CHAPTER 14

Configuring FlexAttach Virtual pWWN

This chapter describes the FlexAttach virtual port world-wide name (pWWN) feature and includes the following sections:

About FlexAttach Virtual pWWN

FlexAttach virtual pWWN feature facilitates server and configuration management. In a SAN environment, the server installation or replacement, requires interaction and coordination among the SAN and server administrators. For coordination, it is important that the SAN configuration does not change when a new server is installed, or when an existing server is replaced. FlexAttach virtual pWWN minimizes the interaction between the server administrator and the SAN administrator by abstracting the real pWWN using virtual pWWNs.

When FlexAttach virtual pWWN is enabled on an interface, a virtual pWWN is assigned to the server interface. The real pWWN is replaced by a virtual pWWN, which is used for SAN configuration like zoning.

Administrators can benefit from FlexAttach in the following scenarios:

- Pre-configure : Pre-configure SAN for new servers which are not physical there yet--may be onorder. FlexAttach can be enabled on the ports designated for the new servers and use the virtual WWNs assigned for configuring SAN. The new servers are then plugged into the fabric without any change needed in the SAN.
- Replacement to the same port : A failed server can be replaced onto the same port without changing the SAN. The new server gets a same pWWN as the failed server because the virtual pWWN is assigned to the port.
- Replacement to (spare)— A spare server--which is on the same NPV device or a different NPV device) can be brought online without changes to the SAN. This is achieved by moving the virtual port WWN from the current server port to the spare port.
- Server Mobility - A server can be moved to another port on the same NPV device or another NPV device without changing the SAN. This is accomplished by moving the virtual pWWN to the new port. No change is needed if FlexAttach was configured using physical port WWN of the server to the virtual port WWN mapping.

FlexAttach Virtual pWWN Guidelines and Requirements

Following are recommended guidelines and requirements when deploying FlexAttach virtual pWWN:

- FlexAttach configuration is supported only on NPV switches.
- Cisco Fabric Services (CFS) IP version 4 (IPv4) distribution should be enabled.
- Virtual WWNs should be unique across the fabric.

Configuring FlexAttach Virtual pWWN

This section describes how to configure FlexAttach virtual pWWN feature and includes the following topics:

Enabling FlexAttach Virtual pWWN

The FlexAttach virtual pWWN feature is enabled automatically, manually, or by mapping pWWN to virtual pWWN. Figure 14-1 shows how the FlexAttach virtual pWWN feature is enabled.

Automatically Enabling FlexAttach Virtual pWWN

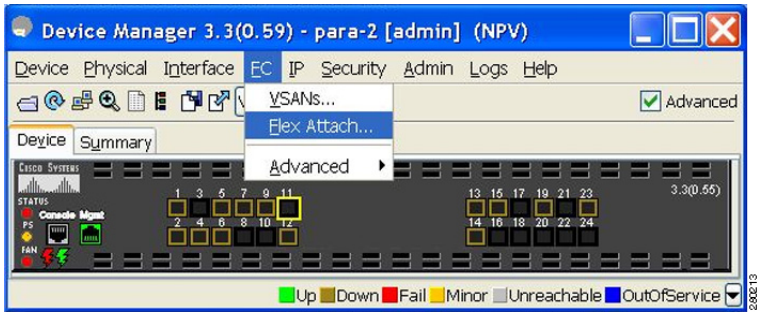
The virtual pWWN is enabled automatically on all the NPV switches, or per port on the NPV box. When enabled automatically, a virtual WWN is generated from the device switch WWN. This WWN is used as the virtual pWWN. Virtual pWWNs are generated using the local switch WWNs.

Note The port must be in a shut state when the virtual pWWN is enabled.

To enable virtual pWWN automatically for all the Interfaces, follow these steps:

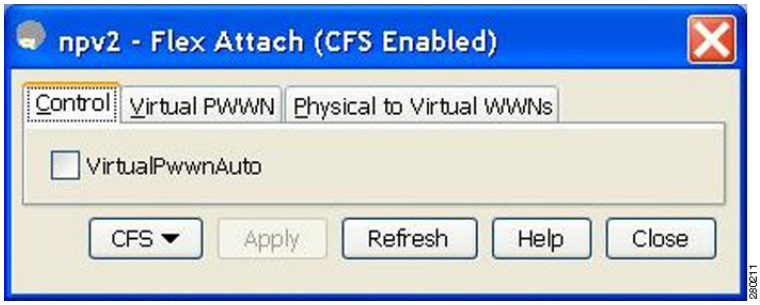
Step 1 Click **FC** menu in the Device Manger menu bar and select **FlexAttach** as shown in Figure 14-1.

