NOKIA

CLI Quick Start Guide for Nokia IPSO

Part No. N450000564 Rev 001

Published June 2007

070101

Contents

About the CLI Up and Running Guide 5
Command Syntax Conventions 6
Additional Documentation 7

1 Restoring Network Connectivity 9

2 Introducing the Command-Line Interface 11
General CLI Features 12
Commands and Command Operations 13
Command Completion 13
Using Tab to Expand Commands 14
Using Esc to Expand Commands 15
Command Help 15
Command Recall 15
Command-Line Movement and Editing 15
Using Default Values 16
Exiting an Output Screen 17
Setting Configuration Locks 17
Using IPSO Shell Commands 18
Saving Configuration Changes 19

3 Interface Commands 21
General Commands 21
Viewing All Interfaces 21
Interface Names 21
Deleting Any Logical Interface 22

Viewing Status and Statistics 23
Ethernet Interfaces 24
Physical Ethernet Interfaces 24
Logical Ethernet Interfaces 26

4 System Configuration Commands 29

Host Name Configuration 29
Adding Host Names 29
Modifying Host Names 29
Deleting Host Names 30
Showing Host Names 30
Date and Time Configuration 30
Setting Date and Time from Server 31
Setting Date and Time Manually 31
Show Date and Clock Commands 32
Package Commands 33
Managing Packages 33

5 Network Security and Access Commands 37

Network Access and Services 37
SSH 39
Enabling/Disabling SSH Service 39
Voyager Web Access (SSL) 40
Enabling SSL Voyager Web Access 40
Generating a Certificate and Private Key 41
Installing a Certificate and Private Key 43

6 Routing Commands 45

Static Routes 45
Configuring Static Routes 45

Index 49

About the CLI Up and Running Guide

This guide introduces the IPSO command-line interface (CLI) and describes some of the most common commands that you can run from it.

Note
If you need to quickly restore connectivity to a platform, see Chapter 1, “Restoring Network Connectivity” on page 9.

To learn about the complete set of commands provided by the CLI, see the *CLI Reference Guide.*

The IPSO CLI complements Nokia Network Voyager, the Nokia web-based interface for IPSO platforms. Most tasks that you can accomplish with Network Voyager you can also do with the CLI. You can enter CLI commands individually and you can also create batch files of CLI commands to automate configuration tasks.

Command Syntax Conventions

The notation conventions described below are used in the CLI command descriptions and related text.

Note
The Nokia CLI prompt is omitted from the examples shown in this guide.

Command Syntax Example 1

```
set interface phys_if_name
        speed <10M | 100M | 1000M>
        duplex <full | half>
        auto-advertise <on | off>
        link-recog-delay <1-255>
        active <on | off>
        flow-control <on | off>
        udld-enable <on | off>
        descriptor_size <128-512>
```

Text you enter literally is shown as monospace font; for example, `set interface`. If a phrase or term in the command syntax is italicized, then that term or phrase is a placeholder for an entry you select. In the above example, where the line reads *phys_if_name*, your actual entry might be `eth-s1p1`.

Each line that is indented under an earlier component of the command is an argument for that command; for example, `speed <10M | 100M | 1000M>` is an argument for the `set interface` command.

If more than one choice is applicable in the command string, the alternative, mutually exclusive choices are surrounded by angle brackets (< >) and separated by vertical lines (|) or by a hyphen if the choices cover a range; for example, `<on | off>` and `<128-512>`. If a default value is applicable, that value is shown underlined; for example, `128`.

Command Syntax Example 2

```
add interface <log_if_name | phys_if_name> [vlanid <2—4094>]
address ip_address/<0—31>
```

If one or more phrases or terms are surrounded by square brackets, as in `[vlanid <2—4094>]` in this example, then the information inside the brackets is optional and might or might not be included in your use of the command.

Additional Documentation

For supporting documentation, see the following documents:

- *Nokia Network Voyager Reference Guide*, which is available on the Nokia customer support Web site and is also available from the Network Voyager navigation tree (if you install the IPSO documentation package).
- *Clustering Configuration Guide for Nokia IPSO*, which is available on the Nokia customer support Web site and is also available from the Network Voyager navigation tree (if you install the IPSO documentation package).

  This guide explains many details about how to implement IP clusters.
- *Getting Started Guide and Release Notes for Nokia IPSO*, which is available on the Nokia customer support Web site.

  This document contains descriptions of the new features for the current IPSO release, installation instructions, and known limitations.

1 Restoring Network Connectivity

If you need to quickly restore network connectivity to your Nokia network security platform, follow these steps:

1. Log on to the platform using a command-line connection (SSH, console, or telnet) over a TCP/IP network as an admin user.
2. Invoke the CLI by entering

   ```
   clish
   ```

3. View your interface names and other information by entering

   ```
   show interfaces
   ```

4. Check the physical configuration of an interface by entering

   ```
   show interface phys_if_name all
   ```

   For example, your actual command might be

   ```
   show interface eth-s1p1 all
   ```

5. Check the logical configuration of an interface by entering

   ```
   show interface log_if_name all
   ```

   For example, your actual command might be

   ```
   show interface eth-s1p1c0 all
   ```

6. Modify any incorrect settings by using the appropriate `set interface` commands. See Chapter 2, “Interface Commands” on page 21 for more information.
7. If you need to modify the host name of the system, see Chapter 3, “System Configuration Commands” on page 29.

