(注)

独立した VRF を作成して設定し、その vPC ピアキーブアライブ リンクのための VRF 内の各 vPC ピア デバイス上でレイヤ 3 ポートを設定することを推奨します。ピアキーブアライブのデフォルト ポートとデフォルト VRF は、管理ポートと管理 VRF です。

ソフトウェアは、ピアキーブアライブ リンクを介したキーブアライブ 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ブアライブ メッセージの送信には、独立したリンク (vPC ピア キーブアライブ リンク) を使用します。vPC ピアキーブアライブ リンク上のキーブアライブ 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。キーブアライブ メッセージは、ピア リンク内のすべてのリンクで障害が発生した場合にだけ使用されます。キーブアライブ メッセージの詳細については、「[ピアキーブアライブ リンクとメッセージ](#)」(P.6-9) 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](#)」(P.6-16) 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。
  - 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 Rapid PVST+ を設定し、プライマリ デバイスがすべてのインターフェイスのルートになるように MST を設定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 デバイスからのレイヤ 3 接続を設定します。
- HSRP アクティブ：vPC ピア デバイス上で 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 デバイスは HSRP スタンバイになるように設定します。また、同じ管理/動作モードにある各 vPC デバイス上に VLAN インターフェイスが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](#)」(P.6-18) を参照してください)。

vPC ピア リンクの両側で Unidirectional Link Detection (UDLD; 単方向リンク検出) を設定することを推奨します。

UDLD を設定する手順については「[UDLD モードの設定](#)」(P.2-25) を参照してください。

## レイヤ 3 接続のための VLAN インターフェイスの設定

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。ただし、この目的には VLAN ネットワーク インターフェイスを使用するよりも、vPC ピア デバイスからのルーティングのためのレイヤ 3 リンクを別途設定することを推奨します。



(注)

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方法の詳細については、第 4 章「レイヤ 3 インターフェイスの設定」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。

Cisco NX-OS 4.2(1) から、指定した VLAN インターフェイスが vPC ピア リンクに障害が発生しても vPC セカンダリ デバイス上で停止しないようにすることができるようになりました。



(注)

vPC ドメインにレイヤ 3 デバイスを接続した場合、vPC ピアリンク上でも送信される VLAN を使用したルーティング プロトコルのピアリンクはサポートされません。vPC ピア デバイスおよび汎用レイヤ 3 デバイスの間でルーティング プロトコルの隣接関係が必要な場合は、相互接続に物理的にルーティングされたインターフェイスを使用する必要があります。vPC ピアゲートウェイ機能の使用では、この要件は変わりません。

この機能の設定の詳細については、『Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 5.x』を参照してください。

## ピアキープアライブ リンクとメッセージ

Cisco NX-OS ソフトウェアは、vPC ピア間のピアキープアライブ リンクを使用して、設定可能なキープアライブ メッセージを定期的に送信します。これらのメッセージを送信するには、ピア デバイス間にレイヤ 3 接続がなくはなりません。ピアキープアライブ リンクが有効になって稼動していないと、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 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ピア リンク自体を使用することはしないでください。

VRF の設定方法の詳細については、『Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 5.x』を参照してください。

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、ピアキープアライブ メッセージを受信しなくなることによってその障害を感知します。vPC ピア キープアライブ メッセージのデフォルトの間隔は、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 リンクが停止した時点で開始します。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 キープアライブ 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 キープアライブ 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、受信したキープアライブ メッセージに基づくアクションは一切行いません。これは、スーパーバイザがピア リンクの停止後数秒間の間に失敗したなどが原因で、システムが一時的なキープアライブを受信した場合に、システムがアクションを取ることを防ぐためです。
- 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プアライブ 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。

ピアキープアライブ メッセージ パラメータの設定の詳細については、「[vPC の設定](#)」(P.6-21) を参照してください。



(注)

ピアキープアライブ メッセージに使用される送信元 IP アドレスと宛先 IP アドレスの両方が、ネットワーク上で一意であり、それらの IP アドレスがその vPC ピア キープアライブ リンクに関連付けられている VRF から到達できることを確認してください。

Command-Line Interface (CLI; コマンドライン インターフェイス) 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。次に、インターフェイスを信頼できるポートとして設定する例を示します。

```
(config)# class-map type qos match-all trust-map
(config-cmap-qos)# match cos 4-7

(config)# policy-map type qos ingresspolicy
(config-pmap-qos)# class trust-map

(config)# interface Ethernet8/11
(config-if)# service-policy type qos input ingresspolicy
```

信頼できるポートと優先順位の設定方法の詳細については、『Cisco Nexus 7000 Series NX-OS Quality of Service Configuration Guide, Release 5.x』を参照してください。

## vPC ピア ゲートウェイ

Cisco NX-OS 4.2(1) から、vPC ピア デバイスを、vPC ピア デバイスの MAC アドレスを送信先とす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るようになりました。この機能を設定するには、**peer-gateway** コマンドを使用します。

一部の Network-Attached Storage (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ことを目的とした機能を備えている場合があります。基本的に、こういった機能では、同じサブネットにローカルには接続されていないホストから発生した要求に応答する場合に、ルーティング テーブル ルックアップの実行が避けられます。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 7000 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。このような動作は、一部の基本的なイーサネット RFC 規格と互換性がありません。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、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、この機能は、ピアリンクの使用を最適化し、トラフィック損失の可能性をなくします。

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、デバイスの稼動も 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場合は、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、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 リダイレクトをディセーブルにする必要があります。vPC ドメイン内でこの機能をイネーブルにすると、このような要件があることが、適切なメッセージによってユーザに通知されます。

ピアゲートウェイ vPC デバイスに到達するパケットは、その TTL がデクリメントされるため、TTL = 1 となっているパケットは TTL の失効が原因で伝送中にドロップされる可能性があります。ピアゲートウェイ機能がイネーブルになっており、パケットを TTL = 1 で送出する特定のネットワーク プロトコルが vPC VLAN 上で稼動している場合は、これを考慮する必要があります。

## 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 ドメインを作成するには、1 ~ 100 の数字を使用して vPC ドメイン ID を作成する必要があります。vPC ドメインは、デバイスごとに 1 つだけ持つことができます。1 ~ 4096 の範囲で、ダウンストリーム デバイスにリンクされているポート チャネルを識別する vPC 番号を作成します。

各デバイス上で、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設定する必要があります。各デバイス上でピア 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、静的にしか設定できません。各 vPC ピア デバイス上の vPC 内のすべてのポートが、同じ VDC 内になくてもなりません。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設定できます。可能であれば、各 vPC 内で LACP をアクティブ モードのインターフェイスと一緒に使用してポート チャネルを設定する

ことを推奨します。これにより、ポート チャネルのフェールオーバーが発生した場合の最適化されたスマートな回復が保証され、さらにポート チャネル自体の間での設定の不一致に対する設定チェックが提供されます。

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 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 は稼動しません。

## vPC ピア リンクの互換パラメータ

多くの設定パラメータおよび動作パラメータが、vPC 内のすべてのインターフェイスで同じでなければなりません。vPC 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。

両方の vPC ピア デバイス上で vPC 機能をイネーブルにし、ピア リンクを設定したら、CFS メッセージによって、ローカル vPC ピア デバイス上の設定のコピーがリモート vPC ピア デバイスに提供されます。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、「[CFS](#)」(P.6-19) を参照してください)。

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、[第 5 章「ポート チャネルの設定」](#)を参照してください。

ここで説明する内容は、次のとおりです。

- 「同じでなければならない設定パラメータ」(P.6-12)
- 「同じにすべき設定パラメータ」(P.6-13)

## 同じでなければならない設定パラメータ

ここで示す設定パラメータは、vPC ピア リンクの両方のデバイスで同じように設定する必要があります。そうならないと、vPC はサスペンドモードに移行します。



(注)

vPC 内のすべてのインターフェイスで、下に示す動作パラメータおよび設定パラメータの値が同じになっていなければなりません。

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りません。

- ポート チャネル モード：オン、オフ、またはアクティブ
- チャネルごとのリンク速度
- チャネルごとのデュプレックス モード



- チャンネルごとのトランク モード：
  - Native VLAN
  - トランク上の許可 VLAN
  - ネイティブ VLAN トラフィックのタグging
- Spanning Tree Protocol (STP; スパニング ツリー プロトコル) モード
- 多重スパニング ツリーの 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
- STP グローバル設定：
  - Bridge Assurance の設定
  - ポート タイプの設定
  - ループ ガードの設定
- STP インターフェイス設定：
  - ポート タイプの設定
  - ループ ガード
  - ルート ガード
- Maximum Transmission Unit (MTU; 最大伝送ユニット)

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。

これらの設定と一致しないピア リンクを作成しようとすると、DCNM インターフェイスによって、エラー メッセージが表示されます。DCNM を使用して vPC を設定する場合、プライマリ vPC ピア デバイスを設定すると、その設定が自動的にセカンダリ vPC ピア デバイスに転送されます。不一致が発生した場合、システムは vPC ピア リンクを確立させることができず、[vPC Summary] テーブルの vPC および vPC ピア リンクの [Consistency] フィールドに「Failed」と表示されます。

2 つの vPC デバイスでのブロッキングの不一致を表示して自動的に解決するには、[Failed in the Consistency] 列を右クリックし、ポップアップ メニューから [Synchronize] を選択します。DCNM を使用した vPC デバイスの同期化の詳細については、「[vPC と vPC ピア リンクの同期化](#)」(P.6-28) を参照してください。

## 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。ピア リンクの片方のデバイスだけで設定されている VLAN は、vPC またはピア リンクを使用してトラフィックを通過させることはしません。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。そうならない 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)
- Dynamic Host Configuration Protocol (DHCP) スヌーピング
- Network Access Control (NAC; ネットワーク アクセス コントロール)
- Dynamic ARP Inspection (DAI; ダイナミック ARP インスペクション)
- IP Source Guard (IPSG; IP ソース ガード)
- Internet Group Management Protocol (IGMP; インターネット グループ管理プロトコル) スヌーピング
- Hot Standby Routing Protocol (HSRP; ホット スタンバイ ルーティング プロトコル)
- Protocol Independent Multicast (PIM; プロトコル独立マルチキャスト)
- Gateway Load-Balancing Protocol (GLBP; ゲートウェイ ロード バランシング プロトコル)
- 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。

## vPC 番号

vPC ドメイン ID と vPC ピア リンクを作成し終えたら、ダウンストリーム 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。STP ポートのタイプの詳細については、『Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide, Release 5.x』を参照してください。

最後に、各 vPC ピア デバイス上で作業して、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 vPC 番号を割り当てます。vPC を作成するときには、最小限のトラフィックの中断が発生します。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。



## 他のポート チャンネルの vPC への移行



(注)

ダウンストリーム デバイスは、ポート チャン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 チャンネルを作成し、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 チャンネルを作成します。最後に、各 vPC ピア デバイス上で作業して、ダウンストリーム デバイスに接続されているポート チャンネルに vPC 番号を割り当てます。vPC を作成するときには、最小限のトラフィックの中断が発生します。

## 単一モジュール上での vPC ピア リンクとコアへのリンクの設定



(注)

異なる N7K-M132XP-12 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推奨します。復元力を最適にしたい環境では、少なくとも 2 つの N7K-M132XP-12 モジュールを使用してください。

Cisco NX-OS Release 4.2 以降では、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の N7K-M132XP-12 モジュール上で設定する必要がある場合は、両方の vPC ピア デバイス上のすべての vPC ピア リンク上の、およびコアへのレイヤ 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。

この機能の設定の詳細については、『Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 5.x』を参照してください。

## その他の機能との vPC の相互作用

ここでは、次の内容について説明します。

- 「vPC と LACP」 (P.6-16)
- 「vPC ピア リンクと STP」 (P.6-16)
- 「vPC マルチキャスト : PIM、IGMP、および IGMP スヌーピング」 (P.6-18)
- 「vPC ピア リンクとルーティング」 (P.6-18)
- 「CFSOE」 (P.6-19)

## 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 と LACP については、[第 5 章「ポート チャネルの設定」](#)を参照してください)。

ダウンストリーム デバイスからのチャネルも含めて、すべての vPC ポート チャネル上の 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 リンクは、8 個のアクティブ リンクと 8 個のホット スタンバイ リンクとで、16 個の LACP インターフェイスをサポートします。ダウンストリーム vPC チャネル上では、8 個のアクティブ リンクと 8 個のホット スタンバイ リンクとで、16 個の LACP リンクを設定できます。LACP を使用せずにポート チャネルを設定する場合は、各チャネルに 8 個のリンクしか持てません。

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 は稼動しません。

## vPC ピア リンクと STP

vPC を初めて稼動させたときに、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 Bridge Assurance が自動的にイネーブルになるようにすることを推奨します。また、vPC ピア リンク上ではどの STP 拡張機能もイネーブルにしないことも推奨します。STP 拡張がすでに設定されている場合は何も問題は発生しませんが、これらを設定する必要はありません。

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 拡張機能と PVST シミュレーションの詳細については、『*Cisco DCNM Layer 2 Switching Configuration Guide, Release 5.x*』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。これらの一致していなければならない必須設定については、『[vPC ピア リンクの互換パラメータ](#)」(P.6-12)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 については、『[CFS over E](#)」(P.6-19)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」(P.6-9) 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
  - Bridge Assurance の設定
  - ポート タイプの設定
  - ループ ガードの設定
- STP インターフェイス設定：
  - ポート タイプの設定
  - ループ ガード
  - ルート ガード

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。

**(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 ポートのタイプの詳細については、『Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide, Release 5.x』を参照してください)。

## vPC マルチキャスト : PIM、IGMP、および IGMP スヌーピング



(注)

Nexus 7000 シリーズ デバイスの Cisco NX-OS ソフトウェアは、PIM SSM も BIDR on vPC もサポートしていません。Cisco NX-OS ソフトウェアは、PIM ASM on vPC を完全にサポートします。

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。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 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。

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。

vPC とマルチキャストに関する情報を表示するコマンドについては、『Cisco Nexus 7000 Series NX-OS Interfaces Command Reference, Release 5.x』を参照してください。

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、vPC ピア デバイスの片方だけがマルチキャスト 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 デバイスを選出します。
- **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 デバイスでの DR 情報を同期させます。vPC モードになっているときには、IGMP についてデュアル DR という概念があります。これは、vPC モードでないときは使用できないもので、両方の vPC ピア デバイスにピア間でマルチキャスト グループ情報を維持させます。

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。

マルチキャストの詳細については、『Cisco Nexus 7000 Series NX-OS Multicast Routing Configuration Guide, Release 5.x』を参照してください。

## vPC ピア リンクとルーティング

First Hop Routing Protocols (FHRP; ファーストホップ冗長プロトコル) は、vPC と相互運用できます。Hot Standby Routing Protocol (HSRP; ホットスタンバイ ルーティング プロトコル)、Gateway Load Balancing Protocol (GLBP; ゲートウェイ ロード バランシング プロトコル)、および Virtual Router Redundancy Protocol (VRRP; 仮想ルータ冗長プロトコル) 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。



(注)

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 デバイスからのレイヤ 3 接続をイネーブルにする必要があります (VLAN ネットワーク インターフェイスの作成については、第 4 章「レイヤ 3 インターフェイスの設定」を参照してください)。

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こと、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。

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。GLBP については、両方の vPC ピア デバイス上のフォワーダがトラフィックを転送します。

プライマリ vPC ピア デバイ스에 장애가 발생한 경우는, 세컨다리 vPC 피아 데바이스에 페일 오버버사레, FHRP 트라피크는 시ーム레스에 흐름에 계속됩니다.

この目的には VLAN ネットワーク インターフェイスを使用するよりも、vPC ピア デバイスからのルーティングのためのレイヤ 3 リンクを別途設定してください。

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 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스에 동일한 MAC アドレスを設定する必要があります。

Cisco NX-OS 4.2(1) から、ピアの隣接が形成されて VLAN インターフェイスがバックアップされるまで vPC の再稼動を遅らせる復元タイマーを設定できるようになりました。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。

この機能の設定の詳細については、『Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 5.x』を参照してください。

FHRP とルーティングの詳細については、『Cisco DCNM Unicast Routing Configuration Guide, Release 5.x』を参照してください。

## CFS over E

Cisco Fabric Services over Ethernet (CFS over E) 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。CFS over E は、vPC にリンクされている、STP、IGMP などの多くの機能のメッセージとパケットを伝送します。情報は、CFS/CFS over E プロトコル データ ユニット (PDU) に入れて伝送されます。

CFS over E は、vPC 機能をイネーブルにすると、デバイスによって自動的にイネーブルになります。何も設定する必要はありません。vPC の CFS over E 分散には、IP を介してまたは CFS リージョンに分散する機能は必要ありません。CFS over E 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。

Cisco Fabric Services は、TCP/IP を介したデータの転送も行います。CFS over IP の詳細については、『Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 5.x』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。

## ハイ アベイラビリティ

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 7000 Series NX-OS High Availability and Redundancy Guide, Release 5.x』を参照してください。

## vPC のライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
DCNM	vPC には LAN Enterprise ライセンスが必要です。ライセンスの取得方法と適用方法についての詳細は、『Cisco DCNM Fundamentals Configuration Guide, Release 5.x』を参照してください。
Cisco NX-OS	vPC には、ライセンスは必要ありません。ライセンス パッケージに含まれていない機能はすべて Cisco NX-OS システム イメージにバンドルされており、追加費用は一切発生しません。Cisco NX-OS のライセンス スキームの詳細については、『Cisco Nexus 7000 Series NX-OS Licensing Guide, Release 5.x』を参照してください。

## vPC の前提条件

vPC の前提条件は、次のとおりです。

- LAN Enterprise ライセンスがインストールされていることを確認します。

## 注意事項および制約事項

vPC には、次の注意事項と制約事項があります。

- 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 リンクを形成するには、その前にピアキープアライブ リンクとピアキープアライブ 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。
- 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。互換性に関する推奨事項について、「[vPC ピア リンクの互換パラメータ](#)」(P.6-12) 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 および SSM 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。
- CFS リージョンはサポートされていません。
- ポート チャンネル上でのポート セキュリティは、サポートされていません。
- 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。
- この目的には VLAN ネットワーク インターフェイスを使用するよりも、vPC ピア デバイスからのルーティングのためのレイヤ 3 リンクを別途設定してください。

## vPC の設定



(注) DCNM インターフェイスでは、プライマリ vPC ピア デバイスのパラメータを設定でき、それらのパラメータはセカンダリ vPC デバイスに自動的に伝播されます。

ここでは、DCNM を使用して vPC を設定する方法を説明します。内容は次のとおりです。

- 「[vPC のイネーブル化](#)」(P.6-22)
- 「[vPC のディセーブル化](#)」(P.6-23)
- 「[vPC の作成と変更](#)」(P.6-23)
- 「[vPC と vPC ピア リンクの同期化](#)」(P.6-28)
- 「[ピアキープアライブ リンクおよびメッセージの手動による設定](#)」(P.6-29)
- 「[vPC のプライオリティ設定の手動による設定](#)」(P.6-30) 「[vPC の削除](#)」(P.6-31)
- 「[\[Details\] タブのペインを使用した vPC 設定の変更](#)」(P.6-32)

[Port Channel] ペインで、[Summary] テーブルに vPC ポート チャンネルの追加アイコンが表示されます。vPC に設定できるのは、レイヤ 2 ポート チャンネルだけです。



(注) [Feature Selector] の Topology 機能は、vPC を設定する際に非常に役立ちます。

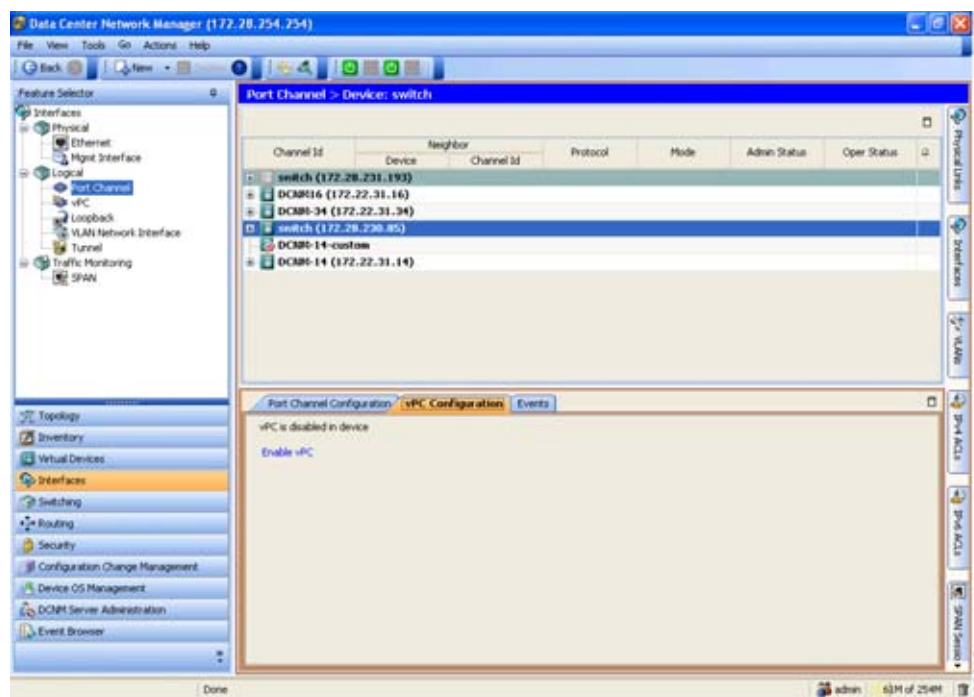
Topology 機能の詳細については、『*Cisco DCNM Fundamentals Configuration Guide, Release 5.x*』を参照してください。



## vPC のイネーブル化

vPC を設定するには、その前に vPC 機能をイネーブルにする必要があります。vPC をイネーブルにするには、[Port Channel] ペインを使用します（図 6-5 を参照）。

図 6-5 vPC のイネーブル化



### 作業を開始する前に

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

### 手順の詳細

vPC をイネーブルにするには、次の手順を実行します。

- ステップ 1** [Feature Selector] ペインで、[Interfaces] > [Logical] > [Port Channel] を選択し、[Port Channel] ペインを開きます。
- ステップ 2** [Contents] ペインの [Summary] ペインで、vPC 機能をイネーブルにするデバイスをクリックします。そのデバイスが [Summary] ペイン内で強調表示され、一連のタブが [Details] ペインに表示されます。
- ステップ 3** [Details] ペインの [VPC Configuration] タブをクリックします。
- ステップ 4** [Enable vPC] をクリックします。
- ステップ 5** (任意) メニュー バーで [File] > [Deploy] を選択して変更をデバイスに適用します。



## vPC のディセーブル化



(注)

vPC 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。

vPC をディセーブルにするには、[Port Channel] ペインを使用します (図 6-5 を参照)。

### 手順の詳細

vPC をディセーブルにするには、次の手順を実行します。

- ステップ 1 [Feature Selector] ペインで、[Interfaces] > [Logical] > [Port Channel] を選択し、[Port Channel] ペインを開きます。
- ステップ 2 [Contents] ペインの [Summary] ペインで、vPC 機能をディセーブルにするデバイスをクリックします。そのデバイスが [Summary] ペイン内で強調表示され、一連のタブが [Details] ペインに表示されます。
- ステップ 3 vPC をディセーブルにするには、メニュー バーで [Actions] > [Disable vPC] を選択します。
- ステップ 4 (任意) メニュー バーで [File] > [Deploy] を選択して変更をデバイスに適用します。

## vPC の作成と変更

[vPC] ペインから vPC ウィザードを起動します (図 6-6 および図 6-7 を参照)。[\[Port Channel\]](#) ペインを使用してポート チャネルを作成することも (ポート チャネルの作成の詳細については、[第 5 章「ポートチャネルの設定」](#)を参照)、vPC ウィザードから直接ポート チャネルを作成することもできます。

図 6-6 [vPC] ペイン

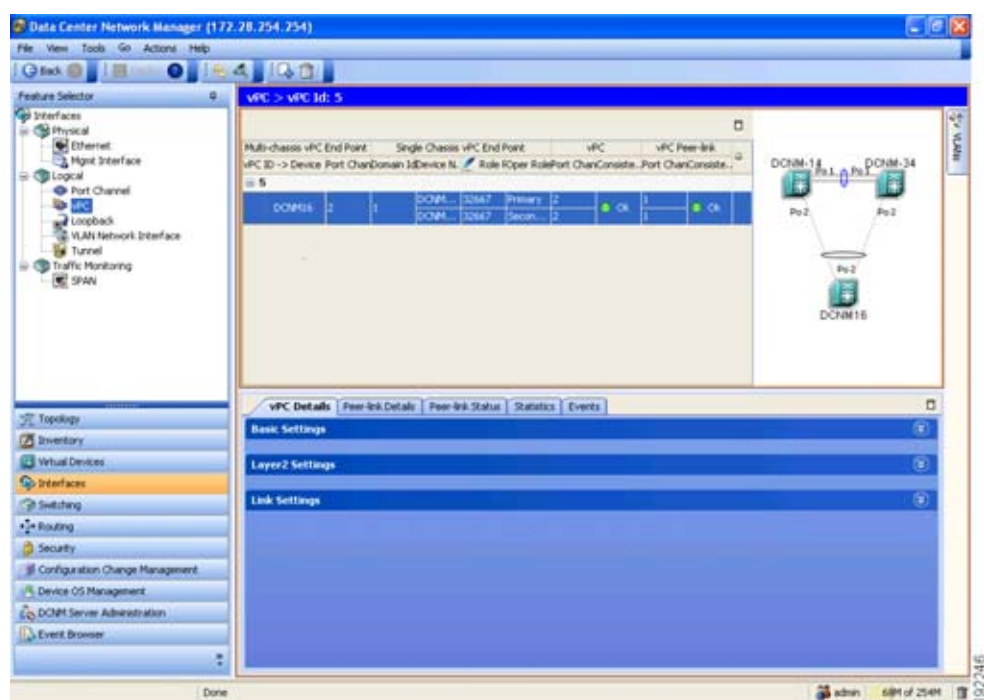
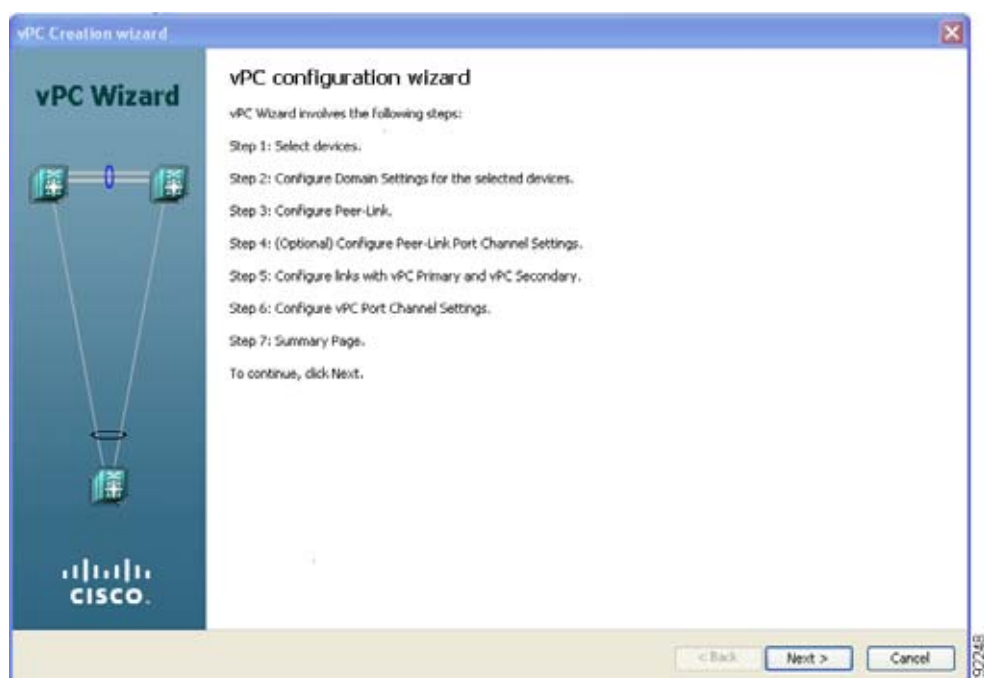


図 6-7 vPC ウィザード



## 作業を開始する前に

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

## 手順の詳細

vPC ウィザードを使用して vPC を作成または変更するには、次の手順を実行します。

- 
- ステップ 1** [Feature Selector] ペインで、[Interfaces] > [Logical] > [vPC] を選択します。
- ステップ 2** vPC ウィザードを起動するには、次のいずれかを実行します。
- a. 新しい vPC を作成するには、メニュー バーで [Actions] > [New] を選択します。  
vPC Creation ウィザードが起動し、vPC を作成するために必要な手順が表示されます。  
または
  - b. 既存の vPC を変更するには、編集する vPC を強調表示し、メニュー バーで [Actions Edit] を選択します。  
vPC Modification ウィザードが起動し、vPC を変更するために必要な手順が表示されます。
- ステップ 3** [Next] をクリックします。  
[Select devices] ペインが表示されます。
- ステップ 4** [vPC ID] フィールドで、この vPC の値を入力します。
- ステップ 5** [Select Multi-chassis vPC Switch] フィールドで、チェックボックスをオンにします。
- a. [Select Multi-chassis vPC Switch] ドロップダウン リストから、マルチシャーシ vPC デバイスにするデバイスを選択します。
- ステップ 6** [Select Single Chassis vPC Pair] 領域に移動し、次の手順を実行します。
- a. [vPC Switch (Primary)] ドロップダウン リストから、vPC ピア リンク上のプライマリ デバイスにするデバイスを選択します。
  - b. [vPC Switch (Secondary)] ドロップダウン リストから、vPC ピア リンク上のセカンダリ デバイスにするデバイスを選択します。
  - c. [Domain ID] フィールドで、vPC ドメイン ID を入力します。
- ステップ 7** (任意) プロトコルを使用せずにポート チャネルを作成する場合、[Enable LACP-based Port Channels for setting up vPC] をクリックして LACP をディセーブルにします。  
デフォルトでは、vPC のすべてのポート チャネルで LACP がイネーブルになっています。これらのすべてのポート チャネルで LACP を使用することを推奨します。LACP を使用しない場合は、このオプションをオフにします。
- ステップ 8** [Next] をクリックします。  
[Domain Settings] ペインが表示されます。このペインは DCNM Release 4.2 以降で使用できます。プライマリ vPC ピア デバイスのみの設定を行います。その後、設定がセカンダリ vPC ピア デバイスに適用されます。
- ステップ 9** システム MAC アドレス、ロール プライオリティ、システム プライオリティのいずれかの設定を変更する場合、情報を入力します。
- ステップ 10** (任意) [Source IP] フィールドで、各デバイスからピアキープアライブ メッセージを送信するために使用するポートの IP アドレスを入力します。



