## Table of Contents

### Chapter 1
**Introducing the Command-Line Interface**
- Environment Commands .................................................................................................................. 16
- Transaction Mode ................................................................................................................................. 18
- General CLI Features ............................................................................................................................ 20
- Saving Configuration Changes ............................................................................................................. 31

### Chapter 2
**Interface Commands**
- General Commands ............................................................................................................................. 34
  - Viewing All Interfaces ........................................................................................................................ 34
  - Deleting Any Logical Interface ........................................................................................................ 35
  - Viewing Tunnels ............................................................................................................................... 35
  - Viewing Status and Statistics ............................................................................................................. 35
- Routing Instances ................................................................................................................................. 37
- ARP .................................................................................................................................................... 38
  - ARP Commands ............................................................................................................................... 38
- Ethernet Interfaces ............................................................................................................................... 41
  - Physical Ethernet Interfaces ............................................................................................................ 41
  - Logical Ethernet Interfaces .............................................................................................................. 43
  - Transparent Mode ............................................................................................................................. 49
  - Configuring Transparent Mode .......................................................................................................... 49
- Link Aggregation ................................................................................................................................ 52
  - Configuring Link Aggregation ........................................................................................................... 52
- Link Redundancy .................................................................................................................................. 57
  - Configuring Link Redundancy ........................................................................................................... 58
- Point-to-Point Over Ethernet ................................................................................................................. 59
  - Configuring Profiles .......................................................................................................................... 59
  - Configuring PPPoE Logical Interface ................................................................................................. 60
  - Configuring PPPoE Physical Interface ............................................................................................... 61
- Loopback Interfaces ............................................................................................................................... 64
  - Logical Loopback Interfaces ............................................................................................................. 64
  - Logical or Physical Loopback Interfaces .......................................................................................... 65
- Tunnels .................................................................................................................................................. 66
- Modem Interfaces ................................................................................................................................. 70

### Chapter 3
**System Configuration Commands**
- System Configuration Summary .......................................................................................................... 75
- Configuring Banner and Login Messages ............................................................................................. 76
- Configuring DHCP ................................................................................................................................. 77
  - DHCP Service Commands .................................................................................................................. 77
  - Configuring DHCP Clients .................................................................................................................. 77
  - Configuring DHCP Servers .................................................................................................................. 79
Disk Mirroring Commands ................................................................. 135
  Configuring Disk Mirroring ................................................................. 135
NTP ........................................................................................................... 137
  Configuring NTP ................................................................................ 137
Package Commands ............................................................................. 141
  Managing Packages ........................................................................... 141
Advanced System Tuning Commands ..................................................... 144
  Controlling Sequence Validation ....................................................... 144
  Tuning the TCP/IP Stack ................................................................. 144
  Router Alert IP Option ................................................................. 144
  IP1260 Port Optimization ............................................................. 144

Chapter 4
High Availability Commands
  External Load Balancer Command ..................................................... 148
VRRP Commands .................................................................................. 149
  General VRRP Commands ............................................................... 149
  Simplified Method Monitored-Circuit VRRP .................................... 151
  Full Method Monitored-Circuit VRRP ............................................. 153
  VRRPv2 ......................................................................................... 155

Chapter 5
IP Clustering Commands
  General Clustering Commands .......................................................... 160
  Clustering Administration ............................................................... 172
    Managing Join-Time Shared Features ........................................... 173
    Configuring Join-Time Shared Features ........................................ 173
    Installing IPSO Images on a Cluster .............................................. 174

Chapter 6
SNMP Commands
  SNMP Description ............................................................................. 178
  SNMP Command Set ......................................................................... 179
  Enabling/Disabling and Setting SNMP .............................................. 181
  Enabling and Disabling SNMP Traps ............................................... 184
  Managing SNMP Users .................................................................... 187
  Show SNMP Implementation and Trap Commands ........................ 188
  SNMP Error Messages ..................................................................... 189

Chapter 7
IPv6 Commands
  Configuration Summary .................................................................... 194
  Interface Commands .......................................................................... 195
  Neighbor Discovery Protocol ........................................................... 197
  IPv6 to IPv4 ..................................................................................... 199
  IPv6 Over IPv4 ................................................................................ 200
  IPv6 Routing Configuration ............................................................ 201
    RIPng ........................................................................................ 201
    Route Aggregation ....................................................................... 202
Network Security and Access Commands

Network Access and Services .................................................................................. 220
Licenses ..................................................................................................................... 224
  Configuring Software Licenses ........................................................................... 224
IPsec Commands (IPSO Implementation) ................................................................. 226
  General IPsec Commands .................................................................................. 226
  Proposal Commands .......................................................................................... 226
  Filter Commands ................................................................................................. 228
  Certificate Commands ....................................................................................... 230
  Policy Commands ............................................................................................... 235
  Rule Commands ................................................................................................. 237
  Miscellaneous IPsec Commands ........................................................................... 241
AAA ........................................................................................................................... 244
  Viewing AAA Configuration ............................................................................... 244
  Configuring Service Modules ............................................................................ 244
  Configuring Service Profiles .............................................................................. 245
  Configuring Authentication Profiles ................................................................... 247
  Configuring Account Profiles ............................................................................. 250
  Configuring Session Profiles ............................................................................. 251
  Configuring RADIUS ......................................................................................... 253
  Configuring TACPLUS ....................................................................................... 255
SSH ........................................................................................................................... 258
  Enabling/Disabling SSH Service ........................................................................ 258
  Configuring Server Options ............................................................................... 258
  Configuring and Managing SSH Key Pairs ......................................................... 265
Voyager Web Access (SSL) ........................................................................................ 269
  Enabling SSL Voyager Web Access ................................................................... 269
  Generating a Certificate and Private Key ........................................................... 270
  Installing a Certificate and Private Key ............................................................... 272
Password and Account Management ........................................................................ 273
Users and Roles Management .................................................................................. 278
  Managing System Users ...................................................................................... 278
  Managing Roles ................................................................................................... 280
  Changing the Admin and Monitor Password ..................................................... 282
  Configuring S/Key for Admin and Monitor ......................................................... 283
  Show Commands .................................................................................................. 284
Group Management .................................................................................................. 285
  Managing Groups ................................................................................................. 285
  Show Commands ................................................................................................... 285
VPN Acceleration ..................................................................................................... 286
  Configuring VPN Acceleration .......................................................................... 286
Chapter 9

Routing Commands

Route Map Commands ................................................................. 289
Set Routemap Commands ......................................................... 290
Show Routemap Commands ...................................................... 297
Routemap Protocol Commands ................................................ 297
Supported Route Map Statements by Protocol............................ 298
Route Map Examples .................................................................. 300
Multiple Routing Instances .......................................................... 304
BGP .......................................................................................... 305
External BGP ............................................................................ 306
BGP Peers ................................................................................. 307
BGP Confederations ................................................................. 312
BGP Route Reflection .............................................................. 313
BGP Route Dampening ............................................................ 314
Internal BGP ............................................................................ 316
BGP Communities ..................................................................... 323
BGP Show Commands .............................................................. 323
OSPF ....................................................................................... 324
OSPF Areas .............................................................................. 324
OSPF Interfaces ........................................................................ 327
OSPF Virtual Links ................................................................. 332
OSPF Global Settings .............................................................. 334
OSPF Show Commands ............................................................ 336
RIP .......................................................................................... 343
RIP Interfaces ........................................................................... 343
General RIP Properties .......................................................... 343
RIP Show Commands .............................................................. 345
IGRP ....................................................................................... 347
General IGRP Properties ........................................................ 347
IGRP Interfaces ....................................................................... 348
IGRP Show Commands ............................................................ 351
IGMP ....................................................................................... 352
IGMP Commands ...................................................................... 352
IGMP Show Commands ............................................................ 354
PIM .......................................................................................... 356
PIM Interfaces ........................................................................... 356
PIM With IP Clustering ........................................................... 356
Sparse Mode PIM ................................................................. 356
Timer and Assert Rank Parameters for Dense Mode and Sparse Mode 358
Show PIM Commands .............................................................. 364
Static Multicast Routes ............................................................ 366
Route Aggregation ................................................................. 368
BOOTP .................................................................................... 371
BOOTP Interfaces ................................................................. 371
BOOTP Show Commands ....................................................... 371
DVMRP .................................................................................... 373
Configuring CPU Utilization Reports ........................................................... 436
Configuring Memory Utilization Reports ....................................................... 437
Configuring Interface Linkstate Reports ...................................................... 438
Configuring Rate Shaping Bandwidth Reports .............................................. 439
Configuring Interface Throughput Reports ................................................... 439
Useful System Information ............................................................................. 442
Displaying Useful System Statistics ............................................................ 442
Displaying Interface Settings ...................................................................... 442
Displaying System Logs ............................................................................. 442
Displaying Interface Traffic and Error Statistics ........................................... 444
Displaying the Interface Monitor ................................................................. 446
Displaying Resource Statistics .................................................................... 446
Displaying the Forwarding Table ................................................................. 447
Displaying Hardware Monitors ......................................................................... 449
Displaying a Temperature Sensor Information .............................................. 449
Displaying a Watchdog Timer Information .................................................... 450
Displaying Voltage Sensor Information ......................................................... 451
Displaying Power Supply Information .......................................................... 452
Displaying Fan Sensor Information ............................................................. 453
Displaying a Network Interface Card Slot Status ........................................... 454
Chapter 1
Introducing the Command-Line Interface

This chapter describes the configuration, administration, and monitoring tasks you can perform using the Check Point 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. See Chapter 5, “IP Clustering Commands” for information about administering a cluster.

   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 one of the procedures explained in the next section.

   **Note** - Check Point recommends that you press q instead of Ctrl-C to return to the CLI prompt. Under certain circumstances, entering Ctrl-C repeatedly might result in the system dumping a core file and exiting the CLI.

   If this occurs and there are configuration changes that you have not saved that you want to save, restart the CLI by entering clish and then entering save config at the CLI prompt.
In This Chapter

Invoking the CLI  page 14
IPSO Shell Options for CLI Commands  page 15
Environment Commands  page 16
Transaction Mode  page 18
Output Formats  page 18
General CLI Features  page 20
Saving Configuration Changes  page 31

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.

<table>
<thead>
<tr>
<th>Execute From</th>
<th>To Implement</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPSO shell</td>
<td>Enter clish to invoke the CLI shell. The prompt changes, and you can then enter CLI commands.</td>
<td>Lets you enter any CLI commands in an interactive mode with help text and other helpful CLI features.</td>
</tr>
<tr>
<td>IPSO shell</td>
<td>Enter clish -c &quot;cli_command&quot;</td>
<td>Lets you execute a single CLI command. You must place double-quotiation marks around the CLI command</td>
</tr>
</tbody>
</table>
| 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. |
**IPSO Shell Options for CLI Commands**

In addition to the `-c` and `-f` options, the IPSO shell supports the following command-line options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-d</code></td>
<td>Sets the debug level; Enter an integer from 0 to 5 as the parameter</td>
</tr>
<tr>
<td><code>-o</code></td>
<td>Sets output format; enter either <code>pretty</code>, <code>structured</code>, or <code>xml</code></td>
</tr>
<tr>
<td><code>-s</code></td>
<td>Use with <code>-c</code> or <code>-f</code> to force a permanent configuration save. For example, enter <code>clish -s -f filename</code> or <code>clish -s -c &quot;cli_command&quot;</code></td>
</tr>
<tr>
<td><code>-i</code></td>
<td>Use before <code>-f</code> option to continue loading commands from a file even if a command within the file fails</td>
</tr>
</tbody>
</table>
Environment Commands

Use the following commands to set an environment for a particular session to modify the .cshrc file to set the environment permanently:

```bash
set clienv
  debug <0-5>
  echo-cmd <on | off>
  on-failure <stop | continue>
  output <pretty | structured | xml>
  prompt name
  rows integer
  syntax-check <on | off>
  save clienv
```

**Arguments**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug &lt;0-5&gt;</td>
<td>Specifies the debug level. Level 0 specifies not to perform any debugging, to display error messages only. Level 5 specifies the highest level of debugging. 0</td>
</tr>
<tr>
<td>echo-cmd &lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td>on-failure &lt;stop</td>
<td>continue&gt;</td>
</tr>
<tr>
<td>output &lt;pretty</td>
<td>structured</td>
</tr>
</tbody>
</table>
**Environment Commands**

**prompt name**  
Specifies the appearance of the command prompt. To set the prompt back to the default, use the keyword default.

**rows integer**  
Specifies the number of rows to display on your console. Specified by your console or xterm window.

**syntax-check**  
Specifies to put the shell into syntax-check only mode. Commands you enter are checked syntactically and are not executed, but values are validated.

**save clienv**  
Specifies to save the environment variables that the user modifies with the `set clienv` commands.

Use the following commands to view the environment settings on your system.

```
show clienv
  debug
  echo-cmd
  output
  on-failure
  output
  rows
  syntax-check
```

**Arguments**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug</td>
<td>Displays the configured debug level.</td>
</tr>
<tr>
<td>echo-cmd</td>
<td>Displays whether or not echo-cmd is enabled.</td>
</tr>
<tr>
<td>on-failure</td>
<td>Displays whether or not on-failure is enabled.</td>
</tr>
<tr>
<td>output</td>
<td>Displays the configured output.</td>
</tr>
<tr>
<td>rows</td>
<td>Displays the number of screen rows configured.</td>
</tr>
<tr>
<td>syntax-check</td>
<td>Displays whether or not syntax-check is enabled.</td>
</tr>
</tbody>
</table>
## Transaction Mode

You can use transaction mode to enter a series of CLI commands that are executed as a group. This mode is particularly useful if you want to use configuration scripts and don’t want to commit changes to the configuration database unless all the commands in the group are executed successfully.

When transaction mode is active, you can enter as many CLI commands as you want. The commands are executed but not committed to the configuration database, and you see an error message if a command fails. You can have a script look for error messages and roll back (undo) all the changes if it detects any errors.

To start transaction mode, enter

```
start transaction
```

[Xact] is appended to the prompt to let you know that transaction mode is active.

Enter changes that should be implemented as a group.

To implement changes made in transaction mode and commit them to the configuration database, enter

```
commit
```

To roll back the changes you just made in transaction mode, enter

```
rollback
```

After you enter commit or rollback, the CLI leaves transaction mode.

## Output Formats

CLI supports three output formats: pretty, structured, and xml. Use the -o option at the command line to set one of the supported formats, except for pretty output, which is the default. For example, to enter the CLI shell and print output in xml format, enter clish -o xml from the IPSO shell.

The pretty mode generates output, as in the following example:

```
User admin
  gid 0
  home /var/admin
  passwd $1$J9..w8j$yBA/JaVED1rk2DiPm1XHF
  realname Admin
  shell /bin/csh
  uid 0
```
The structured mode generates output, as in the following example:

```
User;Admin;
gid;0
home;/var/admin;
passwd;$1$J9..w8j$7BA/JaVEDlrk2DiPm1XHF/;
realname;Admin;
shell;bin/csh;
uid;0;
```

The xml mode generates output that is embedded in xml, as in the following example:

```
<user> admin
    <gid>0</gid>
    <home>/var/admin</home>
</user>
```
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,

  ```
  Nokia> set vrrp <Space><Tab>
  accept-connections - Accept-connections
  coldstart-delay - Coldstart-Delay
  interface - Interface
  Nokia> set vrrp
  ```

- 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, as shown in the following example.

```
Nokia> set in<Esc><Esc>
set inatmarp holdoff-time VALUE
set inatmarp keep-time VALUE
set inatmarp max-retries VALUE
set inatmarp timeout VALUE
set interface VALUE [ vlanid VALUE logical-name VALUE comments VALUE ]
set interface VALUE [ vlanid VALUE logical-name VALUE disable enable ]
set interface VALUE logical-name VALUE
set interface VALUE status VALUE
set interface VALUE vc-max VALUE
.
.
.
```

**Viewing Related Commands**

Use the following command to display all the available commands for a combination of operation and feature.

```
show commands [ op <value> ] [ feature <value>]
```

**Arguments**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>op &lt;value&gt;</td>
<td>Displays commands for the particular operation you enter. The range is show, set add, and delete.</td>
</tr>
<tr>
<td>feature &lt;value&gt;</td>
<td>Displays commands for the specific feature you enter, for example, bgp or snmp.</td>
</tr>
</tbody>
</table>
For example, if you enter

```
show commands op set feature interface
```

the system responds

```
set interface VALUE [ vlanid VALUE logical-name VALUE comments VALUE ]
set interface VALUE [ vlanid VALUE logical-name VALUE disable enable ]
set interface VALUE logical-name VALUE
set interface VALUE status VALUE
set interface VALUE vc-max VALUE
set interface VALUE vcs VALUE
```

You can also omit specifying an operation. If you do so, the system displays all of
the commands that are valid for the specified feature. For example, if you enter

```
show commands feature interface
```

the system lists all of the commands that you can use to manage interfaces.

**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 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.
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.

For example:
Nokia> set ipsec?
Commands to configure IPsec.

Nokia> set ipsec log-level?
Verbosity of the logs generated.
Can be ERROR, DEBUG or INFO. Default value is ERROR

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.

Executing Previous Commands

The following list shows the history commands you can enter that execute complete commands:

- **history**—displays the last 100 commands.
- **!!**—executes the most recent command.
- **!nn**—in which nn is the number of a specific command from the history list, executes a previous command.
- **!-nn**—in which nn is the nth previous command. For example, entering !-3 executes the third from the last command.
- **!str**—executes the most recent command starts with str.
- **!\?str\?**—executes the most recent command containing str. The trailing ? may be omitted if str is followed immediately by a new line.
- **!!:s/str1/str2** —repeats the last command, replacing str1 with str2.
Reusing Parts of Commands

You can combine word designators with history commands to refer to specific words used in previous commands. Words are numbered from the beginning of the line with the first word being denoted by 0. Use a colon to separate a history command from a word designator. For example, you could enter `!!:1` to refer to the first argument in the previous command. In the command `show interfaces`, `interfaces` is word 1.

- 0—The operation word.
- n—The nth word.
- ^—The first argument; that is, word 1.
- $—The last argument.
- %—The word matched by the most recent `\?str\?` search.

Immediately after word designators, you can add a sequence of one or more of the following modifiers, each preceded by a colon:

- p—Print the new command but do not execute.
- s/str1/str2—Substitute new for the first occurrence of old in the word being referred to.
- g—Apply changes over the entire command. Use this modified in conjunction with s, as in `gs/str1/str2`.

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.
General CLI Features

- 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.

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 the Inactivity Timeout

Use the following commands to configure IPSO to time out (end) a CLI or shell session after a specified period of inactivity (a period in which there is no typing and no active foreground process).

Note - Executing these commands does not affect the current CLI or shell session.

```plaintext
set inactivity-timeout
  minutes
  Hh
  HhMm
show inactivity-timeout
```

Arguments

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>minutes</td>
<td>Specifies the number of minutes of inactivity before a timeout occurs.</td>
</tr>
<tr>
<td></td>
<td>0 (no timeout)</td>
</tr>
<tr>
<td>Hh</td>
<td>Specifies the number of hours of inactivity before a timeout occurs.</td>
</tr>
<tr>
<td></td>
<td>0 (no timeout)</td>
</tr>
<tr>
<td>HhMm</td>
<td>Specifies the number of hours and minutes of inactivity before a timeout occurs.</td>
</tr>
<tr>
<td></td>
<td>0 (no timeout)</td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th>&lt;on</th>
<th>off&gt;</th>
<th>Specifies whether to enable or disable configuration lock. When you enable config-lock, the default timeout value is 300 seconds.</th>
</tr>
</thead>
<tbody>
<tr>
<td>off</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>on timeout &lt;5-900&gt;</th>
<th>Specifies to enable config-lock for the specified interval in seconds.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>on override</th>
<th>Specifies to override an existing config-lock and thus disable config-lock.</th>
</tr>
</thead>
</table>

### Monitoring the File System and Processes

Use the following commands to monitor the system’s file system and processes and to view memory capacity.

```
show fsinfo
show processes
show swapinfo
```

**Arguments**

<table>
<thead>
<tr>
<th>fsinfo</th>
<th>Displays the number of file systems, the directories in which they are mounted, and their capacity.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>processes</th>
<th>Displays the currently running processes</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>swapinfo</th>
<th>Displays the amount of memory available for swapping into the kernel.</th>
</tr>
</thead>
</table>
Loading Commands From a File

You can execute a series of CLI commands from a text file. The file can contain only commands and comments. Each comment line must begin with the pound character (#). To split a command between multiple lines, type an escape character (\) at the end of each line. Do not type any characters, including spaces, after the escape character.

You can create and edit the file on the IPSO system using the VI text editor. You can also create the file on a remote system and copy the file to the IPSO system using FTP.

For example, you could create a file `foo.txt` that contains a series of CLI commands. To execute the commands in the file from the IPSO shell (not the CLI) you would enter:

```
IPSO[admin]# clish -f foo.txt
```

This assumes that `foo.txt` is in the `/var/admin` directory, which is the default directory for `admin`. If the command file is in a different directory or if you have changed to a different directory, modify the path accordingly.

The `-f` option allows the system to read commands from a file. You can also use the `-i` option to force the system to ignore errors in the results of the commands. The CLI normally stops reading commands from a file when a command fails.

You could execute the commands in `foo.txt` from the CLI by entering:

```
Nokia> load foo.txt
```

If you want the CLI to ignore errors in the results of commands and continue executing the commands in the file, enter the following command before loading the file:

```
Nokia> set clienv on-failure continue
```

Reset the CLI to stop on errors by entering:

```
Nokia> set clienv on-failure stop
```

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.
Chapter 2

Interface Commands

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

In This Chapter

General Commands ........................................ page 34
Routing Instances ........................................ page 37
Ethernet Interfaces ........................................ page 41
Link Aggregation .......................................... page 52
Link Redundancy .......................................... page 57
Loopback Interfaces ...................................... page 64
Tunnels ....................................................... page 66
Modem Interfaces ......................................... page 70
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
\texttt{show interfaces}

\textit{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 \texttt{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.

