Configuring Network Connections

This chapter contains the following sections:

VLANs

In Cisco UCS, a VLAN, also known as a named VLAN, creates a connection to a specific external LAN. The VLAN isolates traffic to that external LAN, including broadcast traffic.

The name that you assign to a VLAN ID adds a layer of abstraction that allows you to globally update all servers associated with service profiles that use the named VLAN. You do not need to reconfigure the servers individually to maintain communication with the external LAN.

You can create more than one named VLAN with the same VLAN ID. For example, if servers that host business services for HR and Finance must access the same external LAN, you can create VLANs named HR and Finance with the same VLAN ID. Then, if the network is reconfigured and Finance is assigned to a different LAN, you only have to change the VLAN ID for the named VLAN for Finance.

In a cluster configuration, you can configure a named VLAN to be accessible only to one fabric interconnect or to both fabric interconnects.

For more information about VLANs in Cisco UCS, including guidelines and recommendations, see the Cisco UCS Manager configuration guides.

Guidelines for VLAN IDs

Note You cannot create VLANs with IDs from 3968 to 4047. This range of VLAN IDs is reserved.

VLANs in the LAN cloud and FCoE VLANs in the SAN cloud must have different IDs. Using the same ID for a VLAN and an FCoE VLAN in a VSAN results in a critical fault and traffic disruption for all vNICs and uplink ports using that VLAN. Ethernet traffic is dropped on any VLAN that has an ID that overlaps with an FCoE VLAN ID.

The VLAN name is case-sensitive.

Creating a VLAN

In a Cisco UCS domain that is configured for high availability, you can create a VLAN that is accessible to both fabric interconnects or to only one fabric interconnect.

Note You cannot create VLANs with IDs from 3968 to 4047. This range of VLAN IDs is reserved.

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **VLANs**.

Step 4 Click **Add**.

Step 5 On the **Add VLAN** screen, complete the following fields:

Name	Description
VLAN Name field	For a single VLAN, this is the VLAN name. The VLAN name is case-sensitive.
VLAN ID field	A single numeric ID for the VLAN. A VLAN ID can be one of the following: • Between 1 and 3967 • Between 4048 and 4093 • Overlap with other VLAN IDs already defined on the system You cannot create VLANs with IDs from 3968 to 4047. This range of VLAN IDs is reserved. VLANs in the LAN cloud and FCoE VLANs in the SAN cloud must have different IDs. Using the same ID for a VLAN and an FCoE VLAN in a VSAN results in a critical fault and traffic disruption for all vNICs and uplink ports using that VLAN. Ethernet traffic is dropped on any VLAN that has an ID that overlaps with an FCoE VLAN ID.

Name	Description
Type drop-down list	Choose the type of VLAN. This can be one of the following: • **LAN Cloud** • **Appliances**
Fabric ID drop-down list	Choose how to configure the VLAN. This can be one of the following: • **Common/Global**—The VLAN maps to the same VLAN ID in all available fabrics. • **Fabric A**—The VLAN maps to a VLAN ID that exists only in fabric A. • **Fabric B**—The VLAN maps to a VLAN ID that exists only in fabric B.
Sharing drop-down list	Choose the type of sharing for the VLAN.

Step 6 Click **Submit**.

VLAN Port Count Optimization

VLAN port count optimization allows you to map the state of multiple VLANs into a single internal state. When you enable VLAN port count optimization, Cisco UCS logically groups VLANs based on the port VLAN membership. This grouping increases the port VLAN count limit. VLAN port count optimization also compresses the VLAN state and reduces the CPU load on the fabric interconnect. This reduction in the CPU load enables you to deploy more VLANs over more vNICs. Optimizing the VLAN port count does not change any of the existing VLAN configurations on the vNICs.

VLAN port count optimization is disabled by default. You can enable or disable the option based on your needs.

Note Enabling VLAN port count optimization increases the number of available VLAN ports for use. If the port VLAN count exceeds the maximum number of VLANs in a nonoptimized state, you cannot disable VLAN port count optimization.

Note VLAN port count optimization is not supported in Cisco UCS 6100 series fabric interconnects.

