Network Policies

Network Control Policy

This policy configures the network control settings for the Cisco UCS domain, including the following:

- Whether the Cisco Discovery Protocol (CDP) is enabled or disabled
- How the virtual interface (VIF) behaves if no uplink port is available in end-host mode
- The action that Cisco UCS Central takes on the remote Ethernet interface, vEthernet interface , or vFibre Channel interface when the associated border port fails
- Whether the server can use different MAC addresses when sending packets to the fabric interconnect
- Whether MAC registration occurs on a per-VNIC basis or for all VLANs

Action on Uplink Fail

By default, the **Action on Uplink Fail** property in the network control policy is configured with a value of link-down. For adapters such as the Cisco UCS M81KR Virtual Interface Card, this default behavior directs Cisco UCS Central to bring the vEthernet or vFibre Channel interface down if the associated border port fails. For Cisco UCS systems using a non-VM-FEX capable converged network adapter that supports both Ethernet and FCoE traffic, such as Cisco UCS CNA M72KR-Q and the Cisco UCS CNA M72KR-E, this default

behavior directs Cisco UCS Central to bring the remote Ethernet interface down if the associated border port fails. In this scenario, any vFibre Channel interfaces that are bound to the remote Ethernet interface are brought down as well.

Note if your implementation includes those types of non-VM-FEX capable converged network adapters mentioned in this section and the adapter is expected to handle both Ethernet and FCoE traffic, we recommend that you configure the **Action on Uplink Fail** property with a value of warning. Note that this configuration might result in an Ethernet teaming driver not being able to detect a link failure when the border port goes down.

MAC Registration Mode

MAC addresses are installed only on the native VLAN by default, which maximizes the VLAN port count in most implementations.

Note If a trunking driver is being run on the host and the interface is in promiscuous mode, we recommend that you set the Mac Registration Mode to All VLANs.

Creating or Editing a Network Control Policy

Step 1 In the **Actions** bar, type **Create Network Control Policy** and press Enter.

Step 2 In the **Network Control Policy** dialog box, choose whether to create a default or appliance network control policy.

Step 3 Choose the **Organization** where you want to create the policy, and enter the **Name** and optional **Description**.

The name is case sensitive.

Step 4 Choose whether to enable **Cisco Discovery Protocol (CDP)**.

Step 5 Select values for **Action on Uplink Failure**, **MAC Address Registration**, and **MAC Address Forging**.

Step 6 Choose whether to enable or disable **Link Layer Discovery Protocol (LLDP) Transmit** and **Link Layer Discovery Protocol (LLDP) Receive**.

Step 7 Click **Create**.

Deleting a Network Control Policy

Step 1 On the menu bar, click **Network**.

Step 2 In the **Navigation** Pane, expand **Network** > **Policies** > **root**.

If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Expand **Network Control Policies**.

Step 4 Right-click the policy that you want to delete and choose **Delete**.

Step 5 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

Ethernet Adapter Policy

Ethernet adapter policies govern the host-side behavior of the adapter, including how the adapter handles traffic. For example, you can use these policies to change default settings for the following:

- Queues
- Interrupt handling
- Performance enhancement
- RSS hash
- Failover in an cluster configuration with two fabric interconnects

Operating System Specific Adapter Policies

By default, Cisco UCS provides a set of Ethernet adapter policies. These policies include the recommended settings for each supported server operating system. Operating systems are sensitive to the settings in these policies. Storage vendors typically require non-default adapter settings. You can find the details of these required settings on the support list provided by those vendors.

Note We recommend that you use the values in these policies for the applicable operating system. Do not modify any of the values in the default policies unless directed to do so by Cisco Technical Support.

If you are creating an Ethernet adapter policy (instead of using the default Windows adapter policy) for a Windows operating system, you must use the following formulas to calculate values that work with Windows:

Completion Queues = Transmit Queues + Receive Queues

Interrupt Count = (Completion Queues + 2) rounded up to nearest power of 2

For example, if Transmit Queues = 1 and Receive Queues = 8 then:

Completion Queues = 1 + 8 = 9

Interrupt Count = (9 + 2) rounded up to the nearest power of 2 = 16

Creating and Editing an Ethernet Adapter Policy

Step 1 In the **Actions** bar, type **Create Ethernet Adapter Policy** and press Enter.