<table>
<thead>
<tr>
<th>if_name</th>
<th>Physical or logical interface name is acceptable.</th>
</tr>
</thead>
<tbody>
<tr>
<td>phys_if_name</td>
<td>Only a physical interface name is acceptable. Physical interface names are assigned by the system and cannot be changed.</td>
</tr>
<tr>
<td>log_if_name</td>
<td>Only a logical interface name is acceptable. The default name for a logical interfaces is the name of the physical interface with \texttt{cunit_number} appended (in which \texttt{unit_number} uniquely identifies the logical interface). For example, the default name for the first logical interface created for physical Ethernet interface \texttt{eth-s1p1} is \texttt{eth-s1p1c0}. You can change the logical names of interfaces.</td>
</tr>
</tbody>
</table>
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 IP system 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. See the section in this chapter on the appropriate type of physical interface for information about how to do this.

Viewing Tunnels

To see information about all the VPN tunnels configured on a system, enter

```
show tunnels
```

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 an interface and whether the interface is active, enter

```
show interface if_name all
```
Routing Instances

You can configure multiple virtual routers (called routing instances) on your IP system. Each routing instance has its own routing table and forwarding table. Using instances allows you to control or prevent the system from routing traffic or sharing routing information between the virtual routers.

A physical interface can have logical interfaces in multiple routing instances, but a given logical interface/address family combination can only apply to one instance.

Address family refers to IPv4 and IPv6 addresses. For example, assume that you have configured two routing instances—A and B. If interface eth-s1/s1p1c0 has IPv4 addresses in instance A, it cannot also have IPv4 addresses in instance B. However, it can have an IPv6 address in instance B (or A).

All of the following combinations are valid for a given logical interface:

- IPv4 address(es) in instance A and IPv6 address in instance A
- IPv4 address(es) in instance B and IPv6 address in instance B
- IPv4 address(es) in instance A and IPv6 address in instance B
- IPv4 address(es) in instance B and IPv6 address in instance A

The following combinations are not valid for a given logical interface:

- IPv4 address(es) in instances A and B
- IPv6 address in instances A and B

If a logical interface can have multiple IPv4 IP addresses (such as an ethernet logical interface), this is also true when the interface belongs to a routing instance. For example (continuing with the previous example), an ethernet logical interface can have multiple IPv4 IP addresses in instance A.
This section contains commands to configure the Address Resolution Protocol (ARP).

**ARP Commands**

Use the following commands to configure global ARP behavior.

```plaintext
set arp
  keep-time <60–86400>
  retry-limit <1–100>
  accept-multicast-replies <on | off>
  mirroring <on | off>
```

Use the following commands to show the current ARP settings.

```plaintext
show arp
  keep-time
  retry-limit
  accept-multicast-replies
  mirroring
  all
```

**Arguments**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Shows all the current configuration settings.</td>
</tr>
<tr>
<td>keep-time &lt;60–86400&gt;</td>
<td>Specifies or shows the number of seconds to keep resolved dynamic ARP entries. If an entry is not referred to and is not used by traffic before the time elapses, it is deleted (and the system will have to send a new request for the MAC address before it can send traffic to the interface). 14400 seconds (4 hours).</td>
</tr>
<tr>
<td>retry-limit &lt;1–100&gt;</td>
<td>Specifies or shows the number of times to retry ARP requests (up to once per second) until holding off requests for the holdoff time (20 seconds). 3</td>
</tr>
</tbody>
</table>
### ARP Commands

Use the following commands to add proxy and static ARP addresses.

**add**

```
arpproxy address ip_address <macaddress mac_address | interface log_if_name>
arpstatic address ip_address macaddress mac_address
```

#### Arguments

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>arpproxy address</td>
<td>A proxy ARP entry makes this system respond to ARP requests for ip_address with mac_address or log_if_name. mac_address must be a valid MAC address (on this system) with six hexadecimal octets separated by colons. If you use the interface argument, log_if_name must be the logical name of an interface. (If the relevant physical interface has more than one logical interface, you must use the first logical interface.) If you use this argument, the system responds to ARP requests for ip_address with the MAC address of the interface specified by log_if_name. Proxy ARP entries will not be used when forwarding packets.</td>
</tr>
<tr>
<td>interface</td>
<td>Specifies or shows whether the router accepts ARP replies with a multicast address. off</td>
</tr>
<tr>
<td>mirroring</td>
<td>Specifies or shows whether the VRRP-enabled interfaces on VRRP backup routers have the same ARP information as the master. 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. off</td>
</tr>
</tbody>
</table>
Use the following commands to show the current proxy, static, and dynamic ARP entries.

```
show arpproxy all
show arpstatic all
show arpdynamic all
```

**Arguments**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>arpproxy all</code></td>
<td>Shows all the proxy ARP entries for the system.</td>
</tr>
<tr>
<td><code>arpstatic all</code></td>
<td>Shows all the static ARP entries for the system.</td>
</tr>
<tr>
<td><code>arpdynamic all</code></td>
<td>Shows all the dynamic ARP entries for the system.</td>
</tr>
</tbody>
</table>

Use the following commands to delete ARP addresses.

```
delete
    arpproxy address ip_address
    arpstatic address ip_address
```
Ethernet Interfaces

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

**Note** - Ethernet is the only interface type supported by the IP2250 and IP2255 platforms.

### Physical Ethernet Interfaces

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

```plaintext
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

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>`speed &lt;10M</td>
<td>100M</td>
</tr>
<tr>
<td>`duplex &lt;full</td>
<td>half&gt;`</td>
</tr>
<tr>
<td>`auto-advertise &lt;on</td>
<td>off&gt;`</td>
</tr>
<tr>
<td><code>link-recog-delay &lt;1–255&gt;</code></td>
<td>Specifies how many seconds a link must be before the system declares the interface is up.</td>
</tr>
<tr>
<td>`flow-control &lt;on</td>
<td>off&gt;`</td>
</tr>
<tr>
<td>`active &lt;on</td>
<td>off&gt;`</td>
</tr>
<tr>
<td><code>status</code></td>
<td>Shows whether the physical interface is active.</td>
</tr>
<tr>
<td>`udld-enable &lt;on</td>
<td>off&gt;`</td>
</tr>
<tr>
<td><strong>10M</strong></td>
<td></td>
</tr>
<tr>
<td><strong>half</strong></td>
<td></td>
</tr>
<tr>
<td><strong>on</strong></td>
<td></td>
</tr>
<tr>
<td><strong>6</strong></td>
<td></td>
</tr>
<tr>
<td><strong>off</strong></td>
<td></td>
</tr>
<tr>
<td><strong>on</strong></td>
<td></td>
</tr>
<tr>
<td><strong>off</strong></td>
<td></td>
</tr>
</tbody>
</table>
descriptive_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 acceptable values are 128, 256, and 512.
Logical Ethernet Interfaces

comments
vlanid
logical-name
mss
mtu
rx-ringsize
tx-ringsize
instance

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.

daddress
ip_address/<0–31>  Specifies the IP address and subnet mask length for the logical interface.

instance name  Specifies the routing instance that this address belongs to. If you do not specify an instance, the address will belong to the default instance.
Transparent Mode

Use transparent mode to allow your IPSO appliance to behave like a layer 2 device such as a bridge. Benefits of this type of network configuration include being able to maintain your current local area network configuration or maintain your existing IP address with your ISP.

Using transparent mode, you configure Ethernet interfaces (including aggregated interfaces) on IP Appliance platforms to behave like ports on a bridge. The interfaces then forward traffic using layer 2 addressing. You can configure some interfaces to use transparent mode while other interfaces on the same platform are configured normally. Traffic between transparent mode interfaces is inspected at layer 2 while traffic between normal interfaces, or between transparent and normal interfaces, is inspected at layer 3.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>logical-name</td>
<td>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.</td>
</tr>
<tr>
<td>new_log_if_name</td>
<td>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.</td>
</tr>
<tr>
<td>enable</td>
<td>Enables or disables the logical interface.</td>
</tr>
<tr>
<td>disable</td>
<td>Enables or disables the logical interface.</td>
</tr>
<tr>
<td>mss &lt;536-65535&gt;</td>
<td>Specifies the maximum segment size to advertise. 536</td>
</tr>
<tr>
<td>MTU &lt;1500-16,000&gt;</td>
<td>Specifies the maximum transfer unit for the interface. 1500 The value must be an integer.</td>
</tr>
<tr>
<td>rx-ringsize &lt;1-1024&gt;</td>
<td>Specifies the buffer ring size on the receiving side. The value must be a multiple of 8. Note: Network connectivity will be lost on the interface for which this value is changed. Users should re-login.</td>
</tr>
<tr>
<td>tx-ringsize &lt;1-1024&gt;</td>
<td>Specifies the buffer ring size on the transmitting side. The value must be a multiple of 8. Note: Network connectivity will be lost on the interface for which this value is changed. Users should re-login.</td>
</tr>
</tbody>
</table>

For “show interface”, displays the ring size on the receiving side.

For “show interface”, displays the ring size on the transmitting side.
**Note** - Transparent mode does not provide complete bridging functionality such as loop detection or spanning tree.

**Configuring Transparent Mode**

Use the following commands to create a transparent mode groups and add an interface to a transparent mode group.

```sh
add xmode
  id <1-2147483647>
  interface logical_if_name
  filter encap <DIX | LLC | SNAP> proto hex_value action
  <forward | discard>
```

Use the following commands to delete a transparent mode group and delete an interface from a transparent mode group.

```sh
delete xmode id <1-2147483647>
  interface logical_if_name
  filter encap <DIX | LLC | SNAP> proto hex_value action
  <forward | discard>
```

Use the following commands to configure a transparent mode group.

```sh
set xmode id <1-2147483647>
  state <on | off>
  vrrp_enabled <on | off>
  cross-connect-enabled <on | off>
```

Use the following commands to view transparent mode configurations.

```sh
show
  xmode id <1-2147483647> cross-connect-enabled
  xmode id <1-2147483647> info
  xmode id <1-2147483647> interfaces
  xmode id <1-2147483647> filters
  xmode id <1-2147483647> stat
  xmode id <1-2147483647> state
  xmode id <1-2147483647> vrrp_enabled
```
Transparent Mode

```markdown
xmodes
instance

Arguments

id <1-2147483647> Specifies an integer associated with a transparent mode group. When you use the argument with the `add xmode` command, you create a transparent mode group.

interface
logical_if_name Specifies the name of the logical interface, for example, `eth-s1p1c0`.

filter encap <DIX | LLC | SNAP> Specifies the Ethernet frame encapsulation for the filter you are creating or deleting.

proto hex_value Specifies the hexadecimal value of the protocol that is forwarded or dropped by the filter. Do not include “0x” before the hexadecimal value.

action <forward | discard> Specifies whether a filter should forward or discard the specified traffic.

state <on | off> Enables or disables a transparent mode group.

Default: off

vrrp_enabled <on | off> Enables or disables VRRP for a transparent mode group.

Default: off

cross-connect-enabled <on | off> Specifies whether traffic for protocols other than IP and ARP should be forwarded by default:

- on: Traffic other than IP and ARP should be forwarded (unless blocked by a filter).
- off: Traffic other than IP and ARP should be discarded (unless allowed by a filter).

cross-connect-enabled Shows whether traffic for protocols other than IP and ARP is being forwarded by default.

info Shows the configuration of the specified transparent mode group.

interfaces Shows the interfaces associated with the specified transparent mode group.
```
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>stat</td>
<td>Shows the statistics associated with the specified transparent mode group.</td>
</tr>
<tr>
<td>state</td>
<td>Shows the state of the specified transparent mode group—0 for disabled and 1 for enabled.</td>
</tr>
<tr>
<td>vrrp_enabled</td>
<td>Show whether VRRP is enabled or disabled on the specified transparent mode group—0 disabled and 1 for enabled.</td>
</tr>
<tr>
<td>xmodes</td>
<td>Shows the configuration of all transparent mode groups on the platform.</td>
</tr>
</tbody>
</table>
Transparent Mode

Use transparent mode to allow your IPSO appliance to behave like a layer 2 device such as a bridge. Benefits of this type of network configuration include being able to maintain your current local area network configuration or maintain your existing IP address with your ISP.

Using transparent mode, you configure Ethernet interfaces (including aggregated interfaces) on IP Appliance platforms to behave like ports on a bridge. The interfaces then forward traffic using layer 2 addressing. You can configure some interfaces to use transparent mode while other interfaces on the same platform are configured normally. Traffic between transparent mode interfaces is inspected at layer 2 while traffic between normal interfaces, or between transparent and normal interfaces, is inspected at layer 3.

Note - Transparent mode does not provide complete bridging functionality such as loop detection or spanning tree.
Note - The IP2250 and IP2255 platforms do not support transparent mode.

Configuring Transparent Mode

Use the following commands to create a transparent mode groups and add an interface to a transparent mode group.

add xmode
  id <1-2147483647>
  interface logical_if_name
  filter encap <DIX | LLC | SNAP> proto hex_value action <forward | discard>

Use the following commands to delete a transparent mode group and delete an interface from a transparent mode group.

delete xmode id <1-2147483647>
  interface logical_if_name
  filter encap <DIX | LLC | SNAP> proto hex_value action <forward | discard>

Use the following commands to configure a transparent mode group.

set xmode id <1-2147483647>
  state <on | off>
  vrrp_enabled <on | off>
  cross-connect-enabled <on | off>
Use the following commands to view transparent mode configurations.

```bash
show
xmode id <1-2147483647> cross-connect-enabled
xmode id <1-2147483647> info
xmode id <1-2147483647> interfaces
xmode id <1-2147483647> filters
xmode id <1-2147483647> stat
xmode id <1-2147483647> state
xmode id <1-2147483647> vrrp_enabled
xmodes
```

**Arguments**

- **id <1-2147483647>** Specifies an integer associated with a transparent mode group. When you use the argument with the `add xmode` command, you create a transparent mode group.

- **interface logical_if_name** Specifies the name of the logical interface, for example, eth-s1p1c0.

- **filter encap <DIX | LLC | SNAP>** Specifies the Ethernet frame encapsulation for the filter you are creating or deleting.

- **proto hex_value** Specifies the hexadecimal value of the protocol that is forwarded or dropped by the filter. Do not include “0x” before the hexadecimal value.

- **action <forward | discard>** Specifies whether a filter should forward or discard the specified traffic.

- **state <on | off>** Enables or disables a transparent mode group.

- **vrrp_enabled <on | off>** Enables or disables VRRP for a transparent mode group.
### cross-connect-enabled <on | off>

Specifies whether traffic for protocols other than IP and ARP should be forwarded by default:

- **on**: Traffic other than IP and ARP should be forwarded (unless blocked by a filter).
- **off**: Traffic other than IP and ARP should be discarded (unless allowed by a filter).

### cross-connect-enabled

Shows whether traffic for protocols other than IP and ARP is being forwarded by default.

### info

Shows the configuration of the specified transparent mode group.

### interfaces

Shows the interfaces associated with the specified transparent mode group.

### stat

Shows the statistics associated with the specified transparent mode group.

### state

Shows the state of the specified transparent mode group—0 for disabled and 1 for enabled.

### vrrp_enabled

Shows whether VRRP is enabled or disabled on the specified transparent mode group—0 disabled and 1 for enabled.

### xmodes

Shows the configuration of all transparent mode groups on the platform.
You can aggregate (combine) Ethernet ports so that they function as one logical port with higher bandwidth. For example, if you aggregate two 10/100 mbps ports, they function as a single port with a theoretical bandwidth of 200 mbps. Another benefit of link aggregation is redundancy—if one of the physical links in an aggregated group fails, the other physical links remain active and the logical link continues to function.

You can specify a minimum number of ports that must be active for the logical interface to remain active. If the number of active ports is less than this number, the logical interface is deactivated. This option is particularly useful in VRRP configurations. For example, you might have a VRRP pair in which both the master and backup systems use two aggregated Gigabit Ethernet ports as their external connection. If one of the Gigabit Ethernet ports in the master fails, you probably would prefer that the backup system becomes the master so that there is no loss of bandwidth in the external connection. In this case, you would set the minimum number of active ports to be two.

To configure link aggregation, you create an aggregation group and then add interfaces to it. When you add an interface to an aggregation group, its configuration information is deleted. Be careful not to aggregate the interface that you are using for your CLI connection because doing so breaks your connection to the appliance.

When interfaces participate in an aggregation group, you cannot configure them individually—you configure the group instead, using the appropriate interface commands. When you use interface commands, use the format ae xx for the physical interface and the format ae xx c0 for the logical interface. For example, the physical name of a group with the ID 10 is ae 10 and its logical name is ae 10 c0.

You must configure an aggregation group with an IP address and so on. You cannot configure an aggregation group with logical information until you have added an interface to the group.

**Configuring Link Aggregation**

Use the following commands to create, configure, delete, and view link aggregation information.

add linkaggregation
Configuring Link Aggregation

```
  group <1-1024>
  port phys_if_name [type primary]
set linkaggregation
  group <1-1024>
  min_ports number_of_ports
delete linkaggregation
  group <1-1024>
  port phys_if_name
```

**Arguments**

- **group <1-1024>**
  Creates or specifies an aggregation group with the specified ID.

- **port phys_if_name**
  Specifies a physical interface to add to or delete from an aggregation group. You must delete all the ports from a group before you can delete the group itself.

- **type primary**
  Specifies that this is the first port added to the group. When deleting ports, you must delete this port last.

- **min_ports number_of_ports**
  Specifies the minimum number of ports in the group that must be active for the logical interface to remain active.

1

Use the following commands to view link aggregation settings.

```
  show
  linkaggregation
  groups
  group <1-1024>
```

**Arguments**

- **linkaggregation**
  Shows how many link aggregation groups are configured.

- **groups**
  Shows the configuration information of all the link aggregation groups.
Configuring Link Aggregation

<table>
<thead>
<tr>
<th>group &lt;1–1024&gt;</th>
<th>Shows the configuration information of the specified link aggregation group.</th>
</tr>
</thead>
</table>

```
add linkaggregation
  group <1–1024>
  port phys_if_name [type primary]
set linkaggregation group <1–1024>
  lACP_mode <active | passive | off>
  lACP_timer <short | long>
  min_ports number_of_ports
  port_priority <1–65535>
  system_priority <1–65535>
  txpolicy <L2 | L3 | L4 | round-robin> <enable | disable>
```

delete linkaggregation
  group <1–1024>
  port phys_if_name

```
show
  linkaggregation
  groups
  group <1–1024>
  lACP_mode
  lACP_timer
  min_ports
  port_priority
  system_priority
  txpolicy
```

**Arguments**

<p>| group &lt;1–1024&gt; | Creates or specifies an aggregation group with the specified ID. |</p>
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>port phys_if_name</td>
<td>Specifies a physical interface to add to or delete from an aggregation group. You must delete all the ports from a group before you can delete the group itself.</td>
</tr>
<tr>
<td>type primary</td>
<td>Specifies that this is the first port added to the group. When deleting ports, you must delete this port last.</td>
</tr>
<tr>
<td>lacp_mode &lt;active</td>
<td>Specify <strong>active</strong> to enable dynamic link aggregation and configure the interfaces in the aggregation group to send LACP control traffic repeatedly. Check Point recommends that you use this setting.</td>
</tr>
<tr>
<td></td>
<td>Specify <strong>passive</strong> to enable dynamic link aggregation and configure the interfaces in the aggregation group to send LACP control traffic only in the following circumstances:</td>
</tr>
<tr>
<td></td>
<td>• An interface needs to provide information about itself to the other end of the link (as happens when an interface becomes active and receives a packet).</td>
</tr>
<tr>
<td></td>
<td>• When a configuration setting changes on the interface.</td>
</tr>
<tr>
<td></td>
<td>Specify <strong>off</strong> to disable dynamic link aggregation.</td>
</tr>
<tr>
<td>lacp_timer &lt;short</td>
<td>Specifies how long IPSO should wait for LACP control packets to determine whether to drop inactive interfaces from a link aggregation group:</td>
</tr>
<tr>
<td></td>
<td>• <strong>short</strong>: IPSO expects to receive an LACP control packet every 30 seconds on each physical interface in the link aggregation group. If it does not receive a control packet on an interface within 30 seconds, it drops the interface from the group.</td>
</tr>
<tr>
<td></td>
<td>• <strong>long</strong>: IPSO expects to receive an LACP control packet every 90 seconds on each physical interface in the link aggregation group. If it does not receive a control packet on an interface within 90 seconds, it drops the interface from the group.</td>
</tr>
<tr>
<td></td>
<td>Shows how many link aggregation groups are configured.</td>
</tr>
</tbody>
</table>
Configuring Link Aggregation

**min_ports number_of_ports**

Specifies the minimum number of ports in the group that must be active for the logical interface to remain active.

1

**port_priority <1–65535>**

Specifies a port priority value. This value identifies all the physical interfaces in the link aggregation group. This value is only an identifier—it does not provide any prioritization of any kind.

**system_priority <1–65535>**

Specifies a system priority value. This value identifies the IPSO system to the device at the other end of the link (which might be connected to other devices on which LACP is enabled). This value is only an identifier—it does not provide any prioritization of any kind.

**txpolicy <L2 | L3 | L4 | round-robin> <enable | disable>**

Specifies a method for distributing outgoing traffic between the aggregated interfaces.

- Round Robin: IPSO distributes the outgoing traffic across all the physical interfaces equally.
- L2: IPSO distributes the outgoing traffic across the physical interfaces using hash values based on the destination MAC addresses of packets. This is not a suitable choice if the other end of the link is another router (because all packets will have the same destination MAC address).
- L3: IPSO distributes the outgoing traffic across the physical interfaces using hash values based on the destination IP addresses of packets. This is not a suitable choice if all packets have the same destination IP address (as might be the case if NAT is used at the other end of the link).
- L4: IPSO distributes the outgoing traffic across the physical interfaces using hash values based on the destination TCP or UDP port numbers.

**round-robin**

**Note** - The device at the other end of the link does not need to use the same method for distributing traffic between its aggregated ports.
Link Redundancy

You can configure redundant Ethernet interfaces for resiliency purposes. For example, if you create a link redundancy group that includes two physical interfaces and the active interface fails, the second interface takes over and there is no interruption in service. You might want to use this feature if your IPSO platform is connected to a switch that does not support link aggregation.

There are significant differences between link redundancy (Ethernet bonding) and link aggregation:

- There is no load balancing within a link redundancy group—only one of the interfaces in a group is active at a given time.
- The interfaces in a link redundancy group do not need to be configured identically. For example, they can have different speeds and duplicity settings.
- You can include a link aggregation group within a redundancy group, but a redundancy group cannot be part of an aggregation group.

You can combine interfaces from different network interface cards in a single link redundancy group, and you can create as many as eight link redundancy groups per system. Each group can include as many as eight interfaces. (If you include a link aggregation group, it counts as one redundancy interface regardless of how many physical ports are in the aggregation group.) An interface can participate in only one redundancy group.

On IP2250 and IP2255 platforms, link redundancy is subject to the same constraints as link aggregation:

- Do not include interfaces on different ADP I/O cards in the same link redundancy group.
- Do not combine any of the built-in Ethernet management interfaces with interfaces on an ADP I/O card to form a redundancy group.
- You can combine management interfaces to create a redundancy group.

When you create a link redundancy group, you must designate a primary interface. This is the default active interface—if the primary interface fails and later returns to service it becomes the active interface again. For this reason you should configure the fastest interface in the group to be the primary interface.

All the interfaces in a link redundancy group must connect to the same device at the other end of the link. You cannot configure a single redundancy group across multiple switches.
Configuring Link Redundancy

Use the following commands to create, configure, and delete a link redundancy group.

add linkredundancy
  group <1–1024>
  port phys_if_name
delete linkredundancy
  group <1–1024>
  port phys_if_name

Arguments

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>group &lt;1–1024&gt;</td>
<td>Creates or specifies a redundancy group with the specified ID.</td>
</tr>
<tr>
<td>port phys_if_name</td>
<td>Specifies a physical interface to add to or delete from a redundancy group. You must delete all the ports from a group before you can delete the group itself.</td>
</tr>
</tbody>
</table>

Use the following commands to view link redundancy settings.

show linkredundancy
  groups
  group <1–1024>

Arguments

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>linkredundancy</td>
<td>Shows how many link redundancy groups are configured.</td>
</tr>
<tr>
<td>groups</td>
<td>Shows the configuration information of all the link redundancy groups.</td>
</tr>
<tr>
<td>group &lt;1–1024&gt;</td>
<td>Shows the configuration information of the specified link redundancy group.</td>
</tr>
</tbody>
</table>
Point-to-Point Over Ethernet

Use the commands explained in this section to configure Point-to-Point Over Ethernet (PPPoE).

Configuring Profiles

Use the following commands to add a profile without authentication.