Figure 14-1 FlexAttach in Device Manager



You see FlexAttach window.

Figure 14-2 FlexAttach Window in Device Manager



Step 2 Select the **VirtualPwwnAuto** box to enable automatic generation of Virtual WWNs on all the Fabric port interfaces.

Note

- When the *interface-list* is not included in the command, virtual pWWN is enabled globally.
- All the interfaces mentioned in the *interface-list* must be in a shut state.

Launching FlexAttach in Fabric Manager

To launch FlexAttach in Fabric Manager follow these steps:

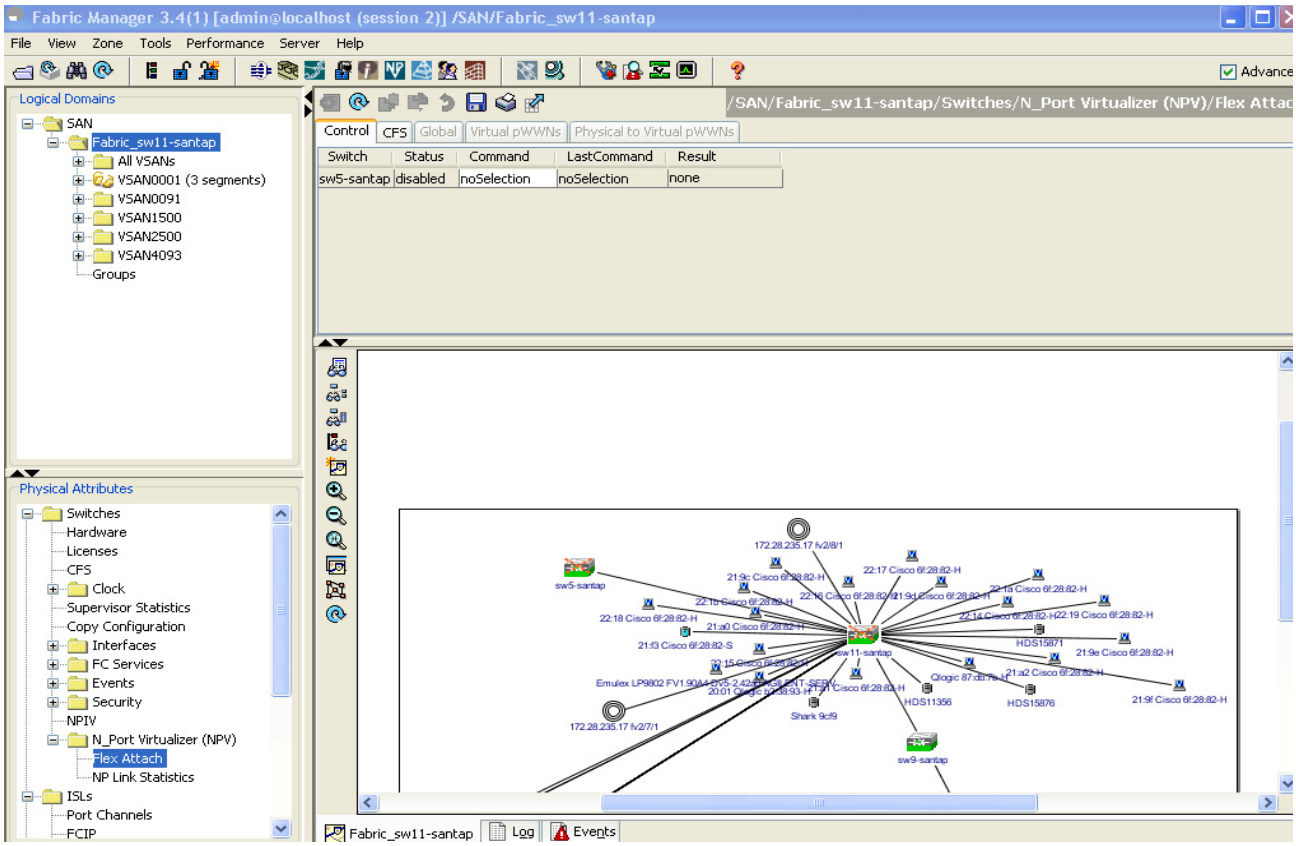
Step 1 Select the switch in the Logical Domains pane.

