Configuring Network-Related Settings

This chapter includes the following sections:

- Server NIC Configuration, on page 1
- Common Properties Configuration, on page 4
- Configuring Single IP Properties, on page 6
- Configuring IPv4, on page 7
- Configuring IPv6, on page 10
- Configuring ICMP, on page 14
- Configuring VLAN, on page 15
- Connecting to a Port Profile, on page 17
- Configuring Interface Properties, on page 19
- Network Security Configuration, on page 20
- Network Time Protocol Configuration, on page 22
- Pinging an IP address, on page 23

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 and M5 servers, the NIC mode is set to **Shared LOM Extended** by default.

Default NIC Mode Setting:

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

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.

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 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.

SUMMARY STEPS

1. Server # **scope network**
2. Server /network # **set mode** {**dedicated** | **cisco_card**}
3. Server /network # **set redundancy** {**none** | **active-active** | **active-standby**}
4. Server /network # **commit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Server # **scope network**	Enters the network command mode.
Step 2	Server /network # **set mode** {**dedicated** | **cisco_card**}	Sets the NIC mode to one of the following: • Dedicated—The management Ethernet port is used to access the . • Cisco card—The ports on the adapter card are used to access the .
Step 3	Server /network # **set redundancy** {**none** | **active-active** | **active-standby**}	Sets the NIC redundancy mode when the NIC mode is Shared LOM. The redundancy mode can be one of the following: • **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 4	Server /network # **commit**	Commits the transaction to the system configuration.

	Command or Action	Purpose
		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.

Example

This example configures the network interface:

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 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.

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.

SUMMARY STEPS

1. Server # **scope network**
2. Server /network # **set hostname-bmc1 hostname-bmc2hostname-cmc1hostname-cmc2***host-name*
3. Server /network # **commit**
4. At the prompt, enter **y** to confirm.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Server # **scope network**	Enters the network command mode.
Step 2	Server /network # **set hostname-bmc1 hostname-bmc2hostname-cmc1hostname-cmc2***host-name*	Specifies the name of the host for the following components: • **BMC 1** • **BMC 2** • **CMC 1** • **CMC 2** 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.
Step 3	Server /network # **commit**	Commits the transaction to the system configuration.
Step 4	At the prompt, enter **y** to confirm.	Configures common properties.

Example

This example shows how to configure the common properties:

```
Server # scope network
Server /network # set hostname-cmc1 cmc1
Server /network *# set ddns-enabled
Server /network *# set ddns-update-domain 1.2.3.4
Server /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 /network #
```

What to do next

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

Configuring Single IP Properties

Before you begin

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

SUMMARY STEPS

1. Server # **scope network**
2. Server /network # **set enable-single-ip** {**yes** | **no**}
3. Server /network # **set starting-port** *port number*
4. Server /network * # **commit**
5. Server /network # **show** [**detail**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	Server # **scope network**	Enters the network command mode.
Step 2	Server /network # **set enable-single-ip** {**yes** | **no**}	Enables the Single IP feature.
Step 3	Server /network # **set starting-port** *port number*	Specifies the starting port number for the single IP configuration. When single IP is enabled ports 9000-9006 are used bu Cisco IMC for the starting port configuration. These ports cannot be used for any other configuration.
Step 4	Server /network * # **commit**	Choose **y** at the confirmation prompt, commits the transaction to the system configuration.
Step 5	Server /network # **show** [**detail**]	(Optional) Displays the network settings.