```
add pppoe profile name profile_name interface phys_if_name mode
<connect-on-demand | keep-alive> noauth
  timeout  <30-259200; 300, 60>
  peername name
  description name
  mss  mss_value
  mtu  <136-1492>
```

Use the following commands to add a profile with authentication.

```
add pppoe profile name profile_name interface phys_if_name mode
mode_name username name password password
  authtype PAP | CHAP CASE
  timeout  <30-259200; 300, 60>
  peername name
  description name
  mss  mss_value
  mtu  <136-1492>
```

Use the following commands to modify a profile without authentication.

```
set pppoe profile name profile_name interface phys_if_name mode
mode_name noauth
  timeout  time_in_seconds
  peername name
  description name
  mtu  mtu_value
```

Use the following commands to modify a profile with authentication.

set pppoe profile name profile_name interface phys_if_name mode mode_name username name password password
  authtype PAP | CHAP CASE
  timeout time_in_seconds
  peername name
  description name
  mtu mtu_value

Use the following command to delete a profile.
dele te pppoe profile name profile_name

Note - You cannot delete a pppoe profile if it is associated with a logical interface. You must first delete the pppoe logical interface. See “Configuring PPPoE Logical Interface” on page 60.

Use the following command to view profiles.
show pppoe profile
  all
  name profile_name

**Configuring PPPoE Logical Interface**

Use the following commands to add or configure a logical pppoe interface in dynamic mode.
add interface pppoe0 mode dynamic profile-name profile_name
  interface-name log_if_name
  enable off | on
set interface pppoe0 mode dynamic profile-name profile_name
  interface-name log_if_name
  enable off | on

Use the following commands to add or configure a logical pppoe interface in static mode.
add interface pppoe0 mode static local-ipaddress ip_address
remote-ipaddress ip_address profile-name profile_name
  interface-name log_if_name
  enable off | on
set interface pppoe0 mode static local-ipaddress ip_address
remote-ipaddress ip_address profile-name profile_name
  interface-name log_if_name
  enable off | on
interface-name log_if_name
enable off | on

Use the following commands to add or configure a logical pppoe interface in unnumbered mode.
add interface pppoe0 mode unnumbered logical-interface log_if_name profile-name profile_name
  interface-name log_if_name
  enable off | on
set interface pppoe0 mode unnumbered logical-interface log_if_name profile-name profile_name
  interface-name log_if_name
  enable off | on

Use the following command to delete the pppoe logical interface.
delete interface log_if_name

Use the following command to modify the pppoe logical interface.
set interface log_if_name
  admin-status enable | disable
  link_trap on | off

**Configuring PPPoE Physical Interface**

Use the following command to modify the pppoe physical interface.
set interface pppoe0
  admin-status enable | disable
  link_trap on | off

**Arguments**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>profile name</td>
<td>The name used to identify the profile with the associated logical interface. The profile name may be 1 to 31 characters long.</td>
</tr>
<tr>
<td>interface phys_if_name</td>
<td>Specifies the physical ethernet interface.</td>
</tr>
</tbody>
</table>
### Configuring PPPoE Physical Interface

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>mode</strong> &lt;connect-on-demand</td>
<td>Specifies the available connection modes.</td>
</tr>
<tr>
<td>keep-alive&gt;</td>
<td>• connect-on-demand: The interface comes up when IP traffic is generated.</td>
</tr>
<tr>
<td></td>
<td>• keep-alive: The interface is always up.</td>
</tr>
<tr>
<td><strong>noauth</strong></td>
<td>Specifies no authentication will be used.</td>
</tr>
<tr>
<td><strong>authtype</strong> &lt;PAP</td>
<td>If you specify an authentication type, you must also specify the user name and password.</td>
</tr>
<tr>
<td></td>
<td>CASE&gt;</td>
</tr>
<tr>
<td><strong>username</strong> user_name</td>
<td>Specifies the user name when using authentication. The user name may be 1 to 63 characters long</td>
</tr>
<tr>
<td><strong>password</strong> pass_word</td>
<td>Specifies the password the user must log in with. The password may be 1 to 31 characters long.</td>
</tr>
<tr>
<td><strong>timeout</strong> &lt;30-259200;</td>
<td>If the mode is connect-on-demand, the specified timeout indicates idle timeout. If the mode is keep-alive, the specified timeout indicates connection check period. If no value is specified, the system will use 300 seconds for idle timeout and a value of 300 seconds for connection check period.</td>
</tr>
<tr>
<td>300&gt;</td>
<td><strong>peername</strong> name</td>
</tr>
<tr>
<td><strong>description</strong> name</td>
<td>Specifies an identity that the user may use to remember the profile.</td>
</tr>
<tr>
<td><strong>mss</strong> mss_value</td>
<td>Specifies the size in bytes of the maximum segment size.</td>
</tr>
<tr>
<td><strong>mtu</strong> &lt;136-1492&gt;</td>
<td>Specifies the size in bytes of the maximum transmission unit.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>mode</strong></td>
<td>Specifies how the logical interface will be assigned an IP address.</td>
</tr>
<tr>
<td><strong>local-ipaddress</strong></td>
<td>Used with mode static command to specify the local interface address.</td>
</tr>
<tr>
<td><strong>remote-ipaddress</strong></td>
<td>Used with mode static command to specify the remote interface address.</td>
</tr>
<tr>
<td><strong>enable</strong></td>
<td>Enables or disables the logical interface.</td>
</tr>
<tr>
<td><strong>admin-status</strong></td>
<td>Enable or disable the logical interface.</td>
</tr>
<tr>
<td><strong>link_trap</strong></td>
<td>Enable or disable the link-trap for the logical interface.</td>
</tr>
</tbody>
</table>

**mode**

- **unnumbered**: The interface does not have its own unique IP address. Instead, another interface address is used.
  
  **Note** - When using the unnumbered command, the Ethernet interface used in the logical-interface variable must have an IP address associated with it.

- **dynamic**: The interface is not configured with any IP address because the address is assigned by the peer during session establishment.

- **static**: The local and remote IP addresses must be configured. Use dotted-quad format, for example, 10.0.93.1.
Loopback Interfaces

If you do not explicitly assign an OSPF router ID, the system will automatically use the address of one of the installed interfaces as the router ID. If the interface that has that address assigned to it goes down, the system will have to tear down and rebuild its OSPF configuration with a new router ID. To prevent this from happening, you can assign an IP address to a loopback interface (which will not go down). The system will choose this address as the router ID instead of using the address of one of the installed interfaces.

You may also want to assign an IP address to a loopback interface so that you can use the loopback interface as the proxy interface for an unnumbered interface. Again, the benefit of using the loopback interface as a proxy is that it will not go down.

Logical Loopback Interfaces

Use the commands explained in this section to configure logical loopback interfaces.

```
add interface log_if_name address ip_address [instance name]
delete interface log_if_name address ip_address [instance name]
set interface log_if_name logical-name log_name
show interface log_if_name addresses
```
Logical or Physical Loopback Interfaces

Use the commands explained in this section to configure logical or physical loopback interfaces.

```
show interface if_name
  status
  disabled,proto
  enabled,proto
  all
```

**Arguments**

<table>
<thead>
<tr>
<th>instance name</th>
<th>Specifies the routing instance that this address belongs to. If you do not specify an instance, the address will belong to the default instance.</th>
</tr>
</thead>
<tbody>
<tr>
<td>if_name</td>
<td>You can specify the logical or physical name of the interface.</td>
</tr>
<tr>
<td>status</td>
<td>Displays whether the interface is active or not.</td>
</tr>
<tr>
<td>disabledPROTO</td>
<td>Displays protocols that are not enabled for the interface.</td>
</tr>
<tr>
<td>enabledPROTO</td>
<td>Displays protocols that are enabled for the interface.</td>
</tr>
<tr>
<td>all</td>
<td>Displays all configuration options for the interface.</td>
</tr>
</tbody>
</table>
Tunnels

Tunnels are point-to-point links that transport packets from a source interface to a destination interface.

Use the following commands to create tunnels by using a specified encapsulation scheme. For GRE and DVMRP tunnels, add an interface with this encapsulation first and then set the tunnel endpoints with a separate `set` command. To encapsulate IPv4 packets in IPv6 tunnels or IPv4 packets in IPv6 tunnels, use the `add` command to select the interface and specify the tunnel endpoint addresses. You can specify other optional arguments depending on the encapsulation scheme you select.

```
add interface phys_if_name encapsulation
dvmrp
gre
    v6inv4 address ip_address remote ip_address [local-link-local linklocal_address] [remote-link-local linklocal_address] [ttl <1–255>] [instance name]
v4inv6 address ip6_address remote ip6_address
destination <ip_address | ip_address> [instance name]
```

**Arguments**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface phy_if_name</td>
<td>Specifies the physical tunnel interface name. The value must be a tunnel that exists on the system.</td>
</tr>
<tr>
<td>gre</td>
<td>Specifies a GRE tunnel.</td>
</tr>
<tr>
<td>dvmrp</td>
<td>Specifies a DVMRP tunnel.</td>
</tr>
<tr>
<td>v6inv4</td>
<td>Specifies a tunnel that encapsulates IPv6 packets in IPv4 packets. This argument allows you to connect IPv6 enabled interfaces (typically on different systems) over existing IPv4 connections.</td>
</tr>
<tr>
<td>v4inv6</td>
<td>Specifies a tunnel that encapsulates IPv4 packets in IPv6 packets. This argument allows you to connect IPv4 enabled systems over existing IPv6 connections.</td>
</tr>
</tbody>
</table>
Use the following commands to configure properties for existing tunnels:

```
set interface if_name
  interface-binding <on | off>
  local-endpoint <ip_address | ip6_address> <enable | disable>
  address <ip_address | ip6_address> destination
  <ip_address | ip6_address> remote-endpoint
  <ip_address | ip6_address>
```

- **address <ipv4_address | ip6_address>**
  Specifies the interface address of the local tunnel endpoint. If you use IPv6 in IPv4 encapsulation, the local address is in IPv4 address format. For IPv4 in IPv6 encapsulation, use a valid IPv6 address format:
  - IPv4 example: 192.168.50.5
  - IPv6 example: 2222::1:2:3

- **destination <ipv4_address | ip6_address>**
  Specifies the interface address of the remote tunnel endpoint. If you use IPv6 in IPv4 encapsulation, the destination address is in IPv4 address format. For IPv4 in IPv6 encapsulation, use a valid IPv6 address format:
  - IPv4 example: 192.168.80.8
  - IPv6 example: 2222::4:5:6

- **local-link-local linklocal_address**
  Specifies the link-local address of the local interface to which the local end of the tunnel is bound. This argument is optional. If you specify an address, it should be unique. In other words, it should not be a link-local address that already exists on your system.
  Example: FE80::32

- **remote-link-local linklocal_address**
  Specifies the link-local address of the interface on the remote system to which the remote end of the tunnel is bound. This argument is optional. If you specify an address, it should be unique. In other words, it should not be a link-local address that already exists on the remote system.
  Example: FE80::52

- **ttl <1-225>**
  Specifies the time to live of packets sent on the tunnel. This argument is optional.
## Arguments

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface if_name</td>
<td>Specifies the logical tunnel interface name. The value must be a tunnel that exists on the system:</td>
</tr>
<tr>
<td></td>
<td>• Example: tun0c3</td>
</tr>
<tr>
<td>interface-binding</td>
<td>Specifies whether to bind a tunnel to an outgoing interface.</td>
</tr>
<tr>
<td>on/ off</td>
<td>• on: Bind the tunnel to the interface.</td>
</tr>
<tr>
<td></td>
<td>• off: Do not bind the tunnel to the interface.</td>
</tr>
<tr>
<td>local-endpoint</td>
<td>Specifies the IPv6 or IPv4 address of the local interface to which the local end of the tunnel is bound. Disabling the tunnel will not delete the configured address information.</td>
</tr>
<tr>
<td>&lt;ip_address</td>
<td>ip6_address&gt; &lt;enable</td>
</tr>
<tr>
<td>address</td>
<td>Specifies the address of the local tunnel endpoint. If the tunnel uses IPv6 in IPv4 encapsulation, the local address will be in IPv4 address format. For IPv4 in IPv6 encapsulation, use a valid IPv6 address format:</td>
</tr>
<tr>
<td>&lt;ipv4_address</td>
<td>ip6_address&gt;</td>
</tr>
<tr>
<td>destination</td>
<td>Specifies the address of the remote tunnel endpoint. If the tunnel uses IPv6 in IPv4 encapsulation, the destination address will be in IPv4 address format. For IPv4 in IPv6 encapsulation, use a valid IPv6 address format:</td>
</tr>
<tr>
<td>&lt;ipv4_address</td>
<td>ip6_address&gt;</td>
</tr>
<tr>
<td>remote-endpoint</td>
<td>Specifies the IPv6 or IPv4 address of the interface on the remote system to which the remote end of the tunnel is bound.</td>
</tr>
<tr>
<td>&lt;ipv4_address</td>
<td>ip6_address&gt;</td>
</tr>
</tbody>
</table>

Use the following command to delete a specified logical tunnel:

```bash
delete interface if_name
```
Use the following commands to view properties for existing tunnels.

```
show interface VALUE interface-binding
```

```
show interface VALUE { local-endpoint lname state encapsulation address destination remote-endpoint }
```

Use the following commands to view summary information about the IPv6 tunnels configured on your system:

```
show ipv6 tunnels
```
Modem Interfaces

Use the following commands to enable dialup access to the system through a modem and view the current modem settings.

`set modem <com2 | com3 | com4>`
- `country-code <<0–99> | <00–FF>>`  
- `enable | disable`  
- `inactivity-timeout <0–5>`  
- `poll-interval <0–59>`  
- `dialback <on | off>`  
- `dialback-number phone_num`  
- `type <5oC1 | 5oC2> [country-code <<0–99> | <00–FF>>]`  
- `rings < 1 – 4 >`  

`show modem <com2 | com3 | com4>`
- `active`  
- `inactivity-timeout`  
- `poll-interval`  
- `dialback`  
- `dialback-number`  
- `rings`  
- `country-code`  
- `status`  
- `all`

**Arguments**

| `com2 | com3 | com4` | Specifies the communications port that the modem is using. |
|-------|--------|-------------------------------------------------------------|
| `enable | disable` | Enables or disables the modem using the specified communications port. |
| `active` | Shows whether the modem on the specified port is active. |
### Modem Interfaces

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>inactivity-timeout</strong> <code>&lt;0–5&gt;</code></td>
<td>Specifies or shows the number of minutes that a call on the modem can remain inactive (no traffic sent or received) before the call is disconnected. Setting the value to 0 disables the timer, and calls will never be disconnected because of inactivity.</td>
</tr>
<tr>
<td><strong>poll-interval</strong> <code>&lt;0–59&gt;</code></td>
<td>Specifies or shows the number of minutes between modem “line status” tests. The system will test whether the modem is present and online once every interval. If a modem is not detected or is offline, an appropriate message appears in syslog. Setting the value to 0 disables the test.</td>
</tr>
<tr>
<td><strong>dialback</strong> `&lt;on</td>
<td>off&gt;`</td>
</tr>
<tr>
<td><strong>dialback-number</strong> <code>phone_num</code></td>
<td>Specifies or shows the number that the system will call after it drops an incoming call. You can enter commas to cause the dialing to pause briefly. To increase the length of the pause, enter multiple adjacent commas, as in 650,,555,,1212.</td>
</tr>
<tr>
<td><strong>type</strong> `&lt;5oC1</td>
<td>5oC2&gt;`</td>
</tr>
<tr>
<td><strong>country-code</strong> `&lt;0–99</td>
<td>00–FF&gt;`</td>
</tr>
<tr>
<td><strong>rings</strong></td>
<td>Specifies or shows the number of rings after which the modem answers an incoming call.</td>
</tr>
<tr>
<td><strong>status</strong></td>
<td>Shows whether there is a modem on the specified port.</td>
</tr>
</tbody>
</table>
Chapter 3
System Configuration Commands

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

In This Chapter

System Configuration Summary  page 75
Configuring Banner and Login Messages  page 76
Configuring DHCP  page 77
Backup and Restore Files  page 88
Schedule Jobs Through Crontab File  page 100
System Failure Notification Configuration  page 103
DNS  page 104
Static Host Address Assignment Configuration  page 106
Host Name Configuration  page 108
Managing IPSO Images  page 109
Downloading IPSO Images  page 111
Managing Configuration Sets  page 113
Mail Relay Configuration  page 115
System Logging Configuration  page 116
Optional Disk Configuration (Flash-Based Systems)  page 123
Core-Dump Server Configuration (Flash-Based Systems)  page 125
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date and Time Configuration</td>
<td>127</td>
</tr>
<tr>
<td>Disk Commands</td>
<td>134</td>
</tr>
<tr>
<td>Disk Mirroring Commands</td>
<td>135</td>
</tr>
<tr>
<td>NTP</td>
<td>137</td>
</tr>
<tr>
<td>Package Commands</td>
<td>141</td>
</tr>
<tr>
<td>Advanced System Tuning Commands</td>
<td>144</td>
</tr>
</tbody>
</table>
**System Configuration Summary**

Use the following command to view the configuration summary:

```
show summary
```

**Arguments**

<table>
<thead>
<tr>
<th>show summary</th>
<th>Displays the configuration of the platform.</th>
</tr>
</thead>
</table>
Configuring Banner and Login Messages

Use the following commands to configure a banner message, an FTP welcome message, and a “message of the day” (MOTD) that users see when they log in using the command line.

```
set message
    banner <on | off> [msgvalue "message"]
    ftpwelcome <on | off> [msgvalue "message"]
    motd <on | off> [msgvalue "message"]
delete message
    all
    banner
    ftpwelcome
    motd
show message
    all [status]
    banner [status]
    ftpwelcome [status]
    motd [status]
```

**Arguments**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>banner</strong></td>
<td>Specifies the banner message that users see when they connect to the system (before they log in) or when they log out.</td>
</tr>
<tr>
<td><strong>ftpwelcome</strong></td>
<td>Specifies the message that users see when they log into the system using FTP.</td>
</tr>
<tr>
<td><strong>motd</strong></td>
<td>Specifies the message that users see when they log into the system using the command line.</td>
</tr>
<tr>
<td><strong>all</strong></td>
<td>Specifies all the messages.</td>
</tr>
<tr>
<td><strong>[msgvalue “message”]</strong></td>
<td>Specifies the text of the message.</td>
</tr>
<tr>
<td>**&lt;on</td>
<td>off&gt;**</td>
</tr>
<tr>
<td><strong>[status]</strong></td>
<td>Displays whether a message is enabled or disabled.</td>
</tr>
</tbody>
</table>
Configuring DHCP

Use the following commands to configure DHCP clients and DHCP servers.

**DHCP Service Commands**

Use the following commands to select the type of DHCP service.

```
set dhcp service
  server
  client
  relay
  none

show dhcp service

show dhcp server all
```

**Arguments**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>server</td>
<td>Specifies that the server process will be configured on the appliance.</td>
</tr>
<tr>
<td>client</td>
<td>Specifies that the client process will be configured on the appliance.</td>
</tr>
<tr>
<td>none</td>
<td>No DHCP process is specified. None is the default.</td>
</tr>
</tbody>
</table>

**Configuring DHCP Clients**

Use the following commands to add a DHCP client configuration.

