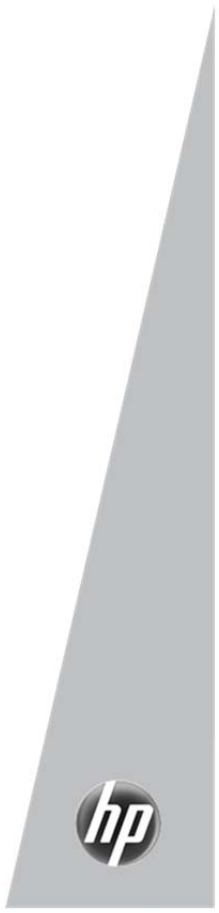
HP Discover 2013
HOL 2653
HP Virtual Connect 4.01 features and capabilities

Lab Guide

HP Virtual Connect 4.01 features and capabilities

Lab Guide



Rev. 1.1

Contents

Lab 1 — Accessing the LAB Environment and using the Domain Creation Wizard

Lab 2 — Implementing a Simple vNet

Lab 3 — Implementing Boot from SAN with FlexFabric

Lab 4A — Implementing Shared Uplink Sets (Optional)

Lab 4B — Implementing Shared Uplink Sets (with FCoE) (Optional)

Lab 5 — Configuring QoS

Lab 6 — Implementing Direct Attached SAN Fabrics

HP Virtual Connect 4.01 features and capabilities
Lab guide
June 2013

Accessing the LAB environment and using the Domain Creation Wizard

Lab 1

Objectives

After completing this lab, you should be able to:

- Access the remote lab network
- Use the Domain Setup Wizard to create a Virtual Connect (VC) domain
- Delete a default server profile
- Delete the Networks
- The SAN Fabrics will remain and be used in a later Lab

Introduction

In this lab, you will gain access to the Remote LAB equipment. Each POD consists of a c7000 enclosure with FlexFabric modules in Bays 1 and 2, a pair of HPN 5820 LAN switches and shared access to both EVA and 3PAR SAN. Each POD has full control over their dedicated c7000 and Virtual Connect Domain.

You will then use the Virtual Connect Manager (VCM) setup wizards to perform the first-time configuration of a VC domain. These wizards can also be used after a VC domain has been created. The Domain Setup Wizard is the wizard you use during this lab exercise. This wizard automatically invokes several other wizards for you, including the Network Setup, Fibre Channel Setup, and Server Profile Setup wizards.

> **!** **Important**
> When running the Domain Setup Wizard, make note of the MAC address, World Wide Name (WWN), and server serial number ranges you configure.

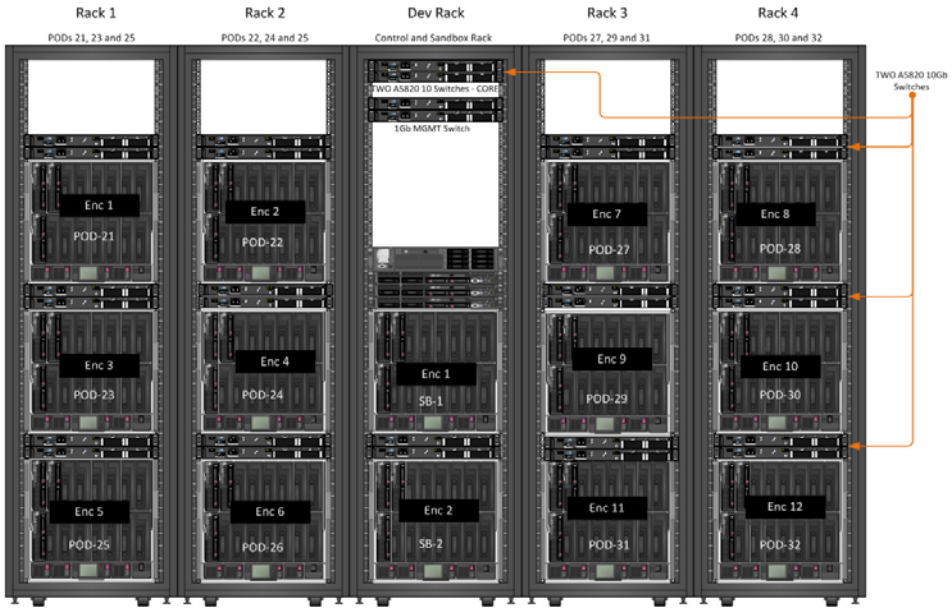
During this lab you will also delete the server profile, Network and SAN Fabrics created as this lab is intended to provide experience with lab access and the Domain Creation Wizard.

In this lab environment, you will use HP predefined (software-assigned) values for MAC addresses, WWNs, and server serial numbers. The particular range you will use is based on your student group number, which is referred to as your *POD ID*.

Exercise 1 - Accessing the remote lab network

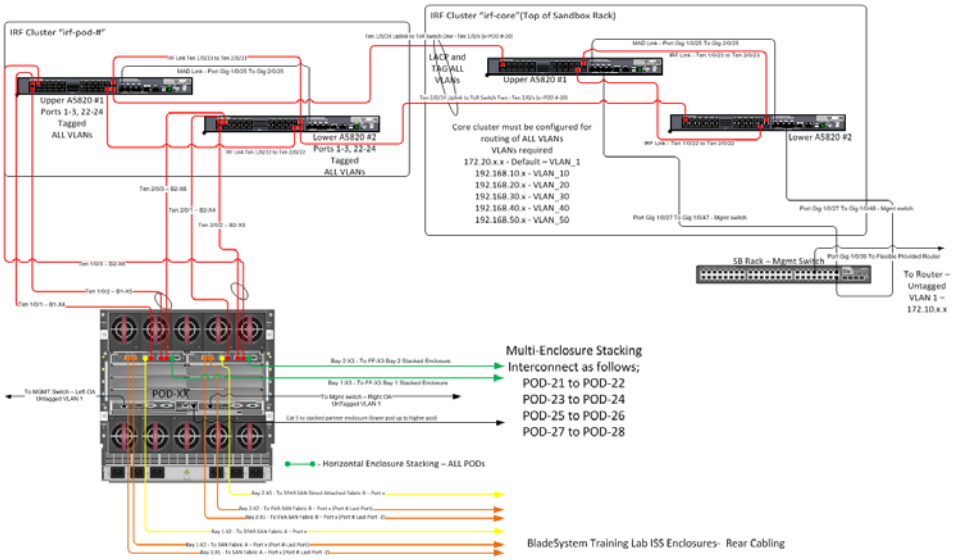
Student Access

The lab environment is located in a remote data center and consists of 12 c7000 blade enclosures, FlexFabric and supporting LAN and SAN connectivity.



BladeSystem Training Lab Front View

Each POD is configured with a c7000 Blade enclosure, TWO FlexFabric modules and TWO 5820 10Gb LAN switches configured in an IRF cluster. An EVA SAN is connected through FlexFabric ports X1 and X2 to a Brocade SAN fabric and a 3PAR storage array is directly connected to the FlexFabric Modules, port X3, for "FLAT SAN" connectivity.



BladeSystem Training Lab ISS Enclosures- Rear Cabling

Student access is provided through two terminal servers (TS1 or TS2) using Remote Desktop Services and a Windows login account assigned based on the POD ID. A common password is used for all login accounts. *<The instructor will provide the password>*.

There are two RDC servers implemented as Windows 2008 R2 virtual machines that are Internet-visible. Two RDC servers are provided for use, TS1 and TS2.

- All odd numbered PODs will use TS1
- All even numbered PODs will use TS2

RDC Terminal Servers				
Name	**External IP Address**	**TCP Port**	**Internal IP Address**	**Default Gateway**
TS1.cinetworking.lab	69.74.245.21	5001	172.20.200.14/16	172.20.0.1
TS2.cinetworking.lab	69.74.245.21	5002	172.20.200.15/16	172.20.0.1

1. On the desktop of the LAB PC, open a Remote desktop Connect and enter the IP address and port number of the Terminal Server assigned to you, based on POD number.

Student logins are shown in the table below.

Remote Desktop Servers: Windows Login Accounts		
POD ID	**User Name**	**Password**
21	CINETWORKING\pod-21	<*instructor-defined*>
22	CINETWORKING\pod-22	<*instructor-defined*>
23	CINETWORKING\pod-23	<*instructor-defined*>
24	CINETWORKING\pod-24	<*instructor-defined*>
25	CINETWORKING\pod-25	<*instructor-defined*>
26	CINETWORKING\pod-26	<*instructor-defined*>
27	CINETWORKING\pod-27	<*instructor-defined*>
28	CINETWORKING\pod-28	<*instructor-defined*>
29	CINETWORKING\pod-29	<*instructor-defined*>
30	CINETWORKING\pod-30	<*instructor-defined*>
31	CINETWORKING\pod-31	<*instructor-defined*>
32	CINETWORKING\pod-32	<*instructor-defined*>

2. Once logged in, access the HP Onboard Administrator (OA) of your enclosure by opening a web browser.
3. Specify the URL listed in the following table that corresponds to your assigned student POD ID, verify you have the correct POD ID when launching the shortcut.

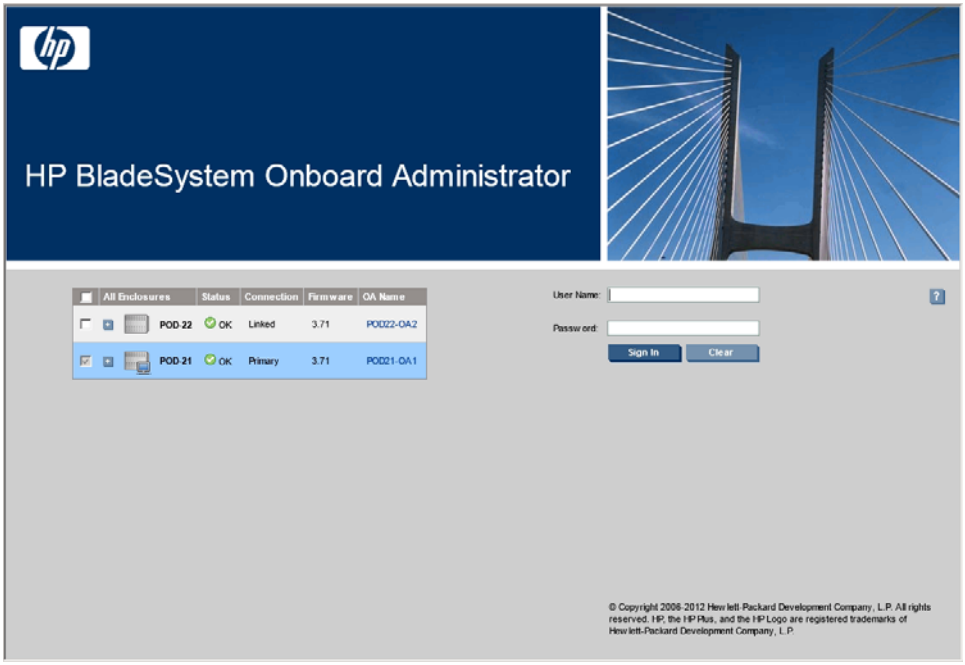
Note
The third octet of the IP address corresponds to your POD ID.

POD ID	URL
21	https://172.20.21.100
22	https://172.20.22.100
23	https://172.20.23.100
24	https://172.20.24.100
25	https://172.20.25.100
26	https://172.20.26.100
27	https://172.20.27.100
28	https://172.20.28.100
29	https://172.20.29.100
30	https://172.20.30.100
31	https://172.20.31.100
32	https://172.20.32.100

4. Unless otherwise indicated by the instructor, enter the following user credentials to log in to the Onboard Administrator of your enclosure. (Do NOT change this or any password) and ensure only your enclosure is selected in the tab to the left.

   User Name: `admin`

   Password: `hpinvent`



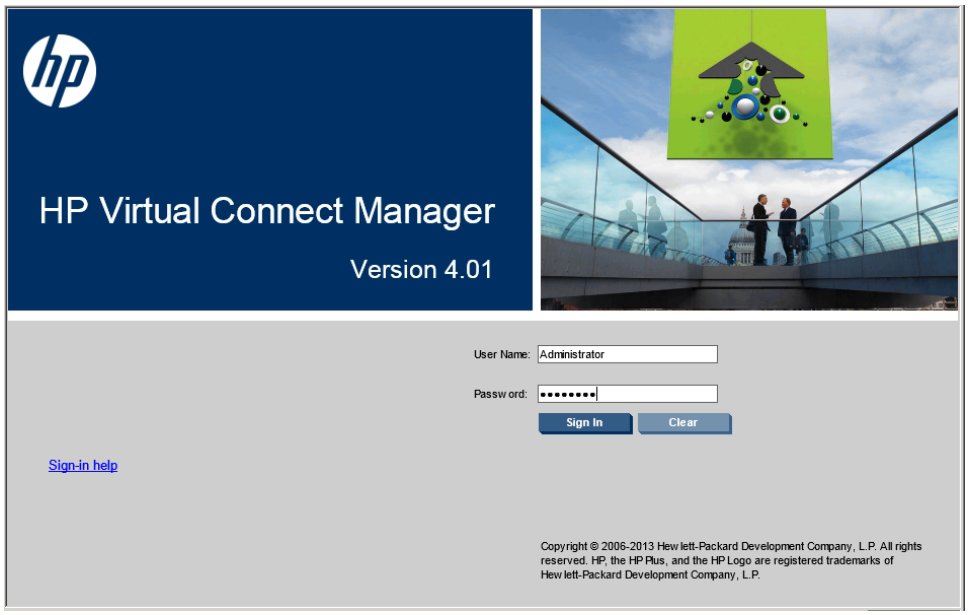
5. In the navigation pane, click the following links to examine the components installed in your enclosure:

   - **Device Bays**
   - **Interconnect Bays**

6. Access Virtual Connect Manager. In the navigation pane, click **Virtual Connect Manager**.
7. Unless otherwise indicated by the instructor, enter the following user credentials to log in.

   User Name: `Administrator`

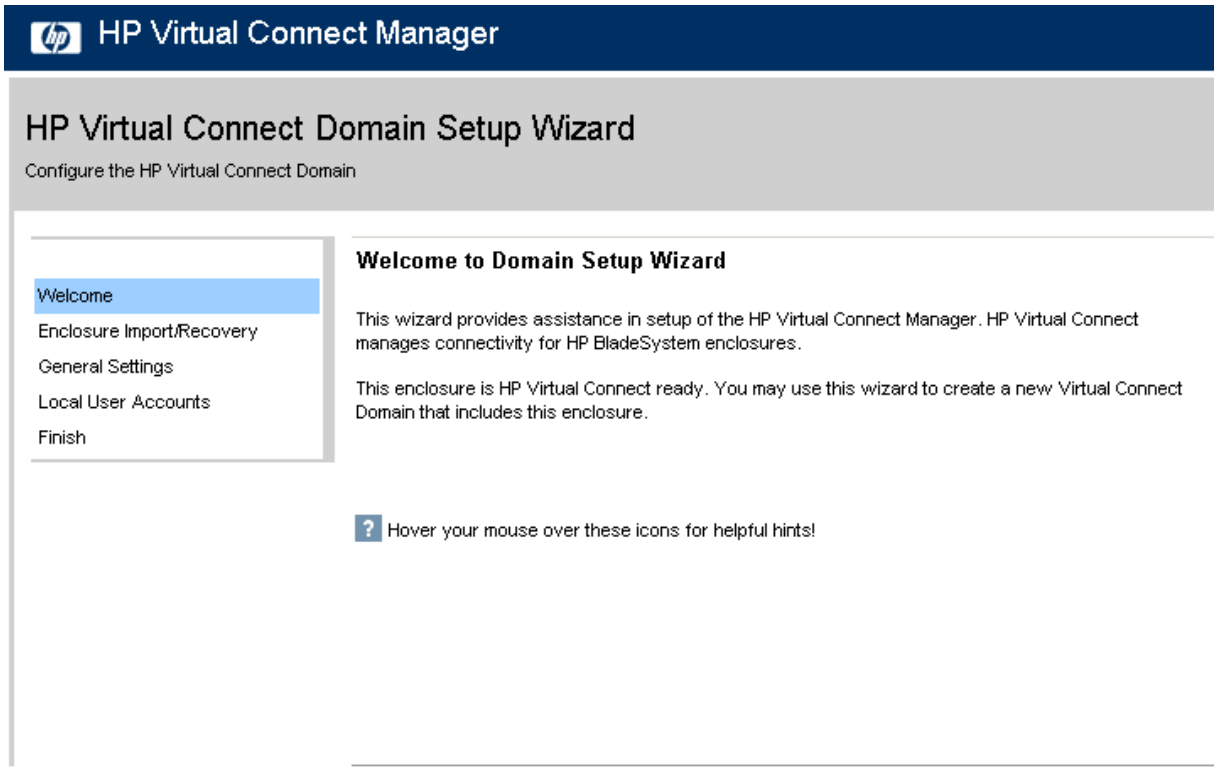
   Password: *`<See table below, use the password for your POD, Bay 1 module>`*



Virtual Connect Manager: Factory-assigned Passwords				
POD	**Module**	**IP Address**	**User Name**	**Password**
21	1	172.20.21.118	Administrator	YZJRR92G
	2	172.20.21.119		FQVJ9DMY
22	1	172.20.22.118	Administrator	FQRZ39M6
	2	172.20.22.119		YR8V60B8
23	1	172.20.23.118	Administrator	X5WF98F8
	2	172.20.23.119		FFKNR4WS
24	1	172.20.24.118	Administrator	SWBY0NFM
	2	172.20.24.119		HKGSQ8FM
25	1	172.20.25.118	Administrator	F69R6V4K
	2	172.20.25.119		XXMJRZP3
26	1	172.20.26.118	Administrator	B605GJW4
	2	172.20.26.119		XF5TZHCP
27	1	172.20.27.118	Administrator	297TD48Z
	2	172.20.27.119		KBP59QY9

28	1	172.20.28.118	Administrator	FGH3J0VZ
	2	172.20.28.119		YR690W9H
29	1	172.20.29.118	Administrator	T7FDBM4Y
	2	172.20.29.119		2JHQYDZ6
30	1	172.20.30.118	Administrator	65SW07XW
	2	172.20.30.119		QQRZ0C3K
31	1	172.20.31.118	Administrator	J5NN2T4V
	2	172.20.31.119		G2TZ8NQ7
32	1	172.20.32.118	Administrator	7HZYKT2G
	2	172.20.32.119		Q69R4YMZ

8. If the following window displays, then no VC domain currently is configured for your enclosure, proceed to Exercise 2.



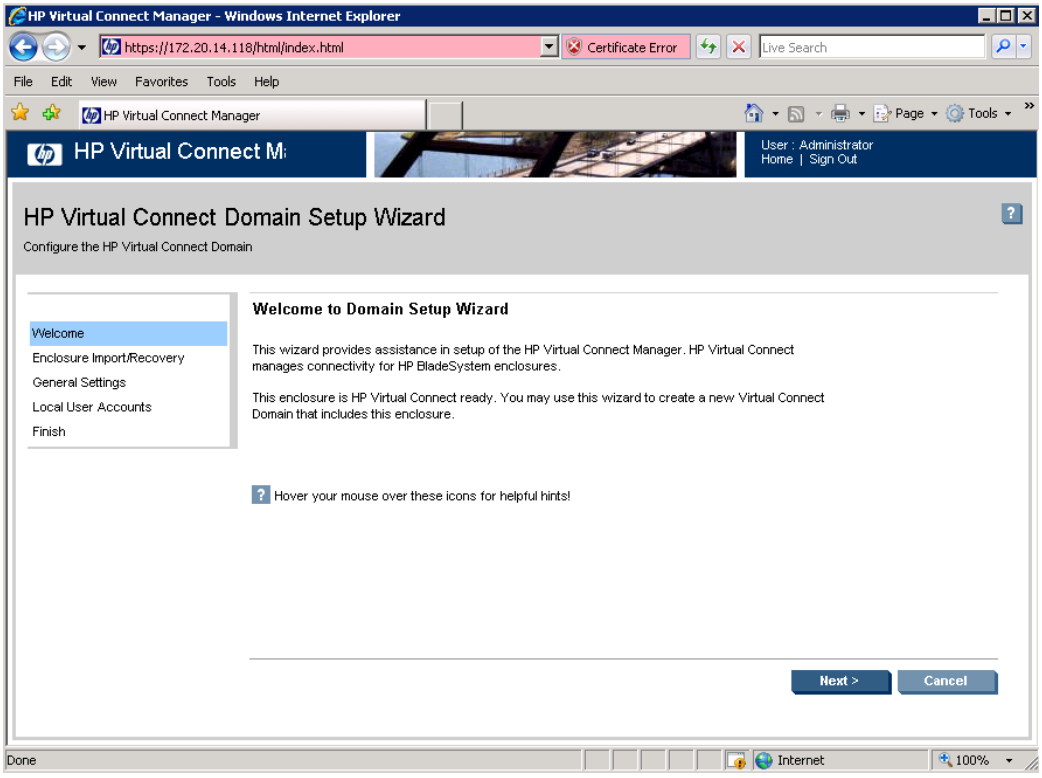
Exercise 2 — Running the Domain Setup Wizard

In this exercise, you will use the Domain Setup Wizard, which starts automatically upon the first login to the Virtual Connect Manager web interface. You will be creating a Virtual Connect domain consisting of just your assigned enclosure at this time.

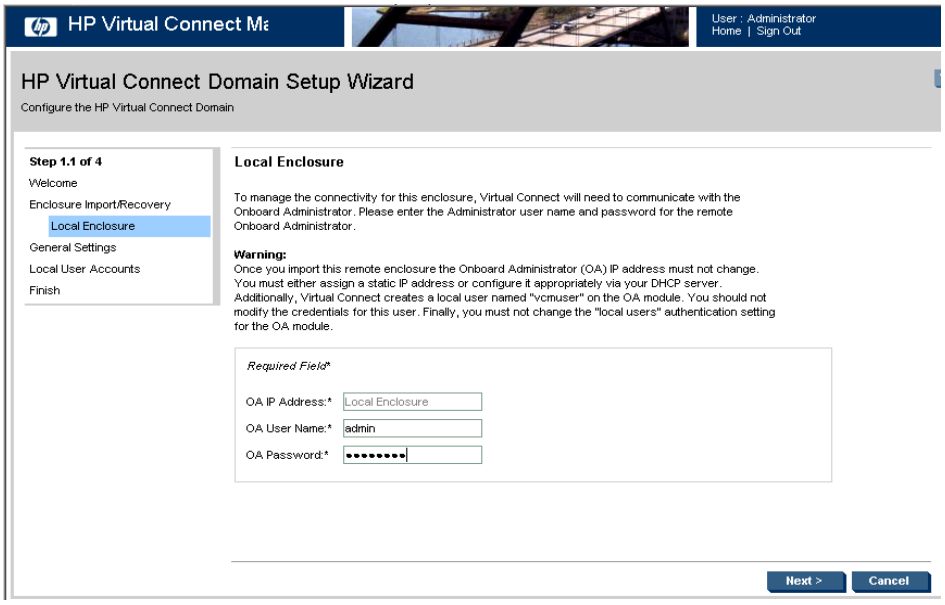
This wizard also invokes setup wizards for configuration of network, Fibre Channel, and server profile elements. These additional wizards will be used, but only to configure the minimum settings. Any of the Ethernet network, Fibre Channel SAN fabrics, and server profiles that you will need during the exercises that follow will be defined as you go through each exercise.

1. After you log in to the VCM, the welcome window of HP Virtual Connect Domain Setup wizard displays automatically. Click **Next**.

Note
This window displays automatically when the VC Ethernet module is at the factory-default settings. If this window does not display, contact your instructor for directions before proceeding.

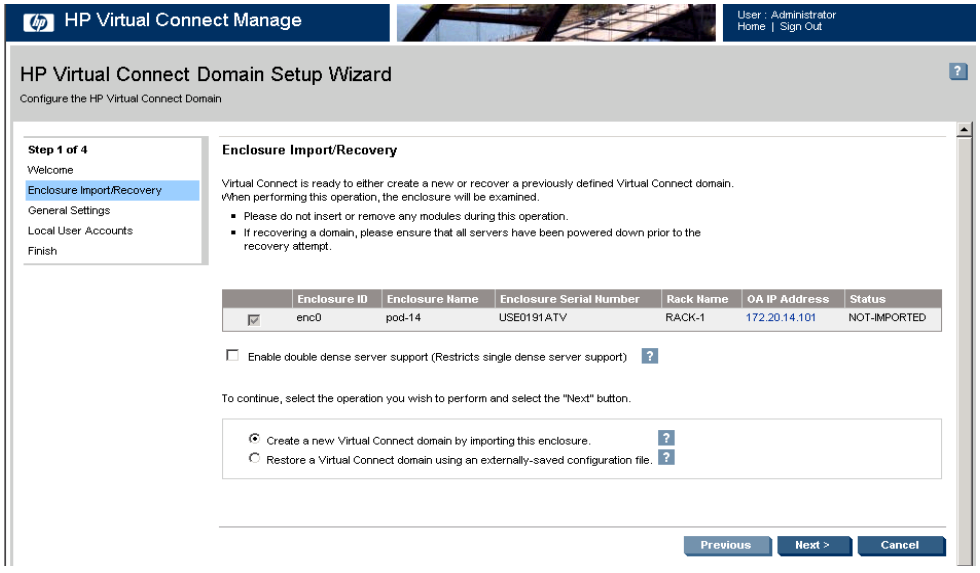


Specify the user name and password of the local OA Administrator account. Then click **Next**. (the OA login is “admin” and the password is “hpinvent”



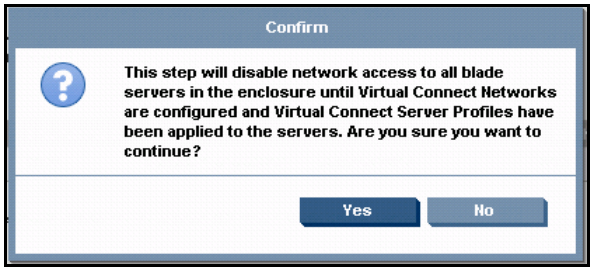
Note
The account used to import the enclosure must be the local OA Administrator of the imported enclosure. A Lightweight Directory Access Protocol (LDAP) account is not supported and will cause the operation to fail.

2. You will be creating a new Virtual Connect Domain. The option to **Create a new Virtual Connect domain by importing this enclosure** should be enabled by default. Ensure that it is and click **Next**.

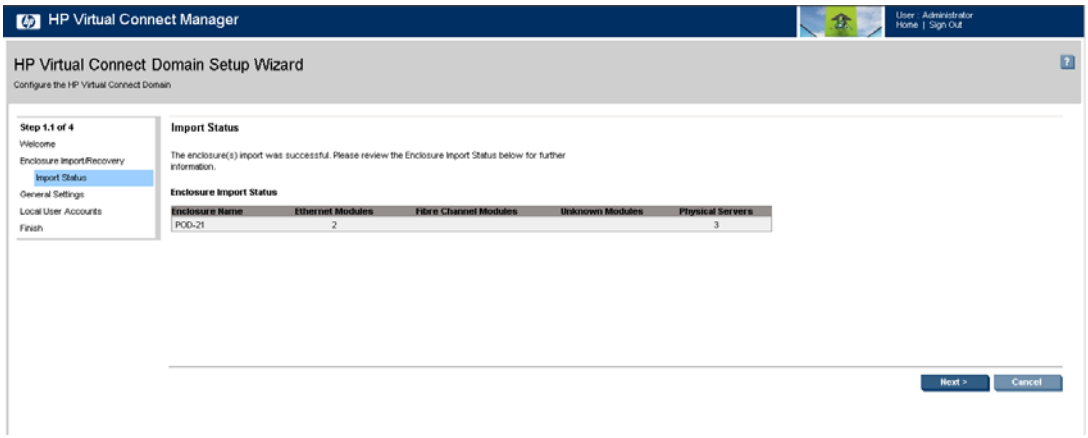


Important
Do **not** enable double dense blade support.

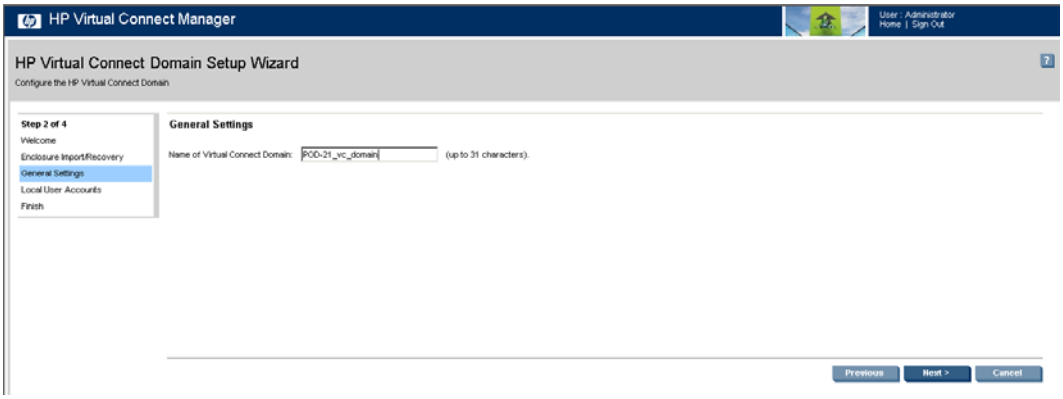
3. By creating a domain, you disable all outbound traffic until at least one VC network and one server profile are defined, and the server profile is assigned to a server bay. Click **Yes** to confirm. The import process will take a few minutes, note the progress indicator at the bottom of the page.



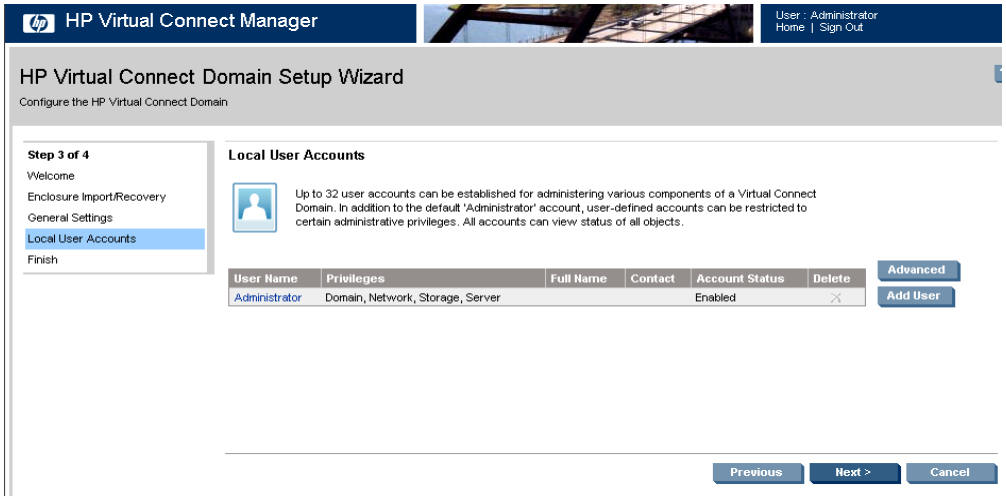
4. The next window simply shows the number of blades and I/O modules in the enclosure. The listing you see might differ from the following example depending on the number of VC Ethernet modules, VC Fibre Channel modules, and server blades installed in the enclosure you are using. Click **Next**.

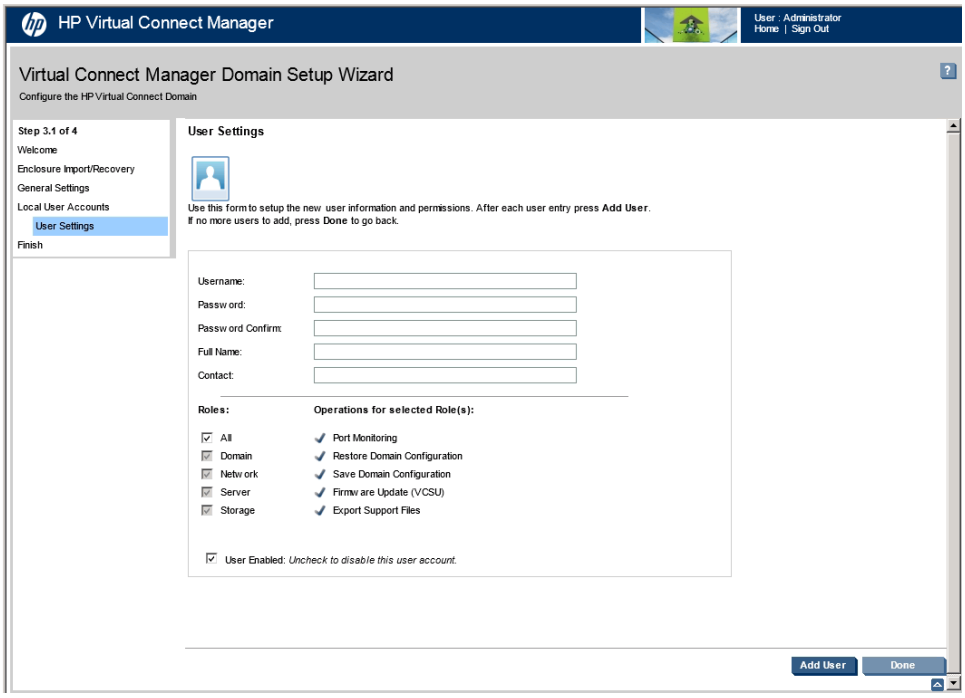


5. Specify `PODnn_vc_domain` or other name of your choosing for the name of your VC domain, substituting your POD ID for `nn`. Then click **Next**.



6. To get a sense of the role-based user accounts capability, add four types of user accounts to your domain. To define a user account, click **Add User** and then specify the information from the following table. Click **Add User** to save the changes and add the next user account. When finished, click **Done.**





Username	Password	Role
admin	hpinvent	All
server	hpinvent	Server
network	hpinvent	Network
storage	hpinvent	Storage

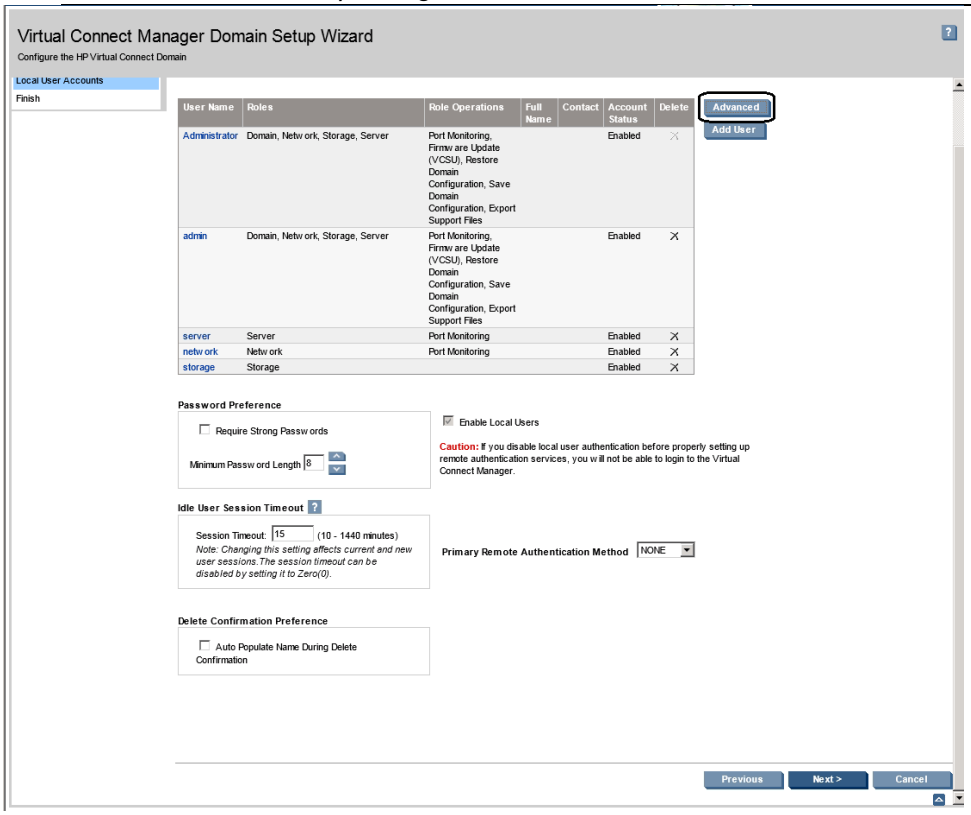
! **Important**
Both usernames and passwords are case-sensitive.

7. **Click Done** to close the Local User Account window.

8. Click the **Advanced** button, you will notice the expanded Password and IDEL Session Timeout parameters. Set the timeout to a value of 30 minutes and enable the "Delete Confirmation Preference" check box at the bottom of this screen, with this selected, during object deletion, VC will auto populate the name of the object being deleted.

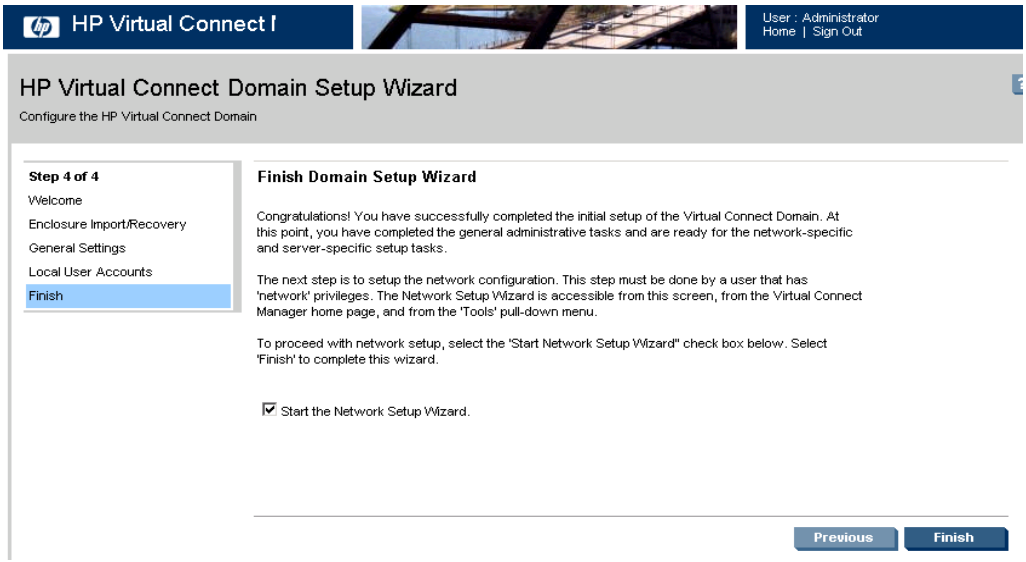
Note

Prior to Firmware release 4.01, the GUI session did not have a configurable timeout value, however, the CLI timed out after 15 minutes of inactivity. The default GUI and CLI timeout value is set to 15 minutes. If set to "0" neither the GUI nor the CLI will timeout. Try setting the timeout value to 30 minutes.

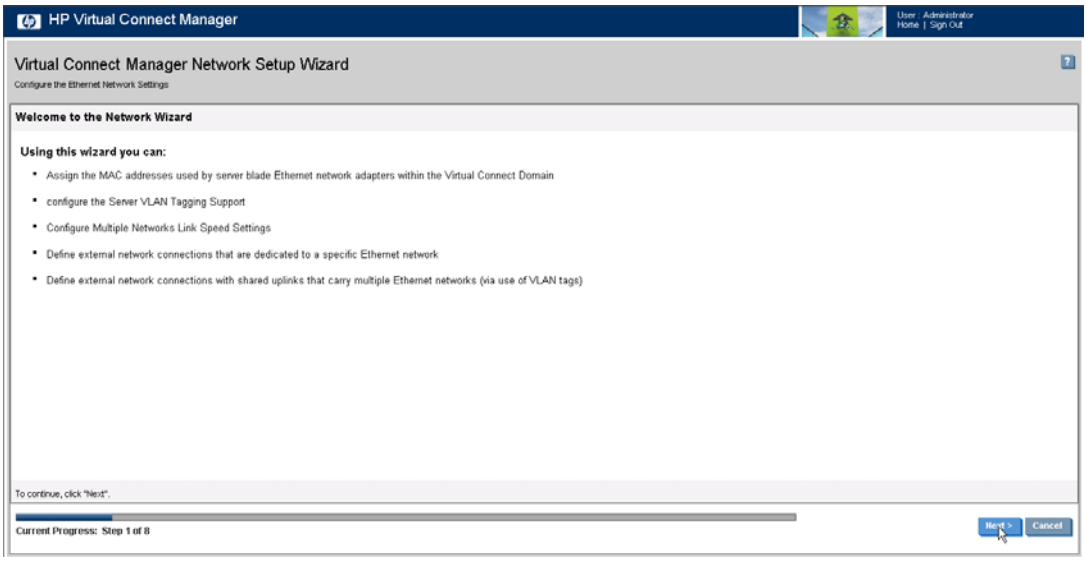


9. **Click Next** to close the Local User Account window.

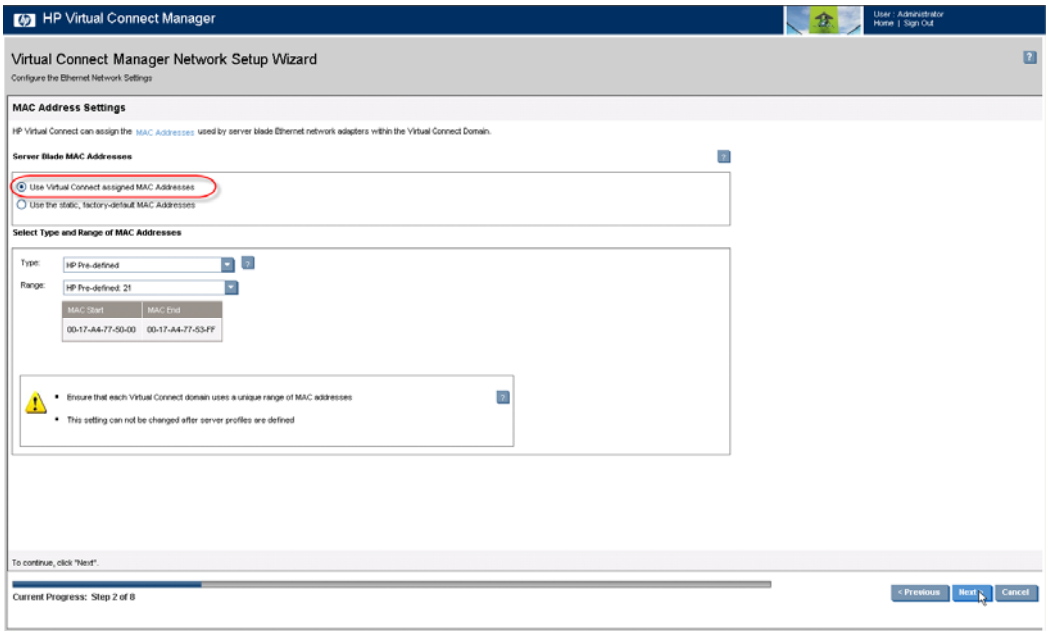
10. The completion window for the Domain Setup Wizard displays. Leave the Start the Network Setup Wizard check mark enabled and **click Finish**.



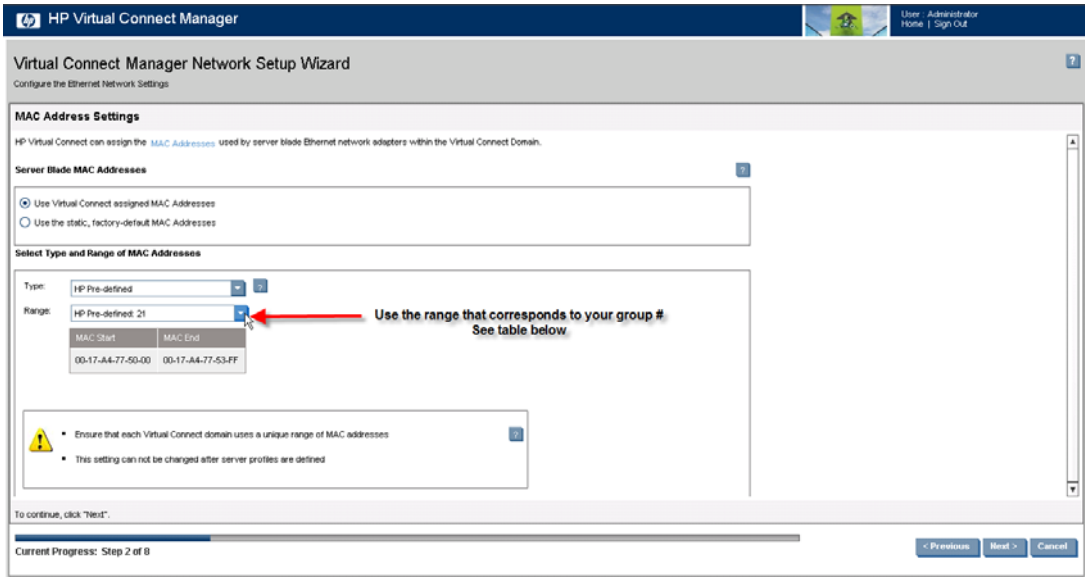
11. When the Welcome to the Network Setup Wizard window displays, read the information provided and then **click Next**.



12. Click **Use Virtual Connect assigned MAC addresses** to allow VC to manage hardware addresses. Then **click Next.**



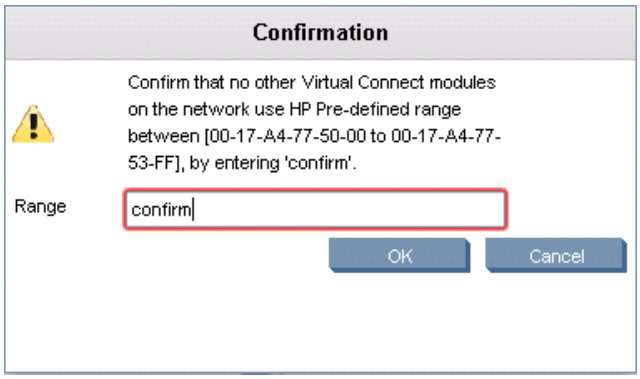
13. In the Type drop-down list, select **HP Pre-Defined**. Based on your POD ID, select **HP Defined: nn** for Range, where **nn** corresponds to your POD ID. Then **click Next**. Refer to the following table to determine your HP-Defined range identifier.



POD ID	Enclosure	Range	Begin and End
21	1	HP-Defined: 21	00-17-A4-77-50-00 to 00-17-A4-77-53-FF
22	2	HP-Defined: 22	00-17-A4-77-54-00 to 00-17-A4-77-57-FF
23	3	HP-Defined: 23	00-17-A4-77-58-00 to 00-17-A4-77-5B-FF
24	4	HP-Defined: 24	00-17-A4-77-5C-00 to 00-17-A4-77-5F-FF
25	5	HP-Defined: 25	00-17-A4-77-60-00 to 00-17-A4-77-63-FF
26	6	HP-Defined: 26	00-17-A4-77-64-00 to 00-17-A4-77-67-FF
27	7	HP-Defined: 27	00-17-A4-77-68-00 to 00-17-A4-77-6B-FF
28	8	HP-Defined: 28	00-17-A4-77-6C-00 to 00-17-A4-77-6F-FF
29	9	HP-Defined: 29	00-17-A4-77-70-00 to 00-17-A4-77-73-FF
30	10	HP-Defined: 30	00-17-A4-77-74-00 to 00-17-A4-77-77-FF
31	11	HP-Defined: 31	00-17-A4-77- 78-00 to 00-17-A4-77-7B-FF
32	12	HP-Defined: 32	00-17-A4-77-7C-00 to 00-17-A4-77-7F-FF

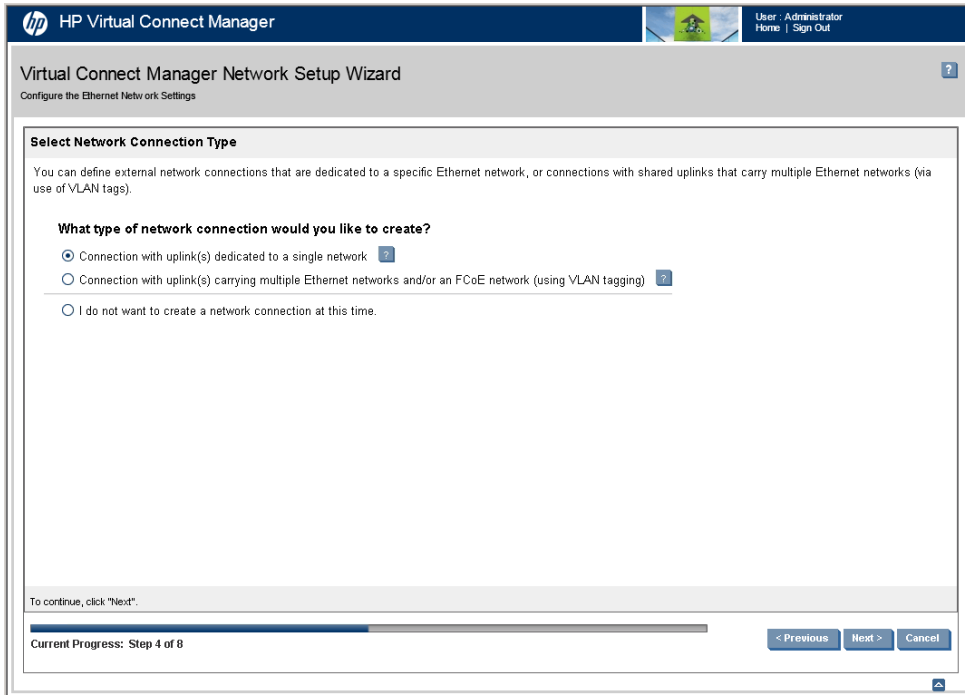
! **Important**
Selecting an HP range that another student team is using will cause a conflict on the network. This is important to note when designing a Virtual Connect solution for customers. If the customer has several or plans to implement several Virtual Connect based enclosures, the customer needs to ensure that each enclosure is configured with a unique MAC address range.

