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.

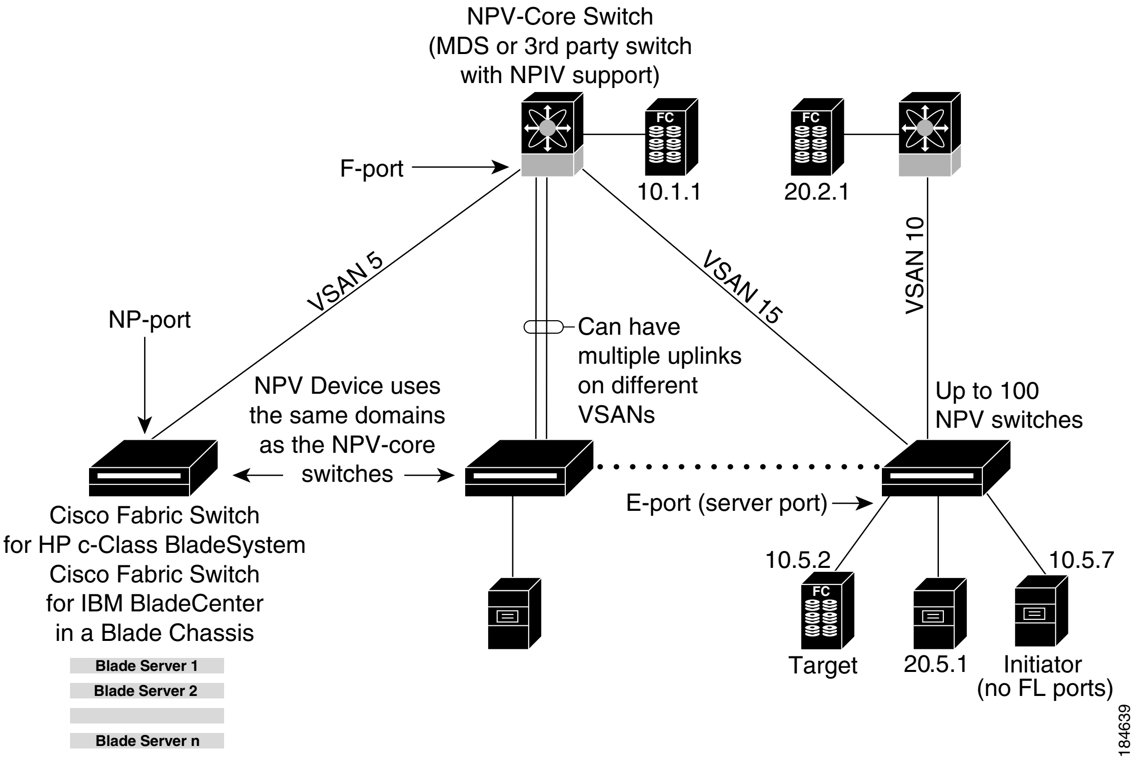
This chapter includes the following sections:

About NPV

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.

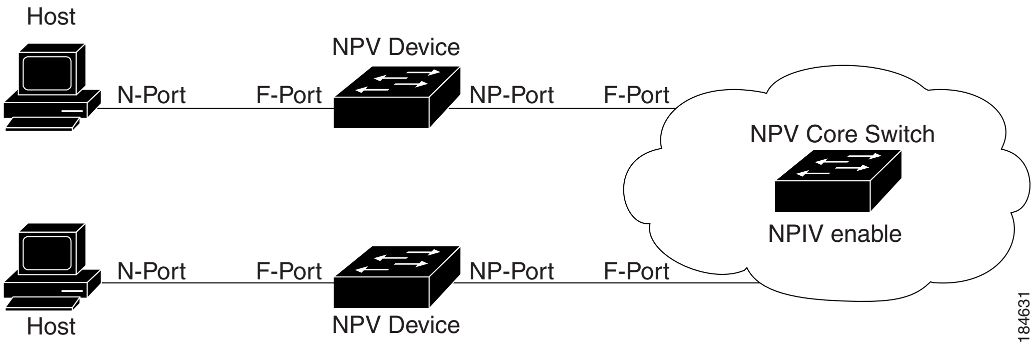
Figure 21-1 Cisco NPV Fabric Configuration



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



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.

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

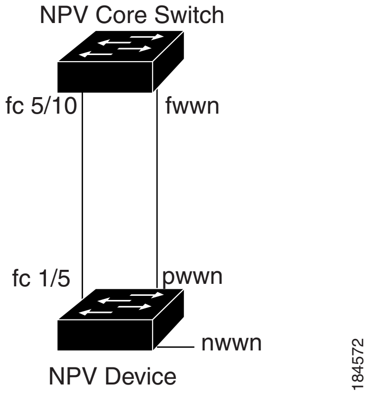


Table 21-1 identifies the internal FLOGI parameters that appear in Figure 21-3.

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, `switch: fc1/5`.
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."

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 67, "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.

:

Configuring NPV

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

Multiple VSAN Support

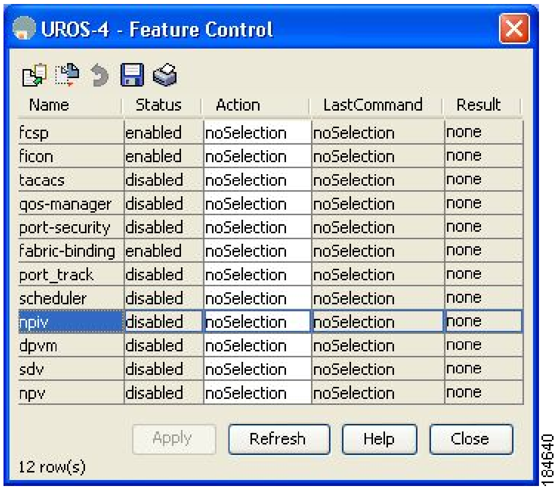
By grouping devices into different NPV sessions based on VSANs, it is possible to support multiple VSANs at the NPV-enabled switch. The correct uplink must be selected based on the VSAN(s) that the uplink can carry.

Configuring NPV with Fabric Manager

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

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.

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 prior versions, shut the F-port, enable and disable the FC domain persistency for that VSAN and then up the F-port.