Enabling VLAN Port Count Optimization

Step 1 Choose **Physical** > **Compute**.
Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.
Step 3 Click **LAN Global Policies**.
Step 4 Check the **Enable VLAN Port Count Optimization** check box.
Step 5 Click **Save**.

Viewing VLAN Optimization Sets

VLAN port count optimization groups are automatically created by Cisco UCS, based on the VLAN IDs in the system. All the VLANs in the group share the same IGMP policy. The following VLANs are not included in a VLAN optimization set:

- FCoE VLANs
- Primary PVLANs and secondary PVLANs
- VLANs that are specified as a SPAN source
- VLANs configured as a single allowed VLAN on an interface and port profiles with a single VLAN

Step 1 Choose **Physical** > **Compute**.
Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.
Step 3 Click **VLAN Optimization Sets**.

Disabling VLAN Port Count Optimization

Note If the port VLAN count exceeds the maximum number of VLANs in a nonoptimized state, you cannot disable VLAN port count optimization.

Step 1 Choose **Physical** > **Compute**.
Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.
Step 3 Click **LAN Global Policies**.
Step 4 Uncheck the **Enable VLAN Port Count Optimization** check box.
Step 5 Click **Save**.

VLAN Permissions

VLAN permissions restrict access to VLANs based on specified organizations. Based on the service profile organizations that the VLANs belong to, VLAN permissions also restrict the set of VLANs that you can assign to service profile vNICs. VLAN permissions is an optional feature and is disabled by default. You can enable or disable the feature based on your requirements. If you disable the feature, all the VLANs are globally accessible to all organizations. VLAN permissions are also known as org permissions for VLANs.

If you do not enable VLAN permissions, you cannot modify the permissions for VLANs.

If you enable VLAN permissions, you can specify the organizations available for a VLAN. The VLAN is then only available to that specific organization and all its suborganizations. Users from other organizations cannot access the VLAN. You can also modify VLAN permissions at any point, based on changes in your VLAN access requirements.

Caution When you assign VLAN permissions to an organization at the root level, all suborganizations can access that VLAN. After you assign VLAN permissions at the root level, if you change the permissions for a VLAN that belong to a suborganization, that VLAN becomes unavailable to the root level organization.

Enabling VLAN Permissions

By default, VLAN permissions are disabled. If you want to restrict VLAN access by creating permissions for different organizations, enable the org permission option.

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **LAN Global Policies**.

Step 4 Check the **Enable Org Permissions** check box.

Step 5 Click **Save**.

Modifying Permissions on a VLAN

Before you begin

Enable VLAN permissions before you assign org permissions to a VLAN.

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **VLANs**.

Step 4 Click the row for the VLAN for which you want to modify org permissions.

Step 5 Click **Modify Org Permissions**.

Step 6 On the **Organization List** screen, check the check boxes for the organizations for which you want to give permissions to the VLAN and click **Submit**.

Disabling VLAN Permissions

By default, VLAN permissions are disabled. If you had enabled the option, assigned VLAN permissions to different network groups, and no longer want to use the option, you can disable the option globally. When VLAN org permissions are disabled, the permissions that you assigned to the VLANs still exist in the system but they are not enforced. If you want to use VLAN permissions later, you can enable the feature to use the previously assigned permissions.

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **LAN Global Policies**.

Step 4 Uncheck the **Enable Org Permissions** check box.

Step 5 Click **Save**.

VLAN Groups

VLAN groups allow you to group VLANs on Ethernet uplink ports by function or by VLANs that belong to a specific network. You can define VLAN membership and apply the membership to multiple Ethernet uplink ports on the fabric interconnect.

After you assign a VLAN to a VLAN group, any changes made to the VLAN group are applied to all Ethernet uplink ports that are part of that VLAN group. The VLAN group also enables you to identify VLAN overlaps between disjoint VLANs that must not be connected.

You can configure uplink Ethernet ports under a VLAN group. After you configure an uplink Ethernet port for a VLAN group, that port will only support the VLANs in that group.

