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

The **NIC Mode** drop-down list in the **NIC Properties** area determines which ports can reach the CIMC. The following mode options are available, depending on your platform:

- 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.

Note Dedicated mode is not applicable to the EHWIC E-Series NCE.

NIC Redundancy

The **NIC Redundancy** drop-down list in the **NIC Properties** area determines how NIC redundancy is handled:

- None—Redundancy is not available.
- Active-Standby—One port fails over to the other.

The available redundancy modes vary depending on the selected network mode and your platform.

Configuring CIMC NICs

Use this procedure 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

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, click **Network**.

Step 3 In the **Network** pane, click the **Network Settings** tab.

Step 4 In the **NIC Properties** area, update the following properties:

Name	Description
NIC Mode drop-down list	The NIC mode. This can be one of the following: • **Dedicated—**The management port is used to access the CIMC. • **Shared LOM—**The LOM (LAN On Motherboard) ports are used to access the CIMC. **Note** Dedicated mode is not applicable to the EHWIC E-Series NCE.

Name	Description
NIC Redundancy drop-down list	The NIC redundancy options depend on the mode chosen in the **NIC Mode** drop-down list and the model of the server that you are using. If you do not see a particular option, then it is not available for the selected mode or server model. The available options are: • **none—**Each port associated with the configured NIC mode operates independently. The ports do not fail over if there is a problem. • **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.
NIC Interface field	The interface used by the NIC. **Important** If you are using the external GE2 interface on an EHWIC E-Series NCE or the NIM E-Series NCE to configure CIMC access, you might lose connectivity with CIMC during server reboot. This is expected behavior. If you must maintain connectivity with CIMC during a reboot, we recommend that you use one of the other network interfaces to configure CIMC access. See the "CIMC Access Configuration Options—EHWIC E-Series NCE" and the "CIMC Access Configuration Options—NIM E-Series NCE" sections in the *Getting Started Guide for Cisco UCS E-Series Servers and the Cisco UCS E-Series Network Compute Engine*.
MAC Address field	The MAC address of the CIMC network interface selected in the **NIC Mode** field.

Note The available NIC mode options may vary depending on your platform.

If you select Shared LOM, make sure that all host ports belong to the same subnet.

Step 5 Click **Save Changes**.

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

Step 1 In the **Navigation** pane, click the **Admin** tab.
Step 2 On the **Admin** tab, click **Network**.
Step 3 In the **Network** pane, click the **Network Settings** tab.
Step 4 In the **Hostname** field, enter the name of the host.
Step 5 Click **Save Changes**.

Configuring IPv4

Before You Begin

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

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.
Step 2 On the **Admin** tab, click **Network**.
Step 3 In the **Network** pane, click the **Network Settings** tab.
Step 4 In the **IPv4 Properties** area, update the following properties:

Name	Description
Enable IPv4 check box	If checked, IPv4 is enabled.
Use DHCP check box	If checked, the CIMC uses DHCP.
IP Address field	The IP address for the CIMC.
Subnet Mask field	The subnet mask for the IP address.
Gateway field	The IP address of the gateway.
Obtain DNS Server Addresses from DHCP check box	If checked, the CIMC retrieves the DNS server addresses from DHCP.
Preferred DNS Server field	The IP address of the primary DNS server.
Alternate DNS Server field	The IP address of the secondary DNS server.

Step 5 Click **Save Changes**.

Connecting to a VLAN

Before You Begin

You must be logged in as admin to connect to a VLAN.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, click **Network**.

Step 3 In the **Network** pane, click the **Network Settings** tab.

Step 4 In the **VLAN Properties** area, update the following properties:

Name	Description
Enable VLAN check box	If checked, the CIMC is connected to a virtual LAN.
VLAN ID field	The VLAN ID.
Priority field	The priority of this system on the VLAN.

Step 5 Click **Save Changes**.

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.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, click **Network**.

Step 3 In the **Network** pane, click the **Network Security** tab.

Step 4 In the **IP Blocking Properties** area, update the following properties:

Name	Description
Enable IP Blocking check box	If checked, enables IP blocking.
IP Blocking Fail Count field	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.
IP Blocking Fail Window field	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.
IP Blocking Penalty Time field	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 5 Click **Save Changes**.

Enabling the Network Analysis Capability

Before You Begin

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

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.
Step 2 On the **Admin** tab, click **Network**.
Step 3 In the **Network** pane, click the **Network Analysis** tab.
Step 4 In the **Network Analysis Capability** area, check the **Enabled** check box.
The router is notified to turn on the Network Analysis Module (NAM) capability.
Step 5 Click **Save Changes**.

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

Configuring NTP disables the IPMI **Set SEL time** command.

Before You Begin

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

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.
Step 2 On the **Admin** tab, click **Network**.
Step 3 In the **Network** pane, click the **NTP Settings** tab.
Step 4 In the **NTP Settings** area, update the following properties:

Name	Description
Enable NTP check box	If checked, enables the NTP service.

Name	Description
Server 1	The IP address or domain name of one of the four servers that act as an NTP server or the time source server.
Server 2	The IP address or domain name of one of the four servers that act as an NTP server or the time source server.
Server 3	The IP address or domain name of one of the four servers that act as an NTP server or the time source server.
Server 4	The IP address or domain name of one of the four servers that act as an NTP server or the time source server.

Step 5 Click **Save Changes**.