Step 2 Expand Switches> NPIV in the Physical Attributes pane.

Step 3 Select **FlexAttach** under NPIV.

The FlexAttach menus display in the Information pane, as shown in Figure 14-3.

Figure 14-3 FlexAttach Menu



Manually Enabling FlexAttach Virtual pWWN

You can manually assign a WWN to the interface, without generating it through the switch. Several checks are done by the NPV core to ensure the uniqueness of virtual pWWNs in the switch. When duplicate virtual pWWNs are configured, the subsequent logins are rejected by the NPV core switch.

Note

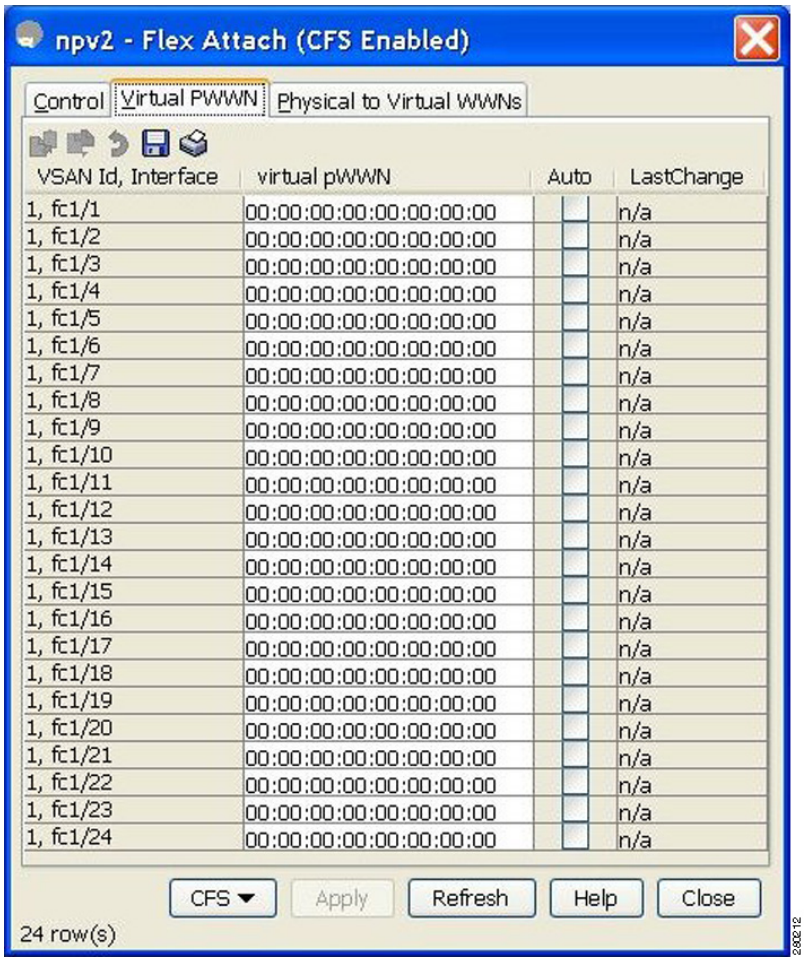
- Some ports may be in automode, some in manual mode, and the virtual pWWNs need not be assigned.
- The port must be in a shut state when virtual pWWN is enabled.

To enable virtual pWWN on each interface manually, follow the steps below:

Step 1 Click the **Virtual PWWN** tab.

You see virtual pWWN tab view.

