Command Reference Guide for Cisco Prime Infrastructure 2.1

First Published: June 11, 2014

C O N T E N T S

Preface

This guide describes how you can configure and maintain the Cisco Prime Infrastructure Release 2.0 using the command-line interface (CLI). Each topic provides a high-level summary of the tasks required for using the CLI for the Prime Infrastructure in the Unified Network Solution that runs on supported appliances for small, medium, and large Cisco Prime Infrastructure deployments.

- Who Should Read This Guide, page ix
- How to Use This Guide, page ix
- How This Guide Is Organized, page x
- Document Conventions, page x
- Documentation Updates, page xi
- Related Documentation, page xi
- Obtaining Documentation and Submitting a Service Request, page xii

Who Should Read This Guide

The majority of the instructions in this guide are straightforward; however, a few are complex. Therefore, only experienced users should use these instructions.

Note Use this guide in conjunction with the documentation listed in Related Documentation, on page xi.

How to Use This Guide

We recommend that you use the information in this guide as follows:

- Read the document in its entirety. Subsequent sections build on information and recommendations discussed in previous sections.
- Use this document for all-inclusive information about the Prime Infrastructure appliance.
- Do not vary the command-line conventions.

How This Guide Is Organized

The following table lists the major sections of this guide.

Chapter	Title	Description
Overview of the Cisco Prime Infrastructure Command-Line Interface	Overview of the Cisco Prime Infrastructure Command-Line Interface	Provides an overview of the Prime Infrastructure CLI environment and command modes.
Using the Command-Line Interface	Using the Cisco Prime Infrastructure Command-Line Interface	Describes how you can access and administer Prime Infrastructure using the CLI.
Command Reference	Cisco Prime Infrastructure Command Reference	Provides a complete description of all Prime Infrastructure CLI commands.

Document Conventions

This guide uses the following conventions to convey instructions and information.

Convention	Description
bold font	Commands and keywords.
italic font	Variables for which you supply values.
[......]	Keywords or arguments that appear within square brackets are optional.
{x	y	z}	A choice of required keywords appears in braces separated by vertical bars. You must select one.
courier font	Examples of information displayed on the screen.
bold courier font	Examples of information you must enter.
<.....>	Nonprinting characters (for example, passwords) appear in angle brackets.
[....]	Default responses to system prompts appear in square brackets.

Note   Means reader take note. Notes contain helpful suggestions or references to material not covered in the manual.

Tip   Means the following information will help you solve a problem.

Caution   Means reader be careful. In this situation, you might perform an action that could result in equipment damage or loss of data.

Documentation Updates

This table lists the documentation updation dates.

Table 1: Updates to the CLI Reference Guide for the Cisco Prime Infrastructure

Date	Description
11/1/10	Cisco Network Control System (NCS) Release 1.0
05/31/12	Cisco Network Control System (NCS) Release 1.1
08/27/12	Cisco Prime Infrastructure Release 1.2
04/04/13	Cisco Prime Infrastructure Release 1.4

Related Documentation

The tables lists the Cisco Prime Infrastructure documents.

Table 2: Product Documentation

Document Title	Location
Cisco Prime Infrastructure 1.2 Release Notes	http://www.cisco.com/en/US/partner/docs/net_mgmt/prime/infrastructure/1.2/release/notes/cpi_rn.html
Cisco Prime Infrastructure 1.2 Configuration Guide	http://www.cisco.com/en/US/docs/wireless/prime_infrastructure/1.2/configuration/guide/pi_12_cg.html

Cisco Prime Infrastructure 1.2 Command Reference Guide	http://www.cisco.com/en/US/docs/wireless/prime_infrastructure/1.2/command/reference/cli12.html
Cisco Prime Infrastructure 1.4 Release Notes	http://www.cisco.com/en/US/docs/net_mgmt/prime/infrastructure/1.4/release/notes/cpi_rn_14.html
Cisco Prime Infrastructure 1.4 Configuration Guide	http://www.cisco.com/en/US/docs/wireless/prime_infrastructure/1.4/configuration/guide/pi_14_cg.html
Cisco Prime Infrastructure 1.4 Command Reference Guide	http://www.cisco.com/en/US/docs/wireless/prime_infrastructure/1.4/command/reference/cli14.html

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly What's New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

Overview of the Cisco Prime Infrastructure Command-Line Interface

This chapter provides an overview of how to access the Cisco Prime Infrastructure command-line interface (CLI), the different command modes, and the commands that are available in each mode.

You can configure and monitor the Prime Infrastructure through the web interface. You can also use the CLI to perform the configuration and monitoring tasks described in this guide.

Accessing the Prime Infrastructure Command Environment

You can access the Prime Infrastructure CLI through a secure shell (SSH) client or the console port using one of the following machines:

- Windows PC running Windows XP/Vista
- Apple Computer running Mac OS X 10.4 or later
- PC running Linux

User Accounts and Modes in the Prime Infrastructure CLI

Two different types of accounts are available on the Prime Infrastructure CLI:

- Admin (administrator)

- Operator (user)

When you power on the Prime Infrastructure appliance for the first time, you are prompted to run the setup utility to configure the appliances. During this setup process, an administrator user account, also known as an Admin account, is created. After you enter the initial configuration information, the appliance automatically reboots and prompts you to enter the username and the password that you specified for the Admin account. You must use this Admin account to log in to the Prime Infrastructure CLI for the first time.

An Admin can create and manage Operator (user) accounts (which have limited privileges and access to the Prime Infrastructure server). An Admin account also provides the functionality that is needed to use the Prime Infrastructure CLI.

To create more users (with admin and operator privileges) with SSH access to the Prime Infrastructure CLI, you must enter the **username** command in configuration mode (see Command Modes in the Prime Infrastructure CLI).

Table 3: Command Privileges lists the command privileges for each type of user account: Admin and Operator (user).

Table 3: Command Privileges

	User Account	
	Admin	Operator (User)
application commands	*	
backup	*	
backup-logs	*	
cdp run	*	
clock	*	
configure terminal	*	
copy commands	*	
debug	*	
delete	*	
dir	*	
exit	*	*

	User Account	
	Admin	**Operator (User)**
forceout	*	
halt	*	
mkdir	*	
ncs	*	
nslookup	*	*
patch	*	
patch install	*	
patch remove	*	
ping	*	*
ping6	*	*
reload	*	
repository	*	
restore commands	*	
rmdir	*	
root	*	
root_enable	*	
show application	*	
show backup	*	
show cdp	*	*
show clock	*	*
show cpu	*	*
show disks	*	*
show icmp_status	*	*

	User Account	
	Admin	**Operator (User)**
show icmp_status	*	*
show interface	*	*
show ip route	*	
show logging	*	*
show logins	*	*
show memory	*	*
show ntp	*	*
show ports	*	*
show process	*	*
show repository	*	
show restore	*	
show running-config	*	
show startup-config	*	
show tech-support	*	
show terminal	*	*
show timezone	*	*
show timezones	*	
show udi	*	*
show uptime	*	*
show users	*	
show version	*	*
ssh	*	*
tech	*	

	User Account	
	Admin	**Operator (User)**
telnet	*	*
terminal	*	*
traceroute	*	*
undebug	*	
write	*	

Logging in to the Prime Infrastructure server places you in operator (user) mode or admin (EXEC) mode, which always requires a username and password for authentication.

You can tell which mode you are in by looking at the prompt. A right angle bracket (>) appears at the end of operator (user) mode prompt; a pound sign (#) appears at the end of admin mode prompt, regardless of the submode.

Command Modes in the Prime Infrastructure CLI

This section describes the command modes supported in Prime Infrastructure.

EXEC Commands

EXEC commands primarily include system-level commands such as **show** and **reload** (for example, application installation, application start and stop, copy files and installations, restore backups, and display information).

- Table 4: Summary of EXEC Commands describes the EXEC commands

- Table 5: Summary of show Commands describes the show commands in EXEC mode

For detailed information on EXEC commands, see Understanding Command Modes, page 2-5.

EXEC or System-Level Commands

Table 4: Summary of EXEC Commands describes EXEC mode commands.

Table 4: Summary of EXEC Commands

	Description
application install	Installs a specific application bundle.
application remove	Removes a specific application.
application start	Starts or enables a specific application.
application stop	Stops or disables a specific application.
application upgrade	Upgrades a specific application bundle.
backup	Performs a backup and places the backup in a repository.
backup-logs	Performs a backup of all of the logs on the Prime Infrastructure to a remote location.
clock	Sets the system clock on the Prime Infrastructure server.
configure	Enters configuration mode.
copy	Copies any file from a source to a destination.
debug	Displays any errors or events for various command situations; for example, backup and restore, configuration, copy, resource locking, file transfer, and user management.
delete	Deletes a file in the Prime Infrastructure server.
dir	Lists the files in the Prime Infrastructure server.
exit	Disconnects the encrypted session with a remote system. Exits from the current command mode to the previous command mode.
forceout	Forces the logout of all of the sessions of a specific Prime Infrastructure server system user.
halt	Disables or shuts down the Prime Infrastructure server.
help	Describes the help utility and how to use it in the Prime Infrastructure server.
mkdir	Creates a new directory.
ncs	NCS-related commands used to start, stop and back up the server.

	Description
nslookup	Queries the IPv4 address or hostname of a remote system.
patch	Installs System or Application patch.
ping	Determines the IPv4 network connectivity to a remote system.
ping6	Determines the IPv6 network connectivity to a remote system.
reload	Reboots the Prime Infrastructure server.
restore	Restores a previous backup.
rmdir	Removes an existing directory.
root	Executes the root shell.
root_enable	Activates the **root** command.
show	Provides information about the Prime Infrastructure server.
ssh	Starts an encrypted session with a remote system.
tech	Provides Cisco Technical Assistance Center (TAC) commands.
telnet	Establishes a Telnet connection to a remote system.
terminal length	Sets terminal line parameters.
terminal session-timeout	Sets the inactivity timeout for all terminal sessions.
terminal session-welcome	Sets the welcome message on the system for all terminal sessions.
terminal terminal-type	Specifies the type of terminal connected to the current line of the current session.
traceroute	Traces the route of a remote IP address.
undebug	Disables the output (display of errors or events) of the **debug** command for various command situations; for example, backup and restore, configuration, copy, resource locking, file transfer, and user management.
write	Erases the startup configuration that forces to run the setup utility and prompt the network configuration, copies the running configuration to the startup configuration, and displays the running configuration on the console.

show Commands

The **show** commands are used to display the Prime Infrastructure settings and are among the most useful commands. See Table 5: Summary of show Commands for a summary of the **show** commands. The **show** commands must be followed by a keyword; for example, **show application status**. Some **show** commands require an argument or variable after the keyword to function; for example, **show application version**.

Table 5: Summary of show Commands

	Description
application (requires keyword)	Displays information about the installed application; for example, status information or version information.
backup (requires keyword)	Displays information about the backup.
cdp (requires keyword)	Displays information about the enabled Cisco Discovery Protocol interfaces.
clock	Displays the day, date, time, time zone, and year of the system clock.
cpu	Displays CPU information.
disks	Displays file-system information of the disks.
icmp-status	Displays the Internet Control Message Protocol (ICMP) echo response configuration information.
interface	Displays statistics for all of the interfaces configured on the Prime Infrastructure.
inventory	Displays information about the hardware inventory, including the Prime Infrastructure appliance model and serial number.
logging (requires keyword)	Displays the Prime Infrastructure server logging information.
logins (requires keyword)	Displays the login history of the Prime Infrastructure server.
memory	Displays memory usage by all running processes.
ntp	Displays the status of the Network Time Protocol (NTP) servers.
ports	Displays all of the processes listening on the active ports.
process	Displays information about the active processes of the Prime Infrastructure server.
repository (requires keyword)	Displays the file contents of a specific repository.

	Description
restore (requires keyword)	Displays the restore history in the Prime Infrastructure.
running-config	Displays the contents of the configuration file that currently runs in the Prime Infrastructure.
startup-config	Displays the contents of the startup configuration in the Prime Infrastructure.
tech-support	Displays system and configuration information that you can provide to the TAC when you report a problem.
terminal	Displays information about the terminal configuration parameter settings for the current terminal line.
timezone	Displays the current time zone in the Prime Infrastructure.
timezones	Displays all of the time zones available for use in the Prime Infrastructure.
udi	Displays information about the unique device identifier (UDI) of the Prime Infrastructure.
uptime	Displays how long the system you are logged in to has been up and running.
users	Displays information about the system users.
version	Displays information about the currently loaded software version, along with hardware and device information.

Configuration Commands

Configuration commands include **interface** and **repository**. To access configuration mode, run the **configure** command in EXEC mode.

Some of the configuration commands require that you enter the configuration submode to complete the configuration.

Table 6: Summary of Configuration Commands describes the configuration commands.

Table 6: Summary of Configuration Commands

	Description
backup-staging-url	Specifies a Network File System (NFS) temporary space or staging area for the remote directory for backup and restore operations.
cdp holdtime	Specifies the amount of time the receiving device should hold a Cisco Discovery Protocol packet from the Prime Infrastructure server before discarding it.
cdp run	Enables Cisco Discovery Protocol.
cdp timer	Specifies how often the Prime Infrastructure server sends Cisco Discovery Protocol updates.
clock timezone	Sets the time zone for display purposes.
do	Executes an EXEC-level command from configuration mode or any configuration submode. **Note** To initiate, the **do** command precedes the EXEC command.
end	Returns to EXEC mode.
exit	Exits configuration mode.
hostname	Sets the hostname of the system.
icmp echo	Configures the ICMP echo requests.
interface	Configures an interface type and enters interface configuration mode.
ipv6 address autoconfig	Enables IPv6 stateless autoconfiguration in interface configuration mode.
ipv6 address dhcp	Enables IPv6 address DHCP in interface configuration mode.
ip address	Sets the IP address and netmask for the Ethernet interface. **Note** This is an interface configuration command.

	Description
ip default-gateway	Defines or sets a default gateway with an IP address.
ip domain-name	Defines a default domain name that a Prime Infrastructure server uses to complete hostnames.
ip name-server	Sets the Domain Name System (DNS) servers for use during a DNS query.
kron occurrence	Schedule one or more Command Scheduler commands to run at a specific date and time or a recurring level.
kron policy-list	Specifies a name for a Command Scheduler policy.
logging	Enables the system to forward logs to a remote system.
logging loglevel	Configures the log level for the **logging** command.
no	Disables or removes the function associated with the command.
ntp	Synchronizes the software clock through the NTP server for the system.
password-policy	Enables and configures the password policy.
repository	Enters repository submode.
service	Specifies the type of service to manage.
snmp-server community	Sets up the community access string to permit access to the Simple Network Management Protocol (SNMP).
snmp-server contact	Configures the SNMP contact the Management Information Base (MIB) value on the system.
snmp-server host	Sends SNMP traps to a remote system.
snmp-server location	Configures the SNMP location MIB value on the system.
username	Adds a user to the system with a password and a privilege level.

For detailed information on configuration mode and submode commands, see Understanding Command Modes, page 2-5.

CLI Audit

You must have administrator access to execute the Prime Infrastructure configuration commands. Whenever an administrator logs in to configuration mode and executes a command that causes configurational changes in the Prime Infrastructure server, the information related to those changes is logged in the Prime Infrastructure operational logs.

Table 7: Configuration Mode Commands for the Operation Log describes configuration mode commands that generate operational logs.

Table 7: Configuration Mode Commands for the Operation Log

	Description
clock	Sets the system clock on the Prime Infrastructure server.
ip name-server	Sets the DNS servers for use during a DNS query.
hostname	Sets the hostname of the system.
ip address	Sets the IP address and netmask for the Ethernet interface.
ntp server	Allows synchronization of the software clock by the NTP server for the system.

In addition to configuration mode commands, some commands in EXEC mode generate operational logs.

Table 8: EXEC Mode Commands for the Operation Log describes EXEC mode commands that generate operational logs.

Table 8: EXEC Mode Commands for the Operation Log

	Description
backup	Performs a backup and places the backup in a repository.
restore	Restores from backup the file contents of a specific repository.
backup-logs	Backs up system logs.

Using the Command-Line Interface

This chapter provides helpful tips for understanding and configuring the Cisco Prime Infrastructure from the command-line interface (CLI). The Prime Infrastructure can be deployed for small, medium, and large deployments and is available on different platforms and also as a software that can run on VMware.

Before Accessing the CLI

Before logging in to the Prime Infrastructure CLI, ensure that you have completed the installation tasks as specified in the *Cisco Prime Infrastructure 2.0 Quick Start Guide*.

Running the Setup Utility to Configure the Prime Infrastructure

When you power on the Prime Infrastructure appliances for the first time, you are prompted to run the setup utility to configure the Prime Infrastructure appliances. Before you run the utility using the **setup** command, ensure that you have values for the following network configuration prompts:

- Hostname

- IP address

- Netmask

- Gateway

- Domain

- Nameserver

- Network Time Protocol (NTP) server (optional)

- User ID

- Password

The following is a sample output from the **setup** command:

```
************************************************
Please type 'setup' to configure the appliance
************************************************
localhost login:  setup
Press 'Ctrl-C' to abort setup
Enter hostname[]: NCS
Enter IP address[]: 172.16.90.183
Enter IP default netmask[]: 255.255.255.0
Enter IP default gateway[]: 172.16.90.1
Enter default DNS domain[]: example.com
Enter primary nameserver[]: 172.16.168.183
Add/Edit another nameserver? Y/N : n
Enter primary NTP server[time.nist.gov]:
Add/Edit secondary NTP server? Y/N : n
Enter username[admin]:
Enter password:
Enter password again:
Bringing up network interface...
Pinging the gateway...
Pinging the primary nameserver...
Do not use 'Ctrl-C' from this point on...
Appliance is configured
```

After you enter the required information, the Prime Infrastructure appliance automatically reboots and the following login prompt appears:

```
machine_name login:
```

where *machine_name* identifies the hostname that you specified when you ran the **setup** command.

In this example, this prompt appears:

```
NCS login:
```

To log in, use the administrator user account (and the corresponding password) that you created during the setup process. You must also use this Admin account to log in to the Prime Infrastructure CLI for the first time. After accessing the CLI as an administrator, you can create more users (with admin and operator privileges) with SSH access to the CLI by running the **username** command in configuration mode.

> ✎ **Note**   The administrator user account and the corresponding password (a CLI user account) that you created during the initial setup wizard can be used to manage the Prime Infrastructure application using the CLI. The CLI user has privileges to start and stop the application software, backup and restore the Prime Infrastructure application data, apply software patches and upgrades to the Prime Infrastructure application software, view all of the system and the application logs, and reload or shut down the Prime Infrastructure appliance. To protect the CLI user credentials, explicitly create users with access to the CLI.

> ✎ **Note**   Any users that you create from the Prime Infrastructure web interface cannot automatically log in to the Prime Infrastructure CLI. You must explicitly create users with access to the CLI. To create these users, you must log in to the CLI using the Admin account that you created during setup; then, enter configuration mode, and run the **username** command.

Accessing the Prime Infrastructure CLI

Before logging in to the Prime Infrastructure CLI, ensure that you have completed the hardware installation and configuration process outlined in the

To log in to the Prime Infrastructure server and access the CLI, use an SSH secure shell client or the console port. You can log in from:

- A PC running Windows XP/Vista.

- A PC running Linux.

- An Apple computer running Mac OS X 10.4 or later.

- Any terminal device compatible with VT100 or ANSI characteristics. On the VT100-type and ANSI devices, you can use cursor-control and cursor-movement key. Keys include left arrow, up arrow, down arrow, right arrow, Delete, and Backspace. The CLI senses the use of the cursor-control keys and automatically uses the optimal device characteristics.

To exit the CLI, use the **exit** command from EXEC mode. If you are currently in one of the configuration modes and you want to exit the CLI, enter the **end**, **exit**, or press **Ctrl z** command to return to EXEC mode, and then enter the **exit** command.

Supported Hardware and Software Platforms

The following valid terminal types can access the Prime Infrastructure:

- 1178

- 2621

- 5051

- 6053

- 8510

- altos5

- amiga

- ansi

- apollo

- Apple_Terminal

- att5425

- ibm327x

- kaypro

- vt100

You can also access the Prime Infrastructure through an SSH client or the console port.

Opening the CLI with Secure Shell

> **Note** To access the Prime Infrastructure CLI environment, use any SSH client that supports SSH v2.

The following example shows you how to log in with a Secure Shell (SSH) client (connecting to a wired WAN) via a PC by using Windows XP. Assuming that Prime Infrastructure is preconfigured through the setup utility to accept an Admin (administrator) user, log in as Admin.

Step 1 Use any SSH client and start an SSH session.
The SSH window appears.

Step 2 Press **Enter** or **Spacebar** to connect.
The Connect to Remote Host window appears.

Step 3 Enter a hostname, username, port number, and authentication method.
In this example, you enter **ncs** for the hostname, **admin** for the username, and **22** for the port number; and, for the authentication method, choose **Password** from the drop-down list.

Step 4 Click **Connect**, or press **Enter**.
The Enter Password window appears.

Step 5 Enter your assigned password for the administrator.
The SSH with the Add Profile window appears.

Step 6 (Optional) Enter a profile name in the text box and click **Add to Profile**.

Step 7 Click **Close** in the Add Profile window.
The Prime Infrastructure command prompt appears. You can now enter Prime Infrastructure CLI commands.

Opening the CLI Using a Local PC

If you need to configure Prime Infrastructure locally (without connecting to a wired LAN), you can connect a PC to the console port on the Prime Infrastructure appliance by using a null-modem cable.

The serial console connector (port) provides access to the CLI locally by connecting a terminal to the console port. The terminal is a PC running terminal-emulation software or an ASCII terminal. The console port (EIA/TIA-232 asynchronous) requires only a null-modem cable.

To connect a PC running terminal-emulation software to the console port, use a DB-9 female to DB-9 female null-modem cable.

To connect an ASCII terminal to the console port, use a DB-9 female to DB-25 male straight-through cable with a DB-25 female to DB-25 female gender changer.

The default parameters for the console port are 9600 baud, 8 data bits, no parity, 1 stop bit, and no hardware flow control.

Note	If you are using a Cisco switch on the other side of the connection, set the switchport to duplex auto, speed auto (the default).

Step 1   Connect a null-modem cable to the console port on the Cisco ISE-3315 and to the COM port on your PC.

Step 2   Set up a terminal emulator to communicate with the Prime Infrastructure. Use the following settings for the terminal emulator connection: 9600 baud, 8 data bits, no parity, 1 stop bit, and no flow control.

Step 3   When the terminal emulator activates, press **Enter**.

Step 4   At the console, enter your username, then press **Enter**.

Step 5   Enter the password, then press **Enter**.
When the CLI activates, you can enter CLI commands to configure the Prime Infrastructure.

Understanding Command Modes

This section describes the Prime Infrastructure command modes in detail.

EXEC Mode

When you start a session on the Prime Infrastructure, you begin in admin or EXEC mode. From EXEC mode, you can enter configuration mode. Most of the EXEC commands (one-time commands), such as **show** commands, display the current configuration status. The admin or EXEC mode prompt consists of the device name or hostname before a pound sign (#), as shown:

```
ncs/admin# (Admin or EXEC mode)
```

Note Throughout this guide, the Prime Infrastructure server uses the name *ncs* in place of the hostname and *admin* of the Prime Infrastructure server for the user account.

You can always tell when you are in EXEC mode or configuration mode by looking at the prompt.

- In EXEC mode, a pound sign (#) appears after the NCS server hostname and your username.

  For example:

  ```
  ncs/admin#
  ```

- In configuration mode, the 'config' keyword and a pound sign (#) appear after the hostname of the Prime Infrastructure server and your username.

  For example:

  ```
  ncs/admin# configure
  Enter configuration commands, one per line.  End with CNTL/Z.
  ncs/admin(config)# (configuration mode)
  ```

If you are familiar with UNIX, you can equate EXEC mode to *root* access. You could also equate it to the administrator level in Windows NT or the supervisor in NetWare. In this mode, you have permission to access everything in the Prime Infrastructure server, including the configuration commands. However, you cannot enter configuration commands directly. Before you can change the actual configuration of the Prime Infrastructure server, you must enter configuration mode by entering the **configure** or **configure terminal (conf t)** command. Enter this command only when in EXEC mode.

For example:

```
ncs/admin# conf t
Enter configuration commands, one per line. End with CNTL-Z.
ncs(config)# (configuration mode)
```
The configuration mode has several submodes; each has its own prompt. To enter these submodes, you must first enter configuration mode by entering the **configure terminal** command.

To exit configuration mode, enter the **end**, **exit**, or **Ctrl-z** command. To exit EXEC mode, enter the **exit** command. To exit both configuration and EXEC modes, enter this sequence of commands:

```
ncs/admin(config)# exit
ncs/admin# exit
```
To obtain a listing of commands in EXEC mode, enter a question mark (**?**):

```
ncs/admin# ?
```

Configuration Mode

Use configuration mode to make changes to the existing configuration. When you save the configuration, these commands remain across Prime Infrastructure server reboots, but only if you run either of these commands:

- **copy running-config startup-config**

- **write memory**

To enter configuration mode, run the **configure** or **configure terminal (conf t)** command in EXEC mode. When in configuration mode, the Prime Infrastructure expects configuration commands.

For example:

```
ncs/admin# configure
Enter configuration commands, one per line. End with CNTL-Z.
ncs/admin(config)# (configuration mode)
```

From this level, you can enter commands directly into the Prime Infrastructure configuration. To obtain a listing of commands in this mode, enter a question mark (**?**):

```
ncs/admin(config)# ?
```

The configuration mode has several configuration submodes. Each of these submodes places you deeper in the prompt hierarchy. When you enter the **exit**, command the Prime Infrastructure backs you out one level and returns you to the previous level. When you enter the **exit** command again, the Prime Infrastructure backs you out to the EXEC level.

Note In configuration mode, you can alternatively press the **Ctrl-z** instead of entering the **end** or **exit** command.

Configuration Submodes

In the configuration submodes, you can enter commands for specific configurations. For example:

```
ncs/admin# config t
ncs/admin(config)# interface GigabitEthernet 0
ncs/admin(config-GigabitEthernet)#
```
To obtain a list of commands in this mode, enter a question mark (**?**):

```
ncs/admin(config-GigabitEthernet)# ?
```
Use the **exit** or **end** command to exit this prompt and return to the configuration prompt.

The following table lists the commands in the interface GigabitEthernet 0 configuration submode. Other configuration submodes exist including those specific to the **kron**, **repository**, and **password policy** commands.

Table 9: Command Options in the Interface GigabitEthernet 0 Configuration Submode

	Comment
| ```
ncs/admin(config)# interface GigabitEthernet 0
ncs/admin(config-GigabitEthernet)# ?
Configure ethernet interface:
  do        EXEC command
  end       Exit from configure mode
  exit      Exit from this submode
  ip        Configure IP features
  ipv6      Configure IPv6 features
  no        Negate a command or set its defaults
  shutdown  Shutdown the interface
ncs/admin(config-GigabitEthernet)#
``` | Enter the command that you want to configure for the interface. This example uses the **interface GigabitEthernet** command.<br><br>Enter **?** to display what you must enter next on the command line. This example shows the available **interface GigabitEthernet** configuration submode commands. |
| ```
ncs/admin(config-GigabitEthernet)# ip ?
  address  Configure IP address
ncs/admin(config-GigabitEthernet)# ip
``` | Enter the command that you want to configure for the interface. This example uses the **ip** command.<br><br>Enter **?** to display what you must enter next on the command line. This example shows the available **ip** configuration submode commands. |
| ```
ncs/admin(config-GigabitEthernet)# ip address ?
  <A.B.C.D>  IPv4 address
ncs/admin(config-GigabitEthernet) ip address
``` | Enter the command that you want to configure for the interface. This example uses the **ip addresss** command.<br><br>Enter **?** to display what you must enter next on the command line. In this example, you must enter an IPv4 address.<br><br>A carriage return <cr> does not appear; therefore, you must enter additional arguments to complete the command. |
| ```
ncs/admin(config-GigabitEthernet)# ip address 172.16.0.1 ?
  <A.B.C.D>  Network mask
ncs/admin(config-GigabitEthernet)# ip address 172.16.0.1
``` | |

	Comment
	Enter the keyword or argument that you want to use. This example uses the 172.16.0.1 IP address.
	Enter **?** to display what you must enter next on the command line. In this example, you must enter a network mask.
	A carriage return <cr> does not display; therefore, you must enter additional arguments to complete the command.
| ```
ncs/admin(config-GigabitEthernet)# ip address 172.16.0.1
255.255.255.224 ?
  <cr>  Carriage Return
ncs/admin(config-GigabitEthernet)# ip address 172.16.0.1
255.255.255.224 ?
``` | Enter the network mask. This example uses the 255.255.255.224 IP address. |
| | Enter **?** to display what you must enter next on the command line. In this example, you can press **Enter**. |
| | A carriage return <cr> displays; you can press **Enter** to complete the command. |

Navigating the CLI Commands

This section describes how to navigate the commands and modes on the

Getting Help

Use the question mark (**?**) and the arrow keys to help you enter commands:

- For a list of available commands, enter a question mark (**?**):

  ```
  ncs/admin# ?
  ```

- To complete a command, enter a few known characters before **?** (with no space):

  ```
  ncs/admin# s?
  ```

- To display keywords and arguments for a command, enter **?** at the prompt or after entering part of a command followed by a space:

  ```
  ncs/admin# show ?
  ```
  The Prime Infrastructure displays a list and brief description of available keywords and arguments.

  Note The <cr> symbol in command help stands for "carriage return", which means to press the **Return** or the **Enter** key). The <cr> at the end of command help output indicates that you have the option to press **Enter** to complete the command and that the arguments and keywords in the list preceding the <cr> symbol are optional. The <cr> symbol by itself indicates that no more arguments or keywords are available, and that you must press **Enter** to complete the command.

- To redisplay a command that you previously entered, press the **Up Arrow** key. Continue to press the **Up Arrow** key to see more commands.

Using the No and Default Forms of Commands

Some EXEC or configuration commands have a **no** form. In general, use the **no** form to disable a function. Use the command without the **no** keyword to re-enable a disabled function or to enable a function disabled by default; for example, an IP address enabled by default. To disable the IP address, use the **no ip address** command; to re-enable the IP address, use the **ip address** command.

Configuration commands can also have a **default** form, which returns the command settings to the default values. Most commands disable by default, so in such cases using the **default** form has the same result as using the **no** form of the command. However, some commands are enabled by default and have variables set to certain default values. In these cases, the **default** form of the command enables the command and sets the variables to their default values.

See for a description of the complete syntax of the configuration commands, and the **no** and **default** forms of a command.

Command-Line Conventions

Command-Line Editing Key Conventions

The Prime Infrastructure provides a number of keyboard shortcuts that you can use to edit an entered line.

Tab

Press **Tab** to try to finish the current command.

If you press the **Tab** key:

- At the beginning of a line, the system lists all of the short-form options.

- When you enter a partial command, the system lists all of the short form options beginning with those characters.

- When only one possible option is available, the system fills in the option automatically.

Ctrl-c

Press **Ctrl-c** to abort the sequence. Pressing this key sequence breaks out of any executing command and returns to the previous mode.

Ctrl-z

Press **Ctrl-z** to exit configuration mode and return to previous configuration mode.

?

Enter a question mark (?) at the prompt to list the available commands.

Command Line Completion

Command-line completion makes the Prime Infrastructure CLI more user-friendly. It saves you extra key strokes and helps out when you cannot remember the syntax of a command.

For example, for the **show running-config** command:

