CHAPTER 12

Configuring N-Port Virtualization

N-port virtualization (NPV) reduces the number of Fibre Channel domain IDs used in a SAN fabric. Edge switches operating in NPV mode do not join a fabric; they pass traffic between the NPV core switch and the end devices, which eliminates the need for a unique domain ID in each edge switch.

This chapter includes the following sections:

Information 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, resulting in a dramatic increase in the number of domain IDs (the maximum number supported in one SAN is 239). This challenge becomes even more difficult when a large number of blade switches are deployed in a Fibre Channel network.

NPV solves the increase in the number of domain IDs by sharing the domain ID of the NPV core switch among multiple NPV switches.

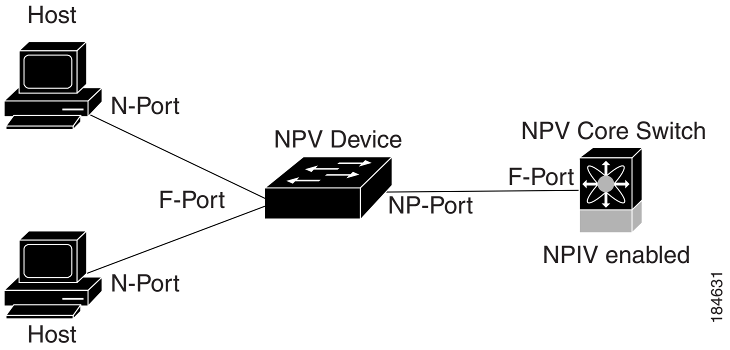
The NPV edge switch aggregates multiple locally connected N ports into one or more external NP links. The edge switch appears as a host to the core Fibre Channel switch, and as a Fibre Channel switch to the servers in the fabric switch or blade switch.

NPV reduces the need for additional ports on the core switch because multiple devices attach to the same port on the NPV core switch.

Figure 12-1 shows an interface-level view of an NPV configuration.

In Cisco Nexus 5000 Series switches, physical Fibre Channel interfaces can be NP ports or F ports. Virtual Fibre Channel interfaces can be F ports.

Figure 12-1 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 configured.

Switch operation in NPV mode is described in the following topics:

- NP Ports, page 12-2
- NP Links, page 12-2
- FLOGI Operation, page 12-2

NP Ports

An NP port (proxy N port) is a port on a switch that is in NPV mode and connected to the core NPV switch through an F port. NP ports operate as N ports that 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 switches in this NP link are converted to FDISCs.

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.

FLOGI Operation

When an NP port comes up, the Cisco Nexus 5000 Series switch first logs itself in to the NPV core switch and sends a FLOGI request that includes the following parameters:

- The fabric port WWN (fWWN) of the NP port used as the pWWN in the internal login.
- The VSAN-based switch WWN (sWWN) of the Cisco Nexus 5000 Series switch used as node WWN (nWWN) in the internal FLOGI.

After completing its FLOGI request, the Cisco Nexus 5000 Series switch registers itself with the fabric name server using the following additional parameters:

- Switch name and interface name (for example, fc2/4) 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 Cisco Nexus 5000 Series switch 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 12-2 shows the internal FLOGI flows between an NPV core switch and an NPV device.

Figure 12-2 Internal FLOGI Flows

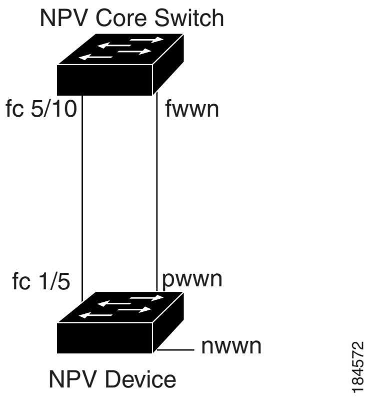


Table 12-1 identifies the internal FLOGI parameters that appear in Figure 12-2.

Table 12-1 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 read “switch.” For example, switch: fc2/3.
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 of these factors:

- Zoning is not enforced at the NPV device (rather, it is enforced on the NPV core switch).
- Multiple devices attached to an NPV device log in through the same F port on the core, so they 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.

Guidelines and Limitations

The following are recommended guidelines and requirements when deploying NPV:

- 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, domain or port of the NPV core switch should be used.
- Port tracking is supported in NPV mode. See the "Information About Port Tracking" section on page 27-1.
- Port security is supported on the NPV core switch for devices logged in through the NPV switch. 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 through an NPV switch, 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 and links.
  - All the end device pWWNs must also be in the port security database.

  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 VSANs that the uplink can carry.
- 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 an end device to a specific core switch link.
- If a server interface goes down and then returns to service, the interface may not be assigned to the same core switch link.
- The server interface is only operational when its assigned core switch link is operational.
- Both servers and targets can be connected to the switch when in NPV mode.
- Local switching is not supported; all traffic is switched in 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.

Configuring NPV

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

Note We recommend that you save your current configuration either in boot flash memory or to a TFTP server before NPV (if the configuration is required for later use).

Configuring NPV with Device Manager

To use Device Manager to configure NPV, perform this task:

Step 1 Launch Device Manager from the Cisco Nexus 5000 Series switch to enable NPV.

Step 2 From the Admin drop-down menu, choose **Feature Control**. In the **Action** field, choose **enable** for the NPV feature and click **Apply**.

Step 3 From the Interface drop-down list, choose **FC All** to configure the external interfaces on the NPV device.

Step 4 In the Mode Admin column, choose the **NP** port mode for each external interface and click **Apply**.

Step 5 To configure the server interfaces on the Cisco Nexus 5000 Series switch, from the Interface drop-down list, choose **FC All**.

Step 6 In the Mode Admin column, choose **F** port mode for each server interface and click **Apply**.

Step 7 The default Admin status is **down**. After configuring port modes, you must choose **up** Admin Status to bring up the links.