8. If you need to create a static route (to allow two-way communication), see Chapter 5, “Routing Commands” on page 45.
9. When you are sure that all the settings are correct, connect to a management interface using Network Voyager.

2 Introducing the Command-Line Interface

This chapter describes the configuration, administration, and monitoring tasks you can perform using the Nokia IPSO command-line interface (CLI).

To use the CLI:

1. Log on to the platform using a command-line connection (SSH, console, or telnet) over a TCP/IP network as an admin, cadmin, or monitor user.

   If you log in as a cadmin (cluster administrator) user, you can change and view configuration settings on all the cluster nodes.

   If you log in as a monitor user, you can execute only the `show` form of commands. That is, you can view configuration settings, but you cannot change them.

2. Invoke the CLI using the one of the procedures explained in the next section.

Invoking the CLI

You can execute CLI commands from the CLI shell and the IPSO shell. Most users have the CLI shell as their default shell. However, the admin user has the IPSO shell (C shell) as their default shell.

Execute From	To Implement	Purpose
IPSO shell	Enter `clish` to invoke the CLI shell. The prompt changes, and you can then enter CLI commands.	Lets you enter any CLI commands in an interactive mode with help text and other helpful CLI features.
IPSO shell	Enter `clish -c "`*`cli_command`*`"`	Lets you execute a single CLI command. You must place double-quotation marks around the CLI command
Command files	• Enter `clish -f` *`filename`* • Enter `clish` to invoke the shell. Then enter `load commands` *`filename`*	Lets you load commands from a file that contains commands. The argument must be the name of a regular file.

General CLI Features

This section describes general CLI features.

Commands and Command Operations

A command always starts with a operation, such as `set` or `add`, followed by a feature, such as vrrp, followed by one or more arguments, such as accept-connections. The possible operations are:

- add—adds a new value to the system.
- commit—ends transaction by committing changes.
- delete—removes a value from the system.
- download—downloads an IPSO image
- exit—exits from the CLI or IPSO shell.
- halt—halts the system.
- load—loads commands from a file.
- quit—exits from the CLI.
- reboot—reboot the system.
- rollback—ends transaction by discarding changes.
- save—saves the configuration changes made since the last save.
- set—sets a value in the system.
- show—displays a value or values from the system.
- start—starts transactions.
- upgrade—upgrades packages
- ver—displays the version of the active IPSO image.

Command Completion

Press Enter to execute a finished command string. The cursor does not have to be at the end of the line when you press Enter. You can usually abbreviate the command to the smallest number of unambiguous characters.

Using Tab to Expand Commands

The Tab key provides two methods of automatic command-line completion.

- If you enter the main keyword for a command, such as vrrp as in the example below, press Space, and then press Tab, the console displays the initial arguments that the command for that feature accepts. After the initial argument display, the command prompt and the command you originally entered are displayed.

  For example,

```
set interface eth-s1p1 <Space><Tab>
active            - sets the physical state to on or off
auto-advertise    - specifies if this interface will advertise the
   configured speed and duplicity using Ethernet Auto Negotiation....
descriptor_size   - Set descriptor size for an interface
duplex            - specifies the duplex mode....
flow-control     - enables or disables the flow control for GigE ethernet
.
.
.
```

- If you enter the feature keyword and part of an argument and press Tab (without pressing Space), the console displays the possible arguments that match the characters you typed. command option for that argument only. In this case, the console does not display all the command arguments.

  For example,

```
Nokia> set in<Tab>
inatmarp  - Set the parameters which regulate Inverse ATM ARP
protocol behavior
interface - Configures the interface related parameters
```

In either case, pressing Tab causes the CLI to display possible values for the next argument only. The CLI does not indicate what arguments (if any) can be typed after the next argument.

Using Esc to Expand Commands

You can use Esc to see all the possible arguments that could be used to complete a command. To use this form of command completion, enter a partial command and then press Esc twice.

Command Help

If you enter a command or part of a command and enter a question mark (?), the console displays help on that command, keyword, or value. This help feature is not available for routing commands.

Command Recall

You can recall commands using the up and down arrow keys, similar to the UNIX Bash shell. The up arrow first recalls the last command, the next to last command, and so on.

Command-Line Movement and Editing

You can back up in a command you are typing to correct a mistake. To edit a command, use the left and right arrow keys to move around and the Backspace key to delete characters. You can enter commands that span more than one line.