Step 2 In the **Ethernet Adapter Policy** dialog box, In **Basic**, choose the **Organization** where you want to create the ethernet adapter policy.

Step 3 Enter the **Name** and optional **Description**.

Step 4 In **Resources**, complete the following:

a) In **Transmit Queues**, enter the number of transmit queue resources to allocate.

b) In **Transmit Queue Ring Size**, enter the number of descriptors in each transmit queue.
c) In **Receive Queues**, enter the number of receive queue resources to allocate.
d) In **Receive Queues Ring Size**, enter the number of descriptors in each receive queue.
e) In **Completion Queues**, enter the number of completion queue resources to allocate. In general, the number of completion queue resources you allocate should be equal to the number of transmit queue resources, plus the number of receive queue resources.
f) In **Interrupts**, enter the number of interrupt resources to allocate. In general, this value should be equal to the number of completion queue resources.

Step 5 In **Settings**, complete the following:

a) Choose whether to enable **Transmit Checksum Offloading**, **Receive Checksum Offloading**, **TCP Segmentation Offloading**, **Large TCP Receive Offloading**, **Receive Side Scaling**, **Virtual Extensible LAN (VXLAN)**, **RDMA over Converged Ethernet (RoCE)**, **Accelerated Receive Flow Steering (ARF)**, and **NVGRE**.
b) Select an **Interrupt Mode**.
c) Enter the **Interrupt Timer** value in microseconds.
d) Select the **Interrupt Coalescing Type**.
e) Enter the **Failback Timeout** in seconds.

Step 6 Click **Create**.

Dynamic vNIC Connection Policy

The dynamic vNIC connection policy determines how the connectivity between VMs and dynamic vNICs is configured. This policy is required for Cisco UCS domains that include servers with VIC adapters on which you have installed VMs and configured dynamic vNICs.

Each dynamic vNIC connection policy includes an Ethernet adapter policy and designates the number of vNICs that can be configured for any server associated with a service profile that includes the policy.

Note Server Migration:

- If you migrate a server that is configured with dynamic vNICs or another migration tool, the dynamic interface used by the vNICs fails and Cisco UCS Central notifies you of that failure.
- When the server comes back up, Cisco UCS Central assigns new dynamic vNICs to the server. If you are monitoring traffic on the dynamic vNIC, you must reconfigure the monitoring source.

Creating or Editing a Dynamic vNIC Connection Policy

Step 1 In the **Actions** bar, type **Create Dynamic vNIC Connection Policy** and press Enter.

Step 2 In the **Dynamic vNIC Connection Policy** dialog box, choose the **Organization** in which you want to create the dynamic vNIC connection policy.

Step 3 Enter a **Name** and optional **Description**.

The policy name is case sensitive.

Step 4 Enter the number of dynamic vNICS that you want to create.

Step 5 Select the protection mode that you want to use.

Step 6 Select the adapter profile to be associated with this policy.

The profile must already exist to be included in the **Ethernet Adapter** drop-down list.

Step 7 Click **Create**.

usNIC Connection Policy

The Cisco user-space NIC (Cisco usNIC) connection policy page displays the details of your usNIC connection policy and what service profiles it is associated with.

Creating or Editing a usNIC Connection Policy

Step 1 In the **Actions** bar, type **Create usNIC Connection Policy** and press Enter.

Step 2 In the **usNIC Connection Policy** dialog box, choose the **Organization** in which you want to create the policy.

Step 3 Enter a **Name** and optional **Description**.

The policy name is case sensitive.

Step 4 Enter the **Number of usNICs** that you want to create.

Step 5 Select the **Adapter Policy** that you want to specify for the usNIC.

We recommend that you use the global-usNIC adapter policy, which is created by default.

Step 6 Click **Create**.

