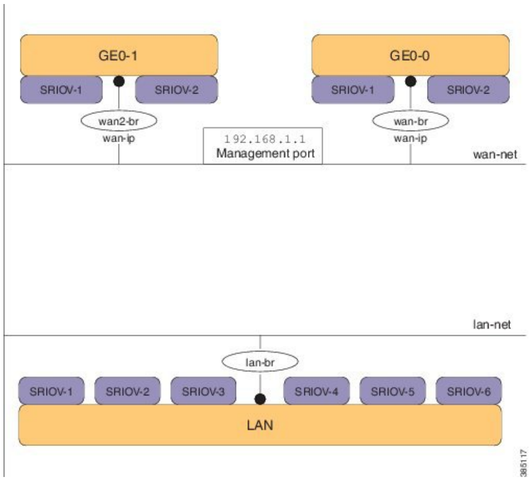
Setting Up System Configuration

Default System Configuration on the Cisco ENCS

The diagram below illustrates the default network configuration of Cisco Enterprise NFVIS with the Cisco ENCS.

Figure 1: Default Network Configuration of Cisco Enterprise NFVIS with the Cisco ENCS



- LAN ports—Eight physical Gigabit Ethernet ports for inbound and outbound traffic.
- WAN port—You can use one of the dual media Ethernet ports for DHCP connection.

- Bridges—They form a Layer 2 domain between virtual network interface controllers (vNICs) of VMs. A vNIC is used by a virtual machine to provide virtual network interfaces by defining a range of MAC addresses. The default management IP address (192.168.1.1) for the NFVIS host is configured on the management port. Multiple VMs can use the same LAN port for local connectivity.
- Network—It is a segment Layer 2 bridge domain where only the specific VLAN traffic is allowed.

Note The following networks and bridges are automatically configured. You can configure more as required.

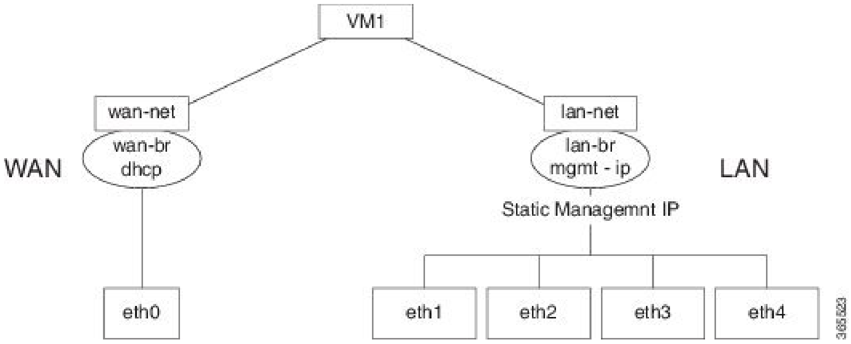
- A LAN network (lan-net) and a LAN bridge (lan-br)
- A WAN network (wan-net) and a WAN bridge (wan-br)

The default networks and bridges cannot be deleted.

Default System Configuration on the Cisco UCS C220 M4 Server

Configuring the networks in Cisco Enterprise NFVIS allows inbound and outbound traffic and VMs to be service chained. The following diagram illustrates the default network configuration:

Figure 2: Default Network Configuration with Cisco UCS C220 M4



The following networks and bridges are created by default, and cannot be deleted. You can configure more as required.

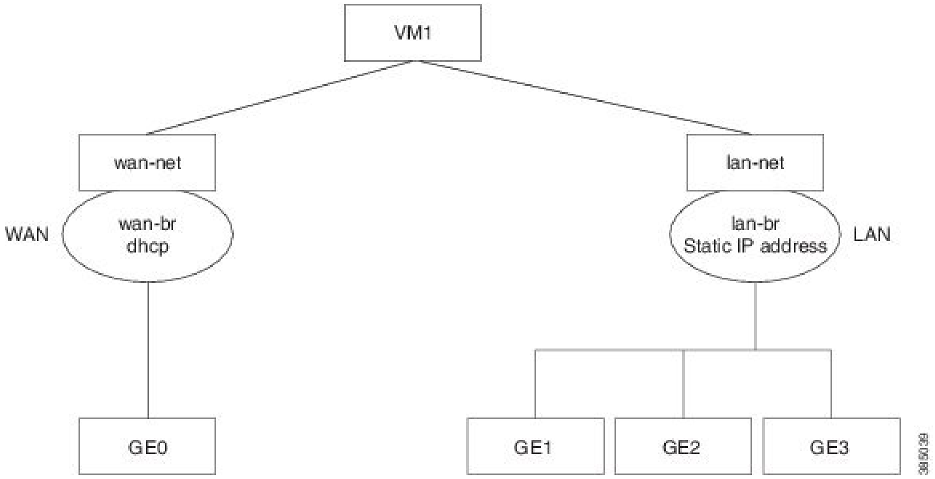
- A LAN network (lan-net) and a LAN bridge (lan-br)—The default static management IP address (192.168.1.1) for the NFVIS host is configured on the LAN bridge. All other ports for inbound and outbound traffic are associated with the LAN bridge. Any LAN port can be used to access the default static IP address. By default, the hostname is set to "nfvis".
- A WAN network (wan-net) and a WAN bridge (wan-br)—This is created with the "eth0" port, and is configured to enable the DHCP connection.