The following list shows the keystroke combinations you can use:

- Alt-B—Go to the previous word.
- Alt-D—Delete next word.
- Alt-F—Go to the next word.
- Alt-Ctrl-H—Delete the previous word.
- Alt-Ctrl-L—Clear the screen and show the current line at the top of the screen.

- Alt-Ctrl-_ —Repeat the previous word.
- Ctrl-A—Move to the beginning of the line.
- Ctrl-B—Move to the previous character.
- Ctrl-E—Move to the end of the line.
- Ctrl-F—Move to the next character.
- Ctrl-H—Delete the previous character.
- Ctrl-L—Clear the screen and show the current line at the top of the screen.
- Ctrl-N—Next history item.
- Ctrl-P—Previous history item.
- Ctrl-R—Redisplay the current line.
- Ctrl-U—Delete the current line.

Using Default Values

Some values are in effect by default. If you change one of these to something other than the default, you can change it back by using the argument `default`.

For example, the default ARP keep-time value is 14400 seconds. If you had set the keep-time value to something else, you could reset it to 14400 seconds by entering

```
set arp keep-time default
```

Using the argument `default` is a convenient way to configure the system to use standard values without having to know what the values are .

In this document, default values are shown underlined. For example, the default speed of non-Gigabit ethernet interfaces is 10 megabits per second, and this is shown in the syntax example like this:

```
speed <10M | 100M | 1000M>
```

In some cases, default values is are not indicated in syntax examples. For example, the range of valid ARP keep-time values is 1–86400 seconds, so the relevant syntax example is shown like this:

```
keep-time <1-86400>
```

The accompanying text notes that the default keep-time value is 14400 seconds.

Exiting an Output Screen

When you enter a CLI command that produces more than one screen of output (such as `show route all`), the display stops scrolling when the window is full and the `-- More --` prompt is shown. To exit the output screen, enter `q`.

If you enter a number of commands such as these and repeatedly press Ctrl-C when the `-- More --` prompt is displayed, the system might dump a core file and exit from the CLI. If there are any configuration changes that you have not saved (and that you want to save), follow these steps:

1. Restart the CLI by entering **`clish`**.
2. At the CLI prompt enter

   `save config`

Setting Configuration Locks

When you launch the CLI shell, the shell attempts to acquire an exclusive configuration lock. If there is an active CLI or Voyager session that has already acquired an exclusive configuration lock, a message appears. You can execute show commands, but you cannot change any settings unless you override the configuration lock.

Use the following commands temporarily restrict the ability of other admin users to make configuration changes. This feature allows you to lock out other users for a specified period of time while you make configuration changes.

```
set config-lock
        <on | off>
        on timeout <5-900>
        on override
```

Arguments

`<on | off>`	Specifies whether to enable or disable configuration lock. When you enable config-lock, the default timeout value is 300 seconds. **Default:** off
`on timeout <5-900>`	Specifes to enable config-lock for the specified interval in seconds.
`on override`	Specifies to override an existing config-lock and thus disable config-lock.

Using IPSO Shell Commands

While using the CLI, you can start a standard shell that allows you to execute standard shell commands (such as `ping`, `traceroute`, and so on) by entering

```
shell
```

To exit this shell and return to the CLI, enter

```
exit
```

Saving Configuration Changes

Configuration changes you enter using the CLI are applied immediately to the running system. To ensure that these changes remain after you reboot, that is, to save your changes permanently, enter `save config` if you are using interactive mode. If you want to save your configuration changes into a different file**,** enter `save cfgfile` *`filename`***.**

If you use command-line mode and the `-c` option, you must use the `-s` option to save your configuration changes permanently. For example, enter:

`clish -s -c "`*`cli_command`*`"`

If you use the command-line mode and the `-f` option, you can use the `-s` option. For example, enter:

`clish -s -f` *`filename`*

If you use `-f`, you can also save your changes by including `save config` at the end of the file of configuration commands.

3 Interface Commands

This chapter describes the commands that you use to manage physical and logical interfaces network in your Nokia appliance.

General Commands

The commands described in this section apply to all the interfaces installed in the system.

Viewing All Interfaces

To see a variety of information about all the interfaces in a system, enter

```
show interfaces
```

Interface Names

When a physical interface is installed, the system automatically creates a corresponding logical interface and supplies default names for the physical and logical interface. To make an interface functional, you need to configure both the physical interface and at least one corresponding logical interface (you can create multiple logical interfaces for a single physical interface in some cases).

The `show interfaces` command displays the physical and logical names of all the installed interfaces (as well as other information). You use these names when viewing or configuring specific interfaces.

The following table explains the conventions used for interface names in this document.

if_name	Physical or logical interface name is acceptable.
phys_if_name	Only a physical interface name is acceptable. Physical interface names are assigned by the system and cannot be changed.
log_if_name	Only a logical interface name is acceptable. The default name for a logical interfaces is the name of the physical interface with *cunit_number* appended (in which *unit_number* uniquely identifies the logical interface). For example, the default name for the first logical interface created for physical Ethernet interface `eth-s1p1` is `eth-s1p1c0`. You can change the logical names of interfaces.