```
ncs/admin# show running-config
```
You can:

```
ncs/admin# sh run
```
The Prime Infrastructure expands the command **sh run** to **show running-config**.

Another shortcut is to press the **Tab** key after you type **sh**; the Cisco NCS CLI fills in the rest of the command, in this case **show**.

If the Cisco NCS CLI does not understand a command, it repeats the entire command line and places a caret symbol (^) under the point at which it is unable to parse the command.

For example:

```
ncs/admin# show unning-configuration
           ^
% Invalid input detected at '^' marker.
```
The caret symbol (^) points to the first letter in the command line that the Prime Infrastructure does not understand. Usually, this means that you need to provide additional arguments to complete the command or you mispelled the command. In this case, you omitted the "r" in the "unning" command. To fix the error, retype the command.

In another form of command-line completion, you can start a command by entering the first few characters, then pressing the **Tab** key. As long as you can match one command, the Prime Infrastructure CLI will complete the command. For example, if you type **sh** and press **Tab**, the Prime Infrastructure completes the **sh** with **show**. If Prime Infrastructure does not complete the command, you can enter a few more letters and press **Tab** again.

Continuing Output at the --More-- Prompt

When working with the Prime Infrastructure CLI, output often extends beyond the visible screen length. For cases where output continues beyond the bottom of the screen, such as with the output of many **?** or **show** commands, the output pauses and a --More-- prompt appears at the bottom of the screen. To resume output, press **Return** to scroll down one line, or press the **spacebar** to display the next full screen of output.

Tip If the output pauses on your screen but you do not see the **--More--** prompt, try entering a smaller value for the screen length by using the **terminal length** EXEC command. Command output will not pause if you set the length value to zero (0).

Where to Go Next

Now that you are familiar with some of the Prime Infrastructure CLI basics, you can begin to configure the Prime Infrastructure by using the CLI.

Remember that:

- You can use the question mark (**?**) and arrow keys to help you enter commands.

- Each command mode restricts you to a set of commands. If you have difficulty entering a command, check the prompt and then enter the question mark (**?**) to see a list of available commands.

- To disable a feature, enter the keyword **no** before the command; for example, **no ip address**.

- You must save your configuration changes so that you preserve them during a system reload or power outage.

Proceed to for command listings, descriptions, syntax, usage guidelines, and sample output.

Command Reference

This appendix contains necessary information on disk space management for all types of Cisco Prime Infrastructure deployments and an alphabetical listing of the commands specific to the Prime Infrastructure. The Prime Infrastructure comprise the following modes:

- EXEC
    - System-level
    - Show

- Configuration
    - configuration submode

     Use EXEC mode system-level **config** or **configure** command to access configuration mode.

Each of the commands in this appendix is followed by a brief description of its use, command syntax, any command defaults, command modes, usage guidelines, and one or more examples. Throughout this appendix, the Prime Infrastructure server uses the name *ncs* in place of the Prime Infrastructure server's hostname.

Note   If an error occurs in any command usage, use the **debug** command to determine the cause of the error.

Disk Space Management in Prime Infrastructure

This section provides information on disk space in the Prime Infrastructure appliances for all types of deployments. Each of the Prime Infrastructure appliances has a different amount of disk space, and managing that disk space is important to enable you to use the Prime Infrastructure efficiently.

Before proceeding to use the Prime Infrastructure CLI commands, familiarize yourself with disk space management in the Prime Infrastructure appliances. You can deploy the Prime Infrastructure on appliances with small, medium and large form factors and VMware. Table 10: Prime Infrastructure Appliances Configuration provides information on Prime Infrastructure appliances on all of the form factors and the available disk space that you need to manage the Prime Infrastructure.

Table 10: Prime Infrastructure Appliances Configuration

Appliance Form Factor	Prime Infrastructure Appliances	Hard Disk Configuration
Small	-	2 x 250 GB SATA HDD.
Medium	-	2 x 300 GB SAS RAID HDD.
Large	-	4 x 300 GB SAS RAID HDD.
VMware	NCS-DEMO-10 (to run a Demo/Evaluation)	30 GB
	L-NCS-1.0-K9 (to run the PxP production image)	60 GB
	L-NCS-1.0-K9 (to run M&T production image)	200 GB

Table 11: Disk Space on /var Partition lists the disk space that you may use on the /var partition that has a total of 6 GB of disk space. You may use 308 MB of the 6 GB of disk space for the operating system and the Cisco ADE OS 2.0 log files. You can then use the remaining 5.7 GB of disk space for a medium and large type deployment.

Table 11: Disk Space on /var Partition

Process	Files	Small	Medium and Large	VMware
Linux OS	System	-	258 MB	-
Cisco ADE OS 2.0	/var/log/ade/ADE.log	-	50 MB	-

All of the files that you create in the Prime Infrastructure reside in the /opt partition. You must manage the disk space for the files that you create in the /opt partition so that the files increase in size within the limits that do not have an impact on other files and services in the system.

Table 12: Disk Space on /opt Partition lists the disk space that you may use on the /opt partition that has a total of 410 GB of disk space. You may use 161 GB of disk space and the remaining of 249 GB for a medium and large type deployment. The remaining 249 GB of disk space can be better utilized for the database growth after you consider the disk space required for backup, restore, and replication.

Table 12: Disk Space on /opt Partition

Process	Files	Small	Medium and Large	VMware
CSCOcpm	Application product files (includes Oracle, Tomcat, and TimesTen)		7.5 GB	-
PxP Database	/opt/oracle/base/oradata/cpm10/cpm01.dbf		31 GB	-
MnT Database	opt/oracle/base/oradata/cpm10/mnt01.dbf		120 GB	-
TimesTen User Cache Database	opt/oracle/base/product/11.2.0/dbhome_1/dbs/datfttuser.dbf		100 GB	-
Oracle RDBMS System	Redo Logs (redo01.log, redo02.log and redo03.log) Built-in databases: temp01.dbf example01.dbf system01.dbf undotbs01.dbf sysaux01.dbf users01.dbf control01.ctl		50 MB 30 MB 104 MB 770 MB 160 MB 580 MB 5 MB 9 MB	-
Monit	/opt/CSCOcpm/logs/monit.log		55 MB	-
CPM PSC Log	/opt/CSCOcpm/logs/cpm-psc.log*.*		200 MB	-
CPM PrRT Log	/opt/CSCOcpm/logs/cpm-psc.log*.*		200 MB	-
CPM Profiler Log	/opt/CSCOcpm/profiler/logs/profiler.log*		200 MB	-
MnT Collector Log	/opt/CSCOcpm/logs/mnt-collector.out		20 MB	-
MnT Decap Log	/opt/CSCOcpm/logs/mnt-decap.out		100 MB	-
CPM Client Provisioning agent binaries	/opt/CSCOcpm/provisioning		100 MB	-
Tomcat	/opt/CSCOcpm/appsrv/apache-tomcat-6.0.18/logs/*		100 MB	-
PrRT Audit Logger	/opt/CSCOcpm/logs/prrt.log	-	-	-

Command Reference Guide for Cisco Prime Infrastructure 2.1

For detailed information on logging into the Prime Infrastructure, refer to the *Cisco Prime Network Control System Configuration Guide, Release 2.0.*

EXEC Commands

This section lists each EXEC command and each command page includes a brief description of its use, command syntax, any command defaults, command modes, usage guidelines, and an example of the command and any related commands.

application install

✎

Note   You are not allowed to run the **application install** command from the CLI under normal operations because the Prime Infrastructure application is preinstalled with a Cisco IOS image on all supported appliances and VMware.

To install a specific application other than the Prime Infrastructure, use the **application install** command in EXEC mode. To remove this function, use the **application remove** command.

application install *application-bundle remote-repository-name*

Syntax Description

application-bundle	Application bundle filename. Up to 255 alphanumeric characters.
remote-repository-name	Remote repository name. Up to 255 alphanumeric characters.

Command Default   No default behavior or values.

Command Modes   EXEC

Usage Guidelines   Installs the specified application bundle on the appliance. The application bundle file is pulled from the specified repository.

If you enter the **application install** or **application remove** command when another installation or removal operation of an application is in progress, you will see the following warning message:

```
An existing application install, remove, or upgrade is in progress.  Try again shortly.
```

Examples
```
ncs/admin# application install ncs-appbundle-1.0.2.054.i386.tar.gz myrepository
Do you want to save the current configuration ? (yes/no) [yes] ? y
Please enter yes or no
Do you want to save the current configuration ? (yes/no) [yes] ? yes
Generating configuration...
Saved the running configuration to startup successfully
Initiating Application installation...
Extracting NCS database content...
Starting NCS database processes...
Restarting NCS database processes...
Creating NCS M&T session directory...
Performing NCS database priming...

Application successfully installed

ncs/admin# application install ncs-appbundle-1.0.2.054.i386.tar.gz myrepository
Do you want to save the current configuration ? (yes/no) [yes] ? no
Initiating Application installation...
Extracting NCS database content...
Starting NCS database processes...
```

```
Restarting NCSdatabase processes...
Creating NCS M&T session directory...
Performing NCS database priming...

Application successfully installed
```

Related Commands

Command	Description
application remove	Removes or uninstalls an application.
application start	Starts or enables an application.
application stop	Stops or disables an application.
application upgrade	Upgrades an application bundle.
show application	Shows application information for the installed application packages on the system.

application remove

✎

Note   You are not allowed to run the **application remove** command from the CLI to remove the Prime Infrastructure application unless you are explicitly instructed to do so for an upgrade.

To remove a specific application other than the Prime Infrastructure, use the **application remove** command in EXEC mode. To remove this function, use the **no** form of this command.

application remove *application-name*

no application remove *application-name*

Syntax Description

application-name	Application name. Up to 255 alphanumeric characters.

Command Default   No default behavior or values.

Command Modes   EXEC

Usage Guidelines   Removes or uninstalls an application.

Examples
```
ncs/admin# application remove ncs
Continue with application removal? [y/n] y

Application successfully uninstalled
ncs/admin#
```

Related Commands

Command	Description
application install	Installs an application bundle.
application start	Starts or enables an application.
application stop	Stops or disables an application.
application upgrade	Upgrades an application bundle.
show application	Shows application information for the installed application packages on the system.

application reset-config

Note This command is not currently supported by Prime Infrastructure.

To reset an application configuration to factory defaults, use the **application reset-config** command in EXEC mode.

application reset-config *application-name*

Syntax Description

application-name	Name of the application to reset its configuration to factory defaults. Up to 255 alphanumeric characters.

Command Default No default behavior or values.

Command Modes EXEC

Usage Guidelines You can use the **application reset-config** command to reset the Prime Infrastructure configuration to factory defaults without reimaging the Prime Infrastructure appliance or VMware.

Examples
```
ncs/admin# application reset-config ncs
Initialize your identity policy database to factory defaults? (y/n): y
Reinitializing local policy database to factory default state...
Stopping NCS Monitoring & Troubleshooting Log Processor...
Stopping NCS Monitoring & Troubleshooting Log Collector...
Stopping NCS Monitoring & Troubleshooting Alert Process...
Stopping NCS Application Server...
Stopping NCS Monitoring & Troubleshooting Session Database...
Stopping NCS Database processes...
Extracting NCS database content...
Starting NCS database processes...
Restarting NCS database processes...
Creating NCS M&T session directory...
Performing NCS database priming...

Application successfully reset configuration

ncs/admin# application reset-config ncs
Initialize your identity policy database to factory defaults? (y/n): n
Existing policy database will be retained.

Application successfully reset configuration
ncs/admin#
```

application start

To enable a specific application, use the **application start** command in EXEC mode. To remove this function, use the **no** form of this command.

application start *application-name*

Syntax Description

| *application-name* | Name of the predefined application that you want to enable. Up to 255 alphanumeric characters. |

Command Default

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

Enables an application.

You cannot use this command to start the Prime Infrastructure application. If you use this command to start the application, you can see that the Prime Infrastructure is already running.

Examples

```
ncs/admin# application start NCS

NCS Database processes is already running, PID: 7585
NCS M&T Session Database is already running, PID: 7851
NCS Application Server process is already running, PID: 7935
NCS M&T Log Collector is already running, PID: 7955
NCS M&T Log Processor is already running, PID: 8005
NCS M&T Alert Processor is already running, PID: 8046

ncs/admin#
```

Related Commands

Command	Description
application install	Installs an application bundle.
application remove	Removes or uninstalls an application.
application stop	Stops or disables an application.
application upgrade	Upgrades an application bundle.
show application	Shows application information for the installed application packages on the system.

application stop

To disable a specific application, use the **application stop** command in EXEC mode. To remove this function, use the **no** form of this command.

application stop *application-name*

Syntax Description

| *application-name* | Name of the predefined application that you want to disable. Up to 255 alphanumeric characters. |

Command Default   No default behavior or values.

Command Modes   EXEC

Usage Guidelines   Disables an application.

Examples

```
ncs/admin# application stop NCS

Stopping NCS Monitoring & Troubleshooting Log Processor...
Stopping NCS Monitoring & Troubleshooting Log Collector...
Stopping NCS Monitoring & Troubleshooting Alert Process...
Stopping NCS Application Server...
Stopping NCS Monitoring & Troubleshooting Session Database...
Stopping NCS Database processes...

ncs/admin#
```

Related Commands

	Description
application install	Installs an application bundle.
application remove	Removes or uninstalls an application.
application start	Starts or enables an application.
application upgrade	Upgrades an application bundle.
show application	Shows application information for the installed application packages on the system.

application upgrade

To upgrade a specific application bundle, use the **application upgrade** command in EXEC mode. To remove this function, use the **application remove** command.

application upgrade *application-bundle remote-repository-name*

Syntax Description

application-bundle	Application name. Up to 255 alphanumeric characters.
	Note Enter the application name as 'PI' in uppercase.
remote-repository-name	Remote repository name. Up to 255 alphanumeric characters.

Command Default No default behavior or values.

Command Modes EXEC

Usage Guidelines Upgrades an application bundle, and preserves any application configuration data.

If you enter the **application upgrade** command when another application upgrade operation is in progress, you will see the following warning message:

```
An existing application install, remove, or upgrade is in progress. Try again shortly.
```

⚠️
Caution Do not enter the **backup** or **restore** commands when the upgrade is in progress. This action might cause the database to be corrupted.

Examples

```
ncs/admin# application upgrade NCS-appbundle-1.0.2.054.i386.tar.gz myremoterepository
Do you want to save the current configuration ? (yes/no) [yes] ? yes
Generating configuration...
Saved the running configuration to startup successfully
Initiating Application Upgrade...
ncs/admin#

ncs/admin# application upgrade NCS-appbundle-1.0.2.054.i386.tar.gz myremoterepository
Do you want to save the current configuration ? (yes/no) [yes] ? no
Initiating Application Upgrade...
ncs/admin#
```

Related Commands

Command	Description
application install	Installs an application bundle.

Command	Description
application remove	Removes or uninstalls an application.
application start	Starts or enables an application.
application stop	Stops or disables an application.
show application	Shows application information for the installed application packages on the system.

backup

To perform a backup (including the Prime Infrastructure and Cisco ADE OS data) and place the backup in a repository, use the **backup** command in EXEC mode. To perform a backup of only the Prime Infrastructure application data without the Cisco ADE OS data, use the **application** command.

backup *backup-name***repository** *repository-name***application***application-name*

Syntax Description	*backup-name*	Name of the backup file. Up to 100 alphanumeric characters.
	repository-name	Name of the location where the files should be backed up to. Up to 80 alphanumeric characters.
	application-name	Application name. Up to 255 alphanumeric characters.
		Note Enter the application name as 'PI' in uppercase.

Command Default   No default behavior or values.

Command Modes   EXEC

Usage Guidelines   Performs a backup of the Prime Infrastructure and Cisco ADE OS data and places the backup in a repository.

To perform a backup of only the Prime Infrastructure application data without the Cisco ADE OS data, use the **application** command.

Examples

```
ncs/admin# backup mybackup repository myrepository
% Creating backup with timestamped filename: mybackup-100805-1222.tar.gpg
ncs/admin#

ncs/admin# backup mybackup repository myrepository application NCS
% Creating backup with timestamped filename: mybackup-100805-1240.tar.gpg
ncs/admin#
```

Related Commands

Command	Description
backup-logs	Backs up the system logs.
delete	Deletes a file from the Prime Infrastructure server.
dir	Lists a file from the Prime Infrastructure server.
reload	Reboots the system.

Command	Description
repository	Enters the repository submode for configuration of backups.
restore	Restores from backup the file contents of a specific repository.
show backup history	Displays the backup history of the system.
show repository	Displays the available backup files located on a specific repository.

backup-logs

To back up system logs, use the **backup-logs** command in EXEC mode. To remove this function, use the **no** form of this command.

backup-logs *backup-name* **repository***repository-name*

Syntax Description

backup-name	Name of one or more files to back up. Up to 100 alphanumeric characters.
repository-name	Location where files should be backed up to. Up to 80 alphanumeric characters.

Command Default No default behavior or values.

Command Modes EXEC

Usage Guidelines Backs up system logs.

Examples

```
ncs/admin# backup-logs mybackup repository myrepository
% Creating log backup with timestamped filename: mybackup-100805-1754.tar.gz
ncs/admin#
```

Related Commands

Command	Description
backup	Performs a backup (Prime Infrastructure and Cisco ADE OS) and places the backup in a repository.
restore	Restores from backup the file contents of a specific repository.
repository	Enters the repository submode for configuration of backups.
show backup history	Shows the backup history of the system.
show repository	Shows the available backup files located on a specific repository.

clock

To set the system clock, use the **clock** command in EXEC mode. To remove this function, use the **no** form of this command.

clock set *[month day hh:min:ss yyyy]*

Syntax Description

month	Current month of the year by name. Up to three alphabetic characters. For example, Jan for January.
day	Current day (by date) of the month. Value = 0 to 31. Up to two numbers.
hh:mm:ss	Current time in hours (24-hour format), minutes, and seconds.
yyyy	Current year (no abbreviation).

Command Default   No default behavior or values.

Command Modes   EXEC

Usage Guidelines   Sets the system clock. You must restart the Prime Infrastructure server after you reset the clock for the change to take effect.

Examples
```
ncs/admin# clock set May 5 18:07:20 2010
ncs/admin# show clock
Thu May 5 18:07:26 UTC 2010
ncs/admin#
```

Related Commands

Command	Description
show clock	Displays the time and date set on the system software clock.

configure

To enter configuration mode, use the **configure** command in EXEC mode. If the **replace** option is used with this command, copies a remote configuration to the system which overwrites the existing configuration.

configure terminal

Syntax Description

terminal	Executes configuration commands from the terminal.

Command Default   No default behavior or values.

Command Modes   EXEC

Usage Guidelines   Use this command to enter configuration mode. Note that commands in this mode write to the running configuration file as soon as you enter them (press **Enter**).

To exit configuration mode and return to EXEC mode, enter **end**, **exit**, or press**Ctrl-z**.

To view the changes that you have made to the configuration, use the **show running-config** command in EXEC mode.

Examples

```
ncs/admin# configure
Enter configuration commands, one per line.  End with CNTL/Z.
ncs/admin(config)#

ncs/admin# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ncs/admin(config)#
```

Related Commands

Command	Description
show running-config	Displays the contents of the currently running configuration file or the configuration.
show startup-config	Displays the contents of the startup configuration file or the configuration.

copy

To copy any file from a source to a destination, use the **copy** command in EXEC mode.

Syntax Description

running-config	Represents the current running configuration file.
startup-config	Represents the configuration file used during initialization (startup).
protocol	See Table 13: Protocol Prefix Keywords for protocol keyword options.
hostname	Hostname of destination.
location	Location of disk:/<dirpath>.
logs	The system log files.
all	Copies all Prime Infrastructure log files from the system to another location. All logs are packaged as ncslogs.tar.gz and transferred to the specified directory on the remote host.
filename	Allows you to copy a single Prime Infrastructure log file and transfer it to the specified directory on the remote host, with its original name.
log_filename	Name of the Prime Infrastructure log file, as displayed by the **show logs** command (up to 255 characters).
mgmt	Copies the Prime Infrastructure management debug logs and Tomcat logs from the system, bundles them as mgmtlogs.tar.gz, and transfers them to the specified directory on the remote host.
runtime	Copies the Prime Infrastructure runtime debug logs from the system, bundles them as runtimelogs.tar.gz, and transfers them to the specified directory on the remote host.

Command Default No default behavior or values.

Command Modes EXEC

The fundamental function of the **copy** command allows you to copy a file (such as a system image or configuration file) from one location to another location. The source and destination for the file specified uses the file system, through which you can specify any supported local or remote file location. The file system being used (a local memory source or a remote system) dictates the syntax used in the command.

You can enter on the command line all of the necessary source and destination information and the username and password to use; or, you can enter the **copy** command and have the server prompt you for any missing

information. You can enter up to a maximum of 2048 characters of source and destination URL information on the command line.

The **copy** command in the copies a configuration (running or startup).

The active configuration stores itself in the RAM. Every configuration command you enter resides in the running configuration. If you reboot your server, you lose the running configuration. If you make changes that you want to save, you must copy the running configuration to a safe location, such as a network server, or save it as the server startup configuration.

You cannot edit a startup configuration directly. All commands that you enter store themselves in the running configuration, which you can copy into the startup configuration.

In other words, when you boot a server, the startup configuration becomes the initial running configuration. As you modify the configuration, the two diverge: the startup configuration remains the same; the running configuration reflects the changes that you have made. If you want to make your changes permanent, you must save the running configuration to the startup configuration using the **write memory** command. The **write memory** command makes the current running configuration permanent.

> **Note** If you do not save the running configuration, you will lose all your configuration changes during the next reboot of the server. You can also save a copy of the running and startup configurations using the following commands, to recover in case of loss of configuration:
>
> **copy startup-config** *location*
>
> **copy running-config** *location*

> **Note** The **copy** command is supported only for the local disk and not for a repository.

> **Tip** Aliases reduce the amount of typing that you need to do. For example, type **copy run start** (the abbreviated form of the **copy running-config startup-config** command).

The entire copying process might take several minutes and differs from protocol to protocol and from network to network.

Use the filename relative to the directory for file transfers.

Possible error is the standard FTP error message.

Table 13: Protocol Prefix Keywords

Keyword	Destination
ftp	URL for FTP network server. The syntax for this alias: **ftp:**//*location*/*directory*

Keyword	Destination
sftp	URL for an SFTP network server. The syntax for this alias: **sftp:**//*location*/*directory*
tftp	URL for a TFTP network server. The syntax for this alias: **tftp:**//*location*/*directory*

Examples

```
ncs/admin# copy run start
Generating configuration...
ncs/admin#

ncs/admin# copy running-config startup-config
Generating configuration...
ncs/admin#

ncs/admin# copy start run
ncs/admin#

ncs/admin# copy startup-config running-config
ncs/admin#

ncs/admin# copy logs disk:/
 Collecting logs...
ncs/admin#
```
This command is used to copy the certificate file from pnp to ftp.

```
ncs/admin# copy  server.key  /localdisk/tftp
copy  server.crt  /localdisk/tftp
copy  ncs_server_certificate  /localdisk/tftp
```

Examples

This command is used to copy the certificate from ftp tp pnp.

```
copy tftp://<PI Server IP Address>/server.key disk:/
copy tftp://<PI Server IP Address>/server.crt disk:/
 copy tftp://<PI Server IP Address>/ncs_server_certificate.crt disk:/
```

Related Commands

Command	Description
application install	Starts or stops a instance.
backup	Performs a backup (and Cisco ADE OS) and places the backup in a repository.
delete	Deletes a file from the server.
dir	Lists a file from the server.
reload	Reboots the system.
restore	Restores from backup the file contents of a specific repository.

Command	Description
show application	Shows application status and version information.
show version	Displays information about the software version of the system.

debug

To display errors or events for command situations, use the **debug** command in EXEC mode.

debug{all | application | backup-restore | cdp | config | icmp | copy | locks | logging | snmp | system | transfer | user | utils}

Syntax Description

all	Enables all debugging.
application	Application files.
	• *all*—Enables all application debug output. Set level between 0 and 7, with 0 being severe and 7 being all.
	• *install*—Enables application install debug output. Set level between 0 and 7, with 0 being severe and 7 being all.
	• *operation*—Enables application operation debug output. Set level between 0 and 7, with 0 being severe and 7 being all.
	• *uninstall*—Enables application uninstall debug output. Set level between 0 and 7, with 0 being severe and 7 being all.
backup-restore	Backs up and restores files.
	• *all*—Enables all debug output for backup-restore. Set level between 0 and 7, with 0 being severe and 7 being all.
	• *backup*—Enables backup debug output for backup-restore. Set level between 0 and 7, with 0 being severe and 7 being all.
	• *backup-logs*—Enables backup-logs debug output for backup-restore. Set level between 0 and 7, with 0 being severe and 7 being all.
	• *history*—Enables history debug output for backup-restore. Set level between 0 and 7, with 0 being severe and 7 being all.
	• *restore*—Enables restore debug output for backup-restore. Set level between 0 and 7, with 0 being severe and 7 being all.
cdp	Cisco Discovery Protocol configuration files.
	• *all*—Enables all Cisco Discovery Protocol configuration debug output. Set level between 0 and 7, with 0 being severe and 7 being all.
	• *config*—Enables configuration debug output for Cisco Discovery Protocol. Set level between 0 and 7, with 0 being severe and 7 being all.
	• *infra*—Enables infrastructure debug output for Cisco Discovery Protocol. Set level between 0 and 7, with 0 being severe and 7 being all.

config	Configuration files.
	• *all*—Enables all configuration debug output. Set level between 0 and 7, with 0 being severe and 7 being all.
	• *backup*—Enables backup configuration debug output. Set level between 0 and 7, with 0 being severe and 7 being all.
	• *clock*—Enables clock configuration debug output. Set level between 0 and 7, with 0 being severe and 7 being all.
	• *infra*—Enables configuration infrastructure debug output. Set level between 0 and 7, with 0 being severe and 7 being all.
	• *kron*—Enables command scheduler configuration debug output. Set level between 0 and 7, with 0 being severe and 7 being all.
	• *network*—Enables network configuration debug output. Set level between 0 and 7, with 0 being severe and 7 being all.
	• *repository*—Enables repository configuration debug output. Set level between 0 and 7, with 0 being severe and 7 being all.
	• *service*—Enables service configuration debug output. Set level between 0 and 7, with 0 being severe and 7 being all.
icmp	Internet Control Message Protocol (ICMP) echo response configuration.
	all—Enable all debug output for ICMP echo response configuration. Set level between 0 and 7, with 0 being severe and 7 being all.
copy	Copy commands. Set level between 0 and 7, with 0 being severe and 7 being all.
locks	Resource locking.
	• *all*—Enables all resource locking debug output. Set level between 0 and 7, with 0 being severe and 7 being all.
	• *file*—Enables file locking debug output. Set level between 0 and 7, with 0 being severe and 7 being all.
logging	Logging configuration files.
	all—Enables all logging configuration debug output. Set level between 0 and 7, with 0 being severe and 7 being all.
snmp	SNMP configuration files.
	all—Enables all SNMP configuration debug output. Set level between 0 and 7, with 0 being severe and 7 being all.

system	System files.
	• *all*—Enables all system files debug output. Set level between 0 and 7, with 0 being severe and 7 being all.
	• *id*—Enables system ID debug output. Set level between 0 and 7, with 0 being severe and 7 being all.
	• *info*—Enables system info debug output. Set level between 0 and 7, with 0 being severe and 7 being all.
	• *init*—Enables system init debug output. Set level between 0 and 7, with 0 being severe and 7 being all.
transfer	File transfer. Set level between 0 and 7, with 0 being severe and 7 being all.
user	User management.
	• *all*—Enables all user management debug output. Set level between 0 and 7, with 0 being severe and 7 being all.
	• *password-policy*—Enables user management debug output for password-policy. Set level between 0 and 7, with 0 being severe and 7 being all.
utils	Utilities configuration files.
	all—Enables all utilities configuration debug output. Set level between 0 and 7, with 0 being severe and 7 being all.

Command Default   No default behavior or values.

Command Modes   EXEC

Usage Guidelines   Use the **debug** command to identify various failures within the Prime Infrastructure server; for example, setup failures or configuration failures.

Examples

```
ncs/admin# debug all
ncs/admin# mkdir disk:/1
ncs/admin# 6 [15347]: utils: vsh_root_stubs.c[2742] [admin]: mkdir operation success

ncs/admin# rmdir disk:/1
6 [15351]: utils: vsh_root_stubs.c[2601] [admin]: Invoked Remove Directory disk:/1 command
6 [15351]: utils: vsh_root_stubs.c[2663] [admin]: Remove Directory operation success
ncs/admin#

ncs/admin# undebug all
ncs/admin#
```

Related Commands

Command	Description
undebug	Disables the output (display of errors or events) of the **debug** command for various command situations.

delete

To delete a file from the Prime Infrastructure server, use the **delete** command in EXEC mode. To remove this function, use the **no** form of this command.

delete *filename [disk:/path]*

Syntax Description

filename	Filename. Up to 80 alphanumeric characters.
disk:/path	Location.

Command Default   No default behavior or values.

Command Modes   EXEC

Usage Guidelines   If you attempt to delete the configuration file or image, the system prompts you to confirm the deletion. Also, if you attempt to delete the last valid system image, the system prompts you to confirm the deletion.

Examples

```
ncs/admin# delete disk:/hs_err_pid19962.log
ncs/admin#
```

Related Commands

Command	Description
dir	Lists all of the files on the Prime Infrastructure server.

dir

To list a file from the Prime Infrastructure server, use the **dir** command in EXEC mode. To remove this function, use the **no** form of this command.

dir *[word]***[recursive]**

Syntax Description

word	Directory name. Up to 80 alphanumeric characters. Requires **disk:/** preceding the directory name.
recursive	Lists a local directory or filename recursively.

Command Default   No default behavior or values.

Command Modes   EXEC

Examples

```
ncs/admin# dir

Directory of disk:/

    2034113 Aug 05 2010 19:58:39  ADElogs.tar.gz
       4096 Jun 10 2010 02:34:03  activemq-data/
       4096 Aug 04 2010 23:14:53  logs/
      16384 Jun 09 2010 02:59:34  lost+found/
    2996022 Aug 05 2010 19:11:16  mybackup-100805-1910.tar.gz
       4096 Aug 04 2010 23:15:20  target/
       4096 Aug 05 2010 12:25:55  temp/

         Usage for disk: filesystem
             8076189696 bytes total used
             6371618816 bytes free
            15234142208 bytes available
ncs/admin#

ncs/admin# dir disk:/logs

0 Aug 05 2010 11:53:52  usermgmt.log

         Usage for disk: filesystem
             8076189696 bytes total used
             6371618816 bytes free
            15234142208 bytes available
ncs/admin#

ncs/admin# dir recursive

Directory of disk:/

    2034113 Aug 05 2010 19:58:39  ADElogs.tar.gz
    2996022 Aug 05 2010 19:11:16  mybackup-100805-1910.tar.gz
       4096 Aug 04 2010 23:14:53  logs/
       4096 Aug 05 2010 12:25:55  temp/
       4096 Jun 10 2010 02:34:03  activemq-data/
       4096 Aug 04 2010 23:15:20  target/
      16384 Jun 09 2010 02:59:34  lost+found/
```