```
add dhcp client interface logical_name
  clientid name
  hostname name
  timeout <0-4294967295, 60>
  retry <0-4294967295, 300>
  leasetime <0-4294967295>
```
reboot <0-4294967295, 10>

Use the following commands to change a DHCP client configuration.

set dhcp client interface logical_name
  clientid name
  hostname name
  timeout <0-4294967295, 60>
  retry <0-4294967295, 300>
  leasetime <0-4294967295>
  reboot <0-4294967295, 10>
  enable
  disable

Use the following command to delete DHCP client configurations.

delete dhcp client interface logical_name

Use the following commands to view DHCP client configurations.

show dhcp client
  interface logical_name
  interfaces

Arguments

client interface logical_name
Associates a logical Ethernet interface for the DHCP client to send and receive DHCP messages and configuration parameters from a DHCP server.

clientid name
Creates a unique identifier that is used in place of the MAC address of the client.

hostname name
Creates a hostname for the client. If you do not specify a host name, the server will name the client.

timeout <0-4294967295, 60>
Specifies a time limit, in seconds, for the client to gain an IP address from the server. The default is 60 seconds.

retry <0-4294967295, 300>
Specifies a time, in seconds, to retry contacting a server. The default is 300 seconds.

leasetime <0-4294967295>
Specifies the time, in seconds, for which the client requests an IP address. No default.
Configuring DHCP Servers

Use the following commands to configure DHCP servers.

**Configuring Subnets**

Use the following commands to create subnets.

```
add dhcp server subnet ip_address netmask <1-32>
  default-gateway ip_address
  default-lease <0-4294967295, 43200>
  max-lease <0-4294967295, 43200>
  domain name
  dns ip_address
  ntp ip_address
  tftp name | ip_address
  wins ip_address
  ddserver ip_address
  note-type <B-node, P-node, M-node, H-node>
  scope name
  zone name
  swap name | ip_address
```

Use the following commands to change subnet configurations.

```
set dhcp server subnet ip_address netmask <1-32>
```
default-gateway ip_address
default-lease <0-4294967295, 43200>
max-lease <0-4294967295, 43200>
domain name
dns ip_address
ntp ip_address
tftp name | ip_address
wins ip_address
ddserver ip_address
note-type <B-node, P-node, M-node, H-node>
scope name
zone name
swap name | ip_address
enable | disable

Use the following commands to view subnet configurations.
show dhcp server
  subnets
  subnet ip_address

Use the following commands to delete subnets.
delete dhcp server
  subnets
  subnet ip_address

Arguments

add dhcp server subnet
  ip address netmask
  <1-32> Specifies the subnet where the server will listen for DHCP messages from clients.

default-gateway
  ip_address Specifies the default gateway clients will use.

default-lease
  <0-4294967295, 43200> Specifies the IP address lease time, in seconds, that clients will be given if clients do not request a specific lease time. The default is 43200 seconds.
max-lease <0-4294967295, 43200>

Specifies the maximum IP address lease time, in seconds, that clients will be given regardless of client requests. The default is 43200 seconds.

domain name

Specifies the domain name clients will be given, for example, client_name.checkpoint.com.

dns ip_address

Specifies the Domain Name Server (DNS) servers for clients, in order of precedents. Use commas to separate addresses, for example, 195.163.25.3, 195.163.24.1, 195.163.23.5, etc.

ntp ip_address

Specifies the Network Time Protocol (NTP) servers for clients, in order of precedents. Use commas to separate addresses, for example, 195.163.25.3, 195.163.24.1, 195.163.23.5, etc.

tftp name | ip_address

Specifies the Trivial File Transfer Protocol (TFTP) servers for clients. Use a dotted-quad address or a valid hostname.

wins ip_address

When configuring NetBIOS, specifies the Windows Internet Naming Server (WINS) servers for clients, in order of precedents. Use commas to separate addresses, for example, 195.163.25.3, 195.163.24.1, 195.163.23.5, etc.

ddserver ip_address

When configuring NetBIOS, specifies the Datagram Distribution (DD) servers for clients, in order of precedents. Use commas to separate addresses, for example, 195.163.25.3, 195.163.24.1, 195.163.23.5, etc.

node-type <B-node, H-node, M-node, P-node>

When configuring NetBIOS, specifies the nodetype the client should designate itself.

- B-node: Only broadcast on the local network for NetBIOS resolution and advertising.
- H-node: Unicast to WINS servers. If this fails, broadcast.
- M-node: Broadcast on local network, unicast to WINS server.
- P-node: Only unicast to WINS server for NetBIOS resolution and advertising.
### Configuring DHCP Servers

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>scope name</code></td>
<td>When configuring NetBIOS, specifies the scope for the client.</td>
</tr>
<tr>
<td><code>zone name</code></td>
<td></td>
</tr>
<tr>
<td>`swap name</td>
<td>ip_address`</td>
</tr>
<tr>
<td>`enable</td>
<td>disable`</td>
</tr>
<tr>
<td><code>add dhcp server subnet ip_address pool start ip_address end ip_address</code></td>
<td>Creates a pool of addresses to be leased to clients. The start and end addresses of the pool must belong to the subnet being configured.</td>
</tr>
<tr>
<td><code>subnets</code></td>
<td>When used with the show command, displays all the DHCP subnets configured on the appliance. When used with the delete command, deletes all the DHCP subnets configured on the appliance.</td>
</tr>
<tr>
<td><code>subnet ip_address</code></td>
<td>When used with the show command, displays the DHCP subnet specified. When used with the delete command, deletes the DHCP subnet specified.</td>
</tr>
</tbody>
</table>

### Configuring Fixed-IP Addresses

Use the following commands to assign an IP address to a specific host.

```
add dhcp server host name
  clientid name
  mac-address mac_address
  address ip_address
  domain name
  file file_name
  dns ip_address
  ntp ip_address
  smtp name
  tftp name | ip_address
  root file_name
  extension file_name
  time value
```
swap ip_address

Use the following commands to enable or change fixed-ip address configuration.
set dhcp server host name
    enable | disable
    clientid name
    mac-address mac-address
    address ip_address
    domain name
    file file_name
    dns ip_address
    ntp ip_address
    smtp ip_address
    tftp name | ip_address
    root file_name
    extension file_name
    time <-43200 to 43200>
    swap ip_address

Use the following commands to delete fix-ip configurations.
delete dhcp server
    hosts
    host hostname

Use the following commands to view fixed-ip configurations.
show dhcp server
    hosts
    host hostname

Arguments

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dhcp server host name</td>
<td>Specifies the host name for the client using the fixed-ip address.</td>
</tr>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>
### Configuring DHCP Servers

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>clientid name</strong></td>
<td>Specifies a client name which will be used by the server in place of the MAC address of the client.</td>
</tr>
<tr>
<td><strong>mac-address mac_address</strong></td>
<td>Specifies the MAC address of the client. If clientid is configured, the clientid will take precedence.</td>
</tr>
<tr>
<td><strong>address ip_address</strong></td>
<td>Specifies the IP address to be assigned to the client.</td>
</tr>
<tr>
<td><strong>domain name</strong></td>
<td>Specifies the domain name for the client will be given, for example, client_name.checkpoint.com.</td>
</tr>
<tr>
<td><strong>file file_name</strong></td>
<td>Specifies the bootfile name for the client.</td>
</tr>
<tr>
<td><strong>dns ip_address</strong></td>
<td>Specifies the Domain Name System (DNS) servers for the client, in order of precedents. Use commas to separate addresses, for example, 195.163.25.3, 195.163.24.1, 195.163.23.5, etc.</td>
</tr>
<tr>
<td><strong>ntp ip_address</strong></td>
<td>Specifies the Network Time Protocol (NTP) servers for the client, in order of precedents. Use commas to separate addresses, for example, 195.163.25.3, 195.163.24.1, 195.163.23.5, etc.</td>
</tr>
<tr>
<td><strong>smtp ip_address</strong></td>
<td>Specifies the Simple Mail Transfer Protocol (SMTP) servers that are available to the client. Use commas to separate addresses, for example, 195.163.25.3, 195.163.24.1, 195.163.23.5, etc.</td>
</tr>
<tr>
<td>**tftp name</td>
<td>ip_address**</td>
</tr>
<tr>
<td><strong>root file_name</strong></td>
<td>Specifies the full path name to be used as the root disk partition for the client.</td>
</tr>
<tr>
<td><strong>extension file_name</strong></td>
<td>Specifies the full path name of the file that contains additional options for the client.</td>
</tr>
<tr>
<td><strong>time &lt;-43200 to 43200&gt;</strong></td>
<td>Specifies the time zone offset, in seconds, from the coordinated universal time the client should use. A positive offset indicates a location east to zero meridian, and a negative offset indicates a location west to zero meridian.</td>
</tr>
</tbody>
</table>
Configuring DHCP Servers

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>wins ip_address</td>
<td>When configuring NetBIOS, specifies the Windows Internet Naming Server (WINS) servers for clients, in order of precedents. Use commas to separate addresses, for example, 195.163.25.3, 195.163.24.1, 195.163.23.5, etc.</td>
</tr>
<tr>
<td>ddservr ip_address</td>
<td>When configuring NetBIOS, specifies the Datagram Distribution (DD) servers for clients, in order of precedents. Use commas to separate addresses, for example, 195.163.25.3, 195.163.24.1, 195.163.23.5, etc.</td>
</tr>
<tr>
<td>node-type</td>
<td>When configuring NetBIOS, specifies the nodetype the client should designate itself.</td>
</tr>
<tr>
<td>scope name</td>
<td>When configuring NetBIOS, specifies the scope for the client.</td>
</tr>
<tr>
<td>swap name</td>
<td>Specifies the server which provides a swap space for clients. Use a dotted-quad address or valid hostname.</td>
</tr>
<tr>
<td>hosts</td>
<td>All hosts with fixed-ip addresses.</td>
</tr>
<tr>
<td>host name</td>
<td>Specific host named in the variable.</td>
</tr>
</tbody>
</table>

**Configuring Dynamic Domain Name System (DDNS) Service**

Use the following commands to create an initial DDNS configuration, and enable or disable the configuration.

```plaintext
cmd
set dhcp server ddns
  update-style <none | interm>
  ttl <0-255>
  enable | disable
```
Use the following commands to create a DDNS key configuration.
add dhcp server ddns key name
    algorithm HMAC-MD5-SIG-ALG.REG.INT | none
    secret value

Use the following commands to change a DDNS key configuration.
set dhcp server ddns key name
    algorithm HMAC-MD5-SIG-ALG.REG.INT | none
    secret name

Use the following commands to delete a DDNS key configuration.
delete dhcp server key name

Use the following commands to view DDNS key configurations.
show dhcp server
    keys
    key name

Arguments

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>update-style</td>
<td>Specifies the update style for DDNS.</td>
</tr>
<tr>
<td>ttl &lt;0-255)</td>
<td>Specifies the time to live value, in seconds, for DNS update messages.</td>
</tr>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
<tr>
<td>dhcp server ddns key name</td>
<td>Specifies the key name identifier when used with the add command.</td>
</tr>
<tr>
<td>algorithm HMAC-MD5-SIG-ALG.REG.INT</td>
<td>none</td>
</tr>
<tr>
<td>secret value</td>
<td>Secret to be matched by DNS server for this key.</td>
</tr>
<tr>
<td>keys</td>
<td>Shows all keys.</td>
</tr>
<tr>
<td>key name</td>
<td>Shows specified key.</td>
</tr>
</tbody>
</table>

Configuring Dynamic Domain Name System (DDNS) Zones

Use the following commands to create a DDNS zone.
add dhcp server zone name key name primary ip_address
Use the following commands to change DDNS zone configurations.

```bash
set dhcp server zone name key name primary ip_address
secondary ip_address
enable | disable
```

Use the following commands to delete DDNS zones.

```bash
delete dhcp server
zones
zones name
```

Use the following commands to view DDNS key configurations.

```bash
show dhcp server
zones
zone name
```

**Arguments**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dhcp server zone name</td>
<td>Specifies zone name, associates a key and the primary DNS server. Optionally you can specify a secondary DNS server.</td>
</tr>
<tr>
<td>key name primary ip_address</td>
<td>Enable or disables DDNS zones.</td>
</tr>
<tr>
<td>secondary ip_address</td>
<td>All configured zones.</td>
</tr>
<tr>
<td>enable</td>
<td>disable zone name</td>
</tr>
</tbody>
</table>
Backup and Restore Files

Use the following commands to configure your system to perform manual or regularly scheduled backups.

Manually Backing Up

These commands configure your system to perform a manual backup of important system files. The archive file created by a manual backup resides in the var/backup/ directory.

To perform a manual backup, first use the set backup manual command to specify, at minimum, the name of the backup archive file. You can also select optional files to include in the backup, such as log files or home directories. After you have configured the name and contents of the backup file, use the set backup manual on command to tell the system to perform the backup.

```
set backup manual
  on
  filename name
  homedirs <on | off>
  logfiles <on | off>
  package name <on | off>
```

Use the following command to delete an existing backup file from the /var/backup directory:

```
delete backup manual filename name
```

**Arguments**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>on</td>
<td>Tells the system to perform a manual backup. By default, the backup file contains all the configuration (/config), cron (/var/cron), etc (/var/etc), and IPsec files (/var/etc/ipsec). Export versions of IPSO do not include IPsec files.</td>
</tr>
</tbody>
</table>
Scheduling Backups

Use the following commands to configure your system to perform regularly scheduled backups. The archives produced by scheduled backups reside in the /var/backup/sched/ directory and are date-stamped.

When using the following commands, keep these points in mind:

- Use the add backup scheduled command to initially set up the scheduled backup. A backup can be scheduled to run daily, weekly, or monthly. You can have only one scheduled backup at a time.

- When you have finished specifying the scheduled backup, use the set backup scheduled on command to tell the system to schedule the backup for execution.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>filename name</td>
<td>Specifies the base name of the file that includes all the backed up files. You must specify this name to configure a manual backup. The system will append a date stamp to the file name you specify when it creates the backup file. When used with the delete backup manual command, specifies the name of the backup file to be deleted from the /var/backup directory.</td>
</tr>
<tr>
<td>homedirs &lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td>logfiles &lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td>package name &lt;on</td>
<td>off&gt;</td>
</tr>
</tbody>
</table>
Scheduling Backups

- You can use the `set backup scheduled` command to change the scheduled backup settings, except for changing the frequency of the backup: that is, whether it is daily, weekly, monthly. To change the frequency, you must delete the scheduled backup with the `delete backup scheduled` command and then read the scheduled backup with the `add backup scheduled` command.

- The CLI does not have a command to delete existing scheduled backup files from the `/var/backup/sched` directory. However, the system routinely deletes older backup files.

```
add backup scheduled
  filename name
  dayofmonth <1-31>
  minute <0-59>
  dayofweek <0-6>
  hour <0-23>

set backup scheduled
  on
  filename name
  hour <0-23>
  minute <0-59>
  homedirs <on | off>
  logfiles <on | off>
  package name <on | off>
  dayofmonth <1-31>
  dayofweek <0-6>
```

Use the following command to delete a previously configured scheduled backup:
```
delete backup scheduled
```
## Arguments

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>on</td>
<td>Tells the system to schedule the scheduled backup for execution. By default, the backup file contains all the configuration (/config), cron (/var/cron), etc (/var/etc), and IPsec files (/var/etc/ipsec). Export versions of IPSO do not include IPsec files.</td>
</tr>
<tr>
<td>filename name</td>
<td>Specifies the name of the file that includes all the backed up files. You must specify this name to configure a regularly scheduled backup. The system automatically appends the current date to the file name when it creates the backup file.</td>
</tr>
<tr>
<td>homedirs &lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td>logfiles &lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td>package name &lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td>dayofmonth &lt;1-31&gt;</td>
<td>Specifies which day of the month to schedule the backup. This option applies only to monthly scheduled backups.</td>
</tr>
<tr>
<td>dayofweek &lt;0-6&gt;</td>
<td>Specifies which day of the week to schedule the backup. Days are numbered 0 through 6, starting with Sunday. This option applies only to weekly scheduled backups.</td>
</tr>
<tr>
<td>hour &lt;0-23&gt;</td>
<td>Specifies which hour of the day to schedule the backup.</td>
</tr>
<tr>
<td>minute &lt;0-59&gt;</td>
<td>Specifies which minute of the day to schedule the backup.</td>
</tr>
</tbody>
</table>
Transferring Backup Files to a Remote Server

You can transfer backup files to a remote server manually or in an automated manner. To use an automated approach, configure a scheduled backup using the commands explained in “Scheduling Backups” on page 89 and use the commands described in “Configuring Automated Transfers” to configure the system to send the backup files to the remote system. To transfer backup files to a remote server manually, use the commands explained in “Transferring Backup Files Manually” on page 93.

Configuring Automated Transfers

Use the following commands to transfer your backup files to a remote server automatically. If you enable automated transfers, backup files are transferred to the remote server as soon as they are complete, assuming the server is reachable. If the remote server is not reachable, the system waits until the next backup occurs and tries again. Once they have been successfully transferred, the backup files are deleted from the system that created them.

set backup auto-transfer
  ipaddr ip_address
  protocol
    ftp ftp-dir path_name
    tftp

Use the following command to disable automatic transfers of backup files:
delete backup auto-transfer ipaddr ip_address

Arguments

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipaddr ip_address</td>
<td>Specifies or deletes the IP address of the system to which backup files should be sent.</td>
</tr>
<tr>
<td>protocol</td>
<td>Specifies to use FTP when sending backup files and also specifies the path to the location where the files will be stored. If you choose FTP, make sure that your server accepts anonymous FTP logins. You cannot use nonanonymous FTP logins to transfer backup files.</td>
</tr>
</tbody>
</table>
Transferring Backup Files Manually

Use the following commands to manually transfer your backup files to a remote server.

To transfer the backup files, first configure the transfer settings using the following commands:

```
set backup remote
   ftp-site ip_address
   ftp-dir path_name
   ftp-user name
```

Use the following command to perform the transfer after you have configured the transfer settings:

```
set backup remote <manual | scheduled> filename [ftp-passwd password]
```

If you omit the password option when a password is required, you will be prompted to enter the password after you execute the command. Your password in this case will not be echoed to the screen.

Use the following command to disable transfers to an FTP user, site, or directory:

```
delete backup remote
   ftp-site
   ftp-dir
   ftp-user
```

**Arguments**

- `ftp-site ip_addr`: Specifies the IP address of the remote server to transfer your backup files to.
- `ftp_dir path_name`: Specifies the path of the remote server's directory on which the backup files are saved.

---

Transferring Backup Files to a Remote Server

**protocol tftp**  
Specifies to use TFTP when backup files. Because TFTP does not work with TFTP servers running on many Unix-based operating systems, Check Point recommends that you use FTP unless you are sure that your TFTP server accepts writes to files that do not already exist on the server.
**Restore Files from Locally Stored Backup Files**

**set restore**

- **manual filename**
  - Specifies to restore your files to the system from a manual backup that is locally stored. Manual backups are stored in the `var/backup/` directory.

- **scheduled filename**
  - Specifies to restore your files to the system from a scheduled backup that is locally stored. Scheduled backups are stored in the `/var/backup/sched/` directory.

---

**Arguments**

**ftp-user name**

Specifies the name of the user account for connecting to the FTP site. There is no default, but if you do not specify a user account name, the anonymous account is used.

**manual filename**

Specifies the name of the manual backup file you want to transfer to the remote server.

You have the option of omitting the password argument. After you execute the command, you will be prompted for the password if you are using an non-anonymous account. The password you enter in response to the prompt will not be visible on the screen.

**scheduled filename**

Specifies the name of the scheduled backup file you want to transfer to the remote server.

You have the option of omitting the password argument. After you execute the command, you will be prompted for the password if you are using an non-anonymous account. The password you enter in response to the prompt will not be visible on the screen.

---

**Warning** - Restoring from a backup file overwrites your existing files.
Use the following commands to restore files from backup files previously stored on a remote server. See “Transferring Backup Files to a Remote Server” on page 92 for more information on how to transfer backed up files to a remote server.

```
set restore remote
  filename name
  ftp-site ip_addr
  ftp-dir path_name
  ftp-user user_name
  ftp-passwd password
```

**Arguments**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>filename name</td>
<td>Specifies to restore your files from the filename stored on the remote server.</td>
</tr>
<tr>
<td>ftp-site ip_addr</td>
<td>Specifies the IP address of the remote server on which the backup files are stored.</td>
</tr>
<tr>
<td>ftp-dir path_name</td>
<td>Specifies the Unix path to the directory on which the backup files are stored.</td>
</tr>
<tr>
<td>ftp-user user_name</td>
<td>Specifies the name of the user account for connecting to the FTP site on which the backup files are stored. If a username is not set, enter anonymous.</td>
</tr>
</tbody>
</table>
Show Backup Commands

Use the following commands to monitor your backup configuration.