Deleting Any Logical Interface

On systems that support hot swapping of interfaces, removing a physical interface while the system is running will not cause any of its logical interfaces to be modified or deleted. If you reinstall the removed interface in the same slot, you do not have to reconfigure the logical interfaces.

If you permanently remove an interface, you may want to remove its configuration information. (For example, you may want to avoid seeing outdated information when you execute `show interfaces`.) To delete a logical interface, enter the following command.

```
delete interface log_if_name
```

To delete all the configuration information for a physical interface, enter the following command.

```
delete interface phys_if_name
```

To delete the IP address of a logical interface (without deleting the logical interface itself), enter the following command.

```
delete interface log_if_name address ip_address
```

If you delete all the logical interfaces or all the IP addresses for an interface, the interface will no longer be accessible over the network. If you delete all the logical interfaces or all the IP addresses for all the connected interfaces, the platform will no longer be accessible over the network. If this occurs, restore network access to the system by connecting to it using a console connection and creating a logical interface for one of the connected physical interfaces.

Viewing Status and Statistics

To see if an interface is active, enter

```
show interface if_name status
```

To see various statistics about an interface, enter

```
show interface if_name statistics
```

To see the properties of and interface and whether the interface is active, enter

```
show interface if_name all
```

Ethernet Interfaces

Use the commands explained in this section to configure physical and logical ethernet interfaces.

Physical Ethernet Interfaces

Use the following commands to configure and view the settings for physical Ethernet interfaces.

```
set interface phys_if_name
        speed <10M | 100M | 1000M>
        duplex <full | half>
        auto-advertise <on | off>
        link-recog-delay <1-255>
        active <on | off>
        flow-control <on | off>
        udld-enable <on | off>
        descriptor_size <128-512>


show interface phys_if_name
        speed
        duplex
        auto-advertise
        link-recog-delay
        flow-control
        status
        udld-enable
```

Arguments

`speed <10M | 100M | 1000M>`	Specifies the speed, in megabits per second, at which the interface will operate. **Default:** 10M
`duplex <full | half>`	Specifies the duplex mode in which the interface will operate. It must be the same as the port to which it is connected. For Gigabit Ethernet interfaces, this value must be full. **Default:** half
`auto-advertise <on | off>`	Specifies whether the interface will advertise its speed and duplex setting using Ethernet autonegotiation. This argument is not valid for Gigabit Ethernet interfaces. **Default:** on
`link-recog-delay <1-255>`	Specifies how many seconds a link must be before the system declares the interface is up. **Default:** 6
`flow-control <on | off>`	Specifies whether flow control is on. This argment is valid only for Gigabit Ethernet interfaces. **Default:** on
`active <on | off>`	Specifies whether the physical interface is active. **Default:** on
`status`	Shows whether the physical interface is active.

udld-enable <on | off>	Specifies whether to use the Cisco Unidirectional Link Detection (UDLD) protocol to improve detection of partial failures in fiber links. This argument is valid only for fiber-optic interfaces. You must enable UDLD on both ends of the link. **Default:** off
descriptor_size <128-512>	Specifies the number of descriptors that are available for Gigabit Ethernet interfaces. Increasing this value allows the system to temporarily store more packets while waiting for the CPU to service them. The system uses one descriptor per packet unless it receives jumbo frames (Ethernet frames larger than 1518 bytes), in which case it uses multiple descriptors per packet. The value you specify must be a multiple of 8. **Default:** 128

Logical Ethernet Interfaces

Use the following commands to create, configure, and view information about logical Ethernet interfaces.

```
add interface <log_if_name | phys_if_name> [vlanid <2—4094>] address
   ip_address/<0—31>
        comments comments
        logical-name new_log_if_name
        unit <1—4094>
        enable | disable
```

```
set interface log_if_name
        arp-mirroring <on | off>
        comments comments
        vlanid <2—4094>
        logical-name new_log_if_name
        enable | disable
        MTU <1500-16,000>

show interface log_if_name
        arp-mirroring
        comments
        vlanid
        logical-name
        MTU <1500-16,000>
```

Arguments

log_if_name | *phys_if_name*	When configuring the default logical interface, specify the logical name. This name ends with c0—for example, eth-s3p2c0. When adding a logical interface (in addition to the default logical interface), specify the physical interface. When adding a logical interface, you must specify a VLAN ID.
`unit <1—4094>`	Specifies the final digits of the logical name (the digits after the c) when adding a logical interface. If you do not specify the unit, IPSO creates the number.

