



CHAPTER 9

N ポート バーチャライゼーションの設定

N Port Virtualization (NPV; N ポート バーチャライゼーション) を使用すると、SAN におけるファイバチャネル ドメイン ID 数を削減できます。NPV モードで動作するスイッチはファブリックに参加せず、NPV コア スイッチ リンクとエンドデバイスの間でトラフィックを通過させます。このため、これらのエッジスイッチのドメイン ID が不要になります。

NPV は、次の Cisco MDS 9000 スイッチおよび Cisco Nexus 5000 シリーズ だけでサポートされています。

- Cisco MDS 9124 マルチレイヤ ファブリック スイッチ
- Cisco MDS 9134 ファブリック スイッチ
- HP c-Class BladeSystem 用の Cisco ファブリック スイッチ
- IBM BladeCenter 用の Cisco ファブリック スイッチ
- Cisco Nexus 5000 シリーズ スイッチ



(注)

これらのスイッチでは、NPV モードの場合にかぎって NPV を使用できます。スイッチ モードの場合は NPV を使用できません。

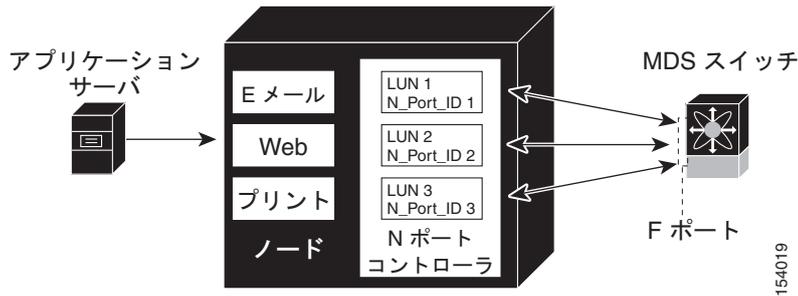
この章の内容は、次のとおりです。

- 「[N ポート ID バーチャライゼーションの概要](#)」(P.9-2)
- 「[N ポート バーチャライゼーションの概要](#)」(P.9-2)
- 「[NPV の注意事項および要件](#)」(P.9-7)
- 「[NPV の設定](#)」(P.9-9)
- 「[NPV Setup ウィザードの使用法](#)」(P.9-14)

N ポート ID バーチャライゼーションの概要

N Port Identifier Virtualization (NPIV; N ポート ID バーチャライゼーション) によって、単一の N ポートに複数の FC ID を割り当てることができます。この機能を使用すると、N ポート上の複数アプリケーションに異なる ID を使用できます。また、アプリケーション レベルでアクセス コントロール、ゾーン分割、およびポート セキュリティを実装できます。図 9-1 に、NPIV の使用例を示します。

図 9-1 NPIV の例



NPIV 対応アプリケーションで複数の N ポート ID を使用できるようにするには、MDS スイッチ上のすべての VSAN で NPIV をグローバルにイネーブルにする必要があります。



すべての N ポート ID は同じ VSAN で割り当てられます。

N ポート ID バーチャライゼーションのイネーブル化

NPIV 対応アプリケーションで複数の N ポート ID を使用できるようにするには、MDS スイッチ上のすべての VSAN で NPIV をグローバルにイネーブルにする必要があります。



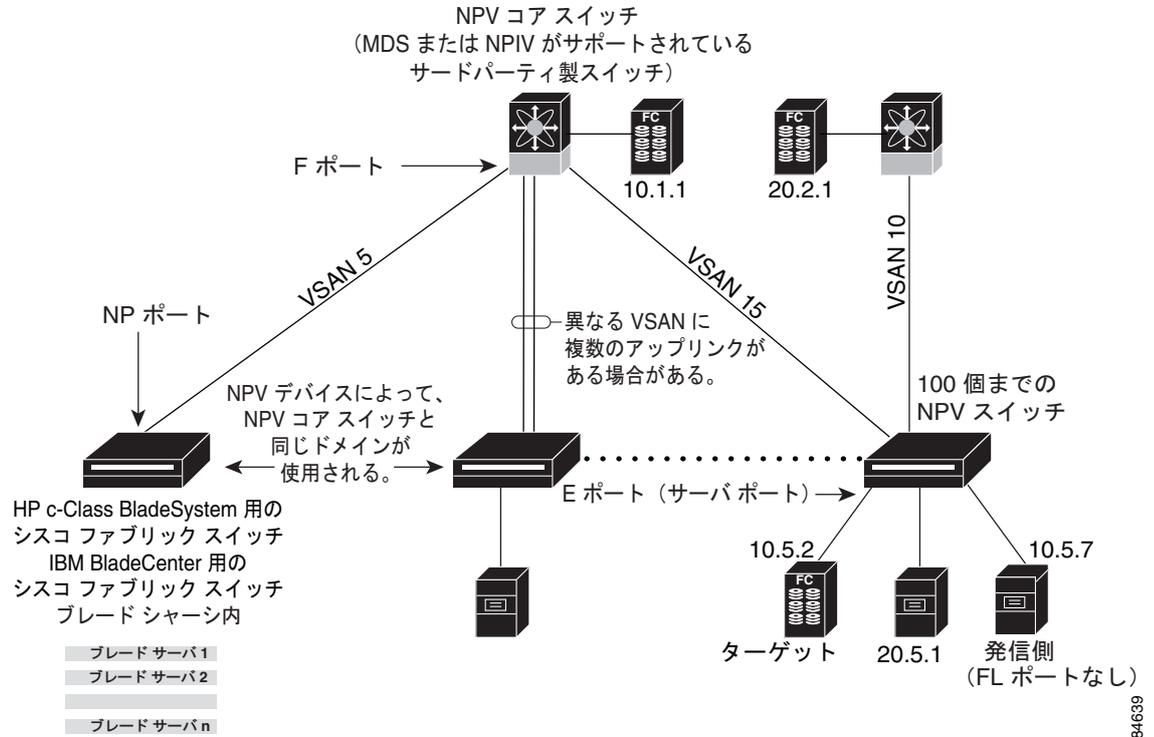
すべての N ポート ID は同じ VSAN で割り当てられます。

N ポート バーチャライゼーションの概要

一般的にファイバチャネル ネットワークは、コアエッジ モデルを使用して、多くのファブリック スイッチをエッジデバイスに接続して展開します。このようなモデルが費用有効性が高い理由は、ディレクタクラス スイッチのポート別コストが、ファイバチャネルのコストよりもはるかに高いためです。しかし、ファブリックのポート数が増えると、展開するスイッチ数も増えて、ドメイン ID の数が大幅に増加することがあります (サポートされている最大数は 239)。ファイバチャネル ネットワークでブレード シャーシをさらに展開すると、この課題は難しくなります。

NPV では、ファブリック スイッチまたはブレード スイッチをコア ファイバチャネル スイッチのホストおよびファブリック スイッチかブレード スイッチのサーバのファイバチャネル スイッチのようすることで、多くのポートの展開に必要なドメイン ID の数の増加に対処します。NPV では、複数のローカル接続 N ポートを 1 つ以上の外部 NP リンクに集約し、NPV コア スイッチのドメイン ID を複数の NPV スイッチ間で共有します。NPV では、NPV コア スイッチの同一ポートに複数のデバイスを接続することもできるので、コアでより多くのポートが必要になることがなくなります。

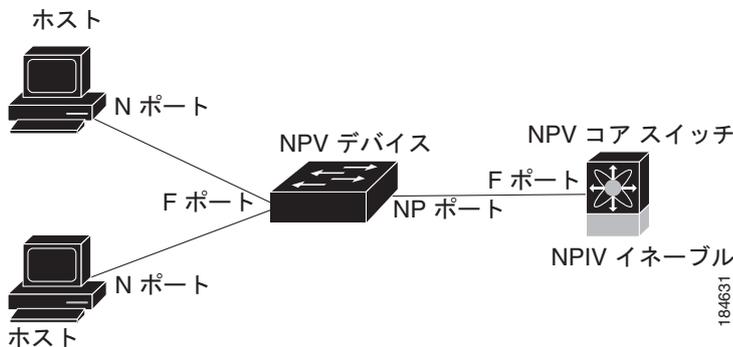
図 9-2 Cisco NPV ファブリック設定



NPV は N Port Identifier Virtualization (NPIV; Nポート ID バーチャライゼーション) に似ていますが、同じ機能を提供するわけではありません。NPIV では複数の FC ID を単一の N ポートに割り当てることができ、N ポートの複数のアプリケーションが別々の ID を使用できます。NPIV では、アクセスコントロール、ゾーン分割、ポートセキュリティをアプリケーションレベルで実装することもできます。NPV では NPIV が使用され、コアスイッチから複数の FCID を NP ポートで割り当てるができます。

図 9-3 に、NPV 設定の詳細 (インターフェイスレベル) を示します。

図 9-3 インターフェイスレベルの Cisco NPV 設定



NPVモード

ユーザが NPV をイネーブルにしてスイッチの再起動に成功すると、スイッチは NPV モードになります。NPV モードはスイッチ全体に適用されます。NPV モードのスイッチに接続するすべてのエンドデバイスは、Nポートとしてログインし、この機能を使用する必要があります（ループ接続デバイスはサポートされていません）。（NPV モードの）エッジスイッチから NPV コアスイッチへのすべてのリンクは、（Eポートではなく）NPポートとして確立されます。このポートは、通常のスイッチ間リンクに使用されます。NPIV は、NPV コアスイッチへのリンクを共有する複数のエンドデバイスにログインするために、NPV モードのスイッチで使用されます。



(注)

2つのエンドデバイス間におけるやり取りでは NPV デバイスからコアへの同じアップリンクが使用されるので、NPV モードでは順序どおりのデータ配信が必要ありません。NPV デバイスを超えるトラフィックの場合、コアスイッチは必要に応じて、または設定されている場合、あるいはその両方で順序どおりの配信を実行します。

NPポート

NPポート（プロキシNポート）は、NPV モードになっているデバイスのポートであり、Fポートで NPV コアスイッチに接続されます。NPポートはNポートのように動作しますが、Nポートの動作を提供することに加えて、複数の物理Nポートのプロキシとして機能します。



(注)

Cisco NX-OS リリース 4.2(1) 以降のリリースを実行する NPV モードの Cisco Nexus 5000 シリーズスイッチは、NPポートでのトランキング Fポートモードをサポートします。NPポートでは、VSAN トランキング、Fポート、またはその両方をイネーブルにできます。

NPリンク

NPリンクは、基本的に特定エンドデバイスへの NPIV アップリンクです。NPリンクは、NPV コアスイッチへのアップリンクがアップしたときに確立します。アップリンクがダウンすると、NPリンクは終了します。アップリンクが確立すると、NPV スイッチは内部 FLOGI を NPV コアスイッチに対して実行し、FLOGI が正常に実行された場合は、NPV コアスイッチのネームサーバに自分自身を登録します。この NPリンクにおけるエンドデバイスからのその後の FLOGI は FDISC に変換されます。詳細については、「内部 FLOGI パラメータ」(P.9-5) を参照してください。

サーバリンクは、NPリンク間で均等に分散されます。サーバリンクの背後にあるすべてのエンドデバイスは、1つの NPリンクだけにマッピングされます。

fWWN ベースのゾーン分割が NPV デバイスでサポートされますが、次のような理由のために推奨できません。

- ゾーン分割は NPV デバイスで実施されない (NPV コア スイッチで実施される)。
- NPV デバイスの背後にある複数のデバイスは、コアで同じ F ポートによってログインする (同じ fWWN が使用され、別々のゾーンに分割できない)。
- 同一デバイスが、コア スイッチで (使用する NPV リンクによって) 別の fWWN を使用してログインすることがあり、別々の fWWN を使用したゾーン分割が必要となることがある。