- (注) システムが vPC ピア リンクを形成するには、その前にピアキープアライブ リンクを設定する必要があります。  
ピアキープアライブ メッセージに使用される送信元と宛先の両方の 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。ピアキープアライブ メッセージの送信にピア リンク自体を使用することはしないでください。  
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。

デフォルト値は管理インターフェイスの IP アドレスです。ただし、このリンクに別の VRF を設定することを強く推奨します。

- ステップ 11** [Destination IP] フィールドで、各デバイスからピアキープアライブ メッセージを受信するために使用するポートの IP アドレスを入力します。
- ステップ 12** (任意) [UDP Port] フィールドで、各デバイスからのピアキープアライブ メッセージの交換に使用する UDP ポート番号を入力します。
- ステップ 13** [VRF] フィールドで、ピアキープアライブ メッセージに使用する VRF の名前を入力します。
- ステップ 14** (任意) [Interval] フィールドで、各ピアキープアライブ メッセージの送信間隔をミリ秒単位で入力します。
- ステップ 15** (任意) [Hold Timeout] フィールドで、vPC セカンダリ ピア デバイスでピアキープアライブ リンクがダウンした後で待機する時間を秒単位で入力します。
- ステップ 16** (任意) [Timeout] フィールドで、vPC プライマリ ピア デバイスでピアキープアライブ リンクがダウンした後で待機する時間を秒単位で入力します。
- ステップ 17** (任意) [Packet Setting] フィールドで、ピアキープアライブ メッセージパケットの優先順位の値、Type of Service (タイプ オブ サービス) の値、または ToS バイトの値を入力します。  
いずれかの値を入力します。
- ステップ 18** [Next] をクリックします。

[Configure Peer-Link] ペインが表示されます。vPC ピア リンクの既存のポート チャネルを使用することも、vPC ピア リンクの新しいポート チャネルを作成することもできます。



- (注) vPC ピア リンクとして指定するレイヤ 2 ポート チャネルはトランク モードに設定し、冗長性のために各 vPC ピア デバイス上で独立したモジュール上の 2 つのポートを使用することを推奨します。

- ステップ 19** [Po ID] フィールドで、vPC ピア リンクとして使用する各デバイスのポート チャネル番号を入力します。  
vPC ピア リンクとして指定する 2 つの vPC デバイス上の 2 つのポート チャネルに異なる番号を使用できます。
- ステップ 20** [Available Interfaces] セクションで、[Interfaces] タブまたは [Links] タブを選択して、各デバイスのインターフェイスを割り当てます。
- ステップ 21** vPC ピア リンクに使用するインターフェイスまたはリンクを選択します。
- ステップ 22** [Add] をクリックします。  
選択したインターフェイスが [Selected Interfaces] 領域に表示されます。
- ステップ 23** [Next] をクリックします。

**ステップ 24** Peer-Link のプライマリのみの設定フィールドで設定を入力します。

[Peer-Link Primary] フィールドに入力した値は、次に示すように Peer-Link セカンダリ デバイスで自動的に設定されます。

- a. vPC を作成する場合、この手順はオプションで、新しいポート チャネルを作成するように選択した場合だけ表示されます。ウィンドウに Peer-Link プライマリの列と Peer-Link セカンダリの列が表示されます。
- b. vPC を変更する場合、この手順が常に表示されます。ウィンドウに Peer-Link プライマリの列と Peer-Link セカンダリの列が表示されます。

**ステップ 25** [Next] をクリックします。

プライマリおよびセカンダリのウィンドウとともに [Configure] リンクが表示されます。このウィンドウを使用して、マルチシャーシ vPC デバイスを vPC ピア デバイスに接続します。

**ステップ 26** [Po ID] フィールドで、vPC に入れる各デバイスのポート チャネルを入力します。

ポート チャネル番号を一致させる必要はありません。

**ステップ 27** [Available Interfaces] セクションで、[Interfaces] タブまたは [Links] タブを選択して、各デバイスのインターフェイスを割り当てます。

**ステップ 28** vPC マルチシャーシ デバイスへのポート チャネルに使用するインターフェイスまたはリンクを選択します。

**ステップ 29** [Add] をクリックします。

選択したインターフェイスが、マルチシャーシ vPC デバイスから各 vPC ピア デバイスへのリンクとして [Selected Interfaces] に表示されます。

**ステップ 30** [Next] をクリックします。

[Configure vPC Port Channel Settings] ペインにマルチシャーシ vPC デバイス、vPC プライマリ ピア デバイス、および vPC セカンダリ ピア デバイスの設定が表示されます。

**ステップ 31** マルチシャーシ vPC デバイスおよび vPC Peer-Link プライマリ デバイスのみのそれぞれの設定フィールドに設定を入力します。

**ステップ 32** [Next] をクリックします。

[Summary] ページに、設定した vPC 設定が表示されます。

**ステップ 33** (任意) 設定のいずれかを変更する場合、[Back] をクリックすると、修正するページに戻ります。

vPC ウィザードの残りのページを続行します。

**ステップ 34** [Finish] をクリックします。

[vPC Deployment Status] ウィンドウに、vPC 設定の進捗がステータス バー、および 5 つの設定タスクのそれぞれが完了すると自動的にチェックされるチェックリストとともに表示されます。

タスクのステップを設定できない場合、タスクの横に十字が表示され、エラー メッセージが表示されます。この場合、正常に展開された部分的な設定が vPC に表示されます。

**ステップ 35** [Done] をクリックします。

**ステップ 36** (任意) メニュー バーで [File] > [Deploy] を選択して変更をデバイスに適用します。

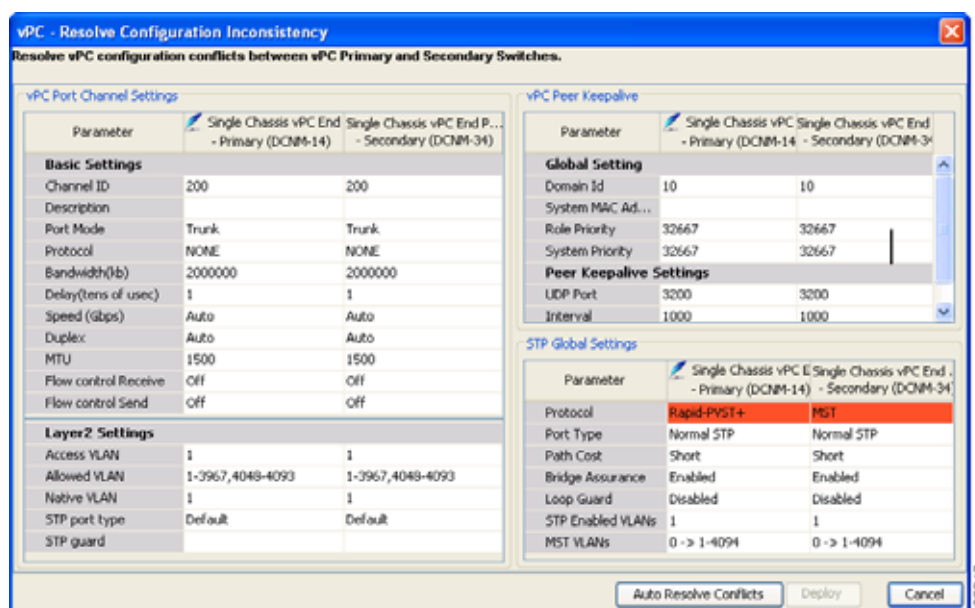
## vPC と vPC ピア リンクの同期化

vPC ピア デバイス間で設定の互換性がない場合、[vPC] ペインの [Summary] 表の [Consistency] 列で、該当する vPC に [Failed] と表示されます。vPC で設定の競合を解決する必要があります。

プライマリ vPC ピア デバイスの設定を変更できます。その後、セカンダリ vPC ピア デバイスに自動的に同じ設定が適用されます。[Auto Resolve Conflicts] オプションを選択した場合、プライマリ vPC ピア デバイスからすべての設定値が自動的にセカンダリ vPC デバイスにコピーされます。

互換性のない vPC ピア リンク設定を解決するには、[Resolve Configuration Inconsistency] ペインを使用します（図 6-8 を参照）。

図 6-8 設定の不一致の解決



### 作業を開始する前に

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

### 手順の詳細

設定の不一致を解決するには、次の手順を実行します。

- ステップ 1** [Feature Selector] ペインで [Interfaces] > [Logical] > [vPC] を選択して [vPC] ペインを開きます。
- ステップ 2** [Contents] ペインの [Summary] ペインで、[Consistency] 列に [Failed] と表示された vPC チャンネルをクリックします。
- ステップ 3** [Consistency] 列で、[Failed] を右クリックします。
- ステップ 4** 表示されるドロップダウン リストから、[Synchronize] を選択します。  
vPC またはピア リンクを同期化できます。
- ステップ 5** vPC を同期化するには、[vPC] をクリックします。  
[Resolve Configuration Inconsistency] ペインが表示されます。設定の不一致が赤で強調表示されます。

- ステップ 6** [Auto Resolve Conflicts] をクリックします。
- ステップ 7** vPC ピア リンク デバイスを同期化するには、[Peer-Link] をクリックします。  
[Resolve Configuration Inconsistency] ペインが表示されます。設定の不一致が赤で強調表示されます。
- ステップ 8** [Auto Resolve Conflicts] をクリックします。

## ピアキープアライブ リンクおよびメッセージの手動による設定

システムが vPC ピア リンクを形成するには、その前にピアキープアライブ リンクを設定する必要があります。DCNM Release 4.2 以降では、ウィザードを使用してすべてのピア キープアライブ パラメータを設定できます。



(注)

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。

ピアキープアライブ メッセージの送信にピア リンク自体を使用することはしないでください。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 の作成と設定の詳細については、『Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 5.x』を参照してください。

ピアキープアライブ メッセージを設定するには、[Port Channel] ペインを使用します (図 6-5 を参照)。

### 作業を開始する前に

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

### 手順の詳細

ピアキープアライブ メッセージを設定するには、次の手順を実行します。

- ステップ 1** [Feature Selector] ペインで、[Interfaces] > [Logical] > [Port Channel] を選択し、[Port Channel] ペインを開きます。
- ステップ 2** [Contents] ペインの [Summary] ペインで、vPC ピアキープアライブ リンクおよびメッセージを設定するデバイスをクリックします。  
そのデバイスが [Summary] ペイン内で強調表示され、一連のタブが [Details] ペインに表示されます。
- ステップ 3** [Details] ペインの [VPC Configuration] タブをクリックします。
- ステップ 4** [Domain Id] フィールドで、ピアキープアライブ リンクおよびメッセージを設定する vPC ドメインの値を入力します。
- ステップ 5** [Source IP] フィールドで、ピアキープアライブ リンクを設定する単一シャーシ vPC デバイスの IP アドレスを入力します。
- ステップ 6** [Destination IP] フィールドで、その他の単一シャーシ vPC デバイスの IP アドレスを入力します。
- ステップ 7** [VRF] ドロップダウン リストを使用して、ピアキープアライブ メッセージの送信に使用する VRF を選択します。  
デフォルトは管理 VRF です。



(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 の作成と設定の詳細については、『Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 5.x』を参照してください。vPC ピアキープアライブ メッセージの送信にピア リンク自体を使用することはいけません。

- ステップ 8** [UDP Port] フィールドで、使用する UDP ポートの番号を入力します。  
デフォルトの UDP ポートは 3200 番です。
- ステップ 9** [Interval] フィールドで、ピアキープアライブ メッセージの送信間隔に使用する数値をミリ秒単位で入力します。  
デフォルトは 1000 ミリ秒です。
- ステップ 10** [Timeout] フィールドで、単一シャーシのプライマリ vPC ピア デバイスで単一シャーシのセカンダリ vPC ピア デバイスからのキープアライブ メッセージの受信を待機する時間をミリ秒単位で入力します。  
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プアライブ 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。  
デフォルトは 5 秒です。
- ステップ 11** (任意) [Hold Timeout] フィールドで、セカンダリ vPC ピア デバイスでピアキープアライブ リンクがダウンした場合に待機する時間を入力します。この任意の手順は DCNM Release 4.2 以降で使用できます。  
ホールドタイムアウトの間は、vPC セカンダリ デバイスは、受信したキープアライブ メッセージに基づくアクションは一切行いません。これは、スーパーバイザがピア リンクの停止後数秒間の間に失敗したなどが原因で、システムが一時的なキープアライブを受信した場合に、システムがアクションを取ることを防ぐためです。  
デフォルト値は 3 秒です。
- ステップ 12** (任意) [Precedence] フィールドで、キープアライブ パケットに割り当てる優先順位の値を入力します。この任意の手順は DCNM Release 4.2 以降で使用できます。  
デフォルトは [network] です。
- ステップ 13** (任意) [Type of Service] フィールドで、キープアライブ パケットに割り当てる ToS の値を入力します。この任意の手順は DCNM Release 4.2 以降で使用できます。
- ステップ 14** [ToS Byte] フィールドで、キープアライブ パケットに割り当てる ToS の優先順位を入力します。この任意の手順は DCNM Release 4.2 以降で使用できます。
- ステップ 15** (任意) メニュー バーで [File] > [Deploy] を選択して変更をデバイスに適用します。

## vPC のプライオリティ設定の手動による設定

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。vPC システム MAC アドレスおよびローカル プライオリティのデフォルト値も変更できます。DCNM Release 4.2 以降では、ウィザードを使用してこれらのパラメータを設定することもできます。



(注) LACP を実行している場合は、手動で vPC システム プライオリティを設定して、vPC ピア デバイスが確実に LACP 上のプライマリ デバイスになるようにすることを推奨します。

vPC プライオリティを設定するには、[Port Channel] ペインを使用します (図 6-5 を参照)。



## 作業を開始する前に

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

## 手順の詳細

vPC プライオリティおよび MAC アドレスを手動で設定するには、次の手順を実行します。

- 
- |               |   |
|---------------|---|
| <b>ステップ 1</b> | [Feature Selector] ペインで、[Interfaces] > [Logical] > [Port Channel] を選択し、[Port Channel] ペインを開きます。                                 |
| <b>ステップ 2</b> | [Contents] ペインの [Summary] ペインで、vPC システム プライオリティを設定するデバイスをクリックします。<br>そのデバイスが [Summary] ペイン内で強調表示され、一連のタブが [Details] ペインに表示されます。 |
| <b>ステップ 3</b> | [Details] ペインの [VPC Configuration] タブをクリックします。  |
| <b>ステップ 4</b> | [Role Priority] フィールドで、ロール プライオリティに割り当てる値を入力します。<br>デフォルト値は 32667 です。   |
| <b>ステップ 5</b> | [System Priority] フィールドで、LACP の vPC ピア デバイスに割り当てる値を入力します。<br>デフォルト値は 32667 です。  |
| <b>ステップ 6</b> | [System MAC Address] フィールドに、vPC に割り当てる MAC アドレスを入力します。<br>デフォルトのシステム MAC アドレスは、vPC の作成時に自動的にシステムによって割り当てられます。                   |
| <b>ステップ 7</b> | (任意) メニュー バーで [File] > [Deploy] を選択して変更をデバイスに適用します。   |
- 

## vPC の削除

vPC を削除するには、[vPC] ペインを使用します。

## 手順の詳細

vPC を削除するには、次の手順を実行します。

- 
- |               |  |
|---------------|--|
| <b>ステップ 1</b> | [Feature Selector] ペインで [Interfaces] > [Logical] > [vPC] を選択して [vPC] ペインを開きます。 |
| <b>ステップ 2</b> | [Contents] ペインの [Summary] ペインで、削除する vPC をクリックします。                              |
| <b>ステップ 3</b> | メニュー バーで [Actions] > [Delete] を選択します。  |
| <b>ステップ 4</b> | (任意) メニュー バーで [File] > [Deploy] を選択して変更をデバイスに適用します。                            |
-

## [Details] タブのペインを使用した vPC 設定の変更

vPC ウィザードを使用して vPC を作成または変更することを推奨します。

### 作業を開始する前に

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

### 手順の詳細

[Detail] ペインを使用して vPC の作成または変更を行うには、次の手順を実行します。

**ステップ 1** [Feature Selector] で、[Interfaces] > [Logical] > [Port Channels] > [vPC Configuration] を選択します。

**ステップ 2** [Details] ペインの [vPC Configuration] タブをクリックします。

a. [Enable vPC] をクリックします。

**ステップ 3** vPC ドメイン ID を割り当て、ピアキープアライブ設定を行い、vPC システム プライオリティを設定するには、[Feature Selector] で [Interfaces] > [Logical] > [Port Channels] > [vPC Configuration] を選択し、次の手順を実行します。

a. vPC ドメイン ID を割り当てるには、[vPC Domain ID] フィールドで数値を入力します。

b. ピアキープアライブ メッセージの送信元 IP アドレスを変更するには、[Source IP] フィールドで単一シャーシプライマリ vPC デバイスの IP アドレスを入力します。

c. ピアキープアライブ メッセージの宛先 IP アドレスを変更するには、[Destination IP] フィールドで単一シャーシ宛先 vPC デバイスの IP アドレスを入力します。

d. ピアキープアライブ メッセージの VRF を変更するには、[VRF] フィールドでドロップダウン リストを使用して、ピアキープアライブ メッセージに使用する VRF を選択します。



(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 の作成と設定の詳細については、『Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 5.x』を参照してください。

e. ピアキープアライブ メッセージの UDP ポートを変更するには、[UDP Port] フィールドで、使用する UDP ポートの番号を入力します。

f. ピアキープアライブ メッセージの送信間隔を変更するには、[Interval] フィールドで、メッセージの送信間隔をミリ秒単位で入力します。

g. ピアキープアライブ メッセージのタイムアウト値を変更するには、[Timeout] フィールドで、数値を秒単位で入力します。

h. ピアキープアライブ メッセージのホールド タイムアウト値を変更するには、[Hold Timeout] フィールドで、数値を秒単位で入力します。この設定は DCNM Release 4.2 以降で使用できます。

i. ピアキープアライブ パケットの優先順位の値を変更するには、[Precedence] フィールドで、目的の優先順位の値を入力します。この設定は DCNM Release 4.2 以降で使用できます。

j. ピアキープアライブ パケットの ToS の値を変更するには、[Type of Service] フィールドで、目的の ToS の値を入力します。この設定は DCNM Release 4.2 以降で使用できます。

k. ピアキープアライブ パケットの ToS 優先順位の値を変更するには、[ToS Byte] フィールドで、目的の ToS 優先順位の値を入力します。この設定は DCNM Release 4.2 以降で使用できます。

- l. ロール プライオリティを変更するには、[Role Priority] フィールドで、目的の数値を入力します。
- m. システム プライオリティを変更するには、[System Priority] フィールドで、LACP のシステム プライオリティに使用する数値を入力します。
- n. システム MAC アドレスを変更するには、[System MAC Address] フィールドで、システム MAC アドレスに使用する数値を入力します。

**ステップ 4** 基本設定、レイヤ 2 設定、または vPC ピア リンクのリンク設定を変更するには、[Feature Selector] ペインで、[Interfaces] > [Logical] > [vPC] を選択し、次の手順を実行します。

- a. 設定を変更するチャンネルが強調表示されます。
- b. [Details] ペインの [vPC Details] をクリックします。  
単一シャーシ プライマリ vPC ピア リンクの設定のみを変更できます。単一シャーシ セカンダリ vPC ピア リンクが、変更された値で自動的に設定されます。
- c. 基本設定を変更するには、[Basic Setting] セクションをクリックします。
- d. レイヤ 2 設定を変更するには、[Layer 2] セクションをクリックします。
- e. リンク設定を変更するには、[Link Settings] セクションをクリックします。

**ステップ 5** vPC ドメイン ID を変更し、ピアキープアライブ設定を行い、vPC システムのプライオリティを設定するには、[Feature Selector] ペインで [Interfaces] > [Logical] > [vPC] を選択し、次の手順を実行します。

- a. [Details] ペインの [Peer-Link Details] をクリックします。
- b. [vPC Global Settings] セクションをクリックします。
- c. 変更する設定を選択し、[Single Chassis vPC End Point-Primary] 列に値を入力します。  
単一シャーシ セカンダリ vPC エンド ポイントが、同じ値で自動的に設定されます。

**ステップ 6** STP 設定を変更するには、[Feature Selector] ペインで、[Interfaces] > [Logical] > [vPC] を選択します。

- a. [Details] ペインの [Peer-Link Details] をクリックし、次の手順を実行します。
- b. [STP Global Settings] セクションをクリックします。
- c. 変更する設定を選択し、[Single Chassis vPC End Point-Primary] 列に値を入力します。  
単一シャーシ セカンダリ vPC エンド ポイントが、同じ値で自動的に設定されます。

**ステップ 7** (任意) メニュー バーで [File] > [Deploy] を選択して変更をデバイスに適用します。

## vPC の統計情報の表示

[Statistics] タブに次の vPC ピアキープアライブ パラメータが表示されます。

- vPC ピア デバイスに送信されるキープアライブ メッセージ数
- vPC ピア デバイスから受信するキープアライブ メッセージ数
- vPC キープアライブ メッセージからの応答を受信までの平均時間
- リモート vPC ピア デバイスへの到達に失敗した回数



(注)

## vPC のフィールドの説明

vPC の設定に次のフィールドの説明が使用されます。ここでは、次の内容について説明します。

- 「[vPC] : [vPC Details] : [Basic Settings] セクション」 (P.6-34)
- 「[vPC] : [vPC Details] : [Layer 2 Settings] セクション」 (P.6-35)
- 「[vPC] : [vPC Details] : [Link Settings] セクション」 (P.6-36)
- 「[vPC] : [Peer-Link Details] : [vPC Global Settings] セクション」 (P.6-37)
- 「[vPC] : [Peer-Link Details] : [STP Global Settings] セクション」 (P.6-37)
- 「[vPC] : [Peer-Link Status] : [Peer Link Status] セクション」 (P.6-38)
- 「[vPC] : [Peer-Link Status] : [Peer Link Error VLANs Status] セクション」 (P.6-39)
- 「[vPC] : [Peer-Link Status] : [vPC Error VLANs Status] セクション」 (P.6-39)
- 「[Resolve Configuration Inconsistency] : [vPC]」 (P.6-39)
- 「[Resolve Configuration Inconsistency] : [Peer Link]」 (P.6-42)

## [vPC] : [vPC Details] : [Basic Settings] セクション

表 6-1 [vPC] : [vPC Details] : [Basic Settings] セクション

フィールド	説明
Channel ID	表示のみ。ポート チャネル インターフェイスに割り当てられたポートチャネル番号。
Description	ポート チャネル インターフェイスの説明。
Port Mode	ポート チャネル インターフェイスのポート モードの設定。有効な値は次のとおりです。 <ul style="list-style-type: none"> <li>• Access</li> <li>• Trunk</li> </ul>
Bandwidth (kb)	ポート チャネル インターフェイスの帯域幅。このデフォルトは、インターフェイスのタイプによって設定されます。
Delay (tens of usec)	ポート チャネル インターフェイスの遅延時間。有効な範囲は 1 ～ 16777215 です。
Speed (Gb/s)	ポート チャネル インターフェイスの送信速度。有効な値は次のとおりです。 <ul style="list-style-type: none"> <li>• 10</li> <li>• 100</li> <li>• 1000</li> <li>• 10000</li> <li>• Auto</li> <li>• Nonnegotiate</li> </ul>

表 6-1 [vPC] : [vPC Details] : [Basic Settings] セクション (続き)

フィールド	説明
Duplex	ポート チャネル インターフェイスのデュプレックス モード。有効な値は次のとおりです。 <ul style="list-style-type: none"> <li>Half</li> <li>Full</li> <li>Auto</li> </ul>
MTU	ポート チャネル インターフェイスの最大伝送ユニット (MTU)。
Flow Control Receive	ポーズ フレームを受信するポート チャネル インターフェイスのステータス。有効な値は次のとおりです。 <ul style="list-style-type: none"> <li>On</li> <li>Off</li> <li>Desired</li> </ul>
Flow Control Send	ポーズ フレームを送信するポート チャネル インターフェイスのステータス。有効な値は次のとおりです。 <ul style="list-style-type: none"> <li>On</li> <li>Off</li> <li>Desired</li> </ul>

## [vPC] : [vPC Details] : [Layer 2 Settings] セクション

表 6-2 [vPC] : [vPC Details] : [Layer 2 Settings] セクション

フィールド	説明
Access VLAN	ポート チャネル インターフェイスのアクセス VLAN。
Allowed VLAN	ポート チャネル インターフェイスの許可 VLAN。
Native VLAN	ポート チャネル トランク インターフェイスのネイティブ VLAN。
STP port type	STP エッジまたはネットワーク ポート タイプ。有効な値は次のとおりです。 <ul style="list-style-type: none"> <li>Default</li> <li>Edge Access</li> <li>Edge Trunk</li> <li>Network</li> <li>Disable</li> </ul>
STP guard	設定された STP ガードの条件。有効な値は次のとおりです。 <ul style="list-style-type: none"> <li>Null string</li> <li>Loop</li> <li>Root</li> </ul>

## [vPC] : [vPC Details] : [Link Settings] セクション

表 6-3 [vPC] : [vPC Details] : [Link Settings] セクション

フィールド	説明
<b>最初の 4 つの列にローカル デバイスのリンクが表示されます。</b>	
Name	表示のみ。vPC 以外のデバイスのポート名。このポートはポート チャネル インターフェイスの一部です。
Mode	表示のみ。リンクのポート チャネル モード。有効な値は次のとおりです。 <ul style="list-style-type: none"> <li>• Active</li> <li>• Passive</li> <li>• On</li> </ul>
Priority	表示のみ。LACP に設定されたポート プライオリティ値。有効範囲は 1 ～ 65535 番です。
Status	表示のみ。リンクのステータス。有効な値は次のとおりです。 <ul style="list-style-type: none"> <li>• Up</li> <li>• Down</li> <li>• Bundled</li> <li>• Standalone</li> <li>• Suspended</li> <li>• Hot Standby</li> </ul>
<b>最後の 5 つの列に、vPC プライマリ デバイスおよびセカンダリ デバイスのリンクが表示されます。</b>	
Device	表示のみ。プライマリまたはセカンダリ vPC デバイスの名前。
Name	表示のみ。ポート チャネル インターフェイスの一部であるネイバー デバイスのポート名。
Mode	表示のみ。リンクのポート チャネル モード。有効な値は次のとおりです。 <ul style="list-style-type: none"> <li>• Active</li> <li>• Passive</li> <li>• On</li> </ul>
Priority	表示のみ。LACP に設定されたポート プライオリティ値。有効範囲は 1 ～ 65535 番です。
Status	表示のみ。リンクのステータス。有効な値は次のとおりです。 <ul style="list-style-type: none"> <li>• Up</li> <li>• Down</li> <li>• Bundled</li> <li>• Standalone</li> <li>• Suspended</li> <li>• Hot Standby</li> </ul>

## [vPC] : [Peer-Link Details] : [vPC Global Settings] セクション

表 6-4 [vPC] : [Peer-Link Details] : [vPC Global Settings] セクション

フィールド	説明
<b>Global Setting</b>	
Domain Id	表示のみ。vPC ドメイン ID。
System MAC Address	表示のみ。vPC システム MAC アドレス。
Role Priority	表示のみ。ピア リンクを形成するロール プライオリティ。指定できる範囲は 1 ～ 65536 で、デフォルトは 32667 です。
System Priority	表示のみ。vPC システム プライオリティ。指定できる範囲は 1 ～ 65536 で、デフォルトは 32667 です。
<b>Peer Keepalive Settings</b>	
Source IP	表示のみ。ローカル vPC ピア デバイスでピアキープアライブ メッセージを送信するために使用される範囲外の IP アドレス。
Destination IP	表示のみ。リモート vPC ピア デバイスでピアキープアライブ メッセージを送信するために使用される範囲外の IP アドレス。
UDP Port	表示のみ。ピアキープアライブ メッセージの交換に使用される UDP ポート。デフォルト値は 3200 です。
VRF	表示のみ。ピアキープアライブ メッセージを送信する範囲外のポートの VRF。デフォルト値は [management] です。
Interval	表示のみ。ピアキープアライブ メッセージの送信間隔。有効な範囲は 400 ～ 10000 ミリ秒です。デフォルト値は 1000 ミリ秒です。
Timeout	表示のみ。ピアキープアライブ メッセージのタイムアウト値。有効範囲は 3 ～ 20 秒で、デフォルト値は 5 秒です。

## [vPC] : [Peer-Link Details] : [STP Global Settings] セクション

表 6-5 [vPC] : [Peer-Link Details] : [STP Global Settings] セクション

フィールド	説明
Protocol	表示のみ。設定済み STP。有効な値は次のとおりです。 <ul style="list-style-type: none"> <li>• Rapid PVST+</li> <li>• MST</li> </ul>
Port Type	表示のみ。STP ポートのタイプ。有効な値は次のとおりです。 <ul style="list-style-type: none"> <li>• Edge</li> <li>• Network</li> <li>• Normal STP</li> </ul>
Path Cost	表示のみ。パス コスト計算方式。有効な値は次のとおりです。 <ul style="list-style-type: none"> <li>• Long</li> <li>• Short</li> </ul>

表 6-5 [vPC] : [Peer-Link Details] : [STP Global Settings] セクション (続き)

フィールド	説明
Bridge Assurance	表示のみ。Bridge Assurance の設定。有効な値は次のとおりです。 <ul style="list-style-type: none"> <li>Enabled</li> <li>Disabled</li> </ul>
Loop Guard	表示のみ。ループ ガードの設定。有効な値は次のとおりです。 <ul style="list-style-type: none"> <li>Enabled</li> <li>Disabled</li> </ul>
STP Enabled VLANs	表示のみ。STP がイネーブルになっている VLAN のリスト。
MST VLAN	表示のみ。MST インスタンスおよび対応する VLAN のリスト。

## [vPC] : [Peer-Link Status] : [Peer Link Status] セクション

表 6-6 [vPC] : [Peer-Link Status] : [Peer Link Status] セクション

フィールド	説明
Domain ID	表示のみ。vPC ドメイン ID。
vPC Consistency	表示のみ。ローカル vPC ピア デバイスの vPC のステータス。有効な値は次のとおりです。 <ul style="list-style-type: none"> <li>Ok</li> <li>Failed</li> </ul>
Reason	表示のみ。vPC ピア リンクの一貫性の障害の原因。 (注) このフィールドは、ステータスが [Ok] の場合には表示されません。
Peer-link Consistency	表示のみ。リモート vPC ピア デバイスの vPC のステータス。有効な値は次のとおりです。 <ul style="list-style-type: none"> <li>Ok</li> <li>Failed</li> </ul>
Reason	表示のみ。vPC ピア リンクの一貫性の障害の原因。 (注) このフィールドは、ステータスが [Ok] の場合には表示されません。
<b>Role Status</b>	
Role	表示のみ。動作ロール。有効な値は次のとおりです。 <ul style="list-style-type: none"> <li>Primary</li> <li>Secondary</li> </ul>
System Priority	表示のみ。vPC の動作システム プライオリティ。有効範囲は 1 ～ 65536 で、デフォルトは 32667 です。
System MAC Address	表示のみ。動作システム MAC アドレス。
<b>vPC Peer keepalive status</b>	
Destination IP	表示のみ。ピアキープアライブ メッセージを交換するために使用されるリモート vPC ピア デバイスの範囲外の IP アドレス。