`arp-mirroring <on | off>`	If VRRP is enabled on this interface, specifies whether it should learn the same ARP information as the master if is on a backup router. Enabling this option can speed VRRP failovers because the new VRRP master does not need to learn the MAC addresses that correspond to its next hop IP addresses before it can forward traffic
`comments` *comments*	Specifies comments about an interface. Bracket multiple word comments with quotation marks.
`vlanid <2—4094>`	Specifies the virtual LAN that the logical interface is assigned to. You cannot assign a virtual LAN ID to the first logical interface for a given physical interface.
`address` *ip_address*`/<0—31>`	Specifies the IP address and subnet mask length for the logical interface.
`logical-name` *new_log_if_name*	Specifies a new logical name for the interface or shows the current logical name. If a logical interface is part of an IPSO cluster, do not change its logical name.
`enable | disable`	Enables or disables the logical interface.
`MTU <1500-16,000>`	Specifies the maximum transfer unit for the interface. The value must be an integer. **Default:** `1500`

4 System Configuration Commands

This chapter describes the system configuration commands that you can enter from the CLI prompt.

Host Name Configuration

Use this group of commands to configure the host name of your platform.

Adding Host Names

Use the following command to add a static host name and associate it with an IP address:

```
add host name name ipv4 ip_address
```

Modifying Host Names

Use the following command to change the IP address associated with a host name:

```
set host name name ipv4 ip_address
```

Deleting Host Names

Use the following command to delete a static host name and IP address:

```
delete hostname name
```

Showing Host Names

Use the following commands to view static host names and IP addresses:

```
show hostname

show host names

show host name name ipv4
```

Arguments

name	Specifies the name of a new or existing static host.The name must be alphanumeric characters, dashes ('-'), and periods ('.'). Periods must be followed by a letter or a digit. The name may not end in a dash or a period.
ipv4 *ip_address*	Specifies the associated IP address.The IPv4 address to be associated with a static hostname must be in a dot-delimited format with the following range: [0-255].[0-255].[0-255].[0-255].

Date and Time Configuration

Use the following commands to manually configure the date and time on your system:

Setting Date and Time from Server

```
set date
        once-from-ntpserver <ip_address | fully qualified domain name>
        timezone-city value
```

Note
To display a complete list of timezone values, press tab after `timezone-city`.
The default value is Greenwich(GMT)

```
day <1-31>
hour <0-23>
minute <0-59>
second <0-59>
month <1-12>
year 4 digit integer value
```

Setting Date and Time Manually

You can also use the one of the following 2 commands to set the date and time:

```
set clock time month date year
```

```
set clock time date month year
```

Arguments

`once-from ntpserver <ip_address | fully qualified domain name>`	Specifies to set the local time by contacting the NTP server. Enter either the NTP server's IP address or fully qualified domain name.
`timezone-city value`	Specifies a time based on the time zone of a particular place. The default is Greenwich Mean Time (GMT). To display the complete list of values, press tab after `timezone-city`.

`day <1-31>`	Specifies which day of the month to use to set the inital time.
`hour <0-23>`	Specifies which hour of the day to use to set the inital time.
`minute <0-59>`	Specifies which minute of the hour to use to set the initial time.
`second <0-59>`	Specifies which second of the minute to use to set the initial time.
`month <1-12>`	Specifies which month of the year to use to set the initial time
`year` *`4 digit integer value`*	Specifies which year to use to set the initial time. For example, enter *`2002`*. The range is 1970-2037.

The following table explains the arguments for the `set clock` command set.

Arguments

`time`	Specifies the time. Use the following format: 2 digits for the hour:2 digits for the minute:2 digits for the seconds. For example, 15:18:30
`month`	Specifies the month of the year. Enter one of the following: jan; feb; mar; apr; may; jun; jul; aug; sep; oct; nov; dec.
`date`	Specifies the date Enter 1-31.
`year`	Specifies the year. Enter a 4 digit value.

Show Date and Clock Commands

Use the following commands to view your date and time settings:

```
show date
```

```
show date timezone-city

show clock
```

Arguments

`date`	Displays the system's configured date and time in the following format: day of the week; month; date time year; timezone. For example: *`Mon Mar 18 22:16:51 2002 GMT`*
`date timezone-city`	Displays the system's configured time only. For example: *`Greenwich (GMT)`*.
`clock`	Displays the system's configure date and time in the following format: day of the week; month; date time year; timezone. For example: *`Mon Mar 18 22:16:51 2002 GMT`*

Package Commands

Use the commands in this section to install, upgrade, and delete packages and to view information about packages on your appliance.

Managing Packages

Use the following command to show information about packages installed on the local system:

```
show package
        all
        active
        inactive
```

Arguments

`all`	Lists both the active and inactive packages installed on the system.
`active`	Lists the active packages installed on the system.
`inactive`	Lists the inactive packages installed on the system.

