



CHAPTER 21

Configuring N Port Virtualization

N Port virtualization (NPV) reduces the number of Fibre Channel domain IDs in SANs. Switches operating in the NPV mode do not join a fabric; rather, they pass traffic between NPV core switch links and end devices, which eliminates the domain IDs for these edge switches.

NPV is supported by the following Cisco MDS 9000 switches only:

- Cisco MDS 9124 Multilayer Fabric Switch
- Cisco MDS 9134 Fabric Switch
- Cisco Fabric Switch for HP c-Class BladeSystem
- Cisco Fabric Switch for IBM BladeCenter



Note

NPV is available on these switches only while in NPV mode; if in switch mode, NPV is not available.

This chapter includes the following sections:

- [About NPV, page 21-1](#)
- [NPV Guidelines and Requirements, page 21-6](#)
- [Configuring NPV, page 21-7](#)
- [Using the NPV Setup Wizard, page 21-12](#)

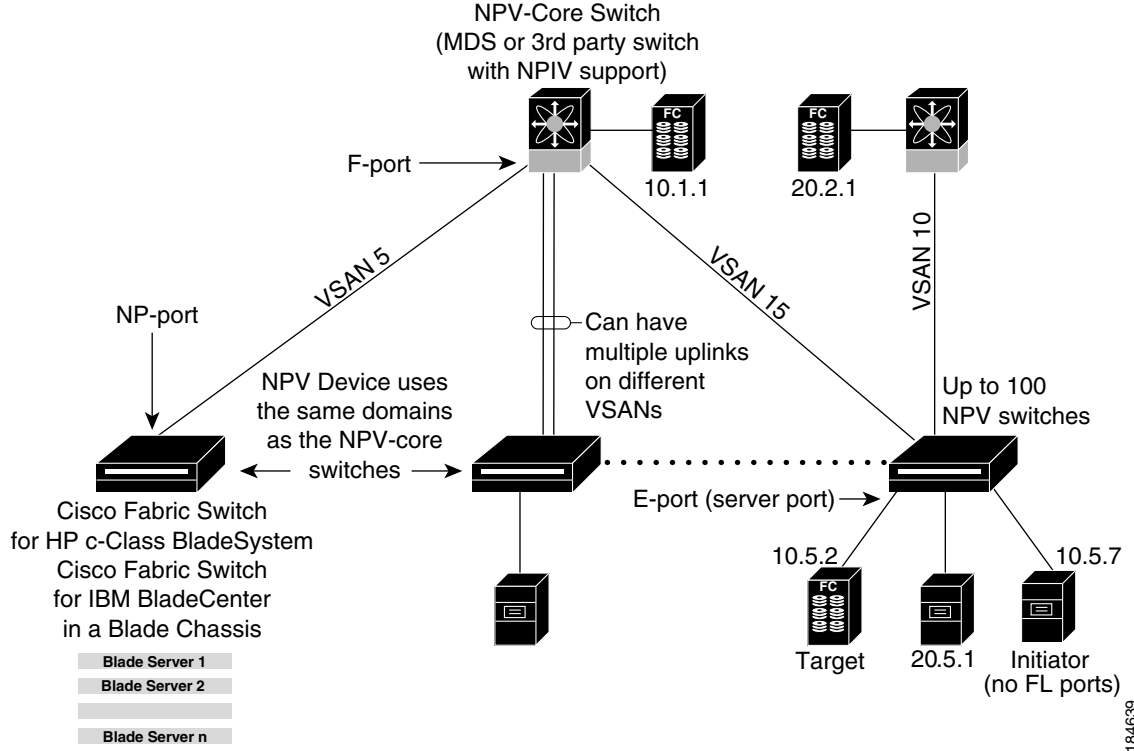
About NPV

Typically, Fibre Channel networks are deployed using a core-edge model with a large number of fabric switches connected to core devices. However, as the number of ports in the fabric increases, the number of switches deployed also increases, and you can end up with a dramatic increase in the number of domain IDs (the maximum number supported is 239). This challenge becomes even more difficult when additional blade chassis are deployed in Fibre Channel networks.

NPV addresses the increase in the number of domain IDs needed to deploy a large number of the ports by making a fabric or module switch appear as a host to the core Fibre Channel switch, and as a Fibre Channel switch to the servers in the fabric or blade switch. NPV aggregates multiple locally connected N ports into one or more external NP links, which shares the domain ID of the NPV core switch among multiple NPV switches (see [Figure 21-1](#)). NPV also allows multiple devices to attach to the same port on the NPV core switch, thereby reducing the need for more ports on the core.

Send documentation comments to mdsfeedback-doc@cisco.com

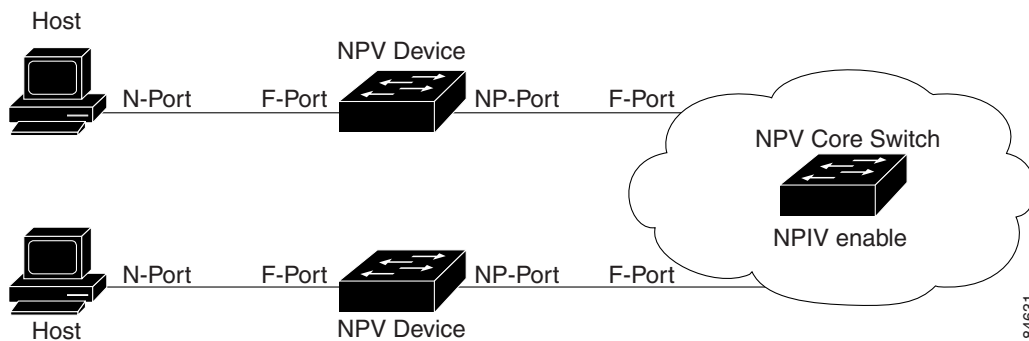
Figure 21-1 Cisco NPV Fabric Configuration



While NPV is similar to N port identifier virtualization (NPIV), it does not offer exactly the same functionality. NPIV provides a means to assign multiple FC IDs to a single N port, and allows multiple applications on the N port to use different identifiers. NPIV also allows access control, zoning, and port security to be implemented at the application level. NPV makes use of NPIV to get multiple FCIDs allocated from the core switch on the NP port.

Figure 21-2 shows a more granular view of an NPV configuration at the interface level.

Figure 21-2 Cisco NPV Configuration–Interface View



[Send documentation comments to mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)

NPV Mode

A switch is in NPV mode after a user has enabled NPV and the switch has successfully rebooted. NPV mode applies to an entire switch. All end devices connected to a switch that is in NPV mode must log in as an N port to use this feature (loop-attached devices are not supported). All links from the edge switches (in NPV mode) to the NPV core switches are established as NP ports (not E ports), which are used for typical interswitch links. NPIV is used by the switches in NPV mode to log in to multiple end devices that share a link to the NPV core switch.



Note

In-order data delivery is not required in NPV mode because the exchange between two end devices always takes the same uplink to the core from the NPV device. For traffic beyond the NPV device, core switches will enforce in-order delivery if needed and/or configured.

NP Ports

An *NP port* (proxy N port) is a port on a device that is in NPV mode and connected to the NPV core switch using an F port. NP ports behave like N ports except that in addition to providing N port behavior, they also function as proxies for multiple, physical N ports.

NP Links

An *NP link* is basically an NPIV uplink to a specific end device. NP links are established when the uplink to the NPV core switch comes up; the links are terminated when the uplink goes down. Once the uplink is established, the NPV switch performs an internal FLOGI to the NPV core switch, and then (if the FLOGI is successful) registers itself with the NPV core switch's name server. Subsequent FLOGIs from end devices in this NP link are converted to FDISCs. For more details refer to the [“Internal FLOGI Parameters” section on page 21-3](#).

Server links are uniformly distributed across the NP links. All the end devices behind a server link will be mapped to only one NP link.

Internal FLOGI Parameters

When an NP port comes up, the NPV device first logs itself in to the NPV core switch and sends a FLOGI request that includes the following parameters:

- The fWWN (fabric port WWN) of the NP port used as the pWWN in the internal login.
- The VSAN-based sWWN (switch WWN) of the NPV device used as nWWN (node WWN) in the internal FLOGI.

After completing its FLOGI request, the NPV device registers itself with the fabric name server using the following additional parameters:

- Switch name and interface name (for example, fc1/4) of the NP port is embedded in the symbolic port name in the name server registration of the NPV device itself.
- The IP address of the NPV device is registered as the IP address in the name server registration of the NPV device.

Send documentation comments to mdsfeedback-doc@cisco.com

**Note**

The BB_SCN of internal FLOGIs on NP ports is always set to zero. The BB_SCN is supported at the F-port of the NPV device.

Figure 21-3 shows the internal FLOGI flows between an NPV core switch and an NPV device.

Figure 21-3 Internal FLOGI Flows

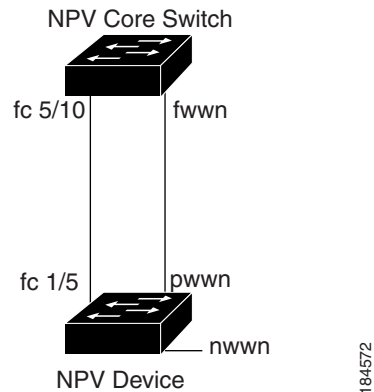


Table 21-1 identifies the internal FLOGI parameters that appear in Figure 21-3.

Table 21-1 Internal FLOGI parameters

Parameter	Derived From
pWWN	The fWWN of the NP port.
nWWN	The VSAN-based sWWN of the NPV device.
fWWN	The fWWN of the F port on the NPV core switch.
symbolic port name	The switch name and NP port interface string. Note If there is no switch name available, then the output will simply read “switch.” For example, <code>switch: fc1/5</code> .
IP address	The IP address of the NPV device.
symbolic node name	The NPV switch name.

Although fWWN-based zoning is supported for NPV devices, it is not recommended because:

- Zoning is not enforced at the NPV device (rather, it is enforced on the NPV core switch).
- Multiple devices behind an NPV device log in via the same F port on the core (hence, they use same fWWN and cannot be separated into different zones).
- The same device might log in using different fWWNs on the core switch (depending on the NPV link it uses) and may need to be zoned using different fWWNs.

Default Port Numbers

Port numbers on NPV-enabled switches will vary depending on the switch model. For details about port numbers for NPV-eligible switches, see [Chapter 11, “On-Demand Port Activation Licensing.”](#)

[Send documentation comments to mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)

NPV CFS Distribution over IP

NPV devices use only IP as the transport medium. CFS uses multicast forwarding for CFS distribution. NPV devices do not have ISL connectivity and FC domain. To use CFS over IP, multicast forwarding has to be enabled on the ethernet IP switches all along the network that physically connects the NPV switch. You can also manually configure the static IP peers for CFS distribution over IP on NPV-enabled switches. For more information, see the [Cisco MDS 9000 Family CLI Configuration Guide](#).

