Configuring N Port Virtualization

This chapter contains the following sections:

Configuring N Port Virtualization

Information About NPV

NPV Overview

By default, Cisco Nexus devices switches operate in fabric mode. In this mode, the switch provides standard Fibre Channel switching capability and features.

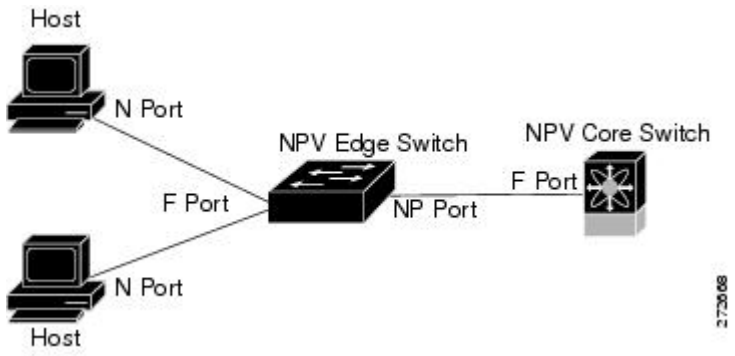
In fabric mode, each switch that joins a SAN is assigned a domain ID. Each SAN (or VSAN) supports a maximum of 239 domain IDs, so the SAN has a limit of 239 switches. In a SAN topology with a large number of edge switches, the SAN may need to grow beyond this limit. NPV alleviates the domain ID limit by sharing the domain ID of the core switch among multiple edge switches.

In NPV mode, the edge switch relays all traffic from server-side ports to the core switch. The core switch provides F port functionality (such as login and port security) and all the Fibre Channel switching capabilities.

The edge switch appears as a Fibre Channel host to the core switch and as a regular Fibre Channel switch to its connected devices.

The following figure shows an interface-level view of an NPV configuration.

Figure 1: NPV Interface Configuration



NPV Mode

In NPV mode, the edge switch relays all traffic to the core switch, which provides the Fibre Channel switching capabilities. The edge switch shares the domain ID of the core switch.

To convert a switch into NPV mode, you set the NPV feature to enabled. This configuration command automatically triggers a switch reboot. You cannot configure NPV mode on a per-interface basis. NPV mode applies to the entire switch.

In NPV mode, a subset of fabric mode CLI commands and functionality is supported. For example, commands related to fabric login and name server registration are not required on the edge switch, because these functions are provided in the core switch. To display the fabric login and name server registration databases, you must enter the **show flogi database** and **show fcns database** commands on the core switch.

Server Interfaces

Server interfaces are F ports on the edge switch that connect to the servers. A server interface may support multiple end devices by enabling the N port identifier virtualization (NPIV) feature. NPIV provides a means to assign multiple FC IDs to a single N port, which allows the server to assign unique FC IDs to different applications.

Note To use NPIV, enable the NPIV feature and reinitialize the server interfaces that will support multiple devices.

In Cisco Nexus devices, server interfaces can be virtual Fibre Channel interfaces.

Related Topics

Configuring N Port Virtualization, on page 1

NP Uplinks

All interfaces from the edge switch to the core switch are configured as proxy N ports (NP ports).

An NP uplink is a connection from an NP port on the edge switch to an F port on the core switch. When an NP uplink is established, the edge switch sends a fabric login message (FLOGI) to the core switch, and then (if the FLOGI is successful) it registers itself with the name server on the core switch. Subsequent FLOGIs from end devices connected to this NP uplink are forwarded as-is to the core switch.

Note In the switch CLI configuration commands and output displays, NP uplinks are called External Interfaces.

In Cisco Nexus devices, NP uplink interfaces are virtual Fibre Channel interfaces.

Related Topics

Fabric Login

FLOGI Operation

When an NP port becomes operational, the switch first logs itself in to the core switch by sending a FLOGI request (using the port WWN of the NP port).

After completing the FLOGI request, the switch registers itself with the fabric name server on the core switch (using the symbolic port name of the NP port and the IP address of the edge switch).

