A black and white logo

AI-generated content may be incorrect.A black background with white text

AI-generated content may be incorrect.

UCS X Series Server Solution Design Document

April 17th, 2025

Version 0.1 (DRAFT)

**Document Classification**

**Cisco Highly Confidential**

Cisco Systems, Inc.

Corporate Headquarters

170 West Tasman Drive

San Jose, CA 95134-1706 USA

Phone: +1 408-526-4000

Toll Free: +1 800-553-NETS (6387)

Fax: +1 408-526-4100

# Introduction

## Preface

This Solution Design document builds upon the {{customer\_name}} CRD document. The SDD will provide the actual physical and logical design as well as technology specific templates which have been developed for {{customer\_name}}'s environment. These templates will be used to generate the actual configurations for the {{customer\_name}} environment.

This document was developed in collaboration with the following teams and organizations through a series of workshops and meetings:

* {{customer\_name}}

# Domain Settings

## Domain Profiles

In Cisco Intersight, a Domain Profile configures a Fabric Interconnect pair through reusable policies, allows for configuration of the ports and port channels, and configures the VLANs and VSANs in the network. It defines the characteristics of and configures ports on Fabric Interconnects. You can create a Domain profile and associate it with a Fabric Interconnect Domain. The Domain-related policies can be attached to the profile either at the time of creation or later. One UCS Domain profile can be assigned to one Fabric Interconnect Domain.

The following domain profiles and associated policies will be created and associated for these two domains.

**Table 1 Domain Profiles**

{{domain\_profiles}}

## Domain Policies

For each Domain Profile, several polices are used to define port types, System QoS, VLANs allowed on the FIs, and other settings.

The following Domain Profiles and their policies are listed below.

**Table 2 Domain Policies**

{{domain\_policies}}

## Ethernet Switching Mode

Cisco UCS has the concept of Ethernet Switching Modes, with two configurable options of *Switching Mode* and *End Host Mode*.

*End Host Mode* is the preferred and recommended configuration to ensure maximum scalability while maintaining the unique simplicity that Cisco UCS can offer. In *End Host Mode*, the Fabric Interconnects act as the name suggests, as an end host, a device with many MAC addresses. Due to it behaving as a host rather than a traditional switch, it does not need to run the Spanning Tree Protocol. UCS is therefore able to deploy a loop-free network architecture whilst enabling full uplink connectivity. Alternatively, if the Fabric Interconnects were configured with the *Ethernet Switching Mode,* it would run the Spanning Tree Protocol to prevent network loops and therefore certain redundant paths would be blocked.

In Ethernet *End Host Mode*, forwarding is based on server-to-uplink pinning. When a server is brought online, a given vNIC is ‘pinned’ to an uplink in a ‘round-robin’ basis. It uses this uplink regardless of the destination it is trying to reach. Therefore, fabric interconnects do not learn MAC addresses from external LAN switches; they learn MAC addresses from servers within UCS only. The address table is managed so that it only contains MAC addresses of stations connected to Server Ports. Addresses are not learned on frames from network ports; and frames from Server Ports are allowed to be forwarded only when their source addresses have been learned into the switch forwarding table. Frames sourced from stations inside UCS take optimal paths to all destinations (unicast or multicast) inside.

If these frames need to leave UCS, they only exit on their pinned network port. Frames received on network ports are filtered, based on various checks, with an overriding requirement that any frame received from outside UCS must not be forwarded back out of UCS. However, a fabric interconnect does perform local switching for server-to-server traffic that is in the same VLAN and on the same Fabric. This is required because a LAN switch will by default never forward traffic back out of the interface it came in on. This design feature will be exploited, where possible, to ensure optimal, low latency switching by designing server vNIC adapters to share a given fabric, enabling switching to occur at the Fabric Interconnect, rather than the northbound network devices.

|  |
| --- |
| The Fabric Interconnects will be configured with the Ethernet Switching Mode of *End Host Mode*. |

Table 3 Switch Control Policies

{{switch\_control\_policies }}

Table 4 Fabric Interconnects

{{fabric\_interconnects}}

## VLAN Policies

VLANs provide the capability within UCS of segregating various types of network traffic. The following is a list of VLAN Policies, and their VLANs.

Table 5 VLAN Policies

{{vlan\_policies}}

## Multicast Policy

This policy configures Internet Group Management Protocol (IGMP) snooping and IGMP querier. IGMP Snooping dynamically determines hosts in a VLAN that should be included in multicast transmissions.