```
show backup
  auto-transfer
  all
  ftp-dir
  ipaddr
  protocol
  manual
  filename
  homedirs
  logfiles
  package name
  packages
```

*Specifies the password to use when connecting to the FTP site. You must change the password whenever the FTP site, FTP directory, or FTP user are changed.*

**Warning** - Restoring from a backup file overwrites your existing files.

**Warning** - Make sure that you have enough disk space available on your Check Point platform before restoring files. If you try to restore files and you do not have enough disk space, you risk damaging the operating system.

**Note** - The system must be running the same version of the operating system and the same packages as those of the backup file(s) from which you restore file(s).
remote ftp-site
ftp-dir
ftp-user
manual filenames
scheduled filenames
scheduled filename
package name
packages
homedirs
dayofmonth
dayofweek
hour
minute
status

**Arguments**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>auto-transfer all</td>
<td>Shows all the auto-transfer settings.</td>
</tr>
<tr>
<td>auto-transfer ftp-dir</td>
<td>Shows the path name of the directory on the remote server where backed up files are stored.</td>
</tr>
<tr>
<td>auto-transfer ipaddr</td>
<td>Shows the IP address of the remote server that backed up files are stored on.</td>
</tr>
<tr>
<td>auto-transfer protocol</td>
<td>Shows the protocol used to transfer files automatically.</td>
</tr>
<tr>
<td>manual filename</td>
<td>Shows the names of the files that have been manually backed up and are stored in the /var/backup/ directory.</td>
</tr>
<tr>
<td>manual homedirs</td>
<td>Shows whether the home directories are manually backed up.</td>
</tr>
<tr>
<td>manual logfiles</td>
<td>Shows whether log files are backed up.</td>
</tr>
<tr>
<td>manual package name</td>
<td>Shows whether a specified package is backed up.</td>
</tr>
<tr>
<td>manual packages</td>
<td>Shows the names of the package files that have been manually backed up and are stored in the /var/backup/ directory.</td>
</tr>
</tbody>
</table>
### Show Backup Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>remote ftp-site</td>
<td>Shows the IP address of the remote server that backed up files are stored.</td>
</tr>
<tr>
<td>remote ftp-dir</td>
<td>Shows the path name of the directory on the remote server where backed up files are stored.</td>
</tr>
<tr>
<td>remote ftp-user</td>
<td>Shows the name of the user account used to connect to the remote server where backed up files are stored.</td>
</tr>
<tr>
<td>remote manual filenames</td>
<td>Shows the names of the files that have been manually backed up and stored on the remote server.</td>
</tr>
<tr>
<td>remote scheduled filenames</td>
<td>Shows the names of the files that have been backed up through scheduled backups and are stored on the remote server.</td>
</tr>
<tr>
<td>scheduled filename</td>
<td>Shows the name of the scheduled backup files stored in the /var/backup/sched/ directory.</td>
</tr>
<tr>
<td>scheduled homedirs</td>
<td>Shows whether home directories are backed up.</td>
</tr>
<tr>
<td>scheduled logfiles</td>
<td>Shows whether log files are scheduled for backup.</td>
</tr>
<tr>
<td>scheduled package name</td>
<td>Shows whether a specified package is scheduled for backup.</td>
</tr>
<tr>
<td>scheduled packages</td>
<td>Shows the names of the packages backed up through scheduled backups and stored in the /var/backup/sched directory.</td>
</tr>
<tr>
<td>scheduled dayofmonth</td>
<td>Shows the day of the month on which regular monthly backups are scheduled.</td>
</tr>
<tr>
<td>scheduled dayofweek</td>
<td>Shows the day of the week on which regular weekly backups are scheduled.</td>
</tr>
<tr>
<td>scheduled hour</td>
<td>Shows which hour of the day regular backups are scheduled.</td>
</tr>
<tr>
<td>scheduled minute</td>
<td>Shows which minute of the day regular backups are scheduled.</td>
</tr>
<tr>
<td>scheduled status</td>
<td>Shows whether regular backups are scheduled and the date and time of scheduled backups.</td>
</tr>
</tbody>
</table>
Show Restore Commands

Use the following command to display information on your current restore configuration.

```
show restore
  manual filenames
  remote dir
  remote filenames
  remote site
  remote user
  scheduled filenames
```

**Arguments**

- **manual filenames**  Displays the names of the manual backup files that are available locally.
- **remote dir**  Displays the path name of the directory on the remote server that contains the backup file to be restored.
- **remote filenames**  Displays the archive files that are available on the remote server.
- **remote site**  Displays the IP address of the remote server from which the backup files will be restored.
- **remote user**  Displays the name of the user account used to connect to the remote server where backed up files are stored.
- **scheduled filenames**  Displays the names of the scheduled backup files that are available locally.
Schedule Jobs Through Crontab File

Use the following commands to configure your system to schedule regular jobs. The cron daemon executes jobs on the dates and times you specify.

Scheduling Jobs

```
set cron
  job name command name
  job name command name timezone <local | utc> dayofmonth <1-31>
  job name command name timezone <local | utc> dayofweek <0-7>
  job name command name timezone <local | utc> hour <0-23>
  job name command name timezone <local | utc> minute <0-59>
  job name on
  mailto email_addr
```

Adding Jobs

Use the following commands add new regular jobs:
```
add cron job name command name timezone <local | utc>
  dayofmonth <1-31>
  hour <0-23>
  minute <0-59>
  dayofweek <0-7>
  hour <0-23>
  minute <0-59>
  mailto email_addr
```

Deleting Jobs

Use the following commands to delete scheduled regular jobs.
```
delete cron
```
Deleting Jobs

job name
timezone <local | utc>
dayofmonth <1-31>
dayofweek <0-7>
job name on
mailto email_addr

Arguments

job name Specifies a name for a job for the cron daemon to execute. Use alphanumeric characters only and do not include spaces. Use the command name argument to associate the job name with a specific Unix command.

command name Specifies the name of the command for the cron daemon to execute. The command can be any Unix command. Associate this command name with a job name.

timezone <local | utc> Specifies which time zone to use to set the configured time. Local refers to the time zone configured on your platform. UTC refers to universal time coordinated, which is kept in the “i” laboratory, where i is any laboratory cooperating in the determination of UTC. In the U.S., the official UTC is kept by the U.S. Naval Observatory.

dayofmonth <1-31> Specifies the day of the month for the cron daemon to execute the scheduled job. Use this argument only to schedule monthly jobs.

dayofweek <0-7> Specifies the day of the week for the cron daemon to execute the scheduled job. Use this argument only to schedule weekly jobs.

hour <0-23> Specifies the hour of the day for the cron daemon to execute the scheduled job.

minute <0-59> Specifies the minute of the day for the cron daemon to execute the scheduled job.

job name on Enables the specified job name

mailto email_addr Specifies the email address for the system to send mail regarding your scheduled jobs.
Show Cron Commands

Use the following commands to monitor and troubleshoot your job scheduler configuration.

`show cron`
- `job name command` Shows the Unix command associated with the specified job name.
- `job name dayofmonth` Shows the day of the month on which the job associated with the specified job name is executed by the cron daemon for a monthly scheduled job.
- `job name dayofweek` Shows the day of the week on which the job associated with the specified job name is executed by the cron daemon for a weekly scheduled job.
- `job name hour` Shows the hour of the day on which the job associated with the specified job name is executed by the cron daemon.
- `job name minute` Shows the minute of the day on which the job associated with the specified job name is executed by the cron daemon.
- `jobs` Shows only the names of jobs are scheduled for the cron daemon to execute.
- `mailto` Shows the email address to which the system sends information regarding scheduled jobs.
System Failure Notification Configuration

Use this group of commands to configure system failure notification.

Note - You must first configure mail relay before you configure system failure notification.

Enabling System Failure Notification

Use the following command to enable system failure notification:

```
set notify
    onfail <on | off>
```

Use the following command to configure a user name or email address for notification of a system failure:

```
add notify onfail
    recipient name
```

Use the following command to delete a user name or email address for notification of a system failure:

```
delete notify onfail
    recipient name
```

Show System Failure Notification

Use the following commands to view the system failure notification configuration:

```
show notify onfail
    all
```

Arguments

<table>
<thead>
<tr>
<th>onfail name</th>
<th>Specifies an email address or user name to which to send email when there is a system failure. If no email address is specified, the email will be sent to the email address specified in Mail Relay.</th>
</tr>
</thead>
</table>
DNS

Setting DNS

Use this group of commands to configure the domain name and domain name servers for your platform:

set dns slot <1-15>
  domainname name
  primary ip_address
  secondary ip_address
  tertiary ip_address

Show DNS

Use the following commands to view your DNS configurations:

show slot <1-15> dns
  dns domainname
  dns primary
  dns secondary
  dns tertiary

Deleting DNS

Use the following commands to delete DNS configurations:

delete dns slot <1-15>
  domainname
  primary
  secondary
  tertiary
### Arguments

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>domainname &lt;name&gt;</td>
<td>Specifies the name that is put at the end of all DNS searches if they fail. This name should be your local domain name and should begin with an alphabetic letter and may consist only of alphanumeric characters and hyphens. Domain names that are also numeric IP addresses are not allowed.</td>
</tr>
<tr>
<td>primary &lt;IPv4 address&gt;</td>
<td>Specifies the IP address of the first server to use when resolving hostnames. This address should be a host running a DNS server.</td>
</tr>
<tr>
<td>secondary &lt;IPv4 address&gt;</td>
<td>Specifies the IP address of the server to use when resolving hostnames if the primary server does not respond. This address should be a host running a DNS server.</td>
</tr>
<tr>
<td>tertiary &lt;IPv4 address&gt;</td>
<td>Specifies the IP address of the server to use when resolving hostnames if the primary and secondary servers do not respond. This address should be a host running a DNS server.</td>
</tr>
</tbody>
</table>
Static Host Address Assignment Configuration

Use this group of commands to configure static host names for particular IP addresses.

Adding New Host Names

Use the following command to add a new 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 an existing static host name and IP address:

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

Deleting Host Names

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

```
delete host name name
```

Showing Host Names

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

```
show host
names
name name ipv4
```
### Arguments

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>name name_ipv4 ip_address</code></td>
<td>Specifies the name of a new or existing static host and the associated IP address. 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. The IPv4 address to be associated with a static hostname must be in a dot-delimited format with the following range: <code>[0-255].[0-255].[0-255].[0-255]</code>.</td>
</tr>
<tr>
<td><code>names</code></td>
<td>Displays all the static host names and addresses on the platform.</td>
</tr>
</tbody>
</table>
Host Name Configuration

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

Use the following commands to view or change your platforms host name:

- show hostname slot <1-15>
- set hostname name slot <1-15>

Arguments

<table>
<thead>
<tr>
<th>Arguments</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hostname name</td>
<td>When you use the argument with the show command and without the variable, the command shows the current host name of your platform. When you use the argument with the set command, it changes the name of your platform to the name indicated in the variable. When the argument takes the form of hostname slot &lt;1-15&gt; and you use the argument with the show command, the command shows the current host name for the particular slot specified in the slot variable. When the argument takes the form: hostname name slot &lt;1-15&gt;, the command changes the host name of the slot specified in the slot variable.</td>
</tr>
</tbody>
</table>
Managing IPSO Images

Use this group of commands to view, select, download and test IPSO images.

**Note** - Flash-based systems can store a maximum of two IPSO images plus Check Point packages.

### Show IPSO Images

Use the following commands to view IPSO images stored on your platform:

```
show slot <1-15>
images
image current
image testboot
```

### Deleting IPSO Images

Use the following command to delete an IPSO image from your platform:

```
delete image <name | last-download>
```

### Test Boot, Reboot, and Halt IPSO Images

Use the following commands to test boot an IPSO image:

```
testboot
    image <name | last-download>
save
keep
cancel
```

Use the following command to reboot your platform with a specified IPSO image:

```
reboot
    image <name | last-download>
save
```
Use the following command to halt the platform with the option to specify an image to use on the next boot:

```
halt
    image <name | last-download>
save
```
Downloading IPSO Images

Use the following command to download an IPSO image to your platform:

```
Note - The download command maintains all currently active packages after a reboot. Use the disable-packages argument as specified below to disable installed packages after a reboot.

download image
  url name <disable-packages>
  http-realm name user name passwd name <disable-packages>
```

### Arguments

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>images</td>
<td>The IPSO images on your platform.</td>
</tr>
<tr>
<td>image current</td>
<td>The currently running IPSO image on your platform.</td>
</tr>
<tr>
<td>image testboot</td>
<td>Displays the image being executed while the in test boot mode.</td>
</tr>
<tr>
<td>delete image &lt;name</td>
<td>last-download&gt;</td>
</tr>
<tr>
<td>testboot image &lt;name</td>
<td>last-download&gt;</td>
</tr>
<tr>
<td>reboot image &lt;name</td>
<td>last-download&gt;</td>
</tr>
<tr>
<td>halt image &lt;name</td>
<td>last-download&gt;</td>
</tr>
<tr>
<td>save</td>
<td>Saves any unsaved configuration changes prior to booting.</td>
</tr>
<tr>
<td>keep</td>
<td>Accepts the IPSO image being tested as the default image. You do not have to reboot.</td>
</tr>
<tr>
<td>cancel</td>
<td>Immediately cancels the test boot and reboots your platform with the previous image.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>url name</td>
<td>Specifies an http or ftp url in dot delimited format. If you want the path to be absolute to your home directory, you must start the directory name from which you want to download with %2F, for example, ftp://10.1.1.1/%2Ftmp/ipso.tgz.</td>
</tr>
<tr>
<td>http-realm name</td>
<td>Specifies the HTTP realm to which authentication is needed. The name must be printable characters, for example, download.</td>
</tr>
<tr>
<td>user name</td>
<td>Specifies a login name if one is required to access the ftp or http server. The format must be printable characters.</td>
</tr>
<tr>
<td>disable-packages</td>
<td>Specifies to deactivate installed packages after the next reboot. The default is for installed packages to remain active after a reboot.</td>
</tr>
<tr>
<td>passwd name</td>
<td>Specifies a password if one is required to access the ftp or http server. The format can be any characters.</td>
</tr>
</tbody>
</table>
Managing Configuration Sets

Use this group of commands to create and manage configuration database files.

Configuration Set Commands

Use the following commands to view the current configuration database files and the current state of the active configuration:

```plaintext
show
cfgfiles
config-state
```

Use the following command to copy the configuration of the running state to the active configuration database file:

```plaintext
copy running-config startup-config
```

Use the following command to select a configuration database to become the current running state:

```plaintext
load cfgfile name
```

Use the following commands to save or create configuration database files:

```plaintext
save
config
cfgfile name
factory-cfg name
```

Use the following command to delete a configuration database file:

```plaintext
delete cfgfile name
```

Arguments

cfgfiles

Displays all the configuration database files on your platform. In the following example, the file titled `initial` is the active configuration file indicated by the word `active` in the left hand column:

```plaintext
cfgfile active.prev
active initial
cfgfile initial_3.6v13
cfgfile initial_3.6v15
```
**Configuration Set Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>config-state</td>
<td>Specifies the current state of the active configuration, which can be either unsaved or saved:</td>
</tr>
<tr>
<td></td>
<td>1. unsaved—a change has been made to the configuration which has not been written to the configuration database file.</td>
</tr>
<tr>
<td></td>
<td>2. saved—the configuration of the system matches the current configuration file.</td>
</tr>
<tr>
<td>cfgfile name</td>
<td>When you use this argument with the load command, you will apply the configuration of the database file in the variable to the currently running system. The command produces a warning message that indicates that unsaved configuration changes are lost and a telnet connection may be lost. The name variable can be “default,” in which case any unsaved configuration changes are lost and /config/active is loaded.</td>
</tr>
<tr>
<td></td>
<td>When you use this argument with the save command, you will save the current state of the system to a file named in the variable. The name variable can be “default,” in which case any unsaved configuration changes are saved to /config/active.</td>
</tr>
<tr>
<td></td>
<td>When you use this argument with the delete command, the configuration database file you named in the variable will be deleted. You cannot delete the active configuration file.</td>
</tr>
<tr>
<td>config</td>
<td>Saves the current running state to the current configuration database.</td>
</tr>
<tr>
<td>factory-cfg name</td>
<td>Creates a new factory default configuration, which is saved in a file named in the variable. The factory default configuration will not bring up any interfaces that you have configured in the new configuration database.</td>
</tr>
<tr>
<td>running-config</td>
<td>Applies the current running configuration to the active configuration database. This is a Cisco-like command.</td>
</tr>
<tr>
<td>startup-config</td>
<td></td>
</tr>
<tr>
<td>name</td>
<td>You may use alphanumeric, dash, dot and underscore characters with no spaces for name variable.</td>
</tr>
</tbody>
</table>
Mail Relay Configuration

Use this group of commands to configure mail relay service.

Mail Relay Commands

Use the following commands to configure the location of a mail hub to which locally originated mail will be relayed via SMTP and the remote user to whom the mail is sent.

```
set mail-relay
    server name
    username name
```

Use the following commands to view the mail server and user configurations:

```
show mail-relay
    server
    username
```

Arguments

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>server name</td>
<td>Specifies the IP address or hostname of a mail server that will relay outgoing mail. You must use a host name or IP address in a dot-delimited format.</td>
</tr>
<tr>
<td>username name</td>
<td>Specifies the username on the mail server to which mail addressed to admin or monitor will be sent, for example, admin@localhost.</td>
</tr>
</tbody>
</table>
System Logging Configuration

Use the commands described in this section to configure system logging. Systems with and without hard disks have different logging commands and functionality. See “Logging Commands (Flash-Based Systems)” on page 119 for information about the commands for flash-based systems.

Logging Commands (Systems with Disks)

Use the following commands to accept system log messages from other platforms and to specify that your platform logs configuration changes made by authorized users:

```
set syslog
  accept-remote-log <yes | no>
  auditlog <disable | transient | permanent>
  auditlog-presentation text <enable | disable>
  filename name
  voyager-auditlog <on | off>
```

Use the following commands to specify a remote host to receive system log messages:

```
add
  syslog log-remote-address ip_address
  level <emerg | alert | crit | err | warning | notice
  info | debug | all>
  logging ip_address
```

Use the following command to specify the severity level of system log messages sent to a remote host:

```
set logging trap <0-7>
```

Use the following commands to delete a remote host to receive system log messages:

```
delete
  logging ip_address
  syslog log-remote-address ip_address
  level <emerg | alert | crit | err | warning | notice
```
info | debug | all>

Use the following commands to view system log configurations:

show
    logging
    syslog all
    syslog log-remote-address ip_address
    syslog log-remote-addresses
    syslog auditlog
    auditlog-presentation text
    syslog filename
    syslog voyager-auditlog

Arguments

accept-remote-log <yes | no>
    Specifies whether network system log messages should be accepted from other platforms. If this option is set to 'no', network syslog packets are silently ignored. Otherwise network syslog packets are tagged with the sending machine's hostname and logged as if the messages had been generated locally.

    no

auditlog <disable | transient | permanent>
    Specifies or shows if the system is logging configuration changes. When you enable the auditlog, you must also specify a destination file with set syslog command.

    • disable: Disables audit log.
    • transient: Log only transient changes.
    • permanent: Log transient changes and changes that have been saved and will persist after a reboot.

    disable

Note: This setting is not saved in the configuration file. You must reset it after rebooting.
auditlog-presentation text <enable | disable>
Specifications or shows whether the system displays certain log messages in a text format that is more useful than the default format.

disable

filename name
Specifies destination log file when you enable auditlog.

/var/log/messages

voyager-auditlog <on | off>
Specifies to set the system to log all Apply and Save actions to the Voyager pages. The log records these actions whether or not the operation succeeded.

Default: off

log-remote-address ip_address
Specifies the IP address of a remote system to which this system will send system log messages. Be careful not to configure two machines to send logs to each other directly or indirectly. Doing so creates a syslog forwarding loop, which causes syslog messages to be repeated indefinitely on both machines.

level <emerg | alert | crit | err | warning | notice | info | debug | all>
When you use the syslog log-remote-address command, specifies an associated severity level for each system log message. A remote system is sent some portion of the locally generated system logging messages. Specifying a given severity means that all messages at least that severe are sent to the associated remote host.

Note: until you configure at least one severity level for a given remote host, the remote host is not sent any system log messages. If you specify multiple severities, the most general least severe severity always takes precedence.
<table>
<thead>
<tr>
<th>logging trap &lt;0-7&gt;</th>
<th>Specifies the severity level for each system log message sent to a remote host. The severity levels are as follows:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0emerg 1alert 2crit 3err 4warning 5notice 6info 7debug 6</td>
</tr>
<tr>
<td>logging</td>
<td>Any command using this argument is a Cisco-like command.</td>
</tr>
</tbody>
</table>

**Logging Commands (Flash-Based Systems)**

Use the following commands to configure logging on flash-based systems:

```
set syslog
  auditlog <disable | transient | permanent>
  flush-frequency <1-24>
  local-log <on | off>
  network-log <on | off>
  primary-log-server ip_address
  secondary-log-server ip_address
  threshold percent
```

Use the following commands to delete a remote host address so that it no longer receives system log messages:

```
delete syslog
  primary-log-server ip_address
  secondary-log-server ip_address
```
**Arguments**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>auditlog</strong> &lt;disable</td>
<td>transient</td>
</tr>
<tr>
<td></td>
<td>disable: Enables the audit log.</td>
</tr>
<tr>
<td></td>
<td>transient: Log only transient changes. These are changes to the active configuration file that have not been saved and will not persist after a reboot.</td>
</tr>
<tr>
<td></td>
<td>permanent: Log transient changes and changes that have been saved and will persist after a reboot.</td>
</tr>
<tr>
<td><strong>flush-frequency</strong> &lt;1-24&gt;</td>
<td>When the specified number of hours elapses, log messages are transferred to the remote server and the log buffer is cleared regardless of how many messages are in the buffer. You can use this option in combination with threshold for saving messages.</td>
</tr>
<tr>
<td><strong>local-log</strong> &lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td></td>
<td>off</td>
</tr>
<tr>
<td><strong>network-log</strong> &lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td></td>
<td>off</td>
</tr>
<tr>
<td><strong>primary-log-server</strong> ip_address</td>
<td>Specifies or deletes the IP address of a remote log server to which the flash-based system will send system log messages.</td>
</tr>
</tbody>
</table>

120
Use the following commands to view system log configurations:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show syslog</td>
<td>Shows all the current configuration settings.</td>
</tr>
<tr>
<td>all</td>
<td>Shows whether the system logs configuration changes.</td>
</tr>
<tr>
<td>auditlog</td>
<td>Shows the frequency (in hours) at which log messages are saved to the remote server.</td>
</tr>
<tr>
<td>flush-frequency</td>
<td>Shows whether the system is configured to save log messages to an optional disk (flash memory PC card or optional hard disk).</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>network-log</td>
<td>Shows whether the system is configured to save log messages to a remote log server.</td>
</tr>
<tr>
<td>primary-log-server</td>
<td>Shows the IP address of the primary remote log server.</td>
</tr>
<tr>
<td>secondary-log-server</td>
<td>Shows the IP address of the secondary remote log server.</td>
</tr>
<tr>
<td>threshold</td>
<td>Shows the threshold level for saving log messages to the remote server.</td>
</tr>
</tbody>
</table>
Optional Disk Configuration (Flash-Based Systems)

On flash-based platforms, you can add a hard disk (in some platforms) or flash memory PC card so that you can store the following kinds of files locally:

- **Log files**—local log files are deleted whenever a flash-based platform is rebooted. You can configure an optional disk to locally store log files so that they survive reboot.

- **Package files**—on select platforms, you can configure the optional disk to store application packages. Doing so frees up space in the built-in flash memory.

- **Kernel dump files**—on select platforms, you can configure the optional disk to store kernel core dump files. This allows the platform to store kernel core-dump files much larger than those allowed by the swap space allocated for kernel core dumps in the built-in flash memory.

The above options are mutually exclusive: in other words, you cannot configure an optional disk to store both logs and kernel dump files.

When you select a hard disk or PC card as an optional disk, any existing data on the device is erased. If you remove a PC card that contains log files and want to permanently store the data, insert the card into a PC or other computer and save the data to that system before reinserting the card into a Check Point flash-based platform. For instructions on installing a flash-memory PC card or a hard disk, see your platform installation guide. After you install an optional disk and configure it to store files, you must reboot the system to make it available for use.

**Note** - The download command maintains all currently active packages after a reboot. Use the disable-packages argument as specified below to disable installed packages after a reboot.

**Note** - If you are configuring an optional disk to store logs, you must also configure the system to store logs on the optional disk. See “System Logging Configuration” for more information.

### Configuring an Optional Disk

Use the following commands to enable or disable an optional disk and to specify what files should be stored on it:

