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

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

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

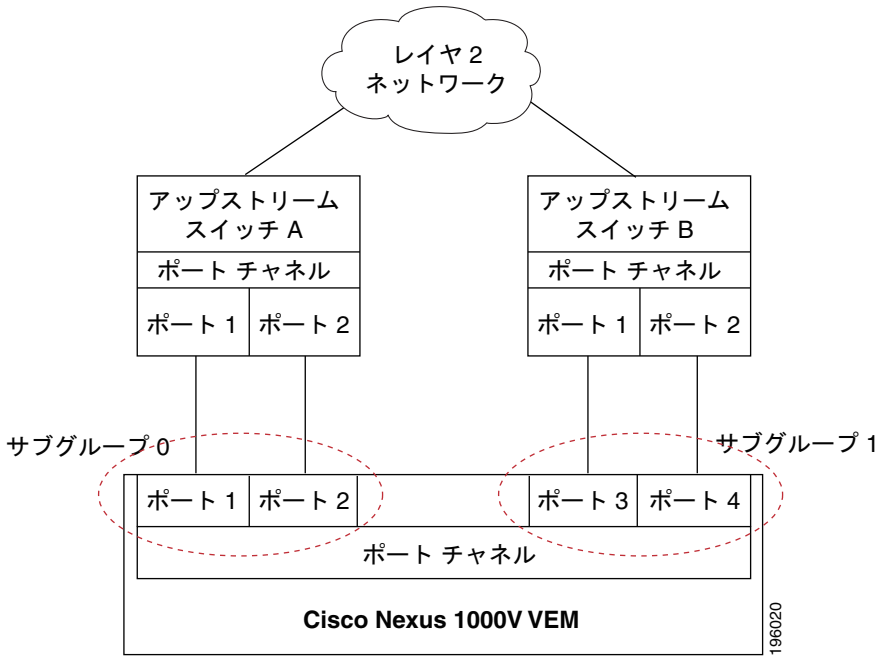
詳細については、使用するプラットフォームのマニュアルを参照してください。

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。

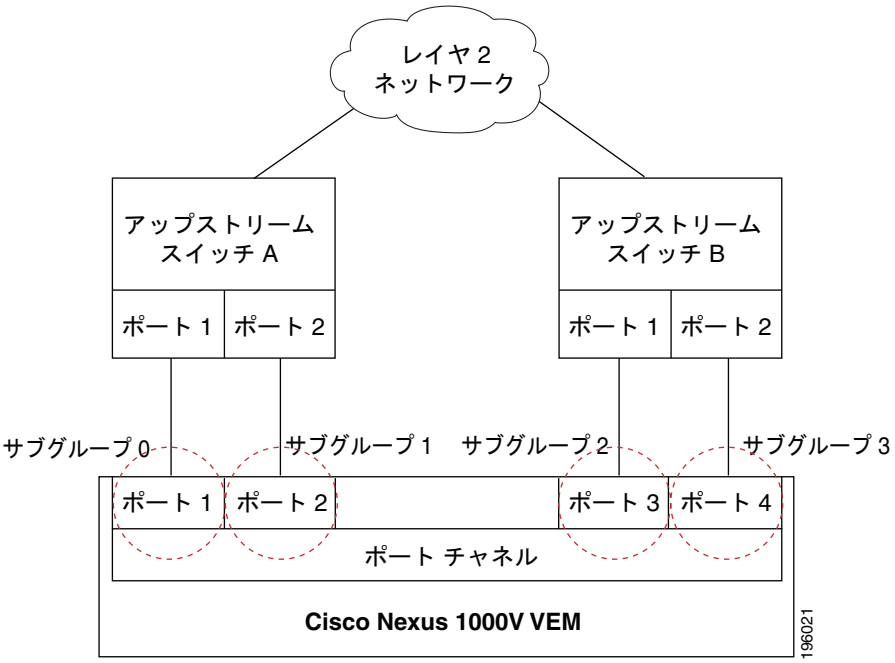
vEthernet インターフェイス、コントロール VLAN、またはパケット VLAN を特定のポート チャネル サブグループに固定する方法については、「コントロールまたはパケット VLAN の静的ピン接続の設定」（P.10-17）を参照してください。