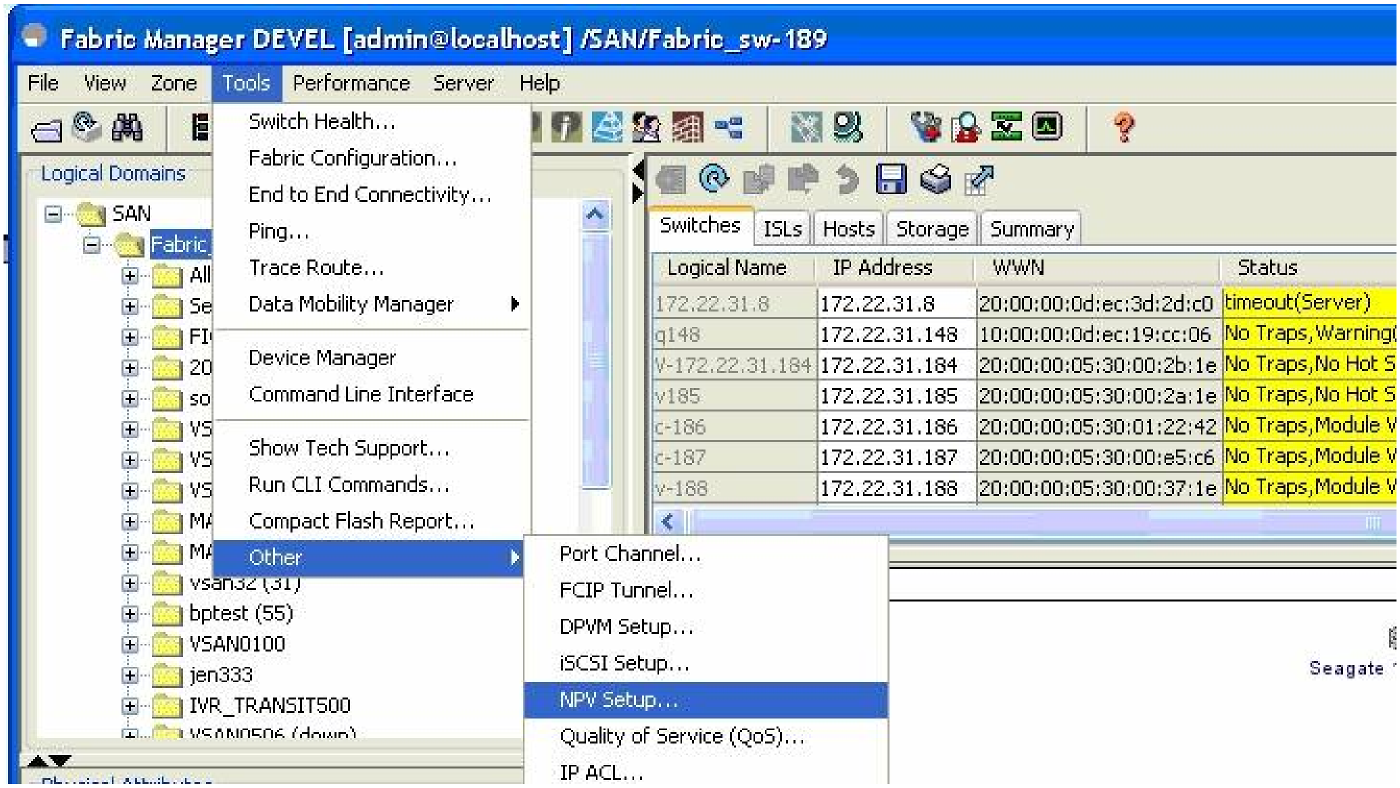
Using the NPV Setup Wizard

To configure NPV using the wizard, follow these steps:

Step 1 From the **Tools** drop-down menu select **Other**, to launch NPV Setup Wizard from Fabric Manager. (See Figure 21-5.)

From the drop-down list items in **Other**, click **NPV Setup...**

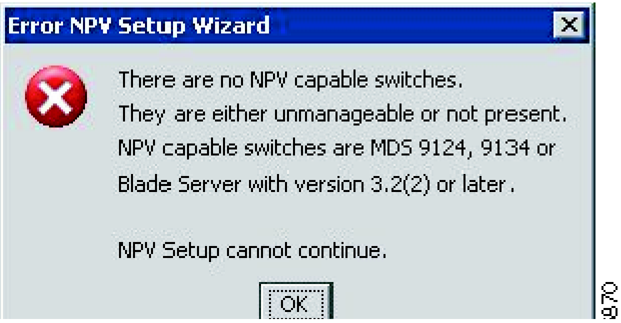
Figure 21-5 Launching NPV Setup Wizard



Logical Name	IP Address	WWN	Status
172.22.31.8	172.22.31.8	20:00:00:0d:ec:3d:2d:c0	timeout(Server)
q148	172.22.31.148	10:00:00:0d:ec:19:cc:06	No Traps,Warning(
V-172.22.31.184	172.22.31.184	20:00:00:05:30:00:2b:1e	No Traps,No Hot S
v185	172.22.31.185	20:00:00:05:30:00:2a:1e	No Traps,No Hot S
c-186	172.22.31.186	20:00:00:05:30:01:22:42	No Traps,Module V
c-187	172.22.31.187	20:00:00:05:30:00:e5:c6	No Traps,Module V
v-188	172.22.31.188	20:00:00:05:30:00:37:1e	No Traps,Module V

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 21-6.)

Figure 21-6 Error in Launching

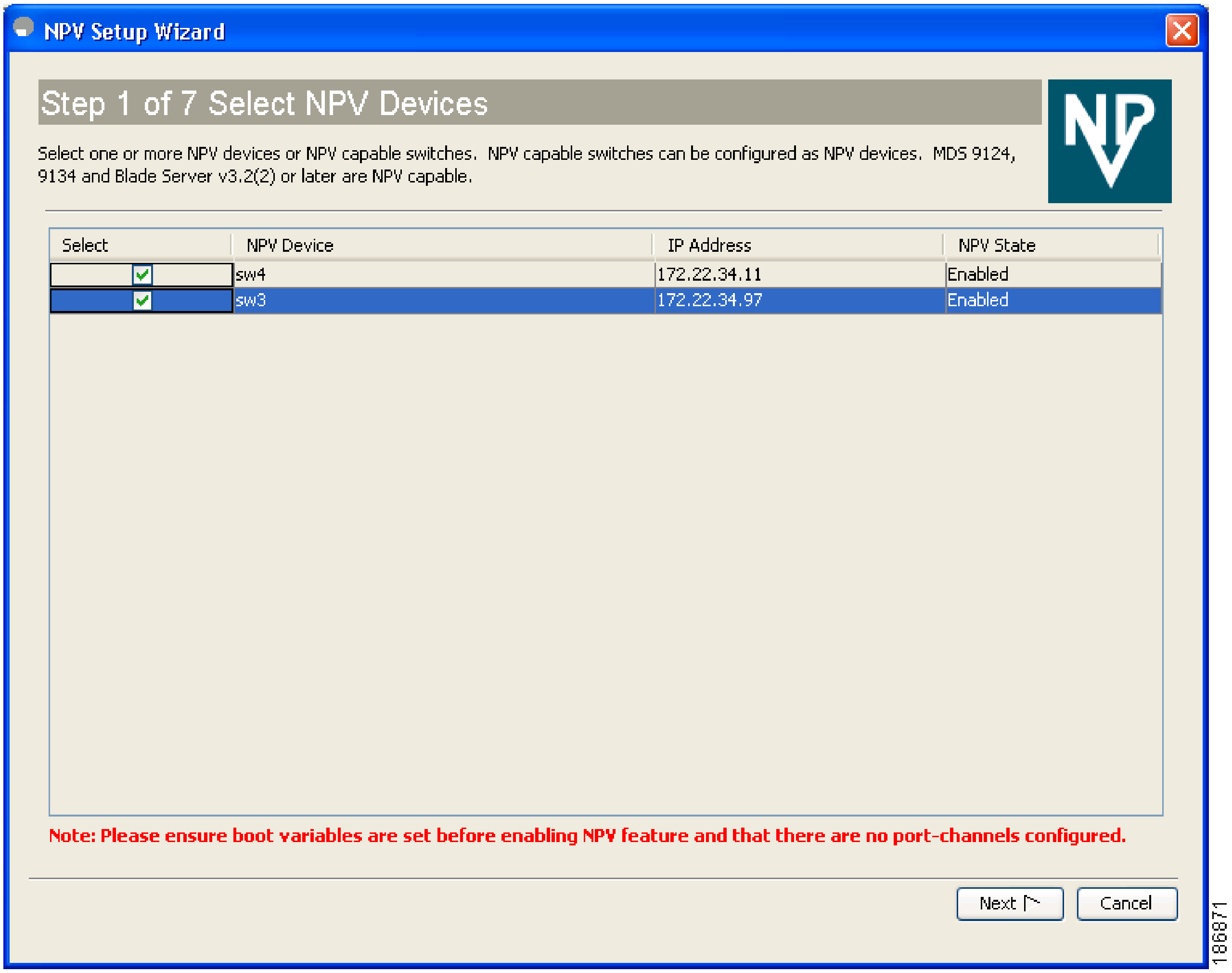


There are no NPV capable switches.
They are either unmanageable or not present.
NPV capable switches are MDS 9124, 9134 or
Blade Server with version 3.2(2) or later.