VMQ Connection Policy

VMQ provides improved network performance to the entire management operating system. From Cisco UCS Central you can create a VMQ connection policy for a vNIC on a service profile. To configure the VMQ vNIC on a service profile for a server, at least one adapter in the server must support VMQ. Make sure the servers have at least one the following adapters installed:

- UCS-VIC-M82-8P
- UCSB-MLOM-40G-01
- UCSC-PCIE-CSC-02

You must have one of the following Operating systems to use VMQ:

- Windows 2012
- Windows 2012R2

When you select the vNIC connection policy for a service profile, make sure to select one of the three options such as Dynamic, usNIC or VMQ connection policy for the vNIC. You can apply only any one of the vNIC connection policies on a service profile at any one time.

When you have selected VMQ policy on the vNIC for a service profile, you must also have the following settings in the service profile:

- Select SRIOV in the BIOS policy.
- Select Windows in the Adapter policy.

Configuring a VMQ vNIC connection policy involves the following:

- Creating a VMQ connection policy
- Creating a static vNIC in a service profile
- Applying the VMQ connection policy to the vNIC

Creating or Editing a VMQ Connection Policy

Step 1 In the **Actions** bar, type **Create VMQ Connection Policy** and press Enter.

Step 2 In the **VMC Connection Policy** dialog box, click **Basic** and choose the **Organization** in which you want to create the policy.

Step 3 Enter the **Name** and optional **Description**.

The name is case sensitive.

Step 4 In **Number of VMQs** filed, enter a number between 1 to 128.

Step 5 In the Number of Interrupts field, enter a number between 1 to 128.

Step 6 Click **Create**.

What to do next

Associate the VMQ connection policy with a vNIC, vNIC template, or LAN connectivity policy.

LAN Connectivity Policy

LAN connectivity policies determine the connections and the network communication resources between the server and the LAN on the network. These policies use pools to assign MAC addresses to servers and to identify the vNICs that the servers use to communicate with the network.

Note These policies are included in service profiles and service profile templates, and can be used to configure multiple servers. So, using static IDs in connectivity policies is not recommended.

Privileges Required for LAN and SAN Connectivity Policies

Connectivity policies enable users without network or storage privileges to create and modify service profiles and service profile templates with network and storage connections. However, users must have the appropriate network and storage privileges to create connectivity policies.

Privileges Required to Create Connectivity Policies

Connectivity policies require the same privileges as other network and storage configurations. For example, you must have at least one of the following privileges to create connectivity policies:

- admin—Can create LAN and SAN connectivity policies
- ls-server—Can create LAN and SAN connectivity policies
- ls-network—Can create LAN connectivity policies
- ls-storage—Can create SAN connectivity policies

Privileges Required to Add Connectivity Policies to Service Profiles

After the connectivity policies have been created, a user with ls-compute privileges can include them in a service profile or service profile template. However, a user with only ls-compute privileges cannot create connectivity policies.

Creating or Editing a LAN Connectivity Policy

Step 1 In the **Actions** bar, type **Create LAN Connectivity Policy** and press Enter.

Step 2 In the **LAN Connectivity Policy** dialog box, click **Basic** and choose the **Organization** in which you want to create the policy.

Step 3 Enter the **Name** and optional **Description**.

The name is case sensitive.

Step 4 In **vNICs**, create one or more vNICs and select these properties:

- **Basic**— Select the **Fabric Interconnect**, **Fabric Failover** option (Enabled or diasabled), **MTU**, and the **CDN Source** (vNIC Name or User Defined Name for the CDN source.
- **MAC Address**— Select the MAC address from a pool.
- **VLANs**— Specify or search for the VLAN name. You can click **Search** and specify a VLAN name to filter the results of VLANs displayed. You can search with a partial or full name of the VLAN that you want to select. For example, you can search for *VLAN100* to filter the list of VLANs with names containing VLAN100. You cannot set multiple native VLANs for a vNIC in a Service Profile. When you click on **Set as Native**, a **Configuration Error** results.
- **VLAN Groups**— Specify the VLAN group name that you have created to group the VLANs. You can add multiple VLAN groups and VLANs you want to associate with the policy.

  Note A VALN group is resolved only if the service profile referencing the template is associated. Once the service profile is associated, the VLAN group gets resolved based on the name on the Domain on the associated server.

- **Policies**— Select the policy that you want to assign to the vNIC.