デフォルト ポート番号

NPV 対応スイッチのポート番号はスイッチ モデルによって異なります。NPV 対応スイッチのポート番号の詳細については、『Cisco NX-OS Family Licensing Guide』を参照してください。

IP を介した NPV CFS 配信

NPV デバイスは、トランスポート メディアとして IP だけを使用します。CFS では、マルチキャスト フォワーディングを使用して CFS 配信を行います。NPV デバイスは ISL 接続を行わず、FC ドメインもありません。IP を介した CFS を使用するには、NPV スイッチに物理的に接続するネットワーク全体で、イーサネット IP スイッチ上のマルチキャスト フォワーディングがイネーブルである必要があります。NPV 対応スイッチで、IP を介した CFS 配信にスタティック IP ピアを手動で設定することもできます。詳細については、『Cisco MDS 9000 Family NX-OS Interoperability Configuration Guide』を参照してください。

NPV トラフィック管理

ここでは、ロード バランシングの次の側面について説明します。

- 「自動」(P.9-6)
- 「トラフィック マップ」(P.9-7)
- 「中断」(P.9-7)

自動

Cisco MDS SAN-OS リリース 3.3(1a) よりも前では、NPV で外部リンクの自動選択がサポートされていました。サーバ インターフェイスが起動すると、使用可能なリンクから負荷が最も小さい外部インターフェイスが選択されます。外部リンクを使用するサーバ インターフェイスでは、手動選択は行われません。また、さらに外部インターフェイスが起動した場合、既存の負荷は新たに起動した外部インターフェイスに自動的に分散されません。この最後に起動したインターフェイスを使用するのは、このインターフェイスよりあとに起動するサーバ インターフェイスだけです。

トラフィック マップ

Cisco MDS SAN-OS リリース 3.3(1a) および NX-OS リリース 4.1(1a) では、NPV でトラフィック管理がサポートされており、サーバがコア スイッチへの接続に使用する外部インターフェイスを選択して設定できます。



(注)

NPV トラフィック管理を設定すると、サーバでは設定された外部インターフェイスだけが使用されます。使用可能な外部インターフェイスが他にあって、そのインターフェイスは使用されません。

NPV トラフィック管理機能には、次のような利点があります。

- NPV に接続したサーバ専用の外部インターフェイスが提供され、トラフィック エンジニアリングが容易になる。
- サーバ インターフェイスごとに外部インターフェイスを選択するので、最短パスが使用される。
- リンクの中断後、または NPV やコア スイッチの再起動後に同じトラフィックが提供され、永続的 FC ID 機能が使用される。
- 外部インターフェイス間で負荷を均等に分散できるので、負荷が分散される。

中断

中断を伴うロード バランスは、インターフェイスの自動選択および外部インターフェイスに設定されたトラフィック マップとは無関係に動作します。この機能によってサーバ インターフェイスは強制的に再初期化され、この機能がイネーブルにされたとき、および新しい外部インターフェイスが起動するたびにロード バランスが行われます。サーバ インターフェイスを何度も無用にフラップしないように、この機能をイネーブルにして必要なロード バランスが実現されたら、この機能を毎回ディセーブルにしてください。

中断を伴うロード バランスをイネーブルにしない場合は、サーバ インターフェイスを手動でフラップし、負荷の一部を新規の外部インターフェイスに移動する必要があります。

複数の VSAN のサポート

VSAN に基づいて別々の NPV セッションにデバイスをグループ化すると、複数の VSAN を NPV 対応スイッチでサポートできます。アップリンクが伝送している VSAN に基づいて、正しいアップリンクを選択する必要があります。

NPV の注意事項および要件

次は、NPV 展開時の注意事項および要件です。

- NPV コア スイッチでは NPIV がサポートされている必要があります。
- 100 までの NPV デバイスを設定できます。
- 中断のないアップグレードがサポートされます。『Cisco MDS 9000 Family NX-OS Fundamentals Configuration Guide』を参照してください。
- ポート トラッキングがサポートされます。『Cisco MDS 9000 Family NX-OS Security Configuration Guide』を参照してください。

- NPV コア スイッチで使用可能なすべてのメンバー タイプを使用し、NPV デバイスに接続されているエンド デバイスにゾーン分割を設定できます。fWWN、sWWN、ドメイン、ポートベースのうちいずれかのゾーン分割を使用する場合は、NPV コア スイッチの fWWN、sWWN、またはドメイン/ポートを使用する必要があります。
- NPV コア スイッチでは、NPV でログインするデバイス用にポート セキュリティがサポートされます。
- NPV ではロード バランシング アルゴリズムが使用され、VSAN のエンド デバイスが最初のログイン時にいずれかの NPV コア スイッチ リンク (同一 VSAN) に自動的に割り当てられます。同一 VSAN に複数の NPV コア スイッチ リンクがある場合は、エンド デバイスに特定の NPV コア スイッチ リンクを割り当てることはできません。
- サーバおよびターゲットを両方とも NPV デバイスに接続できます。
- リモート SPAN はサポートされません。
- ローカル スイッチングはサポートされません。すべてのトラフィックは NPV コア スイッチを使用してスイッチングされます。
- NPV デバイスは複数の NPV コア スイッチに接続できます。つまり、さまざまな NPV ポートをさまざまな NPV コア スイッチに接続できます。
- NPV では NPIV 対応モジュール サーバ (ネスト NPIV) がサポートされます。
- F ポート、NP ポート、SD ポートだけが NPV モードでサポートされます。
- NPV を使用する SAN 上で起動されたサーバの場合、NPV リンクのフェールオーバーが発生すると、サーバは一時的にブート LUN にアクセスできなくなります。
- サードパーティ製コア スイッチとの相互運用性に課題があるため、NPV スイッチでは xNP ポート上の BB_SCN 設定が認識されません。

NPV トラフィック管理の注意事項

NPV トラフィック管理を展開する場合は、次の注意事項に従ってください。

- NPV トラフィック管理は、NPV デバイスによる自動トラフィック エンジニアリングがネットワーク要件を満たさない場合にだけ使用します。
- すべてのサーバに対してトラフィック マップを設定しないでください。未設定のサーバに対しては、NPV によって自動トラフィック エンジニアリングが使用されます。
- コア スイッチで永続的 FC ID を設定します。トラフィック エンジニアリングによって、関連付けられたサーバインターフェイスが同じコア スイッチにつながる外部インターフェイスに転送されます。サーバには、ログインのたびに同じ FC ID が割り当てられます。91x4 スイッチをコア スイッチとして使用している場合、この注意事項は該当しません。
- 外部インターフェイス セットに設定されたサーバ インターフェイスは、設定されているインターフェイスを使用できない場合に、使用できる外部インターフェイスが他にあったとしてもそのインターフェイスを使用できません。
- 中断を伴うロード バランシングは設定しないでください。この機能を設定すると、デバイスが外部インターフェイス間を移動する必要があります。外部インターフェイス間でデバイスを移動するには、NPV が F ポートでコア スイッチに再ログインする必要があります。このときにトラフィックが中断します。
- コア スイッチにリンクした外部インターフェイス セットにサーバを設定して、サーバセットをコア スイッチにリンクします。

NPV の設定

NPV をイネーブルにすると、システム設定は消去され、システムは NPV モードがイネーブルの状態でのリブートします。



(注)

NPV をイネーブルにする前に、現在の設定をブートフラッシュまたは TFTP サーバのいずれかに保存することを推奨します（あとで設定を使用する必要がある場合）。NPV 以外の設定または NPV の設定を保存するには、次のコマンドを使用します。

```
switch# copy running bootflash:filename
```

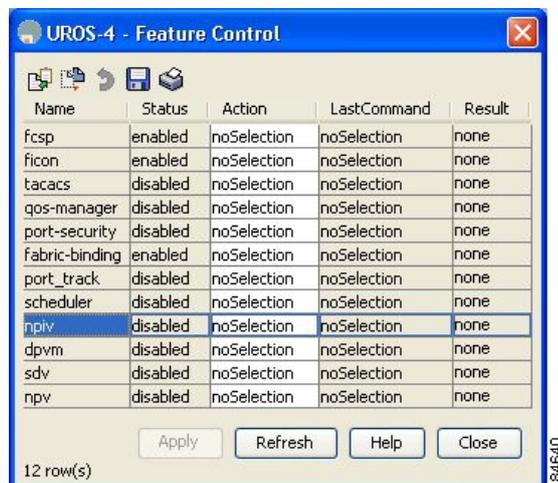
次のコマンドを使用すると、後で設定を再適用できます。

```
switch# copy bootflash:filename running-config
```

Fabric Manager および Device Manager を使用して NPV を設定する手順は、次のとおりです。

- ステップ 1** コア NPV スイッチで NPIV をイネーブルにするには、コア NPV スイッチから Device Manager を起動します。[Admin] ドロップダウンメニューから [Feature Control] を選択します。NPIV 機能に [enable] を選択します（[図 9-5](#) を参照）。

図 9-5 NPIV および NPV のイネーブル化



- ステップ 2** [Apply] をクリックします。
- ステップ 3** NPIV コア スイッチ ポートを F ポートとして設定するには、[Interface] ドロップダウンメニューから [FC All] を選択します。
- ステップ 4** [Mode Admin] カラムで [F] ポート モードを選択し、[Apply] をクリックします。
- ステップ 5** NPV デバイスで NPV をイネーブルにするには、NPV デバイスから Device Manager を起動します。[Admin] ドロップダウンメニューから [Feature Control] を選択します。NPV 機能に [enable] を選択し、[Apply] をクリックします。
- ステップ 6** NPV デバイスで外部インターフェイスを設定するには、[Interface] ドロップダウンメニューから [FC All] を選択します。
- ステップ 7** [Mode Admin] カラムで [NP] ポート モードを選択し、[Apply] をクリックします。

- ステップ 8** NPV デバイスでサーバ インターフェイスを設定するには、[Interface] ドロップダウン メニューから [FC All] を選択します。
- ステップ 9** [Mode Admin] カラムで [F] ポート モードを選択し、[Apply] をクリックします。
- ステップ 10** デフォルトの [Admin] ステータスはダウンです。ポート モードの設定後、[Admin] ステータスにアップを選択し、リンクをアップにする必要があります。
-

NPV トラフィック管理の設定

NPV トラフィック管理機能は、NPV の設定後にイネーブルになります。NPV トラフィック管理の設定では、サーバに対して外部インターフェイスのリストを設定し、中断を伴うロード バランシングをイネーブルまたはディセーブルにします。

サーバ インターフェイスごとの外部インターフェイス リストの設定

外部インターフェイスのリストは、サーバ インターフェイスがダウンしているとき、または指定した外部インターフェイス リストにすでに使用中の外部インターフェイスが含まれている場合に、サーバ インターフェイスにリンクされます。

Fabric Manager を使用して、サーバ インターフェイスごとに外部インターフェイスのリストを設定する手順は、次のとおりです。

-
- ステップ 1** [Physical Attributes] > [Switches] > [N_Port Virtualizer (NPV)] を選択します (図 9-6 を参照)。

図 9-6 NPV の [Traffic Map] タブ

The screenshot shows the Cisco Fabric Manager 3.4(1) interface. The title bar indicates the session is for 'Fabric Manager 3.4(1) [admin@localhost (session 2)] /SAN/Fabric_sw2'. The main window is divided into several sections:

- Logical Domains:** A tree view showing the hierarchy: SAN > Fabric_sw2 > All VSANs, VSAN0001, VSAN0002 (down), VSAN4000, and Groups.
- Physical Attributes:** A tree view showing various attributes: Switches, Hardware, Licenses, CFS, Clock, Supervisor Statistics, Copy Configuration, Interfaces, FC Services, Events, Security, NPIV, N_Port Virtualizer (NPV) (highlighted), Flex Attach, NP Link Statistics, ISLs, and End Devices.
- Traffic Map Tab:** A table listing switch configurations. The table has three columns: Switch, Server Interface, and External Interface List.
- Network Diagram:** A visual representation of the switch network topology, showing three switches (sw1, sw2, sw3) connected by dashed lines. Each switch is associated with a MAC address.