```
set optional-disk device-id < n >
```
Configuring an Optional Disk

```plaintext
  type <log | pkg | kernel-dump> on [force]
  off
```

**Note** - In some cases there might be a long delay before the enabling of an optional disk completes. The CLI prompt will not reappear until the operation is complete.

Use the following command to see whether an optional disk is present and enabled:
```
  show optional-disks
```

**Arguments**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>device-id &lt; n &gt;</td>
<td>Specifies the device to be configured.</td>
</tr>
<tr>
<td></td>
<td>Use the <code>show optional-disks</code> command to display the device IDs associated</td>
</tr>
<tr>
<td></td>
<td>with the optional disks you have installed.</td>
</tr>
<tr>
<td>type &lt;log</td>
<td>pkg</td>
</tr>
<tr>
<td></td>
<td>are supported on all platforms. You can store package files on an optional</td>
</tr>
<tr>
<td></td>
<td>disk only on IP265 systems. You can store kernel core files on an optional</td>
</tr>
<tr>
<td></td>
<td>disk only on certain systems.</td>
</tr>
<tr>
<td>on</td>
<td>Enables a hard disk or a PC card as an optional disk. After enabling an</td>
</tr>
<tr>
<td></td>
<td>optional disk, you must reboot the system.</td>
</tr>
<tr>
<td>force</td>
<td>Forces the CLI to configure an unlabeled but supported hard disk.</td>
</tr>
<tr>
<td></td>
<td>If an optional hard disk is unlabeled, the CLI will report it as possibly</td>
</tr>
<tr>
<td></td>
<td>unsupported. If your hard disk is supported, use the force keyword, which</td>
</tr>
<tr>
<td></td>
<td>forces the CLI to label and configure the optional hard disk.</td>
</tr>
<tr>
<td>off</td>
<td>Disables the storing of files on the optional disk. After disabling an</td>
</tr>
<tr>
<td></td>
<td>optional disk, you must reboot the system.</td>
</tr>
</tbody>
</table>
Core-Dump Server Configuration
(Flash-Based Systems)

On flash-based platforms, application core files are stored in memory in the directory /var/tmp. When the file system is 95% filled, flash-based systems delete older core files to make room for newer ones.

Similarly, flash-based platforms store IPSO kernel core files in the internal compact flash memory card. If necessary, the older core file is deleted to make room for a new file.

You can configure flash-based systems to transfer both application and kernel core files to a remote server so that older files are retained. If you do so, the application core files are transferred to the remote server on a predetermined schedule that is not configurable by users. Kernel core dump files are sent to the remote server after the system recovers from the problem that caused the core dump. You can verify that the core file was successfully transferred by checking the log message file for a message similar to the following:

[LOG_NOTICE] xfer_crash: Transferred kernel core file to ftp_server_IP_address

This message is not displayed on the console.

After core files are transferred to a remote server, they are deleted from memory.

Note - Certain platforms permit you to store kernel core files on an optional disk. If you have configured an optional disk to store kernel core files, you can still configure the remote core dump server feature, allowing the core file on the optional disk to be transferred to the remote server.

Sending Core Files to a Remote Server

Use the following commands to configure the system to send application and kernel core files to a remote server:

```
set dumpserver
   ipaddr ip_address
   protocol
   ftp ftp-dir path_name
   tftp
delete dumpserver ipaddr
show dumpserver
```
all
ftp-dir
ipaddr
protocol

Arguments

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipaddr ip_address</td>
<td>Specifies or deletes the IP address of the system to which core files should be sent.</td>
</tr>
<tr>
<td>protocol ftp ftp-dir path_name</td>
<td>Specifies to use FTP when sending core files and also specifies the path to the location where the files will be stored. If you choose FTP, make sure that your server accepts anonymous FTP logins. You cannot use nonanonymous FTP logins to transfer application core files.</td>
</tr>
<tr>
<td>protocol tftp</td>
<td>Specifies to use TFTP when sending core files. Because TFTP does not work with TFTP servers running on many Unix-based operating systems, Check Point recommends that you use FTP unless you are sure that your TFTP server accepts writes to files that do not already exist on the server.</td>
</tr>
</tbody>
</table>
Date and Time Configuration

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

Setting Date and Time from Server

\texttt{set date}
\begin{verbatim}
  once-from-ntpserver <ip_address | fully qualified domain name>
  timezone-city value
\end{verbatim}

\textbf{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 one of the following 2 commands to set the date and time:

\texttt{set clock time month date year}
\texttt{set clock time date month year}

\textbf{Arguments}

\begin{itemize}
  \item \texttt{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.
  \item \texttt{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`.
\end{itemize}
Show Date and Clock Commands

<table>
<thead>
<tr>
<th>Arguments</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>day &lt;1-31&gt;</strong></td>
<td>Specifies which day of the month to use to set the initial time.</td>
</tr>
<tr>
<td><strong>hour &lt;0-23&gt;</strong></td>
<td>Specifies which hour of the day to use to set the initial time.</td>
</tr>
<tr>
<td><strong>minute &lt;0-59&gt;</strong></td>
<td>Specifies which minute of the hour to use to set the initial time.</td>
</tr>
<tr>
<td><strong>second &lt;0-59&gt;</strong></td>
<td>Specifies which second of the minute to use to set the initial time.</td>
</tr>
<tr>
<td><strong>month &lt;1-12&gt;</strong></td>
<td>Specifies which month of the year to use to set the initial time.</td>
</tr>
<tr>
<td><strong>year 4 digit integer</strong></td>
<td>Specifies which year to use to set the initial time. For example, enter 2002. The range is 1970-2037.</td>
</tr>
</tbody>
</table>

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
Configuring Daylight Savings Rules

You use different commands to configure daylight savings rules depending on whether daylight savings at the appropriate location is:

- Nonrecurring (defined for a specific period of time). For example, the United States currently uses daylight savings rules that expire after 2006.
- Recurring (always occurs, with no defined stopping point). For example, the United States will start using recurring daylight savings rules in 2007.

Note - IPSO will automatically make this change for United States time zones in 2007.

Use the following commands to create daylight savings rules. You must enter a value for all the parameters to form a valid command.

```
add date timezone-dst location non-recurring
   start-year year
   start-month month
   start-date <1-31>
   start-time time
   end-year year
   end-month month
   end-date <1-31>
   end-time time
   dst-offset <00:00-24:00>
```

```
add date timezone-dst location recurring
   start-year year
   start-month month
```
Configuring Daylight Savings Rules

- start-week occurrence
- start-day day
- start-time time
- end-month month
- end-week occurrence
- end-day day
- end-time time
- dst-offset <00:00-24:00>

Use the following commands to configure daylight savings rules. You do not have to enter a value for all the parameters to form a valid command.

- set date timezone-dst location non-recurring rule start-year
  - start-month month
  - start-date <1-31>
  - start-time time
  - end-year year
  - end-month month
  - end-date <1-31>
  - end-time time
  - dst-offset <00:00-24:00>

- set date timezone-dst location recurring rule start-year
  - start-month month
  - start-week occurrence
  - start-day day
  - start-time time
  - end-month month
  - end-week occurrence
  - end-day day
  - end-time time
  - dst-offset <00:00-24:00>
Use the following commands to delete daylight savings rules.

```
delete date timezone-dst location
    non-recurring rule start-year
    recurring> rule
```

delete date timezone-dst location rules all

Use the following commands to view daylight savings rules.

```
show date timezone-dst location
    non-recurring rule start-year
    recurring> rule
```

show date timezone-dst location rules all

**Arguments**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>location</td>
<td>Specifies a location in the time zone. For countries with multiple word names, such as the United States, you must bracket the location string with quotation marks, as in “United States/New_York.” If you use single command mode, bracket multiple word location names with single quotation marks. See “Invoking the CLI” on page 14 for information about single command mode.</td>
</tr>
<tr>
<td>rule start-year</td>
<td>Specifies the rule you want to change by indicating its start year.</td>
</tr>
<tr>
<td>start-year year</td>
<td>Specifies the year in which the DST rule begins.</td>
</tr>
<tr>
<td>start-month month</td>
<td>Specifies the month when DST begins.</td>
</tr>
<tr>
<td>start-week occurrence</td>
<td>Specifies the occurrence of the relevant day in the month specified by start-month. For example, entering 2 for this parameter and entering Sun as the start-day specifies that DST will begin on the second Sunday of the specified month. The valid entries are 1, 2, 3, 4, and last.</td>
</tr>
<tr>
<td>start-date &lt;1-31&gt;</td>
<td>Specifies the day of month when DST begins.</td>
</tr>
<tr>
<td>start-day day</td>
<td>Specifies the day of week when DST begins. The valid entries are Sun, Mon, Tue, Wed, Thur, Fri, and Sat.</td>
</tr>
<tr>
<td>start-time time</td>
<td>Specifies the time when DST begins in 24-hour format.</td>
</tr>
<tr>
<td>end-year year</td>
<td>Specifies the year when the DST rule ends.</td>
</tr>
</tbody>
</table>
Configuring Daylight Savings Rules

<table>
<thead>
<tr>
<th>end-month month</th>
<th>Specifies the month when DST ends. The valid entries are Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, and Dec.</th>
</tr>
</thead>
<tbody>
<tr>
<td>end-week occurrence</td>
<td>Specifies the occurrence of the relevant day in the month specified by end-month. For example, entering 2 for this parameter and entering Sat as the end-day specifies that DST will end on the second Saturday of the specified month. The valid entries are 1, 2, 3, 4, and last.</td>
</tr>
<tr>
<td>end-date &lt;1-31&gt;</td>
<td>Specifies the day of month that DST ends.</td>
</tr>
<tr>
<td>end-day day</td>
<td>Specifies the day of week when DST ends. The valid entries are Sun, Mon, Tue, Wed, Thur, Fri, and Sat.</td>
</tr>
<tr>
<td>end-time time</td>
<td>Specifies the time when DST ends in 24-hour format.</td>
</tr>
<tr>
<td>dst-offset &lt;00:00-24:00&gt;</td>
<td>Specifies the amount by which the time is offset. You can use the following formats:</td>
</tr>
<tr>
<td></td>
<td>• hh</td>
</tr>
<tr>
<td></td>
<td>• hh:mm</td>
</tr>
</tbody>
</table>

**Restoring the Default Rule**

You cannot use the CLI to revert to the default daylight savings rule for a time zone. To configure the system to use the default rule, perform this procedure:

1. Log into the IPSO shell.
   - In the CLI, you can enter `shell` to load the shell.
2. Delete the customized time zone file from `/var/etc/zoninfo` directory.
3. Mount `/` as read-write by entering
   ```
   mount -uw /
   ```
4. Change directory to `/etc/zoneinfo/region`. For example, for a United States time zone enter
   ```
   cd /etc/zoneinfo/America
   ```
5. Delete the symbolic link for the customized time zone.
6. Rename `time_zone.orig` as `time_zone`.
   For example, if you customized `New_York`, you would rename `New_York.orig` to `New_York`. 

132
7. If you are restoring the default time zone rule for the currently selected time zone, perform these steps:

1. Select a different time zone to be the current time zone.
2. Reselect the original time zone.
Disk Commands

Use the commands in this section to show information about the hard drives in your appliance.

Viewing Disk Information

Use the following command to show the disks (by drive identification number) that IPSO detects on the local system:

show disks

Use the following commands to show information about a specified disk:

show disk
  id
  id model
  id type
  id capacity
  id geometry
  id location

Arguments

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>disk id</td>
<td>Specifies the drive identification number of the disks that IPSO detects. If you use this command without any additional arguments, the command displays the information in the rest of this table.</td>
</tr>
<tr>
<td>model</td>
<td>Specifies the model of the drive that IPSO detects.</td>
</tr>
<tr>
<td>type</td>
<td>Specifies whether the disk is a Bootmgr or IPSO disk.</td>
</tr>
<tr>
<td>capacity</td>
<td>Specifies the disk capacity in megabytes.</td>
</tr>
<tr>
<td>geometry</td>
<td>Specifies the logical block address geometry of the drive in CHS format: cylinders x heads x sectors per track detected for each drive.</td>
</tr>
<tr>
<td>location</td>
<td>Specifies the physical location of the drive on the chassis.</td>
</tr>
</tbody>
</table>
Disk Mirroring Commands

For platforms that support the feature, disk mirroring provides fault tolerance by letting your appliance continue working in the event of a disk failure. You can create mirror sets that consist of a source disk (which holds the active copy of the operating system) and mirror hard disk. The mirror disk contains a copy of all the files on the source disk, and if the source disk fails, the mirror disk immediately takes over. Your appliance continues to operate normally.

If you have an appliance on which you have configured disk mirroring, you can “warm swap” disk drives (with the exception of IP500 series appliances) —you can replace a drive without shutting down the appliance. This allows you to replace a failed drive without interrupting service.

Note - A mirror disk must be the same size or larger than the source disk. Before you create a mirror set, verify that this is true by using the show disk commands. See “Viewing Disk Information” on page 134 for information about these commands.

Configuring Disk Mirroring

Use the following command to add a disk mirror set:
add diskmirror

Use the following command to delete a disk mirror set. You cannot delete a disk mirror set until the synchronization is 100 percent.
delete diskmirror id

Use the following command to view the identification number of a disk mirror set on your system:
show diskmirrors

Use the following commands to view properties about disk mirroring on your system:
show diskmirror
  id
  id mrdrive
  id srcdrive
  id syncpercent
## Arguments

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>Specifies the disk mirror set identification number. If you use this command without any additional arguments, the command displays all of the rest of the information in this table.</td>
</tr>
<tr>
<td>mrdrive</td>
<td>Displays the disk ID of the mirror drive.</td>
</tr>
<tr>
<td>srcdrive</td>
<td>Displays the disk ID of the source drive</td>
</tr>
<tr>
<td>syncpercent</td>
<td>Displays the percentage of sync zones that are currently synchronized. Enter this command repeatedly to see updated percentage figures.</td>
</tr>
</tbody>
</table>
NTP

Use the commands in this section to configure Network Time Protocol (NTP) settings for your system.

Configuring NTP

Use the following commands to specify other systems as network time protocol servers or peers for this system:

```
add ntp
    autokey-cert path group-file filename server name
    server ip_address version <1-3> [autokey <yes | no>][prefer <yes | no>]
    peer ip_address version <1-3> [prefer <yes | no>]
```

Arguments

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>autokey-cert path</td>
<td>Specifies the path to the autokey group (client) key file.</td>
</tr>
<tr>
<td>group-file filename</td>
<td>Specifies the name of the autokey group (client) key file.</td>
</tr>
<tr>
<td>server name</td>
<td>Specifies the fully qualified domain name of the NTP server.</td>
</tr>
<tr>
<td>server ip_address</td>
<td>Specifies the address of a time server from which this machine synchronizes its clock. The specified server does not synchronize its clock to the local clock of this system.</td>
</tr>
<tr>
<td>peer ip_address</td>
<td>Specifies the address of a time server with which this machine synchronizes clocks. The specified server can synchronize its clock to the local clock of this system.</td>
</tr>
<tr>
<td>version &lt;1-3&gt;</td>
<td>Specifies which version of NTP to use when synchronizing with the specified system. Check Point recommends that this be set to version 3, the most recent version.</td>
</tr>
<tr>
<td>autokey &lt;yes</td>
<td>no&gt;</td>
</tr>
<tr>
<td>prefer &lt;yes</td>
<td>no&gt;</td>
</tr>
</tbody>
</table>
Use the following commands to configure network time protocol settings and to configure this system as a master NTP server:

```
set ntp
active <on | off>
server ip_address version <1–3> [autokey <yes | no>][prefer <yes | no>]
password password
peer ip_address version <1–3> [prefer <yes | no>]
master <yes | no>
stratum <1–15> source local-clock
```

**Arguments**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>active &lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td>server ip_address</td>
<td>Specifies the NTP server that you want to configure.</td>
</tr>
<tr>
<td>version &lt;1–3&gt;</td>
<td>Specifies which version of NTP to use when synchronizing with the specified system. It is recommended that this be set to version 3—the most recent version.</td>
</tr>
<tr>
<td>autokey &lt;yes</td>
<td>no&gt;</td>
</tr>
<tr>
<td>prefer &lt;yes</td>
<td>no&gt;</td>
</tr>
<tr>
<td>no</td>
<td></td>
</tr>
<tr>
<td>password password</td>
<td>Specifies the autokey group (client) password.</td>
</tr>
<tr>
<td>peer ip_address version</td>
<td>Specifies the NTP peer that you want to configure.</td>
</tr>
</tbody>
</table>
Use the following commands to stop a system from using NTP to synchronize with other systems that it was previously configured to synchronize with:

```
delete ntp
  server ip_address
  peer ip_address
```

**Arguments**

- `server ip_address`: Specifies the NTP server to prevent this system from synchronizing with.
- `peer ip_address`: Specifies the NTP peer to prevent this system from synchronizing with.

Use the following commands to view the NTP configuration settings for this system:

```
show ntp
  active
  servers
  peers
  <server | peer> ip_address
  autokey
  prefer
  version
  master
```

**master <yes | no>**

Configures this system to act as an NTP master server. When configured as a master server, a system will not get its time from other systems.

**stratum <0-15>**

Specifies the stratum—the number of hops away from a source of correct time this system’s clock should is. This should normally be set to 0.

**source local-clock**

0
### Arguments

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>active</td>
<td>Shows whether or not NTP is active.</td>
</tr>
<tr>
<td>servers</td>
<td>Lists any systems configured as NTP servers and shows the appropriate NTP version and prefer settings.</td>
</tr>
<tr>
<td>peers</td>
<td>Lists any systems configured as NTP peers and shows the appropriate NTP version and prefer settings.</td>
</tr>
<tr>
<td>&lt;server</td>
<td>peer&gt; ip_address [autokey][prefer][version]</td>
</tr>
<tr>
<td></td>
<td>• autokey setting</td>
</tr>
<tr>
<td></td>
<td>• prefer setting</td>
</tr>
<tr>
<td></td>
<td>• NTP version</td>
</tr>
<tr>
<td>master</td>
<td>Shows whether this system has been configured as an NTP master server. If it has, this command also shows the appropriate stratum setting.</td>
</tr>
</tbody>
</table>
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.
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

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>addr ip_address</td>
<td>Specifies the IPv4 address of the remote machine containing the package.</td>
</tr>
<tr>
<td></td>
<td>Example: 192.168.10.10</td>
</tr>
<tr>
<td>user name</td>
<td>Specifies the login name for FTP.</td>
</tr>
<tr>
<td>password password</td>
<td>Specifies the password associated with the username parameter for FTP login.</td>
</tr>
<tr>
<td>old name</td>
<td>Specifies the name of the existing package to be replaced. Use the complete path.</td>
</tr>
<tr>
<td>new name</td>
<td>Specifies the name of the package (in .tgz format) you will use to replace the existing package. Use the complete path.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name name</td>
<td>Specifies the name of the package. Use the complete path.</td>
</tr>
</tbody>
</table>
Advanced System Tuning Commands

The commands in this section are intended for very specific purposes, and, under most circumstances, you should not change any of the default settings.

**Controlling Sequence Validation**

Use the following command to enable and disable sequence validation:

```plaintext
set advanced-tuning tcp-options sequence-validation <on | off>
```

Use the following command to view whether sequence validation is enabled or disabled:

```plaintext
show advanced-tuning tcp-options sequence-validation
```

**Tuning the TCP/IP Stack**

Use the following command to set the TCP maximum segment size (MSS) for segments received by your local system:

```plaintext
set advanced-tuning tcp-ip tcp-mss <512-1500>
```

The default value is 1024.

Use the following command to view the configured TCP MSS value:

```plaintext
show advanced-tuning tcp-ip tcp-mss
```

**Router Alert IP Option**

Use the following command to specify whether IPSO should strip the router alert IP option before passing packets to the firewall. (The router alert IP option is commonly enabled in IGMP packets.)

```plaintext
set advanced-tuning ip-options stripra <1 | 0>
```

Use the following command to view the configured setting:

```plaintext
show advanced-tuning ip-options stripra
```

**IP1260 Port Optimization**

You can use the following command to optimize the performance of the interfaces of two-port Gigabit Ethernet NICs in IP1260 platforms when the interfaces forward unidirectional UDP traffic.