NPV Setup cannot continue.

Step 2 Select the NPV devices as shown in Figure 21-7.

Figure 21-7 Selecting the NPV Devices



NPV Setup Wizard

Step 1 of 7 Select NPV Devices

Select one or more NPV devices or NPV capable switches. NPV capable switches can be configured as NPV devices. MDS 9124, 9134 and Blade Server v3.2(2) or later are NPV capable.

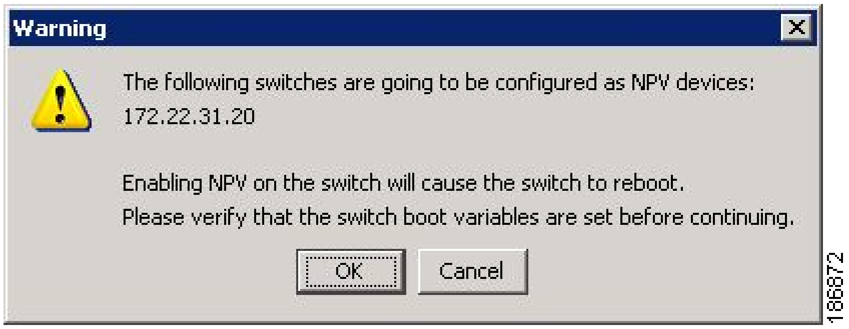
Select	NPV Device	IP Address	NPV State
☑	sw4	172.22.34.11	Enabled
☑	sw3	172.22.34.97	Enabled

Note: Please ensure boot variables are set before enabling NPV feature and that there are no port-channels configured.

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.

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 21-8.)

Figure 21-8 Warning to Enable NPV Feature on NPV-Capable Switches



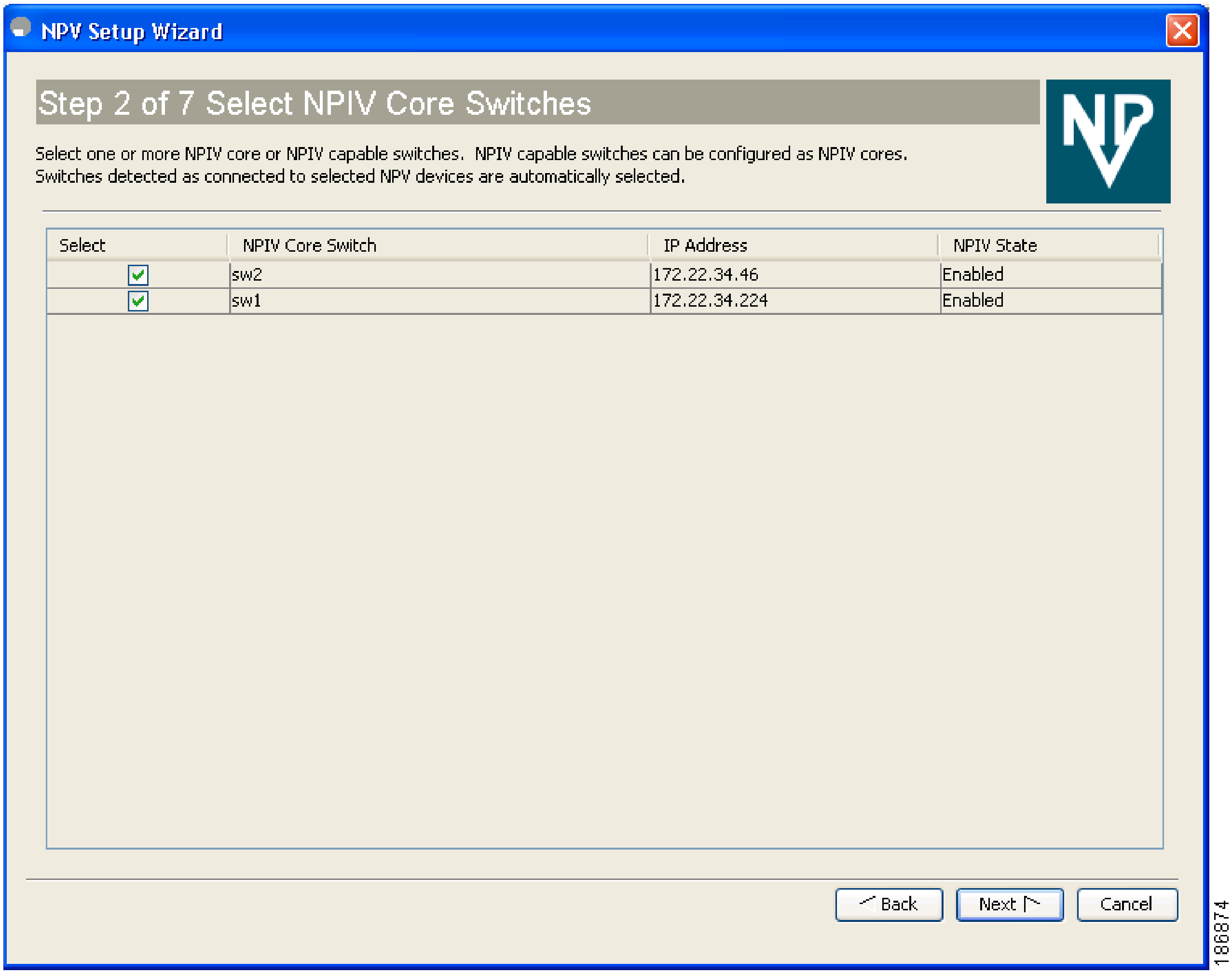
Warning

The following switches are going to be configured as NPV devices:
172.22.31.20

Enabling NPV on the switch will cause the switch to reboot.
Please verify that the switch boot variables are set before continuing.

Step 3 Select the NPIV core switches as shown in Figure 21-9.