Use the following commands to show a specific package or all packages in a specified directory on a remote or local system. The packages are stored in a gnu zipped tar file with a *.tgz file extension.

```
show package media
        ftp addr ip_address user name password password dir name
        anonftp addr ip_address dir name
        cdrom dir name
        local dir name
```

Arguments

`addr` *`ip_address`*	Specifies the IPv4 address of the remote machine containing the package. Example: 192.168.10.10
`user` *`name`*	Specifies the login name for FTP.
`password` *`password`*	Specifies the password associated with the username parameter for FTP login.
`dir` *`name`*	Specifies the full path of the directory on the remote or local system that contans the packages. Example: `/opt/packages`

You can add optional packages to the core system software. The contents of the package must conform to the predefined IPSO directory hierarchy in order for the package to become integrated. The valid suffixes are tzg, tar.gz, tar, and tar.Z. Each package will be installed as a subdirectory of `/opt`.

Use the following commands to add a package located on a remote system or local system:

```
add package media
        ftp addr ip_address user name password password name name
        anonftp addr ip_address name name
        cdrom name name
        local name name
```

Arguments

`addr` *`ip_address`*	Specifies the IPv4 address of the remote machine containing the package. Example: 192.168.10.10
`user` *`name`*	Specifies the login name for FTP.
`password` *`password`*	Specifies the password associated with the username parameter for the FTP login.
`name` *`name`*	Specifies the file name of the package to install. Use the complete path. Example: `/opt/packages/IPSO-3.7.tgz`

Use the following commands to upgrade the existing package (*.tgz) by specifying a different package located on a remote or local system:

```
upgrade package media
        ftp addr ip_address user name password password old name new name
        anonftp addr ip_address old name new name
        cdrom old name new name
        local old name new name
```

Arguments

`addr` *`ip_address`*	Specifies the IPv4 address of the remote machine containing the package. Example: 192.168.10.10
`user` *`name`*	Specifies the login name for FTP.
`password` *`password`*	Specifies the password associated with the username parameter for FTP login.
`old` *`name`*	Specifies the name of the existing package to be replaced. Use the complete path.
`new` *`name`*	Specifies the name of the package (in .tgz format) you will use to replace the existing package. Use the complete path.

Use the following command to activate or deactivate a specified package:

```
set package name name <on | off>
```

Use the following command to uninstall a specified package:

```
delete package name name
```

Arguments

`name` *`name`*	Specifies the name of the package. Use the complete path.

5 Network Security and Access Commands

This chapter describes the commands that you use to manage the security and access features of your system.

Network Access and Services

Use this group of commands to configure and view network access such as FTP, TFTP and telnet sessions.

Use the following commands to configure network access.

```
set net-access
        ftp <yes | no>
               port <1-65535>
        tftp <yes | no>
        telnet <yes | no>
        admin-net-login <yes | no>
        cli-http <yes | no>
        cli-https <yes | no>
        com2-login <yes | no>
        com3-login <yes | no>
        com4-login <yes | no>
```

Use the following commands to view network access configurations.

```
show
        net-access
        net-access ftp
        net-access tftp
        net-access telnet
        net-access admin-net-login
        net-access cli-http
        net-access cli-https
        net-access com2-login
        net-access com3-login
        net-access com4-login
```

Arguments

`ftp <yes | no>`	Specifies FTP access to the platform. **Default:** no
`port <1-65535>`	Specifies a port on which the ftpd server listens. **Default:** 21
`tftp <yes | no>`	Specifies TFTP access to the platform. **Default:** no
`telnet <yes | no>`	Specifies telnet access to the platform. **Default:** no
`admin-net-login <yes | no>`	Specifies “admin” login for telnet access to the platform. This will not affect admin connections through Voyager or FTP. **Default:** yes
`com2-login <yes | no>`	Specifies login on the serial port ttyd1 com2 that may be connected to an external modem. **Default:** no

`com3-login <yes | no>`	Specifies login on the serial port ttyd2 com3 that may be connected to an external modem. **Default:** no
`com4-login <yes | no>`	Specifies login on the serial port ttyd3 com4 that may be connected to an external modem. **Default:** no

SSH

Use the following groups of commands to enable and configure the SSH service on your platform. By default the service is disabled.

Enabling/Disabling SSH Service

Use the following commands to enable, disable and show the status of SSH service.

```
set ssh server
        enable <0 | 1>

show ssh server
        enable
```

Arguments

`enable <0 | 1>`	The value of 0 disables SSH and the value of 1 enables SSH. **Default:** 1

Voyager Web Access (SSL)

Use the following groups of commands to configure Voyager web access service.

