LAN Connectivity

Fabric Interconnect Overview

The fabric interconnect is the core component of Cisco UCS. The Cisco UCS Fabric Interconnects provide uplink access to LAN, SAN, and out-of-band management segment. Cisco UCS infrastructure management is through the embedded management software, Cisco UCS Manager, for both hardware and software management. The Cisco UCS Fabric Interconnects are Top-of-Rack devices, and provide unified access to the Cisco UCS domain.

The Cisco UCS FIs provide network connectivity and management for the connected servers. The Cisco UCS Fabric Interconnects run the Cisco UCS Manager control software and consist of expansion modules for the Cisco UCS Manager software.

For more information about Cisco UCS Fabric Interconnects, see the *Cisco UCS Manager Getting Started Guide*.

Uplink Connectivity

Use fabric interconnect ports configured as uplink ports to connect to uplink upstream network switches. Connect these uplink ports to upstream switch ports as individual links, or as links configured as port channels. Port channel configurations provide bandwidth aggregation as well as link redundancy.

You can achieve northbound connectivity from the fabric interconnect through a standard uplink, a port channel, or a virtual port channel configuration. The port channel name and ID configured on fabric interconnect should match the name and ID configuration on the upstream Ethernet switch.

It is also possible to configure a port channel as a vPC, where port channel uplink ports from a fabric interconnect are connected to different upstream switches. After all uplink ports are configured, create a port channel for these ports.

Downlink Connectivity

Each fabric interconnect is connected to IOMs in the UCS chassis, which provides connectivity to each blade server. Internal connectivity from blade servers to IOMs is transparently provided by Cisco UCS Manager using 10BASE-KR Ethernet standard for backplane implementations, and no additional configuration is required. You must configure the connectivity between the fabric interconnect server ports and IOMs. Each IOM, when connected with the fabric interconnect server port, behaves as a line card to fabric interconnect, hence IOMs should never be cross-connected to the fabric interconnect. Each IOM is connected directly to a single fabric interconnect.

The Fabric Extender (also referred to as the IOM, or FEX) logically extends the fabric interconnects to the blade server. The best analogy is to think of it as a remote line card that's embedded in the blade server chassis, allowing connectivity to the external world. IOM settings are pushed via Cisco UCS Manager and are not managed directly. The primary functions of this module are to facilitate blade server I/O connectivity (internal and external), multiplex all I/O traffic up to the fabric interconnects, and help monitor and manage the Cisco UCS infrastructure.

Configure Fabric interconnect ports that should be connected to downlink IOM cards as server ports. Make sure there is physical connectivity between the fabric interconnect and IOMs. You must also configure the IOM ports and the global chassis discovery policy.

Note For UCS 2200 I/O modules, you can also select the Port Channel option and all I/O module-connected server ports will be automatically added to a port channel.

Configuring the Fabric Interconnects

Fabric Interconnect Information Policy

Fabric Interconnect Information Policy enables you to display the uplink switches that are connected to fabric interconnect.

Important You must enable the information policy on the fabric interconnect to view the details of SAN, LAN, and LLDP neighbours of the fabric interconnect.

Configuring the Information Policy on the Fabric Interconnect

Procedure

Step 1 Navigate to **Equipment** > **Policies** > **Global Policies**

Step 2 In the **Info Policy** group, choose one of the following:

- **Disabled**: Click to disable the information policy on the fabric interconnect. This is the default option.
- **Enabled**: Click to enable the information policy on the fabric interconnect.

Step 3 Click **Save Changes**.

Installing Secure FPGA

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Expand **Equipment** > **Fabric Interconnects** > ***Fabric_Interconnect_Name***.

Step 3 In the **Work** pane, click the **General** tab.

Step 4 In the **Actions** area of the **General** tab, click **Install Secure FPGA**.

Step 5 In the dialog box, click **OK**.

Warning This procedure will upgrade the FPGA and automatically reboot the system after completion of the FPGA upgrade. Kindly refrain from reloading or power-cycling the system during the upgrade, as the manual reboot will result in failure of Fabric Interconnect.

Cisco UCS Manager restarts the fabric interconnect, logs you out, and disconnects Cisco UCS Manager GUI on choosing **Yes** in the warning message.