Switch	Server Interface	External Interface List
sw4	fc1/2	fc1/2
sw3	fc1/10	fc1/19-fc1/21
sw4	fc1/5	fc1/16
sw3	fc1/33	fc1/32,fc1/34
sw4	fc1/8	fc1/2,fc1/6,fc1/9-fc1/10,fc1/14,fc1/17,fc1/21
sw4	fc1/10	fc1/4-fc1/5,fc1/12,fc1/15,fc1/19-fc1/21
sw4	fc1/13	fc1/16,fc1/18
sw4	fc1/15	fc1/20-fc1/21
sw4	fc1/19	fc1/8-fc1/9,fc1/12
sw4	fc1/20	fc1/9-fc1/10,fc1/13,fc1/17

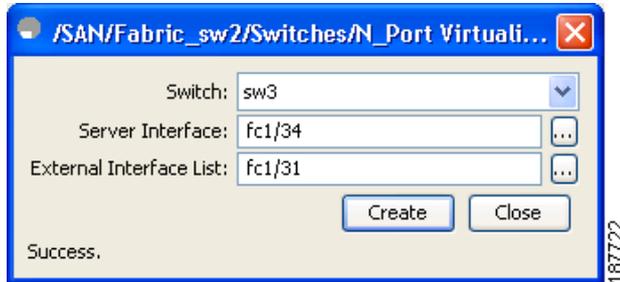
10 rows, queried 2 switches

ステップ 2 [Traffic Map] タブをクリックします。

ステップ 3 ツールバーで  アイコンをクリックするか、または右クリックしてから [Create Row...] を選択します。

ステップ 4 ドロップダウンリストで [Switch] を選択します (図 9-7 を参照)。

図 9-7 [Map Entry] ダイアログボックス



ステップ 5 ポート番号を入力するか、または [...] ボタン (ブレードサーバスイッチでは使用不可) をクリックしてポート選択ダイアログボックスから [Server Interface] および [External Interfaces] を選択します (図 9-8 を参照)。

図 9-8 ポート選択ダイアログボックス



(注) 選択できるサーバインターフェイスは1つだけですが、複数の外部インターフェイスを選択したサーバインターフェイスにマップできます。すでに選択されたポートはディセーブルとなり、選択できません。

マップエントリを削除するには、[Traffic Map] タブの行を選択してから、ツールバーで  アイコンをクリックするか、または右クリックして [Delete Row] を選択します。

中断を伴うロードバランシング用グローバルポリシーのイネーブル化

中断を伴うロードバランシングを使用すると、すべての外部インターフェイスの負荷を確認し、中断を伴ってその負荷を分散できます。このロードバランシングでは、高負荷の外部インターフェイスを使用するサーバが、低負荷で動作している外部インターフェイスに移されます。

Fabric Manager を使用して中断を伴うロードバランシングをイネーブルにする手順は、次のとおりです。

- ステップ 1** [Physical Attributes] > [Switches] > [N_Port Virtualizer (NPV)] を選択します (図 9-9 を参照)。
- ステップ 2** [Load Balance] タブをクリックします。
- ステップ 3** [Enable] チェックボックスをオンにして、中断を伴うロードバランシングをスイッチでイネーブルにします。

すべてのスイッチで中断を伴うロードバランシングをイネーブルにするには、[Enable All] チェックボックスをオンにします (図 9-9 を参照)。

図 9-9 NPV の [Load Balance] タブ

The screenshot shows the Cisco Fabric Manager interface for Fabric_sw2. The 'Load Balance' tab is selected, and the 'Enable All' checkbox is checked. The table below shows the configuration for switches sw4 and sw3, both of which are enabled.

Switch	Enable
sw4	<input checked="" type="checkbox"/>
sw3	<input checked="" type="checkbox"/>

The network diagram shows four switches (sw1, sw2, sw3, sw4) connected in a mesh topology. The status bar at the bottom indicates '2 rows, queried 2 switches'.

サーバインターフェイスに関する外部インターフェイスの使用状況の表示

サーバインターフェイスに関する外部インターフェイスの使用状況を表示するには、次の手順を実行します。

- ステップ 1** [Physical Attributes] > [Switches] > [N_Port Virtualizer (NPV)] を選択します (図 9-10 を参照)。
ステップ 2 [External Interface Usage] タブをクリックします。

図 9-10 外部インターフェイスの使用状況

Switch	Server Interface	External Interface In Use
sw113	fc1/13	fc1/2
sw113	fc1/24	fc1/1

NPV Setup ウィザードの使用方法



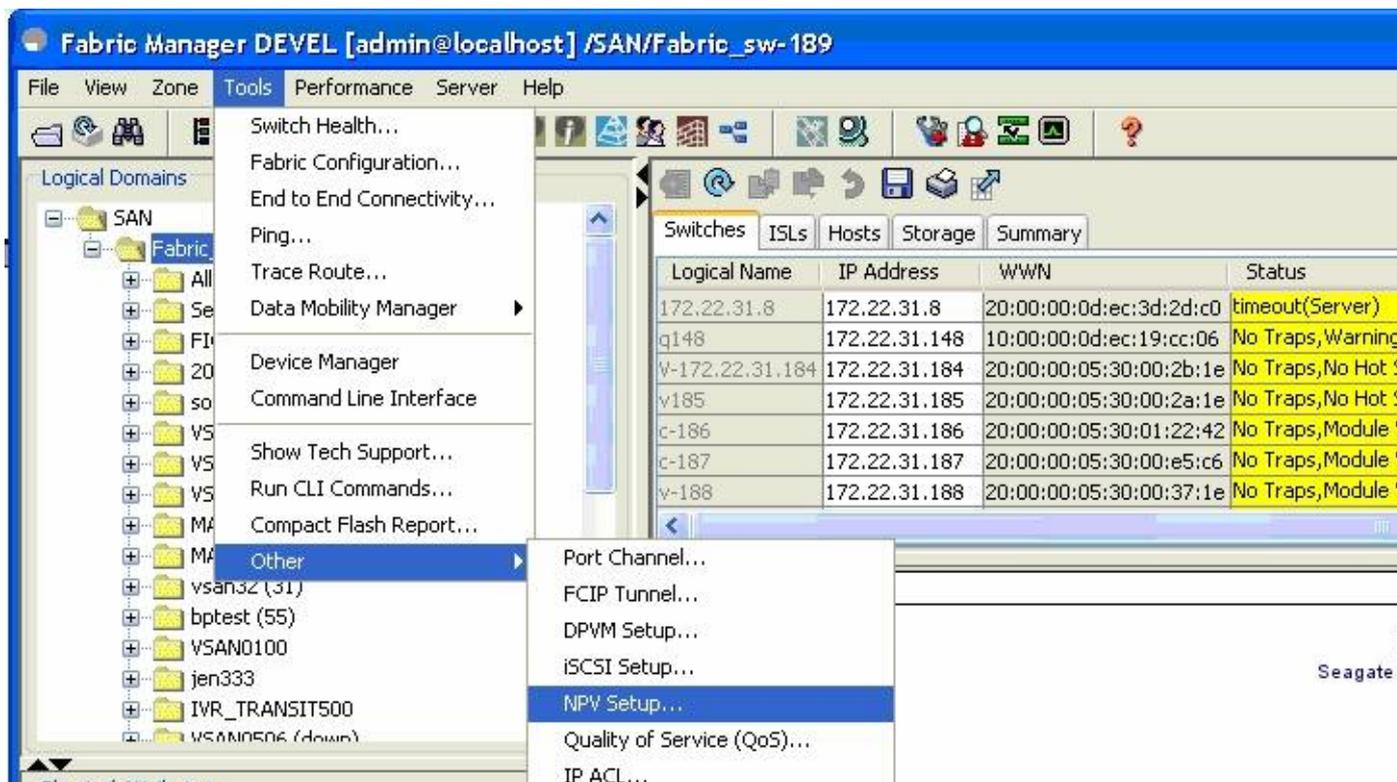
(注)

Cisco Nexus 5000 シリーズ スイッチの場合は、[Physical Attributes] ペインで [Switches] > [N_Port Virtualization (NPV)] を選択し、最初にスイッチの NPV モードをイネーブルにしたあと、NPV ウィザードを使用してスイッチの他の NPV 関連の設定を行う必要があります。

ウィザードを使用して NPV を設定する手順は、次のとおりです。

- ステップ 1** [Tools] > [NPV] > [NPV Setup...] を選択して、Fabric Manager から NPV Setup ウィザードを起動します (図 9-11 を参照)。

図 9-11 NPV Setup ウィザードの起動



Fabric Manager は、ウィザードが起動する前に、クライアントの SAN から NPV 対応スイッチおよび NPIV 対応スイッチが存在するかどうかをチェックします。NPV 対応スイッチは、SAN-OS リリース 3.2.2 以降がインストールされた Cisco MDS 9124、9134、Cisco Nexus 5000 シリーズ スイッチ、HP Blade Server、または IBM Blade Server です。NPIV 対応スイッチは、SAN-OS リリース 3.0.1 以降がインストールされた Cisco スイッチです。NPV 対応スイッチが存在しない場合は、Fabric Manager にエラーメッセージが表示されます (図 9-12 を参照)。