```plaintext
set advanced-tuning ethernet-options <on | off>
```
Enabling this option does not optimize throughput for other types of traffic or other interfaces. This command is not available on the IP1220.

**Warning** - Do not enable this option if more than two Gigabit Ethernet interfaces are installed in the system. Doing so can impair system performance.
Chapter 4
High Availability Commands

Check Point provides the following solutions that you can use to create a highly available and redundant configuration to ensure that your network traffic continues to flow in the event that one of your firewall platforms fails:

- IP clustering
- External load balancer support
- Single license VRRP (in which one firewall license is shared between two systems). There is no CLI command for this feature.
- Multiple license VRRP (in which each system has an individual firewall license installed)

For information about the CLI commands to use with an IP cluster, see the Chapter 5, “IP Clustering Commands.” The commands for external load balancer support and multiple license VRRP are described in this chapter.

In This Chapter

- General VRRP Commands  page 149
- Simplified Method Monitored-Circuit VRRP  page 151
- Full Method Monitored-Circuit VRRP  page 153
- VRRPv2  page 155
You can use an external load balancer to balance traffic to multiple IPSO firewalls without using IP clustering or VRRP. By configuring the firewalls to synchronize traffic with each other you can provide high availability as well. Using an external load balancer also has the advantage of not requiring you to use virtual IP addresses on the IPSO firewalls.

Use the following command to enable or disable support for and external load balancer:

```
set external_load_balancer <on | off>
```

Use the following command to display the state of external load balancer support:

```
show external_load_balancer
```
You can configure the Virtual Router Redundancy Protocol (VRRP) to use either monitored-circuit VRRP or VRRPv2. You can configure monitored-circuit VRRP using either the simplified method or the full method. For more information, refer to the *Network Voyager Reference Guide for IPSO 6.2* [http://supportcontent.checkpoint.com/documentation_download?ID=10293](http://supportcontent.checkpoint.com/documentation_download?ID=10293).

**Note** - Beginning with IPSO 3.8.1, Check Point also supports VRRP for IPv6 addresses. For more information about the CLI commands for this implementation, see “VRRP for IPv6” on page 209.

The CLI commands for these implementations are explained in the following sections.

### General VRRP Commands

Use this group of commands to set and view parameters that apply to any VRRP configuration, regardless of which VRRP implementation you use.

```
set vrrp
    accept-connections <on | off>
    coldstart-delay seconds
    monitor-firewall <on | off>
    monitor-hdd <on | off>
    disable-all-virtual-routers <on | off>
```
Arguments

accept-connection
s <on | off>

The VRRP protocol specifies that a router should not accept or respond to IP packets sent to an adopted VRRP (virtual) backup IP address. Entering off specifies compliance with the specification. Entering on overrides this behavior and allows the master to accept and respond to packets sent to an adopted VRRP backup address. This setting enhances interaction with network management tools and allows you to log into the VRRP master using a backup address. You must enable this option when deploying dynamic routing protocols or any highly available application whose service is tied to a VRRP backup address.

off

coldstart-delay
seconds

Specifies a number of seconds that the system should wait after starting before joining a VRRP group. You might want to configure a delay to allow routing adjacencies to form or for applications to synchronize before a system becomes the VRRP master.

You can use this option with or without firewall monitoring. If you also enable firewall monitoring, the system begins to monitor the firewall after the coldstart delay period has elapsed.

0 seconds

monitor-firewall <on | off>

Specifies whether to monitor the state of the firewall and respond appropriately. If a VRRP master detects that the firewall is not ready to handle traffic or is not functioning properly, the master fails over to a backup system. If all the firewalls on all the systems in the VRRP group are not ready to forward traffic, no traffic will be forwarded.

on

monitor-hdd <on | off>

Specifies whether virtual routers should transition to init state (and a failover should occur) if certain disk errors are detected on the master. If you enable this option on a system on which disk mirroring is also enabled, virtual routers do not transition to init state if the mirror disk takes over for the primary disk.

off
Simplified Method Monitored-Circuit VRRP

Use the commands explained in this section to configure monitored-circuit VRRP implementations using a simplified method. When you use this method, you create backup (virtual) addresses and the system automatically associates the appropriate router interfaces with the backup addresses. This reduces the number of configuration steps you need to perform.

Note - You cannot convert legacy monitored-circuit configurations into a simplified configuration. To use this method, you must first delete any existing legacy monitored-circuit configuration.

Use the following commands to create a virtual router:

```
add mcvr vrid <1-255> priority <1-254> priority-delta <1-254>
  authtype <none|simple> [password passwd]
  hello-interval <1-255>
```

Use the following commands to add backup addresses to a virtual router:

```
add mcvr vrid <1-255> backup-address ip_address
  vmac-mode
    <default-vmac|extended-vmac|interface-vmac|static-vmac
    static-mac static_VMAC>
```

Use the following commands to configure, view, and delete virtual routers:

```
set mcvr vrid <1-255>
  authtype <none|simple> [password passwd]
  hello-interval <1-255>
  priority <1-254>
  priority-delta <1-254>
show mcvr vrid <1-255>
  all
  authtype
  backup-addresses
```

disable-all-virtual-routers <on | off>

Disable all virtual routers on this IPSO appliance. This feature is available in traditional mode, and can be useful in upgrading a firewall pair running simplified mode VRRP, especially when many VRRP interfaces are in use.
You can also enable and disable preempt mode after you configure monitored-circuit VRRP using the simplified method. See “Full Method Monitored-Circuit VRRP” for information about how to do this. The command described in that section also works for simplified monitored-circuit configurations.

**Arguments**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>mcvr vrid &lt;1-255&gt;</code></td>
<td>Specifies a virtual router ID. The ID must be unique on the network that its backup addresses belong to. The ID must be identical on each physical router that participates in the virtual router.</td>
</tr>
<tr>
<td><code>priority &lt;1-254&gt;</code></td>
<td>Specifies or shows this (physical) router's priority during contention for a failed router's addresses.</td>
</tr>
<tr>
<td><code>priority-delta &lt;1-254&gt;</code></td>
<td>If an interface associated with a backup address fails, the value of the priority delta is subtracted from the priority to yields an effective priority for the physical router. When the effective priority on the master is less than the priority of another router in the VRRP group, a new master is selected.</td>
</tr>
<tr>
<td>`authtype &lt;none</td>
<td>simple&gt; [password passwd]`</td>
</tr>
</tbody>
</table>
Use these commands to configure properties for specific interfaces for the monitored circuit implementation of VRRP.

```
set vrrp interface if_name monitored-circuit vrid <1-255>
    monitored-interface if_name <on | off>
    monitored-interface if_name priority delta <1-254>
    auto-deactivation <on | off>
    priority <1-254>
    hello-interval <1-255|default>
```
The following section explains the use and meaning of VRRP monitored circuit commands.

**Arguments**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>monitored-interface</td>
<td>Specifies the ID for a virtual router with monitored circuit dependencies and the associated interface.</td>
</tr>
<tr>
<td>if_name &lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td>monitored-interface</td>
<td>Specifies the priority delta associated with the interface with a dependency on the virtual router.</td>
</tr>
<tr>
<td>if_name priority-delta &lt;1-254&gt;</td>
<td></td>
</tr>
<tr>
<td>monitored interface</td>
<td>Specifies to allow the effective priority to go to 0 and for the virtual router to be removed from the network.</td>
</tr>
<tr>
<td>if_name auto-deactivation</td>
<td>In the typical implementation, if the effective priority goes to 0, the protocol reestablishes a value of 1.</td>
</tr>
<tr>
<td>&lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td>priority &lt;1-254&gt;</td>
<td>Specifies the priority assigned to the virtual router during contention for a fail router’s addresses.</td>
</tr>
<tr>
<td>hello-interval &lt;1-255&gt;</td>
<td>Specifies the interval in seconds between VRRP advertisements. This value should be the same on all the routers participating in the virtual router.</td>
</tr>
<tr>
<td>vmac-mode</td>
<td>Specifies the method to use to set the virtual MAC address for the specified virtual router. For information on the options, see the Network Voyager Reference Guide for IPSO 6.2.</td>
</tr>
<tr>
<td>&lt;default-vmac</td>
<td>extended-vmac</td>
</tr>
<tr>
<td>backup-address &lt;ip_address&gt;</td>
<td>Specifies for the user to enter a backup IP address and enable or disable it.</td>
</tr>
<tr>
<td>&lt;on</td>
<td>off&gt;</td>
</tr>
</tbody>
</table>
VRRPv2

VRRP Show Commands

Use the following commands to monitor and troubleshoot your VRRP implementation.

```
show vrrp
  interfaces
  interface if_name
  stats
  summary
```

VRRPv2

Use the commands explained in this section to configure VRRPv2 implementations.

```
set vrrp interface if_name
  off
  authtype <none|simple password>
set vrrp interface if_name virtual-router vrid <1-255>
  <on | off>
  hello-interval <1-255|default>
  vmac-mode
    <default-vmac|extended-vmac|interface-vmac|static-vmac>
    mac_address>
  backup-address ip_address <on | off>
set vrrp interface if_name virtual-router backup-vrid <1-255>
  <on | off>
  backup-address ip_address <on | off>
  hello-interval <1-255|default>
  preempt-mode <on | off>
  priority <1-254>
```

preempt-mode <on | off>

Set to On to specify that this router will not fail over to a router with higher priority. Use this setting if you want to reduce the number of transitions.
The following section explains the use and meaning of VRRP version 2 commands.

**Arguments**

**off**
- Specifies to disable VRRP on the specified interface.

**<on | off>**
- Specifies the virtual router ID for the virtual router used to backup the local interface's address(es). The VRID must be unique for all virtual routers running on the interface's network. Enter off to remove the specified virtual router.

**hello-interval <1-255>**
- Specifies the interval in seconds between VRRP advertisements. This value must be the same on all the routers participating in the virtual router.

1 second

**authype <none|simple password>**
- None specifies not to use any authentication. Simple specifies to use simple password authentication. Enter plain text between 1 and 8 characters long. This password applies to all the virtual routers configured on an interface.

**vmac-mode**
- Specifies the method to use to set the virtual MAC address for the specified virtual router. For information on the options, see the Network Voyager Reference Guide for IPSO 6.2 http://supportcontent.checkpoint.com/documentation_download?ID=10293.

**backup-address ip_address <on | off>**
- Specifies a virtual router ID for the virtual router used to backup another system's IP address(es). The router you are backing up must also have this virtual router configured for its addresses. Enter an IP address to assign to the virtual router used to backup another system's IP addresses.

**priority <1-254>**
- Specifies this physical router's priority during contention for a failed router's addresses.
### hello-interval

<1-255 | default>

Specifies the interval in seconds between VRRP advertisements. This value must be the same on all routers participating in this virtual router.

1 second

### preempt-mode

<on | off>

Set to on to specify that this router will not fail over to a router with higher priority. Use this setting if you want to reduce the number of transitions. This parameter is only available if the virtual IP address is the same as the interface IP address.
VRRPv2
Chapter 5

IP Clustering Commands

This chapter describes the commands you use to configure clustering on your system and to view current settings.

A cluster is a group of IPSO systems that appear as a single system to devices outside the cluster. IP traffic sent to the cluster IP address is load balanced between the cluster members, and the cluster continues to function if a member fails or is taken out of service for maintenance purposes.

Use the commands in this section to add, configure, and delete clusters.


In This Chapter

General Clustering Commands  page 160
Clustering Administration  page 172
General Clustering Commands

Use the following commands to create a cluster configuration.

```plaintext
add cluster id <0–65535> [passwd passwd]
add cluster id <0–65535>
    feature name
    interface log_if_name cluster-address ip_address
    network network/mask cluster-address ip_address
add cluster
    ip-pool network network/mask member ip_address
    vpn-tunnel network ip_address/mask destination ip_address
```

**Arguments**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>id &lt;0–65535&gt; [passwd passwd]</td>
<td>Creates a cluster configuration and specifies its unique identification number. If you enter this command without specifying a password, the system responds with Enter password for cadmin: If this is the first member of the cluster, create a password for the cadmin user by entering it now. The password must have at least six characters. If this is not the first member of the cluster, enter the cadmin password that was used on the other members. When you enter the password, you are asked to enter it again to verify it.</td>
</tr>
<tr>
<td>feature name</td>
<td>Specifies a feature that should be shared when a system joins the cluster. These are called join-time shared features. This command is valid only if you have removed a feature from the list of join-time shared features and want to make it shared again. See “Managing Join-Time Shared Features” for more information.</td>
</tr>
<tr>
<td>interface log_if_name</td>
<td>Adds an Ethernet interface to a cluster.</td>
</tr>
</tbody>
</table>
Use the following commands to configure properties for an existing cluster:

```
set cluster id <0–65535>
cadmin passwd oldpass passwd newpass passwd
change <0–65535>
coldstart-delay integer
failure-interval integer
firewall-check-required <yes | no>
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>network network/mask</code></td>
<td>Specifies a network to be added to the cluster. You must specify the appropriate subnet mask. The interface that is configured with an address in the specified network is added to the cluster.</td>
</tr>
<tr>
<td><code>cluster-address ip_address</code></td>
<td>Specifies the cluster IP address for this interface. The cluster IP address is shared by all the cluster interfaces on a given network. When specified for an interface, the cluster address must belong to one of the networks with which the interface is configured.</td>
</tr>
<tr>
<td><code>ip-pool network network/mask member ip_address</code></td>
<td>Specifies a range of addresses to use as an IP pool. You must specify which cluster member should manage the specified addresses by entering the real IP address of the primary cluster protocol interface of the appropriate member. Use this command to specify IP pool addresses used with tunnels formed with non-Check Point gateways or clients. If the other end of the tunnel is a Check Point gateway, do not use this command—simply specify the IP pool using VPN-1 NG AI.</td>
</tr>
<tr>
<td><code>vpn-tunnel network network/mask destination ip_address</code></td>
<td>Creates one end of a VPN tunnel. Use <code>network network/mask</code> to specify the IPv4 network address and mask of the remote encryption domain. Use <code>destination ip_address</code> to specify the IPv4 address of the remote tunnel endpoint. Use this command if the other end of the tunnel is a non-Check Point gateway or client. If the other end of the tunnel is a Check Point gateway, do not use this command—simply specify the tunnel using VPN-1 NG AI.</td>
</tr>
</tbody>
</table>
interface log_if_name
cluster-address ip_address
hash <default | on-destination-ip | on-source-ip>
join-remote ip_address
mode <mcast | mcast-group | forwarding | unicast>
network network/mask cluster-address ip_address
performance-rating <0—65535>
primary-interface log_if_name
primary-network network/mask
remote-node ip_address performance-rating integer
secondary-interface log_if_name
secondary-network network/mask
state <up | down>
work-assign <static | dynamic>
set cluster
  ip-pool network network/mask member ip_address
  securemote <yes | no>
  vpn-clients <yes | no>
  vpn-interop <yes | no>
  vpn-tunnel network network/mask destination ip_address

Arguments

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>id &lt;0—65535&gt;</td>
<td>Specifies the unique identification number of an existing cluster.</td>
</tr>
<tr>
<td>cadmin passwd oldpass passwd newpass passwd</td>
<td>Specifies a new password for the cadmin user (the cluster administrator user). You must include the current (old) password as well as the new password. The new password must have at least six characters. See “Clustering Administration” for information about the cadmin user.</td>
</tr>
<tr>
<td>change &lt;0—65535&gt;</td>
<td>Specifies the new cluster identification number.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>coldstart-delay</strong></td>
<td>Specifies the number of seconds the system waits before starting the cluster protocol. This allows VPN-1/FireWall-1 to become active and synchronize before the cluster protocol starts.</td>
</tr>
<tr>
<td>&lt;20–200&gt;</td>
<td>VPN-1/FireWall-1 NG_AL does not require this delay.</td>
</tr>
<tr>
<td><strong>failure-interval</strong></td>
<td>Specifies the number of milliseconds the system waits before assuming the cluster has dissolved. If the specified time passes without the member receiving cluster protocol keep-alive messages, the member leaves the cluster and attempts to rejoin. The range is 500 through 10000.</td>
</tr>
<tr>
<td>&lt;500–10000&gt;</td>
<td>500</td>
</tr>
<tr>
<td><strong>firewall-check-required</strong></td>
<td>Specifies whether this system should become a member of a cluster only if VPN-1/FireWall-1 is running. This option also specifies whether IPSO should monitor VPN-1/FireWall-1 and remove the member from the cluster if the firewall stops functioning.</td>
</tr>
<tr>
<td>&lt;yes</td>
<td>no&gt;</td>
</tr>
<tr>
<td><strong>interface log_if_name</strong></td>
<td>Specifies a logical interface name.</td>
</tr>
<tr>
<td><strong>cluster-address</strong></td>
<td>Specifies a cluster IP address for this interface or network. The cluster IP address is shared by all the cluster interfaces on a given network. When specified for an interface, the cluster address must belong to one of the networks with which the interface is configured.</td>
</tr>
</tbody>
</table>
Use the hash option to configure the manner in which IPSO balances traffic among cluster nodes. If you do not use NAT in the protected networks, use the default option. One node will handle incoming and outgoing traffic for a given connection.

Use the default option if you use NAT in the protected networks and want the cluster to support asymmetric connections. If you select this option, IPSO uses the source and destination IP addresses as inputs to its load balancing mechanism. Because the addresses are changed by NAT, the cluster might split the connection between two nodes.

If you are choosing the hash method for an interface that uses NAT, and the destination interface also uses NAT, use the default hash method for the interfaces at both ends of the link.

The other hash options use only one IP address (source or destination) as inputs to the load balancing mechanism. Use these options if you use NAT in the protected networks and want to force connections to be symmetric.

- For external interfaces, use the on-source-ip.
- For internal interfaces, use on-destination-ip.
General Clustering Commands

*join-remote ip_address* Specifies that the system you are logged into should become a member of an existing cluster by *joining*.

When joining a cluster, a system copies a variety of configuration settings from another cluster member (so you don’t have to configure these settings manually).

Specify an IP address of an existing cluster member that this system should copy configuration settings from. Follow these guidelines when specifying the IP address:

- The address should be assigned to an interface that belongs to the cluster master.
- The interface must be one of the master’s cluster interfaces.
- You should use the “real” address of the interface—not its cluster IP address.

*mode <mcast | mcast-group | forwarding | unicast>* Specifies the clustering mode. All cluster members must use the same mode. Use *mcast-group* if the cluster is connected to switches that are using IGMP snooping. This configuration restricts the clustering protocol traffic to only the cluster nodes.

*network network/mask* Specifies a network connected to one of the cluster interfaces. You must specify the appropriate subnet mask.

*performance-rating <0–65535>* Specifies the performance rating for this member.

*primary-interface log_if_name* Specifies the primary cluster protocol interface. Cluster members use this interface to exchange cluster protocol messages with the other cluster members.

For security reasons this interface should be an internal interface.

*primary-network network/mask* Specifies the primary cluster protocol network. Cluster members exchange cluster protocol messages over this network. Each member must use the same primary cluster protocol network.
remote-node ip_address performance-rating integer

Specifies the performance rating for another cluster member. You must specify the IP address of a cluster interface on the other member.

You can perform this command only if you have logged in as cadmin (a cluster administrator). See “Clustering Administration” for information about the cadmin user.

secondary-interface log_if_name

Specifies the (optional) secondary cluster protocol interface. Cluster members use this interface to exchange cluster protocol messages with the other cluster members if their primary cluster interface fails.