Viewing the LAN Neighbors of a Fabric Interconnect

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 In the **Equipment** tab, expand **Equipment** > **Fabric Interconnects**.

Step 3 Click the fabric interconnect for which you want to view the LAN neighbors.

Step 4 In the **Work** pane, click the **Neighbors** tab.

Step 5 Click the **LAN** subtab.

This subtab lists all the LAN neighbors of the specified Fabric Interconnect.

Viewing the SAN Neighbors of a Fabric Interconnect

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 In the **Equipment** tab, expand **Equipment** > **Fabric Interconnects**.

Step 3 Click the fabric interconnect for which you want to view the SAN neighbors.

Step 4 In the **Work** pane, click the **Neighbors** tab.

Step 5 Click the **SAN** subtab.

This subtab lists all the SAN neighbors of the specified Fabric Interconnect.

Viewing the LLDP Neighbors of a Fabric Interconnect

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Expand **Equipment** > **Fabric Interconnects**.

Step 3 Click the fabric interconnect for which you want to view the LLDP neighbors.

Step 4 In the **Work** pane, click the **Neighbors** tab.

Step 5 Click the **LLDP** subtab.

This subtab lists all the LLDP neighbors of the specified Fabric Interconnect.

Fabric Evacuation

Cisco UCS Manager introduces fabric evacuation, which is the ability to evacuate all traffic that flows through a fabric interconnect from all servers attached to it through an IOM or FEX while upgrading a system. Fabric evacuation is not supported on direct-attached rack servers.

Upgrading the secondary fabric interconnect in a system disrupts active traffic on the fabric interconnect. This traffic fails over to the primary fabric interconnect. You can use fabric evacuation during the upgrade process as follows:

1. Stop all the traffic that is active through a fabric interconnect.

2. For vNICs configured with failover, verify that the traffic has failed over by using Cisco UCS Manager, or tools such as vCenter.
3. Upgrade the secondary fabric interconnect.
4. Restart all the stopped traffic flows.
5. Change the cluster lead to the secondary fabric interconnect.
6. Repeat steps 1 to 4 and upgrade the primary fabric interconnect.

Note

- Fabric interconnect traffic evacuation is supported only in a cluster configuration.
- You can evacuate traffic only from the subordinate fabric interconnect.
- The IOM or FEX backplane ports of the fabric interconnect on which evacuation is configured will go down, and their state will appear as **Admin down**. During the manual upgrade process, to move these backplane ports back to the Up state and resume traffic flow, you must explicitly configure **Admin Evac Mode** as **Off**.
- Starting with Cisco UCS Manager Release 3.1(3), you can use fabric evacuation during Auto Install.
- If you use fabric evacuation outside of the upgrade process, you must re-acknowledge the FEX to get the VIFs back to the online state.

Configuring Fabric Evacuation

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Expand **Equipment** > **Fabric Interconnects** > ***Fabric_Interconnect_Name***.

Step 3 In the **Work** pane, click the **General** tab.

Step 4 In the **Actions** area of the **General** tab, click **Configure Evacuation**.
The Configure Evacuation dialog box appears.

Step 5 To configure fabric evacuation on the specified Fabric Interconnect, click one of the following radio buttons in the **Admin Evac Mode** field:

- **On**—Stops all the traffic that is active through the specified Fabric Interconnect.
- **Off**—Restarts traffic through the specified Fabric Interconnect.

Step 6 (Optional) To evacuate a Fabric Interconnect irrespective of its current evacuation state, check the **Force** check box.

Step 7 Click **Apply**.
A warning dialog box appears.

```
Enabling fabric evacuation will stop all traffic through this Fabric Interconnect from
servers attached through IOM/FEX.
The traffic will fail over to the Primary Fabric Interconnect for fail over vnics.
Are you sure you want to continue?
```

Step 8 Click **OK** to confirm fabric evacuation and continue.

Displaying the Status of Fabric Evacuation on a Fabric Interconnect

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Expand **Equipment** > **Fabric Interconnects** > ***Fabric_Interconnect_Name***.

Step 3 In the **Work** pane, click the **General** tab.