表 6-6 [vPC] : [Peer-Link Status] : [Peer Link Status] セクション (続き)

フィールド	説明
Send Status	表示のみ。ピアキーブアライブ メッセージの送信に成功したステータス。 有効な値は次のとおりです。 <ul style="list-style-type: none"> <li>true</li> <li>false</li> </ul>
Receive Status	表示のみ。ピアキーブアライブ メッセージの受信に成功したステータス。 有効な値は次のとおりです。 <ul style="list-style-type: none"> <li>true</li> <li>false</li> </ul>

## [vPC] : [Peer-Link Status] : [Peer Link Error VLANs Status] セクション

表 6-7 [vPC] : [Peer-Link Status] : [Peer Link Error VLANs Status] セクション

フィールド	説明
VLAN ID	表示のみ。vPC ピア リンクで error-disabled 状態の VLAN。
Reason	表示のみ。vPC ピア リンクで VLAN が error-disabled 状態の原因。

## [vPC] : [Peer-Link Status] : [vPC Error VLANs Status] セクション

表 6-8 [vPC] : [Peer-Link Status] : [vPC Error VLANs Status] セクション

フィールド	説明
VLAN ID	表示のみ。vPC ピア リンクで error-disabled 状態の VLAN。
Reason	表示のみ。vPC ピア リンクで VLAN が error-disabled 状態の原因。

## [Resolve Configuration Inconsistency] : [vPC]

表 6-9 [Resolve Configuration Inconsistency] : [vPC]

フィールド	説明
<b>vPC Port Channel Settings</b>	
<b>Basic Settings</b>	
Channel ID	ポート チャネル インターフェイスに割り当てられたポートチャネル番号。
Description	ポート チャネル インターフェイスの説明。
Port Mode	ポート チャネル インターフェイスのポート モードの設定。有効な値は次のとおりです。 <ul style="list-style-type: none"> <li>Access</li> <li>Trunk</li> </ul>

表 6-9 [Resolve Configuration Inconsistency] : [vPC] (続き)

フィールド	説明
Bandwidth (kb)	ポート チャネル インターフェイスの帯域幅。デフォルトは、インターフェイスのタイプによって設定されます。
Delay (tens of usec)	ポート チャネル インターフェイスの遅延時間。有効な範囲は 1 ～ 16777215 です。
Speed (Gb/s)	ポート チャネル インターフェイスの送信速度。有効な値は次のとおりです。 <ul style="list-style-type: none"> <li>• 10</li> <li>• 100</li> <li>• 1000</li> <li>• 10000</li> <li>• Auto</li> <li>• Nonnegotiate</li> </ul>
Duplex	ポート チャネル インターフェイスのデュプレックス モード。有効な値は次のとおりです。 <ul style="list-style-type: none"> <li>• Half</li> <li>• Full</li> <li>• Auto</li> </ul>
MTU	ポート チャネル インターフェイスの最大伝送ユニット (MTU)。
Flow Control Receive	ポーズ フレームを受信するポート チャネル インターフェイスのステータス。有効な値は次のとおりです。 <ul style="list-style-type: none"> <li>• On</li> <li>• Off</li> <li>• Desired</li> </ul>
Flow Control Send	ポーズ フレームを送信するポート チャネル インターフェイスのステータス。有効な値は次のとおりです。 <ul style="list-style-type: none"> <li>• On</li> <li>• Off</li> <li>• Desired</li> </ul>
<b>Layer 2 Settings</b>	
Access VLAN	ポート チャネル インターフェイスのアクセス VLAN。
Allowed VLAN	ポート チャネル インターフェイスの許可 VLAN。
Native VLAN	ポート チャネル トランク インターフェイスのネイティブ VLAN。
STP port type	STP エッジまたはネットワーク ポート タイプ。有効な値は次のとおりです。 <ul style="list-style-type: none"> <li>• Default</li> <li>• Edge Access</li> <li>• Edge Trunk</li> <li>• Network</li> <li>• Disable</li> </ul>

表 6-9 [Resolve Configuration Inconsistency] : [vPC] (続き)

フィールド	説明
STP guard	設定された STP ガードの条件。有効な値は次のとおりです。 <ul style="list-style-type: none"> <li>Null string</li> <li>Loop</li> <li>Root</li> </ul>
<b>vPC Peer Keepalive</b>	
<b>Global Setting</b>	
Domain Id	vPC ドメイン ID。
System MAC Address	vPC システム MAC アドレス。
Role Priority	ピア リンクを形成するロール プライオリティ。指定できる範囲は 1 ～ 65536 で、デフォルトは 32667 です。
System Priority	vPC システム プライオリティ。指定できる範囲は 1 ～ 65536 で、デフォルトは 32667 です。
<b>Peer Keepalive Settings</b>	
UDP Port	ピアキープアライブ メッセージの交換に使用される UDP ポート。デフォルト値は 3200 です。
Interval	ピアキープアライブ メッセージの送信間隔。有効な範囲は 400 ～ 10000 ミリ秒です。デフォルト値は 1000 ミリ秒です。
<b>STP Global Settings</b>	
Protocol	設定済み STP。有効な値は次のとおりです。 <ul style="list-style-type: none"> <li>Rapid PVST+</li> <li>MST</li> </ul>
Port Type	STP ポートのタイプ。有効な値は次のとおりです。 <ul style="list-style-type: none"> <li>Edge</li> <li>Network</li> <li>Normal STP</li> </ul>
Path Cost	パス コスト計算方式。有効な値は次のとおりです。 <ul style="list-style-type: none"> <li>Long</li> <li>Short</li> </ul>
Bridge Assurance	Bridge Assurance の設定。有効な値は次のとおりです。 <ul style="list-style-type: none"> <li>Enabled</li> <li>Disabled</li> </ul>
Loop Guard	ループ ガードの設定。有効な値は次のとおりです。 <ul style="list-style-type: none"> <li>Enabled</li> <li>Disabled</li> </ul>
STP Enabled VLANs	STP がイネーブルになっている VLAN のリスト。
MST VLAN	MST インスタンスおよび対応する VLAN のリスト。

## [Resolve Configuration Inconsistency] : [Peer Link]

表 6-10 [Resolve Configuration Inconsistency] : [Peer Link]

フィールド	説明
<b>vPC Peer Keepalive</b>	
<b>Global Setting</b>	
Domain Id	vPC ドメイン ID。
System MAC Address	vPC システム MAC アドレス。
Role Priority	ピア リンクを形成するロール プライオリティ。指定できる範囲は 1 ～ 65536 で、デフォルトは 32667 です。
System Priority	vPC システム プライオリティ。指定できる範囲は 1 ～ 65536 で、デフォルトは 32667 です。
<b>Peer Keepalive Settings</b>	
UDP Port	ピアキープアライブ メッセージの交換に使用される UDP ポート。デフォルト値は 3200 です。
Interval	ピアキープアライブ メッセージの送信間隔。有効な範囲は 400 ～ 10000 ミリ秒です。デフォルト値は 1000 ミリ秒です。
<b>Global STP Settings</b>	
Protocol	設定済み STP。有効な値は次のとおりです。 <ul style="list-style-type: none"> <li>• Rapid PVST+</li> <li>• MST</li> </ul>
Port Type	STP ポートのタイプ。有効な値は次のとおりです。 <ul style="list-style-type: none"> <li>• Edge</li> <li>• Network</li> <li>• Normal STP</li> </ul>
Path Cost	パス コスト計算方式。有効な値は次のとおりです。 <ul style="list-style-type: none"> <li>• Long</li> <li>• Short</li> </ul>
Bridge Assurance	Bridge Assurance の設定。有効な値は次のとおりです。 <ul style="list-style-type: none"> <li>• Enabled</li> <li>• Disabled</li> </ul>
Loop Guard	ループ ガードの設定。有効な値は次のとおりです。 <ul style="list-style-type: none"> <li>• Enabled</li> <li>• Disabled</li> </ul>
STP Enabled VLANs	STP がイネーブルになっている VLAN のリスト。
MST VLAN	MST インスタンスおよび対応する VLAN のリスト。

## その他の関連資料

vPC を実装する方法の詳細については、次の項目を参照してください。

- 「関連資料」(P.6-43)
- 「標準規格」(P.6-43)
- 「管理情報ベース (MIB)」(P.6-43)

## 関連資料

関連項目	参照先
ポート チャネルの設定	第 5 章「ポート チャネルの設定」
レイヤ 2 インターフェイスの設定	第 3 章「レイヤ 2 インターフェイスの設定」
レイヤ 3 インターフェイスの設定	第 4 章「レイヤ 3 インターフェイスの設定」
共有および専用ポート	第 2 章「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	『Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 5.x』
システム管理	『Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 5.x』
ハイ アベイラビリティ	『Cisco Nexus 7000 Series NX-OS High Availability and Redundancy Guide, Release 5.x』
リリース ノート	『Cisco DCNM Release Notes, Release 5.x』

## 標準規格

標準規格	タイトル
IEEE 802.3ad	—

## 管理情報ベース (MIB)

管理情報ベース (MIB)	MIB リンク
<ul style="list-style-type: none"><li>• IEEE8023-LAG-CAPABILITY</li><li>• CISCO-LAG-MIB</li></ul>	Management Information Base (MIB; 管理情報ベース) を検索およびダウンロードするには、次の URL にアクセスしてください。 <a href="http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml">http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</a>

## vPC の設定機能の履歴

表 6-11 は、この機能のリリースの履歴です。

表 6-11 vPC の設定機能の履歴

機能名	リリース	機能情報
vPC	4.1(2)	これらの機能が導入されました。
vPC	4.1(4)	サポートが 192 vPC にまで増えました。
vPC	4.2(1)	サポートが 256 vPC にまで増えました。
vPC	4.2(1)	ピアキーブアライブ メッセージおよびロール プライオリティおよびシステム プライオリティを設定するためのウィザード機能が追加されました。
vPC	4.2(1)	ピアキーブアライブ メッセージのホールド時間および優先順位の値のための設定が追加されました。



# CHAPTER 7

## IP トンネルの設定



(注)

管理対象デバイス上で実行される Cisco NX-OS リリースでは、この章で説明する機能や設定がすべてサポートされるとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースのマニュアルとリリース ノートを参照してください。

この章では、Cisco Nexus 7000 シリーズ デバイスで Generic Route Encapsulation (GRE) を使って IP トンネルを設定する手順について説明します。

この章では、次の内容について説明します。

- 「IP トンネルについて」 (P.7-1)
- 「IP トンネルのライセンス要件」 (P.7-3)
- 「IP トンネルの前提条件」 (P.7-4)
- 「注意事項および制約事項」 (P.7-4)
- 「IP トンネルの設定」 (P.7-4)
- 「トンネル インターフェイス統計情報の表示」 (P.7-6)
- 「トンネル インターフェイスのためのフィールドの説明」 (P.7-7)
- 「その他の関連資料」 (P.7-8)
- 「IP トンネル設定の機能履歴」 (P.7-8)

## IP トンネルについて

IP トンネルを使うと、同じレイヤまたは上位レイヤ 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。

ここでは、次の内容について説明します。

- 「IP トンネルの概要」 (P.7-2)
- 「GRE トンネル」 (P.7-2)
- 「Path MTU Discovery (PMTUD)」 (P.7-3)
- 「バーチャライゼーションのサポート」 (P.7-3)
- 「ハイ アベイラビリティ」 (P.7-3)

## 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。

詳細については、「[IP トンネルの設定](#)」(P.7-4) を参照してください。

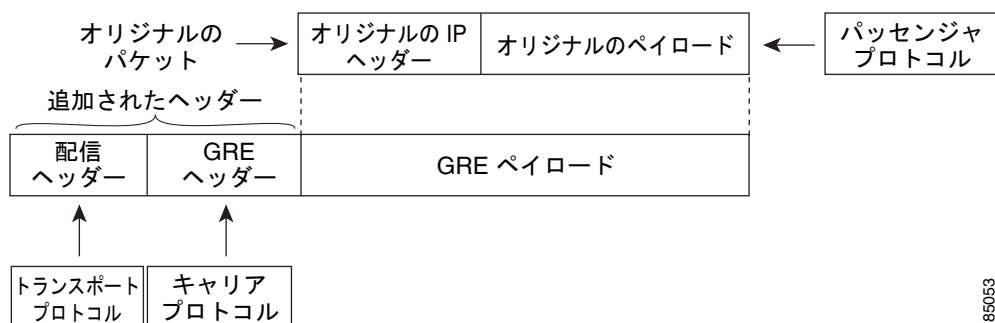
設定の前にトンネル機能をイネーブルにする必要があります。Cisco NX-OS Release 4.2 から、システムは機能のディセーブル化の前に自動的にチェックポイントを作成するため、このチェックポイントにロールバックできます。ロールバックとチェックポイントについては、『*Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 5.x*』を参照してください。

## 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。

図 7-1 に、GRE トンネルの IP トンネル コンポーネントを示します。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 7-1 GRE Protocol Data Unit (PDU)



185053



## Path MTU Discovery (PMTUD)

Path Maximum Transmission Unit (MTU; 最大伝送ユニット) Discovery (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 Internet Control Message Protocol (ICMP; インターネット制御メッセージプロトコル) 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。

## バーチャライゼーションのサポート

IP トンネルはデフォルトの Virtual Device Context (VDC; 仮想デバイス コンテキスト) およびデフォルトの Virtual Routing and Forwarding (VRF; 仮想ルーティング/転送) インスタンスにだけ設定できます。

Cisco DCNM Release 4.2 以降では、トンネル インターフェイスは VDC のメンバとして設定できます。VDC を特別に設定しない限り、デフォルトでは、Cisco DCNM のデフォルトの VDC およびデフォルトの VRF が使用されます。ある VDC に設定されたトンネルは、同じ番号を持つ別の VDC に設定されたトンネルとは区別されます。たとえば、VDC 1 のトンネル 0 は VDC 2 のトンネル 0 とは異なります。

VDC については、『Cisco DCNM Virtual Device Context Configuration Guide, Release 5.x』を、VRF については、『Cisco DCNM Unicast Routing Configuration Guide, Release 5.x』を参照してください。

## ハイ アベイラビリティ

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 トンネルのライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
DCNM	IP トンネルには LAN Enterprise ライセンスが必要です。DCNM ライセンス方式について、およびライセンスの取得方法と適用方法についての詳細は、『Cisco DCNM Fundamentals Configuration Guide, Release 5.x』を参照してください。
Cisco NX-OS	IP トンネルには Enterprise Services ライセンスが必要です。Cisco NX-OS ライセンス方式について、およびライセンスの取得方法と適用方法についての詳細については、『Cisco Nexus 7000 Series NX-OS Licensing Guide, Release 5.x』を参照してください。

## 注意事項および制約事項

- 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こと。
- Cisco NX-OS の Enterprise Services ライセンスをインストールしていること。
- DCNM の LAN Enterprise ライセンスをインストールしていること。
- IP トンネルを設定してイネーブルにする前にデバイスのトンネリング機能をイネーブルにしておくこと。

## IP トンネルの設定

- 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。
- トンネル インターフェイスとトンネル転送の両方は、同一の VRF 内になければなりません。そうでない場合は、ハードウェア データパスにエラーが発生します。

インターフェイス機能を選択すると、IP トンネルにアクセスできます。図 7-2 に、IP トンネルの設定方法を示します。

The screenshot shows the Palo Alto Networks Manager (PAN-OS 7.1.2) interface. The left sidebar displays the configuration tree with 'Network' selected. The main pane shows the 'Tunnel' configuration page. A table lists the tunnel configuration:

Tunnel Name	Tunnel Type	IP Address Profile	Interface	Local Endpoint
tunnel1 (172.16.255.255)				IP 4.4.4.4 (Phy0)

Below the table, the 'Settings' tab is active, showing the message 'Tunnel Service is disabled in device' and a link to 'Enable Tunnel Service'.

- 「トンネリングのイネーブル化」 (P.7-5)
- 「トンネル インターフェイスの作成」 (P.7-5)
- 「トンネル インターフェイスの削除」 (P.7-6)

## 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。

### 手順の詳細

トンネリング機能をイネーブルにするには、次の手順を実行します。

- 
- |        |  |
|--------|--|
| ステップ 1 | [Feature Selector] ペインの [Interfaces] > [Logical] > [Tunnel] を選択します。<br>[Summary] ペインに使用可能なデバイスが表示されます。 |
| ステップ 2 | [Summary] ペインの IP トンネリングをイネーブルにするデバイスをダブルクリックします。  |
| ステップ 3 | [Details] ペインに [Enable Tunnel Service] リンクが表示されている場合、これをクリックします。                                       |
| ステップ 4 | メニュー バーの [File] > [Deploy] を選択して、変更をデバイスに適用します。  |
- 

## 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。

### 作業を開始する前に

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。

### 手順の詳細

トンネル インターフェイスを作成するには、次の手順を実行します。

- 
- |        |  |
|--------|--|
| ステップ 1 | [Feature Selector] ペインの [Interfaces] > [Logical] > [Tunnel] を選択します。<br>[Summary] ペインに使用可能なデバイスが表示されます。 |
| ステップ 2 | [Summary] ペインの既存のトンネルのリストに表示するデバイスをダブルクリックします。   |
| ステップ 3 | メニュー バーの [Actions] > [New Tunnel] を選択します。<br>[Summary] ペインで新しいトンネルが強調表示され、[Details] ペインでタブが更新されます。     |
| ステップ 4 | 強調表示されたトンネルのフィールドで、トンネル番号を入力します。<br>番号の範囲は 0 ～ 32767 です。   |
| ステップ 5 | [Details] ペインの [Tunnel Details] タブをクリックします。<br>[Tunnel Details] タブが表示されます。                             |
| ステップ 6 | [Tunnel Details] タブの [General] セクションを展開します。<br>[Details] ペインにトンネルの全般的な情報が表示されます。                       |
| ステップ 7 | (任意) [General] セクションの [IP Address] フィールドで、このトンネル インターフェイスの IPv4 アドレスを設定します。                            |
| ステップ 8 | (任意) [Network Mask] フィールドで、この IPv4 アドレスのネットワーク マスクをドット付き 10 進表記で設定します。                                 |

- ステップ 9** (任意) [IPv6 Address] フィールドの [Primary/Prefix length] フィールドで、このトンネル インターフェイスの IPv6 アドレスとプレフィックスの長さを設定します。
- 長さの範囲は 1 ～ 128 です。
- ステップ 10** (任意) [Description] フィールドで、このトンネルを説明する文字列を入力します。
- 文字列は 1 ～ 97 文字の英数字にする必要があります。
- ステップ 11** [Details] タブの [Source] セクションを展開します。
- トンネルの送信元および宛先が [Details] ペインに表示されます。
- ステップ 12** ローカル エンドポイント領域で、トンネルの送信元として動作するインターフェイスまたは IP アドレスを選択します。
- ステップ 13** リモート エンドポイント領域で、トンネルの宛先として動作するホストまたは IP アドレスを選択します。
- ステップ 14** メニュー バーの [File] > [Deploy] を選択して、変更をデバイスに適用します。

## トンネル インターフェイスの削除

トンネル インターフェイスは削除できます。

### 手順の詳細

トンネル インターフェイスを削除するには、次の手順を実行します。

- ステップ 1** [Feature Selector] ペインの [Interfaces] > [Logical] > [Tunnel] を選択します。
- [Summary] ペインに使用可能なデバイスが表示されます。
- ステップ 2** [Summary] ペインの既存のトンネルのリストに表示するデバイスをダブルクリックします。
- ステップ 3** 削除するトンネルをクリックします。
- ステップ 4** メニュー バーで [Actions] > [Delete Tunnel] を選択します。
- ステップ 5** 確認を求めるポップアップ ウィンドウで [Yes] をクリックし、変更をデバイスに適用します。

## トンネル インターフェイス 統計情報の表示

トンネル インターフェイス 統計情報を収集するように DCNM を設定できます。[Feature Selector] ペインで、[Interfaces] > [Logical] > [Tunnel] を選択し、統計情報を収集するインターフェイスに移動します。

[Port Traffic Statistics] ウィンドウが表示されます。入力および出力（パケットおよびバイト）カウンタ、ブロードキャスト、マルチキャスト、およびユニキャスト トラフィックについての統計情報を収集できます。

レイヤ 3 インターフェイスの統計情報収集の詳細については、『Cisco DCNM Fundamentals Configuration Guide, Release 5.x』を参照してください。

## トンネル インターフェイスのためのフィールドの説明

ここでは、トンネル インターフェイスの次のフィールドについて説明します。

- 「[Tunnel] : [Details] タブ : [Tunnel Details] セクション」 (P.7-7)
- 「[Tunnels] : [Details] タブ : [Source] セクション」 (P.7-7)
- 「[Tunnels] : [Statistics] タブ」 (P.7-8)

### [Tunnel] : [Details] タブ : [Tunnel Details] セクション

表 7-1 [Tunnel] : [Details] : [Tunnel]

フィールド	説明
Device	表示のみ。トンネル インターフェイスが存在しているデバイス名。
Tunnel ID	表示のみ。トンネル インターフェイスの番号。
Description	トンネル インターフェイスを説明する文字列。
Admin Status	トンネル インターフェイスの管理ステータス。デフォルトは down です。
Oper Status	トンネル インターフェイスの動作ステータス。
MTU	このトンネルの MTU 値。
IP Address	ドット付き 10 進表記の IPv4 アドレス。
Net mask	ドット付き 10 進表記の IPv4 アドレスのネットワーク マスク。
IPv6 Address	x:x:x::x/length 形式の IPv6 プレフィクス。

### [Tunnels] : [Details] タブ : [Source] セクション

表 7-2 [Tunnels] : [Details] : [Source]

フィールド	説明
<b>Local Endpoint</b>	
Interface	トンネルの送信元アドレスのインターフェイス。
IP Address	トンネルの送信元アドレスのドット付き 10 進表記の IPv4 アドレス。
<b>Remote Endpoint</b>	
Host Name	トンネルの宛先のデバイス名。
IP Address	トンネルの宛先アドレスのドット付き 10 進表記の IPv4 アドレス。

## [Tunnels] : [Statistics] タブ

表 7-3 [Tunnels] : [Statistics] タブ

フィールド	説明
Status	統計情報の収集のステータス。[Status] にマウスのカーソルを合わせると、ポップアップのヒントが表示されます。
Select Parameters	トンネル インターフェイスで収集できる統計情報のリスト。
Show Overview Chart	統計情報の概要のポップアップ。

## その他の関連資料

IP トンネルの実装に関する追加情報については、次の項を参照してください。

- 「関連資料」(P.7-8)
- 「標準規格」(P.7-8)

## 関連資料

関連項目	参照先
IP トンネル コマンド	『Cisco Nexus 7000 Series NX-OS Interfaces Command Reference, Release 5.x』
IP フラグメンテーションおよび Path MTU Discovery	『Resolve IP Fragmentation, MTU, MSS, and PMTUD Issues with GRE and IPSEC』

## 標準規格

標準規格	タイトル
この機能でサポートされる新規または改訂された標準規格はありません。また、この機能による既存の標準規格サポートの変更はありません。	—

## IP トンネル設定の機能履歴

表 7-4 は、この機能のリリースの履歴です。

表 7-4 IP トンネル設定の機能履歴

機能名	リリース	機能情報
IP トンネル	4.0(1)	この機能が導入されました。
デフォルト以外の VDC 内の IP トンネル	4.2(1)	この機能が導入されました。



## CHAPTER 8

# 仮想イーサネット インターフェイスの設定

この章では、Cisco Data Center Network Manager (DCNM) で仮想イーサネット (vEthernet または vEth) インターフェイスを設定する方法を説明します。

この章では、次の内容について説明します。

- 「vEthernet インターフェイスについて」 (P.8-1)
- 「vEthernet インターフェイスのライセンス要件」 (P.8-2)
- 「プラットフォーム サポート」 (P.8-2)
- 「vEthernet インターフェイスの設定」 (P.8-2)
- 「vEthernet インターフェイスのためのフィールドの説明」 (P.8-13)
- 「その他の関連資料」 (P.8-15)
- 「vEthernet インターフェイスの機能の履歴」 (P.8-16)

## vEthernet インターフェイスについて

仮想イーサネット (vEthernet または vEth) インターフェイスは、論理インターフェイスです。各 vEthernet インターフェイスは、仮想ポートに接続されたスイッチ インターフェイスに対応します。次のインターフェイス タイプがあります。

- 仮想マシン (VM) (VM NIC に接続されるインターフェイス)
- サービス コンソール
- vmkernel

vEthernet インターフェイスは Cisco DC-OS で作成され、分散仮想スイッチで使用する仮想ポートを示します。



(注)

仮想イーサネット インターフェイス機能に対するシステム メッセージのログ レベルは、Cisco DCNM の要件以上でなければなりません。デバイス検出時に、ログ レベルが不適切であることが検出された場合は、最低限必要なレベルまで Cisco DCNM によって自動的に引き上げられます。ただし、Cisco Nexus 7000 シリーズ スイッチで Cisco NX-OS Release 4.0 を実行する場合は例外です。Cisco NX-OS Release 4.0 の場合は、デバイス検出の前に、コマンドライン インターフェイスを使用してログ レベルを Cisco DCNM の要件以上となるように設定してください。詳細については、『Cisco DCNM Fundamentals Configuration Guide, Release 5.x』を参照してください。

## vEthernet インターフェイスのライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
Cisco DCNM	vEthernet インターフェイスにはライセンスは不要です。ライセンス パッケージに含まれていない機能は Cisco DCNM にバンドルされており、無料で使用できます。Cisco DCNM LAN エンタープライズ ライセンスの取得とインストールの詳細については、『 <i>Cisco DCNM Fundamentals Configuration Guide, Release 5.x</i> 』を参照してください。
Cisco NX-OS	vEthernet インターフェイスにはライセンスは不要です。ライセンス パッケージに含まれていない機能はすべて Cisco NX-OS システム イメージにバンドルされており、追加費用は一切発生しません。各プラットフォームの Cisco NX-OS ライセンス スキームの説明については、そのプラットフォームのライセンス ガイドを参照してください。

## プラットフォーム サポート

この機能をサポートするプラットフォームは次のとおりです。ガイドラインと制限事項、システム デフォルト値、設定制限などのプラットフォーム固有の情報については、対応するマニュアルを参照してください。

プラットフォーム	マニュアル
Cisco Nexus 1000V シリーズ スイッチ	<a href="#">Cisco Nexus 1000V シリーズ スイッチ マニュアル</a>

## vEthernet インターフェイスの設定

vEthernet インターフェイスの設定を Cisco DCNM で行うことができます。

ここでは、次の内容について説明します。

- 「[vEthernet インターフェイスのグローバル設定](#)」(P.8-3)
- 「[vEthernet インターフェイスの説明の設定](#)」(P.8-3)
- 「[vEthernet インターフェイスの VMware DVPort ID の設定](#)」(P.8-4)
- 「[vEthernet インターフェイスの静的ピン接続の設定](#)」(P.8-5)
- 「[vEthernet アクセス インターフェイスの設定](#)」(P.8-6)
- 「[vEthernet トランク インターフェイスの設定](#)」(P.8-7)
- 「[vEthernet インターフェイスでのプライベート VLAN の設定](#)」(P.8-8)
- 「[vEthernet インターフェイスの IPv4 ACL の設定](#)」(P.8-9)
- 「[vEthernet インターフェイスでの MAC ACL の設定](#)」(P.8-9)
- 「[vEthernet インターフェイスでの SPAN の設定](#)」(P.8-10)
- 「[vEthernet インターフェイスのイネーブル化またはディセーブル化](#)」(P.8-11)
- 「[vEthernet インターフェイスの概要の表示](#)」(P.8-11)
- 「[vEthernet インターフェイス ポートのステータスの表示](#)」(P.8-12)
- 「[vEthernet インターフェイス統計情報の表示](#)」(P.8-12)
- 「[仮想イーサネット モジュールの統計情報の表示](#)」(P.8-12)



## vEthernet インターフェイスのグローバル設定

vEthernet インターフェイスの設定や、非アクティブな vEthernet インターフェイスの削除、重複している vEthernet インターフェイス アクティベーションの接続解除が自動的に行われるようにデバイスを設定できます。

### 手順の詳細

- 
- |               |   |
|---------------|---|
| <b>ステップ 1</b> | [Feature Selector] ペインで、[Interfaces] > [Logical] > [Virtual Ethernet] を選択します。<br>この機能をサポートするデバイスが [Summary] ペインに一覧表示されます。 |
| <b>ステップ 2</b> | [Summary] ペインで、目的のデバイスを選択します。   |
| <b>ステップ 3</b> | [Details] ペインの [Device Details] タブをクリックします。   |
| <b>ステップ 4</b> | (任意) vEthernet インターフェイスを自動的に設定するようにデバイスを設定するには、[Auto Setup] をクリックします。   |
| <b>ステップ 5</b> | (任意) 非アクティブな vEthernet インターフェイスを自動的に削除するようにデバイスを設定するには、[Auto Delete] をクリックします。  |
| <b>ステップ 6</b> | (任意) 重複している vEthernet インターフェイス アクティベーションを自動的に接続解除するようにデバイスを設定するには、[Force Detach] をクリックします。                                |
| <b>ステップ 7</b> | メニュー バーで [File] > [Deploy] を選択して、変更をデバイスに適用します。   |
- 

## vEthernet インターフェイスの説明の設定

vEthernet インターフェイスの説明を設定できます。vEthernet インターフェイスに説明を追加しない場合、次のいずれかの説明が接続時に追加されます。説明を追加し、その後で削除する場合、次のいずれかの説明がインターフェイスに追加されます。

- VM の場合：VM 名、ネットワーク アダプタ番号
- VMK の場合：VMware VMkernel、vmk 番号
- VSWIF の場合：VMware Service Console、vswif 番号

### 手順の詳細

- 
- |               |   |
|---------------|---|
| <b>ステップ 1</b> | [Feature Selector] ペインで、[Interfaces] > [Logical] > [Virtual Ethernet] を選択します。<br>この機能をサポートするデバイスが [Summary] ペインに一覧表示されます。   |
| <b>ステップ 2</b> | [Summary] ペインで、目的のデバイスを展開します。<br>vEthernet インターフェイスが保存されているフォルダが表示されます。<br><br>デフォルトでは、vEthernet インターフェイスが、属している Virtual Ethernet Module (VEM; 仮想イーサネット モジュール) に従ってグループ化されます。また、[Summary] ペインの右上にある [VEM-VM-VETH] をクリックして、関連付けられた Virtual Machine (VM; 仮想マシン) に従ってグループ化することもできます。<br><br>[Unknown] という名前のフォルダにネットワーク インターフェイス カードに関連付けられていない (参加していないインターフェイスとも呼ばれる) vEthernet インターフェイスが保存されます。 |
| <b>ステップ 3</b> | 目的のフォルダを展開します。  |

