Equipment Policies

Chassis/FEX Discovery Policy

The chassis/FEX discovery policy determines how the system reacts when you add a new chassis or FEX. Cisco UCS Manager uses the settings in the chassis/FEX discovery policy to determine the minimum threshold for the number of links between the chassis or FEX and the fabric interconnect and whether to group links from the IOM to the fabric interconnect in a fabric port channel.

In a Cisco UCS Mini (Cisco UCS 6324 Fabric Interconnect) setup, chassis discovery policy is supported only on the extended chassis.

Chassis Links

If you have a Cisco UCS domain with some of the chassis' wired with one link, some with two links, some with four links, and some with eight links, Cisco recommends configuring the chassis/FEX discovery policy for the minimum number links in the domain so that Cisco UCS Manager can discover all chassis.

Tip To establish the highest available chassis connectivity in a Cisco UCS domain where Fabric Interconnect is connected to different types of IO Modules supporting different max number of uplinks, select platform max value. Setting the platform max ensures that Cisco UCS Manager discovers the chassis including the connections and servers only when the maximum supported IOM uplinks are connected per IO Module.

After the initial discovery of a chassis, if chassis/FEX discovery policy changes are done, acknowledge IO Modules rather than the entire Chassis to avoid disruption. The discovery policy changes can include increasing the number of links between Fabric Interconnect and IO Module, or changes to the Link Grouping preference.

Make sure that you monitor for faults before and after the IO Module acknowledgement to ensure that the connectivity is restored before proceeding to the other IO Module for the chassis.

Cisco UCS Manager cannot discover any chassis that is wired for fewer links than are configured in the chassis/FEX discovery policy. For example, if the chassis/FEX discovery policy is configured for four links,

Cisco UCS Manager cannot discover any chassis that is wired for one link or two links. Re-acknowledgement of the chassis resolves this issue.

The following table provides an overview of how the chassis/FEX discovery policy works in a multi-chassis Cisco UCS domain:

Table 1: Chassis/FEX Discovery Policy and Chassis Links

Number of Links Wired for the Chassis	1-Link Discovery Policy	2-Link Discovery Policy	4-Link Discovery Policy	8-Link Discovery Policy	Platform-Max Discovery Policy
1 link between IOM and fabric interconnects	Chassis is discovered by Cisco UCS Manager and added to the Cisco UCS domain as a chassis wired with 1 link.	Chassis connections and servers cannot be discovered by Cisco UCS Manager and are not added to the Cisco UCS domain.	Chassis connections and servers cannot be discovered by Cisco UCS Manager and are not added to the Cisco UCS domain.	Chassis connections and servers cannot be discovered by Cisco UCS Manager and are not added to the Cisco UCS domain.	Chassis connections and servers cannot be discovered by Cisco UCS Manager and are not added to the Cisco UCS domain.
2 links between IOM and fabric interconnects	Chassis is discovered by Cisco UCS Manager and added to the Cisco UCS domain as a chassis wired with 1 link. After initial discovery, reacknowledge the chassis and Cisco UCS Manager recognizes and uses the additional links.	Chassis is discovered by Cisco UCS Manager and added to the Cisco UCS domain as a chassis wired with 2 link.	Chassis connections and servers cannot be discovered by Cisco UCS Manager and are not added to the Cisco UCS domain.	Chassis connections and servers cannot be discovered by Cisco UCS Manager and are not added to the Cisco UCS domain.	Chassis connections and servers cannot be discovered by Cisco UCS Manager and are not added to the Cisco UCS domain.

Number of Links Wired for the Chassis	1-Link Discovery Policy	2-Link Discovery Policy	4-Link Discovery Policy	8-Link Discovery Policy	Platform-Max Discovery Policy
4 links between IOM and fabric interconnects	Chassis is discovered by Cisco UCS Manager and added to the Cisco UCS domain as a chassis wired with 1 link. After initial discovery, reacknowledge the chassis and Cisco UCS Manager recognizes and uses the additional links.	Chassis is discovered by Cisco UCS Manager and added to the Cisco UCS domain as a chassis wired with 2 links. After initial discovery, reacknowledge the chassis and Cisco UCS Manager recognizes and uses the additional links.	Chassis is discovered by Cisco UCS Manager and added to the Cisco UCS domain as a chassis wired with 4 link.	Chassis connections and servers cannot be discovered by Cisco UCS Manager and are not added to the Cisco UCS domain.	If the IOM has 4 links, the chassis is discovered by Cisco UCS Manager and added to the Cisco UCS domain as a chassis wired with 4 links. **Note** If the FEX status shows accessibility problem then reacknowledge the chassis a decommissioning/recommiss FEX. If the IOM has 8 links, the chassis is not fully discovered by Cisco UCS Manager.
8 links between IOM and fabric interconnects	Chassis is discovered by Cisco UCS Manager and added to the Cisco UCS domain as a chassis wired with 1 link. After initial discovery, reacknowledge the chassis and Cisco UCS Manager recognizes and uses the additional links.	Chassis is discovered by Cisco UCS Manager and added to the Cisco UCS domain as a chassis wired with 2 links. After initial discovery, reacknowledge the chassis and Cisco UCS Manager recognizes and uses the additional links.	Chassis is discovered by Cisco UCS Manager and added to the Cisco UCS domain as a chassis wired with 4 links. After initial discovery, reacknowledge the chassis and Cisco UCS Manager recognizes and uses the additional links.	Chassis is discovered by Cisco UCS Manager and added to the Cisco UCS domain as a chassis wired with 8 links.	Chassis is discovered by Cisco UCS Manager and added to the Cisco UCS domain as a chassis wired with 8 links.