Figure 21-9 Selecting the NPIV Core Switches



NPV Setup Wizard

Step 2 of 7 Select NPIV Core Switches

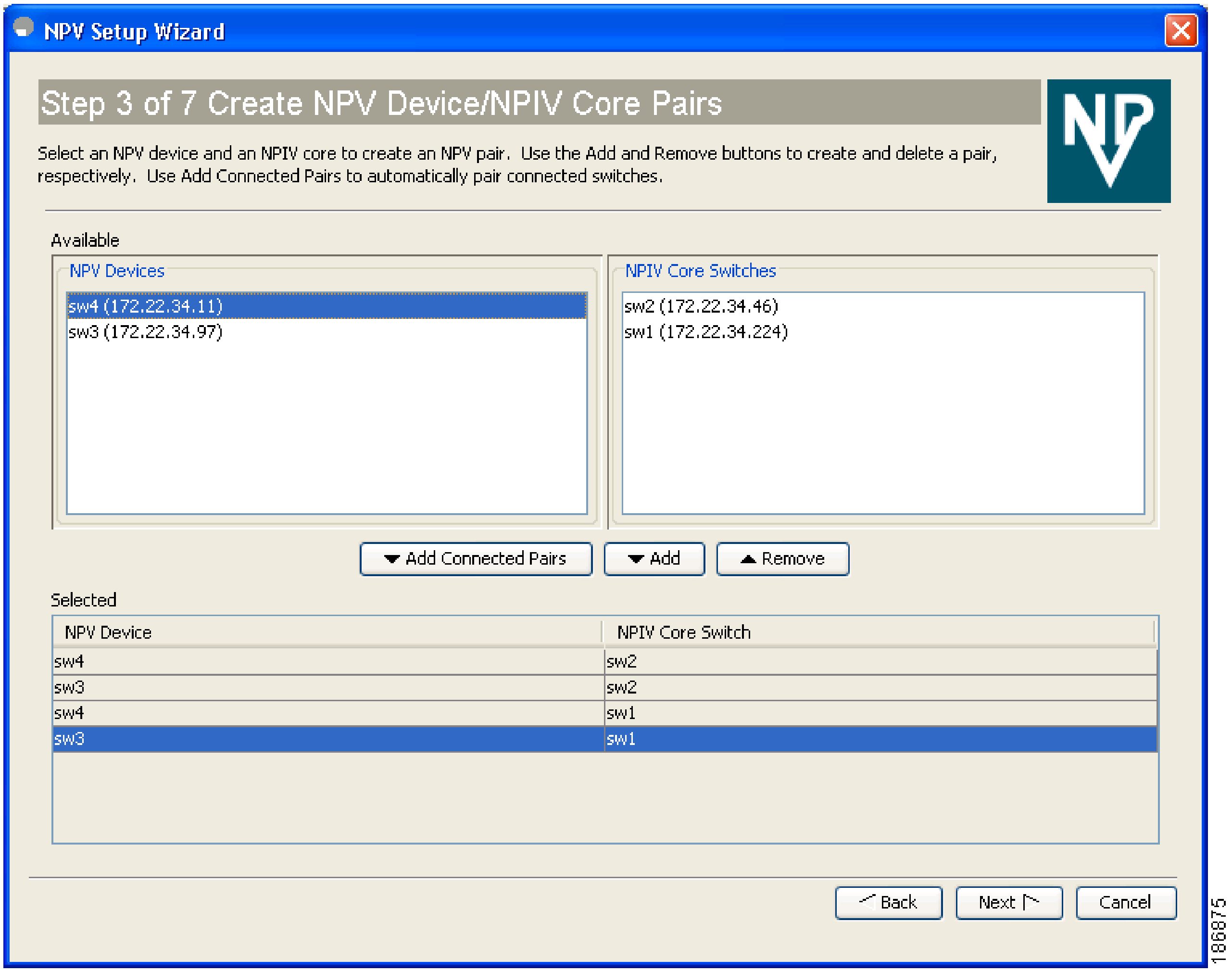
Select one or more NPIV core or NPIV capable switches. NPIV capable switches can be configured as NPIV cores.
Switches detected as connected to selected NPV devices are automatically selected.

Select	NPIV Core Switch	IP Address	NPIV State
☑	sw2	172.22.34.46	Enabled
☑	sw1	172.22.34.224	Enabled

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.

Step 4 Create new NPV device and NPIV core switch pairs as required. (See Figure 21-10.)

Figure 21-10 Creating NPV Device and NPIV Core Switch Pairs



Step 3 of 7 Create NPV Device/NPIV Core Pairs

Select an NPV device and an NPIV core to create an NPV pair. Use the Add and Remove buttons to create and delete a pair, respectively. Use Add Connected Pairs to automatically pair connected switches.

Available

NPV Devices	NPIV Core Switches
sw4 (172.22.34.11)	sw2 (172.22.34.46)
sw3 (172.22.34.97)	sw1 (172.22.34.224)

Selected

NPV Device	NPIV Core Switch
sw4	sw2
sw3	sw2
sw4	sw1
sw3	sw1

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.

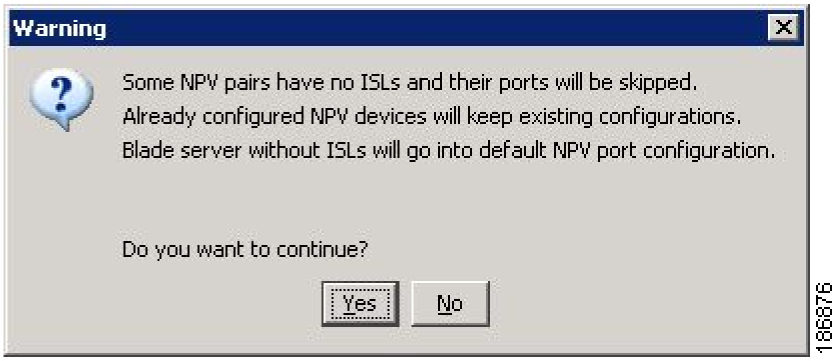
After you click the Next button in Step 3 of 6, the wizard determines if you have selected all the connected pairs. A warning message is displayed (See Figure 21-13), that lists all the connected pairs that you have not selected and warns that they will be segmented after the NPV setup.

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 21-11.)
- See Configuring Port Security, page 46-1. Remove the port channel groups if you require to select those particular ports as F Ports during the setup.

Figure 21-11 Port Channel Group detected.

Figure 21-12 Warning, NPV Setup Wizard

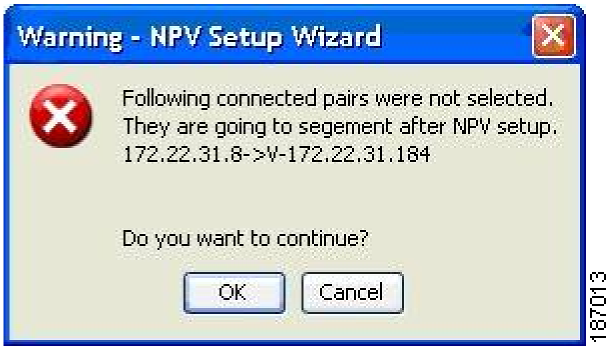


Warning

Some NPV pairs have no ISLs and their ports will be skipped.
Already configured NPV devices will keep existing configurations.
Blade server without ISLs will go into default NPV port configuration.

Do you want to continue?

Figure 21-13 Warning, NPV Setup Wizard.



