



Configuring the Fabric Interconnects

This chapter includes the following sections:

- [Initial System Setup, page 1](#)
- [Performing an Initial System Setup for a Standalone Configuration, page 3](#)
- [Initial System Setup for a Cluster Configuration, page 5](#)
- [Enabling a Standalone Fabric Interconnect for Cluster Configuration, page 10](#)
- [Changing the System Name, page 11](#)
- [Changing the Management Subnet of a Cluster, page 12](#)
- [Changing the Management Prefix of a Cluster, page 13](#)
- [Configuring the Information Policy on the Fabric Interconnect, page 14](#)
- [Fabric Evacuation, page 17](#)
- [Ethernet Switching Mode, page 22](#)
- [Configuring Ethernet Switching Mode, page 23](#)
- [Fibre Channel Switching Mode, page 24](#)
- [Configuring Fibre Channel Switching Mode, page 25](#)

Initial System Setup

The first time that you access a fabric interconnect in a Cisco UCS domain, a setup wizard prompts you for the following information required to configure the system:

- Installation method (GUI or CLI)
- Setup mode (restore from full system backup or initial setup)
- System configuration type (standalone or cluster configuration)
- System name
- Admin password

- Management port IPv4 address and subnet mask, or IPv6 address and prefix
- Default gateway IPv4 or IPv6 address
- DNS Server IPv4 or IPv6 address
- Default domain name

Setup Mode

You can choose to either restore the system configuration from an existing backup file, or manually set up the system by going through the Setup wizard. If you choose to restore the system, the backup file must be reachable from the management network.

System Configuration Type

You can configure a Cisco UCS domain to use a single fabric interconnect in a standalone configuration or to use a redundant pair of fabric interconnects in a cluster configuration.

A cluster configuration provides high availability. If one fabric interconnect becomes unavailable, the other takes over. Only one management port (Mgmt0) connection is required to support a cluster configuration; however, both Mgmt0 ports should be connected to provide link-level redundancy.

In addition, a cluster configuration actively enhances failover recovery time for redundant virtual interface (VIF) connections. When an adapter has an active VIF connection to one fabric interconnect and a standby VIF connection to the second, the learned MAC addresses of the active VIF are replicated but not installed on the second fabric interconnect. If the active VIF fails, the second fabric interconnect installs the replicated MAC addresses and broadcasts them to the network through gratuitous ARP messages, shortening the switchover time.



Note

The cluster configuration provides redundancy only for the management plane. Data redundancy is dependent on the user configuration and might require a third-party tool to support data redundancy.

To use the cluster configuration, you must directly connect the two fabric interconnects together using Ethernet cables between the L1 (L1-to-L1) and L2 (L2-to-L2) high-availability ports, with no other fabric interconnects in between. Also you can connect the fabric interconnects directly through a patch panel to allow the two fabric interconnects to continuously monitor the status of each other and quickly know when one has failed.

Both fabric interconnects in a cluster configuration must go through the initial setup process. You must enable the first fabric interconnect that you set up for a cluster configuration. When you set up the second fabric interconnect, it detects the first fabric interconnect as a peer fabric interconnect in the cluster.

For more information, see to the *Cisco UCS 6100 Series Fabric Interconnect Hardware Installation Guide*.

Management Port IP Address

In a standalone configuration, you must specify only one IPv4 address, gateway, and subnet mask, or only one IPv6 address, gateway, and network prefix for the single management port on the fabric interconnect. You can configure either an IPv4 or an IPv6 address for the management port IP address.

In a cluster configuration, you must specify the following three IPv4 addresses in the same subnet, or three IPv6 addresses with the same prefix:

- Management port IP address for fabric interconnect A
- Management port IP address for fabric interconnect B
- Cluster IP address

**Note**

In a cluster configuration, the management port for both fabric interconnects must be configured with the same address type, either IPv4 or IPv6. If you configure the first FI with an IPv4 address then attempt to configure the second FI with an IPv6 address, the configuration will fail.

Performing an Initial System Setup for a Standalone Configuration

Before You Begin

1 Verify the following physical connections on the fabric interconnect:

- The console port is physically connected to a computer terminal or console server
- The management Ethernet port (mgmt0) is connected to an external hub, switch, or router

For more information, refer to the *Cisco UCS Hardware Installation Guide* for your fabric interconnect.