14. Confirm that a correct non-conflicting address range has been selected by entering `confirm`. Then click **OK**.

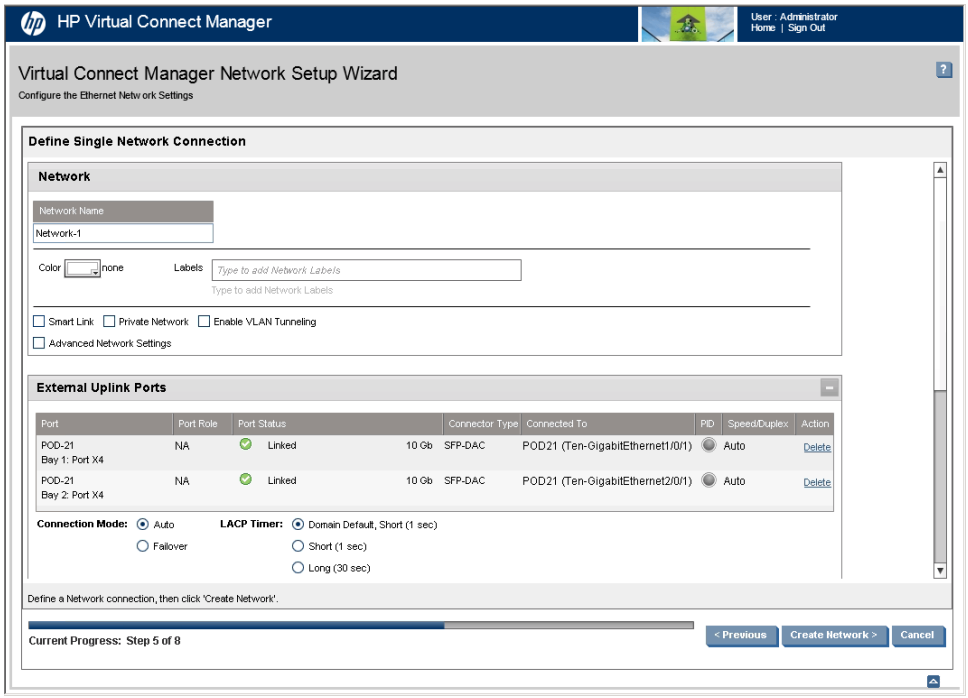


15. On the Server VLAN Tag Settings screen, the default VLAN Capacity setting is Expanded VLAN capacity. Also, notice the Multiple Networks Link Speeds Setting. **Click Next**

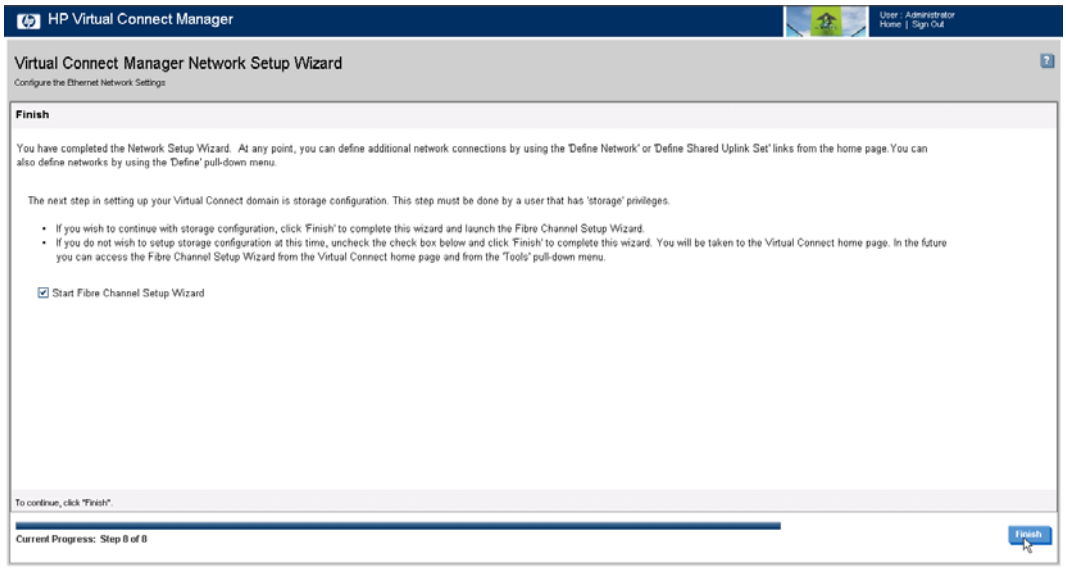
16. Select Connect with Uplinks to a single network and **click next**.



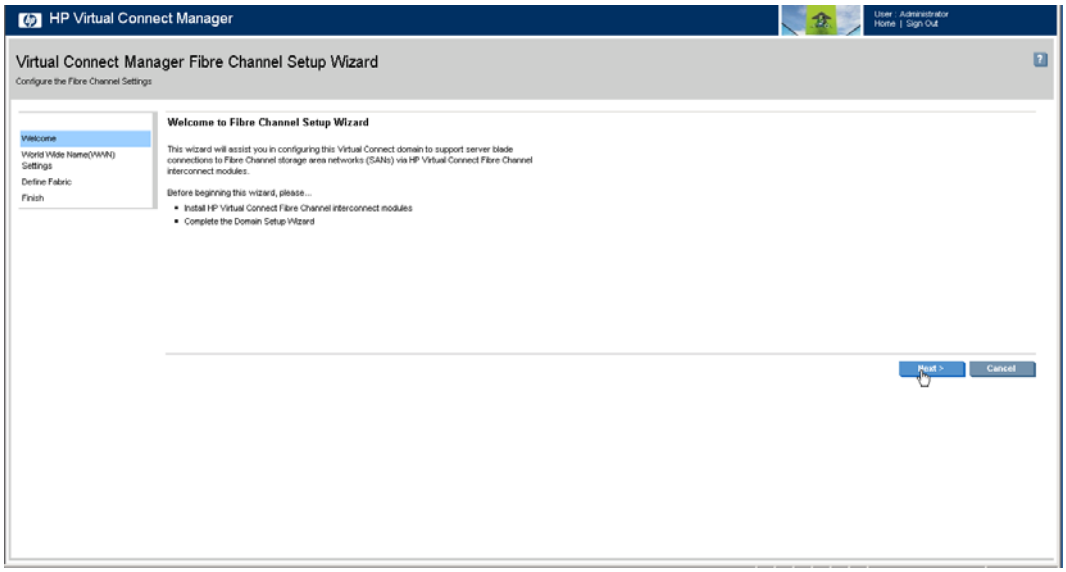
17. In the define a single network screen create a network called Network-1. Do not enable SmartLink or VLAN Tunneling, add Uplink X4 from Bays 1 and 2 modules and Click Create Network. Then **Click Create Network** on the following screen.



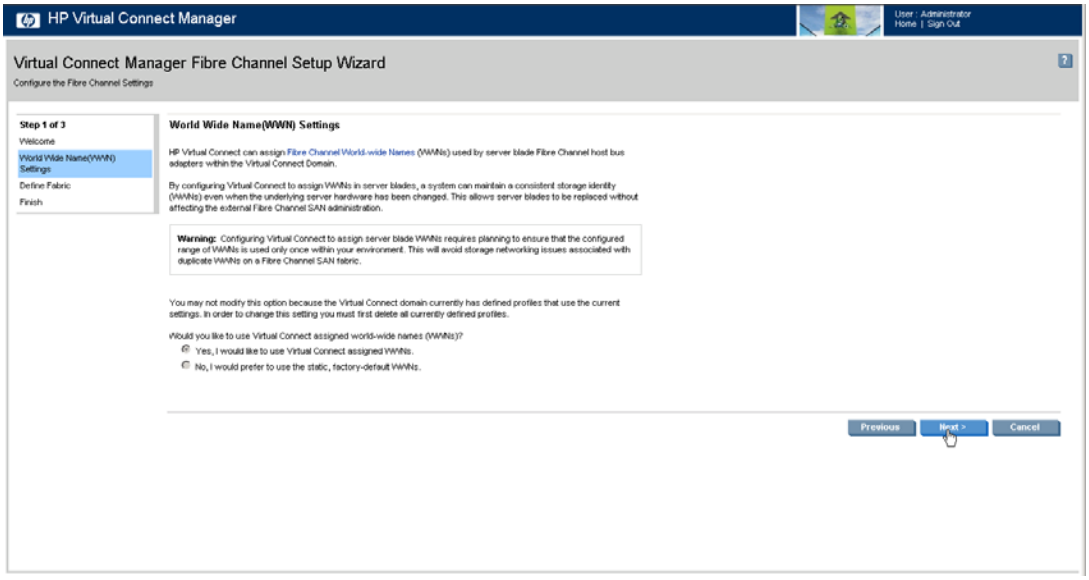
18. The completion window for the Network Setup Wizard displays. Leave the Start the Fibre Channel Setup Wizard check box selected and then **click Finish**.



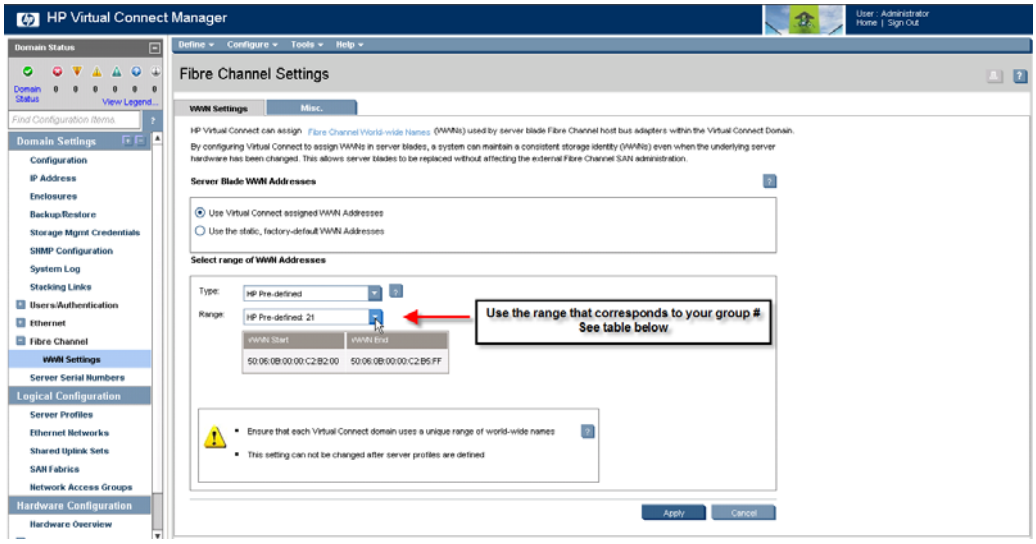
19. When the Welcome to Fibre Channel Setup Wizard screen displays, **click Next**.



20. Select the **Yes, I would like to use Virtual Connect assigned WWNs** button to allow VC to manage Fibre Channel World Wide Names. Then click **Next**.



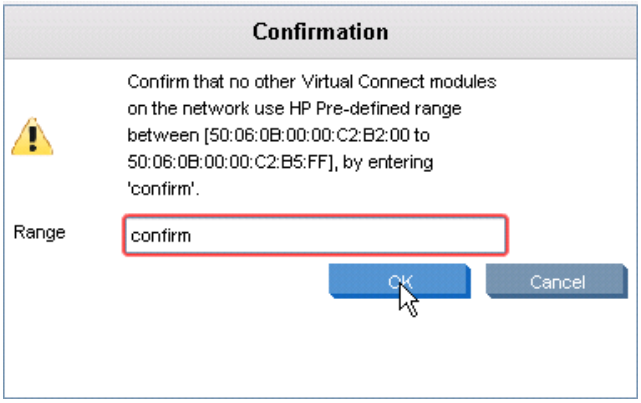
21. From the Type drop-down list, select **HP Pre-Defined**. Refer to the following table to determine your HP-Defined range identifier. Based on your POD ID, select **HP Defined: nn** for Range, where **nn** corresponds to your POD ID. Then **click Next**.



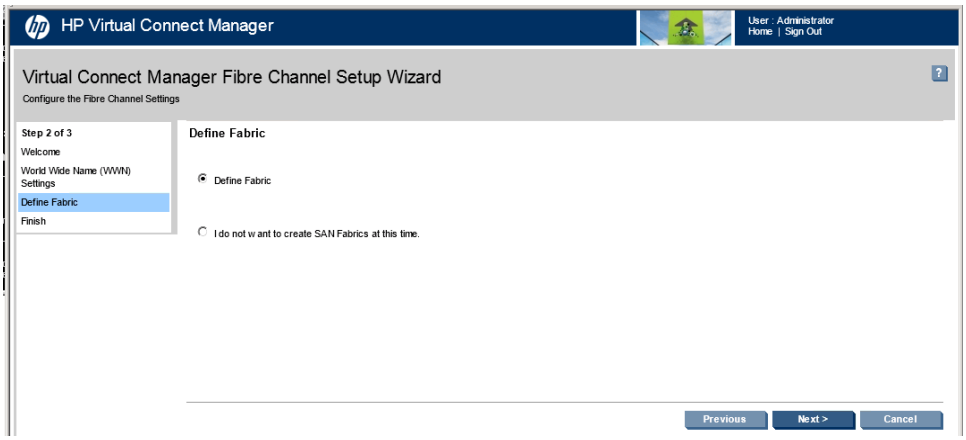
POD ID	Enclosure	Range	Begin and End
21	1	HP-Defined: 21	50:06:0B:00:00:C2:B2:00 to 50:06:0B:00:00:C2:B5:FF
22	2	HP-Defined: 22	50:06:0B:00:00:C2:B6:00 to 50:06:0B:00:00:C2:B9:FF
23	3	HP-Defined: 23	50:06:0B:00:00:C2:BA:00 to 50:06:0B:00:00:C2:BD:FF
24	4	HP-Defined: 24	50:06:0B:00:00:C2:BE:00 to 50:06:0B:00:00:C2:C1:FF
25	5	HP-Defined: 25	50:06:0B:00:00:C2:C2:00 to 50:06:0B:00:00:C2:C5:FF
26	6	HP-Defined: 26	50:06:0B:00:00:C2:C6:00 to 50:06:0B:00:00:C2:C9:FF
27	7	HP-Defined: 27	50:06:0B:00:00:C2:CA:00 to 50:06:0B:00:00:C2:CD:FF
28	8	HP-Defined: 28	50:06:0B:00:00:C2:CE:00 to 50:06:0B:00:00:C2:D1:FF
29	9	HP-Defined: 29	50:06:0B:00:00:C2:D2:00 to 50:06:0B:00:00:C2:D5:FF
30	10	HP-Defined: 30	50:06:0B:00:00:C2:D6:00 to 50:06:0B:00:00:C2:D9:FF
31	11	HP-Defined: 31	50:06:0B:00:00:C2:DA:00 to 50:06:0B:00:00:C2:DD:FF
32	12	HP-Defined: 32	50:06:0B:00:00:C2:DE:00 to 50:06:0B:00:00:C2:E1:FF

Important
Selecting an HP range that another student team uses will cause a conflict on the network. The equivalent concern mentioned previously for ensuring that unique Ethernet MAC address ranges are used applies here.

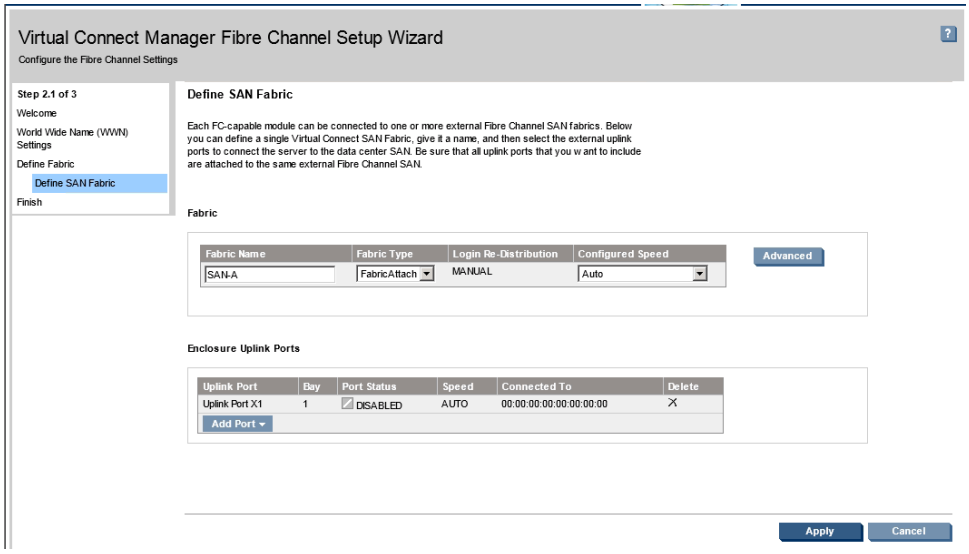
22. Confirm the correct non-conflicting address range has been selected by entering `confirm`. Then click **OK**.



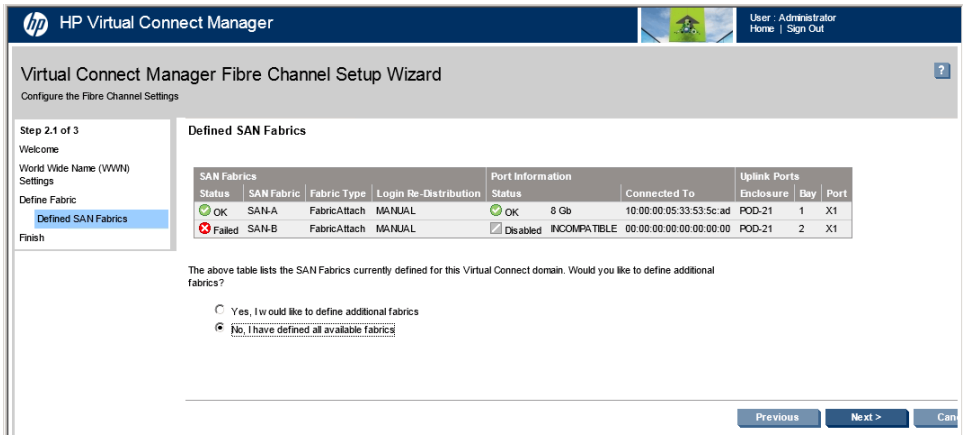
23. Select the **Define Fabrics** button and click **Next**.



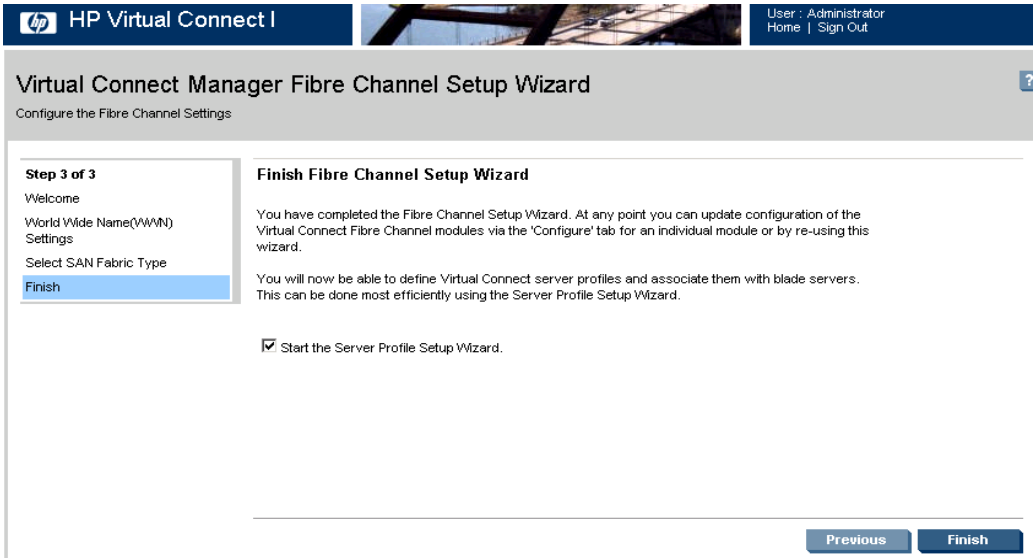
24. Create a SAN Fabric called SAN-A, leave type as Fabric Attached and select port X1 on Bay 1, click Apply, then create a second Fabric called SAN-B and use port X1 on Bay 2 module, **Click Apply**



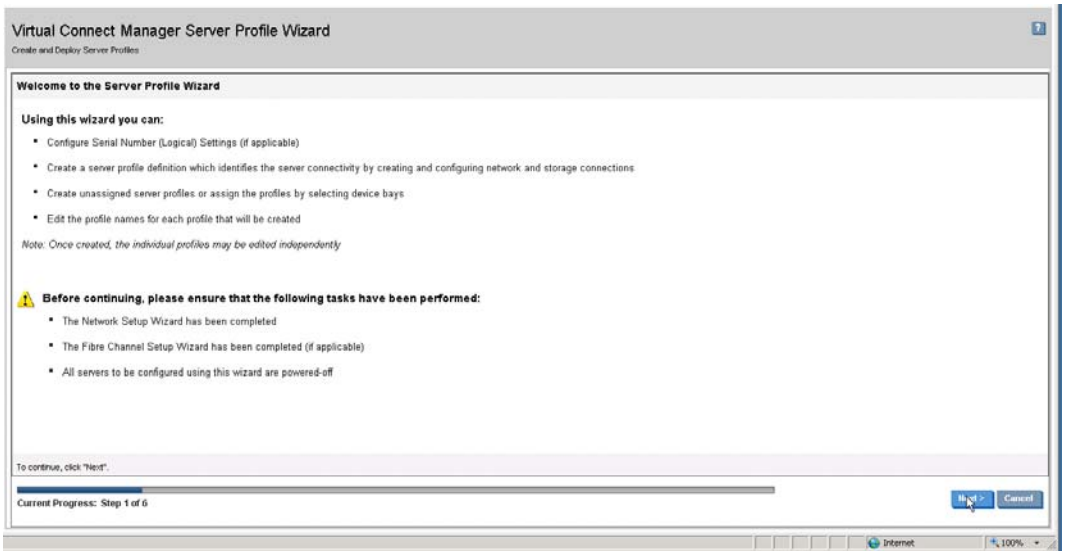
25. Select No, I have defined all available Fabric and **click Next**. The red x on SAN-B will go away once the next button has been pressed.



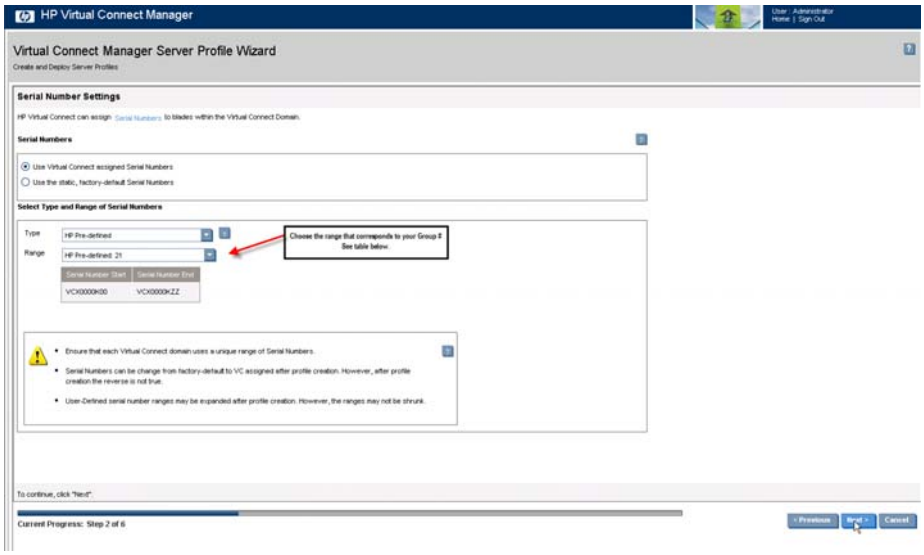
26. The completion window for the Fibre Channel Setup Wizard displays. Leave the check mark for **Start the Server Profile Setup Wizard** enabled and then **click Finish**.



27. At the Welcome screen, read the information and then **click Next**.



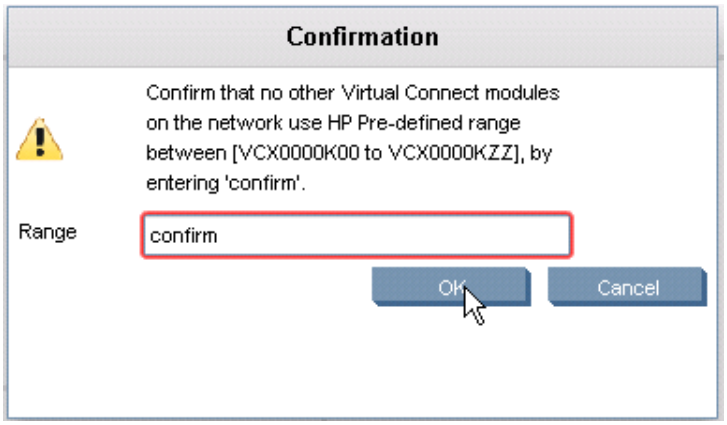
28. Select the **Use Virtual Connect assigned Serial Numbers (Logical)** button to allow VC to manage serial numbers. From the Type drop-down list, select **HP Pre-Defined.** Refer to the following table to determine your HP-Defined range identifier. Based on your POD ID, select **HP Defined: nn** for Range, where **nn** corresponds to your POD ID. **Click Next**.



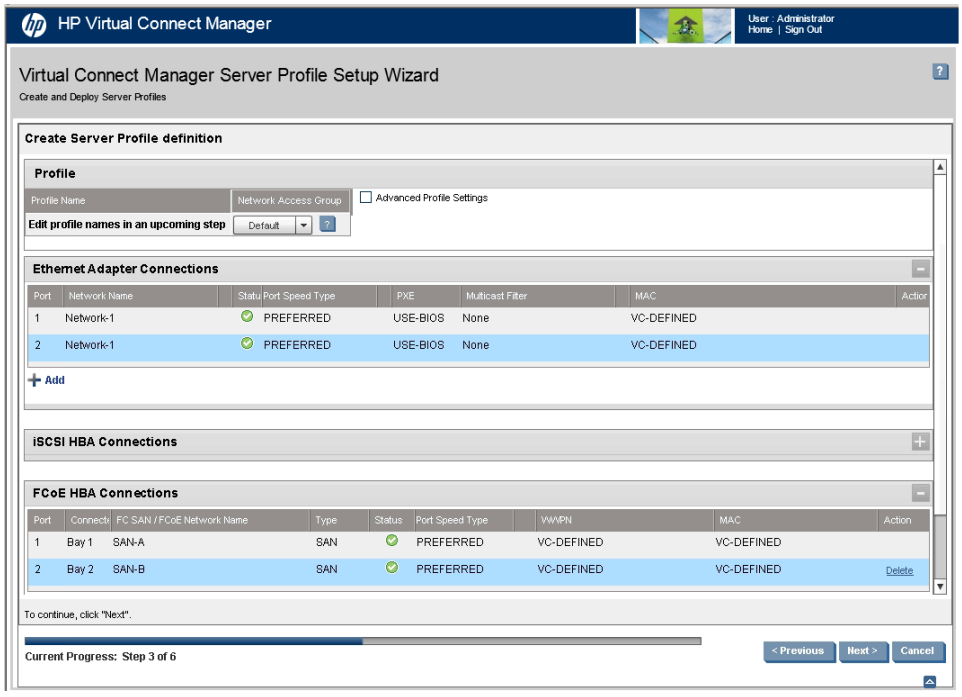
POD ID	Group	Range
21	21	HP-Defined: 21
22	22	HP-Defined: 22
23	23	HP-Defined: 23
24	24	HP-Defined: 24
25	25	HP-Defined: 25
26	26	HP-Defined: 26
27	27	HP-Defined: 27
28	28	HP-Defined: 28
29	29	HP-Defined: 29
30	30	HP-Defined: 30
31	31	HP-Defined: 31
32	32	HP-Defined: 32

! **Important**
Selecting an HP range that another student team uses will cause a conflict on the network. The equivalent concern mentioned previously for ensuring unique Ethernet MAC address and WWN ranges are used applies here.

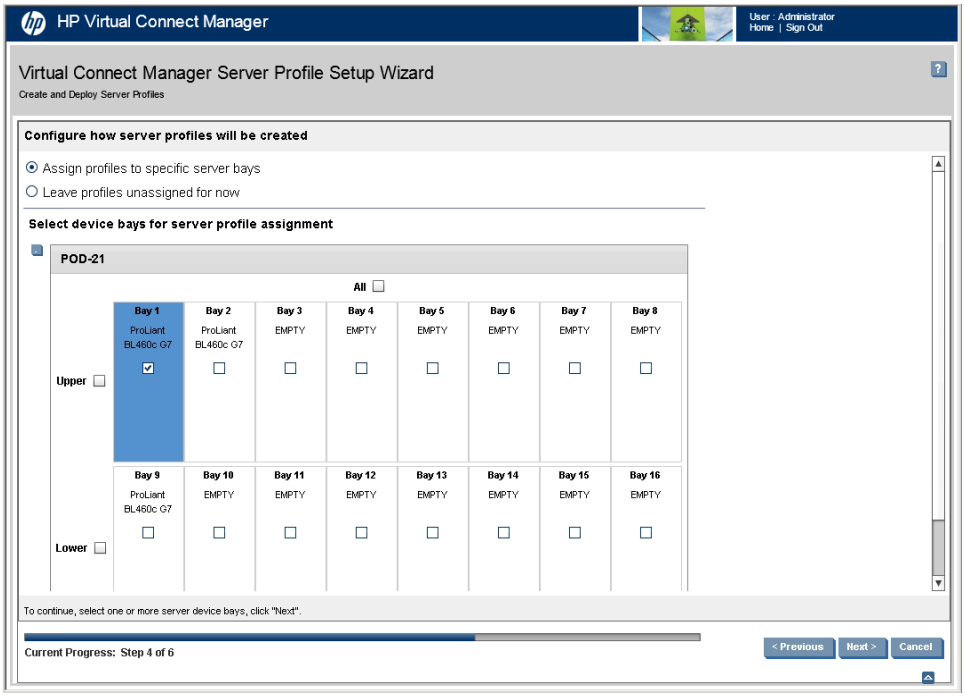
29. Confirm the correct non-conflicting address range has been selected by entering `confirm`. Then **click OK**.



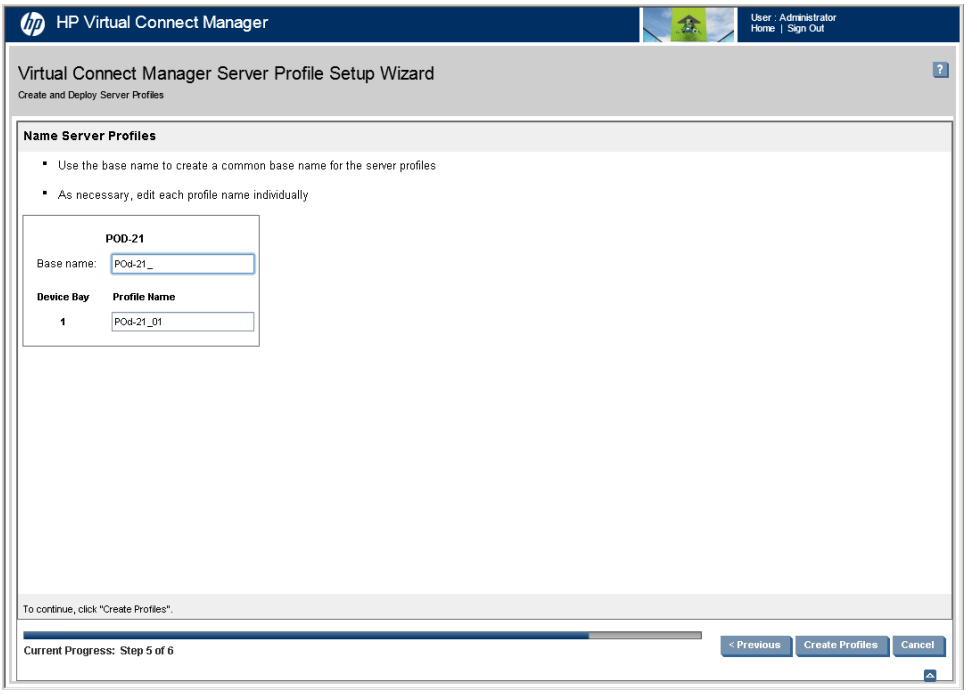
30. At the next screen you will create a profile that will be used as a template and could be assigned to one or many server bays. Click on the Unassigned network for NICs 1 and 2 and assign the network as Network-1. Do not edit the Network Speed at this time. In the FCoE HBA Connections space, assign Bay 1 Port to SAN-A and the bay 2 port to SAN-B. **Click Next**



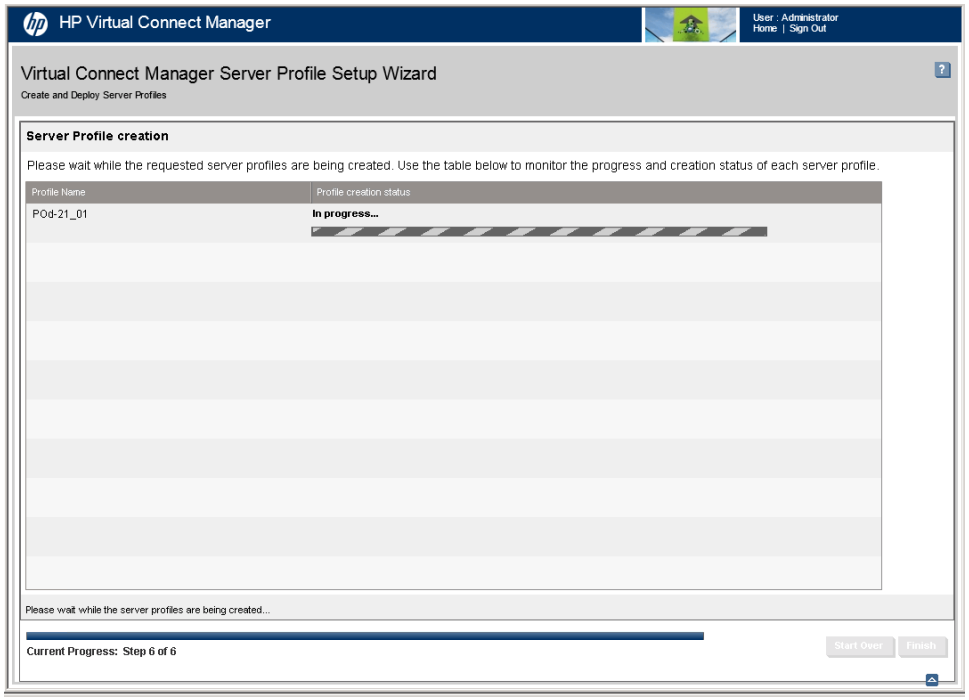
31. On the Configure how server profiles will be created screen, assing the profile to Bay 1 only. Click **Next.**



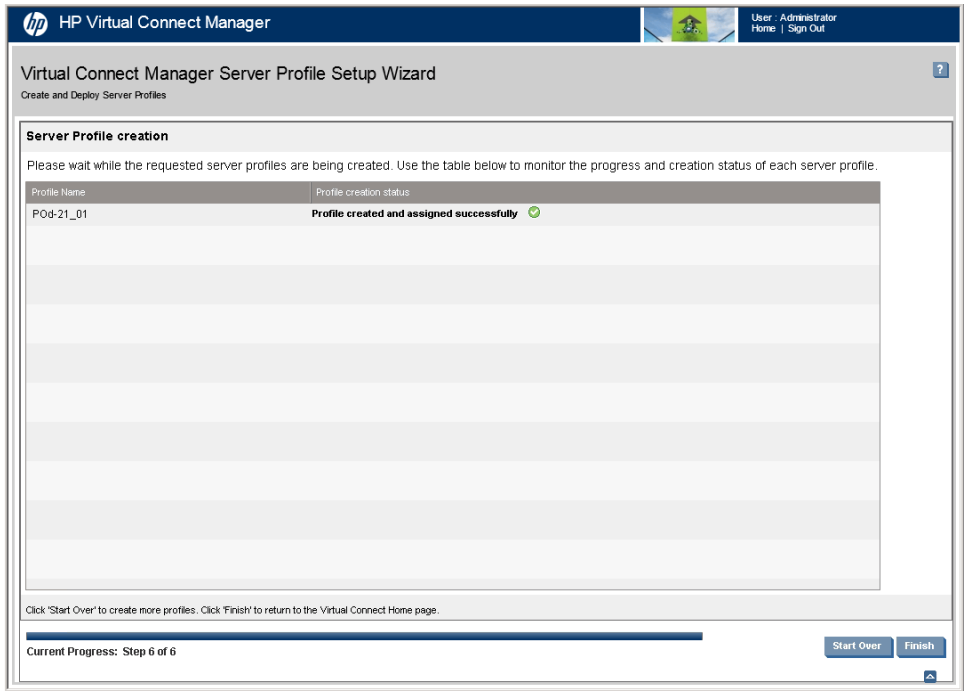
32. In the Name Server profile screen – Base Name – Type POD-xx_, where xx is your POD# and **Click Create Profiles**.



33. The Profile(s) will be created and assigned to the bay identified.



34. Once the profiles have been created **Click Finish**.



35. At this point the Domain has been created, along with the SAN Fabric and a server profile.

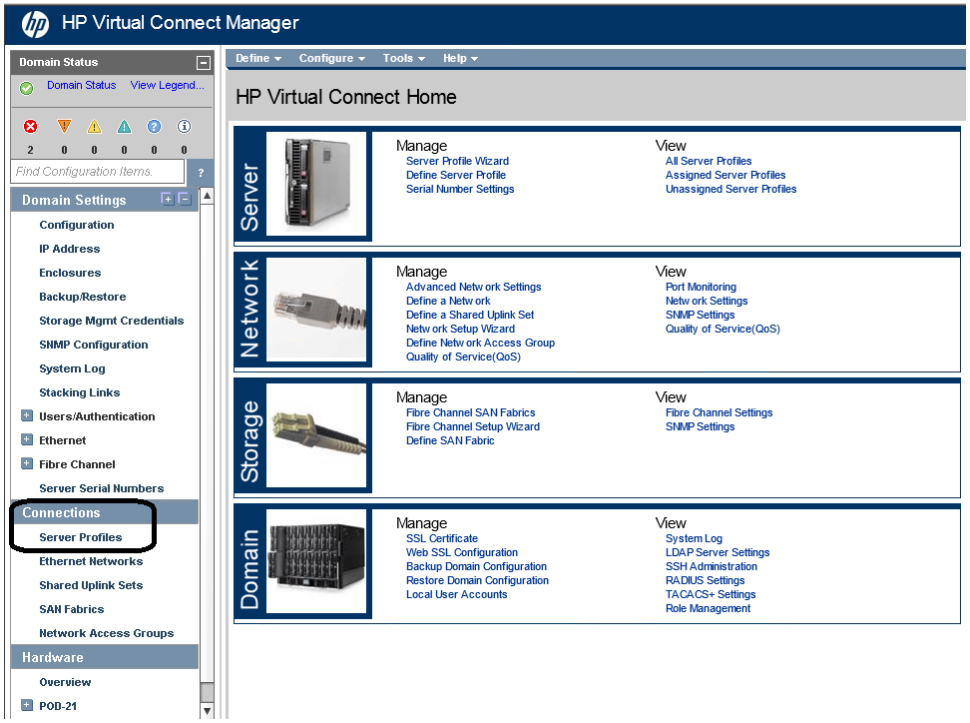
36. Tour around the VC domain and become familiar with the UI, before moving to Exercise 3.

Exercise 3 — Deleting the server profile

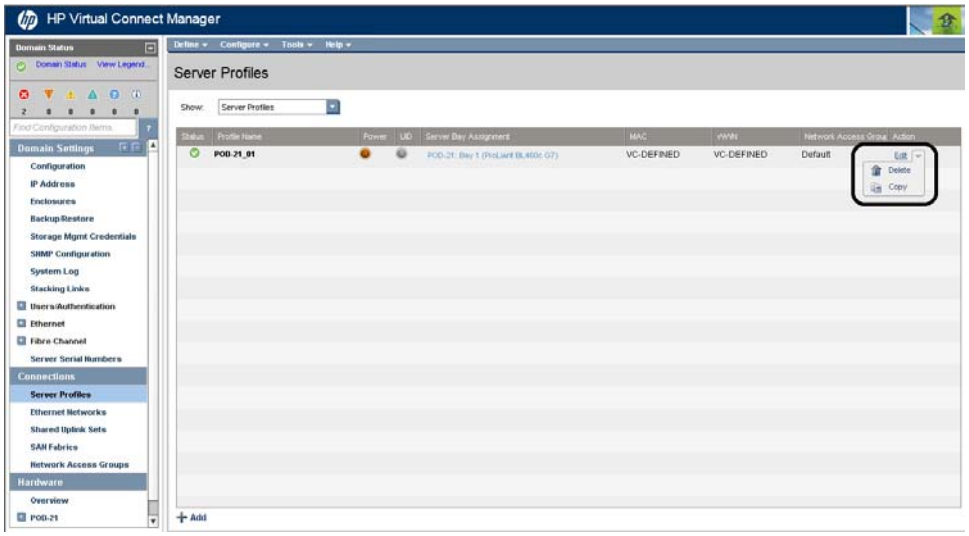
In this exercise, you are asked to delete the server profile and Network created by the Wizard. This server profile will not actually be used in labs that follow. When a server profile is needed, you will be asked to go through the steps to define one to develop familiarity with that process.

Important
Deleting this server profile is necessary to ensure that subsequent labs work appropriately based on the lab environment assumptions. Specifically, for servers that will boot from SAN, you want to ensure that the first set of WWNs is allocated to the server profile you explicitly create (in a later lab).

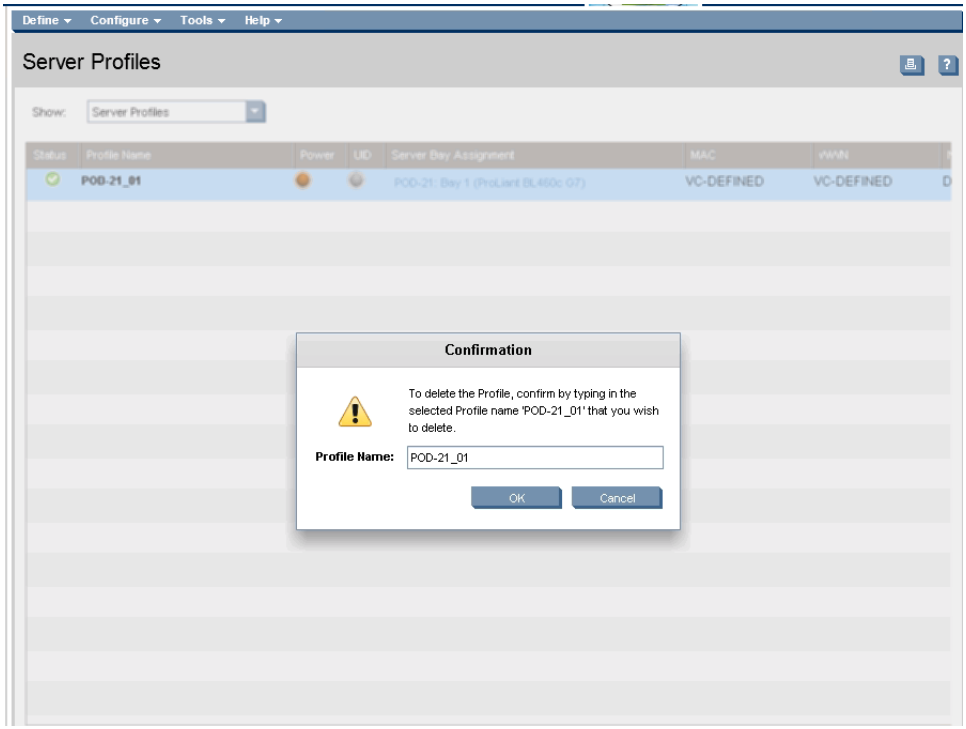
1. Under **Connections** in the navigation pane of the Virtual Connect Manager, click **Server Profiles**.



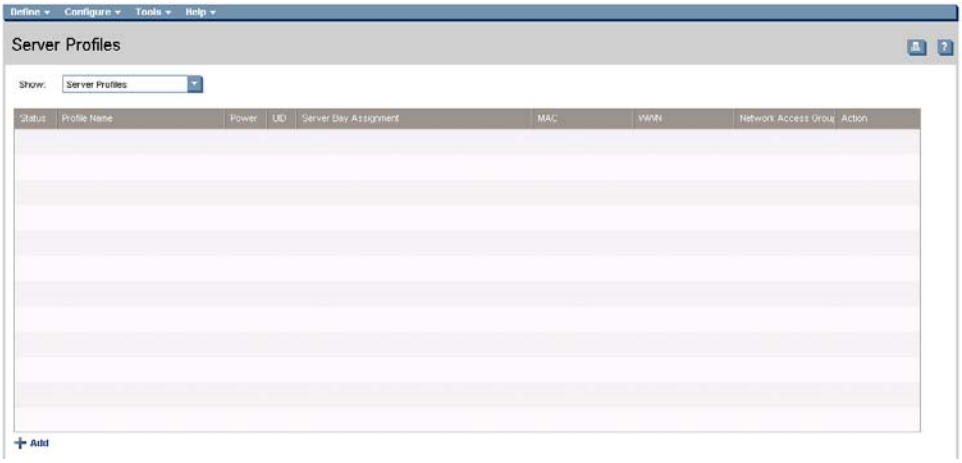
2. In the main window, click the arrow in the **Action** column for the profile to be removed. Then click **Delete**.



3. When asked to confirm, enter the profile name to be deleted. Click **OK**.



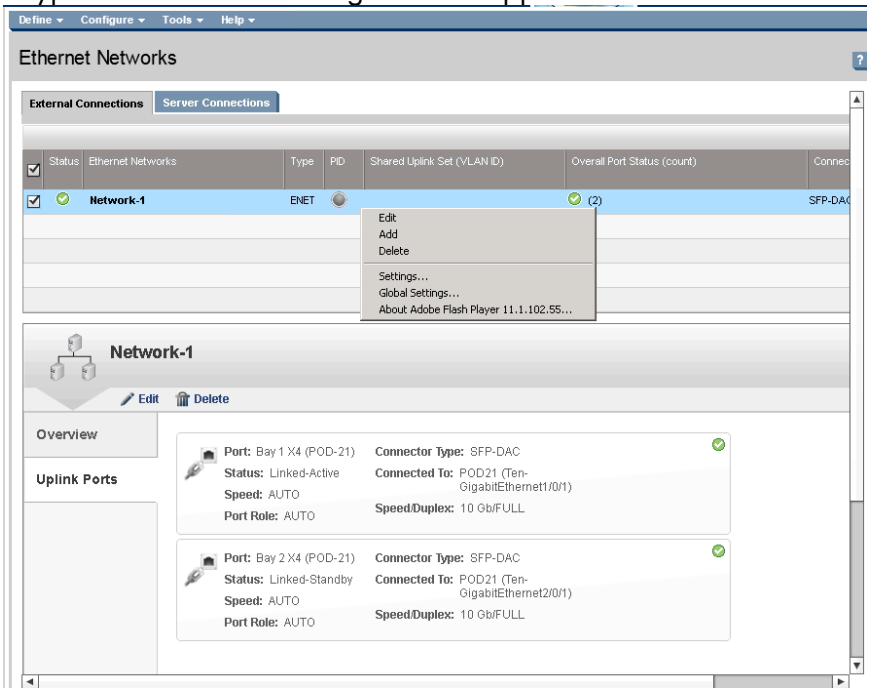
4. The listing of server profiles should now be empty.



Exercise 4 — Deleting the Network

In this exercise, you are asked to delete the networks created by the Network Wizard. In order to delete a network, you must ensure no profiles are using the network, as we already deleted the last profile, we know to be true. We no longer require this network as later labs will create different networks.

1. Under **Connections** in the navigation pane of the Virtual Connect Manager,, click **Ethernet Networks**.
2. Left click on the network, so the blue bar appears, then right click and select Delete. Alternatively, scroll to the far right and click the Edit/Delete drop down.
3. Type "delete" in the dialog box that appears to confirm the deletion



Summary

During this lab exercise you accessed the remote lab and you defined a VC domain using the Virtual Connect Manager's Domain Setup Wizard. Your VC domain consists of a single HP BladeSystem c7000 enclosure and includes:

- Two Virtual Connect FlexFabric modules
- Several server blades

The VC domain has been configured to use HP predefined ranges for Ethernet MAC addresses. The Server VLAN Tagging Support parameter was set by default to Expanded VLAN Capacity mode to provide the extensive and configurable VLAN management strategy used in later lab exercises. This includes defining Shared Uplink Sets and assigning multiple VLANs to a Network Connection, which will be discussed in a later lab.

A Simple vNet was created as was redundant SAN Fabric connections.

You also created a Server Profile, using the profile creation wizard and connected it to the LAN and SAN connections created earlier.

Implementing a Simple vNet

Lab 2

Objectives

After completing this lab, you should be able to:

- Define a simple HP Virtual Connect (VC) network and assign two uplink ports connecting from two different VC Ethernet modules
- Configure the Network Preferred and Maximum speed settings
- Examine the status of the uplink ports corresponds to an active/standby mode of operation
- The Network and server profile created in this lab will be used in the following lab.

Introduction

In this lab, you will use Virtual Connect Manager (VCM) to create an Ethernet Network that is commonly referred to as a *vNet*. Within VCM, a vNet is listed under the folder named Ethernet Networks in the navigation pane.

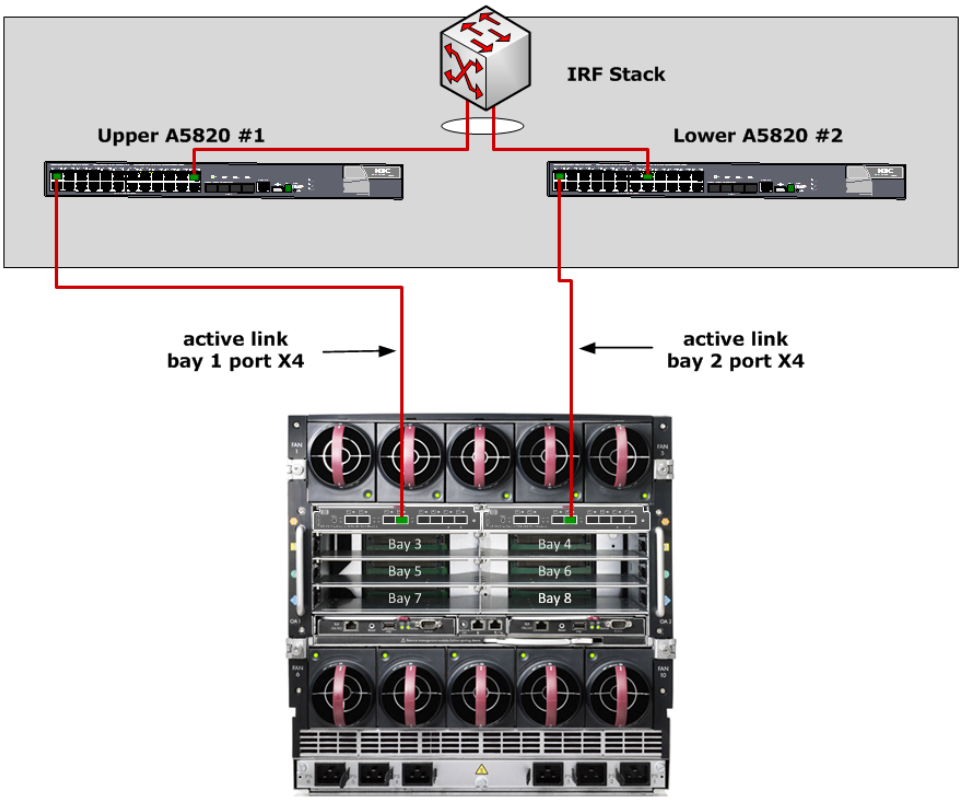
If no VLAN support is required, or if support for a single specific VLAN is needed, a vNet is a very simple network to configure and manage within Virtual Connect. A simple vNet is used to pass untagged frames between server NIC and external switch. In this case the network switch port would be configured as untagged or as an Access port, any/all VLAN tagged frames will be dropped.

