



Configuring Network-Related Settings

This chapter includes the following sections:

- [Server NIC Configuration, on page 1](#)
- [Common Properties Configuration, on page 10](#)
- [Configuring IPv4, on page 12](#)
- [Configuring IPv6, on page 14](#)
- [Configuring ICMP, on page 17](#)
- [Configuring the Server VLAN, on page 18](#)
- [Connecting to a Port Profile, on page 20](#)
- [Network Interface Configuration, on page 21](#)
- [Network Security Configuration, on page 23](#)
- [Network Time Protocol Configuration, on page 25](#)
- [Pinging an IP address, on page 26](#)

Server NIC Configuration

Server NICs

NIC Mode

The NIC mode setting determines which ports can reach the Cisco IMC. The following network mode options are available, depending on your platform:

- **Dedicated**—The management port that is used to access the Cisco IMC.
- **Cisco Card**—Any port on the adapter card that can be used to access the Cisco IMC. The Cisco adapter card has to be installed in a slot with Network the Communications Services Interface protocol support (NCSI).
- **Shared LOM**—Any LOM (LAN on Motherboard) port that can be used to access Cisco IMC.
- **Shared LOM Extended**—Any LOM port or adapter card port that can be used to access Cisco IMC. The Cisco adapter card has to be installed in a slot with NCSI support.



Note **Shared LOM** and **Shared LOM Extended** ports are available only on some C-series servers.



Note For other UCS C-Series M4, M5, C220 M6, and C240 M6 servers, the NIC mode is set to **Shared LOM Extended** by default.

- **Shared OCP**—The OCP adapter card LOM ports are used to access Cisco IMC. You must select either the Active-Active or Active-standby NIC redundancy setting in the following step.
- **Shared OCP Extended**—In this NIC mode, DHCP replies are returned to both the OCP adapter card LOM ports and the Cisco virtual interface card (VIC) ports. If the system determines that the Cisco VIC connection is not getting its IP address from a Cisco UCS Manager system because the server is in standalone mode, further DHCP requests from the Cisco VIC are disabled.



Note **Shared OCP** and **Shared OCP Extended** ports are available only on Cisco UCS C225 M6, C245 M6, C220 M7, and C240 M7 servers.

Default NIC Mode Setting:

- For UCS C-Series C125 M5 servers and S3260 servers, the **NIC Mode** is set to **Cisco Card** by default.

For Cisco UCS C225 M6, C245 M6, C220 M7, and C240 M7 servers:

- if the server has a Cisco VIC card with OCP card, then the default NIC mode is **Shared OCP Extended** and **NIC Redundancy** is set to **active-active**.
- if the server has VIC card populated in NCSI supported slots and no OCP card, then the default NIC mode is **Cisco Card**.
- if the server does not have any VIC card and OCP card, the default NIC mode is **Dedicated** and **NIC Redundancy** is set to **None**.

NIC Redundancy

The following NIC redundancy options are available, depending on the selected NIC mode and your platform:

- **active-active**—If supported, all ports that are associated with the configured NIC mode operate simultaneously. This feature increases throughput and provides multiple paths to the Cisco IMC.
- **active-standby**—If a port that is associated with the configured NIC mode fails, traffic fails over to one of the other ports associated with the NIC mode.



Note If you choose this option, make sure that all ports associated with the configured NIC mode are connected to the same subnet to ensure that traffic is secure regardless of which port is used.

- **None**—In *Dedicated* mode, NIC redundancy is set to *None*.

The available redundancy modes vary depending on the selected network mode and your platform. For the available modes, see the *Hardware Installation Guide* (HIG) for the type of server you are using. The C-Series HIGs are available at the following URL:

http://www.cisco.com/en/US/products/ps10493/prod_installation_guides_list.html

VIC Slots

The VIC slot that can be used for management functions in Cisco card mode.

For C240 M6, C245 M6, and C240 M7, VIC slot options are as follows:

- **Riser 1**—Slot 1 and Slot 2
- **Riser 2**—Slot 4 and Slot 5
- **mLOM**



Note For C240 M6, C245 M6, and C240 M7, after resetting to factory default settings, the slot precedence is as follows:

1. mLOM
2. Riser 1 - Slot 2; and Riser 2 - Slot 5
3. Riser 1 - Slot 1; and Riser 2- Slot 4

For C220 M6, C225 M6, and C220 M7, VIC slot options are as follows:

- **Riser 1**—Slot 1 is selected.
- **Riser 3**—Slot 3 is selected.
- **mLOM**



Note For C220 M6, C225 M6, and C220 M7, after resetting to factory default settings, the slot precedence is as follows:

1. mLOM
2. Riser 1 - Slot 1
3. Riser 3 - Slot 3

For C125 M5, VIC slot option is **Riser 2**.

For C220 M4, C220 M5 and C240 M5 servers, VIC slot options are as follows:

- **Riser 1**—Slot 1 is selected.
- **Riser 2**—Slot 2 is selected.

- **FLEX LOM**—Slot 3 (MLOM) is selected.

For C240 M5 SD servers, VIC slot options are as follows:

- **Riser 2**— Slot 2 is selected.
- **mLOM**—VIC cards in mLOM slot is selected.

For C240 M4 servers, VIC slot options are as follows:

- **Riser 1**—Slot 2 is the primary slot, but you can also use slot 1.
- **Riser 2**—Slot 5 is the primary slot, but you can also use slot 4.
- **FLEX LOM**—Slot 7 (MLOM) is selected.

For C480 M5 ML servers, Cisco card mode slot is Slot 11 and Slot 12.

The following options are available only on some UCS C-Series servers:

- 4
- 5
- 9
- 10



Note This option is available only on some UCS C-Series servers.

Configuring Server NICs

Configure a server NIC when you want to set the NIC mode and NIC redundancy.

Before you begin

You must log in as a user with admin privileges to configure the NIC.