The following table identifies port and node names in the edge switch used in NPV mode.

Table 1: Edge Switch FLOGI Parameters

Parameter	Derived From
pWWN	The fWWN of the NP port on the edge switch.
nWWN	The VSAN-based sWWN of the edge switch.
symbolic port name	The edge switch name and NP port interface string. **Note** If no switch name is available, the output will read "switch." For example, switch: fc 1/5.
IP address	The IP address of the edge switch.
symbolic node name	The edge switch name.

We do not recommend using fWWN-based zoning on the edge switch for the following reasons:

- Zoning is not enforced at the edge switch (rather, it is enforced on the core switch).
- Multiple devices attached to an edge switch 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.

Related Topics

Information About Zones

NPV Traffic Management Guidelines

When deploying NPV traffic management, follow these guidelines:

- Use NPV traffic management only when automatic traffic engineering does not meet your network requirements.
- You do not need to configure traffic maps for all server interfaces. By default, NPV will use automatic traffic management.

NPV Guidelines and Limitations

When configuring NPV, note the following guidelines and limitations:

- In-order data delivery is not required in NPV mode because the exchange between two end devices always takes the same uplink from the edge switch to the core. Upstream of the edge switch, core switches will enforce in-order delivery if configured.
- You can configure zoning for end devices that are connected to edge switches using all available member types on the core switch. For fWWN, sWWN, domain, or port-based zoning, use the fWWN, sWWN, domain, or port of the core switch in the configuration commands.
- Port tracking is not supported in NPV mode.
- Port security is supported on the core switch for devices logged in through the NPV switch. Port security is enabled on the core switch on a per-interface basis. To enable port security on the core switch for devices that log 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 core switch will allow communications and links.
  - All the end device pWWNs must also be in the port security database.
- Servers can be connected to the switch when in NPV mode.
- When initiators and targets are assigned to the same border port (NP or NP-PO), then Cisco Nexus 5000 Series switches in NPIV mode do not support hairpinning.
- Fibre Channel switching is not performed in the edge switch; all traffic is switched in the core switch.
- NPV supports NPIV-capable servers. This capability is called nested NPIV.
- Connecting two Cisco NPV switches together is not supported.
- Only VF and VNP port types are supported in NPV mode.

Configuring NPV

Enabling NPV

When you enable NPV, the system configuration is erased and the switch reboots.

Note We recommend that you save your current configuration either in boot flash memory or to a TFTP server before you enable NPV.

To enable NPV, perform this task:

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters configuration mode.
Step 2	switch(config)# **npv enable**	Enables NPV mode. The switch reboots, and it comes back up in NPV mode. **Note** A write-erase is performed during the initialization.
Step 3	switch(config-npv)# **no npv enable**	Disables NPV mode, which results in a reload of the switch.

Configuring NPV Interfaces

After you enable NPV, you should configure the NP uplink interfaces and the server interfaces.

Configuring an NP Interface

After you enable NPV, you should configure the NP uplink interfaces and the server interfaces. To configure an NP uplink interface, perform this task:

To configure a server interface, perform this task:

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **interface vfc** *vfc-id*	Selects an interface that will be connected to the core NPV switch.

	Command or Action	Purpose
Step 3	switch(config-if)# **switchport mode NP**	Configures the interface as an NP port.
Step 4	switch(config-if)# **no shutdown**	Brings up the interface.

Configuring a Server Interface

To configure a server interface, perform this task:

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **interface vfc** *vfc-id*	Selects an interface that will be connected to the core NPV switch.
Step 3	switch(config-if)# **switchport mode F**	Configures the interface as an F port.
Step 4	switch(config-if)# **no shutdown**	Brings up the interface.

Configuring NPV Traffic Management

Configuring NPV Traffic Maps

An NPV traffic map associates one or more NP uplink interfaces with a server interface. The switch associates the server interface with one of these NP uplinks.

Note If a server interface is already mapped to an NP uplink, you should include this mapping in the traffic map configuration.

To configure a traffic map, perform this task:

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.