By default, the first port on the device is associated with the WAN bridge. All the other ports on the device are associated with the LAN bridge.

For more details on the initial setup, see the Installing the Server chapter in the Cisco UCS C220 M4 Server Installation and Service Guide.

Default System Configuration on the Cisco UCS E-Series Servers

Figure 3: Default Network Configuration with a Cisco UCS E-Series Server



The following networks and bridges are created by default, and cannot be deleted. You can configure more as required.

- A LAN network (lan-net) and a LAN bridge (lan-br)—The default static management IP address (192.168.1.1) for the NFVIS host is configured on the LAN bridge. All other ports for inbound and outbound traffic are associated with the LAN bridge. By default, the hostname is set to "nfvis".
- A WAN network (wan-net) and a WAN bridge (wan-br)— The physical WAN ports are on the Cisco ISR module. They are not externally available on the Cisco UCS E server. The WAN traffic comes from the ISR WAN ports, and goes through the backplane to the Cisco UCS-E server. The backplane has one internal WAN interface (GE0) to establish connection with the Cisco UCS-E server. By default, the "GE0" interface is enabled for the DHCP connection.

For more details on the initial setup, see the Getting Started Guide for Cisco UCS E-Series Servers and the Cisco UCS E-Series Network Compute Engine.

Setting Up Initial Configuration

For initial login, use **admin** as the default user name, and **Admin123#** as the default password. Immediately after the initial login, the system prompts you to change the default password. You must set a strong password as per the on-screen instructions to proceed with the application. All other operations are blocked until default password is changed. API will return 401 unauthorized error if the default password is not reset.

You must follow the rules to create a strong password:

- Must contain at least one upper case and one lower case letter.
- Must contain at least one number and one special character.
- Must contain seven characters or greater. Length should be between 7 and 32 characters.
- Cannot contain whitespace and some special characters (! @ : ; ,).

You can change the default password in three ways:

- Using the Cisco Enterprise NFVIS portal (for details, see the Cisco Enterprise NFVIS Portal Online Help)
- Using the **rbac authentication users user change-password** command.
- Using PnP (for details, see the Cisco Network Plug-n-Play Support).

Note To commit the target configuration to the active (running) configuration, use the **commit** command in any configuration mode in Cisco Enterprise NFVIS Release 3.5.1 and later. Changes made during a configuration session are inactive until the **commit** command is entered. By default, the commit operation is pseudo-atomic, meaning that all changes must succeed for the entire commit operation to succeed.

Connecting to the System

The two interfaces that connect the user to the system are the WAN interface and the management interface. By default, the WAN interface has the DHCP configuration and the management interface is configured with the static IP address 192.168.1.1. If the system has a DHCP server connected to the WAN interface, the WAN interface will receive the IP address from this server. You can use this IP address to connect to the system.

You can connect to the server locally (with an Ethernet cable) using the static management IP address; to connect to the box remotely using a static IP address, the default gateway needs to be configured.

You can connect to the system in the following three ways:

- Using the local portal—After the initial login, you are prompted to change the default password.
- Using the KVM console—After the initial login using the default password, you are prompted to change the default password.

  After logging in, enable the command prompt. Without enabling the prompt, you will not be able to execute any commands.

  ```
  nfvis> enable
  ```
- Using PnP—After the initial provisioning through PnP, the configuration file pushed by the PNP server must include the new password for the default user (admin).

Performing Static Configuration without DHCP

If you want to disable DHCP and use static configuration, initial configuration is done by setting the WAN IP address and/or management IP address, and the default gateway..