```
Directory of disk:/logs

          0  Aug 05 2010 11:53:52  usermgmt.log

Directory of disk:/temp

        281  Aug 05 2010 19:12:45  RoleBundles.xml
       6631  Aug 05 2010 19:12:34  PipDetails.xml
         69  Aug 05 2010 19:12:45  GroupRoles.xml
        231  Aug 05 2010 19:12:34  ApplicationGroupTypes.xml
     544145  Aug 05 2010 19:12:35  ResourceTypes.xml
      45231  Aug 05 2010 19:12:45  UserTypes.xml
        715  Aug 05 2010 19:12:34  ApplicationGroups.xml
        261  Aug 05 2010 19:12:34  ApplicationTypes.xml
       1010  Aug 05 2010 19:12:34  Pdps.xml
    1043657  Aug 05 2010 19:12:44  Groups.xml
     281003  Aug 05 2010 19:12:38  Resources.xml
         69  Aug 05 2010 19:12:45  GroupUsers.xml
       2662  Aug 05 2010 19:12:44  RoleTypes.xml
         79  Aug 05 2010 19:12:34  UserStores.xml
       4032  Aug 05 2010 19:12:38  GroupTypes.xml
       1043  Aug 05 2010 19:12:34  Organization.xml
      58377  Aug 05 2010 19:12:46  UserRoles.xml
        300  Aug 05 2010 19:12:45  Contexts.xml
        958  Aug 05 2010 19:12:34  Applications.xml
      28010  Aug 05 2010 19:12:45  Roles.xml
     122761  Aug 05 2010 19:12:45  Users.xml

Directory of disk:/activemq-data

       4096  Jun 10 2010 02:34:03  localhost/

Directory of disk:/activemq-data/localhost

          0  Jun 10 2010 02:34:03  lock
       4096  Jun 10 2010 02:34:03  journal/
       4096  Jun 10 2010 02:34:03  kr-store/
       4096  Jun 10 2010 02:34:03  tmp_storage/

Directory of disk:/activemq-data/localhost/journal

   33030144  Aug 06 2010 03:40:26  data-1
       2088  Aug 06 2010 03:40:26  data-control

Directory of disk:/activemq-data/localhost/kr-store

       4096  Aug 06 2010 03:40:27  data/
       4096  Aug 06 2010 03:40:26  state/

Directory of disk:/activemq-data/localhost/kr-store/data

        102  Aug 06 2010 03:40:27  index-container-roots
          0  Aug 06 2010 03:40:27  lock

Directory of disk:/activemq-data/localhost/kr-store/state

       3073  Aug 06 2010 03:40:26  hash-index-store-state_state
         51  Jul 20 2010 21:33:33  index-transactions-state
        204  Aug 06 2010 03:40:26  index-store-state
        306  Jun 10 2010 02:34:03  index-kaha
        290  Jun 10 2010 02:34:03  data-kaha-1
      71673  Aug 06 2010 03:40:26  data-store-state-1
          0  Jun 10 2010 02:34:03  lock

Directory of disk:/activemq-data/localhost/tmp_storage

No files in directory

Directory of disk:/target

       4096  Aug 04 2010 23:15:20  logs/
```

```
Directory of disk:/target/logs

        0 Aug 04 2010 23:15:20  ProfilerPDP.log
     2208 Aug 05 2010 11:54:26  ProfilerSensor.log

Directory of disk:/lost+found

No files in directory

        Usage for disk: filesystem
            8076189696 bytes total used
            6371618816 bytes free
           15234142208 bytes available

ncs/admin#
```

Related Commands

Command	Description
delete	Deletes a file from the Prime Infrastructure server.

exit

To close an active terminal session by logging out of the Prime Infrastructure server or to move up one mode level from configuration mode, use the **exit** command in EXEC mode.

exit

Syntax Description This command has no arguments or keywords.

Command Default No default behavior or values.

Command Modes EXEC

Usage Guidelines Use the **exit** command in EXEC mode to exit an active session (log out of the Prime Infrastructure server) or to move up from configuration mode.

Examples

```
ncs/admin# exit
```

Related Commands

Command	Description
end	Exits configuration mode.
exit	Exits configuration mode or EXEC mode.
Ctrl-z	Exits configuration mode.

forceout

To force users out of an active terminal session by logging them out of the Prime Infrastructure server, use the **forceout** command in EXEC mode.

forceout *username*

Syntax Description

username	The name of the user. Up to 31 alphanumeric characters.

Command Default No default behavior or values.

Command Modes EXEC

Examples

```
ncs/admin# forceout user1
ncs/admin#
```

halt

To shut down and power off the system, use the **halt** command in EXEC mode.

halt

This command has no arguments or keywords.

Command Default   No default behavior or values.

Command Modes   EXEC

Usage Guidelines   Before you enter the **halt** command, ensure that the Prime Infrastructure is not performing any backup, restore, installation, upgrade, or remove operation. If you enter the **halt** command while the Prime Infrastructure is performing any of these operations, you will get one of the following warning messages:

```
WARNING: A backup or restore is currently in progress! Continue with halt?
```

```
WARNING: An install/upgrade/remove is currently in progress! Continue with halt?
```
If you get any of these warnings, enter **YEs** to halt the operation, or enter **NO** to cancel the halt.

If no processes are running when you use the **halt** command or if you enter **Yes** in response to the warning message displayed, the Prime Infrastructure asks you to respond to the following option:

```
Do you want to save the current configuration ?
```
Enter YES to save the existing Prime Infrastructure configuration. The Prime Infrastructure displays the following message:

```
Saved the running configuration to startup successfully
```

Examples
```
ncs/admin# halt
ncs/admin#
```

Related Commands

Command	Description
reload	Reboots the system.

mkdir

To create a new directory on the Prime Infrastructure server, use the **mkdir** command in EXEC mode.

mkdir *directory-name [disk:/path]*

Syntax Description

directory-name	The name of the directory to create. Up to 80 alphanumeric characters.
disk:/path	Use *disk:/path* with the directory name.

Command Default   No default behavior or values.

Command Modes   EXEC

Usage Guidelines   Use *disk***:/***path* with the directory name; otherwise, an error appears that indicates that the *disk***:/***path* must be included.

Examples

```
ncs/admin# mkdir disk:/test
ncs/admin# dir

Directory of disk:/

      4096 May 06 2010 13:34:49  activemq-data/
      4096 May 06 2010 13:40:59  logs/
     16384 Mar 01 2010 16:07:27  lost+found/
      4096 May 06 2010 13:42:53  target/
      4096 May 07 2010 12:26:04  test/

          Usage for disk: filesystem
                181067776 bytes total used
              19084521472 bytes free
              20314165248 bytes available
ncs/admin#
```

Related Commands

Command	Description
dir	Displays a list of files on the Prime Infrastructure server.
rmdir	Removes an existing directory.

ncs start

To start the Prime Infrastructure server, use the **ncs start** command.

ncs start [verbose]

Syntax Description

verbose	Displays the detailed messages during the start process.

Command Default   No default behavior or values.

Command Modes   EXEC

Usage Guidelines   To see the messages in the console, use the **ncs start verbose** command.

Examples   This example shows how to start the server:

```
> ncs start verbose
Starting Network Control System...

Starting Health Monitor
Starting Health Monitor as a primary
Checking for Port 8082 availability... OK
Starting Health Montior Web Server...
Health Monitor Web Server Started.
Starting Health Monitor Server...
Health Monitor Server Started.
Starting Service Name: Reporting
Starting dependency service: NMS Server
Starting dependency service: Matlab
Starting remoting: Matlab Server
Checking for Port 20555 availability... OK
Remoting Service Matlab Server application root: /opt/CSCOncs
Starting Remoting Service Web Server Matlab Server...
Remoting Service Web Server Matlab Server Started.
Starting Remoting Service Matlab Server...
Remoting 'Matlab Server' started successfully.
Starting dependency service: Ftp
Starting remoting: Ftp Server
Checking for Port 20558 availability... OK
Starting up FTP server
Started FTP
FTP Server started
Remoting Service Ftp Server application root: /opt/CSCOncs
Starting Remoting Service Web Server Ftp Server...
Remoting Service Web Server Ftp Server Started.
Starting Remoting Service Ftp Server...
Remoting 'Ftp Server' started successfully.
Starting dependency service: Tftp
Starting remoting: Tftp Server
Checking for Port 20559 availability... OK
Starting up TFTP server...
TFTP Server started.
Remoting Service Tftp Server application root: /opt/CSCOncs
Starting Remoting Service Web Server Tftp Server...
```

```
Remoting Service Web Server Tftp Server Started.
Starting Remoting Service Tftp Server...
Remoting 'Tftp Server' started successfully.
Starting NMS Server
Checking for running servers.
  Checking if DECAP is running.
  00:00 DECAP is not running.
00:00 Check complete. No servers running.
  00:10 DECAP setup complete.
Starting Server ...
Reporting started successfully

Starting Service Name: Ftp
Ftp is already running.

Starting Service Name: Database
00:40 Server started.
00:40 DONE
Done
Database is already running.

Starting Service Name: Tftp
Tftp is already running.

Starting Service Name: Matlab
Matlab is already running.

Starting Service Name: NMS Server
NMS Server is already running.

Network Control System started successfully.
```

Related Commands

Command	Description
ncs stop	Stops the Prime Infrastructure server.
ncs status	Displays the current status of the Prime Infrastructure server.

ncs stop

To stop the Prime Infrastructure server, use the **ncs stop** command in EXEC mode. To see the detailed messages, use the **ncs stop verbose** command.

ncs stop [verbose]

Syntax Description

verbose	Displays the detailed messages during the stop process.

Command Default   No default behavior or values.

Command Modes   EXEC

Usage Guidelines   To see the detailed messages, use the **ncs stop verbose** command.

Examples   This example shows how to stop the Prime Infrastructure server:

```
> ncs stop verbose
Stopping Network Control System...
Stopping Network Control System server
Stopping Service Name: Reporting
Stopping Reporting
Reporting successfully shutdown.
Stopping Service Name: Ftp
Stopping NMS Server
Stopping Reporting Server(XMP) ..DONE
NMS Server successfully shutdown.

Stopping remoting: Ftp Server
Stopping FTP server...
Stopped FTP server.
Stopping Remoting Web Server Ftp Server...
Remoting Web Server Ftp Server stopped.
Remoting 'Ftp Server' stopped successfully.
Stopping Service Name: Database
Shutting down database server ...
Stopping XMP ....DONE

Stopping Service Name: Tftp
Stopping remoting: Tftp Server
Stopping TFTP server...
Stopped TFTP server.
Stopping Remoting Web Server Tftp Server...
Remoting Web Server Tftp Server stopped.
Remoting 'Tftp Server' stopped successfully.
Stopping Service Name: Matlab
Stopping remoting: Matlab Server
Stopping Remoting Web Server Matlab Server...
Remoting Web Server Matlab Server stopped.
Warning: latest version of matlab app-defaults file not found.
Contact your system administrator to have this file installed.
Remoting 'Matlab Server' stopped successfully.
```

```
Stopping Service Name: NMS Server
NMS Server is not running.
Stopping Tomcat...
Tomcat Stopped.

Network Control System successfully shutdown.
```

Related Commands

Command	Description
ncs start	Starts the Prime Infrastructure server.
ncs status	Displays the current status of he Prime Infrastructure server.

ncs status

To display the server status, use the **ncs status** command in EXEC mode.

ncs status

This command has no arguments or keywords.

Command Default No default behavior or values.

Command Modes EXEC

Examples This example shows how to display the status of the server:

```
> ncs status
Health Monitor Server is running.
Reporting is running.
Ftp Server is Success
Database server is running
Tftp Server is Success
Matlab Server is Success
NMS Server is running.
```

Related Commands

Command	Description
ncs start	Starts the server.
ncs stop	Stops the server.

ncs password ftpuser password

To change the FTP username and password, use the **ncs password ftpuser password** command in EXEC mode.

ncs passwod ftpuser *username* **password** *password*

Syntax Description

username	The FTP user name
password	The modified password. The password cannot contain 'cisco' or 'ocsic', or any variant obtained by changing the capitalization of letters therein or by substituting '1', '|', or '!' for i, '0' for 'o', or '$' for 's'.

Command Default

No default behavior or values.

Command Modes

EXEC

Examples

This example shows how to change the FTP username and password:

```
> ncs password ftpuser
```

Related Commands

Command	Description
ncs start	Starts Prime Infrastructure sever.
ncs stop	Stops Prime Infrastructure server.
ncs status	Displays the current status of Prime Infrastructure server.
ncs password root password	Changes the root password.

ncs password root password

To change the root password, use the **ncs password root password** command in EXEC mode.

ncs passwod root password *password*

Syntax Description

password	The modified password. The password cannot contain 'cisco' or 'ocsic', or any variant obtained by changing the capitalization of letters therein or by substituting '1', '|', or '!' for i, '0' for 'o', or '$' for 's'.

Command Default   No default behavior or values.

Command Modes   EXEC

Examples   Prime Infrastructure
This example shows how to migrate archived files to server:

```
> ncs password root password Private123
Loading USER - root
Validating new password..
Resetting password ..
Resetting password  COMPLETED.
EXECUTION STATUS : Success
```

Related Commands

Command	Description
ncs start	Start the Prime Infrastructure sever.
ncs stop	Stops the Prime Infrastructure server.
ncs status	Displays the current status of the Prime Infrastructure server.
ncs password ftpuser password	Changes the FTP username and password.

ncs ha authkey

To enter the authentication key for high availability (HA), use the **ncs ha authkey** command in EXEC mode.

ncs ha authkey *authorization key*

Syntax Description

authorization key	The authorization key for high availability. Up to 255 alphanumeric characters.

Command Default　　No default behavior or values.

Command Modes　　EXEC

Usage Guidelines　　The **ncs ha authkey** command changes the authorization for the health monitor.

Examples　　This example shows how to set up the authorization key for high availability:

```
ncs ha authkey cisco123
```

Related Commands

Command	Description
ncs ha remove	Removes the high availability configuration settings from Prime Infrastructure.
ncs ha status	Provides the current status of high availability.

ncs ha remove

To remove the high availability configuration settings from Prime Infrastructure, use the **ncs ha remove** command in EXEC mode.

ncs ha remove

Syntax Description   This command has no arguments or keywords.

Command Default   No default behavior or values.

Command Modes   EXEC

Usage Guidelines   The **ncs ha remove** command removes the high availability configuration settings from Prime Infrastructure. If you enter this command, you will see the following confirmation message:

```
High availability configuration will be removed.
Do you wish to continue? (Y/N)
```

Related Commands

Command	Description
ncs ha authkey	Allows you to enter the authentication key for high availability in Prime Infrastructure. This command also changes the authorization for the health monitor.
ncs ha status	Provides the current status of high availability.

ncs ha status

To display the current status of high availability (HA), use the **ncs ha status** command in EXEC mode.

ncs ha status

Syntax Description   This command has no arguments or keywords.

Command Default   No default behavior or values.

Command Modes   EXEC

Usage Guidelines   Displays the current status of HA.

If you enter the **ncs ha status** command when HA is not configured, you will see the following response:

```
[State] Stand Alone
```

Related Commands

Command	Description
ncs ha authkey	Allows you to enter the authentication key for high availability in Prime Infrastructure. This command also changes the authorization for the health monitor.
ncs ha remove	Removes the high availability configuration.

ncs key genkey

To generate a new RSA key and self-signed certificate, use the **ncs key genkey** command. You can use this command in the following ways:

ncs key genkey

ncs key genkey -newdn

ncs key genkey -csr *csrfilename*

ncs key genkey -csr *csrfilename* **repository** *repositoryname*

Syntax Description

genkey	Generates a new RSA key and self-signed certificate. You can use the following options with this command:
	-csr: Generate Certificate Signing Request(CSR) file
	-newdn: Generate new RSA key and self-signed certificate with domain information
	<cr>: Carriage return.
-newdn	Generates a new RSA key and self-signed cert with domain information. You can use the following options with this command:
	-csr: Generate Certificate Signing Request(CSR) file
	<cr>: Carriage return.
-csr	Generates new CSR certificate file. You can use the following option with this command:
	<WORD>: Type in certificate file name (Max Size - 80)
csrfilename	CSR filename.
repository	Repository command. This option is available when you use the -csr option.
repositoryname	Location where the files should be backed up to. Up to 80 alphanumeric characters.

Command Default   No default behavior or values.

Command Modes   EXEC

Examples   This example shows how to generate new rsa key and certificate files in the Prime Infrastructure server:

```
>ncs key genkey -newdn -csr csrfile.cert repository ncs-sftp-repo
Generating RSA key
INFO: no staging url defined, using local space.          rval:2
```

Related Commands

Command	Description
ncs key importcacert	Applies a CA certificate to the trust store in Prime Infrastructure.
ncs key listcacerts	Lists all of the CA certificates that exist in the Prime Infrastructure trust store.
ncs key deletecacert	Deletes a CA certificates that exist in the Prime Infrastructure trust store.
ncs key importsignedcert	Applies an RSA key and signed certificate to Prime Infrastructure.
ncs key importkey	Applies an RSA key and certificate to Prime Infrastructure.

Note   After entering this command, enter the **ncs stop** and **ncs start** command to restart the Prime Infrastructure server to make changes take effect.

ncs key importcacert

To apply a CA certificate to a trust store in Prime Infrastructure, use the **ncs key importcacert** command in the EXEC mode.

ncs key importcacert *aliasname ca-cert-filename* **repository** *repositoryname*

Syntax Description

aliasname	A short name given for this CA certificate.
ca-cert-filename	CA certificate file name.
repository	Repository command.
repositoryname	The repository name configured in Prime Infrastructure where the ca-cert-filename is hosted.

Command Default No default behavior or values.

Command Modes EXEC

Examples This example shows how to apply the CA certificate file to a trust store in the Prime Infrastructure server:

```
> ncs key importcacert alias1 cacertfile repository ncs-sftp-repo
```

Note After applying this command, enter the **ncs stop** and **ncs start** command to restart the Prime Infrastructure server to make the changes take effect.

Related Commands

Command	Description
ncs key genkey	Generates a new RSA key and self-signed certificate.
ncs key listcacerts	Lists all of the CA certificates that exist in the Prime Infrastructure trust store.
ncs key deletecacert	Deletes a CA certificates that exist in the Prime Infrastructure trust store.
ncs key importsignedcert	Applies an RSA key and signed certificate to Prime Infrastructure.
ncs key importkey	Applies an RSA key and certificate to Prime Infrastructure.

ncs key importkey

To apply an RSA key and signed certificate to the Prime Infrastructure, use the **ncs key importkey** command in EXEC mode.

ncs key importkey *key-filename cert-filename* **repository** *repositoryname*

Syntax Description

key-filename	RSA private key file name.
cert-filename	Certificate file name.
repository	Repository command
repositoryname	The repository name configured in the Prime Infrastructure where the key-file and cert-file is hosted.

Command Default   No default behavior or values.

Command Modes   EXEC

Examples   This example shows how to apply the new RSA key and certificate files to the server.

```
> ncs key importkey keyfile certfile repository ncs-sftp-repo
```

Note   After applying this command, enter the **ncs stop** and **ncs start** command to restart the server to make the changes take effect.

Related Commands

Command	Description
ncs key genkey	Generates a new RSA key and self-signed certificate.
ncs key listcacerts	Lists all of the CA certificates that exist in the Prime Infratsructure trust store.
ncs key deletecacert	Deletes a CA certificates that exist in the Prime Infratsructure trust store.
ncs key importsignedcert	Applies an RSA key and signed certificate to Prime Infratsructure.
ncs key importcacert	Applies an CA certificate to trust store in the Prime Infratsructure.

ncs key listcacerts

To list all of the CA certificates that exist in the Prime Infrastructure trust store, use the **ncs key listcacerts** command EXEC mode.

ncs key listcacerts

Syntax Description   This command has no arguments or keywords.

Command Default   No default behavior or values.

Command Modes   EXEC

Examples   This example shows how to list all of the CA certificates that exist in the Prime Infrastructure trust store:

```
>  ncs key listcacerts

Certificate utnuserfirsthardwareca from CN=UTN-USERFirst-Hardware, OU=http://www.example.com,
 O=The USERTRUST Network, L=Salt Lake City, ST=UT, C=US
Certificate gtecybertrust5ca from CN=GTE CyberTrust Root 5, OU="GTE CyberTrust Solutions,
Inc.", O=GTE Corporation, C=US
Certificate equifaxsecureebusinessca1 from CN=Equifax Secure eBusiness CA-1, O=Equifax
Secure Inc., C=US
Certificate thawtepersonalfreemailca from EMAILADDRESS=email@example.com, CN=Thawte Personal
 Freemail CA, OU=Certification Services Division, O=Thawte Consulting, L=Cape Town, ST=Western
 Cape, C=ZA
Certificate addtrustclass1ca from CN=AddTrust Class 1 CA Root, OU=AddTrust TTP Network,
O=AddTrust AB, C=SE
Certificate aolrootca1 from CN=America Online Root Certification Authority 1, O=America
Online Inc., C=US
Certificate geotrustuniversalca from CN=GeoTrust Universal CA, O=GeoTrust Inc., C=US
Certificate digicertglobalrootca from CN=DigiCert Global Root CA, OU=www.example.com,
O=DigiCert Inc, C=US
Certificate certumtrustednetworkca from CN=Certum Trusted Network CA, OU=Certum Certification
 Authority, O=Unizeto Technologies S.A., C=PL
Certificate swisssignsilverg2ca from CN=SwissSign Silver CA - G2, O=SwissSign AG, C=CH
```

Related Commands

Command	Description
ncs key genkey	Generates a new RSA key and self-signed certificate.
ncs key importkey	Applies an RSA key and signed certificate to the Prime Infrastructure.
ncs key deletecacert	Deletes CA certificates that exist in the Prime Infrastructure trust store.
ncs key importsignedcert	Applies an RSA key and signed certificate to the Prime Infrastructure.
ncs key importcacert	Applies a CA certificate to the trust store in Prime Infrastructure.

ncs key deletecacert

To delete CA certificates that exist in Prime Infrastructure trust store, use the **ncs key deletecacert** command in the EXEC mode.

ncs key deletecacert *aliasname*

Syntax Description

aliasname	The short or alias name of the CA certificate which needs to be deleted from the Prime Infrastructure trust store.

Command Default   No default behavior or values.

Command Modes   EXEC

Examples   This example shows how to delete CA certificates that exist in the Prime Infrastructure trust store:

```
>  ncs key deletecacert certumtrustednetworkca
 Deleting certificate from trust store
```

Related Commands

Command	Description
ncs key genkey	Generates a new RSA key and self-signed certificate.
ncs key importkey	Applies an RSA key and signed certificate to Prime Infrastructure.
ncs key listcacerts	Lists all of the CA certificates that exist in the Prime Infrastructure trust store.
ncs key importsignedcert	Applies an RSA key and signed certificate to Prime Infrastructure.
ncs key importcacert	Applies a CA certificate to the trust store in Prime Infrastructure.

ncs key importsignedcert

To apply an RSA key and signed certificate, use the **ncs key importsignedcert** command EXEC mode.

ncs key importsignedcert *signed-cert-filename* **repository** *repositoryname*

Syntax Description

signed-cert-filename	Signed certificate filename.
repository	Repository command
repositoryname	The repository name configured in Prime Infrastructure where the key-file and cert-file is hosted.

Command Default   No default behavior or values.

Command Modes   EXEC

Examples   This example shows how to apply signed certificate files to the Prime Infrastructure server:

```
> ncs key importsingedcert signed-certfile repository ncs-sftp-repo
```

Note   After applying this command, enter the **ncs stop** and the **ncs start** command to restart the Prime Infrastructure server to make changes take effect.

Related Commands

Command	Description
ncs key genkey	Generates a new RSA key and self-signed certificate.
ncs key importkey	Applies an RSA key and signed certificate to Prime Infrastructure.
ncs key deletecacert	Deletes CA certificates that exist in the Prime Infrastructure trust store.
ncs key listcacerts	Lists all of the CA certificates that exist in the Prime Infrastructure trust store.
ncs key importcacert	Applies a CA certificate to the trust store in Prime Infrastructure.

ncs cleanup

To free up and reclaim the disk space, use the **ncs cleanup** command in EXEC mode.

ncs cleanup

Syntax Description   This command has no arguments or keywords.

Command Default   No default behavior or values.

Command Modes   EXEC

Usage Guidelines   When Prime Infrastructure does not have enough disk space, an alarm is raised to free up and reclaim the disk space. If you enter the **ncs cleanup** command, you will see the following confirmation message:
```
Do you want to delete all the files in the local disk partition? (Y/N)
```

ncs db sql

To run the SQL query from the Prime Infrastructure terminal, use the **ncs db sql** command in EXEC mode.

ncs db sql *query_string*

Syntax Description

query_string	Enter the sql query string enclosed in double quotes.

Command Default No default behavior or values.

Command Modes EXEC

Usage Guidelines The Prime Infrastructure database server should be in running state to successfully execute this command.

Examples This example shows how to run a DB sql query on the Prime Infrastructure server:

```
ncs/admin# ncs db sql "select count(*) from clientcount"
          COUNT(*)
-------------------
                75
ncs/admin#
```

ncs db reinitdb

To reinitialize the Prime Infratsructure database, use the **ncs db reinitdb** command in EXEC mode. This command removes all data present in the database.

ncs db reinitdb

Syntax Description   This command has no arguments or keywords.

Command Default   No default behavior or values.

Command Modes   EXEC

Usage Guidelines   You can use this command if the Prime Infrastructure database becomes unstable or unusable, or if you want to remove the old data and start with a clean database.

Examples   This example shows how to run a DB sql query on the Prime Infrastructure server:

```
admin# ncs db reinitdb
-All data will be lost. Do you wish to continue? (y/n)
y
-Creating a new, empty database. This may take 10 to 20 minutes
-Database re-initialization completed
admin#
```

nslookup

To look up the hostname of a remote system on the Prime Infrastructure server, use the **nslookup** command in EXEC mode.

nslookup *word*

Syntax Description

word	IPv4 address or hostname of a remote system. Up to 64 alphanumeric characters.

Command Default   No default behavior or values.

Command Modes   EXEC

Examples
```
ncs/admin# nslookup 209.165.200.225
Trying "209.165.200.225.in-addr.arpa"
Received 127 bytes from 172.16.168.183#53 in 1 ms
Trying "209.165.200.225.in-addr.arpa"
Host 209.165.200.225.in-addr.arpa. not found: 3(NXDOMAIN)
Received 127 bytes from 172.16.168.183#53 in 1 ms

ncs/admin#

ncs/admin# nslookup 209.165.200.225
Trying "225.200.165.209.in-addr.arpa"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 65283
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 0

;; QUESTION SECTION:
;225.200.165.209.in-addr.arpa.   IN      PTR

;; ANSWER SECTION:
225.200.165.209.in-addr.arpa. 86400 IN  PTR     209-165-200-225.got.net.

;; AUTHORITY SECTION:
192.168.209.in-addr.arpa. 86400 IN      NS      ns1.got.net.
192.168.209.in-addr.arpa. 86400 IN      NS      ns2.got.net.

Received 119 bytes from 172.16.168.183#53 in 28 ms

ncs/admin#
```

patch install

To install a patch bundle of the application, use the **patch** command in EXEC mode.

patch install *patch-bundle repository*

Syntax Description

patch-bundle	The patch bundle file name. Up to 255 alphanumeric characters.
repository	Repository name. Up to 255 alphanumeric characters.

Command Default   No default behavior or values.

Command Modes   EXEC

Usage Guidelines   The **patch install** command installs a patch bundle of the application only on a specific node where you run the **patch install** command from the CLI.

If you attempt to install a patch that is an older version of the existing patch, then you receive the following error message:

```
% Patch to be installed is an older version than currently installed version.
```

✎
Note   In a Prime Infrastructure distributed deployment environment, install the patch bundle of the application from the primary Policy Administration Point (PAP) node in the Prime Infrastructure Administration user interface so that the patch bundle automatically gets installed on all of the secondary nodes.

Examples

```
ncs/admin# patch install ncs-appbundle-1.0.2.054-3.i386.tar.gz myrepository
Do you want to save the current configuration ? (yes/no) [yes] ? yes
Generating configuration...
Saved the running configuration to startup successfully
Initiating Application Patch installation...

Patch successfully installed
ncs/admin#

ncs/admin# patch install ncs-appbundle-1.0.2.054-3.i386.tar.gz myrepository
Do you want to save the current configuration ? (yes/no) [yes] ? no
Initiating Application Patch installation...

Patch successfully installed
ncs/admin#

ncs/admin# patch install ncs-appbundle-1.0.2.054-2.i386.tar.gz disk
Do you want to save the current configuration ? (yes/no) [yes] ? yes
Generating configuration...
Saved the running configuration to startup successfully
Initiating Application Patch installation...
```

```
% Patch to be installed is an older version than currently installed version.
ncs/admin#
```

Related Commands

	Description
patch remove	Removes a specific patch bundle version of the application.
show version	Displays information about the currently loaded software version, along with hardware and device information.

patch remove

To remove a specific patch bundle version of the application, use the **patch remove** command in EXEC mode.

patch remove *word word*

Syntax Description

word	The name of the application for which the patch is to be removed. Up to 255 alphanumeric characters.
word	The patch version number to be removed. Up to 255 alphanumeric characters.

Command Default   No default behavior or values.

Command Modes   EXEC

Usage Guidelines   Removes a specific patch bundle of the application.

If you attempt to remove a patch that is not installed, then you receive the following error message:

Note   In a Prime Infrastructure distributed deployment environment, remove the patch bundle of the application from the primary Policy Administration Point (PAP) node in the Prime Infrastructure Administration user interface so that the patch bundle automatically gets uninstalled from all of the secondary nodes.