You can create, modify, and delete a multicast policy that can be associated to one or more VLANs. When a multicast policy is modified, all VLANs associated with that multicast policy are re-processed to apply the changes. By default, IGMP snooping is enabled and IGMP querier is disabled. On enabling IGMP querier, you can configure the IPv4 addresses for the local and peer IGMP snooping querier interfaces.

Some VLANs in {{customer\_name}}'s environment will require multicast. For these VLANs, they require snooping to be disabled and IGMP Source IP Proxy to be enabled. As of now, IGMP Source IP Proxy is not configurable in Intersight, however, it is enabled by default. Hence, to support multicast VLANs, a multicast-snooping\_disabled policy will be created. For the remainder of the VLANs, they will use multicast-default policy.

**Table 6 Multicast Policy**

{{multicast\_policies}}

|  |
| --- |
| By default, In Cisco Intersight **IGMP Source IP Proxy state** is enabled. When IGMP Source IP Proxy is enabled, the fabric interconnect acts as a proxy for its hosts and manages the membership of hosts and routing devices in multicast groups. IP hosts use IGMP to report their multicast group memberships to any immediately neighboring multicast routing devices. |

|  |
| --- |
| This policy is applicable for Domain Profile only. |

## NTP Policy

This policy allows the UCS System managed by Cisco Intersight to synchronize the time with an NTP server. Up to a maximum of 4 NTP server can be configured with each policy.

For {{customer\_name}}, the following NTP policy will be configured.

**Table 7 NTP Policy**

{{ntp\_policies}}

|  |
| --- |
| This policy is applicable for both Domain Profile and Server Profile. For Server Profile, it is applicable for Standalone servers only. |

## Network Connectivity Policy

This policy configures the DNS Domain settings that are used to add or update the resource records on the DNS server from the endpoints, and the DNS server settings for IPv4 and IPv6 on an endpoint.

In {{customer\_name}}’s environment, the following network connectivity policy will be used.

Table 8 Network Connectivity Policy

{{network\_connectivity\_policies}}

|  |
| --- |
| This policy is applicable for both Domain Profile and Server Profile. For Server Profie, it is applicable for Standalone servers only. |

## System QoS Policy

This policy implements network traffic prioritization based on the importance of the connected network by assigning system classes for individual vNICs. Intersight 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 configuration setup validates each input on the system class to prevent duplicate or invalid entries.

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

**Platinum, Gold, Silver, and Bronze** — A configurable set of system classes that you can include in the QoS policy for a UCS domain 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.

The following System QoS Policies are configured:

Table 9 System QoS Policy

{{system\_qos\_policies}}

|  |
| --- |
| This policy is applicable for Domain Profile only. |

## Syslog Policy

This policy enables to configure the local logging and remote logging (minimum severity) for an endpoint. This policy also provides configuration support to store the syslog messages in the local file and the remote syslog server.

Table 10 Syslog Policy

{{syslog\_policies}}

|  |
| --- |
| This policy is applicable for both Domain Profile and Server Profile. |

## Port Policy

This policy is used for configuring the port parameters such as unified ports that carry Ethernet or Fibre Channel traffic, port roles and speed.

Table 11 Port Policy

{{port\_policies}}

# Server Settings

## Server Profiles

In Cisco Intersight, a Server Profile enables resource management by streamlining policy alignment, and server configuration. You can create Server Profiles using the Server Profile wizard or you can import the configuration details of C-series servers in standalone mode and FI-attached servers in Intersight Managed Mode (IMM), directly from Cisco IMC. You can create Server Profiles using the Server Profile wizard to provision servers, create policies to ensure smooth deployment of servers, and eliminate failures that are caused by inconsistent configuration.

Each server profile can be individually created, or it can be created from template. For profiles created from template, it cannot be modified, unless it is detached from its template. Unique identifiers for each profile are also derived from pools, such as MAC pool and WWN pools.

Table 12 Server Profiles

{{server\_profiles}}

In Cisco Intersight, Server Profile Templates enable the user to define a template from which multiple server profiles can be derived and deployed. Any property modification made in the template syncs with all the derived profiles. You can deploy these modified profiles individually. This feature helps in the quick and easy configuration as multiple profiles can be created and edited simultaneously.