- ステップ 4 目的のインターフェイスを選択します。
- ステップ 5 [Details] ペインの [Port Details] タブをクリックします。
- ステップ 6 [Basic Settings] の内容を展開します。
- ステップ 7 [Description] フィールドに、インターフェイスの説明を入力します。
- ステップ 8 メニュー バーで [File] > [Deploy] を選択して、変更をデバイスに適用します。

## vEthernet インターフェイスの VMware DVPort ID の設定

ネットワーク インターフェイス カードに関連付けられていない（参加していないインターフェイスとも呼ばれる）vEthernet インターフェイスの VMware DVPort ID を設定できます。このようなインターフェイスは [Unknown] フォルダにグループ化されます。

### 作業を開始する前に

デフォルトの説明を割り当てない場合、説明を付けて vEthernet インターフェイスを設定します。詳細については、「[vEthernet インターフェイスの説明の設定](#)」(P.8-3) を参照してください。

### 手順の詳細

- ステップ 1 [Feature Selector] ペインで、[Interfaces] > [Logical] > [Virtual Ethernet] を選択します。  
この機能をサポートするデバイスが [Summary] ペインに一覧表示されます。
- ステップ 2 [Summary] ペインで、目的のデバイスを展開します。  
vEthernet インターフェイスが保存されているフォルダが表示されます。  
デフォルトでは、vEthernet インターフェイスが、属している Virtual Ethernet Module (VEM; 仮想イーサネット モジュール) に従ってグループ化されます。また、[Summary] ペインの右上にある [VEM-VM-VETH] をクリックして、関連付けられた Virtual Machine (VM; 仮想マシン) に従ってグループ化することもできます。
- ステップ 3 [Unknown] フォルダを展開します。
- ステップ 4 目的のインターフェイスを選択します。
- ステップ 5 [Details] ペインの [Port Details] タブをクリックします。
- ステップ 6 [Basic Settings] の内容を展開します。
- ステップ 7 [VMware DVPort ID] フィールドに、1 ～ 4294967294 の範囲で ID 番号を入力します。
- ステップ 8 メニュー バーで [File] > [Deploy] を選択して、変更をデバイスに適用します。

## vEthernet インターフェイスの静的ピン接続の設定

vEthernet インターフェイスに静的ピン接続を設定できます。

### 作業を開始する前に

デフォルトの説明を割り当てない場合、説明を付けて vEthernet インターフェイスを設定します。詳細については、「[vEthernet インターフェイスの説明の設定](#)」(P.8-3) を参照してください。

### 手順の詳細

- 
- |               |   |
|---------------|---|
| <b>ステップ 1</b> | [Feature Selector] ペインで、[Interfaces] > [Logical] > [Virtual Ethernet] を選択します。<br>この機能をサポートするデバイスが [Summary] ペインに一覧表示されます。   |
| <b>ステップ 2</b> | [Summary] ペインで、目的のデバイスを展開します。<br>vEthernet インターフェイスが保存されているフォルダが表示されます。<br><br>デフォルトでは、vEthernet インターフェイスが、属している Virtual Ethernet Module (VEM; 仮想イーサネット モジュール) に従ってグループ化されます。また、[Summary] ペインの右上にある [VEM-VM-VETH] をクリックして、関連付けられた Virtual Machine (VM; 仮想マシン) に従ってグループ化することもできます。<br><br>[Unknown] という名前のフォルダにネットワーク インターフェイス カードに関連付けられていない (参加していないインターフェイスとも呼ばれる) vEthernet インターフェイスが保存されます。 |
| <b>ステップ 3</b> | 目的のフォルダを展開します。  |
| <b>ステップ 4</b> | 目的のインターフェイスを選択します。  |
| <b>ステップ 5</b> | [Details] ペインの [Port Details] タブをクリックします。   |
| <b>ステップ 6</b> | [Basic Settings] の内容を展開します。   |
| <b>ステップ 7</b> | [Pinning ID] フィールドに、1 ～ 31 の範囲で ID 番号を入力します。  |
| <b>ステップ 8</b> | メニュー バーで [File] > [Deploy] を選択して、変更をデバイスに適用します。   |
-

## vEthernet アクセス インターフェイスの設定

vEthernet インターフェイスをアクセス インターフェイスとして使用するよう設定できます。

### 作業を開始する前に

デフォルトの説明を割り当てない場合、説明を付けて vEthernet インターフェイスを設定します。詳細については、「[vEthernet インターフェイスの説明の設定](#)」(P.8-3) を参照してください。

アクセス ポートは、タグなしの 1 つの VLAN だけのパケットを送信します。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 VLAN1 です。

### 手順の詳細

- 
- ステップ 1** [Feature Selector] ペインで、[Interfaces] > [Logical] > [Virtual Ethernet] を選択します。  
この機能をサポートするデバイスが [Summary] ペインに一覧表示されます。
- ステップ 2** [Summary] ペインで、目的のデバイスを展開します。  
vEthernet インターフェイスが保存されているフォルダが表示されます。  
デフォルトでは、vEthernet インターフェイスが、属している Virtual Ethernet Module (VEM; 仮想イーサネット モジュール) に従ってグループ化されます。また、[Summary] ペインの右上にある [VEM-VM-VETH] をクリックして、関連付けられた Virtual Machine (VM; 仮想マシン) に従ってグループ化することもできます。  
[Unknown] という名前のフォルダにネットワーク インターフェイス カードに関連付けられていない (参加していないインターフェイスとも呼ばれる) vEthernet インターフェイスが保存されます。
- ステップ 3** 目的のフォルダを展開します。
- ステップ 4** 目的のインターフェイスを選択します。
- ステップ 5** [Details] ペインの [Port Details] タブをクリックします。
- ステップ 6** [Port Mode Settings] の内容を展開します。
- ステップ 7** [Mode] ドロップダウン リストで [Access] を選択します。
- ステップ 8** [Access VLAN] ドロップダウン リストで、次のいずれかを実行します。
- 既存の VLAN を選択し、[OK] をクリックします。
  - [Assign a new VLAN ID] フィールドで、新しい VLAN ID を入力し、必要に応じて [Create in the device] を選択します。[OK] をクリックします。
- ステップ 9** メニュー バーで [File] > [Deploy] を選択して、変更をデバイスに適用します。
-

## vEthernet トランク インターフェイスの設定

vEthernet インターフェイスをトランク インターフェイスとして使用するよう設定できます。

### 作業を開始する前に

デフォルトの説明を割り当てない場合、説明を付けて vEthernet インターフェイスを設定します。詳細については、「[vEthernet インターフェイスの説明の設定](#)」(P.8-3) を参照してください。

### 手順の詳細

- 
- ステップ 1** [Feature Selector] ペインで、[Interfaces] > [Logical] > [Virtual Ethernet] を選択します。  
この機能をサポートするデバイスが [Summary] ペインに一覧表示されます。
- ステップ 2** [Summary] ペインで、目的のデバイスを展開します。  
vEthernet インターフェイスが保存されているフォルダが表示されます。  
デフォルトでは、vEthernet インターフェイスが、属している Virtual Ethernet Module (VEM; 仮想イーサネット モジュール) に従ってグループ化されます。また、[Summary] ペインの右上にある [VEM-VM-VETH] をクリックして、関連付けられた Virtual Machine (VM; 仮想マシン) に従ってグループ化することもできます。  
[Unknown] という名前のフォルダにネットワーク インターフェイス カードに関連付けられていない (参加していないインターフェイスとも呼ばれる) vEthernet インターフェイスが保存されます。
- ステップ 3** 目的のフォルダを展開します。
- ステップ 4** 目的のインターフェイスを選択します。
- ステップ 5** [Details] ペインの [Port Details] タブをクリックします。
- ステップ 6** [Port Mode Settings] の内容を展開します。
- ステップ 7** [Mode] ドロップダウン リストで [Trunk] を選択します。
- ステップ 8** [Allowed VLAN] ドロップダウン リストで、次のいずれかを選択します。
- (1-3967, 4048-4093) : 許可 VLAN として、VLAN 1 ~ 3967 および 4048 ~ 4093 を指定します。
  - None : 許可 VLAN として、何も指定しません。
  - Specific : 使用可能な VLAN のリストから 1 つまたは複数の VLAN を選択できます。
- ステップ 9** [Native VLAN] ドロップダウン リストで、次のいずれかを実行します。
- 既存の VLAN を選択し、[OK] をクリックします。
  - [Assign a new VLAN ID] フィールドで、新しい VLAN ID を入力し、必要に応じて [Create in the device] を選択します。[OK] をクリックします。
- ステップ 10** メニュー バーで [File] > [Deploy] を選択して、変更をデバイスに適用します。
-

## vEthernet インターフェイスでのプライベート VLAN の設定

vEthernet インターフェイスで Private VLAN (PVLAN; プライベート VLAN) を設定できます。

### 作業を開始する前に

デフォルトの説明を割り当てない場合、説明を付けて vEthernet インターフェイスを設定します。詳細については、「[vEthernet インターフェイスの説明の設定](#)」(P.8-3) を参照してください。

### 手順の詳細

- 
- ステップ 1** [Feature Selector] ペインで、[Interfaces] > [Logical] > [Virtual Ethernet] を選択します。  
この機能をサポートするデバイスが [Summary] ペインに一覧表示されます。
- ステップ 2** [Summary] ペインで、目的のデバイスを展開します。  
vEthernet インターフェイスが保存されているフォルダが表示されます。  
デフォルトでは、vEthernet インターフェイスが、属している Virtual Ethernet Module (VEM; 仮想イーサネット モジュール) に従ってグループ化されます。また、[Summary] ペインの右上にある [VEM-VM-VETH] をクリックして、関連付けられた Virtual Machine (VM; 仮想マシン) に従ってグループ化することもできます。  
[Unknown] という名前のフォルダにネットワーク インターフェイス カードに関連付けられていない (参加していないインターフェイスとも呼ばれる) vEthernet インターフェイスが保存されます。
- ステップ 3** 目的のフォルダを展開します。
- ステップ 4** 目的のインターフェイスを選択します。
- ステップ 5** [Details] ペインの [Port Details] タブをクリックします。
- ステップ 6** [Port Mode Settings] の内容を展開します。
- ステップ 7** [Mode] ドロップダウン リストで、次のいずれかを実行します。
- プライベート VLAN ホストを作成するには、[PVLAN Host] を選択し、[Secondary VLAN] ドロップダウン リストでセカンダリ VLAN を選択します。
  - 無差別モードでプライベート VLAN を作成するには、[PVLAN Promiscuous] を選択し、[Secondary VLANs] ドロップダウン リストで 1 つまたは複数のセカンダリ VLAN を選択します。
- プライマリ VLAN がセカンダリ VLAN に接続され、自動的に [primary VLAN] フィールドに入力されます。
- ステップ 8** メニュー バーで [File] > [Deploy] を選択して、変更をデバイスに適用します。
-

## vEthernet インターフェイスの IPv4 ACL の設定

vEthernet インターフェイスで IPv4 Access Control List (ACL; アクセス コントロール リスト) を設定できます。

### 作業を開始する前に

デフォルトの説明を割り当てない場合、説明を付けて vEthernet インターフェイスを設定します。詳細については、「[vEthernet インターフェイスの説明の設定](#)」(P.8-3) を参照してください。

### 手順の詳細

- 
- |               |   |
|---------------|---|
| <b>ステップ 1</b> | [Feature Selector] ペインで、[Interfaces] > [Logical] > [Virtual Ethernet] を選択します。<br>この機能をサポートするデバイスが [Summary] ペインに一覧表示されます。   |
| <b>ステップ 2</b> | [Summary] ペインで、目的のデバイスを展開します。<br>vEthernet インターフェイスが保存されているフォルダが表示されます。<br>デフォルトでは、vEthernet インターフェイスが、属している Virtual Ethernet Module (VEM; 仮想イーサネット モジュール) に従ってグループ化されます。また、[Summary] ペインの右上にある [VEM-VM-VETH] をクリックして、関連付けられた Virtual Machine (VM; 仮想マシン) に従ってグループ化することもできます。<br>[Unknown] という名前のフォルダにネットワーク インターフェイス カードに関連付けられていない (参加していないインターフェイスとも呼ばれる) vEthernet インターフェイスが保存されます。 |
| <b>ステップ 3</b> | 目的のフォルダを展開します。  |
| <b>ステップ 4</b> | 目的のインターフェイスを選択します。  |
| <b>ステップ 5</b> | [Details] ペインの [Port Details] タブをクリックします。   |
| <b>ステップ 6</b> | [Advanced Settings] の内容を展開します。  |
| <b>ステップ 7</b> | [IPv4 ACL] フィールドで、着信トラフィック用の ACL と発信トラフィック用の ACL を選択します。  |
| <b>ステップ 8</b> | メニュー バーで [File] > [Deploy] を選択して、変更をデバイスに適用します。   |
- 

## vEthernet インターフェイスでの MAC ACL の設定

vEthernet インターフェイスで MAC ACL を設定できます。

### 作業を開始する前に

デフォルトの説明を割り当てない場合、説明を付けて vEthernet インターフェイスを設定します。詳細については、「[vEthernet インターフェイスの説明の設定](#)」(P.8-3) を参照してください。

### 手順の詳細

- 
- |               |   |
|---------------|---|
| <b>ステップ 1</b> | [Feature Selector] ペインで、[Interfaces] > [Logical] > [Virtual Ethernet] を選択します。<br>この機能をサポートするデバイスが [Summary] ペインに一覧表示されます。 |
| <b>ステップ 2</b> | [Summary] ペインで、目的のデバイスを展開します。   |

vEthernet インターフェイスが保存されているフォルダが表示されます。

デフォルトでは、vEthernet インターフェイスが、属している Virtual Ethernet Module (VEM; 仮想イーサネット モジュール) に従ってグループ化されます。また、[Summary] ペインの右上にある [VEM-VM-VETH] をクリックして、関連付けられた Virtual Machine (VM; 仮想マシン) に従ってグループ化することもできます。

[Unknown] という名前のフォルダにネットワーク インターフェイス カードに関連付けられていない (参加していないインターフェイスとも呼ばれる) vEthernet インターフェイスが保存されます。

- ステップ 3** 目的のフォルダを展開します。
- ステップ 4** 目的のインターフェイスを選択します。
- ステップ 5** [Details] ペインの [Port Details] タブをクリックします。
- ステップ 6** [Advanced Settings] の内容を展開します。
- ステップ 7** [MAC ACL] フィールドで、着信トラフィック用の ACL と発信トラフィック用の ACL を選択します。
- ステップ 8** メニュー バーで [File] > [Deploy] を選択して、変更をデバイスに適用します。

## vEthernet インターフェイスでの SPAN の設定

参加している vEthernet インターフェイス (カードに関連付けられている) で SPAN を設定できます。参加していないインターフェイスの場合は、SPAN を設定できません。

### 作業を開始する前に

デフォルトの説明を割り当てない場合、説明を付けて vEthernet インターフェイスを設定します。詳細については、「[vEthernet インターフェイスの説明の設定](#)」(P.8-3) を参照してください。

### 手順の詳細

- ステップ 1** [Feature Selector] ペインで、[Interfaces] > [Logical] > [Virtual Ethernet] を選択します。  
この機能をサポートするデバイスが [Summary] ペインに一覧表示されます。
- ステップ 2** [Summary] ペインで、目的のデバイスを展開します。  
vEthernet インターフェイスが保存されているフォルダが表示されます。  
デフォルトでは、vEthernet インターフェイスが、属している Virtual Ethernet Module (VEM; 仮想イーサネット モジュール) に従ってグループ化されます。また、[Summary] ペインの右上にある [VEM-VM-VETH] をクリックして、関連付けられた Virtual Machine (VM; 仮想マシン) に従ってグループ化することもできます。  
[Unknown] という名前のフォルダにネットワーク インターフェイス カードに関連付けられていない (参加していないインターフェイスとも呼ばれる) vEthernet インターフェイスが保存されます。
- ステップ 3** 目的のフォルダを展開します。
- ステップ 4** 目的のインターフェイスを選択します。
- ステップ 5** [Details] ペインの [Port Details] タブをクリックします。
- ステップ 6** [Advanced Settings] の内容を展開します。
- ステップ 7** [SPAN] フィールドで、送信元または宛先を SPAN インターフェイスとして選択します。



**ステップ 8** メニュー バーで [File] > [Deploy] を選択して、変更をデバイスに適用します。

## vEthernet インターフェイスのイネーブル化またはディセーブル化

vEthernet インターフェイスをイネーブルまたはディセーブルにできます。

### 手順の詳細

- 
- ステップ 1** [Feature Selector] ペインで、[Interfaces] > [Logical] > [Virtual Ethernet] を選択します。  
この機能をサポートするデバイスが [Summary] ペインに一覧表示されます。
- ステップ 2** [Summary] ペインで、目的のデバイスを展開します。  
vEthernet インターフェイスが保存されているフォルダが表示されます。  
デフォルトでは、vEthernet インターフェイスが、属している Virtual Ethernet Module (VEM; 仮想イーサネット モジュール) に従ってグループ化されます。また、[Summary] ペインの右上にある [VEM-VM-VETH] をクリックして、関連付けられた Virtual Machine (VM; 仮想マシン) に従ってグループ化することもできます。  
[Unknown] という名前のフォルダにネットワーク インターフェイス カードに関連付けられていない (参加していないインターフェイスとも呼ばれる) vEthernet インターフェイスが保存されます。
- ステップ 3** 目的のフォルダを展開します。
- ステップ 4** 目的のインターフェイスを選択します。
- ステップ 5** 次のいずれかを行います。
- インターフェイスをイネーブルにするには、[Actions] > [Admin Up] を選択します。
  - インターフェイスをディセーブルにするには、[Actions] > [Admin Down] を選択します。
- ステップ 6** メニュー バーで [File] > [Deploy] を選択して、変更をデバイスに適用します。
- 

## vEthernet インターフェイスの概要の表示

vEthernet インターフェイスの概要 (名前、説明、ポート プロファイル、モード、管理ステータスと動作ステータス、VM 名、VM アダプタなど) を表示できます。

### 手順の詳細

- 
- ステップ 1** [Feature Selector] ペインで、[Interfaces] > [Logical] > [Virtual Ethernet] を選択します。  
この機能をサポートするデバイスが [Summary] ペインに一覧表示されます。
- ステップ 2** [Summary] ペインで、目的のデバイスを展開します。  
vEthernet インターフェイスが保存されているフォルダが表示されます。  
デフォルトでは、vEthernet インターフェイスが、属している Virtual Ethernet Module (VEM; 仮想イーサネット モジュール) に従ってグループ化されます。また、[Summary] ペインの右上にある [VEM-VM-VETH] をクリックして、関連付けられた Virtual Machine (VM; 仮想マシン) に従ってグループ化することもできます。

[Unknown] という名前のフォルダにネットワーク インターフェイス カードに関連付けられていない (参加していないインターフェイスとも呼ばれる) vEthernet インターフェイスが保存されます。

**ステップ 3** 目的のフォルダを展開します。

## vEthernet インターフェイス ポートのステータスの表示

vEthernet インターフェイスのポート ステータス情報を表示できます。

### 手順の詳細

- ステップ 1** [Feature Selector] ペインで、[Interfaces] > [Logical] > [Virtual Ethernet] を選択します。  
この機能をサポートするデバイスが [Summary] ペインに一覧表示されます。
- ステップ 2** [Summary] ペインで、目的のデバイスを展開します。  
vEthernet インターフェイスが保存されているフォルダが表示されます。  
デフォルトでは、vEthernet インターフェイスが、属している Virtual Ethernet Module (VEM; 仮想イーサネット モジュール) に従ってグループ化されます。また、[Summary] ペインの右上にある [VEM-VM-VETH] をクリックして、関連付けられた Virtual Machine (VM; 仮想マシン) に従ってグループ化することもできます。  
[Unknown] という名前のフォルダにネットワーク インターフェイス カードに関連付けられていない (参加していないインターフェイスとも呼ばれる) vEthernet インターフェイスが保存されます。
- ステップ 3** 目的のフォルダを展開します。
- ステップ 4** 目的のインターフェイスを選択します。
- ステップ 5** [Details] ペインの [Port Status] タブをクリックします。  
ポート ステータス情報が表示されます。

## vEthernet インターフェイス統計情報の表示

[Statistics] タブに次のウィンドウが表示されます。

- **Traffic Statistics Chart** : 受信/送信されたパケットの総数、受信/送信されたマルチキャストおよびブロードキャスト パケットの数、受信/送信されたオクテット/バイト数、ドロップされたインバウンド パケット数についての統計情報を表示します。

この機能のための統計情報収集の詳細については、『Cisco DCNM Fundamentals Configuration Guide, Release 5.x』を参照してください。

## 仮想イーサネット モジュールの統計情報の表示

[Statistics] タブに次のウィンドウが表示されます。

- **Uplink Traffic Statistics Chart** : 受信/送信されたパケットの総数、受信/送信されたマルチキャストおよびブロードキャスト パケットの数、受信/送信されたオクテット/バイト数についての統計情報を表示します。

- Vcs Traffic Statistics Chart : 仮想マシンについての統計情報を表示します。

この機能のための統計情報収集の詳細については、『Cisco DCNM Fundamentals Configuration Guide, Release 5.x』を参照してください。

## vEthernet インターフェイスのためのフィールドの説明

ここでは、vEthernet インターフェイス機能に関する以下のフィールドについて説明します。

- 「[Virtual Ethernet] : [Device Details]」 (P.8-13)
- 「[Virtual Ethernet] : [Device Status]」 (P.8-13)
- 「[Virtual Ethernet] : [Port Details] : [Basic Settings] セクション」 (P.8-14)
- 「[Virtual Ethernet] : [Port Details] : [Port Mode Settings] セクション」 (P.8-14)
- 「[Virtual Ethernet] : [Port Details] : [Advanced Settings] セクション」 (P.8-14)
- 「[Virtual Ethernet] : [Port Status] : [Port Status] セクション」 (P.8-15)

### [Virtual Ethernet] : [Device Details]

表 8-1 [Virtual Ethernet] : [Device Details]

フィールド	説明
Auto Setup	デバイスに対して vEthernet インターフェイスを自動的に設定するように指定します。
Auto Delete	デバイスに対して非アクティブな vEthernet インターフェイスを自動的に削除するように指定します。
Force Detach	重複している vEthernet インターフェイス アクティベーションをデバイスが自動的に接続解除するように指定します。

### [Virtual Ethernet] : [Device Status]

表 8-2 [Virtual Ethernet] : [Device Status]

フィールド	説明
Port Mode	表示のみ。ポート モード ([Access]、[Trunk]、[PVLAN Host]、[PVLAN Promiscuous])。
Total	表示のみ。対応するポート モードのインターフェイスの合計数。
Active	表示のみ。対応するポート モードのアクティブ インターフェイスの数。
Admin Down	表示のみ。対応するポート モードの管理的にダウンしているインターフェイスの数。
Operationally Down	表示のみ。対応するポート モードの機能上ダウンしているインターフェイスの数。

## [Virtual Ethernet] : [Port Details] : [Basic Settings] セクション

表 8-3 [Virtual Ethernet] : [Port Details] : [Basic Settings] セクション

フィールド	説明
Name	表示のみ。インターフェイスの名前。
Admin Status	インターフェイスの状態 ([Up] または [Down])。
Pinning ID	インターフェイスが接続されている (ピン接続) サブグループの ID 番号。
Description	インターフェイスを説明する単語またはフレーズ。
Port Profile	インターフェイスが属しているポート プロファイルの名前。
VMWare DVPort ID	VMware DVPort の ID 番号。

## [Virtual Ethernet] : [Port Details] : [Port Mode Settings] セクション

表 8-4 [Virtual Ethernet] : [Port Details] : [Port Mode Settings] セクション

フィールド	説明
Mode	インターフェイスに割り当てられたポート モード。有効な選択肢は [Access]、[Trunk]、[PVLAN Host]、[PVLAN Promiscuous] です。
<b>Access</b>	
Access VLAN	アクセス ポートに使用される VLAN の ID 番号。デフォルトは VLAN 1 です。
<b>Trunk</b>	
Encapsulation	表示のみ。フレームまたはパケットが属している VLAN を識別するために使用されるタグging方式 (IEEE 802.1Q)。
Allowed VLAN	このポート プロファイルに属するインターフェイスでデータを送信できる VLAN の ID 番号。有効範囲は 1 ~ 4094。デフォルトは 1。  VLAN 3968 ~ 4047 および 4094 は、デバイス内部使用のために割り当てられており、データ トラフィックは伝送しません。
Native VLAN	トランク ポートに使用されるネイティブ VLAN の ID 番号。デフォルトは VLAN 1 です。

## [Virtual Ethernet] : [Port Details] : [Advanced Settings] セクション

表 8-5 [Virtual Ethernet] : [Port Details] : [Advanced Settings] セクション

フィールド	説明
<b>IPv4 ACL</b>	
Incoming Ipv4 Traffic	インターフェイス上の入力トラフィックをフィルタリングする IPv4 ACL。デフォルトでは、このリストは空白です。
Outgoing Ipv4 Traffic	インターフェイス上の出力トラフィックをフィルタリングする IPv4 ACL。デフォルトでは、このリストは空白です。
<b>MAC ACL</b>	

表 8-5 [Virtual Ethernet] : [Port Details] : [Advanced Settings] セクション (続き)

フィールド	説明
Incoming Traffic	インターフェイス上の入力トラフィックをフィルタリングする MAC ACL。デフォルトでは、このリストは空白です。
Outgoing Traffic	インターフェイス上の出力トラフィックをフィルタリングする MAC ACL。デフォルトでは、このリストは空白です。
<b>SPAN</b>	
Use Interface as SPAN	このインターフェイスの送信元または宛先。
Session ID	インターフェイスが適用される SPAN セッション ID。
Type	表示のみ。セッションのタイプ。
Direction: Ingress	入力パケットをモニタします。
Direction: Egress	出力パケットをモニタします。

## [Virtual Ethernet] : [Port Status] : [Port Status] セクション

表 8-6 [Virtual Ethernet] : [Port Status] : [Port Status] セクション

フィールド	説明
Operational Status	表示のみ。インターフェイスの動作ステータス。デフォルトは down です。有効な値は次のとおりです。 <ul style="list-style-type: none"><li>Up</li><li>Down</li></ul>
Status Description	表示のみ。動作ステータスの説明。

## その他の関連資料

アクセスおよびトランク ポート モードの実装に関する追加情報については、次の項を参照してください。

- 「関連資料」(P.8-15)
- 「標準規格」(P.8-16)

## 関連資料

関連項目	参照先
ポート プロファイル	『Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.0(4)SVI(2)』
VLAN およびプライベート VLAN	『Cisco Nexus 1000V Layer 2 Switching Configuration Guide, Release 4.0(4)SVI(2)』
システム管理	『Cisco Nexus 1000V System Management Configuration Guide, Release 4.0(4)SVI(2)』

## 標準規格

標準規格	タイトル
この機能でサポートされる新規または改訂された標準規格はありません。また、この機能による既存の標準規格サポートの変更はありません。	—

## vEthernet インターフェイスの機能の履歴

このセクションでは、vEthernet インターフェイス パラメータの機能の履歴を示します。

機能名	リリース	機能情報
vEthernet インターフェイス	5.0	この機能が導入されました。



# CHAPTER 9

## Fabric Extender の設定

この章では、Cisco NX-OS デバイスで Fabric Extender を設定する手順について説明します。  
この章では、次の内容について説明します。

- 「Fabric Extender について」 (P.9-1)
- 「Fabric Extender のライセンス要件」 (P.9-4)
- 「Fabric Extender の前提条件」 (P.9-4)
- 「プラットフォーム サポート」 (P.9-4)
- 「Fabric Extender の設定」 (P.9-5)
- 「Fabric Extender のフィールドの説明」 (P.9-10)
- 「その他の関連資料」 (P.9-12)
- 「Fabric Extender の機能履歴」 (P.9-12)

## Fabric Extender について

DCNM Release 4.2(1) 以降、Cisco Nexus 2000 シリーズ Fabric Extender を Cisco NX-OS デバイスと連携させることで、サーバ集約で高密度かつ低コストの接続を実現します。Fabric Extender は、ギガビットイーサネット、10 ギガビットイーサネット、ユニファイドファブリック、ラック、ブレードサーバなどの環境全体で拡張性を高め、データセンターのアーキテクチャと運用を簡素化するように設計されています。

Fabric Extender は、親スイッチの Cisco NX-OS スイッチに統合されることで、親スイッチから提供される設定情報を使用して、自動的にプロビジョニングおよび設定を行うことができます。この統合により、単一管理ドメインで、多くのサーバやホストが、セキュリティや Quality of Service (QoS) 設定パラメータを含め、親スイッチと同じフィーチャセットを使用してサポートされます。Fabric Extender と親スイッチを統合することにより、スパンニングツリープロトコル (STP) を使用することなく、大規模なマルチパス、ループフリー、およびアクティブ-アクティブのデータセンター トポロジが構築できます。

Cisco Nexus 2148T Fabric Extender は、すべてのトラフィックを親の Cisco NX-OS スイッチに 10 ギガビットイーサネットファブリックアップリンクを介して転送します。このため、すべてのトラフィックが Cisco NX-OS スイッチで確立されているポリシーにより検査されます。

ここでは、次の内容について説明します。

- 「Fabric Extender の用語」 (P.9-2)
- 「オーバーサブスクリプション」 (P.9-2)
- 「管理モデル」 (P.9-3)
- 「Fabric Extender のイメージ管理」 (P.9-3)
- 「ホストインターフェイス」 (P.9-3)

- 「ホスト EtherChannel」 (P.9-3)
- 「Fabric Extender のモデル」 (P.9-4)

## Fabric Extender の用語

このマニュアルでは、次の用語を使用しています。

- ファブリック インターフェイス : Fabric Extender から親スイッチへの接続専用の 10 ギガビットイーサネットのアップリンク ポートです。ファブリック インターフェイスは他の目的には使用できません。親スイッチに直接接続する必要があります。
- EtherChannel ファブリック インターフェイス: Fabric Extender から親スイッチへの EtherChannel アップリンク接続です。この接続は、単一論理チャンネルにバンドルされているファブリック インターフェイスで構成されます。
- ホスト インターフェイス : サーバまたはホスト システムに接続するためのイーサネット ホスト インターフェイスです。ブリッジまたはスイッチをホスト インターフェイスに接続しないでください。これらのインターフェイスは、エンド ホスト接続またはエンド サーバ接続を提供するように設計されています。
- EtherChannel ホスト インターフェイス : サーバまたはホスト システムに接続するための EtherChannel ホスト インターフェイスです。