Procedure

	Command or Action	Purpose
Step 1	Server# scope cimc	Enters the Cisco IMC command mode.
Step 2	Server /cimc # scope network	Enters the Cisco IMC network command mode.
Step 3	Server /cimc/network # set mode {dedicated shared_lom shared_lom_10g shipping cisco_card share_lom_ext shared_ocp shared_ocp_ext}	Sets the NIC mode to one of the following: <ul style="list-style-type: none"> • Dedicated—The management port that is used to access the Cisco IMC. • Cisco Card—Any port on the adapter card that can be used to access Cisco IMC. The Cisco adapter card has to be installed in a

	Command or Action	Purpose
		<p>slot with Network the Communications Services Interface protocol support (NCSI).</p> <ul style="list-style-type: none"> • Shared LOM—Any LOM (LAN on Motherboard) port that can be used to access Cisco IMC. • Shared LOM Extended—Any LOM port or adapter card port that can be used to access Cisco IMC. The Cisco adapter card has to be installed in a slot with NCSI support. <p>Note Shared LOM and Shared LOM Extended ports are available only on some C-series servers.</p> <p>Note For other UCS C-Series M4, M5, C220 M6, and C240 M6 servers, the NIC mode is set to Shared LOM Extended by default.</p> <ul style="list-style-type: none"> • Shared OCP—The OCP adapter card LOM ports are used to access Cisco IMC. You must select either the Active-Active or Active-standby NIC redundancy setting in the following step. • Shared OCP Extended—In this NIC mode, DHCP replies are returned to both the OCP adapter card LOM ports and the Cisco virtual interface card (VIC) ports. If the system determines that the Cisco VIC connection is not getting its IP address from a Cisco UCS Manager system because the server is in standalone mode, further DHCP requests from the Cisco VIC are disabled. <p>Note Shared OCP and Shared OCP Extended ports are available only on Cisco UCS C225 M6, C245 M6, C220 M7, and C240 M7 servers.</p> <p>Default NIC Mode Setting:</p>

	Command or Action	Purpose
		<ul style="list-style-type: none"> • For UCS C-Series C125 M5 servers and S3260 servers, the NIC Mode is set to Cisco Card by default. • For Cisco UCS C225 M6, C245 M6, C220 M7, and C240 M7 servers: <ul style="list-style-type: none"> • if the server has a Cisco VIC card with OCP card, then the default NIC mode is Shared OCP Extended and NIC Redundancy is set to active-active. • if the server has VIC card populated in NCSI supported slots and no OCP card, then the default NIC mode is Cisco Card. • if the server does not have any VIC card and OCP card, the default NIC mode is Dedicated and NIC Redundancy is set to None.
Step 4	Server /cimc/network # set vic-slot {none riser1 riser2 mlom}	<p>VIC slot can be set to Cisco cards available in MLOM or supported Risers.</p> <p>For C240 M6, C245 M6, and C240 M7, VIC slot options are as follows:</p> <ul style="list-style-type: none"> • Riser 1—Slot 1 and Slot 2 • Riser 2—Slot 4 and Slot 5 • mLOM <p>Note For C240 M6, C245 M6, and C240 M7, after resetting to factory default settings, the slot precedence is as follows:</p> <ol style="list-style-type: none"> a. mLOM b. Riser 1 - Slot 2; and Riser 2 - Slot 5 c. Riser 1 - Slot 1; and Riser 2 - Slot 4 <p>For C220 M6, C225 M6, and C220 M7, VIC slot options are as follows:</p> <ul style="list-style-type: none"> • Riser 1—Slot 1 is selected. • Riser 3—Slot 3 is selected.

	Command or Action	Purpose
		<ul style="list-style-type: none"> • mLOM <p>Note For C220 M6, C225 M6, and C220 M7, after resetting to factory default settings, the slot precedence is as follows:</p> <ol style="list-style-type: none"> a. mLOM b. Riser 1 - Slot 1 c. Riser 3 - Slot 3 <p>For C125 M5, VIC slot option is Riser 2.</p> <p>For C220 M4, C220 M5 and C240 M5 servers, VIC slot options are as follows:</p> <ul style="list-style-type: none"> • Riser 1—Slot 1 is selected. • Riser 2—Slot 2 is selected. • FLEX LOM—Slot 3 (MLOM) is selected. <p>For C240 SD M5 servers, VIC slot options are as follows:</p> <ul style="list-style-type: none"> • For servers with PCIe Riser 1 and 2B combination: <ul style="list-style-type: none"> • If you select Riser1, you must install the VIC in slot 2. • If you select Riser2, you must install the VIC in slot 5. • For servers with PCIe Riser 1C and 2E combination: <ul style="list-style-type: none"> • If you select Riser1, you must install the VIC in slot 1. • If you select Riser2, you must install the VIC in slot 2. • If you select Flex-LOM, you must install an mLOM-style VIC in the mLOM slot. <p>For C480 M5 ML servers, Cisco card mode slot is Slot 11 and Slot 12.</p> <p>The following options are available only on some UCS C-Series servers:</p> <ul style="list-style-type: none"> • 4

	Command or Action	Purpose
		<ul style="list-style-type: none"> • 5 • 9 • 10 <p>For C240 M4 servers, VIC slot options are as follows:</p> <ul style="list-style-type: none"> • Riser 1—Slot 2 is the primary slot, but you can also use slot 1. • Riser 2—Slot 5 is the primary slot, but you can also use slot 4. • FLEX LOM—Slot 7 (MLOM) is selected. <p>Important VIC slot is applicable for Cisco cards and on some UCS C-Series servers only.</p>
Step 5	Server /cimc/network # set redundancy {none active-active active-standby}	<p>Sets the NIC redundancy mode when the NIC mode is Shared LOM. The redundancy mode can be one of the following:</p> <ul style="list-style-type: none"> • none—The LOM Ethernet ports operate independently and do not fail over if there is a problem. • active-active—If supported, all LOM Ethernet ports are utilized. • active-standby—If one LOM Ethernet port fails, traffic fails over to another LOM port.
Step 6	Server /cimc/network # commit	<p>Commits the transaction to the system configuration.</p> <p>Note The available NIC mode and NIC redundancy mode options may vary depending on your platform. If you select a mode not supported by your server, an error message displays when you save your changes.</p>
Step 7	At the prompt, enter y to confirm.	Configures the server NIC.