NPV Traffic Management

This section discusses the following aspects of load balancing:

- [Auto](#), page 21-5
- [Traffic Map](#), page 21-5
- [Disruptive](#), page 21-6

Auto

Before Cisco MDS SAN-OS release 3.3(1a), NPV supported **automatic** selection of external links. When a server interface is brought up, an external interface with the minimum load is selected from the available links. There is no manual selection on the server interfaces using the external links. Also, when a new external interface was brought up, the existing load was not distributed automatically to the newly available external interface. This newly brought up interface is used only by the server interfaces that come up after this interface.

Traffic Map

As in Cisco MDS SAN-OS release 3.3(1a) and later, NPV supports traffic management by allowing you to select and **configure the external interfaces** that the server uses to connect to the core switches.



Note

When the NPV traffic management is configured, the server uses only the configured external interfaces. Any other available external interface will not be used.

The NPV traffic management feature provides the following benefits:

- Facilitates traffic engineering by providing dedicated external interfaces for the servers connected to NPV.
- Uses the shortest path by selecting external interfaces per server interface.
- Uses the persistent FC ID feature by providing the same traffic path after a link break, or reboot of the NPV or core switch.
- Balances the load by allowing the user to evenly distribute the load across external interfaces.

Send documentation comments to mdsfeedback-doc@cisco.com

Disruptive

Disruptive load balance works independent of automatic selection of interfaces and configured traffic map of external interfaces. This feature forces re-init of the server interfaces to achieve load balance when this feature is enabled and whenever a new external interface comes up. To avoid flapping the server interfaces too often undesirably, enable this feature once and then disable it whenever the needed load balance is achieved.

If disruptive load balance is not enabled, you need to manually flap the server interface to move some of the load to a new external interface.

Multiple VSAN Support

By grouping devices into different NPV sessions based on VSANs, it is possible to support multiple VSANs on the NPV-enabled switch. The correct uplink must be selected based on the VSAN that the uplink is carrying.

NPV Guidelines and Requirements

Following are recommended guidelines and requirements when deploying NPV:

- NPV core switches must support NPIV.
- You can have up to 100 NPV devices.
- Nondisruptive upgrades are supported. See [Chapter 15, “Software Images.”](#)
- Port tracking is supported. See [Chapter 57, “Configuring Port Tracking.”](#)
- You can configure zoning for end devices that are connected to NPV devices using all available member types on the NPV core switch. If fWWN, sWWN, domain, or port-based zoning is used, then fWWN, sWWN or the domain/port of the NPV core switch should be used.
- Port security is supported on the NPV core switch for devices logged in via NPV.
- NPV uses a load balancing algorithm to automatically assign end devices in a VSAN to one of the NPV core switch links (in the same VSAN) upon initial login. If there are multiple NPV core switch links in the same VSAN, then you cannot assign a specific one to an end device.
- Both servers and targets can be connected to an NPV device.
- Remote SPAN is not supported.
- Local switching is not supported; all traffic is switched using the NPV core switch.
- NPV devices can connect to multiple NPV core switches. In other words, different NP ports can be connected to different NPV core switches.
- NPV supports NPIV-capable module servers (nested NPIV).
- Only F, NP, and SD ports are supported in NPV mode.



Note

In the case of servers that are booted over the SAN with NPV, if an NPV link failover occurs, servers will lose access to their boot LUN temporarily.

[Send documentation comments to mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)

NPV Traffic Management Guidelines

When deploying NPV traffic management, follow these guidelines:

- Use NPV traffic management only when the automatic traffic engineering by the NPV device is not sufficient for the network requirements.
- Do not configure traffic maps for all the servers. For non-configured servers, NPV will use automatic traffic engineering.
- Configure the Persisten FC ID on the core switch. Traffic engineering directs the associated server interface to external interfaces that lead to the core switch.
- Server interfaces configured to a set of external interfaces cannot use any other available external interfaces, even if the configured interfaces are not available.
- Do not configure disruptive load balancing because this involves moving a device from one external interface to another interface. Moving the device between external interfaces requires NPV relogin to the core switch through F port leading to traffic disruption.
- Link a set of servers to a core switch by configuring the server to a set of external interfaces that are linked to the core switch.

Configuring NPV

When you enable NPV, the system configuration is erased and the system is reboots, with the NPV mode enabled.



Note

We recommend that you save the current configuration either on bootflash or a TFTP server before NPV (if the configuration is required for later use). Use the following commands to save either your non-NPV or NPV configuration:

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

The configuration can be reapplied later using the following command:

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

SUMMARY STEPS

1. Enable NPIV on the NPV core switch. Enable NPV on the NPV device.
2. Configure the interfaces connected to the NPV core switch as NP ports.
3. Configure NPV link as an F port on the NPV core switch.
4. Configure server link on the NPV device.



Note

- On the 91x4 platform, before you upgrade to 3.2(2c) or downgrade from 3.2(2c), shut the F ports connected to NPIV-capable hosts, and then disable the NPIV feature. After the upgrade or downgrade is complete, enable the NPIV feature and up the F ports.
- On the 91x4 platform, before you downgrade from 3.2(2c) to earlier versions, shut the F port, enable and disable the FC domain persistency for that VSAN and then up the F port.

Send documentation comments to mdsfeedback-doc@cisco.com

To use Fabric Manager and Device Manager to configure NPV, follow these steps:

- Step 1** Launch Device Manager from the core NPV switch to enable NPIV on the core NPV switch. From the Admin drop-down menu, select Feature Control. Select **enable** for the NPIV feature (see [Figure 21-4](#)).

Figure 21-4 Enabling NPIV and NPV

Name	Status	Action	LastCommand	Result
fcsp	enabled	noSelection	noSelection	none
ficon	enabled	noSelection	noSelection	none
tacacs	disabled	noSelection	noSelection	none
qos-manager	disabled	noSelection	noSelection	none
port-security	disabled	noSelection	noSelection	none
fabric-binding	enabled	noSelection	noSelection	none
port_track	disabled	noSelection	noSelection	none
scheduler	disabled	noSelection	noSelection	none
npiv	disabled	noSelection	noSelection	none
dpvm	disabled	noSelection	noSelection	none
sdv	disabled	noSelection	noSelection	none
npv	disabled	noSelection	noSelection	none

12 row(s)

Apply Refresh Help Close

- Step 2** Click **Apply**.
- Step 3** From the Interface drop-down menu, select FC All to configure the NPIV core switch port as an F Port.
- Step 4** In the Mode Admin column, select the F port mode and click **Apply**.
- Step 5** Launch Device Manager from the NPV device to enable NPV on the NPV device. From the Admin drop-down menu, select Feature Control. Select enable for the NPV feature and click **Apply**.
- Step 6** From the Interface drop-down menu, select FC All to configure the external interfaces on the NPV device.
- Step 7** In the Mode Admin column, select the NP port mode and click **Apply**.
- Step 8** To configure the server interfaces on the NPV device, from the Interface drop-down menu, select FC All.
- Step 9** In the Mode Admin column, select F port mode and click **Apply**.
- Step 10** The default Admin status is down. After configuring port modes, you must select up Admin Status to bring up the links.

Configuring NPV Traffic Management

The NPV traffic management feature is enabled after configuring NPV. Configuring NPV traffic management involves configuring a list of external interfaces to the servers, and enabling or disabling disruptive load balancing.

Configuring List of External Interfaces per Server Interface

A list of external interfaces are linked to the server interfaces when the server interface is down, or if the specified external interface list includes the external interface already in use.

Send documentation comments to mdsfeedback-doc@cisco.com

To configure the list of external interfaces per server interface using Fabric Manager, perform the following tasks:

- Step 1** Choose **Physical Attributes > Switches > N_Port Virtualizer (NPV)** as shown in [Figure 21-5](#)

Figure 21-5 NPV Traffic Map Tab

The screenshot shows the Fabric Manager 3.4(1) interface. The main window is titled "/SAN/Fabric_sw2/Switch" and has tabs for Control, Traffic Map, Load Balance, and NP Link. The Traffic Map tab is active, displaying a table with the following data:


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

Below the table is a network diagram showing three switches (sw1, sw2, sw3) connected in a triangle. Each switch is connected to a host with a specific MAC address: sw1 to 20:00:00:1b:32:07:13:e9-H, sw2 to 20:00:00:1b:32:09:6e:e0-H, and sw3 to 20:00:00:1b:32:09:e8:df-H. The diagram also shows a host connected to sw3 with MAC address 20:00:00:1b:32:09:89:df-H.

The left sidebar shows the Logical Domains tree with SAN > Fabric_sw2 > NPV selected. The Physical Attributes tree shows Switches > NPV > N_Port Virtualizer (NPV) selected.

At the bottom of the window, it says "10 rows, queried 2 switches".

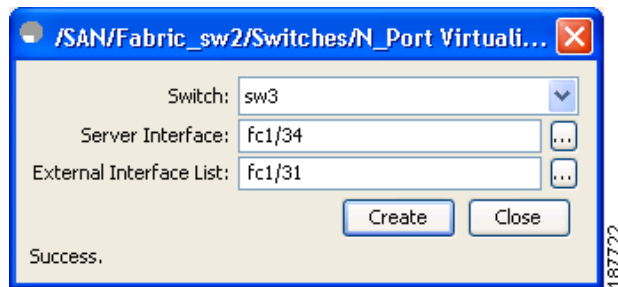
- Step 2** Select the Traffic Map tab.

- Step 3** Click the  icon in the toolbar or right click and then select **Create Row...**

Send documentation comments to mdsfeedback-doc@cisco.com

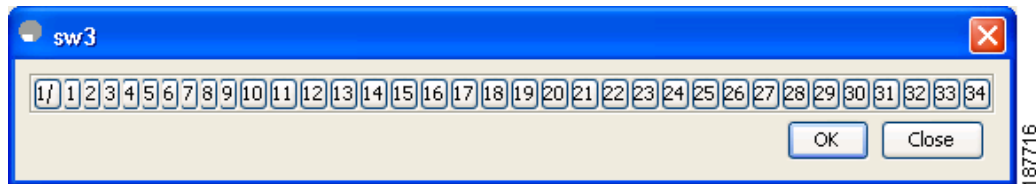
Step 4 Select the Switch from the drop-down list as shown in [Figure 21-6](#).

Figure 21-6 Map Entry Dialog Box




Step 5 Type the port numbers or click the [...] button (not available on blade server switches) to select the Server Interface and External Interfaces from the port selection dialog box as shown in [Figure 21-7](#).