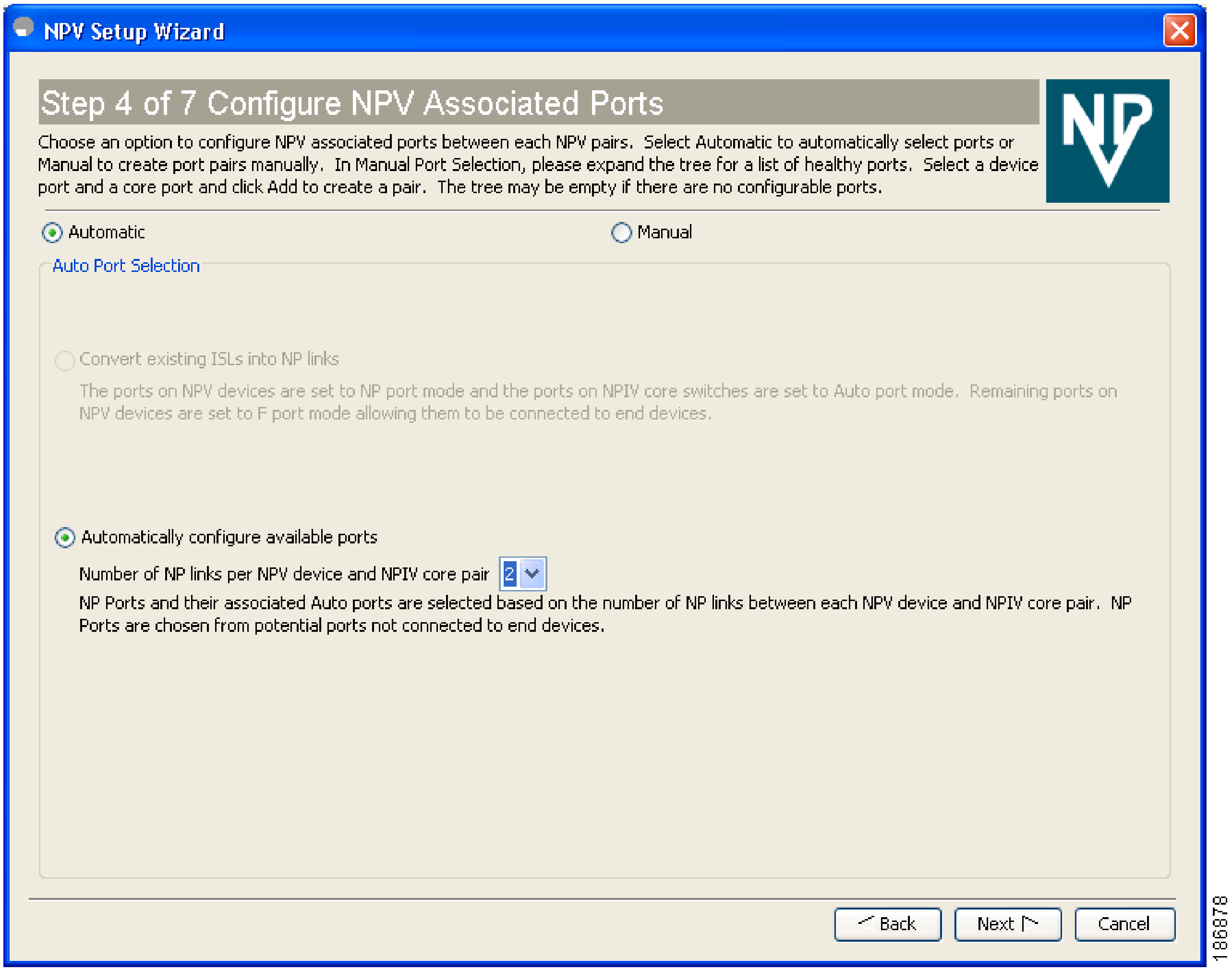
Warning - NPV Setup Wizard

Following connected pairs were not selected.
They are going to segement after NPV setup.
172.22.31.8->V-172.22.31.184

Do you want to continue?

Step 5 You can configure NPV associated ports either through automated or manual methods. (See Figure 21-14.)

Figure 21-14 Configuring NPV Associated Ports by the Automatic Method



Step 4 of 7 Configure NPV Associated Ports

Choose an option to configure NPV associated ports between each NPV pairs. Select Automatic to automatically select ports or Manual to create port pairs manually. In Manual Port Selection, please expand the tree for a list of healthy ports. Select a device port and a core port and click Add to create a pair. The tree may be empty if there are no configurable ports.

● Automatic ○ Manual

Auto Port Selection

○ Convert existing ISLs into NP links

The ports on NPV devices are set to NP port mode and the ports on NPIV core switches are set to Auto port mode. Remaining ports on NPV devices are set to F port mode allowing them to be connected to end devices.

● Automatically configure available ports

Number of NP links per NPV device and NPIV core pair: 2

NP Ports and their associated Auto ports are selected based on the number of NP links between each NPV device and NPIV core pair. NP Ports are chosen from potential ports not connected to end devices.

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.

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.

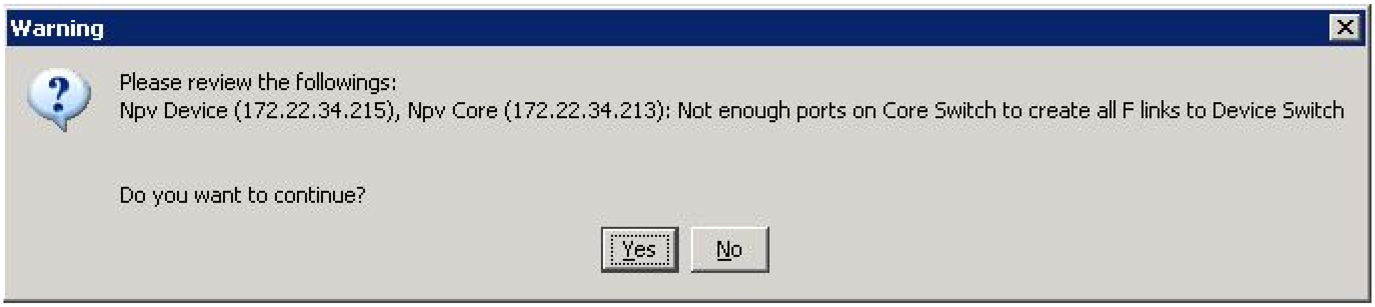
Ports on the NPIV switch are selected the following way:

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 21-15.)

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 21-15 Warning, not Enough Number of Ports.

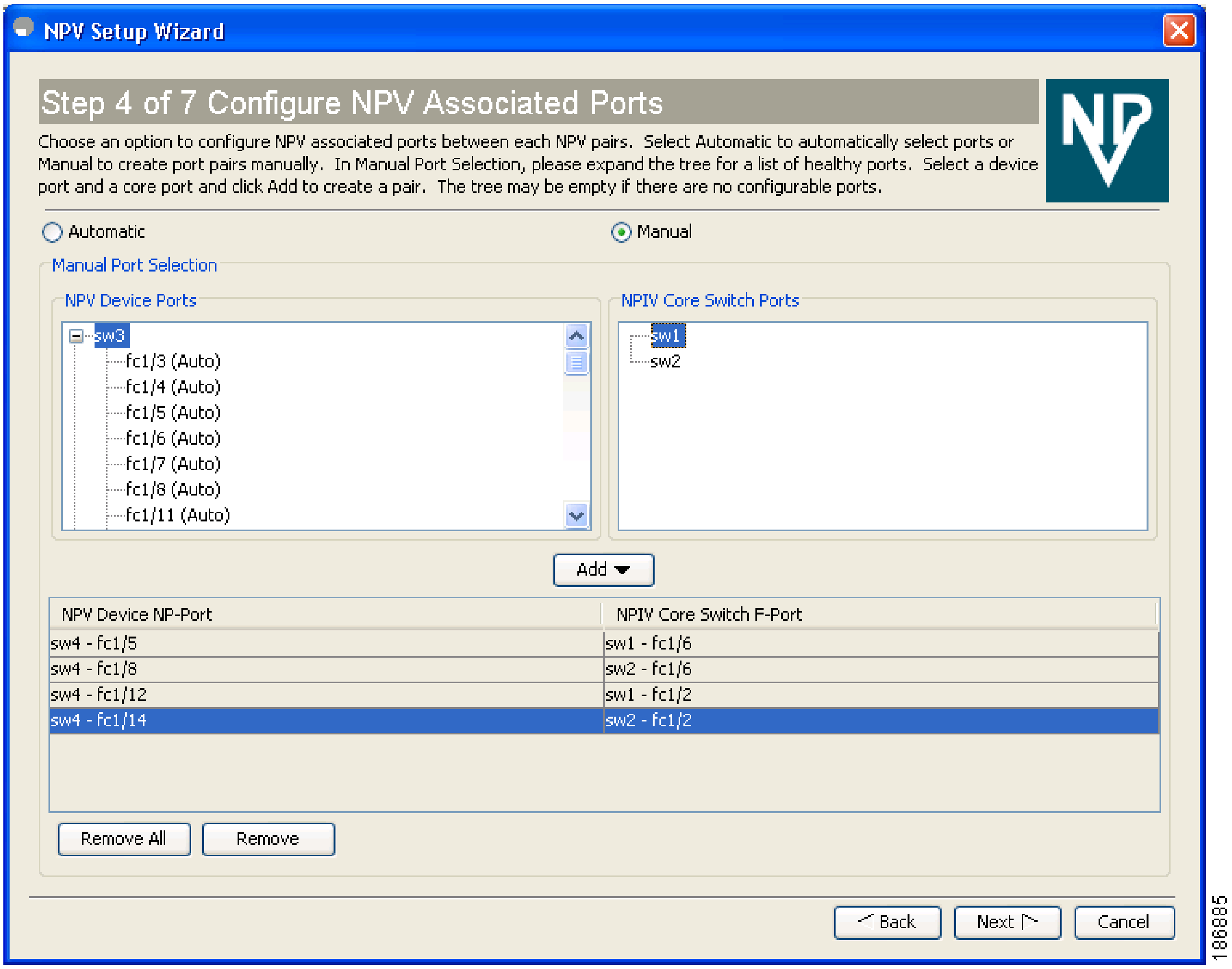


Warning

Please review the followings:
Npv Device (172.22.34.215), Npv Core (172.22.34.213): Not enough ports on Core Switch to create all F links to Device Switch

Do you want to continue?