Example

This example configures the Cisco IMC network interface:

```
scope cimc
Server /cimc # scope network
Server /cimc/network # set mode cisco_card
Server /cimc/network # set vic-slot <mlom>
Server /cimc/network *# set redundancy <active-active>
Server /cimc/network *# commit
Changes to the network settings will be applied immediately.
You may lose connectivity to the Cisco IMC and may have to log in again.
Do you wish to continue? [y/N] y
Server /cimc/network #
```

Cisco VIC mLOM and OCP Card Replacement Considerations

In Cisco UCS C220 M7, C240 M7, C225 M6 and C245 M6 servers, Cisco IMC network connection may be lost in the following situations, while replacing Cisco VIC mLOM and OCP cards:

- If OCP card is replaced by Cisco VIC card in MLOM Slot and the NIC mode is set to **Shared OCP** or **Shared OCP Extended**.
- If Cisco VIC Card in MLOM Slot is replaced by OCP Card and NIC mode is set to **Cisco-card MLOM**.

Follow these recommendations while replacing Cisco VIC mLOM or OCP cards in Cisco UCS C220 M7, C240 M7, C225 M6 or C245 M6 servers to avoid loss of connectivity:

- Before replacing the card, configure any of the NIC modes that has network connected, other than **Cisco card MLOM**, **Shared OCP**, or **Shared OCP Extended**. After replacing the card, configure the appropriate NIC mode.

To set the NIC mode, refer *Server NIC Configuration* section in [Configuration Guides](#) for your Cisco IMC release.

- Or, after replacing the card, configure the appropriate NIC mode using Cisco IMC Configuration Utility/F8. Refer *Connecting to the Server Locally For Setup* section in [Install and Upgrade Guides](#) for your server.
- Or, after replacing the card, perform factory default settings using Cisco IMC Configuration Utility/F8 then perform the following steps:
 1. Once the server is rebooted, boot the system to Cisco IMC Configuration Utility/F8 then change the default password.
 2. Configure the appropriate NIC mode settings.

Table 1: Factory Default Settings

VIC in mLOM slot	Intel OCP 3.0 NIC in mLOM Slot	VIC in Riser Slot	Dedicated Management Port	NIC Mode for CIMC Access
Yes	No	No	Yes	Cisco Card mode with the card in mLOM Slot

VIC in mLOM slot	Intel OCP 3.0 NIC in mLOM Slot	VIC in Riser Slot	Dedicated Management Port	NIC Mode for CIMC Access
No	Yes	No	Yes	Shared OCP Extended
No	Yes	Yes	Yes	Shared OCP Extended
No	No	Yes	Yes	Cisco Card with VIC SLOT based on precedence: For C220 M7 and C225 M6: <ol style="list-style-type: none"> Riser 1 - Slot 1 Riser 3 - Slot 3 For C240 M7 and C245 M6: <ol style="list-style-type: none"> Riser 1 - Slot 2 Riser 2 - Slot 5 Riser 1 - Slot 1 Riser 2 - Slot 4
No	No	No	Yes	Dedicated

Common Properties Configuration

Overview to Common Properties Configuration

Hostname

The Dynamic Host Configuration Protocol (DHCP) enhancement is available with the addition of the hostname to the DHCP packet, which can either be interpreted or displayed at the DHCP server side. The hostname, which is now added to the options field of the DHCP packet, sent in the DHCP DISCOVER packet that was initially sent to the DHCP server.

The default hostname of the server is changed from ucs-c2XX to CXXX-YYYYYY, where XXX is the model number and YYYYYY is the serial number of the server. This unique string acts as a client identifier, allows you to track and map the IP addresses that are leased out to Cisco IMC from the DHCP server. The default serial number is provided by the manufacturer as a sticker or label on the server to help you identify the server.

Dynamic DNS

Dynamic DNS (DDNS) is used to add or update the resource records on the DNS server from Cisco IMC. You can enable Dynamic DNS by using either the web UI or CLI. When you enable the DDNS option, the DDNS service records the current hostname, domain name, and the management IP address and updates the resource records in the DNS server from Cisco IMC.



Note The DDNS server deletes the prior resource records (if any) and adds the new resource records to the DNS server if any one of the following DNS configuration is changed:

- Hostname
- Domain name in the LDAP settings
- When DDNS and DHCP are enabled, if the DHCP gets a new IP address or DNS IP or domain name due to a change in a network or a subnet.
- When DHCP is disabled and if you set the static IP address by using CLI or web UI.
- When you enter the **dns-use-dhcp** command.

Dynamic DNS Update Domain— You can specify the domain. The domain could be either main domain or any sub-domain. This domain name is appended to the hostname of the Cisco IMC for the DDNS update.

Configuring Common Properties

Use common properties to describe your server.

Before you begin

You must log in as a user with admin privileges to configure common properties.

Procedure

	Command or Action	Purpose
Step 1	Server# scope cimc	Enters Cisco IMC command mode.
Step 2	Server /cimc # scope network	Enters Cisco IMC network command mode.
Step 3	Server /cimc/network # set hostname <i>host-name</i>	Specifies the name of the host. When you modify the hostname, you are prompted to confirm whether you want to create a new self-signed certificate with Common Name (CN) as the new hostname. If you enter y at the prompt, a new self-signed certificate is created with CN as the new hostname. If you enter n at the prompt, only the hostname is changed and no certificate will be generated.