To perform initial configuration on the system without using DHCP:

```
configure terminal
system settings mgmt ip address 192.168.1.2 255.255.255.0
system settings wan ip address 209.165.201.22 255.255.255.0
system settings default-gw 209.165.201.1
commit
```

Note When an interface is configured with a static IP address, DHCP is automatically disabled on that interface.

Now you can either use the management IP or WAN IP to access the portal.

Configuring DHCP on the WAN or Management Interface

You can configure DHCP either on the WAN interface or the management interface; you cannot configure DHCP on both the interfaces simultaneously.

To configure DHCP on any one of the interfaces (WAN or management), delete the default gateway.

To configure DHCP on the management interface:

```
configure terminal
no system settings default-gw
system settings mgmt dhcp
commit
exit
hostaction mgmt-dhcp-renew
```

To configure DHCP on the WAN interface:

```
configure terminal
no system settings default-gw
system settings wan dhcp
commit
exit
hostaction wan-dhcp-renew
```

Verifying Initial Configuration

The **show system settings-native** command is used to verify initial configuration.

Extract from the output of the **show system settings-native** command when both WAN and management interfaces have a static configuration:

```
system settings-native mgmt ip-info interface lan-br
system settings-native mgmt ip-info ipv4_address 192.168.1.2
system settings-native mgmt ip-info netmask 255.255.255.0
!
!
!
system settings-native mgmt dhcp disabled
system settings-native wan ip-info interface wan-br
system settings-native wan ip-info ipv4_address 209.165.201.22
system settings-native wan ip-info netmask 255.255.255.0
!
!
!
system settings-native wan dhcp disabled
!
!
system settings-native gateway ipv4_address 209.165.201.1
system settings-native gateway interface wan-br
```

Extract from the output of the **show system settings-native** command when the management interface has a DHCP configuration and the WAN interface has a static configuration:

```
system settings-native mgmt ip-info interface MGMT
system settings-native mgmt ip-info ipv4_address 192.168.1.2
system settings-native mgmt ip-info netmask 255.255.255.0
!
!
!
system settings-native mgmt dhcp enabled
system settings-native wan ip-info interface wan-br
system settings-native wan ip-info ipv4_address 209.165.201.22
system settings-native wan ip-info netmask 255.255.255.0
!
!
!
system settings-native wan dhcp disabled
```

Extract from the output of the **show system settings-native** command when the WAN interface has a DHCP configuration and the management interface has a static configuration:

```
system settings-native mgmt ip-info interface lan-br
system settings-native mgmt ip-info ipv4_address 209.165.201.2
system settings-native mgmt ip-info netmask 255.255.255.0
!
!
!
system settings-native mgmt dhcp disabled
system settings-native wan ip-info interface wan-br
system settings-native wan ip-info ipv4_address 209.165.201.22
system settings-native wan ip-info netmask 255.255.255.0
!
!
!
system settings-native wan dhcp enabled
```

Related APIs and Commands

APIs	Commands
• /api/operational/system/settings-native • /api/config/system/settings	• system settings hostname • system settings default-gw • system settings mgmt ip address • system settings mgmt dhcp • system settings wan ip address • system settings wan dhcp • hostaction wan-dhcp-renew • hostaction mgmt-dhcp-renew

Configuring VLAN for NFVIS Management Traffic

A VLAN is a method of creating independent logical networks within a physical network. VLAN tagging is the practice of inserting a VLAN ID into a packet header in order to identify which VLAN the packet belongs to.

You can configure a VLAN tag on the WAN bridge (wan-br) interface to isolate Cisco Enterprise NFVIS management traffic from VM traffic.

Note You cannot have the same VLAN configured for the NFVIS management and VM traffc.

For more details on the VLAN configuration, see the Understanding and Configuring VLANs module in the Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide.

To configure a VLAN:

```
configure terminal
system settings wan vlan 120

commit
```

Verifying VLAN Configuration

Run the **show system settings-native wan vlan** command to verify the VLAN configuration as shown below:

```
nfvis# show system settings-native wan vlan
system settings-native wan vlan tag 120
```

VLAN APIs and Commands

VLAN APIs	VLAN Commands
• /api/config/system/settings/wan/vlan • /api/operational/system/settings-native/wan/vlan	• system settings wan vlan • show system settings-native wan vlan

Configuring System Routes

In addition to the default routes in the system, you can configure additional system routes. This configuration is specifically useful when certain destinations are not reachable through the default routes.