You can manually create the vNIC, use a vNIC template, or create a redundancy template pair. For more information, see vNIC Templates.

Step 5 In **iSCSI vNICs**, enter the **iSCSI vNIC** and enter the appropriate properties values.

Note If you create a LAN Connectivity Policy in the HTML5 GUI, any iSCSI vNIC parameters that you set on the iSCSI vNICS in the policy can only be updated in the HTML5 GUI.

Step 6 Click **Create**.

Creating a vNIC for a LAN Connectivity Policy

Step 1 On the menu bar, click **Network**.

Step 2 In the **Navigation** Pane, expand **Network** > **Policies** > **root**.

If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Expand **LAN Connectivity Policies**.

Step 4 Select the LAN connectivity policy for which you want to create a vNIC.

Step 5 In the **Work** pane, click the **General** tab.

Step 6 In the **vNICs** area, click **Create vNIC**.

Step 7 In the **Create vNIC** dialog box, enter the name, select a **MAC Address Assignment**, and check the **Use vNIC Template** check box if you want to use an existing vNIC template.

You can also create a MAC pool from this area.

Step 8 In the **Details** area, choose the **Fabric ID**, select the VLANs you want to use, and enter the **MTU**.

You can click **Search** and specify a VLAN name to filter the results of VLANs displayed. You can search with a partial or full name of the VLAN that you want to select. For example, you can search for *VLAN100* to filter the list of VLANs with names containing VLAN100.

Step 9 In the **Pin Group** area, choose a **Pin Group Name**.

Step 10 In the **Operational Parameters** area, choose a **Stats Threshold Policy**.

You can also create a threshold policy from this area.

Step 11 In the **Adapter Performance Profile** area, choose an **Adapter Policy**, **QoS Policy**, and a **Network Control Policy**.

You can also create an ethernet adapter policy, a QoS policy, and a network control policy from this area.

Step 12 Click **OK**.

Creating an iSCSI vNIC for a LAN Connectivity Policy

Step 1 On the menu bar, click **Network**.

Step 2 In the **Navigation** Pane, expand **Network** > **Policies** > **root**.

If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Expand **LAN Connectivity Policies**.

Step 4 Select the LAN connectivity policy for which you want to create an iSCSI vNIC.

Step 5 In the **Work** pane, click the **General** tab.

Step 6 In the **iSCSI vNICs** area, click **Create iSCSI vNIC**.

Step 7 In the **Create iSCSI vNIC** dialog box, enter the name, choose the **Overlay vNIC**, **iSCSI Adapter Policy**, and **VLAN** from the drop-down lists, and select a **MAC Address Assignment**.

You can also create an iSCSI adapter policy and a MAC pool from this dialog box.

You can click **Search** and specify a VLAN name to filter the results of VLANs displayed. You can search with a partial or full name of the VLAN that you want to select. For example, you can search for *VLAN100* to filter the list of VLANs with names containing VLAN100.

Step 8 Click **OK**.

Deleting a LAN Connectivity Policy

Step 1 On the menu bar, click **Network**.

Step 2 In the **Navigation** Pane, expand **Network** > **Policies** > **root**.

If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Expand **LAN Connectivity Policies**.

Step 4 Right-click the policy that you want to delete and choose **Delete**.

Step 5 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

Deleting a vNIC from a LAN Connectivity Policy

Step 1 On the menu bar, click **Network**.

Step 2 In the **Navigation** Pane, expand **Network** > **Policies** > **root**.

If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Expand **LAN Connectivity Policies**.

Step 4 Select the policy for which you want to delete the vNIC.

Step 5 In the **Work** pane, click the **General** tab.

Step 6 In the **vNICs** table, click the vNIC you want to delete.

Step 7 On the **vNICs** table icon bar, click **Delete**.

Step 8 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

Deleting an iSCSI vNIC from a LAN Connectivity Policy

Step 1 On the menu bar, click **Network**.

Step 2 In the **Navigation** Pane, expand **Network** > **Policies** > **root**.

If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Expand **LAN Connectivity Policies**.

Step 4 Select the policy for which you want to delete the iSCSI vNIC.

Step 5 In the **Work** pane, click the **General** tab.