Creating a VLAN Group

SUMMARY STEPS

1. Choose **Physical** > **Compute**.
2. On **Compute** page, choose the pod that includes the Cisco UCS Manager account.
3. Click **VLAN Groups**.
4. Click **Add**.
5. On the **Create VLAN Group** screen, do the following to add VLANs to the group:
6. (Optional) On the **VLAN Group - Add Uplink Ports** page, add the ports that you want to include in the VLAN group and click **Next**.
7. (Optional) On the **VLAN Group - Add Uplink Port Channels** page, add the port channels that you want to include in the VLAN group and click **Next**.

8. Click **Submit**.

DETAILED STEPS

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **VLAN Groups**.

Step 4 Click **Add**.

Step 5 On the **Create VLAN Group** screen, do the following to add VLANs to the group:

a) In the **Name** field, enter a unique name for the VLAN group.

The VLAN group name is case-sensitive.

b) In the **VLANs** table, choose the VLANs that you want to add to the group.

If the VLANs that you want to include in the group do not exist yet, click **Add** in the table and create a new VLAN. For more information, see Creating a VLAN, on page 2.

c) After you have added all desired VLANs to the group, click **Next**.

Step 6 (Optional) On the **VLAN Group - Add Uplink Ports** page, add the ports that you want to include in the VLAN group and click **Next**.

Step 7 (Optional) On the **VLAN Group - Add Uplink Port Channels** page, add the port channels that you want to include in the VLAN group and click **Next**.

Step 8 Click **Submit**.

Modifying the VLAN Permissions for a VLAN Group

When you modify the organization access permissions for a VLAN group, the change in permissions applies to all VLANs in that VLAN group.

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **VLAN Groups**.

Step 4 Click **Modify Org Permissions**.

Step 5 On the **Organization List** screen, check the check boxes for the organizations for which you want to give permissions to the VLAN group and click **Submit**.

MAC Pools

A MAC pool is a collection of network identities, or MAC addresses, that are unique in their Layer 2 environment and are available to be assigned to vNICs on a server. If you use MAC pools in service profiles,

you do not have to manually configure the MAC addresses to be used by the server associated with the service profile.

In a system that implements multitenancy, you can use the organizational hierarchy to ensure that MAC pools can be used only by specific applications or business services. Cisco UCS uses the name resolution policy to assign MAC addresses from the pool.

To assign a MAC address to a server, you must include the MAC pool in a vNIC policy. The vNIC policy is then included in the service profile assigned to that server.

You can specify your own MAC addresses or use a group of MAC addresses provided by Cisco.

Creating a MAC Pool

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **Organizations**.

Step 4 Click the organization in which you want to create the pool and then click **View Details**.

Step 5 Click **MAC Pools**.

Step 6 Click **Add**.

Step 7 On the **Add MAC Pool** screen, complete the following fields:

Name	Description
Name field	A unique name for the pool.
Description field	A description for the pool.
First MAC Address field	The first MAC address in the block.
Size field	The number of MAC addresses in the block.

Step 8 Click **Submit**.

Adding a Block of Addresses to a MAC Pool

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **Organizations**.

Step 4 Click the organization in which you want to modify the pool and then click **View Details**.

Step 5 Click **MAC Pools**.

Step 6 Click the pool to which you want to add a block of addresses and then click **Create a Block of MAC Addresses**.

Step 7 On the **Add MAC Pool Block** screen, complete the following fields:

Name	Description
First MAC Address field	The first MAC address in the block.
Size field	The number of MAC addresses in the block.

Step 8 Click **Submit**.

Configuring Quality of Service

Quality of Service

Cisco UCS provides the following methods to implement quality of service:

- System classes that specify the global configuration for certain types of traffic across the entire system
- QoS policies that assign system classes for individual vNICs
- Flow control policies that determine how uplink Ethernet ports handle pause frames

Global QoS changes made to the QoS system class may result in brief data-plane interruptions for all traffic. Some examples of such changes are:

- Changing the MTU size for an enabled class
- Changing packet drop for an enabled class
- Changing the CoS value for an enabled class

Guidelines and Limitations for Quality of Service on Cisco UCS 6300 Series Fabric Interconnect

- Cisco UCS 6300 Series Fabric Interconnect uses a shared buffer for all system classes.
- Multicast optimization is not supported.
- When you change the QoS parameters for any class causes traffic disruption to all classes. The following table lists the changes in the QoS system class and the conditions that trigger a system reboot.