While you can create a route just by providing the destination and prefix length, a valid route requires that you specify either a device or a gateway or both.

To configure additional system routes:

```
configure terminal
system routes route  209.165.201.1 dev lan-br
commit
```

Verifying the System Routes Configuration

To verify the system routes configuration, use the **show system routes** command as shown below:

```
nfvis# show system routes
DESTINATION  PREFIXLEN  STATUS
----------------------------------
209.165.201.1  12 -
209.165.201.2  12 -
209.165.201.3  24 -
```

System Routes APIs and Commands

System Routes APIs	System Routes Commands
• /api/config/system/routes • /api/config/system/routes/route/<host destination,netmask>	• system routes route • show system routes

User Roles and Authentication

Role based access enables the administrator to manage different levles of access to the system's compute, storage, database, and application services. It uses the access control concepts such as users, groups, and rules, which you can apply to individual API calls. You can also keep a log of all user activities.

Table 1: Supported User Roles and Privileges

User Role	Privilege
Administrators	Owns everything, can perform all tasks including changing of user roles, but cannot delete basic infrastructure. Admin's role cannot be changed; it is always "administrators".
Operators	Start and stop a VM, and view all information
Auditors	Read-only permission

Creating Users and Assigning Roles

The administrator can create users and define user roles as required. You can assign a user to a particular user group. For example, the user "test1" can be added to the user group "administrators".

Note All user groups are craeted by the system. You cannot create or modify a user group.

To create a user:

```
configure terminal
rbac authentication users user admin1 password Cisco123* role administrator

commit
```

Note To change the password, use the **rbac authentication users user change-password** command in global configuartion mode. To change the user role, use the **rbac authentication users user change-role** command in global configuration mode.

User Management APIs and Commands

User Management APIs	User Management Commands
• /api/config/rbac/authentication/users • /api/operations/rbac/authentication/users /user/<user-name>/change-password • /api/operations/rbac/authentication/users/user /oper/change-role • /api/config/rbac/authentication/users/user?deep	• rbac authentication users • rbac authentication users user change-password • rbac authentication users user change-role

Configuring a TACACS+ Server

TACACS+ is a security application that provides centralized validation of users attempting to gain access to a router or network access server. TACACS+ services are maintained in a database on a TACACS+ daemon running, typically, on a UNIX or Windows NT workstation. You must configure a TACACS+ server before the configured TACACS+ features on your network access server are available.

On the TACACS+ server, ensure you configure Cisco attribute-value (AV) pair privilege level (priv-lvl) for Cisco Enterprise NFVIS service for the minimum privilege level of administrators and operators.

For more details on TACACS+ configuration, see the Configuring TACACS module in TACACS+ Configuration Guide, Cisco IOS XE Release 3S.

Note Users with no privilege level or users with a privilege level that is less than the operator's privilege level are considered as auditors with read-only permission.

To configure TACACS+:

```
configure terminal
tacacs-server host 209.165.201.20 shared-secret test1

key 0
admin-priv 14
```

```
oper-priv 9

commit
```

In this configuration, privilege level 14 is assigned to the administrator role, and privilege level 9 is assigned to the operator role. This means a user with privilge level 14 or higher will have all admin privileges when the user logs into the system, and a user with privilege level 9 or higher will have all privileges of an operator at the time of login.

TACACS+ APIs and Commands

TACACS+ APIs	TACACS+ Commands
• /api/config/security_servers/tacacs-server • /api/config/security_servers/tacacs-server?deep • /api/config/security_servers/tacacs-server/host/<ip-address/domain-name>	• tacacs-server host • key • admin-priv • oper-priv

Configuring the Trusted IP Connection

For security reasons, the administrator can restrict access to the host server by enabling trusted IP connection using the management port. This feature helps you specify a single IP address or a range of IP addresses as trusted source IP address or addresses to prevent unauthorized access to the host server.