However, a vNet can also be used to pass many VLANs (a VLAN Tunnel) without modifying the VLAN tags, and therefore can function as a transparent VLAN pass-through or tunnel. The vNet tunnel has no limit to the number of VLANs it can support when configured for Tunnel VLAN Tags mode. In this case the network switch port would be configured as tagged or as a VLAN Trunk port, of the VLANs passed through a tunnel, one VLAN could be untagged.

No special upstream switch configuration is typically required for this scenario, only that the switch port be untagged in the VLAN that transports the untagged traffic.

This initial VC network involves using a single uplink port, (per VC module) connecting to an upstream switch. This lab is focused on vNet and profile configuration, a server profile will be used to examine the new Min/Max NIC speed setting which are configured within each network.

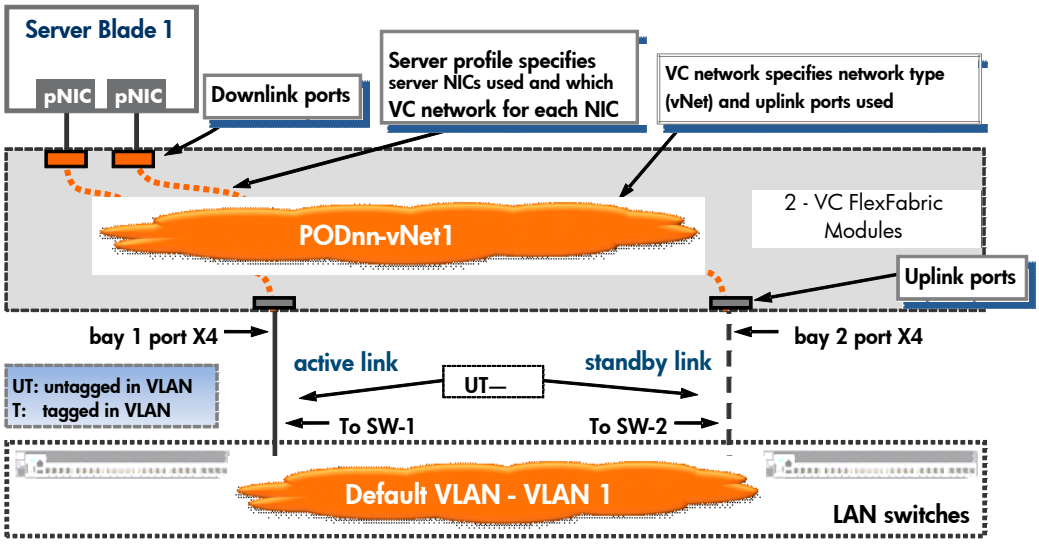
Network diagrams



Physical view of the LAN connections

The Ethernet cables connecting the Virtual Connect Ethernet modules to the upstream LAN switches are already attached. All required switch configuration has been completed before the beginning of class.

Unless otherwise specified by the instructor, you will use port X4 on each of the two Virtual Connect FlexFabric modules installed in Bays 1 and 2 of the enclosure for this lab.



Logical view of the VC network configuration

This diagram shows a logical view of the VC network configuration. You can specify any name you want for the vNet you configure. In this diagram, **PODnn-VNet** is used, where **nn** represents the POD ID.

For this lab, the upstream switches are configured such that the connected ports are untagged members of VLAN 1. This implies that any traffic for VLAN 1 is transmitted as untagged Ethernet frames.

Exercise 1 — Defining a VC Ethernet network

In this exercise, you use Virtual Connect Manager to define an Ethernet network representing a simple vNet.

1. Open a web browser and access the Virtual Connect Manager home page using the IP address (for your POD) used in the previous lab.
2. Login using the "admin" account created in LAB 1

   The login should be "admin" with the password "hpinvent"

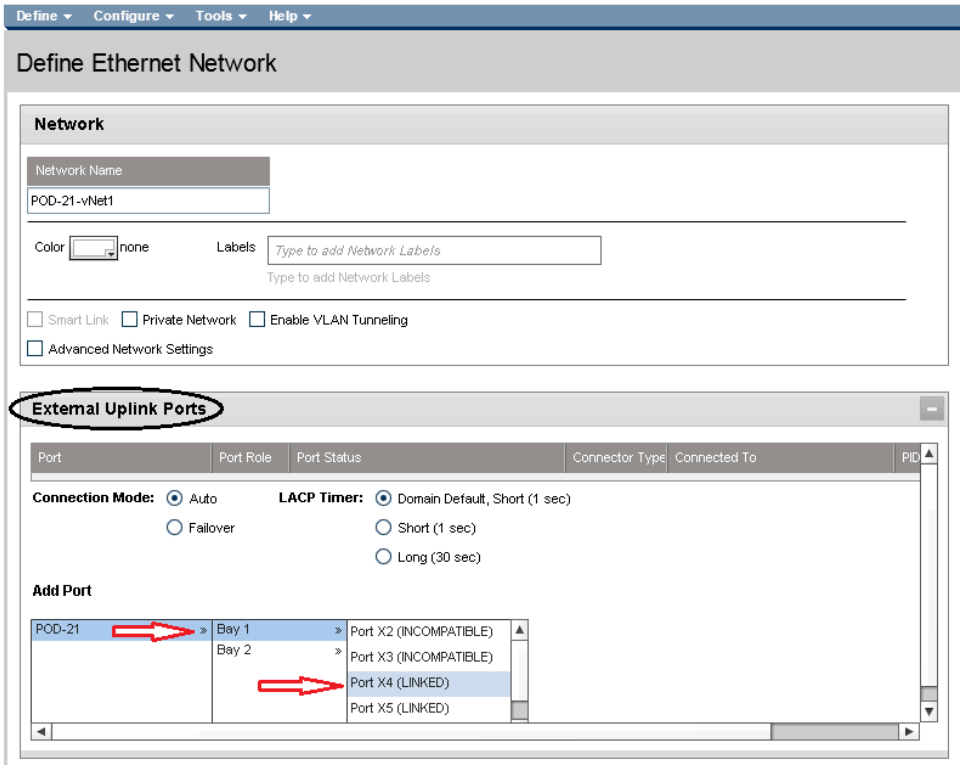
   Note
   If you have trouble logging in with this account, use the Administrator account and password provided in LAB 1

3. From the Virtual Connect Manager home page, in the toolbar, select **Define** → **Ethernet Network**.

4. For the Network Name, enter `PODnn-vNet1`, where **nn** is your POD ID. Add the first external uplink port by clicking **Add Port > <enclosure-name> Bay 1 > Port X4 (Linked)**.

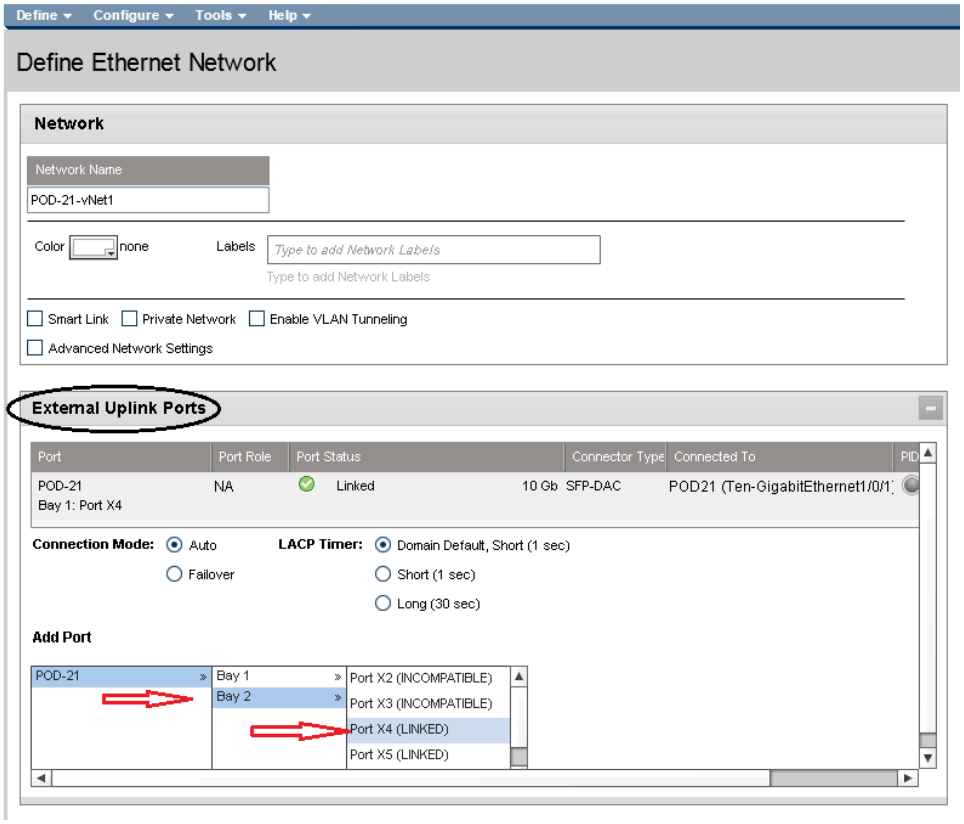
Note
This port is from the VC FlexFabric module in interconnect **Bay 1**.

Important
If you do not have a (Linked) status, have the instructor ensure that the switch ports are in an UP state.



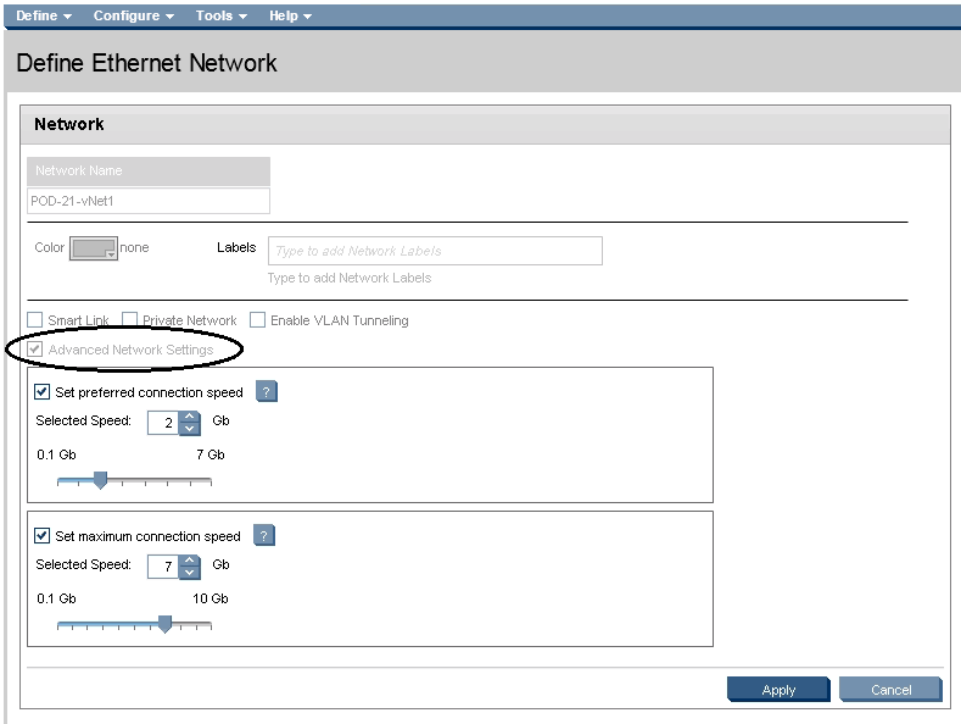
5. Add the second external uplink port by clicking **Add Port section <enclosure-name> Bay 2 > Port X4 (Linked)**. Then click **Add** to save your changes.

Note
This port is from the VC FlexFabric module in interconnect **Bay 2**.



6. **Click** on the Advanced Network Settings check box, then click on Preferred and set the speed to 2Gb. Click on Maximum and set the speed to 7Gb.

7. Click Apply



8. In the following window, click **Apply** to save your changes. This results in a redundant link topology (an Active/Standby network) for the vNet. One uplink port is the active port and the other operates as a standby port.
9. Edit the vNet and verify that both uplinks were added and that the Advanced Speed sets were configured.

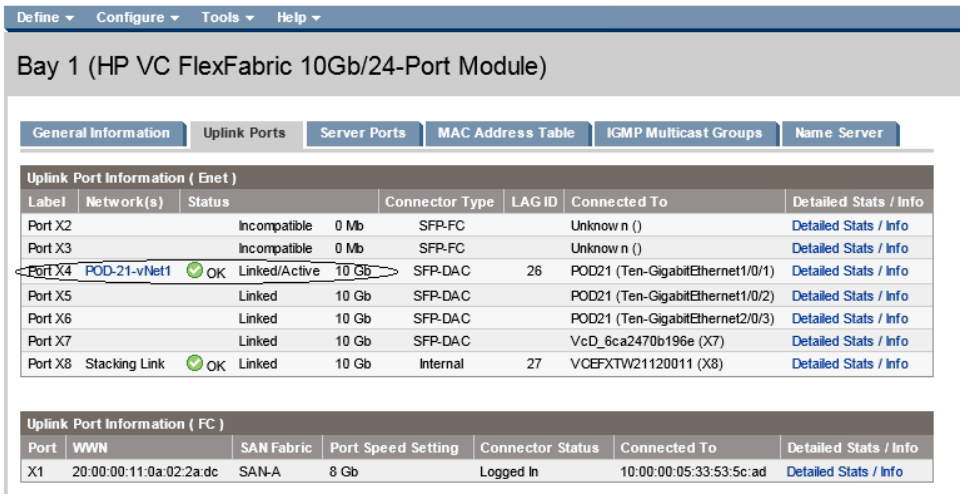
Exercise 2 — Examining the status of the uplink ports

1. In the navigation pane Hardware Configuration section, expand **POD-xx>Interconnect Bays**. In the main window, click **Bay 1 (LAN+SAN),** which contains a VC FlexFabric module.
2. Select the Uplink Posts tab and examine the status of port X4 and notice the LAG ID and MAC address of the upstream switch.

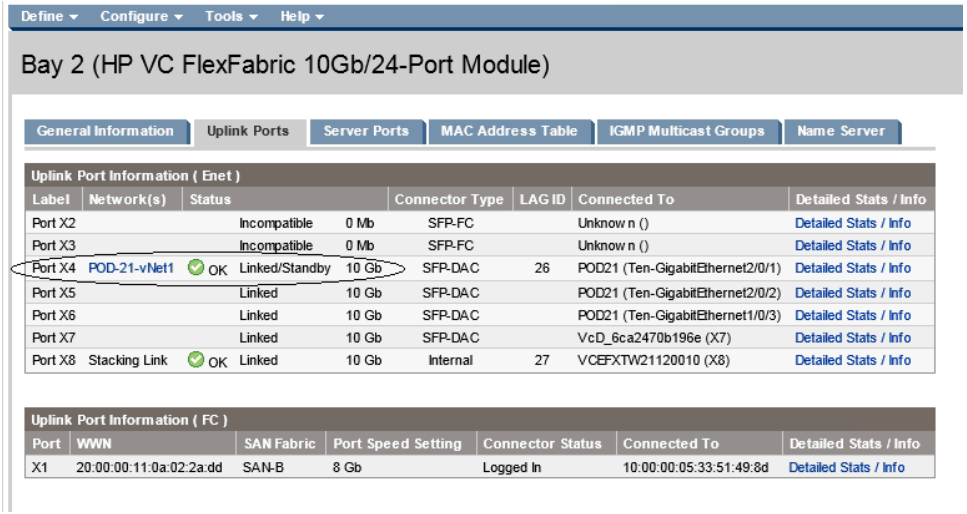
   For this VC network, a single uplink port of the Virtual Connect FlexFabric module in Bay 1 is used to connect to the upstream switch, an additional uplink is provided for redundancy and fail-over.

   Technically, from the Virtual Connect perspective there are two uplinks available to this VC network, one on each FlexFabric module. Only one is allowed to be active in this scenario; otherwise, there would be the potential for a network loop and the need to use a protocol such as Spanning Tree to manage the network loop, which Virtual Connect does not implement. Instead, by ensuring that at one uplink is active (in this scenario); Virtual Connect prevents a network loop from occurring. If the first network switch or cable were to fail, VC would failover to the standby uplink, by making it active.

As you can see from the status windows, the second uplink is in a standby state. Similarly, if there were additional **individual** uplinks assigned to this VC network, they would operate in a standby mode as well. This behavior is identical to the functionality provided to server ports that are configured as members of a network fault-tolerant (NFT) NIC team.



3. In the Hardware Configuration section of the navigation pane, expand **POD-xx>Interconnect Bays**. In the main window, click **Bay 2 (LAN+SAN),** which contains a VC FlexFabric module.



About active/standby operation

By connecting an uplink from each module to a vNet, you have provided a redundant path to the network. Because each uplink originates from a different VC Ethernet module, one uplink is active and the second is in standby mode. This configuration enables you to lose an uplink cable, an upstream switch, or depending on how the NICs are configured at the server (teamed or unteamed), even a VC Ethernet module. The VC FlexFabric modules are connected internally using two 10Gb connections, allowing network traffic to flow between the modules and out to the network.

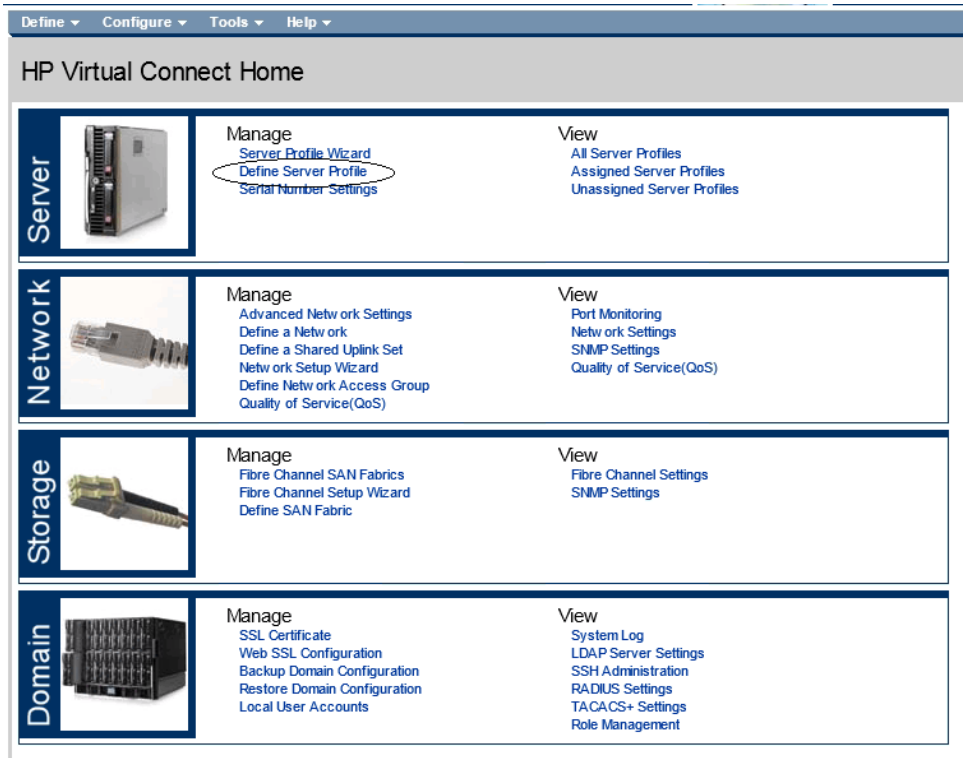
About Smart Link

In this configuration, the Smart Link parameter should **not** be enabled on the vNet. Smart Link is used to turn off downlink ports to servers within Virtual Connect if **all** available uplinks to a VC network (simple vNet or a Shared Uplink Set) are down. You will use Smart Link in a later lab exercise.

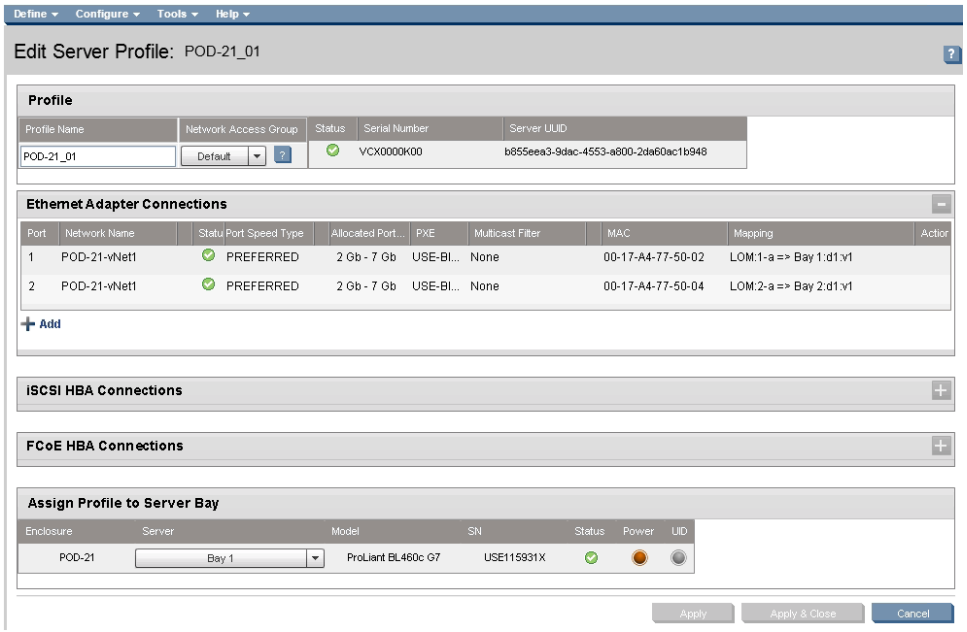
Exercise 3 — Creating a server Profile

In this exercise, you will create a server profile and connect it to your network. You will also validate the new Min/Max NIC speed feature.

4. From the Virtual Connect Manager home page.
5. In the server area select **Define Server Profile**,



6. Create a server Profile called POD-xx_01where **nn** is your POD ID and connect both the default NICs to the Network created earlier. Do not connect to the SAN fabric.
7. Apply the profile to the server in Bay 1

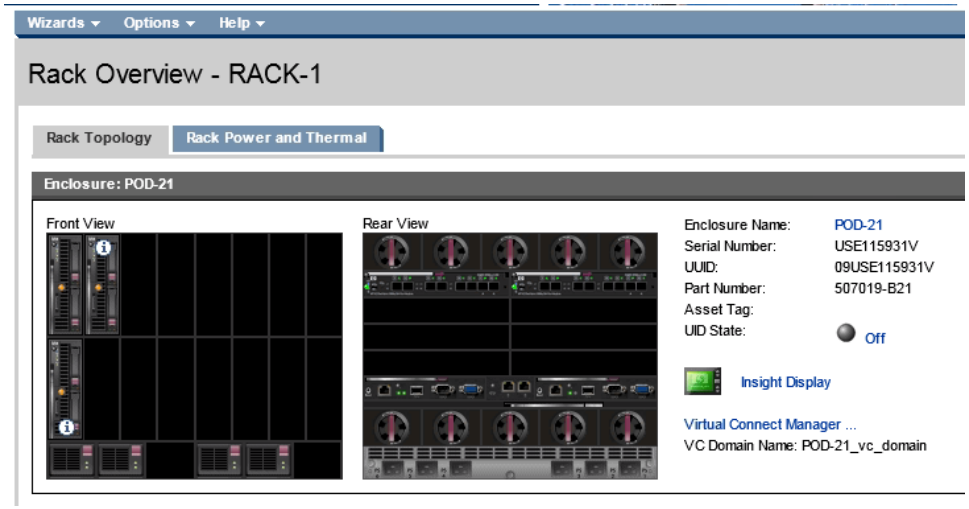


8. Note the speed that each NIC is configured for. Both the Min. and Max.
9. Use the Custom speed setting and attempt to change the speed of the NIC to a Higher Speed. **Click** on **PREFFERED** and **select Custom** and change the NIC speed. What is Max speed you can set the NIC to?
10. Leave the Speed set to Preferred and save any changes made to the server profile.
11. Edit the Network, under Advanced Settings, change the preferred speed to 4Gb and the Maximum speed to 10Gb and save the changes.
12. Go back to the server Profile and determine whether these changes have taken effect. You will need to make a change to the profile and apply it, before these changes will take effect.
13. What is the Min speed now?
14. What is the Max speed now?

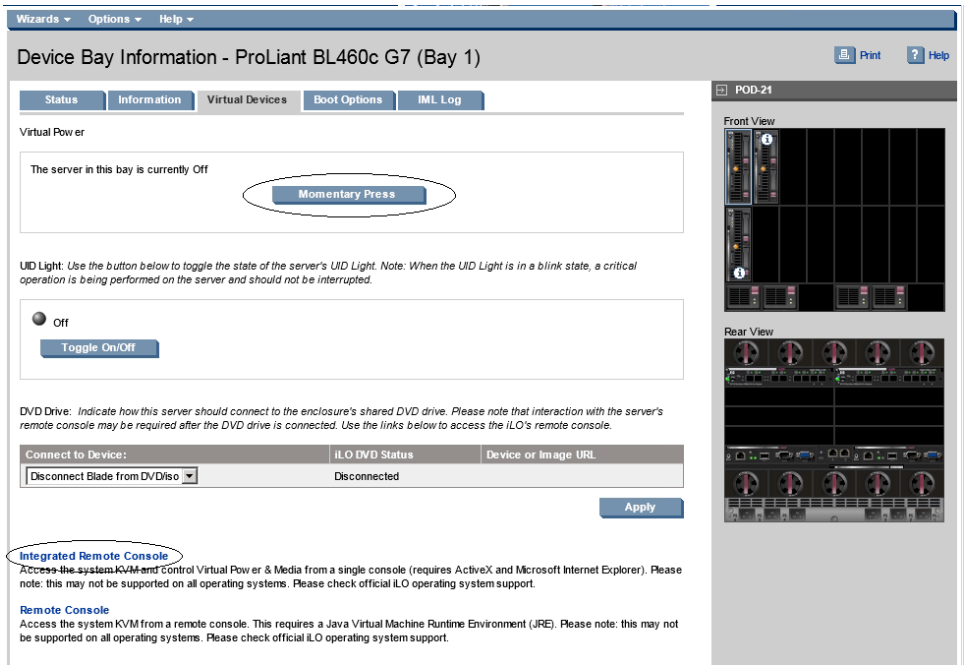
Exercise 4 — Validating Network Connectivity

In this exercise, you will use the OA and iLO to connect to and boot the server in bay 1, then verify that it has received an IP Address from the network.

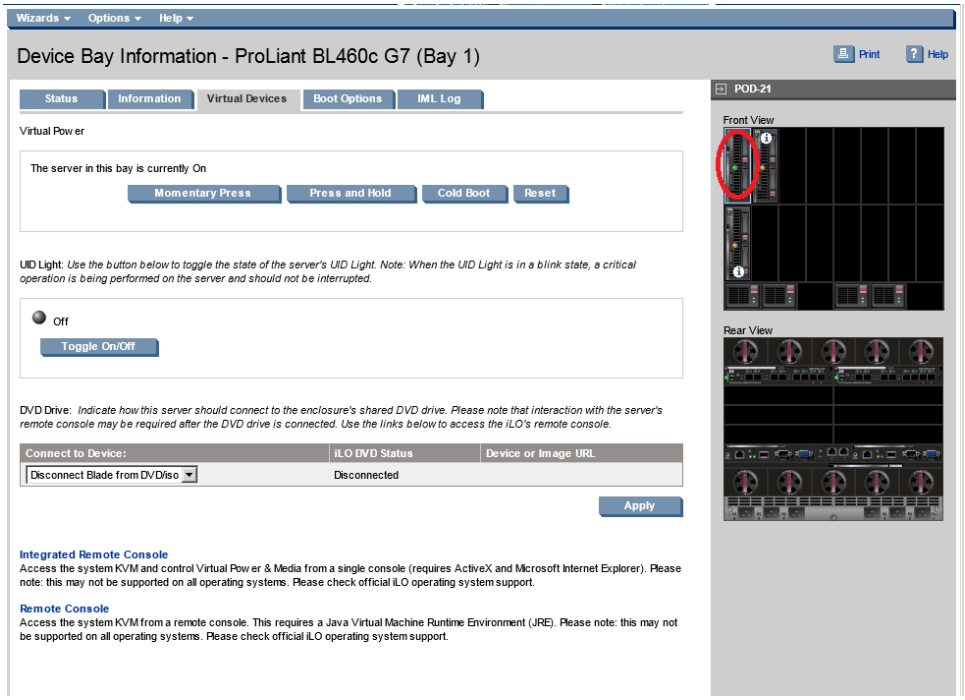
1. From the web browser access the OA home page for your POD.
2. You will notice that the server in Bay 1, have no exclamation mark over it, this indicates the server is ready to use and has a Virtual connect profile assigned, the other servers in the enclosure, do not have profiles assigned at this time.



3. Click on the server in Bay and select the Virtual devices tab and press "Momentary Press". As the server is booting, Select "Integrated Remote Console" from below and open an iLO Session with the server.

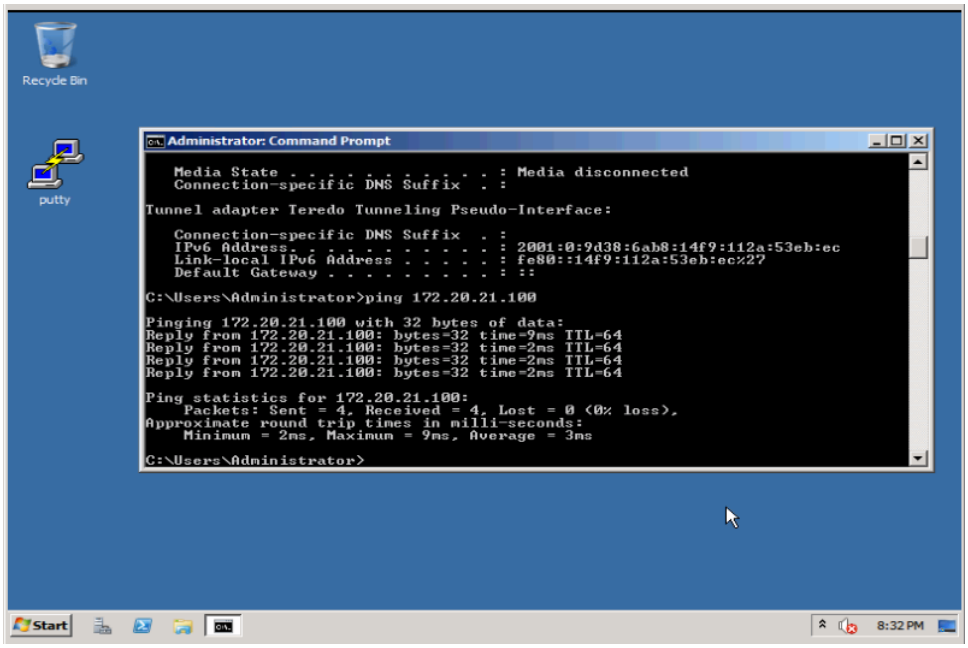


4. You will notice that the server power indicator light is now GREEN.



5. Login to Windows using the "Administrator" account with password "HP1nvent".

6. Once the server has booted, log in to the Windows OS through the iLO, open a COMMAND windows and type IP Config, verify that the server has a DHCP provided address on subnet 172.20.x.x, then ping the OA address at 172.20.xx.100, were xx is you POD ID.



7. Optionally, if you wish to test Virtual Connect Uplink fail-over and the effect it has on the server, you could start a ping –t 172.20.xx.100 in a command window, then Edit the vNet and drop the "Active" uplink and save the network.

Watch the PING and see what the response is. Then add the link back in and save the vNet. Watch to see whether this link becomes active again, or remains as a standby link.

8. When you have completed this activity shut the server OS down gracefully.

Summary

By connecting two uplinks from this vNet through two different VC FlexFabric modules to the upstream switches, you have provided a redundant path to the network. Because each uplink originates from a different VC FlexFabric module, one uplink is active and the second is in standby mode.

This configuration provides the ability to lose an uplink cable, network switch, or depending on how the NICs are configured at the server (teamed or unteamed), even a VC FlexFabric module.

Notice that you were not asked to enable the Smart Link parameter for this vNet. In this type of configuration, Smart Link should not be enabled. Smart Link is used to turn off downlink ports within Virtual Connect, if all available uplinks to a VC network (vNet or Shared Uplink Set) are down.

You configured and experimented with the new Min/Max NIC speed setting. This new feature provides the ability to oversubscribe NIC downlinks, which we previously did not provide.

Implementing Boot from SAN with FlexFabric

Lab 3

Objectives

After completing this lab, you will be able to:

- Define a server profile for a host that will boot from SAN.
- Verify that the host boots into Microsoft Windows.
- Move a server profile from one server bay to another server bay in the Virtual Connect domain and verify server operation.

Description

In this lab exercise, you use Virtual Connect Manager to define a server profile that uses the Boot from SAN (BFS) capability. The Virtual Connect SAN Fabrics you implemented in the previous lab exercise are used for this activity. As part of the environment preparation you delete the existing server profiles and defined a new profile with two FlexNIC connections and two FlexHBA connections.

You verify the Windows host boots from SAN successfully and that you can ping the default gateway for one of the VLANs you also assign to the server profile. Then, you move the server profile to another server bay of the Virtual Connect domain and verify proper operation for that server.

Important: This lab requires that you delete the existing server profiles. The reason is that the BFS entries on the SAN controller are preconfigured. The BFS definitions require a server's WWPN be provided, which in our lab environment is based on particular WWNs associated with your Virtual Connect domain. Specifically, the Virtual Connect-defined WWNs associated with your assigned range based on your POD ID. If the wrong WWN is presented from the server profile to the storage controller, then the Boot from SAN request will fail

---

Network Diagrams

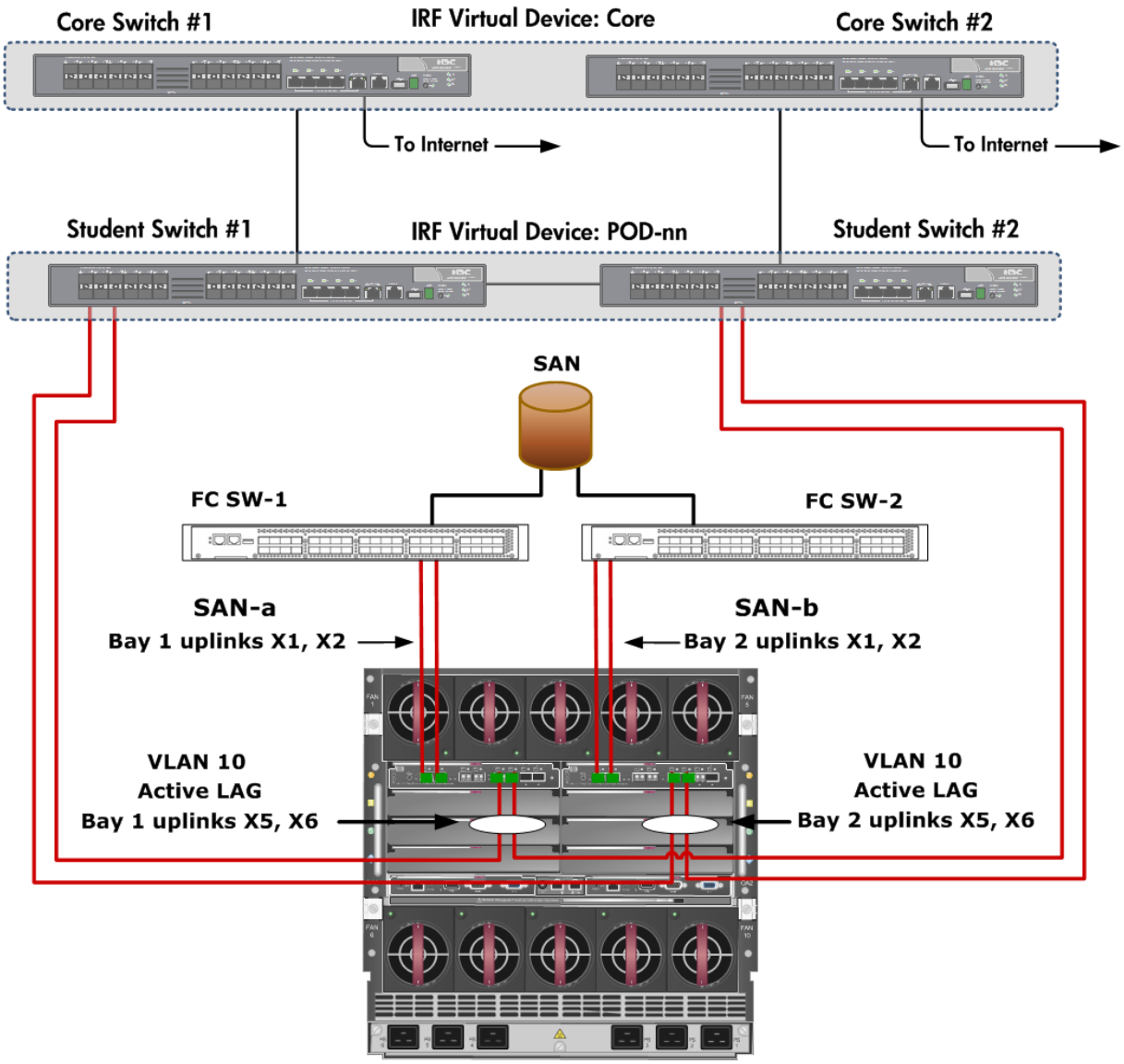


Figure 1: Physical view of the Fibre Channel connections

For this scenario, both Virtual Connect FlexFabric modules are used and two uplinks from each module are connected to the Fibre Channel SAN switches. Your previously defined Shared Uplink Sets will also be used.

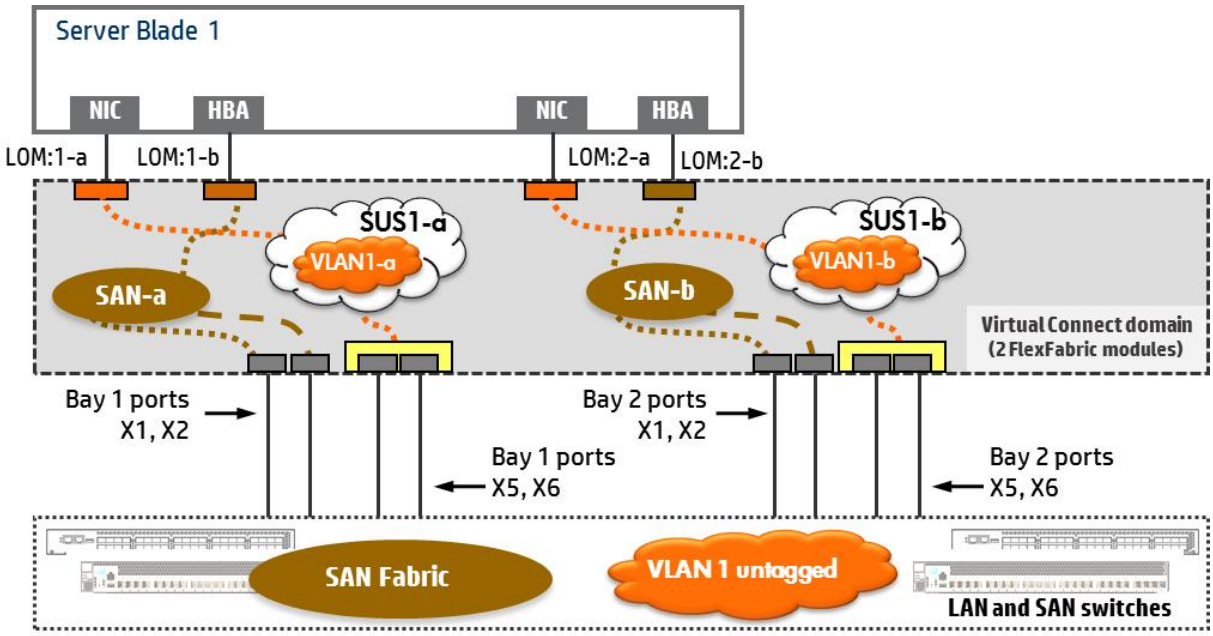


Figure 2: Logical View of the Virtual Connect Networks and SAN Fabric Configurations

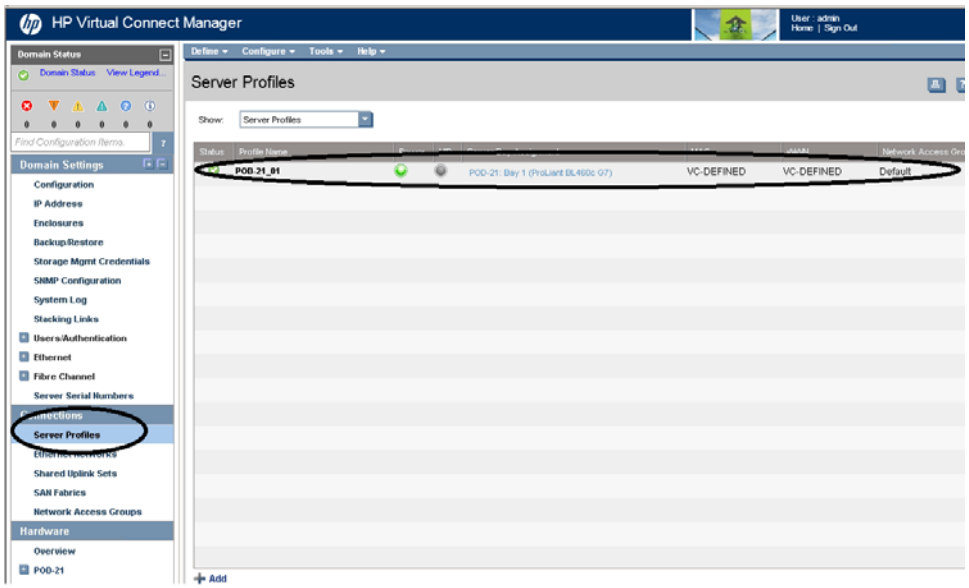
The Virtual Connect server profile will consist of two FlexNIC connections and two FlexHBA connections. The server profile you define in this lab will use two VLANs previously assigned to the Shared Uplink Sets. One VLAN will be assigned to a FlexNIC mapped to Network Connection 1, and the other VLAN to a FlexNIC mapped to Network Connection 2. The Fibre Channel SAN Fabrics will be assigned to two Fibre Channel over Ethernet (FCoE) host bus adapter (HBA) connections in the server profile. For, the FCoE connections, you will also specify a target World Wide Port Name (WWPN) and LUN identifier.

Verification of network access will involve ensuring IP addresses are assigned to the server ports followed by pinging the switch operating as a default gateway. For this simple network environment, you will only verify access to VLAN 10. Initially, you assign the server profile to the server in bay 1, and then then bay 2.

Exercise 1 – Modifying a Server Profiles to Support Boot from SAN

In this exercise, you use the Virtual Connect Manager (VCM) to modify the server profile created in lab 1. When modifying a server profile on a VC Ethernet module that will be used with a server supporting FlexFabric ports (or NICs), you have the option of allocating bandwidth across one to four NICs, or one to three NICs and a FC HBA. In this exercise, you will edit the existing profile and ADD SAN connections, and then configure those connections for Boot to SAN.

1. Open a web browser and access the OA for your POD, verify the servers in Bays 1 and 2 are shutdown.
2. Open a web browser and access the Virtual Connect Manager home page and log in using the admin account created in lab 1.
3. In the left tree view, under connections, click on server profiles.
4. Your profile should be shown in the right pane, select the profile and edit it.

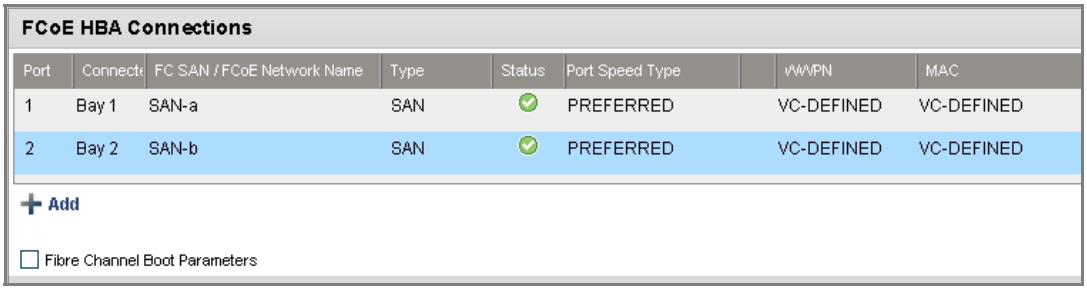


5. From the Edit Server profile page, under FCoE HBA Connections, for Bay 1 select SAN-A and for Bay 2 select SAN-B. The speed should default to 4Gb Min. and 8Gb Max.

Port	Bay	FC SAN Name
1	1	SAN-A
1	2	SAN-B

6. In the FCoE HBA Connections section, assign the information listed in the following table.

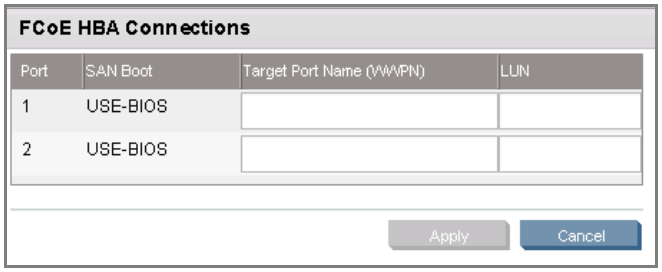
Note: For the blade server you are working with, Port 1 corresponds to FlexNIC 3 (LOM:1-b) and Port 2 corresponds to FlexNIC 4 (LOM:2-b).



7. Click the **Fibre Channel Boot Parameters** checkbox to enable it. Then select **Primary** for Port 1 and **Secondary** for Port 2.

8. Once you check the Fibre Channel Boot Parameters checkbox, the FCoE HBA Connections Box appears. Enter the Boot parameters from the table below.

9. Set USE-BIOS for ports 1 and 2 to Primary and Secondary, respectively.

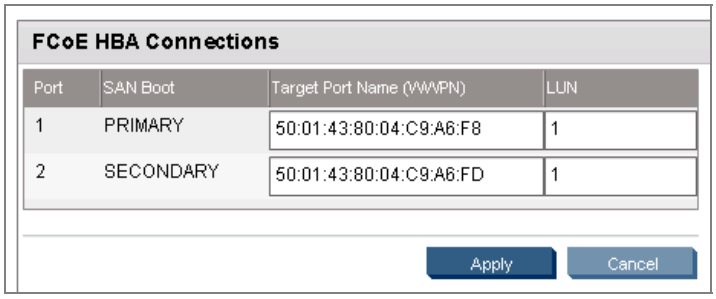


The dialog window shown above appears.

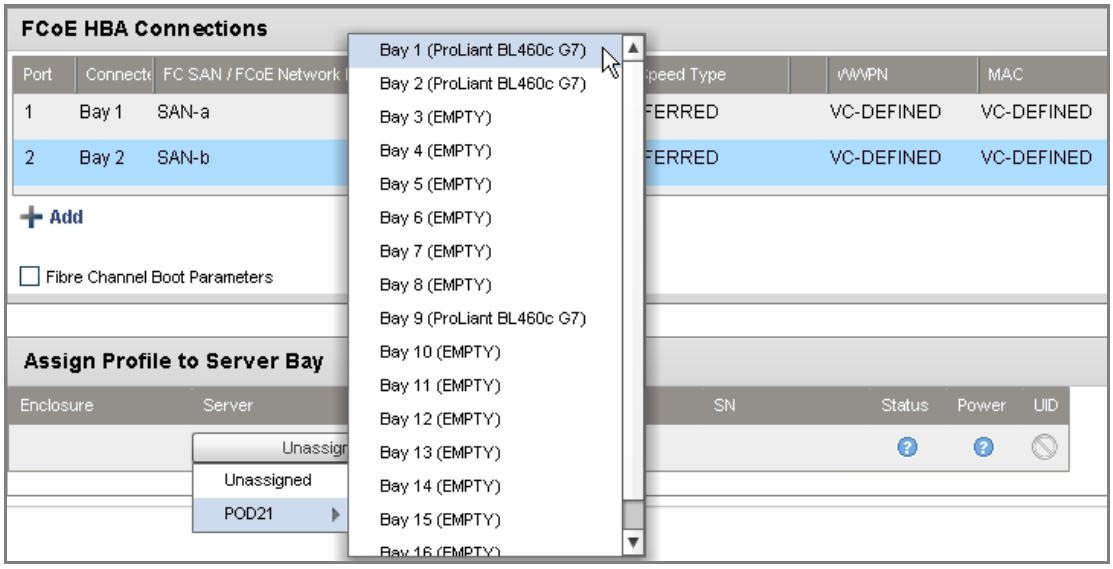
10. Specify the following information.

Port 1	
Use BIOS	Primary
Target Port Name (WWPN)	50:01:43:80:04:C9:A6:F8
LUN	1
Port 2	
Use BIOS	Secondary
Target Port Name (WWPN)	50:01:43:80:04:C9:A6:FD
LUN	1

The target world-wide port name (WWPN) is that of a storage controller as opposed to the WWPN of a SAN switch.