## オーバーサブスクリプション

スイッチ環境におけるオーバーサブスクリプションとは、ポート使用を最適化するために、複数のデバイスを同じインターフェイスに接続することです。インターフェイスは最大速度で動作する接続をサポートしますが、ほとんどのインターフェイスは最大速度で動作しないため、ポートを共有することにより未使用の帯域幅を有効活用できます。Cisco Nexus 2000 シリーズ Fabric Extender の場合、オーバーサブスクリプションは、アクティブなホスト インターフェイスへの利用可能なファブリック インターフェイスの機能で、イーサネット環境にコスト効果の高い拡張性と柔軟性をもたらします。

Cisco Nexus 2148T Fabric Extender には、4 つの 10 ギガビットイーサネット ファブリック インターフェイスと 48 の 1000 Base-T イーサネット ホスト インターフェイスが用意されています。このため、多くの種類の設定が可能です。たとえば次のように設定できます。

- オーバーサブスクリプションなし (4 つのファブリック インターフェイスに対して 40 のホスト インターフェイス)
- 1.2:1 のオーバーサブスクリプション (4 つのファブリック インターフェイスに対して 48 のホスト インターフェイス)
- 4.8:1 のオーバーサブスクリプション (1 つのファブリック インターフェイスに対して 48 のホスト インターフェイス)

Cisco Nexus 2248TP Fabric Extender には、4 つの 10 ギガビットイーサネット ファブリック インターフェイスと 48 の 100/1000 Base-T (100 メガビット/1 ギガビット) イーサネット ホスト インターフェイスが用意されています。ホスト インターフェイスがギガビットイーサネット モードで動作しているときは、Cisco Nexus 2148T と同様の設定が用意されています。ホスト インターフェイスが 100 メガビット モードで動作しているときは、オーバーサブスクリプションなしで簡単に動作できます。

Cisco Nexus 2232PP Fabric Extender には、8 つの 10 ギガビットイーサネット ファブリック インターフェイスと 32 の 10 GBase-T イーサネット ホスト インターフェイスが用意されています。このため、4:1 (1 つのファブリック インターフェイスに対して 4 つのホスト インターフェイス) 以上のオーバーサブスクリプションを使用できます。



## 管理モデル

Cisco Nexus 2000 シリーズ Fabric Extender は、親スイッチにより、ゼロタッチ設定モデルを使用してファブリック インターフェイスを介して管理されます。スイッチは Fabric Extender のファブリック インターフェイスを検出することにより、Fabric Extender を検出します。

Fabric Extender が検出され、親スイッチに正常に関連付けられていると、次のアクションが実行されます。

1. スイッチはソフトウェア イメージの互換性を確認し、必要に応じて、Fabric Extender をアップグレードします。
2. スイッチと Fabric Extender は、相互にインバンド IP 接続を確立します。スイッチは、ネットワークで使用されている可能性のある IP アドレスとの競合を避けるために、Fabric Extender にループバック アドレスの範囲 (127.0.0.0/8) で IP アドレスを割り当てます。
3. スイッチは、設定データを Fabric Extender にプッシュします。Fabric Extender は、設定をローカルに保存しません。
4. Fabric Extender は、更新された動作ステータスをスイッチに通知します。

## Fabric Extender のイメージ管理

Cisco Nexus 2000 シリーズ Fabric Extender にソフトウェアは同梱されません。Fabric Extender のイメージは、親スイッチのシステム イメージにバンドルされています。イメージは、スイッチと Fabric Extender との間の関連付け処理時に自動的に検証され、必要に応じてアップデートされます。

## ホスト インターフェイス

ホスト インターフェイスは、ホストまたはサーバとの接続用にだけ使用されます。ホスト インターフェイスは他のネットワークに接続できません。このインターフェイスは、エッジ ポートとして常にイネーブルです。このポートはアップすると、ただちにフォワーディング状態になります。ホスト インターフェイスでは、BPDU ガードが常にイネーブルです。BPDU が受信されると、ポートはエラー ディセーブル状態になり、リンクはダウンしたままになります。

シスコ検出プロトコル (CDP) パケットを受け入れるようにホスト インターフェイスをイネーブルにできます。このプロトコルは、リンクの両端でイネーブルになっている場合にだけ機能します。



(注) Fabric Extender が仮想ポート チャネル (vPC) トポロジで設定されているときは、ファブリック インターフェイスで CDP がサポートされません。

入力パケット数および出力パケット数は、ホスト インターフェイスごとに提供されます。

## ホスト EtherChannel

Cisco Nexus 2248TP および Cisco Nexus 2232PP は、EtherChannel ホスト インターフェイス設定をサポートします。最大で 8 つのインターフェイスを EtherChannel で結合できます。EtherChannel は LACP ありでもなしでも設定できます。



(注) ホスト インターフェイス EtherChannel のサポートは、Cisco NX-OS Release 4.2(1)N1(1) から Fabric Extender に追加されました。

## Fabric Extender のモデル

Cisco Nexus 2000 シリーズ Fabric Extender には 3 つのモデルがあります。

- Cisco Nexus 2148T には、サーバまたはホストへのダウンリンク接続用に 48 個の 1000 Base-T イーサネット ホスト インターフェイスが搭載されています。また、親スイッチへのアップリンク接続用に SFP+ インターフェイス アダプタが付いた 10 ギガビット イーサネット ファブリック インターフェイスが 4 個搭載されています。
- Cisco Nexus 2248TP には、サーバまたはホストへのダウンリンク接続用に 48 個の 100 Base-T/1000 Base-T イーサネット ホスト インターフェイスが搭載されています。また、親スイッチへのアップリンク接続用に SFP+ インターフェイス アダプタが付いた 10 ギガビット イーサネット ファブリック インターフェイスが 4 個搭載されています。
- Cisco Nexus 2232PP には、親スイッチへのアップリンク接続用に SFP+ インターフェイス アダプタが付いた 32 個の 10 ギガビット イーサネット ホスト インターフェイス、および SFP+ インターフェイス アダプタを備えた 8 個の 10 ギガビット イーサネット ファブリック インターフェイスが搭載されています。

## Fabric Extender のライセンス要件

Cisco NX-OS デバイス に付属する DCNM ライセンスでは、Cisco Nexus 2000 シリーズ Fabric Extender を台数制限なしで使用できます。

## Fabric Extender の前提条件

Fabric Extender の管理には、次の前提条件があります。

- DCNM では、Release 4.2 以降を実行する Fabric Extender を管理します。
- DCNM を使用して Fabric Extender のアソシエーションを設定する管理対象デバイスごとに、FEX のログレベルを 5（通知）以上に設定します。最低限必要なログ設定でデバイスを設定するには、デバイスのコマンドライン インターフェイスにログインし、次のコマンドを使用します。

```
switch(config)# logging level fex 5
switch(config)# logging logfile messages 6
switch(config)# logging event link-status default
```

- Fabric Extender が 2 つの NX-OS デバイスに接続されている場合は（アクティブ-アクティブ モード）、これらの NX-OS デバイスを同期する必要があります。それには、両方の NX-OS デバイスで同じ NTP サーバを使用します。

## プラットフォーム サポート

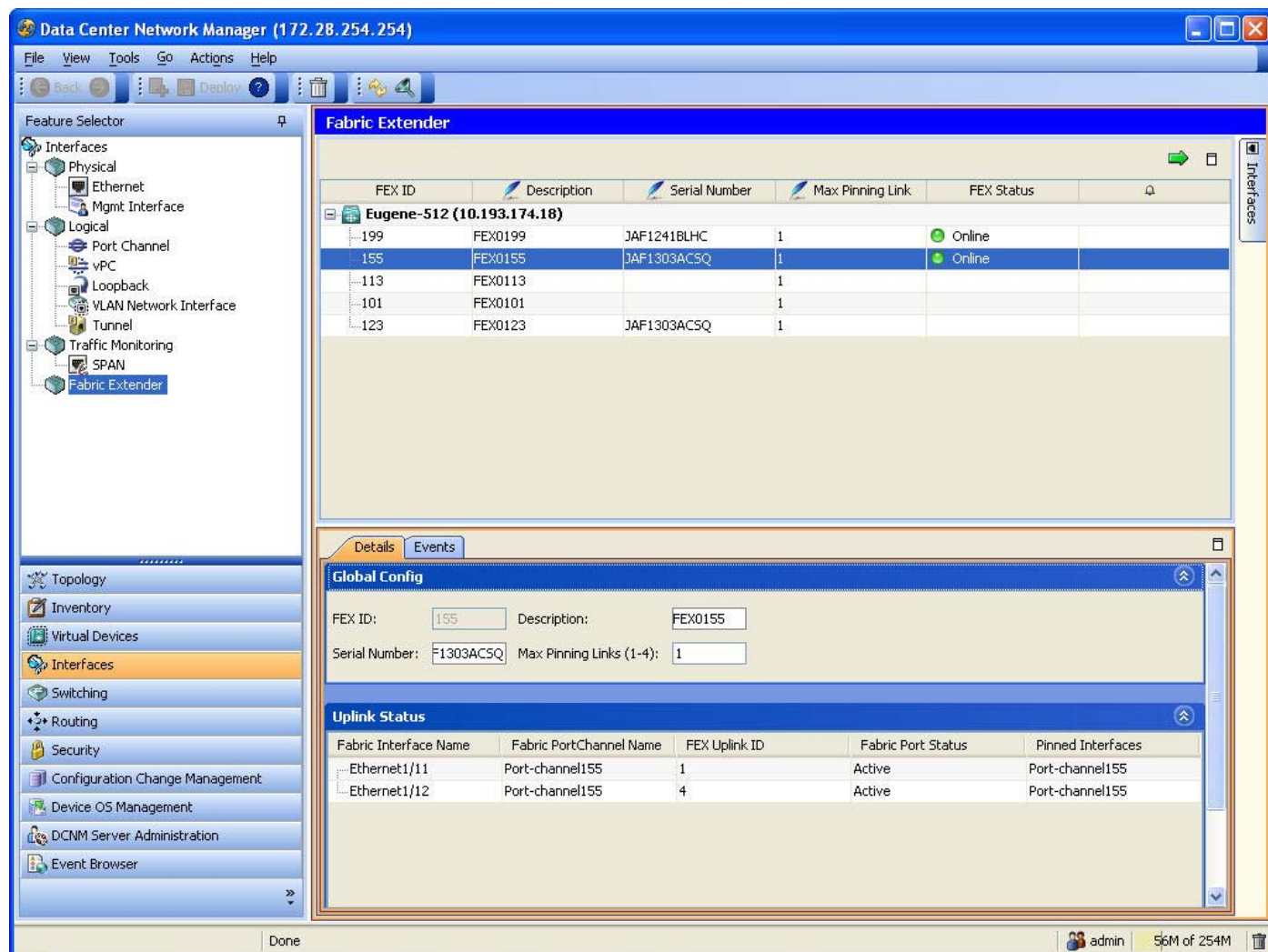
この機能をサポートするプラットフォームは次のとおりです。ガイドラインと制限事項、システム デフォルト値、設定制限などのプラットフォーム固有の情報については、対応するマニュアルを参照してください。

プラットフォーム	マニュアル
Cisco Nexus 5000 シリーズ スイッチ	<a href="#">Cisco Nexus 5000 シリーズ スイッチ マニュアル</a>

# Fabric Extender の設定

図 9-1 に Fabric Extender のコンテンツ ペインを示します。

図 9-1 Fabric Extender のコンテンツ ペイン



ここでは、次の内容について説明します。

- 「Fabric Extender の追加」 (P.9-6)
- 「Fabric Extender の削除」 (P.9-6)
- 「Fabric Extender の編集」 (P.9-7)
- 「リンクの再配布」 (P.9-7)
- 「ピン接続順序の維持」 (P.9-8)
- 「Fabric Extender とイーサネット インターフェイスの関連付け」 (P.9-8)
- 「Fabric Extender とポート チャネルの関連付け」 (P.9-9)

## Fabric Extender の追加

Fabric Extender をデバイスに追加できます。

### 手順の詳細

Fabric Extender を追加するには、次の手順を実行します。

- 
- |               |   |
|---------------|---|
| <b>ステップ 1</b> | [Feature Selector] ペインで [Interfaces] > [Fabric Extender] を選択します。<br>[Summary] ペインに使用可能なデバイスが表示されます。 |
| <b>ステップ 2</b> | [Summary] ペインでデバイスを右クリックします。<br>ドロップダウン リストが表示されます。   |
| <b>ステップ 3</b> | ドロップダウン リストから [New] を選択します。   |
| <b>ステップ 4</b> | [FEX ID] フィールドで FEX ID (100 ~ 199) を入力し、Enter を押して新しい Fabric Extender を配置します。                       |
- 

## Fabric Extender の削除

Fabric Extender をデバイスから削除できます。

### 手順の詳細

Fabric Extender を削除するには、次の手順を実行します。

- 
- |               |   |
|---------------|---|
| <b>ステップ 1</b> | [Feature Selector] ペインで [Interfaces] > [Fabric Extender] を選択します。<br>[Summary] ペインに使用可能なデバイスが表示されます。 |
| <b>ステップ 2</b> | [Summary] ペインでデバイスをダブルクリックして、既存の Fabric Extender のリストを表示します。  |
| <b>ステップ 3</b> | 削除する Fabric Extender を右クリックします。<br>ドロップダウン リストが表示されます。  |
| <b>ステップ 4</b> | ドロップダウン リストから [Delete] を選択します。<br>確認のポップアップ ウィンドウが表示されます。   |
| <b>ステップ 5</b> | 確認のポップアップ ウィンドウで [Yes] をクリックして Fabric Extender の削除を確認し、変更をデバイスに適用します。                               |
-

## Fabric Extender の編集

Fabric Extender では次のフィールド値を編集できます。

- Description
- Serial Number
- Max Pinning Links ([「リンク数の変更」\(P.9-7\)](#) を参照)

### 手順の詳細

Fabric Extender を編集するには、次の手順を実行します。

- 
- ステップ 1** [Feature Selector] ペインで [Interfaces] > [Fabric Extender] を選択します。  
[Summary] ペインに使用可能なデバイスが表示されます。
- ステップ 2** [Summary] ペインでデバイスをダブルクリックして、既存の Fabric Extender のリストを表示します。
- ステップ 3** 編集するデバイスをクリックします。
- ステップ 4** 該当するフィールドに変更を入力します。  
編集したフィールドから移動すると、変更が自動的に適用されます。
- 

## リンクの再配布

静的ピン接続されたインターフェイスで Fabric Extender をプロビジョニングすると、Fabric Extender のダウンリンク ホストインターフェイスは、最初に設定された順序でファブリック インターフェイスにピン接続されます。ファブリック インターフェイスへのホスト インターフェイスの特別な関係がリブートしても維持されるようにするには、リンクを再びピン接続する必要があります。

この機能は、次の 2 つの状況で行うことができます。

- max-links 設定を変更する必要がある場合。
- ファブリック インターフェイスへのホスト インターフェイスのピン接続順序を維持する必要がある場合。

## リンク数の変更

最初に親スイッチのポート 33 を唯一のファブリック インターフェイスとして設定すると、48 のすべてのホスト インターフェイスがこのポートにピン接続されます。別のポート（たとえば 35）をプロビジョニングした場合、この手順を実行してホスト インターフェイスを再配布する必要があります。これにより、すべてのホスト インターフェイスがダウンし、ホスト インターフェイス 1 ～ 24 はファブリック インターフェイス 33 に、ホスト インターフェイス 25 ～ 48 はファブリック インターフェイス 35 にピン接続されます。

### 手順の詳細

ピン接続リンクの数を変更するには、次の手順を実行します。

- 
- ステップ 1** [Feature Selector] ペインで [Interfaces] > [Fabric Extender] を選択します。  
[Summary] ペインに使用可能なデバイスが表示されます。

- ステップ 2** [Summary] ペインでデバイスをダブルクリックして、既存の Fabric Extender のリストを表示します。
- ステップ 3** 編集するデバイスをクリックします。
- ステップ 4** [Details] ペインで、[Max Pinning Links] フィールドに新しい値を入力します。
- ステップ 5** メニュー バーの [File] > [Deploy] を選択して、変更をデバイスに適用します。

## ピン接続順序の維持

ホスト インターフェイスのピン接続順序は、最初、ファブリック インターフェイスが設定された順序で決定されます。

Fabric Extender を次回リブートすると、設定されたファブリック インターフェイスは、ファブリック インターフェイスのポート番号の昇順でホスト インターフェイスにピン接続されます。

### 手順の詳細

ピン接続順序を維持するには、次の手順を実行します。

- ステップ 1** [Feature Selector] ペインで [Interfaces] > [Fabric Extender] を選択します。  
[Summary] ペインに使用可能なデバイスが表示されます。
- ステップ 2** [Summary] ペインで Fabric Extender のリストを展開し、編集する対象を選択します。
- ステップ 3** 編集する Fabric Extender を右クリックします。  
ドロップダウン リストが表示されます。
- ステップ 4** ドロップダウン リストから [Redistribute Pinning] を選択します。  
Cisco DCNM からデバイスへピン接続を再配布するように指示が出されます。

## Fabric Extender とイーサネット インターフェイスの関連付け

Fabric Extender をイーサネット インターフェイスと関連付けることができます。ここでは、次の内容について説明します。

### Fabric Extender の関連付け

#### 手順の詳細

Fabric Extender を関連付けるには、次の手順を実行します。

- ステップ 1** [Feature Selector] ペインで [Interfaces] > [Fabric Extender] を選択します。  
[Summary] ペインに使用可能なデバイスが表示されます。
- ステップ 2** デバイスをダブルクリックして、既存の Fabric Extender のリストを表示します。
- ステップ 3** イーサネット インターフェイスと関連付ける Fabric Extender をクリックします。

- ステップ 4** ウィンドウの右側にある [Association] ツールバーの [Interfaces] タブにマウスをあわせると、[Association Interfaces] ペインを表示します。
- ステップ 5** [Association Interfaces] ペインでイーサネット インターフェイスを右クリックします。  
ドロップダウン リストが表示されます。
- ステップ 6** ドロップダウン リストから [Associate FEX] を選択します。  
ブラウザ ウィンドウのステータス バーに [Deploying Configuration] 経過表示バーが表示されます。

## イーサネット ポート モードを Fabric Extender に設定

### 手順の詳細

イーサネット ポート モードを Fabric Extender に設定するには、次の手順を実行します。

- ステップ 1** [Feature Selector] ペインで [Interfaces] > [Ethernet] を選択します。  
[Summary] ペインに使用可能なイーサネット インターフェイスが表示されます。
- ステップ 2** 設定するイーサネット インターフェイスを探し、[Mode] フィールドをダブルクリックします。  
[Mode] フィールドは、ドロップダウン リストとして表示されます。
- ステップ 3** ポート モードを変更するには、[Mode] ドロップダウン メニューから [Fex Fabric] を選択します。

## Fabric Extender とポート チャネルの関連付け

Fabric Extender をポート チャネルと関連付けることができます。



(注)

ポート チャネルのメンバである各イーサネット インターフェイスをファブリック インターフェイスとして関連付ける必要があります。

## Fabric Extender の関連付け

### 手順の詳細

Fabric Extender をポート チャネルと関連付けるには、次の手順を実行します。

- ステップ 1** [Feature Selector] ペインで [Interfaces] > [Fabric Extender] を選択します。  
[Summary] ペインに使用可能なデバイスが表示されます。
- ステップ 2** デバイスをダブルクリックして、既存の Fabric Extender のリストを表示します。
- ステップ 3** ポート チャネルと関連付ける Fabric Extender をクリックします。
- ステップ 4** ウィンドウの右側にある [Association] ツールバーの [Interfaces] タブにマウスをあわせると、[Association Interfaces] ペインを表示します。

- ステップ 5** [Association Interfaces] ペインでポート チャネルを右クリックします。  
ドロップダウン リストが表示されます。
- ステップ 6** ドロップダウン リストから [Associate FEX] を選択します。  
ブラウザ ウィンドウのステータス バーに [Deploying Configuration] 経過表示バーが表示されます。
- 

## ポート モードを Fabric Extender に設定

### 手順の詳細

ポート モードを Fabric Extender に設定するには、次の手順を実行します。

- ステップ 1** [Feature Selector] ペインで [Interfaces] > [Port Channel] を選択します。  
[Summary] ペインに使用可能なデバイスが表示されます。
- ステップ 2** デバイスをダブルクリックして、ポート チャネルのリストを表示します。
- ステップ 3** 設定するポート チャネルをクリックします。
- ステップ 4** [Port Channels Details] ペインで、[Port Channel Details] タブをクリックします。
- ステップ 5** [Common Settings] セクションを表示します。
- ステップ 6** [Mode] ドロップダウン リストから [Fex Fabric] を選択します。  
ブラウザ ウィンドウのステータス バーに [Deploying Configuration] 経過表示バーが表示されます。
- 

## Fabric Extender のフィールドの説明

次の表では、DCNM の Fabric Extender 関連フィールドについて説明します。

- 「[Fabric Extender の \[Summary\] ペイン](#)」
- 「[Fabric Extender の \[Details\] ペイン](#)」



## Fabric Extender の [Summary] ペイン

表 9-1 Fabric Extender の [Summary] ペイン

フィールド	説明
FEX ID	Cisco NX-OS デバイスに接続されている Fabric Extender を一意に識別します。
Description	Fabric Extender に設定されている説明です。
Serial Number	設定済みのシリアル番号です。  (注) この設定済みシリアル番号と Fabric Extender の実際のシリアル番号が同じでない場合、Fabric Extender はアクティブになりません。
Max Pinning Links	一度にアクティブである、Fabric Extender の最大ピン接続アップリンク数を表す整数値です。
FEX Status	Fabric Extender のステータスです。
Events	Fabric Extender に関するあらゆる syslog イベントは DCNM によって収集され、その Fabric Extender の [Events] 列にベル記号が表示されます。特定のイベントを表示するには、詳細ペインで [Events] タブを開きます。

## Fabric Extender の [Details] ペイン

表 9-2 Fabric Extender の [Details] ペイン

フィールド名	説明
<b>[General] セクション</b>	
FEX ID	Cisco NX-OS デバイスに接続されている Fabric Extender を一意に識別します。
Description	Fabric Extender に設定されている説明です。
Serial Number	設定済みのシリアル番号です。  (注) この設定済みシリアル番号と Fabric Extender の実際のシリアル番号が同じでない場合、Fabric Extender はアクティブになりません。
Max Pinning Links	一度にアクティブである、Fabric Extender の最大ピン接続アップリンク数を表す整数値です。
FEX Status	Fabric Extender のステータスです。
<b>[Uplink Status] セクション</b>	
Uplink-ID	Fabric Extender のアップリンク ポート番号です。
Fabric Port Name	Fabric Extender アップリンクに使用する Cisco NX-OS デバイス ポートの名前です。
Fabric Port Channel Name	ファブリック ポートがポート チャネルのメンバである場合に、ポート チャネル名が表示されます。
Pinned Downlink Interfaces	このアップリンク上をトラフィックが伝送されるサテライト ポート名です。

## その他の関連資料

Fabric Extender の実装に関する追加情報については、『Cisco Nexus 2000 Series Fabric Extender Software Configuration Guide』を参照してください。

## Fabric Extender の機能履歴

機能名	リリース	機能情報
Fabric Extender の DCNM サポート	4.2	このリリースで DCNM サポートが追加されました。



# CHAPTER 10

## ポート プロファイルの設定

この章では、Cisco DCNM でポート プロファイルを設定する手順について説明します。

この章では、次の内容について説明します。

- 「ポート プロファイルについて」 (P.10-1)
- 「ポート プロファイルのライセンス要件」 (P.10-7)
- 「プラットフォーム サポート」 (P.10-7)
- 「ポート プロファイルの設定」 (P.10-7)
- 「ポート プロファイルのフィールドの説明」 (P.10-26)
- 「その他の関連資料」 (P.10-32)
- 「ポート プロファイルの機能履歴」 (P.10-32)

## ポート プロファイルについて

ポート プロファイルとは、インターフェイスの設定を単純化するためのメカニズムです。ポート プロファイルを 1 つ設定して複数のインターフェイスに割り当てると、これらのインターフェイスの設定を統一することができます。ポート プロファイルに加えた変更は、そのポート プロファイルが割り当てられているすべてのインターフェイスの設定に自動的に反映されます。

設定できるポート プロファイルのタイプにはイーサネットと vEthernet があり、同じタイプのインターフェイス（イーサネットまたは vEthernet）を割り当てることができます。



(注)

割り当てられたインターフェイスの設定に変更を加えると、ポート プロファイルの設定は無効になるため、このような変更は推奨しません。インターフェイスの設定に変更を加えるのは、変更の影響を簡単にテストしたい場合や、特定のポートをディセーブルにする場合に限定してください。



(注)

ポート プロファイル機能に対するシステム メッセージのログ レベルは、Cisco DCNM の要件以上でなければなりません。デバイス検出時に、ログ レベルが不適切であることが検出された場合は、最低限必要なレベルまで Cisco DCNM によって自動的に引き上げられます。ただし、Cisco Nexus 7000 シリーズ スイッチで Cisco NX-OS Release 4.0 を実行する場合は例外です。Cisco NX-OS Release 4.0 の場合は、デバイス検出の前に、コマンドライン インターフェイスを使用してログ レベルを Cisco DCNM の要件以上となるように設定してください。詳細については、『Cisco DCNM Fundamentals Configuration Guide, Release 5.x』を参照してください。

ここでは、次の内容について説明します。

- ・「ポート プロファイルのステート」(P.10-2)
- ・「ポート プロファイルの継承」(P.10-2)
- ・「システム ポート プロファイル」(P.10-2)
- ・「ポート プロファイルとポート グループ」(P.10-2)
- ・「ポート プロファイルの特性」(P.10-3)
- ・「ポート プロファイルと vPC ホスト モード」(P.10-3)
- ・「ポート プロファイルと MAC ピン接続」(P.10-5)
- ・「ポート プロファイルとレイヤ 3 制御」(P.10-6)
- ・「ポート プロファイルと iSCSI マルチパス」(P.10-7)

## ポート プロファイルのステート

ポート プロファイルのステートは、「イネーブル」と「ディセーブル」のいずれかです。

ディセーブルのポート プロファイルは、割り当てられたポートに適用されません。さらに、そのポート プロファイルがポリシーを VMware ポート グループにエクスポートするものであっても、そのポート グループが vCenter Server 上で作成されることはありません。

イネーブルのポート プロファイルは、割り当てられたポートに適用されます。ポリシーを VMware ポート グループから継承するようにポート プロファイルが設定されている場合は、そのポート グループが vCenter Server 上に作成されます。

## ポート プロファイルの継承

ポート プロファイルを他のポート プロファイルに割り当てることができます。親ポート プロファイルの設定属性が子ポート プロファイルに上書きコピーされて保存されます。継承された属性よりも優先する属性を指定するには、その属性を明示的に子ポート プロファイルの中で設定します。

新しいポート プロファイルの設定を直接変更すると、その設定は継承された設定よりも優先されます。

また、ポート プロファイルの継承を明示的に削除することもできます。削除すると、ポート プロファイルは、直接設定されたものを除いてデフォルト設定に戻ります。

4 つのレベルの継承がサポートされています。任意の数のポート プロファイルで同じポート プロファイルを継承できます。

## システム ポート プロファイル

システム ポート プロファイルとは、vCenter Server 接続を確立して保護するためのポート プロファイルです。システム ポート プロファイルには、システム VLAN（コントロール VLAN とパケット VLAN）が設定されています。

## ポート プロファイルとポート グループ

ポート グループとは、ポート プロファイルの vCenter Server 上での表現です。vCenter Server 上のポート グループはそれぞれ、Cisco DC-OS 上のポート プロファイルが 1 つ関連付けられます。ネットワーク管理者によってポート プロファイルが設定されたら、サーバ管理者は vCenter Server 上の対応するポート グループを使用してポートをポート プロファイルに割り当てます。

## ポート プロファイルの特性

次に示すポート プロファイルの特性を設定できます。

- 説明
- VMware 設定
- ポート チャンネル
- 静的ピン接続
- スイッチポート モード
- VLAN
- DHCP スヌーピング
- IP ソース ガード
- ARP 検査
- ポート セキュリティ
- MAC または IP ACL

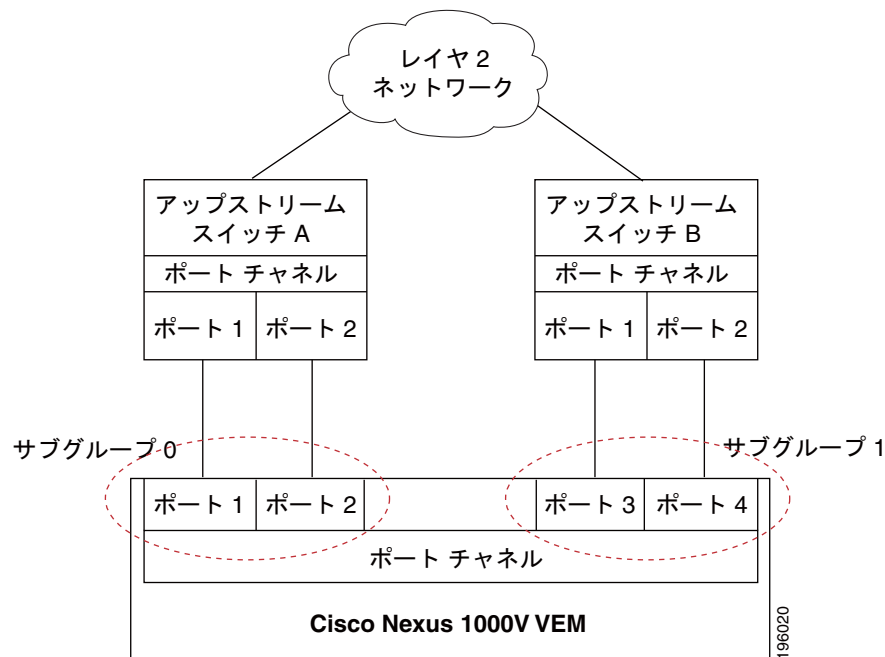
詳細については、使用するプラットフォームのマニュアルを参照してください。

## ポート プロファイルと vPC ホスト モード

ポート プロファイルを設定するときに、Virtual Port Channel Host Mode (vPC-HM; 仮想ポート チャンネル ホスト モード) 機能を指定できます。vPC-HM を使用すると、1 つのポート チャンネルのメンバポートを複数のアップストリーム スイッチに接続することができます。vPC-HM を使用するときは、トラフィック分離のためにポートが 0 ～ 31 のサブグループに分類されます。

図 10-1 では、vPC-HM を使用してトラフィックを分離するために、メンバポート 1 と 2 をサブグループ ID 0 に割り当て、メンバポート 3 と 4 をサブグループ ID 1 に割り当てています。

図 10-1 vPC-HM によるポート チャンネルから複数のアップストリーム スイッチへの接続



アップストリーム スイッチがポート チャンネルをサポートしていない場合は、MAC ピン接続を使用します。この機能を使用すると、各イーサネット ポート メンバを特定のポート チャンネル サブグループに割り当てることができます。詳細については、「[ポート プロファイルと MAC ピン接続](#)」(P.10-5) を参照してください。



(注)