2 Verify that the console port parameters on the computer terminal (or console server) attached to the console port are as follows:

- 9600 baud
- 8 data bits
- No parity
- 1 stop bit

3 Collect the following information that you will need to supply during the initial setup:

- System name
- Password for the admin account. Choose a strong password that meets the guidelines for Cisco UCS Manager passwords. This password cannot be blank.
- Management port IPv4 and subnet mask, or IPv6 address and prefix.
- Default gateway IPv4 or IPv6 address.
- DNS server IPv4 or IPv6 address (optional).
- Domain name for the system (optional).

Procedure

- Step 1** Connect to the console port.
- Step 2** Power on the fabric interconnect.
You will see the power on self-test messages as the fabric interconnect boots. The system will run a DHCP client to check for a lease.
- Step 3** When the unconfigured system boots, it prompts you for the setup method to be used. Enter **console** to continue the initial setup using the console CLI.
- Step 4** Enter **setup** to continue as an initial system setup.
- Step 5** Enter **y** to confirm that you want to continue the initial setup.
- Step 6** Enter the password for the admin account.
- Step 7** To confirm, re-enter the password for the admin account.
- Step 8** Enter **no** to continue the initial setup for a standalone configuration.
- Step 9** Enter the system name.
- Step 10** Enter the IPv4 or IPv6 address for the management port of the fabric interconnect.
If you enter an IPv4 address, you will be prompted to enter an IPv4 subnet mask. If you enter an IPv6 address, you will be prompted to enter an IPv6 network prefix.
- Step 11** Enter the respective IPv4 subnet mask or IPv6 network prefix, then press Enter.
You are prompted for an IPv4 or IPv6 address for the default gateway, depending on the address type you entered for the management port of the fabric interconnect.
- Step 12** Enter either the:
- IPv4 address of the default gateway
 - IPv6 address of the default gateway
- Step 13** Enter **yes** if you want to specify the IP address for the DNS server, or **no** if you do not.
- Step 14** (Optional) Enter the IPv4 or IPv6 address for the DNS server.
The address type must be the same as the address type of the management port of the fabric interconnect.
- Step 15** Enter **yes** if you want to specify the default domain name, or **no** if you do not.
- Step 16** (Optional) Enter the default domain name.
- Step 17** Enter **yes** if you want to join the centralized management environment (Cisco UCS Central), or **no** if you do not.
- Step 18** Review the setup summary and enter **yes** to save and apply the settings, or enter **no** to go through the Setup wizard again to change some of the settings.
If you choose to go through the Setup wizard again, it provides the values you previously entered, and the values appear in brackets. To accept previously entered values, press Enter.

The following example sets up a standalone configuration using the console setup method and IPv4 management addresses:

```
Enter the installation method (console/gui)? console
Enter the setup mode (restore from backup or initial setup) [restore/setup]? setup
You have chosen to setup a new switch. Continue? (y/n): y
Enter the password for "admin": adminpassword%958
Confirm the password for "admin": adminpassword%958
```

```

Do you want to create a new cluster on this switch (select 'no' for standalone setup or if
you want this switch to be added to an existing cluster)? (yes/no) [n]: no
Enter the system name: foo
Mgmt0 address: 192.168.10.10
Mgmt0 IPv4 netmask: 255.255.255.0
IPv4 address of the default gateway: 192.168.10.1
Configure the DNS Server IPv4 address? (yes/no) [n]: yes
  DNS IP address: 20.10.20.10
Configure the default domain name? (yes/no) [n]: yes
  Default domain name: domainname.com
Join centralized management environment (UCS Central)? (yes/no) [n]: no
Following configurations will be applied:
  Switch Fabric=A
  System Name=foo
  Physical Switch Mgmt0 IP Address=192.168.10.10
  Physical Switch Mgmt0 IP Netmask=255.255.255.0
  Default Gateway=192.168.10.1
  DNS Server=20.10.20.10
  Domain Name=domainname.com
Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no): yes
The following example sets up a standalone configuration using the console setup method and IPv6 management
addresses:

Enter the installation method (console/gui)? console
Enter the setup mode (restore from backup or initial setup) [restore/setup]? setup
You have chosen to setup a new switch. Continue? (y/n): y
Enter the password for "admin": adminpassword%652
Confirm the password for "admin": adminpassword%652
Do you want to create a new cluster on this switch (select 'no' for standalone setup or if
you want this switch to be added to an existing cluster)? (yes/no) [n]: no
Enter the system name: foo
Mgmt0 address: 2001::107
Mgmt0 IPv6 prefix: 64
IPv6 address of the default gateway: 2001::1
Configure the DNS Server IPv6 address? (yes/no) [n]: yes
  DNS IP address: 2001::101
Configure the default domain name? (yes/no) [n]: yes
  Default domain name: domainname.com
Join centralized management environment (UCS Central)? (yes/no) [n]: no
Following configurations will be applied:
  Switch Fabric=A
  System Name=foo
  Enforced Strong Password=no
  Physical Switch Mgmt0 IPv6 Address=2001::107
  Physical Switch Mgmt0 IPv6 Prefix=64
  Default Gateway=2001::1
  Ipv6 value=1
  DNS Server=2001::101
  Domain Name=domainname.com
Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no): yes

