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

You must configure the information policy to display the uplink switches that are connected to Cisco UCS.

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

Enabling the Information Policy on the Fabric Interconnect

Note By default, the information policy is disabled on the fabric interconnect.

Procedure

	Command or Action	Purpose
Step 1	UCS-A # **scope system**	Enters system mode.
Step 2	UCS-A/system # **scope info-policy**	Enters the information policy state.
Step 3	(Optional) UCS-A/system/info-policy # **show**	Shows if the information policy is enabled or disabled.
Step 4	UCS-A/system/info-policy # **enable**	Enables the information policy on the fabric interconnect.
Step 5	UCS-A/system/info-policy* # **commit-buffer**	Enables the information policy on the fabric interconnect.

Example

The following example shows how to enable the information policy on the fabric interconnect:

```
UCS-A#  scope system
UCS-A/system # scope info-policy
UCS-A/system/info-policy # show
Info Policy:
State: Disabled
UCS-A/system/info-policy # enable
UCS-A/system/info-policy* # commit-buffer
UCS-A/system/info-policy #
```

Disabling the Information Policy on the Fabric Interconnect

Procedure

	Command or Action	Purpose
Step 1	UCS-A # **scope system**	Enters system mode.
Step 2	UCS-A/system # **scope info-policy**	Enters the information policy state.
Step 3	(Optional) UCS-A/system/info-policy # **show**	Shows if the information policy is enabled or disabled.
Step 4	UCS-A/system/info-policy # **disable**	Disables the information policy on the fabric interconnect.
Step 5	UCS-A/system/info-policy* # **commit-buffer**	Disables information policy on the fabric interconnect.

Example

The following example shows how to disable the information policy on the fabric interconnect:

```
UCS-A#  scope system
UCS-A/system # scope info-policy
UCS-A/system/info-policy # show
Info Policy:
State: Enabled
UCS-A/system/info-policy # disable
UCS-A/system/info-policy* # commit-buffer
UCS-A/system/info-policy #
```

Viewing the LAN Neighbors of the Fabric Interconnect

You must enable the information policy on the fabric interconnect to view the LAN neighbors.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope fabric-interconnect** {**a** | **b**}	Enters fabric interconnect mode for the specified fabric interconnect.
Step 2	UCS-A/fabric-interconnect # **show lan-neighbors**	Displays the fabric interconnect LAN neighbors.

Example

The following example shows how to display the LAN neighbors of the fabric interconnect:

```
UCS-A #  scope fabric-interconnect a
UCS-Afabric-interconnect # show lan-neighbors
Info Policy:Enabled
Lan Neighbors:
Local Interface: Ethernet1/2
Device Id: bgl-samc02-B(SSI140305YK)
IPv4 Address: 10.105.214.105
FI Port DN: sys/switch-A/slot-1/switch-ether/port-2
```

Viewing the SAN Neighbors of the Fabric Interconnect

You must enable the information policy on the fabric interconnect to view the SAN neighbors.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope fabric-interconnect** {**a** | **b**}	Enters fabric interconnect mode for the specified fabric interconnect.
Step 2	UCS-A/fabric-interconnect # **show san-neighbors**	Displays the fabric interconnect SAN neighbors.

Example

The following example shows how to display the SAN neighbors of the fabric interconnect :

```
UCS-A #  scope fabric-interconnect a
UCS-A/fabric-interconnect # show san-neighbors
Info Policy: Enabled
San neighbors:
Local Interface: fc2/1
Port VSAN: 100
Fabric Mgmt Addr: 10.65.124.252
Fabric pwwn: 20:02:00:05:9b:22:ad:C0
Fabric nwwn: 20:64:00:05:9b:22:ad:C1
My pwwn: 20:41:00:0d:ec:ee:dd:00
My nwwn: 20:64:00:0d:ec:ee:dd:01
FI Port DN: sys/switch-A/slot-2/switch-fc/port-1
```

Viewing the LLDP Neighbors of the Fabric Interconnect

You must enable the information policy on the fabric interconnect to view the LLDP neighbors.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope fabric-interconnect** {**a** | **b**}	Enters fabric interconnect mode for the specified fabric interconnect.
Step 2	UCS-A/fabric-interconnect # **show lldp-neighbors**	Displays the fabric interconnect LLDP neighbors.