アップストリーム スイッチで vPC がイネーブルになっている場合は、vPC-HM を Cisco DC-OS 上で設定しないでください。vPC-HM が Cisco DC-OS 上で設定されていて、vPC がアップストリーム スイッチ上で設定されている場合は、接続が中断されるか、ディセーブルになる可能性があります。

vPC-HM でポート プロファイルを設定するには、「[ポート チャンネルの設定](#)」(P.10-15) を参照してください。

サブグループの作成方法とインターフェイスの割り当て方法については、次の各項を参照してください。

- 「[CDP または手動方式によるサブグループの作成](#)」(P.10-4)
- 「[静的ピン接続によるインターフェイスの割り当て](#)」(P.10-5)

## CDP または手動方式によるサブグループの作成

Cisco Discovery Protocol (CDP) がアップストリーム スイッチでイネーブルになっている場合は、サブグループは自動的に CDP 情報を使用して作成されます。CDP がアップストリーム スイッチでイネーブルになっていない場合は、インターフェイスでサブグループを手動で作成する必要があります。

この設定は、ポート プロファイルの設定の一部として行います。詳細については、「[ポート チャンネルの設定](#)」(P.10-15) を参照してください。

## 静的ピン接続によるインターフェイスの割り当て

静的ピン接続機能を使用すると、vEthernet インターフェイス、コントロール VLAN、またはパケット VLAN を特定のポート チャネル サブグループに割り当てる（またはピン接続する）ことができます。静的ピン接続を使用すると、vEthernet インターフェイス、コントロール VLAN、またはパケット VLAN からのトラフィックが、指定されたサブグループ内のメンバー ポートだけを通して転送されるようになります。

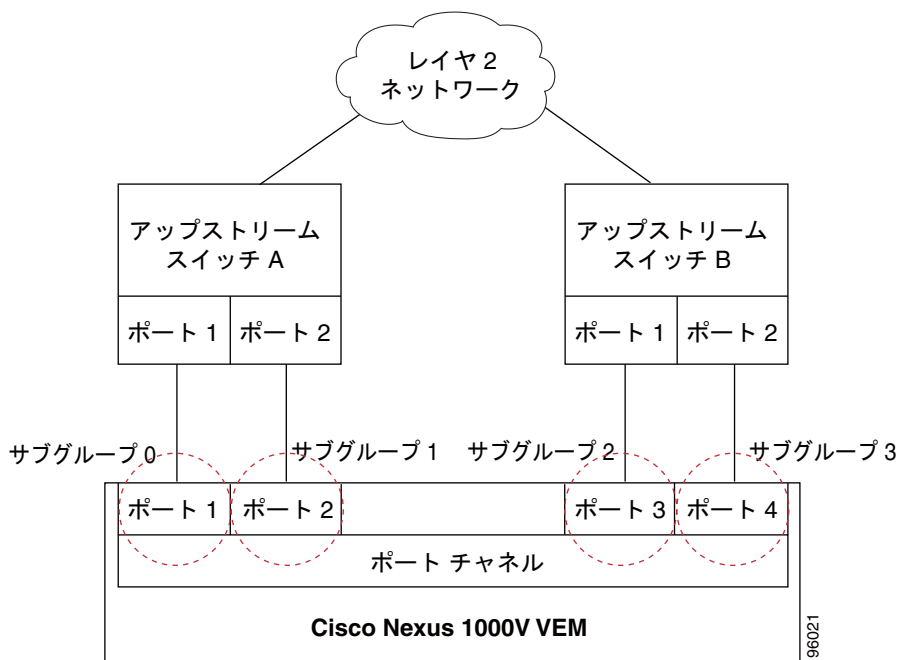
vEthernet インターフェイス、コントロール VLAN、またはパケット VLAN を特定のポート チャネル サブグループに固定する方法については、「[コントロールまたはパケット VLAN の静的ピン接続の設定](#)」(P.10-17) を参照してください。

また、インターフェイス コンフィギュレーション モードで vEthernet インターフェイスをサブグループにピン接続することもできます。詳細については、「[vEthernet インターフェイスの静的ピン接続の設定](#)」(P.8-5) を参照してください。

## ポート プロファイルと MAC ピン接続

MAC ピン接続機能を使用すると、イーサネット ポート メンバを特定のポート チャネル サブグループに割り当てることができます。MAC ピン接続は、ポート チャネルをサポートしていないアップストリーム スイッチがある場合に使用します。図 10-2 に、MAC ピン接続を使用して特定のポート チャネル サブグループに割り当てられる各メンバー ポートを示します。

図 10-2 MAC ピン接続によるポート チャネルから複数のアップストリーム スイッチへの接続



## ポート プロファイルとレイヤ 3 制御

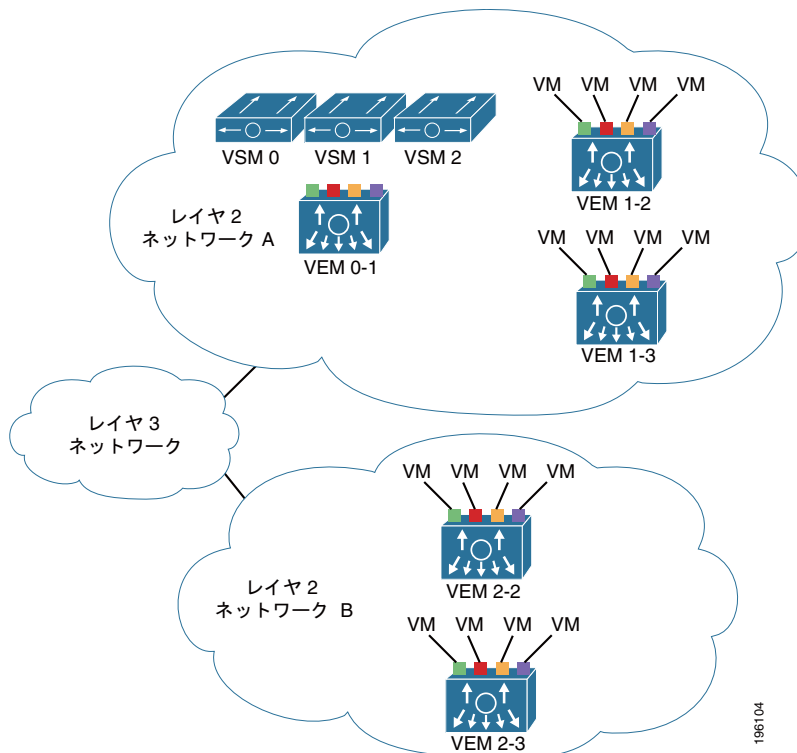
レイヤ 3 制御 (IP 接続) とは、Virtual Supervisor Module (VSM) と Virtual Ethernet Module (VEM) の間の制御およびパケットのトラフィックに対してサポートされる機能であり、Cisco Nexus 1000V ドメインには必須です。レイヤ 3 制御を行うと、VSM はレイヤ 3 経由でアクセス可能になり、別のレイヤ 2 ネットワークに存在するホストを制御できるようになります。ただし、その場合も、同じ VSM によって制御されるホストはすべて同じレイヤ 2 ネットワーク内に存在する必要があります。VSM は、自身が制御するレイヤ 2 ネットワークの外にあるホストの制御はできないので、VSM 自身が存在するホストは別の VSM によって制御する必要があります。

レイヤ 3 制御を実装するには、次の設定作業を行う必要があります。

- VSM ドメイン トランスポート モードをレイヤ 3 として設定します。  
詳細については、使用するプラットフォームとソフトウェア リリースのマニュアルとリリース ノートを参照してください。
- 「レイヤ 3 制御のためのポート プロファイルの設定」(P.10-11) を参照してポート プロファイルを設定します。
- VMware カーネル NIC インターフェイスを各ホスト上に作成し、レイヤ 3 制御ポート プロファイルを割り当てます。  
詳細については、VMware のマニュアルを参照してください。

図 10-3 に、レイヤ 3 制御の例を示します。この図では、VSM0 が VEM\_0\_1 を制御しており、VEM\_0\_1 が VSM1 と VSM2 をホスティングしています。VSM1 と VSM2 は、別のレイヤ 2 ネットワーク上にある VEM を制御します。

図 10-3 レイヤ 3 制御 IP 接続の例





## ポート プロファイルと iSCSI マルチパス

iSCSI マルチパスとは、サーバとそのストレージ デバイスとの間に複数のルートをセットアップする機能です。常時接続の維持と、トラフィック 負荷の分散が可能になります。マルチパス ソフトウェアによって、すべての入力/出力要求が処理され、要求は最善のパスを通して送信されます。ホスト サーバから共有ストレージへのトラフィックの伝送には、iSCSI プロトコルが使用されます。この iSCSI プロトコルによって、SCSI コマンドが iSCSI パケットにパッケージ化され、このパケットがイーサネット ネットワーク上で伝送されます。

パスまたはパス上のコンポーネントに障害が発生した場合は、使用可能な別のパスがサーバによって選択されます。

## ポート プロファイルのライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
Cisco DCNM	ポート プロファイルにライセンスは必要ありません。ライセンス パッケージに含まれていない機能は Cisco DCNM にバンドルされており、無料で使用できます。Cisco DCNM LAN エンタープライズ ライセンスの取得とインストールの詳細については、『 <i>Cisco DCNM Fundamentals Configuration Guide, Release 5.x</i> 』を参照してください。
Cisco NX-OS	ポート プロファイルにライセンスは必要ありません。ライセンス パッケージに含まれていない機能はすべて Cisco NX-OS システム イメージにバンドルされており、追加費用は一切発生しません。各プラットフォームの Cisco NX-OS ライセンス スキームの説明については、そのプラットフォームのライセンス ガイドを参照してください。

## プラットフォーム サポート

この機能をサポートするプラットフォームは次のとおりです。ガイドラインと制限事項、システム デフォルト値、設定制限などのプラットフォーム固有の情報については、対応するマニュアルを参照してください。

プラットフォーム	マニュアル
Cisco Nexus 1000V シリーズ スイッチ	<a href="#">Cisco Nexus 1000V シリーズ スイッチ マニュアル</a>

## ポート プロファイルの設定

ポート プロファイルの設定を Cisco DCNM で行うことができます。

ここでは、次の内容について説明します。

- 「ポート プロファイルの作成」(P.10-8)
- 「ポート プロファイルの削除」(P.10-9)
- 「ポート プロファイルのイネーブル化とディセーブル化」(P.10-9)
- 「ポート プロファイル継承の設定」(P.10-10)

- ・「システム ポート プロファイルの設定」(P.10-10)
- ・「仮想サービス ドメインのポート プロファイルの設定」(P.10-11)
- ・「レイヤ 3 制御のためのポート プロファイルの設定」(P.10-11)
- ・「iSCSI マルチパスのためのポート プロファイルの設定」(P.10-13)
- ・「VMware ポート グループとしてのポート プロファイルの設定」(P.10-14)
- ・「ポート チャネルの設定」(P.10-15)
- ・「vEthernet インターフェイスの静的ピン接続の設定」(P.10-16)
- ・「コントロールまたはパケット VLAN の静的ピン接続の設定」(P.10-17)
- ・「ポート管理の設定」(P.10-17)
- ・「プライベート VLAN としてのポート プロファイルの設定」(P.10-18)
- ・「DHCP スヌーピングの設定」(P.10-19)
- ・「IP ソース ガードの設定」(P.10-20)
- ・「ARP 検査の設定」(P.10-20)
- ・「レイヤ 2 インターフェイスに対するポート セキュリティのイネーブル化またはディセーブル化」(P.10-21)
- ・「スティッキ MAC アドレス学習のイネーブル化またはディセーブル化」(P.10-22)
- ・「MAC アドレスの最大数の設定」(P.10-22)
- ・「アドレス エージングのタイプと期間の設定」(P.10-23)
- ・「セキュリティ違反時の処理の設定」(P.10-24)
- ・「IPv4 ACL の設定」(P.10-24)
- ・「MAC ACL の設定」(P.10-25)
- ・「CLI の確認」(P.10-25)
- ・「複数デバイスへのポート プロファイルのコピー」(P.10-26)

## ポート プロファイルの作成

イーサネットまたは vEthernet のポート プロファイルを作成できます。

### 手順の詳細

- 
- |               |  |
|---------------|--|
| <b>ステップ 1</b> | [Feature Selector] ペインで、[Interfaces] > [Port Profile] を選択します。<br>この機能をサポートするデバイスが [Summary] ペインに一覧表示されます。              |
| <b>ステップ 2</b> | [Summary] ペインでポート プロファイルを作成する必要があるデバイスを選択します。  |
| <b>ステップ 3</b> | メニュー バーで、[Actions] > [New] > [L2 Ethernet Profile] または [vEthernet Profile] を選択します。<br>新しいプロファイルが [Summary] ペインに表示されます。 |
| <b>ステップ 4</b> | [Summary] ペインで、名前を [Name] フィールドに入力します。   |
| <b>ステップ 5</b> | [Settings] タブで、説明を [Description] フィールドに入力します。  |
| <b>ステップ 6</b> | メニュー バーで [File] > [Deploy] を選択して、変更をデバイスに適用します。  |
-

## ポート プロファイルの削除

今後使用しないポート プロファイルを削除できます。

### 手順の詳細

- 
- |        |   |
|--------|---|
| ステップ 1 | [Feature Selector] ペインで、[Interfaces] > [Port Profile] を選択します。<br>この機能をサポートするデバイスが [Summary] ペインに一覧表示されます。 |
| ステップ 2 | [Summary] ペインで、削除するポート プロファイルが属するデバイスを展開します。  |
| ステップ 3 | 削除するポート プロファイルを選択します。   |
| ステップ 4 | メニュー バーで、[Actions] > [Delete Port Profile] を選択し、[Yes] をクリックして確定します。                                       |
| ステップ 5 | メニュー バーで [File] > [Deploy] を選択して、変更をデバイスに適用します。   |
- 

## ポート プロファイルのイネーブル化とディセーブル化

ポート プロファイルをイネーブルにするかディセーブルにするかを設定できます。

### 作業を開始する前に

ポート プロファイルを新規作成します。または、使用する既存のポート プロファイルを決定します。

### 手順の詳細

- 
- |        |   |
|--------|---|
| ステップ 1 | [Feature Selector] ペインで、[Interfaces] > [Port Profile] を選択します。<br>この機能をサポートするデバイスが [Summary] ペインに一覧表示されます。 |
| ステップ 2 | [Summary] ペインで、イネーブルまたはディセーブルにするポート プロファイルが属するデバイスを展開します。   |
| ステップ 3 | イネーブルまたはディセーブルにするポート プロファイルを選択します。  |
| ステップ 4 | メニュー バーで、[Actions] > [Enable Port Profiles] または [Disable Port Profiles] を選択します。                           |
| ステップ 5 | メニュー バーで [File] > [Deploy] を選択して、変更をデバイスに適用します。   |
-


## ポート プロファイル継承の設定

ポート プロファイルが別のポート プロファイルの設定を継承するように設定することができます。

### 作業を開始する前に

ポート プロファイルを新規作成します。または、使用する既存ポート プロファイルを決めます。

### 手順の詳細

- 
- ステップ 1** [Feature Selector] ペインで、[Interfaces] > [Port Profile] を選択します。  
この機能をサポートするデバイスが [Summary] ペインに一覧表示されます。
- ステップ 2** [Summary] ペインで、別のポート プロファイルを割り当てるポート プロファイルを選択します。
- ステップ 3** [Details] ペインの [Settings] タブをクリックします。
- ステップ 4** [Basic Settings] セクションを展開します。
- ステップ 5** [Parent Profile] ドロップダウン リストから、継承元のポート プロファイルを選択します。
-  **(注)** 親ポート プロファイルを削除するには、[Parent Profile] フィールドに表示されている名前を削除します。
- 
- ステップ 6** メニュー バーで [File] > [Deploy] を選択して、変更をデバイスに適用します。
- 

## システム ポート プロファイルの設定

ポート プロファイルが別のポート プロファイルの設定を継承するように設定することができます。

### 作業を開始する前に

ポート プロファイルを新規作成します。または、使用する既存ポート プロファイルを決めます。

ポートの管理ステータスをアクティブ (Up) に設定します。

ポート モードをアクセスまたはトランクに設定します。

システム VLAN として使用する VLAN を作成します。

アクセスまたはトランク許可 VLAN を設定します。

### 手順の詳細

- 
- ステップ 1** [Feature Selector] ペインで、[Interfaces] > [Port Profile] を選択します。  
この機能をサポートするデバイスが [Summary] ペインに一覧表示されます。
- ステップ 2** [Summary] ペインで、システム ポート プロファイルとして設定するポート プロファイルを選択します。
- ステップ 3** [Details] ペインの [Advanced Settings] タブをクリックします。
- ステップ 4** [System, VM Settings] セクションを展開します。
- ステップ 5** [System VLAN] ドロップダウン リストで、システム VLAN として使用する VLAN を選択します。
- ステップ 6** メニュー バーで [File] > [Deploy] を選択して、変更をデバイスに適用します。
-

## 仮想サービス ドメインのポート プロファイルの設定

Virtual Service Domain (VSD; 仮想サービス ドメイン) を設定すると、指定したポート プロファイルの中でネットワーク サービスのトラフィックを分類して分離することができます。

### 作業を開始する前に

ポート プロファイルを新規作成します。または、使用する既存ポート プロファイルを決定します。

### 手順の詳細

- |        |   |
|--------|---|
| ステップ 1 | [Feature Selector] ペインで、[Interfaces] > [Port Profile] を選択します。<br>この機能をサポートするデバイスが [Summary] ペインに一覧表示されます。 |
| ステップ 2 | [Summary] ペインで、仮想サービス ドメインで設定するポート プロファイルを選択します。  |
| ステップ 3 | [Details] ペインの [Advanced Settings] タブをクリックします。  |
| ステップ 4 | [System, VM Settings] セクションを展開します。  |
| ステップ 5 | [Virtual Service Domain] フィールドに、仮想サービス ドメインの名前を入力します。   |
| ステップ 6 | メニュー バーで [File] > [Deploy] を選択して、変更をデバイスに適用します。   |

## レイヤ 3 制御のためのポート プロファイルの設定

レイヤ 3 制御を行うようにポート プロファイルを設定すると、Virtual Supervisor Module (VSM; 仮想スーパーバイザ モジュール) と Virtual Ethernet Module (VEM; 仮想イーサネット モジュール) が制御およびパケットのトラフィックを IP 経由で送受信できるようになります。

### 作業を開始する前に

VSM ドメインのトランスポート モードがレイヤ 3 として設定済みであることを確認してください。詳細については、使用するプラットフォームとソフトウェア リリースのマニュアルとリリース ノートを参照してください。

すべての VEM が同じレイヤ 2 ドメインに属していることを確認してください。

ホストを Cisco DC-OS Distributed Virtual Switch (DVS; 分散仮想スイッチ) に追加するときに VEM VM カーネル NIC がこのレイヤ 3 制御ポート プロファイルに接続することを確認してください。

このレイヤ 3 制御ポート プロファイルに割り当てることができる VM カーネル NIC は、ホストあたり 1 つのみであることに注意してください。

- 複数の VMware カーネル NIC が同じホストに割り当てられている場合は、最後に割り当てられたものが有効になります。
- 2 つの VMware カーネル NIC が同じホストに割り当てられている場合に、2 番目に割り当てられたものを削除しても、最初に割り当てられたものが VEM によって使用されることはありません。代わりに、VMware カーネル NIC を両方とも削除してから 1 つだけをもう一度割り当てる必要があります。

このレイヤ 3 制御ポート プロファイルに追加する VLAN の VLAN ID を確認してください。

- その VLAN は Cisco DC-OS 上であらかじめ作成しておく必要があります。

- このレイヤ 3 制御ポート プロファイルに割り当てられる VLAN は、システム VLAN でなければなりません。
- いずれかのアップリンク ポートのシステム VLAN 範囲にこの VLAN がすでに含まれている必要があります。



このポート プロファイルがアクセス ポート プロファイルであることを確認してください。トランク ポート プロファイルであってはなりません。ここで説明する手順の中で、ポート プロファイルをアクセス ポート プロファイルとして設定します。

複数のポート プロファイルは、レイヤ 3 制御で設定できることに注意してください。

レイヤ 3 制御を行うときに、ホストごとに異なる VLAN を使用できることに注意してください。

vEthernet ポート プロファイルを新規作成します。または、使用する既存の vEthernet ポート プロファイルを決めます。

## 手順の詳細

- |                |   |
|----------------|---|
| <b>ステップ 1</b>  | [Feature Selector] ペインで、[Interfaces] > [Port Profile] を選択します。<br>この機能をサポートするデバイスが [Summary] ペインに一覧表示されます。   |
| <b>ステップ 2</b>  | [Summary] ペインで、レイヤ 3 制御を設定する vEthernet ポート プロファイルを選択します。  |
| <b>ステップ 3</b>  | [Details] ペインの [Advanced Settings] タブをクリックします。  |
| <b>ステップ 4</b>  | [System, VM Settings] セクションを展開します。  |
| <b>ステップ 5</b>  | [System VLAN] ドロップダウン リストで、このポート プロファイルのシステム VLAN を選択します。システム VLAN を設定すると、ホストが初めて追加されたときや後で再起動されたときに、VEM が VSM に到達できるようになります。   |
|                |  <div style="border: 1px solid black; padding: 5px; margin-top: 5px;"> <b>(注)</b> いずれかのアップリンク ポートのシステム VLAN 範囲にこの VLAN が含まれている必要があります。         </div>                            |
| <b>ステップ 6</b>  | [Capability] ドロップダウン リストで、[Layer 3 Control] を選択します。これで、このポート プロファイルを IP 接続に使用できるようになります。  |
|                |  <div style="border: 1px solid black; padding: 5px; margin-top: 5px;"> <b>(注)</b> vCenter Server で、このレイヤ 3 制御ポート プロファイルが選択されて VM カーネル NIC 物理ポートに割り当てられている必要があります。         </div> |
| <b>ステップ 7</b>  | VMware ポート グループをこのポート プロファイルに割り当てるために、[VM Port Group] チェックボックスをオンにします。  |
| <b>ステップ 8</b>  | [Port Group Name] フィールドに、このポート プロファイルのマッピング先となる VMware ポート グループの名前を入力します。   |
| <b>ステップ 9</b>  | [Details] ペインの [Features] タブをクリックします。   |
| <b>ステップ 10</b> | [Interfaces] を展開して、[Ethernet] を選択します。   |
| <b>ステップ 11</b> | [Admin Status] ドロップダウン リストで [Up] を選択し、すべてのポートを管理上イネーブルにします。   |
| <b>ステップ 12</b> | [Mode] ドロップダウン リストで [Access] を選択し、インターフェイスをスイッチ アクセス ポート (デフォルト) に指定します。  |
| <b>ステップ 13</b> | [Switching] を展開して、[VLAN] を選択します。  |

- ステップ 14** [Access VLAN] ドロップダウン リストで、システム VLAN の ID を選択します。
- ステップ 15** [Details] ペインの [Settings] タブをクリックします。
- ステップ 16** [Basic Settings] セクションを展開します。
- ステップ 17** [State] ドロップダウン リストで、[Enabled] を選択します。
- ステップ 18** メニュー バーで [File] > [Deploy] を選択して、変更をデバイスに適用します。
- このポート プロファイルの設定が、割り当てられたポートに適用されます。また、vCenter Server 上の VMware vSwitch 内にポート グループが作成されます。

## iSCSI マルチパスのためのポート プロファイルの設定

ホストとターゲットとの通信を iSCSI プロトコルを使用してマルチパス化するには、iSCSI マルチパス ポート プロファイルを作成して、インターフェイスをそのプロファイルに割り当てます。

### 作業を開始する前に

ホストにポート チャネルが設定済みで、2 つ以上の物理 NIC が含まれていることを確認してください。SAN 外部ストレージにアクセスするための VMware カーネル NIC が作成済みであることを確認してください。

この iSCSI マルチパス ポート プロファイルに使用するシステム VLAN を Cisco DC-OS 上に新規作成します。または、使用するシステム VLAN を決定します。いずれかのアップリンク ポートのシステム VLAN 範囲にこの VLAN がすでに含まれていることを確認してください。

vEthernet ポート プロファイルを新規作成します。または、使用する既存の vEthernet ポート プロファイルを決めます。

このポート プロファイルがアクセス ポート プロファイルであることを確認してください。トランク ポート プロファイルであってはなりません。

### 手順の詳細

- ステップ 1** [Feature Selector] ペインで、[Interfaces] > [Port Profile] を選択します。
- この機能をサポートするデバイスが [Summary] ペインに一覧表示されます。
- ステップ 2** [Summary] ペインで、iSCSI マルチパスを設定する vEthernet ポート プロファイルを選択します。
- ステップ 3** [Details] ペインの [Advanced Settings] タブをクリックします。
- ステップ 4** [System, VM Settings] セクションを展開します。
- ステップ 5** [System VLAN] ドロップダウン リストで、このポート プロファイルのシステム VLAN を選択します。システム VLAN を設定すると、ホストが初めて追加されたときや後で再起動されたときに、VEM が VSM に到達できるようになります。



**(注)** いずれかのアップリンク ポートのシステム VLAN 範囲にこの VLAN が含まれている必要があります。

- ステップ 6** [Capability] ドロップダウン リストで、[ISCSI-MULTIPATH] を選択します。これで、このポート プロファイルを iSCSI マルチパスに使用できるようになります。



(注) vCenter Server で、iSCSI マルチパス ポート プロファイルが選択されて、VM カーネル NIC ポートに割り当てられている必要があります。

- ステップ 7** VMware ポート グループをこのポート プロファイルに割り当てるために、[VM Port Group] チェックボックスをオンにします。
- ステップ 8** [Port Group Name] フィールドに、このポート プロファイルのマッピング先となる VMware ポート グループの名前を入力します。
- ステップ 9** [Details] ペインの [Features] タブをクリックします。
- ステップ 10** [Interfaces] を展開して、[Ethernet] を選択します。
- ステップ 11** [Admin Status] ドロップダウン リストで [Up] を選択し、すべてのポートを管理上イネーブルにします。
- ステップ 12** [Mode] ドロップダウン リストで [Access] を選択し、インターフェイスをスイッチ アクセス ポート (デフォルト) に指定します。
- ステップ 13** [Switching] を展開して、[VLAN] を選択します。
- ステップ 14** [Access VLAN] ドロップダウン リストで、システム VLAN の ID を選択します。
- ステップ 15** [Details] ペインの [Settings] タブをクリックします。
- ステップ 16** [Basic Settings] セクションを展開します。
- ステップ 17** [State] ドロップダウン リストで、[Enabled] を選択します。
- ステップ 18** メニュー バーで [File] > [Deploy] を選択して、変更をデバイスに適用します。

このポート プロファイルの設定が、割り当てられたポートに適用されます。また、vCenter Server 上の VMware vSwitch 内にポート グループが作成されます。

## VMware ポート グループとしてのポート プロファイルの設定

ポート プロファイルを VMware ポート グループとして設定することができます。vCenter Server 接続が確立すると、Cisco DC-OS で作成されたポート グループは、vCenter Server の仮想スイッチに配信されます。

### 作業を開始する前に

ポート プロファイルを新規作成します。または、使用する既存ポート プロファイルを決定します。

VMware ポート グループを VMware サーバ上に作成します。詳細については、VMware のマニュアルを参照してください。

### 手順の詳細

- ステップ 1** [Feature Selector] ペインで、[Interfaces] > [Port Profile] を選択します。  
この機能をサポートするデバイスが [Summary] ペインに一覧表示されます。
- ステップ 2** [Summary] ペインで、目的のポート プロファイルを選択します。
- ステップ 3** [Details] ペインの [Advanced Settings] タブをクリックします。



- ステップ 4** VMware ポート グループをこのポート プロファイルに割り当てるために、[VM Port Group] チェックボックスをオンにします。
- ステップ 5** [Port Group Name] フィールドに、このポート プロファイルのマッピング先となる VMware ポート グループの名前を入力します。
- ステップ 6** (任意) このポート プロファイルに割り当てられるポートの数を制限するには、[Max Ports] フィールドにポート数を入力します。有効な範囲は 1 ～ 1024 です。



(注) この制限を指定できるのは、ポート プロファイルのタイプがアップリンクではない場合のみです。

- ステップ 7** メニュー バーで [File] > [Deploy] を選択して、変更をデバイスに適用します。

## ポート チャネルの設定

vPC-HM のためのポート チャネルをポート プロファイルの中で設定できます。

### 作業を開始する前に

ポート プロファイルを新規作成します。または、使用する既存ポート プロファイルを決定します。

アップストリーム スイッチ内で Cisco Discovery Protocol (CDP) が設定されているかどうかを確認してください。CDP を使用するとき CDP タイマーがデフォルト (60 秒) の場合は、リンクが動作中であるというアドバタイズの直後に動作を停止したときに、再び動作状態に戻るのに最大 60 秒かかることがあります。

ポート チャネルが複数のアップストリーム スイッチに接続する場合は、vPC-HM を設定しておく必要があります。vPC-HM が設定されていない場合は、Cisco DC-OS の背後にある VM が、不明ユニキャスト、マルチキャスト フラッド、およびブロードキャストの重複パケットをネットワークから受け取ります。

アップストリーム スイッチで vPC がイネーブルになっている場合は、vPC-HM を Cisco DC-OS 上で設定しないでください。vPC-HM が Cisco DC-OS 上で設定され、vPC がアップストリーム スイッチ上で設定されている場合は、接続問題が発生する可能性があります。

### 手順の詳細

- ステップ 1** [Feature Selector] ペインで、[Interfaces] > [Port Profile] を選択します。  
この機能をサポートするデバイスが [Summary] ペインに一覧表示されます。
- ステップ 2** [Summary] ペインで、目的のポート プロファイルを選択します。
- ステップ 3** [Details] ペインの [Advanced Settings] タブをクリックします。
- ステップ 4** [Port Channel, Pinning Settings] セクションを展開します。
- ステップ 5** [Channel Group Auto] チェックボックスをオンにしてから、[Protocol Mode] ドロップダウン リストで [Active]、[Passive]、または [On] を選択します。  
[On] がデフォルトのチャネル モードです。Link Aggregation Control Protocol (LACP) を実行していないポート チャネルはすべて、このモードであることが必要です。

[Active] は、LACP がイネーブルのときにインターフェイスがアクティブ ネゴシエーション ステートになります。このステートのときは、ポートが LACP パケットを送信して他のポートとのネゴシエーションを開始します。

[Passive] は、LACP がイネーブルのときにインターフェイスがパッシブ ネゴシエーション ステートになります。このステートのときは、ポートは受信した LACP パケットに応答しますが、LACP ネゴシエーションを開始することはありません。

**ステップ 6** (任意) 次のいずれかを行います。

- アップストリーム スイッチ上で CDP が設定されている場合は、[SubGroup] ドロップダウン リストで [CDP] を選択します。
- アップストリーム スイッチ上で CDP が設定されていない場合は、[SubGroup] ドロップダウン リストで [Manual] を選択します。
- アップストリーム スイッチがポート チャネルをサポートしていない場合は、[MAC Pinning] チェックボックスをオンにしてから、[Subgroup ID] フィールドに、アップストリーム スイッチのトラフィックを管理するサブグループの ID 番号 (0 ~ 31) を入力します。