```
% Patch is not installed
```

Examples

```
ncs/admin# patch remove ncs 3
Continue with application patch uninstall? [y/n] y

Application patch successfully uninstalled
ncs/admin#

ncs/admin# patch remove ncs 3
Continue with application patch uninstall? [y/n] y

% Patch is not installed
ncs/admin#
```

Related Commands

Command	Description
patch install	Installs a specific patch bundle of the application.
show version	Displays information about the currently loaded software version, along with hardware and device information.

ping

To diagnose the basic IPv4 network connectivity to a remote system, use the **ping** command in EXEC mode.

ping *{ip-address | hostname} [***Df***df][***packetsize***packetsize][***pingcount***pingcount]*

Syntax Description

ip-address	IP address of the system to ping. Up to 32 alphanumeric characters.
hostname	Hostname of the system to ping. Up to 32 alphanumeric characters.
df	Specification for packet fragmentation.
df	Specifies the value as **1** to prohibit packet fragmentation, or **2** to fragment the packets locally, or **3** to not set df.
packetsize	Size of the ping packet.
packetsize	Specifies the size of the ping packet; the value can be between 0 and 65507.
pingcount	Number of ping echo requests.
pingcount	Specifies the number of ping echo requests; the value can be between 1 and 10.

Command Default

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

The **ping** command sends an echo request packet to an address, then awaits a reply. The ping output can help you evaluate path-to-host reliability, delays over the path, and whether you can reach a host.

Examples

```
ncs/admin# ping 172.16.0.1 df 2 packetsize 10 pingcount 2
PING 172.16.0.1 (172.16.0.1) 10(38) bytes of data.
18 bytes from 172.16.0.1: icmp_seq=0 ttl=40 time=306 ms
18 bytes from 172.16.0.1: icmp_seq=1 ttl=40 time=300 ms

--- 172.16.0.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 300.302/303.557/306.812/3.255 ms, pipe 2
ncs/admin#
```

Related Commands

Command	Description
ping6	Pings a remote IPv6 address.

ping6

To diagnose the basic IPv6 network connectivity to a remote system, use the **ping6** command in EXEC mode.

ping6 *{ip-address | hostname}* *[***GigabitEthernetpacketsize***packetsize]*[**pingcount***pingcount]*

Syntax Description	

ip-address	IP address of the system to ping. Up to 64 alphanumeric characters.
hostname	Hostname of the system to ping. Up to 64 alphanumeric characters.
GigabitEthernet	Selects the ethernet interface.
packetsize	Size of the ping packet.
packetsize	Specifies the size of the ping packet; the value can be between 0 and 65507.
pingcount	Number of ping echo requests.
pingcount	Specifies the number of ping echo requests; the value can be between 1 and 10.

Command Default   No default behavior or values.

Command Modes   EXEC

Usage Guidelines   The IPv6 **ping6** command sends an echo request packet to an address, then awaits a reply. The ping output can help you evaluate path-to-host reliability, delays over the path, and whether you can reach a host.

The IPv6 **ping6** command is similar to the existing IPv4 ping command that does not support the IPv4 ping fragmentation (df in IPv4) options, but allows an optional specification of an interface. The interface option is primarily useful for pinning with link-local addresses that are interface-specific. The packetsize and pingcount options work identically the same as they do with the IPv4 command.

Examples

```
ncs/admin# ping6 3ffe:302:11:2:20c:29ff:feaf:da05
PING 3ffe:302:11:2:20c:29ff:feaf:da05(3ffe:302:11:2:20c:29ff:feaf:da05) from
3ffe:302:11:2:20c:29ff:feaf:da05 eth0: 56 data bytes
64 bytes from 3ffe:302:11:2:20c:29ff:feaf:da05: icmp_seq=0 ttl=64 time=0.599 ms
64 bytes from 3ffe:302:11:2:20c:29ff:feaf:da05: icmp_seq=1 ttl=64 time=0.150 ms
64 bytes from 3ffe:302:11:2:20c:29ff:feaf:da05: icmp_seq=2 ttl=64 time=0.070 ms
64 bytes from 3ffe:302:11:2:20c:29ff:feaf:da05: icmp_seq=3 ttl=64 time=0.065 ms

--- 3ffe:302:11:2:20c:29ff:feaf:da05 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3118ms
rtt min/avg/max/mdev = 0.065/0.221/0.599/0.220 ms, pipe 2

ncs/admin#

ncs/admin# ping6 3ffe:302:11:2:20c:29ff:feaf:da05 GigabitEthernet 0 packetsize 10 pingcount
 2
```

```
PING 3ffe:302:11:2:20c:29ff:feaf:da05(3ffe:302:11:2:20c:29ff:feaf:da05) from
3ffe:302:11:2:20c:29ff:feaf:da05 eth0: 10 data bytes
18 bytes from 3ffe:302:11:2:20c:29ff:feaf:da05: icmp_seq=0 ttl=64 time=0.073 ms
18 bytes from 3ffe:302:11:2:20c:29ff:feaf:da05: icmp_seq=1 ttl=64 time=0.073 ms

--- 3ffe:302:11:2:20c:29ff:feaf:da05 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1040ms
rtt min/avg/max/mdev = 0.073/0.073/0.073/0.000 ms, pipe 2

ncs/admin#
```

Related Commands

	Description
ping	Pings a remote IP address.

reload

To reload the Prime Infrastructure operating system, use the **reload** command in EXEC mode.

reload

Syntax Description   This command has no arguments or keywords.

Command Default   The command has no default behavior or values.

Command Modes   EXEC

Usage Guidelines   The **reload** command reboots the system. Use the **reload** command after you enter configuration information into a file and save the running-configuration to the persistent startup-configuration on the CLI and save any settings in the web Administration user interface session.

Before you enter the **reload** command, ensure that the Prime Infrastructure is not performing any backup, restore, installation, upgrade, or remove operation. If the Prime Infrastructure performs any of these operations and you enter the **reload** command, you will notice any of the following warning messages:

```
WARNING: A backup or restore is currently in progress! Continue with reload?
```

```
WARNING: An install/upgrade/remove is currently in progress! Continue with reload?
```
If you get any of these warnings, enter YES to halt the operation, or enter NO to cancel the halt.

If no processes are running when you use the **reload** command or you enter YES in response to the warning message displayed, the Prime Infrastructure asks you to respond to the following option:

```
Do you want to save the current configuration ?
```
Enter YES to save the existing Prime Infrastructure configuration. The Prime Infrastructure displays the following message:

```
Saved the running configuration to startup successfully
```

Examples
```
ncs/admin# reload
Do you want to save the current configuration ? (yes/no) [yes] ? yes
Generating configuration...
Saved the running configuration to startup successfully
Continue with reboot? [y/n] y

Broadcast message from root (pts/0) (Fri Aug  7 13:26:46 2010):

The system is going down for reboot NOW!

ncs/admin#
```

Related Commands

Command	Description
halt	Disables the system.

restore

To perform a restore of a previous backup, use the **restore** command in EXEC mode.

Use the following command to restore data related to the Prime Infrastructure application and Cisco ADE OS:

restore filename **repository** repository-name

Use the following command to restore data related only to the Prime Infrastructure application:

restore *filename***repository***repository-name***application***application*

Syntax Description	*filename*	Name of the backed-up file that resides in the repository. Up to 120 alphanumeric characters.
		Note You must add the .tar.gpg extension after the filename (for example, myfile.tar.gpg).
	repository	The repository keyword.
	repository-name	Name of the repository you want to restore from backup.
	application	The application keyword.
	application name	The name of the application data to be restored. Up to 255 alphanumeric characters.
		Note Enter the application name as 'PI' in upper case.

Command Default   No default behavior or values.

Command Modes   EXEC

Usage Guidelines   A restore operation restores data related to the Prime Infrastructure as well as the Cisco ADE OS. To perform a restore of a previous backup of the application data of the Prime Infrastructure only, add the **application** command to the **restore** command in EXEC mode. To remove this function, use the **no** form of this command.

When you use these two commands in the Prime Infrastructure, the Prime Infrastructure server restarts automatically.

Examples

```
ncs/admin# restore mybackup-100818-1502.tar.gpg repository myrepository
Restore may require a reboot to successfully complete. Continue? (yes/no) [yes] ? yes
Stopping NCS Monitoring & Troubleshooting Log Processor...
Stopping NCS Monitoring & Troubleshooting Log Collector...
Stopping NCS Monitoring & Troubleshooting Alert Process...
Stopping NCS Monitoring & Troubleshooting Session Database...
Stopping NCS Application Server...
Stopping NCS Database processes...
```

```
Starting NCS Database processes...
Starting NCS Application Server...
Starting NCS Monitoring & Troubleshooting Session Database...
Starting NCS Monitoring & Troubleshooting Log Collector...
Starting NCS Monitoring & Troubleshooting Log Processor...
Starting NCS Monitoring & Troubleshooting Alert Process...
Note: NCS Processes are initializing. Use 'show application status NCS'
      CLI to verify all processes are in running state.

Broadcast message from root (pts/0) (Wed Aug 18 15:34:58 2010):

The system is going down for reboot NOW!
ncs/admin# Last login: Wed Aug 18 14:00:27 2010 from 10.77.137.60
ncs/admin# show application status NCS

NCS Database listener is running, PID: 3024
NCS Database is running, number of processes: 34
NCS Application Server is still initializing.
NCS M&T Session Database is running, PID: 2793
NCS M&T Log Collector is running, PID: 3336
NCS M&T Log Processor is running, PID: 3379
NCS M&T Alert Process is running, PID: 3442

ncs/admin#
```

Related Commands

Command	Description
backup	Performs a backup (Prime Infrastructure and Cisco ADE OS) and places the backup in a repository.
backup-logs	Backs up system logs.
repository	Enters the repository submode for configuration of backups.
show repository	Displays the available backup files located on a specific repository.
show backup history	Displays the backup history of the system.

rmdir

To remove an existing directory, use the **rmdir** command in EXEC mode.

rmdir *word*

Syntax Description

word	Directory name. Up to 80 alphanumeric characters.

Command Default

No default behavior or values.

Command Modes

EXEC

Examples

```
ncs/admin# mkdir disk:/test
ncs/admin# dir

Directory of disk:/

        4096 May 06 2010 13:34:49  activemq-data/
        4096 May 06 2010 13:40:59  logs/
       16384 Mar 01 2010 16:07:27  lost+found/
        4096 May 06 2010 13:42:53  target/
        4096 May 07 2010 12:26:04  test/

        Usage for disk: filesystem
              181067776 bytes total used
            19084521472 bytes free
            20314165248 bytes available
ncs/admin#

ncs/admin# rmdir disk:/test
ncs/admin# dir

Directory of disk:/

        4096 May 06 2010 13:34:49  activemq-data/
        4096 May 06 2010 13:40:59  logs/
       16384 Mar 01 2010 16:07:27  lost+found/
        4096 May 06 2010 13:42:53  target/

        Usage for disk: filesystem
              181063680 bytes total used
            19084525568 bytes free
            20314165248 bytes available
ncs/admin#
```

Related Commands

Command	Description
dir	Displays a list of files on the Prime Infrastructure server.
mkdir	Creates a new directory.

root

This command has no arguments or keywords.

To execute the root shell, use the **root** command in EXEC mode.

> ✎
> **Note**   For developer use only, not for end users.

root

Syntax Description   This command has no arguments or keywords.

Command Default   No default behavior or values.

Command Modes   EXEC

Usage Guidelines   Requires installation of the root_enable application or patch. The **root** command prompts for the password used with root_enable and puts you in a bash shell with root privileges.

There are no defaults for the password.

If the password is already set, the **root_enable** command generates the following error message:

```
% Error : root patch password already set
```
If the password is not set, the **root** command generates the following error message:

```
% Error : root patch password not set.
```

> ✎
> **Note**   This command and the **root_enable** command can only be used on the Prime Infrastructure locally hard-wired console port via Telnet. If you try to access this port over a LAN via SSH or Telnet, the commands are disallowed and the following message appears: % Error : root patch only available on a console port.

Examples   The following example illustrates the use of the **root** command:

```
ncs/admin# root
% Error : root patch password not set
```

Related Commands

Command	Description
root_enable	Activates the **root** command.

root_disable

To disable the **root** user restoring admin shell access, use the **root_disable** command in the EXEC mode.

> **Note** For developer use only, not for end users.

root_disable

Syntax Description This command has no arguments or keywords.

Command Default No default behavior or values.

Command Modes EXEC

Usage Guidelines

> **Note** This command and the **root_enable** command can only be used on the Prime Infrastructure locally hard-wired console port via Telnet. If you try to access this port over a LAN via SSH or Telnet, the commands are disallowed and the following message appears:
> ```
> % Error : root patch only available on a console port.
> ```

Examples The following example illustrates the use of the **root_disable** command:

```
ncs/admin# root_disable
```

Related Commands

Command	Description
root_enable	Executes the root shell.

root_enable

To activate the **root** command, use the **root_enable** command in the EXEC mode.

Note For developer use only, not for end users.

root_enable

Syntax Description This command has no arguments or keywords.

Command Default No default behavior or values.

Command Modes EXEC

Usage Guidelines Requires installation of the root_enable application or patch. The **root** command prompts for the password used with root_enable and puts you in a bash shell with root privileges.

There are no defaults for the password.

If the password is already set, the **root_enable** command generates the following error message:

```
% Error : root patch password already set
```
If the password is not set, the **root** command generates the following error message:

```
% Error : root patch password not set
```

Note This command and the **root** command can only be used on the Prime Infrastructure locally hard-wired console port via Telnet. If you try to access this port over a LAN via SSH or Telnet, the commands are disallowed and the following message appears:
```
% Error : root patch only available on a console port.
```

Examples The following example illustrates the use of the **root_enable** command:

```
ncs/admin# root_enable
% Error : root patch password already set
```

Related Commands

Command	Description
root	Executes the root shell.

show

To show the running system information, use the **show** command in EXEC mode. The **show** commands are used to display the Prime Infrastructure settings and are among the most useful commands.

The commands in Table A-6 require the **show** command to be followed by a keyword; for example, **show application status**. Some **show** commands require an argument or variable after the keyword to function; for example, **show application version**.

For detailed information on all of the Prime Infrastructure **show** commands, see show Commands.

show keyword

Syntax Description

Table 14: Summary of show Commands

Command(1)	Description
application (requires keyword)(2)	Displays information about the installed application; for example, status or version.
backup (requires keyword)	Displays information about the backup.
cdp (requires keyword)	Displays information about the enabled Cisco Discovery Protocol interfaces.
clock	Displays the day, date, time, time zone, and year of the system clock.
cpu	Displays CPU information.
disks	Displays file-system information of the disks.
interface	Displays statistics for all of the interfaces configured on the Cisco ADE OS.
logging (requires keyword)	Displays system logging information.
logins (requires keyword)	Displays login history.
memory	Displays memory usage by all running processes.
ntp	Displays the status of the Network Time Protocol (NTP).
ports	Displays all of the processes listening on the active ports.
process	Displays information about the active processes of the Prime Infrastructure server.

Command(1)	Description
repository (requires keyword)	Displays the file contents of a specific repository.
restore (requires keyword)	Displays restore history on the Prime Infrastructure server.
running-config	Displays the contents of the currently running configuration file on the Prime Infrastructure server.
startup-config	Displays the contents of the startup configuration on the Prime Infrastructure server.
tech-support	Displays system and configuration information that you can provide to the TAC when you report a problem.
terminal	Displays information about the terminal configuration parameter settings for the current terminal line.
timezone	Displays the time zone of the Prime Infrastructure server.
timezones	Displays all of the time zones available for use on the Prime Infrastructure server.
udi	Displays information about the unique device identifier (UDI) of the Prime Infrastructure.
uptime	Displays how long the system you are logged in to has been up and running.
users	Displays information for currently logged in users.
version	Displays information about the installed application version.

12

[1] (1) The commands in this table require that the show command precedes a keyword; for example, show application.

[2] (2) Some show commands require an argument or variable after the keyword to function; for example, show application version. This show command displays the version of the application installed on the system (see show application).

Command Default No default behavior or values.

Command Modes EXEC

Usage Guidelines All **show** commands require at least one keyword to function.

Examples

```
ncs/admin# show application
```

```
<name>          <Description>
ncs     Cisco Network Control System
ncs/admin#
```

ssh

To start an encrypted session with a remote system, use the **ssh** command in EXEC mode.

Note   An Admin or Operator (user) can use this command (see Table 3: Command Privileges).

ssh *[ip-address | hostname] username***port***[number]***version[1|2] delete hostkey***word*

Syntax Description

ip-address	IP address of the remote system. Up to 64 alphanumeric characters.
hostname	Hostname of the remote system. Up to 64 alphanumeric characters.
username	Username of the user logging in through SSH.
port [*number*]	(Optional) Indicates the port number of the remote host. From 0 to 65,535. Default 22.
version [1 | 2]	(Optional) Indicates the version number. Default 2.
delete hostkey	Deletes the SSH fingerprint of a specific host.
word	IPv4 address or hostname of a remote system. Up to 64 alphanumeric characters.

Command Default   Disabled.

Command Modes   EXEC (Admin or Operator).

Usage Guidelines   The **ssh** command enables a system to make a secure, encrypted connection to another remote system or server. This connection provides functionality similar to that of an outbound Telnet connection except that the connection is encrypted. With authentication and encryption, the SSH client allows for secure communication over an insecure network.

Examples

```
ncs/admin# ssh ncs1 admin
admin@ncs1's password:
Last login: Wed Jul 11 05:53:20 2008 from ncs.cisco.com

ncs1/admin#

ncs/admin# ssh delete host ncs
ncs/admin#
```

tech dumptcp

To dump a Transmission Control Protocol (TCP) package to the console, use the **tech dumptcp** command in EXEC mode.

tech dumptcp *gigabit-ethernet*

Syntax Description

gigabit-ethernet	Gigabit Ethernet interface number 0 to 1.

Command Default   Disabled.

Command Modes   EXEC

Examples

```
ncs/admin# tech dumptcp 0
140816:141088(272) ack 1921 win 14144
08:26:12.034630 IP NCS.cisco.com.ssh > dhcp-64-102-82-153.cisco.com.2221: P 141088:141248(160)
 ack 1921 win 14144
08:26:12.034635 IP dhcp-64-102-82-153.cisco.com.2221 > NCS.cisco.com.ssh: . ack 139632 win
 64656
08:26:12.034677 IP NCS.cisco.com.ssh > dhcp-64-102-82-153.cisco.com.2221: P 141248:141520(272)
 ack 1921 win 14144
08:26:12.034713 IP NCS.cisco.com.ssh > dhcp-64-102-82-153.cisco.com.2221: P 141520:141680(160)
 ack 1921 win 14144
08:26:12.034754 IP NCS.cisco.com.ssh > dhcp-64-102-82-153.cisco.com.2221: P 141680:141952(272)
 ack 1921 win 14144
08:26:12.034756 IP dhcp-64-102-82-153.cisco.com.2221 > NCS.cisco.com.ssh: . ack 140064 win
 65520
08:26:12.034796 IP NCS.cisco.com.ssh > dhcp-64-102-82-153.cisco.com.2221: P 141952:142112(160)
 ack 1921 win 14144
1000 packets captured
1000 packets received by filter
0 packets dropped by kernel
ncs/admin#
```

telnet

To log in to a host that supports Telnet, use the **telnet** command in operator (user) or EXEC mode.

telnet *[ip-address | hostname] port number*

Syntax Description

ip-address	IP address of the remote system. Up to 64 alphanumeric characters.
hostname	Hostname of the remote system. Up to 64 alphanumeric characters.
port number	(Optional) Indicates the port number of the remote host. From 0 to 65,535.

Command Default   No default behavior or values.

Command Modes   EXEC

Examples

```
ncs/admin# telnet 172.16.0.11 port 23
ncs.cisco.com login: admin
password:
Last login: Mon Jul  2 08:45:24 on ttyS0
ncs/admin#
```

terminal length

To set the number of lines on the current terminal screen for the current session, use the **terminal length** command in EXEC mode.

terminal length *integer*

Syntax Description

integer	Number of lines on the screen. Contains between 0 to 511 lines, inclusive. A value of zero (0) disables pausing between screens of output.

Command Default   24 lines.

Command Modes   EXEC

Usage Guidelines   The system uses the length value to determine when to pause during multiple-screen output.

Examples

```
ncs/admin# terminal length 0
ncs/admin#
```

terminal session-timeout

To set the inactivity timeout for all sessions, use the **terminal session-timeout** command in EXEC mode.

terminal session-timeout *minutes*

Syntax Description

minutes	Sets the number of minutes for the inactivity timeout. From 0 to 525,600. Zero (0) disables the timeout.

Command Default

30 minutes.

Command Modes

EXEC

Usage Guidelines

Setting the **terminal session-timeout** command to zero (0) results in no timeout being set.

Examples

```
ncs/admin# terminal session-timeout 40
ncs/admin#
```

Related Commands

Command	Description
terminal session-welcome	Sets a welcome message on the system for all users who log in to the system.

terminal session-welcome

To set a welcome message on the system for all users who log in to the system, use the **terminal session-welcome** command in EXEC mode.

terminal session-welcome *string*

Syntax Description

string	Welcome message. Up to 2,048 alphanumeric characters.

Command Default   No default behavior or values.

Command Modes   EXEC

Usage Guidelines   Specify a message using up to 2048 characters.

Examples

```
ncs/admin# terminal session-welcome Welcome
ncs/admin#
```

Related Commands

Command	Description
terminal session-timeout	Sets the inactivity timeout for all sessions.

terminal terminal-type

To specify the type of terminal connected to the current line for the current session, use the **terminal terminal-type** command in EXEC mode.

terminal terminal-type *type*

Syntax Description

type	Defines the terminal name and type, and permits terminal negotiation by hosts that provide that type of service. Up to 80 alphanumeric characters.

Command Default   VT100.

Command Modes   EXEC

Usage Guidelines   Indicate the terminal type if it is different from the default of VT100.

Examples

```
ncs/admin# terminal terminal-type vt220
ncs/admin#
```

traceroute

To discover the routes that packets take when traveling to their destination address, use the **traceroute** command in EXEC mode.

traceroute *[ip-address | hostname]*

Syntax Description

ip-address	IP address of the remote system. Up to 32 alphanumeric characters.
hostname	Hostname of the remote system. Up to 32 alphanumeric characters.

Command Default   No default behavior or values.

Command Modes   EXEC

Examples

```
ncs/admin# traceroute 172.16.0.11
traceroute to 172.16.0.11 (172.16.0.11), 30 hops max, 38 byte packets
 1  172.16.0.11 0.067 ms  0.036 ms  0.032 ms

ncs/admin#
```

undebug

To disable debugging functions, use the **undebug** command in EXEC mode.

undebug *{all | application | backup-restore | cdp | config | copy | icmp | locks | logging | snmp | system | transfer | user | utils}*

Syntax Description

all	Disables all debugging.
application	Application files. • *all*—Disables all application debug output. • *install*—Disables application install debug output. • *operation*—Disables application operation debug output. • *uninstall*—Disables application uninstall debug output.
backup-restore	Backs up and restores files. • *all*—Disables all debug output for backup-restore. • *backup*—Disables backup debug output for backup-restore. • *backup-logs*—Disables backup-logs debug output for backup-restore. • *history*—Disables history debug output for backup-restore. • *restore*—Disables restore debug output for backup-restore.
cdp	Cisco Discovery Protocol configuration files. • *all*—Disables all Cisco Discovery Protocol configuration debug output. • *config*—Disables configuration debug output for Cisco Discovery Protocol. • *infra*—Disables infrastructure debug output for Cisco Discovery Protocol.

config	Configuration files.
	• *all*—Disables all configuration debug output.
	• *backup*—Disables backup configuration debug output.
	• *clock*—Disables clock configuration debug output.
	• *infra*—Disables configuration infrastructure debug output.
	• *kron*—Disables command scheduler configuration debug output.
	• *network*—Disables network configuration debug output.
	• *repository*—Disables repository configuration debug output.
	• *service*—Disables service configuration debug output.
copy	Copy commands.
icmp	ICMP echo response configuration.
	all—Disable all debug output for ICMP echo response configuration. Set level between 0 and 7, with 0 being severe and 7 being all.
locks	Resource locking.
	• *all*—Disables all resource locking debug output.
	• *file*—Disables file locking debug output.
logging	Logging configuration files.
	all—Disables all debug output for logging configuration.
snmp	SNMP configuration files.
	all—Disables all debug output for SNMP configuration.
system	System files.
	• *all*—Disables all system files debug output.
	• *id*—Disables system ID debug output.
	• *info*—Disables system info debug output.
	• *init*—Disables system init debug output.
transfer	File transfer.
user	User management.
	• *all*—Disables all user management debug output.
	• *password-policy*—Disables user management debug output for password-policy.

| *utils* | Utilities configuration files. |
| | *all*—Disables all utilities configuration debug output. |

Command Default   No default behavior or values.

Command Modes   EXEC

Examples

```
ncs/admin# undebug all
ncs/admin#
```

Related Commands

Command	Description
debug	Displays errors or events for command situations.

write

To copy, display, or erase Prime Infrastructure server configurations, use the **write** command with the appropriate argument in EXEC mode.

write *{erase | memory | terminal}*

Syntax Description

erase	Erases the startup configuration.
memory	Copies the running configuration to the startup configuration.
terminal	Copies the running configuration to console.

Command Default

No default behavior or values.

Command Modes

EXEC

Examples

The following is an example of the write command with the memory keyword:

```
ncs/admin# write memory
Generating configuration...
ncs/admin#
```
The following is an example of the write command with the terminal keyword:

```
ncs/admin# write terminal

Generating configuration...
!
hostname ncs
!
ip domain-name cisco.com
!
interface GigabitEthernet 0
  ip address 10.201.2.121 255.255.255.0
  ipv6 address autoconfig
!
interface GigabitEthernet 1
  shutdown
!
interface GigabitEthernet 2
  shutdown
!
interface GigabitEthernet 3
  shutdown
!
ip name-server 172.16.226.120
!
ip default-gateway 10.201.2.1
!
clock timezone UTC
!
ntp server clock.cisco.com
!
```

```
username admin password hash $1$6yQQaFXM$UBgbp7ggD1bG3kpExywwZ0 role admin
!
service sshd
!
repository myrepository
  url disk:
  user admin password hash 2b50ca94445f240f491e077b5f49fa0375942f38
!
password-policy
  lower-case-required
  upper-case-required
  digit-required
  no-username
  disable-cisco-passwords
  min-password-length 6
!
logging localhost
logging loglevel 6
!
cdp timer 60
cdp holdtime 180
cdp run GigabitEthernet 0
!
icmp echo on
!

ncs/admin#
```

Cisco Plug and Play Gateway Commands

This section lists the **pnp** commands along with a brief description of their use, command defaults, command modes, command syntax, usage guidelines, command examples, and related commands, where applicable.

Prime Infrastructure Integrated Server Commands

This section lists the **ncs pnp gateway commands** along with a brief description of its use, command defaults, command modes, command syntax, usage guidelines, command examples, and related commands, where applicable.

ncs pnp-gateway

To enable or disable the local Cisco Plug and Play Gateway on the Prime Infrastructure Integrated Server and modify or view the properties of the software image on the Cisco Plug and Play Gateway, use the **ncs pnp-gateway** command in privileged EXEC mode.

ncs pnp-gateway {**enable** | **disable** | **modify** | **property**}

Syntax Description

enable	Enables the Cisco Plug and Play Gateway.
disable	Disables the Cisco Plug and Play Gateway.
modify	Enables the modification of the Cisco Plug and Play Gateway image's properties. The properties that can be modified are: activation timeout value, distribution timeout value, and transfer timeout value.
property	Enables viewing of the properties pertaining to the software image on the Cisco Plug and Play Gateway.

Command Modes   Privileged EXEC

Command History

Release	Modification
Cisco Prime Infrastructure 2.0	This command was introduced.

Examples   The following is sample output from the **ncs pnp-gateway** command:

```
admin# ncs  pnp-gateway?

  disable   PNP Gateway Disable Command
  enable    PNP Gateway Enable command
  modify    Modify PnP Gateway properties and variables
  property  Show PnP properties and configuration
```

Examples   The following is sample output from the **ncs pnp-gateway disable** command:

ncs pnp-gateway disable

```
Disabling Plug and Play Gateway.....
Plug and Play Gateway is successfully disabled. Please restart Prime Infrastructure on this
 server
```

Examples   The following is a sample output of the **ncs pnp-gateway enable** command:

ncs pnp-gateway enable

```
Enabling Plug and Play Gateway.....
```

```
        Plug and Play Gateway is successfully enabled. Please restart Prime Infrastructure on this
         server.
```

Examples   The following is a sample output of the **ncs pnp-gateway modify** command:

ncs pnp-gateway modify

```
bgl-dt-ncs-vm6-70/ayyanna# ncs pnp-gateway modify image ?
  activation-timeout    Activation timeout for PnP image upgrade job
  distribution-timeout  Distribution timeout for PnP image upgrade job
  transfer-timeout      Transfer timeout for PnP image upgrade job
bgl-dt-ncs-vm6-70/ayyanna# ncs pnp-gateway modify image
  activation-timeout ? <60-1048576> Type the image activation timeout value (seconds)
```

Examples   The following is a sample output of the **ncs pnp-gateway property image** command:

```
admin# ncs pnp-gateway property image

PnP Gateway Image Transfer Timeout = 2400
PnP Gateway Image Distribution Timeout = 2200
PnP Gateway Image Activation Timeout = 1600
```

Prime Infrastructure PnP Gateway Standalone Server Command

This section lists the **pnp gateway standalone server commands** along with a brief description of their use, command defaults, command modes, command syntax, usage guidelines, command examples, and related commands, where applicable.

pnp backup

To create a backup of the Cisco Plug and Play Gateway configuration, use the **pnp backup** command in privileged EXEC mode.

pnp backup

Command Modes   Privileged EXEC

Command History

Release	Modification
Cisco Prime Infrastructure 1.2	This command was introduced.
Cisco Prime Infrastructure 2.0	This command was modified.

Usage Guidelines   The backup file is usually created in a compressed tar file format in the *disk:/ directory* that corresponds to the */localdisk/ directory* on the Linux file system.

Examples   The following is sample output from the **pnp backup** command:

```
admin# pnp backup

The backup file created : /localdisk/20130130220403.pnp_backup.tar.gz
```

The following table describes the significant field shown in the display.

Table 15: pnp backup Field Description

Field	Description
20130130220403.pnp_backup.tar.gz	The backup file created in the above example, where *2013* is the year, *01* is the month, *30* is the date, *22* is the hour, *04* is the minute, and *03* is the second at which the backup file was created.

pnp modify image

To modify the properties of the Cisco Plug and Play Gateway software image in the Prime Infrastructure Plug and Play Standalone Gateway, use the **pnp modify image** command in privileged EXEC mode.

pnp modify image {**activation-timeout** | **distribution-timeout** | **transfer-timeout** | **transfer-timeout**}**timeout-value**

Syntax Description

activation timeout value	Activation timeout value, in seconds, for the Cisco Plug and Play Gateway software image upgrade job. The range is from 60 to 1048576. The default is 600.
distribution timeout value	Distribution timeout value, in seconds, for the Cisco Plug and Play Gateway software image upgrade job. The valid range is from 60 to 1048576. The default is 1200.
transfer timeout value	Transfer timeout value, in seconds, for the Cisco Plug and Play Gateway software image upgrade job. The valid range is from 60 to 1048576. The default is 1200.

Command Modes   Privileged EXEC

Command History

Release	Modification
Cisco Prime Infrastructure 1.2	This command was introduced.
Cisco Prime Infrastructure 2.0	This command was modified.

Usage Guidelines   The Cisco Plug and Play Gateway does not have to be restarted for the timeout value to take effect. The timeout value that you specify will take effect for the next software image.

Examples   The following is sample output from the **pnp modify image** command:

```
admin# pnp modify image ?