```

Initial System Setup for a Cluster Configuration

Performing an Initial System Setup for the First Fabric Interconnect

This procedure describes setting up the first fabric interconnect using IPv4 or IPv6 addresses for the management port, the default gateway, and the DNS server.

Before You Begin

- 1 Verify the following physical connections on the fabric interconnect:

- A console port on the first fabric interconnect is physically connected to a computer terminal or console server
- The management Ethernet port (mgmt0) is connected to an external hub, switch, or router
- The L1 ports on both fabric interconnects are directly connected to each other
- The L2 ports on both fabric interconnects are directly connected to each other

For more information, refer to the *Cisco UCS Hardware Installation Guide* for your fabric interconnect.

- 2 Verify that the console port parameters on the computer terminal (or console server) attached to the console port are as follows:
 - 9600 baud
 - 8 data bits
 - No parity
 - 1 stop bit
- 3 Collect the following information that you will need to supply during the initial setup:
 - System name.
 - Password for the admin account. Choose a strong password that meets the guidelines for Cisco UCS Manager passwords. This password cannot be blank.
 - Three static IPv4 or IPv6 addresses: two for the management port on both fabric interconnects (one per fabric interconnect) and one for the cluster IP address used by Cisco UCS Manager.
 - Subnet mask for the three static IPv4 addresses, or network prefix for the three static IPv6 addresses.
 - Default gateway IPv4 or IPv6 address.
 - DNS server IPv4 or IPv6 address (optional).
 - Domain name for the system (optional).

Procedure

- Step 1** Connect to the console port.
- Step 2** Power on the fabric interconnect.

You will see the power on self-test messages as the fabric interconnect boots. The system will run a DHCP client to check for a lease.

- Step 3** When the unconfigured system boots, it prompts you for the setup method to be used. Enter **console** to continue the initial setup using the console CLI.
- Step 4** Enter **setup** to continue as an initial system setup.
- Step 5** Enter **y** to confirm that you want to continue the initial setup.
- Step 6** Enter the password for the admin account.
- Step 7** To confirm, re-enter the password for the admin account.
- Step 8** Enter **yes** to continue the initial setup for a cluster configuration.
- Step 9** Enter the fabric interconnect fabric (either **A** or **B**).
- Step 10** Enter the system name.
- Step 11** Enter the IPv4 or IPv6 address for the management port of the fabric interconnect. If you enter an IPv4 address, you will be prompted to enter an IPv4 subnet mask. If you enter an IPv6 address, you will be prompted to enter an IPv6 network prefix.
- Step 12** Enter the respective IPv4 subnet mask or IPv6 network prefix, then press Enter. You are prompted for an IPv4 or IPv6 address for the default gateway, depending on the address type you entered for the management port of the fabric interconnect.
- Step 13** Enter either the:
- IPv4 address of the default gateway
 - IPv6 address of the default gateway
- Step 14** Enter **yes** if you want to specify the IP address for the DNS server, or **no** if you do not.
- Step 15** (Optional) Enter the IPv4 or IPv6 address for the DNS server. The address type must be the same as the address type of the management port of the fabric interconnect.
- Step 16** Enter **yes** if you want to specify the default domain name, or **no** if you do not.
- Step 17** (Optional) Enter the default domain name.
- Step 18** Review the setup summary and enter **yes** to save and apply the settings, or enter **no** to go through the Setup wizard again to change some of the settings. If you choose to go through the Setup wizard again, it provides the values you previously entered, and the values appear in brackets. To accept previously entered values, press **Enter**.