Figure 14-4 Virtual PWWN Tab View in Device Manager



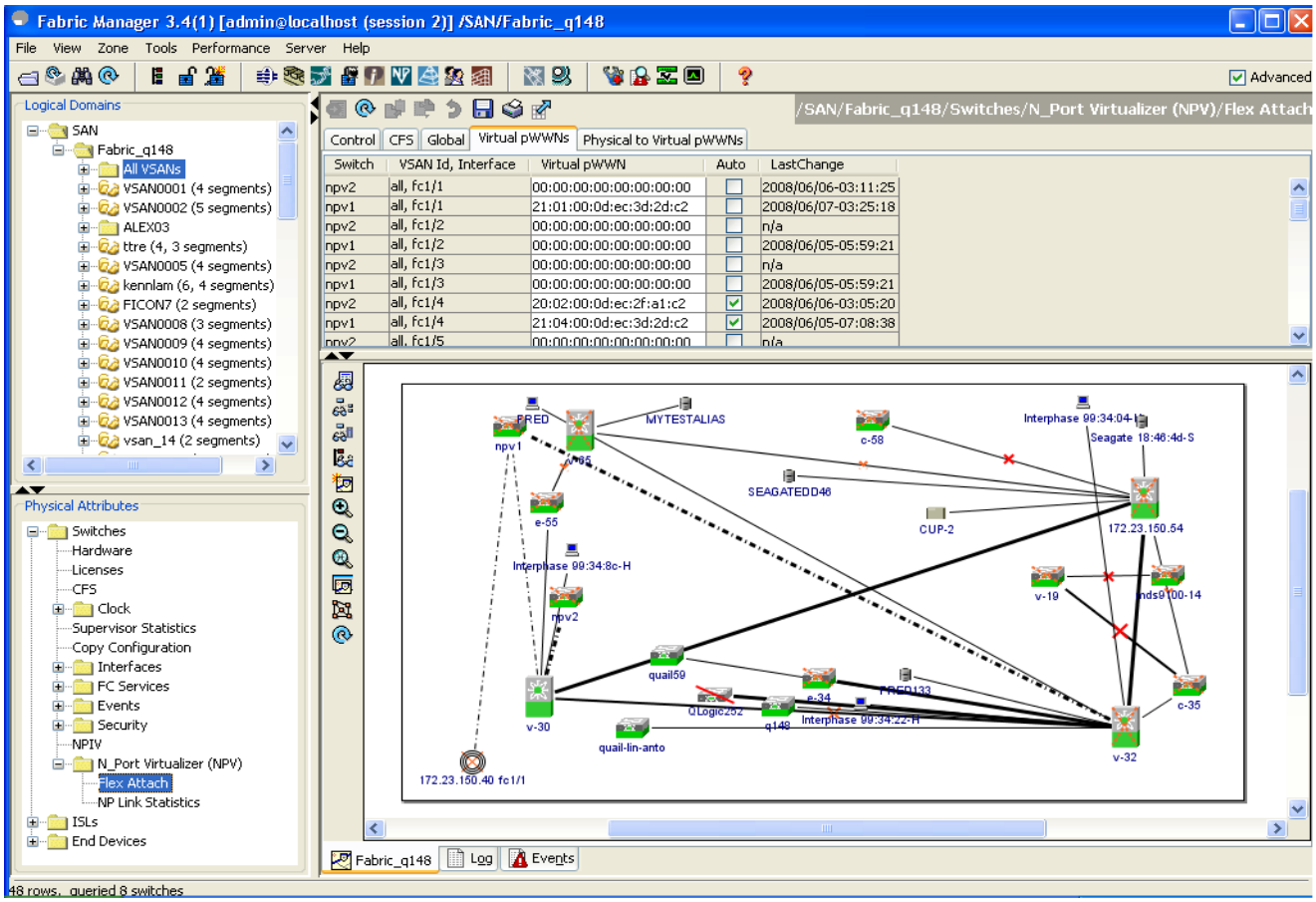
The Virtual pWWN tab view displays a list of the interfaces.

Step 2 Select **Auto** to automatically generate the virtual pWWN value for the selected interface.

Note The interface mentioned in the interface value must be in a shut state.

Follow Step 2 to automatically generate the virtual port WWN value for the selected interface in Fabric Manager, as shown in Figure 14-5.

Figure 14-5 Virtual pWWN Tab View in Fabric Manager



Note The interface mentioned in the *interface* value must be in a shut state.