QoS System class status	Condition	FI Reboot Status
Enabled	Change between drop and no drop	Yes
No-drop	Change between enable and disable	Yes
Enable and no-drop	Change in MTU size	Yes

- The subordinate FI reboots first as a result of the change in the QoS system class. The primary FI reboots only after you acknowledge it in **Pending Activities**.

Guidelines and Limitations for Quality of Service on Cisco UCS Mini

- Cisco UCS Mini uses a shared buffer for all system classes.
- The bronze class shares the buffer with SPAN. We recommend using either SPAN or the bronze class.
- Multicast optimization is not supported.
- Changing the QoS parameters for any class causes traffic disruption to all classes.
- When mixing Ethernet and FC or FCoE traffic, the bandwidth distribution is not equal.
- Multiple streams of traffic from the same class may not be distributed equally.
- Use the same CoS values for all no-drop policies to avoid any FC or FCoE performance issues.
- Only the platinum and gold classes support no-drop policies.

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.

The following table describes the system classes that you can configure.

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. For Cisco UCS Mini, packet drop can only be disabled on the platinum and gold classes. Only one platinum and one gold class can be configured as a no drop class at a time.
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.

System Class	Description
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.

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.

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.

Changing QoS System Classes

The type of adapter in a server limits the maximum transmission unit (MTU) supported. For example, network MTU above the maximums may cause the packet to be dropped for the following adapters:

- The Cisco UCS M71KR CNA adapter, which supports a maximum MTU of 9216.
- The Cisco UCS 82598KR-CI adapter, which supports a maximum MTU of 14000.

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **QoS System Class**.

Step 4 Click the row for the QoS system class that you want to modify.

Step 5 Click **Edit**.

Step 6 On the **Modify QoS System Class** screen, change one or more of the following fields:

Name	Description
Enabled check box	If checked, the associated QoS class is configured on the fabric interconnect and can be assigned to a QoS policy. If unchecked, the class is not configured on the fabric interconnect and any QoS policies associated with this class default to Best Effort or, if a system class is configured with a CoS of 0, to the CoS 0 system class. **Note** This field is always checked for the Best Effort and Fibre Channel system classes.
CoS field	The class of service. You can enter an integer value between 0 and 6, with 0 being the lowest priority and 6 being the highest priority. We recommend that you do not set the value to 0, unless you want that system class to be the default system class for traffic if the QoS policy is deleted or the assigned system class is disabled. **Note** This field is set to 7 for internal traffic and to any for Best Effort. Both of these values are reserved and cannot be assigned to any other priority.
Packet Drop check box	If checked, packet drop is allowed for this class. If unchecked, packets cannot be dropped during transmission. **Note** This check box is always unchecked for the Fibre Channel class, which never allows dropped packets, and always checked for Best Effort, which always allows dropped packets.
Weight drop-down list	Choose the weight assigned to packets in the system class. This can be one of the following: • An integer between 1 and 10. If you enter an integer, the system determines the percentage of network bandwidth assigned to the priority level as described in the Weight (%) field. • **best-effort**. • **none**.

Name	Description
Multicast Optimized check box	If checked, the class is optimized to send packets to multiple destinations simultaneously. **Note** This option is not applicable to the Fibre Channel system class.
MTU drop-down list	Choose the MTU for the channel. This can be one of the following: • An integer between 1500 and 9216. This value corresponds to the maximum packet size. • **fc**—A predefined packet size of 2240. • **normal**—A predefined packet size of 1500. **Note** This field is always set to fc for the Fibre Channel system class.

Step 7 Click **Submit**.

Enabling a QoS System Class

The Best Effort and Fibre Channel system classes are enabled by default.

Step 1 Choose **Physical** > **Compute**.
Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.
Step 3 Click **QoS System Class**.
Step 4 Click the row for the QoS system class that you want to enable.
Step 5 Click **Edit**.
Step 6 On the **Modify QoS System Class** screen, uncheck the **Enabled** check box and click **Submit**.

Disabling a QoS System Class

You cannot disable the Best Effort or Fibre Channel system classes.