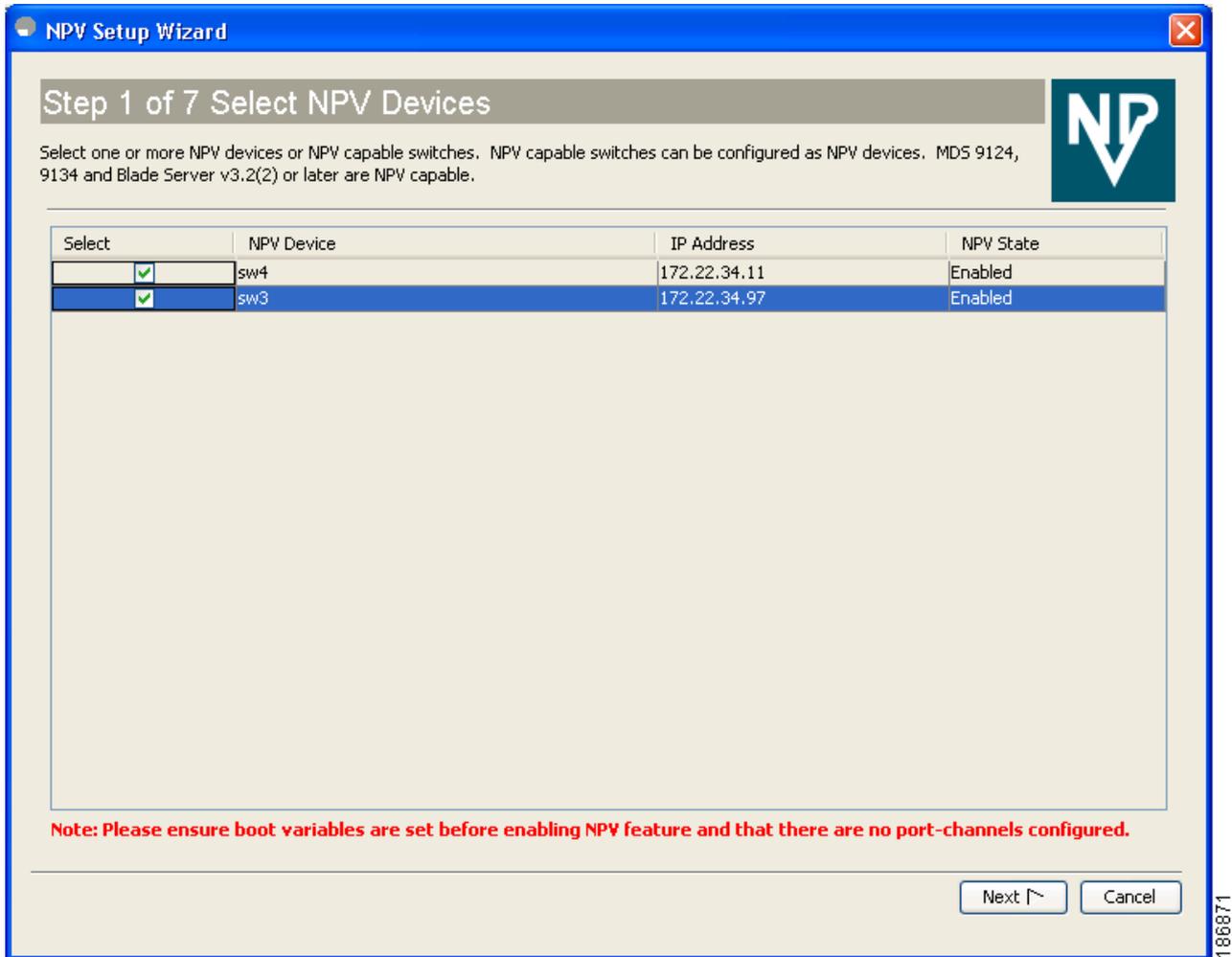
図 9-12 起動時のエラー



NPV の設定

ステップ 2 NPV デバイスを選択します (図 9-13 を参照)。

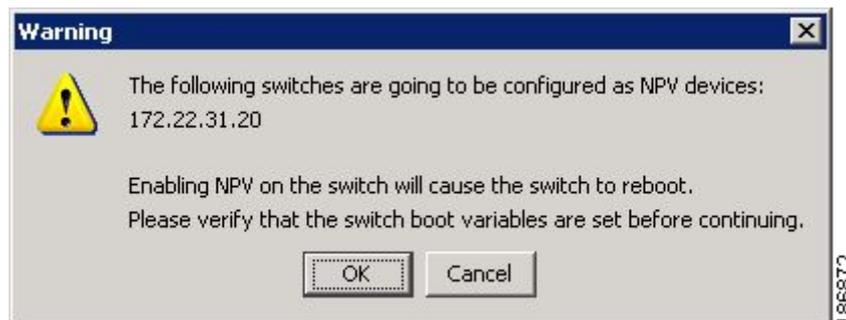
図 9-13 NPV デバイスの選択



テーブルには、使用可能な NPV 対応スイッチおよび NPV がまだイネーブルでないスイッチがすべて表示されます。チェックボックスをオンにして、必要な NPV デバイスを選択してください。NPV がイネーブルでないデバイスについては、このウィザードの最後のステップでそのデバイスの NPV をイネーブルにします。

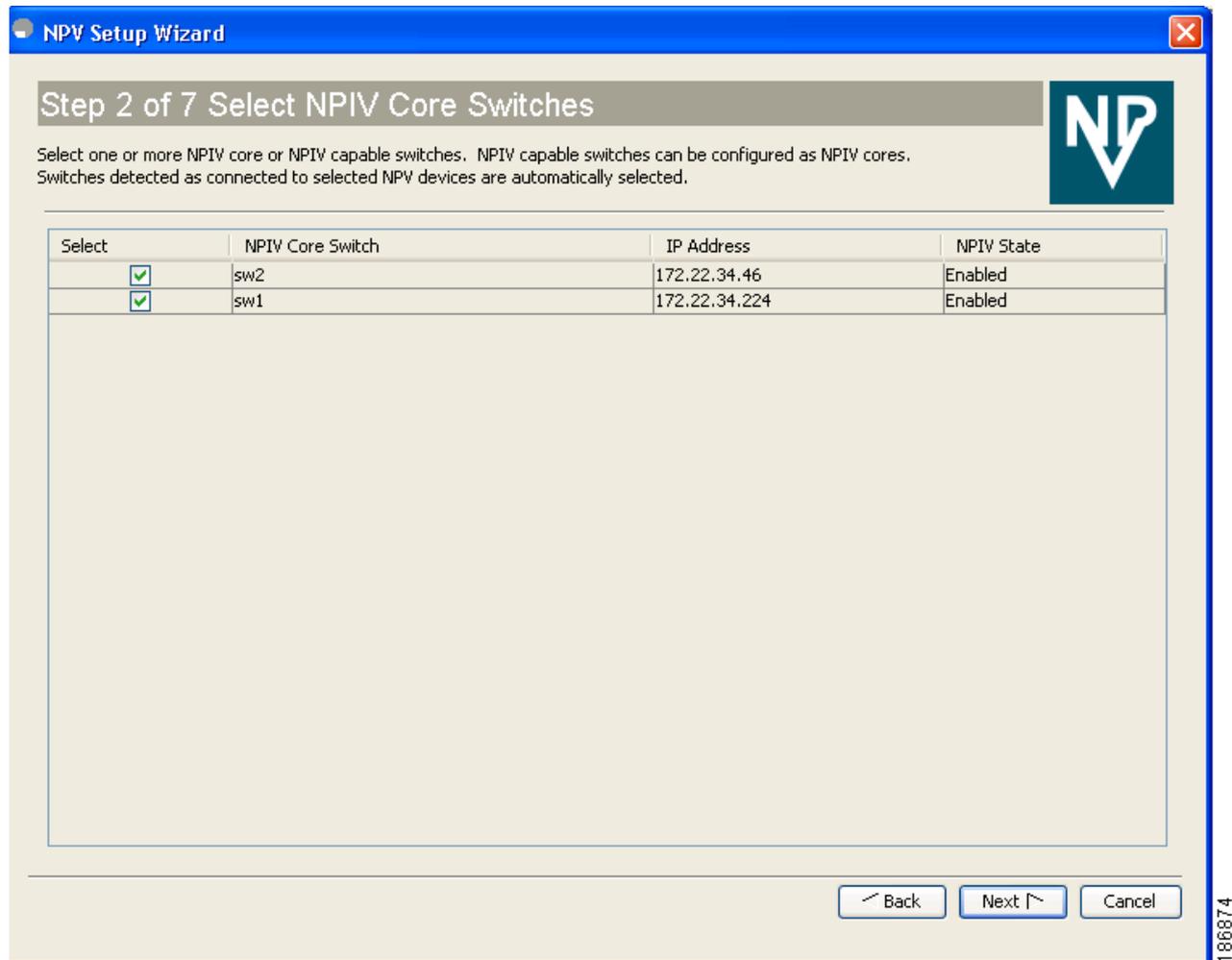
NPV がディセーブルなスイッチを選択して [Next] をクリックすると、警告メッセージが表示されて NPV がイネーブルな NPV デバイスの IP アドレス リストが表示されます。スイッチで NPV をイネーブルにすると、そのスイッチは再起動します。このウィザードを使用してスイッチで NPV をイネーブルにする場合は、スイッチのブート変数が設定されている必要があります (図 9-14 を参照)。

図 9-14 NPV 対応スイッチで NPV 機能をイネーブルにした場合の警告



ステップ 3 NPIV コア スイッチを選択します (図 9-15 を参照)。

図 9-15 NPIV コア スイッチの選択

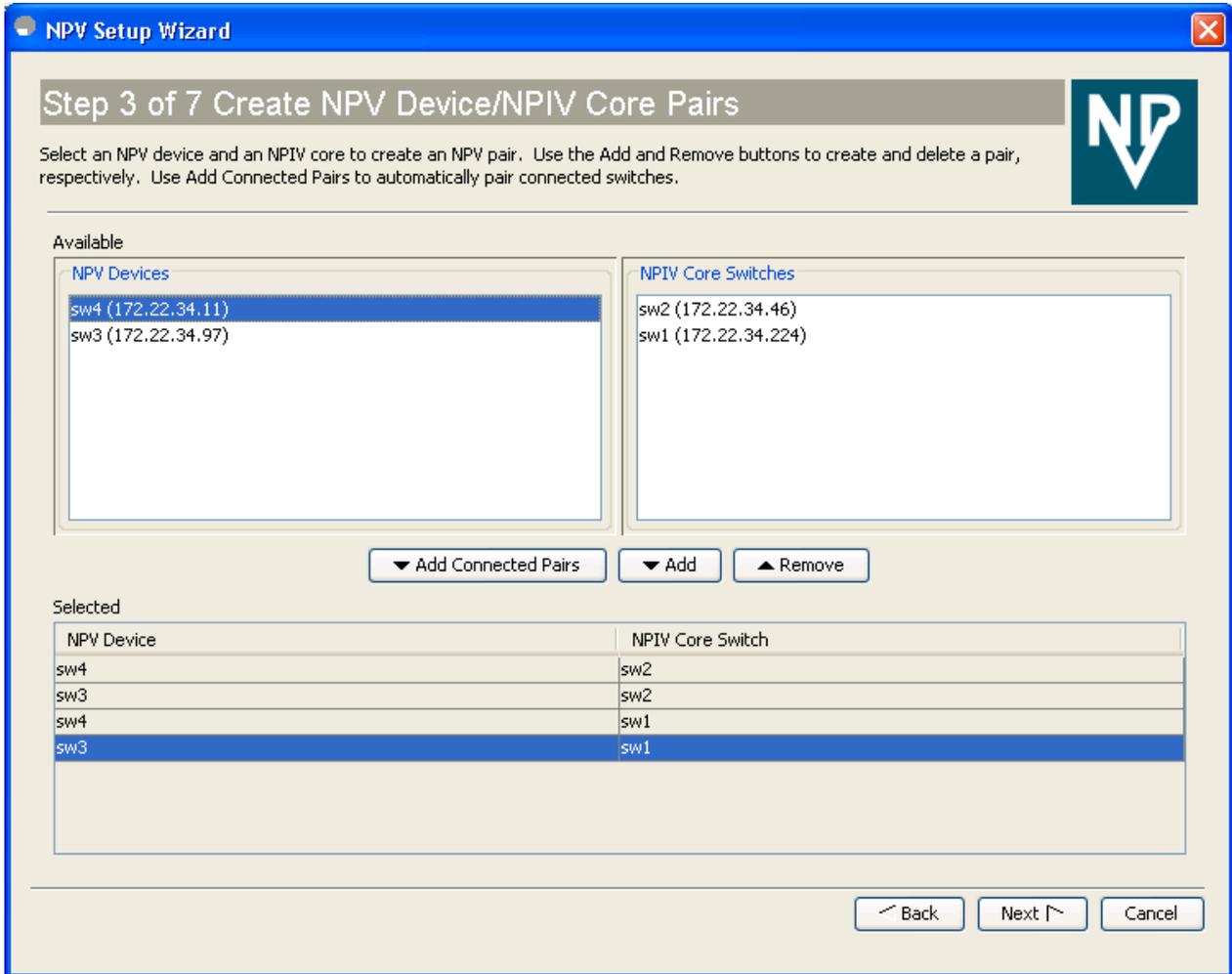


チェックボックスをオンにして、必要な NPIV コア スイッチを選択します。テーブルには、使用可能な NPIV コア スイッチおよび NPIV 機能がまだイネーブルでないコア スイッチがすべて表示されます。NPIV 対応ではない NPIV コア スイッチについては、このウィザードの最後のステップでそのコア スイッチの NPIV をイネーブルにします。