	Command or Action	Purpose
Step 4	(Optional) Server /cimc/network # set ddns-enabled	Enables the DDNS service for Cisco IMC
Step 5	(Optional) Server /cimc/network # set ddns-update-domain <i>value</i>	Updates the selected domain or its subdomain.
Step 6	Server /cimc/network # commit	Commits the transaction to the system configuration.
Step 7	At the prompt, enter y to confirm.	Configures common properties.

Example

This example shows how to configure the common properties:

```
Server# scope cimc
Server /cimc # scope network
Server /cimc/network # set hostname Server
Create new certificate with CN as new hostname? [y|N]
y
New certificate will be generated on committing changes.
All HTTPS and SSH sessions will be disconnected.
Server /cimc/network # set ddns-enabled
Server /cimc/network # set ddns-update-domain 1.2.3.4
Server /cimc/network *# commit
Changes to the network settings will be applied immediately.
You may lose connectivity to the Cisco IMC and may have to log in again.
Do you wish to continue? [y/N] y
Server /cimc/network #
```

What to do next

Changes to the network are applied immediately. You might lose connectivity to Cisco IMC and have to log in again. Because of the new SSH session created, you may be prompted to confirm the host key.

Configuring IPv4

Before you begin

You must log in as a user with admin privileges to configure IPv4 network settings.

Procedure

	Command or Action	Purpose
Step 1	Server# scope cimc	Enters the Cisco IMC command mode.
Step 2	Server /cimc # scope network	Enters the Cisco IMC network command mode.

	Command or Action	Purpose
Step 3	Server /cimc/network # set dhcp-enabled {yes no}	Selects whether the Cisco IMC uses DHCP. Note If DHCP is enabled, we recommend that the DHCP server be configured to reserve a single IP address for the Cisco IMC. If the Cisco IMC is reachable through multiple ports on the server, the single IP address must be reserved for the full range of MAC addresses of those ports.
Step 4	Server /cimc/network # set v4-addr <i>ipv4-address</i>	Specifies the IP address for the Cisco IMC.
Step 5	Server /cimc/network # set v4-netmask <i>ipv4-netmask</i>	Specifies the subnet mask for the IP address.
Step 6	Server /cimc/network # set v4-gateway <i>gateway-ipv4-address</i>	Specifies the gateway for the IP address.
Step 7	Server /cimc/network # set dns-use-dhcp {yes no}	Selects whether the Cisco IMC retrieves the DNS server addresses from DHCP.
Step 8	Server /cimc/network # set preferred-dns-server <i>dns1-ipv4-address</i>	Specifies the IP address of the primary DNS server.
Step 9	Server /cimc/network # set alternate-dns-server <i>dns2-ipv4-address</i>	Specifies the IP address of the secondary DNS server.
Step 10	Server /cimc/network # commit	Commits the transaction to the system configuration.
Step 11	At the prompt, enter y to confirm.	Configures IPv4.
Step 12	Server /cimc/network # show [detail]	(Optional) Displays the IPv4 network settings.

Example

This example configures and displays the IPv4 network settings:

```
Server# scope cimc
Server /cimc # scope network
Server /cimc/network # set dhcp-enabled yes
Server /cimc/network *# set v4-addr 10.20.30.11
Server /cimc/network *# set v4-netmask 255.255.248.0
Server /cimc/network *# set v4-gateway 10.20.30.1
Server /cimc/network *# set dns-use-dhcp-enabled no
Server /cimc/network *# set preferred-dns-server 192.168.30.31
Server /cimc/network *# set alternate-dns-server 192.168.30.32
Server /cimc/network *# commit
Changes to the network settings will be applied immediately.
You may lose connectivity to the Cisco IMC and may have to log in again.
```

```

Do you wish to continue? [y/N] y
Server /cimc/network # show detail
Network Setting:
  IPv4 Address: 10.20.30.11
  IPv4 Netmask: 255.255.248.0
  IPv4 Gateway: 10.20.30.1
  DHCP Enabled: yes
  Obtain DNS Server by DHCP: no
  Preferred DNS: 192.168.30.31
  Alternate DNS: 192.168.30.32
  IPv6 Enabled: no
  IPv6 Address: ::
  IPv6 Prefix: 64
  IPv6 Gateway: ::
  IPv6 Link Local: ::
  IPv6 SLAAC Address: ::
  IPV6 DHCP Enabled: no
  IPV6 Obtain DNS Server by DHCP: no
  IPV6 Preferred DNS: ::
  IPV6 Alternate DNS: ::
  VLAN Enabled: no
  VLAN ID: 1
  VLAN Priority: 0
  Port Profile:
  Hostname: C240-FCH1938V17L
  MAC Address: E4:AA:5D:AD:19:81
  NIC Mode: shared_lom_ext
  NIC Redundancy: active-active
  VIC Slot: riser1
  Auto Negotiate: no
  Admin Network Speed: NA
  Admin Duplex: NA
  Operational Network Speed: NA
  Operational Duplex: NA

Server /cimc/network #

```

Configuring IPv6

Before you begin

You must log in as a user with admin privileges to configure IPv6 network settings.

Procedure

	Command or Action	Purpose
Step 1	Server# scope cimc	Enters the Cisco IMC command mode.
Step 2	Server /cimc # scope network	Enters the Cisco IMC network command mode.
Step 3	Server /cimc/network # set v6-enabled {yes no}	Enables IPv6.