The following example sets up the first fabric interconnect for a cluster configuration using the console and IPv4 management addresses:

```
Enter the installation method (console/gui)? console
Enter the setup mode (restore from backup or initial setup) [restore/setup]? setup
You have chosen to setup a new switch. Continue? (y/n): y
Enter the password for "admin": adminpassword%958
Confirm the password for "admin": adminpassword%958
Do you want to create a new cluster on this switch (select 'no' for standalone setup or if
you want this switch to be added to an existing cluster)? (yes/no) [n]: yes
Enter the switch fabric (A/B): A
Enter the system name: foo
Mgmt0 IPv4 address: 192.168.10.10
Mgmt0 IPv4 netmask: 255.255.255.0
IPv4 address of the default gateway: 192.168.10.1
Virtual IPv4 address: 192.168.10.12
```

```

Configure the DNS Server IPv4 address? (yes/no) [n]: yes
  DNS IPv4 address: 20.10.20.10
Configure the default domain name? (yes/no) [n]: yes
  Default domain name: domainname.com
Join centralized management environment (UCS Central)? (yes/no) [n]: no
Following configurations will be applied:
  Switch Fabric=A
  System Name=foo
  Management IP Address=192.168.10.10
  Management IP Netmask=255.255.255.0
  Default Gateway=192.168.10.1
  Cluster Enabled=yes
  Virtual Ip Address=192.168.10.12
  DNS Server=20.10.20.10
  Domain Name=domainname.com
Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no): yes
The following example sets up the first fabric interconnect for a cluster configuration using the console and IPv6 management addresses:

Enter the installation method (console/gui)? console
Enter the setup mode (restore from backup or initial setup) [restore/setup]? setup
You have chosen to setup a new switch. Continue? (y/n): y
Enter the password for "admin": adminpassword%652
Confirm the password for "admin": adminpassword%652
Do you want to create a new cluster on this switch (select 'no' for standalone setup or if you want this switch to be added to an existing cluster)? (yes/no) [n]: yes
Enter the switch fabric (A/B): A
Enter the system name: foo
Mgmt0 address: 2001::107
Mgmt0 IPv6 prefix: 64
IPv6 address of the default gateway: 2001::1
Configure the DNS Server IPv6 address? (yes/no) [n]: yes
  DNS IP address: 2001::101
Configure the default domain name? (yes/no) [n]: yes
  Default domain name: domainname.com
Join centralized management environment (UCS Central)? (yes/no) [n]: no
Following configurations will be applied:
  Switch Fabric=A
  System Name=foo
  Enforced Strong Password=no
  Physical Switch Mgmt0 IPv6 Address=2001::107
  Physical Switch Mgmt0 IPv6 Prefix=64
  Default Gateway=2001::1
  Ipv6 value=1
  DNS Server=2001::101
  Domain Name=domainname.com
Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no): yes

```

Performing an Initial System Setup for the Second Fabric Interconnect

This procedure describes setting up the second fabric interconnect using IPv4 or IPv6 addresses for the management port.

Before You Begin

- 1 Verify the following physical connections on the fabric interconnect:
 - A console port on the second fabric interconnect is physically connected to a computer terminal or console server
 - The management Ethernet port (mgmt0) is connected to an external hub, switch, or router
 - The L1 ports on both fabric interconnects are directly connected to each other
 - The L2 ports on both fabric interconnects are directly connected to each other

For more information, refer to the *Cisco UCS Hardware Installation Guide* for your fabric interconnect.

- 2 Verify that the console port parameters on the computer terminal (or console server) attached to the console port are as follows:
 - 9600 baud
 - 8 data bits
 - No parity
 - 1 stop bit

- 3 Collect the following information that you will need to supply during the initial setup:
 - Password for the admin account of the peer fabric interconnect. Choose a strong password that meets the guidelines for Cisco UCS Manager passwords. This password cannot be blank.
 - Management port IPv4 address in the same subnet, or management port IPv6 with the same network prefix as the peer fabric interconnect.