NPV の設定

ステップ 4 必要に応じて、新しい NPV デバイスと NPIV コア スイッチのペアを作成します (図 9-16 を参照)。

図 9-16 NPV デバイスと NPIV コア スイッチ ペアの作成



これまでのステップで選択した内容に基づいて、ウィザードには使用可能な NPV デバイスと NPIV コア スイッチが別々のリストにすべて表示されます。それぞれのリストから 1 つずつ選択し、[Add] ボタンまたは [Remove] ボタンをクリックすると、新しい NPV デバイスと NPIV コア スイッチの組み合わせまたはペアを作成できます。

NPV ウィザードは、前のステップで選択した NPV デバイスに接続済みの NPIV コア スイッチが存在するかどうかをチェックします。[Add Connected Pairs] ボタンをクリックすると、相互接続した既存ペアのリストがすべて [Selected] テーブルに追加されます。

その後、既存のペアおよび目的のペアが [Selected] テーブルに入力されます。各 NPIV コア スイッチは、複数の NPV デバイスとペアにすることができます。

ステップ 6 が終わると、まだ接続されていない新規ペアを物理的に接続するためのプロンプトが表示されます。

ペアになっていないスイッチでは、NPV ウィザードによって NPV モードおよび NPIV モードがイネーブルになります。ただし、このようなペアになっていないスイッチは分割され、ファブリック上に存在しなくなる可能性があります。

3/6 ステップで [Next] ボタンをクリックすると、すべての接続済みペアが選択されているかどうか判定されます。警告メッセージが表示されて (図 9-19 を参照)、このメッセージに未選択の接続済みペアがすべて表示され、これらのペアが NPV セットアップ後に分割されることを示す警告が表示されます。



(注)

- NPV ウィザードは、チャンネル グループ内にあるポートおよび ISL によって接続されていないポートは検出しません。ポート チャンネル グループ内のポートはコア スイッチの F ポートには設定されません。ポート チャンネルのグループ化は NPV デバイスには適用できません (図 9-17 を参照)。
- セットアップ中にポート チャンネル グループの特定のポートを F ポートとして選択する必要がある場合は、ポート チャンネル グループを削除します。詳細については、『Cisco MDS 9000 Family NX-OS Security Configuration Guide』を参照してください。

図 9-17 検出されたポート チャンネル グループ

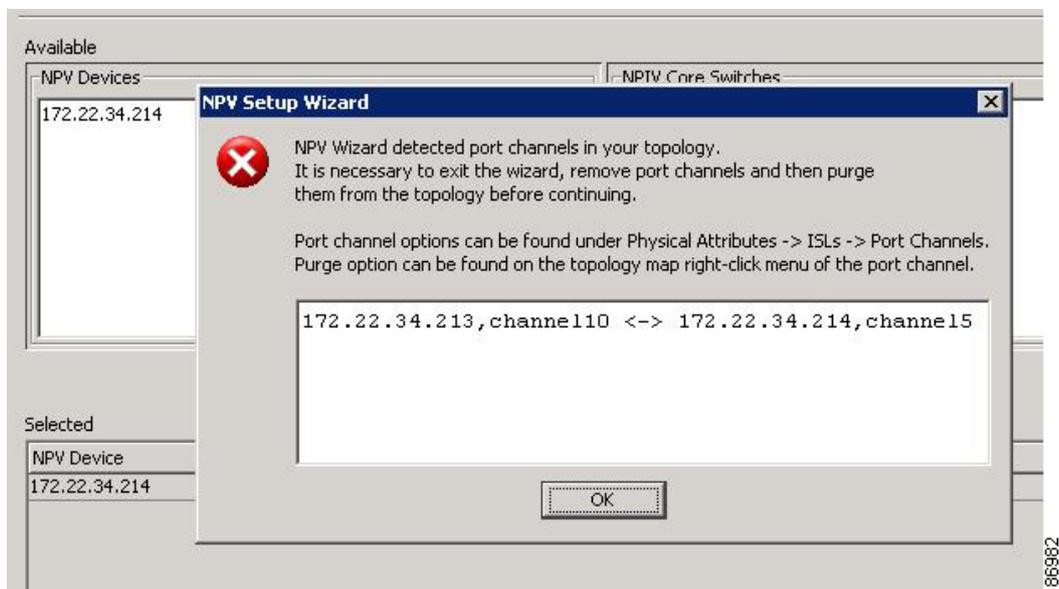


図 9-18 警告 (NPV Setup ウィザード)

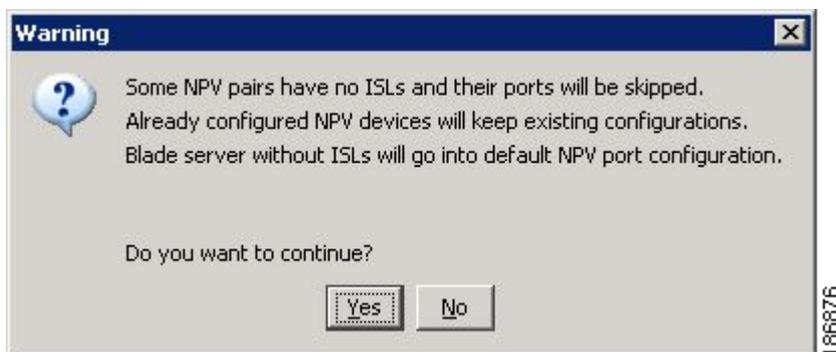
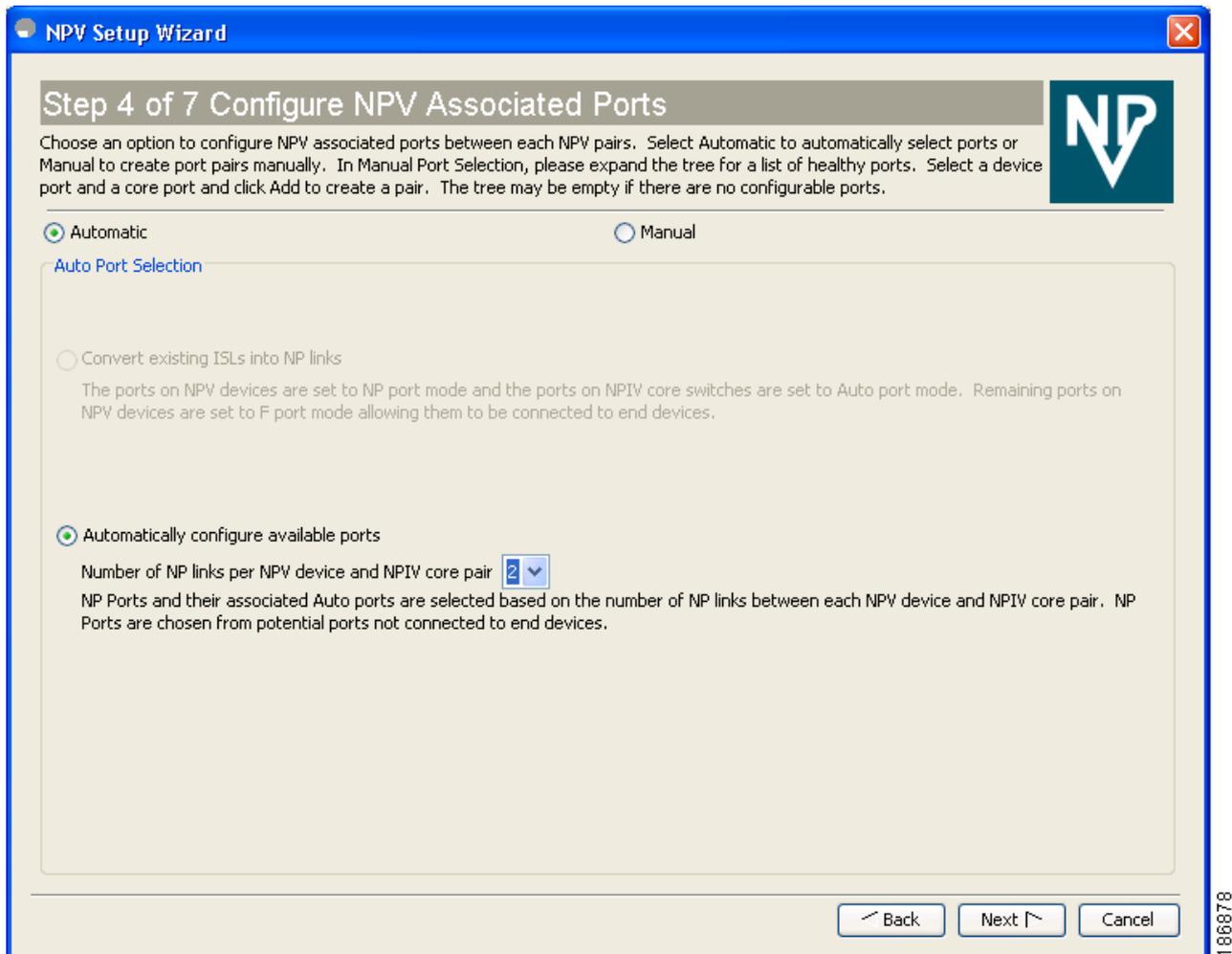


図 9-19 警告 (NPV Setup ウィザードの続き)



ステップ 5 NPV 関連のポートは、自動方式または手動方式のいずれかで設定できます (図 9-20 を参照)。

図 9-20 自動方式による NPV 関連ポートの設定



自動ポート選択には2つのオプションがあります。

- 1つめのオプションを選択すると、既存の ISL を変換して NPV リンクとして実行できます。ISL を優先する場合は、[Convert existing ISLs] オプションを選択します。

ウィザードによって、ウィザードの起動時に使用可能な、選択されたスイッチ間の ISL（アップまたはダウン）が検出されます。

- 2つめのオプションを選択すると、NPV ウィザードで空きポートを自動的に設定し、NPV に使用できます。2つめのオプションでは、NPV デバイスとコアスイッチのペアごとに、最大で6つまでの追加 NPV リンクを選択できます。

NPV スイッチでの自動ポート選択時には、ポートは「Operational status」が Auto で「Status Cause」が none(2)、offline(8)、または sfp not present(29) および「Operational Status」が TE または E のライセンス済み FC ポートとして定義されます。

NPV スイッチのポートは次のように選択されます。

ISL は2つめの方式で考慮されます。選択アルゴリズムによって空きポートの選択が拡大され、4ポートごとに最初のポートが選択されます（1番め、5番め、9番めなど）。4ポートごとに最初のポートをすべて処理しても、十分なポートが選択されていない場合は（推奨されたポートが空いていないため）、次に4つのポートごとに2つめのポートに移ります（2番め、6番め、10番めなど）。スイッチが異なるとポート設定も異なります。

NPIV スイッチ上のポートは、次の方法で選択されます。

NPIV スイッチでの自動ポート選択時には、空きポートがライセンス済み FC ポートおよび「Operational status」が Auto、「Status Cause」が none(2)、offline(8)、または sfp not present(29) のポートとして定義されます。ポートが他の動作ステート（F、NP、E、TE など）にあることが検出されると、そのポートは使用中と見なされます。ただし、このウィザードのセッションで NPV モードをイネーブルにする NPV デバイス スイッチに接続された ISL に含まれる E ポートおよび TE ポートは例外で、これらのポートは空いていると見なされます。ただし、これらの ISL ポートの扱いには他の空きポートの扱いと違いがないため、必ずしも自動ポート選択アルゴリズムによって選択されたポートである必要はありません。このような使用中の ISL ポートを変換する場合は、まず [Convert existing ISLs] オプションを選択してから2回目のウィザードを実行し、[Automatic] ポート選択（オプション2）を選択してさらにリンクを追加してください。