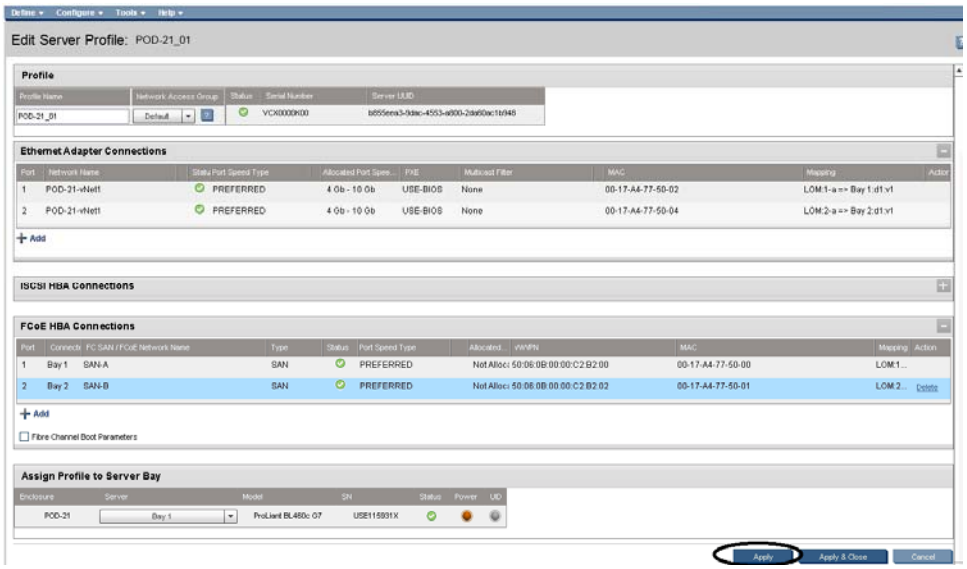


11. Click Apply to save the Boot from SAN settings.



12. In the Assign Profile to Server Bay section, click the down arrow and then click PODnn > Bay 1 (ProLiant 460c Gen7).

13. Then click Apply to save the changes to the server profile.



14. Examine the Mapping column for the Ethernet and FCoE connections.

    Notice that LOM:1-a and LOM:2-a are mapped to the two Ethernet FlexNICs, and LOM:1-b and LOM:2-b are mapped to the two FCoE FlexHBAs.

    Also, notice the Allocated Port Speed column for the FlexNICs and FlexHBAs. Since the FlexHBA connections take precedence in terms of initial bandwidth allocation, 4 Gb has been allocated as the minimum speed. Since FCoE in Virtual Connect supports speeds of 1, 2, 4 and 8 Gb, the maximum speed allowed will be 8 Gb.

    The FlexNICs are therefore allocated the remaining bandwidth of each physical adapter, which is 6 Gb.

15. Click Cancel to close the Server Profile window.

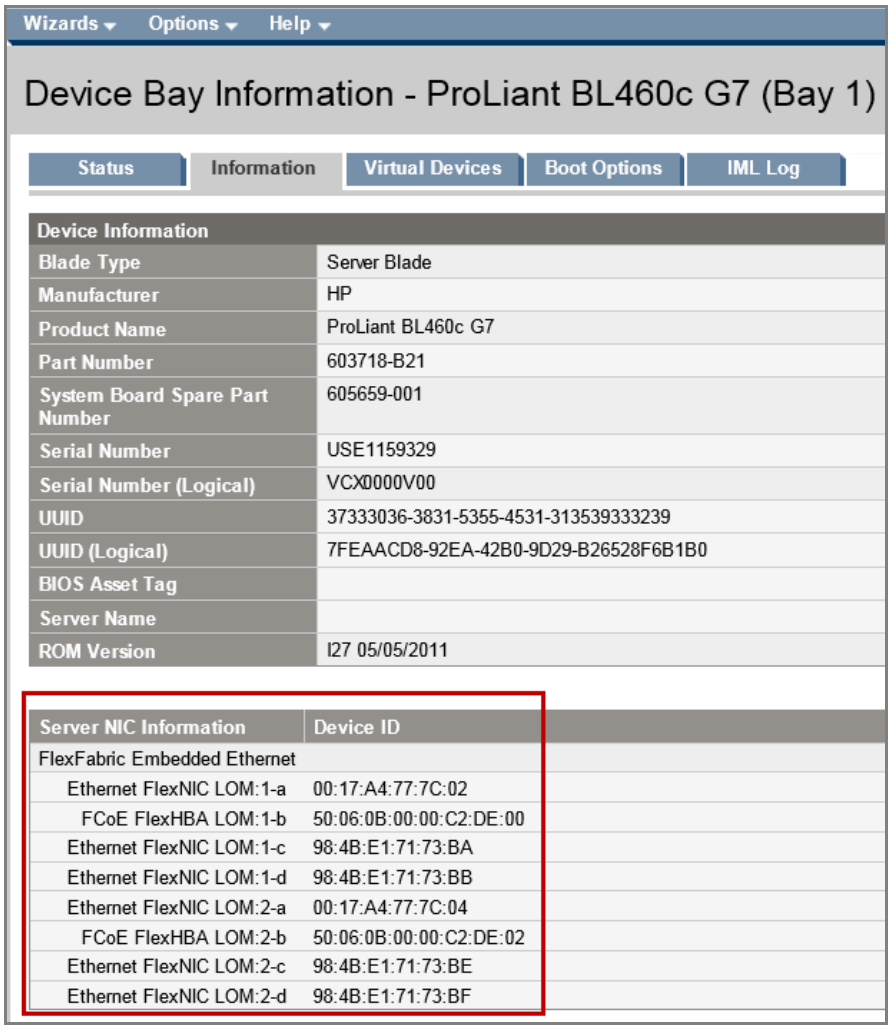
Exercise 2 - Power-on the Server and Verify Boot from SAN Operation

In this task, you use the Onboard Administrator (OA) management interface to examine the status of the server in bay 1. You then power on the server to cause the server profile to be activated. You also examine the IP addresses assigned to the FlexNICs through DHCP.

1. Go to the browser window you have for the OA.

2. In the navigation pane, click Enclosure Information > Device Bays > 1 to view the status of the server blade in Device Bay 1.

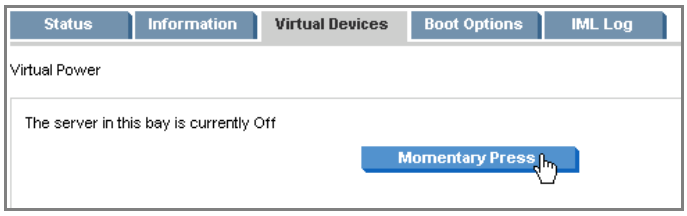
3. Click the Information tab.



4. Examine the server NIC information.

   Notice that all 8 connections are represented here, 6 FlexNICs and 2 FlexHBAs. The other 4 FlexNICs that you did not explicitly configure are presented to the blade server Operating System. These additional 4 LAN Connections that would appear in Windows, or vmnics in VMware ESXI, can be ignored.

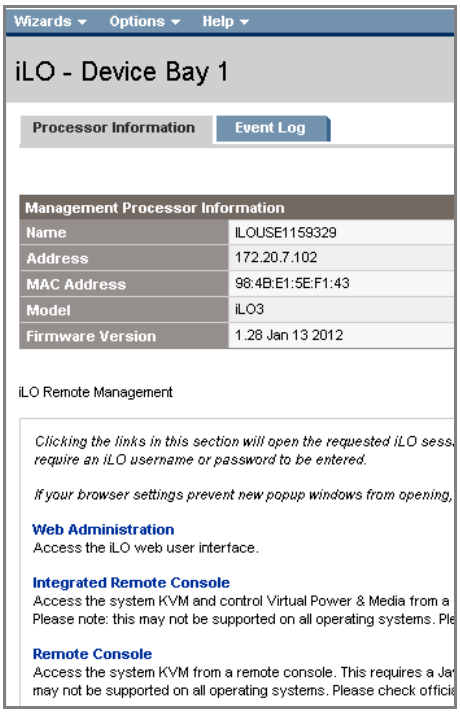
5. Click the Virtual Devices tab. At this point, the server is powered off, which allowed you to assign the server profile previously.



6. Click Momentary Press to power on the server.

   You can also access the Virtual Power feature through the Virtual Connect Manager interface, but going through the OA also gives you easy access to the Remote Console functionality of the HP integrated Lights-Out (iLO).

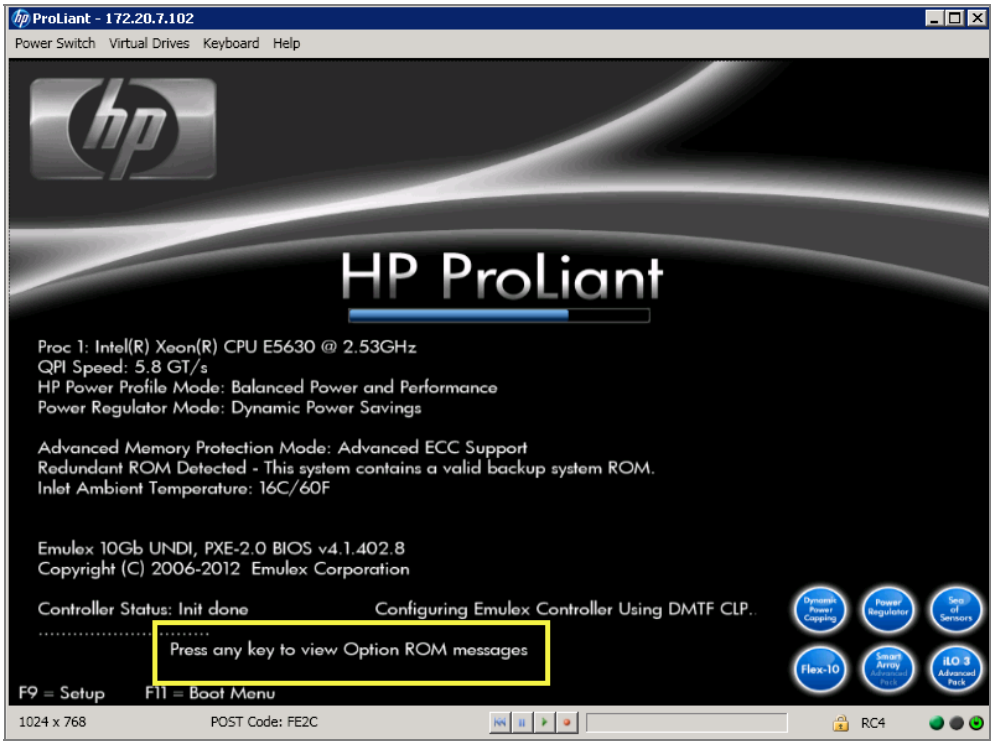
7. To access the Windows Server console, in the navigation pane of the OA, click iLO under the folder entry for Device Bay 1.



8. In the iLO Device Bay window, perform one of the following actions.

   1) If you are using Internet Explorer, click **Integrated Remote Cons**ole.

   2) If you are using Firefox, click **Remote Console**.

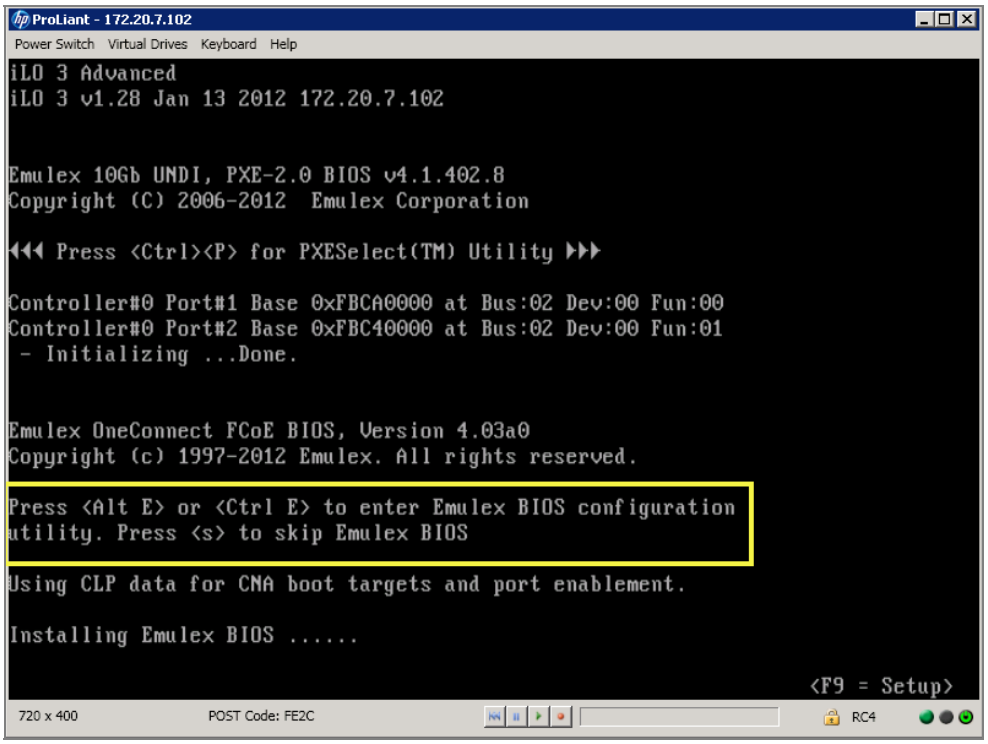


To verify the Emulex BIOS configuration was modified by the Server Profile you examine the settings applied to the adapters by Virtual Connect. During the POST processing stage, you will see a prompt to “Press any key to see POST Messages.”

Note: It is important to watch for the message and respond or you will have to go through the boot process again.

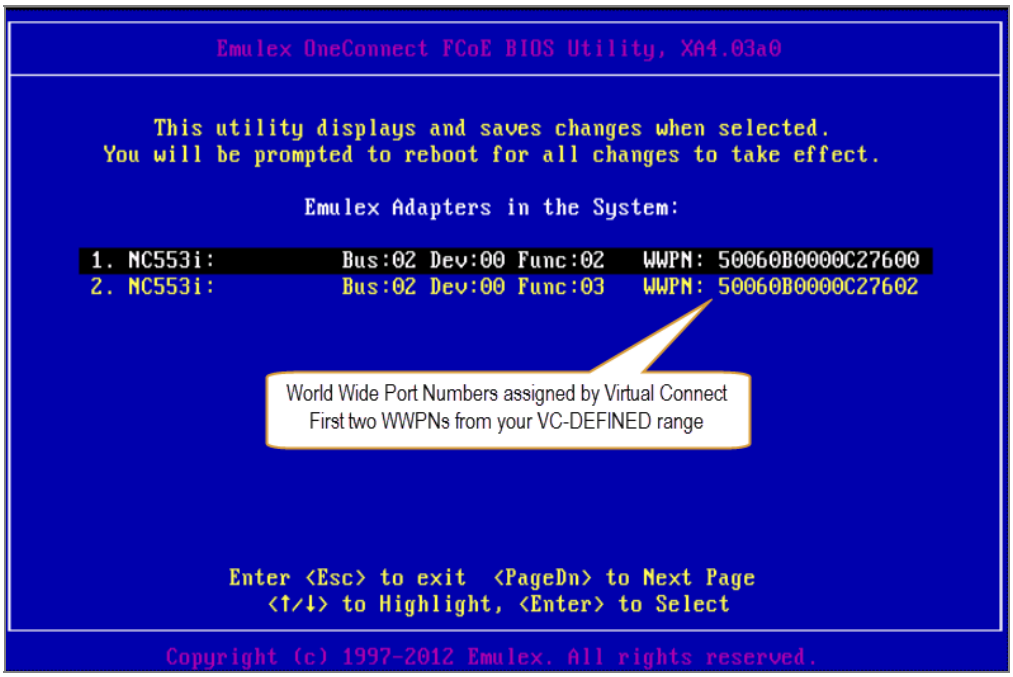
---

9. Press the <Space> bar or any other key to view the Option ROM messages.

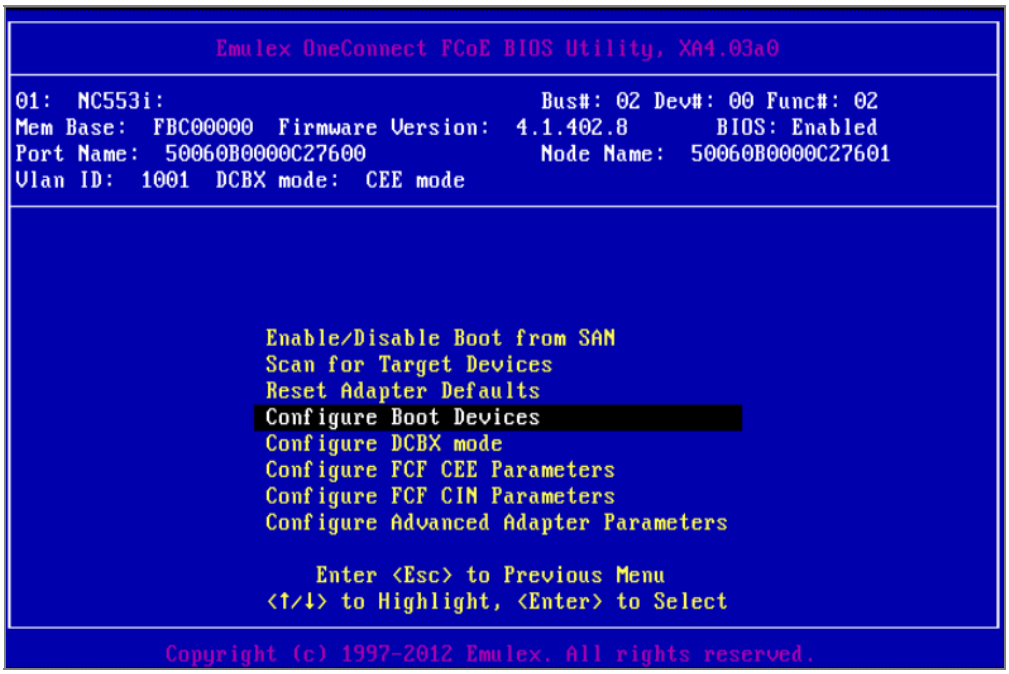


10. Watch for the Emulex OneConnect FCoE BIOS messages.

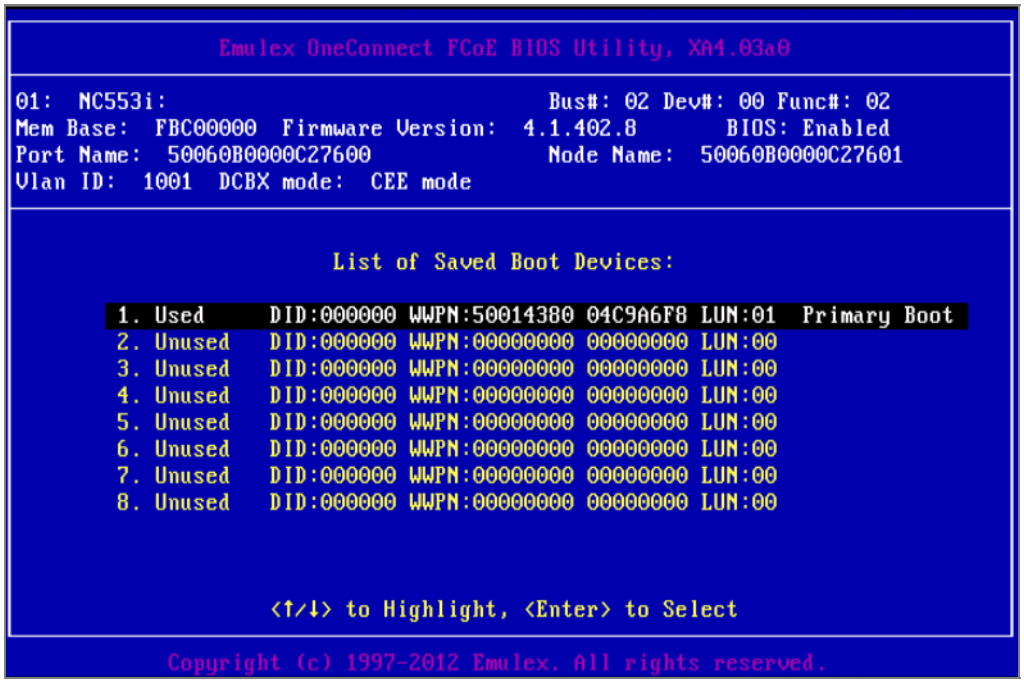
11. Press <Alt>-e or <Ctrl>-e as instructed on the screen to access the Emulex BIOS configuration utility.



12. Highlight the top adapter using the keyboard arrow keys and press <Enter> to view its configuration.

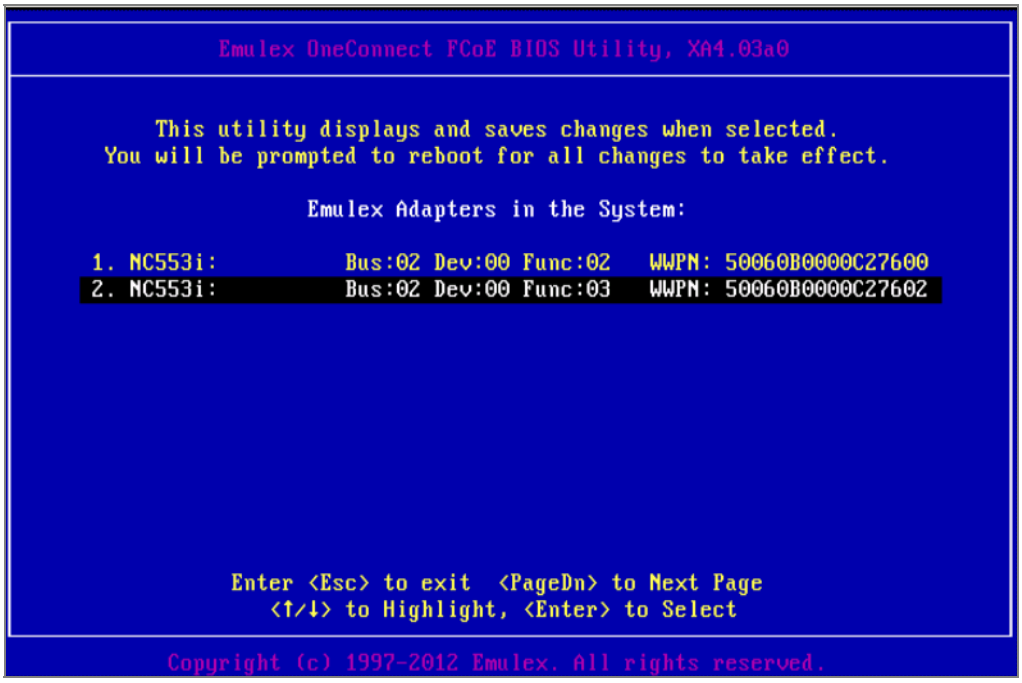


13. Arrow down to Configure Boot Devices and press <Enter> to view its configuration.

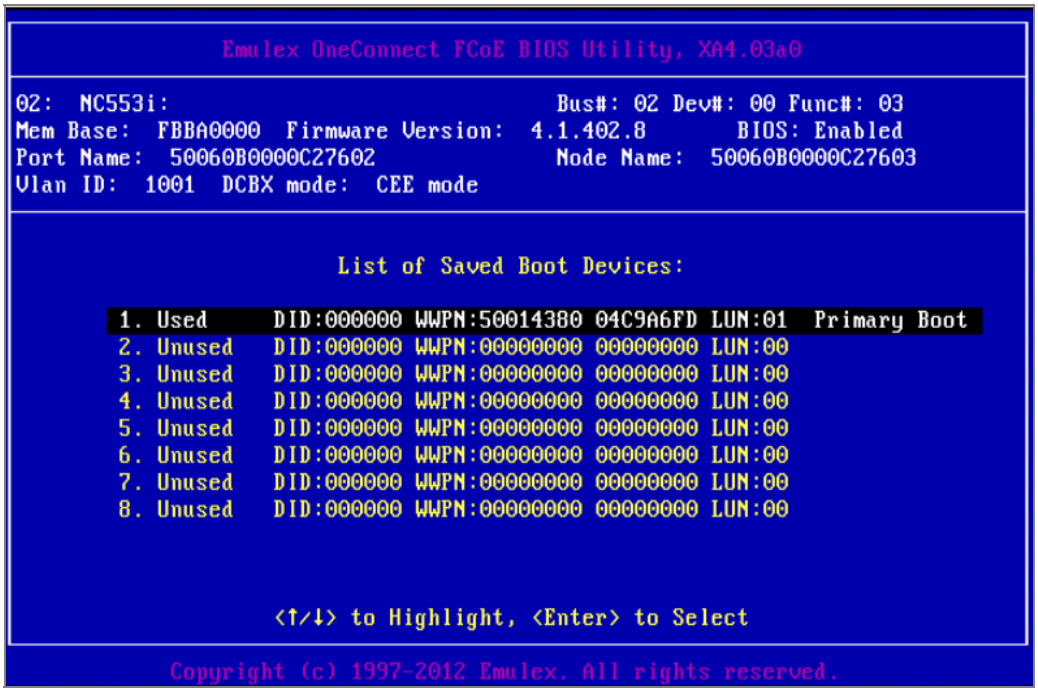


14. Compare the WWPN displayed with the value you entered for Port 1 when you configured the Boot from SAN settings in the server profile.

15. Press <Esc> twice to return to the Emulex Adapters in the System menu.

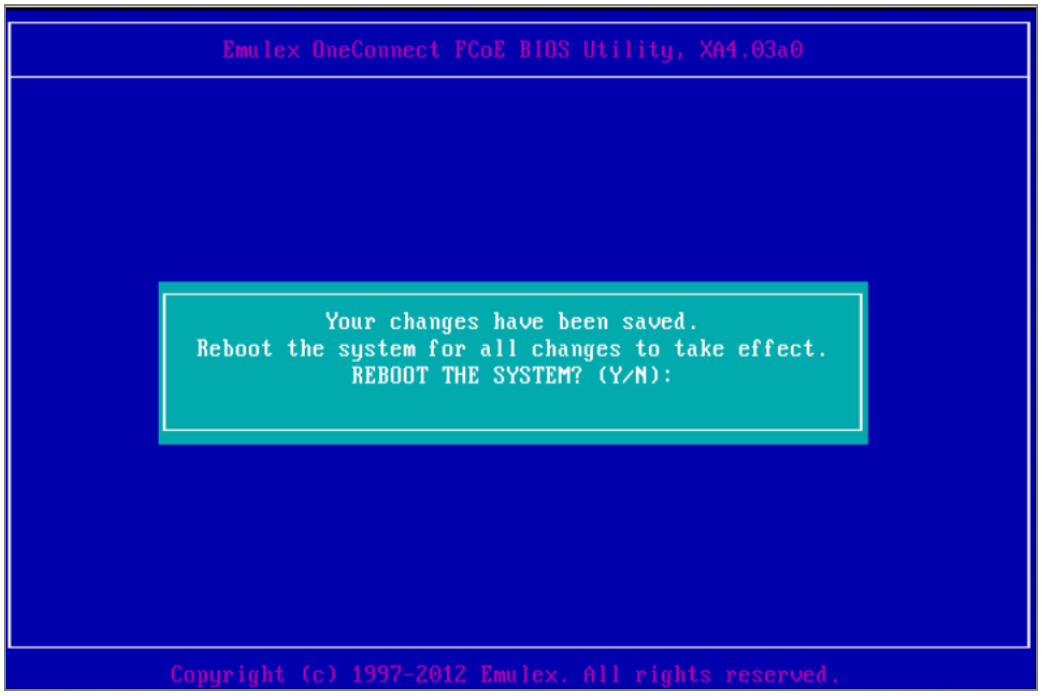


16. Use the arrow keys to choose the second adapter and repeat the previous steps to view the WWPN of its target controller.



17. Compare the WWPN displayed with the value you entered for Port 2 when you configured the Boot from SAN settings in the server profile.

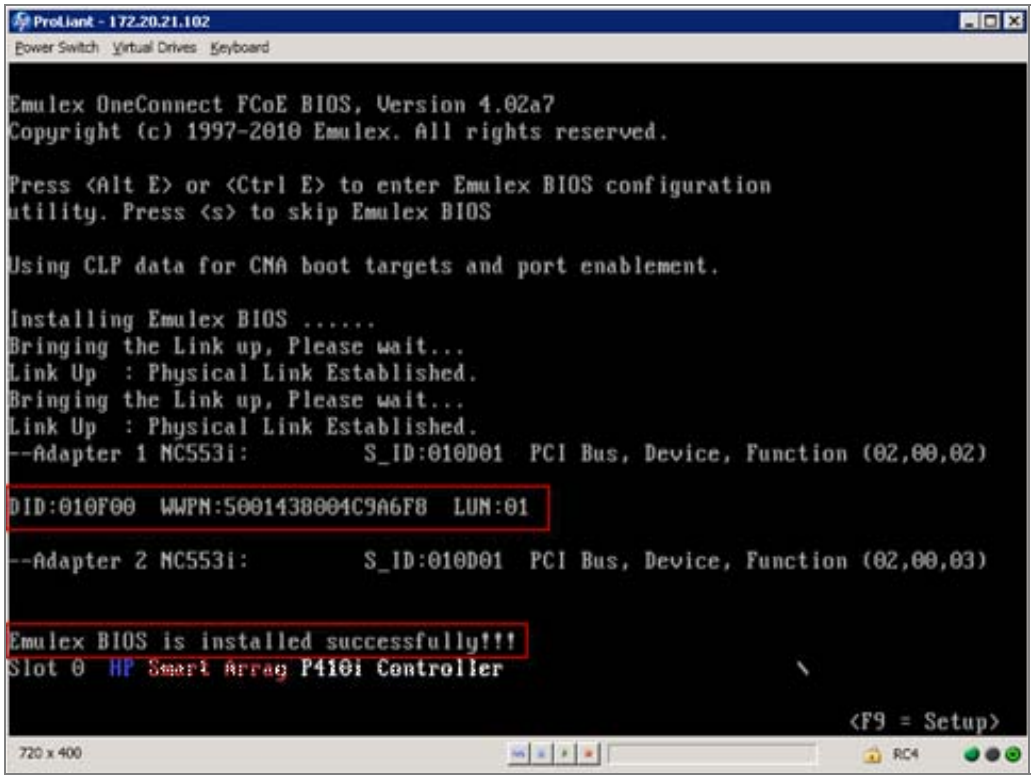
18. Press <Esc> three times to display the reboot prompt.



19. Then type “Y” to reboot the system.

20. To verify that the HBA BIOS loads during the POST processing stage, watch again for the prompt to “Press any key to see POST Messages.”

21. Press the <Space> bar or any other key to view the Option ROM messages.



22. View the messages that display to verify that the Emulex adapter BIOS is installed successfully.

23. Wait for the server to boot from SAN and load the Windows OS.

Exercise 3 - Examine the Server's Network Status

In this task, you verify that IP addresses have been assigned to the two FlexNICs of your blade server through DHCP.

1. When the Windows login screen displays, move the mouse to the top of the iLO window and click Keyboard > CTRL+ALT+DEL.

2. Log in to Windows with the credentials administrator / HP1nvent.

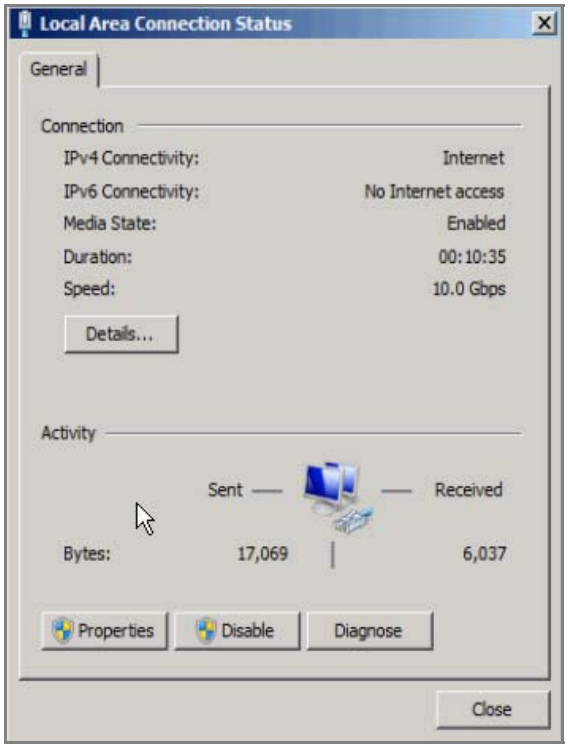
3. Click Start > All Programs > Administrative Tools > Server Manager.

4. In the Server Manager window, in the navigation pane, click Server Manager.

5. In right-side pane, click View Network Connections.

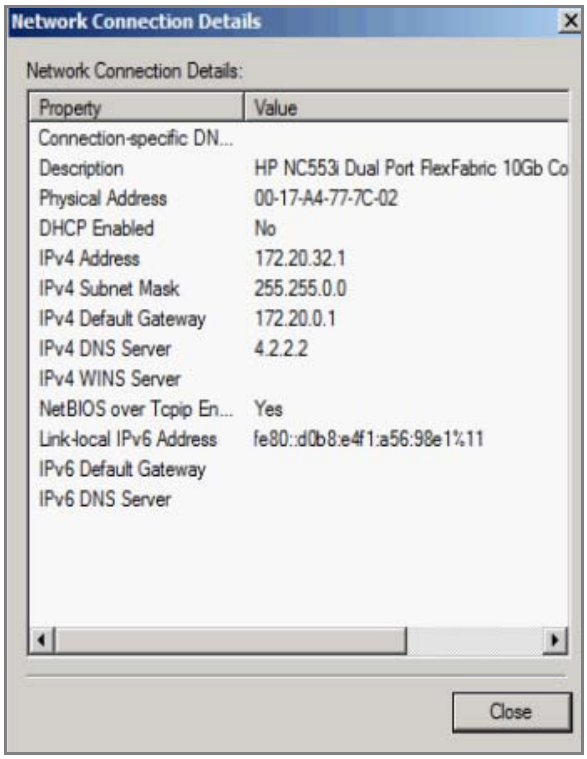
6. In the Network Connections window, right-click an active connection and click Status.

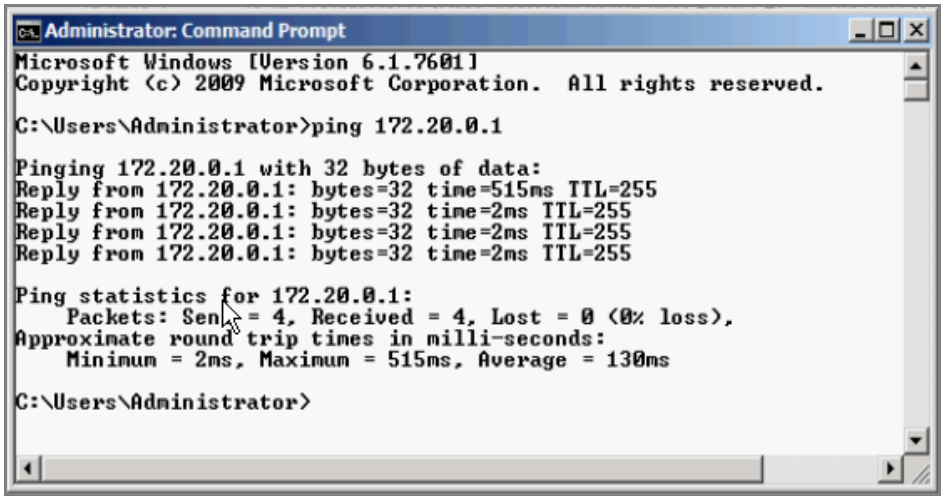
7. Right-click an active connection and in the drop-down menu, click Status.



Notice that the Speed field corresponds to the Virtual Connect maximum speed for the FlexNIC, not the minimum.

8. To verify that an IP address has been assigned to the server's FlexNIC, click Details.





9. Open a Command Prompt window and ping the default gateway using the address found in the details window.

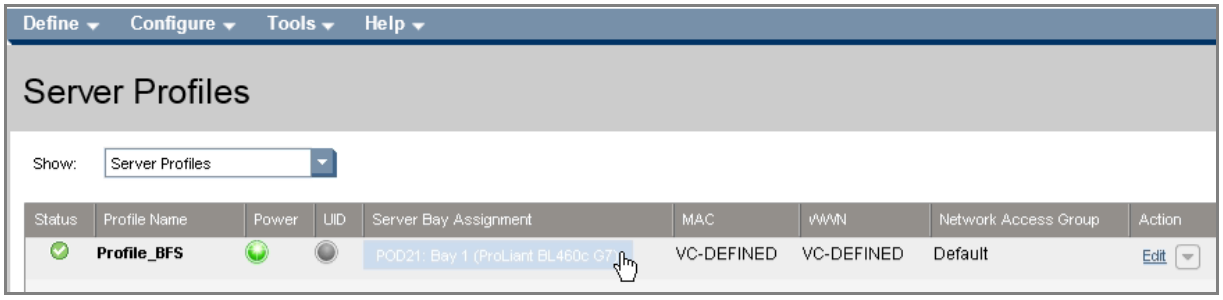
10. Close the application windows and exit the Remote Console.

Exercise 4 - Move the Server Profile to another Blade Server

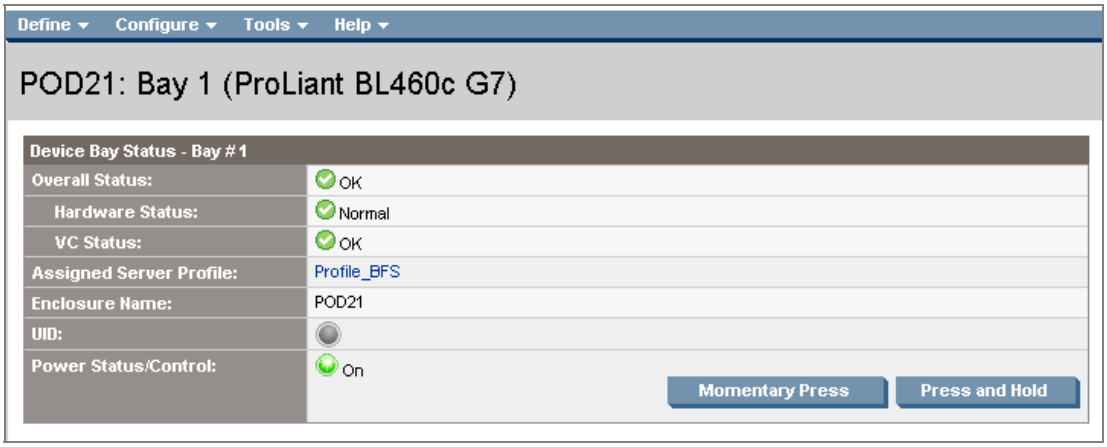
In this task, you move the server profile, which is currently assigned to the first blade server, to the second blade server. Before you can move a server profile, you must first power off the blade server to which the server profile is currently assigned. Then, you reassign the server profile to the second blade server and power on that second server.

In this task, to power off the server blade, you will use the power button feature from within Virtual Connect Manager.

1. From the Virtual Connect Manager, in the navigation pane, click **Server Profiles**.



2. In the Server Bay Assignment column, click the link to the server.



3. To power off your server, click **Momentary Press**.

   The server should now be powered off.

4. To reassign the server profile to a different blade server, in the navigation pane click **Server Profiles**.

5. Under the Action column, click **Edit**.

6. Scroll down to the Assign Profile to Server Bay section, click the down arrow on the server selection box and reassign the profile to the blade server in Device Bay 2.

7. Then click **Apply & Close**.

8. Power on the second blade server that now has the server profile assigned by clicking the link to the server in the Server Profiles window. Click **Momentary Press** to power on the server.

   The server should now be powered on. The system personality should now be migrated to the server in Device Bay 2. You should be able to verify that the Virtual Connect-defined MAC and WWN addresses have in fact migrated to the second server.

9. You can use the procedures described in the previous steps to start an iLO Remote Console session with the blade server in device bay 2 and verify Boot from SAN operation and network connectivity.

Summary

During this lab exercise, you used the Virtual Connect Manager to define a Virtual Connect server profile that used the Boot from SAN (BFS) capability. The Virtual Connect SAN Fabrics you implemented in the previous lab exercise were used for this activity. As part of the environment preparation you deleted existing server profiles and defined a new profile with two FlexNIC connections and two FlexHBA connections.

You verified the Windows host booted from SAN successfully and that you could ping the default gateway for one of the VLANs you also assigned to the server profile. Then, you moved the server profile to another server bay of the Virtual Connect domain and verified proper operation for that server.

Implementing Shared Uplink Sets (Optional)

Lab 4A

Objectives

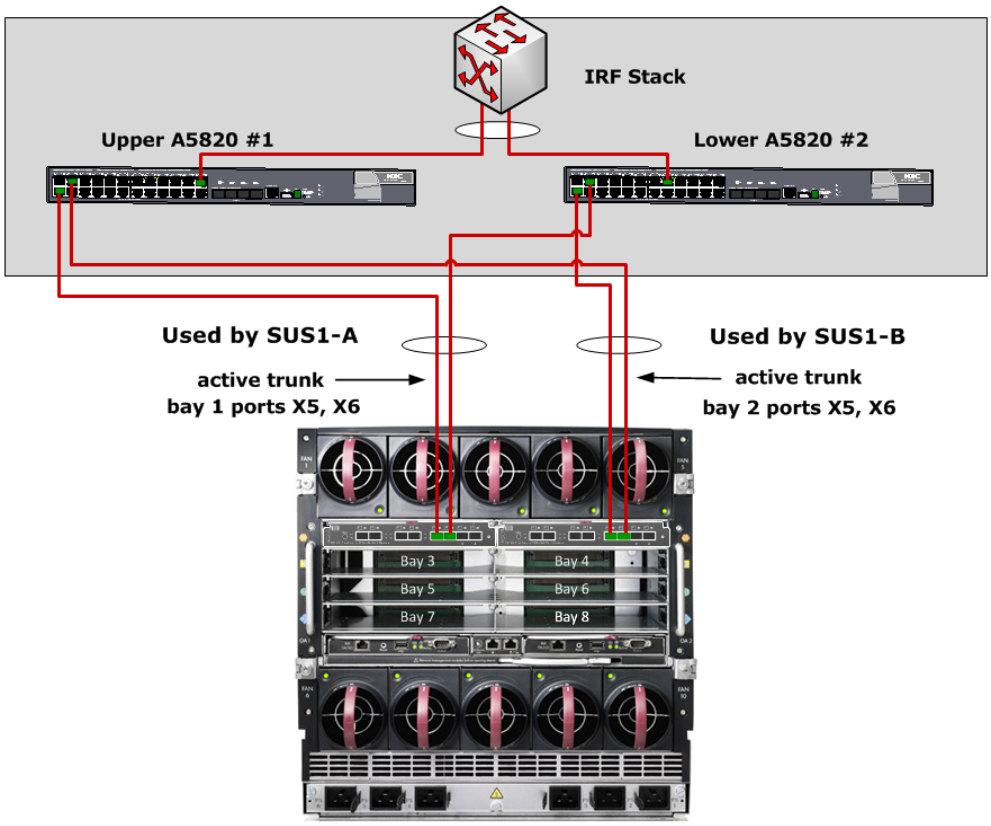
After completing this activity, you should be able to:

- Define two redundant shared uplink sets (SUSs)
- Delete two Virtual Connect (VC) networks
- Examine the status of the uplink ports

Introduction

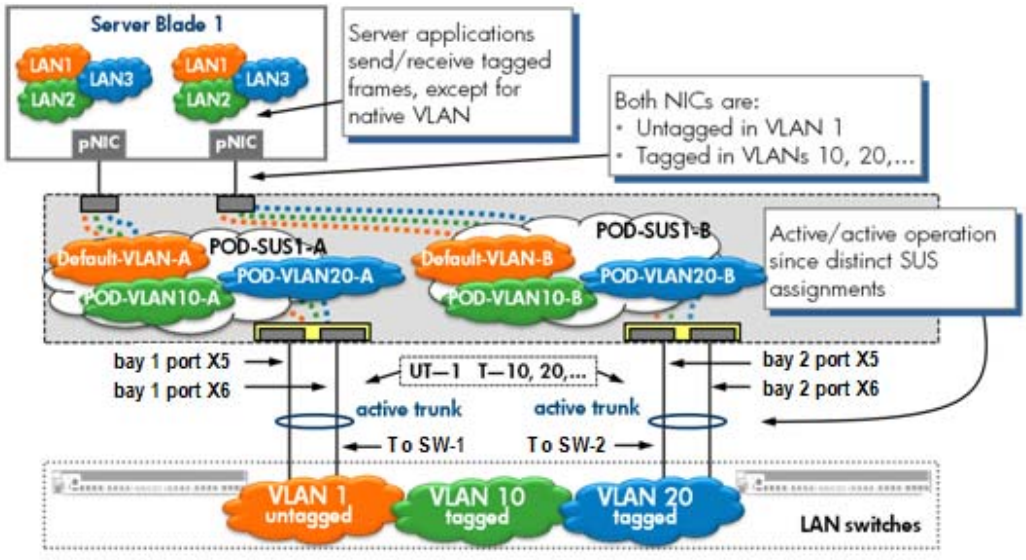
In this lab, you will configure Virtual Connect to support two Shared Uplink Sets (SUS) that will provide redundant access to the data center network. Each SUS will have a pair of uplink ports (port trunk) assigned to it, uplinks initiated from each module will be connected using Link Aggregation (LACP). In addition, each SUS will support one untagged VLAN and several tagged VLANs.

Network diagrams



Physical view of the LAN connections

In this lab, both port trunks are active because they are assigned to separate SUSs. In additional, it should be noted that each SUS' uplinks are split across both network switches, this is accomplished as the switches are in a cluster, using HP's IRF technology. Additional uplinks could be added to improve uplink bandwidth and network availability.



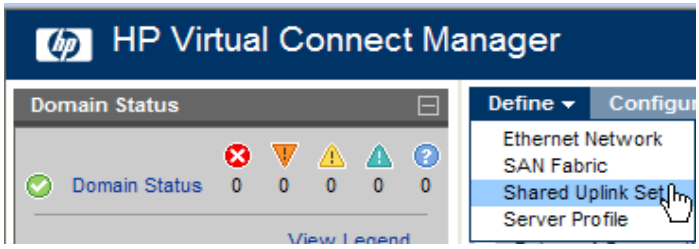
Logical view of the VC network configuration

SUS1-A uses the port trunk comprising the uplink ports from the VC FlexFabric module in Bay 1; SUS1-B uses the port trunk comprising uplink ports from the VC FlexFabric module in Bay 2. Because two separate collections of VC networks are involved as a result of the SUSs, Virtual Connect allows each port trunk to operate in an active state.

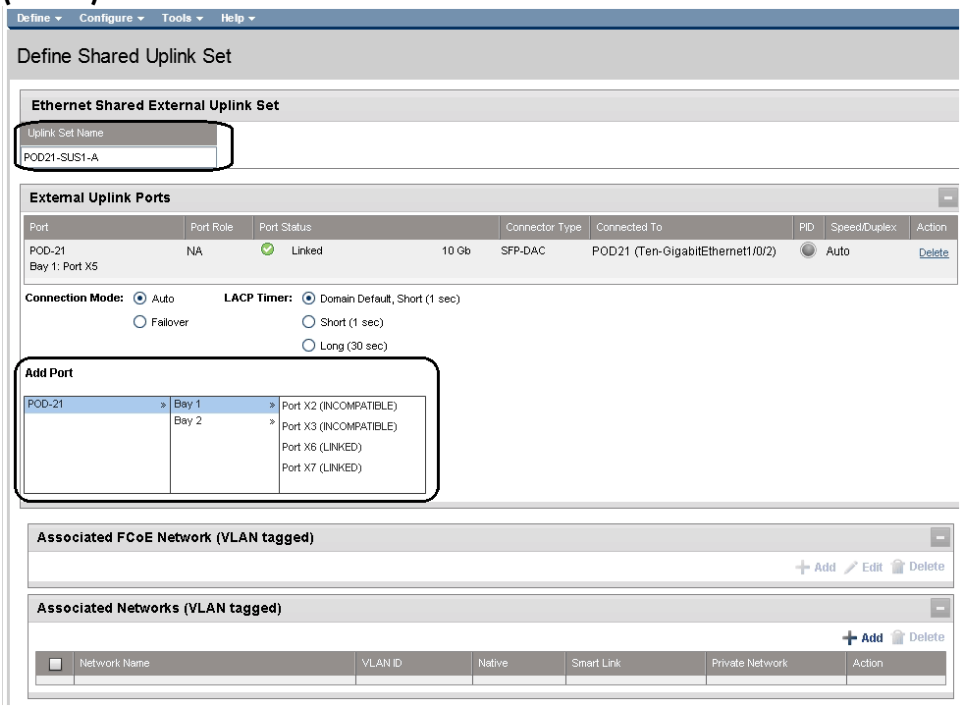
Exercise 1 — Defining two redundant Shared Uplink Sets

In this exercise, you will define two SUSs that will function as redundant networks. This is accomplished by assigning the SUSs to the same uplink ports. As part of the procedures for defining an SUS, you will assign uplink ports and will also define the VLANs the SUS will support. You will be able to define VLAN identifiers for various VC networks that will comprise each SUS.

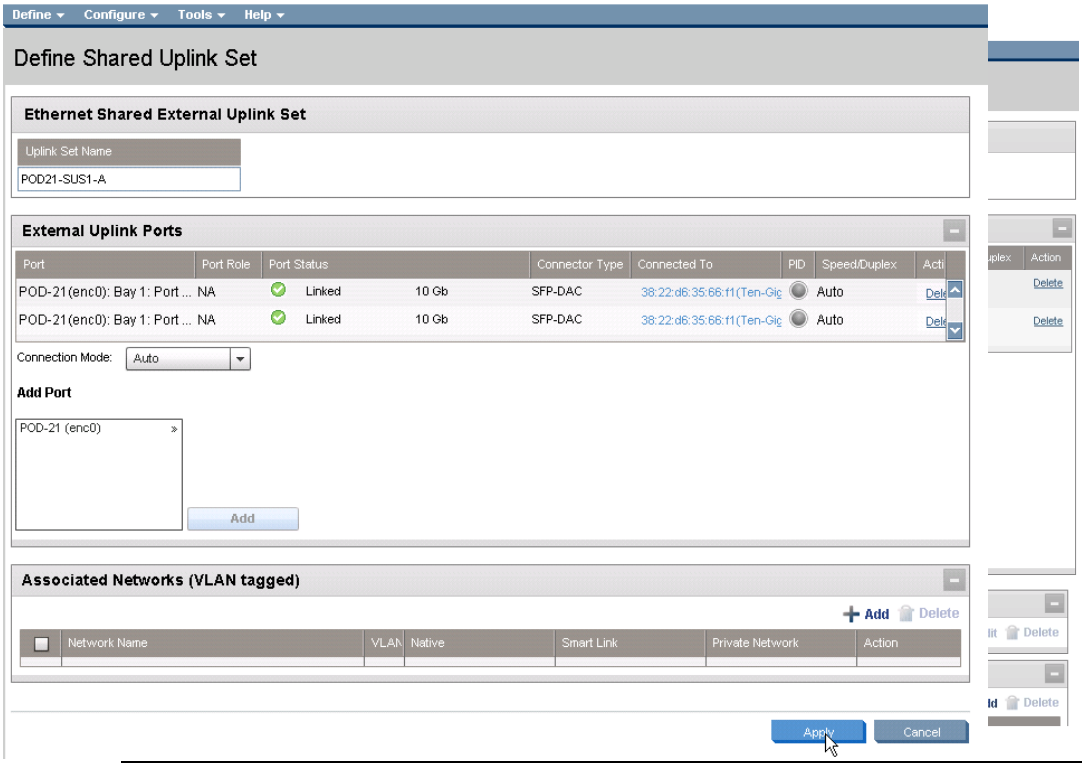
1. In the toolbar, click **Define**. Then in the drop-down menu, click **Shared Uplink Set**.