Figure 21-16 Configuring NPV Associated Ports by manual method.



NPV Setup Wizard

Step 4 of 7 Configure NPV Associated Ports

Choose an option to configure NPV associated ports between each NPV pairs. Select Automatic to automatically select ports or Manual to create port pairs manually. In Manual Port Selection, please expand the tree for a list of healthy ports. Select a device port and a core port and click Add to create a pair. The tree may be empty if there are no configurable ports.

○ Automatic ● Manual

Manual Port Selection

NPV Device Ports

- sw3
  - fc1/3 (Auto)
  - fc1/4 (Auto)
  - fc1/5 (Auto)
  - fc1/6 (Auto)
  - fc1/7 (Auto)
  - fc1/8 (Auto)
  - fc1/11 (Auto)

NPIV Core Switch Ports

- sw1
- sw2

NPV Device NP-Port	NPIV Core Switch F-Port
sw4 - fc1/5	sw1 - fc1/6
sw4 - fc1/8	sw2 - fc1/6
sw4 - fc1/12	sw1 - fc1/2
sw4 - fc1/14	sw2 - fc1/2

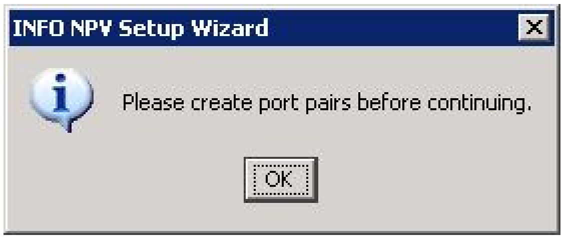
Select the **Manual** method to manually create port pairs (see Figure 21-16.) Click on a satellite switch and select the NP device port expanded under each of the NPV switches listed. Then select the required the F port on the NPIV core switch and click **Add** for them to pair.

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.

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 21-17 Message Alert to Connect Port Pair.

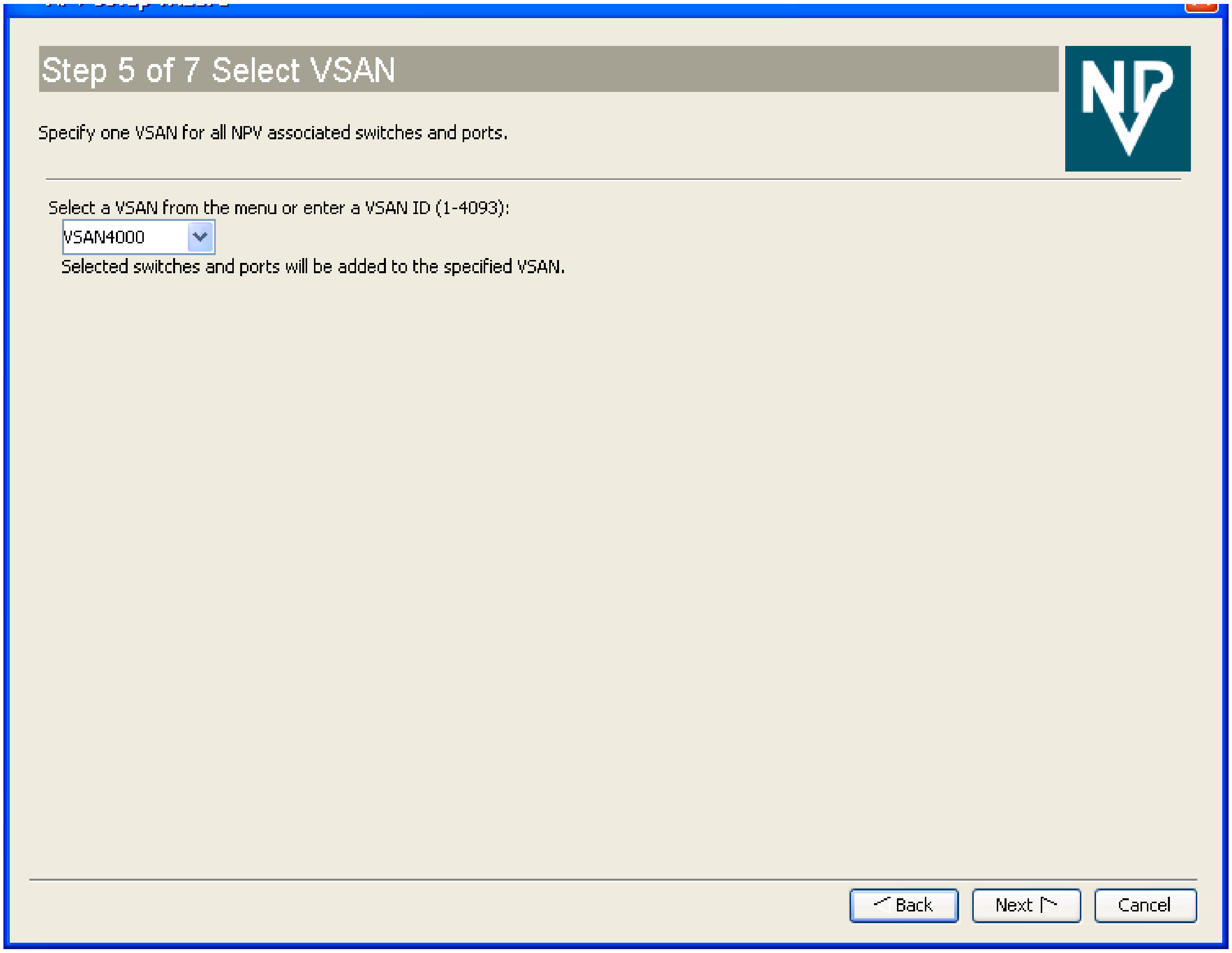


INFO NPV Setup Wizard

Please create port pairs before continuing.

Step 6 Select a VSAN as shown in Figure 21-18.

Figure 21-18 Selecting A VSAN



Step 5 of 7 Select VSAN

Specify one VSAN for all NPV associated switches and ports.

Select a VSAN from the menu or enter a VSAN ID (1-4093):

