Configuring Network-Related Settings

This chapter includes the following sections:

CIMC NIC Configuration

CIMC NICs

Two NIC modes are available for connection to the CIMC.

NIC Mode

- Dedicated—A connection to the CIMC is available through the management Ethernet port or ports.
- Shared LOM—A connection to the CIMC is available through the LAN On Motherboard (LOM) Ethernet host ports and through the router's PCIe and MGF interfaces.

Note In shared LOM mode, all host ports must belong to the same subnet.

The following examples show the link state:

```
server /cimc/network # show link-state detail
Interface                      State
------------------------------ --------------------
Console                        Link Detected
TE1                            No Link Detected
GE2                            No Link Detected
TE3                            No Link Detected
```

```
TE4                             No Link Detected
Dedicated                       Link Detected
```

The following examples show the LOM MAC list:

```
Server /cimc/network # show lom-mac-list
Interface                       MAC Address
------------------------------- --------------------
Console                         1C:D1:E0:26:05:A6
TE1                             1C:D1:E0:26:05:A7
GE2                             1C:D1:E0:26:05:AA
TE3                             1C:D1:E0:26:05:A8
TE4                             1C:D1:E0:26:05:A9
```

Configuring CIMC NICs

Use this procedure to set the NIC mode and Interface.

Before you begin

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

SUMMARY STEPS

1. Server# **scope cimc**
2. Server /cimc # **scope network**
3. Server /cimc/network # **set mode** {**dedicated** | **shared_lom**}
4. Server /cimc/network # **set interface** {**console** | **te1** | **ge2** | **te3** | **te4**}
5. Server /cimc/network # **commit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Server# **scope cimc**	Enters CIMC command mode.
Step 2	Server /cimc # **scope network**	Enters CIMC network command mode.
Step 3	Server /cimc/network # **set mode** {**dedicated** | **shared_lom**}	Sets the NIC mode to one of the following: • **dedicated**: The management Ethernet port is used to access the CIMC. • **shared LOM mode**: The LAN On Motherboard (LOM) Ethernet host ports are used to access the CIMC. **Note** In shared LOM mode, all host ports must belong to the same subnet.
Step 4	Server /cimc/network # **set interface** {**console** | **te1** | **ge2** | **te3** | **te4**}	Sets the NIC interface to one of the following: • **console**: Internal interface, which is used to connect either the router's PCIe interface to the E-Series Server.

	Command or Action	Purpose
		• **te1**: Internal interface, which is used to access the CIMC over a high-speed backplane switch. • **ge2**: External interface, which can be used as a primary interface or as a backup interface. • **te3**: External interface, which can be used as a primary interface or as a backup interface. • **te4**: External interface, which can be used as a primary interface or as a backup interface.
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.

Example

This example configures the CIMC network interface:

```
Server# scope cimc
Server /cimc # scope network
Server /cimc/network # set mode shared_lom
WARNING: Changing this configuration may cause the Router network configuration to be out
of sync.
You may still commit your changes, but it is recommended that changes be done on the Router.
Server /cimc/network *# set interface ge2
WARNING: Changing this configuration may cause the Router network configuration to be out
of sync.
You may still commit your changes, but it is recommended that changes be done on the Router.
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 #
```

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 cimc**

2. Server /cimc # **scope network**
3. Server /cimc/network # **set hostname** *host-name*
4. Server /cimc/network # **commit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Server# **scope cimc**	Enters CIMC command mode.
Step 2	Server /cimc # **scope network**	Enters CIMC network command mode.
Step 3	Server /cimc/network # **set hostname** *host-name*	Specifies the name of the host.
Step 4	Server /cimc/network # **commit**	Commits the transaction to the system configuration.

Example

This example configures the common properties:

```
Server# scope cimc
Server /cimc # scope network
server /cimc/network # set hostname Server
WARNING: Changing this configuration may cause the Router network configuration to be out
of sync.
You may still commit your changes, but it is recommended that changes be done on the Router.
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 #
Server /cimc/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 cimc**
2. Server /cimc # **scope network**
3. Server /cimc/network # **set dhcp-enabled** {**yes** | **no**}
4. Server /cimc/network # **set v4-addr** *ipv4-address*
5. Server /cimc/network # **set v4-netmask** *ipv4-netmask*
6. Server /cimc/network # **set v4-gateway** *gateway-ipv4-address*
7. Server /cimc/network # **set dns-use-dhcp** {**yes** | **no**}
8. Server /cimc/network # **set preferred-dns-server** *dns1-ipv4-address*
9. Server /cimc/network # **set alternate-dns-server** *dns2-ipv4-address*

10. Server /cimc/network # **commit**
11. Server /cimc/network # **show** [**detail**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	Server# **scope cimc**	Enters CIMC command mode.
Step 2	Server /cimc # **scope network**	Enters CIMC network command mode.
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.

Example

This example configures and displays the IPv4 network settings:

```
Server# scope cimc
Server /cimc # scope network
Server /cimc/network # set dns-use-dhcp no
WARNING: Changing this configuration may cause the Router network configuration to be out
of sync.
You may still commit your changes, but it is recommended that changes be done on the Router.
Server /cimc/network *# set dhcp-enabled no
WARNING: Changing this configuration may cause the Router network configuration to be out
of sync.
You may still commit your changes, but it is recommended that changes be done on the Router.
Server /cimc/network *# set v4-addr 10.20.30.11
WARNING: Changing this configuration may cause the Router network configuration to be out
```

```
of sync.
You may still commit your changes, but it is recommended that changes be done on the Router.
Server /cimc/network *# set v4-gateway 10.20.30.1
WARNING: Changing this configuration may cause the Router network configuration to be out
of sync.
You may still commit your changes, but it is recommended that changes be done on the Router.
Server /cimc/network *# set v4-netmask 255.255.248.0
WARNING: Changing this configuration may cause the Router network configuration to be out
of sync.
You may still commit your changes, but it is recommended that changes be done on the Router.
Server /cimc/network *# set preferred-dns-server 192.168.30.31
WARNING: Changing this configuration may cause the Router network configuration to be out
of sync.
You may still commit your changes, but it is recommended that changes be done on the Router.
Server /cimc/network *# set alternate-dns-server 192.168.30.32
WARNING: Changing this configuration may cause the Router network configuration to be out
of sync.
You may still commit your changes, but it is recommended that changes be done on the Router.
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 #

Server /cimc/network # show detail
Network Setting:
IPv4 Enabled: yes
IPv4 Address: 10.20.30.11
IPv4 Netmask: 255.255.248.0
IPv4 Gateway: 10.20.30.1
DHCP Enabled: no
DDNS Enabled: yes
DDNS Update Domain:
DDNS Refresh Interval(0-8736 Hr): 0
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: Server
MAC Address: 1C:D1:E0:26:0F:81
NIC Mode: shared_lom
NIC Redundancy: none
NIC Interface: ge2
VIC Slot: 0
```

Note This configuration can take a few minutes to reflect in the **show detail** command.

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 cimc**
2. Server /cimc # **scope network**
3. Server /cimc/network # **set v6-dhcp no**
4. Server /cimc/network # **set v6-enabled yes**
5. Server /cimc/network # **set v6-addr** *ipv6-address*
6. Server /cimc/network # **set v6-gateway** *gateway-ipv6address*
7. Server /cimc/network # **commit**
8. Server /cimc/network # **show** [**detail**]

DETAILED STEPS

	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 v6-dhcp no**	Disables DHCP.
Step 4	Server /cimc/network # **set v6-enabled yes**	Enables the IPv6 addressing.
Step 5	Server /cimc/network # **set v6-addr** *ipv6-address*	Specifies the IP address for the CIMC.
Step 6	Server /cimc/network # **set v6-gateway** *gateway-ipv6address*	Specifies the gateway for the IP address.
Step 7	Server /cimc/network # **commit**	Commits the transaction to the system configuration.
Step 8	Server /cimc/network # **show** [**detail**]	(Optional) Displays the IPv4 and IPv6 network settings.

Example

This example configures and displays the IPv6 network settings:

```
Server# scope cimc
Server /cimc # scope network
Server /cimc/network # set v6-dhcp-enabled no
WARNING: Changing this configuration may cause the Router network configuration to be out
of sync.
You may still commit your changes, but it is recommended that changes be done on the Router.
Please set "v6-enabled" to "yes" before you commit
Otherwise your setting for "v6-dhcp-enabled" will not be reflected
Server /cimc/network *# set v6-enabled yes
WARNING: Changing this configuration may cause the Router network configuration to be out
```

```
of sync.
You may still commit your changes, but it is recommended that changes be done on the Router.
Warning: You have chosen to change IPv6 property without a valid IPv6 address.
Server /cimc/network *# set v6-addr 2001:db8:101:f101:f2f7::14
WARNING: Changing this configuration may cause the Router network configuration to be out
of sync.
You may still commit your changes, but it is recommended that changes be done on the Router.
Server /cimc/network *# set v6-gateway 2001:db8:101:f101:f2f7::1
WARNING: Changing this configuration may cause the Router network configuration to be out
of sync.
You may still commit your changes, but it is recommended that changes be done on the Router.
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 #