Figure 21-7 Port Selection Dialog Box



Note You can select only one Server Interface but multiple External Interfaces can be mapped on to it. Previously selected ports are disabled and cannot be selected.

To delete the map entry, select the row from the Traffic Map tab, and then click the  icon in the toolbar or right click and select **Delete Row**.

Enable or Disable the Global Policy for Disruptive Load Balancing

Disruptive load balancing allows you to review the load on all the external interfaces and balance the load disruptively. Disruptive load balancing is done by moving the servers using heavily loaded external interfaces, to the external interfaces running with fewer loads.

To enable disruptive load balancing using Fabric Manager, perform the following tasks:

Step 1 Choose **Physical Attributes > Switches > N_Port Virtualizer (NPV)** as shown in [Figure 21-8](#).

Step 2 Select the Load Balance tab.

Step 3 Check the **Enable** checkbox to enable disruptive load balancing on the switch.

Send documentation comments to mdsfeedback-doc@cisco.com

To enable disruptive load balancing on all the switches, check the **Enable All** checkbox as shown in Figure 21-8.

Figure 21-8 NPV Load Balance Tab

The screenshot shows the Fabric Manager 3.4(1) interface for configuring NPV Load Balance. The main window title is "Fabric Manager 3.4(1) [admin@localhost (session 2)] /SAN/Fabric_sw2". The interface is divided into several sections:

- Logical Domains:** A tree view showing the hierarchy: SAN > Fabric_sw2 > All VSANs > VSAN0001 > VSAN0002 (down) > VSAN4000 > Groups.
- Physical Attributes:** A tree view showing various attributes: Switches, Hardware, Licenses, CFS, Clock, Supervisor Statistics, Copy Configuration, Interfaces, FC Services, Events, Security, NPV, N_Port Virtualizer (NPV), Flex Attach, NP Link Statistics, ISLs, and End Devices.
- Configuration Area:**
 - Buttons: Control, Traffic Map, Load Balance (selected), NP Link.
 - Table:

Switch	Enable
sw4	<input checked="" type="checkbox"/>
sw3	<input checked="" type="checkbox"/>
 - Checkbox: Enable All
- Network Diagram:** A diagram showing four switches (sw1, sw2, sw3, sw4) connected in a mesh topology. Each switch is represented by a server icon with a unique MAC address:
 - sw1: 20:00:00:1b:32:07:13:e9-H
 - sw2: 20:00:00:1b:32:09:8e:e0-H
 - sw3: 20:00:00:1b:32:09:89:df-H
 - sw4: 20:00:00:1b:32:09:e8:df-H

At the bottom of the interface, there is a status bar that reads "2 rows, queried 2 switches".

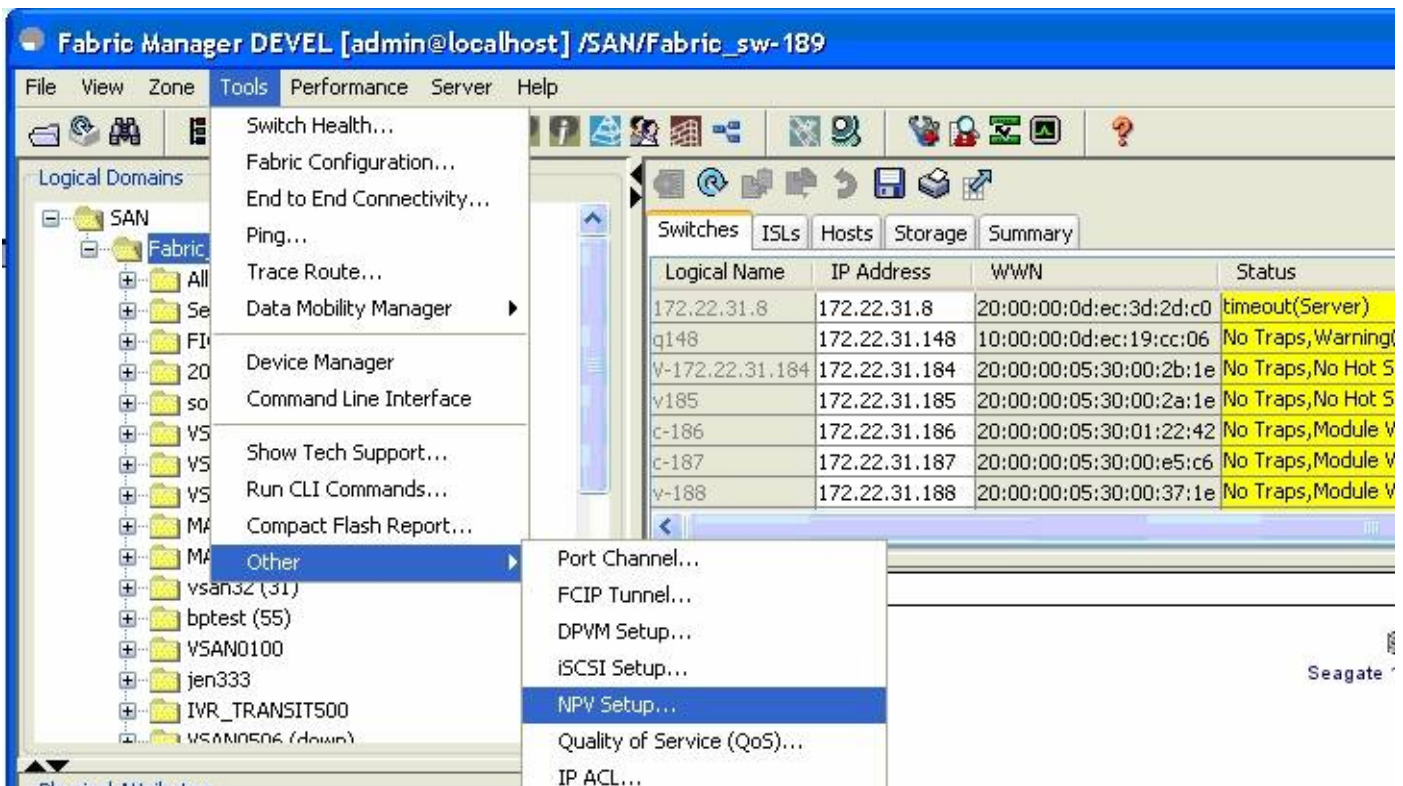
Send documentation comments to mdsfeedback-doc@cisco.com

Using the NPV Setup Wizard

To configure NPV using the wizard, follow these steps:

- Step 1** Select **Tools > Other > NPV Setup...** to launch NPV Setup Wizard from Fabric Manager. (See [Figure 21-9](#).)

Figure 21-9 Launching NPV Setup Wizard



Send documentation comments to mdsfeedback-doc@cisco.com

Before the wizard starts, Fabric Manager checks if there are any NPV and NPIV capable switches from the client's SAN. An NPV-capable switch has to be a Cisco MDS 9124, 9134, a HP Blade Server, or an IBM Blade Server with SAN-OS version 3.2.2 and later. An NPIV capable switch has to be Cisco switch with SAN-OS 3.0.1 and later. If there are no NPV-capable switches, FM displays an error message. (See [Figure 21-10](#).)

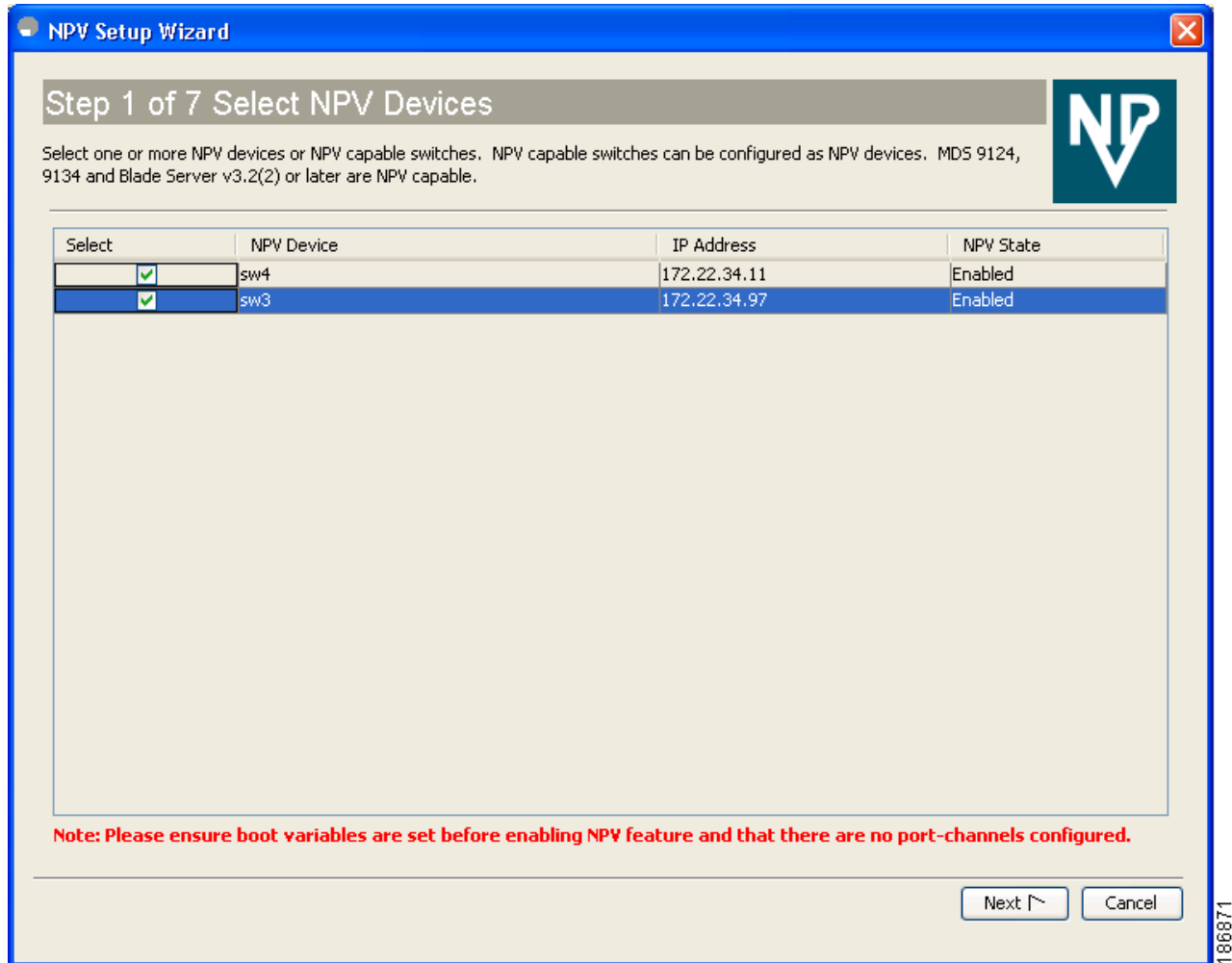
Figure 21-10 Error in Launching



Send documentation comments to mdsfeedback-doc@cisco.com

Step 2 Select the NPV devices as shown in [Figure 21-11](#).