  activation-timeout    Activation timeout for PnP image upgrade job
  distribution-timeout  Distribution timeout for PnP image upgrade job
  transfer-timeout      Transfer timeout for PnP image upgrade job

admin# pnp modify image activation-timeout 1200
Done

admin# pnp modify image distribution-timeout 2400
Done
```

```
admin# pnp modify image transfer-timeout 2200
Done
```

pnp modify log-level

To modify the log-level settings of the Cisco Plug and Play Gateway, use the **pnp modify log-level** command in privileged EXEC mode.

The Cisco Plug and Play Gateway supports these log levels: **debug, error, fatal, info, trace, and warn**.

pnp modify log-level {**fatal** | **error** | **warn** | **info** | **debug** | **trace**}

Syntax Description

fatal	Enables the collection of fatal-level log messages.
error	Enables the collection of fatal-level and error-level log messages.
warn	Enables the collection of fatal-level, error-level, and warn-level log messages.
info	Enables the collection of fatal-level, error-level, warn-level, and information-level log messages.
debug	Enables the collection of fatal-level, error-level, warn-level, information-level, and debug-level log messages.
trace	Enables the collection of fatal-level, error-level, warn-level, information-level, debug-level, and trace-level log messages.

Command Default By default, the Cisco Plug and Play Gateway logs the error-level log messages.

Command Modes Privileged EXEC

Command History

Release	Modification
Cisco Prime Infrastructure 1.2	This command was introduced.
Cisco Prime Infrastructure 2.0	This command was modified.

Usage Guidelines The **pnp modify log-level** command can be used to dynamically change the log level at run time. However, when you restart the Cisco Plug and Play Gateway, it will reset to the error-log level, which is the default.

Examples The following is sample output from the **pnp modify log-level** command:

```
admin# pnp modify log-level ?

  debug  Log level: Debug
  error  Log level: Error
  fatal  Log level: Fatal
```

```
  info   Log level: Info
  trace  Log level: Trace
  warn   Log level: Warn

admin# pnp modify log-level debug
admin# pnp modify log-level error
admin# pnp modify log-level fatal
admin# pnp modify log-level info
admin# pnp modify log-level trace
admin# pnp modify log-level warn
```

pnp restore

To restore the configuration settings from an existing backup of the Cisco Plug and Play Gateway, use the **pnp restore** command in privileged EXEC mode.

To force a restore of the Cisco Plug and Play Gateway settings either when the **pnp setup** command is in operation or another instance of the **pnp restore** command is already running, use the **pnp restore force** command in privileged EXEC mode.

pnp restore *backup filename*

pnp restore force

Syntax Description

backup filename	Name of the Cisco Plug and Play Gateway backup file whose server settings must be restored.
force	Forces a restore of the Cisco Plug and Play Gateway settings.

Command Modes   Privileged EXEC

Command History

Release	Modification
Cisco Prime Infrastructure 1.2	This command was introduced.
Cisco Prime Infrastructure 2.0	This command was modified.

Usage Guidelines   When you run the **pnp restore** command, the server reads the backup files from the */localdisk/ directory*. If there is more than one backup file in the */localdisk/ directory*, a list of the available backup files is displayed. You must provide the name of the backup file that is to be used for restoring the configuration settings.

After the Cisco Plug and Play Gateway settings have been restored, you are prompted to commit the changes. Press **y** to commit the changes or **n** to cancel the restore operation.

> **Note**   You must restart the Cisco Plug and Play Gateway for changes to take effect.

> **Note**   For information on how to copy files to the local disk, see copy, on page 51 command.

Use the **pnp restore force** command when you have to force a restore operation. This condition is normally seen when different instances of the **restore** command is already running or when the **pnp setup** command is in operation. The **pnp restore force** command forces the restore operation using an existing backup file.

Examples   The following is a sample output of the **pnp restore** command:

```
admin# pnp restore

-----------------------------------------------
Tue Oct 2 23:05:53 UTC 2012
Restore operation started
-----------------------------------------------
Please copy the backup required for restoration.
20121002230546.pnp_backup.tar.gz
20121002224919.pnp_backup.tar.gz
Please provide the backup file name [20121002230546.pnp_backup.tar.gz]:
Backup Filename used is /localdisk/20121002230546.pnp_backup.tar.gz

Commit changes and restart (y/n): y
```

pnp setup

To set up the Cisco Plug and Play Gateway information, use the **pnp setup** command in privileged EXEC mode.

To forcefully execute a setup operation of the Cisco Plug and Play Gateway when other commands are running and the **pnp setup** command cannot be used for setting up the server, use the **pnp setup force** command in privileged EXEC mode.

> **Note** The **pnp setup** command can be executed only if Prime Infrastructure and the Cisco Plug and Play Gateway are running on different servers.

pnp setup

pnp setup force

Syntax Description

force	Executes a setup operation of the Cisco Plug and Play Gateway forcefully.

Command Modes Privileged EXEC

Command History

Release	Modification
Cisco Prime Infrastructure 1.2	This command was introduced.
Cisco Prime Infrastructure 2.0	This command was modified.

Usage Guidelines The setup.log file is available in the *var/KickStart/install/ directory*.

Examples The following is sample output from the **pnp setup** command:

```
admin# pnp setup
        ##########################################################################
        Enter Plug and Play Gateway Setup (setup log /var/KickStart/install/setup.log)
        For detail information about the parameters in this setup,
        refer to Plug and Play Gateway Admin Guide.
        ##########################################################################
Enter Prime Infrastructure IP Address: [10.104.105.70]
Enable self certificate for server bgl-dt-ncs-vm64-228 (y/n) [y]
Self Signed Certificate already available do you want to recreate (y/n)? [n]

        Automatic download of SSL Certificate is possible if
        Prime Infrastructure Server is up and running.

Automatically download the certificate for server 10.104.105.70 (y/n) [y]
```

```
         The maximum number of Event Gateways allowed is '10' for both plain text
         and ssl combined. The Event Gateway ports 11011 and 11012 are reserved for port
         automatic allocation. These ports are not counted while taking the maximum number
of ports.

         Each Event Gateway can serves up to a maximum of 1000 devices.

Enter number of Event Gateways that will be started with crypto operation: [5]

         The maximum number of plain text event gateways ports possible is 5.

Enter number of Event Gateways that will be started with plaintext operation: [5]

          The CNS Event command configures how the managed devices should
       connect to this particular Plug and Play Gateway. The command entered in the following

          line should match what's configured on the devices WITHOUT the port
          number and keyword 'encrypt' if cryptographic is enabled.

          For example, if the following CLI is configured on devices
          "cns event bgl-dt-ncs-vm64-228 encrypt 11012 keepalive 120 2 reconnect 10",
          then `encrypt 11012` should be removed and the below line should be entered :
          "cns event bgl-dt-ncs-vm64-228 keepalive 120 2 reconnect 10"

          Another example, if this is a backup Plug and Play Gateway and the following CLI
is
          configured on devices
          "cns event bgl-dt-ncs-vm64-228 11011 source Vlan1 backup", then `11011`
          should be removed and the below line should be entered :
          "cns event bgl-dt-ncs-vm64-228 source Vlan1 backup"

          Unable to enter a correct CLI could cause the managed devices not
          be able to connect to this Plug and Play Gateway. For details, please refer to
          Installation and Configuration Guide.

Enter CNS Event command: [cns event bgl-dt-ncs-vm64-228 keepalive 120 2 reconnect 10]


Commit changes (y/n): y
Attempting to disable the local Plug and Play Gateway in Prime Infrastructure Machine
10.104.105.70
Enter the username to login to the Prime Infrastructure Machine: [admin]  ayyanna
Enter the password to login to the Prime Infrastructure Machine:
Operation Successful. Plug and Play Gateway is successfully disabled.
Setup is in progress.......
Stop Plug and Play Gateway server
Done. Plug and Play Gateway setup completed
Start Plug and Play Gateway server....
Done. Plug and Play Gateway server started!

####################################################################
Disabling the local Plug and Play Gateway on Prime Infrastructure server is successful.
Please restart the Prime Infrastructure server.
####################################################################
bgl-dt-ncs-vm64-228/admin#
```

Note For more information on how to copy files from the local disk, see command.

pnp setup advanced

To change port level settings, use the **pnp setup advanced** command in the privileged EXEC mode.

To forcefully execute a setup operation of the Cisco Plug and Play Gateway when other commands are running and the **pnp setup advanced** command cannot be used for setting up the server, use the **pnp setup advanced force** command in privileged EXEC mode.

pnp setup advanced

pnp setup advanced force

Syntax Description	force	Executes a setup operation of the Cisco Plug and Play Gateway forcefully.

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco Prime Infrastructure 2.0	This command was introduced.

Usage Guidelines The setup.log file is available in the *var/KickStart/install/ directory*.

Examples The following is a sample output of the **pnp setup advanced** command:

```
pnp setup  advanced
#####################################################################
        Enter Plug and Play Gateway Setup (setup log /var/KickStart/install/setup.log)
        For detail information about the parameters in this setup,
        refer to Plug and Play Gateway Admin Guide.
        #####################################################################

Enter IP Address of Plug and Play Gateway server [10.104.105.228]
Enter the fully qualified host name of Plug and Play Gateway server [bgl-dt-ncs-vm64-228]
Enter Prime Infrastructure IP Address: [10.104.105.70]
Enter Prime Infrastructure Event Port Parameter: [61617]
Enable self certificate for server bgl-dt-ncs-vm64-228 (y/n) [y]
Self Signed Certificate already available do you want to recreate (y/n)? [n]

        Automatic download of SSL Certificate is possible if
        Prime Infrastructure Server is up and running.

Automatically download the certificate for server 10.104.105.70 (y/n) [y]
Enable secure HTTPS/SSL encryption to secure Plug and Play Gateway Web GUI (y/n) [y]
Enter port number for https web access: [443]

        Enabling clear text operation
        between Plug and Play Gateway and device(s) increases security risk.

Enable clear text operation between device CNS Agent and Plug and Play Gateway (y/n) [y]
Enter Tomcat internal port number: [8009]
Enter Tomcat shutdown port number: [8005]
```

```
        The maximum number of Event Gateways allowed is '10' for both plain text
        and ssl combined. The Event Gateway ports 11011 and 11012 are reserved for port
        automatic allocation. These ports are not counted while taking the maximum number
of ports.

        Each Event Gateway can serves up to a maximum of 1000 devices.

Enter number of Event Gateways that will be started with crypto operation: [5]
Enter port number for http web access: [80]

        The maximum number of plain text event gateways ports possible is 5.

Enter number of Event Gateways that will be started with plaintext operation: [5]

        The CNS Event command configures how the managed devices should
 connect to this particular Plug and Play Gateway. The command entered in the following

        line should match what's configured on the devices WITHOUT the port
        number and keyword 'encrypt' if cryptographic is enabled.

        For example, if the following CLI is configured on devices
        "cns event bgl-dt-ncs-vm64-228 encrypt 11012 keepalive 120 2 reconnect 10",
        then `encrypt 11012` should be removed and the below line should be entered :
        "cns event bgl-dt-ncs-vm64-228 keepalive 120 2 reconnect 10"

        Another example, if this is a backup Plug and Play Gateway and the following CLI
is
        configured on devices
        "cns event bgl-dt-ncs-vm64-228 11011 source Vlan1 backup", then `11011`
        should be removed and the below line should be entered :
        "cns event bgl-dt-ncs-vm64-228 source Vlan1 backup"

        Unable to enter a correct CLI could cause the managed devices not
        be able to connect to this Plug and Play Gateway. For details, please refer to
        Installation and Configuration Guide.

Enter CNS Event command: [cns event bgl-dt-ncs-vm64-228 keepalive 120 2 reconnect 10]

        Enter IP address for CNS Gateway to listen to.
        Enter 1 to have CNSGateway listens to all IP addresses.
IP addresses:[1]
Enter Plug and Play Gateway Event Port Parameter: [62616]
Enter base directory for Plug and Play Gateway log : [/var/log]

        Data directory contains Template and Image files

Enter data directory for Plug and Play Gateway : [/var/KickStart]


Commit changes (y/n): y
Attempting to disable the local Plug and Play Gateway in Prime Infrastructure Machine
10.104.105.70
Enter the username to login to the Prime Infrastructure Machine: [admin]  ayyanna
Enter the password to login to the Prime Infrastructure Machine:
Plug and Play Gateway is already disabled
Setup is in progress.......
Stop Plug and Play Gateway server
Done. Plug and Play Gateway setup completed
Start Plug and Play Gateway server....
Done. Plug and Play Gateway server started!
admin#
```

pnp start

To start the Cisco Plug and Play Gateway and display the status messages in detail during the startup process, use the **pnp start** command in privileged EXEC mode.

pnp start

Command Modes   Privileged EXEC

Command History

Release	Modification
Cisco Prime Infrastructure 1.2	This command was introduced.
Cisco Prime Infrastructure 2.0	This command was modified.

Usage Guidelines   Before you execute the **pnp start** command, stop the Cisco Plug and Play gateway. For more information on stopping the Cisco Plug and Play gateway, refer to the section pnp stop, on page 136.

Examples   The following is sample output from the **pnp start** command:

```
admin# pnp start

httpd is stopped
Monitoring process started.
Plug and Play Gateway start...................
Started Event Manager process
Starting tomcat...
Starting httpd:
                                                        [  OK  ]

Starting CNS Gateway:
Start of Plug and Play Gateway Completed!!
admin#
```

pnp status

To determine the status of the individual tasks and services that are currently running on the Cisco Plug and Play Gateway, use the **pnpstatus** command in privileged EXEC mode.

pnp status

Command Modes   Privileged EXEC

Command History

Release	Modification
Cisco Prime Infrastructure 1.2	This command was introduced.
Cisco Prime Infrastructure 2.0	This command was modified.

Usage Guidelines   This command can also be used to determine whether the tasks that are running on the Cisco Plug and Play Gateway are secure or nonsecure, and whether the services are up and running or down, along with their port and PID number, where applicable.

Examples   The following is sample output from the **pnp status** command:

```
admin# pnp status
SERVICE                     | MODE         | STATUS | ADDITIONAL INFO
-----------------------------------------------------------------------------------------------
System                      |              | UP     |
-----------------------------------------------------------------------------------------------
Event Messaging Bus         | PLAIN TEXT   | UP     | pid: 3839
CNS Gateway Dispatcher      | PLAIN TEXT   | UP     | pid: 4216, port: 11011
CNS Gateway                 | PLAIN TEXT   | UP     | pid: 4245, port: 11013
CNS Gateway                 | PLAIN TEXT   | UP     | pid: 4279, port: 11015
CNS Gateway                 | PLAIN TEXT   | UP     | pid: 4313, port: 11017
CNS Gateway                 | PLAIN TEXT   | UP     | pid: 4404, port: 11019
CNS Gateway                 | PLAIN TEXT   | UP     | pid: 4442, port: 11021
CNS Gateway Dispatcher      | SSL          | UP     | pid: 4645, port: 11014
CNS Gateway                 | SSL          | UP     | pid: 4645, port: 11014
CNS Gateway                 | SSL          | UP     | pid: 4706, port: 11016
CNS Gateway                 | SSL          | UP     | pid: 4881, port: 11018
CNS Gateway                 | SSL          | UP     | pid: 4921, port: 11020
CNS Gateway                 | SSL          | UP     | pid: 4955, port: 11022
HTTPD                       |              | UP     |
Image Web Service           | SSL          | UP     |
Config Web Service          | SSL          | UP     |
Resource Web Service        | SSL          | UP     |
Image Web Service           | PLAIN TEXT   | UP     |
Config Web Service          | PLAIN TEXT   | UP     |
Resource Web Service        | PLAIN TEXT   | UP     |
Prime Infrastructure Broker | SSL          | UP     | port: 61617,connection:1
```

pnp stop

To stop the Cisco Plug and Play Gateway and display detailed messages during the stop process, use the **pnp stop** command in privileged EXEC mode.

pnp stop

Command Modes   Privileged EXEC

Command History

Release	Modification
Cisco Prime Infrastructure 1.2	This command was introduced.
Cisco Prime Infrastructure 2.0	This command was modified.

Examples   The following is sample output from the **pnp stop** command:

```
admin# pnp stop

start   status  stop
bgl-dt-ncs-vm64-228/admin# pnp stop
Plug and Play Gateway is being shut down..... Please wait!!!
Stopping monitoring process ...
Stopping CNS Gateway Processes:
Stopping tomcat...
Stopping httpd:
OK                                                      [  OK  ]
Stopping Event Manager Processes :
Stop of Plug and Play Gateway Completed!!
admin#
```

pnp tech

To view the environment variables of the Cisco Plug and Play Gateway process, use the **pnp tech** command in privileged EXEC mode.

pnp tech

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco Prime Infrastructure 1.2	This command was introduced.
Cisco Prime Infrastructure 2.0	This command was modified.

Examples

The following is sample output from the **pnp tech** command:

```
admin# pnp tech

-------------------------------------------
Cisco Prime Network Control System
Plug and Play
-------------------------------------------
Environment variables
-------------------------------------------
LOGMANAGER_OPTS=-DPNP_LOG_DIR=/var/log/KickStart -Dlog4j.configuration=log4j.properties
-DPNP_PROCESS_LOG=logmanager
MONITOR_PROCESS=com.cisco.pnp.ks.monitor.Monitor
NCS_PNP_WEB_DIR=/opt/CSCOlumos/tomcat/webapps/
PNP_VAR_INSTALL=/var/KickStart/install
GREP=grep
SETUP_FLAG_FILE=/var/KickStart/install/.setupRunning
PNP_ENABLE_AUTH=n
GREP_CMD=/bin/grep
SED_CMD=/bin/sed
KILL_CMD=/bin/kill
CNS_ENABLE_AUTO_PASS=y
TOMCAT_HOME=/opt/CSCOlumos/KickStart/tomcat
NCS_SERVER_CERTIFICATE=/root/server.crt
HTTPD_MODULES=/etc/httpd/modules
PNP_NCS_MOM_HOST_NAME=127.0.0.1
INIT_DIR=/etc/init.d
RPM_CMD=/bin/rpm
CNS_ENCRYPT_SERVER_TRUST_STORE=/var/KickStart/install/kickstart.truststore
PNP_DATA_BASE=/var
LN_CMD=/bin/ln -sf
CNS_MAX_NO_DEVICE_PER_PORT=500
PNP_ENABLE_DMZ=y
PNP_VAR_TOMCAT_LOG=/var/KickStart/tomcat/logs
MKDIR_CMD=/bin/mkdir -p
PNP_DEFAULT_NO_OF_PORT=5
PNP_CNS_EVENT_CMD=cns event bgl-pnp-dev1-ovf keepalive 120 2 reconnect 10
TOMCAT_SHUTDOWN_PORT=8005
NCS_PNP_WEBAPP_DIR=/opt/CSCOlumos/tomcat/conf/Catalina/localhost
PNP_HTTP_PORT=80
NCS_PROJECT_DISPLAY_NAME=Prime Infrastructure
DATE_CMD=/bin/date
PNP_LOG_FILE=/var/KickStart/install/pnp_start_stop.log
```

```
RM_CMD=/bin/rm -f
ECHO_CMD=/bin/echo -e
TERM=xterm
SHELL=NONE
PNP_NCS_LIB_DIR=/opt/CSCOlumos/lib/lib_pnp_ks
CNS_ENCRYPT_SERVER_KEY_STORE=/var/KickStart/install/kickstart.keystore
GREP_ENHANCED_CMD=/bin/grep -E
TAR_CMD=/bin/tar
ENV_CMD=/bin/env
SSH_CLIENT=10.21.84.117 54389 22
PNP_DATE_FORMAT=%Y%m%d%H%M%S
PNP_ENABLE_HTTPS=Y
CNS_GATEWAY_IP=
PNP_LOG_BASE=/var/log
PNP_MODJK_PACKAGE=mod_jk-ap20
CATALINA_BASE=/var/KickStart/tomcat
TOMCAT_VAR_DIR=/var/KickStart/tomcat
SE_ENABLED=0
HOST_NAME_SHORT_CMD=/bin/hostname -s
SSH_TTY=/dev/pts/1
PNP_WEBAPP_FILE=/var/KickStart/tomcat/conf/Catalina/localhost/cns.xml
PNP_VAR_TOMCAT=/var/KickStart/tomcat
PNP_CARSCLI_PACKAGE=PNPCARSCli
PNP_BIN=/opt/CSCOlumos/KickStart/bin
PNP_JAVA_VERSION=1.6
TOUCH_CMD=/bin/touch
CD_CMD=cd
USER=admin
PNP_IMAGE_TRANSFER_TIMEOUT=1200
CNS_NO_OF_PLAINTEXT_EVENTGW=5
CNS_NO_OF_CRYPTO_EVENTGW=5
PNP_DATA_IMAGE=/var/KickStart/image
PNP_ENABLE_SELF_SIGNED=y
PNP_ENABLE=Y
CPUFILE=/proc/cpuinfo
EVT_NCS_EVENT_PROTOCOL=ssl
PNP_VAR_HTTPD_CONF=/var/KickStart/httpd/conf
MORE_CMD=/bin/more
WGET_CMD_SSL=/usr/bin/wget --no-check-certificate
HEAD_CMD=/usr/bin/head
PNP_PROJECT_RPM_NAME=Lumos_PNP_Server
PNP_LOG_DIR=/var/log/KickStart
PNP_INSTALL_PREFIX=/opt/CSCOlumos
USERNAME_CMD=/usr/bin/id -un
IPTABLE=iptables
CNS_GATEWAY_OPTS=-DPNP_LOG_DIR=/var/log/KickStart -Dlog4j.configuration=cnslog4j.properties
PNP_ENABLE_EMBEDDED_FT=y
PNP_HTTPS_PORT=443
PNP_HTTPD_PACKAGE=httpd
PNP_IMAGE_ACTIVATION_TIMEOUT=600
PNP_ENABLE_AUTO_NCS=n
PNP_ENABLE_SSL=y
PNP_BACKUP_NAME=pnp_backup
SE_ENABLE_HTTPD_DIR=/usr/bin/chcon -Rv --type=httpd_sys_content_t
LOCAL_DISK_DIR=/localdisk
COREFILE=unlimited
PWD_CMD=pwd
MV_CMD=/bin/mv -f
PNP_STARTUP_FILE=/var/KickStart/install/cnsGatewayStartup.txt
MEMFILE=/proc/meminfo
PNP_CE_NG=n
MAIL=/var/mail/admin
PATH=/bin:/usr/bin:/sbin:/usr/sbin:/usr/local/bin:/usr/local/sbin:/opt/system/bin:/opt/system/lib:/opt/system/etc/carscli
IPTABLE_SAVE_CMD=service iptables save
IPTABLE_FILE=/etc/sysconfig/iptables
EVT_NCS_EVENT_PORT=61617
PNP_NCS=n
PNP_SETUP_LOG=/var/KickStart/install/setup.log
PNP_HTTPD_INIT_DIR=/opt/CSCOlumos/KickStart/httpd//etc/init.d
PNP_HOME=/opt/CSCOlumos/KickStart
IPTABLE_RESTART_CMD=service iptables restart
PNP_PRIMARY=y
EVT_MANAGER_PROCESS=com.cisco.pnp.ks.eventmanager.server.StartPNPKSMOMServer
```

```
EVT_MGR_EVENT_PORT=62616
PNP_VAR_HTTPD=/var/KickStart/httpd
PNP_SYSTEM_MONITOR_NAME=pnp_systemmonitor
PWD=/localdisk
JAVA_HOME=/usr/lib/jvm/java-1.6.0-sun-1.6.0.21.x86_64/jre
HTTP_SERVER_KEY=/var/KickStart/install/pnp_selfsigned_server.key
RPM_INSTALL_CMD=/bin/rpm -ivh
DF_CMD=/bin/df
CP_CMD=/bin/cp -f
NCS_TRUST_STORE=/opt/CSCOlumos/conf/truststore
DISKSIZE_CMD=/bin/df -lk
IPTABLE_ENABLE_TCP_PORT=/sbin/iptables -I INPUT -p tcp -j ACCEPT --dport
CAT_CMD=/bin/cat
NCS_KEY_STORE=/opt/CSCOlumos/conf/keystore
NETSTAT_CMD=/bin/netstat
PNP_SERVER_SSL_KEY=/var/KickStart/conf/server.key
PNP_HOST_NAME=bgl-pnp-dev1-ovf
RPM_REMOVE_CMD=/bin/rpm -e
TAIL_CMD=/bin/tail
PNP_SERVER_SSL_CERT=/var/KickStart/conf/server.crt
CATALINA_OPTS=-DPNP_LOG_DIR=/var/log/KickStart -DPNP_PROCESS_LOG=tomcat
CNS_ENABLE_PLAINTEXT=Y
HOST_NAME_FULL_CMD=/bin/hostname -f
NCS_PNP_WEBAPP_FILE=/opt/CSCOlumos/tomcat/conf/Catalina/localhost/cns.xml
PNP_FT_USERNAME=ciscopnp
PNP_PROJECT_NAME=KickStart
NETCONF_CMD=/sbin/ifconfig
AWK_CMD=/bin/awk
PNP_ENABLE_PORT_ALLOCATION=y
PNP_VAR_HTTPD_HTML=/var/KickStart/httpd/html
IPTABLE_STATUS_CMD=service iptables status
PNP_SHUTDOWN_FILE=/var/KickStart/install/cnsGatewayShutdown.txt
PNP_SERVER_IP=10.104.105.167
PNP_VAR_SERVICE=/var/KickStart/services
PNP_DEPLOYMENT_WEBAPP_FILE=/var/KickStart/tomcat/webapps/pnp-deployment-service.war
NCS_LOG_BASE=/opt/CSCOlumos/logs
PNP_VAR_CONF=/var/KickStart/conf
SHLVL=3
HOME=/home/admin
PNP_JAVA_OPTS=-DPNP_LOG_DIR=/var/log/KickStart -DPNP_PROCESS_LOG=tomcat
PNP_LIB=/opt/CSCOlumos/KickStart/lib
PS_CMD=/bin/ps
WGET_CMD=/usr/bin/wget
DIFF_CMD=/usr/bin/diff
EVT_MGR_OPTS=-DPNP_LOG_DIR=/var/log/KickStart -DPNP_PROCESS_LOG=evtmgr
HTTPD_CONF=/var/KickStart/httpd/conf
PNP_DATA_DIR=/var/KickStart
CUT_CMD=/bin/cut
PNP_DATA_TEMPLATE=/var/KickStart/template
PNP_PROJECT_RELEASE=1
MONITOR_OPTS=-DPNP_LOG_DIR=/var/log/KickStart -Dlog4j.configuration=monitorlog4j.properties
 -DPNP_PROCESS_LOG=monitor
TOMCAT_LOG_DIR=/var/log/KickStart/tomcat
SESTATUS_CMD=/usr/sbin/sestatus
OPENSSL_CMD=/usr/bin/openssl
LOGNAME=admin
PNP_NCS_CONTEXT_FILE=/opt/CSCOlumos/conf/pnp-ks-bean-context.xml
EVT_MGR_EVENT_PROTOCOL=tcp
PNP_END_PORT_STANDALONE=12010
DU_CMD=/usr/bin/du
CLASSPATH=:/var/KickStart/conf
NCS_PNP_DEPLOYMENT_WEBAPP_DIR=/opt/CSCOlumos/tomcat/webapps/pnp-deployment-service
IPTABLE_STOP_CMD=service iptables stop
PNP_PROJECT_VERSION=2.0.0.0
SSH_CONNECTION=10.21.84.117 54389 10.104.105.167 22
PNP_FT_PORT=21
PNP_PLAINTEXT_HTTPD=y
PNP_PROJECT_DISPLAY_NAME=PnP Gateway
PNP_START_PORT=11011
PNP_SETUP_COUNT=1
TOMCAT_AJP13_PORT=8009
MAXOPENFILE=4096
RPM_QUERY_PKG_CMD=/bin/rpm -qi
```

```
                   NCS_PROJECT_NAME=NCS
                   PNP_DATA=/var/KickStart
                   PNP_HOME_HTTPD=/opt/CSCOlumos/KickStart/httpd
                   CNS_TOTAL_EVENTGW=10
                   HTTP_SERVER_CERTIFICATE=/var/KickStart/install/pnp_self_signedserver.crt
                   EVT_MGR_EVENT_FAILOVER=y
                   LS_CMD=/bin/ls
                   NCS_INSTALL_PREFIX=/opt/CSCOlumos
                   NCS_PKG_NAME=LumosApp
                   PNP_LOG4J_OPTS=-DPNP_LOG_DIR=/var/log/KickStart
                   PNP_VAR_TOMCAT_CONF=/var/KickStart/tomcat/conf
                   PNP_VAR_DIR=/var/KickStart
                   SLEEP_CMD=/bin/sleep
                   PNP_IMAGE_DISTRIBUTION_TIMEOUT=1200
                   EVT_MGR_NETWORK_IP=10.104.105.167
                   RPM_FORCED_REMOVE_CMD=/bin/rpm -e --force --noscripts
                   PNP_LOG_LEVEL=warn
                   HTTPD_HOME=/usr
                   PNP_FT_PROTOCOL=ftp
                   CNS_GATEWAY_PROCESS=com.cisco.pnp.ks.cnsgateway.connection.ConnectionManagerBean
                   SE_DEL_HTTPD_MUTEX=/bin/rm -f -r /etc/httpd/logs/ssl_mutex*
                   PNP_END_PORT_NCS=11014
                   _=/bin/env
                   ---------------------------------------
                   admin#
```

pnp tech log

To create a system-monitoring log file for the Cisco Plug and Play Gateway, use the **pnp tech log** command in privileged EXEC mode.

pnp tech log

Command Modes   Privileged EXEC

Command History

Release	Modification
Cisco Prime Infrastructure 1.2	This command was introduced.
Cisco Prime Infrastructure 2.0	This command was modified.

Usage Guidelines   The **pnp tech log** command creates a system-monitoring log file in a compressed tar format with the extension .pnp_systemmonitor.tar.gz.

Examples   The following is sample output from the **pnp tech log** command:

```
admin# pnp tech log

The System Status file created : /localdisk/20121003032209.pnp_systemmonitor.tar.gz
admin#
```

Note   For more information on how to copy files from the local disk, see copy, on page 51 command.

show Commands

This section lists Prime Infrastructure **show** commands. Each command includes a brief description of its use, any command defaults, command modes, usage guidelines, an example of the command syntax and any related commands.

show application

To show application information of the installed application packages on the system, use the **show application** command in EXEC mode.

show application [**status** | **version** [app_name]]

Syntax Description

status	Displays the status of the installed application.
version	Displays the application version for an installed application—the Prime Infrastructure.
app_name	Name of the installed application.

Table 16: Output Modifier Variables for Count or Last

		Output modifier variables:

|	Output modifier variables:
	
	• *begin*—Matched pattern. Up to 80 alphanumeric characters.
	
	• *count*—Counts the number of lines in the output. Add number after the word *count*.
	
	  |—Output modifier variables.
	
	• *end*—Ends with line that matches. Up to 80 alphanumeric characters.
	
	• *exclude*—Excludes lines that match. Up to 80 alphanumeric characters.
	
	• *include*—Includes lines that match. Up to 80 alphanumeric characters.
	
	• *last*—Displays last few lines of output. Add number after the word *last*. Up to 80 lines to display. Default 10.
	
	  |—Output modifier variables (see Table A-8).

Command Default   No default behavior or values.

Command Modes   EXEC

Examples   **Example 1**

```
ncs/admin# show application
<name>          <Description>
ncs             Cisco Network Control System
ncs/admin#
```

Example 2

```
ncs/admin# show application version NCS

Cisco Network Control System
-------------------------------------------
Version      : 1.0.2.051
Build Date   : Mon Aug  2 00:34:25 2010
Install Date : Thu Aug  5 17:48:49 2010

ncs/admin#
```
Example 3

```
ncs/admin# show application status NCS

NCS Database listener is running, PID: 21096
NCS Database is running, number of processes: 27
NCS Application Server is running, PID: 21432
NCS M&T Session Database is running, PID: 21365
NCS M&T Log Collector is running, PID: 21468
NCS M&T Log Processor is running, PID: 21494
NCS M&T Alert Process is running, PID: 21524

ncs/admin#
```

Related Commands

	Description
application install	Installs an application bundle.
application remove	Removes or uninstalls an application.
application start	Starts or enables an application.
application stop	Stops or disables an application.
application upgrade	Upgrades an application bundle.

show backup history

To display the backup history of the system, use the **show backup history** command in EXEC mode.

show backup history

Syntax Description This command has no arguments or keywords.

Command Default No default behavior or values.

Command Modes EXEC

Examples

Example 1

```
ncs/admin# show backup history
Wed Aug 18 12:55:21 UTC 2010: backup logs logs-0718.tar.gz to repository fileserver007:
success
Wed Aug 18 12:55:53 UTC 2010: backup full-0718.tar.gpg to repository fileserver007: success
ncs/admin#
```

Example 2

```
ncs/admin# show backup history
backup history is empty
ncs/admin#
```

Related Commands

Command	Description
backup	Performs a backup (Prime Infrastructure and Cisco ADE OS) and places the backup in a repository.
restore	Restores from backup the file contents of a specific repository.
repository	Enters the repository submode for configuration of backups.
show repository	Displays the available backup files located on a specific repository.

show banner pre-login

To display the banner that you installed, use the **show banner pre-login** command in EXEC mode.

show banner pre-login

Syntax Description   This command has no arguments or keywords.

Command Default   No default behavior or values.

Command Modes   EXEC

Examples   **Example**

admin# show banner pre-login

Related Commands

Command	Description
banner install pre-login	Enables you to install a pre-login banner.

show cdp

To display information about the enabled Cisco Discovery Protocol interfaces, use the **show cdp** command in EXEC mode.

show cdp {**all** | **neighbors**}

Syntax Description

all	Shows all of the enabled Cisco Discovery Protocol interfaces.
neighbors	Shows the Cisco Discovery Protocol neighbors.

Command Default   No default behavior or values.

Command Modes   EXEC

Examples   **Example 1**

```
ncs/admin# show cdp all
CDP protocol is enabled ...
        broadcasting interval is every 60 seconds.
        time-to-live of cdp packets is 180 seconds.