Example

This example configures and displays the single IP network settings:

```
Server# scope network
Server /network # set enable-single-ip yes
Server /network * #  set starting-port 9000
Server /network * #  commit
Server /network # show detail
Chassis Network Setting:
    IPv4 Enabled: yes
    SingleIP Mode: yes
    Starting Port: 10000
    IPv4 Netmask: 255.255.255.0
    IPv4 Gateway: 10.104.236.1
    DHCP Enabled: yes
    DDNS Enabled: yes
    DDNS Update Domain:
    DDNS Refresh Interval(0-8736 Hr): 0
    Obtain DNS Server by DHCP: yes
    Preferred DNS: 10.104.236.99
```

```
    Alternate DNS: 0.0.0.0
    IPv6 Enabled: yes
    IPv6 Prefix: 64
    IPv6 Gateway: fe80::3e08:f6ff:fe21:29c0
    IPV6 DHCP Enabled: yes
    IPV6 Obtain DNS Server by DHCP: yes
    IPV6 Preferred DNS: ::
    IPV6 Alternate DNS: ::
    VLAN Enabled: no
    VLAN ID: 1
    VLAN Priority: 0
    Port Profile:
    NIC Mode: cisco_card
    NIC Redundancy: active-active
    SIOC Slot: 2
    Management IPv4 Address: 10.104.236.135
    Management IPv6 Address: ::
    Management Hostname: S3260-FOX2111P7VD
    Auto Negotiate: no
    Admin Network Speed: NA
    Admin Duplex: NA
    Operational Network Speed: NA
    Operational Duplex: NA
CMC 1 Network Setting:
    IPv6 Address CMC 1: ::
    IPv6 Link Local CMC 1: ::
    IPv6 SLAAC Address CMC 1: ::
    Hostname CMC 1: UCS-C3260-FCH21277KB8-1
    MAC Address CMC 1: 96:09:5C:EF:B6:32
CMC 2 Network Setting:
    IPv6 Address CMC 2: ::
    IPv6 Link Local CMC 2: fe80::522f:a8ff:fed2:34aa
    IPv6 SLAAC Address CMC 2: ::
    Hostname CMC 2: UCS-C3260-FCH21277KCA-2
    MAC Address CMC 2: 50:2F:A8:D2:34:AA
BMC 1 Network Setting:
    IPv6 Address BMC 1: ::
    IPv6 Link Local BMC 1: fe80::3a90:a5ff:fe7f:a840
    IPv6 SLAAC Address BMC 1: ::
    Hostname BMC 1: S3X60M5-FCH21187159
    MAC Address BMC 1: 38:90:A5:7F:A8:40

Server /network #
```

Configuring IPv4

Before you begin

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

SUMMARY STEPS

1. Server # **scope network**
2. Server /network # **set dhcp-enabled** {**yes** | **no**}
3. Server /network # **set v4-addr** *ipv4-address*
4. Server /network # **set v4-netmask** *ipv4-netmask*
5. Server /network # **set v4-gateway** *gateway-ipv4-address*

6. Server /network # **set dns-use-dhcp** {**yes** | **no**}
7. Server /network # **set preferred-dns-server** *dns1-ipv4-address*
8. Server /network # **set alternate-dns-server** *dns2-ipv4-address*
9. Server /network # **commit**
10. Server /network # **show** [**detail**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	Server # **scope network**	Enters the network command mode.
Step 2	Server /network # **set dhcp-enabled** {**yes** | **no**}	Selects whether the uses DHCP. **Note** If DHCP is enabled, we recommend that the DHCP server be configured to reserve a single IP address for the . If the 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 3	Server /network # **set v4-addr** *ipv4-address*	Specifies the IP address for the .
Step 4	Server /network # **set v4-netmask** *ipv4-netmask*	Specifies the subnet mask for the IP address.
Step 5	Server /network # **set v4-gateway** *gateway-ipv4-address*	Specifies the gateway for the IP address.
Step 6	Server /network # **set dns-use-dhcp** {**yes** | **no**}	Selects whether the retrieves the DNS server addresses from DHCP.
Step 7	Server /network # **set preferred-dns-server** *dns1-ipv4-address*	Specifies the IP address of the primary DNS server.
Step 8	Server /network # **set alternate-dns-server** *dns2-ipv4-address*	Specifies the IP address of the secondary DNS server.
Step 9	Server /network # **commit**	Commits the transaction to the system configuration.
Step 10	Server /network # **show** [**detail**]	(Optional) Displays the IPv4 network settings.