	Command or Action	Purpose
Step 2	switch(config)# **npv traffic-map server-interface vfc** *vfc-id* **external-interface vfc** *vfc-id*	Configures a mapping between a server interface (or range of server interfaces) and an NP uplink interface (or range of NP uplink interfaces).
Step 3	switch(config)# **no npv traffic-map server-interface vfc** *vfc-id* **external-interface vfc** *vfc-id*	Removes the mapping between the specified server interfaces and NP uplink interfaces.

Enabling Disruptive Load Balancing

If you configure additional NP uplinks, you can enable the disruptive load-balancing feature to distribute the server traffic load evenly among all the NP uplinks.

To enable disruptive load balancing, perform this task:

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters configuration mode on the NPV.
Step 2	switch(config)# **npv auto-load-balance disruptive**	Enables disruptive load balancing on the switch.
Step 3	switch (config)# **no npv auto-load-balance disruptive**	Disables disruptive load balancing on the switch.

Verifying NPV

To display information about NPV, perform the following task:

Procedure

	Command or Action	Purpose
Step 1	switch# **show npv flogi-table** [**all**]	Displays the NPV configuration.

Verifying NPV Examples

To display a list of devices on a server interface and their assigned NP uplinks, enter the **show npv flogi-table** command on the Cisco Nexus device:

```
switch# show npv flogi-table
--------------------------------------------------------------------------------
SERVER                                                                          EXTERNAL
INTERFACE VSAN FCID            PORT NAME               NODE NAME               INTERFACE
--------------------------------------------------------------------------------
vfc31     1    0xee0008 10:00:00:00:c9:60:e4:9a 20:00:00:00:c9:60:e4:9a  vfc21
vfc31     1    0xee0009 20:00:00:00:0a:00:00:01 20:00:00:00:c9:60:e4:9a  vfc22
vfc31     1    0xee000a 20:00:00:00:0a:00:00:02 20:00:00:00:c9:60:e4:9a  vfc23
vfc31     1    0xee000b 33:33:33:33:33:33:33:33 20:00:00:00:c9:60:e4:9a  vfc24

Total number of flogi = 4
```

Note For each server interface, the External Interface value displays the assigned NP uplink.

To display the status of the server interfaces and the NP uplink interfaces, enter the **show npv status** command:

```
switch# show npv status
npiv is enabled

External Interfaces:
====================
  Interface: vfc21, VSAN: 1, FCID: 0x1c0000, State: Up
  Interface: vfc22, VSAN: 1, FCID: 0x040000, State: Up
  Interface: vfc23, VSAN: 1, FCID: 0x260000, State: Up
  Interface: vfc24, VSAN: 1, FCID: 0x1a0000, State: Up

  Number of External Interfaces: 4

Server Interfaces:
==================
  Interface: vfc31, VSAN: 1, NPIV: No, State: Up

  Number of Server Interfaces: 1
```

Note To view fcns database entries for NPV edge switches, you must enter the **show fcns database** command on the core switch.

To view all the NPV edge switches, enter the **show fcns database** command on the core switch:

```
core-switch# show fcns database
```

For additional details (such as IP addresses, switch names, interface names) about the NPV edge switches that you see in the **show fcns database** output, enter the **show fcns database detail** command on the core switch:

```
core-switch# show fcns database detail
```

Verifying NPV Traffic Management

To display the NPV traffic map, enter the **show npv traffic-map** command.

```
switch# show npv traffic-map
NPV Traffic Map Information:
----------------------------------------
Server-If       External-If(s)
----------------------------------------
vfc13           vfc110,vfc111
```

```
vfc15           vfc11,vfc12
----------------------------------------
```

To display the NPV internal traffic details, enter the **show npv internal info traffic-map** command.

To display the disruptive load-balancing status, enter the **show npv status** command:

```
switch# show npv status
npiv is enabled
disruptive load balancing is enabled
External Interfaces:
====================
  Interface: vfc21, VSAN: 2, FCID: 0x1c0000, State: Up
...
```