        CDP is enabled on port GigabitEthernet0.
ncs/admin#
```
Example 2

```
ncs/admin# show cdp neighbors
CDP Neighbor : 000c297840e5
        Local Interface    : GigabitEthernet0
        Device Type        : L-NCS-1.0-50
        Port               : eth0
        Address            : 172.23.90.114

CDP Neighbor : isexp-esw5
        Local Interface    : GigabitEthernet0
        Device Type        : cisco WS-C3560E-24TD
        Port               : GigabitEthernet0/5
        Address            : 172.23.90.45

CDP Neighbor : 000c29e29926
        Local Interface    : GigabitEthernet0
        Device Type        : L-NCS-1.0-50
        Port               : eth0
        Address            : 172.23.90.115

CDP Neighbor : 000c290fba98
        Local Interface    : GigabitEthernet0
        Device Type        : L-NCS-1.0-50
        Port               : eth0
        Address            : 172.23.90.111

ncs/admin#
```

Related Commands

Command	Description
cdp holdtime	Specifies the length of time that the receiving device should hold a Cisco Discovery Protocol packet from your router before discarding it.
cdp run	Enables the Cisco Discovery Protocol.
cdp timer	Specifies how often the Prime Infrastructure server sends Cisco Discovery Protocol updates.

show clock

To display the day, month, date, time, time zone, and year of the system software clock, use the **show clock** command in EXEC mode.

show clock

Syntax Description   This command has no arguments or keywords.

Command Default   No default behavior or values.

Command Modes   EXEC

Examples

```
ncs/admin# show clock
Fri Aug  6 10:46:39 UTC 2010
ncs/admin#
```

Note   The **show clock** output in the previous example includes Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT), Great Britain, or Zulu time (see Tables Table 19: Common Time Zones, Table 20: Australia Time Zones, and Table 21: Asia Time Zones on pages A-84 and A-85 for sample time zones).

Related Commands

Command	Description
clock	Sets the system clock for display purposes.

show cpu

To display CPU information, use the **show cpu** command in EXEC mode.

show cpu [statistics] [|] [|]

Syntax Description

statistics	Displays CPU statistics.

		Output modifier variables:
		
		• *begin*—Matched pattern. Up to 80 alphanumeric characters.
		
		• *count*—Counts the number of lines in the output. Add number after the word *count*.
		
		    |—Output modifier variables (see Table A-9).
		
		• *end*—Ends with line that matches. Up to 80 alphanumeric characters.
		
		• *exclude*—Excludes lines that match. Up to 80 alphanumeric characters.
		
		• *include*—Includes lines that match. Up to 80 alphanumeric characters.
		
		• *last*—Displays last few lines of output. Add number after the word *last*. Up to 80 lines to display. Default 10.
		
		    |—Output modifier variables (see Table A-9).

Command Default No default behavior or values.

Command Modes EXEC

Examples **Example 1**

```
ncs/admin# show cpu

processor : 0
model     : Intel(R) Xeon(R) CPU          E5320  @ 1.86GHz
speed(MHz): 1861.914
cache size: 4096 KB

ncs/admin#
```

Example 2

```
ncs/admin# show cpu statistics
user time:           265175
kernel time:         166835
idle time:          5356204
i/o wait time:       162676
irq time:              4055

ncs/admin#
```

Related Commands

Command	Description
show disks	Displays the system information of all disks.
show memory	Displays the amount of system memory that each system process uses.

show disks

To display the disks file-system information, use the **show disks** command in EXEC mode.

show disks [|] [|]

Syntax Description

		Output modifier variables:
		• *begin*—Matched pattern. Up to 80 alphanumeric characters.
		• *count*—Counts the number of lines in the output. Add number after the word *count*.
		|—Output modifier variables (see Table A-10).
		• *end*—Ends with line that matches. Up to 80 alphanumeric characters.
		• *exclude*—Excludes lines that match. Up to 80 alphanumeric characters.
		• *include*—Includes lines that match. Up to 80 alphanumeric characters.
		• *last*—Displays last few lines of output. Add number after the word *last*. Up to 80 lines to display. Default 10.
		|—Output modifier variables (see Table A-10).

Command Default

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

Only platforms that have a disk file system support the **show disks** command.

Examples

```
ncs/admin# show disks

temp. space 2% used (17828 of 988116)
disk: 3% used (143280 of 5944440)

Internal filesystems:
  all internal filesystems have sufficient free space

ncs/admin#
```

Related Commands

Command	Description
show cpu	Displays CPU information.
show memory	Displays the amount of system memory that each system process uses.

show icmp-status

To display the Internet Control Message Protocol echo response configuration information, use the **show icmp_status** command in EXEC mode.

show icmp_status {> file | |}

Syntax Description		
>	Output direction.
file	Name of file to redirect standard output (stdout).
		Output modifier commands:

- *begin*—Matched pattern. Up to 80 alphanumeric characters.
- *count*—Counts the number of lines in the output. Add number after the word count.

  ○ |—Output modifier commands (see Table A-11).

- *end*—Ends with line that matches. Up to 80 alphanumeric characters.
- *exclude*—Excludes lines that match. Up to 80 alphanumeric characters.
- *include*—Includes lines that match. Up to 80 alphanumeric characters.
- last—Displays last few lines of output. Add number after the word last. Up to 80 lines to display. Default 10.

  ○ |—Output modifier commands (see Table A-11).

Command Default   No default behavior or values.

Command Modes   EXEC

Examples   **Example 1**

```
ncs/admin# show icmp_status
icmp echo response is turned on
ncs/admin#
```
Example 2

```
ncs/admin# show icmp_status
icmp echo response is turned off
ncs/admin#
```

Related Commands

Command	Description
icmp echo	Configures the Internet Control Message Protocol (ICMP) echo requests.

show interface

To display the usability status of interfaces configured for IP, use the **show interface** command in EXEC mode.

show interface [GigabitEthernet] |

Syntax Description		
	GigabitEthernet	Shows the Gigabit Ethernet interface. Either 0 or 1.

		Output modifier variables:
	|	• *begin*—Matched pattern. Up to 80 alphanumeric characters.
		• *count*—Counts the number of lines in the interface. Add number after the word *count*.
		• *end*—Ends with line that matches. Up to 80 alphanumeric characters.
		• *exclude*—Excludse lines that match. Up to 80 alphanumeric characters.
		• *include*—Includes lines that match. Up to 80 alphanumeric characters.
		• *last*—Displays last few lines of output. Add number after the word *last*. Up to 80 lines to display. Default 10.

Command Default No default behavior or values.

Command Modes EXEC

Usage Guidelines In the **show interface GigabitEthernet 0** output, you can find that the interface has three IPv6 addresses. The first internet address (starting with 3ffe) is the result of using stateless autoconfiguration. For this to work, you need to have IPv6 route advertisement enabled on that subnet. The next address (starting with fe80) is a link local address that does not have any scope outside the host. You always see a link local address regardless of the IPv6 autoconfiguration or DHCPv6 configuration. The last address (starting with 2001) is the result obtained from an IPv6 DHCP server.

Examples **Example 1**

```
ncs/admin# show interface
eth0      Link encap:Ethernet  HWaddr 00:0C:29:6A:88:C4
          inet addr:172.23.90.113  Bcast:172.23.90.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe6a:88c4/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:48536 errors:0 dropped:0 overruns:0 frame:0
          TX packets:14152 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:6507290 (6.2 MiB)  TX bytes:12443568 (11.8 MiB)
          Interrupt:59 Base address:0x2000
```

```
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:1195025 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1195025 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:649425800 (619.3 MiB)  TX bytes:649425800 (619.3 MiB)

sit0      Link encap:IPv6-in-IPv4
          NOARP  MTU:1480  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)

ncs/admin#
```
Example 2

```
ncs/admin# show interface GigabitEthernet 0
eth0      Link encap:Ethernet  HWaddr 00:0C:29:AF:DA:05
          inet addr:172.23.90.116  Bcast:172.23.90.255  Mask:255.255.255.0
          inet6 addr: 3ffe:302:11:2:20c:29ff:feaf:da05/64 Scope:Global
          inet6 addr: fe80::20c:29ff:feaf:da05/64 Scope:Link
          inet6 addr: 2001:558:ff10:870:8000:29ff:fe36:200/64 Scope:Global
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:77848 errors:0 dropped:0 overruns:0 frame:0
          TX packets:23131 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:10699801 (10.2 MiB)  TX bytes:3448374 (3.2 MiB)
          Interrupt:59 Base address:0x2000
```

Related Commands

Command	Description
interface	Configures an interface type and enters the interface configuration submode.
ipv6 address autoconfig	Enables IPv6 stateless autoconfiguration on an interface.
ipv6 address dhcp	Enables IPv6 address DHCP on an interface.

show inventory

To display information about the hardware inventory, including the Prime Infrastructure appliance model and serial number, use the **show inventory** command in EXEC mode.

show inventory |

Syntax Description	

	Output modifier variables:
	• *begin*—Matched pattern. Up to 80 alphanumeric characters.
	• *count*—Counts the number of lines in the interface. Add number after the word *count*.
	• *end*—Ends with line that matches. Up to 80 alphanumeric characters.
	• *exclude*—Excludse lines that match. Up to 80 alphanumeric characters.
	• *include*—Includes lines that match. Up to 80 alphanumeric characters.
	• *last*—Displays last few lines of output. Add number after the word *last*. Up to 80 lines to display. Default 10.

Command Default   No default behavior or values.

Command Modes   EXEC

Examples

```
ncs/admin# show inventory

NAME: "L-NCS-1.0-50 chassis", DESCR: "L-NCS-1.0-50 chassis"
PID: L-NCS-1.0-50 , VID: V01 , SN: H8JESGOFHGG
Total RAM Memory: 1035164 kB
CPU Core Count: 1
CPU 0: Model Info: Intel(R) Xeon(R) CPU           E5320  @ 1.86GHz
Hard Disk Count(*): 1
Disk 0: Device Name: /dev/sda
Disk 0: Capacity: 64.40 GB
Disk 0: Geometry: 255 heads 63 sectors/track 7832 cylinders
NIC Count: 1
NIC 0: Device Name: eth0
NIC 0: HW Address: 00:0C:29:6A:88:C4
NIC 0: Driver Descr: eth0: registered as PCnet/PCI II 79C970A

(*) Hard Disk Count may be Logical.

ncs/admin#
```

show logging

To display the state of system logging (syslog) and the contents of the standard system logging buffer, use the **show logging** command in EXEC mode.

show logging {**application** [*application-name*]} {**internal**} {**system**} |

Syntax Description

application	Displays application logs.
application-name	Application name. Up to 255 alphanumeric characters.
	• *tail*—Tail system syslog messages.
	• *count*—Tail last count messages. From 0 to 4,294,967,295.
	|—Output modifier variables (see below).
internal	Displays the syslogs configuration.
system	Displays the system syslogs.
|	Output modifier variables:
	• *begin*—Matched pattern. Up to 80 alphanumeric characters.
	• *count*—Counts the number of lines in the interface. Add number after the word *count*.
	• *end*—Ends with line that matches. Up to 80 alphanumeric characters.
	• *exclude*—Excludes lines that match. Up to 80 alphanumeric characters.
	• *include*—Includes lines that match. Up to 80 alphanumeric characters.
	• *last*—Displays last few lines of output. Add number after the word *last*. Up to 80 lines to display. Default 10.

Command Default   No default behavior or values.

Command Modes   EXEC

Usage Guidelines   This command displays the state of syslog error and event logging, including host addresses, and for which, logging destinations (console, monitor, buffer, or host) logging is enabled.

Examples   **Example 1**

```
ncs/admin# show logging system
```

```
            ADEOS Platform log:
            ----------------

            Aug  5 10:44:32 localhost debugd[1943]: [16618]: config:network: main.c[252] [setup]: Setup
             is complete
            Aug  5 10:45:02 localhost debugd[1943]: [17291]: application:install cars_install.c[242]
            [setup]: Install initiated with bundle - ncs.tar.gz,
            repo - SystemDefaultPkgRepos
            Aug  5 10:45:02 localhost debugd[1943]: [17291]: application:install cars_install.c[256]
            [setup]: Stage area - /storeddata/Installing/.1281030
            302
            Aug  5 10:45:02 localhost debugd[1943]: [17291]: application:install cars_install.c[260]
            [setup]: Getting bundle to local machine
            Aug  5 10:45:03 localhost debugd[1943]: [17291]: transfer: cars_xfer.c[58] [setup]: local
            copy in of ncs.tar.gz requested
            Aug  5 10:45:46 localhost debugd[1943]: [17291]: application:install cars_install.c[269]
            [setup]: Got bundle at - /storeddata/Installing/.1281
            030302/ncs.tar.gz
            Aug  5 10:45:46 localhost debugd[1943]: [17291]: application:install cars_install.c[279]
            [setup]: Unbundling package ncs.tar.gz
            Aug  5 10:47:06 localhost debugd[1943]: [17291]: application:install cars_install.c[291]
            [setup]: Unbundling done. Verifying input parameters.
            ..
            Aug  5 10:47:06 localhost debugd[1943]: [17291]: application:install cars_install.c[313]
            [setup]: Manifest file is at - /storeddata/Installing
            /.1281030302/manifest.xml
            Aug  5 10:47:07 localhost debugd[1943]: [17291]: application:install cars_install.c[323]
            [setup]: Manifest file appname - ncs
            Aug  5 10:47:09 localhost debugd[1943]: [17291]: application:install cars_install.c[386]
            [setup]: Manifest file pkgtype - CARS
            Aug  5 10:47:09 localhost debugd[1943]: [17291]: application:install cars_install.c[398]
            [setup]: Verify dependency list -
            Aug  5 10:47:09 localhost debugd[1943]: [17291]: application:install cars_install.c[410]
            [setup]: Verify app license -
            Aug  5 10:47:09 localhost debugd[1943]: [17291]: application:install cars_install.c[420]
            [setup]: Verify app RPM's
            Aug  5 10:47:09 localhost debugd[1943]: [17291]: application:install cars_install.c[428]
            [setup]: No of RPM's - 9
            Aug  5 10:47:09 localhost debugd[1943]: [17291]: application:install cars_install.c[439]
            [setup]: Disk - 50
            Aug 5 10:47:09 localhost debugd[1943]: [17291]: application:install ci_util.c[325] [setup]:
             Disk requested = 51200 KB
            Aug  5 10:47:09 localhost debugd[1943]: [17291]: application:install ci_util.c[345] [setup]:
             More disk found Free = 40550400, req_disk = 51200
            Aug  5 10:47:09 localhost debugd[1943]: [17291]: application:install cars_install.c[450]
            [setup]: Mem requested by app - 100
            Aug  5 10:47:09 localhost debugd[1943]: [17291]: application:install ci_util.c[369] [setup]:
             Mem requested = 102400
            Aug  5 10:47:09 localhost debugd[1943]: [17291]: application:install ci_util.c[384] [setup]:
             Found MemFree = MemFree:          13028 kB
            Aug  5 10:47:09 localhost debugd[1943]: [17291]: application:install ci_util.c[390] [setup]:
             Found MemFree value = 13028
            Aug  5 10:47:09 localhost debugd[1943]: [17291]: application:install ci_util.c[393] [setup]:
             Found Inactive = Inactive:        948148 kB
            Aug  5 10:47:09 localhost debugd[1943]: [17291]: application:install ci_util.c[399] [setup]:
             Found Inactive MemFree value = 948148
            Aug  5 10:47:09 localhost debugd[1943]: [17291]: application:install ci_util.c[409] [setup]:
             Sufficient mem found
            Aug  5 10:47:09 localhost debugd[1943]: [17291]: application:install ci_util.c[415] [setup]:
             Done checking memory...
            Aug  5 10:47:09 localhost debugd[1943]: [17291]: application:install cars_install.c[461]
            [setup]: Verifying RPM's...
            --More--
            (press Spacebar to continue)
```

Example 2

```
            ncs/admin# show logging internal

            log server:          localhost
            Global loglevel:     6
            Status:              Enabled
            ncs/admin#
```

Example 3

```
ncs/admin# show logging internal

log server:          localhost
Global loglevel:     6
Status:              Disabled
ncs/admin#
```

show logins

To display the state of system logins, use the **show logins** command in EXEC mode.

show logins cli

Syntax Description

cli	Lists the **cli** login history.

Command Default

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

Requires the **cli** keyword; otherwise, an error occurs.

Examples

```
ncs/admin# show logins cli
admin     pts/0          10.77.137.60     Fri Aug  6 09:45   still logged in
admin     pts/0          10.77.137.60     Fri Aug  6 08:56 - 09:30  (00:33)
admin     pts/0          10.77.137.60     Fri Aug  6 07:17 - 08:43  (01:26)
reboot    system boot  2.6.18-164.el5PA Thu Aug  5 18:17           (17:49)
admin     tty1                            Thu Aug  5 18:15 - down   (00:00)
reboot    system boot  2.6.18-164.el5PA Thu Aug  5 18:09           (00:06)
setup     tty1                            Thu Aug  5 17:43 - 18:07  (00:24)
reboot    system boot  2.6.18-164.el5PA Thu Aug  5 16:05           (02:02)

wtmp begins Thu Aug  5 16:05:36 2010

ncs/admin#
```

show memory

To display the memory usage of all of the running processes, use the **show memory** command in EXEC mode.

show memory

Syntax Description   This command has no arguments or keywords.

Command Default   No default behavior or values.

Command Modes   EXEC

Examples

```
ncs/admin# show memory
total memory:    1035164 kB
free memory:       27128 kB
cached:           358888 kB
swap-cached:      142164 kB

ncs/admin#
```

show ntp

To show the status of the NTP associations, use the **show ntp** command in EXEC mode.

show ntp

Syntax Description   This command has no arguments or keywords.

Command Default   No default behavior or values.

Command Modes   EXEC

Examples

```
ncs/admin# show ntp
Primary NTP   : cd-ncs-ntp.cisco.com

synchronised to NTP server (10.56.60.29) at stratum 3
   time correct to within 99 ms
   polling server every 1024 s

     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
 127.127.1.0     .LOCL.         10 l   36   64  377   0.000    0.000   0.001
*10.56.60.29     64.103.34.15    2 u  906 1024  377 270.657    3.831  14.345


Warning: Output results may conflict during periods of changing synchronization.
ncs/admin#
ncs/admin# show ntp
% no NTP servers configured
ncs/admin#
```

Related Commands

Command	Description
ntp server	Allows synchronization of the software clock by the NTP server for the system.

show ports

To display information about all of the processes listening on active ports, use the **show ports** command in EXEC mode.

show ports [|] [|]

	Output modifier variables:
	• *begin*—Matched pattern. Up to 80 alphanumeric characters.
	• *count*—Counts the number of lines in the interface. Add number after the word *count*.
	|—Output modifier variables (see Table A-12).
	• *end*—Ends with line that matches. Up to 80 alphanumeric characters.
	• *exclude*—Excludes lines that match. Up to 80 alphanumeric characters.
	• *include*—Includes lines that match. Up to 80 alphanumeric characters.
	• *last*—Displays last few lines of output. Add number after the word *last*. Up to 80 lines to display. Default 10.
	|—Output modifier variables (see Table A-12).

Syntax Description

Command Default   No default behavior or values.

Command Modes   EXEC

Usage Guidelines   When you run the **show ports** command, the port must have an associated active session.

Examples

```
ncs/admin# show ports
Process : timestensubd (21372)
     tcp: 127.0.0.1:11298
Process : timestenorad (21609)
     tcp: 127.0.0.1:51715
     udp: ::1:28314, ::1:59055, ::1:45113, ::1:49082, ::1:64737, ::1:62570, ::1:19577,
::1:29821
Process : ttcserver (21382)
     tcp: 127.0.0.1:16612, 0.0.0.0:53385
Process : timestenrepd (21579)
     tcp: 127.0.0.1:62504, 0.0.0.0:18047
     udp: ::1:51436
Process : timestend (21365)
     tcp: 0.0.0.0:53384
Process : rpc.statd (2387)
     tcp: 0.0.0.0:873
     udp: 0.0.0.0:867, 0.0.0.0:870
Process : timestensubd (21373)
     tcp: 127.0.0.1:43407
```

```
Process : portmap (2350)
      tcp: 0.0.0.0:111
      udp: 0.0.0.0:111
Process : Decap_main (21468)
      tcp: 0.0.0.0:2000
      udp: 0.0.0.0:9993
Process : timestensubd (21369)
      tcp: 127.0.0.1:37648
Process : timestensubd (21374)
      tcp: 127.0.0.1:64211
Process : sshd (2734)
      tcp: 172.23.90.113:22
Process : java (21432)
    tcp: 127.0.0.1:8888, :::2080, :::2020, ::ffff:127.0.0.1:8005, :::8009, :::8905, :::8010,
  :::2090, :::1099, :::9999, :::61616, :::8080, ::
:80, :::60628, :::8443, :::443
      udp: 0.0.0.0:1812, 0.0.0.0:1813, 0.0.0.0:1700, 0.0.0.0:10414, 0.0.0.0:3799, 0.0.0.0:1645,
  0.0.0.0:1646, :::8905, :::8906
Process : monit (21531)
      tcp: 127.0.0.1:2812
Process : java (21524)
      tcp: :::62627
Process : java (21494)
      tcp: ::ffff:127.0.0.1:20515
      udp: 0.0.0.0:20514
Process : tnslsnr (21096)
      tcp: :::1521
Process : ora_d000_ncs1 (21222)
      tcp: :::26456
      udp: ::1:63198
Process : ntpd (2715)
      udp: 172.23.90.113:123, 127.0.0.1:123, 0.0.0.0:123, ::1:123, fe80::20c:29ff:fe6a:123,
  :::123
Process : ora_pmon_ncs1 (21190)
      udp: ::1:51994
Process : ora_mmon_ncs1 (21218)
      udp: :::38941
Process : ora_s000_ncs1 (21224)
      udp: ::1:49864

ncs/admin#
```

show process

To display information about active processes, use the **show process** command in the EXEC mode.

show process |

Syntax Description

	(Optional) Output modifier variables:
	• *begin*—Matched pattern. Up to 80 alphanumeric characters.
	• *count*—Counst the number of lines in the interface. Add number after the word *count*.
	• *end*—Ends with line that matches. Up to 80 alphanumeric characters.
	• *exclude*—Excludes lines that match. Up to 80 alphanumeric characters.
	• *include*—Includes lines that match. Up to 80 alphanumeric characters.
	• *last*—Displays last few lines of output. Add number after the word *last*. Up to 80 lines to display. Default 10.

Command Default

No default behavior or values.

Command Modes

EXEC

Examples

```
ncs/admin# show process
```
USER PID TIME TT COMMAND

root 1 00:00:02 ? init

root 2 00:00:00 ? migration/0

root 3 00:00:00 ? ksoftirqd/0

root 4 00:00:00 ? watchdog/0

root 5 00:00:00 ? events/0

root 6 00:00:00 ? khelper

root 7 00:00:00 ? kthread

root 10 00:00:01 ? kblockd/0

root 11 00:00:00 ? kacpid

root 170 00:00:00 ? cqueue/0

root 173 00:00:00 ? khubd

root 175 00:00:00 ? kseriod

root 239 00:00:32 ? kswapd0

root 240 00:00:00 ? aio/0

root 458 00:00:00 ? kpsmoused

root 488 00:00:00 ? mpt_poll_0

root 489 00:00:00 ? scsi_eh_0

root 492 00:00:00 ? ata/0

root 493 00:00:00 ? ata_aux

root 500 00:00:00 ? kstriped

root 509 00:00:07 ? kjournald

root 536 00:00:00 ? kauditd

root 569 00:00:00 ? udevd

root 1663 00:00:00 ? kmpathd/0

root 1664 00:00:00 ? kmpath_handlerd

root 1691 00:00:00 ? kjournald

root 1693 00:00:00 ? kjournald

root 1695 00:00:00 ? kjournald

root 1697 00:00:00 ? kjournald

root 2284 00:00:00 ? auditd

root 2286 00:00:00 ? audispd

root 2318 00:00:10 ? debugd

rpc 2350 00:00:00 ? portmap

root 2381 00:00:00 ? rpciod/0

--More--

ncs/admin#

Table 17: Show Process Field Descriptions

Field	Description
USER	Logged-in user.
PID	Process ID.
TIME	The time that the command was last used.
TT	Terminal that controls the process.
COMMAND	Type of process or command used.

show repository

To display the file contents of the repository, use the **show repository** command in EXEC mode.

show repository repository-name

Syntax Description

repository-name	Name of the repository whose contents you want to view. Up to 30 alphanumeric characters.

Command Default   No default behavior or values.

Command Modes   EXEC

Examples

```
ncs/admin# show repository myrepository
back1.tar.gpg
back2.tar.gpg
ncs/admin#
```

Related Commands

Command	Description
backup	Performs a backup (Prime Infrastructure and Cisco ADE OS) and places the backup in a repository.
restore	Restores from backup the file contents of a specific repository.
repository	Enters the repository submode for configuration of backups.
show backup history	Displays the backup history of the system.

show restore

To display the restore history, use the **show restore** command in EXEC mode.

show restore {**history**}

Syntax Description

history	Displays the restore history.

Command Default No default behavior or values.

Command Modes EXEC

Examples

Example 1

```
ncs/admin# show restore history
ncs/admin#
```

Example 2

```
ncs/admin# show restore history
restore history is empty
ncs/admin#
```

Related Commands

Command	Description
backup	Performs a backup (Prime Infrastructure and Cisco ADE OS) and places the backup in a repository.
restore	Restores from backup the file contents of a specific repository.
repository	Enters the repository submode for configuration of backups.
show backup history	Displays the backup history of the system.

show running-config

To display the contents of the currently running configuration file or the configuration, use the **show running-config** command in EXEC mode.

showrunning-config

Syntax Description   This command has no arguments or keywords.

Command Default   The **show running-config** command displays all of the configuration information.

Command Modes   EXEC

Examples

```
ncs/admin# show running-config
Generating configuration...
!
hostname ncs
!
ip domain-name cisco.com
!
interface GigabitEthernet 0
  ip address 172.23.90.113 255.255.255.0
  ipv6 address autoconfig
!
ip name-server 172.16.168.183
!
ip default-gateway 172.23.90.1
!
clock timezone UTC
!
ntp server time.nist.gov
!
username admin password hash $1$JbbHvKVG$xMZ/XL4tH15Knf.FfcZZr. role admin
!
service sshd
!
password-policy
  lower-case-required
  upper-case-required
  digit-required
  no-username
  disable-cisco-passwords
  min-password-length 6
!
logging localhost
logging loglevel 6
!
cdp timer 60
cdp holdtime 180
cdp run GigabitEthernet 0
!
icmp echo on
!

ncs/admin#
```

Related Commands

Command	Description
configure	Enters configuration mode.
show startup-config	Displays the contents of the startup configuration file or the configuration.

show startup-config

To display the contents of the startup configuration file or the configuration, use the **show startup-config** command in EXEC mode.

showstartup-config

This command has no arguments or keywords.

Command Default The **show startup-config** command displays all of the startup configuration information.

Command Modes EXEC

Examples
```
ncs/admin# show startup-config
!
hostname ncs
!
ip domain-name cisco.com
!
interface GigabitEthernet 0
  ip address 172.23.90.113 255.255.255.0
  ipv6 address autoconfig
!
ip name-server 172.16.168.183
!
ip default-gateway 172.23.90.1
!
clock timezone UTC
!
ntp server time.nist.gov
!
username admin password hash $1$JbbHvKVG$xMZ/XL4tH15Knf.FfcZZr. role admin
!
service sshd
!
password-policy
  lower-case-required
  upper-case-required
  digit-required
  no-username
  disable-cisco-passwords
  min-password-length 6
!
logging localhost
logging loglevel 6
!
cdp timer 60
cdp holdtime 180
cdp run GigabitEthernet 0
!
icmp echo on
!
ncs/admin#
```

Related Commands

Command	Description
configure	Enters configuration mode.
show running-config	Displays the contents of the currently running configuration file or the configuration.

show security-status

To display the security-related configuration information, use the **show security-status** command in EXEC mode.

show security-status

Syntax Description   This command has no arguments or keywords.

Command Default   No default behavior or values.

Command Modes   EXEC

Examples   **Example**

```
admin# show security-status
Open TCP Ports  : 21 22 443 1522 8082 11011:11014 61617
Open UDP Ports  : 69 162 514 9991

FIPS Mode       : disabled
TFTP Service    : enabled
FTP Service     : enabled

JMS port(61617) : enabled
Root Access     : enabled

Note : Shows currently configured values
Changes made after last system start if any,
will be effective after next restart
```

admin# show security-status

show tech-support

To display technical support information, including email, use the **show tech-support** command in EXEC mode.

show tech-support file [word]

Syntax Description

file	Saves any technical support data as a file in the local disk.
word	Filename to save. Up to 80 alphanumeric characters.

Command Default   Passwords and other security information do not appear in the output.

Command Modes   EXEC

Usage Guidelines   The **show tech-support** command is useful for collecting a large amount of information about your Prime Infrastructure server for troubleshooting purposes. You can then provide output to technical support representatives when reporting a problem.

Examples