VSAN4000

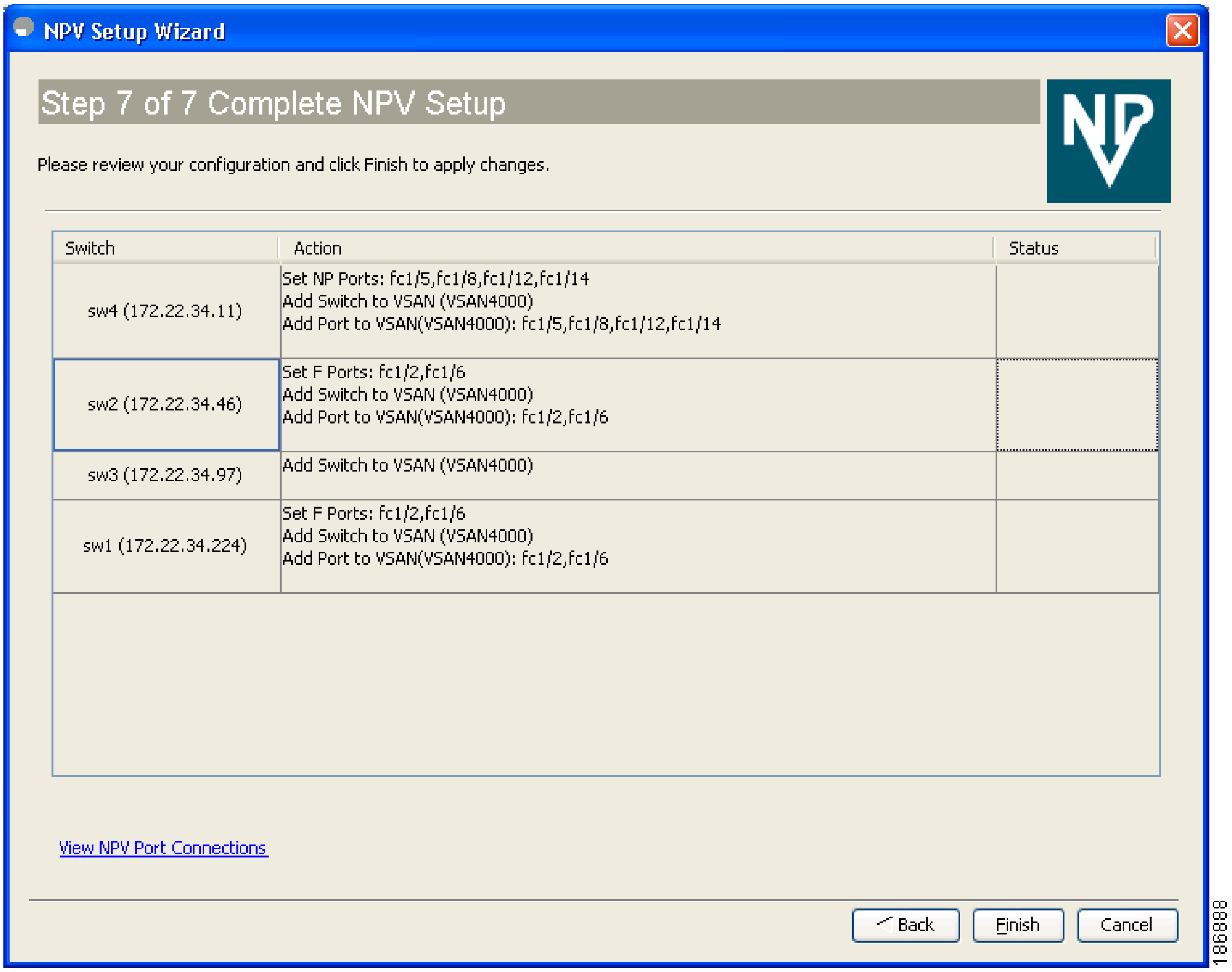
Selected switches and ports will be added to the specified VSAN.

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 Complete the NPV Setup. All the configurations captured from previous steps are shown in the respective panes in this step for confirmation as shown in Figure 21-19.

Figure 21-19 Completing the NPV Setup



NPV Setup Wizard

Step 7 of 7 Complete NPV Setup

Please review your configuration and click Finish to apply changes.

Switch	Action	Status
sw4 (172.22.34.11)	Set NP Ports: fc1/5,fc1/8,fc1/12,fc1/14 Add Switch to VSAN (VSAN4000) Add Port to VSAN(VSAN4000): fc1/5,fc1/8,fc1/12,fc1/14	
sw2 (172.22.34.46)	Set F Ports: fc1/2,fc1/6 Add Switch to VSAN (VSAN4000) Add Port to VSAN(VSAN4000): fc1/2,fc1/6	
sw3 (172.22.34.97)	Add Switch to VSAN (VSAN4000)	
sw1 (172.22.34.224)	Set F Ports: fc1/2,fc1/6 Add Switch to VSAN (VSAN4000) Add Port to VSAN(VSAN4000): fc1/2,fc1/6	

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.

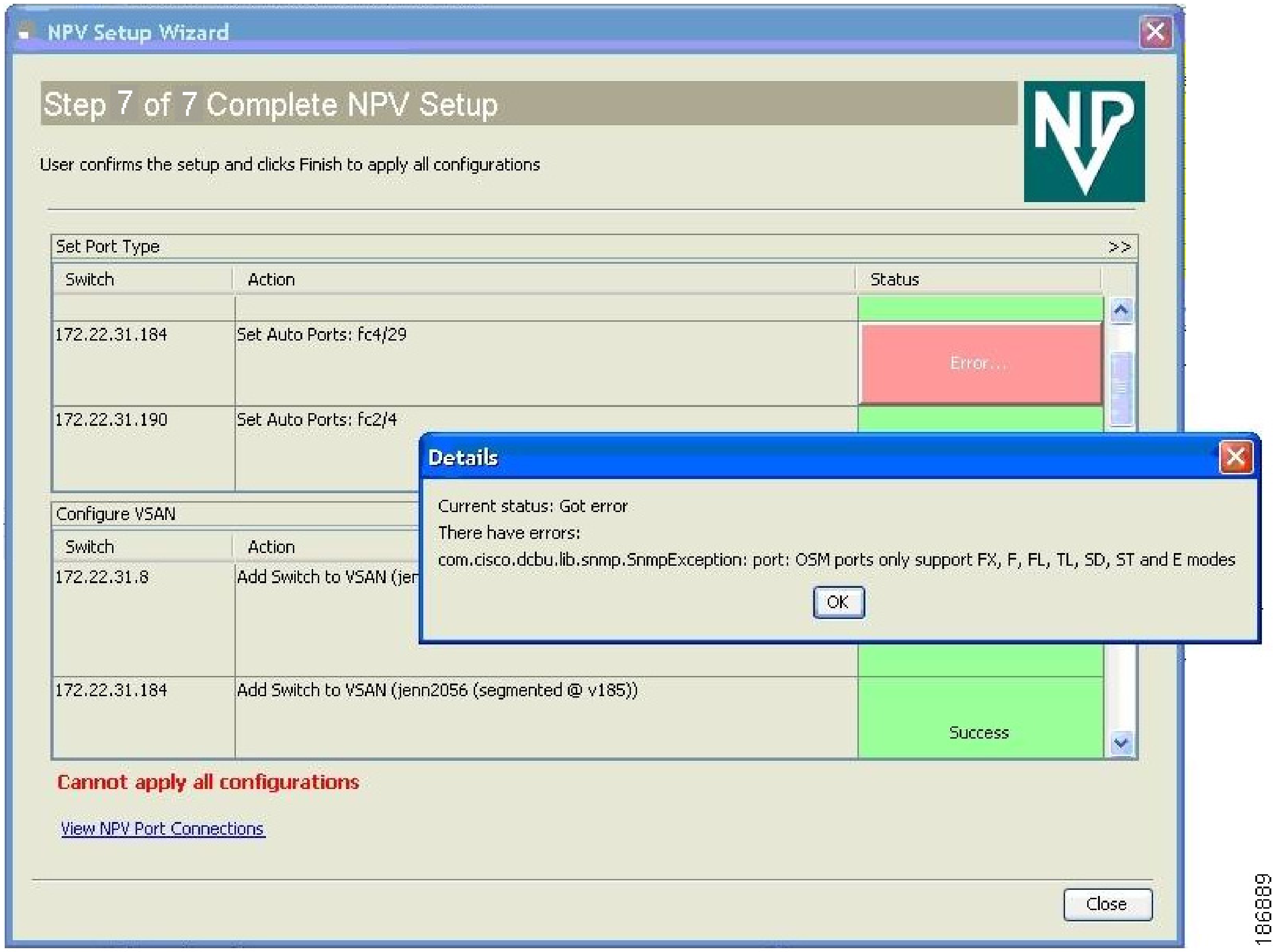
Configure VSAN lists the switches and ports to be added to the specified VSAN.