4

Procedure

-
- Step 1** Connect to the console port.
 - Step 2** Power on the fabric interconnect.
You will see the power on self-test messages as the fabric interconnect boots. The system will run a DHCP client to check for a lease.
 - Step 3** When the unconfigured system boots, it prompts you for the setup method to be used. Enter **console** to continue the initial setup using the console CLI.
Note The fabric interconnect should detect the peer fabric interconnect in the cluster. If it does not, check the physical connections between the L1 and L2 ports, and verify that the peer fabric interconnect has been enabled for a cluster configuration.
 - Step 4** Enter **y** to add the subordinate fabric interconnect to the cluster.
 - Step 5** Enter the admin password of the peer fabric interconnect.
 - Step 6** Enter the IP address for the management port on the subordinate fabric interconnect.
 - Step 7** Review the setup summary and enter **yes** to save and apply the settings, or enter **no** to go through the Setup wizard again to change some of the settings.
If you choose to go through the Setup wizard again, it provides the values you previously entered, and the values appear in brackets. To accept previously entered values, press **Enter**.
-

The following example sets up the second fabric interconnect for a cluster configuration using the console and the IPv4 address of the peer:

```
Enter the installation method (console/gui)? console
Installer has detected the presence of a peer Fabric interconnect. This Fabric interconnect
will be added to the cluster. Continue (y/n) ? y
Enter the admin password of the peer Fabric Interconnect: adminpassword%958
Peer Fabric interconnect Mgmt0 IPv4 Address: 192.168.10.11
Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no): yes
```

The following example sets up the second fabric interconnect for a cluster configuration using the console and the IPv6 address of the peer:

```
Enter the installation method (console/gui)? console
Installer has detected the presence of a peer Fabric interconnect. This Fabric interconnect
will be added to the cluster. Continue (y/n) ? y
Enter the admin password of the peer Fabric Interconnect: adminpassword%958
Peer Fabric interconnect Mgmt0 IPv6 Address: 2001::107
Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no): yes
```

Adding Out-of-band IPv4 Addresses to a Fabric Interconnect

All fabric interconnects require an OOB IPv4 address, network mask and gateway. This procedure describes how to configure an OOB IPv4 address for a fabric interconnect that was set up with static IPv6 addresses.

Before You Begin

Collect the out-of-band (OOB) IPv4 address you want to assign to the fabric interconnect.

Procedure

	Command or Action	Purpose
Step 1	UCS-A # scope fabric interconnect a	Enters fabric configuration mode for Fabric A.
Step 2	UCS-A/fabric-interconnect # set out-of-band ip ip-addr netmask ip-addr gw ip-addr	Sets the OOB IPv4 address, network mask and gateway address. The system warns that the console session change may be disconnected when the change is committed.
Step 3	UCS-A/fabric-interconnect # commit-buffer	Commits the transaction to the system configuration.

The following example shows configuring an OOB IPv4 address for fabric interconnect A:

```
UCS-A# scope fabric-interconnect a
UCS-A /fabric-interconnect # set out-of-band ip 10.105.214.107 netmask 255.255.255.0 gw 10.105.214.1
Warning: When committed, this change may disconnect the current CLI session
UCS-A /fabric-interconnect* # commit-buffer
```

Enabling a Standalone Fabric Interconnect for Cluster Configuration

You can add a second fabric interconnect to an existing Cisco UCS domain that uses a single standalone fabric interconnect. To do this, you must enable the standalone fabric interconnect for cluster operation by configuring it with the virtual IP or IPv6 address of the cluster, and then add the second fabric interconnect to the cluster.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# connect local-mgmt	Enters local management mode.
Step 2	UCS-A(local-mgmt) # enable cluster { <i>virtual-ip-addr virtual-ip6-addr</i> }	Enables cluster operation on the standalone fabric interconnect with the specified IPv4 or IPv6 address. When you enter this command, you are prompted to confirm that you want to enable cluster operation. Type yes to confirm. The IP address must be the virtual IPv4 or IPv6 address for the cluster configuration, not the IP address assigned to the fabric interconnect that you are adding to the cluster.

The following example enables a standalone fabric interconnect with a virtual IPv4 address of 192.168.1.101 for cluster operation:

```
UCS-A# connect local-mgmt
UCS-A(local-mgmt)# enable cluster 192.168.1.101
This command will enable cluster mode on this setup. You cannot change it
back to stand-alone. Also, any GUI or KVM sessions may be terminated. Are you sure you want
to continue? (yes/no): yes
UCS-A(local-mgmt)#
```

The following example enables a standalone fabric interconnect with a virtual IPv6 address of 2001::109 for cluster operation:

```
UCS-A# connect local-mgmt
UCS-A(local-mgmt)# enable cluster ipv6 2001::109
This command will enable IPv6 cluster mode on this setup. You cannot change it
back to stand-alone. Also, any GUI or KVM sessions may be terminated. Are you sure you want
to continue? (yes/no): yes
UCS-A(local-mgmt)#
```

What to Do Next

Add the second fabric interconnect to the cluster.