2. From the Define New Shared Uplink Set screen, follow these steps:
   a. For the Uplink Set Name, enter `PODnn-SUS1-A` where `nn` is your POD ID.
   b. Add the first external uplink port by clicking the Add Port section **<enclosure-name> Bay 1 → Port X5 (Linked)**



c. Add the second external uplink port by clicking the Add Port section **<enclosure-name> Bay 1 → Port X6**



Note
Both ports are from the VC FlexFabric module in Interconnect **Bay 1**.

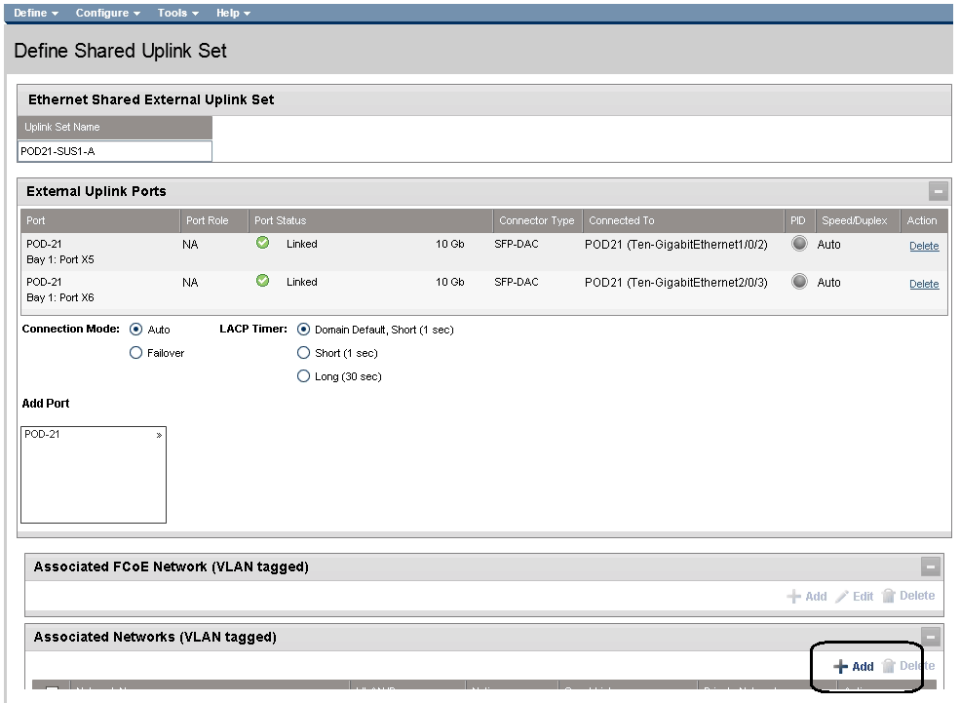
3. These are the VLANs that will be configured within this SUS.

Network Name	VLAN ID	Native	Smart Link
Default-VLAN-A	1	checked	Checked
PODnn-VLAN10-A	10		Checked
PODnn-VLAN20-A	20		Checked
PODnn-VLAN30-A	30		Checked
PODnn-VLAN40-A	40		Checked
PODnn-VLAN50-A	50		Checked

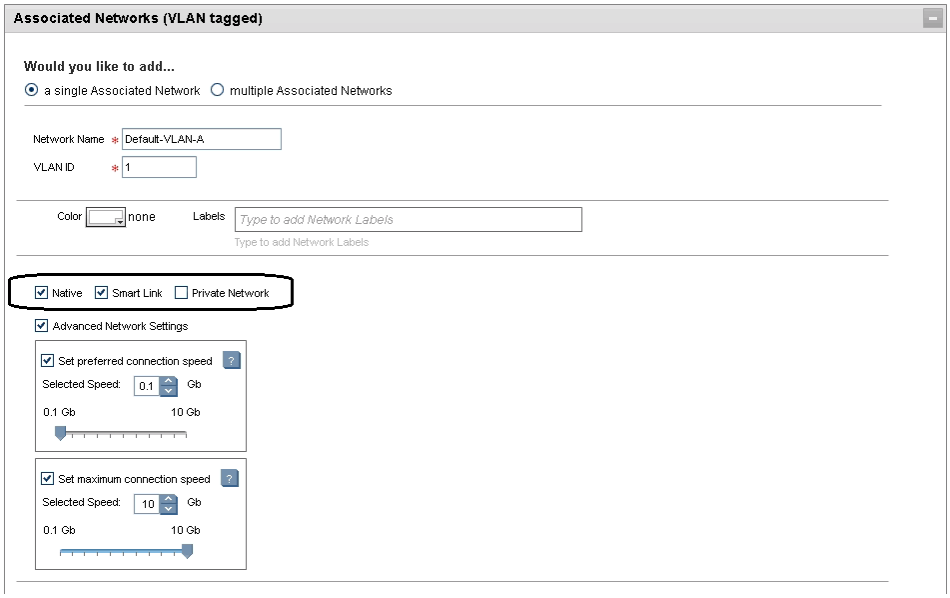
These networks are essentially just VC networks that will be listed under the Ethernet Networks folder of the navigation pane. In contrast to the VC networks you defined in previous lab exercises, these VC networks will be "assigned" to an SUS. That is, these networks are not simple vNets.

- **About the Native Parameter** — Only one network can have the Native option checked (that is, enabled in an SUS. This option indicates that the VLAN carries untagged frames only. In general, a given physical or logical link (port trunk) can transport at most one untagged VLAN. Hence, the SUS assigned one or more uplinks must operate according to that fundamental network rule.
- **About the Smart Link Parameter** — In this configuration, the Smart Link parameter is enabled on each of the VC networks that you define for this SUS. Smart Link will monitor the state of the uplinks and will turn off downlink ports to servers within Virtual Connect if all available uplinks assigned to a VC network are down.

4. To add the Default network, click **Add Network** and then specify the information from the table.



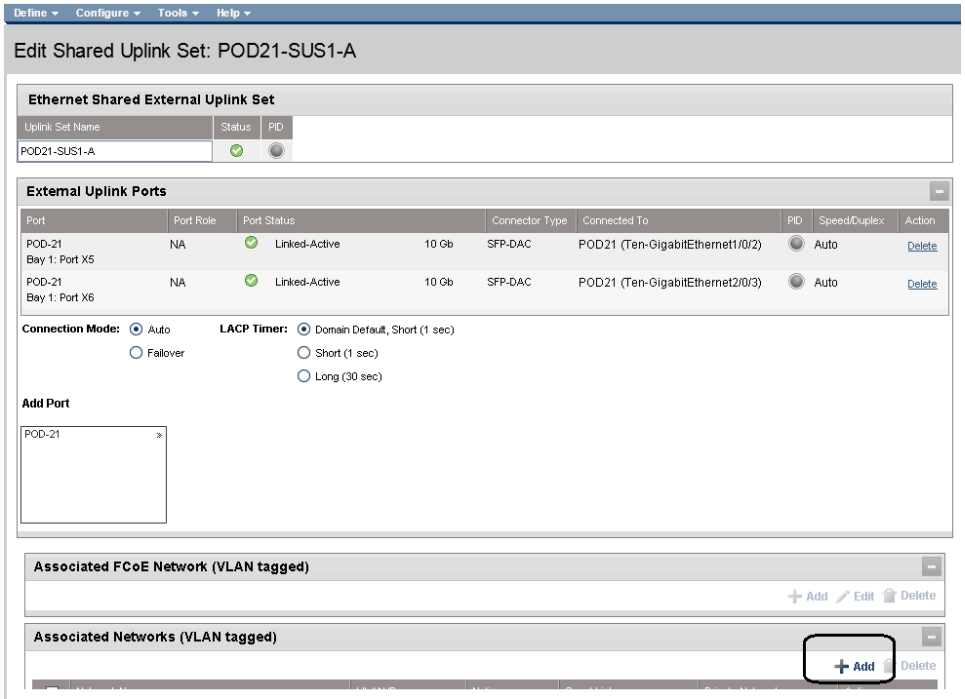
5. Enter the name for the "Default" network, and then specify the information from the table. Optionally, select Advanced and set the Preferred and Maximum Speeds.



6. Scroll to the bottom of the page and **Click Apply.**

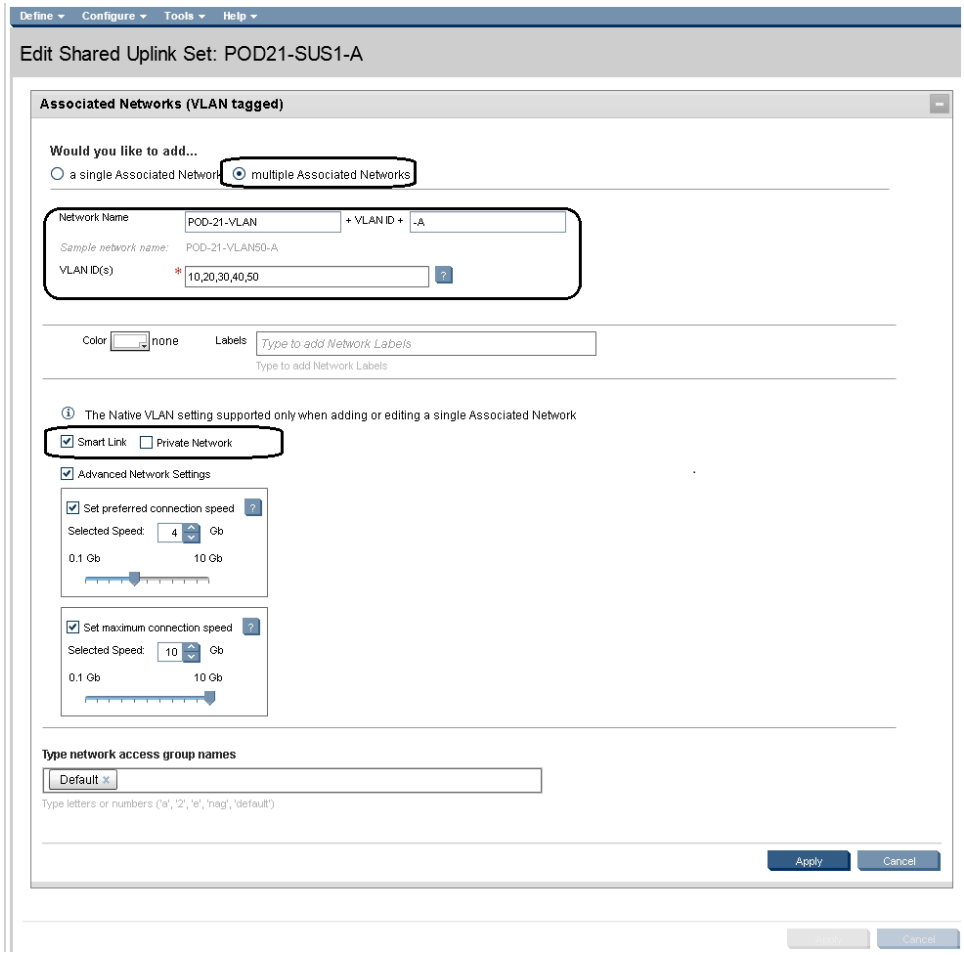
7. In the shared Uplink Sets Screen, select to Edit the SUS you just created as additional Networks will be added to this SUS.

8. Under the Associated Networks (VLAN tagged) box **Click ADD**

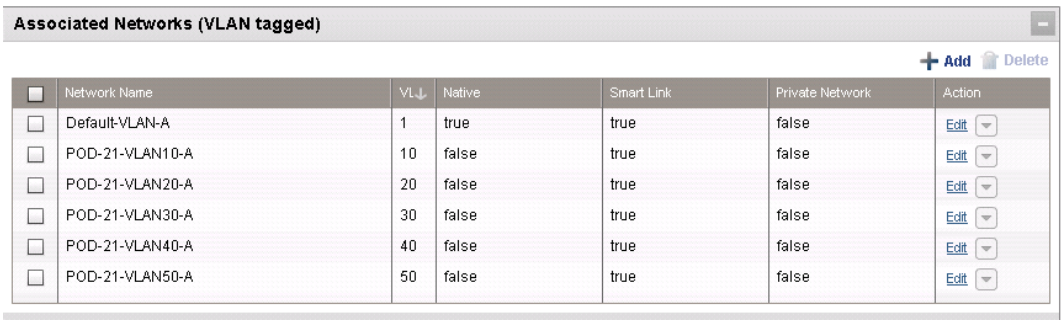


9. Under the Associated Networks (VLAN tagged) box **Click ADD,** when the windows opens, select the "multiple Associated Networks" radio button. The ability to create multiple networks in a single action was added to Virtual Connect in firmware release 3.70. The Advanced Networks Settings feature was added in release 4.01.

10. Scroll down and **click Apply.**



11. After you complete the data entry, the Associated Networks section of the window should display as follows.

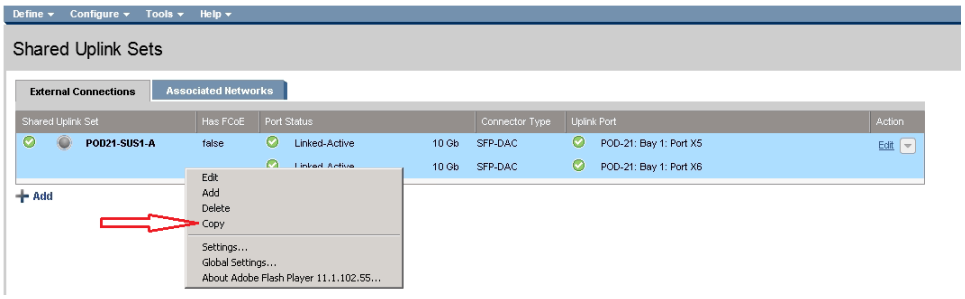


Network Name	VL	Native	Smart Link	Private Network	Action
Default-VLAN-A	1	true	true	false	Edit
POD-21-VLAN10-A	10	false	true	false	Edit
POD-21-VLAN20-A	20	false	true	false	Edit
POD-21-VLAN30-A	30	false	true	false	Edit
POD-21-VLAN40-A	40	false	true	false	Edit
POD-21-VLAN50-A	50	false	true	false	Edit

12. Verify that **Smart Link** is enabled for each network, but **Native** is only enabled for the first network (Default-VLAN-A). **The Click Apply.**

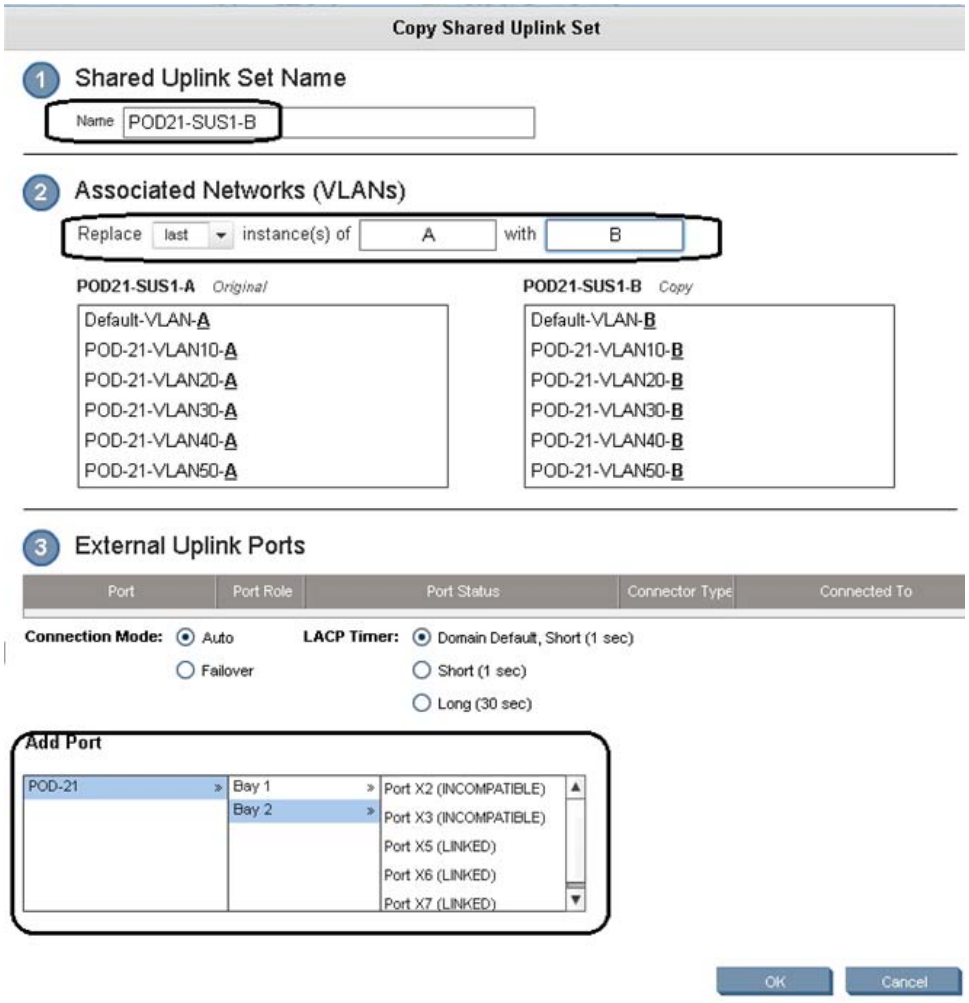
13. To define the second Shared Uplink Set, we will **COPY** the SUS you just created. In the Logical Configuration section of the navigation pane, click the **Shared Uplink Sets** entry to go to the Shared Uplink Sets page.

14. In the Shared Uplink Sets window, Left click on SUS you just created and **Click COPY.**



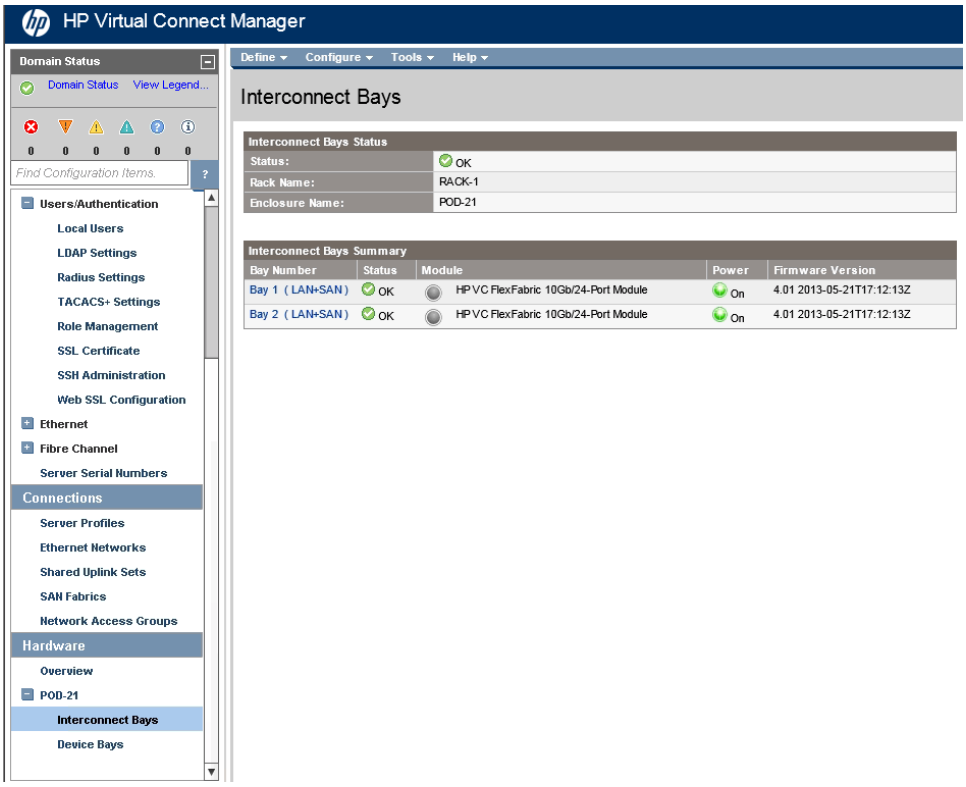
15. In the Shared Uplink Sets window, Left click on SUS you just created and **Click COPY.**

16. In the "Copy Shared Uplink Set" dialog box, Chance the SUS Name to end in "B", select Replace "last" instance of "A" with "B". **Scroll down** and under ADD ports, Select ports X5 and X6 from Bay 2, **Click OK**

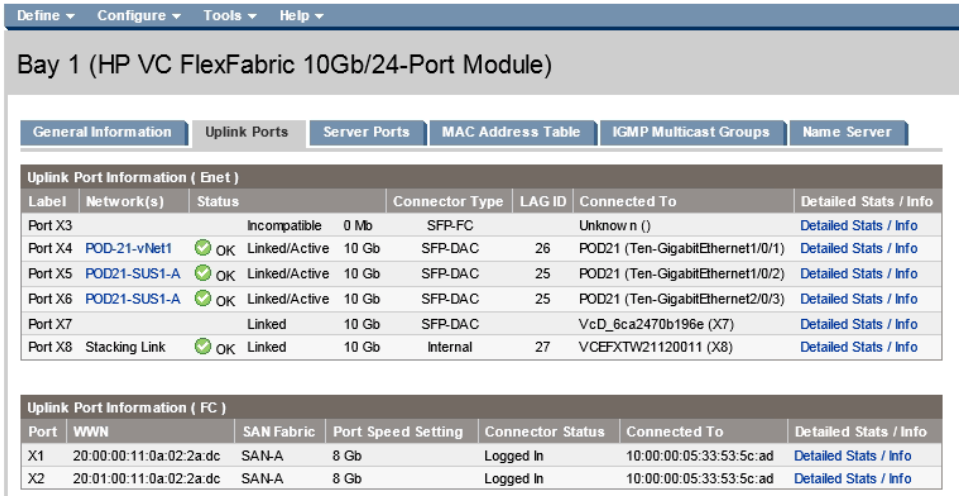


Exercise 2 — Examining the status of the uplink ports

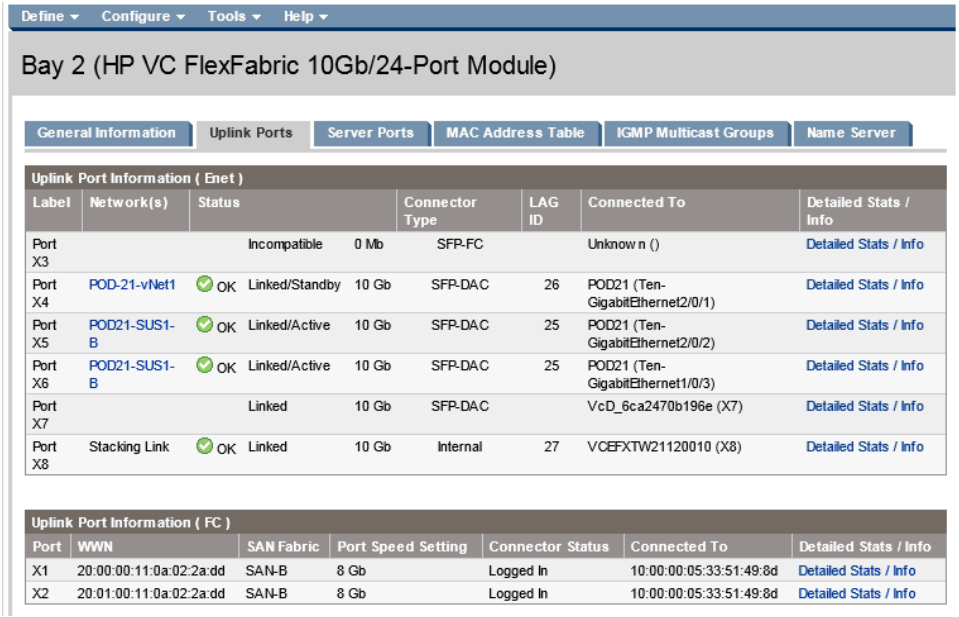
1. In the navigation pane Hardware Configuration section, click **<enclosure-name> > Interconnect Bays**. Then in the main window, click the **Bay 1 (LAN+SAN)** link, which contains a VC FlexFabric module.



2. Notice on the Uplinks Tab that Bay 1: Port X5 and Bay 1: Port X6, which are assigned to Shared Uplink Set PODnn-SUS1-A, have the same LAG ID. This shows that Virtual Connect has formed a Link Aggregation Control Protocol (LACP) link aggregation group (LAG) with these two uplink ports. Also notice that the uplink ports are both in the Active state, which you would expect because they are in the same port trunk. If the LAG IDs are not the same or one of the links is in standby, contact your instructor for assistance.



3. Repeat Step 1, choosing instead **Bay 2**, which contains the second VC Flex-Fabric module.



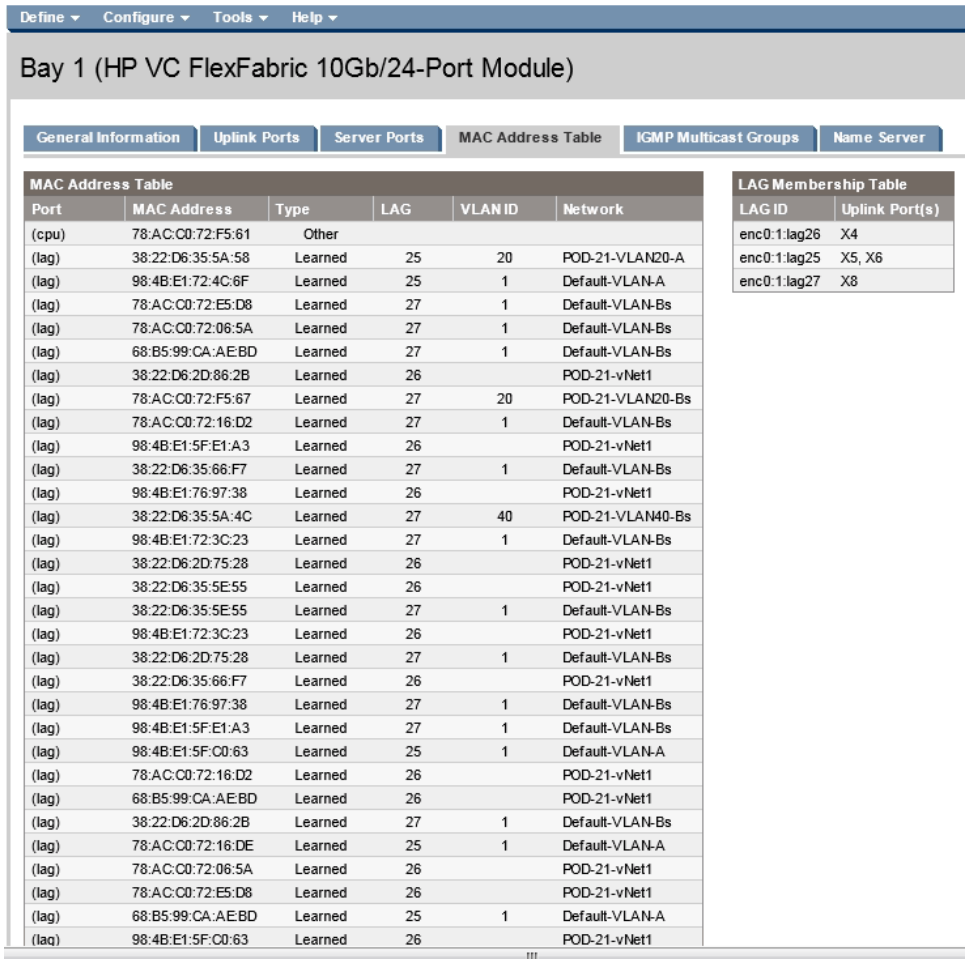
Similar to the first Shared Uplink Set, notice that Bay 2: Port X5 and Bay 2: Port X6, which are assigned to Shared Uplink Set PODnn-SUS1-B, have the same LAG ID. This shows that Virtual Connect has also formed an LACP LAG with these two uplink ports. If the LAG IDs are not the same or one of the links is in standby, contact your instructor for assistance. Also, even though both Bay 1 and Bay 2 module SUS have the SAME LAG ID, all ports have and ID of 25,

these are TWO separate link aggregation groups, one on module Bay 1 and another on the module in Bay 2.

Like the other Shared Uplink Set, the uplink ports are both in the Active state, just like those assigned to PODnn-SUS1-A. This is because this port trunk used by PODnn-SUS1-B is distinct from the port trunk used by PODnn-SUS1-A.

4. While in the Bay 2 module page, take a look at some of the other tabs on this page, such as Server Ports,

5. And MAC address Table etc.



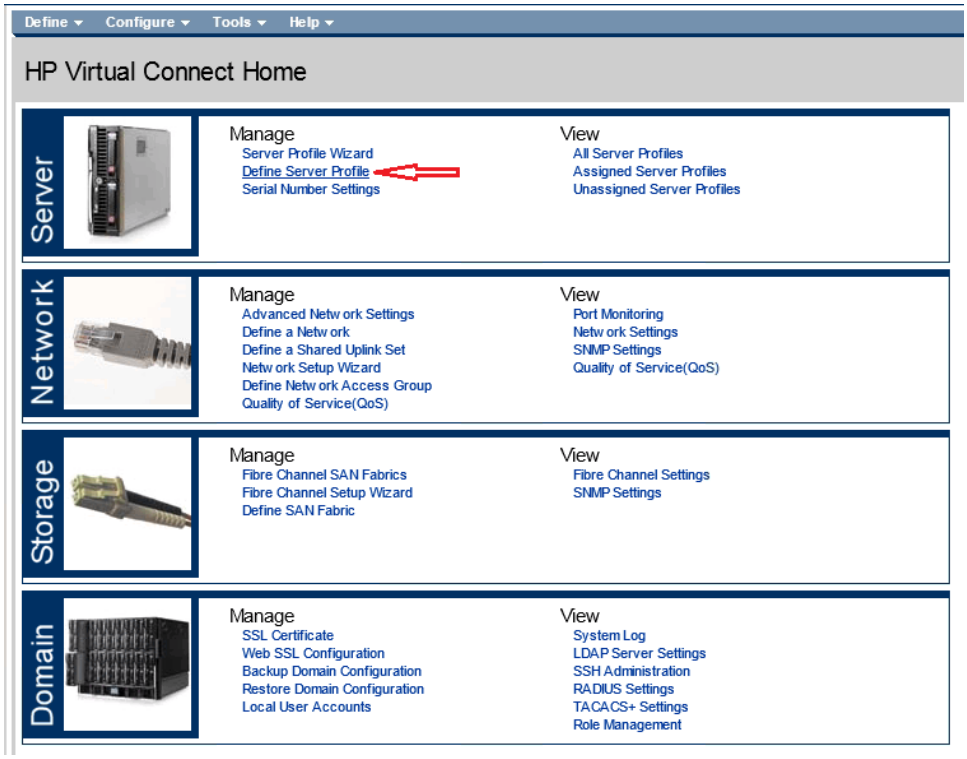
Exercise 3 — Creating a server profile

In this exercise, you will create a new server profile to be configured with multiple networks and SAN connections. This server profile will be used to connect an ESX host to the network. For this exercise, you will use the server in Bay 9 of you c7000 enclosure.

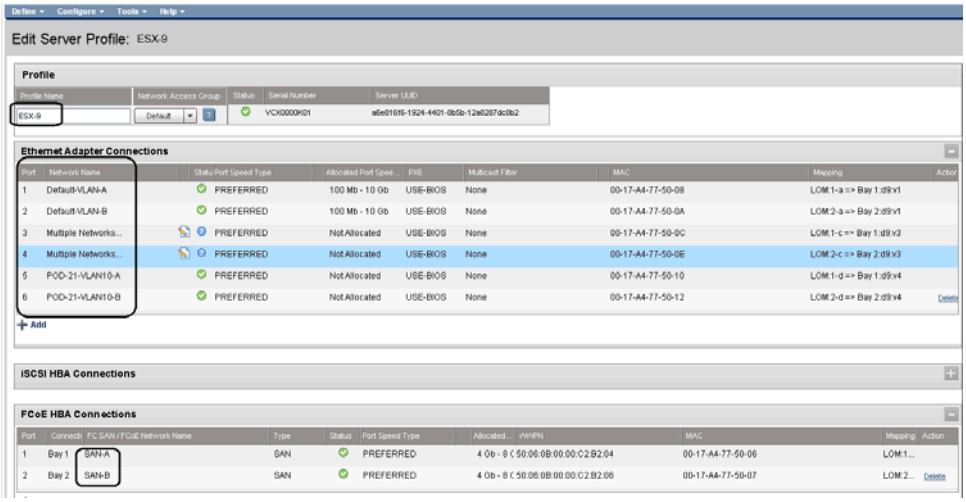
1. Open a web browser and access the Virtual Connect Manager home page.

> **!** **Important**
> In the previous LAB if you created a server profile and assigned networks to it, that profile should still be applied to the server in Bay 2 and booting to SAN. Do NOT delete that profile

2. In the Virtual Connect Manage Home page, **click Define Server Profiles**.

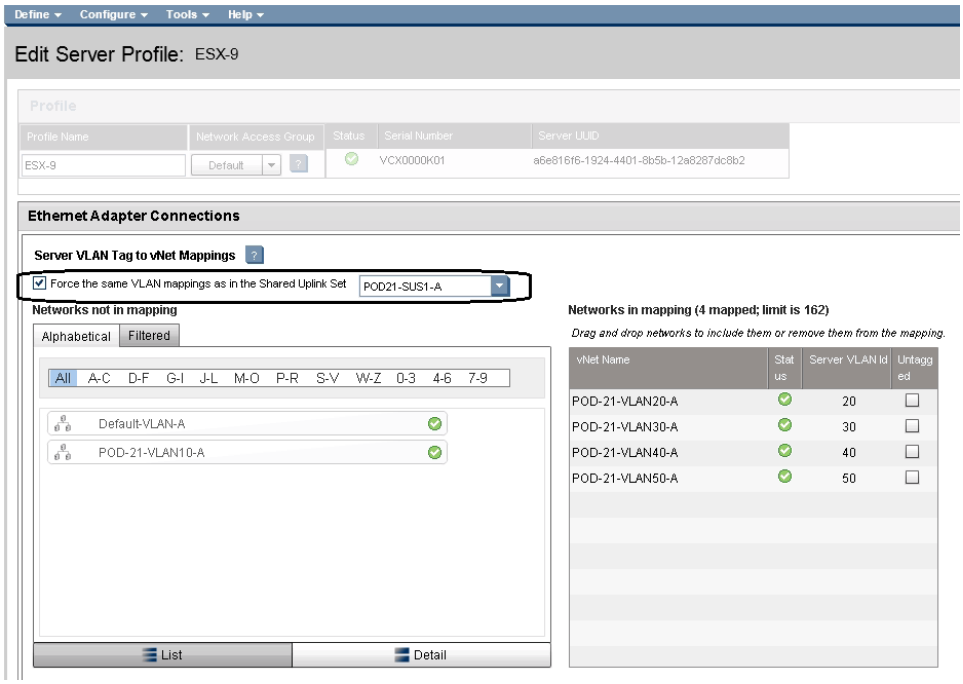


3. Create new server profile as shown in the graphic below. In the Ethernet Adapter Connections box, **click ADD** to add four additional NICs, for a total of 6 NICs. Connect the Ports (NICs) as follows;

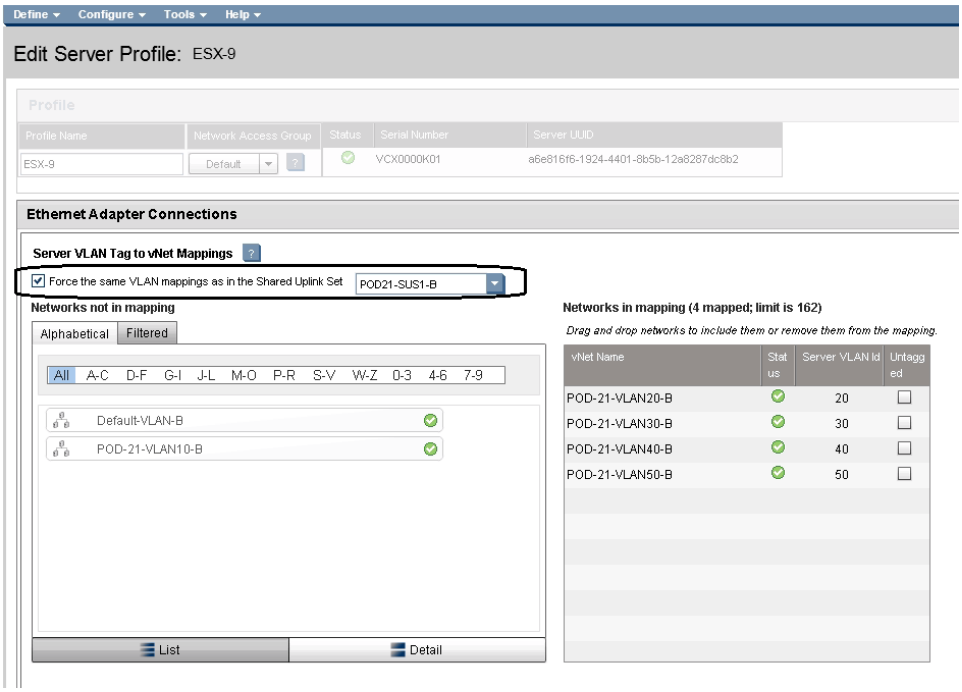


4. Connect the SAN ports to SAN-A and SAN-B.

5. NIC Ports 3 and 4 are connected to Multiple VLANs, as shown in the following two graphics. When multiple networks are connected to a server NIC port using the Multiple Networks connections, the VLAN tags are forwarded to the server NIC. One VLAN could be defined as untagged. NIC port 3 is connected to networks associated with POD-xx-SUS1-A which uses uplinks from Bay 1.



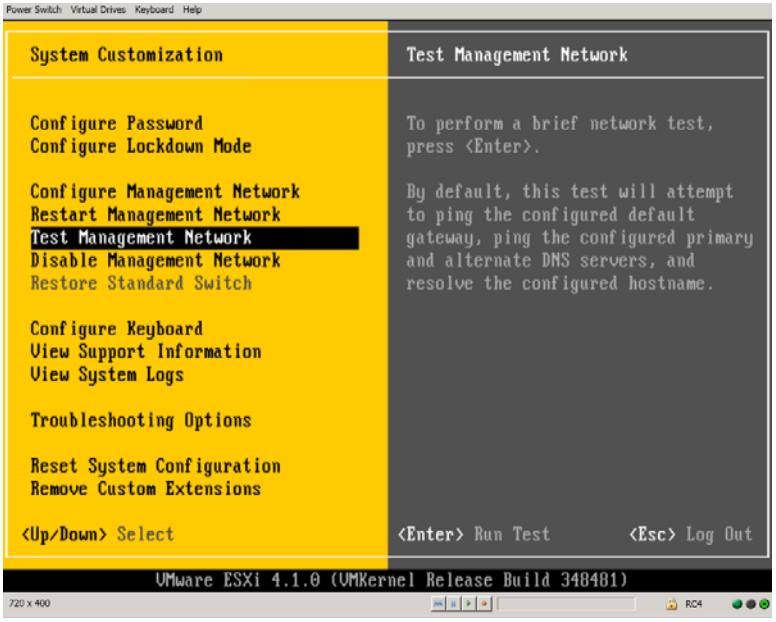
6. NIC port 4 is connected to networks associated with PODxx-SUS1-B which uses uplinks from Bay 2.



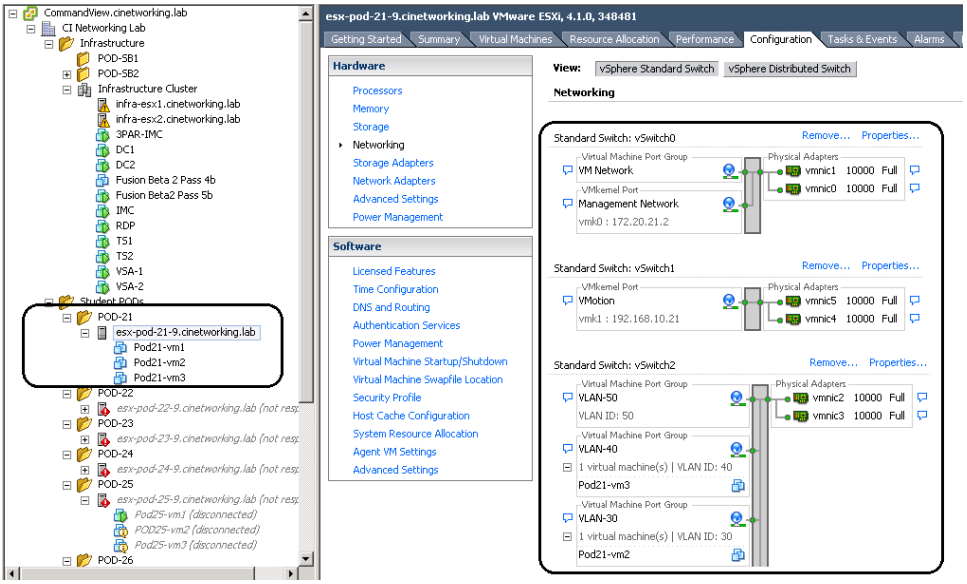
7. Apply the network configuration, assign the profile to the server in Bay 9.

8. Power on the server in Bay 9 and open an iLO connection to it. Once the server boots to ESXi, Press F2 on the ESX server screen and log in to ESXi as "root" with the password "hpinvent".

9. Select TEST Management Network and verify a successful PING to the address 172.20.0.1.



10. From Windows, log in to vCenter using the "Windows session credentials" and find your POD, under Student PODs. Verify that vCenter can see your ESXi host. Select the host and Click on the Configuration tab, then select Networking and verify that ALL SIX NICs are connected as shown below.



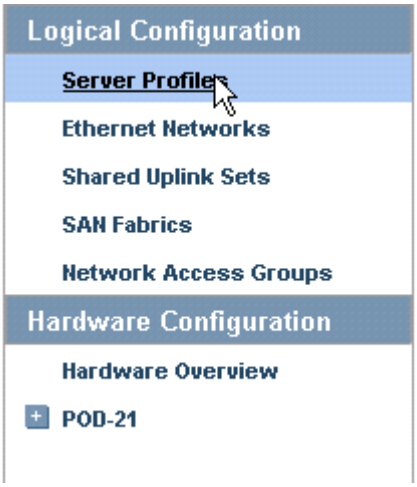
11. Time permitting, you can optionally start one of the VMs on this server, then move the VM between VLANs and verify that Virtual Connect is trunking the configured VLANs to this vSwitch.

12. Once complete, shut down the ESX host gracefully and close the iLO session.

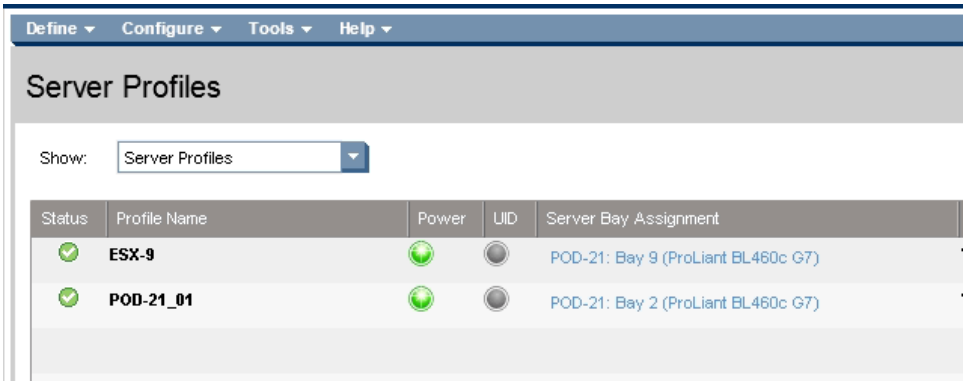
Exercise 4 — Deleting the server Profile and VC networks

In this exercise, you will ALL previously created Profiles and Networks that were created in earlier labs as they will not be required in the next lab.

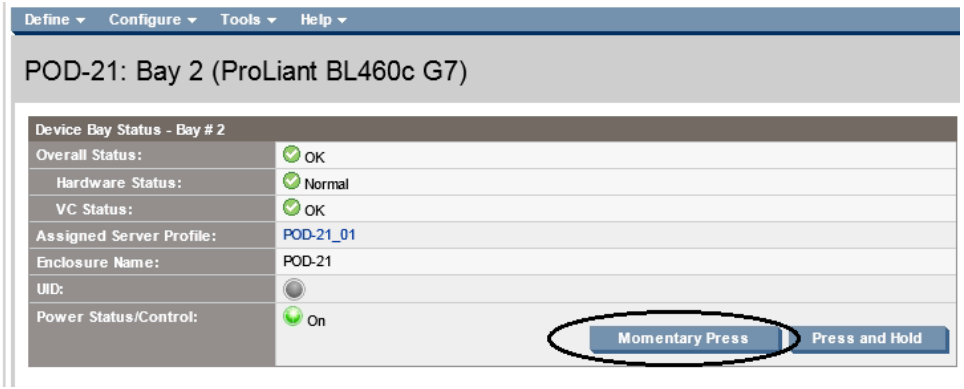
1. Open a web browser and access the Virtual Connect Manager home page.
2. In the navigation pane Logical Configuration section, click **Server Profiles**.



3. In the Server Bay Assignment column, click the link to the server in Bay 1.



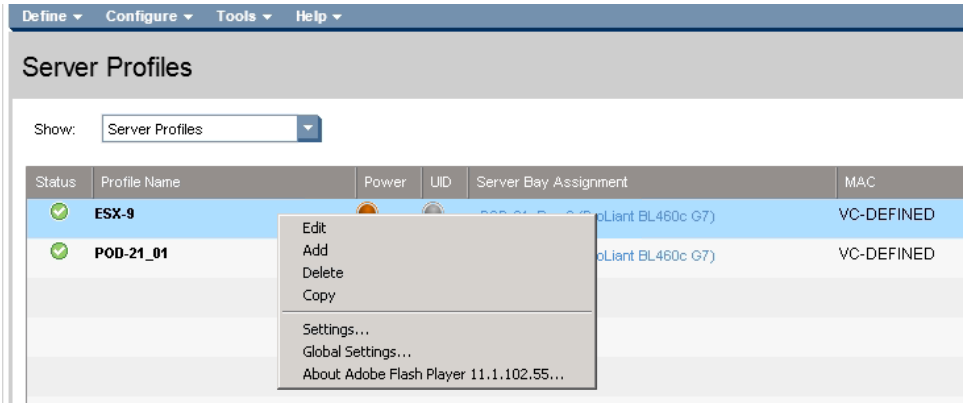
4. Click **Momentary Press** to power-off the server. Repeat these steps to shut down all servers.



5. In the Connections section in the navigation pane, click **Server Profiles** to go to the Server Profile page.

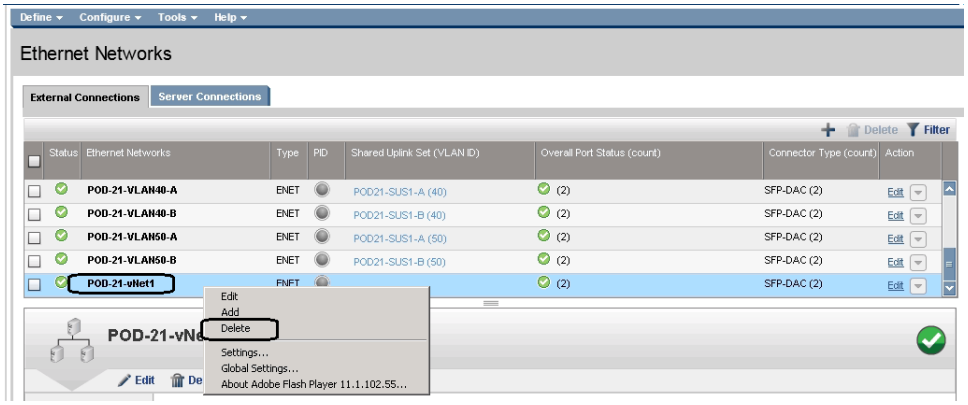
6. Ensure all servers have shut down, if they don't shut down right away, log in their iLO and verify that the OS is shutting down, shutdown manually through the iLO if needed. The do the same for the remaining profiles.

7. Left click on the ESX profile, the expose the "blue bar", right click on the blue bar area and select Delete to delete the profile.



8. As will require the use of uplinks X4 from each of the FlexFabric modules for the next lab, we will need to delete the network created in an earlier lab, POD-xx-vNet1.

9. In the left tree view, select Ethernet Networks, in the right pane scroll down to expose the network POD-xx-vnet1, where xx=your POD ID. Left click on the network to expose the Blue Bar, then right click and select Delete.



Summary

In this lab, you created two independent Share Uplink Sets (SUSs), each using uplink ports from a separate VC FlexFabric module. PODnn-SUS1-A uses two uplink ports from the FlexFabric module in Bay1, and PODnn-SUS1-B uses two uplink ports from the VC FlexFabric module in Bay2.

By defining the SUSs in this manner, you have set up separate and redundant connections from Virtual Connect to the upstream switches. When a server profile is assigned these SUSs, the NICs can connect to VLANs accessed through each VC Ethernet module. This enables you to create an active/active uplink scenario.

Alternatively, you could have created a single SUS and assigned both of these port trunks to the same SUS. However, this would have provided an active/standby uplink scenario.

With the Enhanced VLAN Capacity parameter enabled, which is the current setting in your VC domain, you can create an SUS that contains all the VLANs you might potentially present to a collection of servers. Then you can present selected VLANs to each operating system instance running on the server when you have an implementation involving a vSwitch such as with VMware ESXi. The vSwitch can separate the VLANs and present them to the guest operating system instances. By using Mapped VLAN Tags and an SUS, you minimize the number of uplink ports required for such a situation.