**ステップ 7** メニュー バーで [File] > [Deploy] を選択して、変更をデバイスに適用します。

## vEthernet インターフェイスの静的ピン接続の設定

vEthernet インターフェイス上の静的ピン接続を vEthernet ポート プロファイルの中で設定することができます。



(注)

静的ピン接続の設定は、特定の vEthernet インターフェイスに対して行うこともできます。詳細については、「[vEthernet インターフェイスの静的ピン接続の設定](#)」(P.8-5) を参照してください。

### 作業を開始する前に

ポート プロファイルを新規作成します。または、使用する既存ポート プロファイルを決定します。

### 手順の詳細

- ステップ 1** [Feature Selector] ペインで、[Interfaces] > [Port Profile] を選択します。  
この機能をサポートするデバイスが [Summary] ペインに一覧表示されます。
- ステップ 2** [Summary] ペインで、目的の vEthernet ポート プロファイルを選択します。
- ステップ 3** [Details] ペインの [Advanced Settings] タブをクリックします。
- ステップ 4** [Port Channel, Pinning Settings] セクションを展開します。
- ステップ 5** [Subgroup ID] フィールドに、1 ~ 31 の範囲で ID 番号を入力します。
- ステップ 6** メニュー バーで [File] > [Deploy] を選択して、変更をデバイスに適用します。

## コントロールまたはパケット VLAN の静的ピン接続の設定

コントロールまたはパケット VLAN の静的ピン接続を設定することができます。

### 作業を開始する前に

イーサネット タイプのシステム ポート プロファイルを作成します。詳細については、「[システム ポート プロファイルの設定](#)」(P.10-10) を参照してください。

静的ピン接続をコントロール VLAN に対して設定するには、そのコントロール VLAN が、このポート プロファイルのシステム VLAN の 1 つとして指定されていることを確認してください。

静的ピン接続をパケット VLAN に対して設定するには、そのパケット VLAN が、このポート プロファイルのパケット VLAN の 1 つとして指定されていることを確認してください。

### 手順の詳細

- 
- |               |   |
|---------------|---|
| <b>ステップ 1</b> | [Feature Selector] ペインで、[Interfaces] > [Port Profile] を選択します。<br>この機能をサポートするデバイスが [Summary] ペインに一覧表示されます。   |
| <b>ステップ 2</b> | [Summary] ペインで、目的のポート プロファイルを選択します。   |
| <b>ステップ 3</b> | [Details] ペインの [Advanced Settings] タブをクリックします。  |
| <b>ステップ 4</b> | [Port Channel, Pinning Settings] セクションを展開します。   |
| <b>ステップ 5</b> | 次のいずれかを行います。 <ul style="list-style-type: none"><li>コントロール VLAN に対して静的ピン接続を設定するには、[Control VLAN Subgroup ID] フィールドに 1 ～ 31 の範囲で ID 番号を入力します。</li><li>パケット VLAN に対して静的ピン接続を設定するには、[Packet VLAN Subgroup ID] フィールドに 1 ～ 31 の範囲で ID 番号を入力します。</li></ul> |
| <b>ステップ 6</b> | メニュー バーで [File] > [Deploy] を選択して、変更をデバイスに適用します。   |
- 

## ポート管理の設定

ポートの管理（アクセス/トランク モード、各ポートの管理ステートなど）をプロファイルの中で設定することができます。

### 作業を開始する前に

ポート プロファイルを新規作成します。または、使用する既存ポート プロファイルを決定します。

### 手順の詳細

- 
- |               |   |
|---------------|---|
| <b>ステップ 1</b> | [Feature Selector] ペインで、[Interfaces] > [Port Profile] を選択します。<br>この機能をサポートするデバイスが [Summary] ペインに一覧表示されます。 |
| <b>ステップ 2</b> | [Summary] ペインで、目的のポート プロファイルを選択します。   |
| <b>ステップ 3</b> | [Details] ペインの [Features] タブをクリックします。   |
| <b>ステップ 4</b> | [Interfaces] を展開して、[Ethernet] を選択します。   |

**ステップ 5** [Mode] ドロップダウン リストで、次のいずれかを選択します。

- **Access** : パケットは 1 つの非タグ付き VLAN のみに送信されます。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 VLAN1 です。
- **Trunk** : ネイティブ VLAN のタグなしパケットを送信し、他のすべての VLAN のカプセル化されたタグ付きパケットを送信します。

**ステップ 6** [Admin Status] ドロップダウン リストで [Up] を選択します。

**ステップ 7** メニュー バーで [File] > [Deploy] を選択して、変更をデバイスに適用します。

## プライベート VLAN としてのポート プロファイルの設定

ポート プロファイルをプライベート VLAN (PVLAN) として使用するように設定することができます。プライベート VLAN の詳細については、使用するプラットフォームとソフトウェア リリースのマニュアルを参照してください。

### 作業を開始する前に

ポート プロファイルを新規作成します。または、使用する既存ポート プロファイルを決定します。

### 手順の詳細

**ステップ 1** [Feature Selector] ペインで、[Interfaces] > [Port Profile] を選択します。

この機能をサポートするデバイスが [Summary] ペインに一覧表示されます。

**ステップ 2** [Summary] ペインで、目的のポート プロファイルを選択します。

**ステップ 3** [Details] ペインの [Features] タブをクリックします。

**ステップ 4** [Interfaces] を展開して、[Ethernet] を選択します。

**ステップ 5** [Mode] ドロップダウン リストで、次のいずれかを選択します。

- **PVLAN Promiscuous** : プライマリ VLAN に属する無差別モード ポートを指定し、レイヤ 3 ゲートウェイと通信します。無差別モード ポートは、セカンダリ VLAN に関連付けられているインターフェイスを含む、PVLAN ドメイン内の任意のインターフェイスと通信できます。
- **PVLAN Host** : PVLAN ペアのセカンダリ VLAN に、コミュニティまたは独立 PVLAN ホストポートとして属しているホスト ポートを指定します。

**ステップ 6** [Switching] セクションを展開して、[VLAN] を選択します。

**ステップ 7** [PVLAN Host] フィールドに、プライマリ VLAN の ID 番号と、セカンダリ VLAN の ID 番号を 1 つ以上入力します。

**ステップ 8** メニュー バーで [File] > [Deploy] を選択して、変更をデバイスに適用します。

## DHCP スヌーピングの設定

ポート プロファイルに属する仮想インターフェイスが DHCP メッセージの送信元として信頼できるものかどうかと、各ポートで受信される DHCP パケットのレート制限を設定することができます。

### 作業を開始する前に

Virtual Supervisor Module (VSM) とすべての Virtual Ethernet Module (VEM) で、この機能をサポートするソフトウェア リリースが実行されていることと、VEM 機能レベルが更新済みであることを確認してください（使用するプラットフォームとソフトウェアのマニュアルを参照）。

vEthernet インターフェイスは、デフォルトでは信頼されていないことに注意してください。ただし、仮想サービス ドメイン (VSD) などの他の機能で使用する特別な vEthernet ポートは例外であり、信頼されています。

vEthernet インターフェイスがレイヤ 2 インターフェイスとして設定されていることを確認してください。

DHCP スヌーピングをシームレスに実行するために、Dynamic ARP Inspection (DAI; ダイナミック ARP インスペクション)、IP ソース ガード、および VSD サービス Virtual Machine (VM; 仮想マシン) のポートがデフォルトでは信頼できるポートとなっていることに注意してください。これらのポートを「信頼できない」と設定しても、その設定は無視されます。

設定されたレートを順守できない場合は、ポートが errdisable ステートに変更されることに注意してください。

ポート プロファイルを新規作成します。または、使用する既存ポート プロファイルを決定します。

### 手順の詳細

- 
- |               |   |
|---------------|---|
| <b>ステップ 1</b> | [Feature Selector] ペインで、[Interfaces] > [Port Profile] を選択します。<br>この機能をサポートするデバイスが [Summary] ペインに一覧表示されます。               |
| <b>ステップ 2</b> | [Summary] ペインで、目的のポート プロファイルを選択します。   |
| <b>ステップ 3</b> | [Details] ペインの [Features] タブをクリックします。   |
| <b>ステップ 4</b> | [Switching] セクションを展開して、[DHCP Snooping] を選択します。  |
| <b>ステップ 5</b> | [Trust State] ドロップダウン リストで、インターフェイスを DHCP スヌーピングに関して「信頼できる」と設定する場合は [Trusted] を選択し、「信頼できない」と設定する場合は [Untrusted] を設定します。 |
| <b>ステップ 6</b> | [Rate Limit] フィールドに、1 ~ 2048 の範囲で数値を入力します。  |
| <b>ステップ 7</b> | メニュー バーで [File] > [Deploy] を選択して、変更をデバイスに適用します。   |
-

## IP ソース ガードの設定

ポート プロファイルに属するインターフェイスに対して IP ソース ガードをイネーブルにするかディセーブルにするかを設定できます。

### 作業を開始する前に

Virtual Supervisor Module (VSM) とすべての Virtual Ethernet Module (VEM) で、この機能をサポートするソフトウェア リリースが実行されていることと、VEM 機能レベルが更新済みであることを確認してください（使用するプラットフォームとソフトウェアのマニュアルを参照）。

デフォルトでは、すべてのインターフェイスに対して IP ソース ガードがディセーブルになっていることに注意してください。

DHCP スヌーピングがイネーブルになっていることを確認してください。詳細については、「[DHCP スヌーピングの設定](#)」(P.10-19) を参照してください。

ポート プロファイルを新規作成します。または、使用する既存ポート プロファイルを決定します。

### 手順の詳細

- 
- |               |   |
|---------------|---|
| <b>ステップ 1</b> | [Feature Selector] ペインで、[Interfaces] > [Port Profile] を選択します。<br>この機能をサポートするデバイスが [Summary] ペインに一覧表示されます。 |
| <b>ステップ 2</b> | [Summary] ペインで、目的のポート プロファイルを選択します。   |
| <b>ステップ 3</b> | [Details] ペインの [Features] タブをクリックします。   |
| <b>ステップ 4</b> | [Switching] セクションを展開して、[IP Source Guard] を選択します。  |
| <b>ステップ 5</b> | この機能をイネーブルにする場合は、[IP Source Guard] チェックボックスをオンにし、ディセーブルにする場合はオフにします。                                      |
| <b>ステップ 6</b> | メニュー バーで [File] > [Deploy] を選択して、変更をデバイスに適用します。   |
- 

## ARP 検査の設定

ポート プロファイルに属する vEthernet インターフェイスを、Address Resolution Protocol (ARP; アドレス解決プロトコル) 検査に関して信頼できると設定することができます。

### 作業を開始する前に

vEthernet インターフェイスは、デフォルトでは信頼されないことに注意してください。ただし、Virtual Switch Domain (VSD; 仮想スイッチ ドメイン) に属している場合を除きます。

インターフェイスが信頼されていない場合は、ARP の要求と応答はすべて、有効な IP-MAC アドレス バインディングを持つかどうかの確認を受け、確認後にローカル キャッシュが更新されてパケットが転送されることに注意してください。パケットの IP-MAC アドレス バインディングが無効な場合は、パケットがドロップされます。

信頼できるインターフェイスで受信された ARP パケットは転送されますが、チェックされないことに注意してください。

vEthernet ポート プロファイルを新規作成します。または、使用する既存の vEthernet ポート プロファイルを決定します。

## 手順の詳細

- 
- |        |  |
|--------|--|
| ステップ 1 | [Feature Selector] ペインで、[Interfaces] > [Port Profile] を選択します。<br>この機能をサポートするデバイスが [Summary] ペインに一覧表示されます。          |
| ステップ 2 | [Summary] ペインで、目的のポート プロファイルを選択します。  |
| ステップ 3 | [Details] ペインの [Features] タブをクリックします。  |
| ステップ 4 | [Switching] セクションを展開して、[ARP Inspection] を選択します。  |
| ステップ 5 | [Trust State] ドロップダウン リストで、インターフェイスを ARP 検査に関して「信頼できる」と設定する場合は [Trusted] を選択し、「信頼できない」と設定する場合は [Untrusted] を選択します。 |
| ステップ 6 | [Rate Limit] フィールドに、1 ～ 2048 の範囲で数値を入力します。   |
| ステップ 7 | メニュー バーで [File] > [Deploy] を選択して、変更をデバイスに適用します。  |
- 

## レイヤ 2 インターフェイスに対するポート セキュリティのイネーブル化 またはディセーブル化

ポート プロファイルに属するインターフェイスに対してポート セキュリティをイネーブルにするかディセーブルにするかを設定できます。



(注) ルーテッド インターフェイスでは、ポート セキュリティをイネーブルにできません。

## 作業を開始する前に

デフォルトでは、すべてのインターフェイスに対してポート セキュリティがディセーブルになっていることに注意してください。

インターフェイスのポート セキュリティをイネーブルにすると、MAC アドレスのダイナミック学習もイネーブルになります。スティック方式の MAC アドレス学習をイネーブルにするには、「[スティック MAC アドレス学習のイネーブル化またはディセーブル化](#)」(P.10-22) の手順も完了する必要があります。

vEthernet ポート プロファイルを新規作成します。または、使用する既存の vEthernet ポート プロファイルを決めます。

## 手順の詳細

- 
- |        |   |
|--------|---|
| ステップ 1 | [Feature Selector] ペインで、[Interfaces] > [Port Profile] を選択します。<br>この機能をサポートするデバイスが [Summary] ペインに一覧表示されます。 |
| ステップ 2 | [Summary] ペインで、目的のポート プロファイルを選択します。   |
| ステップ 3 | [Details] ペインの [Features] タブをクリックします。   |
| ステップ 4 | [Switching] セクションを展開して、[Port Security] を選択します。  |
| ステップ 5 | [Port Security] ドロップダウン リストで、この機能をイネーブルにする場合は [Enabled]、ディセーブルにする場合は [Disabled] を選択します。                   |
| ステップ 6 | メニュー バーで [File] > [Deploy] を選択して、変更をデバイスに適用します。   |
-

## スティッキ MAC アドレス学習のイネーブル化またはディセーブル化

ポート プロファイルに属するインターフェイスに対してスティッキ MAC アドレス学習をイネーブルにするかディセーブルにするかを設定できます。

### 作業を開始する前に

ダイナミック MAC アドレス学習がインターフェイスのデフォルトであることに注意してください。

デフォルトでは、スティッキ MAC アドレス学習がディセーブルになっていることに注意してください。

vEthernet ポート プロファイルを新規作成します。または、使用する既存の vEthernet ポート プロファイルを決めます。

設定するポート プロファイルに対してポート セキュリティがイネーブルになっていることを確認してください。

### 手順の詳細

- 
- |               |   |
|---------------|---|
| <b>ステップ 1</b> | [Feature Selector] ペインで、[Interfaces] > [Port Profile] を選択します。<br>この機能をサポートするデバイスが [Summary] ペインに一覧表示されます。 |
| <b>ステップ 2</b> | [Summary] ペインで、目的のポート プロファイルを選択します。   |
| <b>ステップ 3</b> | [Details] ペインの [Features] タブをクリックします。   |
| <b>ステップ 4</b> | [Switching] セクションを展開して、[Port Security] を選択します。  |
| <b>ステップ 5</b> | このポート プロファイルに対してポート セキュリティ機能をイネーブルにする場合は [Stickiness] チェックボックスをオンにし、ディセーブルにする場合はオフにします。                   |
| <b>ステップ 6</b> | メニュー バーで [File] > [Deploy] を選択して、変更をデバイスに適用します。   |
- 

## MAC アドレスの最大数の設定

ポート プロファイルに属するインターフェイスに対して、学習またはスタティックに設定できる MAC アドレスの最大数を設定できます。



- (注) インターフェイスですでに学習されているアドレス数またはインターフェイスにスタティックに設定されたアドレス数よりも小さい数を最大数に指定すると、コマンドは拒否されます。
- 

### 作業を開始する前に

セキュア MAC は L2 Forwarding Table (L2FT; L2 転送テーブル) を共有します。各 VLAN の転送テーブルには最大 1024 エントリを保持できます。

VLAN には、セキュア MAC アドレス数のデフォルトの最大値はありません。

vEthernet ポート プロファイルを新規作成します。または、使用する既存の vEthernet ポート プロファイルを決めます。

設定するポート プロファイルに対してポート セキュリティがイネーブルになっていることを確認してください。



## 手順の詳細

- 
- |        |  |
|--------|--|
| ステップ 1 | [Feature Selector] ペインで、[Interfaces] > [Port Profile] を選択します。<br>この機能をサポートするデバイスが [Summary] ペインに一覧表示されます。      |
| ステップ 2 | [Summary] ペインで、目的のポート プロファイルを選択します。  |
| ステップ 3 | [Details] ペインの [Features] タブをクリックします。  |
| ステップ 4 | [Switching] セクションを展開して、[Port Security] を選択します。   |
| ステップ 5 | [Maximum Secure MAC to add] フィールドに、1 ～ 1024 の範囲で数値を入力します。これは、このポート プロファイルに対して学習またはスタティックに設定できる MAC アドレスの最大数です。 |
| ステップ 6 | メニュー バーで [File] > [Deploy] を選択して、変更をデバイスに適用します。  |
- 

## アドレス エージングのタイプと期間の設定

ダイナミック方式で学習された MAC アドレスがエージング期限に到達したかどうかを判断するために使用される、MAC アドレス エージングのタイプと期間を設定することができます。

## 作業を開始する前に

vEthernet ポート プロファイルを新規作成します。または、使用する既存の vEthernet ポート プロファイルを決めます。

ポート セキュリティが目的のインターフェイスでイネーブルになっていることを確認します。

## 手順の詳細

- 
- |        |   |
|--------|---|
| ステップ 1 | [Feature Selector] ペインで、[Interfaces] > [Port Profile] を選択します。<br>この機能をサポートするデバイスが [Summary] ペインに一覧表示されます。             |
| ステップ 2 | [Summary] ペインで、目的のポート プロファイルを選択します。   |
| ステップ 3 | [Details] ペインの [Features] タブをクリックします。   |
| ステップ 4 | [Switching] セクションを展開して、[Port Security] を選択します。  |
| ステップ 5 | [Aging Type] フィールドに、ダイナミックに学習された MAC アドレスに適用されるエージングのタイプ ([Absolute] または [InActivity]) を入力します。デフォルトは [Absolute] です。   |
| ステップ 6 | [Age] フィールドに、ダイナミックに学習された MAC アドレスがドロップされるまでのエージング タイムを分単位で入力します。 <i>minutes</i> の最大値は 1440 です。デフォルトは 0 分（エージングなし）です。 |
| ステップ 7 | メニュー バーで [File] > [Deploy] を選択して、変更をデバイスに適用します。   |
-

## セキュリティ違反時の処理の設定

ポート プロファイルに属するインターフェイスがセキュリティ違反にどのように応答するかを設定できます。

### 作業を開始する前に

vEthernet ポート プロファイルを新規作成します。または、使用する既存の vEthernet ポート プロファイルを決定します。  
ポート セキュリティが目的のインターフェイスでイネーブルになっていることを確認します。

### 手順の詳細

- 
- |               |  |
|---------------|--|
| <b>ステップ 1</b> | [Feature Selector] ペインで、[Interfaces] > [Port Profile] を選択します。<br>この機能をサポートするデバイスが [Summary] ペインに一覧表示されます。  |
| <b>ステップ 2</b> | [Summary] ペインで、目的のポート プロファイルを選択します。  |
| <b>ステップ 3</b> | [Details] ペインの [Features] タブをクリックします。  |
| <b>ステップ 4</b> | [Switching] セクションを展開して、[Port Security] を選択します。   |
| <b>ステップ 5</b> | [Violation Action] ドロップダウン リストで、このポート プロファイルに割り当てられたインターフェイスがセキュリティ違反に対して実行するアクション ([Protect]、[Restrict]、または [Shutdown]) を選択します。デフォルトは、インターフェイスのシャットダウンです。 |
| <b>ステップ 6</b> | メニュー バーで [File] > [Deploy] を選択して、変更をデバイスに適用します。  |
- 

## IPv4 ACL の設定

ポート プロファイルに属するインターフェイスに対して IPv4 Access Control List (ACL; アクセス コントロール リスト) を設定することができます。

ACLの詳細については、使用するプラットフォームとソフトウェア リリースのマニュアルを参照してください。

### 作業を開始する前に

ポート プロファイルを新規作成します。または、使用する既存ポート プロファイルを決定します。

### 手順の詳細

- 
- |               |   |
|---------------|---|
| <b>ステップ 1</b> | [Feature Selector] ペインで、[Interfaces] > [Port Profile] を選択します。<br>この機能をサポートするデバイスが [Summary] ペインに一覧表示されます。 |
| <b>ステップ 2</b> | [Summary] ペインで、目的のポート プロファイルを選択します。   |
| <b>ステップ 3</b> | [Details] ペインの [Features] タブをクリックします。   |
| <b>ステップ 4</b> | [Security] を展開して、[IPv4 ACL] を選択します。   |
| <b>ステップ 5</b> | [Incoming IPv4 Traffic] ドロップダウン リストで、着信トラフィックに使用する ACL を選択します。  |
| <b>ステップ 6</b> | [Outgoing IPv4 Traffic] ドロップダウン リストで、発信トラフィックに使用する ACL を選択します。  |
| <b>ステップ 7</b> | メニュー バーで [File] > [Deploy] を選択して、変更をデバイスに適用します。   |
-

## MAC ACL の設定

ポート プロファイルに属するインターフェイスに対して MAC Access Control List (ACL; アクセス コントロール リスト) を設定できます。

ACL の詳細については、使用するプラットフォームのマニュアルを参照してください。

### 作業を開始する前に

ポート プロファイルを新規作成します。または、使用する既存ポート プロファイルを決定します。

### 手順の詳細

- 
- |        |   |
|--------|---|
| ステップ 1 | [Feature Selector] ペインで、[Interfaces] > [Port Profile] を選択します。<br>この機能をサポートするデバイスが [Summary] ペインに一覧表示されます。 |
| ステップ 2 | [Summary] ペインで、目的のポート プロファイルを選択します。   |
| ステップ 3 | [Details] ペインの [Features] タブをクリックします。   |
| ステップ 4 | [Security] を展開して、[MAC ACL] を選択します。  |
| ステップ 5 | [Incoming Traffic] ドロップダウン リストで、着信トラフィックに使用する ACL を選択します。   |
| ステップ 6 | [Outgoing Traffic] ドロップダウン リストで、発信トラフィックに使用する ACL を選択します。   |
| ステップ 7 | メニュー バーで [File] > [Deploy] を選択して、変更をデバイスに適用します。   |
- 

## CLI の確認

ポート プロファイルに対して作成した設定を確認して、必要に応じてコマンドを追加、変更、または削除できます。

### 作業を開始する前に

ポート プロファイルを新規作成します。または、使用する既存ポート プロファイルを決定します。

### 手順の詳細

- 
- |        |   |
|--------|---|
| ステップ 1 | [Feature Selector] ペインで、[Interfaces] > [Port Profile] を選択します。<br>この機能をサポートするデバイスが [Summary] ペインに一覧表示されます。 |
| ステップ 2 | [Summary] ペインで、目的のポート プロファイルを選択します。   |
| ステップ 3 | [Details] ペインの [CLI] タブをクリックします。<br>選択したポート プロファイルの設定が表示されます。   |
| ステップ 4 | (任意) 必要に応じてコマンドを追加、変更、削除します。  |
| ステップ 5 | メニュー バーで [File] > [Deploy] を選択して、変更をデバイスに適用します。   |
-

## 複数デバイスへのポート プロファイルのコピー

コンフィギュレーション変更管理機能を使用すると、ポート プロファイルの設定をコピーして複数のデバイスに展開することができます。コンフィギュレーション変更管理機能では、CLI コマンドを使用して設定に変更を加えることもできます。詳細については、『*Cisco DCNM System Management Configuration Guide, Release 5.x*』を参照してください。

### 作業を開始する前に

ポート プロファイルを新規作成します。または、使用する既存のポート プロファイルを決定します。

### 手順の詳細

- 
- |               |   |
|---------------|---|
| <b>ステップ 1</b> | [Feature Selector] ペインで、[Interfaces] > [Port Profile] を選択します。<br>この機能をサポートするデバイスが [Summary] ペインに一覧表示されます。                 |
| <b>ステップ 2</b> | [Summary] ペインで、目的のポート プロファイルを選択します。   |
| <b>ステップ 3</b> | メニュー バーで、[Actions] > [Copy to Multiple Devices] を選択します。<br>[Configuration Delivery Jobs] コンテンツ ペインが表示されます。                |
| <b>ステップ 4</b> | コンフィギュレーション配信ジョブをカスタマイズして展開します。詳細については、『 <i>Cisco DCNM System Management Configuration Guide, Release 5.x</i> 』を参照してください。 |
- 

## ポート プロファイルのフィールドの説明

ここでは、ポート プロファイル機能に関する以下のフィールドについて説明します。

- 「[Port Profile] : [Settings] : [Basic Settings] セクション」 (P.10-27)
- 「[Port Profile] : [Settings] : [Inherited Interfaces] セクション」 (P.10-27)
- 「[Port Profile] : [Advanced Settings] : [System, VM Settings] セクション」 (P.10-27)
- 「[Port Profile] : [Advanced Settings] : [Port Channel, Pinning] セクション」 (P.10-28)
- 「[Port Profile] : [Features] : [Interfaces] : [Ethernet]」 (P.10-29)
- 「[Port Profile] : [Features] : [Switching] : [VLAN]」 (P.10-29)
- 「[Port Profile] : [Features] : [Switching] : [DHCP Snooping]」 (P.10-30)
- 「[Port Profile] : [Features] : [Switching] : [IP Source Guard]」 (P.10-30)
- 「[Port Profile] : [Features] : [Switching] : [ARP Inspection]」 (P.10-30)
- 「[Port Profile] : [Features] : [Switching] : [Port Security]」 (P.10-31)
- 「[Port Profile] : [Features] : [Security] : [IPv4 ACL]」 (P.10-31)
- 「[Port Profile] : [Features] : [Security] : [MAC ACL]」 (P.10-31)

## [Port Profile] : [Settings] : [Basic Settings] セクション

表 10-1 [Port Profile] : [Settings] : [Basic Settings] セクション

フィールド	説明
Name	表示のみ。ポート プロファイルの名前。
Description	ポート プロファイルを表す単語またはフレーズ。
Type	ポート プロファイルのタイプ。[Ethernet] または [vEthernet]。
Interface Count	選択されているポート プロファイルを継承するインターフェイスの数。
State	ポート プロファイルのステート。[Enabled] または [Disabled]。
Parent Profile	選択されているポート プロファイルの特性の継承元であるポート プロファイルの名前。選択されているポート プロファイルが階層内の最後のレベル（4 番目のレベル）の場合、このフィールドはディセーブル。

## [Port Profile] : [Settings] : [Inherited Interfaces] セクション

表 10-2 [Port Profile] : [Settings] : [Inherited Interfaces] セクション

フィールド	説明
Name	表示のみ。インターフェイスの名前。
Description	表示のみ。インターフェイスを表す単語またはフレーズ。
Host Name	表示のみ。インターフェイスが存在するホストの名前。
VM Name	表示のみ。インターフェイスが存在する仮想マシンの名前。
VM Adapter	表示のみ。インターフェイスが存在する仮想マシン アダプタの名前。

## [Port Profile] : [Advanced Settings] : [System, VM Settings] セクション

表 10-3 [Port Profile] : [Advanced Settings] : [System, VM Settings] セクション

フィールド	説明
<b>System</b>	
Virtual Service Domain	VM ポートが存在する Virtual Service Domain (VSD; 仮想サービス ドメイン) の名前。
System VLAN	ポート プロファイルに対して定義されているシステム LAN。有効な選択肢は、1 ～ 3967 と 4048 ～ 4093、[None]、および 1 つ以上の特定の VLAN。
Capability	この vEthernet ポート プロファイルが対応している機能 (iSCSI マルチパスまたはレイヤ 3)。このオプションは、イーサネット ポート プロファイルの場合はディセーブル。
<b>VM Setting</b>	
VM Port Group	このポート プロファイルが VMware ポート グループかどうかを表す設定。
Port Group Name	[VM Port Group] が選択されていない場合は表示のみ。VMware ポート グループの名前。
Max Ports	このポート プロファイルに割り当てることができるポートの最大数。

## [Port Profile] : [Advanced Settings] : [Port Channel, Pinning] セクション

表 10-4 [Port Profile] : [Advanced Settings] : [Port Channel, Pinning] セクション

フィールド	説明
<b>Channel Setting</b>	
Channel Group Auto	このポート プロファイルに属するすべてのインターフェイスに対するチャンネルグループの作成と定義を指定する設定。
Protocol Mode	<p>関連付けられたポート チャンネルのプロトコル モード。</p> <p>[On] がデフォルトのチャンネル モードです。Link Aggregation Control Protocol (LACP) を実行していないポート チャンネルはすべて、このモードであることが必要です。</p> <p>[Active] は、LACP がイネーブルのときにインターフェイスがアクティブ ネゴシエーション ステートになることを示します。このステートのときは、ポートが LACP パケットを送信して他のポートとのネゴシエーションを開始します。</p> <p>[Passive] は、LACP がイネーブルのときにインターフェイスがパッシブ ネゴシエーション ステートになります。このステートのときは、ポートは受信した LACP パケットに応答しますが、LACP ネゴシエーションを開始することはありません。</p>
MAC Pinning	ポート チャンネルをサポートしていないアップストリーム スイッチの VEM の関連付けを指定する設定。サブグループの最大数はポート チャンネルあたり 32。したがって、最大 32 個のポート メンバを割り当て可能。
SubGroup Mode	サブグループの割り当てに使用される方法。アップストリーム スイッチで CDP がイネーブルになっている場合は [CDP] を選択し、サブグループを手動で設定する場合は [Manual] を選択。
<b>Pinning</b>	
Subgroup ID	このポート プロファイルを継承した vEthernet インターフェイスからのトラフィックの転送に使用されるポート チャンネル サブグループの ID 番号 (0 ~ 31)。
Control VLAN Subgroup ID	このポート プロファイルを継承したコントロール VLAN からのトラフィックの転送に使用されるポート チャンネル サブグループの ID 番号 (0 ~ 31)。
Packet VLAN Subgroup ID	このポート プロファイルを継承したパケット VLAN からのトラフィックの転送に使用されるポート チャンネル サブグループの ID 番号 (0 ~ 31)。

## [Port Profile] : [Features] : [Interfaces] : [Ethernet]

表 10-5 [Port Profile] : [Features] : [Interfaces] : [Ethernet]