Table 13 Server Profile Templates

{{server\_profile\_templates}}

## Server Ethernet Policies

### LAN Connectivity Policy

Determines the connections and the network communication resources between the server and the LAN on the network. You must create the Ethernet Adapter, Ethernet QoS, and Ethernet Network policies as part of the LAN connectivity policy. For IMM servers, use a MAC pool, or static MAC addresses, to assign MAC addresses to servers and to identify the vNICs that the servers use to communicate with the network.

The LAN Connectivity Policy determines the connectivity between the server and the ethernet network. vNICs, its placement, ordering, and pin groups are configured in this policy. MAC addresses can be statically assigned or assigned from MAC pool. Ethernet Network Group Policy, Ethernet Network Control Policy, Ethernet QoS, and Ethernet Adapter are required policies for each vNIC.

Table 14 LAN Connectivity Policies

{{lan\_connectivity\_policies}}

Table 15 Server Profile vNICs

{{server\_profile\_vnics}}

### vNIC Templates

A vNIC template consists of common configurations that you can reuse across multiple vNICs, used in various Server Profiles. This approach simplifies network configuration across multiple servers. You can create vNICs from the template using the **Derive** operation while creating the policy. Additionally, you can attach an existing vNIC to a template to utilize the configurations set in the template. These templates can be created with or without override options. The override option allows the configuration of the derived vNIC to override the template configuration.

Table 16 vNIC Templates

{{vnic\_templates}}

### Ethernet Network Group Policy

This policy configures the allowed VLANs and native VLAN for appliance ports, port channels or vNICs. In this deployment, this policy is applicable for ethernet uplink port, ethernet uplink port-channel, and vNICs.

When multiple uplinks are used in a Dis-joint L2 configuration, each ethernet uplink would requires its own Ethernet Network Group Policy.

{{ethernet\_network\_group\_policies}}

### Ethernet Adapter Policy

An Ethernet adapter policy governs the host-side behavior of the adapter, including how the adapter handles traffic. For each VIC Virtual Ethernet Interface, you can configure various features like Virtual Extensible LAN (VXLAN), Network Virtualization using Generic Routing Encapsulation (NVGRE), Accelerated Receive Flow Steering (ARFS), Interrupt settings, and TCP Offload settings.

The Ethernet Adapter policy include the recommended settings for the virtual Ethernet interface, for each supported server operating system. Operating systems are sensitive to the settings in these policies. In general, the storage vendors require non-default adapter settings. You can find the details of these required settings on the support list provided by those vendors.

{{ethernet\_adapter\_policies}}

## Server Profile Fibre-Channel Policies

### SAN Connectivity Policy

Determines the network storage resources and the connections between the server and the SAN on the network. This policy enables you to configure vHBAs that the servers use to communicate with the Storage Area Network. You can use WWPN and WWNN address pools, or static WWPN and WWNN addresses, to add vHBAs and to configure them. You must create the Fibre Channel Adapter, Fibre Channel QoS, and Fibre Channel Network policies as part of the SAN connectivity policy.

Table 17 SAN Connectivity Policies

{{san\_connectivity\_policies}}

Table 18 Server Profile vHBAs

{{server\_profile\_vhbas}}

### vHBA Templates

A vHBA template consists of common configurations that you can reuse across multiple vHBA, used in various Server Profiles. This approach simplifies network configuration across multiple servers. You can create vHBAs from the template using the **Derive** operation while creating the policy. Additionally, you can attach an existing vHBAs to a template to utilize the configurations set in the template. These templates can be created with or without override options. The override option allows the configuration of the derived vHBA to override the template configuration.

Table 19 vHBA Templates

{{vhba\_templates}}

### Fibre Channel Network Policies

A Fibre Channel Network policy governs the Virtual Storage Area Network (VSAN) configuration for the virtual interfaces.

Table 20 FC Network Policies

{{fc\_network\_policies}}

### Fibre Channel Adapter Policy

A Fibre Channel adapter policy governs the host-side behavior of the adapter, including how the adapter handles traffic. You can enable FCP Error Recovery, change the default settings of Queues, and Interrupt handling for performance enhancement.

This policy includes the recommended default configurations for the supported server operating systems. The policy supports nine default configurations. During the policy creation, you can select and import a default configuration.

Table 21 FC Adapater Policies

{{fc\_adapter\_policies}}

## Server Profile Policies

### Boot Order Policies

The Boot Order policy configures the linear ordering of devices and enables you to change the boot order and boot mode. You can also add multiple devices under various device types, rearrange the boot order, and set parameters for each boot device type.