All QoS policies that are associated with a disabled system class default to Best Effort, unless the disabled system class is configured with a Cos of 0. If the disabled system class is configured with a Cos of 0, the associated QoS policies default to the Cos 0 system class.

Step 1 Choose **Physical** > **Compute**.
Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.
Step 3 Click **QoS System Class**.

Step 4 Click the row for the QoS system class that you want to disable.

Step 5 Click **Edit**.

Step 6 On the **Modify QoS System Class** screen, uncheck the **Enabled** check box and click **Submit**.

Creating a QoS Policy

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **Organizations**.

Step 4 Click the organization in which you want to create the policy and then click **View Details**.

Step 5 Click **QoS Policies**.

Step 6 Click **Add**.

Step 7 On the **Create QoS Policy** screen, complete the following fields:

Name	Description
Name field	A unique name for the policy.
Description field	A description for the policy.
Priority drop-down list	Choose the priority assigned to this QoS policy. This can be one of the following: • **Fc**—Use this priority for QoS policies that control vHBA traffic only. • **Platinum**—Use this priority for QoS policies that control vNIC traffic only. • **Gold**—Use this priority for QoS policies that control vNIC traffic only. • **Silver**—Use this priority for QoS policies that control vNIC traffic only. • **Bronze**—Use this priority for QoS policies that control vNIC traffic only. • **Best Effort**—Do not use this priority. It is reserved for the Basic Ethernet traffic lane. If you assign this priority to a QoS policy and configure another system class as CoS 0, Cisco UCS does not default to this system class. It defaults to the priority with CoS 0 for that traffic.

Name	Description
Burst field	The normal burst size for servers that use this policy. This field determines how large traffic bursts can be before some traffic is considered to exceed the rate limit. The default is 10240. The minimum value is 0, and the maximum value is 65535. This setting is not applicable to all adapters.
Rate drop-down list	Choose the expected average rate of traffic. Traffic that falls under this rate will always conform. This can be one of the following: • **line-rate**—Equals a value of 0 and specifies no rate limiting. This is the default value. • **Specify Manually**—Enables you to specify the rate in a field. The minimum value is 0, and the maximum value is 40,000,000. The granularity for rate limiting on a Cisco UCS M81KR Virtual Interface Card adapter is 1 Mbps. These adapters treat the requested rate as a "not-to-exceed" rate. Therefore, a value of 4.5 Mbps is interpreted as 4 Mbps. Any requested rate of more than 0 and less than 1 Mbps is interpreted as 1 Mbps, which is the lowest supported hardware rate limit. Rate limiting is not applicable to all adapters. For example, this setting is not supported on the Cisco UCS VIC-1240 Virtual Interface Card.
Host Control drop-down list	Choose whether Cisco UCS controls the class of service (CoS) for a vNIC. This setting has no effect on a vHBA. This can be one of the following: • **None**—Cisco UCS uses the CoS value associated with the priority selected in the Priority drop-down list regardless of the CoS value assigned by the host. • **Full**—If the packet has a valid CoS value assigned by the host, Cisco UCS uses that value. Otherwise, Cisco UCS uses the CoS value associated with the priority selected in the **Priority** drop-down list. This setting is not applicable to all adapters.

Step 8 Click **Submit**.

Creating a Flow Control Policy

Before you begin

Configure the network port with the corresponding setting for the flow control that you need. For example, if you enable the send setting for flow-control pause frames in the policy, make sure that the receive parameter in the network port is set to on or desired. If you want the Cisco UCS port to receive flow-control frames, make sure that the network port has a send parameter set to on or desired. If you do not want to use flow control, you can set the send and receive parameters on the network port to off.

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **Flow Control Policies**.

Step 4 Click **Add**.

Step 5 On the **Create Flow Control Policy** screen, complete the following fields:

Name	Description
Name field	A unique name for the policy.
Priority drop-down list	Choose the PPP configuration. This can be one of the following: • **Auto**—Cisco UCS and the network negotiate whether PPP is used on this fabric interconnect. • **On**—PPP is enabled on this fabric interconnect.
Receive drop-down list	Choose what happens when pause requests are received from the network. This can be one of the following: • **Off**—Pause requests from the network are ignored and traffic flow continues as normal. • **On**—Pause requests are honored and all traffic is halted on that uplink port until the network cancels the pause request.
Send drop-down list	Choose what happens if the incoming packet rate becomes too high. This can be one of the following: • **Off**—Traffic on the port flows normally regardless of the packet load. • **On**—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.