Example

This example configures and displays the IPv4 network settings:

```
Server  # scope network
Server /network # set dhcp-enabled yes
Server /network *# set v4-addr 10.20.30.11
Server /network *# set v4-netmask 255.255.248.0
Server /network *# set v4-gateway 10.20.30.1
Server /network *# set dns-use-dhcp-enabled no
Server /network *# set preferred-dns-server 192.168.30.31
Server /network *# set alternate-dns-server 192.168.30.32
Server /network *# commit

Server /network # show detail
```

```
Network Setting:
    IPv4 Enabled: yes
    IPv4 Netmask: 255.255.248.0
    IPv4 Gateway: 10.20.30.1
    DHCP Enabled: no
    DDNS Enabled: yes
    DDNS Update Domain:
    Obtain DNS Server by DHCP: no
    Preferred DNS: 192.168.30.31
    Alternate DNS: 192.168.30.32
    IPv6 Enabled: no
    IPv6 Prefix: 64
    IPv6 Gateway: ::
    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
    NIC Mode: dedicated
    NIC Redundancy: none
    SIOC Slot: 1
    Management IPv4 Address: 10.106.145.202
    Management IPv6 Address: ::
    Management Hostname: S3260-FCH18207WF3
    Network Speed: 100Mbps
    Duplex: full
    Auto Negotiate: yes
    Admin Network Speed: auto
    Admin Duplex: auto
    Operational Network Speed: 1Gbps
    Operational Duplex: full
CMC 1 Network Setting:
    IPv4 Address CMC 1: 10.20.30.11
    IPv6 Address CMC 1: ::
    IPv6 Link Local CMC 1: ::
    IPv6 SLAAC Address CMC 1: ::
    Hostname CMC 1: UCS-S3260-FCH181772ZP-1
    MAC Address CMC 1: F4:CF:E2:77:7F:D2
CMC 2 Network Setting:
    IPv4 Address CMC 2: 10.20.30.11
    IPv6 Address CMC 2: ::
    IPv6 Link Local CMC 2: ::
    IPv6 SLAAC Address CMC 2: ::
    Hostname CMC 2: UCS-S3260--2
    MAC Address CMC 2: F4:CF:E2:77:80:83
BMC 1 Network Setting:
    IPv4 Address BMC 1: 10.20.30.11
    IPv6 Address BMC 1: ::
    IPv6 Link Local BMC 1: ::
    IPv6 SLAAC Address BMC 1: ::
    Hostname BMC 1: S3260-FCH1827K9YT
    MAC Address BMC 1: 7C:0E:CE:5A:EF:26
BMC 2 Network Setting:
    IPv4 Address BMC 2: 10.20.30.11
    IPv6 Address BMC 2: ::
    IPv6 Link Local BMC 2: ::
    IPv6 SLAAC Address BMC 2: ::
    Hostname BMC 2: S3260-FCH18407MYD
    MAC Address BMC 2: A0:EC:F9:85:90:3F
```

```
Server /network #
```

Configuring IPv6

Before you begin

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

SUMMARY STEPS

1. Server # **scope network**
2. Server /network # **set v6-enabled** {**yes** | **no**}
3. Server /network # **set v6-dhcp-enabled** {**yes** | **no**}
4. Server /network # **set v6-addr-bmc1v6-addr-bmc2v6-addr-cmc1v6-addr-cmc2 v6-addr-mgmt***ipv6-address*
5. Server /network # **set v6-prefix** *ipv6-prefix-length*
6. Server /network # **set v6-gateway** *gateway-ipv6-address*
7. Server /network # **set v6-dns-use-dhcp** {**yes** | **no**}
8. Server /network # **set v6-preferred-dns-server** *dns1-ipv6-address*
9. Server /network # **set v6-alternate-dns-server** *dns2-ipv6-address*
10. Server /network # **commit**
11. Server /network # **show** [**detail**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	Server # **scope network**	Enters the network command mode.
Step 2	Server /network # **set v6-enabled** {**yes** | **no**}	Enables IPv6.
Step 3	Server /network # **set v6-dhcp-enabled** {**yes** | **no**}	Selects whether the uses DHCP. **Note** If DHCP is enabled, we recommend that the DHCP server be configured to reserve a single IPv6 address for the . If the 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 4	Server /network # **set v6-addr-bmc1v6-addr-bmc2v6-addr-cmc1v6-addr-cmc2 v6-addr-mgmt***ipv6-address*	Specifies the IP address for the following components: • BMC1 IPv6 Address • BMC2 IPv6 Address • CMC1 IPv6 Address • CMC2 IPv6 Address