```
ncs/admin# show tech-support
##################################################
Application Deployment Engine(ADE) - 2.0.0.568
Technical Support Debug Info follows...
##################################################


*****************************************
Checking dmidecode Serial Number(s)
*****************************************
  None
 VMware-56 4d 14 cb 54 3d 44 5d-49 ee c4 ad a5 6a 88 c4

*****************************************
Displaying System Uptime...
*****************************************
 12:54:34 up 18:37,  1 user,  load average: 0.14, 0.13, 0.12

*****************************************
Display Memory Usage(KB)
*****************************************
             total        used        free      shared     buffers      cached
Mem:       1035164     1006180       28984           0       10784      345464
-/+ buffers/cache:      649932      385232
Swap:      2040244      572700     1467544

*****************************************
Displaying Processes(ax --forest)...
*****************************************
  PID TTY       STAT     TIME COMMAND
    1 ?         Ss       0:02 init [3]
    2 ?         S<       0:00 [migration/0]
    3 ?         SN       0:00 [ksoftirqd/0]
    4 ?         S<       0:00 [watchdog/0]
```

```
    5 ?        S<     0:00 [events/0]
--More--
(press Spacebar to continue)

ncs/admin#
```

Related Commands

Command	Description
show interface	Displays the usability status of the interfaces.
show process	Displays information about active processes.
show running-config	Displays the contents of the current running configuration.

show terminal

To obtain information about the terminal configuration parameter settings, use the **show terminal** command in EXEC mode.

show terminal

Syntax Description
This command has no arguments or keywords.

Command Default
No default behavior or values.

Command Modes
EXEC

Examples
```
ncs/admin# show terminal
TTY: /dev/pts/0 Type: "vt100"
Length: 27 lines, Width: 80 columns
Session Timeout: 30 minutes
ncs/admin#
```
show terminal, on page 178 describes the fields of the **show terminal** output.

Table 18: Show Terminal Field Descriptions

Field	Description
TTY: /dev/pts/0	Displays standard output to type of terminal.
Type: "vt100"	Type of current terminal used.
Length: 24 lines	Length of the terminal display.
Width: 80 columns	Width of the terminal display, in character columns.
Session Timeout: 30 minutes	Length of time, in minutes, for a session, after which the connection closes.

show timezone

To display the time zone set on the system, use the **show timezone** command in EXEC mode.

show timezone

Syntax Description   This command has no arguments or keywords.

Command Default   No default behavior or values.

Command Modes   EXEC

Examples

```
ncs/admin# show timezone
UTC
ncs/admin#
```

Related Commands

Command	Description
clock timezone	Sets the time zone on the system.
show timezones	Displays the time zones available on the system.

show timezones

To obtain a list of time zones from which you can select, use the **show timezones** command in EXEC mode.

show timezones

Syntax Description   This command has no arguments or keywords.

Command Default   No default behavior or values.

Command Modes   EXEC

Usage Guidelines   See the clock timezone command, for examples of the time zones available for the Prime Infrastructure server.

Examples

```
ncs/admin# show timezones
Africa/Blantyre
Africa/Dar_es_Salaam
Africa/Dakar
Africa/Asmara
Africa/Timbuktu
Africa/Maputo
Africa/Accra
Africa/Kigali
Africa/Tunis
Africa/Nouakchott
Africa/Ouagadougou
Africa/Windhoek
Africa/Douala
Africa/Johannesburg
Africa/Luanda
Africa/Lagos
Africa/Djibouti
Africa/Khartoum
Africa/Monrovia
Africa/Bujumbura
Africa/Porto-Novo
Africa/Malabo
Africa/Ceuta
Africa/Banjul
Africa/Cairo
Africa/Mogadishu
Africa/Brazzaville
Africa/Kampala
Africa/Sao_Tome
Africa/Algiers
Africa/Addis_Ababa
Africa/Ndjamena
Africa/Gaborone
Africa/Bamako
Africa/Freetown
--More--
(press Spacebar to continue)

ncs/admin#
```

Related Commands

Command	Description
show timezone	Displays the time zone set on the system.
clock timezone	Sets the time zone on the system.

show udi

To display information about the UDI of the Cisco ISE 3315 appliance, use the **show udi** command in EXEC mode.

show udi

Syntax Description   This command has no arguments or keywords.

Command Default   No default behavior or values.

Command Modes   EXEC

Examples   **Example 1**

```
ncs/admin# show udi
SPID: L-NCS-1.0-50
VPID: V01
Serial: LAB12345678

ncs/admin#
```

The following output appears when you run the **show udi** command on VMware servers.

Example 2

```
ncs/admin# show udi
SPID: L-NCS-1.0-50
VPID: V01
Serial: 5C79C84ML9H

ncs/admin#
```

show uptime

To display the length of time that you have been logged in to the Prime Infrastructure server, use the **show uptime** command in EXEC mode.

show uptime |

Syntax Description		(Optional) Output modifier variables:

- *begin*—Matched pattern. Up to 80 alphanumeric characters.
- *count*—Counts the number of lines in the output. Add number after the word *count*.
- *end*—Ends with line that matches. Up to 80 alphanumeric characters.
- *exclude*—Excludes lines that match. Up to 80 alphanumeric characters.
- *include*—Includse lines that match. Up to 80 alphanumeric characters.
- *last*—Displays last few lines of output. Add number after the word *last*. Up to 80 lines to display. Default 10.

Command Default   No default behavior or values.

Command Modes   EXEC

Examples

```
ncs/admin# show uptime
3 day(s), 18:55:02
ncs/admin#
```

show users

To display the list of users logged in to the Prime Infrastructure server, use the **show users** command in EXEC mode.

show users

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

EXEC

Examples

```
ncs/admin# show users
USERNAME        ROLE   HOST                    TTY      LOGIN DATETIME

admin           Admin  10.77.137.60            pts/0    Fri Aug  6 09:45:47 2010

ncs/admin#
```

show version

To display information about the software version of the system, use the **show version** command in EXEC mode.

show version

Syntax Description   This command has no arguments or keywords.

Command Default   No default behavior or values.

Command Modes   EXEC

Usage Guidelines   This command displays version information about the Cisco ADE-OS software running on the Prime Infrastructure server, and displays the Prime Infrastructure version.

Examples
```
ncs/admin# show version
Cisco Application Deployment Engine OS Release: 2.0
ADE-OS Build Version: 2.0.0.568
ADE-OS System Architecture: i386

Copyright (c) 2005-2010 by Cisco Systems, Inc.
All rights reserved.
Hostname: pmbudev-vm3


Version information of installed applications
---------------------------------------------

Cisco Prime Network Control System
---------------------------------------------
Version    : 1.0.2.051
Vendor    : Wireless Networking Business Unit
ncs/admin#
```

Configuration Commands

This section lists the **configuration commands** along with a brief description of their use, command defaults, command syntax, command modes, usage guidelines, command examples, and related commands, where applicable.

Configuration commands include **interface** and **repository**.

Note   Some of the configuration commands require you to enter the configuration submode to complete the command configuration.

To access configuration mode, you must use the **configure** command in EXEC mode.

aaa authentication

To configure external authentication, use the **aaa authentication** command in configuration mode.

aaa authentication tacacs+ server *TACACS server address* **key plain** *shared-key*

Syntax Description		
TACACS server address	IP address or hostname of the TACACS+ server.	
shared-key	Indicates the shared secret text string.	

Command Default No default behavior or values.

Command Modes Configuration

backup-staging-url

To allow you to configure a Network File System (NFS) location that the backup and restore operations will use as a staging area to package and unpackage backup files, use the **backup-staging-url** command in configuration mode.

backup-staging-url *word*

Syntax Description

word	NFS URL for staging area. Up to 2048 alphanumeric characters. Use **nfs:**//*server***:***path*(1) .

Command Default
No default behavior or values.

Command Modes
Configuration

Usage Guidelines
The URL is NFS only. The format of the command is **backup-staging-url nfs:**//server:path.

⚠
Caution
Ensure that you secure your NFS server in such a way that the directory can be accessed only by the IP address of the Prime Infrastructure server.

Examples

```
ncs/admin(config)# backup-staging-url nfs://loc-filer02a:/vol/local1/private1/jdoe
ncs/admin(config)#
```

banner install pre-login

To set up a pre-login banner, use the **banner install pre-login** command. To remove the pre-login banner, use the **banner remove pre-login** command.

banner install pre-login *banner-text-file* **repository** *repo-name*

Syntax Description

banner-text-file	Banner text file name.
repo-name	Repository name.

Command Default

No default behavior or values.

Command Modes

EXEC

Examples

```
admin(config)#  banner install pre-login myBanner repository myRepository
```

Related Commands

Command	Description
show banner pre-login	Enables you to display a pre-login banner.

cdp holdtime

To specify the amount of time for which the receiving device should hold a Cisco Discovery Protocol packet from the Prime Infrastructure server before discarding it, use the **cdp holdtime** command in configuration mode. To revert to the default setting, use the **no** form of this command.

[no] cdp holdtime *seconds*

Syntax Description

seconds	Specifies the hold time, in seconds. Value from 10 to 255 seconds.

Command Default   180 seconds

Command Modes   Configuration

Usage Guidelines   Cisco Discovery Protocol packets transmit with a time to live, or hold time, value. The receiving device will discard the Cisco Discovery Protocol information in the Cisco Discovery Protocol packet after the hold time has elapsed.

The **cdp holdtime** command takes only one argument; otherwise, an error occurs.

Examples

```
ncs/admin(config)# cdp holdtime 60
ncs/admin(config)#
```

Related Commands

	Description
cdp timer	Specifies how often the Prime Infrastructure server sends Cisco Discovery Protocol updates.
cdp run	Enables the Cisco Discovery Protocol.

cdp run

To enable the Cisco Discovery Protocol, use the **cdp run** command in configuration mode. To disable the Cisco Discovery Protocol, use the **no** form of this command.

[no] cdp run *[GigabitEthernet]*

Syntax Description

GigabitEthernet	Specifies the Gigabit Ethernet interface on which to enable the Cisco Discovery Protocol.

Command Default

No default behavior or values.

Command Modes

Configuration

Usage Guidelines

The command has one optional argument, which is an interface name. Without an optional interface name, the command enables the Cisco Discovery Protocol on all interfaces.

Note

The default for this command is on interfaces that are already up and running. When you are bringing up an interface, stop the Cisco Discovery Protocol first; then, start the Cisco Discovery Protocol again.

Examples

```
ncs/admin(config)# cdp run GigabitEthernet 0
ncs/admin(config)#
```

Related Commands

	Description
cdp holdtime	Specifies the length of time that the receiving device should hold a Cisco Discovery Protocol packet from the Prime Infrastructure server before discarding it.
cdp timer	Specifies how often the Prime Infrastructure server sends Cisco Discovery Protocol updates.

cdp timer

To specify how often the Prime Infrastructure server sends Cisco Discovery Protocol updates, use the **cdp timer** command in configuration mode. To revert to the default setting, use the **no** form of this command.

[no] cdp timer *seconds*

Syntax Description

seconds	Specifies how often, in seconds, the Prime Infrastructure server sends Cisco Discovery Protocol updates. Value from 5 to 254 seconds.

Command Default   60 seconds

Command Modes   Configuration

Usage Guidelines   Cisco Discovery Protocol packets transmit with a time to live, or hold time, value. The receiving device will discard the Cisco Discovery Protocol information in the Cisco Discovery Protocol packet after the hold time has elapsed.

The **cdp timer** command takes only one argument; otherwise, an error occurs.

Examples

```
ncs/admin(config)# cdp timer 60
ncs/admin(config)#
```

Related Commands

	Description
cdp holdtime	Specifies the amount of time that the receiving device should hold a Cisco Discovery Protocol packet from the Prime Infrastructure server before discarding it.
cdp run	Enables the Cisco Discovery Protocol.

clock timezone

To set the time zone, use the **clock timezone** command in configuration mode. To disable this function, use the **no** form of this command.

clock timezone *timezone*

Syntax Description

timezone	Name of the time zone visible when in standard time. Up to 64 alphanumeric characters.

Command Default   UTC

Command Modes   Configuration

Usage Guidelines   The system internally keeps time in Coordinated Universal Time (UTC). If you do not know your specific time zone, you can enter the region, country, and city (see Tables clock timezone, Table 20: Australia Time Zones, and Table 21: Asia Time Zones for sample time zones to enter on your system).

Table 19: Common Time Zones

Acronym or name	Time Zone Name
Europe	
GMT, GMT0, GMT-0, GMT+0, UTC, Greenwich, Universal, Zulu	Greenwich Mean Time, as UTC
GB	British
GB-Eire, Eire	Irish
WET	Western Europe Time, as UTC
CET	Central Europe Time, as UTC + 1 hour
EET	Eastern Europe Time, as UTC + 2 hours
United States and Canada	
EST, EST5EDT	Eastern Standard Time, as UTC -5 hours
CST, CST6CDT	Central Standard Time, as UTC -6 hours

Acronym or name	Time Zone Name
MST, MST7MDT	Mountain Standard Time, as UTC -7 hours
PST, PST8PDT	Pacific Standard Time, as UTC -8 hours
HST	Hawaiian Standard Time, as UTC -10 hours

Table 20: Australia Time Zones

AustraliaFootnote.			
ACTFootnote.	Adelaide	Brisbane	Broken_Hill
Canberra	Currie	Darwin	Hobart
Lord_Howe	Lindeman	LHIFootnote.	Melbourne
North	NSWFootnote.	Perth	Queensland
South	Sydney	Tasmania	Victoria
West	Yancowinna		

3456

3 (1) Enter the country and city together with a forward slash (/) between them; for example, Australia/Currie.

4 (2) ACT = Australian Capital Territory

5 (3) LHI = Lord Howe Island

6 (4) NSW = New South Wales

Table 21: Asia Time Zones

AsiaFootnote.			
AdenFootnote.	Almaty	Amman	Anadyr
Aqtau	Aqtobe	Ashgabat	Ashkhabad
Baghdad	Bahrain	Baku	Bangkok
Beirut	Bishkek	Brunei	Calcutta
Choibalsan	Chongqing	Columbo	Damascus
Dhakar	Dili	Dubai	Dushanbe

Asia**Footnote.**			
Gaza	Harbin	Hong_Kong	Hovd
Irkutsk	Istanbul	Jakarta	Jayapura
Jerusalem	Kabul	Kamchatka	Karachi
Kashgar	Katmandu	Kuala_Lumpur	Kuching
Kuwait	Krasnoyarsk		

78

7 (1) The Asia time zone includes cities from East Asia, Southern Southeast Asia, West Asia, and Central Asia.

8 (2) Enter the region and city or country together separated by a forward slash (/); for example, Asia/Aden.

Note Several more time zones are available to you. On your Prime Infrastructure server, enter the **show timezones** command. A list of all of the time zones available in the Prime Infrastructure server appears. Choose the most appropriate one for your time zone.

Examples

```
ncs/admin(config)# clock timezone EST
ncs/admin(config)# exit
ncs/admin# show timezone
EST
ncs/admin#
```

Related Commands

	Description
show timezones	Displays a list of available time zones on the system.
show timezone	Displays the current time zone set on the system.

do

To execute an EXEC-level command from configuration mode or any configuration submode, use the **do** command in any configuration mode.

do

Syntax Description   This command has no arguments or keywords.

Table 22: Command Options for the Do Command

	Description
application install	Installs a specific application.
application remove	Removes a specific application.
application start	Starts or enables a specific application
application stop	Stops or disables a specific application.
application upgrade	Upgrades a specific application.
backup	Performs a backup (Prime Infrastructure and Cisco ADE OS) and places the backup in a repository.
backup-logs	Performs a backup of all of the logs on the Prime Infrastructure server to a remote location.
clock	Sets the system clock on the Prime Infrastructure server.
configure	Enters configuration mode.
copy	Copies any file from a source to a destination.
debug	Displays any errors or events for various command situations; for example, backup and restore, configuration, copy, resource locking, file transfer, and user management.
delete	Deletes a file on the Prime Infrastructure server.
dir	Lists files on the Prime Infrastructure server.
forceout	Forces the logout of all of the sessions of a specific Prime Infrastructure node user.
halt	Disables or shuts down the Prime Infrastructure server.

	Description
help	Describes the help utility and how to use it on the Prime Infrastructure server.
mkdir	Creates a new directory.
nslookup	Queries the IPv4 address or hostname of a remote system.
patch	Install System or Application patch.
pep	Configures the Inline PEP node.
ping	Determines the IPv4 network activity on a remote system.
ping6	Determines the IPv6 network activity on a IPv6 remote system.
reload	Reboots the Prime Infrastructure server.
restore	Performs a restore and retrieves the backup out of a repository.
rmdir	Removes an existing directory.
show	Provides information about the Prime Infrastructure server.
ssh	Starts an encrypted session with a remote system.
tech	Provides Technical Assistance Center (TAC) commands.
telnet	Establishes a Telnet connection to a remote system.
terminal length	Sets terminal line parameters.
terminal session-timeout	Sets the inactivity timeout for all terminal sessions.
terminal session-welcome	Sets the welcome message on the system for all terminal sessions.
terminal terminal-type	Specifies the type of terminal connected to the current line of the current session.
traceroute	Traces the route of a remote IP address.
undebug	Disables the output (display of errors or events) of the **debug** command for various command situations; for example, backup and restore, configuration, copy, resource locking, file transfer, and user management.
write	Erases the startup configuration that forces the setup utility to run and prompts the network configuration, copies the running configuration to the startup configuration, and displays the running configuration on the console.

do

Command Default   No default behavior or values.

Command Modes   Configuration

Usage Guidelines   Use this command to execute EXEC commands (such as **show**, **clear**, and **debug** commands) while configuring your server. After the EXEC command executes, the system will return to the configuration mode that you were using.

Examples

```
ncs/admin(config)# do show run
Generating configuration...
!
hostname ncs
!
ip domain-name cisco.com
!
interface GigabitEthernet 0
  ip address 172.23.90.113 255.255.255.0
  ipv6 address autoconfig
!
ip name-server 172.16.168.183
!
ip default-gateway 172.23.90.1
!
clock timezone EST
!
ntp server time.nist.gov
!
username admin password hash $1$JbbHvKVG$xMZ/XL4tH15Knf.FfcZZr. role admin
!
service sshd
!
backup-staging-url nfs://loc-filer02a:/vol/local1/private1/jdoe
!
password-policy
  lower-case-required
  upper-case-required
  digit-required
  no-username
  disable-cisco-passwords
  min-password-length 6
!
logging localhost
logging loglevel 6
!
--More--

ncs/admin(config)#
```

end

To end the current configuration session and return to EXEC mode, use the **end** command in configuration mode.

end

Syntax Description   This command has no arguments or keywords.

Command Default   No default behavior or values.

Command Modes   Configuration

Usage Guidelines   This command brings you back to EXEC mode regardless of what configuration mode or submode you are in.

Use this command when you finish configuring the system and you want to return to EXEC mode to perform verification steps.

Examples

```
ncs/admin(config)# end
ncs/admin#
```

Related Commands

Command	Description
exit	Exits configuration mode.
exit (EXEC)	Closes the active terminal session by logging out of the Prime Infrastructure server.

exit

To exit any configuration mode to the next-highest mode in the CLI mode hierarchy, use the **exit** command in configuration mode.

exit

Syntax Description   This command has no arguments or keywords.

Command Default   No default behavior or values.

Command Modes   Configuration

Usage Guidelines   The **exit** command is used in the Prime Infrastructure server to exit the current command mode to the next highest command mode in the CLI mode hierarchy.

For example, use the **exit** command in configuration mode to return to EXEC mode. Use the **exit** command in the configuration submodes to return to configuration mode. At the highest level, EXEC mode, the **exit** command exits the EXEC mode and disconnects from the Prime Infrastructure server (see exit, for a description of the **exit** (EXEC) command).

Examples

```
ncs/admin(config)# exit
ncs/admin#
```

Related Commands

Command	Description
end	Exits configuration mode.
exit (EXEC)	Closes the active terminal session by logging out of the Prime Infrastructure server.

hostname

To set the hostname of the system, use the **hostname** command in configuration mode. To delete the hostname from the system, use the **no** form of this command, which resets the system to localhost.

[no] hostname word

Syntax Description

word	Name of the host. Contains at least 2 to 64 alphanumeric characters and an underscore (_). The hostname must begin with a character that is not a space.

Command Default

No default behavior or values.

Command Modes

Configuration

Usage Guidelines

A single instance type of command, **hostname** only occurs once in the configuration of the system. The hostname must contain one argument; otherwise, an error occurs.

Examples

```
ncs/admin(config)# hostname ncs-1
Changing the hostname or IP may result in undesired side effects,
such as installed application(s) being restarted.
Are you sure you want to proceed? [y/n] y
Stopping NCS Monitoring & Troubleshooting Log Processor...
Stopping NCS Monitoring & Troubleshooting Log Collector...
Stopping NCS Monitoring & Troubleshooting Alert Process...
Stopping NCS Application Server...
Stopping NCS Monitoring & Troubleshooting Session Database...
Stopping NCS Database processes...
Starting NCS Database processes...
Starting NCS Monitoring & Troubleshooting Session Database...
Starting NCS Application Server...
Starting NCS Monitoring & Troubleshooting Log Collector...
Starting NCS Monitoring & Troubleshooting Log Processor...
Starting NCS Monitoring & Troubleshooting Alert Process...
Note: NCS Processes are initializing. Use 'show application status ncs'
      CLI to verify all processes are in running state.

ncs-1/admin(config)#

ncs-1/admin# show application status ncs

NCS Database listener is running, PID: 11142
NCS Database is running, number of processes: 29
NCS Application Server is still initializing.
NCS M&T Session Database is running, PID: 11410
NCS M&T Log Collector is running, PID: 11532
NCS M&T Log Processor is running, PID: 11555
NCS M&T Alert Process is running, PID: 11623

ncs-1/admin#
```

icmp echo

To configure the Internet Control Message Protocol (ICMP) echo responses, use the **icmp echo** command in configuration mode.

icmp echo {off | on}

Syntax Description

off	Disables ICMP echo response.
on	Enables ICMP echo response.

Command Default   The system behaves as if the ICMP echo response is on (enabled).

Command Modes   Configuration

Examples

```
ncs/admin(config)# icmp echo off
ncs/admin(config)#
```

Related Commands

Command	Description
show icmp-status	Display ICMP echo response configuration information.

interface

To configure an interface type and enter interface configuration mode, use the **interface** command in configuration mode.

> **Note** VMware virtual machine may have a number of interfaces available. This depends on how many network interfaces (NIC) are added to the virtual machine.

interface GigabitEthernet ip-address

Syntax Description

GigabitEthernet	Configures the Gigabit Ethernet interface.
0 - 3	Number of the Gigabit Ethernet port to configure.

> **Note** After you enter the Gigabit Ethernet port number in the **interface** command, you enter config-GigabitEthernet configuration submode (see the following Syntax Description).

do	EXEC command. Allows you to perform any EXEC commands in this mode (see do).
end	Exits config-GigabitEthernet submode and returns you to EXEC mode.
exit	Exits the config-GigabitEthernet configuration submode.
ip	Sets IP address and netmask for the Ethernet interface (see ip address).
ipv6	Configures the IPv6 autoconfiguration address and IPv6 address from DHCPv6 server. (see ipv6 address autoconfig and ipv6 address dhcp).
no	Negates the command in this mode. Two keywords are available: • ip—Sets the IP address and netmask for the interface. • shutdown—Shuts down the interface.
shutdown	Shuts down the interface (see shutdown).

Command Default No default behavior or values.

Command Modes Configuration

Usage Guidelines   You can use the **interface** command to configure subinterfaces to support various requirements.

Examples

```
ncs/admin(config)# interface GigabitEthernet 0
ncs/admin(config-GigabitEthernet)#
```

Related Commands

Command	Description
show interface	Displays information about the system interfaces.
ip address (interface configuration mode)	Sets the IP address and netmask for the interface.
shutdown (interface configuration mode)	Shuts down the interface (see shutdown).

ipv6 address autoconfig

To enable IPv6 stateless autoconfiguration, use the **ipv6 address autoconfig** command in configuration mode. To remove the address from the interface, use the **no** form of this command.

[no] ipv6 address autoconfig [default]0

Syntax Description	**default** (Optional) If a default router is selected on this interface, the default keyword causes a default route to be installed using that default router.
	The **default** keyword can be specified only on one interface.

Command Default   No default behavior or values.

Command Modes   Configuration

Usage Guidelines   IPv6 stateless autoconfiguration has the security downfall of having predictable IP addresses. This downfall is resolved with privacy extensions. You can verify that the privacy extensions feature is enabled using the **show** command.

IPv6 address autoconfiguration is enabled by default in Linux. Cisco ADE 2.0 shows the IPv6 address autoconfiguration in the running configuration for any interface that is enabled.

Examples   **Example 1**

```
ncs/admin# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ncs/admin(config)# interface GigabitEthernet 0
ncs/admin(config)# (config-GigabitEthernet)# ipv6 address autoconfig
ncs/admin(config)# (config-GigabitEthernet)# end
ncs/admin#
```
When IPv6 autoconfiguration is enabled, the running configuration shows the interface settings similar to the following:

```
!
interface GigabitEthernet 0
  ip address 172.23.90.116 255.255.255.0
  ipv6 address autoconfig
!
```
You can use the **show interface GigabitEthernet 0** command to display the interface settings. In example 2, you can see that the interface has three IPv6 addresses. The first address (starting with 3ffe) is obtained using the stateless autoconfiguration. For the stateless autoconfiguration to work, you must have IPv6 route advertisement enabled on that subnet. The next address (starting with fe80) is a link-local address that does not have any scope outside the host. You will always see a link local address regardless of the IPv6 autoconfiguration or DHCPv6 configuration. The last address (starting with 2001) is obtained from a IPv6 DHCP server.

Example 2

```
ncs/admin# show interface GigabitEthernet 0
eth0      Link encap:Ethernet  HWaddr 00:0C:29:AF:DA:05
          inet addr:172.23.90.116  Bcast:172.23.90.255  Mask:255.255.255.0
          inet6 addr: 3ffe:302:11:2:20c:29ff:feaf:da05/64 Scope:Global
          inet6 addr: fe80::20c:29ff:feaf:da05/64 Scope:Link
          inet6 addr: 2001:558:ff10:870:8000:29ff:fe36:200/64 Scope:Global
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:77848 errors:0 dropped:0 overruns:0 frame:0
          TX packets:23131 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:10699801 (10.2 MiB)  TX bytes:3448374 (3.2 MiB)
          Interrupt:59 Base address:0x2000

ncs/admin#
```

To verify that the privacy extensions feature is enabled, you can use the **show interface GigabitEthernet 0** command. You can see two autoconfiguration addresses: one address is without the privacy extensions, and the other is with the privacy extensions.

In the example 3 below, the MAC is 3ffe:302:11:2:20c:29ff:feaf:da05/64 and the non-RFC3041 address contains the MAC, and the privacy-extension address is 302:11:2:9d65:e608:59a9:d4b9/64.

The output appears similar to the following:

Example 3

```
ncs/admin# show interface GigabitEthernet 0
eth0      Link encap:Ethernet  HWaddr 00:0C:29:AF:DA:05
          inet addr:172.23.90.116  Bcast:172.23.90.255  Mask:255.255.255.0
          inet6 addr: 3ffe:302:11:2:9d65:e608:59a9:d4b9/64 Scope:Global
          inet6 addr: 3ffe:302:11:2:20c:29ff:feaf:da05/64 Scope:Global
          inet6 addr: fe80::20c:29ff:feaf:da05/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:60606 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2771 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:9430102 (8.9 MiB)  TX bytes:466204 (455.2 KiB)
          Interrupt:59 Base address:0x2000

ncs/admin#
```

Related Commands

Command	Description
show interface	Displays information about the system interfaces.
ip address (interface configuration mode)	Sets the IP address and netmask for the interface.
shutdown (interface configuration mode)	Shuts down the interface (see shutdown).
ipv6 address dhcp	Enables IPv6 address DHCP on an interface.
show running-config	Displays the contents of the currently running configuration file or the configuration.

ipv6 address dhcp

To enable IPv6 address DHCP, use the **ipv6 address dhcp** command in configuration mode. To remove the address from the interface, use the **no** form of this command.

[no] ipv6 address dhcp [rapid-commit] 0

Syntax Description

[rapid-commit]	(Optional) Allows the two-message exchange method for address assignment.
0	Gigabit Ethernet port number to be configured.

Command Default   No default behavior or values.

Command Modes   Configuration

Usage Guidelines   None.

Examples
```
ncs/admin# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ncs/admin(config)# interface GigabitEthernet 0
ncs/admin(config-GigabitEthernet)# ipv6 address dhcp
ncs/admin(config-GigabitEthernet)# end
ncs/admin#
```
When IPv6 DHCPv6 is enabled, the running configuration shows the interface settings similar to the following:

```
!
interface GigabitEthernet 0
  ip address 172.23.90.116 255.255.255.0
  ipv6 address dhcp
!
```

Note   The IPv6 stateless autoconfiguration and IPv6 address DHCP are not mutually exclusive. It is possible to have both IPv6 stateless autoconfiguration and IPv6 address DHCP on the same interface. You can use the **show interface** to display what IPv6 addresses are in use for a particular interface.

When both the IPv6 stateless autoconfiguration and IPv6 address DHCP are enabled, the running configuration shows the interface settings similar to the following:

```
!
interface GigabitEthernet 0
  ip address 172.23.90.116 255.255.255.0
  ipv6 address dhcp
!
```

Related Commands

Command	Description
show interface	Displays information about the system interfaces.
ip address (interface configuration mode)	Sets the IP address and netmask for the interface.
shutdown (interface configuration mode)	Shuts down the interface (see shutdown).
ipv6 address autoconfig	Enables IPv6 stateless autoconfiguration on an interface.
show running-config	Displays the contents of the currently running configuration file or the configuration.

ip address

To set the IP address and netmask for the Ethernet interface, use the **ip address** command in interface configuration mode. To remove an IP address or disable IP processing, use the **no** form of this command.

[no] ip address ip-address netmask

Note You can configure the same IP address on multiple interfaces. You might want to do this to limit the configuration steps that are needed to switch from using one interface to another.

Syntax Description

ip-address	IPv4 version IP address.
netmask	Mask of the associated IP subnet.

Command Default Enabled.

Command Modes Interface configuration

Usage Guidelines Requires exactly one address and one netmask; otherwise, an error occurs.

Examples