Step 4 The Status area displays

Fabric Interconnect Switching Modes

The Cisco UCS Fabric Interconnects operate in two main switching modes: Ethernet or Fibre Channel. These modes are independent of each other. They determine how the fabric interconnect behaves as a device between the server and network/server and storage device.

Ethernet Switching Mode

The Ethernet switching mode determines how the fabric interconnect behaves as a switching device between the servers and the network. The fabric interconnect operates in either of the following Ethernet switching modes:

End-Host Mode

End-host mode allows the fabric interconnect to act as an end host to the network, representing all servers (hosts) connected to it through vNICs. This behavior is achieved by pinning (either dynamically pinning or hard pinning) vNICs to uplink ports, which provides redundancy to the network, and makes the uplink ports appear as server ports to the rest of the fabric.

In end-host mode, the fabric interconnect does not run the Spanning Tree Protocol (STP), but it avoids loops by denying uplink ports from forwarding traffic to each other and by denying egress server traffic on more than one uplink port at a time. End-host mode is the default Ethernet switching mode and should be used if either of the following is used upstream:

- Layer 2 switching for Layer 2 aggregation
- Virtual Switching System (VSS) aggregation layer

Note When you enable end-host mode, if a vNIC is hard pinned to an uplink port and this uplink port goes down, the system cannot repin the vNIC, and the vNIC remains down.

Switch Mode

Switch mode is the traditional Ethernet switching mode. The fabric interconnect runs STP to avoid loops, and broadcast and multicast packets are handled in the traditional way. Use the switch mode only if the fabric interconnect is directly connected to a router, or if either of the following is used upstream:

- Layer 3 aggregation
- VLAN in a box

Note For both Ethernet switching modes, even when vNICs are hard-pinned to uplink ports, all server-to-server unicast traffic in the server array is sent only through the fabric interconnect and is never sent through uplink ports. Server-to-server multicast and broadcast traffic is sent through all uplink ports in the same VLAN.

Cisco UCS Fabric Interconnect in Switch Mode with Cisco MDS 9000 Family Fibre Channel Switching Modules

While creating a port channel between a Cisco MDS 9000 family FC switching module and a Cisco UCS Fabric Interconnect in switch mode, use the following order:

1. Create the port channel on the MDS side.
2. Add the port channel member ports.
3. Create the port channel on the Fabric Interconnect side.
4. Add the port channel member ports.

If you create the port channel on the Fabric Interconnect side first, the ports will go into a suspended state.

When the Cisco UCS Fabric Interconnect is in switch mode, the port channel mode can only be in **ON** mode and not **Active**. However, to get the peer wwn information for the Fabric Interconnect, the port channel must be in **Active** mode.

Configuring Ethernet Switching Mode

Important When you change the Ethernet switching mode, Cisco UCS Manager logs you out and restarts the fabric interconnect. For a cluster configuration, Cisco UCS Manager restarts both fabric interconnects. The subordinate fabric interconnect reboots first as a result of the change in switching mode. The primary fabric interconnect reboots only after you acknowledge it in **Pending Activities**. The primary fabric interconnect can take several minutes to complete the change in Ethernet switching mode and become system ready. The existing configuration is retained.

While the fabric interconnects are rebooting, all blade servers lose LAN and SAN connectivity, causing a complete outage of all services on the blades. This might cause the operating system to fail.

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Expand **Equipment** > **Fabric Interconnects** > ***Fabric_Interconnect_Name***.

Step 3 In the **Work** pane, click the **General** tab.

Step 4 In the **Actions** area of the **General** tab, click one of the following links:

- **Set Ethernet Switching Mode**
- **Set Ethernet End-Host Mode**

The link for the current mode is dimmed.

Step 5 In the dialog box, click **Yes**.

Cisco UCS Manager restarts the fabric interconnect, logs you out, and disconnects Cisco UCS Manager GUI.

Fibre Channel Switching Mode

The Fibre Channel switching mode determines how the fabric interconnect behaves as a switching device between the servers and storage devices. The fabric interconnect operates in either of the following Fibre Channel switching modes:

End-Host Mode

End-host mode is synonymous with N Port Virtualization (NPV) mode. This mode is the default Fibre Channel Switching mode. End-host mode allows the fabric interconnect to act as an end host to the connected fibre channel networks, representing all servers (hosts) connected to it through virtual host bus adapters (vHBAs). This behavior is achieved by pinning (either dynamically pinning or hard-pinning) vHBAs to Fibre Channel uplink ports, which makes the Fibre Channel ports appear as server ports (N-ports) to the rest of the fabric. When in end-host mode, the fabric interconnect avoids loops by preventing uplink ports from receiving traffic from one another.