Step 6 Click **Submit**.

vNICs

vNIC Template

This policy defines how a vNIC on a server connects to the LAN. This policy is also referred to as a vNIC LAN connectivity policy.

A VM-FEX port profile is not automatically created with the correct settings when you create a vNIC template. If you want to create a VM-FEX port profile, you must configure the target of the vNIC template as a VM.

You need to include this policy in a service profile for it to take effect.

Note If your server has two Emulex or QLogic NICs (Cisco UCS CNA M71KR-E or Cisco UCS CNA M71KR-Q), you must configure vNIC policies for both adapters in your service profile to get a user-defined MAC address for both NICs. If you do not configure policies for both NICs, Windows still detects both of them in the PCI bus. Because the second Ethernet interface is not part of your service profile, Windows assigns it a hardware MAC address. If you then move the service profile to a different server, Windows sees additional NICs because one NIC did not have a user-defined MAC address.

Creating a vNIC Template

Before you begin

One or more of the following resources must already exist:

- Named VLAN
- MAC pool
- QoS policy
- LAN pin group
- Statistics threshold policy

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **Organizations**.

Step 4 Click the organization in which you want to create the policy and then click **View Details**.

Step 5 Click **vNIC Templates**.

Step 6 Click **Add**.

Step 7 On the **Add vNIC Template** screen, complete the following fields:

Name	Description
Name field	A unique name for the policy.
Description field	A description for the policy.
Fabric ID drop-down list	Choose the fabric interconnect that vNICs created with this template are associated with. If you want vNICs created from this template to be able to access the second fabric interconnect if the default one is unavailable, check the **Enable Failover** check box. **Note** Do not enable vNIC fabric failover under the following circumstances: • If the Cisco UCS domain is running in Ethernet Switch Mode. vNIC fabric failover is not supported in that mode. If all Ethernet uplinks on one fabric interconnect fail, the vNICs do not fail over to the other. • If you plan to associate one or more vNICs created from this template with a server adapter that does not support a fabric failover, such as the Cisco UCS 82598KR-CI 10-Gigabit Ethernet Adapter. If you do so, Cisco UCS Manager generates a configuration fault when you associate the service profile with the server.
Target check boxes	If checked, the target that you choose determines whether a VM-FEX port profile is automatically created with the appropriate settings for the vNIC template. This can be one of the following: • **Adapter**—The vNICs apply to all adapters. No VM-FEX port profile is created if you choose this option. • **VM**—The vNICs apply to all virtual machines. A VM-FEX port profile is created if you choose this option.
Template Type drop-down list	Choose the type of template. This can be one of the following: • **Initial Template**—vNICs created from this template are not updated if the template changes. • **Updating Template**—vNICs created from this template are updated if the template changes.

Step 8 In the **VLANs** area, do the following to select the VLAN to be assigned to vNICs created from this template:

a) Click + (add).

b) In the **Add Entry to VLANs** dialog box, complete the following fields and click **Submit**:

- **Name** drop-down list—Choose the VLAN that you want to associate with the vNIC template.
- **Set as Native VLAN** check box—Check the check box if you want this VLAN to be the native VLAN for the port.

Step 9 To associate policies with vNICs created from this template, complete the following fields:

Name	Description
MTU field	The maximum transmission unit (MTU), or packet size, that vNICs created from this vNIC template should use. Enter an integer between 1500 and 9216. **Note** If the vNIC template has an associated QoS policy, the MTU specified here must be equal to or less than the MTU specified in the associated QoS system class. If this MTU value exceeds the MTU value in the QoS system class, packets might be dropped during data transmission.
MAC Pool drop-down list	Choose the MAC address pool that vNICs created from this vNIC template should use.
QoS Policy drop-down list	Choose the quality of service policy that vNICs created from this vNIC template should use.
Network Control Policy drop-down list	Choose the network control policy that vNICs created from this vNIC template should use.
Pin Group drop-down list	Choose the LAN pin group that vNICs created from this vNIC template should use.
Stats Threshold Policy drop-down list	Choose the statistics collection policy that vNICs created from this vNIC template should use.
VNIC Template Connection Policy drop-down list	Choose the collection policy that vNICs created from this template should use. It can be one of the following: • **Dynamic Policy** • **usNIC Policy** • **VMQ Policy** Only usNIC and VM connection policies created in Cisco UCS Manager are displayed in this drop-down list. **Note** This field is available only with Cisco UCS Manager Release 2.2.