Enabling SSL Voyager Web Access

Use the following commands to enable SSL web access and encryption.

```
set voyager
        daemon-enable <0 | 1>
        port <1-65535>
        ssl-port <1-65535>
        ssl-level <0-168>
```

Use the following commands to view the SSL configuration.

```
show voyager
        port
        ssl-port
        ssl-level
        daemon-enable
```

Arguments

`daemon-enable <0 | 1>`	Enables and disables web configuration for the platform. **Default:** 1
`port <1-65535>`	Specifies the port number on which the Voyager web configuration tool can be accessed when *not* using SSL-secured connections. If you change the port number, you will have to change the URL used when accessing Voyager from http://hostname/ to http://hostname:PORTNUMBER/ **Default:** 80

`ssl-port <1-65535>`	Specifies the port number on which the Voyager web configuration tool can be accessed when using SSL-secured connections. If you change the port number, you will have to change the URL used when accessing Voyager from https://hostname/ to https://hostname:PORTNUMBER/ **Default:** 443
`ssl-level <0-168>`	Specifies the required level of security for Voyager web connections. The value zero (0) indicates that SSL-secured connections will not be used. Setting the level of encryption requires remote connections to use a level of encryption *at least* as strong as the one you specify. The following are the standard encryption levels: • 40-bit • 56-bit • 128-bit • 168-bit (Triple-DES) Once you specify a level of encryption, you must change your URL from http://hostname/ to https://hostname/ to access your platform. **Default:** 0

Generating a Certificate and Private Key

Use the following command to generate a certificate and its associated private key. To better ensure your security, you should generate the certificate and private key over a trusted connection.

```
generate voyager ssl-certificate key-bits <512 | 768| 1024> <passphrase
   name | prompt-passphrase> country name state-or-province name
```

```
locality name organization name organizational-unit name common-name
name email-address name <cert-file path | cert-request-file path>
key-file path
```

Arguments

`key-bits <512 | 768 | 1024>`	Specifies how large your newly generated private key will be in bits. Larger sizes are generally considered more secure. **Default:** 1024
`passphrase` *name*	Specifies a string that this tool will use to encrypt your new private key. Using this syntax will echo your passphrase as you type. If you do not wish to use a passphrase, enter an empty one as ("").
`prompt-passphrase`	Specifies a string that this tool will use to encrypt your new private key. Using this syntax will not echo your passphrase as you type.
`country` *name*	Specifies a two letter code indicating your country, for example, US. This is a required entry.
`state-or-province` *name*	Specifies the *name* of your state or province. This is a required entry.
`locality` *name*	Specifies the name of your city or town, for example Sunnyvale. If you do not wish to use a passphrase, enter an empty one as ("").
`organization` *name*	Specifies the name of your company or organization, for example Worldwide Widgets. This is a required entry.
`organizational-unit` *name*	Specifies the name of a subunit within your company or organization. If you do not wish to use a passphrase, enter an empty one as ("").

`common-name` *`name`*	Identifies where the certificate will go. The name is most commonly the fully qualified domain name for your platform, for example, www.ship.wwwidgets.com. If you are generating a request for a certificate authority, the issuer may impose a different standard.
`email-address` *`name`*	Specifies an e-mail address that could be used for contacting the person responsible for platform and its certificate, for example, “webmaster@ship.wwwidgets.dom”
`cert-file path`	Specifies a file that will receive a certificate. The keyword should be followed by the path name to a file on the IPSO system. Use absolute pathnames.The certificate will be signed with a SHA-1 hash.
`cert-request-file path`	Specifies a file that will receive a certificate request. The keyword should be followed by the path name to a file on the IPSO system. Use absolute pathnames. The request will be signed with a SHA-1 hash.
`key-file path`	Specifies a file that will receive, a private key. The keyword should be followed by the path name to a file on the IPSO system. Use absolute pathnames.

Installing a Certificate and Private Key

Use the following commands to copy a certificate and its associated private key in the /var/etc/voyager_ssl_server.crt and /var/etc/voyager_ssl_server.key files. Copying the certificate and private key to these files makes them available to establish SSL-secure web connections.

```
set voyager ssl-certificate
        cert-file path key-file path <passphrase
          name | prompt-passphrase>
```

Arguments

`cert-file` *path*	Specifies a file that contains the certificate you want to copy. The keyword should be followed by the path name to the file on the IPSO system. Use absolute pathnames.
`key-file` *path*	Specifies a file that contains the private key you want to copy. The keyword should be followed by the path name to a file on the IPSO system. Use absolute pathnames.
`passphrase` *name*	Enter the passphrase you used when generating the certificate and private key or certificate request. Using this syntax will echo your passphrase as you type.
`prompt-passphrase`	Prompts you to enter the passphrase you used whtn generating the certificate and private key or certificate request. Using this syntax will not echo your passphrase as you type.

6 Routing Commands

This chapter describes the routing commands that you can enter from the CLI prompt.

Static Routes

Static routes cause packets moving between a source and a destination to take a specified next hop. Static routes allow you to add routes to destinations that are not described by dynamic routing protocols. A static route can also be useful in providing a default route.