Normally, Virtual Connect tags all frames presented to the server NICs by an SUS — unless the Native check box is selected for one of the networks. In such a case, any untagged frames leaving the server would be placed on the network designated as the native VLAN.

You then deleted the all server profiles and network created in an earlier lab.

Implementing Shared Uplink Sets (with FCoE)

Lab 4B

Objectives

After completing this activity, you should be able to:

- Define two shared uplink sets (SUS')
- Add FCoE networks to the SUS'
- Assign FCoE connects to a server profile
- Examine the status of the uplink ports

Note: This lab includes the steps required to configure Virtual Connect release 4.01 for Dual Hop FCoE. The switches currently provided in this LAB environment do not support Dual Hop FCoE, therefore the final steps of proving connectivity will not be provided, however; the steps for configuring a Nexus switch for Dual Hop FCoE are provided in the LAB Appendices.

Introduction

In this lab, you will configure Virtual Connect to support two SUSs that will provide redundant access to the data center network and SAN Fabrics for FCoE connections. Each SUS will have one uplink port assigned to it. In addition, each SUS will support one untagged VLAN, several tagged VLANs and one tagged FCoE VLAN.

Virtual Connect Dual Hop FCoE

Dual-Hop FCoE support is a new feature provided in firmware release 4.01. This new feature allows the FCoE traffic to be propagated out of the enclosure to an external bridge which will handle the conversion of FCoE to FC traffic.

This feature is described as FCoE Dual Hop because there are two FCoE 'hops' between the server and the storage – the VC Module and the external FCoE -> FC bridge that connects the HP Virtual Connect modules to the storage. No additional external bridges are currently allowed in this configuration in order for Virtual Connect to guarantee the lossless of the FCoE connection.

Virtual Connect Requirements

Dual-Hop FCoE with HP Virtual Connect is currently supported with the following modules when running Virtual Connect firmware release 4.01 or later:

- HP Virtual Connect FlexFabric 10Gb/24-port Module
- HP Virtual Connect Flex-10/10D Ethernet Module

Converged Shared Uplink Sets (SUS) Details and Restrictions

- FCoE-capable Shared Uplink Sets (SUS) can contain both the FCoE network and non-FCoE networks.
- FCoE-capable SUS can support port aggregation (802.3ad).
- FCoE-capable SUS can support only one FCoE network.
- FCoE-capable SUS must always contain ports from a single VC module.

Note: For Multi Enclosure (ME) environments, all corresponding ports in remote enclosures will be included in the same SUS. (e.g. selecting enc0:bay1:X1 means bay1:X1 in all remote enclosures is also included).

Port limitations

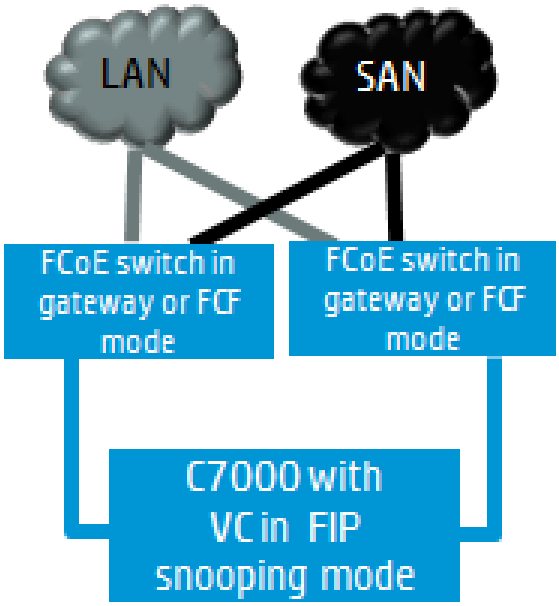
- The VC FlexFabric modules can only support FCoE on uplink port X1 to X4.
- The VC Flex-10/10D modules can support FCoE on ALL uplink ports (X1-X10)

Note: SFP+ LR transceivers are not supported on FCoE VC uplinks.

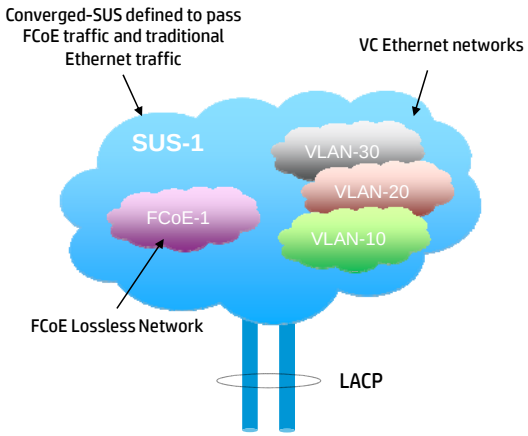
Virtual Connect Limitations

- Only Dual-Hop FCoE is supported by HP at this time
- Only Active/Active SUS configurations are supported for FCoE
- Stacking of a FCoE configured SUS is not supported
- FCoE-capable Shared Uplink Set (SUS) can be used to allow concurrent Ethernet and FCoE traffic, but only one of the networks in the SUS can be an FCoE Network
- Only one FCoE network can be associated with any single set of uplink ports

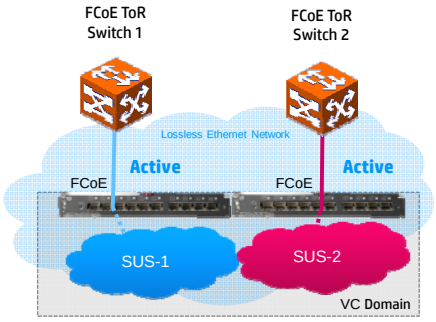
Dual-Hop FCoE Split FC & Ethernet at Top of Rack FCoE switch

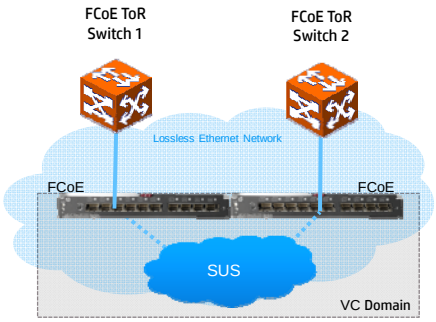


Virtual Connect SUS configuration when using FCoE



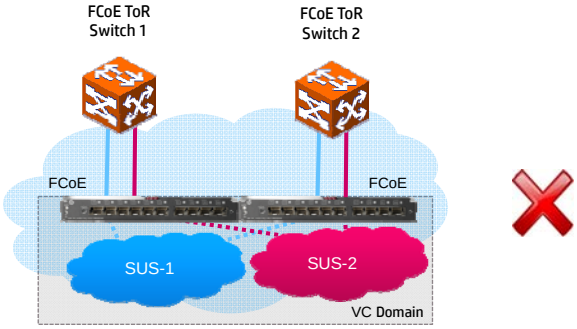
Active-Active FCoE Virtual Connect Configuration

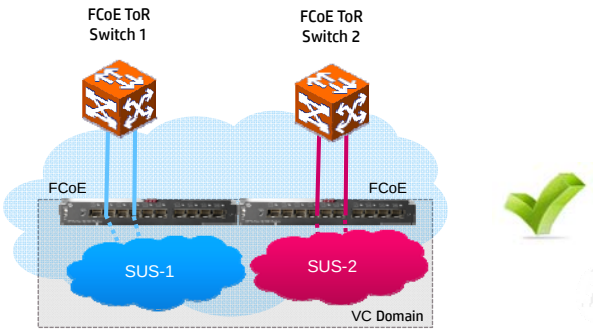




Note: FCoE-capable Shared Uplink Sets must always contain ports from a single VC module in order to maintain the SAN-A/B isolation.

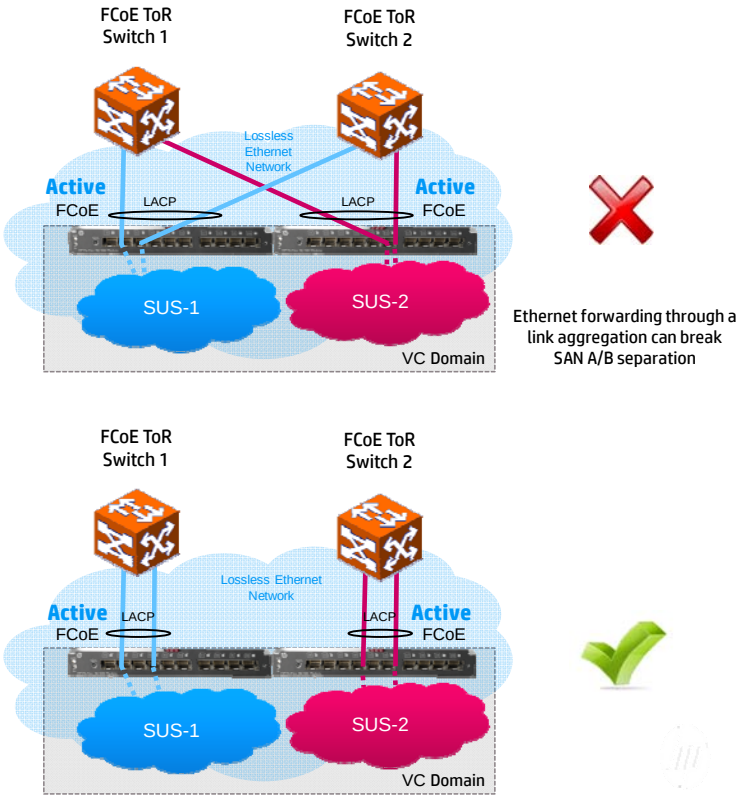
FCoE-capable Shared Uplink Set configuration support





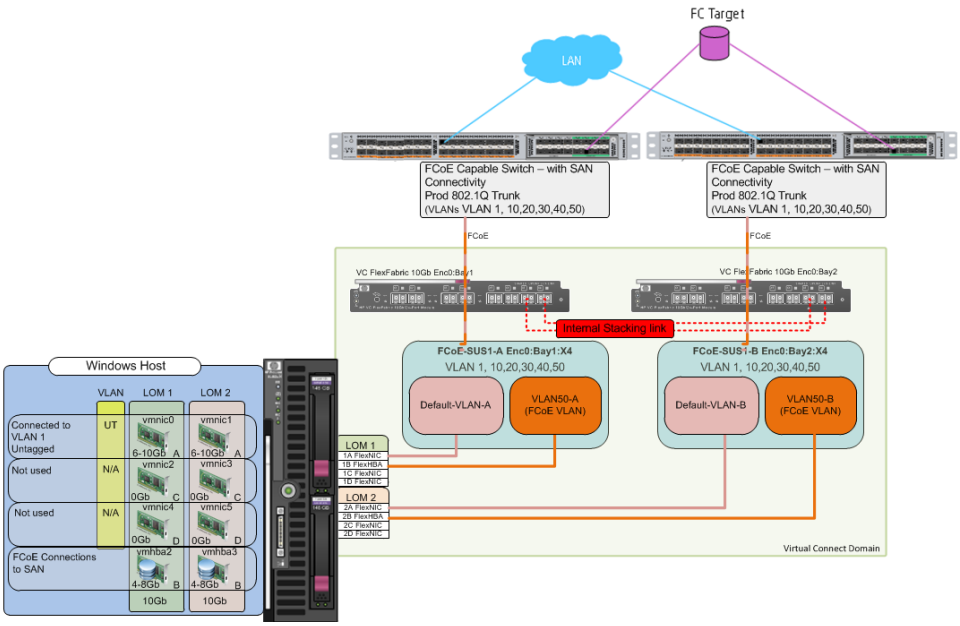
Note: FCoE-capable Shared Uplink Sets must always be connected to a single Top of Rack switch in order to maintain the SAN-A/B isolation.

FCoE-capable Shared Uplink Set LACP configuration support



Network diagrams

Example of Physical view of the LAN connections



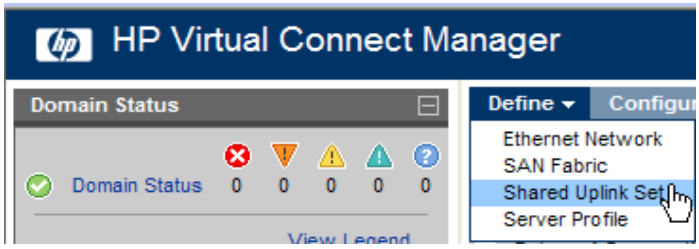
In this lab, both port trunks are active because they are assigned to separate SUSs. Although it is not done in this lab, additional uplinks could be used to increase uplink bandwidth and provide additional availability.

FCoE-SUS1-A uses the port trunk comprising the uplink port X4 from the VC FlexFabric module in Bay 1; FCoE-SUS1-B uses the port trunk comprising uplink port X4 from the VC FlexFabric module in Bay 2. Because two separate collections of VC networks are involved as a result of the SUSs, Virtual Connect allows each port trunk to operate in an active state.

Exercise 1 — Defining two redundant Shared Uplink Sets for use with FCoE Networks

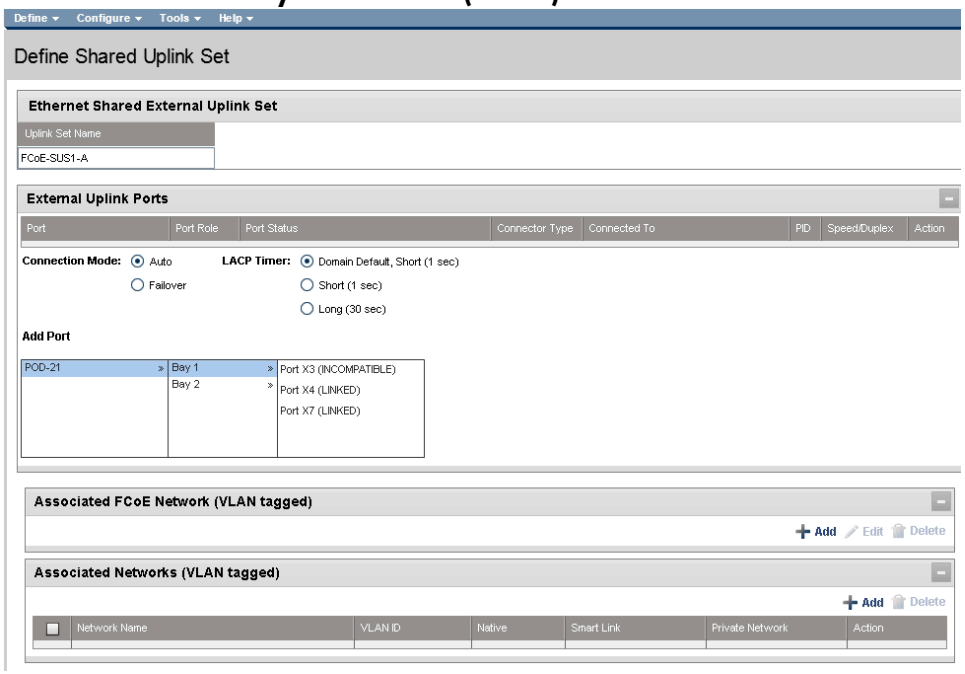
In this exercise, you will define two SUSs that will function as redundant networks and provide support for both Ethernet and FCoE connections. As part of the procedures for defining an SUS, you will assign an uplink port and will also define the VLANs the SUS will support, as this is a FlexFabric module, FCoE is only supported on Ports X1-X4, you will use port X4 on each module. You will be able to define VLAN identifiers for various VC networks that will comprise each SUS.

1. In the toolbar, click **Define**. Then in the drop-down menu, click **Shared Uplink Set**.

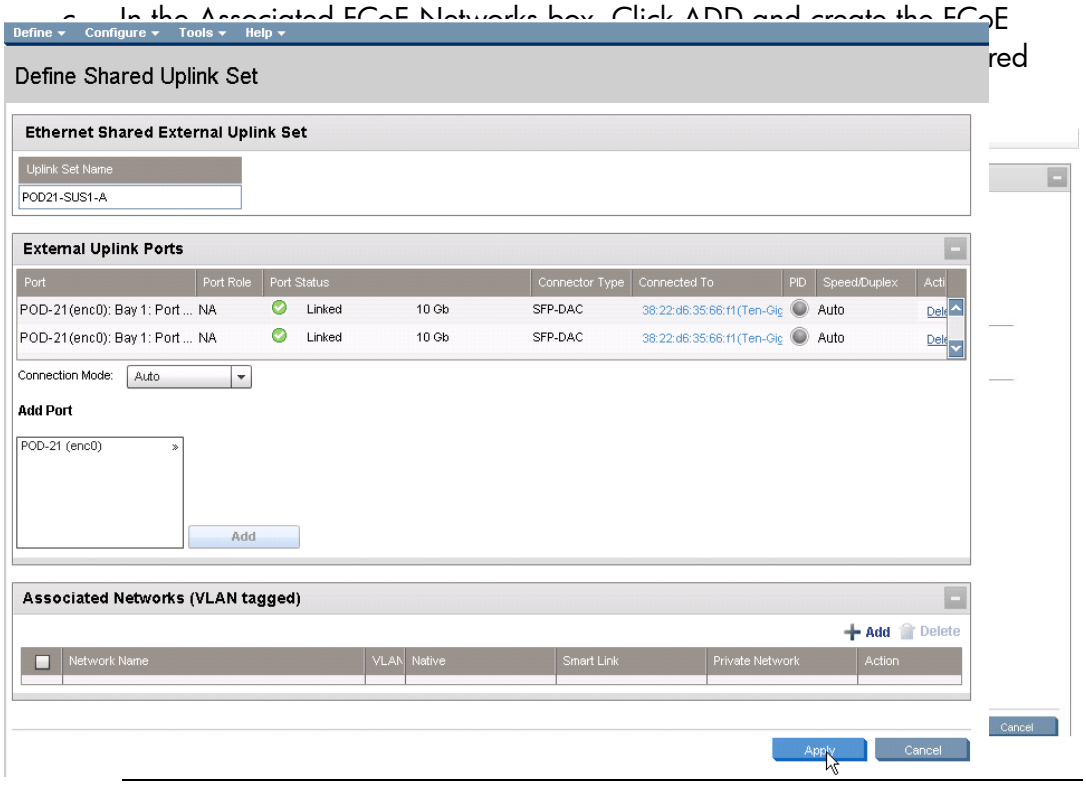


2. From the Define New Shared Uplink Set screen, follow these steps:
   a. For the Uplink Set Name, enter `FCoE-SUS1-A`.

b. Add the first external uplink port by clicking the Add Port section **<enclosure-name> Bay 1 → Port X4 (Linked)**



c. In the Associated FCoE Networks box, Click ADD and create the FCoE



Note

The port above is from the VC FlexFabric module in Interconnect **Bay 1**.

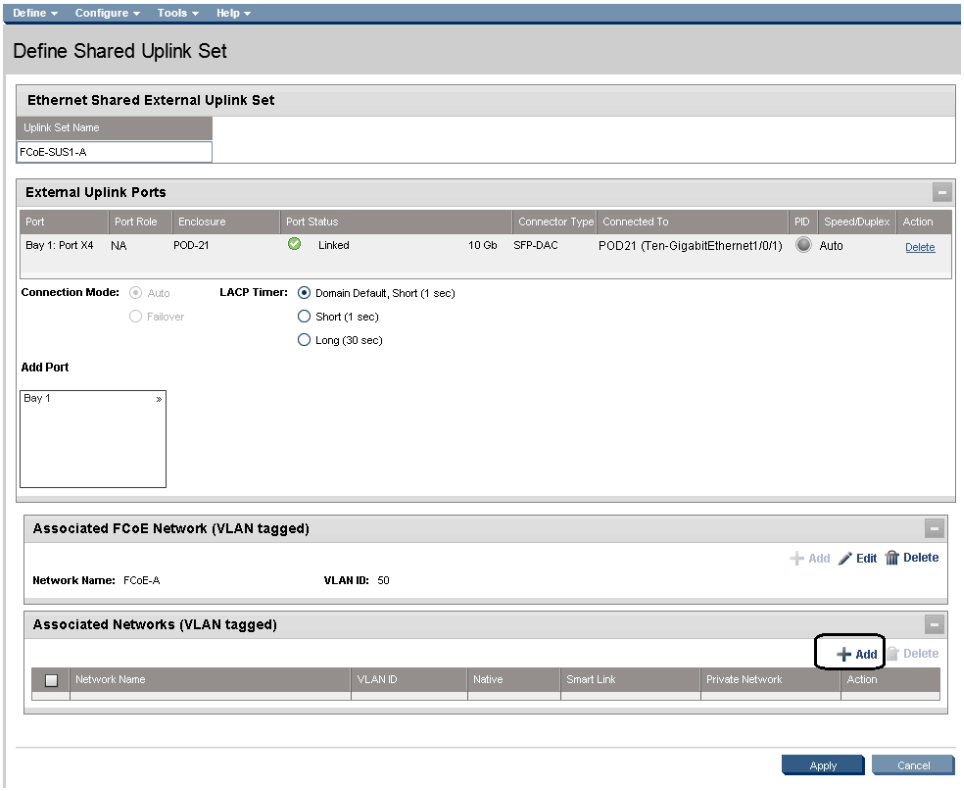
4. These are the VLANs that will be configured within this SUS.

Network Name	VLAN ID	Native	Smart Link
VLAN1-A	1	checked	Checked
VLAN10-A	10		Checked
VLAN20-A	20		Checked
VLAN30-A	30		Checked
VLAN40-A	40		Checked
FCoE-A	50		N/A

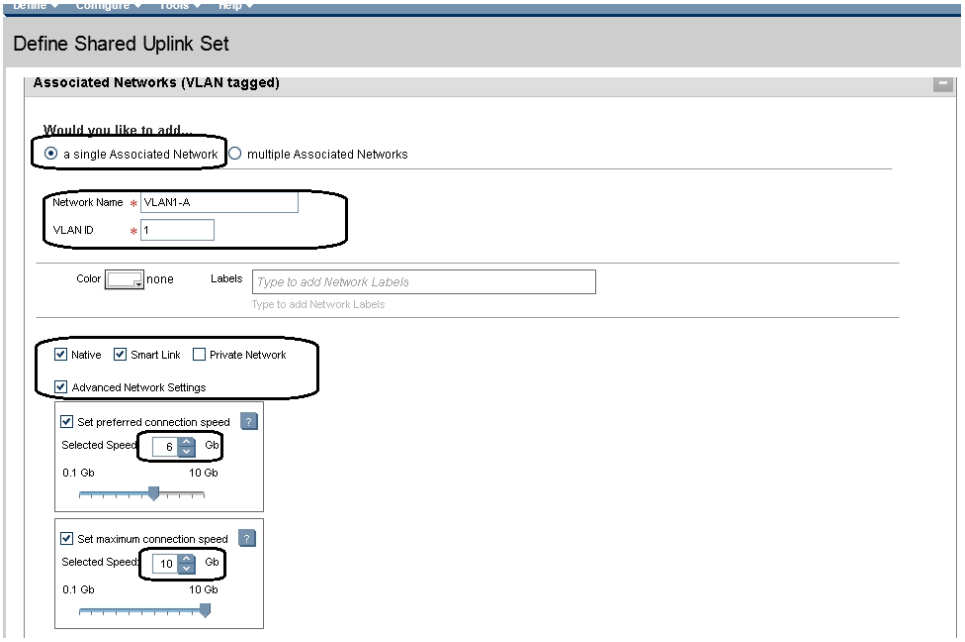
These networks are essentially just VC networks that will be listed under the Ethernet Networks folder of the navigation pane. In contrast to the VC networks you defined in previous lab exercises, these VC networks will be "assigned" to an SUS. That is, these networks are not simple vNets.

- **About the Native Parameter** — Only one network can have the Native option checked (that is, enabled in an SUS. This option indicates that the VLAN carries untagged frames only. In general, a given physical or logical link (port trunk) can transport at most one untagged VLAN. Hence, the SUS assigned one or more uplinks must operate according to that fundamental network rule.
- **About the Smart Link Parameter** — In this configuration, the Smart Link parameter is enabled on each of the VC networks that you define for this SUS. Smart Link will monitor the state of the uplinks and will turn off downlink ports to servers within Virtual Connect if all available uplinks assigned to a VC network are down.

4. To add the Default network, click **Add Network** and then specify the information from the table.

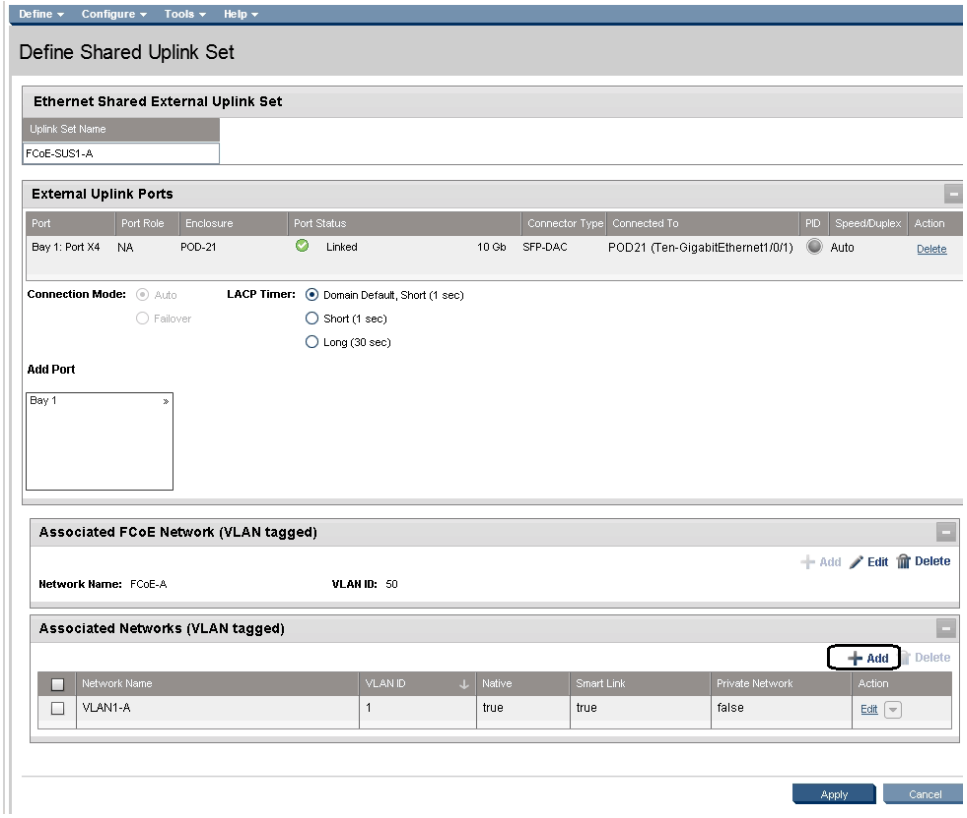


5. Enter the name for the "Default" network, and then specify the information from the table. Optionally, select Advanced and set the Preferred and Maximum Speeds.



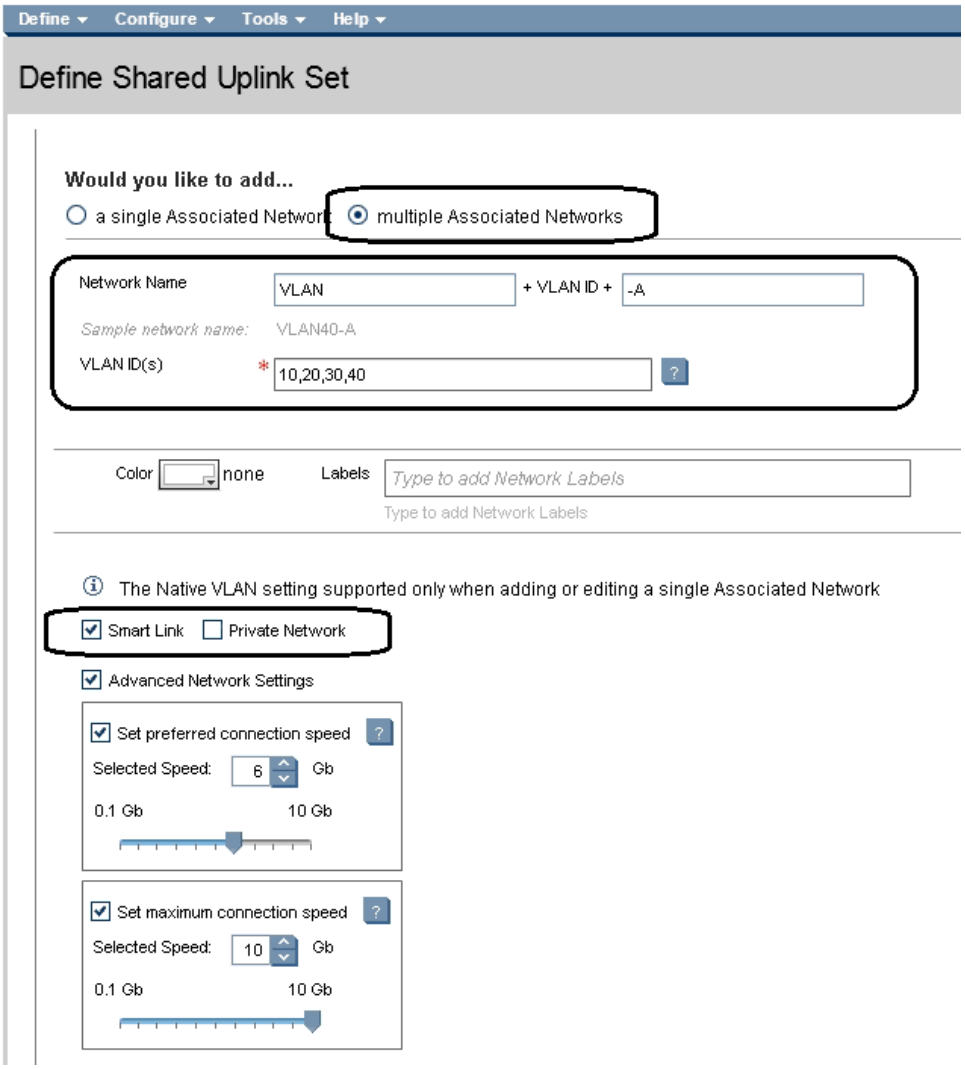
6. Scroll to the bottom of the page and **Click Apply.**

7. In the shared Uplink Sets Screen, select to Edit the SUS you just created as additional Networks will be added to this SUS.
8. Under the Associated Networks (VLAN tagged) box **Click ADD**

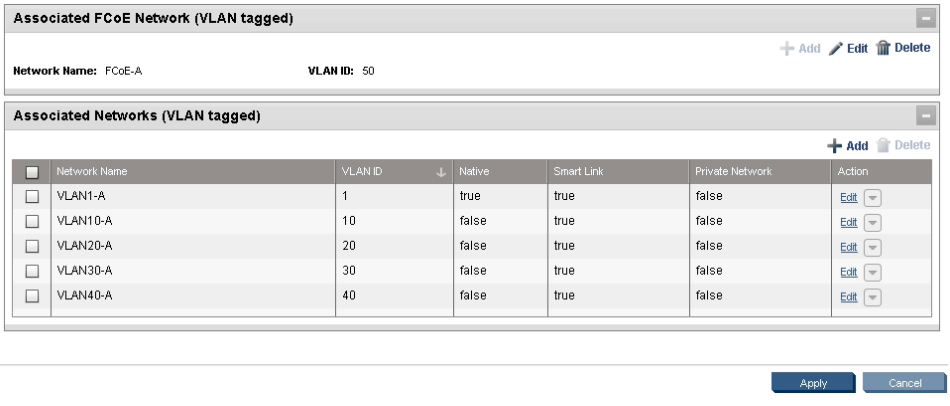


9. Under the Associated Networks (VLAN tagged) box **Click ADD,** when the windows opens, select the "multiple Associated Networks" radio button. The ability to create multiple networks in a single action was added to Virtual Connect in firmware release 3.70. The Advanced Networks Settings feature was added in release 4.01.

10. Scroll down and **click Apply.**

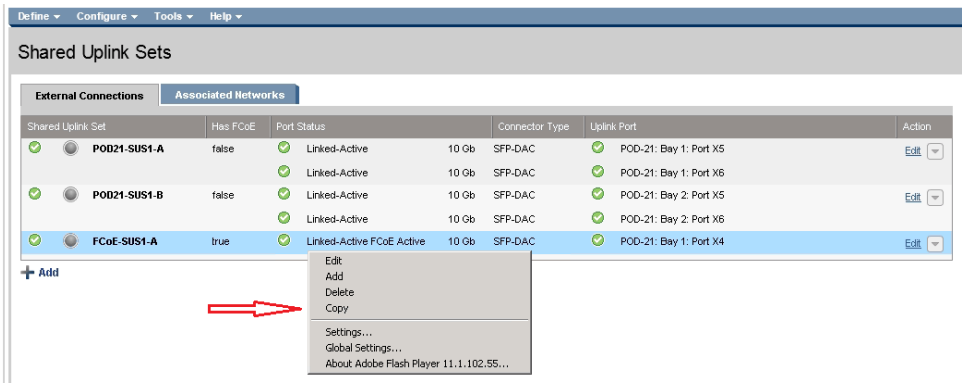


11. After you complete the data entry, the Associated Networks section of the window should display as follows.



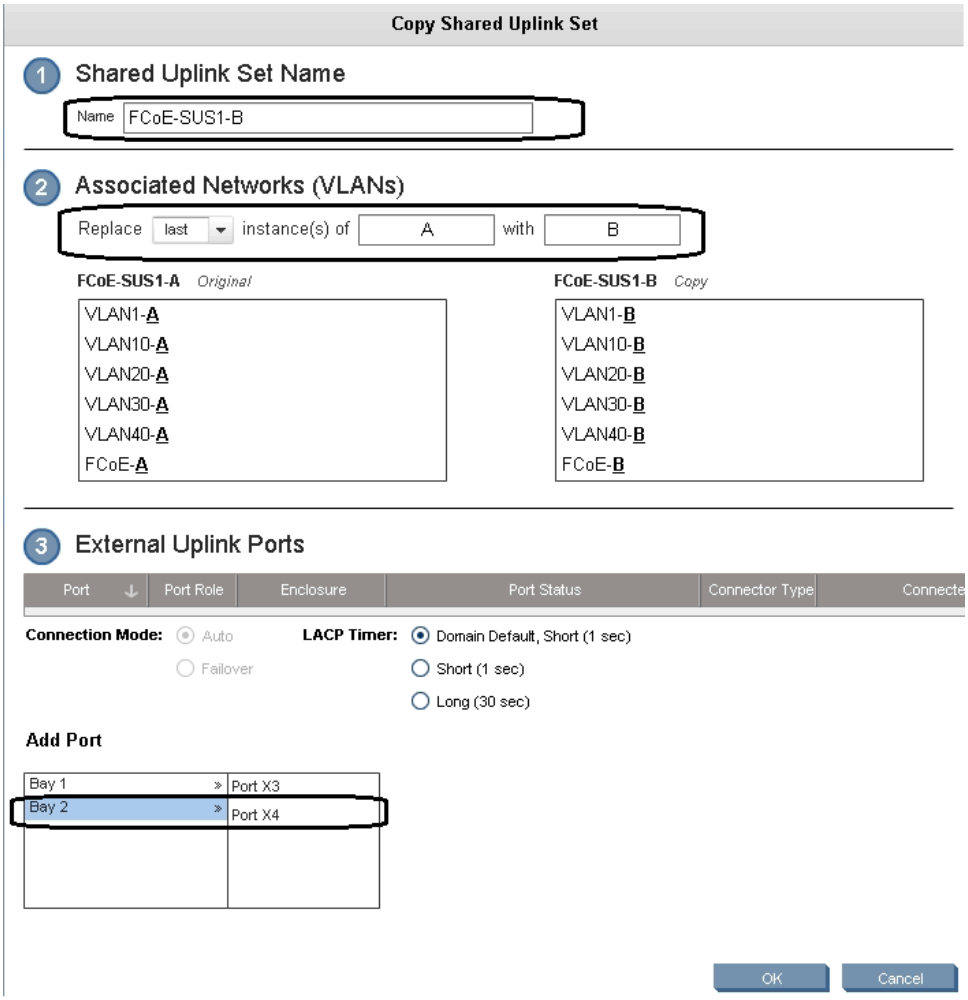
12. Verify that **Smart Link** is enabled for each network, but **Native** is only enabled for the first network (Default-VLAN-A). **The Click Apply.**

13. To define the second Shared Uplink Set, we will **COPY** the SUS you just created. In the Logical Configuration section of the navigation pane, click the **Shared Uplink Sets** entry to go to the Shared Uplink Sets page.
14. In the Shared Uplink Sets window, Left click on SUS you just created and **Click COPY.**



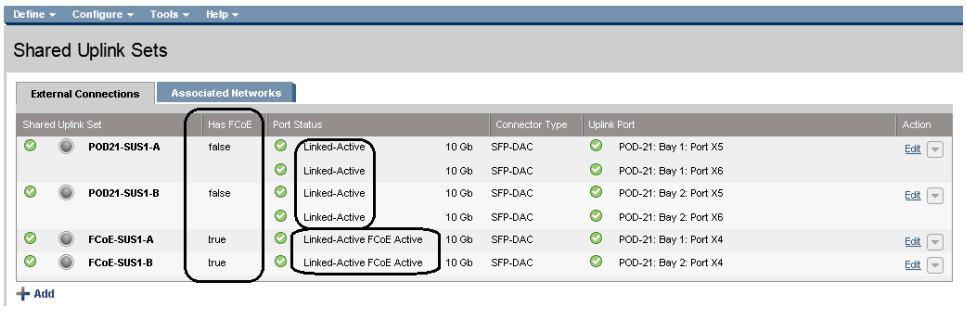
15. In the Shared Uplink Sets window, Left click on SUS you just created and **Click COPY.**

16. In the "Copy Shared Uplink Set" dialog box, Change the SAS Name to end in "B", select Replace "last" instance of "A" with "B". **Scroll down** and under ADD ports, Select port X4 from Bay 2, **Click OK**



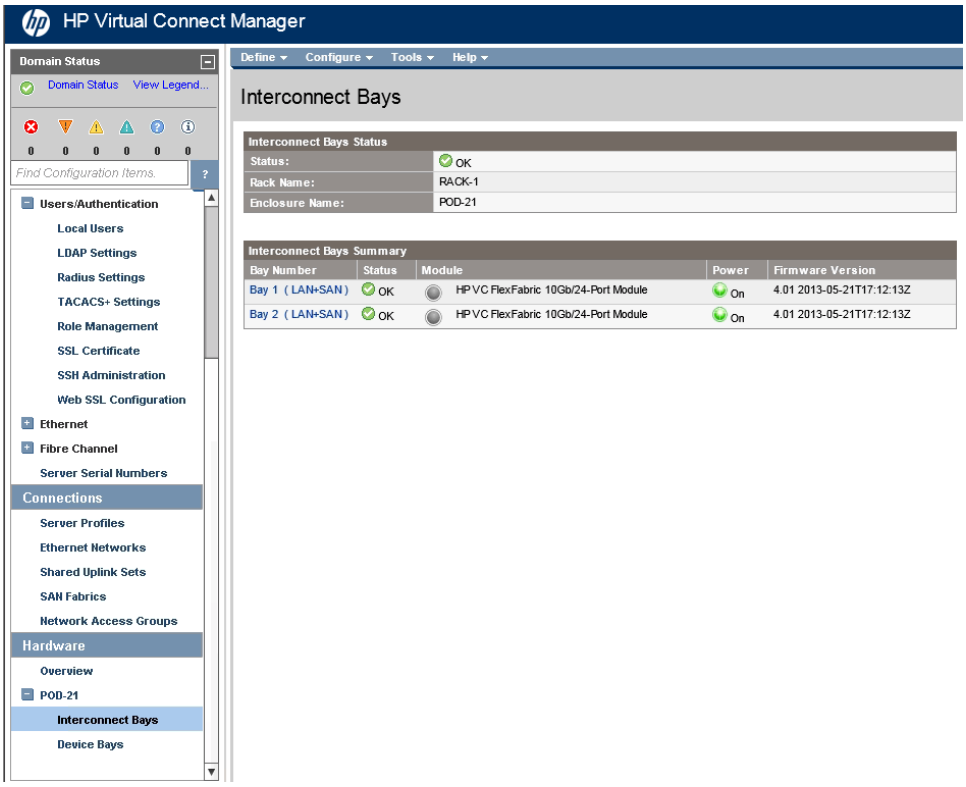
17. In the Shared Uplink Set s window, Left click on SUS you just created and **Click COPY.**

18. In the "Copy Shared Uplink Set" Table view, not that the new Shared Uplink Sets are present, along with the original Shared Uplink Sets created earlier. Also, notice the difference between the Shared Uplink Sets, under the "Has FCoE" column, the New SUS' have FCoE active

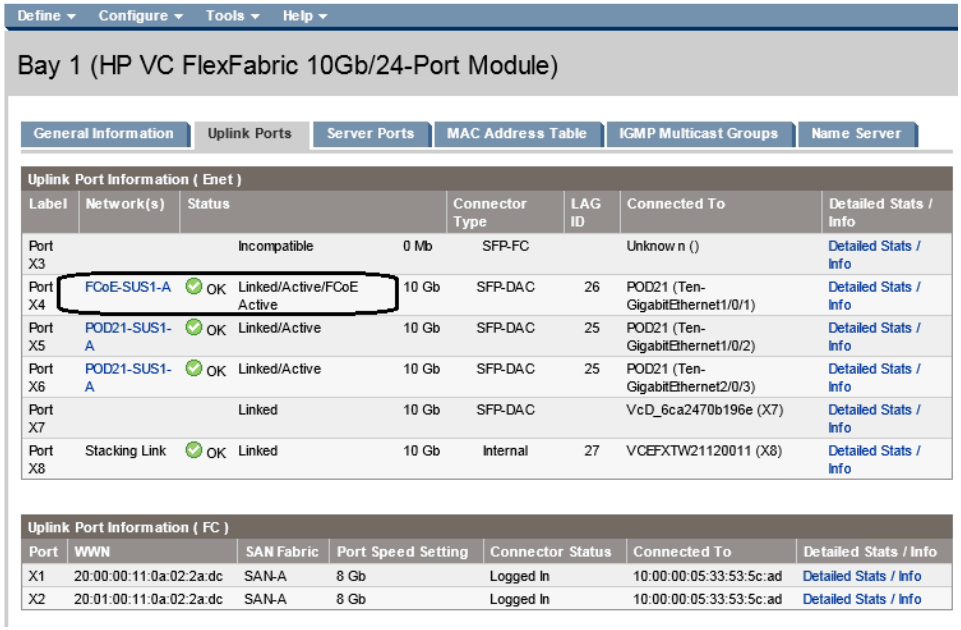


Exercise 2 — Examining the status of the uplink ports

1. In the navigation pane Hardware Configuration section, click **<enclosure-name> > Interconnect Bays**. Then in the main window, click the **Bay 1 (LAN+SAN)** link, which contains a VC FlexFabric module.



2. Notice that Bay 1: Port X4 which is assigned to Shared Uplink Set FCoE-SUS1-A and is Active with FCoE.



3. Repeat Step 1, choosing instead **Bay 2**, which contains the second VC FlexFabric module.

4. While in the Bay 2 module page, take a look at some of the other tabs on this page, such as Server Ports.

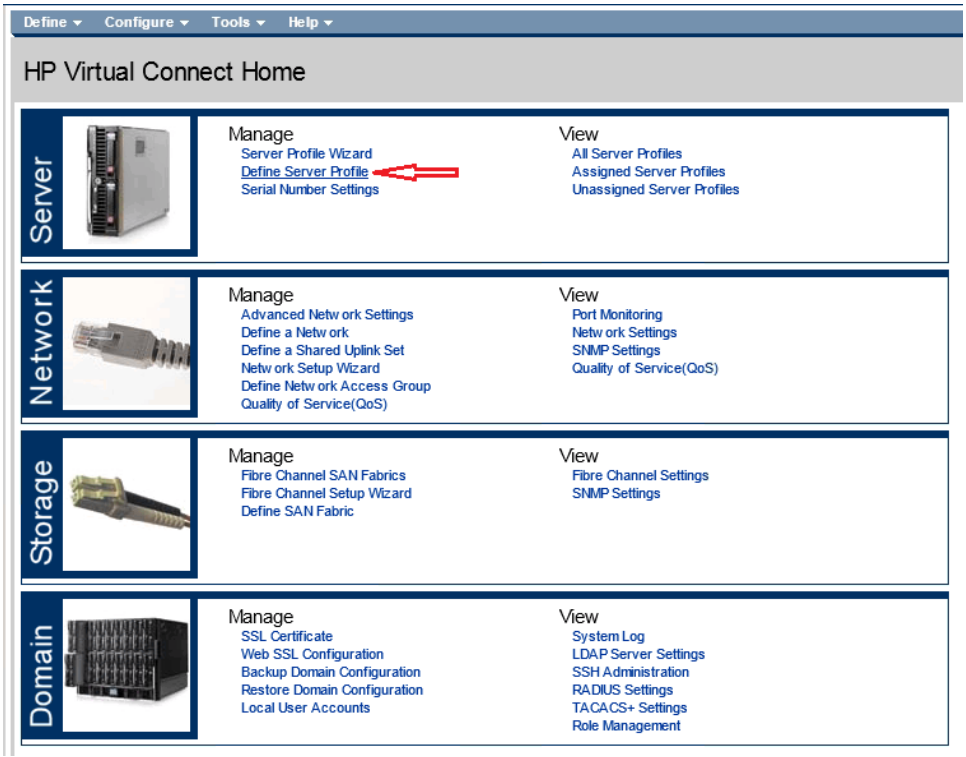
Exercise 3 — Creating a server profile

In this exercise, you will create a new server profile to be configured with a single network connection and an FCoE Storage connection to the SAN. This server profile will be used to connect a a locally booted Windows host to the network. For this exercise, you will use the server in Bay 1 of your c7000 enclosure.

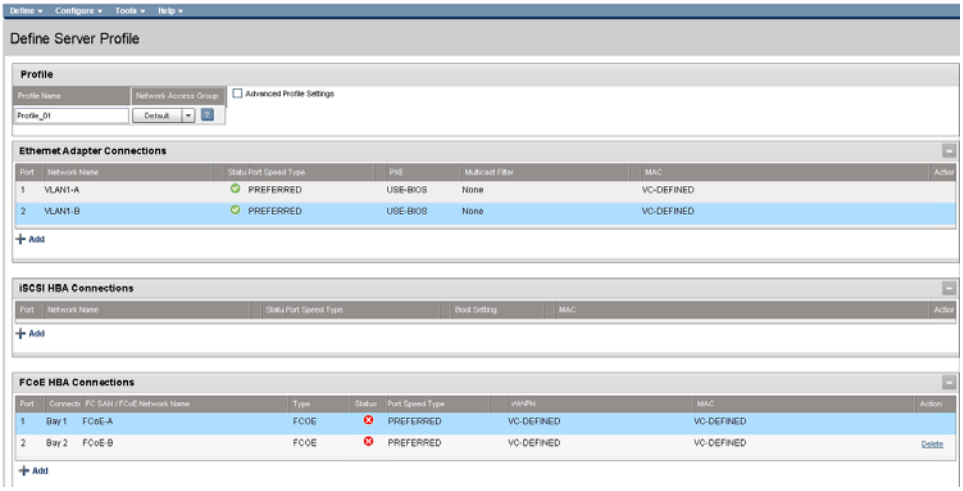
3. Open a web browser and access the Virtual Connect Manager home page.

> **!** **Important**
> As previously stated, the switches connected to this lab do not support dual hop FCoE, so proving the connection will not be possible at this time.

5. In the Virtual Connect Manage Home page, **click Define Server Profiles**.



6. Create new server profile as shown in the graphic below. In the Ethernet Adapter Connections box Assign Port 1 VLAN1-A and Port 2 to VLAN1-B. Connect the FCoE HBA ports to FCoE-A and FCoE-B, assign the profile to Bay 1 and **Click Apply.**



7. As the Upstream switch is not configured for FCoE connections, the SAN connections will present in an error state.

Summary

In this lab, you created two independent Share Uplink Sets (SUSs), each using uplink ports from a separate VC FlexFabric module. FCoE-SUS1-A uses one uplink port from the FlexFabric module in Bay1, and FCoE-SUS1-BB uses one uplink port from the VC FlexFabric module in Bay2.

By defining the SUSs in this manner, you have set up separate and redundant connections from Virtual Connect to the upstream switches. When a server profile is assigned these SUSs, the NICs can connect to VLANs accessed through each VC Ethernet module. This enables you to create an active/active uplink scenario.

You then define an FCoE VLAN within each SUS and created a Server profile to utilize both the LAN and FCoE connections.

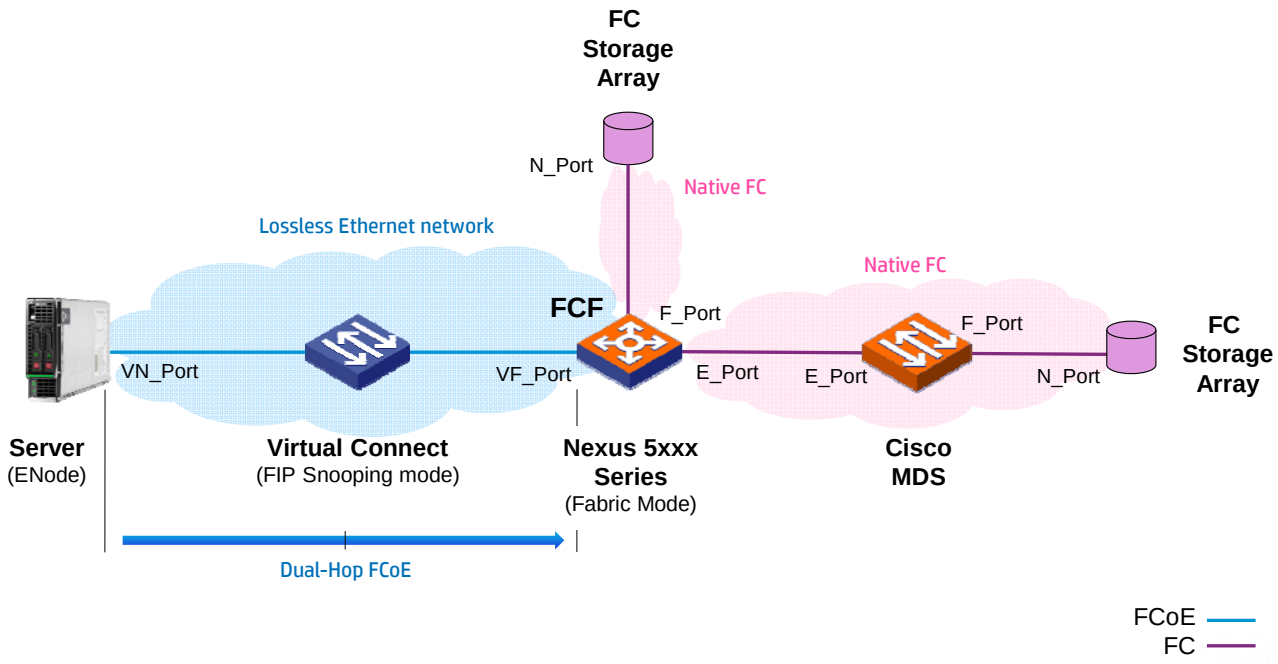
This lab was intended to show the steps required to configure Virtual Connect release 4.01 to utilize FCoE (Dual hop) to an external switch that supports FCoE connections. The Appendix that follows this lab provides the commands required to configure a Nexus 5000 switch to support these connections.