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 21-20

Figure 21-20 Error in Applying Configurations and Details



Step 7 of 7 Complete NPV Setup

User confirms the setup and clicks Finish to apply all configurations

Set Port Type

Switch	Action	Status
172.22.31.184	Set Auto Ports: fc4/29	Error...
172.22.31.190	Set Auto Ports: fc2/4	

Configure VSAN

Switch	Action	
172.22.31.8	Add Switch to VSAN (jer	
172.22.31.184	Add Switch to VSAN (jenn2056 (segmented @ v185))	Success

Details

Current status: Got error
There have errors:
com.cisco.dcbu.lib.snmp.SnmpException: port: OSM ports only support FX, F, FL, TL, SD, ST and E modes

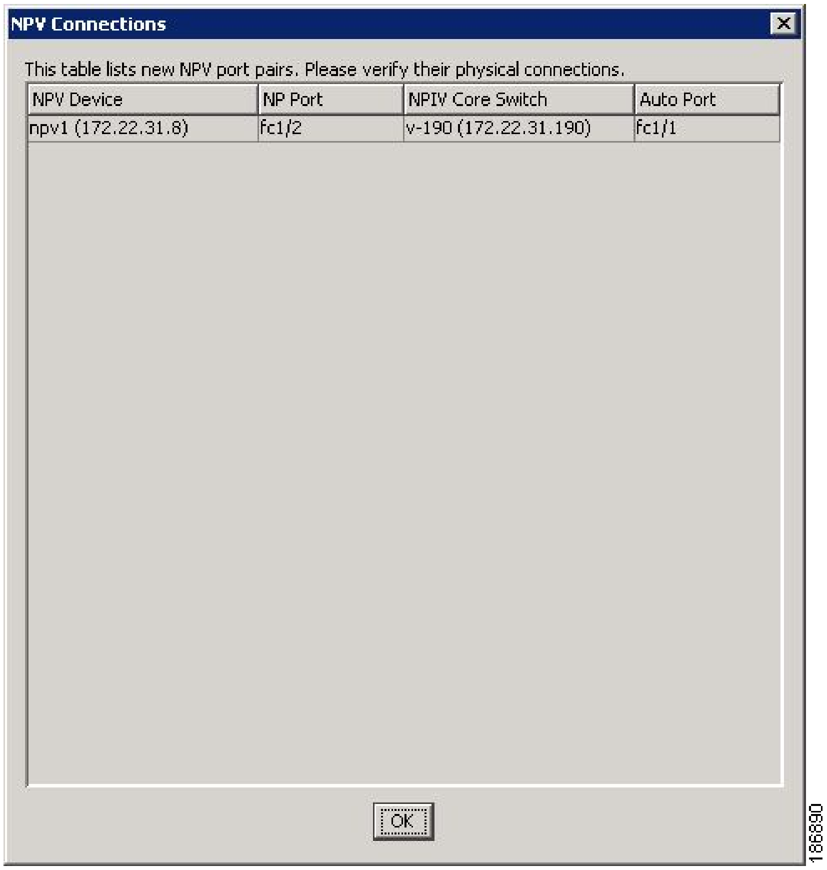
Cannot apply all configurations

View NPV Port Connections

After the completion of all the tasks a link **View NPV Port Connections** is displayed in the place of the progress bar. (See Figure 21-20.)

Click **View NPV Port Connections** to view the NPV port connections in a table (See Figure 21-22). 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.

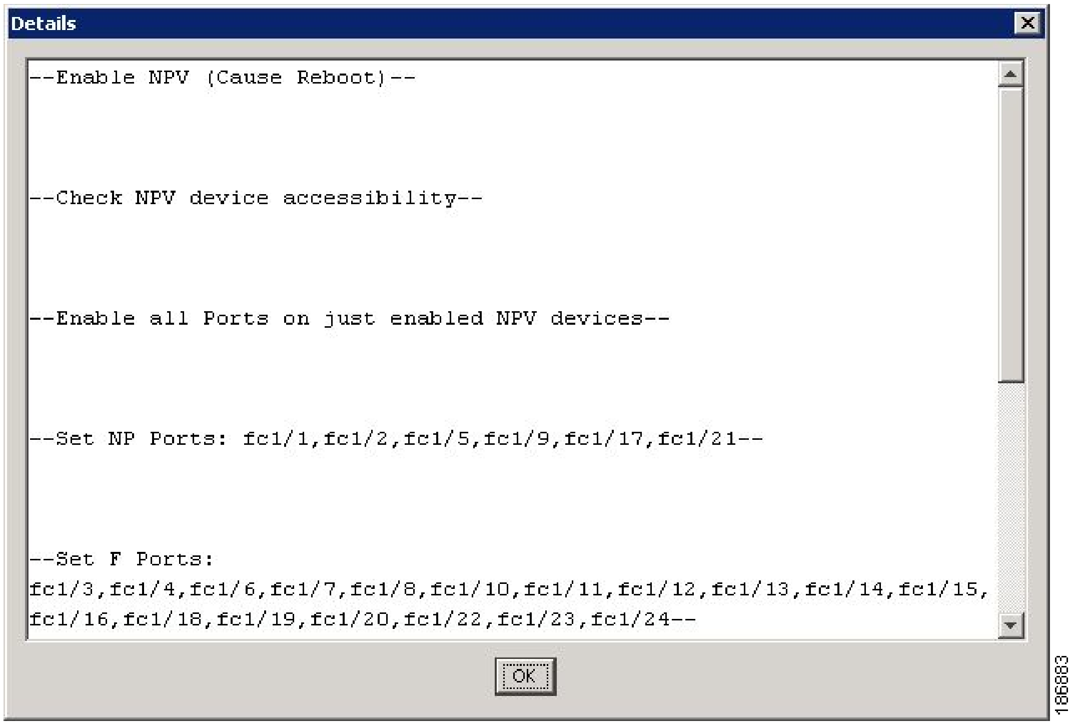
Figure 21-21 New NPV Port Pairs



This table lists new NPV port pairs. Please verify their physical connections.

NPV Device	NP Port	NPIV Core Switch	Auto Port
npv1 (172.22.31.8)	fc1/2	v-190 (172.22.31.190)	fc1/1

Figure 21-22 New NPV Port Pairs, Details



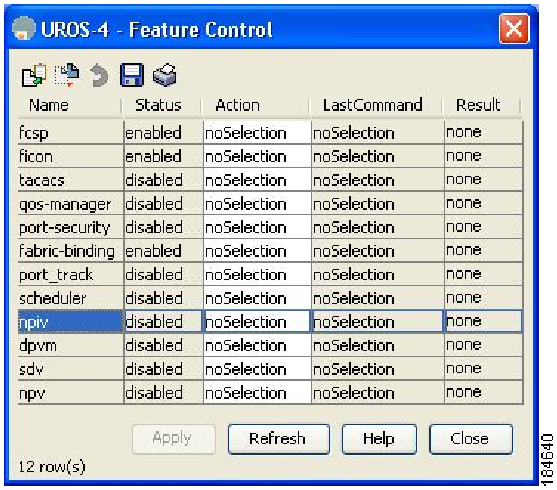
```
--Enable NPV (Cause Reboot)--


--Check NPV device accessibility--


--Enable all Ports on just enabled NPV devices--


--Set NP Ports: fc1/1,fc1/2,fc1/5,fc1/9,fc1/17,fc1/21--


--Set F Ports:
fc1/3,fc1/4,fc1/6,fc1/7,fc1/8,fc1/10,fc1/11,fc1/12,fc1/13,fc1/14,fc1/15,
fc1/16,fc1/18,fc1/19,fc1/20,fc1/22,fc1/23,fc1/24--
```

Configuring NPV with Fabric Manager

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 21-23 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)

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.

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.

Note On the 91x4 platform, before you downgrade from 3.2(2c) to prior versions, shut the F-port, enable and disable the FC domain persistency for that VSAN and then up the F-port.

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.

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 46, "Configuring Port Security."