	Command or Action	Purpose
Step 4	Server /cimc/network # set v6-dhcp-enabled {yes no}	Selects whether the Cisco IMC uses DHCP. Note If DHCP is enabled, we recommend that the DHCP server be configured to reserve a single IPv6 address for the Cisco IMC. If the Cisco IMC is reachable through multiple ports on the server, the single IPv6 address must be reserved for the full range of MAC addresses of those ports.
Step 5	Server /cimc/network # set v6-addr <i>ipv6-address</i>	Specifies the IP address for the Cisco IMC.
Step 6	Server /cimc/network # set v6-prefix <i>ipv6-prefix-length</i>	Specifies the prefix length for the IP address.
Step 7	Server /cimc/network # set v6-gateway <i>gateway-ipv6-address</i>	Specifies the gateway for the IP address.
Step 8	Server /cimc/network # set v6-dns-use-dhcp {yes no}	Selects whether the Cisco IMC retrieves the DNS server addresses from DHCP. Note You can use this option only when DHCP enabled.
Step 9	Server /cimc/network # set v6-preferred-dns-server <i>dns1-ipv6-address</i>	Specifies the IP address of the primary DNS server.
Step 10	Server /cimc/network # set v6-alternate-dns-server <i>dns2-ipv6-address</i>	Specifies the IP address of the secondary DNS server.
Step 11	Server /cimc/network # commit	Commits the transaction to the system configuration.
Step 12	At the prompt, enter y to confirm.	Configures IPv6.
Step 13	Server /cimc/network # show [detail]	(Optional) Displays the IPv6 network settings.

Example

This example enables static IPv6 and displays the IPv6 network settings:

```
Server# scope cimc
Server /cimc # scope network
Server /cimc/network # set v6-enabled yes
Server /cimc/network *# set v6-addr 2010:201::279
Server /cimc/network *# set v6-gateway 2010:201::1
Server /cimc/network *# set v6-prefix 64
Server /cimc/network *# set v6-dns-use-dhcp no
Server /cimc/network *# set v6-preferred-dns-server 2010:201::100
```

```

Server /cimc/network *# set v6-alternate-dns-server 2010:201::101
Changes to the network settings will be applied immediately.
You may lose connectivity to the Cisco IMC and may have to log in again.
Server /cimc/network *# commit
Changes to the network settings will be applied immediately.
You may lose connectivity to the Cisco IMC and may have to log in again.
Do you wish to continue? [y/N] y
Server /cimc/network # show detail
Network Setting:
  IPv4 Enabled: yes
  IPv4 Address: 10.106.145.76
  IPv4 Netmask: 255.255.255.0
  IPv4 Gateway: 10.106.145.1
  DHCP Enabled: yes
  DDNS Enabled: yes
  DDNS Update Domain: example.com
  Obtain DNS Server by DHCP: no
  Preferred DNS: 171.70.168.183
  Alternate DNS: 0.0.0.0
  IPv6 Enabled: yes
  IPv6 Address: 2010:201::279
  IPv6 Prefix: 64
  IPv6 Gateway: 2010:201::1
  IPv6 Link Local: fe80::523d:e5ff:fe9d:395d
  IPv6 SLAAC Address: 2010:201::523d:e5ff:fe9d:395d
  IPV6 DHCP Enabled: no
  IPV6 Obtain DNS Server by DHCP: no
  IPV6 Preferred DNS: 2010:201::100
  IPV6 Alternate DNS: 2010:201::101
  VLAN Enabled: no
  VLAN ID: 1
  VLAN Priority: 0
  Port Profile:
  Hostname: CIMC_C220
  MAC Address: 50:3D:E5:9D:39:5C
  NIC Mode: dedicated
  NIC Redundancy: none
  Network Speed: 100Mbps
  Duplex: full
  Auto Negotiate: no
  Admin Network Speed: NA
  Admin Duplex: NA
  Operational Network Speed: NA
  Operational Duplex: NA

```

```
Server /cimc/network #
```

This example enables DHCP for IPv6 and displays the IPv6 network settings:

```

Server# scope cimc
Server /cimc # scope network
Server /cimc/network # set v6-enabled yes
Server /cimc/network *# set v6-dhcp-enabled yes
Changes to the network settings will be applied immediately.
You may lose connectivity to the Cisco IMC and may have to log in again.
Server /cimc/network *# commit
Changes to the network settings will be applied immediately.
You may lose connectivity to the Cisco IMC and may have to log in again.
Do you wish to continue? [y/N] y
Server /cimc/network # show detail
Network Setting:
  IPv4 Enabled: yes
  IPv4 Address: 10.106.145.76
  IPv4 Netmask: 255.255.255.0

```



```

IPv4 Gateway: 10.106.145.1
DHCP Enabled: yes
DDNS Enabled: yes
DDNS Update Domain: example.com
Obtain DNS Server by DHCP: no
Preferred DNS: 171.70.168.183
Alternate DNS: 0.0.0.0
IPv6 Enabled: yes
IPv6 Address: 2010:201::253
IPv6 Prefix: 64
IPv6 Gateway: fe80::222:dff:fec2:8000
IPv6 Link Local: fe80::523d:e5ff:fe9d:395d
IPv6 SLAAC Address: 2010:201::523d:e5ff:fe9d:395d
IPV6 DHCP Enabled: yes
IPV6 Obtain DNS Server by DHCP: no
IPV6 Preferred DNS: ::
IPV6 Alternate DNS: ::
VLAN Enabled: no
VLAN ID: 1
VLAN Priority: 0
Port Profile:
Hostname: CIMC_C220
MAC Address: 50:3D:E5:9D:39:5C
NIC Mode: dedicated
NIC Redundancy: none
Network Speed: 100Mbps
Duplex: full
Auto Negotiate: no
Admin Network Speed: NA
Admin Duplex: NA
Operational Network Speed: NA
Operational Duplex: NA

```

```
Server /cimc/network #
```

Configuring ICMP

In the release 4.1(3b), Cisco IMC allows you to enable or disable processing of incoming ICMP redirect and destination unreachable packets on BMC.



Note This option is available only on some Cisco UCS M5 servers.

Procedure

	Command or Action	Purpose
Step 1	Server# scope cimc	Enters the Cisco IMC command mode.
Step 2	Server /cimc # scope network	Enters the Cisco IMC network command mode.
Step 3	Server /cimc/network # scope icmp-configuration	Enters the ICMP configuration mode.
Step 4	Server /cimc/network/icmp-configuration # show-detail	Displays the ICMP configuration settings.