Table 22 Boot Policies

{{boot\_policies}}

### Firmware Policies

This policy allows you to see the firmware present in your systems, as against the firmware baseline. Firmware policy also enables you to bring the firmware of your systems in line with the desired version and thereby enables the drive to compliance.

Table 23 Firmware Policies

{{firmware\_policies}}

### IMC Access Policies

The IMC Access policy allows you to configure your network and associate an IP address from an IP Pool with a server. In-Band IP address, Out-Of-Band IP address, or both In-Band and Out-Of-Band IP addresses can be configured using IMC Access Policy and is supported on Drive Security, SNMP, Syslog, and vMedia policies.

Table 24 IMC Access Policies

{{imc\_access\_policies}}

### Memory Policies

Memory Policy allows you to enable or disable the blocklisting of Dual In-line Memory Modules (DIMMs). When DIMM Blocklisting enabled, the DIMMs that encounter uncorrectable ECC error when the server is up and running will be disabled during next server reboot.

Table 25 Memory Policies

{{memory\_policies}}

### Power Policies

This policy enables the configuration of power redundancy, power profiling, and power restoration for servers.

Table 26 Memory Policies

{{power\_policies}}

### SNMP Policies

The SNMP policy configures the SNMP settings for sending fault and alert information by SNMP traps from the managed devices. This policy supports SNMP versions such as SNMPv1, SNMPv2(includes v2c), and SNMPv3. Any existing SNMP Users or SNMP Traps configured previously on the managed devices are removed and replaced with users or traps that you configure in this policy. If you have not added any users or traps in the policy, the existing users or traps on the server are removed.

Using the SNMP Policy you can enable or disable SNMP, specify the access and community strings, and provide the SNMP user details that is used to retrieve data.

Table 27 SNMP Policies

{{snmp\_policies}}

### Storage Policies

The Storage policy allows you to create drive groups, virtual drives, configure the storage capacity of a virtual drive, and configure the M.2 RAID controllers.

Table 28 Storage Policies

{{storage\_policies}}

### KVM Policies

The KVM console is an interface that emulates a direct keyboard, video, and mouse (KVM) connection to the server. It allows you to control the server from a remote location and to map physical locations to virtual drives that can be accessed by the server during this KVM session.

Enables specific grouping of virtual KVM properties. This policy lets you specify the number of allowed concurrent KVM sessions, port information, and video encryption options.

Table 29 KVM Policies

{{kvm\_policies}}

## Server Profile Pools

### IP Pools

An IP Pool can contain one or more blocks of IPs that will get consumed in sequential order, beginning with the lowest block. IP pools support both IPv4 and IPv6 addresses.

Table 30 IP Pools

{{ip\_pools}}

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

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

Table 31 MAC Pools

{{mac\_pools}}

### WWPN Pools

A World Wide Name (WWN) pool is a collection of WWNs for use by the Fibre Channel vHBAs in a Cisco UCS Domain. You create separate pools for the following:

* WW node names assigned to the server
* WW port names assigned to the server

**Note**: A WWN ID cannot be reused across WWPN and WWNN pools. To ensure the uniqueness of the Cisco UCS WWNNs and WWPNs in the SAN fabric, Cisco Intersight uses the following WWN prefix for all blocks in a pool: 20:00:00:25:B5:xx:xx:xx.

If you use WWN pools in server profiles, you do not have to manually configure the WWNs that will be used by the server associated with the server profile. In a system that implements multi-tenancy, you can use a WWN pool to control the WWNs used by each organization. You assign WWNs to pools in blocks.

**WWNN Pools**

A WWNN pool is a WWN pool that contains only WW node names. If you include a pool of WWNNs in a server profile, the associated server is assigned a WWNN from that pool.

**WWPN Pools**

A WWPN pool is a WWN pool that contains only WW port names. If you include a pool of WWPNs in a server profile, the port on each vHBA of the associated server is assigned a WWPN from that pool.

Table 32 WWPN and WWNN Pools

{{fc\_pools}}

### UUID Pools

A Universally Unique Identifier (UUID) pool is a collection of UUIDs that are assigned to servers. The prefix and suffix of the UUID are variable values. A UUID pool ensures that these variable values are unique for each server associated with a server profile that uses a particular pool to avoid conflicts.

Table 33 UUID Pools

{{uuid\_pools}}