Configuring Network-Related Settings

This chapter includes the following sections:

- Server NIC Configuration, page 1
- Configuring Common Properties, page 3
- Configuring IPv4, page 4
- Configuring the Server VLAN, page 6
- Connecting to a Port Profile, page 7
- Network Interface Configuration, page 8
- Network Security Configuration, page 9
- Network Time Protocol Configuration, page 10

Server NIC Configuration

Server NICs

NIC Mode

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

- **Dedicated—**The management port is used to access the CIMC.
- **Shared LOM—**Any LOM (LAN On Motherboard) port can be used to access the CIMC.
- **Shared LOM 10G—**Any 10G LOM port can be used to access the CIMC. This option is only available for some adapter cards.
- **Cisco Card—**Any port on the adapter card can be used to access the CIMC. The Cisco adapter card has to be installed in a slot with Network Communications Services Interface protocol (NCSI) support.
- **Shared LOM Extended—**Any LOM port or adapter card port can be used to access the CIMC. The Cisco adapter card has to be installed in a slot with NCSI support.

NIC Redundancy

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

- **none**—Each port associated with the configured NIC mode operates independently. The ports do not fail over if there is a problem.
- **active-active**—If supported, all ports associated with the configured NIC mode operate simultaneously. This increases throughput and provides multiple paths to the CIMC.
- **active-standby**—If a port associated with the configured NIC mode fails, traffic will fail over to one of the other ports associated with the NIC mode.

Note If you select this option, make sure 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.

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

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 CIMC command mode.
Step 2	Server /cimc # **scope network**	Enters the CIMC network command mode.
Step 3	Server /cimc/network # **set mode** {**dedicated** | **shared_lom** | **shared_lom_10g** | **shipping** | **cisco_card**}	Sets the NIC mode to one of the following: • Dedicated—The management Ethernet port is used to access the CIMC. • Shared LOM—The LAN On Motherboard (LOM) Ethernet host ports are used to access the CIMC. **Note** If you select Shared LOM, make sure that all host ports belong to the same subnet. • Shared LOM 10G—The 10G LOM Ethernet host ports are used to access the CIMC. • Shipping—A limited configuration for initial connection. Select another mode for normal operation.

	Command or Action	Purpose
		• Cisco card—The ports on the adapter card are used to access the CIMC.
Step 4	Server /cimc/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 5	Server /cimc/network # **commit**	Commits the transaction to the system configuration. **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.

This example configures the CIMC network interface:

```
Server# scope cimc
Server /cimc # scope network
Server /cimc/network # set mode dedicated
Server /cimc/network *# commit
Server /cimc/network #
```

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 the CIMC command mode.
Step 2	Server /cimc # **scope network**	Enters the CIMC network command mode.
Step 3	Server /cimc/network # **set hostname** *host-name*	Specifies the name of the host.

	Command or Action	Purpose
		On modifying the hostname, you are prompted to confirm whether you want to create a new self-signed certificate with CN as the new hostname. If you enter **y** at the prompt, a new self-signed certificate will be created with CN as the new hostname. If you enter **n** at the prompt, only hostname will be changed and no certificate will be generated.
Step 4	Server /cimc/network # **commit**	Commits the transaction to the system configuration.

This example configures 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 *# commit
Server /cimc/network #
```

What to Do Next

Changes to the network will be applied immediately. You may lose connectivity to the CIMC and may 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 CIMC command mode.
Step 2	Server /cimc # **scope network**	Enters the CIMC network command mode.

	Command or Action	Purpose
Step 3	Server /cimc/network # **set dhcp-enabled** {**yes** | **no**}	Selects whether the CIMC uses DHCP. **Note** If DHCP is enabled, we recommend that the DHCP server be configured to reserve a single IP address for the CIMC. If the CIMC 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** *ipv4-address*	Specifies the IP address for the CIMC.
Step 5	Server /cimc/network # **set v4-netmask** *ipv4-netmask*	Specifies the subnet mask for the IP address.
Step 6	Server /cimc/network # **set v4-gateway** *gateway-ipv4-address*	Specifies the gateway for the IP address.
Step 7	Server /cimc/network # **set dns-use-dhcp** {**yes** | **no**}	Selects whether the CIMC retrieves the DNS server addresses from DHCP.
Step 8	Server /cimc/network # **set preferred-dns-server** *dns1-ipv4-address*	Specifies the IP address of the primary DNS server.
Step 9	Server /cimc/network # **set alternate-dns-server** *dns2-ipv4-address*	Specifies the IP address of the secondary DNS server.
Step 10	Server /cimc/network # **commit**	Commits the transaction to the system configuration.
Step 11	Server /cimc/network # **show** [**detail**]	(Optional) Displays the IPv4 network settings.

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
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
    VLAN Enabled: no
    VLAN ID: 1
    VLAN Priority: 0
    Hostname: Server
    MAC Address: 01:23:45:67:89:AB
```

```
    NIC Mode: dedicated
    NIC Redundancy: none

Server /cimc/network #
```