Figure 21-11 Selecting the NPV Devices

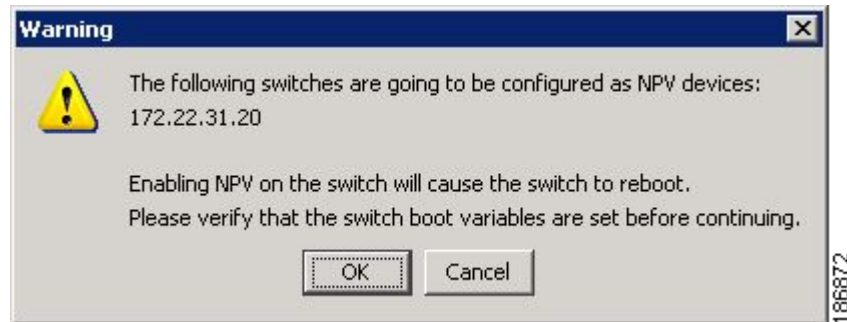


A table lists all the available NPV-capable switches including the switches on which NPV is not yet enabled. Check the check boxes to select the required NPV devices. On devices that are not NPV enabled, this wizard will enable NPV on the devices in the final step.

Send documentation comments to mdsfeedback-doc@cisco.com

If you choose switches that are NPV disabled and click **Next**, a warning message appears with a list of IP addresses of the NPV devices on which NPV will be enabled. Enabling NPV on the switch will result in reboot of the switch. Boot variables of the switches have to be set, to enable NPV on them through this wizard. (See [Figure 21-12](#).)

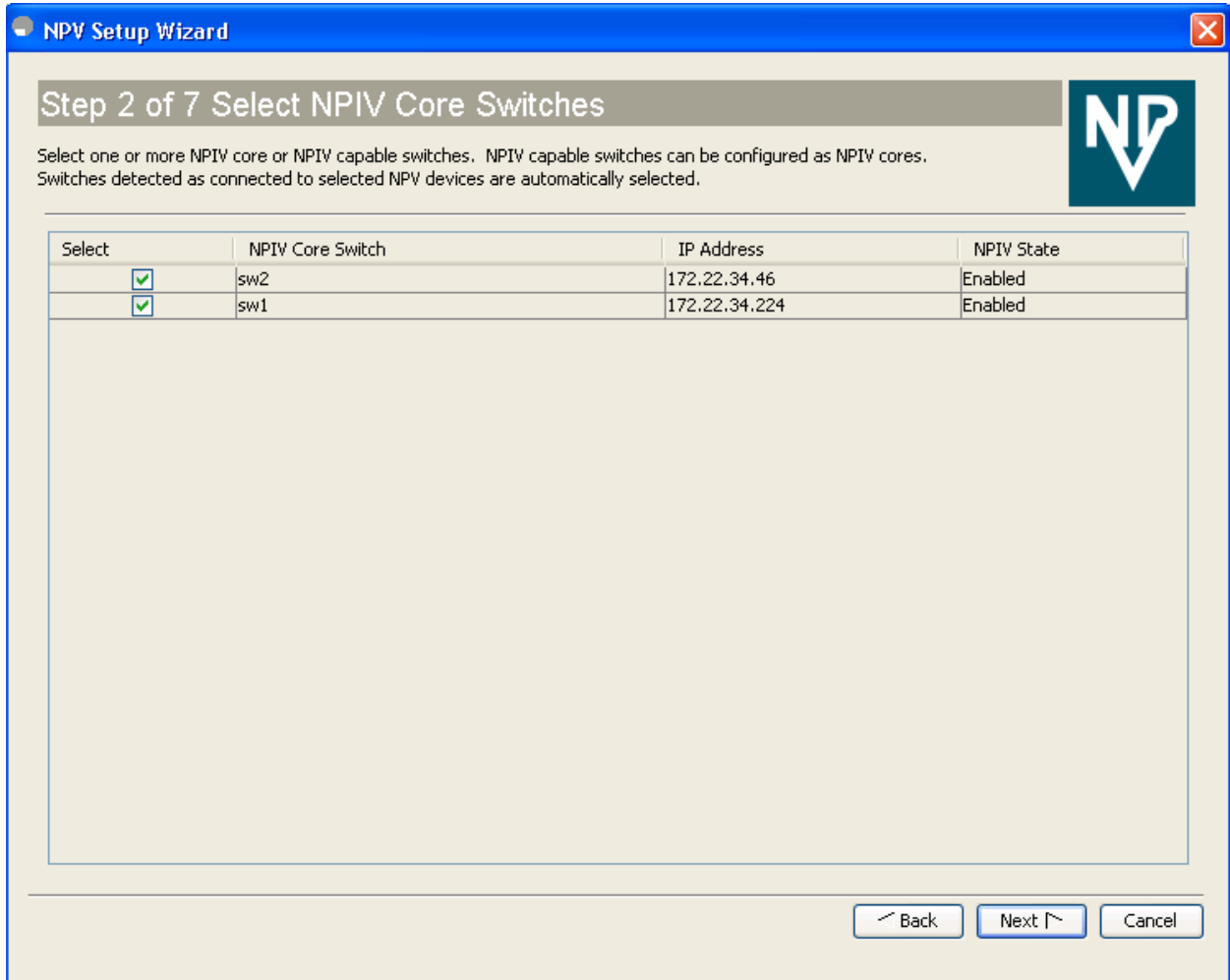
Figure 21-12 Warning to Enable NPV Feature on NPV-Capable Switches



Send documentation comments to mdsfeedback-doc@cisco.com

Step 3 Select the NPIV core switches as shown in Figure 21-13.

Figure 21-13 Selecting the NPIV Core Switches

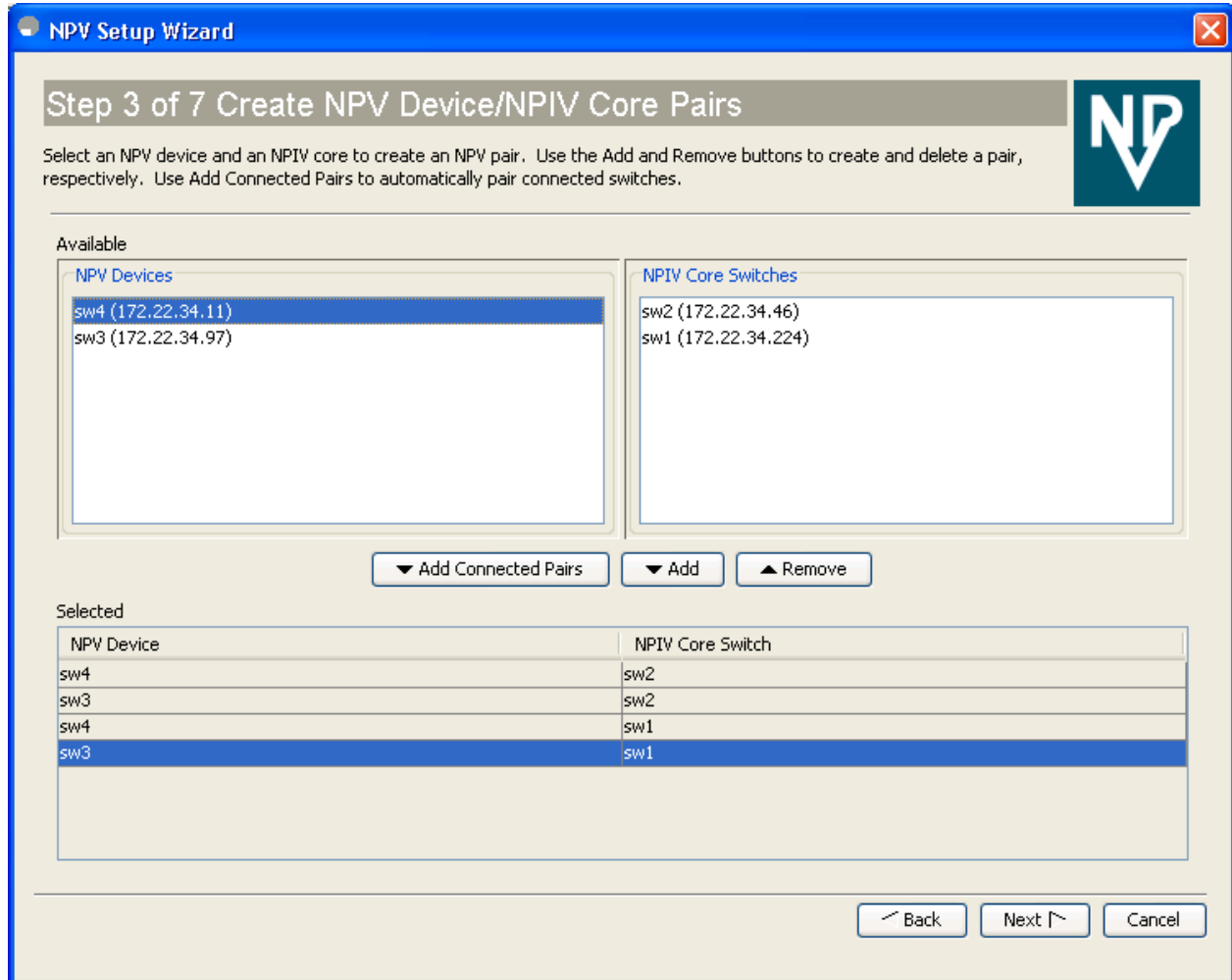


Check the check boxes to select the required NPIV core switches. The table lists all the available NPIV core switches including the core switches that have not yet enabled the NPIV feature. The NPIV core switches which are not NPIV enabled, this wizard will enable NPIV on them in the final step.

Send documentation comments to mdsfeedback-doc@cisco.com

Step 4 Create new NPV device and NPIV core switch pairs as required. (See [Figure 21-14](#).)

Figure 21-14 Creating NPV Device and NPIV Core Switch Pairs



Based on selections in the previous steps, the wizard displays all available NPV devices and NPIV core switches in separate lists. You can select one from each list and click **Add** or **Remove** buttons to create new NPV device and NPIV core switch combinations or pairs.

The NPV wizard checks if there are any NPIV core switches that are already connected to the NPV devices selected in the previous step. Click the **Add Connected Pairs** button to add a list of all the existing pairs that are interconnected, to the **Selected** table.

The **Selected** table below is then populated with both the existing and the intended pairs. Each NPIV core switch can be paired with multiple NPV devices.

After Step 6 the wizard prompts you to physically connect the new pairs that are not yet connected.