	Command or Action	Purpose
Step 5	Server /cimc/network/icmp-configuration # set destination-unreachable-enabled yes	Enables the Destination Unreachable configuration setting in ICMP.
Step 6	Server /cimc/network/icmp-configuration # set redirect-enabled yes	Enables the redirect configuration setting in ICMP.
Step 7	Server /cimc/network/icmp-configuration # commit	Commits the transaction to the system configuration.
Step 8	Server /cimc/network/icmp-configuration # show-detail	Displays the updated ICMP configuration settings.

Example

This example shows how to configure the ICMP configuration settings:

```
Server# scope cimc
Server /cimc # scope network
Server /cimc/network # scope icmp-configuration
Server /network/icmp-configuration # show detail
ICMP Settings:
  Destination Unreachable Enabled: no
  Redirect Enabled: no
Server /cimc/network/icmp-configuration # set destination-unreachable-enabled yes
Server /cimc/network/icmp-configuration # set redirect yes
Server /cimc/network/icmp-configuration # commit
Server /cimc/network/icmp-configuration # show detail
ICMP Settings:
  Destination Unreachable Enabled: yes
  Redirect Enabled: yes
Server /cimc/network/icmp-configuration #
```

Configuring the Server VLAN

Before you begin

You must be logged in as admin to configure the server VLAN.

Procedure

	Command or Action	Purpose
Step 1	Server# scope cimc	Enters the Cisco IMC command mode.
Step 2	Server /cimc # scope network	Enters the Cisco IMC network command mode.
Step 3	Server /cimc/network # set vlan-enabled {yes no}	Selects whether the Cisco IMC is connected to a VLAN.
Step 4	Server /cimc/network # set vlan-id id	Specifies the VLAN number.

	Command or Action	Purpose
Step 5	Server /cimc/network # set vlan-priority <i>priority</i>	Specifies the priority of this system on the VLAN.
Step 6	Server /cimc/network # commit	Commits the transaction to the system configuration.
Step 7	At the prompt, enter y to confirm.	Configures the server LAN.
Step 8	Server /cimc/network # show [detail]	(Optional) Displays the network settings.

Example

This example configures the server VLAN:

```

Server# scope cimc
Server /cimc # scope network
Server /cimc/network # set vlan-enabled yes
Server /cimc/network *# set vlan-id 10
Server /cimc/network *# set vlan-priority 32
Server /cimc/network *# commit
Changes to the network settings will be applied immediately.
You may lose connectivity to the Cisco IMC and may have to log in again.
Do you wish to continue? [y/N] y
Server /cimc/network # show detail
Network Setting:
  IPv4 Address: 10.20.30.11
  IPv4 Netmask: 255.255.248.0
  IPv4 Gateway: 10.20.30.1
  DHCP Enabled: yes
  Obtain DNS Server by DHCP: no
  Preferred DNS: 192.168.30.31
  Alternate DNS: 192.168.30.32
  IPv6 Enabled: no
  IPv6 Address: ::
  IPv6 Prefix: 64
  IPv6 Gateway: ::
  IPv6 Link Local: ::
  IPv6 SLAAC Address: ::
  IPV6 DHCP Enabled: no
  IPV6 Obtain DNS Server by DHCP: no
  IPV6 Preferred DNS: ::
  IPV6 Alternate DNS: ::
  VLAN Enabled: yes
  VLAN ID: 10
  VLAN Priority: 32
  Port Profile:
  Hostname: C240-FCH1938V17L
  MAC Address: E4:AA:5D:AD:19:81
  NIC Mode: shared_lom_ext
  NIC Redundancy: active-active
  VIC Slot: riser1
  Auto Negotiate: no
  Admin Network Speed: NA
  Admin Duplex: NA
  Operational Network Speed: NA
  Operational Duplex: NA

Server /cimc/network #

```

Connecting to a Port Profile



Note You can configure a port profile or a VLAN, but you cannot use both. If you want to use a port profile, make sure the **set vlan-enabled** command is set to **no**.

Before you begin

You must be logged in as admin to connect to a port profile.

Procedure

	Command or Action	Purpose
Step 1	Server# scope cimc	Enters the Cisco IMC command mode.
Step 2	Server /cimc # scope network	Enters the Cisco IMC network command mode.
Step 3	Server /cimc/network # set port-profile <i>port_profile_name</i>	Specifies the port profile Cisco IMC should use to configure the management interface, the virtual Ethernet, and the VIF on supported adapter cards such as the Cisco UCS VIC 1225 Virtual Interface Card. Enter up to 80 alphanumeric characters. You cannot use spaces or other special characters except for - (hyphen) and _ (underscore). In addition, the port profile name cannot begin with a hyphen. Note The port profile must be defined on the switch to which this server is connected.
Step 4	Server /cimc/network # commit	Commits the transaction to the system configuration.
Step 5	At the prompt, enter y to confirm.	Connects to a port profile.
Step 6	(Optional) Server /cimc/network # show [detail]	Displays the network settings.