Changing the System Name

Procedure

	Command or Action	Purpose
Step 1	UCS-A # scope system	Enters system mode.
Step 2	UCS-A /system # set name name	Sets the system name.
Step 3	UCS-A /system # commit-buffer	Commits the transaction to the system configuration.

The name is updated on both fabric interconnects within about 30 seconds after the transaction is committed.

The following example changes the system name and commits the transaction:

```
UCS-A# scope system
UCS-A /system* # set name SanJose5
UCS-A /system* # commit-buffer
UCS-A /system #
```

Changing the Management Subnet of a Cluster

When changing the IPv4 management subnet in a cluster configuration, you must change the following three IPv4 addresses simultaneously and you must configure all three in the same subnet:

- Management port IP address for fabric interconnect A
- Management port IP address for fabric interconnect B
- Cluster IP (virtual IP) address

Procedure

	Command or Action	Purpose
Step 1	UCS-A# scope fabric-interconnect a	Enters fabric interconnect mode for fabric A.
Step 2	UCS-A /fabric-interconnect # set out-of-band ip ip-address netmask netmask gw gateway-ip-address	Sets the IP address, network mask, and gateway IP address of the fabric interconnect.
Step 3	UCS-A /fabric-interconnect # scope fabric-interconnect b	Enters fabric interconnect mode for fabric B.
Step 4	UCS-A /fabric-interconnect # set out-of-band ip ip-address netmask netmask gw gateway-ip-address	Sets the IP address, netmask, and gateway IP address of the fabric interconnect.
Step 5	UCS-A /fabric-interconnect # scope system	Enters system mode.
Step 6	UCS-A /system # set virtual-ip vip-address	Sets the virtual IP address for the cluster.
Step 7	UCS-A /system # commit-buffer	Commits the transaction to the system configuration.

When you commit the transaction, you are disconnected from the management session. Reconnect at the new management IP address.

This example changes both fabric-interconnect IP addresses, changes the virtual IP address, and commits the transaction, disconnecting the session:

```
UCS-A# scope fabric-interconnect a
UCS-A /fabric-interconnect # set out-of-band ip 192.0.2.111 netmask 255.255.255.0 gw 192.0.2.1
UCS-A /fabric-interconnect* # scope fabric-interconnect b
UCS-A /fabric-interconnect* # set out-of-band ip 192.0.2.112 netmask 255.255.255.0 gw
192.0.2.1
UCS-A /fabric-interconnect* # scope system
```

```
UCS-A /system* # set virtual-ip 192.0.2.113
UCS-A /system* # commit-buffer
```

Changing the Management Prefix of a Cluster

When changing the IPv6 management prefix in a cluster configuration, you must change the following three IPv6 addresses simultaneously and you must configure all three with the same network prefix:

- Management port IPv6 address for fabric interconnect A
- Management port IPv6 address for fabric interconnect B
- Cluster IPv6 (virtual IPv6) address

Procedure

	Command or Action	Purpose
Step 1	UCS-A# scope fabric-interconnect a	Enters fabric interconnect mode for fabric A.
Step 2	UCS-A fabric-interconnect # scope ipv6-config	Enters IPv6 configuration mode for fabric A.
Step 3	UCS-A fabric-interconnect/ ipv6-config # set out-of-band ipv6 ipv6-addr ipv6-gw ipv6-gw-addr ipv6-prefix prefix	Sets the management IPv6 address, gateway IPv6 address, and network prefix for fabric A.
Step 4	UCS-A fabric-interconnect/ipv6-config # scope fabric-interconnect b	Enter fabric interconnect mode for fabric B.
Step 5	UCS-A fabric-interconnect/ # scope ipv6-config	Enter IPv6 configuration mode for fabric B.
Step 6	UCS-A/fabric-interconnect/ipv6-config # set out-of-band ipv6 ipv6-addr ipv6-gw ipv6-gw-addr ipv6-prefix prefix	Sets the management IPv6 address, gateway IPv6 address, and network prefix for fabric B.
Step 7	UCS-A/fabric-interconnect/ipv6-config # scope system	Enters system mode.
Step 8	UCS-A/system # set virtual-ip ipv6 virtual-ip-addr	Sets the virtual IPv6 address for the cluster.
Step 9	UCS-A/system # commit-buffer	Commits the transaction to the system configuration.