Link Grouping

For hardware configurations that support fabric port channels, link grouping determines whether all of the links from the IOM to the fabric interconnect are grouped in to a fabric port channel during chassis discovery.

If the link grouping preference is set to **Port Channel**, all of the links from the IOM to the fabric interconnect are grouped in a fabric port channel. If set to **None**, links from the IOM are pinned to the fabric interconnect.

☞

Important For Cisco UCS 6454 Fabric Interconnects, the link grouping preference is always set to **Port Channel**.

After a fabric port channel is created through Cisco UCS Manager, you can add or remove links by changing the link group preference and re-acknowledging the chassis, or by enabling or disabling the chassis from the port channel.

Note The link grouping preference only takes effect if both sides of the links between an IOM or FEX and the fabric interconnect support fabric port channels. If one side of the links does not support fabric port channels, this preference is ignored and the links are not grouped in a port channel.

Multicast Hardware Hash

In a port channel, by default, ingress multicast traffic on any port in the fabric interconnect (FI) selects a particular link between the IOM and the fabric interconnect to egress the traffic. To reduce potential issues with the bandwidth, and to provide effective load balancing of the ingress multicast traffic, hardware hashing is used for multicast traffic. When multicast hardware hashing is enabled, all links between the IOM and the fabric interconnect in a port channel can be used for multicast traffic.

Note Cisco UCS 6454 Fabric Interconnect do not support multicast hardware hashing.

Pinning

Pinning in Cisco UCS is only relevant to uplink ports. If you configure **Link Grouping Preference** as **None** during chassis discovery, the IOM forwards traffic from a specific server to the fabric interconnect through its uplink ports by using static route pinning.

The following table showcases how pinning is done between an IOM and the fabric interconnect based on the number of active fabric links between the IOM and the fabric interconnect.

Table 2: Pinning on an IOM

Number of Active Fabric Links	Server slot pinned to fabric link
1-Link	All the HIF ports are pinned to the active link
2-Link	1,3,5,7 to link-1 2,4,6,8 to link-2

Number of Active Fabric Links	Server slot pinned to fabric link
4-Link	1,5 to link-1
	2,6 to link-2
	3,7 to link-3
	4,8 to link-4
8-Link (Applies only to 2208XP)	1 to link-1
	2 to link-2
	3 to link-3
	4 to link-4
	5 to link-5
	6 to link-6
	7 to link-7
	8 to link-8

Only 1,2,4 and 8 links are supported. 3,5,6, and 7 links are not valid configurations.

Port-Channeling

While pinning traffic from a specific server to an uplink port provides you with greater control over the unified fabric and ensures optimal utilization of uplink port bandwidth, it could also mean excessive traffic over certain circuits. This issue can be overcome by using port channeling. Port channeling groups all links between the IOM and the fabric interconnect into one port channel. The port channel uses a load balancing algorithm to decide the link over which to send traffic. This results in optimal traffic management.

Cisco UCS supports port-channeling only through the Link Aggregation Control Protocol (LACP). For hardware configurations that support fabric port channels, link grouping determines whether all of the links from the IOM to the fabric interconnect are grouped into a fabric port channel during chassis discovery. If the **Link Grouping Preference** is set to **Port Channel**, all of the links from the IOM to the fabric interconnect are grouped in a fabric port channel. If this parameter is set to **None**, links from the IOM to the fabric interconnect are not grouped in a fabric port channel.

Once a fabric port channel is created, links can be added or removed by changing the link group preference and reacknowledging the chassis, or by enabling or disabling the chassis from the port channel.

Configuring the Chassis/FEX Discovery Policy

Procedure

Step 1	In the **Navigation** pane, click **Equipment**.
Step 2	Click the **Equipment** node.
Step 3	In the **Work** pane, click the **Policies** tab.

Step 4   Click the **Global Policies** subtab.

Step 5   In the **Chassis/FEX Discovery Policy** area, specify the action and the link grouping preference.

    a)   In the **Action** field, specify the minimum threshold for the number of links between the chassis or FEX and the fabric interconnect.

    b)   In the **Link Grouping Preference** field, specify whether the links from the IOMs or FEXes to the fabric interconnects are grouped in a port channel.