To configure the trusted IP connection:

```
configure terminal
system settings trusted-source 192.0.2.0/24
commit
```

Verifying the Trusted IP Connection

Use the **show system settings-native trusted-source** command to verify the configuration of trusted IP connection, and to get details of valid IP addresses or the range of valid IP addresses.

```
nfvis# show system settings-native trusted-source
system settings-native trusted-source [ 192.0.2.0/24 ]
```

Trusted IP Connection APIs and Commands

Trusted IP Connection APIs	Trusted IP Connection Commands
• /api/config/system/settings • /api/operational/system/settings-native/trusted-source • /api/operational/system/settings-native?deep • /api/operational/system/settings?deep	• system settings trusted-source • show system settings-native trusted-source

Configuring Your Banner and Message of the Day

Cisco Enterprise NFVIS supports two types of banners: system-defined and user-defined banners. You cannot edit or delete the system-defined banner, which provides copyright information about the application. Banners are displayed on the login page of the portal.

You can post messages using the Message of the Day option. The message is displayed on the portal's home page when you log into the portal.

To configure your banner and message:

```
configure terminal
banner-motd banner "This is a banner" motd "This is the message of the day"
commit
```

Note Currently, you can create banners and messages in English only. You can view the system-defined banner using the **show banner-motd** command. This command does not display the user-defined banner or message.

Banner and Message APIs and Commands

Banner and Message APIs	Banner and Message Commands
• /api/config/banner-motd • /api/operational/banner-motd	• banner-motd • show banner-motd

Setting the System Time Manually or With NTP

You can configure the Cisco Enterprise NFVIS system time manually or synchronise with an external time server using Network Time Protocol (NTP).

To set the system time manually:

```
configure terminal
system time manual_time
2016-11-22T11:38:00
commit
```

Note NTP is automatically disabled when the time clock is set manually.

To set the system time using NTP:

```
configure terminal
system time  ntp preferred_server
209.165.201.20 backup_server 1.ntp.esl.cisco.com
commit
```

Verifying the System Time Configuration

To verify all system time configuration details, use the **show system time** command in privileged EXEC mode as shown below:

```
nfvis# show system time
system time date 2016-11-24T02:48:38-00:00
system time timezone "America/Chicago (CST, -0600)"
system time ntp-status synchronised
system time preferred-server 171.68.38.65
system time backup-server ntp.esl.cisco.com
system time ntp current-server 171.68.38.65
system time ntp stratum-level "stratum 2"
system time ntp time-correct-within "18 ms"
system time ntp polling-server-every "512 s"
```

If the NTP server is invalid, the NTP status becomes "unsynchronised". The NTP server takes some time to get synchronised. During this time of synchronisation also, the **show system time** command output displays NTP status as "unsynchronised".

System Time APIs and Commands

APIs	Commands
• /api/config/system/time/manual_time • /api/config/system/time/ntp/preferred_server • /api/config/system/time/ntp/backup_server • /api/config/system/time/timezone • /api/operational/system/host_time	• system time • show system time

Enabling or Disabling the Portal Access

The Cisco Enterprise NFVIS portal access is enabled by default. You can disable the access if required.

To disable the portal access:

```
configure terminal
system portal access disabled
commit
```

Note You can enable the portal access using the **enable** keyword with the **system portal access** command.

Verifying the Portal Access

Use the **show system portal status** command to verify the portal access status as shown below:

```
nfvis# show system portal status
system portal status "access disabled"
```

Portal Access APIs and Commands

Portal Access APIs	Portal Access Commands
• /api/config/system/portal • /api/operational/system/portal/status	• system portal access • show system portal status

Configuring System Logs

You can set system logs for troubleshooting purpose. There are two log types and five log levels. The two log types are configuration and operational.

The following table explains the log levels:

Log Level	Purpose
DEBUG	Information, typically of interest only when diagnosing problems.
INFO	Confirmation that things are working as expected.
WARNING	An indication that something unexpected happened, or indicative of some problem in the near future (for example, ‘disk space low’). The software application is still working as expected.
ERROR	Due to a serious problem, the software application is not able to perform some function.
CRITICAL	A serious error, indicating that the program itself may not be ble to continue running.

Note The INFO and WARNING log levels are set by default respectively for the configuration and operational log types. You can change them as required. However, the change to the log level is not persisted across a reboot. After a reboot, the default log levels are used.

You can configure system logs using the **system set-log** command in global configuration or privileged EXEC mode:

```
system set-log level error logtype configuration
```

Verifying the System Log Configuration

To verify the system log configuration, use the **show system logging-level** command as shown below:

```
nfvis# show system logging-level
system logging-level configuration error
```

System Log APIs and Commands

System Log APIs	System Log Commands
- /api/config/system/upgrade - /api/operational/system/upgrade/reg-info - /api/operational/system/upgrade/apply-image	- system set-log - show system logging-level