Step 6 In the **iSCSI vNICs** table, click the vNIC you want to delete.

Step 7 On the **iSCSI vNICs** table icon bar, click **Delete**.

Step 8 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

UniDirectional Link Detection (UDLD)

UniDirectional Link Detection (UDLD) is a Layer 2 protocol that enables devices connected through fiber-optic or twisted-pair Ethernet cables to monitor the physical configuration of the cables and detect when a unidirectional link exists. All connected devices must support UDLD for the protocol to successfully identify and disable unidirectional links. When UDLD detects a unidirectional link, it marks the link as unidirectional. Unidirectional links can cause a variety of problems, including spanning-tree topology loops.

UDLD works with the Layer 1 mechanisms to determine the physical status of a link. At Layer 1, autonegotiation takes care of physical signaling and fault detection. UDLD performs tasks that autonegotiation cannot perform, such as detecting the identities of neighbors and shutting down misconnected interfaces. When you enable both autonegotiation and UDLD, the Layer 1 and Layer 2 detections work together to prevent physical and logical unidirectional connections and the malfunctioning of other protocols.

A unidirectional link occurs whenever traffic sent by a local device is received by its neighbor but traffic from the neighbor is not received by the local device.

Modes of Operation

UDLD supports two modes of operation: normal (the default) and aggressive. In normal mode, UDLD can detect unidirectional links due to misconnected interfaces on fiber-optic connections. In aggressive mode, UDLD can also detect unidirectional links due to one-way traffic on fiber-optic and twisted-pair links and to misconnected interfaces on fiber-optic links.

In normal mode, UDLD detects a unidirectional link when fiber strands in a fiber-optic interface are misconnected and the Layer 1 mechanisms do not detect this misconnection. If the interfaces are connected correctly but the traffic is one way, UDLD does not detect the unidirectional link because the Layer 1 mechanism, which is supposed to detect this condition, does not do so. In case, the logical link is considered undetermined, and UDLD does not disable the interface. When UDLD is in normal mode, if one of the fiber strands in a pair is disconnected and autonegotiation is active, the link does not stay up because the Layer 1 mechanisms did not detect a physical problem with the link. In this case, UDLD does not take any action, and the logical link is considered undetermined.

UDLD aggressive mode is disabled by default. Configure UDLD aggressive mode only on point-to-point links between network devices that support UDLD aggressive mode. With UDLD aggressive mode enabled, when a port on a bidirectional link that has a UDLD neighbor relationship established stops receiving UDLD packets, UDLD tries to reestablish the connection with the neighbor and administratively shuts down the affected port. UDLD in aggressive mode can also detect a unidirectional link on a point-to-point link on which no failure between the two devices is allowed. It can also detect a unidirectional link when one of the following problems exists:

- On fiber-optic or twisted-pair links, one of the interfaces cannot send or receive traffic.
- On fiber-optic or twisted-pair links, one of the interfaces is down while the other is up.
- One of the fiber strands in the cable is disconnected.

Methods to Detect Unidirectional Links

UDLD operates by using two mechanisms:

- Neighbor database maintenance

  UDLD learns about other UDLD-capable neighbors by periodically sending a hello packet (also called an advertisement or probe) on every active interface to keep each device informed about its neighbors. When the switch receives a hello message, it caches the information until the age time (hold time or time-to-live) expires. If the switch receives a new hello message before an older cache entry ages, the switch replaces the older entry with the new one.

  UDLD clears all existing cache entries for the interfaces affected by the configuration change whenever an interface is disabled and UDLD is running, whenever UDLD is disabled on an interface, or whenever the switch is reset. UDLD sends at least one message to inform the neighbors to flush the part of their caches affected by the status change. The message is intended to keep the caches synchronized.

- Event-driven detection and echoing

  UDLD relies on echoing as its detection mechanism. Whenever a UDLD device learns about a new neighbor or receives a resynchronization request from an out-of-sync neighbor, it restarts the detection window on its side of the connection and sends echo messages in reply. Because this behavior is the same on all UDLD neighbors, the sender of the echoes expects to receive an echo in reply.