Note When you enable end-host mode, if a vHBA is hard-pinned to an uplink Fibre Channel port and this uplink port goes down, the system cannot repin the vHBA, and the vHBA remains down.

Switch Mode

Switch mode is not the default Fibre Channel switching mode. Switch mode allows the fabric interconnect to connect directly to a storage device. Enabling Fibre Channel switch mode is useful in Pod models where there is no SAN (for example, a single Cisco UCS domain that is connected directly to storage), or where a SAN exists (with an upstream MDS). In Fibre Channel switch mode, SAN pin groups are irrelevant. Any existing SAN pin groups are ignored.

Configuring Fibre Channel Switching Mode

Important When you change the Fibre Channel switching mode, Cisco UCS Manager logs you out and restarts the fabric interconnect. For a cluster configuration, Cisco UCS Manager restarts both fabric interconnects simultaneously in Cisco UCS Manager Release 3.1(1) and earlier releases. In Cisco UCS Manager Release 3.1(2), when the Fibre Channel switching mode is changed, the UCS fabric interconnects reload sequentially. In Cisco UCS Manager Release 3.1(3), and later releases, the subordinate fabric interconnect reboots first as a result of the change in switching mode. The primary fabric interconnect reboots only after you acknowledge it in **Pending Activities**. The primary fabric interconnect can take several minutes to complete the change in Fibre Channel switching mode and become system ready.

Note When the Fibre Channel switching mode is changed, both UCS fabric interconnects will reload simultaneously. Reloading of fabric interconnects will cause a system-wide downtime lasting approximately 10-15 minutes.

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Expand **Equipment** > **Fabric Interconnects** > ***Fabric_Interconnect_Name***.

Step 3 In the **Work** pane, click the **General** tab.

Step 4 In the **Actions** area of the **General** tab, click one of the following links:

- **Set Fibre Channel Switching Mode**
- **Set Fibre Channel End-Host Mode**

The link for the current mode is dimmed.

Step 5 In the dialog box, click **Yes**.

Cisco UCS Manager restarts the fabric interconnect, logs you out, and disconnects Cisco UCS Manager GUI.

Changing the Properties of the Fabric Interconnects

Note To change the subnet or network prefix for a Cisco UCS domain, you must simultaneously change all subnets or prefixes, the virtual IPv4 or IPv6 address used to access Cisco UCS Manager, and the IPv4 or IPv6 addresses for both fabric interconnects.

Both fabric interconnects must maintain the same management address type, either IPv4 or IPv6. You cannot change the management address type for Fabric A without changing the management address type for Fabric B.

Procedure

Step 1 In the **Navigation** pane, click **Admin**.

Step 2 Expand **Admin** > **All**.

Step 3 In the **Work** pane, click the **General** tab.

Step 4 In the **Actions** area, click **Management Interfaces** to open the **Management Interfaces** dialog box.

Step 5 In the **Management Interfaces** dialog box, modify the values as necessary.

Step 6 To change only the virtual IP address that you use to access Cisco UCS Manager, enter the desired IP address in either the **IPv4 Address** or the **IPv6 Address** field in the **Virtual IP** area.

Step 7 To change only the name assigned to the Cisco UCS domain, enter the desired name in the **Name** field in the **Virtual IP** area.

Step 8 To change the subnet and IPv4 address, or the network prefix and IPv6 address, and default gateway assigned to the fabric interconnects, update the following fields:

a) In the **Virtual IP** area, change the IP address used to access Cisco UCS Manager in the **IPv4 Address** or **IPv6 Address** field.

b) In the **Fabric Interconnect** area for each fabric interconnect, click either the IPv4 or IPv6 tab.

c) On the IPv4 tab, update the IP address, subnet mask, and default gateway.

d) On the IPv6 tab, update the IP address, prefix, and default gateway.

Step 9 Click **OK**.

Step 10 Log out of Cisco UCS Manager GUI and log back in again to see your changes.