```
ncs/admin(config)# interface GigabitEthernet 1
ncs/admin(config-GigabitEthernet)# ip address 209.165.200.227 255.255.255.224
Changing the hostname or IP may result in undesired side effects,
such as installed application(s) being restarted.
........
To verify that NCS processes are running, use the
'show application status ncs' command.
ncs/admin(config-GigabitEthernet)#
```

Related Commands

Command	Description
shutdown (interface configuration mode)	Disables an interface (see shutdown).
ip default-gateway	Sets the IP address of the default gateway of an interface.
show interface	Displays information about the system IP interfaces.
interface	Configures an interface type and enters the interface mode.

ip default-gateway

To define or set a default gateway with an IP address, use the **ip default-gateway** command in configuration mode. To disable this function, use the **no** form of this command.

[no] ip default-gateway ip-address

Syntax Description

| ip-address | IP address of the default gateway. |

Command Default   Disabled.

Command Modes   Configuration

Usage Guidelines   If you enter more than one argument or no arguments at all, an error occurs.

Examples

```
ncs/admin(config)# ip default-gateway 209.165.202.129
ncs/admin(config)#
```

Related Commands

Command	Description
ip address (interface configuration mode)	Sets the IP address and netmask for the Ethernet interface.

ip domain-name

To define a default domain name that the Prime Infrastructure server uses to complete hostnames, use the **ip domain-name** command in configuration mode. To disable this function, use the **no** form of this command.

[no] ip domain-name word

Syntax Description	word	Default domain name used to complete the hostnames. Contains at least 2 to 64 alphanumeric characters.

Command Default Enabled.

Command Modes Configuration

Usage Guidelines If you enter more or fewer arguments, an error occurs.

Examples
```
ncs/admin(config)# ip domain-name cisco.com
ncs/admin(config)#
```

Related Commands

	Description
ip name-server	Sets the DNS servers for use during a DNS query.

ip name-server

To set the Domain Name Server (DNS) servers for use during a DNS query, use the **ip name-server** command in configuration mode. You can configure one to three DNS servers. To disable this function, use the **no** form of this command.

✎
Note   Using the **no** form of this command removes all of the name servers from the configuration. Using the **no** form of this command and one of the IP names removes only that IP name server.

[no] ip name-server *ip-address [ip-address*]}*

Syntax Description

ip-address	Address of a name server.
ip-address*	(Optional) IP addresses of additional name servers.
	Note You can configure a maximum of three name servers.

Command Default   No default behavior or values.

Command Modes   Configuration

Usage Guidelines   The first name server that is added with the **ip name-server** command occupies the first position and the system uses that server first to resolve the IP addresses.

You can add name servers to the system one at a time or all at once, until you reach the maximum (3). If you already configured the system with three name servers, you must remove at least one server to add additional name servers.

To place a name server in the first position so that the subsystem uses it first, you must remove all name servers with the **no** form of this command before you proceed.

Examples

```
ncs/admin(config)# ip name-server 209.165.201.1


To verify that NCS processes are running, use the
'show application status ncs' command.
ncs/admin(config)#
```
You can choose not to restart the Prime Infrastructure server; nevertheless, the changes will take effect.

Related Commands

Command	Description
ip domain-name	Defines a default domain name that the server uses to complete hostnames.

ip route

To configure the static routes, use the **ip route** command in configuration mode. To remove static routes, use the **no** form of this command.

ip route prefix mask **gateway** ip-address

no ip route prefix mask

Syntax Description

prefix	IP route prefix for the destination.
mask	Prefix mask for the destination.
gateway	Route-specific gateway
ip-address	IP address of the next hop that can be used to reach that network.

Command Default

No default behavior or values.

Configuration.

Usage Guidelines

Static routes are manually configured, which makes them inflexible (they cannot dynamically adapt to network topology changes), but extremely stable. Static routes optimize bandwidth utilization, because no routing updates need to be sent to maintain them. They also make it easy to enforce routing policy.

Examples

```
ncs/admin(config)# ip route 192.168.0.0 255.255.0.0 gateway 172.23.90.2
ncs/admin(config)#
```

kron occurrence

To schedule one or more Command Scheduler commands to run at a specific date and time or a recurring level, use the **kron occurrence** command in configuration mode. To delete this schedule, use the **no** form of this command.

[no] kron {**occurrence**} *occurrence-name*

Syntax Description

occurrence-name	Name of the occurrence. Up to 80 alphanumeric characters. (See the following note and Syntax Description.)

> **Note** After you enter the *occurrence-name* in the **kron occurrence** command, you enter the config-occurrence configuration submode (see the following syntax description).

at	Identifies that the occurrence is to run at a specified calendar date and time. Usage: at [*hh:mm*] [*day-of-week* | *day-of-month* | *month day-of-month*].
do	EXEC command. Allows you to perform any EXEC commands in this mode (see do).
end	Exits the kron-occurrence configuration submode and returns you to EXEC mode.
exit	Exits the kron-occurrence configuration mode.
no	Negates the command in this mode. Three keywords are available: • at—Usage: at [*hh:mm*] [*day-of-week* | *day-of-month* | *month day-of-month*]. • policy-list—Specifies a policy list to be run by the occurrence. Up to 80 alphanumeric characters. • recurring—Execution of the policy lists should be repeated.
policy-list	Specifies a Command Scheduler policy list to be run by the occurrence.
recurring	Identifies that the occurrences run on a recurring basis.

Command Default No default behavior or values.

Command Modes Configuration

Command Reference Guide for Cisco Prime Infrastructure 2.1

Usage Guidelines   Use the **kron occurrence** and **policy-list** commands to schedule one or more policy lists to run at the same time or interval.

Use the **kron policy-list** command in conjunction with the **cli** command to create a Command Scheduler policy that contains the EXEC CLI commands to be scheduled to run on the Prime Infrastructure server at a specified time. See the kron policy-list command.

Examples

| **Note** | When you run the **kron** command, backup bundles are created with a unique name (by adding a time stamp) to ensure that the files do not overwrite each other. |

Example 1: Weekly Backup

```
ncs/admin(config)# kron occurrence WeeklyBackup
ncs/admin(config-Occurrence)# at 14:35 Monday
ncs/admin(config-Occurrence)# policy-list SchedBackupPolicy
ncs/admin(config-Occurrence)# recurring
ncs/admin(config-Occurrence)# exit
ncs/admin(config)#
```

Example 2: Daily Backup

```
ncs/admin(config)# kron occurrence DailyBackup
ncs/admin(config-Occurrence)# at 02:00
ncs/admin(config-Occurrence)# exit
ncs/admin(config)#
```

Command	Description
kron policy-list	Specifies a name for a Command Scheduler policy.

kron policy-list

To specify a name for a Command Scheduler policy and enter the kron-Policy List configuration submode, use the **kron policy-list** command in configuration mode. To delete a Command Scheduler policy, use the **no** form of this command.

[no] kron {**policy-list**} *list-name*

Syntax Description

policy-list	Specifies a name for Command Scheduler policies.
list-name	Name of the policy list. Up to 80 alphanumeric characters.

> **Note** After you enter the *list-name* in the **kron policy-list** command, you enter the config-Policy List configuration submode (see the following Syntax Description).

cli	Command to be executed by the scheduler. Up to 80 alphanumeric characters.
do	EXEC command. Allows you to perform any EXEC commands in this mode (see the do) command.
end	Exits from the config-policy list configuration submode and returns you to EXEC mode.
exit	Exits this submode.
no	Negates the command in this mode. One keyword is available: • cli—Command to be executed by the scheduler.

Command Default No default behavior or values.

Command Modes Configuration

Usage Guidelines Use the **kron policy-list** command in conjunction with the **cli** command to create a Command Scheduler policy that contains the EXEC CLI commands to be scheduled to run on the Prime Infrastructure server at a specified time. Use the **kron occurrence** and **policy list** commands to schedule one or more policy lists to run at the same time or interval. See the ip route command.

Examples

```
ncs/admin(config)# kron policy-list SchedBackupMonday
```

```
ncs/admin(config-Policy List)# cli backup SchedBackupMonday repository SchedBackupRepo
ncs/admin(config-Policy List)# exit
ncs/admin(config)#
```

Related Commands

Command	Description
ip route	Specifies schedule parameters for a Command Scheduler occurrence and enters config-Occurrence configuration mode.

logging

To enable the system to forward logs to a remote system or to configure the log level, use the **logging** command in configuration mode. To disable this function, use the **no** form of this command.

[no] logging *{ip-address | hostname}* {**loglevel** *level*}

Syntax Description	*ip-address*	IP address of remote system to which you forward logs. Up to 32 alphanumeric characters.
	hostname	Hostname of remote system to which you forward logs. Up to 32 alphanumeric characters.
	loglevel	The command to configure the log level for the **logging** command.
	level	Number of the desired priority level at which you set the log messages. Priority levels are (enter the number for the keyword): • 0-emerg—Emergencies: System unusable. • 1-alert—Alerts: Immediate action needed. • 2-crit—Critical: Critical conditions. • 3-err—Error: Error conditions. • 4-warn—Warning: Warning conditions. • 5-notif—Notifications: Normal but significant conditions. • 6-inform—(Default) Informational messages. • 7-debug—Debugging messages.

Command Default No default behavior or values.

Command Modes Configuration

Usage Guidelines This command requires an IP address or hostname or the **loglevel** keyword; an error occurs if you enter two or more of these arguments.

Examples **Example 1**

```
ncs/admin(config)# logging 209.165.200.225
ncs/admin(config)#
```

Example 2

```
ncs/admin(config)# logging loglevel 0
ncs/admin(config)#
```

Related Commands

Command	Description
show logging	Displays the list of logs for the system.

ncs run client-auth

To configure client authentication, use the **ncs run client-auth** command in configuration mode.

ncs run client-auth {enable | disable}

In addition, for online certificate validation, you can set up custom OCSP responders by using the following commands. You can configure upto two URLs as OSCP responders.

- **ocsp responder custom** {enable | disable}
- **ocsp responder set** {url1 | url2}
- **ocsp responder clear** {url1 | url2}

Syntax Description

enable	Enables client authentication.
disalbe		Disables client authentication.

Command Default   No default behavior or values.

Command Modes   Configuration

Examples

```
admin(config)#  ncs run client-auth enable
```

ncs run csrf

The cross-site request forgery check can be disabled (not recommended). The CLI provided only for backward compatibility with API clients which are not programmed for CSRF protection. For CSRF protection, this option should be enabled using the following command.

ncs run csrf enable

To disable, use the following command:

ncs run csrf disable

Command Default	No default behavior or values.

Command Modes	Configuration

Examples
```
admin(config)#  ncs run csrf enable
```

ntp server

To allow for software clock synchronization by the NTP server for the system, use the **ntp server** command in configuration mode. Allows up to three servers. To disable this capability, use the **no** form of this command.

[no] ntp server *{ip-address | hostname}* [ip-address | hostname] [ip-address | hostname] {ntp-key-id} **plain** {ntp-key}

Syntax Description

*ip-address	hostname*	IP address or hostname of the server providing the clock synchronization. Arguments are limited to 255 alphanumeric characters.
ntp-key-id	Indicates the md5 key ID of the NTP server.
ntp-key-	Indicates the md5 key of the NTP server.

Command Default   No servers are configured by default.

Command Modes   Configuration

Usage Guidelines   Use this command if you want to allow the system to synchronize with a specified server.

To terminate NTP service on a device, you must enter the **no ntp** command without keywords or arguments. For example, if you previously entered the **ntp server** command and you now want to remove not only the server synchronization capability, but all NTP functions from the device, use the **no ntp** command without any keywords. This command ensures that all NTP functions are disabled and that the NTP service also terminates.

> **Note**   This command gives conflicting information during the sync process. The sync process can take up to 20 minutes to complete.

Examples

```
ncs/admin(config)# ntp server ncs ncs1 ncs2
ncs/admin(config)#

ncs/admin# show ntp
Primary NTP   : ncs
Secondary NTP : ncs1
Tertiary NTP  : ncs2

synchronised to local net at stratum 11
   time correct to within 11 ms
   polling server every 1024 s

     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
*127.127.1.0     .LOCL.          10 l   22   64  377   0.000    0.000   0.001
 172.23.90.113   .INIT.          16 u    - 1024    0   0.000    0.000   0.000
 172.23.90.114   .INIT.          16 u    - 1024    0   0.000    0.000   0.000
 172.23.90.115   .INIT.          16 u    - 1024    0   0.000    0.000   0.000
```

```
        Warning: Output results may conflict during periods of changing synchronization.
ncs admin#
```

Related Commands

Command	Description
show ntp	Displays the status information about the NTP associations.

password-policy

To enable or configure the passwords on the system, use the **password-policy** command in configuration mode. To disable this function, use the **no** form of this command.

[no] password-policy option

Note The **password-policy** command requires a policy option (see Syntax Description). You must enter the **password-expiration-enabled** command before the other password-expiration commands.

Syntax Description

option	Different command options.

Note After you enter the **password-policy** command, you can enter config-password-policy configuration submode.

digit-required	Requires a digit in the password.
disable-repeat-characters	Disables the ability of the password to contain more than four identical characters.
disable-cisco-password	Disables the ability to use the word Cisco or any combination as the password.
do	EXEC command.
end	Exits from configure mode.
exit	Exits from this submode.
lower-case-required	Requires a lowercase letter in the password.
min-password-length	Specifies a minimum number of characters for a valid password. Integer length from 0 to 4,294,967,295.
no	Negates a command or set its defaults.
no-previous-password	Prevents users from reusing a part of their previous password.
no-username	Prohibits users from reusing their username as a part of a password.
password-expiration-days	Number of days until a password expires. Integer length from 0 to 80.

password-expiration-enabled	Enables password expiration.
	Note You must enter the **password-expiration-enabled** command before the other password-expiration commands.
password-expiration-warning	Number of days before expiration that warnings of impending expiration begin. Integer length from 0 to 4,294,967,295.
password-lock-enabled	Locks a password after several failures.
password-lock-retry-count	Number of failed attempts before password locks. Integer length from 0 to 4,294,967,295.
upper-case-required	Requires an uppercase letter in the password.
special-required	Requires a special character in the password.

Command Default   No default behavior or values.

Command Modes   Configuration

Examples

```
ncs/admin(config)# password-policy
ncs/admin(config-password-policy)# password-expiration-days 30
ncs/admin(config-password-policy)# exit
ncs/admin(config)#
```

repository

To enter the repository submode for configuration of backups, use the **repository** command in configuration mode.

repository *repository-name*

Syntax Description

repository-name	Name of repository. Up to 80 alphanumeric characters.

Note After you enter the name of the repository in the **repository** command, you enter repository configuration submode.

do	EXEC command.
end	Exits repository config submode and returns you to EXEC mode.
exit	Exits this mode.

no	Negates the command in this mode.
	
	Two keywords are available:
	
	    • url—Repository URL.
	
	    • user—Repository username and password for access.

url	URL of the repository. Up to 80 alphanumeric characters (see Table A-20).
user	Configure the username and password for access. Up to 30 alphanumeric characters.

Table 23: URL Keywords

Keyword	Source of Destination
word	Enter the repository URL, including server and path info. Up to 80 alphanumeric characters.
cdrom:	Local CD-ROM drive (read only).

Keyword	Source of Destination
disk:	Local storage. You can enter the **show repository** *repository_name* command to view all of the files in the local repository. **Note** All local repositories are created on the /localdisk partition. When you specify disk:/ in the repository URL, the system creates directories in a path that is relative to /localdisk. For example, if you entered **disk:/backup,** the directory is created at /localdisk/backup.
ftp:	Source or destination URL for an FTP network server. Use url ftp://*server*/*path*(1) .
nfs:	Source or destination URL for an NFS network server. Use url nfs://*server:path*1.
sftp:	Source or destination URL for an SFTP network server. Use url sftp://*server*/*path*1.
tftp:	Source or destination URL for a TFTP network server. Use url tftp://*server*/*path*1. **Note** You cannot use a TFTP repository for performing a Prime Infrastructure upgrade.

Command Default   No default behavior or values.

Command Modes   Configuration

Examples   **Example 1**

```
ncs/admin# configure termainal
ncs/admin(config)# repository myrepository
ncs/admin(config-Repository)# url sftp://example.com/repository/system1
ncs/admin(config-Repository)# user abcd password example
ncs/admin(config-Repository)# exit
ncs/admin(config)# exit
ncs/admin#
```
Example 2

```
ncs/admin# configure termainal
ncs/admin(config)# repository myrepository
ncs/admin(config-Repository)# url disk:/
ncs/admin(config-Repository)# user xyz password plain example
ncs/admin(config-Repository)# exit
ncs/admin(config)# exit
ncs/admin#
```

Related Commands

Command	Description
backup	Performs a backup (Prime Infrastructure and Cisco ADE OS) and places the backup in a repository.

Command	Description
restore	Performs a restore and takes the backup out of a repository.
show backup history	Displays the backup history of the system.
show repository	Displays the available backup files located on a specific repository.

service

To specify a service to manage, use the **service** command in configuration mode. To disable this function, use the **no** form of this command.

[no] service sshd

Syntax Description

sshd	Secure Shell Daemon. The daemon program for SSH.

Command Default No default behavior or values.

Command Modes Configuration

Examples

```
ncs/admin(config)# service sshd
ncs/admin(config)#
```

shutdown

To shut down an interface, use the **shutdown** command in interface configuration mode. To disable this function, use the **no** form of this command.

[no] shutdown

Syntax Description   This command has no arguments or keywords.

Command Default   No default behavior or values.

Command Modes   Interface

Usage Guidelines   When you shut down an interface using this command, you lose connectivity to the Cisco ISE-3315 appliance through that interface (even though the appliance is still powered on). However, if you have configured the second interface on the appliance with a different IP and have not shut down that interface, you can access the appliance through that second interface.

To shut down an interface, you can also modify the ifcfg-eth[0,1] file, which is located at */etc/sysconfig/network-scripts,* using the ONBOOT parameter:

- Disable an interface: set ONBOOT="no"

- Enable an interface: set ONBOOT="yes"

You can also use the **no shutdown** command to enable an interface.

Examples
```
ncs/admin(config)# interface GigabitEthernet 0
ncs/admin(config-GigabitEthernet)# shutdown
```

Related Commands

Command	Description
interface	Configures an interface type and enters interface mode.
ip address (interface configuration mode)	Sets the IP address and netmask for the Ethernet interface.
show interface	Displays information about the system IP interfaces.
ip default-gateway	Sets the IP address of the default gateway of an interface.

snmp-server community

To set up the community access string to permit access to the Simple Network Management Protocol (SNMP), use the **snmp-server community** command in configuration mode. To disable this function, use the **no** form of this command.

[no] snmp-server community *word* **ro**

Syntax Description

word	Accessing string that functions much like a password and allows access to SNMP. No blank spaces allowed. Up to 255 alphanumeric characters.
ro	Specifies read-only access.

Command Default   No default behavior or values.

Command Modes   Configuration

Usage Guidelines   The **snmp-server community** command requires a community string and the **ro** argument; otherwise, an error occurs.

Examples
```
ncs/admin(config)# snmp-server community new ro
ncs/admin(config)#
```

Related Commands

Command	Description
snmp-server host	Sends traps to a remote system.
snmp-server location	Configures the SNMP location MIB value on the system.
snmp-server contact	Configures the SNMP contact MIB value on the system.

snmp-server contact

To configure the SNMP contact Management Information Base (MIB) value on the system, use the **snmp-server contact** command in configuration mode. To remove the system contact information, use the **no** form of this command.

[no] snmp-server contact *word*

Syntax Description

word	String that describes the system contact information of the node. Up to 255 alphanumeric characters.

Command Default   No default behavior or values.

Command Modes   Configuration

Usage Guidelines   None.

Examples
```
ncs/admin(config)# snmp-server contact Abcd
ncs/admin(config)#
```

Related Commands

Command	Description
snmp-server host	Sends traps to a remote system.
snmp-server community	Sets up the community access string to permit access to the SNMP.
snmp-server location	Configures the SNMP location MIB value on the system.

snmp-server host

To send SNMP traps to a remote user, use the **snmp-server host** command in configuration mode. To remove trap forwarding, use the **no** form of this command.

[no] snmp-server host {*ip-address* | *hostname*} **version** {1 | 2c} *community*

Syntax Description

ip-address	IP address of the SNMP notification host. Up to 32 alphanumeric characters.
hostname	Name of the SNMP notification host. Up to 32 alphanumeric characters.

version {1	2c}	(Optional) Version of the SNMP used to send the traps. Default = 1.
		
		If you use the version keyword, specify one of the following keywords:
		
		    • 1—SNMPv1.
		
		    • 2c—SNMPv2C.

community	Password-like community string that is sent with the notification operation.

Command Default   Disabled.

Command Modes   Configuration

Usage Guidelines   The command takes arguments as listed; otherwise, an error occurs.

Examples

```
ncs/admin(config)# snmp-server community new ro
ncs/admin(config)# snmp-server host 209.165.202.129 version 1 password
ncs/admin(config)#
```

Related Commands

Command	Description
snmp-server community	Sets up the community access string to permit access to SNMP.
snmp-server location	Configures the SNMP location MIB value on the system.
snmp-server contact	Configures the SNMP contact MIB value on the system.

snmp-server location

To configure the SNMP location MIB value on the system, use the **snmp-server location** command in configuration mode. To remove the system location information, use the **no** form of this command.

[no] snmp-server location *word*

Syntax Description

word	String that describes the physical location information of the system. Up to 255 alphanumeric characters.

Command Default   No default behavior or values.

Command Modes   Configuration

Usage Guidelines   We recommend that you use underscores (_) or hyphens (-) between the terms within the *word* string. If you use spaces between terms within the *word* string, you must enclose the string in quotation marks (").

Examples   **Example 1**

```
ncs/admin(config)# snmp-server location Building_3/Room_214
ncs/admin(config)#
```
Example 2

```
ncs/admin(config)# snmp-server location "Building 3/Room 214"
ncs/admin(config)#
```

Related Commands

Command	Description
snmp-server host	Sends traps to a remote system.
snmp-server community	Sets up the community access string to permit access to SNMP.
snmp-server contact	Configures the SNMP location MIB value on the system.

username

To add a user who can access the Cisco ISE-3315 using SSH, use the **username** command in configuration mode. If the user already exists, the password, the privilege level, or both change with this command. To delete the user from the system, use the **no** form of this command.

[no] username *username* **password** {**hash** | **plain**} *password* **role** {**admin** | **user**] [**disabled** [**email** email-address]] [**email** email-address]

For an existing user, use the following command option:

username username **password role** {admin | **user**} password

Syntax Description

username	You should enter only one word which can include hyphen (-), underscore (_) and period (.).
	Note Only alphanumeric characters are allowed at an initial setup.
password	The command to use specify password and user role.
password	Password character length up to 40 alphanumeric characters. You must specify the password for all new users.
**hash	plain**	Type of password. Up to 34 alphanumeric characters.
**role admin	user**	Sets the privilege level for the user.
disabled	Disables the user according to the user's email address.
email *email-address*	The user's email address. For example, user1@example.com.

Command Default   The initial user during setup.

Command Modes   Configuration

Usage Guidelines   The **username** command requires that the username and password keywords precede the hash | plain and the admin | user options.

Examples   **Example 1**

```
ncs/admin(config)# username admin password hash ###### role admin
ncs/admin(config)#
```

Example 2

```
ncs/admin(config)# username admin password plain Secr3tp@swd role admin
ncs/admin(config)#
```

Example 3

```
ncs/admin(config)# username admin password plain Secr3tp@swd role admin email
admin123@example.com
ncs/admin(config)#
```

Related Commands

	Description
password-policy	Enables and configures the password policy.
show users	Displays a list of users and their privilege level. It also displays a list of logged-in users.

username

Glossary

A

ADE

Application Deployment Engine

C

CDP

Cisco Discovery Protocol. A proprietary tool that network administrators use to access a summary of protocol and address information about other devices that are directly connected to the device initiating the command

CDP runs over the data-link layer connecting the physical media to the upper-layer protocols. Because CDP operates at this level, two or more CDP devices that support different network layer protocols (for example, IP and Novell IPX) can learn about each other.

Physical media supporting the Subnetwork Access Protocol (SNAP) encapsulation connect CDP devices. These can include all LANs, Frame Relay, and other WANs, and ATM networks.

Cisco Discovery Protocol

See CDP

CLI

Command-line interface. An interface through which the user can interact with the software operating system by entering commands and optional arguments.

client

Node or software program that requests services from a server. For example, the Secure Shell (SSH) client.

See also server.

command-line interface

See CLI

community string

> A text string that acts as a password, which is used to authenticate messages sent between a management station and an IP Transfer Point (ITP) containing a SNMP agent. The community string sends in every packet between the manager and the agent.

D

DNS

> Domain Name System. DNS associates various sorts of information with so-called domain names; most importantly, it serves as the "phone book" for the Internet: it translates human-readable computer hostnames into the IP addresses that networking equipment needs for delivering information. It also stores other information, such as the list of mail exchange servers that accept e-mail for a given domain. In providing a worldwide keyword-based redirection service, the DNS is an essential component of contemporary Internet use.

DNS name

> Initial name of a node.

domain name

> The style of identifier—a sequence of case-insensitive ASCII labels separated by dots (.) (for example, example.com.)—defined for subtrees in the Internet DNS [R1034] and used in other Internet identifiers, such as hostnames, mailbox names, and URLs.

Domain Name System

> *See* DNS

F

FTP

> File Transfer Protocol. Application protocol, part of the TCP/IP protocol stack, used for transferring files between network nodes. FTP is defined in RFC 959.

H

host

> Computer system on a network. Similar to the term node; except, that host usually implies a computer system, whereas node generally applies to any network system, including access servers and ITPs.

host name

> The name of the operating system's server or computer that contains the major program files.

I

IP

Internet Protocol. Network layer protocol in the TCP/IP stack offering a connectionless internetwork service. IP provides features for addressing, type-of-service specification, fragmentation and reassembly, and security. Documented in RFC 791.

IP address

32-bit address assigned to hosts by using TCP/IP. An IP address belongs to one of five classes (A, B, C, D, or E) and written as 4 octets separated by periods (.) (dotted-decimal format). Each address consists of a network number, an optional subnetwork number, and a host number. For routing, the network and subnetwork numbers stay together, while the host number addresses an individual host within the network or subnetwork. A subnet mask extracts network and subnetwork information from the IP address.

M

MIB

Management Information Base. A directory listing information used and maintained by a network's management protocol, such as SNMP.

N

name server

A name server is a computer server that implements a name-service protocol. It will normally map a computer-usable identifier of a host to a human-usable identifier for that host.

Network Time Protocol

See NTP.

NTP

Network Time Protocol. A protocol for synchronizing the clocks of computer systems over packet-switched, variable-latency data networks. NTP uses User Datagram Protocol (UDP) port 123 as its transport layer. NTP is designed particularly to resist the effects of variable latency (jitter).

NTP is one of the oldest Internet protocols still in use (since before 1985). NTP was originally designed by Dave Mills of the University of Delaware, who still maintains it, along with a team of volunteers.

NTP is not related to the much simpler DAYTIME (RFC 867) and TIME (RFC 868) protocols.

NFS

Network File System. NFS allows a system to share directories and files with others over a network. By using NFS, users and programs can access files on remote systems almost as if they were local files. In Prime Infrastructure, the NFS must be open shared which basically mean that it should not need any credentials.

P

Port

In IP terminology, an upper-layer process that receives information from lower layers. Each numbered port associates with a specific process. For example, SMTP associates with port 25.

S

Secure Shell

See SSH.

server

An application or device that performs services for connected clients as part of a client-server architecture. A server application, as defined by RFC 2616 (HTTP/1.1), is "an application program that accepts connections in order to service requests by sending back responses." Server computers are devices designed to run such an application or applications, often for extended periods of time, with minimal human direction. Examples of servers include web servers, e-mail servers, and file servers.

See also client.

Simple Network Management Protocol

See SNMP.

SSH

Secure Shell. A network protocol in which data is exchanged over a secure channel between two computers. Encryption provides confidentiality and integrity of data. SSH uses public-key cryptography to authenticate the remote computer and allow the remote computer to authenticate the user.

SSH is typically used to log in to a remote machine and execute commands; but, it also supports tunneling, forwarding arbitrary TCP ports, and X Window System (X11) connections. It can transfer files by using the associated SSH File Transfer Protocol (SFTP) or Secure Copy (SCP) protocols.

An SSH server, by default, listens on the standard TCP port 22. An SSH client program is typically used for establishing connections to an sshd daemon accepting remote connections. Both are commonly present on most modern operating systems. Proprietary, freeware, and open-source versions of various levels of complexity and completeness exist.

SNMP

Simple Network Management Protocol. Network management protocol used almost exclusively in TCP/IP networks. SNMP provides a means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security.

SNMPv1

SNMPv1 is a simple request/response protocol. In the SNMPv1 framework, the network-management system installed a request, and managed devices return responses.

SNMPv2C

The second release of SNMP, described in RFC 1902. It provides additions to data types, counter size, and protocol operations. SNMPv2C support includes a bulk-retrieval mechanism and more detailed error message reporting to management stations. The bulk-retrieval mechanism supports the retrieval of tables and large quantities of information, minimizing the number of round-trip transmissions required. SNMPv2C improved error-handling support includes expanded error codes that distinguish different kinds of error conditions; these conditions are reported through a single error code in SNMPv1. Error return codes now report the error type. Three kinds of exceptions are also reported: No such object, No such instance, and End of MIB view.

T

TCP

Transmission Control Protocol. Connection-oriented transport-layer protocol that provides reliable full-duplex data transmission. Part of the TCP/IP protocol stack.

Telnet

Telnet (TELetype NETwork). A network protocol used on the Internet or LAN connections. It was developed in 1969 beginning with RFC 0015 and standardized as IETF STD 8, one of the first Internet standards.

The term Telnet also refers to software that implements the client part of the protocol. Telnet clients have been available on most UNIX systems for many years and are available for virtually all platforms. Most network equipment and operating systems with a TCP/IP stack support some kind of Telnet service server for their remote configuration (including ones based on Windows NT). Recently, Secure Shell has begun to dominate remote access for UNIX-based machines.

Most often, a user telnets to a UNIX-like server system or a simple network device such as a switch. For example, you might "telnet in from home to check your e-mail at work." In doing so, you would be using a Telnet client to connect from your computer to one of your servers. Once the connection is established, you would then log in with your account information and execute the operating system commands remotely on that computer, such as ls or cd.

TFTP

Trivial File Transfer Protocol. Simplified version of FTP that allows files to be transferred from one computer to another over a network.

Transmission Control Protocol

See TCP.

Trivial File Transfer Protocol

See TFTP.

U

UDI

Unique Device Identifier. Each identifiable product is an entity, as defined by the Entity MIB (RFC 2737) and its supporting documents. Some entities, such as a chassis, will have subentities like slots. An Ethernet switch might be a member of a super entity like a stack. Most Cisco entities that are orderable products will leave the factory with an assigned UDI. The UDI information is printed on a label that is affixed to the physical hardware device, and it is also stored electronically on the device in order to facilitate remote retrieval.

A UDI consists of the following elements: product identifier (PID), version identifier (VID), and serial number (SN).

The PID is the name by which the product can be ordered; it has been historically called the "Product Name" or "Part Number." You use this identifier to order an exact replacement part.

The VID is the version of the product. Whenever a product is revised, the VID is incremented, according to a rigorous process derived from Telcordia GR-209-CORE, an industry guideline that governs product change notices.

The SN is the vendor-unique serialization of the product. Each manufactured product carries a unique serial number assigned at the factory, which cannot be changed in the field. This number identifies an individual, specific instance of a product.

Unique Device Identifier

See UDI.

I N D E X