	Command or Action	Purpose
		• Management IPv6 Address
Step 5	Server /network # **set v6-prefix** *ipv6-prefix-length*	Specifies the prefix length for the IP address.
Step 6	Server /network # **set v6-gateway** *gateway-ipv6-address*	Specifies the gateway for the IP address.
Step 7	Server /network # **set v6-dns-use-dhcp** {**yes** | **no**}	Selects whether the retrieves the DNS server addresses from DHCP. **Note** You can use this option only when DHCP enabled.
Step 8	Server /network # **set v6-preferred-dns-server** *dns1-ipv6-address*	Specifies the IP address of the primary DNS server.
Step 9	Server /network # **set v6-alternate-dns-server** *dns2-ipv6-address*	Specifies the IP address of the secondary DNS server.
Step 10	Server /network # **commit**	Commits the transaction to the system configuration.
Step 11	Server /network # **show** [**detail**]	(Optional) Displays the IPv6 network settings.

Example

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

```
Server # scope network
Server /network # set v6-enabled yes
Server /network *# set v6-addr-bmc1 2010:201::279
Server /network *# set v6-gateway 2010:201::1
Server /network *# set v6-prefix 64
Server /network *# set v6-dns-use-dhcp no
Server /network *# set v6-preferred-dns-server 2010:201::100
Server /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 /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 /network # show detail
Network Setting:
    IPv4 Enabled: yes
    IPv4 Netmask: 255.255.255.0
    IPv4 Gateway: 10.106.145.1
    DHCP Enabled: no
    DDNS Enabled: yes
    DDNS Update Domain:
    Obtain DNS Server by DHCP: no
    Preferred DNS: 171.70.168.183
    Alternate DNS: 0.0.0.0
    IPv6 Enabled: no
    IPv6 Prefix: 64
    IPv6 Gateway: 2010:201::1
    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: abcde12345
    NIC Mode: dedicated
    NIC Redundancy: none
    SIOC Slot: 1
    Management IPv4 Address: 10.106.145.202
    Management IPv6 Address: ::
    Management Hostname: S3260-FCH18207WF3
    Network Speed: 100Mbps
    Duplex: full
    Auto Negotiate: yes
    Admin Network Speed: auto
    Admin Duplex: auto
    Operational Network Speed: 1Gbps
    Operational Duplex: full
CMC 1 Network Setting:
    IPv4 Address CMC 1: 10.106.145.135
    IPv6 Address CMC 1:  ::
    IPv6 Link Local CMC 1: ::
    IPv6 SLAAC Address CMC 1: ::
    Hostname CMC 1: UCS-S3260-FCH181772ZP-1
    MAC Address CMC 1: F4:CF:E2:77:7F:D2
CMC 2 Network Setting:
    IPv4 Address CMC 2: 10.106.145.248
    IPv6 Address CMC 2:  ::
    IPv6 Link Local CMC 2: ::
    IPv6 SLAAC Address CMC 2: ::
    Hostname CMC 2: UCS-S3260--2
    MAC Address CMC 2: F4:CF:E2:77:80:83
BMC 1 Network Setting:
    IPv4 Address BMC 1: 10.106.145.41
    IPv6 Address BMC 1:  2010:201::279
    IPv6 Link Local BMC 1: ::
    IPv6 SLAAC Address BMC 1: ::
    Hostname BMC 1: S3260-FCH1827K9YT
    MAC Address BMC 1: 7C:0E:CE:5A:EF:26
BMC 2 Network Setting:
    IPv4 Address BMC 2: 10.106.145.39
    IPv6 Address BMC 2:  ::
    IPv6 Link Local BMC 2: ::
    IPv6 SLAAC Address BMC 2: ::
    Hostname BMC 2: S3260-FCH18407MYD
    MAC Address BMC 2: A0:EC:F9:85:90:3F

Server /network #
```