Configuring Static Routes

Use the following group of commands to configure specific static routes.

```
set static-route ip_prefix
        nexthop gateway address gateway_address priority <1-8> on
        nexthop gateway logical gateway_address priority <1-8> on
        nexthop gateway address gateway_address off
        nexthop gateway logical gateway_address off
        nexthop reject
        nexthop blackhole
        off
        rank default
        rank <0-255>
```

Arguments

`nexthop gateway address` *`gateway_address`* `priority <1-8> on`	Specifies the static route and the gateway address. The gateway address is an IP address or a logical interface. If your gateway address is a logical interface, enter the interface name. If the your gateway address is an unnumbered interface, use its logical interface as the gateway address. The priority value determines the order in which the next hops are selected and multiple next hops are defined with different priorities. Switching over to the next hop in the list happens only when an interface fails. Switching over does not happen for "non-reachability" next hops if the interface state is still up. If the route has the same priority as another, and the corresponding interface is up, the route is an equal-cost, multipath route. Lower priority next hops are preferred. You must configure a priority value. This option does not have a default value.
`nexthop logical` *`if_name`* `priority <1-8> on`	Specifies the static route and the logical gateway. For a logical gateway, enter the interface name. For example, if your gateway is an unnumbered interface, use its logical interface as the gateway. The priority value determines the order in which the next hops are selected and multiple next hops are defined with different priorities. Switching over to the next hop in the list happens only when an interface fails. Switching over does not happen for "non-reachability" next hops if the interface state is still up. If the route has the same priority as another, and the corresponding interface is up, the route is an equal-cost, multipath route. Lower priority next hops are preferred. You must configure a priority value. This option does not have a default value.
`nexthop gateway address` *`gateway_address`* `off`	Disables the gateway address only for the IP address configured as the endpoint of the static route from your system. This option does not delete the route itself.

`nexthop gateway logical` *`if_name`* `off`	Disables the gateway only for the logical interface configured as the endpoint of the static route from your system. This option does not delete the route itself.
`nexthop reject`	Specifies for packets to be dropped rather than forwarded and for unreachable messages to be sent to the packet originators. Specifying this option causes this route to be installed as a reject route.
`nexthop blackhole`	Specifies for packets to be dropped rather than forwarded. Unlike reject option, however, the blackhole option does not result in unreachable messages being sent to the packet originators.
`off`	deletes the specified static route and deletes any next hops associated with the route.
`rank default`	Specifies the rank for the specified static route the routing system uses to determine which route to use when there are routes from different protocols to the same destination. For each route, the route from the protocol with the lowest rank number is used. The default rank for static routes is 60.
`rank <0-255>`	Specifies the rank for the specified static route the routing system uses to determine which route to use when there are routes from different protocols to the same destination. For each route, the route from the protocol with the lowest rank number is used.

Use the following commands to define an existing default static route. To establish a new default route, use the commands in the preceding section to create a new static route and then use the set static-route default command to disable the old default static route.

```
set static-route default
        next hop gateway address gateway_address priority <1-8> on
        nexthop gateway logical gateway_address priority <1-8> on
        nexthop gateway address gateway_address off
        nexthop gateway logical gateway_address off
        nexthop reject
        nexthop blackhole
        ip_prefix off
        ip_prefix rank default
        ip_prefix rank <0-255>
```

Index

A

Access, Network 37

C

Certificates
  SSL 43
Certificates, SSL 41
CLI
  Editing 15
  Features 12
  Invoking 12
  Modes 12
  Movement 15
  Operations 13
Clock, Setting 31
Command
  Completion 13
  Default Values 16
  Expanding 14
  Help 15
  Recall 15
  Syntax Conventions 6
Configuration
  Save 19
Configuration Locks, Setting 17

D

Date, Configuring 30
Default Values 16
Disks, Viewing 33

E

Escape Key 15
Ethernet
  Configure a Physical Interface 24
  Interfaces 24
  Logical Interfaces 26
  Physical Interfaces 24
Exiting An Output Screen 17
Expand Commands 14

F

FTP
  Access 37

G

Getting Started Guide and Release Notes 7

H

Help With Commands 15
Host Name
  Adding 29
  Deleting 30
  Modifying 29
  Viewing 30

I

Images, IPSO 30
Interface
  Commands 21
  Delete IP Address 23
  Names 21
Interfaces, Viewing 21
Invoking The CLI 12
IPSO Images
  Managing 30

L

Logical Interface, Deleting 22

N

Network Access 37
Network Security And Access 37
Network Services 37

O

Operations, CLI 13
Output Screen, Exiting 17

P

Package 33
  Adding 35
  Deleting 36
  Upgrade 35
Private Keys, SSL 43

R

Recall, Command 15
Related Commands, Displaying 16
Release Notes 7
Routes, Static 45
Routing 45

S

Saving Configuration Changes 19
Security, Network 37
SSH 39
  Configuring Server Options 40
  Service, Enabling and Disabling 39
SSL
  Private Key and Certificate 41
  Voyager Web Access 40
Static Routes 45
Statistics, System 23
Status 23
Syntax, Command 6
System Configuration 29
System Statistics 23
System Status 23
System Tuning 36

T

Tab Key 14
TELNET
  Access 37
TFTP
  Access 37
Time, Configuring 30
Transparent Mode 28

U

Upgrading Packages 35
User Management 44

V

Voyager SSL Certificate 41
Voyager Web Access, SSL 40