使用可能なポートからポートを設定するように選択すると、まだ NP リンク設定に参加していないポートがウィザードによって検索されます。すべてのポートが NP ポート設定に参加することも可能です。この場合は、警告メッセージが表示されます（図 9-21 を参照）。



(注) NPV 関連ポート設定の手動方式および自動方式では、正常でないポートまたは adminDown ステートのポートはポート選択時に考慮されません。

図 9-21 警告（ポート数の不足）

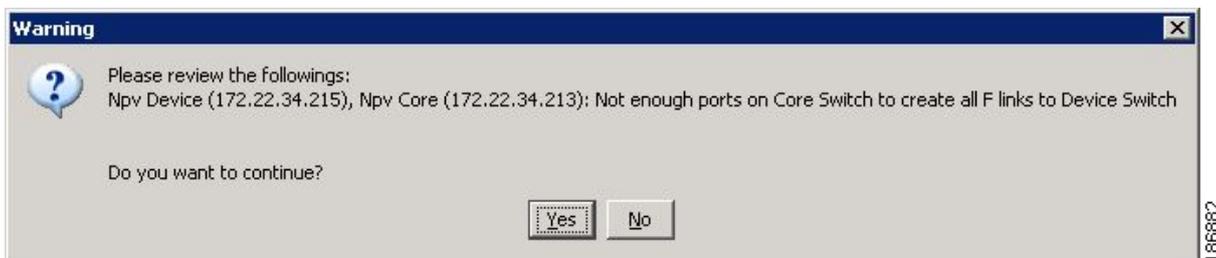
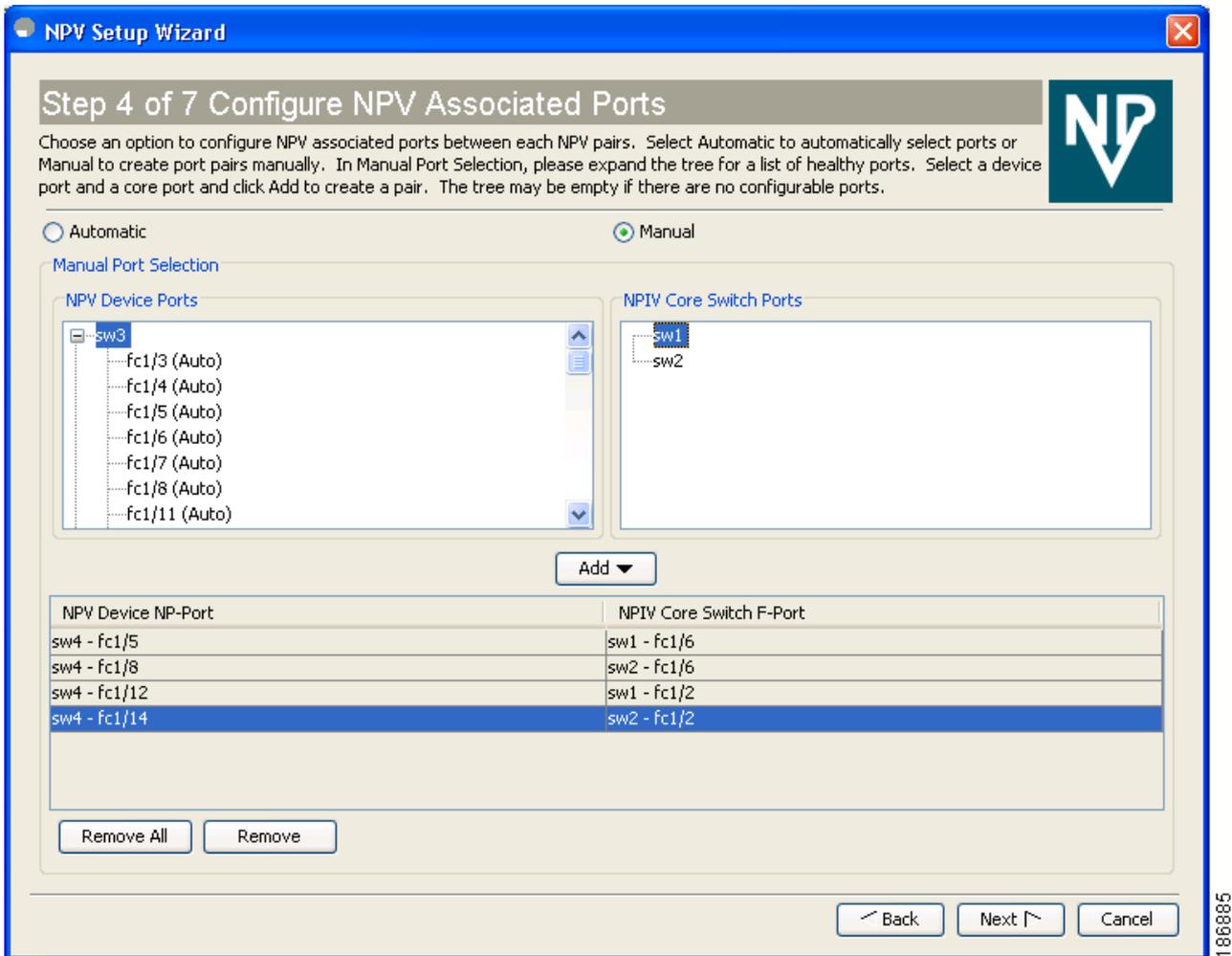


図 9-22 手動方式による NPV 関連ポートの設定



ポートのペアを手動で作成するには、[Manual] 方式を選択します（図 9-22 を参照）。サテライト スイッチをクリックし、表示された各 NPV スイッチの下に展開された NP デバイス ポートを選択します。次に、NPIV コア スイッチで必要な F ポートを選択し、[Add] をクリックしてポートのペアを作成します。

NPV と NPIV のリストから手動で選択するときは、ポートが「Operational status」が Auto、「Status Cause」が none(2)、offline(8)、または sfp not present(29) で「Operational Status」が TE または E のライセンス済み FC ポートとして定義されます。



(注) 動作ステートが Auto で、障害の発生したポートは表示されません。動作ステートが E で、障害の発生したポートは表示され、NPV 設定に使用できます。

ウィザードは、ユーザの選択に基づいて NPV デバイス側の NP ポートに設定されたポートおよびコア スイッチ側の F ポートを判断し、NPV 接続を行います。



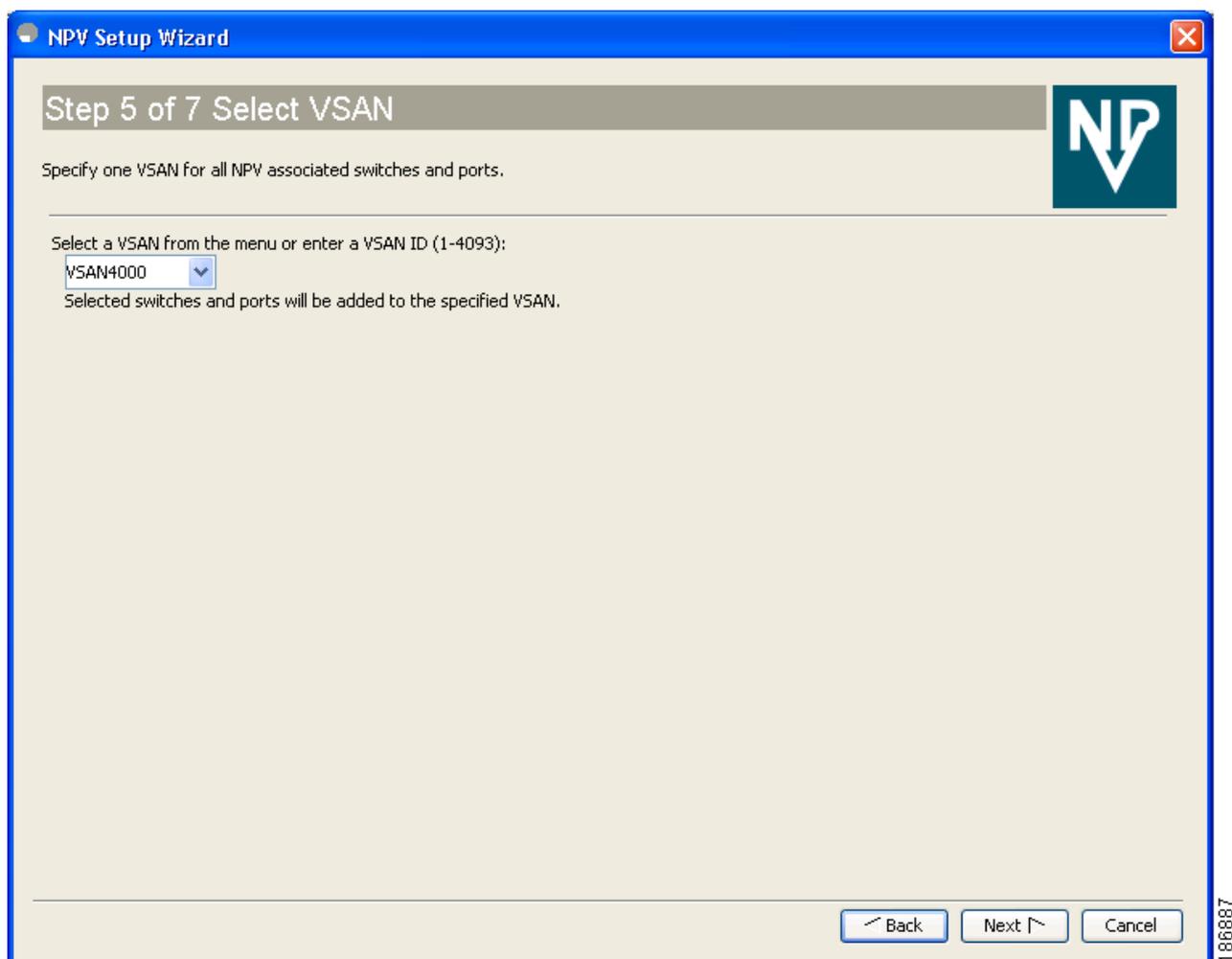
(注) NPV ウィザードによって障害ステートまたはダウンステートのポートが除外されるため、ステップ4の [Manual] 選択で NPV スイッチ ツリーを展開したときに、ポートが表示されないことがあります。NPV スイッチのツリーでは正常なポートだけが表示されます。ポート設定を確認してください。