On the switches that are not paired, the NPV wizard enables the NPV and NPIV modes. However, there is a possibility that these unpaired switches may be segmented and lose their presence on the fabric.

Send documentation comments to mdsfeedback-doc@cisco.com

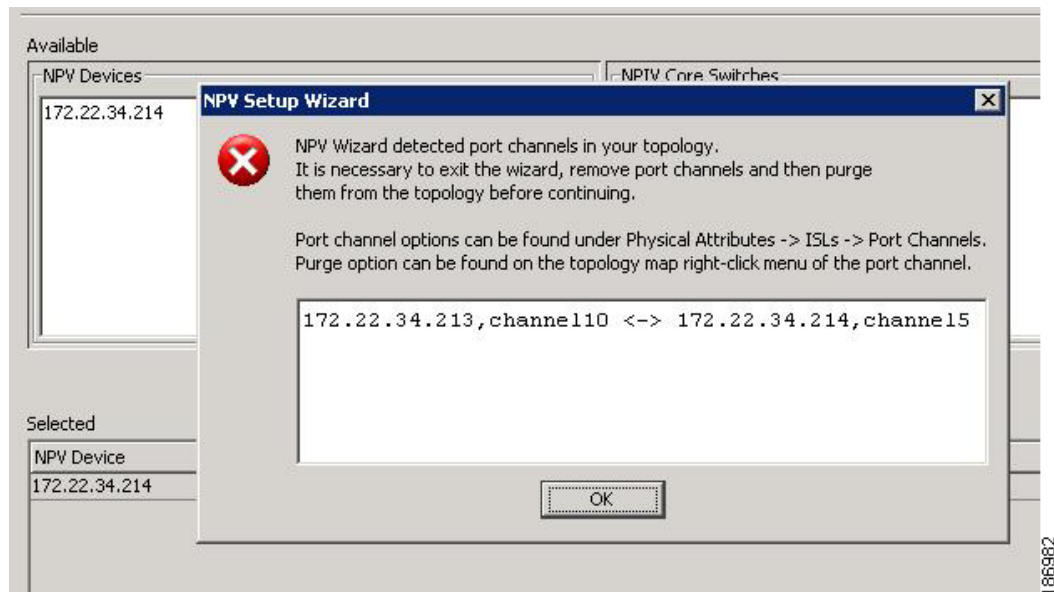
After you click the Next button in Step 3 of 6, the wizard determines if you have selected all the connected pairs. A warning message is displayed (See [Figure 21-17](#)), that lists all the connected pairs that you have not selected and warns that they will be segmented after the NPV setup.



Note

- NPV wizard does not detect ports that are in a channel-group and that are not connected by ISLs. The wizard does not configure any port in a Port Channel Group to F-ports on the core switch. Port channel grouping is not applicable to NPV devices. (See [Figure 21-15](#).)
- Remove the port channel groups if you need to select those particular ports as F ports during the setup. For more information, see the “[Configuring Port Security](#)” section on page 37-1.

Figure 21-15 Port Channel Group Detected.



Send documentation comments to mdsfeedback-doc@cisco.com

Figure 21-16 Warning, NPV Setup Wizard

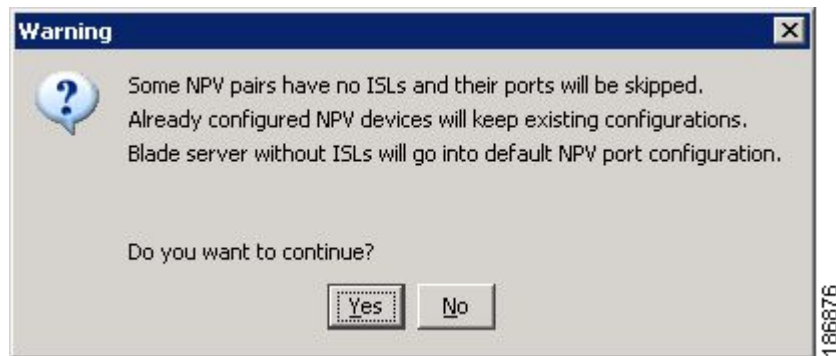


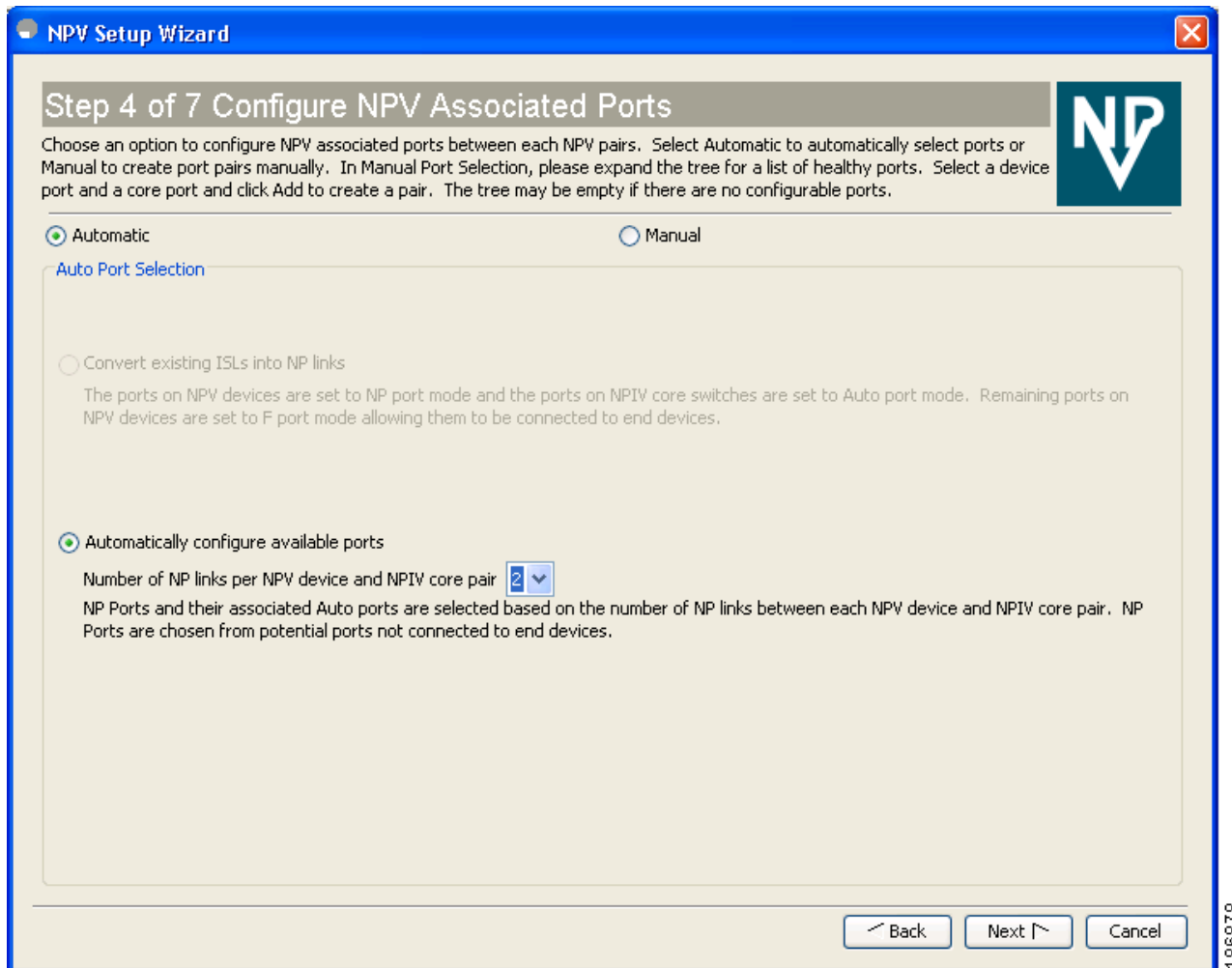
Figure 21-17 Warning, NPV Setup Wizard.



Send documentation comments to mdsfeedback-doc@cisco.com

- Step 5** You can configure NPV associated ports either through automated or manual methods. (See [Figure 21-18](#).)

Figure 21-18 Configuring NPV Associated Ports by the Automatic Method



The **Auto Port Selection** has two options.

Choosing the first option allows you to convert the existing ISLs to be run as NPV links. If you want ISLs to take priority, then choose the **Convert existing ISLs** option.

The wizard discovers ISLs (Up or Down) between the selected switches, that are available at the time of wizard launch.

Choosing the second option allows the NPV wizard to automatically configure Free ports for NPV usage. In the second option, you can choose up to a maximum of Six additional NPV links per NPV device and core switch pair.

During automatic port selection on the NPV switch, ports are defined as licensed FC ports with “Operational status” = Auto and “Status Cause” = none(2), offline(8), or sfp not present(29) and “Operational Status” = TE or E.

Send documentation comments to mdsfeedback-doc@cisco.com

Ports on the NPV switch are selected in the following way:

The ISLs are considered in the second method. The selection algorithm spreads out the free port selections, so that the first port in every four ports is selected, for example, the 1st, 5th, 9th, etc. If after going through the 1st port in every four you still have not selected enough ports (because the preferred ports were not free) then move to the second port in every four, for example, the 2nd, 6th, 10th etc. Different switches have different port preferences.

Ports on the NPIV switch are selected in the following way:

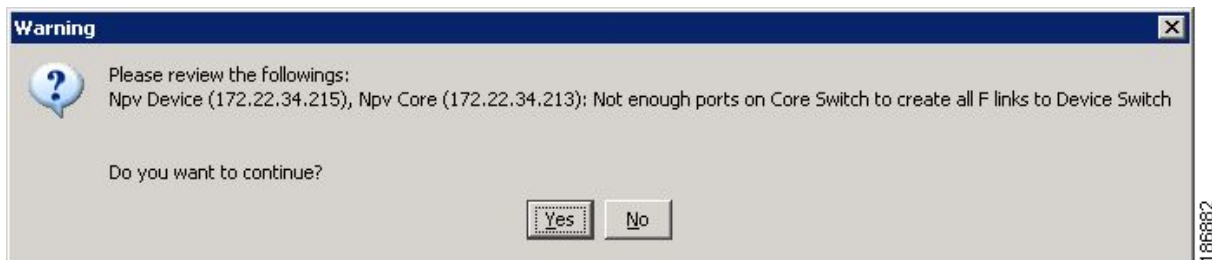
During automatic port selection on the NPIV switch free ports are defined as ports that are licensed FC ports and ports that have "Operational status" = Auto and "Status Cause" =none(2), offline(8) or sfp not present(29). If the ports are found in any other operational state, (for example F, NP, E, TE etc), then they are considered used, except for E and TE ports that are in ISLs connected to NPV device switches that will be enabled for NPV mode in this wizard session, as they will be considered to be free. However, these ISL ports will not necessarily be the ports selected by the automatic port selection algorithm as they are treated no different then any other free port. If you want to convert those used ISL ports, then choose the convert existing ISLs first and then run the wizard a second time choosing Automatic port selection (option 2) to add additional links.