Appendices

Dual-Hop FCoE with Nexus 5xxx Series ToR switch in FCF mode

The Nexus switches operate as Fiber Channel Forwarders (FCF). This is the default Cisco Nexus 5xxx Series switches mode, it's also called the fabric mode. In this mode, the switch provides standard Fibre Channel switching capability and features.

Figure 1 - Cisco Nexus 5xxx switches operating as FC Forwarder (FCF)

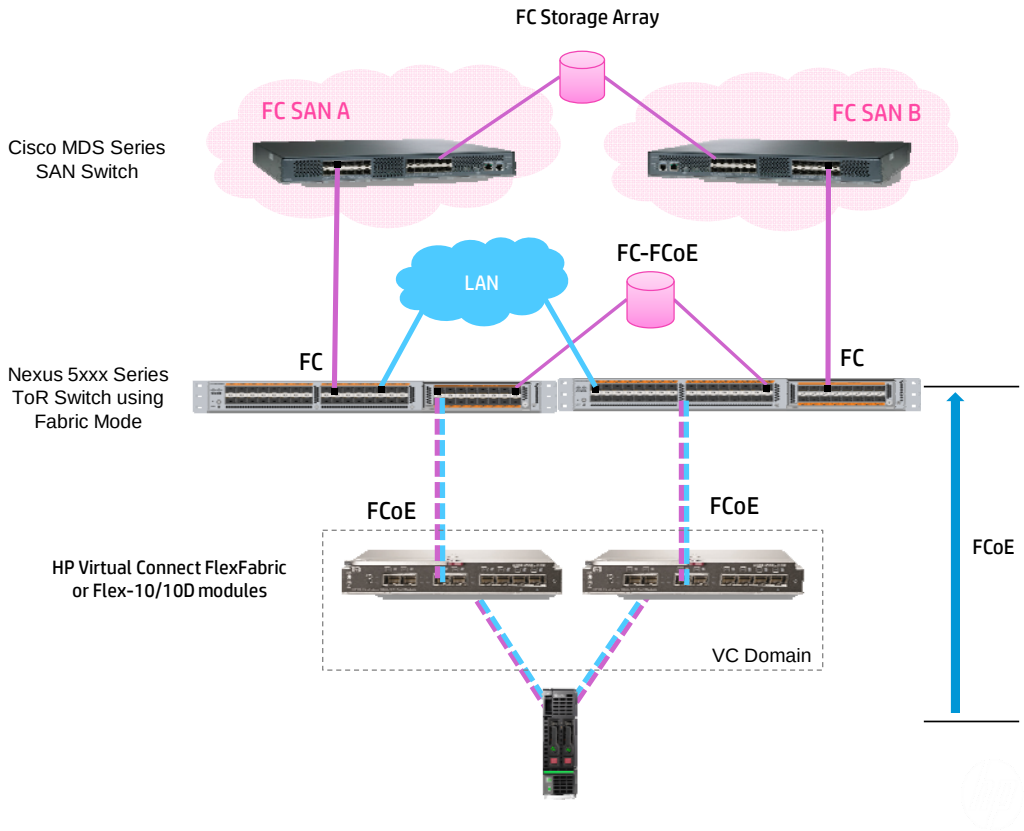


FCF mode recommendations:

Nexus switches must either bridge to native FC infrastructure or directly connect to FC/FCoE-based Storage devices. Refer to the Cisco Nexus or Storage vendor interoperability Matrix.

When bridged to a native FC infrastructure, it is mandatory to use Cisco MDS directors or fabric switches in order to provide interoperability between fabrics.

Figure 2 - Physical view



Requirements

Minimum NX-OS version 5.2(1)N1(3).

FCoE requires the Nexus Storage Protocols Services license (FC_FEATURES_PKG).

Note: The license is an option which is activated when the Nexus switch is shipped from Cisco.

Guidelines

To increase the FCoE traffic identification and to better control the span of this traffic over the Ethernet network, it is recommended to use different FCoE VLANs and VSANs numbers between the two fabrics.

The FCoE VLAN should be dedicated to FCoE traffic (i.e. it should not carry IP traffic).

The FCoE VLAN must not be configured as a native VLAN (the VLAN that carries untagged traffic on trunk ports, by default VLAN 1).

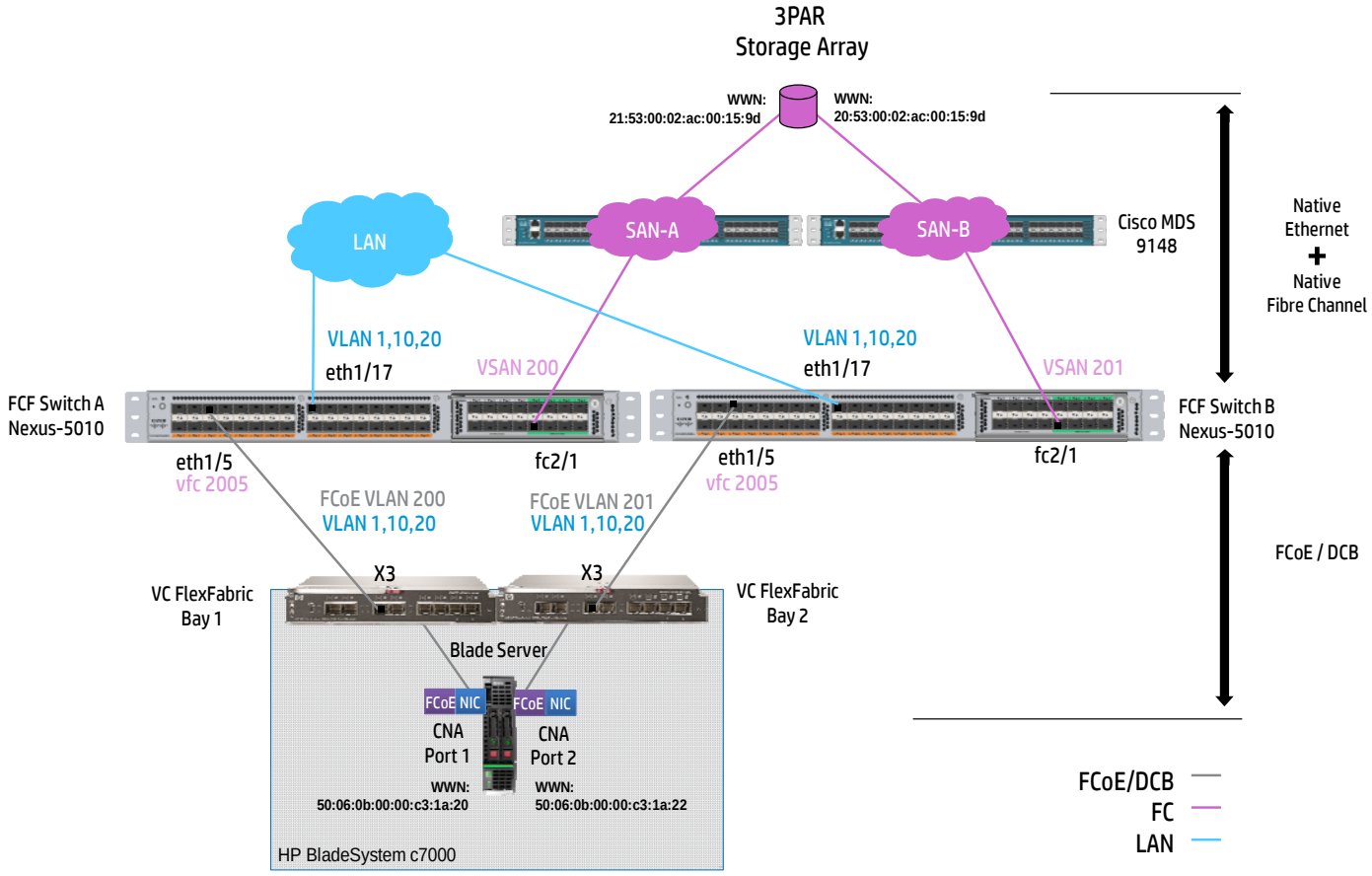
Interfaces connecting to VC must be configured as **trunk** ports and **STP edge ports**. (STP does not run on FCoE VLANs between FCFs (VE_Ports) but does run on FCoE VLANs towards the host (VF_Ports)).

Nexus configuration when using a single VC to Nexus link

Details about the configuration:

- Interfaces eth1/5 are connected to the VC modules.
- Interfaces fc2/1 are directly connected to Cisco MDS 9148 switches.
- VLAN IDs 200 and 201 are used for the FCoE networks.
- VLAN IDs 1, 10 and 20 are the standard Ethernet networks (non-FCoE networks).
- The vfc interface (virtual Fibre Channel interface) binds to eth1/5.

Figure 3 - Physical diagram



Nexus switch-A configuration

- Upgrade the first Nexus switch with minimum System version 5.0(2)N2(1) (enter: show version)
- Enable FCoE on the switch:
  - **conf t**
  - **feature fcoe**
- Map a VSAN for FCoE traffic onto a VLAN:
  - **vlan 200**
  - **fcoe vsan 200**
- Create a virtual Fibre Channel interface to carry the FCoE traffic through eth1/5:
  - **interface vfc 2005**
  - **bind interface ethernet 1/5**
  - **no shutdown**
- Create the VLANs for the IP traffic:
  - **vlan 1,10,20**
- Create a trunk on the interface to pass the FCoE (VLAN 200) and Ethernet traffic (VLAN 1,10,20):
  - **interface Ethernet1/5**
  - **description FCoE uplink to FlexFabric**
  - **switchport mode trunk**
  - **switchport trunk allowed vlan 1,10,20,200**
  - **spanning-tree port type edge trunk**
- Assign the vfc interface to the appropriate VSAN:
  - **vsan database**
  - **vsan 200**
  - **vsan 200 interface vfc 2005**
- Configure the interface connected to the datacenter LAN:
  - **interface eth 1/17**
  - **switchport mode trunk**
  - **switchport trunk allowed vlan 1,10,20**
- Configuration of the zone:

a. Create zones:
  - **zone name fcoe-zone vsan 200**
  - **member pwwn 21:53:00:02:ac:00:15:9d** {This is the WWN of the first 3PAR controller port}
  - **member pwwn 50:06:0b:00:00:c3:1a:20** {This is the WWN of the Blade FlexFabric Adapter port 1}

b. Create zoneset:
  - **zoneset name zoneset1 vsan 200**
  - **member fcoe-zone**

c. Activate zoneset:
  - **zoneset activate name zoneset1 vsan 200**

Nexus switch-B configuration

- Upgrade the second Nexus switch with minimum System version 5.0(2)N2(1) (enter: show version)
- Enable FCoE on the switch:
  - **conf t**
  - **feature fcoe**
- Map a VSAN for FCoE traffic onto a VLAN:
  - **vlan 201**
  - **fcoe vsan 201**
- Create a virtual Fibre Channel interface to carry the FCoE traffic through eth1/5:
  - **interface vfc 2005**
  - **bind interface ethernet 1/5**
  - **no shutdown**
- Create the VLANs for the IP traffic:
  - **vlan 1,10,20**
- Create a trunk on the interface to pass the FCoE (VLAN 200) and Ethernet traffic (VLAN 1,10,20):
  - **interface Ethernet1/5**
  - **description FCoE uplink to FlexFabric**
  - **switchport mode trunk**
  - **switchport trunk allowed vlan 1,10,20,201**
  - **spanning-tree port type edge trunk**
- Assign the vfc interface to the appropriate VSAN:
  - **vsan database**
  - **vsan 201**
  - **vsan 201 interface vfc 2005**
- Configure the interface connected to the datacenter LAN:
  - **interface eth 1/17**
  - **switchport mode trunk**
  - **switchport trunk allowed vlan 1,10,20**
- Configuration of the zone:

a. Create zones:
  - **zone name fcoe-zone vsan 201**
  - **member pwwn 20:53:00:02:ac:00:15:9d** {This is the WWN of the second 3PAR controller port}
  - **member pwwn 50:06:0b:00:00:c3:1a:22** {This is the WWN of the Blade FlexFabric Adapter port 2}

b. Create zoneset:
  - **zoneset name zoneset1 vsan 201**
  - **member fcoe-zone**

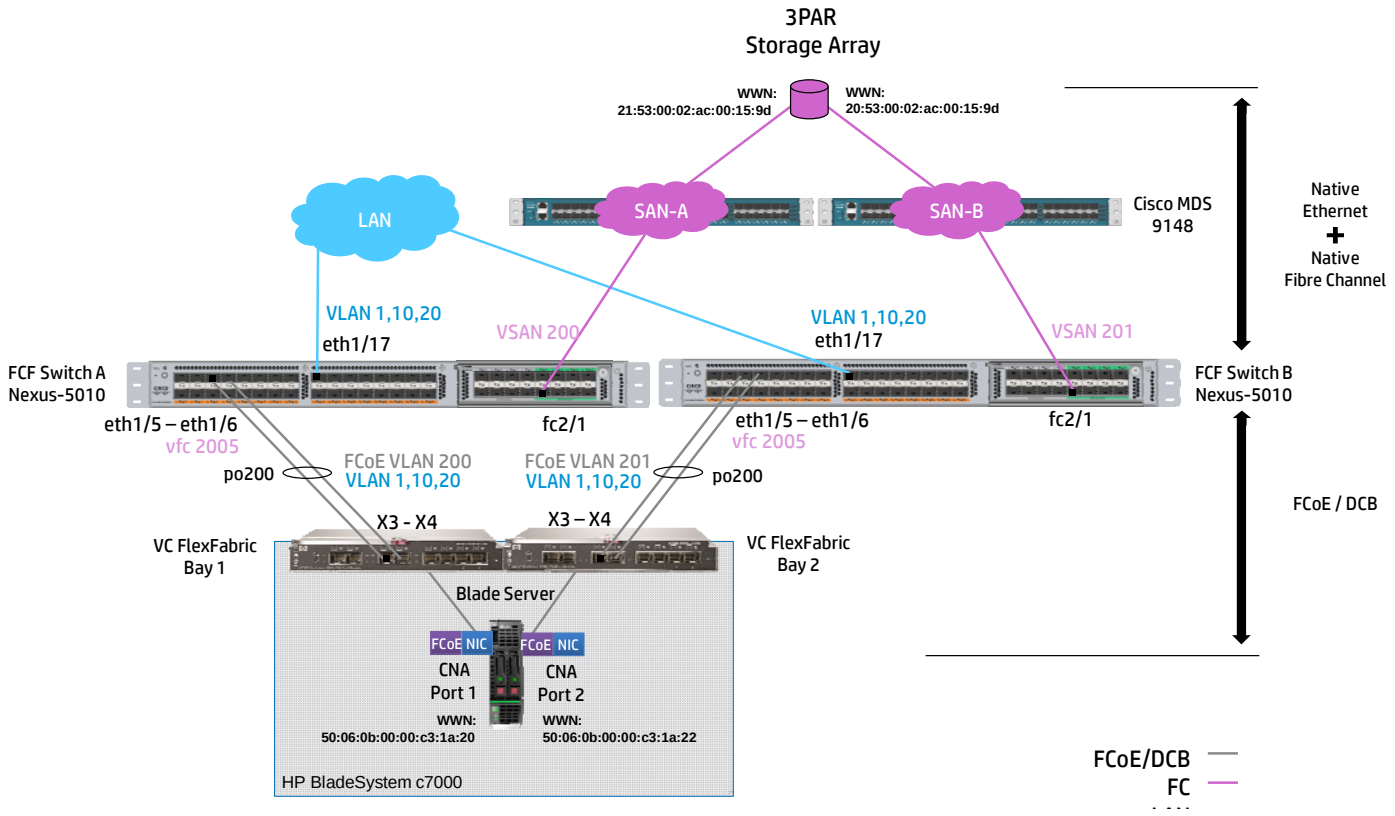
c. Activate zoneset:
  - **zoneset activate name zoneset1 vsan 201**

Nexus configuration when using a port channel between VC and Nexus

Details about the configuration:

- Interfaces **eth1/5** and **eth1/6** are connected to the VC modules.
- Interfaces **fc2/1** are directly connected to Cisco MDS 9148 switches.
- VLAN IDs **200** and **201** are used for the FCoE networks.
- VLAN IDs **1**, **10** and **20** are the standard Ethernet networks (non-FCoE networks).
- The **vfc** interface (virtual Fibre Channel interface) binds to the Port Channel **200** configured with **eth1/5** and **eth1/6**.

Figure 4 - Physical diagram



Nexus switch-A configuration

- Upgrade the first Nexus switch with minimum System version 5.0(2)N2(1) (enter: show version)
- Enable FCoE and LACP on the switch:
  - **conf t**
  - **feature fcoe**
  - **feature lacp**
- Map a VSAN for FCoE traffic onto a VLAN:
  - **vlan 200**
  - **fcoe vsan 200**
- Create a port channel with eth1/5 and eth1/6 with the same LACP Timer as defined by default in the Virtual Connect Domain:
  - **Interface ethernet 1/5**
  - **channel-group 200 mode active**
  - **lacp rate fast**
  - **interface ethernet 1/6**
  - **channel-group 200 mode active**
  - **lacp rate fast**
- Create the VLANs for the IP traffic:
  - **vlan 1,10,20**
- Create a trunk on the port channel interface to pass the FCoE (VLAN 200) and Ethernet traffic (VLAN 1,10,20):
  - **interface port-channel 200**
  - **switchport mode trunk**
  - **switchport trunk allowed vlan 1,10,20,200**
  - **spanning-tree port type edge trunk**
- Create a virtual Fibre Channel interface to carry the FCoE traffic through the port channel:
  - **interface vfc 2005**
  - **bind interface port-channel 200**
  - **no shutdown**
- Assign the vfc interface to the appropriate VSAN:
  - **vsan database**
  - **vsan 200**
  - **vsan 200 interface vfc 2005**
- Configure the interface connected to the datacenter LAN:
  - **interface eth 1/17**
  - **switchport mode trunk**
  - **switchport trunk allowed vlan 1,10,20**
- Configuration of the zone:

a. Create zones:

  - **zone name fcoe-zone vsan 200**
  - **member pwwn 21:53:00:02:ac:00:15:9d** {This is the WWN of the first 3PAR controller port}
  - **member pwwn 50:06:0b:00:00:c3:1a:20** {This is the WWN of the Blade FlexFabric Adapter port 1}

b. Create zoneset:

  - **zoneset name zoneset1 vsan 200**
  - **member fcoe-zone**

c. Activate zoneset:

  - **zoneset activate name zoneset1 vsan 200**

Nexus switch-B configuration

- Upgrade the first Nexus switch with minimum System version 5.0(2)N2(1) (enter: show version)
- Enable FCoE and LACP on the switch:
  - **conf t**
  - **feature fcoe**
  - **feature lacp**
- Map a VSAN for FCoE traffic onto a VLAN:
  - **vlan 201**
  - **fcoe vsan 201**
- Create a port channel with eth1/5 and eth1/6 with the same LACP Timer as defined by default in the Virtual Connect Domain:
  - **Interface ethernet 1/5**
  - **channel-group 200 mode active**
  - **lacp rate fast**
  - **interface ethernet 1/6**
  - **channel-group 200 mode active**
  - **lacp rate fast**
- Create the VLANs for the IP traffic:
  - **vlan 1,10,20**
- Create a trunk on the port channel interface to pass the FCoE (VLAN 200) and Ethernet traffic (VLAN 1,10,20):
  - **interface port-channel 200**
  - **switchport mode trunk**
  - **switchport trunk allowed vlan 1,10,20,201**
  - **spanning-tree port type edge trunk**
- Create a virtual Fibre Channel interface to carry the FCoE traffic through the port channel:
  - **interface vfc 2005**
  - **bind interface port-channel 200**
  - **no shutdown**
- Assign the vfc interface to the appropriate VSAN:
  - **vsan database**
  - **vsan 201**
  - **vsan 201 interface vfc 2005**
- Configure the interface connected to the datacenter LAN:
  - **interface eth 1/17**
  - **switchport mode trunk**
  - **switchport trunk allowed vlan 1,10,20**
- Configuration of the zone:

a. Create zones:

  - **zone name fcoe-zone vsan 201**
  - **member pwwn 20:53:00:02:ac:00:15:9d** {This is the WWN of the second 3PAR controller port}
  - **member pwwn 50:06:0b:00:00:c3:1a:22** {This is the WWN of the Blade FlexFabric Adapter port 2}

b. Create zoneset:

  - **zoneset name zoneset1 vsan 201**
  - **member fcoe-zone**

c. Activate zoneset:

  - **zoneset activate name zoneset1 vsan 201**

Configuring Virtual Connect QoS

Lab 5

Objectives

After completing this activity, you should be able to:

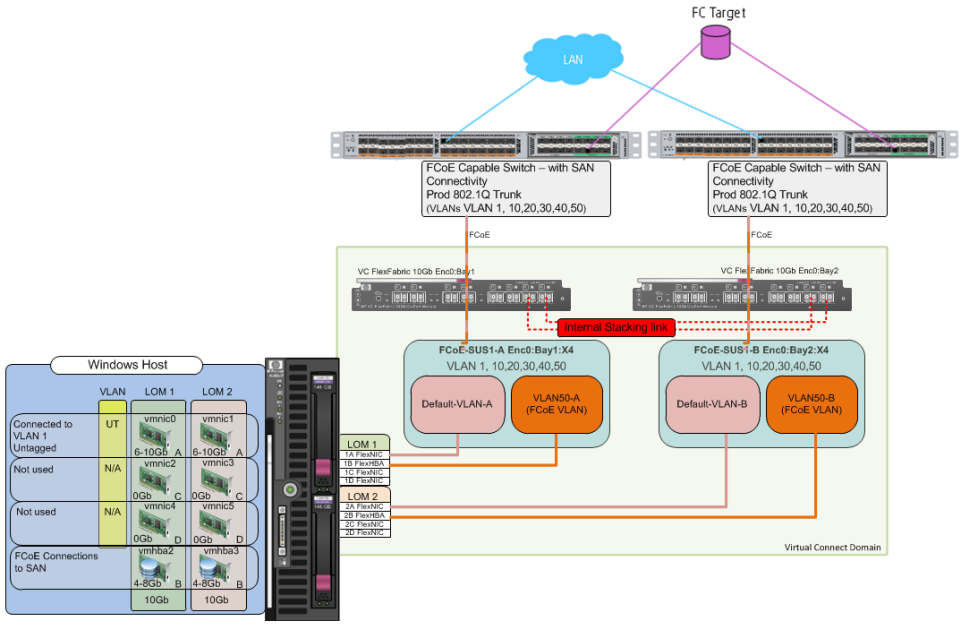
- Configure Virtual Connect for QoS

Introduction

In this lab, you will configure Virtual Connect for QoS support. The default configuration for Virtual Connect is QoS pass-through. In this lab you will enable QoS with Lossless FCoE. to support two SUSs that will provide redundant access to the data center network. Each SUS will have a pair of uplink ports (port trunk) assigned to it. Each SUS will support one untagged VLAN and several tagged VLANs.

In addition, QoS will be configured within Virtual Connect to coincide with the QoS configuration of the upstream switch.

Network diagrams



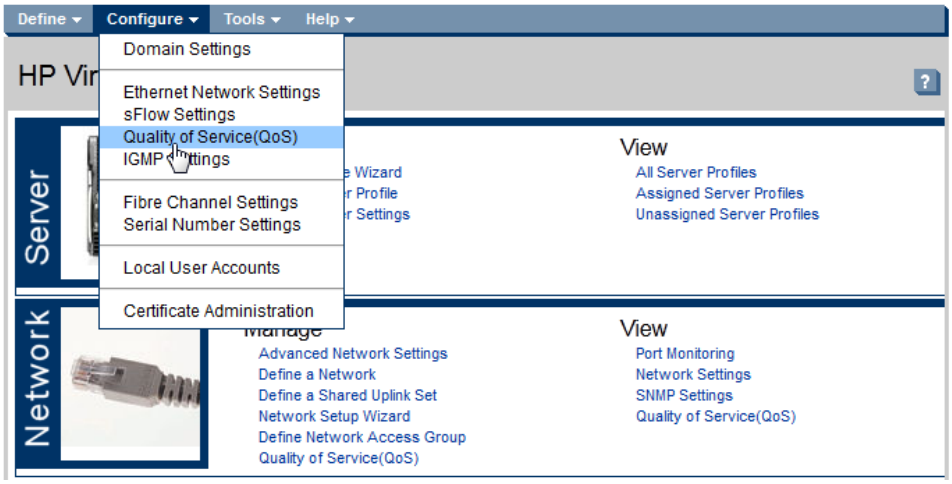
Physical view of the LAN connections

In this lab, both port trunks are active because they are assigned to separate SUSs. Although it is not done in this lab, additional uplinks could be used to increase uplink bandwidth and provide additional availability.

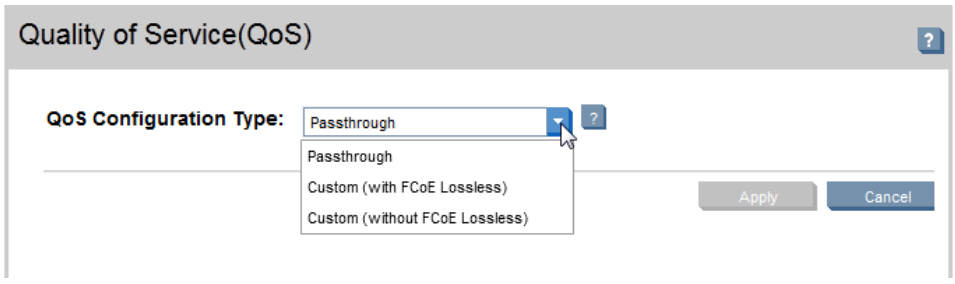
FCoE-SUS1-A uses the port trunk comprising the uplink port X4 from the VC FlexFabric module in Bay 1; FCoE-SUS1-B uses the port trunk comprising uplink port X4 from the VC FlexFabric module in Bay 2. Because two separate collections of VC networks are involved as a result of the SUSs, Virtual Connect allows each port trunk to operate in an active state.

Exercise 1 — Configuring QoS

To change the QoS config type inside the GUI you need to visit the Quality of Service (QoS) section from the configuration bar. All changes in this area have VC domain wide responsibilities.



Under the QoS section you select the QoS configuration type. This specifies the QoS operation mode. The default mode is "Pass-through". If FCoE is not being used, select Custom (without FCoE Lossless), by doing so, you free up an extra queue that would normally be assigned to Lossless FCoE. However; if FCoE connections have been created or will be used, then select Custom (with FCoE Lossless). For this lab, select Custom (with FCoE Lossless)

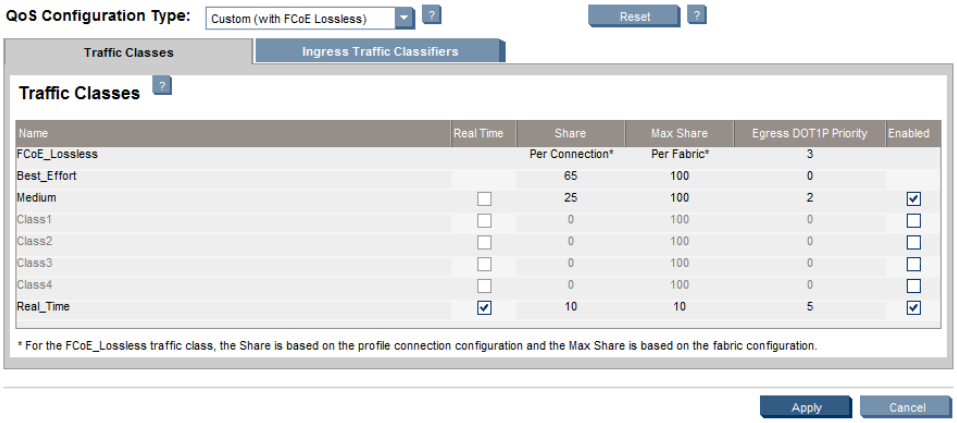


Note: You cannot switch to Custom (without FCoE Lossless) when the domain has a fabric associated with an FCoE capable interconnect module, a Shared Uplink Set has an associated FCoE network, or a server profile has an FCoE connection.

Configuring the QoS Traffic Class

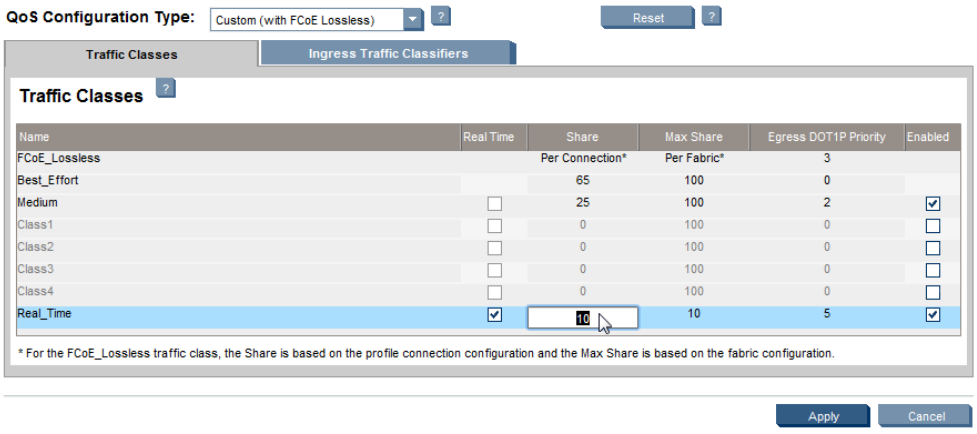
The next section is only available when you have not chosen the "Custom (with Lossless FCoE)" QoS configuration type. Once selected, you will see the following menu option where you have the possibility to enable specific queues, define the minimum and maximum bandwidth per queue and the associated 802.1p (COS) priority.

GUI QoS Configuration Type



The "Share" parameter defines the available bandwidth per output queue. The sum of all individual Share values must be 100. If you add more bandwidth to a specific queue the requested bandwidth is deducted from the "Best_Effort" traffic class. The "Best_Effort" Share is therefore not changeable because it automatically receives the remaining unallocated bandwidth.

GUI QoS bandwidth share

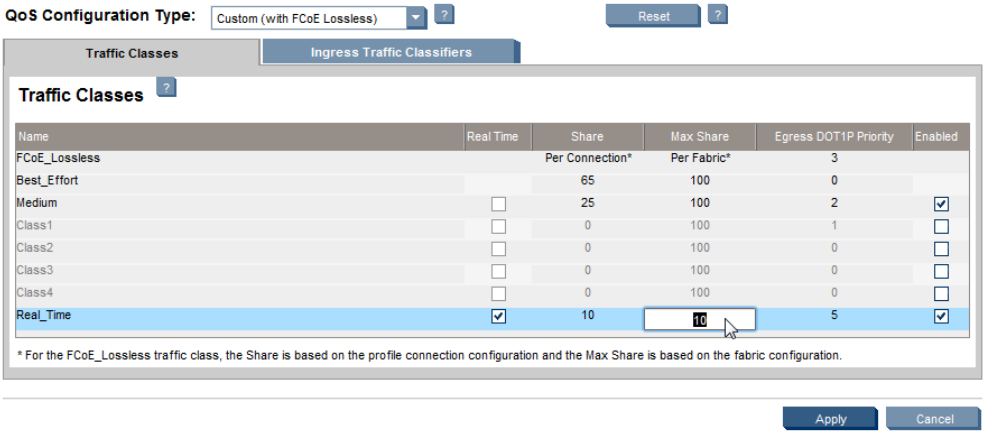


Note: For the "FCoE_Lossless" traffic class the "Share" is based on the FCoE HBA configuration inside a server profile and must also be considered.

Note: The "Share" parameter cannot be zero for enabled traffic classes.

With the "Max Share" parameter you can specify the maximum bandwidth per traffic queue. By default all vales are configured to 100 which means that 100% of the uplink or server-link bandwidth could be used when other queues do not consume there guaranteed bandwidth.

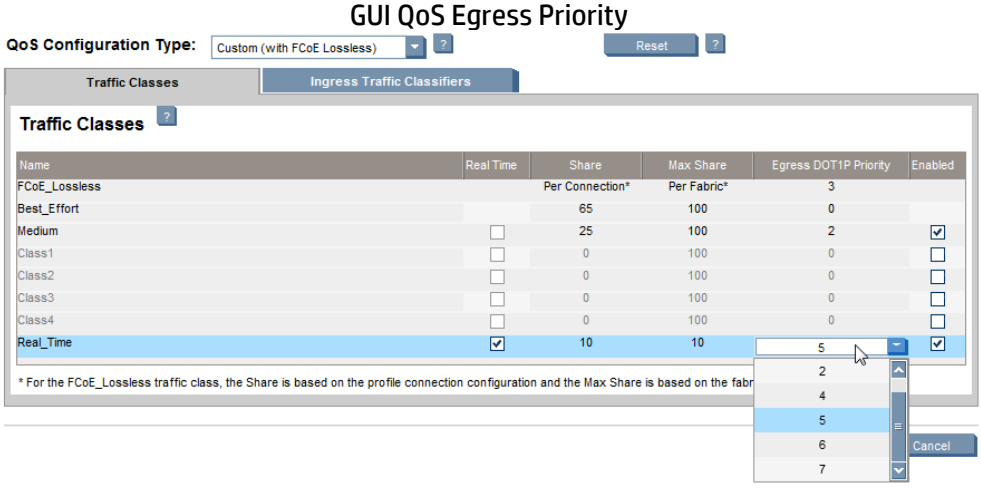
GUI QoS bandwidth Max Share



Note: Max Share must be >= Share

Each individual Traffic class has an associated 802.1p (COS) priority. If some 802.1p values (0-7) are not assigned to a specific traffic class, the traffic class gets processed by the "Best_Effort" class. All other Traffic Classes can only be used by one 802.1p priority.

GUI QoS Egress Priority

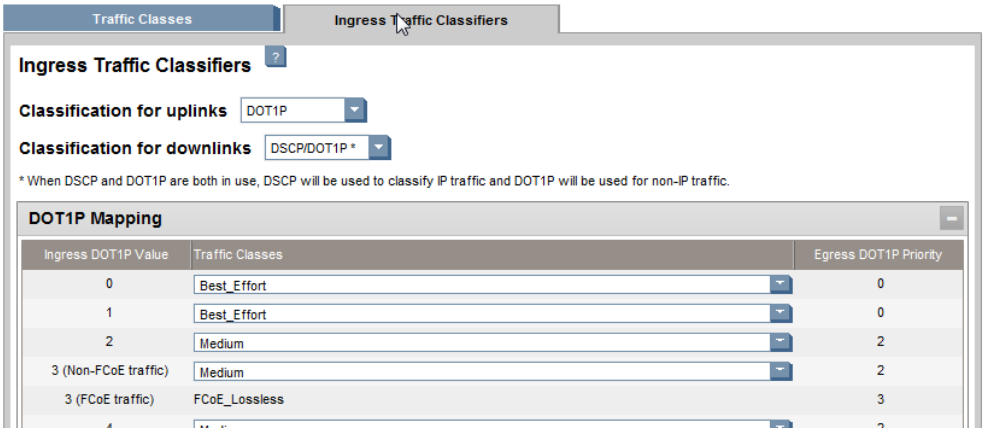


Note: Please make sure that if you use FCoE on uplinks, the FCoE traffic from the upstream device is already marked with an 802.1p value of 3 when it reaches the VC module as you cannot change this setting in Virtual Connect.

Exercise 2 - Configuring the QoS Ingress Traffic Classifier

In this section you can define what QoS marking will be trusted when packets are received and how the 802.1p and DSCP mapping is handled.

GUI QoS Ingress Traffic Classifier

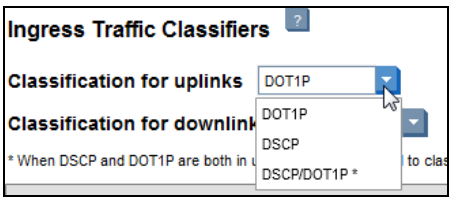


You must first you specify what priority values you trust when packets are received from the up- or downlinks (server-links).

You have the choice to select between:

- 802.1p (COS value inside the Layer2 VLAN tag)
- DSCP (Differentiated services code point inside a Layer 3 IPv4 header)
- DSCP/802.1p (When DSCP and DOT1P are both in use, DSCP will be used to classify IP traffic and DOT1P will be used for non-IP traffic)

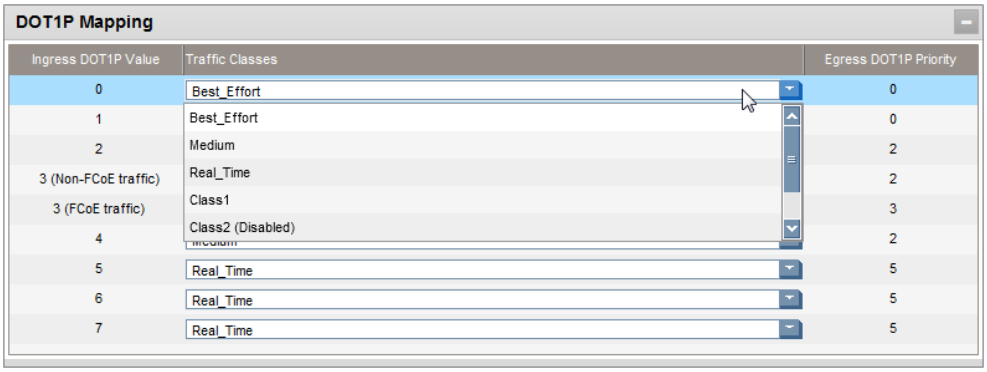
GUI QoS bandwidth max share



Exercise 3 - Configuring the QoS Ingress Traffic Mappings

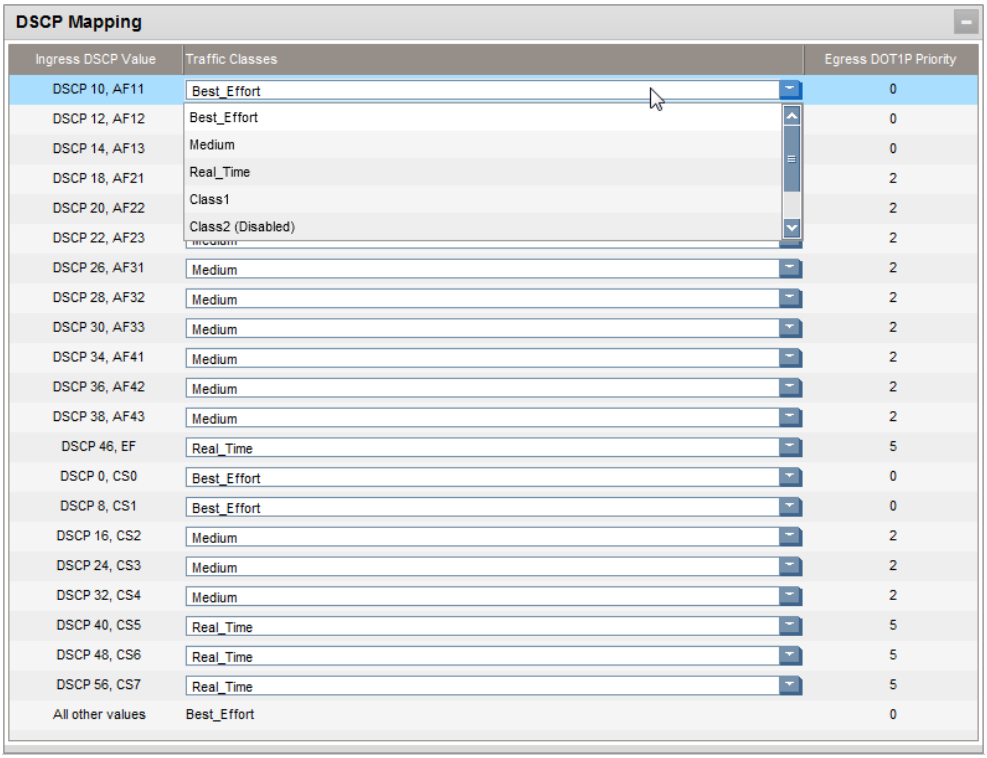
You can overwrite the egress 802.1q field based on the ingress 802.1p or DSCP values. In the next two screenshots you can see how to map the marked ingress traffic to a specific VC Traffic Class. The system will then automatically apply the corresponding egress 802.1p value to this traffic.

GUI QoS 802.1p mapping



Note: Non FCoE traffic with an 802.1p value of 3 is enforced to use a different value. This is done to protect FCoE against other traffic.

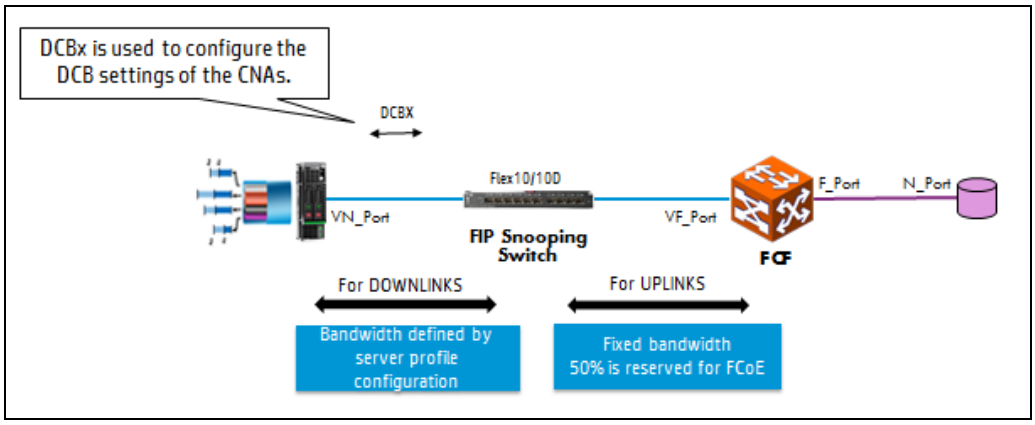
GUI QoS DHCP mapping



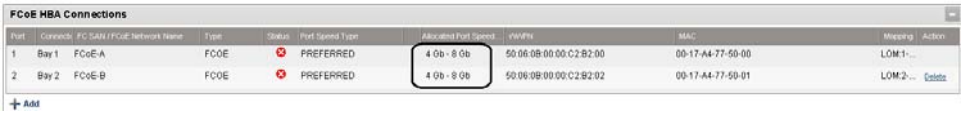
Configuring the FCoE Network Bandwidth via GUI

For FCoE enabled uplink the "FCoE_Lossless" Traffic Class has a fixed configured value of 50% bandwidth share and max = 100% assigned.

FCoE bandwidth overview



FCoE bandwidth overview, as configured within the server profile.



Note: the fabrics are showing as RED/error state as the upstream switch has not been configured to support FCoE/SAN connections, once the switch is configured then sate of the fabrics will be green.

Summary

In this lab you changed from the default Virtual Connect QoS configuration to QoS with Lossless FCoE. You then proceeded to configure the various queue settings within Virtual Connect.

Appendices – CLI Commands

Configuring the QoS Config Type via CLI

The following command can be copied and pasted into an SSH based CLI session with Virtual Connect:

```
# Set QoS Config Type to Passthrough
set qos Passthrough
```

or

```
# Set QoS Config Type to Custom with FCoE Lossless class
set qos CustomWithFCoE
```

or

```
# Set QoS Config Type to Custom no FCoE Lossless class
set qos CustomNoFCoE
```

Configuring the QoS Traffic Class via CLI

```
# Set QoS Config Traffic classes
set qos-class Medium Enabled=true RealTime=false Share=25 EgressDOT1P=2 MaxShare=100
set qos-class Real_Time Enabled=true RealTime=true Share=10 EgressDOT1P=5 MaxShare=10
set qos-class Class1 Enabled=false RealTime=false MaxShare=100
set qos-class Class2 Enabled=false RealTime=false MaxShare=100
set qos-class Class3 Enabled=false RealTime=false MaxShare=100
set qos-class Class4 Enabled=false RealTime=false MaxShare=100
set qos-class Best_Effort MaxShare=100
```

Configuring the QoS Ingress Traffic Classifier via CLI

```
# Set QoS Ingress Traffic Classifier
set qos-classifier Downlinks Classifiers=DOT1P,DSCP
set qos-classifier Uplinks Classifiers=DOT1P
```

Configuring the QoS Ingress Traffic Mapping via CLI

```
# Set QoS Ingress Traffic Mapping
set qos-map DOT1P Class=Best_Effort Values="0-7"
set qos-map DOT1P Class=Best_Effort Values="0,1"
set qos-map DOT1P Class=Medium Values="2,3,4"
set qos-map DOT1P Class=Real_Time Values="5,6,7"

set qos-map DSCP Class=Best_Effort Values="AF11-CS7"
set qos-map DSCP Class=Best_Effort Values="AF11,AF12,AF13,CS0,CS1"
set qos-map DSCP Class=Medium
Values="AF21,AF22,AF23,AF31,AF32,AF33,AF41,AF42,AF43,CS2,CS3,CS4"
set qos-map DSCP Class=Real_Time Values="CS5,CS6,CS7,EF"
```

Implementing Direct Attached SAN Fabrics

Lab 6

Objectives

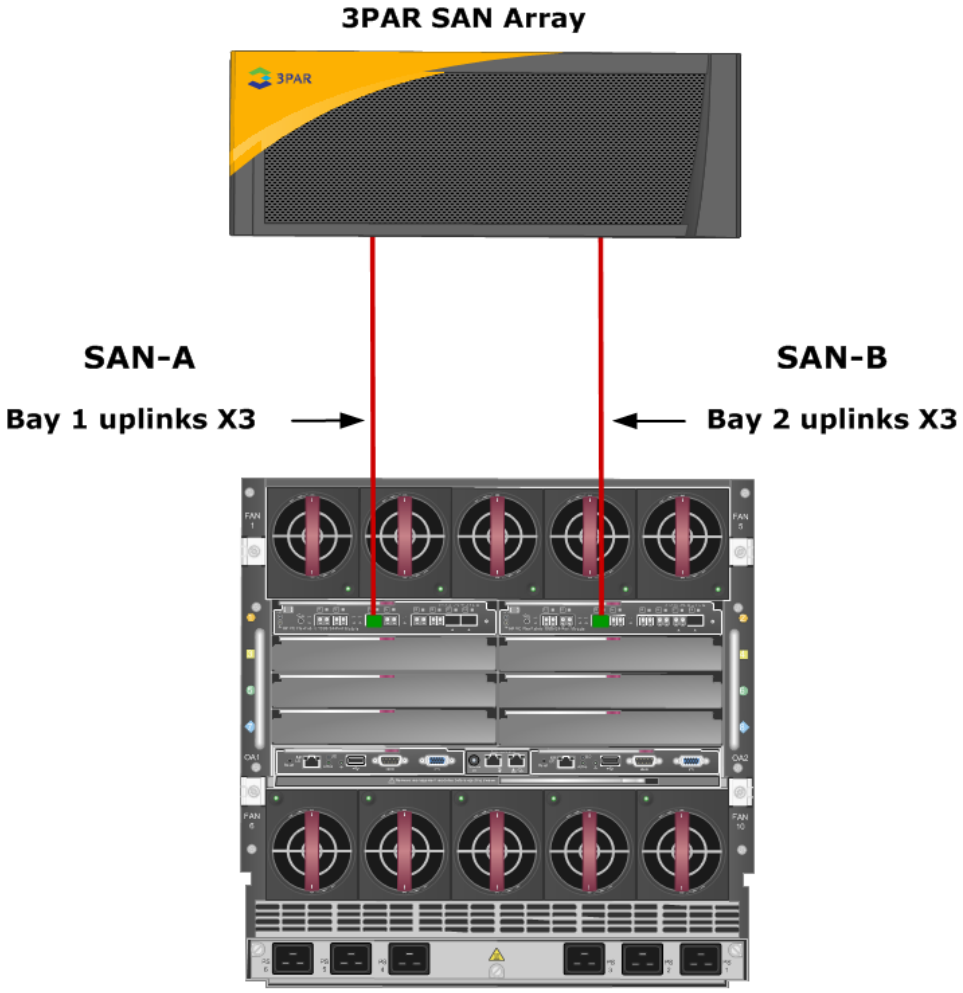
After completing this lab, you should be able to:

- Implement a redundant Virtual Connect (VC) SAN fabric configuration
- Examine the status of the VC FlexFabric modules and uplink ports connecting to the Fibre Channel switches

Introduction

In this lab, you will augment the basic VC Fibre Channel configuration you set up in the previous lab by implementing a second VC SAN fabric that will support redundant access to the SAN. This will enable you to see how you can create additional VC SAN fabrics for connectivity to other SAN islands.

Network diagrams



Physical view of the Fibre Channel connections without SAN Fabric

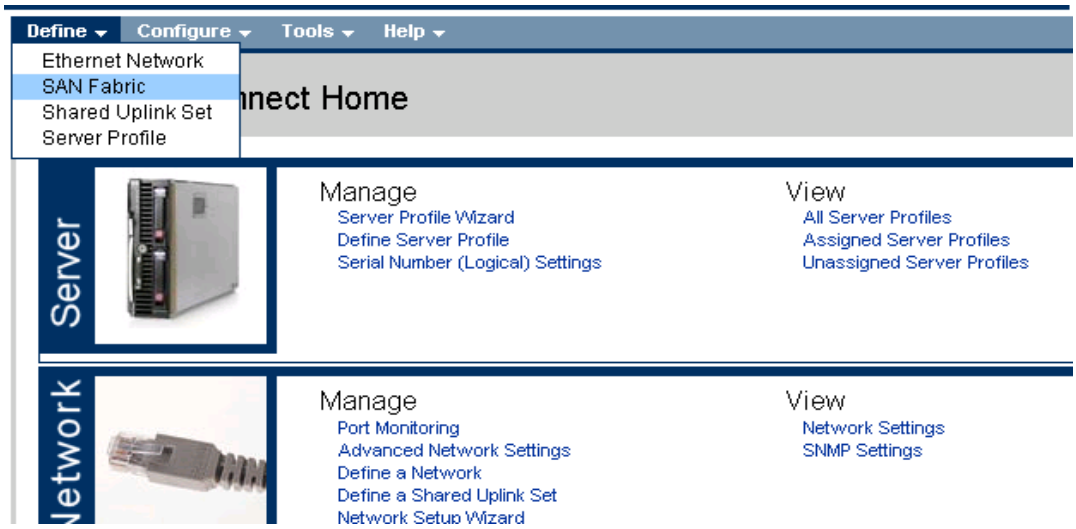
The Fibre Channel cables connecting your Virtual Connect FlexFabric modules to the upstream Fibre Channel switches might already be attached. Note that only Ports X1-X4 can be configured for connections other than Ethernet. Any necessary switch configuration tasks will have been completed before the beginning of class.