図 9-23 ポート ペア接続時の警告メッセージ



ステップ 6 VSAN を選択します (図 9-24 を参照)。

図 9-24 VSAN の選択

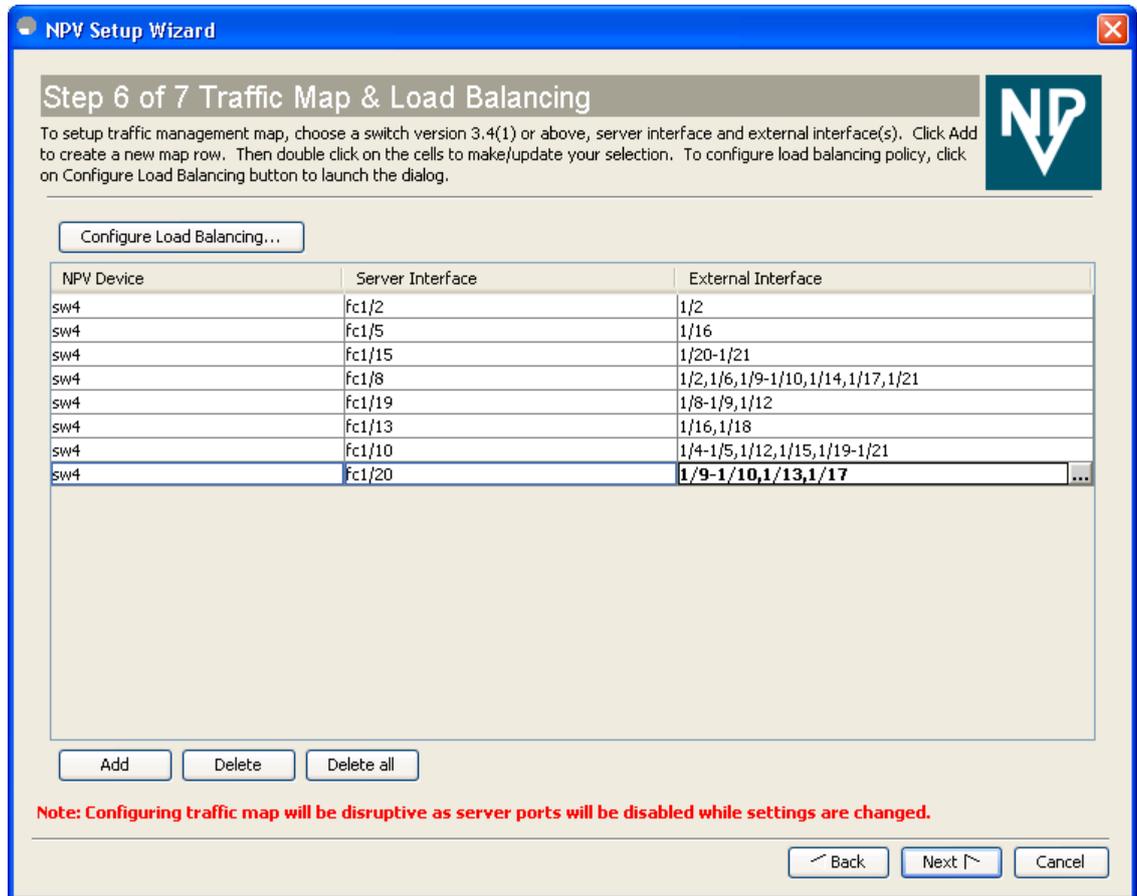


ドロップダウン リストから VSAN を選択するか、または VSAN ID を入力して VSAN を指定します。選択されたすべての NPV デバイスと NPIV コア スイッチが、指定された VSAN に追加されます。選択された NPV デバイスのポートおよび NPIV コア スイッチの関連ポートが、VSAN に追加されます。

VSAN 設定は最後のステップで適用されます。

- ステップ 7** サーバ インターフェイスを外部インターフェイスにマッピングし、中断を伴うロード バランシングを設定します (図 9-25 を参照)。

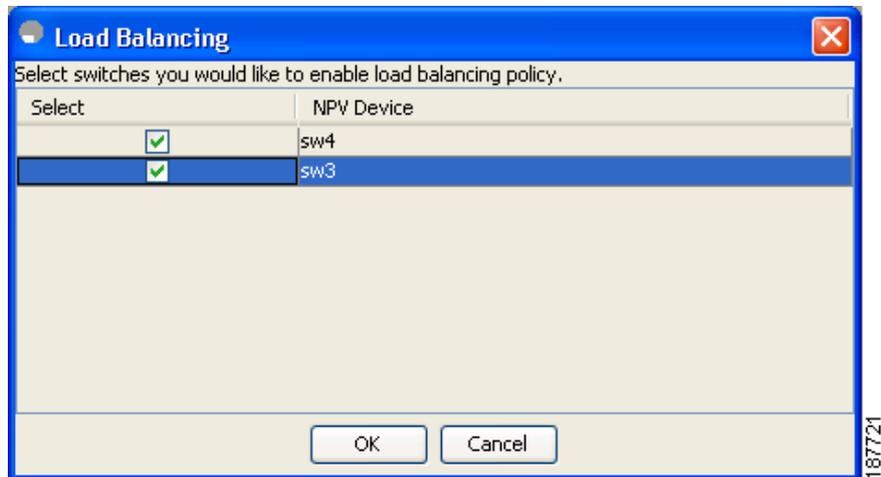
図 9-25 サーバ インターフェイスと外部インターフェイスのマッピングによるロード バランシングの設定



187720

ロード バランシングが必要な NPV デバイスを選択するには、[Configure Load Balancing] をクリックしてから、中断を伴うロード バランシングを行う NPV デバイスを選択します (図 9-26 を参照)。

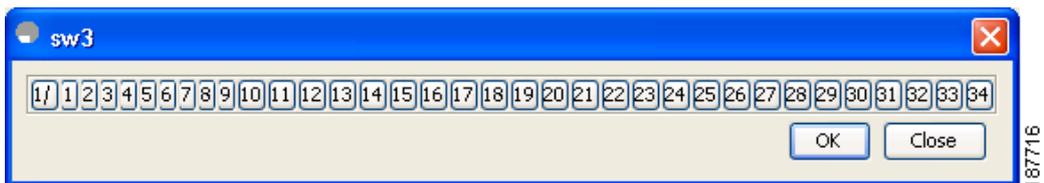
図 9-26 ロード バランシングを行う NPV デバイスの選択



トラフィック管理マップを設定するには、バージョン 4.1(1a) 以降のスイッチを少なくとも 1 つ、サーバインターフェイス、および外部インターフェイスを選択します。マップ エントリを追加する手順は、次のとおりです。

- a. [Add] をクリックして新しいマップ行を作成します。
- b. [NPV Device] セルをダブルクリックし、ドロップダウン リストからスイッチを選択します。
- c. [Server Interface] セルをダブルクリックしてからポート番号を入力するか、またはセルの [...] ボタン (ブレードサーバスイッチでは使用不可) をクリックしてポート選択ダイアログボックスを表示します。ポート選択ダイアログボックスで番号付きのボタンをクリックし、ポートを選択します (図 9-27 を参照)。

図 9-27 インターフェイスの選択



(注) 行から選択できるサーバインターフェイス ポートは 1 つだけですが、複数の外部インターフェイス ポートをそのポートにマップできます。すでに選択されたポートはディセーブルとなり、選択できません。

- d. [External Interfaces] セルをダブルクリックしてポート番号を入力するか、またはセルの [...] ボタン (ブレードサーバスイッチでは使用不可) をクリックしてポート選択ダイアログボックスを表示します。ポート選択ダイアログボックスで番号付きのボタンをクリックし、ポートを選択します (図 9-27 を参照)。

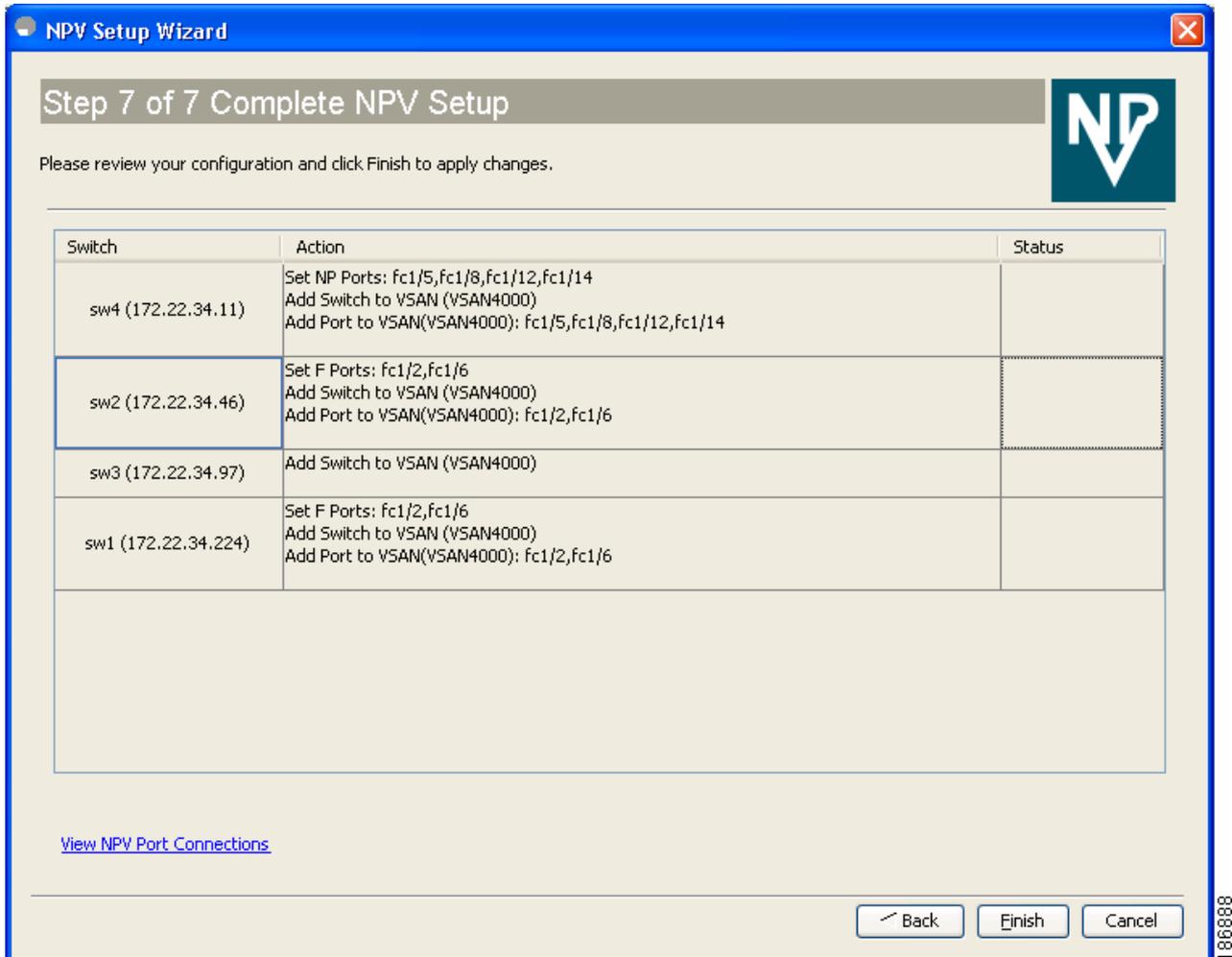
既存のマップ エントリを削除するには、行を選択してから [Delete] をクリックします。

既存のマップ エントリをすべて削除するには、[Delete All] をクリックします。

NPV の設定

- ステップ 8** これまでのステップで入力したすべての NPV Setup 設定を確認し、[Finish] をクリックしてセットアップを完了します (図 9-28 を参照)。