When you choose to configure ports from available ports, the wizard searches for ports that are not currently participating in NP link configuration. It is possible that all ports can be participating in NP port configuration. In that case a warning message is displayed. (See [Figure 21-19](#).)

**Note**

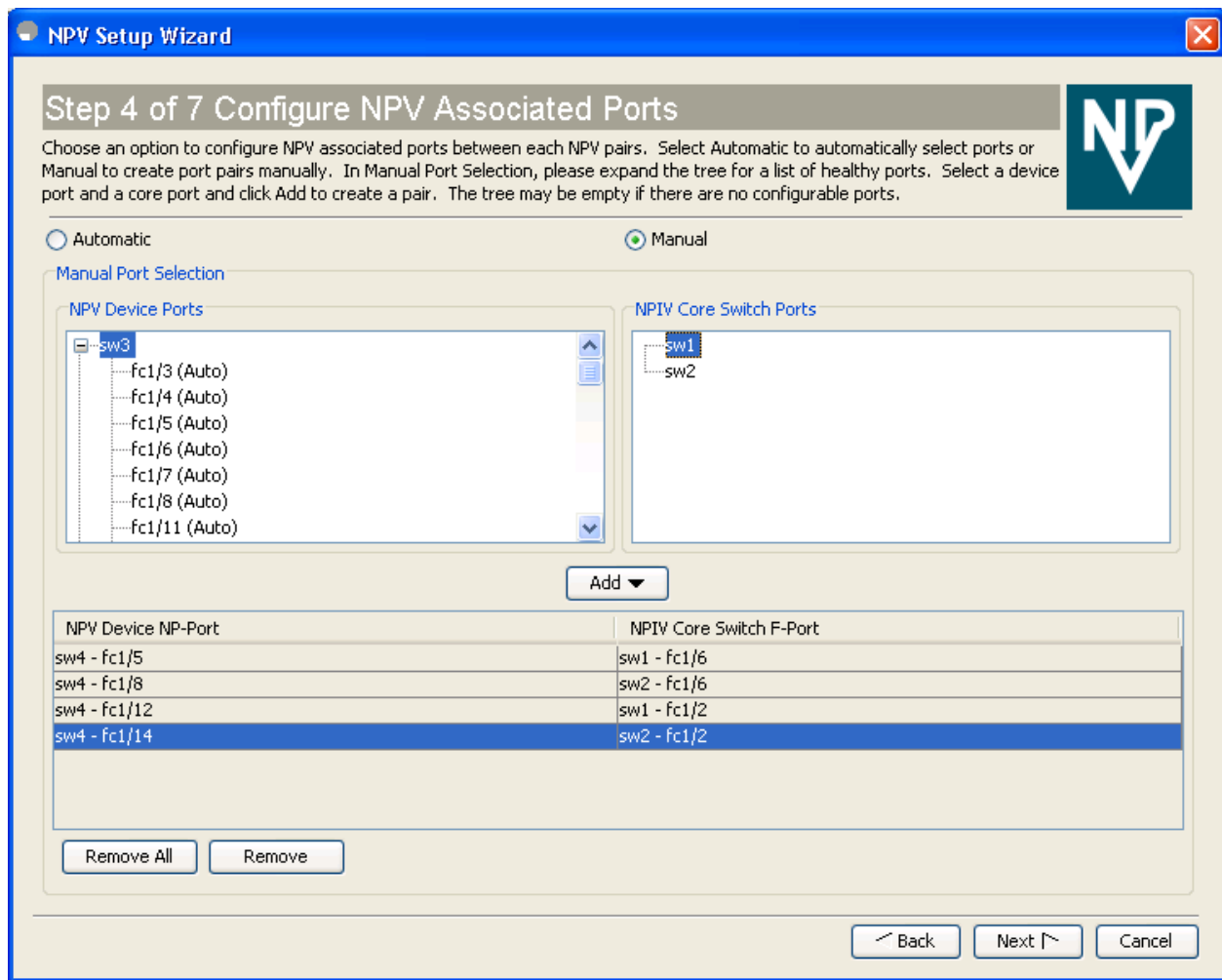
In both manual and automatic methods of Configuring NPV associated ports, the ports that are unhealthy or which are in *adminDown* state are not considered during port selection.

Figure 21-19 Warning, not Enough Number of Ports.



Send documentation comments to mdsfeedback-doc@cisco.com

Figure 21-20 Configuring NPV Associated Ports by the Manual Method.



Select the **Manual** method to manually create port pairs (see [Figure 21-20](#).) Click on a satellite switch and select the NP device port expanded under each of the NPV switches listed. Then select the required the F port on the NPIV core switch and click **Add** for them to pair.

During manual selection from the list for NPV and NPIV, ports are defined as the licensed FC ports with "Operational status" = Auto and "Status Cause" = none(2), offline(8), or sfp not present(29) and 'Operational Status' = TE or E.

Based on user selection, the wizard decides which ports are set to NP ports on the NPV device side and which are F ports on the core switch side to make an NPV connection.

Send documentation comments to mdsfeedback-doc@cisco.com

**Note**

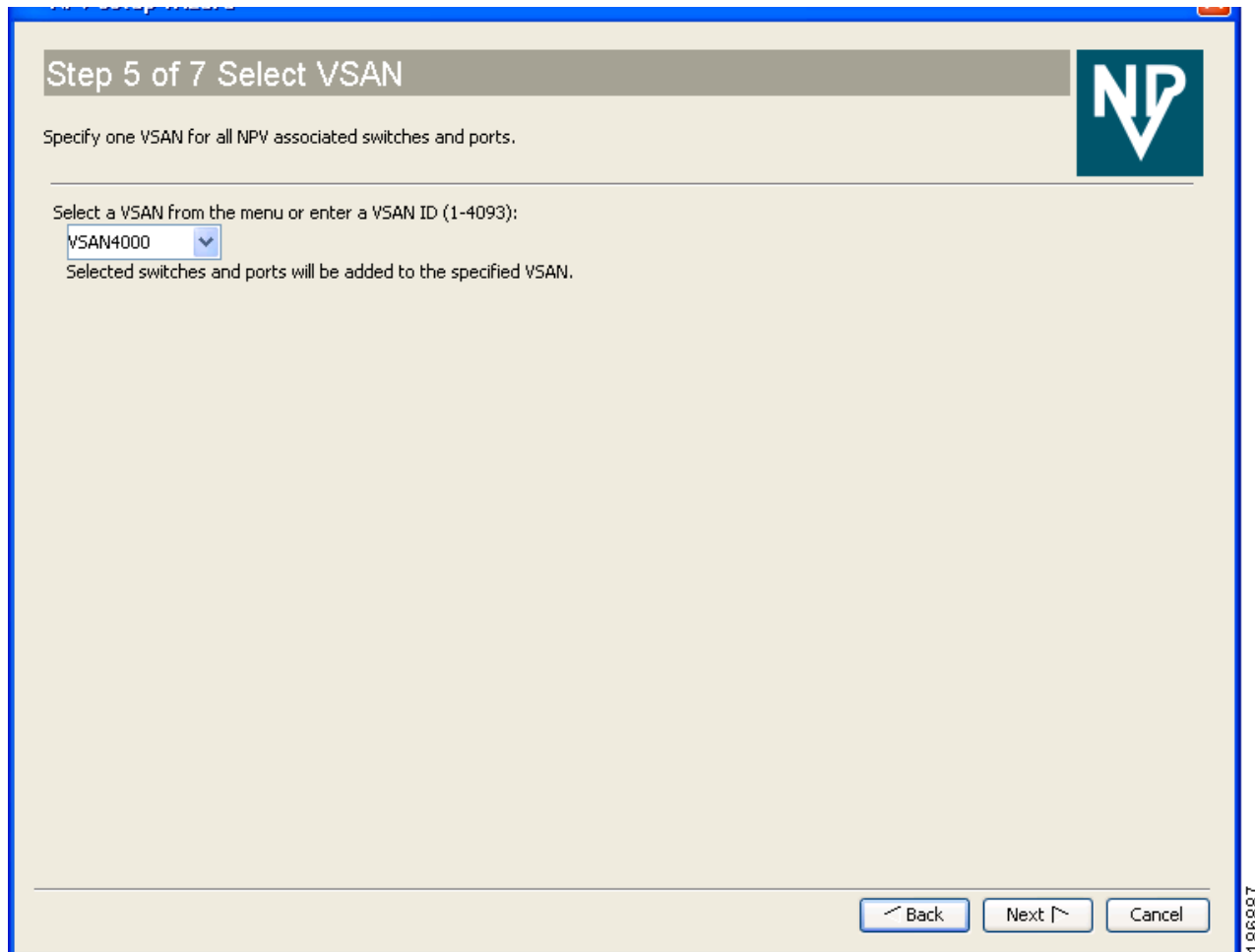
Some times the **Manual** selection in step 4 does not show any port when the NPV switch tree is expanded as the NPV Wizard filters out ports that are in fail or down status. Only healthy ports are made visible in the NPV Switch tree. Check your port settings.

Figure 21-21 Message Alert to Connect Port Pair.



Step 6 Select a VSAN as shown in [Figure 21-22](#).