Mapping pWWN to Virtual pWWN

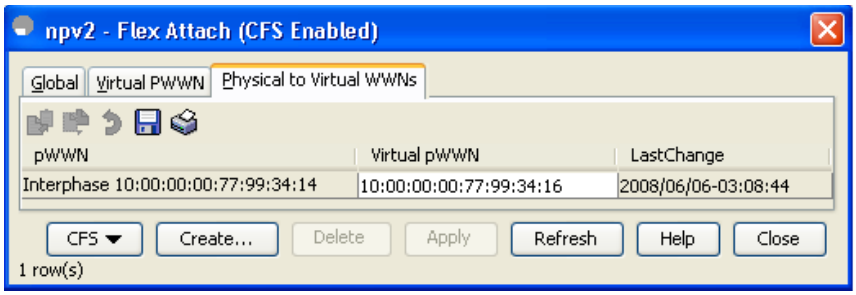
You can configure virtual pWWNs through real pWWNs. This is required for NPIV hosts containing multiple pWWNs, of which only FLOGI is mapped to the virtual pWWN. Subsequent FDSIDs will have different mappings.

Several checks are done by the NPV core to ensure the uniqueness of virtual pWWNs in the switch across the NPV switches. When duplicate virtual pWWNs are configured, the subsequent logins are rejected by the NPV core switch.To map pWWN to virtual pWWN, follow these steps:

Step 1 Click the **Physical to Virtual WWNs** tab in the FlexAttach window.

Step 2 You see the **Physical to Virtual WWWNs** tab view as shown in Figure 14-6.

Figure 14-6 Physical to Virtual WWNs Tab View in Device Manager

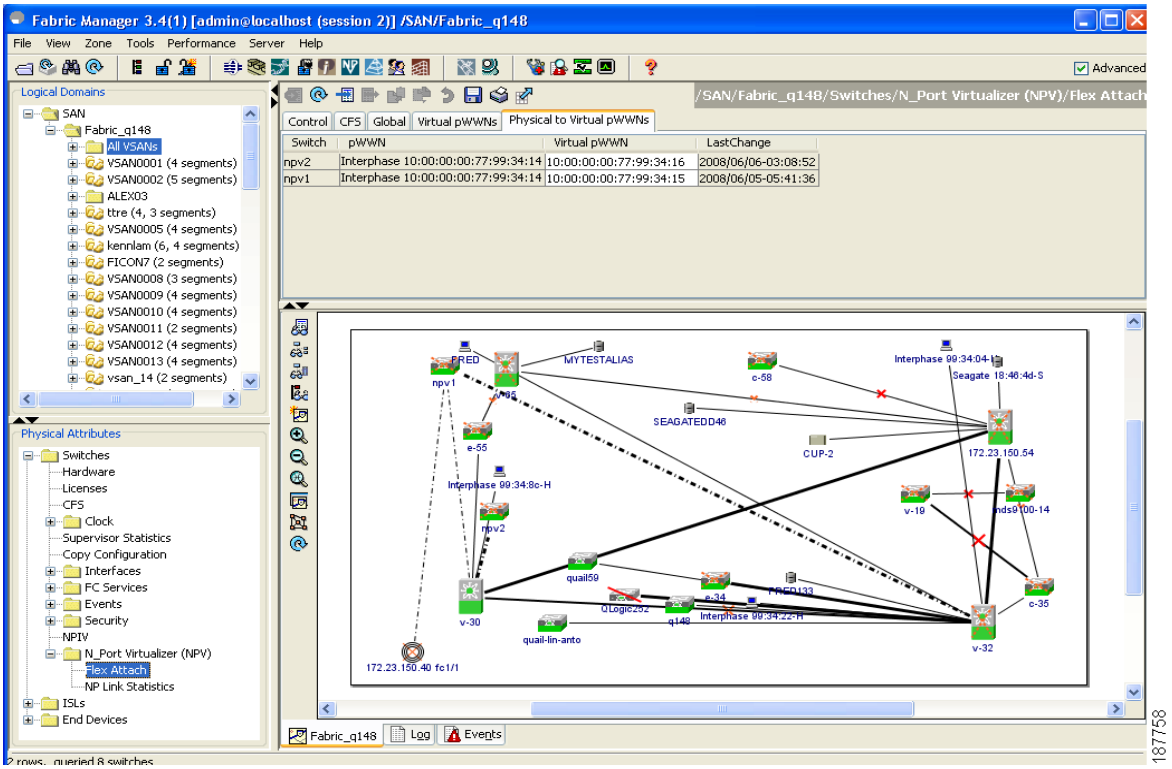


The **LastChange** field displays the time when the virtual pWWN was changed.