Determining the Primary Fabric Interconnect

Important If the admin password is lost, you can determine the primary and secondary roles of the fabric interconnects in a cluster by opening the Cisco UCS Manager GUI from the IP addresses of both fabric interconnects. The subordinate fabric interconnect fails with the following message:

```
UCSM GUI is not available on secondary node.
```

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Expand **Equipment** > **Fabric Interconnects**.

Step 3 Click the fabric interconnect for which you want to identify the role.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the **General** tab, click the down arrows on the **High Availability Details** bar to expand that area.

Step 6 View the **Leadership** field to determine whether the fabric interconnect is primary or subordinate.

Fabric Interconnect Port Types

By default, all fabric interconnect ports are unconfigured. For Ethernet LAN connectivity, fabric interconnect ports can be in the following states:

- **Unconfigured**—Port is not configured and cannot be used.
- **Server Port**—Port is configured for downlink connection to an IOM Fabric Extender (FEX) module in a blade chassis.
- **Uplink Port**—Port is configured for uplink connection to the upstream Ethernet switch. Uplink ports are always configured as trunk ports.
- **Disabled**—Port is configured either as an uplink or server port and is currently disabled by the administrator.

For 6200 series fabric interconnects, all ports are unified ports; therefore you also configure all the ports as 1/10 Gigabit Ethernet, Fibre Channel (FC), FC uplink, appliance port, or FCoE port.

For 6300 series fabric interconnects, see the *UCS Manager Getting Started Guide*.

For Cisco UCS 6454 and 64108 Fabric Interconnects, ports 1 to 16 are unified ports. These ports can be configured as either Ethernet or FC ports. The *UCS Manager Getting Started Guide* has detailed information.

vNICs

Once the connectivity between upstream uplink switches and downstream IOMs is established, we can connect vNICs from blade servers configuring vNICs. We recommended that you create a vNIC template to provide ease of management .

vNICs can be created within server profiles or by using a vNIC template. Using a vNIC template is the recommended method for configuring the NIC settings once, for each template, and then quickly creating new vNICs with the desired configuration. The vNIC configuration settings can be optimized for various operating systems, storage devices, and hypervisors.

A vNIC template can be configured as either of the following:

- Initiating template: This vNIC template will provide one-time configuration for the vNICs created using this template. Any subsequent changes to the template are not propagated to abstracted vNICs.
- Updating template: This vNIC template will provide initial configuration for the vNICs created using this template. Any subsequent changes to the template will also be propagated to abstracted vNICs. We recommend that you to create an updating vNIC template for production environments.

vNIC MAC addresses can be assigned manually or by configuring a MAC address pool. It is possible to either use the burned-in MAC addresses or abstract MAC addresses from an identity pool with system-defined prefixes. Stateless computing is the salient feature of the Cisco UCS platform. Therefore we recommend to you abstract vNIC MAC addresses for server profiles, and consequently use server vNIC MAC addresses from MAC address identity pools instead of using burned-in NIC MAC addresses. The benefit of abstracting the MAC identity is that in case of physical server failure, the server profile can be easily associated with the replacement server. The new server will acquire all the identities associated with the old server including the vNIC MAC addresses. From the operating system perspective, there is no change at all.

We recommend that you create vNIC templates with different configurations and create individual vNICs from vNIC templates as required. Also, define MAC address pools and assign MAC addresses to individual vNICs using those MAC address pools.

A vNIC is typically abstracted from the physical mezzanine card. Older Emulex, QLogic, and Intel NIC cards have fixed ports. The Cisco mezzanine NIC card, also known as a Palo card or Virtual Interface Card (VIC), provides dynamic server interfaces. Cisco VIC cards provide up to 256 dynamic interfaces. vNICs can be created within server profiles or by using a vNIC template. Using a vNIC template is the recommended method for configuring the NIC settings, doing so once for each template and then quickly creating additional vNICs with the desired configurations. The vNIC configuration settings can be optimized for various operating systems, storage devices, and hypervisors.

The vNIC creation for servers is part of the server profile, or server profile template creation. Once **Create Service Profile Template** or **Service Profile (Expert)** is started for the blade servers, creating the vNIC is the second step in the configuration wizard.