Figure 21-22 Selecting a VSAN



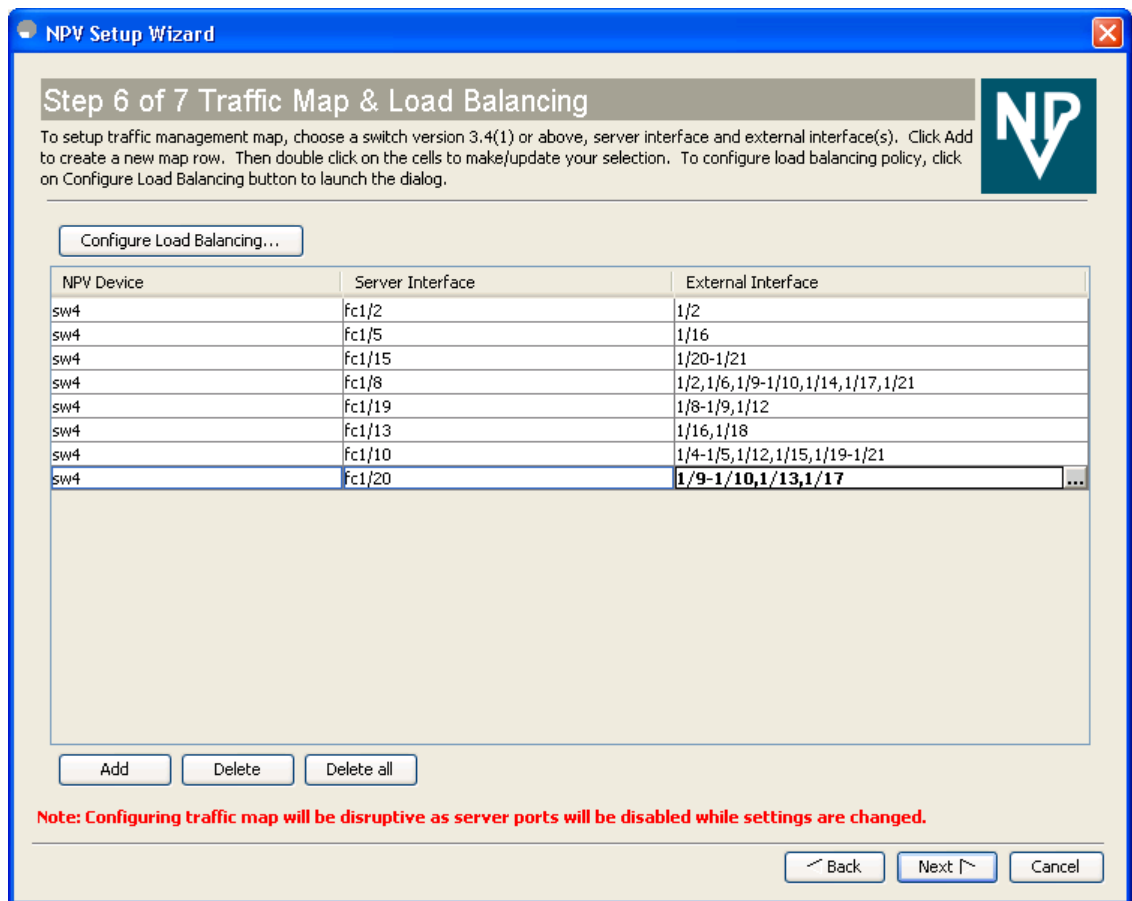
Send documentation comments to mdsfeedback-doc@cisco.com

From the drop-down list select a VSAN or enter a VSAN ID to specify the VSAN. All selected NPV devices and NPIV core switches are added to the specified VSAN. All ports on the selected NPV devices and associated ports on the NPIV core switches are added to the VSAN.

The VSAN configuration is applied in the final step.

- Step 7** Map the server interfaces with external interfaces for disruptive load balancing as shown in [Figure 21-23](#).

Figure 21-23 Mapping Server Interfaces with External Interfaces for Load Balancing

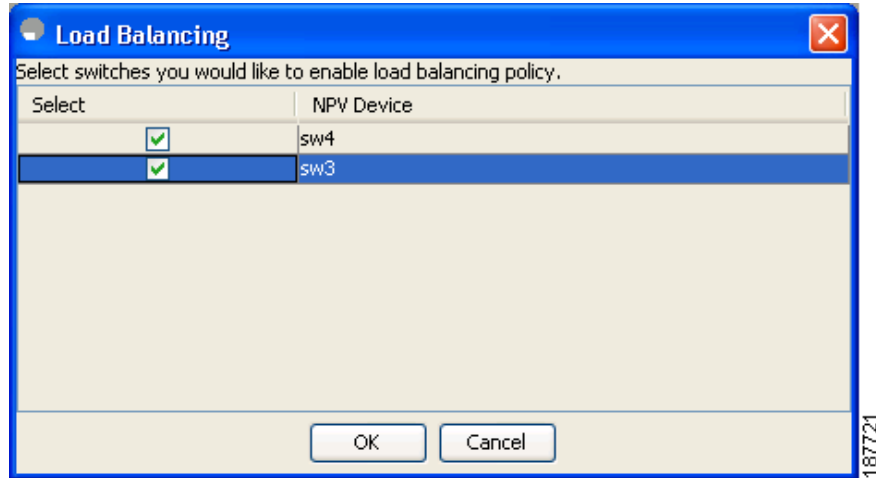


187720

Send documentation comments to mdsfeedback-doc@cisco.com

To select the NPV devices that need load balancing, click **Configure Load Balancing**, and then select the NPV devices for disruptive load balancing as shown in [Figure 21-24](#).

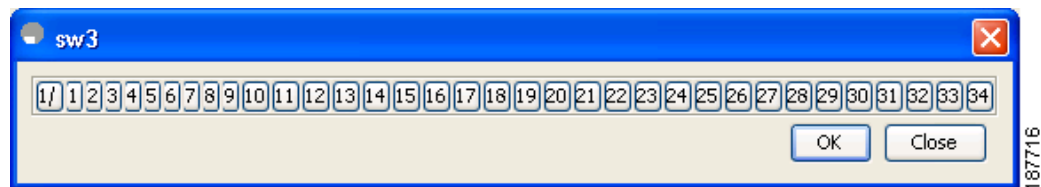
Figure 21-24 Select the NPV Devices for Load Balancing



To set up the traffic management map, select at least one switch of version 3.4(1) or above, a server interface, and external interfaces. To add a map entry, follow these steps:

- a. Click **Add** to create a new map row.
- b. Double click the NPV Device cell and select the switch from the drop-down list.
- c. Double click the Server Interface cell and then type the port numbers or click the [...] button (not available on blade server switches) in the cell to display the port selection dialog box. In the port selection dialog box, click the numbered buttons to select the ports as shown in [Figure 21-25](#).

Figure 21-25 Select the Interfaces



Note

You can select only one Server If port in a row, but multiple External IF ports can be mapped to it. Previously selected ports are disabled and cannot be selected.

- d. Double click the External Interfaces cell and type the port numbers or click the [...] button (not available on blade server switches) in the cell to display the port selection dialog box. In the port selection dialog box, click the numbered buttons to select the ports as shown in [Figure 21-25](#).

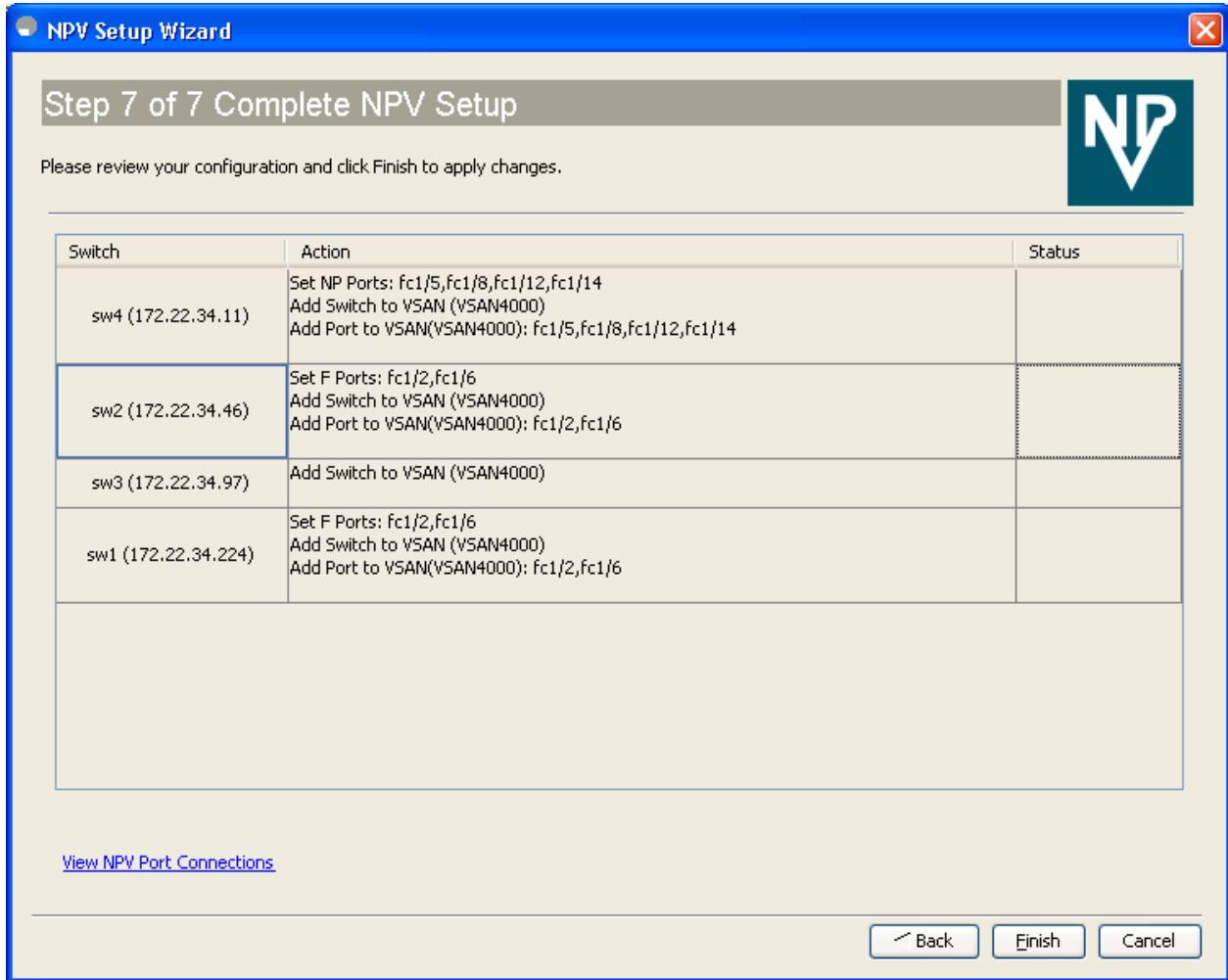
To delete an existing map entry, select the row, and then click **Delete**.

To delete all the existing map entries, click **Delete All**.

Send documentation comments to mdsfeedback-doc@cisco.com

- Step 8** Review all the NPV Setup configurations you entered in the earlier steps and click **Finish** to complete the setup as shown in [Figure 21-26](#).

Figure 21-26 Completing the NPV Setup



Enable Switch Feature lists the switches, the impending actions against them with reference to features, and the resultant status.

Set Port Type lists the switches and the ports to be set on the switches to configure NPV associate ports.

Configure VSAN lists the switches and ports to be added to the specified VSAN.