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

```
Server  # scope network
Server /network # set v6-enabled yes
Server /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 /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 /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: auto
    Admin Duplex: auto
    Operational Network Speed: 1Gbps
    Operational Duplex: full
CMC 1 Network Setting:
    IPv4 Address CMC 1: 10.106.145.135
    IPv6 Address CMC 1: ::
    IPv6 Link Local CMC 1: ::
    IPv6 SLAAC Address CMC 1: ::
    Hostname CMC 1: UCS-S3260-FCH181772ZP-1
    MAC Address CMC 1: F4:CF:E2:77:7F:D2
CMC 2 Network Setting:
    IPv4 Address CMC 2: 10.106.145.248
    IPv6 Address CMC 2: ::
    IPv6 Link Local CMC 2: ::
    IPv6 SLAAC Address CMC 2: ::
    Hostname CMC 2: UCS-S3260--2
    MAC Address CMC 2: F4:CF:E2:77:80:83
BMC 1 Network Setting:
    IPv4 Address BMC 1: 10.106.145.41
    IPv6 Address BMC 1: ::
    IPv6 Link Local BMC 1: ::
    IPv6 SLAAC Address BMC 1: ::
    Hostname BMC 1: S3260-FCH1827K9YT
    MAC Address BMC 1: 7C:0E:CE:5A:EF:26
BMC 2 Network Setting:
    IPv4 Address BMC 2: 10.106.145.39
    IPv6 Address BMC 2: ::
    IPv6 Link Local BMC 2: ::
    IPv6 SLAAC Address BMC 2: ::
    Hostname BMC 2: S3260-FCH18407MYD
    MAC Address BMC 2: A0:EC:F9:85:90:3F


Server /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 Cisco UCS S-series 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.
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 VLAN

Before you begin

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

SUMMARY STEPS

1. Server # **scope network**
2. Server /network # **set vlan-enabled** {**yes** | **no**}
3. Server /network # **set vlan-id** *id*
4. Server /network # **set vlan-priority** *priority*
5. Server /network # **commit**
6. Server /network # **show** [**detail**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	Server # **scope network**	Enters the network command mode.
Step 2	Server /network # **set vlan-enabled** {**yes** | **no**}	Selects whether the is connected to a VLAN.
Step 3	Server /network # **set vlan-id** *id*	Specifies the VLAN number.
Step 4	Server /network # **set vlan-priority** *priority*	Specifies the priority of this system on the VLAN.
Step 5	Server /network # **commit**	Commits the transaction to the system configuration.
Step 6	Server /network # **show** [**detail**]	(Optional) Displays the network settings.

Example

This example configures the VLAN:

```
Server # scope network
Server /network # set vlan-enabled yes
Server /network *# set vlan-id 5
Server /network *# set vlan-priority 7
Server /network *# commit

Server /network # show detail
Network Setting:
    IPv4 Enabled: yes
    IPv4 Netmask: 255.255.255.0
    IPv4 Gateway: 10.106.145.1
    DHCP Enabled: no
    DDNS Enabled: yes
    DDNS Update Domain:
    Obtain DNS Server by DHCP: no
    Preferred DNS: 171.70.168.183
    Alternate DNS: 0.0.0.0
```