Example

The following example shows how to display the LLDP neighbors of the fabric interconnect :

```
UCS-A #  scope fabric-interconnect a
UCS-A/fabric-interconnect # show lldp-neighbors
Info Policy: Enabled

Lldp Neighbors:

Local Interface: Eth1/5
Chassis Id: 000d.ecff.5e90
Remote Interface: Eth1/9
Remote Port Description: Ethernet1/9
System Name: bgl-samc02-B
System Description: Cisco Nexus Operating System (NX-OS) Software TAC support:
http://www.cisco.com/tac Copyright (c) 2002-2011, Cisco Systems, Inc
System Capabilities: B
Enabled Capabilities: B
Native VLAN: 1
IPv4 Mgmt Address: 10.105.214.105
FI Port DN: sys/switch-A/slot-1/switch-ether/port-5
```

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.

Stopping Traffic on a Fabric Interconnect

Procedure

	Command or Action	Purpose
Step 1	UCS-A # **scope fabric-interconnect** {**a** | **b**}	Enters the fabric interconnect mode.
Step 2	UCS-A /fabric-interconnect # **stop server traffic** [**force**]	Stops all the traffic that is active through the specified Fabric Interconnect. Use the **force** option to evacuate a fabric interconnect regardless of its current evacuation state.

	Command or Action	Purpose
Step 3	UCS-A /fabric-interconnect # **commit-buffer**	Commits the transaction to the system configuration.

Example

This example shows how to stop all traffic that is active through Fabric Interconnect B:

```
UCS-A# scope fabric-interconnect b
UCS-A /fabric-interconnect # stop server traffic
Warning: 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.
UCS-A /fabric-interconnect # commit-buffer
```

Displaying the Status of Evacuation for a Fabric Interconnect

Procedure

	Command or Action	Purpose
Step 1	UCS-A # **scope fabric-interconnect** {**a** | **b**}	Enters fabric interconnect mode for the specified fabric interconnect.
Step 2	UCS-A /fabric-interconnect # **show detail**	Displays details about the specified fabric interconnect.

Example

This example shows how to display the status of a fabric interconnect.

Note **Admin Evacuation**and **Oper Evacuation** and show the status of evacuation at the fabric interconnect.

```
 UCS-A /fabric-interconnect # show detail

Fabric Interconnect:
    ID: B
    Product Name: Cisco UCS 6248UP
    PID: UCS-FI-6248UP
    VID: V01
    Vendor: Cisco Systems, Inc.
    Serial (SN): SSI171400HG
    HW Revision: 0
    Total Memory (MB): 16165
    OOB IP Addr: 10.193.32.172
    OOB Gateway: 10.193.32.1
    OOB Netmask: 255.255.255.0
    OOB IPv6 Address: ::
```

```
    OOB IPv6 Gateway: ::
    Prefix: 64
    Operability: Operable
    Thermal Status: Ok
    Admin Evacuation: On
    Oper Evacuation: On
    Current Task 1:
    Current Task 2:
    Current Task 3:
```

Displaying the Status of Evacuation for an IOM

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope chassis** *chassis-num*	Enters chassis mode for the specified chassis.
Step 2	UCS-A /chassis # **scope iom** *iom-id*	Enters chassis IOM mode for the specified IOM.
Step 3	UCS-A /chassis/iom # **show detail**	Displays evacuation status details for the specified IOM.

Example

This example shows how to display the evacuation status details for an IOM.

Note **Oper Evacuation** shows the operational status of evacuation for the IOM.

```
UCS-A# scope chassis 1
UCS-A /chassis # scope iom 1
UCS-A /chassis/iom # show detail

IOM:
    ID: 1
    Side: Left
    Fabric ID: A
    User Label:
    Overall Status: Fabric Conn Problem
    Oper qualifier: Server Port Problem
    Operability: Operable
    Presence: Equipped
    Thermal Status: OK
    Discovery: Online
    Config State: Ok
    Peer Comm Status: Connected
    Product Name: Cisco UCS 2204XP
    PID: UCS-IOM-2204XP
    VID: V02
    Part Number: 73-14488-02
    Vendor: Cisco Systems Inc
    Serial (SN): FCH1718J9FT
```

```
    HW Revision: 0
    Mfg Date: 2013-05-12T00:00:00.000
    Controller Subject: Iocard
    Fabric Port Aggregation Capability: Port Channel
    Oper Evacuation: On
    Current Task 1:
    Current Task 2:
```

Verifying Fabric Evacuation

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **show service-profile circuit server** *server-id*	Shows the network circuit information for the service profile associated with the specified server.