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。

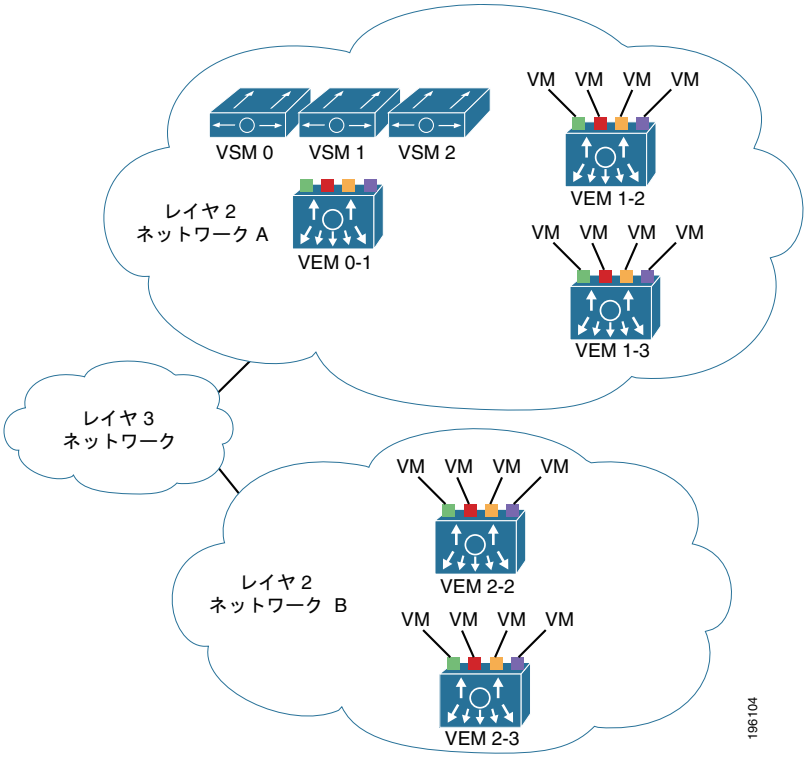
- 「レイヤ 3 制御のためのポート プロファイルの設定」（P.10-11）を参照してポート プロファイルを設定します。

- 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、『*Cisco DCNM Fundamentals Configuration Guide, Release 5.x*』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	Cisco Nexus 1000V シリーズ スイッチ マニュアル

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

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

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。

ステップ 3　メニュー バーで、[Actions] > [New] > [L2 Ethernet Profile] または [VEthernet Profile] を選択します。
新しいプロファイルが [Summary] ペインに表示されます。

ステップ 4　[Summary] ペインで、名前を [Name] フィールドに入力します。

ステップ 5　[Settings] タブで、説明を [Description] フィールドに入力します。

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。

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。
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。
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、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 プロファイルを決定します。
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。

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、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。

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、[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。

（注）　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。

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。

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 プロファイルを決定します。

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 を使用するときに 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

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　次のいずれかを行います。

- 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。
- 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。

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。

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

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。

- 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される特別な 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

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　[Switching] セクションを展開して、[DHCP Snooping] 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 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。

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。

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

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　[Switching] セクションを展開して、[IP Source Guard] を選択します。

ステップ 5　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。

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。

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。

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。スティッキ方式の 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）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　[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 プロファイルを決定します。

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。

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　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。

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。

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 プロファイルを決定します。

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。

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

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　[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。*minutes* 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

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　[Switching] セクションを展開して、[Port Security] を選択します。

ステップ 5　[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。

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。

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

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　[Security] を展開して、[IPv4 ACL] を選択します。

ステップ 5　[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。

ステップ 6　[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。

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。

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。

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。

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。

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

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　メニュー バーで、[Actions] > [Copy to Multiple Devices] を選択します。

[Configuration Delivery Jobs] コンテンツ ペインが表示されます。

ステップ 4　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、『*Cisco DCNM System Management Configuration Guide, Release 5.x*』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

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
System	
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。
VM Setting	
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の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
Channel Setting	
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ネル グループの作成と定義を指定する設定。
Protocol Mode	関連付けられたポート チャネルのプロトコル モード。 [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。 [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。
MAC Pinning	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。
Pinning	
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	ポート管理モード。有効な選択肢は次のとおりです。 • 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。 • 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。

[Port Profile] : [Features] : [Switching] : [VLAN]

表 10-6　[Port Profile] : [Features] : [Switching] : [VLAN]

フィールド	説明
PVLAN Host	
Primary VLAN	プライマリ VLAN の ID 番号。
Secondary VLAN	セカンダリ VLAN の ID 番号。
PVLAN Promiscuous	
Primary VLAN	プライマリ VLAN の ID 番号。
Secondary VLAN	セカンダリ VLAN の ID 番号。
Trunk	
Encapsulation	*表示のみ*。IEEE 802.1Q 仮想 LAN。
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。
Access	
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 秒当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
Secure Interface Config	
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。
Dynamic Config	
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。