For this scenario, both VC FlexFabric modules are used and one uplink (port X3) from each module are connected directly to the 3PAR Fibre Channel SAN.

Exercise 1 — Defining Virtual Connect Direct Attached SAN fabrics

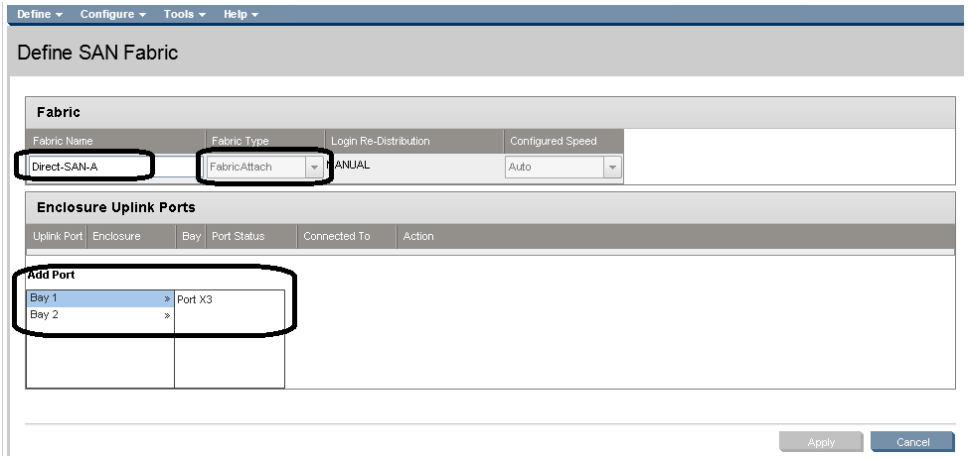
In this exercise, you will use Virtual Connect Manager to define a Virtual Connect direct Attached SAN connection to a 3PAR SAN. The VC SAN fabric is a configuration element that identifies one or more uplinks of a Virtual Connect Fibre Channel module used to connect to a SAN.

1. Open a web browser and access the Virtual Connect Manager home page.
2. From the Virtual Connect Manager home page, in the toolbar, select **Define** → **SAN Fabric**.

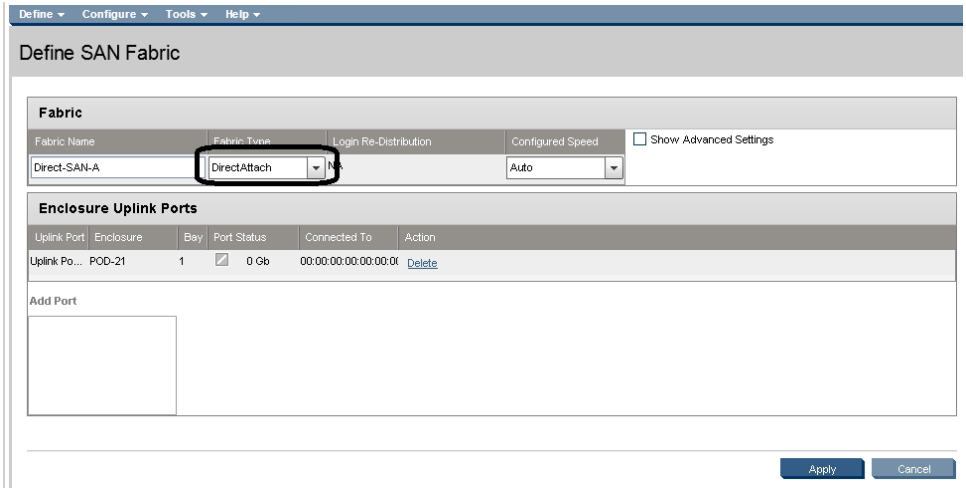


3. For the Fabric name, enter Direct-SAN_A. Add a single external uplink port by clicking **Add Port** → **Bay 1** → **Port X3**.

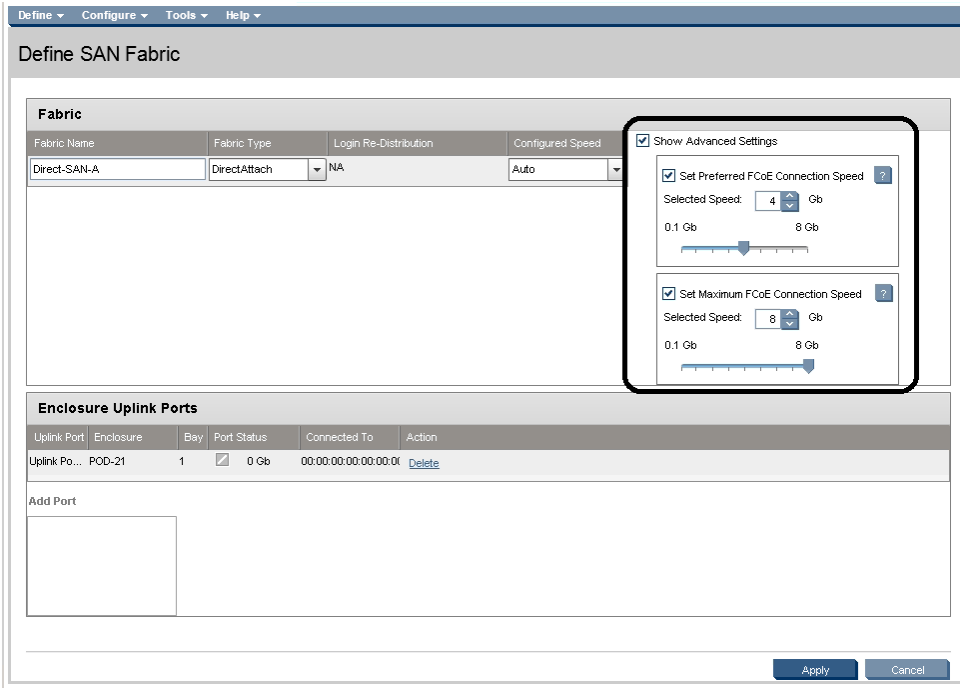
> **Note**
> This port is from the VC FlexFabric module in interconnect **Bay 1.**



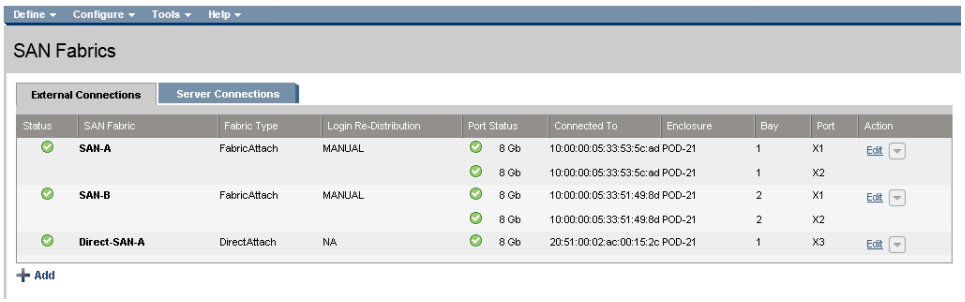
4. Before Clicking Apply, select DirectAttach in the Fabric Type Box.



5. Click the Show Advanced Settings box and configure the Preferred and Maximum bandwidth setts as shown, then **click apply.**



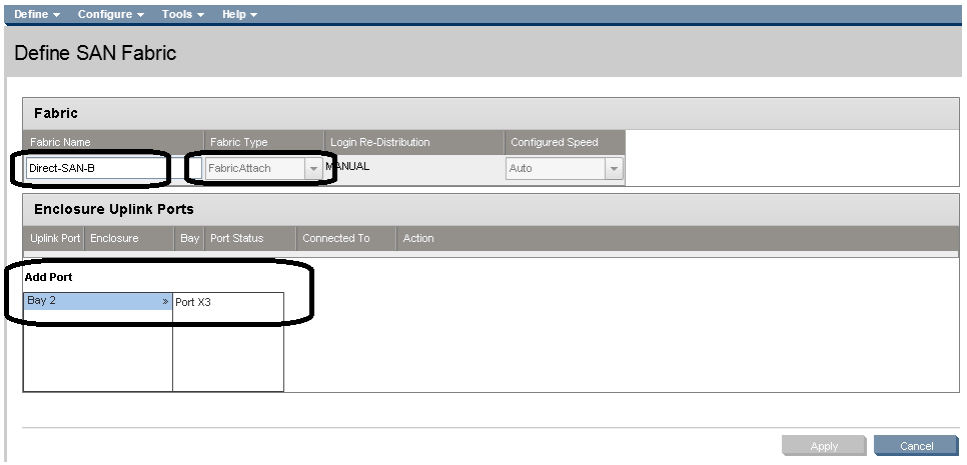
6. In the Define SAN Fabrics window, click the **Add** **link**. To define the second fabric.



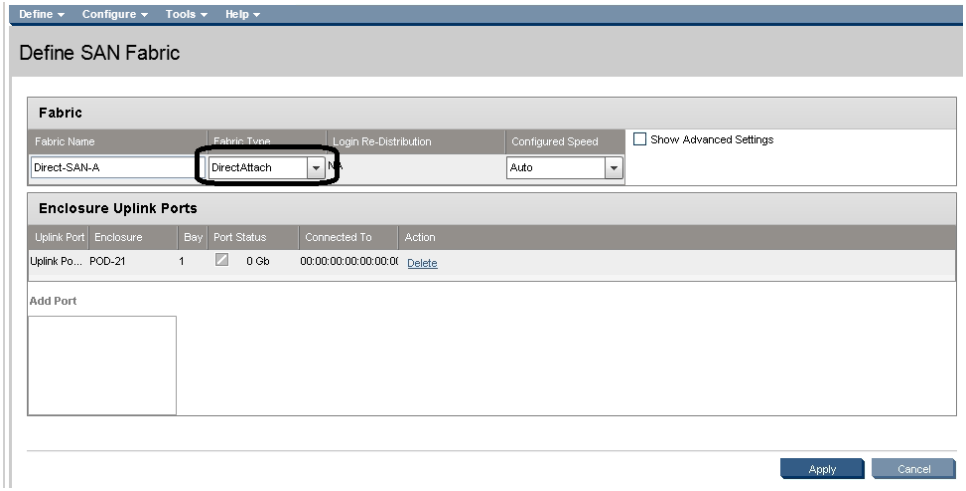
7. For the Fabric Name, enter Direct-SAN_B. Add a single external uplink port by clicking the Add Port window **Bay 2** → **Port X3**.

> **Note**
> This port is from the VC FlexFabric module in interconnect **Bay 2**.

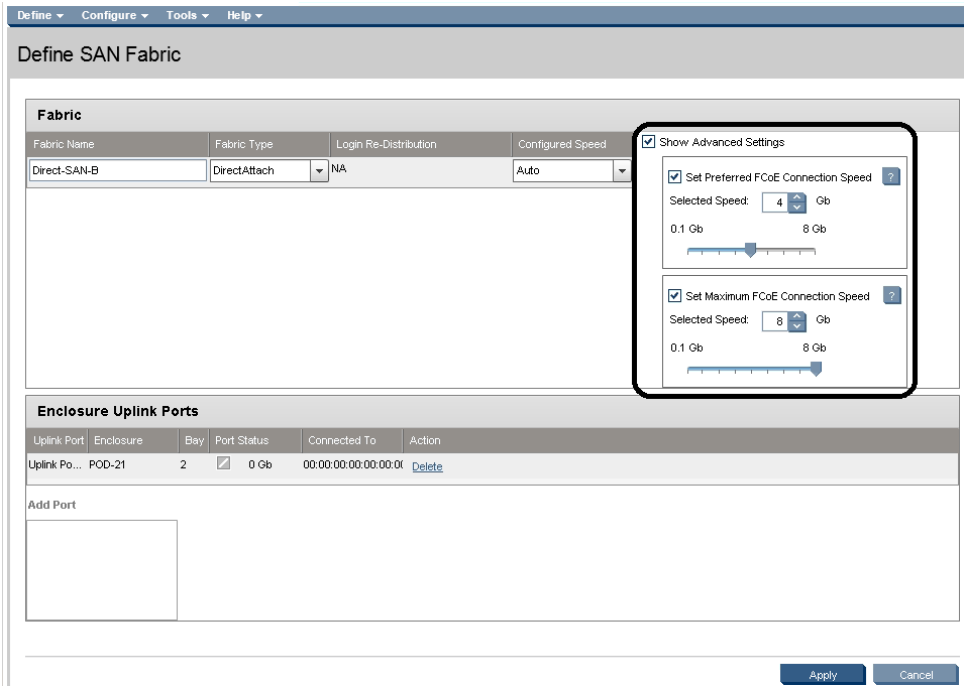
Click **Add** to save your changes.



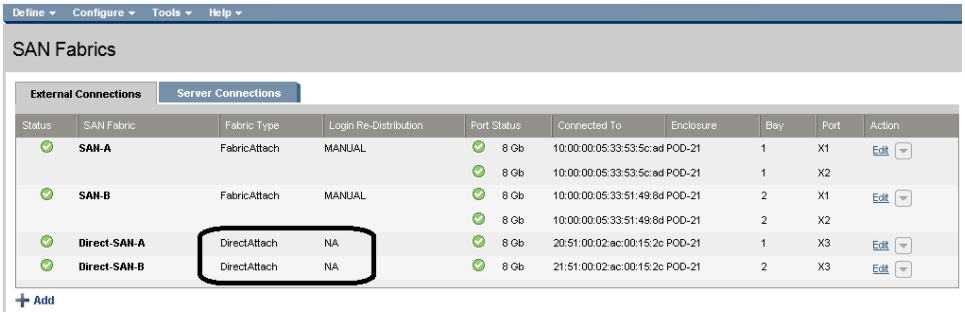
8. Before Clicking Apply, select DirectAttach in the Fabric Type Box.



9. Click the Show Advanced Settings box and configure the Preferred and Maximum bandwidth setts as shown, then **click apply.**

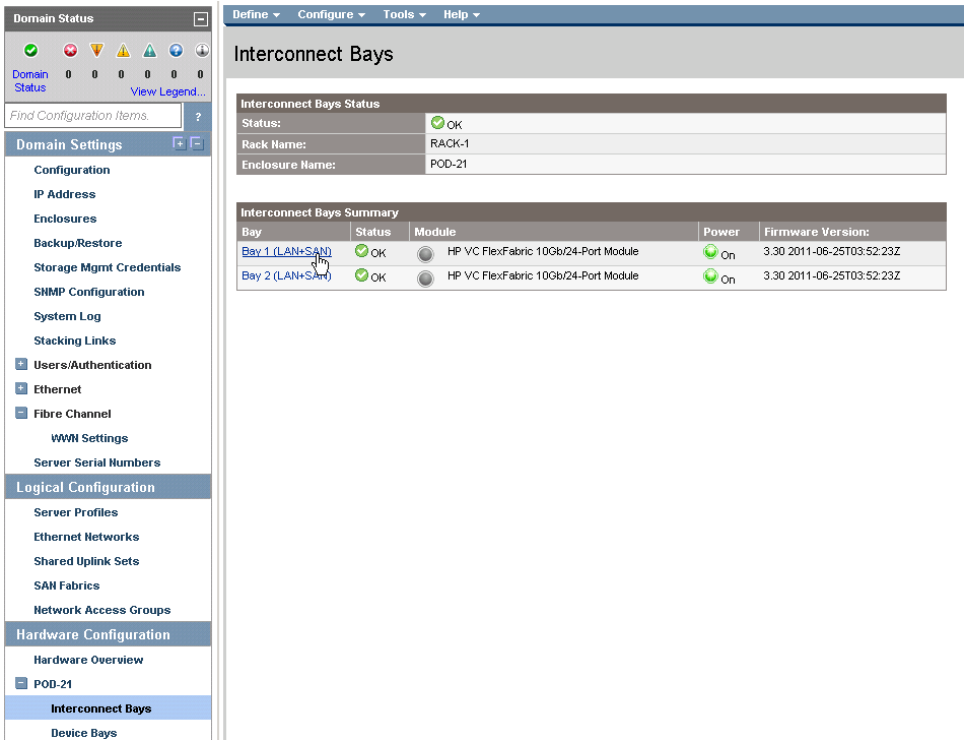


10. Confirm both the new DirectAttach SAN Fabrics have been created and are connected.

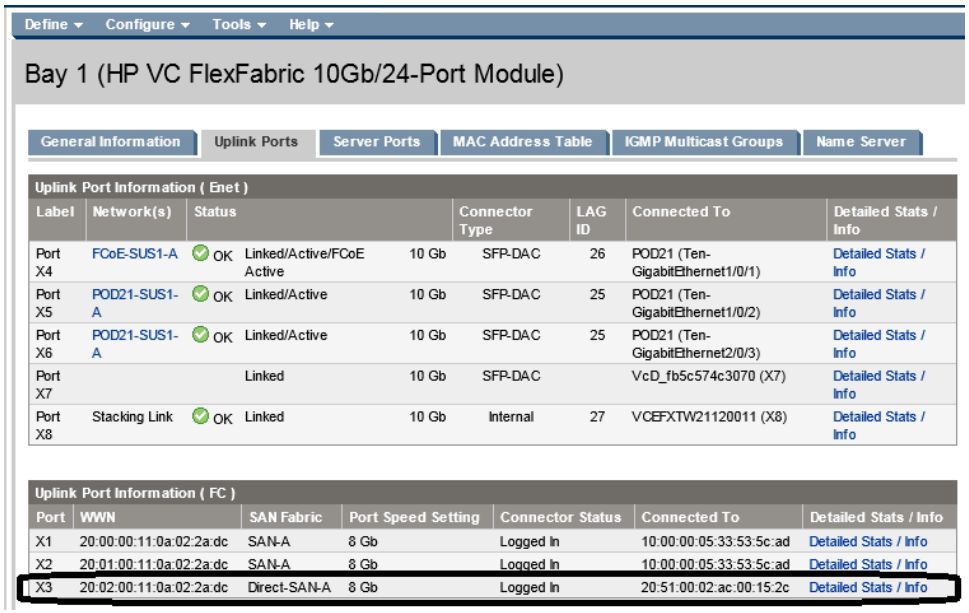


Exercise 2 — Examining the status of the VC FlexFabricl module and uplink ports

1. In the Hardware Configuration section of the navigation pane, expand **<enclosure-name> > Interconnect Bays**. Then click the link for **Bay 1**.



2. From the Uplink Ports tab, Examine the status of the FlexFabric interconnect module. Scroll down to the Uplink Information (FC) section to view the status of uplink port X3 of this VC FlexFabric module.

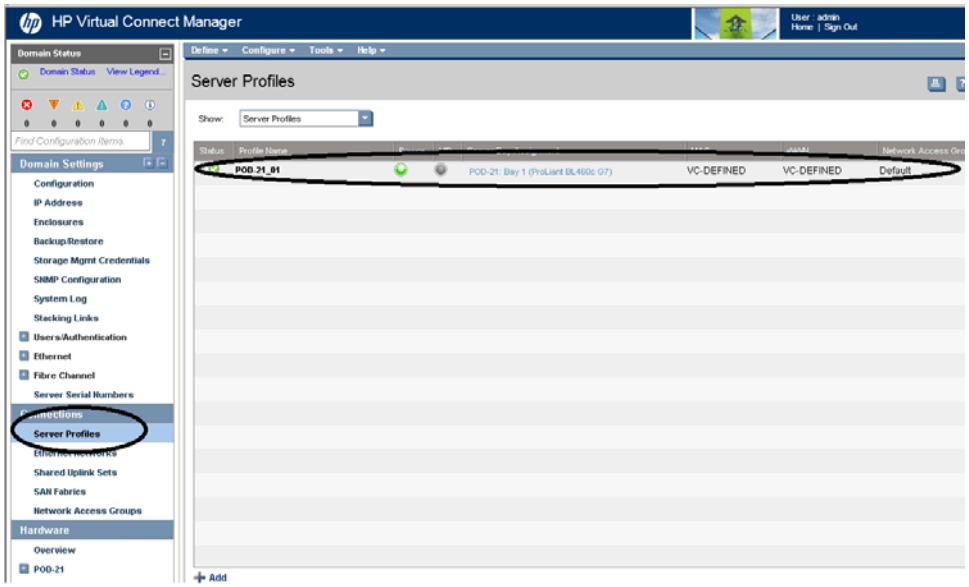


Notice the WWN that is assigned to each uplink port of the Fibre Channel module port, which is listed in the WWN column. The WWN of the upstream Fibre Channel switch is listed in the Connected To column for the Fabric Attached Fabrics and the controller port address of the 3PAR is shown for the Direct Attached fabric.

Exercise 3 – Modifying a Server Profiles to Connect to the SAN

In this exercise, you use the Virtual Connect Manager (VCM) to modify the server profile created in lab 1. When modifying a server profile on a VC Ethernet module that will be used with a server supporting FlexFabric ports (or NICs), you have the option of allocating bandwidth across one to four NICs, or one to three NICs and a FC HBA. In this exercise, you will edit the existing profile and ADD SAN connections, and then configure those connections for Boot to SAN.

1. Open a web browser and access the OA for your POD, verify the servers in Bays 1 and 2 are shutdown.
2. Open a web browser and access the Virtual Connect Manager home page and log in using the admin account created in lab 1.
3. In the left tree view, under connections, click on server profiles.
4. Your profile should be shown in the right pane, select the profile and edit it.

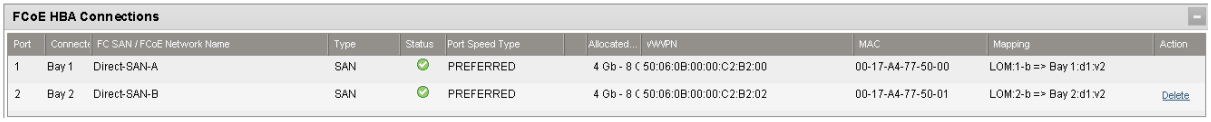


5. From the Edit Server profile page, under FCoE HBA Connections, for Bay 1 select SAN-A and for Bay 2 select SAN-B. The speed should default to 4Gb Min. and 8Gb Max.

Port	Bay	FC SAN Name
1	1	Direct-SAN-A
1	2	Direct-SAN-B

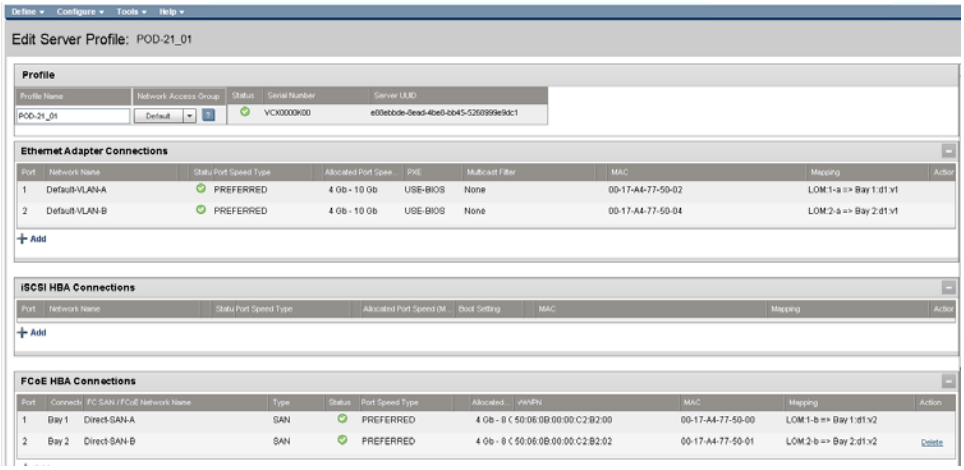
6. In the FCoE HBA Connections section, assign the information listed in the following table.

Note: For the blade server you are working with, Port 1 corresponds to FlexNIC 3 (LOM:1-b) and Port 2 corresponds to FlexNIC 4 (LOM:2-b).



7. In the Assign Profile to Server Bay section, click the down arrow and then click PODnn > Bay 1 (ProLiant 460c Gen7).

8. Then click Apply to save the changes to the server profile.



9. Examine the Mapping column for the Ethernet and FCoE connections.

   Notice that LOM:1-a and LOM:2-a are mapped to the two Ethernet FlexNICs, and LOM:1-b and LOM:2-b are mapped to the two FCoE FlexHBAs.

   Also, notice the Allocated Port Speed column for the FlexNICs and FlexHBAs now shows a Preferred or Min. speed and a Maximum speed. The FlexHBA connections have an initial bandwidth allocation of 4 Gb and can burst to 8Gb. The NIC is configured for 4Gb and could burst to 10Gb.

10. Click Cancel to close the Server Profile window.

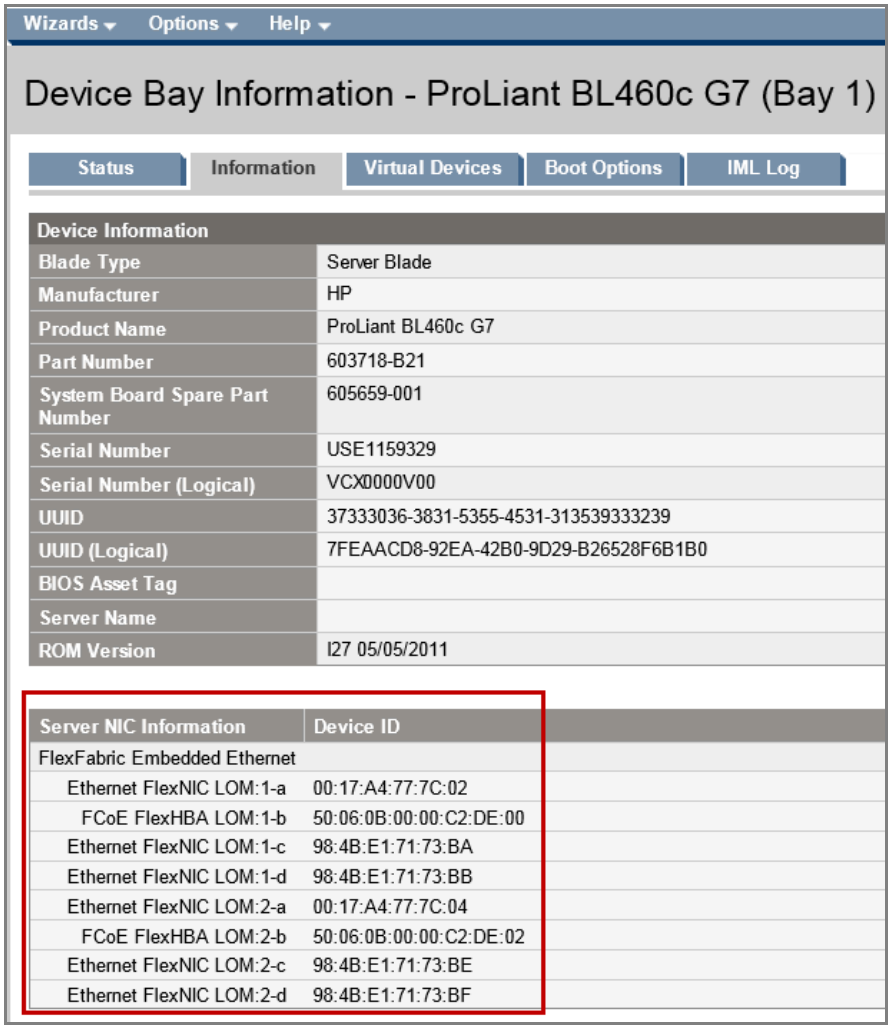
Exercise 4 - Power-on the Server and Verify SAN Connectivity

In this task, you use the Onboard Administrator (OA) management interface to examine the status of the server in bay 1. You then power on the server to cause the server profile to be activated. You also examine the IP addresses assigned to the FlexNICs through DHCP.

1. Go to the browser window you have for the OA.

2. In the navigation pane, click Enclosure Information > Device Bays > 1 to view the status of the server blade in Device Bay 1.

3. Click the Information tab.

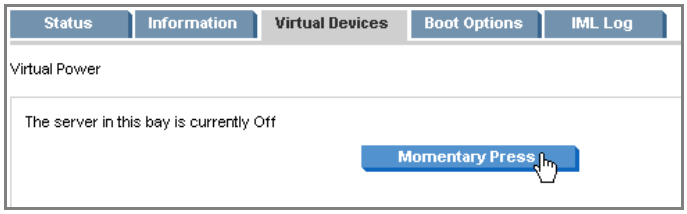


4. Examine the server NIC information.

   Notice that all 8 connections are represented here, 6 FlexNICs and 2 FlexHBAs. The other 4 FlexNICs that you did not explicitly configure are presented to the

blade server Operating System. These additional 4 LAN Connections that would appear in Windows, or vmnics in VMware ESXI, can be ignored.

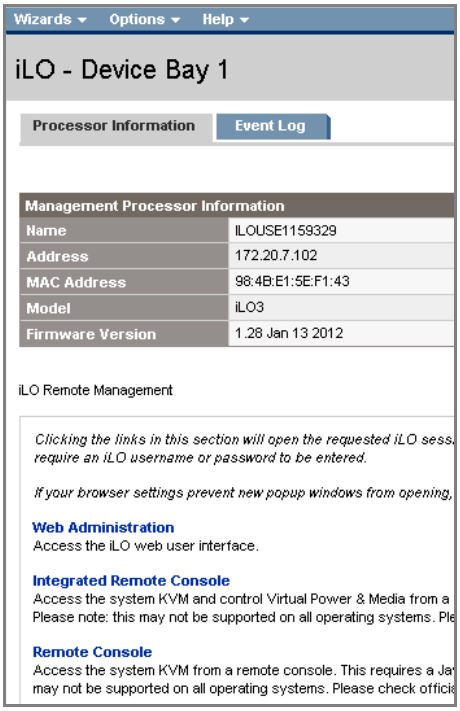
5. Click the Virtual Devices tab. At this point, the server is powered off, which allowed you to assign the server profile previously.



6. Click Momentary Press to power on the server.

   You can also access the Virtual Power feature through the Virtual Connect Manager interface, but going through the OA also gives you easy access to the Remote Console functionality of the HP integrated Lights-Out (iLO).

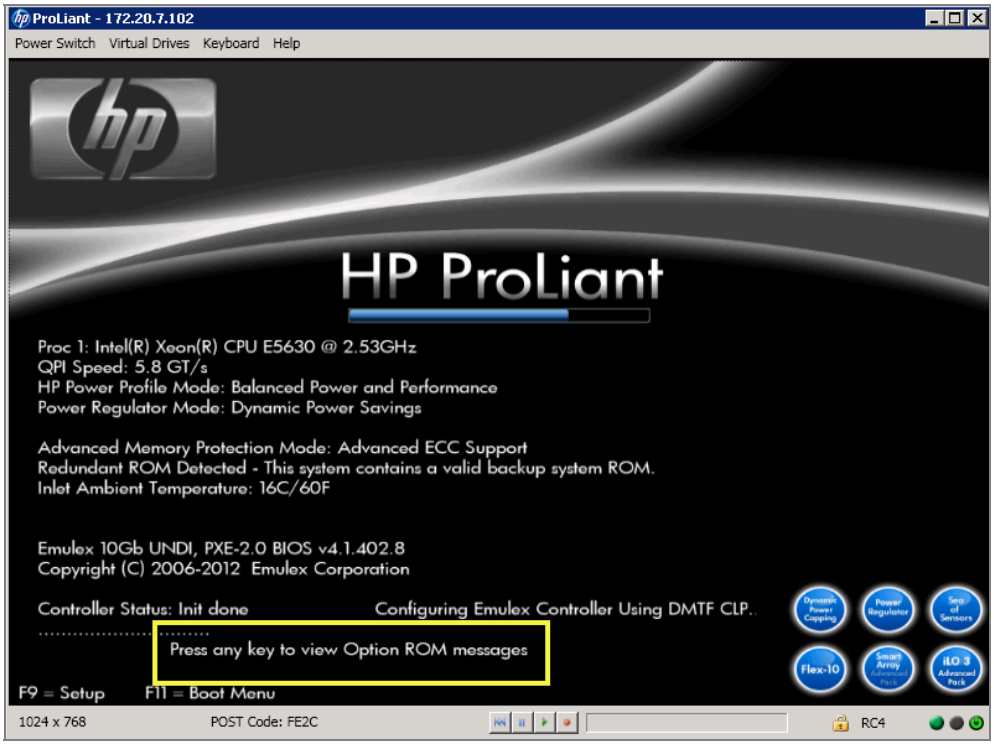
7. To access the Windows Server console, in the navigation pane of the OA, click iLO under the folder entry for Device Bay 1.



8. In the iLO Device Bay window, perform one of the following actions.

   1) If you are using Internet Explorer, click **Integrated Remote Cons**ole.

   2) If you are using Firefox, click **Remote Console**.

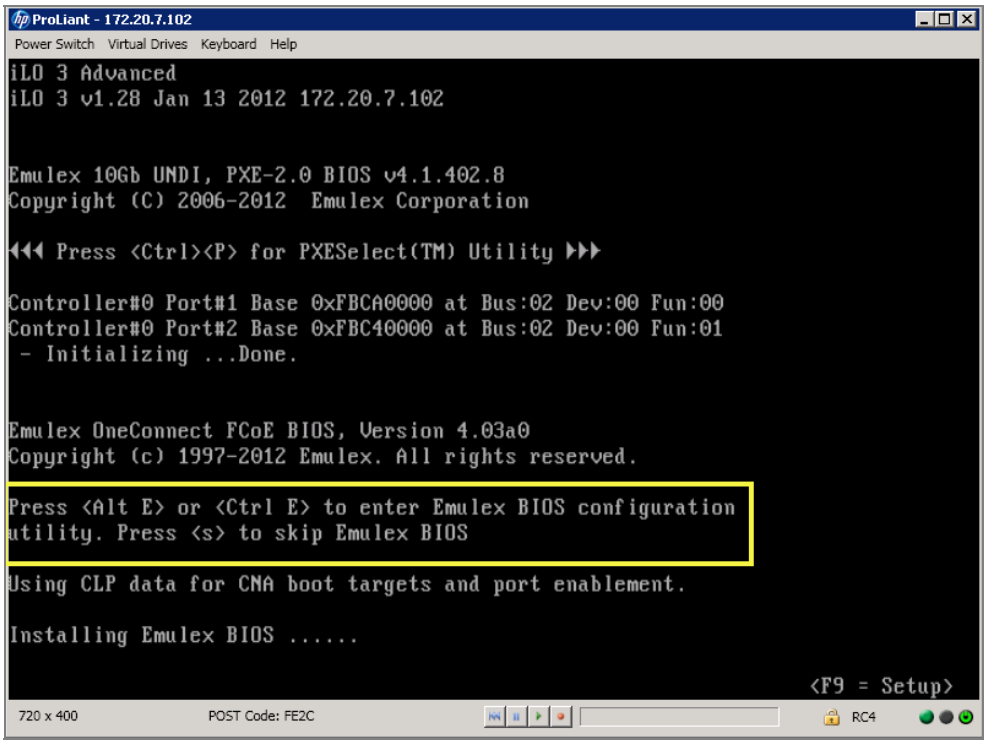


To verify the Emulex BIOS configuration was modified by the Server Profile you examine the settings applied to the adapters by Virtual Connect. During the POST processing stage, you will see a prompt to "Press any key to see POST Messages."

Note: It is important to watch for the message and respond or you will have to go through the boot process again.

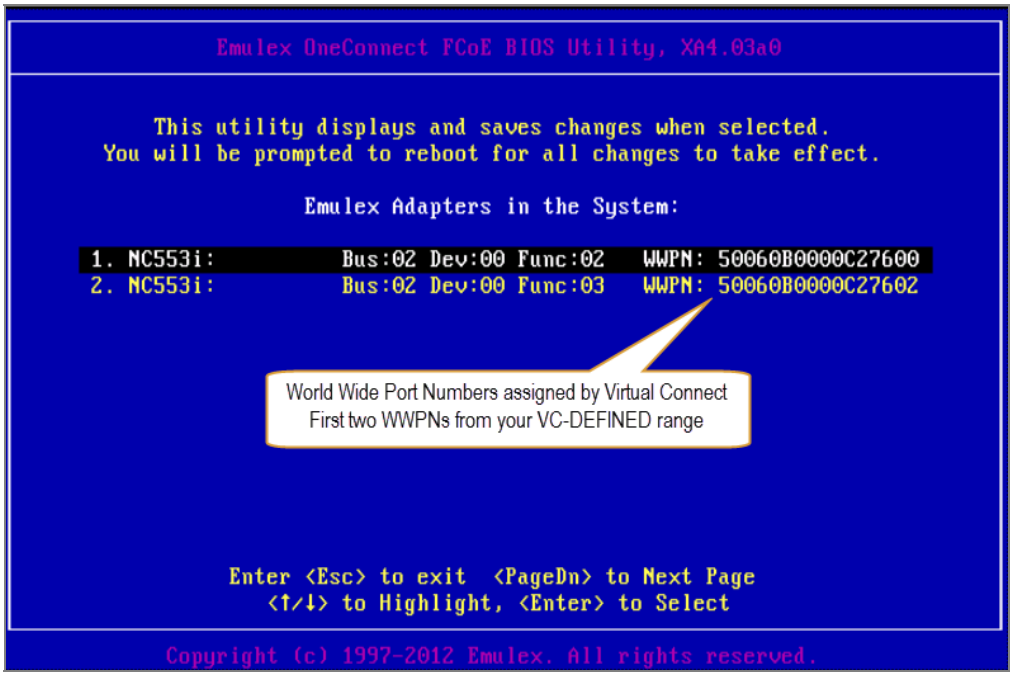
---

9. Press the <Space> bar or any other key to view the Option ROM messages.

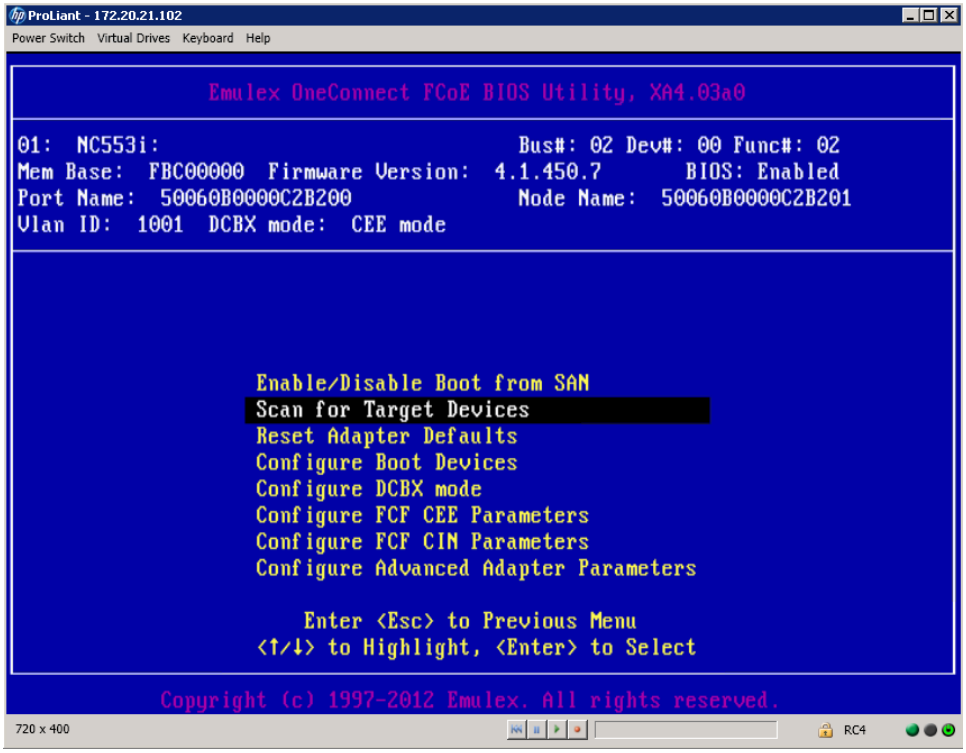


10. Watch for the Emulex OneConnect FCoE BIOS messages.

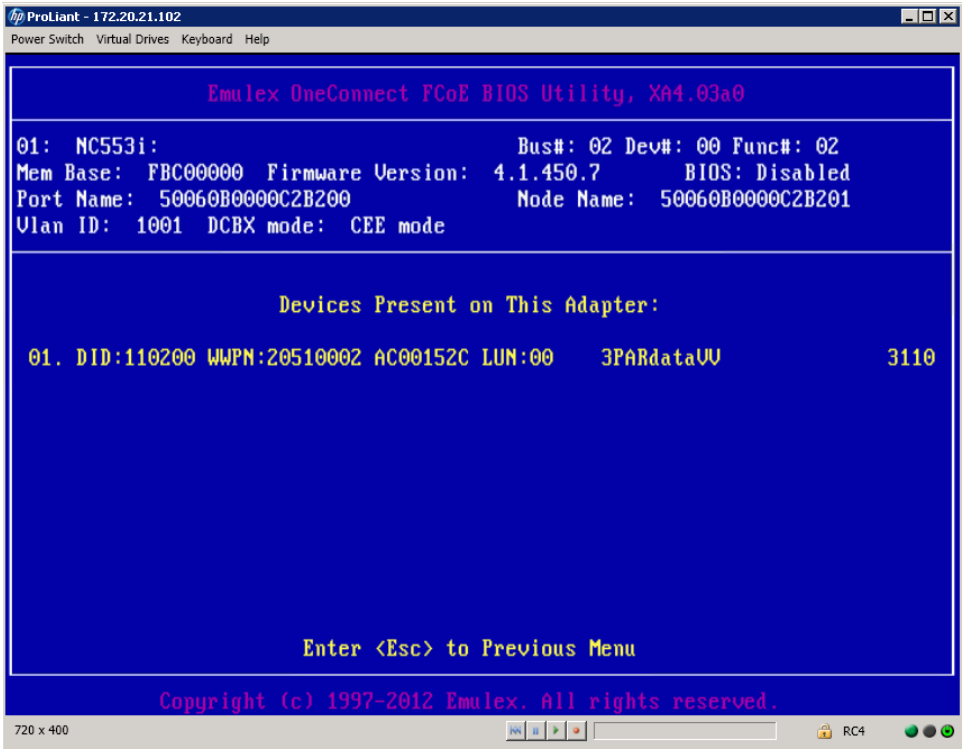
11. Press <Alt>-e or <Ctrl>-e as instructed on the screen to access the Emulex BIOS configuration utility.



12. Highlight the top adapter using the keyboard arrow keys and press <Enter> to view its configuration.

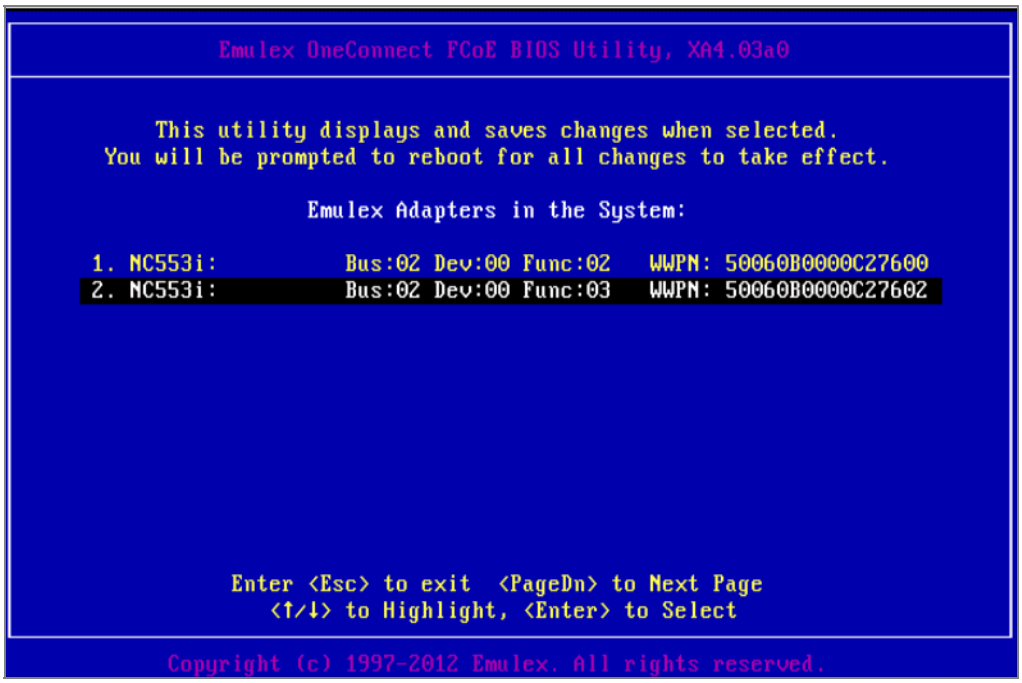


13. Arrow down to Configure Boot Devices and press <Enter> to view its configuration.

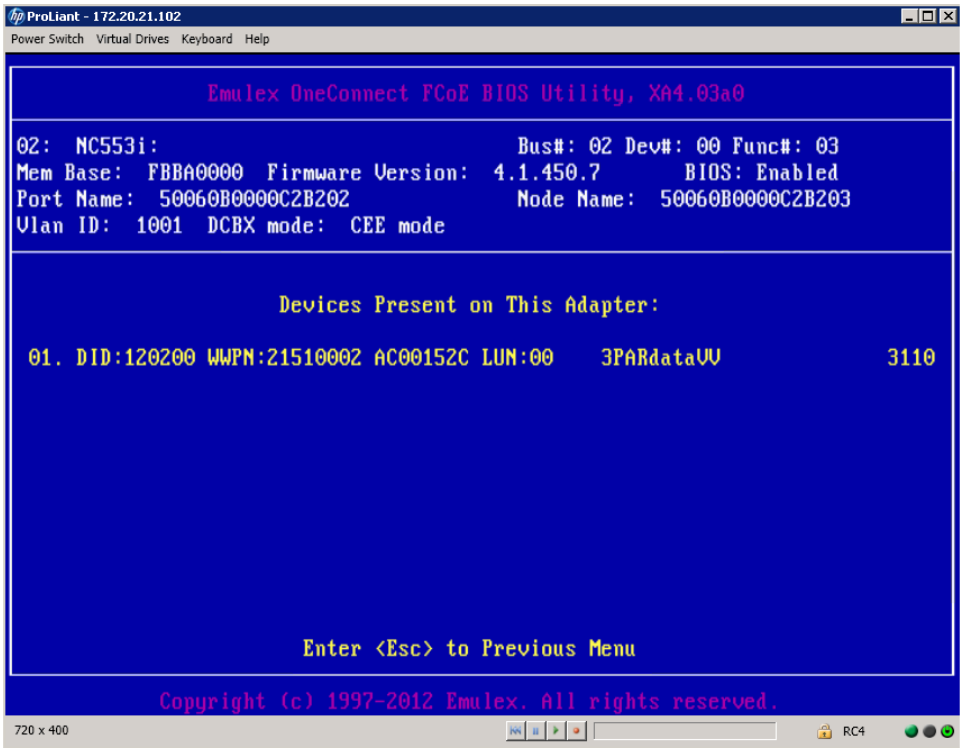


14. Compare the WWPN displayed with the value you entered for Port 1 when you configured the Boot from SAN settings in the server profile.

15. Press <Esc> twice to return to the Emulex Adapters in the System menu.

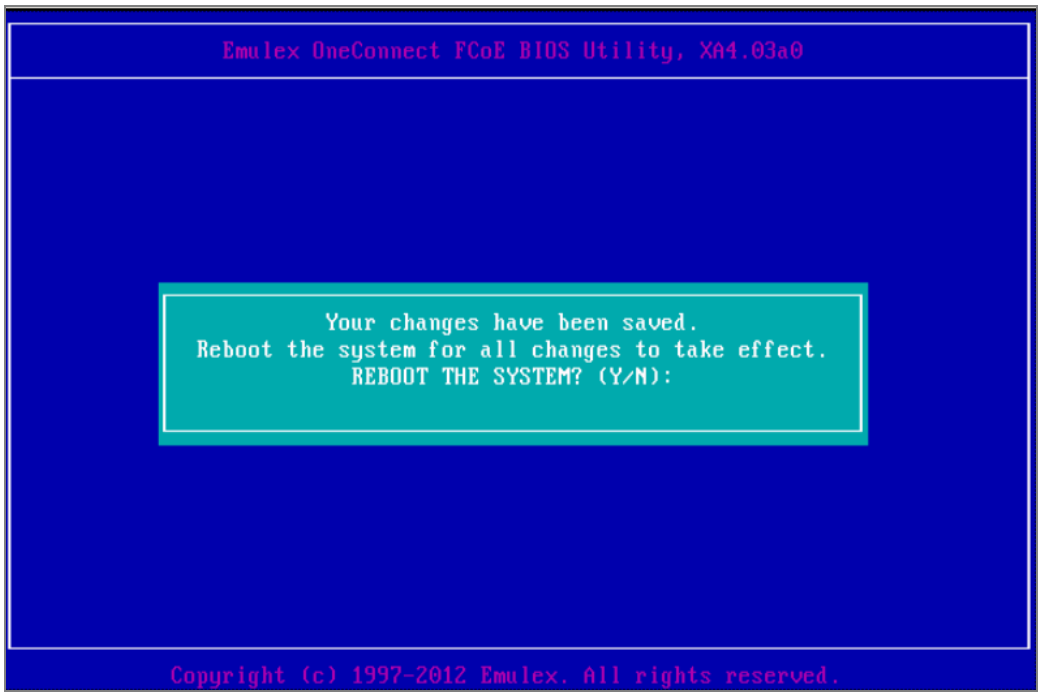


16. Use the arrow keys to choose the second adapter and repeat the previous steps to view the WWPN of its target controller.



17. Compare the WWPN displayed with the value you entered for Port 2 when you configured the Boot from SAN settings in the server profile.

18. Press <Esc> three times to display the reboot prompt.



19. Then type "Y" to reboot the system.

20. Go back to the OA and shut the server down.

Summary

During this lab, you defined a pair of Direct Attached Virtual Connect SAN fabrics to a 3PAR array. You were able to connect to that array through the HBA in the server and see the controllers on the fabric. The next step could be to configure Boot to SAN and install an OS, or simply connect to and mount a LUN from a locally installed OS.