図 9-28 NPV Setup の完了



[Enable Switch Feature] には、スイッチ、機能に関してスイッチで実行されるアクション、および結果のステータスが表示されます。

[Set Port Type] には、スイッチ、および NPV 関連ポートを設定するためにスイッチに設定されるポートが表示されます。

[Configure VSAN] には、指定された VSAN に追加されるスイッチおよびポートが表示されます。

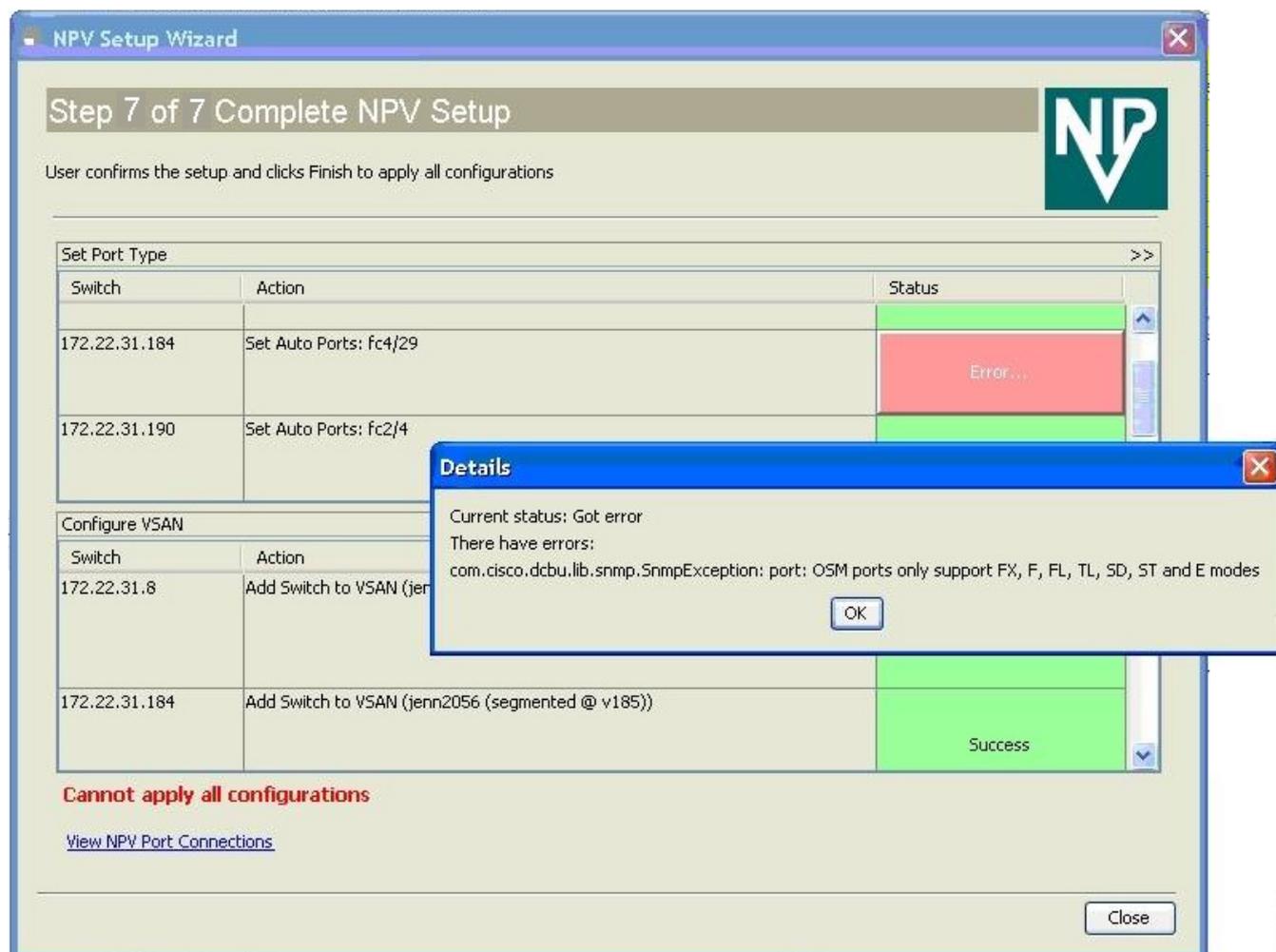
[>>] をクリックするとペインが展開されて表示されます。[<<] をクリックするとペインが折りたたまれます。

ウィンドウの下部にある経過表示バーは、設定作業全体の進行状況を示しています。経過表示バーの下に表示されるテキストメッセージは、現在進行中のタスクを示します。

各項目に対する [Status] セルには、[In progress]、[Success]、および [Error] の各ステートが表示されます。設定を適用できない場合は、タスクの [Status] セルが [Error] に変更されます。[Error] をクリックすると [Details] が表示されます。経過表示バーが開始される代わりに、「Cannot apply all

configurations」というメッセージが表示されます (図 9-29 を参照)。

図 9-29 設定適用時のエラーおよび [Details]



すべてのタスクが完了すると、経過表示バーの代わりに [View NPV Port Connections] リンクが表示されます (図 9-29 を参照)。

[View NPV Port Connections] をクリックすると、テーブルに NPV ポート接続が表示されます (図 9-31 を参照)。このリストを参照して、NPV デバイス上の NP ポートと NPV コア スイッチ上の Auto ポート間の物理接続を確認してください。ISL の場合は物理接続がすでに存在するので、その接続を確認する必要があります。場合によっては物理接続が存在しないことがあるので、その場合は物理接続を手動で確立する必要があります。

図 9-30 新規 NPV ポート ペア

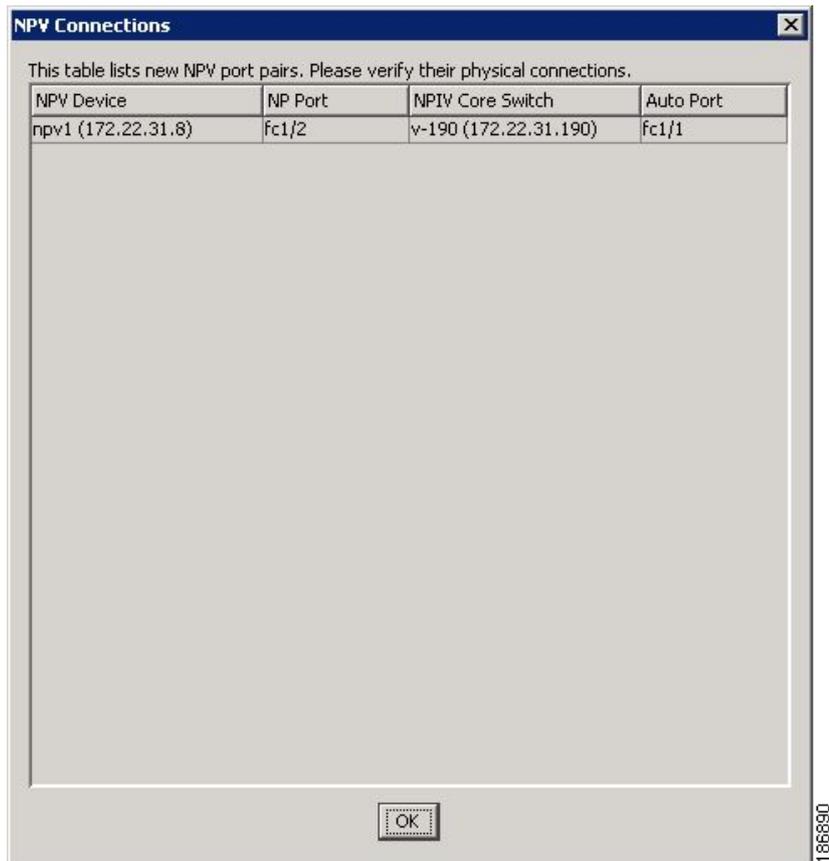
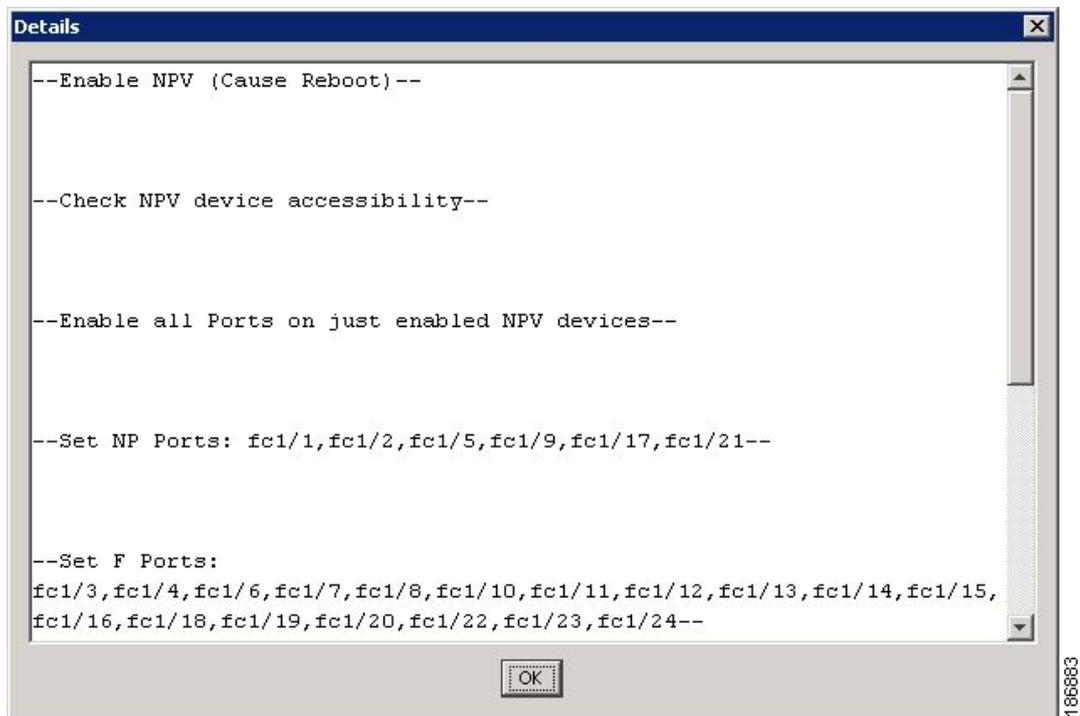


図 9-31 新規 NPV ポート ペア ([Details])



DPVM の設定

NPV をイネーブルにするときは、次の要件を満たしてから DPVM を NPV コア スイッチで設定する必要があります。

- 内部 FLOGI の WWN を DPVM で明示的に設定する必要があります。NPV デバイスに接続されているエンド デバイス用に NPV コア スイッチで DPVM を設定する場合は、同一 VSAN に含まれるようにそのエンド デバイスを設定する必要があります。別の VSAN に含まれるようにデバイスを設定すると、NPV デバイスに接続されているデバイスからのログインはエラーになります。VSAN の不一致を防ぐには、内部 FLOGI VSAN を NP ポートのポート VSAN と一致させます。
- NP ポートからの最初のログインにより、そのポートの VSAN が決まります。この最初のログイン、つまり NPV デバイスの内部ログイン用に DPVM を設定すると、NPV コア スイッチの VSAN F ポートがその VSAN で特定されます。DPVM を設定しない場合、ポート VSAN は変更されません。

DPVM 設定の詳細については、『Cisco MDS 9000 Family NX-OS Fabric Configuration Guide』を参照してください。

NPV およびポート セキュリティ

NPV コア スイッチでは、ポート セキュリティがインターフェイスごとにイネーブルになります。NPV でログインするデバイス用に NPV コア スイッチでポート セキュリティをイネーブルにするには、次の要件に従う必要があります。

- 内部 FLOGI をポート セキュリティ データベースに含める必要があります。これにより、NPV コア スイッチのポートで通信やリンクが許可されます。
- すべてのエンド デバイスの pWWN も、ポート セキュリティ データベースに含める必要があります。

この要件を満たしたら、その他のコンテキストと同じようにポート セキュリティをイネーブルにすることができます。ポート セキュリティのイネーブル化の詳細については、『Cisco MDS 9000 Family NX-OS Security Configuration Guide』を参照してください。