```
    IPv6 Enabled: no
    IPv6 Prefix: 64
    IPv6 Gateway: ::
    IPV6 DHCP Enabled: no
    IPV6 Obtain DNS Server by DHCP: no
    IPV6 Preferred DNS: ::
    IPV6 Alternate DNS: ::
    VLAN Enabled: yes
    VLAN ID: 2
    VLAN Priority: 7
    Port Profile: abcde12345
    NIC Mode: dedicated
    NIC Redundancy: none
    SIOC Slot: 1
    Management IPv4 Address: 10.106.145.202
    Management IPv6 Address: ::
    Management Hostname: S3260-FCH18207WF3
    Network Speed: 100Mbps
    Duplex: full
    Auto Negotiate: yes
    Admin Network Speed: auto
    Admin Duplex: auto
    Operational Network Speed: 1Gbps
    Operational Duplex: full
CMC 1 Network Setting:
    IPv4 Address CMC 1: 10.106.145.135
    IPv6 Address CMC 1: ::
    IPv6 Link Local CMC 1: ::
    IPv6 SLAAC Address CMC 1: ::
    Hostname CMC 1: UCS-S3260-FCH181772ZP-1
    MAC Address CMC 1: F4:CF:E2:77:7F:D2
CMC 2 Network Setting:
    IPv4 Address CMC 2: 10.106.145.248
    IPv6 Address CMC 2: ::
    IPv6 Link Local CMC 2: ::
    IPv6 SLAAC Address CMC 2: ::
    Hostname CMC 2: UCS-S3260--2
    MAC Address CMC 2: F4:CF:E2:77:80:83
BMC 1 Network Setting:
    IPv4 Address BMC 1: 10.106.145.41
    IPv6 Address BMC 1: ::
    IPv6 Link Local BMC 1: ::
    IPv6 SLAAC Address BMC 1: ::
    Hostname BMC 1: S3260-FCH1827K9YT
    MAC Address BMC 1: 7C:0E:CE:5A:EF:26
BMC 2 Network Setting:
    IPv4 Address BMC 2: 10.106.145.39
    IPv6 Address BMC 2: ::
    IPv6 Link Local BMC 2: ::
    IPv6 SLAAC Address BMC 2: ::
    Hostname BMC 2: S3260-FCH18407MYD
    MAC Address BMC 2: A0:EC:F9:85:90:3F

Server /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.

SUMMARY STEPS

1. Server # **scope network**
2. Server /network # **set port-profile** *port_profile_name*
3. Server /network # **commit**
4. (Optional) Server /network # **show** [**detail**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	Server # **scope network**	Enters the network command mode.
Step 2	Server /network # **set port-profile** *port_profile_name*	Specifies the port profile 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 3	Server /network # **commit**	Commits the transaction to the system configuration.
Step 4	(Optional) Server /network # **show** [**detail**]	Displays the network settings.

Example

This example connects to port profile abcde12345:

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

Server /network # show detail
Network Setting:
```

```
    IPv4 Enabled: yes
    IPv4 Netmask: 255.255.255.0
    IPv4 Gateway: 10.106.145.1
    DHCP Enabled: no
    DDNS Enabled: yes
    DDNS Update Domain:
    Obtain DNS Server by DHCP: no
    Preferred DNS: 171.70.168.183
    Alternate DNS: 0.0.0.0
    IPv6 Enabled: no
    IPv6 Prefix: 64
    IPv6 Gateway: ::
    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
    NIC Mode: dedicated
    NIC Redundancy: none
    SIOC Slot: 1
    Management IPv4 Address: 10.106.145.202
    Management IPv6 Address: ::
    Management Hostname: S3260-FCH18207WF3
    Network Speed: 100Mbps
    Duplex: full
    Auto Negotiate: yes
    Admin Network Speed: auto
    Admin Duplex: auto
    Operational Network Speed: 1Gbps
    Operational Duplex: full
CMC 1 Network Setting:
    IPv4 Address CMC 1: 10.106.145.135
    IPv6 Address CMC 1: ::
    IPv6 Link Local CMC 1: ::
    IPv6 SLAAC Address CMC 1: ::
    Hostname CMC 1: UCS-S3260-FCH181772ZP-1
    MAC Address CMC 1: F4:CF:E2:77:7F:D2
CMC 2 Network Setting:
    IPv4 Address CMC 2: 10.106.145.248
    IPv6 Address CMC 2: ::
    IPv6 Link Local CMC 2: ::
    IPv6 SLAAC Address CMC 2: ::
    Hostname CMC 2: UCS-S3260--2
    MAC Address CMC 2: F4:CF:E2:77:80:83
BMC 1 Network Setting:
    IPv4 Address BMC 1: 10.106.145.41
    IPv6 Address BMC 1: ::
    IPv6 Link Local BMC 1: ::
    IPv6 SLAAC Address BMC 1: ::
    Hostname BMC 1: S3260-FCH1827K9YT
    MAC Address BMC 1: 7C:0E:CE:5A:EF:26
BMC 2 Network Setting:
    IPv4 Address BMC 2: 10.106.145.39
    IPv6 Address BMC 2: ::
    IPv6 Link Local BMC 2: ::
    IPv6 SLAAC Address BMC 2: ::
    Hostname BMC 2: S3260-FCH18407MYD
    MAC Address BMC 2: A0:EC:F9:85:90:3F