  If the detection window ends and no valid reply message is received, the link might shut down, depending on the UDLD mode. When UDLD is in normal mode, the link might be considered undetermined and might not be shut down. When UDLD is in aggressive mode, the link is considered unidirectional, and the interface is shut down.

If UDLD in normal mode is in the advertisement or in the detection phase and all the neighbor cache entries are aged out, UDLD restarts the link-up sequence to resynchronize with any potentially out-of-sync neighbors.

If you enable aggressive mode when all the neighbors of a port have aged out either in the advertisement or in the detection phase, UDLD restarts the link-up sequence to resynchronize with any potentially out-of-sync neighbor. UDLD shuts down the port if, after the fast train of messages, the link state is still undetermined.

UDLD Configuration Guidelines

The following guidelines and recommendations apply when you configure UDLD:

- A UDLD-capable interface also cannot detect a unidirectional link if it is connected to a UDLD-incapable port of another switch.

- When configuring the mode (normal or aggressive), make sure that the same mode is configured on both sides of the link.
- UDLD should be enabled only on interfaces that are connected to UDLD capable devices. The following interface types are supported:
  - Ethernet uplink
  - FCoE uplink
  - Ethernet uplink port channel member
  - FCoE uplink port channel member

Creating or Editing a UDLD Link Policy

Step 1 In the **Actions** bar, type **Create UDLD Link Policy** and press Enter.

Step 2 In the **UDLD Link Policy** dialog box, click **Basic** and choose the **Organization** in which you want to create the policy.

Step 3 Enter a **Name** and optional **Description**.

The policy name is case sensitive.

Step 4 Choose whether to enable **Admin State**.

Step 5 Choose the **Mode**. This can be one of the following:

- **Normal**—UDLD can detect unidirectional links due to misconnected interfaces on fibre-optic connections.
- **Aggressive**—UDLD can detect unidirectional links due to one-way traffic on fiber-optic and twisted-pair links, as well as misconnected interfaces on fiber-optic links.

Step 6 Click **Create**.

Creating or Editing a Link Profile

Step 1 In the **Actions** bar, type **Create Link Profile** and press Enter.

Step 2 In the **Link Profile** dialog box, click **Basic** and choose the **Domain Group Location** in which you want to create the link profile.

Step 3 Enter a **Name** and optional **Description**.

The policy name is case sensitive.

Step 4 In **UDLD Link**, select the UDLD link policy that you want to associate with the link profile.

Step 5 Click **Save**.

LACP Policy

Link Aggregation combines multiple network connections in parallel to increase throughput and to provide redundancy. Cisco UCS uses Link Aggregation Control Protocol (LACP) to group uplink ethernet ports into a port channel. You can create an LACP policy in Cisco UCS Central to manage how a particular port channel uses LACP. The following port channel types support LACP:

- Ethernet Port Channels
- FCoE Port Channels
- Appliance Port Channels

A default LACP policy is automatically assigned to all port channels that you create. You can edit this LACP policy or create a new one and assign it to a port channel. The LACP policy controls the following:

- **Suspend Individual**—When enabled, the ports in the port channel go into suspended mode if they do not receive LACP PDUs.
- **LACP Rate**—Modifies the duration of the LACP timeout. The normal timeout rate is 30 seconds, and the fast timeout rate is 1 second.

Creating or Editing a LACP Policy

Step 1 In the **Actions** bar, type **Create Link Aggression Control Protocol (LACP) Policy** and press Enter.

Step 2 In the **Link Aggression Control Protocol (LACP) Policy** dialog box, click **Domain Group Location** and select where you want to create the policy.

Step 3 Enter the **Name**.

The name is case sensitive.

Step 4 Choose whether to enable **Suspend Individual**.

Step 5 Choose the **LACP Rate** that you want to use.

Step 6 Click **Create**.

Flow Control Policy

Flow control policies determine whether the uplink Ethernet ports in a Cisco UCS domain send and receive IEEE 802.3x pause frames when the receive buffer for a port fills. These pause frames request that the transmitting port stop sending data for a few milliseconds until the buffer clears.

For flow control to work between a LAN port and an uplink Ethernet port, you must enable the corresponding receive and send flow control parameters for both ports. For Cisco UCS, the flow control policies configure these parameters.