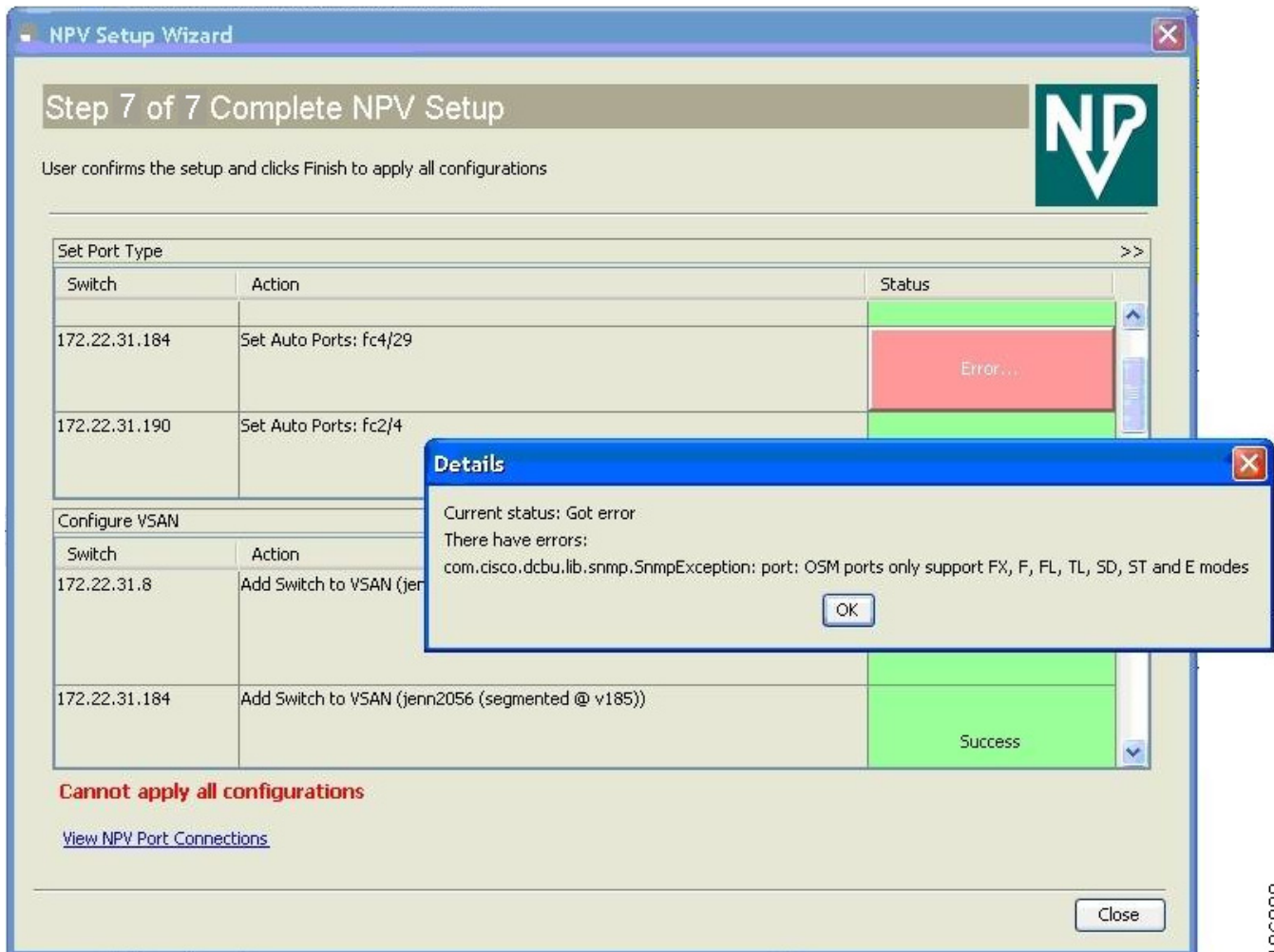
Click >> to view the expanded the panes. Click << to collapse the panes.

A progress bar at the bottom of the window indicates the overall extent of completion of the configuration tasks. A text message that runs below the progress bar indicates the current task in progress.

The status cells against each item indicate **In progress**, **Success**, and **Error** states. When a configuration cannot be applied, the status cell against the task is changed to **Error**. Click **Error** to view **Details**. A message is displayed in place of the progress bar stating, 'Cannot apply all configurations,' as shown in [Figure 21-27](#)

Send documentation comments to mdsfeedback-doc@cisco.com

Figure 21-27 Error in Applying Configurations and Details



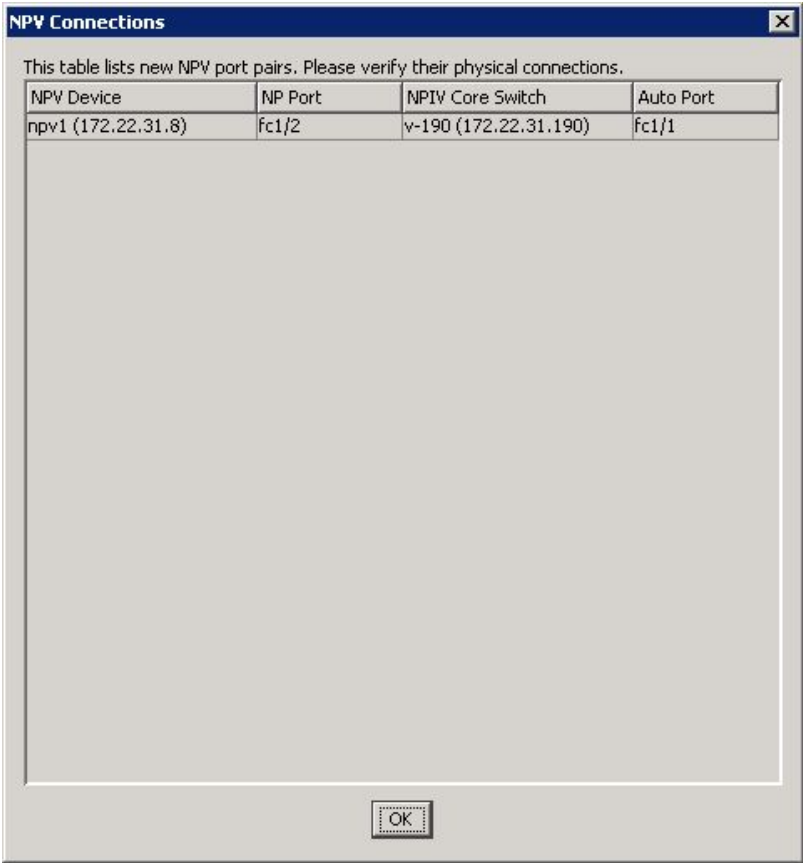
After the completion of all the tasks a link **View NPV Port Connections** is displayed in the place of the progress bar. (See [Figure 21-27](#).)

Click **View NPV Port Connections** to view the NPV port connections in a table (See [Figure 21-29](#)). Refer to this list to verify the physical connections between NP Port on NPV devices and Auto ports) on NPIV core switches. The physical connections already exist in case of the ISLs and they have to be verified. In some cases when the physical connections do not exist, they have to be established manually.

186889

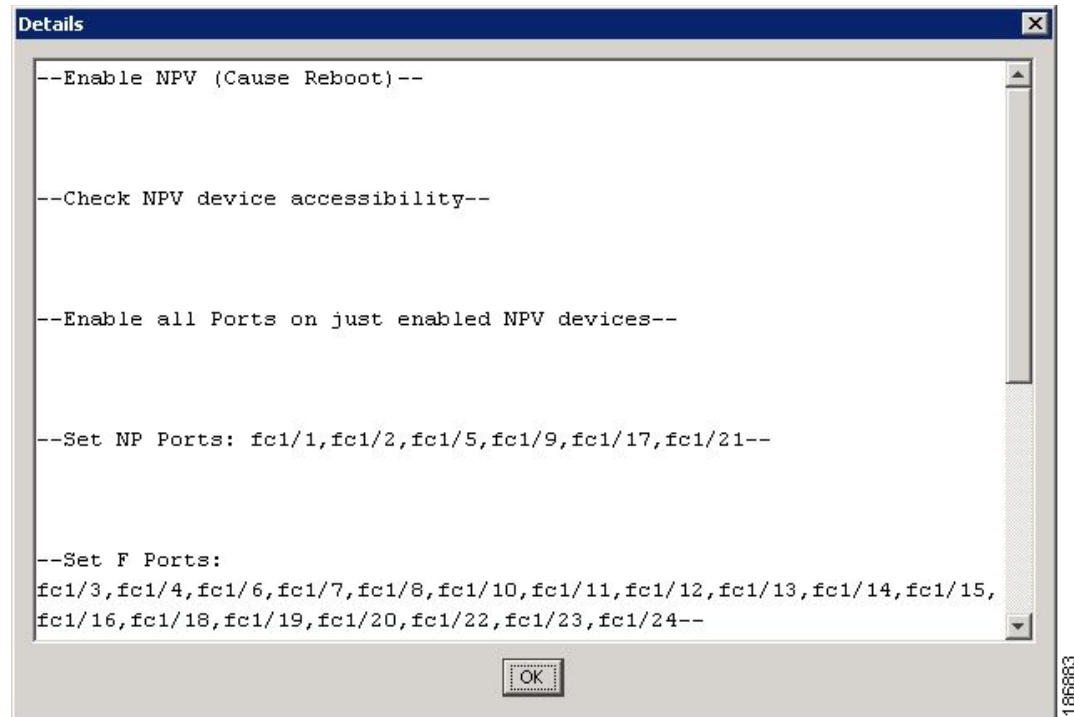
Send documentation comments to mdsfeedback-doc@cisco.com

Figure 21-28 New NPV Port Pairs



Send documentation comments to mdsfeedback-doc@cisco.com

Figure 21-29 New NPV Port Pairs, Details



DPVM Configuration

When NPV is enabled, the following requirements must be met before you configure DPVM on the NPV core switch:

- You must explicitly configure the WWN of the internal FLOGI in DPVM. If DPVM is configured on the NPV core switch for an end device that is connected to the NPV device, then that end device must be configured to be in the same VSAN. Logins from a device connected to an NPV device will fail if the device is configured to be in a different VSAN. To avoid VSAN mismatches, ensure that the internal FLOGI VSAN matches the port VSAN of the NP port.
- The first login from an NP port determines the VSAN of that port. If DPVM is configured for this first login—which is the internal login of the NPV device—then the NPV core switch’s VSAN F port is located in that VSAN. Otherwise, the port VSAN remains unchanged.

For details about DPVM configuration, see [Chapter 28, “Creating Dynamic VSANs.”](#)

NPV and Port Security

Port security is enabled on the NPV core switch on a per interface basis. To enable port security on the NPV core switch for devices logging in via NPV, you must adhere to the following requirements:

- The internal FLOGI must be in the port security database; in this way, the port on the NPV core switch will allow communications/links.
- All the end device pWWNs must also be in the port security database.

Send documentation comments to mdsfeedback-doc@cisco.com

Once these requirements are met, you can enable port security as you would in any other context. For details about enabling port security, see [Chapter 37, “Configuring Port Security.”](#)