フィールド	説明
Admin Status	このポート プロファイルを継承するイーサネット インターフェイスのステータス。
Mode	<p>ポート管理モード。有効な選択肢は次のとおりです。</p> <ul style="list-style-type: none"> <li>• <b>Access</b> : パケットは 1 つの非タグ付き VLAN のみに送信されます。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 VLAN1 です。</li> <li>• <b>Trunk</b> : ネイティブ VLAN のタグなしパケットを送信し、他のすべての VLAN のカプセル化されたタグ付きパケットを送信します。</li> <li>• <b>PVLAN Promiscuous</b> : プライマリ VLAN に属する無差別モード ポートを指定し、レイヤ 3 ゲートウェイと通信します。無差別モード ポートは、セカンダリ VLAN に関連付けられているインターフェイスを含む、PVLAN ドメイン内の任意のインターフェイスと通信できます。</li> <li>• <b>PVLAN Host</b> : PVLAN ペアのセカンダリ VLAN に、コミュニティまたは独立 PVLAN ホスト ポートとして属しているホスト ポートを指定します。</li> </ul>

## [Port Profile] : [Features] : [Switching] : [VLAN]

表 10-6 [Port Profile] : [Features] : [Switching] : [VLAN]

フィールド	説明
<b>PVLAN Host</b>	
Primary VLAN	プライマリ VLAN の ID 番号。
Secondary VLAN	セカンダリ VLAN の ID 番号。
<b>PVLAN Promiscuous</b>	
Primary VLAN	プライマリ VLAN の ID 番号。
Secondary VLAN	セカンダリ VLAN の ID 番号。
<b>Trunk</b>	
Encapsulation	表示のみ。IEEE 802.1Q 仮想 LAN。
Allowed VLAN	<p>このポート プロファイルに属するインターフェイスでデータを送信できる VLAN の ID 番号。有効範囲は 1 ～ 4094。デフォルトは 1。</p> <p>VLAN 3968 ～ 4047 および 4094 は、デバイス内部使用のために割り当てられており、データ トラフィックは伝送しません。</p>
Native VLAN	トランク ポートに使用されるネイティブ VLAN の ID 番号。デフォルトは VLAN 1 です。
<b>Access</b>	
Access VLAN	アクセス ポートに使用される VLAN の ID 番号。デフォルトは VLAN 1 です。

## [Port Profile] : [Features] : [Switching] : [DHCP Snooping]

表 10-7 [Port Profile] : [Features] : [Switching] : [DHCP Snooping]

フィールド	説明
Trust State	このポート プロファイル内のインターフェイスが DHCP スヌーピングに関して信頼されるかどうかを示す設定。有効な選択肢は [Trusted] と [Untrusted]。デフォルトは [Untrusted]。
Rate Limit	1 秒あたりの DHCP パケットの数。

## [Port Profile] : [Features] : [Switching] : [IP Source Guard]

表 10-8 [Port Profile] : [Features] : [Switching] : [IP Source Guard]

フィールド	説明
IP Source Guard	このポート プロファイル内のすべてのインターフェイスに対して IP ソース ガードをイネーブルにする。デフォルトでは、すべてのインターフェイスに対して IP ソース ガードはディセーブル。

## [Port Profile] : [Features] : [Switching] : [ARP Inspection]

表 10-9 [Port Profile] : [Features] : [Switching] : [ARP Inspection]

フィールド	説明
Trust State	このポート プロファイル内のインターフェイスが ARP 検査に関して信頼されるかどうかを示す設定。有効な選択肢は [Trusted] と [Untrusted]。デフォルトは [Untrusted]。
Rate Limit	1 秒あたりの ARP 検査パケットの数。信頼されないインターフェイスのデフォルトは 15 パケット/秒。信頼できるインターフェイスのデフォルトは、1 秒あたりのパケット数は無制限。



## [Port Profile] : [Features] : [Switching] : [Port Security]

表 10-10 [Port Profile] : [Features] : [Switching] : [Port Security]

フィールド	説明
<b>Secure Interface Config</b>	
Port Security	ポート セキュリティをイネーブルにするかディセーブルにするかを示す設定。有効な選択肢は [Enabled] と [Disabled]。デフォルトでは、ポート セキュリティはすべてのインターフェイスでディセーブルです。
Violation Action	ポート セキュリティ違反の検出時に実行されるアクション。有効な選択肢は [Protect] と [Shutdown]。デフォルトのセキュリティ処理では、セキュリティ違反が発生したポートがシャットダウンされます。
Maximum Secure MACs to add	レイヤ 2 インターフェイス 1 つあたりの、学習またはスタティックに設定できる MAC アドレスの最大数。デフォルトでは、各インターフェイスのセキュア MAC アドレスの最大数は 1 です。
Stickiness	インターフェイスのスティッキ MAC アドレス学習をイネーブルにするかディセーブルにするかを示す設定。ダイナミック MAC アドレス学習がインターフェイスのデフォルトです。
<b>Dynamic Config</b>	
Aging Type	ダイナミックに学習された MAC アドレスに適用されるエージング方法のタイプ ([Absolute] または [InActivity])。デフォルトのエージング タイプは絶対エージングです。
Age	ダイナミックに学習された MAC アドレスがドロップされるまでのエージング タイム (分単位)。デフォルトは 0 分 (エージングなし) です。

## [Port Profile] : [Features] : [Security] : [IPv4 ACL]

表 10-11 [Port Profile] : [Features] : [Security] : [IPv4 ACL]

フィールド	説明
Incoming IPv4 Traffic	着信 IP トラフィックに適用される ACL。デフォルトは ACL なしです。
Outgoing IPv4 Traffic	発信 IP トラフィックに適用される ACL。デフォルトは ACL なしです。

## [Port Profile] : [Features] : [Security] : [MAC ACL]

表 10-12 [Port Profile] : [Features] : [Security] : [MAC ACL]

フィールド	説明
Incoming Traffic	IP 以外の着信トラフィックに適用される ACL。デフォルトは ACL なしです。
Outgoing Traffic	IP 以外の発信トラフィックに適用される ACL。デフォルトは ACL なしです。

## その他の関連資料

ポート プロファイルの実装に関する追加情報については、次の項を参照してください。

- 「関連資料」(P.10-32)
- 「標準規格」(P.10-32)

## 関連資料

関連項目	参照先
ポート プロファイル コンフィギュレーション	『Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.0(4)SV1(2)』
インターフェイス コンフィギュレーション	『Cisco Nexus 1000V Interface Configuration Guide, Release 4.0(4)SV1(2)』
Cisco DC-OS のすべてのコマンドのコマンド構文、コマンドモード、コマンド履歴、デフォルト値、使用上の注意、および例	『Cisco Nexus 1000V Command Reference, Release 4.0(4)SV1(2)』

## 標準規格

標準規格	タイトル
この機能でサポートされる新規または改訂された標準規格はありません。また、この機能による既存の標準規格サポートの変更はありません。	—

## ポート プロファイルの機能履歴

ポート プロファイル機能のリリース履歴は次のとおりです。

機能名	リリース	機能情報
ポート プロファイル	5.0	この機能が導入されました。



# APPENDIX A

## 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 DCNM 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 に関する RFC の参考資料

RFC	タイトル
RFC 1981	『Path MTU Discovery for IP version 6』
RFC 2373	『IP Version 6 Addressing Architecture』
RFC 2374	『An Aggregatable Global Unicast Address Format』
RFC 2460	『Internet Protocol, Version 6 (IPv6) Specification』
RFC 2461	『Neighbor Discovery for IP Version 6 (IPv6)』
RFC 2462	『IPv6 Stateless Address Autoconfiguration』
RFC 2463	『Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification』
RFC 2464	『Transmission of IPv6 Packets over Ethernet Networks』
RFC 2467	『Transmission of IPv6 Packets over FDDI Networks』
RFC 2472	『IP Version 6 over PPP』
RFC 2492	『IPv6 over ATM Networks』
RFC 2590	『Transmission of IPv6 Packets over Frame Relay Networks Specification』
RFC 3152	『Delegation of IP6.ARPA』
RFC 3162	『RADIUS and IPv6』
RFC 3513	『Internet Protocol Version 6 (IPv6) Addressing Architecture』
RFC 3596	『DNS Extensions to Support IP version 6』
RFC 4193	『Unique Local IPv6 Unicast Addresses』





## APPENDIX **B**

# Cisco NX-OS インターフェイスの設定制限

Cisco NX-OS がサポートする機能には最大設定制限があります。一部の機能については、最大値に達していない制限値をサポートする設定を検証しました。表 B-1 に、Cisco NX-OS Release 5.x が稼動するスイッチで、シスコが確認した制限値および最大制限値を示します。

表 B-1 Cisco NX-OS Release 5.x 設定の制限値

機能	最大制限
VDC あたりの VLAN	4000
デバイスあたりのポート チャンネル	256
デバイスあたりの vPC	256





## INDEX

---

### 数字

- 10 ギガビット イーサネット インターフェイス [9-4](#)
- 1 GBaseT イーサネット インターフェイス [9-4](#)

---

### A

#### ACL

- IPv4 [10-24](#)
- MAC [10-25](#)

#### ARP 検査

- ポート プロファイルでの設定 [10-20](#)

---

### C

#### CDP

- 設定 [2-24](#)

#### CFSOE

- vPC [6-19](#)
- 定義 [6-7, 6-19](#)

#### CLI

- ポート プロファイル設定 [10-25](#)

---

### D

#### DHCP スヌーピング

- ポート プロファイルでの設定 [10-19](#)

---

### F

#### Fabric Extender [1-5, 9-1](#)

- イーサネット インターフェイス [9-4](#)
- イメージ管理 [9-3](#)
- リンクの再配布 [9-8](#)

---

### H

#### HSRP

- vPC [6-8](#)

---

### I

#### IEEE 802.1Q

- STP [3-7](#)
- アクセス ポート [3-4](#)
- 制約事項 [3-7](#)
- 注意事項 [3-7](#)
- トランク ポート [3-3](#)

#### IEEE 802.3ad

- LACP [5-2](#)

#### IPv4 ACL

- vEthernet インターフェイスでの設定 [8-9](#)
- ポート プロファイルでの設定 [10-24](#)

#### IP アドレス

- ポート チャネル [5-19](#)

#### IP ソース ガード

- ポート プロファイルでの設定 [10-20](#)

#### iSCSI のマルチパス [10-7](#)

---

### L

#### LACP

- MAC アドレス [5-10](#)
- Marker Protocol [5-11](#)
- VDC [5-12](#)
- vPC [6-30, 6-33](#)
- イネーブル化 [5-24](#)
- 管理キー [5-11](#)

グレースフル コンバージェンス [5-27](#)

個別一時停止 [5-29](#)

作成 [5-16](#)

システム ID [5-11, 5-26](#)

システム プライオリティ [5-10, 5-26](#)

制約事項 [5-14](#)

説明 [5-8 ~ 5-12](#)

チャンネル グループ [5-9](#)

チャンネルごとのメンバ数 [5-8](#)

チャンネル モード [5-9 ~ 5-10](#)

注意事項 [5-14](#)

ディセーブル化 [5-9](#)

統計情報 [5-30](#)

トラブルシューティング [5-9](#)

フィールドの説明 [5-31](#)

ポート チャンネル [5-9](#)

ポート プライオリティ [5-26](#)

他の機能との相互運用性 [5-14](#)

ライセンス [5-13](#)

Link Aggregation Control Protocol。「LACP」を参照

## M

### MAC ACL

vEthernet インターフェイスでの設定 [8-9](#)

ポート プロファイルでの設定 [10-25](#)

### MAC アドレス

vPC [6-7](#)

ポート プロファイルでのエージングのタイプと期間の設定 [10-23](#)

ポート プロファイルでの最大数の設定 [10-22](#)

ポート プロファイルでのスティッキ MAC アドレスのイネーブル化 [10-22](#)

ポート プロファイルでのスティッキ MAC アドレスのディセーブル化 [10-22](#)

MAC ピン接続 [10-5](#)

### MDIX

設定 [2-16](#)

定義 [2-2](#)

Medium [2-2](#)

MIB [3-13, 5-38](#)

MTU

設定 [2-20](#)

定義 [2-5](#)

## P

PAgP、サポート対象外 [5-3](#)

[Port Channel] ペイン

アイコン [6-21, 6-33](#)

PVLAN

PVLAN としてのポート プロファイルの設定 [10-18](#)

## S

SFP+ [9-4](#)

インターフェイス アダプタ [9-4](#)

SPAN

vEthernet インターフェイスでの設定 [8-10](#)

STP

EtherChannel [5-2](#)

vPC [6-8, 6-16](#)

トランク [3-7](#)

SVI

「VLAN インターフェイス」を参照

switchport コマンド [2-10](#)

## U

UDLD

vPC [6-8](#)

設定 [2-25](#)

定義 [2-7](#)

メッセージの間隔 [2-7](#)



## V

## VDC

LACP 5-12

## VEM

統計情報 8-12

## vEthernet インターフェイス

IPv4 ACL による設定 8-9

MAC ACL による設定 8-9

SPAN による設定 8-10

VMware DVPort ID の設定 8-4

アクセス インターフェイスとしての設定 8-6

イネーブル化 8-11

概要情報の表示 8-11

関連資料 8-15

グローバル設定の設定 8-3

自動削除 8-3

自動設定 8-3

静的ピン接続による設定 8-5

説明 8-1

説明の設定 8-3

重複しているインターフェイスの接続解除 8-3

ディセーブル化 8-11

トラフィック統計情報の表示 8-12

トランク インターフェイスとしての設定 8-7

標準規格 8-16

プライベート VLAN による設定 8-8

ポート ステータスの表示 8-12

## VLAN

デフォルト 3-5

## VLAN インターフェイス

削除 4-15

作成 4-14

## VLAN ネットワーク インターフェイス

キャリア遅延 2-9

## VLAN、プライベート

「PVLAN」を参照

## VMware DVPort ID

vEthernet インターフェイスでの設定 8-4

## vPC

Auto-Resolve オプション 6-28, 6-33

CFSOE 6-16, 6-19

GLBP 6-18

HSRP 6-8, 6-18

IGMP スヌーピング 6-18

LACP 6-25, 6-30, 6-33

MAC アドレス 6-7

MST および Rapid PVST+ を使用 6-16

PVST シミュレーション 6-16

STP 6-8, 6-16

[Topology] タブ 6-21, 6-33

UDLD 6-8

VLAN 6-13

VLAN インターフェイス 6-9

VLAN ネットワーク インターフェイス 6-8, 6-18

vPC ウィザード 6-23, 6-33

vPC システム プライオリティ

設定 6-30, 6-33

vPC の同期 6-28, 6-33

vPC ピア リンクの同期 6-28, 6-33

vPC ロール 6-7

VRRP 6-18

アイコン 6-21, 6-33

イネーブル化 6-33

キープアライブ メッセージ 6-9, 6-16, 6-33

互換性のある設定 6-28, 6-33

互換パラメータ 6-12

コンフィギュレーション モード 6-5, 6-11

削除 6-33

作成 6-23, 6-33

サスペンド モード 6-12

システム MAC アドレス 6-25, 6-33

システム プライオリティ 6-12, 6-16, 6-25, 6-33

推奨される VRF 6-5

セカンダリ デバイス 6-7, 6-9

セカンダリ ピア デバイスの設定 6-25, 6-33

設定の同期 6-13, 6-33

前提条件 6-3

タイマー [6-9](#)  
 タイムアウト [6-10](#)  
 ダウンストリーム ポート チャンネル [6-33](#)  
 単一モジュール上 [6-3, 6-15](#)  
 ディセーブル化 [6-33](#)  
 統計情報 [6-33](#)  
 トラブルシューティング [6-3, 6-8, 6-9, 6-12, 6-14, 6-21, 6-25, 6-28, 6-29, 6-33](#)  
 ピア キープアライブ メッセージ [6-5, 6-9](#)  
 ピアキープアライブ リンク [6-5, 6-9](#)  
     設定 [6-25, 6-29, 6-33](#)  
 ピア デバイス [6-5, 6-6](#)  
 ピア リンク [6-3, 6-5](#)  
     冗長性 [6-6](#)  
 必要なライセンス [6-20](#)  
 フィールドの説明 [6-33](#)  
 フェールオーバー [6-7, 6-9](#)  
 プライマリ デバイス [6-7, 6-9](#)  
 プライマリ ピア デバイスの設定 [6-25, 6-33](#)  
 変更 [6-23, 6-33](#)  
 ポート チャンネル [6-25, 6-33](#)  
 ポート モード [6-3, 6-6](#)  
 ホールドタイムアウト [6-9](#)  
 要求される設定の一貫性 [6-12, 6-13, 6-33](#)  
 要求される設定の一致 [6-12](#)  
 レイヤ 3 接続 [6-8](#)  
 ロード バランシング [6-7](#)  
 ロール プライオリティ [6-25, 6-30, 6-33](#)  
 ログ レベル [6-1](#)

## vPC-HM

CDP [10-4](#)  
 概要 [10-3](#)  
 手動で作成されたサブグループ [10-4](#)

## vPC ピア リンク

設定の同期 [6-13, 6-33](#)  
 トラフィック パターン [6-7](#)  
 トラブルシューティング [6-3, 6-7](#)

## あ

アクセス ポート  
     VLAN [3-2, 3-4](#)  
     アクセス VLAN [3-4](#)  
     設定 [3-8](#)  
     ホスト ポート [3-3](#)  
 アクセス モード  
     vEthernet インターフェイスでの設定 [8-6](#)

## い

イーサネット インターフェイス [9-4](#)  
 イネーブル化  
     vEthernet インターフェイス [8-11](#)  
 イメージ管理 [9-3](#)  
 インターフェイス  
     CDP  
         設定 [2-24](#)  
     Error Disabled [2-3](#)  
     LACP [5-8](#)  
     MDIX  
         設定 [2-16](#)  
         定義 [2-2](#)  
     MTU  
         設定 [2-20](#)  
         定義 [2-5](#)  
     no shutdown [2-23](#)  
     SFP ステータスおよび診断 [2-12](#)  
     UDLD  
         設定 [2-25](#)  
         定義 [2-7](#)  
     VLAN インターフェイスの削除 [4-15](#)  
     VLAN インターフェイスの設定 [4-14](#)  
     アクセス ポート [3-8](#)  
     仮想イーサネット。「vEthernet インターフェイス」を参照  
     管理 [1-3](#)

## 管理ステータス

設定 [2-23](#)定義 [2-6](#)共有ポート [2-15](#)再起動 [2-23](#)サブインターフェイス、設定 [4-9](#)サブインターフェイスの削除 [4-11](#)指定 [2-12](#)シャットダウン [2-23](#)ジャンボ MTU の設定 [2-21](#)

## スループット遅延

設定 [2-22](#)定義 [2-6](#)セカンダリ IPv4 アドレスの設定 [4-8](#)セカンダリ IPv6 アドレスの設定 [4-9](#)設定 [2-12](#)

## 説明

定義 [2-2](#)専用ポート [2-15](#)

## 速度

設定 [2-17](#)定義 [2-4](#)帯域幅 [4-13](#)設定 [2-22](#)定義 [2-6](#)帯域幅、設定 [4-13](#)帯域幅レートモード [2-15](#)タイプ、指定 [2-12](#)

## デバウンス タイマー

設定 [2-17](#)定義 [2-2](#)

## デュプレックス モード

設定 [2-17](#)定義 [2-4](#)統計情報 [3-11](#)

## トランク ポート

事前プロビジョニング [3-9](#)タグ付きネイティブ VLAN トラフィック [3-10](#)

## ビーコン モード

設定 [2-15](#)定義 [2-2](#)フィールドの説明 [3-11](#)

## フロー制御

設定 [2-18](#)注意事項 [2-10](#)定義 [2-5](#)ポート チャンネル [5-4](#)ポートチャンネルサブインターフェイスの削除 [4-12](#)ポートチャンネルサブインターフェイスの作成 [4-11](#)ポート モード [4-7](#)ルーテッド [4-7](#)ルーテッドとして設定 [4-7](#)ループバック [4-4](#)ループバック、設定 [4-15](#)ループバックの削除 [4-16](#)レイヤ 2 [3-1](#)レイヤ 2 とレイヤ 3 を切り替え [2-10](#)

## レート モード

定義 [2-3](#)

## お

## オーバーサブスクリプション

比率 [9-2](#)

## か

## 概要情報

vEthernet インターフェイスの概要情報の表示 [8-11](#)

仮想イーサネット インターフェイス。「vEthernet インターフェイス」を参照

仮想イーサネット モジュール

統計情報 [8-12](#)

仮想デバイス コンテキスト。「VDC」を参照

仮想ポート チャンネル ホスト モード

「vPC-HM」を参照 [10-3](#)

## 管理ステータス

- 設定 [2-23](#)
- 定義 [2-6](#)
- 管理ポート [1-3](#)
- 関連資料 [xviii, xix](#)

## き

- キャリア遅延 [2-9](#)
- 許容 VLAN
  - トランク ポート [3-5](#)

## け

- 継承
  - ポート プロファイル [10-2](#)

## こ

- コミュニティ ポート [10-18, 10-29](#)

## さ

- 最大伝送ユニット。「MTU」を参照
- サブインターフェイス
  - 物理インターフェイスからの削除 [4-11](#)
  - 物理インターフェイス上の設定 [4-9](#)
  - ポート チャネル上の削除 [4-12](#)
  - ポート チャネル上の作成 [4-11](#)

## し

- システム ポート プロファイル [10-2, 10-10](#)
- ジャンボ MTU、設定 [2-21](#)
- 資料
  - その他の資料 [xviii, xix](#)
  - 表記法 [xviii](#)

## す

- スパニング ツリー プロトコル。「STP」を参照
- スループット遅延
  - 設定 [2-22](#)
  - 定義 [2-6](#)

## せ

- 制限
  - 説明（表） [B-1](#)
- 静的ピン接続 [10-5](#)
  - vEthernet インターフェイスでの設定 [8-5](#)
  - パケット VLAN 上の設定 [10-17](#)
  - コントロール VLAN 上の設定 [10-17](#)
  - ポート プロファイル [10-16](#)
- 制約事項
  - ポート チャネル [5-14](#)
- セキュリティ違反
  - 処理の設定 [10-24](#)
- 設定制限
  - 説明（表） [B-1](#)
- 設定データ [9-3](#)
- 設定変更管理
  - ポート プロファイルを複数デバイスにコピーするために使用 [10-26](#)
- 説明
  - vEthernet インターフェイスでの設定 [8-3](#)
  - 定義 [2-2](#)

## そ

- 速度
  - 設定 [2-17](#)
  - 定義 [2-4](#)

## た

### 帯域幅

設定 [2-22, 4-13](#)

定義 [2-6](#)

### レート モード

定義 [2-3](#)

単方向リンク検出。「UDLD」を参照 [2-7](#)

## ち

着脱可能小型フォームファクタ トランシーバ、「SFP+」を参照

### チャンネル モード

active [5-25](#)

LACP [5-9](#)

passive [5-25](#)

アクティブ モード [5-10](#)

設定 [5-25](#)

デフォルト設定 [5-10](#)

パッシブ モード [5-10](#)

ポート チャンネル [5-9](#)

### 注意事項

ポート チャンネル [5-14](#)

## て

### ディセーブル化

vEthernet インターフェイス [8-11](#)

### デバウンス タイマー

定義 [2-2](#)

### デフォルト設定

VLAN [3-5](#)

ポート チャンネル [5-10](#)

### デュプレックス モード

設定 [2-17](#)

定義 [2-4](#)

## と

### 統計情報

LACP [5-30](#)

VEM [8-12](#)

インターフェイス [3-11](#)

仮想イーサネット モジュール [8-12](#)

ポート チャンネル [5-30](#)

独立ポート [10-18, 10-29](#)

### トラフィック統計情報

vEthernet インターフェイスのトラフィック統計情報の表示 [8-12](#)

### トラブルシューティング

vPC [6-3, 6-9, 6-12, 6-14, 6-21, 6-33](#)

vPC ピア リンク [6-3](#)

### トランク ポート

802.1X [3-8](#)

STP [3-7](#)

VLAN [3-2](#)

許容 VLAN [3-5](#)

制約事項 [3-7](#)

設定 [3-9](#)

タギング VLAN [3-3](#)

タグなしトラフィック [3-5](#)

注意事項 [3-7](#)

トラブルシューティング [3-6](#)

### ネイティブ VLAN

タギング トラフィック [3-5](#)

定義 [3-5](#)

ポート チャンネル [3-7](#)

### トランク モード

vEthernet インターフェイスでの設定 [8-7](#)

### トランシーバ

シスコがサポートするトランシーバを使用 [2-10](#)

### トンネル

VDC [7-2](#)

## ひ

## ビーコン モード

設定 [2-15](#)定義 [2-2](#)非対称ポート チャンネル [10-3](#)

## ピン接続

MAC [10-5](#)静的 [10-5](#)

## ふ

## フィールドの説明

LACP [5-31](#)vPC [6-33](#)インターフェイス [3-11](#)ポート チャンネル [5-31](#)

## プライベート VLAN

「PVLAN」を参照

vEthernet インターフェイスでの設定 [8-8](#)

## フロー制御

注意事項 [2-10](#)定義 [2-5](#)

## ほ

## ポート

複数の VLAN [3-1](#)レイヤ 2 [3-1, 3-2](#)

## ポート管理

ポート プロファイルでの設定 [10-17](#)ポート グループ [10-2](#)

## ポート集約プロトコル。「PAgP」を参照

## ポート ステータス

vEthernet インターフェイスのポート ステータスの表示 [8-12](#)

## ポート セキュリティ

ポート プロファイルでのイネーブル化 [10-21](#)ポート プロファイルでのディセーブル化 [10-21](#)

## ポート チャンネル

CDP [5-21](#)IP アドレス [5-19](#)LACP [5-9](#)passive [5-25](#)STP [5-2](#)アクティブ モード [5-25](#)管理アップ [5-20](#)強制 [5-21](#)互換性要件 [5-5 ~ 5-6, 5-18](#)削除 [5-17](#)作成 [5-16](#)サブインターフェイス [5-2, 5-3, 5-19](#)システムあたり最大 [5-12](#)スイッチド [5-16](#)制約事項 [5-14](#)設定 [5-3](#)説明 [5-2 ~ 5-13, 5-22](#)速度 [5-23](#)速度とデブプレックスの設定 [5-23](#)チャンネル モード [5-5, 5-25](#)注意事項 [5-14](#)統計情報 [5-30](#)動作している [5-2](#)トラブルシューティング [5-24](#)トランク ポート [3-7](#)フィールドの説明 [5-31](#)ポートの削除 [5-20](#)ポート モード [5-25](#)ポートを強制的に参加 [5-5](#)他の機能との相互運用性 [5-14](#)ホスト モード [10-3](#)メンバ ポート、設定 [5-5](#)メンバ ポート設定 [5-5](#)目的 [5-3](#)ライセンス [5-13](#)リンクの削除 [5-22](#)ルーテッド [5-16](#)レイヤ 2 [5-16](#)

- レイヤ 2 ポート チャンネル [5-2](#)
  - レイヤ 2 ポート チャンネル、ポートの追加 [5-18](#)
  - レイヤ 2 ポートの追加 [5-18](#)
  - レイヤ 3 [5-16](#)
  - レイヤ 3 ポート チャンネル [5-2](#)
  - レイヤ 3 ポート チャンネル、ポートの追加 [5-19](#)
  - レイヤ 3 ポートの追加 [5-19](#)
  - ロード バランシング [5-6, 5-24](#)
  - ポート プロファイルでの設定 [10-15](#)
  - ポート プロファイル
    - ARP 検査の設定 [10-20](#)
    - CLI の表示 [10-25](#)
    - DHCP スヌーピングの設定 [10-19](#)
    - IPv4 ACL の設定 [10-24](#)
    - IP ソース ガードの設定 [10-20](#)
    - iSCSI のマルチパス [10-7](#)
    - iSCSI のマルチパス用の設定 [10-13](#)
    - MAC ACL の設定 [10-25](#)
    - MAC アドレス エージングのタイプと期間の設定 [10-23](#)
    - MAC アドレスの最大数の設定 [10-22](#)
    - MAC ピン接続 [10-5](#)
    - VMware ポート グループとしての設定 [10-14](#)
    - VSD での設定 [10-11](#)
    - イネーブル化 [10-9](#)
    - 関連資料 [10-32](#)
    - 機能履歴 [10-32](#)
    - 継承 [10-2, 10-10](#)
    - 削除 [10-9](#)
    - 作成 [10-8](#)
    - システム [10-2](#)
    - システム ポート プロファイルの設定 [10-10](#)
    - 状態 [10-2](#)
    - スティッキ MAC アドレスのイネーブル化 [10-22](#)
    - スティッキ MAC アドレスのディセーブル化 [10-22](#)
    - 静的ピン接続 [10-5](#)
    - 静的ピン接続の設定 [10-16](#)
    - セキュリティ違反時の処理の設定 [10-24](#)
    - 設定変更管理の使用 [10-26](#)
    - 説明 [10-1](#)
    - ディセーブル化 [10-9](#)
    - 特性 [10-3](#)
    - 標準規格 [10-32](#)
    - フィールドの説明 [10-26](#)
    - 複数デバイスへのコピー [10-26](#)
    - プライベート VLAN としての設定 [10-18](#)
    - ポート管理の設定 [10-17](#)
    - ポート グループ [10-2](#)
    - ポート セキュリティのイネーブル化 [10-21](#)
    - ポート セキュリティのディセーブル化 [10-21](#)
    - ポート チャンネルの設定 [10-15](#)
    - レイヤ 3 制御 [10-6](#)
    - レイヤ 3 制御用の設定 [10-11](#)
    - ポート、プライベート VLAN [10-18, 10-29](#)
    - ホスト ポート [10-18, 10-29](#)
- 
- ## ま
- マルチキャスト トラフィック
    - ポート チャンネルを使用したロード バランシング [5-7](#)
- 
- ## む
- 無差別モード ポート [10-18, 10-29](#)
- 
- ## め
- メディア依存インターフェイス クロスオーバー
    - 「MDIX」を参照
- 
- ## ら
- ライセンス
    - LACP [5-13](#)
    - vPC [6-20](#)
    - ポート チャンネル [5-13](#)
    - レイヤ 2 ポート モード [3-6](#)

## り

リンクの再配布 [9-8](#)

## る

ループバック

削除 [4-16](#)

設定 [4-15](#)

## れ

レイヤ 2 インターフェイス

概要 [3-1](#)

レイヤ 2 ポート

アクセス [3-1](#)

注意事項 [3-7](#)

トラブルシューティング [3-3](#)

トランク [3-1](#)

ライセンス [3-6](#)

レイヤ 3 制御

ポート プロファイル [10-6](#)

レート モード

定義 [2-3](#)

## ろ

ロード バランシング

MPLS トラフィック [5-7](#)

vPC [6-7](#)

アルゴリズム [5-7](#)

設定 [5-24](#)

デフォルトのアルゴリズム [5-7](#)

ポート チャネル [5-6 ~ 5-7, 5-24](#)

マルチキャスト トラフィック [5-7](#)

モジュールごと [5-6](#)