When you enable the send function, the uplink Ethernet port sends a pause request to the network port if the incoming packet rate becomes too high. The pause remains in effect for a few milliseconds before traffic is

reset to normal levels. If you enable the receive function, the uplink Ethernet port honors all pause requests from the network port. All traffic is halted on that uplink port until the network port cancels the pause request.

Because you assign the flow control policy to the port, changes to the policy have an immediate effect on how the port reacts to a pause frame or a full receive buffer.

Creating or Editing a Flow Control Policy

Note If you have selected global port configuration for **Policy Resolution Control** in Cisco UCS Manager, then all local flow control policies will be deleted, and global flow control policies belonging to the same domain group in Cisco UCS Central will be created in Cisco UCS Manager.

Step 1 Click **Domain Group Location** and select the domain group for which you want to create the policy.

Step 2 Enter a **Name**.

The policy name is case sensitive.

Step 3 Select the **Priority**. This can be one of the following:

- **On**—PPP is enabled on this fabric interconnect.
- **Auto**—Cisco UCS and the network negotiate whether PPP is used on this fabric interconnect.

Step 4 Choose whether to enable or disable **Receive**. This can be one of the following:

- **Enabled**—Pause requests are honored and all traffic is halted on that uplink port until the network cancels the pause request.
- **Disabled**—Pause requests from the network are ignored and traffic flow continues as normal.

Step 5 Choose whether to enable or disable **Send**. This can be one of the following:

- **Enabled**—Cisco UCS sends a pause request to the network if the incoming packet rate becomes too high. The pause remains in effect for a few milliseconds before traffic is reset to normal levels.
- **Disabled**—Traffic on the port flows normally regardless of the packet load.

Step 6 Click **Save**.

Quality of Service Policy

A quality of service (QoS) policy assigns a system class to the outgoing traffic for a vNIC or vHBA. This system class determines the quality of service for that traffic. For certain adapters, you can also specify additional controls on the outgoing traffic, such as burst and rate.

You must include a QoS policy in a vNIC policy or vHBA policy and then include that policy in a service profile to configure the vNIC or vHBA.

Creating or Editing a Quality of Service Policy

Step 1 In the **Actions** bar, type **Create Quality of Service (QoS) Policy** and press Enter.

Step 2 In the **Create Quality of Service (QoS) Policy** dialog box, click **Organization** and select the location in which you want to create the policy.

Step 3 Enter the **Name** and optional **Description**.

The name is case sensitive.

Step 4 Select an **Egress Priority**.

Step 5 Choose whether to enable **Host Control Class of Service (CoS)**.

Step 6 Enter an **Egress Burst Size**, and select the egress average traffic rate.

Step 7 Click **Create**.

Deleting a QoS Policy

Step 1 On the menu bar, click **Network**.

Step 2 In the **Navigation** Pane, expand **Network** > **Policies** > **root**.

If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Expand **QoS Policies**.

Step 4 Right-click the policy that you want to delete and choose **Delete**.

Step 5 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

QoS System Classes

Cisco UCS uses Data Center Ethernet (DCE) to handle all traffic inside a Cisco UCS domain. This industry standard enhancement to Ethernet divides the bandwidth of the Ethernet pipe into eight virtual lanes. Two virtual lanes are reserved for internal system and management traffic. You can configure quality of service (QoS) for the other six virtual lanes. System classes determine how the DCE bandwidth in these six virtual lanes is allocated across the entire Cisco UCS domain.

Each system class reserves a specific segment of the bandwidth for a specific type of traffic, which provides a level of traffic management, even in an oversubscribed system. For example, you can configure the Fibre Channel Priority system class to determine the percentage of DCE bandwidth allocated to FCoE traffic.

Creating QoS System Class Settings

Step 1 In the **Actions** bar, type **Create QoS System Class Settings** and press Enter.

Step 2 In the **Create QoS System Class Settings** dialog box, choose the **Organization** in which you want to create the policy.

Step 3 Enter the **Name** and optional **Description**.

The name is case sensitive.

Step 4 Click **Create**.

To understand the impact of the policy, click **Evaluate**.