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 CIMC command mode.
Step 2	Server /cimc # **scope network**	Enters the CIMC network command mode.
Step 3	Server /cimc/network # **set vlan-enabled** {**yes** | **no**}	Selects whether the CIMC is connected to a VLAN.
Step 4	Server /cimc/network # **set vlan-id** *id*	Specifies the VLAN number.
Step 5	Server /cimc/network # **set vlan-priority** *priority*	Specifies the priority of this system on the VLAN.
Step 6	Server /cimc/network # **commit**	Commits the transaction to the system configuration.
Step 7	Server /cimc/network # **show** [**detail**]	(Optional) Displays the network settings.

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
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
    VLAN Enabled: yes
    VLAN ID: 10
    VLAN Priority: 32
    Hostname: Server
    MAC Address: 01:23:45:67:89:AB
    NIC Mode: dedicated
    NIC Redundancy: none

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 CIMC command mode.
Step 2	Server /cimc # **scope network**	Enters the CIMC network command mode.
Step 3	Server /cimc/network # **set port-profile** *port_profile_name*	Specifies the port profile CIMC should use to configure the management interface, the virtual Ethernet, and the VIF on supported adapter cards such as the Cisco UCS VIC1225 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	Server /cimc/network # **show** [**detail**]	(Optional) Displays the network settings.

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
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
    VLAN Enabled: no
    VLAN ID: 1
    VLAN Priority: 0
    Port Profile: abcde12345
    Hostname: Server
```

```
    MAC Address: 50:3D:E5:9D:63:3C
    NIC Mode: dedicated
    NIC Redundancy: none

Server /cimc/network #
```

Network Interface Configuration

Overview to Network Interface Configuration

This support is added to configure network speed and duplex mode for the CIMC management port. Auto negotiate mode and duplex mode can be set for dedicated mode only. When auto negotiate mode is enabled the settings for duplex is ignored by the system and the network speed is set to either 1000 Mbps or 100 Mbps as per the speed configured on the switch. When auto negotiate mode is disabled, you can set the duplex to either **Full** or **Half**, a default speed of 100 Mbps is set, and the duplex retains its previous value.

When you reset CIMC to factory defaults, **Shared LOM Extended** mode is configured to **Full** duplex mode with 100 Mbps speed, and auto negotiate mode is disabled. You can enable auto negotiate mode when you change the settings to **Dedicated** mode.

Configuring Interface Properties

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

Procedure

	Command or Action	Purpose
Step 1	Server # **scope cimc**	Enters the CIMC 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. • If you enter **yes**, the setting for duplex will be ignored by the system. The CIMC 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 5	Server/cimc/network* # **set duplex** {**full** | **half**}	Sets specified duplex mode type. By default, the duplex mode is set to **Full**

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
 If speed and duplex are not set then a default speed of 100Mbps will be applied
 Duplex will retain its previous value
Server/cimc/network* # commit
Server/cimc/network # set duplex full
Server/cimc/network* # commit
Server/cimc/network #
```

Network Security Configuration

Network Security

The CIMC 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. CIMC 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 CIMC command mode.
Step 2	Server /cimc # **scope network**	Enters the CIMC network command mode.
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*	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. 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.

	Command or Action	Purpose
Step 6	Server /cimc/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 7	Server /cimc/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 8	Server /cimc/network/ipblocking # **commit**	Commits the transaction to the system configuration.

This example configures IP blocking:

```
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 #
```

Network Time Protocol Configuration

Configuring Network Time Protocol Settings

By default, when CIMC is reset, it synchronizes the time with the host. With the introduction of the NTP service, you can configure CIMC to synchronize the time with an NTP server. The NTP server does not run in CIMC 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, CIMC synchronizes the time with the configured NTP server. The NTP service can be modified only through CIMC.

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 CIMC 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.
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.

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 #
```