Example

This example connects to port profile abcde12345:

```
Server# scope cimc
Server /cimc # scope network
Server /cimc/network # set port-profile abcde12345
Server /cimc/network *# commit
```

```

Changes to the network settings will be applied immediately.
You may lose connectivity to the Cisco IMC and may have to log in again.
Do you wish to continue? [y/N] y
Server /cimc/network # show detail
Network Setting:
  IPv4 Address: 10.193.66.174
  IPv4 Netmask: 255.255.248.0
  IPv4 Gateway: 10.193.64.1
  DHCP Enabled: no
  Obtain DNS Server by DHCP: no
  Preferred DNS: 0.0.0.0
  Alternate DNS: 0.0.0.0
  IPv6 Enabled: no
  IPv6 Address: ::
  IPv6 Prefix: 64
  IPv6 Gateway: ::
  IPv6 Link Local: ::
  IPv6 SLAAC Address: ::
  IPV6 DHCP Enabled: no
  IPV6 Obtain DNS Server by DHCP: no
  IPV6 Preferred DNS: ::
  IPV6 Alternate DNS: ::
  VLAN Enabled: no
  VLAN ID: 1
  VLAN Priority: 0
  Port Profile: abcde12345
  Hostname: C240-FCH1938V17L
  MAC Address: E4:AA:5D:AD:19:81
  NIC Mode: shared_lom_ext
  NIC Redundancy: active-active
  VIC Slot: riser1
  Auto Negotiate: no
  Admin Network Speed: NA
  Admin Duplex: NA
  Operational Network Speed: NA
  Operational Duplex: NA

Server /cimc/network #

```

Network Interface Configuration

Overview to Network Interface Configuration

This support is added to configure network speed and duplex mode for the Cisco IMC management port. Auto Negotiation mode can be set for dedicated mode only. When auto negotiation is enabled the network port speed and duplex settings are ignored by the system and Cisco IMC retains the speed at which the switch is configured. When auto negotiation is disabled, you can configure the network port speed (10 Mbps, 100 Mbps, or 1 Gbps) and set the duplex value at either full or half.

Port Properties can be managed in the following two modes:

- **Admin Mode**—You can configure the network speed and duplex values by disabling the **Auto Negotiation** option. The default value of the network speed in the admin mode is 100 Mbps and the duplex mode is set to Full. Before changing the network speed ensure that the switch you connected to has the same port speed.

- **Operation Mode**—Displays the operation network port speed and duplex values. If you enabled auto negotiation mode, the network port speed and duplex details of the switch are displayed. If unchecked, the network port speed and duplex values that you set at the **Admin Mode** are displayed.

When you reset Cisco IMC 1.5(x), 2.0(1), and 2.0(3) versions to factory defaults, **Shared LOM** mode is configured by default.

Configuring Interface Properties

The settings on the switch must match with the Cisco IMC settings to avoid any speed or duplex mismatch.



Important This action is available only on some UCS C-Series servers.

Procedure

	Command or Action	Purpose
Step 1	Server # scope cimc	Enters the Cisco IMC command mode.
Step 2	Server/cimc # scope network	Enters the network command mode.
Step 3	Server/cimc/network* # set mode dedicated	Enters dedicated command mode.
Step 4	Server/cimc/network # set auto-negotiate {yes no}	Enables or disables auto negotiation command mode. <ul style="list-style-type: none"> • If you enter yes, the network port speed and duplex settings are ignored by the system and Cisco IMC retains the speed at which the switch is configured. • If you enter no, you can configure the network port speed and duplex values.
Step 5	Server/cimc/network # set net-speed {10 Mbps 100 Mbps 1 Gbps}	Sets specified network port speed. <p>Note This option is available only if auto-negotiate is set to no. Before changing the port speed, ensure that the switch you connected to has the same port speed. When auto-negotiate is set to yes, by default the network port speed is set to 100 Mbps.</p>
Step 6	Server/cimc/network* # set duplex {full half}	Sets specified duplex mode type. By default, the duplex mode is set to Full . <p>Note For network speed of 1 Gbps, only full duplex mode is allowed.</p>

	Command or Action	Purpose
Step 7	Server/cimc/network* # commit	Commits the transaction to the system.

Example

This example shows how to configure the interface properties and commit the transaction:

```
Server # scope cimc
Server/cimc # scope network
Server/cimc/network* # set mode dedicated
Server/cimc/network # set auto-negotiate no
Warning: You have chosen to set auto-negotiate to no
Please set speed and duplex
If not set then a default speed of 100Mbps and duplex full will be applied
Server/cimc/network* # commit
Server/cimc/network* # set net-speed 100 Mbps
Server/cimc/network # set duplex full
Server/cimc/network* # commit
Changes to the network settings will be applied immediately.
You may lose connectivity to the Cisco IMC and may have to log in again.
Do you wish to continue? [y/N] y
Server/cimc/network #
```

Network Security Configuration

Network Security

The Cisco IMC uses IP blocking as network security. IP blocking prevents the connection between a server or website and certain IP addresses or ranges of addresses. IP blocking effectively bans undesired connections from those computers to a website, mail server, or other Internet servers.

IP banning is commonly used to protect against denial of service (DoS) attacks. Cisco IMC bans IP addresses by setting up an IP blocking fail count.

Configuring Network Security

Configure network security if you want to set up an IP blocking fail count.

Before you begin

You must log in as a user with admin privileges to configure network security.

Procedure

	Command or Action	Purpose
Step 1	Server# scope cimc	Enters the Cisco IMC command mode.
Step 2	Server /cimc # scope network	Enters the Cisco IMC network command mode.

	Command or Action	Purpose
Step 3	Server /cimc/network # scope ipblocking	Enters the IP blocking command mode.
Step 4	Server /cimc/network/ipblocking # set enabled {yes no}	Enables or disables IP blocking.
Step 5	Server /cimc/network/ipblocking # set fail-count fail-count	<p>Sets the number of times a user can attempt to log in unsuccessfully before the system locks that user out for a specified length of time.</p> <p>The number of unsuccessful login attempts must occur within the time frame specified in the IP Blocking Fail Window field.</p> <p>Enter an integer between 3 and 10.</p>
Step 6	Server /cimc/network/ipblocking # set fail-window fail-seconds	<p>Sets the length of time, in seconds, in which the unsuccessful login attempts must occur in order for the user to be locked out.</p> <p>Enter an integer between 60 and 120.</p>
Step 7	Server /cimc/network/ipblocking # set penalty-time penalty-seconds	<p>Sets the number of seconds the user remains locked out if they exceed the maximum number of login attempts within the specified time window.</p> <p>Enter an integer between 300 and 900.</p>
Step 8	Server /cimc/network/ipblocking # commit	Commits the transaction to the system configuration.
Step 9	Server /cimc/network/ipblocking # exit	Exits the IP blocking to the network command mode.
Step 10	Server /cimc/network # scope ipfiltering	Enters the IP filtering command mode.
Step 11	Server /cimc/network/ipfiltering # set enabled {yes no}	Enables or disables IP filtering. At the prompt enter y to enable IP filtering.
Step 12	Server /cimc/network/ipfiltering # set filter-1 IPv4 or IPv6 address or a range of IP addresses	You can set four IP filters. You can assign an IPv4 or IPv6 IP address or a range of IP addresses.
Step 13	Server /cimc/network/ipfiltering # commit	Commits the transaction to the system configuration.