Step 5 In **System Classes**, define the following:

Table 1: System Classes

System Class	Description
Platinum Gold Silver Bronze	A configurable set of system classes that you can include in the QoS policy for a service profile. Each system class manages one lane of traffic. All properties of these system classes are available for you to assign custom settings and policies.
Best Effort	A system class that sets the quality of service for the lane reserved for basic Ethernet traffic. Some properties of this system class are preset and cannot be modified. For example, this class has a drop policy that allows it to drop data packets if required. You cannot disable this system class.
Fibre Channel	A system class that sets the quality of service for the lane reserved for Fibre Channel over Ethernet traffic. Some properties of this system class are preset and cannot be modified. For example, this class has a no-drop policy that ensures it never drops data packets. You cannot disable this system class. **Note** FCoE traffic has a reserved QoS system class that should not be used by any other type of traffic. If any other type of traffic has a CoS value that is used by FCoE, the value is remarked to 0.

ID Range Access Control Policy

Use the ID range access control policy to limit what pools can be utilized in a specific domain group. When you apply the access control policy to a pool, only the domain groups selected can access those pools.

Creating or Editing an ID Range Access Control Policy

Step 1 In the **Actions** bar, type **Create ID Range Access Control Policy** and press Enter.

Step 2 In the **ID Range Access Control Policy** dialog box, click **Basic** and choose the **Organization** in which you want to create the policy.

Step 3 Enter the **Name** and optional **Description**.

The name is case sensitive.

Step 4 In **Domain Groups**, click **Add** to select the **Permitted Domain Groups** associated with this policy.

Step 5 Click **Create**.

Multicast Policy

Multicast Policy is used to configure Internet Group Management Protocol (IGMP) snooping and IGMP querier. IGMP snooping dynamically determines hosts in a VLAN that should be included in particular multicast transmissions. You can create, modify, and delete a Multicast Policy that can be associated with one or more VLANs. When a Multicast Policy is modified, all VLANs associated with that Multicast Policy are reprocessed to apply the changes. By default, IGMP snooping is enabled and IGMP querier is disabled. For private VLANs, you can set a Multicast Policy for primary VLANs but not for their associated isolated VLANs. This is due to a Cisco NX-OS forwarding implementation.

The **Multicast Policy** view displays the IGMP Snooping State, IGMP Snooping Querier State, and the FI-A and FI-B Querier IPv4 Addresses for the specific policy.

Creating a Multicast Policy

Step 1 In the **Actions** bar, type **Multicast Policy** and press Enter.

Step 2 In the **Multicast Policy** dialog box, choose the **Domain Group Location** in which you want to create the policy.

Step 3 Enter a **Name** for the Multicast Policy.

The name is case sensitive.

Step 4 Select the **IGMP Snooping State** that determines if IGMP snooping examines IGMP protocol messages within a VLAN to discover which interfaces are connected to hosts or other devices interested in receiving multicast traffic:

- If **Enabled**, IGMP snooping is used for VLANs associated with this policy. IGMP snooping is **Enabled** by default.
- If **Disabled**, IGMP snooping is not used for associated VLANs.

Step 5 Select the **IGMP Snooping Querier State** that determines if the IGMP snooping querier sends out periodic IGMP queries that trigger IGMP report messages from hosts that want to receive IP multicast traffic. This can be one of the following:

- If **Enabled** periodic IGMP queries are sent out.
- If **Disabled** no IGMP queries are sent out.

IGMP querier is **Disabled** by default.

Step 6 Specify the IPv4 addresses for the IGMP snooping querier interfaces on the designated fabric interconnects in the **FI A Querier IPv4 Addresses** field. These fields are displayed only if the **IGMP Snooping Querier State** is **Enabled**.

Step 7 Click **Create**.

- Cisco UCS Central supports Multicast Policy for Cisco UCS Manager release 3.1(3) and later.
- You cannot create a create policy with the same name on Cisco UCS Manager. A global service profile displays a conflict when the multicast policy already exists in Cisco UCS Manager.

Step 8 On the **Multicast policy** page, click the **Delete** icon.

A dialog box prompting you to confirm the deletion of the policy appears.