Note The interface must be in a shut state and the specified Virtual pWWN should not be logged in.

Figure 14-7 shows the Physical to Virtual WWNs tab view.

Figure 14-7 Physical to Virtual WWNs Tab View in Fabric Manager



Note The specified virtual pWWN and the real pWWN must not be logged in.

Debugging FlexAttach Virtual pWWN

For specific problems and the workarounds, refer to the following real-time scenarios:

Table 14-1FlexAttach Errors and the Workaround

Error	Description	Workaround
fc1/1 : interface is not down	FlexAttach configuration fails with this error as the configuration is enabled for an active interface with the operation state as **up**.	To move the port to the shut state, enable the FlexAttach configuration and then move the port to no shut state.
FlexAttach configuration is not distributed to the peers	This occurs when the FlexAttach configuration on one peer NPV is not available to any other peer NPV.	FlexAttach configuration will not be distributed if **cfs ipv4 distribute**, or **cfs ipv6 distribute** is disabled. Enable **cfs ipv4 distribute**, or **cfs ipv6 distribute**.
Even with CFS distribution enabledm Inagua doesn't become peer with other NPVs	This occurs whenCFS over IP is enabled, and when the Inagua in one blade center is not the peer NPV for other NPVs.	CFS over IP uses IP multicast to discover the NPV peers in the network. IBM MM does not support multicast and cannot act as a peer with NPV. This prevents the FlexAttach configuration from getting disrtibuted to other peer NPVs in the network.
NP port uses physical pWWN instead of virtual pWWN confgured through FlexAttach	This occurs whenNP port uses physical pWWN instead of virtual pWWN, that is configured through FlexAttach.	FlexAttach is supported on server interfaces like F ports, and not on external interfaces like NP port.
real port WWN and virtual WWN cannot be same	This occurs when you try to configure FlexAttach with a similar value for pWWN and virtual pWWN.	Use different values for pWWN and virtual pWWN, as similar values for pWWN and virtual pWWn are not allowed.
Virtual port WWN already exists	This occurs when you try to configure an already defined pWWN to a different interface.	Use undefined virtual pWWN for a new interface.

Security Settings for FlexAttach Virtual pWWN

Security settings for FlexAttach virtual pWWN feature are done by port security at the NPV core. Node WWN of the end device is used to provide physical security.

For more details on enabling port security, see Chapter 37, "Configuring Port Security".

FlexAttach Virtual pWWN CFS Distribution

FlexAttach virtual pWWN configuration is distributed for CFS through IPv4, and is enabled by default. The FlexAttach virtual pWWN distribution, by default, is on CFS region 201. The CFS region 201 links only to the NPV enabled switches. Other CFS feature like syslog is on region 0. Region 0 will be linked through IPv4 for all NPV switches on the same physical fabric. If CFS has an option to link through IPv4 or ISL, then CFS will select the ISL path.

Note NPV switches do not have ISL (E or TE ports) and are linked through IPv4.

Difference Between San Device Virtualization and FlexAttach Port Virtualization

Figure 14-8 describes the difference between SAN Device Virtualization (SDV) and FlexAttach Port Virtualization.

Figure 14-8 Difference Between SDV and FlexAttach Virtualization

FlexAttach Virtualization	SDV
Facilitates server management and has no restriction on the end devices used.	Facilitates target and disk management, and only facilitates disk and data migration.
WWN and Network Address Transport (NAT) is allocated to host bus adapter (HBA)	WWN NAT and Fibre Channel ID (FC-ID) are allocated on the virtual device, both primary and secondary
No rewrite requirements.	FC-ID rewrite on the switch indicates a rewrite-capable switch on the path.
Configuration distribution is not required for any of the interface-based configurations.	Configuration is distributed. This allows programming rewrites and connectivity anywhere.
Does not require device alias for virtual pWWN.	Configuration is secured to device alias.
Allows automapping to the new HBA. Mapping process is manual for NPIV.	Does not allow automapping to the secondary device