Example

The following example shows the VIF (Virtual NIC) paths before fabric evacuation.

Note

- VIF at Fabric Interconnect A shows that traffic is initially active through the fabric interconnect.
- VIF at Fabric Interconnect B is passive before evacuation.

```
UCS-A# show service-profile circuit server 1/6
Service Profile: test1
Server: 1/6
    Fabric ID: A
        Path ID: 1
        VIF        vNIC            Link State  Oper State Prot State    Prot Role   Admin
Pin  Oper Pin   Transport
       ---------- --------------- ----------- ---------- ------------ ----------- ----------
 ---------- ---------
              692 eth0            Up          Active     Active        Primary     0/0
     1/15       Ether
    Fabric ID: B
        Path ID: 1
        VIF        vNIC            Link State  Oper State Prot State    Prot Role   Admin
Pin  Oper Pin   Transport
       ---------- --------------- ----------- ---------- ------------ ----------- ----------
 ---------- ---------
              693 eth0            Up          Active     Passive       Backup      0/0
     1/15       Ether
UCS-A#
```

The following example shows the VIF paths after Fabric Interconnect A is evacuated.

Note

- After failover, the VIF state at Fabric Interconnect A goes into error.
- VIF at Fabric Interconnect B takes over as active.

```
UCS-A# show service-profile circuit server 1/6
Service Profile: test1
Server: 1/6
    Fabric ID: A
        Path ID: 1
        VIF        vNIC            Link State  Oper State Prot State    Prot Role   Admin
Pin  Oper Pin   Transport
      ---------- --------------- ----------- ---------- ------------- ----------- ----------
 ---------- ---------
               692 eth0            Error       Error      Active        Primary     0/0
     0/0        Ether
    Fabric ID: B
        Path ID: 1
        VIF        vNIC            Link State  Oper State Prot State    Prot Role   Admin
Pin  Oper Pin   Transport
      ---------- --------------- ----------- ---------- ------------- ----------- ----------
 ---------- ---------
               693 eth0            Up          Active     Passive       Backup      0/0
     1/15       Ether
UCS-A#
```

Restarting Traffic on a Fabric Interconnect

Procedure

	Command or Action	Purpose
Step 1	UCS-A # **scope fabric-interconnect** {**a** | **b**}	Enters the fabric interconnect mode.
Step 2	UCS-A /fabric-interconnect # **start server traffic**	Restarts traffic through the specified fabric interconnect.
Step 3	UCS-A /fabric-interconnect # **commit-buffer**	Commits the transaction to the system configuration.

Example

This example shows how to restart traffic through Fabric Interconnect B:

```
UCS-A# scope fabric-interconnect b
UCS-A /fabric-interconnect # start server traffic
Warning: Resetting fabric evacuation will cause server traffic that failed over to the
Primary Fabric Interconnect to fail back to this Fabric Interconnect.
UCS-A /fabric-interconnect # commit-buffer
```

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*.

Fabric Interconnect Switching Modes

The Cisco UCS Fabric Interconnects are operated 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

	Command or Action	Purpose
Step 1	UCS-A# **scope eth-uplink**	Enters Ethernet uplink mode.
Step 2	UCS-A /eth-uplink # **set mode** {**end-host** | **switch**}	Sets the fabric interconnect to the specified switching mode.
Step 3	UCS-A /eth-uplink # **commit-buffer**	Commits the transaction to the system configuration. Cisco UCS Manager restarts the fabric interconnect, logs you out, and disconnects Cisco UCS Manager CLI.

Example

The following example sets the fabric interconnect to end-host mode and commits the transaction:

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # set mode end-host
Warning: When committed, this change will cause the switch to reboot
UCS-A /eth-uplink* # commit-buffer
UCS-A /eth-uplink #
```

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

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

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope fc-uplink**	Enters Fibre Channel uplink mode.
Step 2	UCS-A /fc-uplink # **set mode** {**end-host** | **switch**}	Sets the fabric interconnect to the specified switching mode.
Step 3	UCS-A /fc-uplink # **commit-buffer**	Commits the transaction to the system configuration. Cisco UCS Manager restarts the fabric interconnect, logs you out, and disconnects Cisco UCS Manager CLI.

Example

The following example shows how to set the fabric interconnect to end-host mode and commit the transaction:

```
UCS-A # scope fc-uplink
UCS-A /fc-uplink # set mode end-host
UCS-A /fc-uplink* # commit-buffer
UCS-A /fc-uplink #
```