Server /network #
```

Configuring Interface Properties

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

SUMMARY STEPS

1. Server # **scope network**
2. Server /network* # **set mode dedicated**
3. Server /network* # **set auto-negotiate** {**yes | no**}
4. Server /network* # **set duplex** {**full | half**}

DETAILED STEPS

	Command or Action	Purpose
Step 1	Server # **scope network**	Enters the network command mode.
Step 2	Server /network* # **set mode dedicated**	Enters dedicated command mode.
Step 3	Server /network* # **set auto-negotiate** {**yes	no**}	Enables or disables auto negotiation command mode. • If you enter **yes**, the setting for duplex will be ignored by the system. The retains the speed at which the switch is configured. • If you enter **no**, you can set duplex. Else, a default speed of 100 Mbps will be applied, and duplex will retain its previous value.
Step 4	Server /network* # **set duplex** {**full	half**}	Sets specified duplex mode type. By default, the duplex mode is set to **Full**

Example

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

```
Server # scope network
Server /network* # set mode dedicated
Server /network* # set auto-negotiate no
Warning: You have chosen to set auto negotiate to no
 If speed and duplex are not set then a default speed of 100Mbps will be applied
 Duplex will retain its previous value
Server /network* # commit
Server /network # set duplex full
Server /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 /network #
```

Network Security Configuration

Network Security

The 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. 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.

SUMMARY STEPS

1. Server # **scope network**
2. Server /network # **scope ipblocking**
3. Server /network/ipblocking # **set enabled** {**yes** | **no**}
4. Server /network/ipblocking # **set fail-count** *fail-count*
5. Server /network/ipblocking # **set fail-window** *fail-seconds*
6. Server /network/ipblocking # **set penalty-time** *penalty-seconds*
7. Server /network/ipblocking # **commit**
8. Server /network/ipblocking # **exit**
9. Server /network # **scope ipfiltering**
10. Server /network/ipfiltering # **set enabled** {**yes** | **no**}
11. Server /network/ipfiltering # **set filter-1** *IPv4 or IPv6 address or a range of IP addresses*
12. Server /network/ipfiltering # **commit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Server # **scope network**	Enters the network command mode.
Step 2	Server /network # **scope ipblocking**	Enters the IP blocking command mode.
Step 3	Server /network/ipblocking # **set enabled** {**yes** | **no**}	Enables or disables IP blocking.
Step 4	Server /network/ipblocking # **set fail-count** *fail-count*	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.

	Command or Action	Purpose
		The number of unsuccessful login attempts must occur within the time frame specified in the IP Blocking Fail Window field. Enter an integer between 3 and 10.
Step 5	Server /network/ipblocking # **set fail-window** *fail-seconds*	Sets the length of time, in seconds, in which the unsuccessful login attempts must occur in order for the user to be locked out. Enter an integer between 60 and 120.
Step 6	Server /network/ipblocking # **set penalty-time** *penalty-seconds*	Sets the number of seconds the user remains locked out if they exceed the maximum number of login attempts within the specified time window. Enter an integer between 300 and 900.
Step 7	Server /network/ipblocking # **commit**	Commits the transaction to the system configuration.
Step 8	Server /network/ipblocking # **exit**	Exits the IP blocking to the network command mode.
Step 9	Server /network # **scope ipfiltering**	Enters the IP filtering command mode.
Step 10	Server /network/ipfiltering # **set enabled** {**yes** | **no**}	Enables or disables IP filtering. At the prompt enter **y** to enable IP filtering.
Step 11	Server /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 12	Server /network/ipfiltering # **commit**	Commits the transaction to the system configuration.

Example

This example configures network security:

```
Server # scope network
Server /network # scope ipblocking
Server /network/ipblocking # set enabled yes
Server /network/ipblocking *# set fail-count 5
Server /network/ipblocking *# set fail-window 90
Server /network/ipblocking *# set penalty-time 600
Server /network/ipblocking *# commit
Server /network/ipblocking #  exit
Server /network # scope ipfiltering
Server /network/ipfiltering # set enabled yes
This will enable IP Filtering
Do you wish to continue? [y/N] y
Server /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 /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 is reset, it synchronizes the time with the host. With the introduction of the NTP service, you can configure to synchronize the time with an NTP server. The NTP server does not run in 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, synchronizes the time with the configured NTP server. The NTP service can be modified only through .

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.

SUMMARY STEPS

1. Server # **scope time**
2. Server /time # **scope ntp**
3. Server /time/ntp # **set enabled yes**
4. Server /time/ntp* # **commit**
5. Server /time/ntp # **set server-1 10.120.33.44**
6. Server /time/ntp # **set server-2 10.120.34.45**
7. Server /time/ntp # **set server-3 10.120.35.46**
8. Server /time/ntp # **set server-4 10.120.36.48**
9. Server /time/ntp # **commit**
10. Server /time/ntp # **show detail**

DETAILED STEPS

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

	Command or Action	Purpose
Step 5	Server /time/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 6	Server /time/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 7	Server /time/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 8	Server /time/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 9	Server /time/ntp # **commit**	Commits the transaction.
Step 10	Server /time/ntp # **show detail**	Displays the NTP configuration details.

Example

This example shows how to configure the NTP service:

```
Server  # scope time
Server /time # scope ntp
Server /time/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 /time/ntp* # commit
Server /time/ntp # set server-1 10.120.33.44
Server /time/ntp* # set server-2 10.120.34.45
Server /time/ntp* # set server-3 10.120.35.46
Server /time/ntp* # set server-4 10.120.36.48
Server /time/ntp* # commit
Server /time/ntp # show details
NTP Service Settings:
    NTP Enabled: yes
    NTP Server 1: 10.120.33.44
    NTP Server 2: 10.120.34.45
    NTP Server 3: 10.120.35.46
    NTP Server 4: 10.120.36.48
    Status: NTP service enabled
```

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.

SUMMARY STEPS

1. Server # **scope network**
2. Server /network# **ping** *IP address* | **retries***number* | **timeout***seconds*
3. Server /network # **commit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Server # **scope network**	Enters the network command mode.
Step 2	Server /network# **ping** *IP address* | **retries***number* | **timeout***seconds*	Pings the IP address or host name for a specified number of times until timeout. • **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. • **Component** - The controller that you can ping.
Step 3	Server /network # **commit**	Commits the transaction to the system configuration.

Example

This example pings an IP address:

```
Server # scope network
Server /network # ping 10.10.10.10
PING 10.10.10.10 (10.10.10.10): 56 data bytes
64 bytes from 10.10.10.10: seq=0 ttl=238 time=146.343 ms
64 bytes from 10.10.10.10: seq=1 ttl=238 time=146.140 ms
64 bytes from 10.10.10.10: seq=2 ttl=238 time=146.238 ms

--- 10.10.10.10 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 146.140/146.240/146.343 ms
Server /cimc/network #
```