When you commit the transaction, you are disconnected from the management session. Reconnect at the new management IPv6 address.

This example changes both management IPv6 addresses, changes the virtual IPv6 address, and commits the transaction:

```
UCS-A# scope fabric-interconnect a
UCS-A /fabric-interconnect # scope ipv6-config
UCS-A /fabric-interconnect/ipv6-config # set out-of-band ipv6 2001:10::157
```

```

UCS-A /fabric-interconnect/ipv6-config* # set out-of-band ipv6-gw 2001:10::1
UCS-A /fabric-interconnect/ipv6-config* # set out-of-band ipv6-prefix 64
UCS-A /fabric-interconnect/ipv6-config* # scope fabric-interconnect b
UCS-A /fabric-interconnect* # scope ipv6-config
UCS-A /fabric-interconnect/ipv6-config* # set out-of-band ipv6 2001:10::158
UCS-A /fabric-interconnect/ipv6-config* # set out-of-band ipv6-gw 2001:10::1
UCS-A /fabric-interconnect/ipv6-config* # set out-of-band ipv6-prefix 64
UCS-A /fabric-interconnect/ipv6-config* # scope system
UCS-A /system* # set virtual-ip ipv6 2001:10::156
UCS-A /system* # commit-buffer
UCS-A /system #

```

Configuring the Information Policy on the Fabric Interconnect

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	UCS-A/system/info-policy # show	(Optional) Displays if the information policy is enabled or disabled.
Step 4	UCS-A/system/info-policy # enable	Determines if the information policy can be enabled on the fabric interconnect.
Step 5	UCS-A/system/info-policy* # commit-buffer	Enables the information policy on the fabric interconnect.

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	UCS-A/system/info-policy # show	(Optional) Displays if the information policy is enabled or disabled.
Step 4	UCS-A/system/info-policy # disable	Determines if the information policy can disabled on the fabric interconnect.
Step 5	UCS-A/system/info-policy* # commit-buffer	Disables information policy on the fabric interconnect.

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 Information Policy on the Fabric Interconnect

You can view the information policy state of 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	UCS-A/system/info-policy # show	Displays if the information policy is enabled or disabled.

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

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

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.

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(SS1140305YK)
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.

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 pwnn: 20:02:00:05:9b:22:ad:C0
Fabric nwnn: 20:64:00:05:9b:22:ad:C1
My pwnn: 20:41:00:0d:ec:ee:dd:00
My nwnn: 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.

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 2.2(4) 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.

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

- 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 other Fabric Interconnect.



Note Fabric evacuation is supported only with the following:

- Manual install
- Cluster configuration

Stopping Traffic on 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 # 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 irrespective of its current evacuation state.
Step 3	UCS-A /fabric-interconnect # commit-buffer	Commits the transaction to the system configuration.

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 at 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.

This example shows how to display the detailed status of a Fabric Interconnect.



Note

Admin Evacuation and Oper Evacuation 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 at an IOM

Procedure

	Command or Action	Purpose
Step 1	UCS-A# scope chassis <i>chassis-num</i>	Enters chassis mode for the specified chassis.

	Command or Action	Purpose
Step 2	UCS-A /chassis # scope iom <i>iom-id</i>	Enters chassis IOM mode for the specified IOM.
Step 3	UCS-A /chassis/iom # show detail	Displays details about the specified IOM.

This example shows how to display the detailed status of an IOM.



Note Oper Evacuation shows the operational status of evacuation at 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 <i>server-id</i>	Shows the network circuit information for the service profile associated with the specified server.

This example shows the VIF 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#
```

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



Note

- After fail over, 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 fabric interconnect mode for the specified Fabric Interconnect.
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.

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
```

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 pinned or hard pinned) 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 are 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. Switch mode is not the default Ethernet switching mode, and should be used only if the fabric interconnect is directly connected to a router, or if either of the following are 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.

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.

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 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 pinned or hard pinned) 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 denying uplink ports from receiving traffic from one another.

End-host mode is synonymous with N Port Virtualization (NPV) mode. This mode is the default Fibre Channel Switching mode.



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 the traditional 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).

Switch mode is not the default Fibre Channel switching mode.



Note

In Fibre Channel switch mode, SAN pin groups are irrelevant. Any existing SAN pin groups are ignored.

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 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.

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 #
```