Server /cimc/network # show detail
Network Setting:
IPv4 Enabled: yes
IPv4 Address: 10.20.30.11
IPv4 Netmask: 255.255.248.0
IPv4 Gateway: 10.20.30.1
DHCP Enabled: no
DDNS Enabled: yes
DDNS Update Domain:
DDNS Refresh Interval(0-8736 Hr): 0
Obtain DNS Server by DHCP: no
Preferred DNS: 192.168.30.31
Alternate DNS: 192.168.30.32
IPv6 Enabled: yes
IPv6 Address: 2001:db8:101:f101:f2f7::14
IPv6 Prefix: 64
IPv6 Gateway: 2001:db8:101:f101:f2f7::1
IPv6 Link Local: fe80::1ed1:e0ff:fe26:f81
IPv6 SLAAC Address: 6666:1000::1ed1:e0ff:fe26:f81
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: Server
MAC Address: 1C:D1:E0:26:0F:81
NIC Mode: shared_lom
NIC Redundancy: none
NIC Interface: ge2
VIC Slot: 0
Server /cimc/network #
```

Configuring the Server VLAN

Before you begin

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	Server# **scope cimc**	Enters CIMC command mode.
Step 2	Server /cimc # **scope network**	Enters 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.

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
Server /cimc/network # show detail
Network Setting:
    IPv4 Enabled: yes
     IPv4 Address: 10.20.30.11
     IPv4 Netmask: 255.255.248.0
     IPv4 Gateway: 10.20.30.1
     DHCP Enabled: no
     DDNS Enabled: yes
     DDNS Update Domain:
    DDNS Refresh Interval(0-8736 Hr): 0
    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: yes
    VLAN ID: 10
    VLAN Priority: 32
    Port Profile:
    Hostname: Server
    MAC Address: 1C:D1:E0:26:05:A5
    NIC Mode: dedicated
    NIC Redundancy: none
    NIC Interface:
    VIC Slot: 0

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. The 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.

SUMMARY STEPS

1. Server# **scope cimc**
2. Server /cimc # **scope network**
3. Server /cimc/network # **scope ipblocking**
4. Server /cimc/network/ipblocking # **set enabled** {**yes** | **no**}
5. Server /cimc/network/ipblocking # **set fail-count** *fail-count*
6. Server /cimc/network/ipblocking # **set fail-window** *fail-seconds*
7. Server /cimc/network/ipblocking # **set penalty-time** *penalty-seconds*
8. Server /cimc/network/ipblocking # **commit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Server# **scope cimc**	Enters CIMC command mode.
Step 2	Server /cimc # **scope network**	Enters CIMC network command mode.
Step 3	Server /cimc/network # **scope ipblocking**	Enters 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.
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.

Example

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 #
```

Configuring Network Analysis Module Capability

Before you begin

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

SUMMARY STEPS

1. Server# **scope cimc**
2. Server /cimc # **scope network**
3. Server /cimc/network # **scope nam**
4. Server /cimc/network/nam # **set enabled yes**
5. Server /cimc/network/nam # **show detail**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Server# **scope cimc**	Enters CIMC command mode.
Step 2	Server /cimc # **scope network**	Enters CIMC network command mode.
Step 3	Server /cimc/network # **scope nam**	Enters Network Analysis Module (NAM) command mode.
Step 4	Server /cimc/network/nam # **set enabled yes**	Enables the NAM capability. To disable the NAM capability, use the **set enabled no** command.
Step 5	Server /cimc/network/nam # **show detail**	Verifies that the NAM capability is enabled or disabled.

Example

This example configures the common properties:

```
Server# scope cimc
Server /cimc # scope network
Server /cimc/network # scope nam
Server /cimc/network/nam # set enabled yes
Server /cimc/network/nam # show detail
Network Analysis Module:
    Enabled: yes
```

NTP Settings Configuration

NTP Settings

By default, when CIMC is reset, it synchronizes the time with the host. With the introduction of the Network Time Protocol (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 or 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.

Configuring NTP Settings

Before you begin

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

SUMMARY STEPS

1. Server# **scope cimc**
2. Server /cimc # **scope network**
3. Server /cimc/network # **scope ntp**
4. Server /cimc/network/ntp # **set enabled yes**
5. Server /cimc/network/ntp # **set** [**server-1** | **server-2** | **server-3** | **server-4**] *ip-address or domain-name*
6. Server /cimc/network/ntp # **show detail**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Server# **scope cimc**	Enters CIMC command mode.
Step 2	Server /cimc # **scope network**	Enters CIMC network command mode.
Step 3	Server /cimc/network # **scope ntp**	Enters NTP command mode.
Step 4	Server /cimc/network/ntp # **set enabled yes**	Enables the NTP service. To disable the NTP service, use the **set enabled no** command.
Step 5	Server /cimc/network/ntp # **set** [**server-1** | **server-2** | **server-3** | **server-4**] *ip-address or domain-name*	Configures the IP address or domain name for the specified server to act as an NTP server or the time source server. You can configure a maximum of four servers.

	Command or Action	Purpose
Step 6	Server /cimc/network/ntp # **show detail**	Displays whether the NTP service is enabled and the IP address or domain name of the NTP servers.

Example

This example configures NTP settings:

```
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 # set server-1 10.50.171.9
Server /cimc/network/ntp # set server-2 time.cisco.com

Server /cimc/network/ntp # show detail
NTP Service Settings:
    Enabled: yes
    Server 1: 10.50.171.9
    Server 2: time.cisco.com
    Server 3:
    Server 4:
    Status: unsynchronised
    Server /cimc/network/ntp #
```