Name	Description
usNIC Template Connection Policy drop-down list	(*Displays only if you choose* **usNIC Policy** *as the VNIC Template connection policy*.) Choose the usNIC collection policy that vNICs created from this vNIC template should use.
VMQ Template Connection Policy drop-down list	(*Displays only if you choose* **VMQ Policy** *as the VNIC Template connection policy.*) Choose the VM collection policy that vNICs created from this vNIC template should use.

Step 10 Click **Submit**.

What to do next

Include the vNIC template in a network policy.

Creating a vNIC

Step 1 Choose **Policies** > **Physical Infrastructure Policies** > **UCS Manager**.

Step 2 Click **vNIC**.

Step 3 Click **Add**.

Step 4 On the **Create vNIC** screen, complete the following fields to specify the Cisco UCS connections for the vNIC:

Name	Description
vNIC Name field	A unique name for the vNIC.
UCS Account Name drop-down list	Choose the Cisco UCS Manager account to which you want to add this vNIC.
UCS Organization Name drop-down list	Choose the Cisco UCS organization to which you want to add this vNIC.
vNIC Template drop-down list	Choose the vNIC template that you want to assign to this vNIC.
Adapter Policy drop-down list	Choose one of the following Ethernet adapter policies: • **Default** • **Windows** • **VMware** • **Linux**

Step 5 Click **Submit**.

What to do next

Include this vNIC in a network 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 We do not recommend that you use static IDs in connectivity policies because these policies are included in service profiles and service profile templates and can be used to configure multiple servers.

Creating a LAN Connectivity Policy

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **Organizations**.

Step 4 Click the organization in which you want to create the policy and then click **View Details**.

Step 5 Click **LAN Connectivity Policies**.

Step 6 Click **Add**.

Step 7 On the **LAN Connectivity Policy** screen, enter a name and description for the policy.

Step 8 In the **vNICs** table, click **Add** and do the following:

a) Enter a name for the vNIC.

b) To use a vNIC template to create the vNIC, check the **Use vNIC Template** check box and select the appropriate template and adapter policy from the drop-down lists that are displayed.

c) To create a new vNIC without a template, do not check the **Use vNIC Template** check box and complete the fields that are displayed.

For more information about these fields, see Creating a vNIC, on page 20.

d) Click **Submit**.

Repeat this step if you want to add additional vNICs to the policy.

Step 9 After you have created all vNICs required for the policy, click **Submit**.

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 taken 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 Manager 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 Manager 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. 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 a Network Control Policy

MAC address-based port security for Emulex Converged Network Adapters (N20-AE0102) is not supported. When MAC address-based port security is enabled, the fabric interconnect restricts traffic to packets that contain the MAC address that it first learns, which is either the source MAC address used in the Fibre Channel over Ethernet (FCoE) Initialization Protocol packet or the MAC address in an Ethernet packet, whichever is sent first by the adapter. This configuration can result in either FCoE or Ethernet packets being dropped.

Step 1 Choose **Physical** > **Compute**.

Step 2 On **Compute** page, choose the pod that includes the Cisco UCS Manager account.

Step 3 Click **Organizations**.

Step 4 Click the organization in which you want to create the policy and then click **View Details**.

Step 5 Click **Network Control Policies**.

Step 6 Click **Add**.