> **Note**
> - In a setup with Cisco UCS 6454 Fabric Interconnects, the **Link Grouping Preference** value for Chassis/FEX Discovery Policy is not user configurable. The value is set to **Port Channel**.
> - For Cisco UCS Manager to discover VIC 1455 and VIC 1457, **Link Grouping Preference** must be configured as **Port Channel**.

    c)   In the **Multicast Hardware Hash** field, specify whether all the links from the IOMs or FEXes to the fabric interconnects in a port channel can be used for multicast traffic.

        Cisco UCS 6454 Fabric Interconnects do not support **Multicast Hardware Hash**.

Step 6   Click **Save Changes**.

What to do next

To customize fabric port channel connectivity for a specific chassis, configure the chassis connectivity policy.

Chassis Connectivity Policy

The chassis connectivity policy determines the whether a specific chassis is included in a fabric port channel after chassis discovery. This policy is helpful for users who want to configure one or more chassis differently from what is specified in the global chassis discovery policy. The chassis connectivity policy also allows for different connectivity modes per fabric interconnect, further expanding the level of control offered with regards to chassis connectivity.

By default, the chassis connectivity policy is set to global. This means that connectivity control is configured when the chassis is newly discovered, using the settings configured in the chassis discovery policy. Once the chassis is discovered, the chassis connectivity policy controls whether the connectivity control is set to none or port channel.

> ☞
>
> **Important**   The 40G backplane setting is not applicable for 22xx IOMs.

The chassis connectivity policy is created by Cisco UCS Manager only when the hardware configuration supports fabric port channels.

> ☞
>
> **Important**   For Cisco UCS 6454 Fabric Interconnects , the chassis connectivity policy is always **Port Channel**.

In a Cisco UCS Mini setup, the creation of a chassis connectivity policy is supported only on the extended chassis.

Configuring a Chassis Connectivity Policy

☞

Important   The 40G backplane setting is not applicable for 22xx IOMs.

Changing the connectivity mode for a chassis might result in decreased VIF namespace.

⚠

Caution   Changing the connectivity mode for a chassis results in chassis re-acknowledgement. Traffic might be disrupted during this time.

Procedure

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

Step 2   Expand **Equipment** > **Chassis**.

Step 3   Click the chassis for which you want to configure the connectivity between the IOMs and fabric interconnects.

Step 4   In the **Work** pane, click the **Connectivity Policy** tab.

Step 5   For each IOM in the chassis, choose one of the following values in the **Admin State** field for the chassis and fabric connectivity:

- **None**—No links are grouped in a port channel

- **Port Channel**—All links from an IOM to a fabric interconnect are grouped in a port channel.

    Note   Cisco UCS 6454 Fabric Interconnects support only Port Channel mode.

- **Global**—The chassis inherits this configuration from the chassis discovery policy. This is the default value.

Step 6   Click **Save Changes**.

Rack Server Discovery Policy

The rack server discovery policy determines how the system reacts when you perform any of the following actions:

- Add a new rack-mount server

- Decommission/recommission a previously added or discovered rack-mount server

Cisco UCS Manager uses the settings in the rack server discovery policy to determine whether any data on the hard disks are scrubbed and whether server discovery occurs immediately or needs to wait for explicit user acknowledgement.

Cisco UCS Manager cannot discover any rack-mount server that has not been correctly cabled and connected to the fabric interconnects. For information about how to integrate a supported Cisco UCS rack-mount server with Cisco UCS Manager, see the appropriate rack-mount server integration guide.

☞

Important   Cisco UCS VIC 1400 series 4 port adapters support 10G/25G speed.. When connecting to the Fabric Interconnects, use the same speed cables on all the adapter ports that are connected to same Fabric Interconnect. When the mix speed cables are used, rack server discovery will fail and ports may go to a suspended state. Cisco UCS Manager does not raise any faults.

Configuring the Rack Server Discovery Policy

Procedure

Step 1	In the **Navigation** pane, click **Equipment**.
Step 2	Click the **Equipment** node.
Step 3	In the **Work** pane, click the **Policies** tab.
Step 4	Click the **Global Policies** subtab.
Step 5	In the **Rack Server Discovery Policy** area, specify the action and the scrub policy that you want to occur when:

- A new rack-mount server is added

- Previously added or discovered rack-mount server is decommissioned/recommissioned

Step 6	Click **Save Changes**.

Aging Time for the MAC Address Table

To efficiently switch packets between ports, the fabric interconnect maintains a MAC address table. It dynamically builds the MAC address table by using the MAC source address from the packets received and the associated port on which the packets were learned. The fabric interconnect uses an aging mechanism, defined by a configurable aging timer, to determine how long an entry remains in the MAC address table. If an address remains inactive for a specified number of seconds, it is removed from the MAC address table.

You can configure the amount of time (age) that a MAC address entry (MAC address and associated port) remains in the MAC address table.

Configuring the Aging Time for the MAC Address Table

Procedure

Step 1	In the **Navigation** pane, click **Equipment**.
Step 2	Click the **Equipment** node.
Step 3	In the **Work** pane, click the **Policies** tab.
Step 4	Click the **Global Policies** subtab.
Step 5	In the **MAC Address Table Aging** area, specify the aging time and the length of time.
Step 6	Click **Save Changes**.