Example

This example configures network security:

```
Server# scope cimc
Server /cimc # scope network
Server /cimc/network # scope ipblocking
Server /cimc/network/ipblocking # set enabled yes
```



```

Server /cimc/network/ipblocking *# set fail-count 5
Server /cimc/network/ipblocking *# set fail-window 90
Server /cimc/network/ipblocking *# set penalty-time 600
Server /cimc/network/ipblocking *# commit
Server /cimc/network/ipblocking # exit
Server /cimc/network # scope ipfiltering
Server /cimc/network/ipfiltering # set enabled yes
This will enable IP Filtering
Do you wish to continue? [y/N] y
Server /cimc/network/ipfiltering *# set filter-1 1.1.1.1-255.255.255.255
                               set filter-2 10.10.10.10
                               set filter-3 2001:xxx::-2xxx:xx8::0001
                               set filter-4
2001:xxx::-2xxx:xx8::0001-2001:xxx::-2xxx:xx8::0020
Server /cimc/network/ipfiltering *# commit
Changes to the ipfiltering will be applied immediately.
You may lose connectivity to the Cisco IMC and may have to log in again.
Do you wish to continue? [y/N] Y

```

Network Time Protocol Configuration

Configuring Network Time Protocol Settings

By default, when Cisco IMC is reset, it synchronizes the time with the host. With the introduction of the NTP service, you can configure Cisco IMC to synchronize the time with an NTP server. The NTP server does not run in Cisco IMC by default. You must enable and configure the NTP service by specifying the IP/DNS address of at least one server or a maximum of four servers that function as NTP servers or time source servers. When you enable the NTP service, Cisco IMC synchronizes the time with the configured NTP server. The NTP service can be modified only through Cisco IMC.



Note To enable the NTP service, it is preferable to specify the IP address of a server rather than the DNS address.

Before you begin

You must log in with admin privileges to perform this task.

Procedure

	Command or Action	Purpose
Step 1	Server# scope cimc	Enters the Cisco IMC command mode.
Step 2	Server /cimc # scope network	Enters network command mode.
Step 3	Server /cimc/network # scope ntp	Enters NTP service command mode.
Step 4	Server /cimc/network/ntp # set enabled yes	Enables the NTP service on the server.
Step 5	Server /cimc/network/ntp* # commit	Commits the transaction.

	Command or Action	Purpose
Step 6	Server /cimc/network/ntp # set server-1 10.120.33.44	Specifies the IP/DNS address of one of the four servers that act as an NTP server or the time source server.
Step 7	Server /cimc/network/ntp # set server-2 10.120.34.45	Specifies the IP/DNS address of one of the four servers that act as an NTP server or the time source server.
Step 8	Server /cimc/network/ntp # set server-3 10.120.35.46	Specifies the IP/DNS address of one of the four servers that act as an NTP server or the time source server.
Step 9	Server /cimc/network/ntp # set server-4 10.120.36.48	Specifies the IP/DNS address of one of the four servers that act as an NTP server or the time source server.
Step 10	Server /cimc/network/ntp # commit	Commits the transaction.

Example

This example shows how to configure the NTP service:

```
Server # scope cimc
Server /cimc # scope network
Server /cimc/network # scope ntp
Server /cimc/network/ntp # set enabled yes
Warning: IPMI Set SEL Time Command will be
disabled if NTP is enabled.
Do you wish to continue? [y|N]
y
Server /cimc/network/ntp* # commit
Server /cimc/network/ntp # set server-1 10.120.33.44
Server /cimc/network/ntp* # set server-2 10.120.34.45
Server /cimc/network/ntp* # set server-3 10.120.35.46
Server /cimc/network/ntp* # set server-4 10.120.36.48
Server /cimc/network/ntp* # commit
Server /cimc/network/ntp #
```

Pinging an IP address

Ping an IP address when you want to validate network connectivity with the IP address in the Cisco IMC.

Before you begin

You must log in as a user with administration privileges to ping an IP address.

Procedure

	Command or Action	Purpose
Step 1	Server# scope cimc	Enters the CIMC command mode.

	Command or Action	Purpose
Step 2	Server /cimc # scope network	Enters the CIMC network command mode.
Step 3	Server /cimc /network# ping IP address retriesnumber timeout.seconds	<p>Pings the IP address or host name for a specified number of times until timeout.</p> <ul style="list-style-type: none"> • IP address/hostname - The IP address or the host name of the server. • Number of retries - The number of times the system tries to connect to the server. Default value is 3. Valid range is from 1 to 10. • Timeout - The number of seconds the system waits before it stops pinging. Default maximum value is 20 seconds. Valid range is from 1 to 20 seconds.
Step 4	Server /cimc/network # commit	Commits the transaction to the system configuration.
Step 5	At the prompt, enter y to confirm.	Pings the IP address.

Example

This example pings an IP address:

```

Server# scope cimc
Server /cimc # scope network
Server /cimc/network # ping 10.10.10.10
Server /cimc/network *# commit
Changes to the network settings will be applied immediately.
You may lose connectivity to the Cisco IMC and may have to log in again.
Do you wish to continue? [y/N] y
Server /cimc/network #

```