Step 7 On the **Create Network Control Policy** screen, complete the following fields:

Name	Description
Name field	A unique name for the policy.
CDP drop-down list	Choose whether the Cisco Discovery Protocol (CDP) is enabled on servers associated with a service profile that includes this policy. This can be one of the following: • **Disabled** • **Enabled**
Action on Uplink Fail drop-down list	Choose how the virtual interface (VIF) behaves if no uplink port is available when the fabric interconnect is in end-host mode. This can be one of the following: • **Link Down**—Changes the operational state of a vNIC to down when uplink connectivity is lost on the fabric interconnect, and enables a fabric failover for vNICs. • **Warning**—Maintains server-to-server connectivity even when no uplink port is available, and disables a fabric failover when uplink connectivity is lost on the fabric interconnect. The default is **Link Down**. **Note** If your implementation includes those types of non-VM-FEX capable converged network adapters 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.

Name	Description
Forge drop-down list	Choose whether forged MAC addresses are allowed or denied when packets are sent from the server to the fabric interconnect. This can be one of the following: • **Allow**—All server packets are accepted by the fabric interconnect, regardless of the MAC address associated with the packets. • **Deny**—After the first packet has been sent to the fabric interconnect, all other packets must use the same MAC address or they will be silently rejected by the fabric interconnect. This option enables port security for the associated vNIC. If you plan to install VMware ESX on the associated server, you must configure MAC Security to allow for the network control policy applied to the default vNIC. If you do not configure MAC Security to **Allow**, the ESX installation might fail because the MAC Security permits only one MAC address while the installation process requires more than one MAC address.

Step 8 Click **Submit**.

Network Policy

The network policy is a Cisco UCS Director policy that configures the connections between a server and the LAN, including the virtual network interface cards (vNICs) used by the server. Depending upon the configuration you choose, this policy can be used to configure two or more vNICs for the server. You can choose to create the vNICs in this policy or use a LAN connectivity policy to determine the vNIC configuration.

You must include this policy in a service profile and that service profile must be associated with a server for it to take effect.

Creating a Network Policy

Step 1 Choose **Policies** > **Physical Infrastructure Policies** > **UCS Manager**.

Step 2 Click **Network Policy**.

Step 3 Click **Add**.

Step 4 On the **Add Network Policy** screen, complete the following fields:

Name	Description
Policy Name field	The name of the policy.
Policy Description field	The description of the policy.

Name	Description
UCS Account Name drop-down list	Choose the Cisco UCS Manager account to which you want to add this policy.
UCS Organization Name drop-down list	Choose the Cisco UCS organization to which you want to add this policy.
Dynamic vNIC Connection Policy drop-down list	Choose a dynamic vNIC connection policy if the policy is being assigned to service profiles for servers that support dynamic vNICs.
LAN Connectivity Type drop-down list	Choose one of the following connectivity types: • **Expert**—Allows you to create up to 10 vNICs that the server can use to access the LAN. • **Simple**—Allows you to create a maximum of two vNICs that the server can use to access the LAN. • **No vNICs**—Does not allow you to create any vNICs. If you choose this option, any server associated with a service profile that includes this policy is not connected to the LAN. • **Hardware Inherited**—Uses the vNICs assigned to the Ethernet adapter profile associated with the server. • **Use LAN Connectivity Policy**—Uses a LAN connectivity policy to determine the LAN connectivity for the server.

Step 5 If you chose the **Expert** LAN option, do the following:

a) In the **Add vNIC** drop-down, choose the number of vNICs that you want to add to the network policy. Up to 10 vNICS can be created.

b) From the **Template For vNIC1 ... vNIC10** drop-down list, choose a vNIC template.

c) Go to Step 8.

Step 6 If you chose the **Simple** LAN option, do the following:

a) In the **vNIC0 (Fabric A)** area, complete the following fields:

- In the **vNIC0 Name** field, enter a unique name for the vNIC.
- From the **Select VLAN** drop-down list, choose the name of the VLAN with which this vNIC should be associated.

b) In the **vNIC1 (Fabric B)** area, complete the following fields:

- In the **vNIC1 Name** field, enter a unique name for the vNIC.
- From the **Select VLAN** drop-down list, choose the name of the VLAN with which this vNIC should be associated.

c) Go to Step 8.

Step 7 If you chose the **Use LAN Connectivity Policy** option, choose the policy that you want to associate with the server from the **LAN Connectivity Policy** drop-down list.

Step 8 Click **Submit**.

What to do next

Include the network policy in a service profile.