For security reasons this interface should be an internal interface.

secondary-network network/mask

Specifies the (optional) secondary cluster protocol network. Cluster members exchange cluster protocol messages over this network if the primary cluster protocol network fails. Each member must use the same secondary cluster protocol network.

state <up | down>

Configures the cluster state. The cluster state can be set to up only if:

- A primary interface is selected.
- The cluster has two interfaces configured with cluster IP addresses.
- All dynamic routing protocols and routing services are disabled.
- The member is configured with a valid performance rating.
### General Clustering Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>**work-assign &lt;static</td>
<td>dynamic&gt;**</td>
</tr>
<tr>
<td></td>
<td>- <strong>static</strong> prevents the cluster from moving active connections between nodes. Use for Check Point applications and features that require “bidirectional stickiness,” which means that all the packets for a given connection must be processed by the same node. Also use if you are using IP pools with non-Check Point gateways or clients.</td>
</tr>
<tr>
<td></td>
<td>- <strong>dynamic</strong> allows the cluster to periodically rebalance the load by moving active connections between nodes. Use for optimum load balancing.</td>
</tr>
<tr>
<td><strong>ip-pool network network/mask member ip_address</strong></td>
<td>Specifies a cluster member to manage the IP pool specified by network network/mask. range of addresses to use as an IP pool. ip_address must be the real IP address of the primary cluster protocol interface of the member that should manage the pool of addresses.</td>
</tr>
<tr>
<td></td>
<td>Use this command to specify IP pool addresses used with tunnels formed with non-Check Point gateways or clients. If the other end of the tunnel is a Check Point gateway, do not use this command—simply specify the IP pool using VPN-1 NG AI.</td>
</tr>
<tr>
<td>**securemote &lt;yes</td>
<td>no&gt;**</td>
</tr>
<tr>
<td>no</td>
<td></td>
</tr>
<tr>
<td>**vpn-clients &lt;yes</td>
<td>no&gt;**</td>
</tr>
<tr>
<td>no</td>
<td></td>
</tr>
<tr>
<td>**vpn-interop &lt;yes</td>
<td>no&gt;**</td>
</tr>
<tr>
<td>no</td>
<td></td>
</tr>
<tr>
<td><strong>vpn-tunnel network network/mask destination ip_address</strong></td>
<td>Specifies the end of a VPN tunnel formed with a non-Check Point gateway. Use network network/mask to specify the IPv4 network address and mask of the remote encryption domain. Use destination ip_address to specify the IPv4 address of the remote tunnel endpoint (non-Check Point gateway).</td>
</tr>
</tbody>
</table>

---

**Chapter 5  IP Clustering Commands  167**
Use the following commands to delete a cluster or to turn off specified features:

- delete cluster id <0–65535>
- delete cluster id <0–65535>
- feature feature
- interface log_if_name
- network network/mask
- secondary-interface log_if_name
- secondary-network network/mask
- delete cluster
- ip-pool network network/mask
- vpn-tunnel network network/mask

**Arguments**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>id &lt;0–65535&gt;</td>
<td>Specifies the unique identification number of the cluster.</td>
</tr>
<tr>
<td>feature feature</td>
<td>Specifies a feature to remove from the list of join-time shared features.</td>
</tr>
<tr>
<td>interface log_if_name</td>
<td>Specifies the logical name of an interface to disassociate from the cluster. You cannot delete the primary cluster protocol interface.</td>
</tr>
<tr>
<td>network network/mask</td>
<td>Specifies a network to disassociate from the cluster. You cannot delete the primary cluster protocol network.</td>
</tr>
<tr>
<td>secondary-interface log_if_name</td>
<td>Reconfigures the cluster so that the specified interface is no longer the secondary cluster protocol network. This command does not disassociate the interface from the cluster.</td>
</tr>
<tr>
<td>secondary-network network/mask</td>
<td>Reconfigures the cluster so that the specified network is no longer the secondary cluster protocol network. This command does not disassociate the network from the cluster.</td>
</tr>
<tr>
<td>ip-pool network network/mask</td>
<td>Deletes the specified IP pool.</td>
</tr>
<tr>
<td>vpn-tunnel network network/mask</td>
<td>Deletes the specified VPN tunnel.</td>
</tr>
</tbody>
</table>
Use the following commands to view various information about IPSO clusters:

```
show clusters
show cluster id <0-65535>
  coldstart-delay
  failure-interval
  features
  firewall-check-required
  info
  interfaces
  interface log_if_name cluster-address
  member info
  mode
  network network/mask cluster-address
  networks
  performance-rating
  primary-interface
  proto-state
  remote-node ip_address performance-rating
  secondary-interface
  secondary-network
  state
  work-assign
show cluster
  ip-pools
  securemote
  securemote clients
  vpn-clients
  vpn-interop
  vpn-tunnels
```
### Arguments

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>clusters</strong></td>
<td>Shows summary information a cluster configured on this system. If you logged in as admin, this command also shows a variety of cluster-related information about the member you logged into. If you logged in as cadmin, this command also shows a variety of information about each member of the cluster. See “Clustering Administration” for information about the cadmin user.</td>
</tr>
<tr>
<td><strong>coldstart-delay</strong></td>
<td>Shows the number of seconds the system waits before starting the cluster protocol.</td>
</tr>
<tr>
<td><strong>failure-delay</strong></td>
<td>Shows the number of milliseconds the system waits before assuming the cluster has dissolved.</td>
</tr>
<tr>
<td><strong>info</strong></td>
<td>Shows all the configuration and monitoring information for the specified cluster.</td>
</tr>
<tr>
<td><strong>features</strong></td>
<td>Shows the join-time shared features.</td>
</tr>
<tr>
<td><strong>firewall-check-required</strong></td>
<td>Shows whether the system will wait for VPN-1/FireWall-1 to start before it becomes a member of a cluster. This command also shows whether IPSO will monitor VPN-1/FireWall-1 and remove the member from the cluster if the firewall stops functioning.</td>
</tr>
<tr>
<td><strong>interfaces</strong></td>
<td>Shows the logical names of all the cluster interfaces.</td>
</tr>
<tr>
<td><strong>interface log_if_name cluster-address</strong></td>
<td>Shows the cluster IP address for the specified interface.</td>
</tr>
<tr>
<td><strong>member info</strong></td>
<td>If you logged in as admin, this command shows a variety of cluster-related information about the member you logged into. If you logged in as cadmin, this command shows a variety of information about each member of the cluster.</td>
</tr>
<tr>
<td><strong>mode</strong></td>
<td>Shows the clustering mode.</td>
</tr>
<tr>
<td><strong>network network/mask cluster-address</strong></td>
<td>Shows the cluster IP address for the specified network.</td>
</tr>
<tr>
<td><strong>networks</strong></td>
<td>Shows all the networks in which this cluster is participating.</td>
</tr>
<tr>
<td><strong>performance-rating</strong></td>
<td>Shows the performance rating of this member.</td>
</tr>
<tr>
<td><strong>primary-interface</strong></td>
<td>Shows logical name of the primary cluster protocol interface for the cluster.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>proto-state</td>
<td>Shows the cluster protocol state (master, member, or uninitialized).</td>
</tr>
<tr>
<td>remote-node ip_address</td>
<td>Shows the performance rating of the member specified by ip_address, which must be an IP address of the primary cluster protocol interface of one of the cluster members (including the member you are logged into).</td>
</tr>
<tr>
<td>performance-rating</td>
<td></td>
</tr>
<tr>
<td>secondary-interface</td>
<td>Shows the logical name of the secondary cluster protocol interface for the cluster.</td>
</tr>
<tr>
<td>secondary-network</td>
<td>Shows the secondary cluster protocol network for the cluster.</td>
</tr>
<tr>
<td>state</td>
<td>Shows the cluster state (up or down).</td>
</tr>
<tr>
<td>work-assign</td>
<td>Shows the work assignment method.</td>
</tr>
<tr>
<td>ip-pools</td>
<td>Shows the configuration of any IP pools used with VPN tunnels formed with non-Check Point gateways or clients.</td>
</tr>
<tr>
<td>secureremote</td>
<td>Shows whether SecuRemote client access is enabled.</td>
</tr>
<tr>
<td>secureremote clients</td>
<td>Shows whether there are any SecuRemote clients connected.</td>
</tr>
<tr>
<td>vpn-clients</td>
<td>Shows whether the cluster supports VPNs with non-Check Point clients.</td>
</tr>
<tr>
<td>vpn-interop</td>
<td>Shows whether the cluster supports VPNs with non-Check Point gateways.</td>
</tr>
<tr>
<td>vpn-tunnels</td>
<td>Shows the configuration of any VPN tunnels formed with non-Check Point gateways or clients.</td>
</tr>
</tbody>
</table>
If you log into command-line session with cadmin privileges (for example, if you use the user name cadmin), you are logged in as a cluster administrator. The prompt indicates this by showing CCLI and indicating the cluster ID. For example, the following prompt is for a cluster with the cluster ID 10:

NokiaCCLI:173 Cluster(10)>

(If there is no cluster configuration on a system, a cadmin user has not been created and you cannot log into the system as a cadmin user.)

As a cluster administrator, you can change and view configuration settings on all the cluster members in one command-line session.

A cluster administrator can configure each of the cluster members to use the same configuration settings for most clustering-related features. For example, if you are logged in as cadmin and enter

set cluster id 10 coldstart-delay 40

the coldstart delay is set to 40 seconds on all the cluster members.

Some cluster settings are not appropriate for being configured identically on all the members. For example, you cannot change the IP address of interfaces using the CCLI because interfaces on different members have different IP addresses. You can change cluster IP addresses because these must be consistent on all the members.

If you are logged in as cadmin and enter a command that is not available to a cluster administrator, the CLI responds that the command is invalid.
Managing Join-Time Shared Features

You may want to have many configuration settings be identical on each cluster node. Voyager makes this easy for you by letting you specify which features will be configured the same on all cluster nodes. The features that are configured this way are called *join-time shared features*. Their configurations are shared when:

- a node joins (or rejoins) the cluster
- a new master is selected because the original master has left the cluster (for example, if it was rebooted)

In addition to helping you make sure that all cluster members are configured consistently, using this feature makes the configuration process easier and faster.

To see the list of features that are shared at join time, enter

```
show cluster id integer features
```

To remove a feature from this list so that its configuration information is not copied to a system when the system joins a cluster, enter

```
delete cluster id integer feature feature
```

**Note** - To ensure that cluster members are configured identically, you should avoid deleting features from the list of join-time shared features after the cluster is operational.

Configuring Join-Time Shared Features

When you log in as cadmin and change a setting of a join-time shared feature, the change is made on all the members. If a system later joins the cluster, it copies the modified settings for this feature.

To configure the settings of join-time shared features, you use the same CLI commands as an admin user. To learn these commands, see the appropriate sections in this guide. For example, to configure ARP entries for a cluster, see the chapter on configuring interfaces.

Changes made to the configuration settings of shared features overwrite any conflicting settings made by someone logged into an individual member as admin. For example, assume that DNS is a shared feature and an admin user sets the domain name on one member to foo.bar.com. If you log in as cadmin and change the domain name to your.company.com, the new name replaces foo.bar.com.

However, nonconflicting changes made as admin on an individual member are not overwritten. For example, if an admin user configures a static route on a member and you later configure a static route as cadmin, the new route is added to the original route.

If you remove a feature from the list of join-time shared features, you can still configure this feature while logged in as cadmin. The change is made on all the members, but systems that join the cluster later do not copy the configuration settings for that feature. You see a message that alerts you to the fact that systems join later will not copy this setting.

If you log into a member as admin and change a setting of join-time shared feature, the change is implemented on the system you are logged into but not implemented on the other members. Check Point recommends that you do not make changes to cluster settings or cluster shareable features on individual members—log in as cadmin to make these changes.

Some settings of join-time shared features cannot be configured using the CCLI. For example, you cannot set SSH host and identity keys. To configure these settings, you must log into the individual cluster members as admin.

### Installing IPSO Images on a Cluster

As cadmin, you can upgrade the IPSO image on all the cluster members using one CLI session. (See “Managing IPSO Images” for information about upgrading images.)

After the new image has been successfully installed on all the members, you need to reboot them so that they will run the new image. Use the following commands to reboot cluster members:

```
reboot
reboot
image <name | last-download>
cluster-all
cluster-force
save
```
## Arguments

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>reboot</strong></td>
<td>Reboots each of the cluster members in a staggered manner so that only one member is out of service at a time. Used by itself, <em>reboot</em> will reboot the cluster members with the image they are running prior to the reboot.</td>
</tr>
<tr>
<td>**image &lt;name</td>
<td>last-download&gt;**</td>
</tr>
<tr>
<td><strong>cluster-all</strong></td>
<td>Use this command to reboot all the cluster members simultaneously. You will be prompted to verify that you want to reboot all the cluster members. If you reboot a cluster this way, there will be an interruption in service while all the members are rebooting.</td>
</tr>
<tr>
<td><strong>cluster-force</strong></td>
<td>Use this command to reboot all the cluster members simultaneously. You will not be prompted to verify that you want to reboot all the cluster members. If you reboot a cluster this way, there will be an interruption in service while all the members are rebooting.</td>
</tr>
<tr>
<td><strong>save</strong></td>
<td>Saves any unsaved configuration changes prior to booting.</td>
</tr>
</tbody>
</table>
This chapter describes the SNMP configuration commands that you can enter from the initial CLI prompt, called Command mode.

In This Chapter

SNMP Description  page 178
SNMP Command Set  page 179
Enabling/Disabling and Setting SNMP  page 181
Enabling and Disabling SNMP Traps  page 184
Managing SNMP Users  page 187
Show SNMP Implementation and Trap Commands  page 188
SNMP Error Messages  page 189
SNMP Description

Use this group of commands to set and view parameters for SNMP. Through the SNMP protocol, network management applications can query a management agent using a supported MIB. The Check Point SNMP implementation lets an SNMP manager monitor the system and modify selected objects only. You can define and change one read-only community string and one read-write community string. You can set, add, and delete trap receivers and enable or disable various traps. You can also enter the location and contact strings for the system.

For more detailed information about the MIBs that the Check Point implementation supports, download a pdf version of the online documentation from the Check Point support site at http://support.checkpoint.com. To view detailed information about each supported MIB, go to the /etc/snmp/mibs directory.

The Check Point implementation also supports the User-based Security model (USM) portion of SNMPv3.
SNMP Command Set

Use the following commands for configuring SNMP parameters.

set snmp

    daemon <on | off>
    snmp smp-version <v1/v2/v3 | v3-Only>
    trapreceiver ip_address community string version <v1 | v2>
    trapreceiver ip_address version <v1 | v2>
    trapPduAgent ip_address
    location string
    contact string

Use the following commands to configure SNMP traps.

set snmp traps

    coldstart status <on | off>
    link-up-down status <on | off>
    authorization status <on | off>
    vrrp-newmaster status <on | off>
    vrrp-authfail status <on | off>
    sys-config-change status <on | off>
    sys-config-filechange status <on | off>
    sys-config-savechange status <on | off>
    sys-lowdiskspace status <on | off>
    sys-nodiskspace status <on | off>
    sys-diskfailure status <on | off>
    sys-diskmirr-create status <on | off>
    sys-diskmirr-delete status <on | off>
    sys-diskmirr-syncfail status <on | off>
    sys-diskmirr-syncc-success status <on | off>
    cluster-member-join status <on | off>
    cluster-member-left status <on | off>
SNMP Command Set

cluster-new-master status <on | off>
cluster-member-reject status <on | off>
cluster-protocol-interface-change status <on | off>
sys-fan-failure status <on | off>
sys-powersupply-failure status <on | off>
sys-overtemperature status <on | off>

Use the following commands to configure other SNMP parameters.
add snmp
  address ipaddress
  community string read-only
  community string read-write

Note - The default community string is public.

trapreceiver ip_addr community string version <v1 | v2>
delete snmp
  address ipaddress
  community string read-only
  community string read-write
  trapreceiver ip_address

For more detailed information about how to enable SNMP and configure basic settings, see "Enabling/Disabling and Setting SNMP" on page 181.

For more detailed information about SNMP traps, see "Enabling and Disabling SNMP Traps" on page 184.

For more detailed information about SNMPv3 and USM Users, see "Managing SNMP Users" on page 187.
Enabling/Disabling and Setting SNMP

Use the following commands to enable or disable SNMP and to set and change such parameters as the community strings, the Trap Receiver and PDU Agent address.

```
set snmp
  daemon <on | off>
```

**Warning** - If you run the Check Point and IPSO SNMP daemons simultaneously, you must start the Check Point SNMP daemon after you start VPN-1/FireWall-1 NG. If you start the Check Point daemon before you start VPN-1/FireWall-1 NG, the IPSO daemon does not start.

```
  snmp smp-version <v1/v2/v3 | v3-Only>
  trapreceiver ip_address community string version <v1 | v2>
  trapreceiver ip_address version <v1 | v2>
  trapPduAgent ip_address
  location string
  contact string
add snmp
  address ip_address
  community string read-only
  community string read-write
  trapreceiver ip_addr community string version <v1 | v2>
```

```
delete snmp
  address ip_address
  community string read-only
  community string read-write
  trapreceiver ip_address
```

**Note** - Use the set commands to configure initial settings and use the add commands to configure community strings and additional trap receivers.
## Arguments

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>daemon &lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td>snmp-version &lt;v1/v2/v3</td>
<td>v3-Only&gt;</td>
</tr>
<tr>
<td>snmp address ip_address</td>
<td>Specifies a IP address on which the agent responds to requests. The default is for the protocol to respond to requests from all interfaces. If you set a specific address, and want to revert to the default, use the delete snmp ip_address command.</td>
</tr>
<tr>
<td>snmp community string read-only</td>
<td>Sets a read-only community string. Use alphanumeric characters with no spaces, the hyphen symbol and the underscore symbol only. If you delete the read-only community strings, SNMP GETS are not possible unless a read-write community string is configured that equals the input read community string.</td>
</tr>
<tr>
<td>snmp community string read-write</td>
<td>Sets a read-write community string. Use alphanumeric characters with no spaces, the hyphen symbol and the underscore symbol only. If you disable the SNMP community read-write string, SNMP SETS are not possible.</td>
</tr>
<tr>
<td>trapreceiver ip_address community string version &lt;v1</td>
<td>v2&gt;</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><code>trapPduAgent ip_address</code></td>
<td>Specifies the address used as the agent address in the protocol data unit of traps sent. This IP address must belong to a configured interface. Beginning with IPSO 3.7, if you do not configure a Trap PDU Agent address, the system identifies the PDU Trap Agent address as 0.0.0.0 in SNMP traps. This change is in accordance with RFC 2089. For all previous releases of IPSO, the default was to use the IP address of the first valid interface.</td>
</tr>
<tr>
<td><code>location string</code></td>
<td>Specifies a string that contains the location for the system. The maximum length for the string is 128 characters including letters, numbers, spaces, special characters. For example: Bldg 1, Floor 3, WAN Lab, Fast Networks, Speedy, CA</td>
</tr>
<tr>
<td><code>contact string</code></td>
<td>Specifies a string that contains the contact information for the device. The maximum length for the string is 128 characters including letters, numbers, spaces, special characters. For example: John Doe, Network Administrator, (111) 222-3333</td>
</tr>
</tbody>
</table>
Enabling and Disabling SNMP Traps

Use the following command to enable or disable individual SNMP Traps.

```
set snmp traps

coldstart status <on | off>
link-up-down status <on | off>
authorization status <on | off>
vrp-newmaster status <on | off>
vrp-authfail status <on | off>
sys-config-change status <on | off>
sys-config-filechange status <on | off>
sys-config-savechange status <on | off>
sys-lowdiskspace status <on | off>
sys-nodiskspace status <on | off>
sys-diskfailure status <on | off>
sys-diskmirr-create status <on | off>
sys-diskmirr-delete status <on | off>
sys-diskmirr-syncfail status <on | off>
sys-diskmirr-syncsuccess status <on | off>
cluster-member-join status <on | off>
cluster-member-left status <on | off>
cluster-new-master status <on | off>
cluster-member-reject status <on | off>
cluster-protocol-interface-change status <on | off>
sys-fan-failure status <on | off>
sys-powersupply-failure status <on | off>
sys-overtemperature status <on | off>
```

**Note** - Only the cold start and authorization traps are enabled by default. You must enable all other traps.
# Enabling and Disabling SNMP Traps

## Arguments

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>status &lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td>coldstart</td>
<td>coldstart trap signifies that the SNMPv2 entity, acting in an agent role, is reinitializing itself and that its configuration might have been altered. The coldstart trap is enabled by default.</td>
</tr>
<tr>
<td>link-up-down</td>
<td>ifLinkUpDown trap is sent when one of the links, which is administratively up, either has come up or been lost. The linkUpDown trap is enabled by default.</td>
</tr>
<tr>
<td>authorization</td>
<td>authenticationFailure trap sends notification that the SNMP message received from the sending entity is not properly authenticated.</td>
</tr>
<tr>
<td>vrrp-newmaster</td>
<td>vrrpTrapNewMaster sends notification of a new VRRP master router.</td>
</tr>
<tr>
<td>vrrp-authfail</td>
<td>vrrpTrapAuthFailure sends notification of a VRRP authentication failure.</td>
</tr>
<tr>
<td>sys-config-change</td>
<td>systemTrapConfigurationChange is sent when a change is made to the running system configuration</td>
</tr>
<tr>
<td>sys-config-filechange</td>
<td>systemTrapConfigurationChange is sent when a change is made to system configuration files</td>
</tr>
<tr>
<td>sys-config-savechange</td>
<td>systemTrapConfigurationSaveChange is sent when a change is made to the running system configuration and saved to the database.</td>
</tr>
<tr>
<td>sys-lowdiskspace</td>
<td>systemTrapLowDiskSpace sent when the disk utilization, as seen by a non-superuser, in any of the local file systems exceeds 80%. The trap is initially sent within the scan interval (currently 30 seconds), and subsequently, at preset intervals of 15 minutes, until the disk utilization falls below 80%.</td>
</tr>
<tr>
<td>sys-nodiskspace</td>
<td>systemTrapNoDiskSpace is sent when the disk utilization, as seen by a non-superuser, in any of the local file systems exceeds 98%. The trap is initially sent within the scan interval (currently 30 seconds), and subsequently, at preset intervals of 15 minutes, until the disk utilization falls below 98%.</td>
</tr>
</tbody>
</table>
Enabling and Disabling SNMP Traps

<table>
<thead>
<tr>
<th>Trap Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sys-diskfailure</td>
<td>systemTrapDiskFailure is sent when a particular disk drive fails, that is, there is no response from the disk for read/write operations. This trap applies on the IP530 and the IP740.</td>
</tr>
<tr>
<td>sys-diskmirr-create</td>
<td>systemTrapDiskMirrorSetCreate is sent when a particular mirror set has been created on the system.</td>
</tr>
<tr>
<td>sys-diskmirr-delete</td>
<td>systemTrapDiskMirrorSetDelete is sent when a particular mirror set has been deleted from the system.</td>
</tr>
<tr>
<td>sys-diskmirr-syncfail</td>
<td>systemTrapDiskMirrorSyncFailure is sent when a particular mirror set fails during syncing.</td>
</tr>
<tr>
<td>sys-diskmirr-syncsuccess</td>
<td>systemTrapDiskMirrorSyncSuccess is sent when a particular mirror set has been successfully synced.</td>
</tr>
<tr>
<td>cluster-member-join</td>
<td>ipsoLBClusterMemberJoin trap is sent when a member node joins the cluster by the master.</td>
</tr>
<tr>
<td>cluster-member-left</td>
<td>ipsoLBClusterMemberLeft trap is sent when a member node leaves the cluster by the master.</td>
</tr>
<tr>
<td>cluster-new-master</td>
<td>ipsoLBClusterNewMember trap is sent when a cluster is formed and a new master is elected.</td>
</tr>
<tr>
<td>cluster-member-reject</td>
<td>ipsoLBJoinReject trap is sent when a member’s request to join a cluster is rejected.</td>
</tr>
<tr>
<td>cluster-protocol-interface-change</td>
<td>clusterProtocolInterfaceChange trap is sent when a failover occurs from the primary cluster to the secondary cluster network.</td>
</tr>
<tr>
<td>sys-fan-failure</td>
<td>systemFanFailure trap is sent when a fan fails. This trap includes the fan index and is supported only on the IP530 and IP740 platforms.</td>
</tr>
<tr>
<td>sys-powersupply-failure</td>
<td>systemPowerSupplyFailure trap is sent when a power supply for the system fails. This trap includes the power supply index and is supported only on the IP530 and IP740 platforms.</td>
</tr>
<tr>
<td>sys-overtemperature</td>
<td>systemOverTemperature trap is sent when a power supply failure occurs because of high temperature. This trap is followed by a power supply failure that specifies the power supply index that failed. This trap is supported only on the IP530 and IP740 platforms.</td>
</tr>
</tbody>
</table>
Managing SNMP Users

Use the following commands to add users who are authorized to use SNMPv3.
add snmp usm user username
   seclvl <authPriv | authNoPriv | authPrivReq>
   authpassphrase authphrase privpassphrase privacyphrase

Use the following command to change a user security-level setting or pass phrases.
set snmp usm user username
   seclvl <authPriv | authNoPriv | authPrivReq>
   authpassphrase authphrase privpassphrase privacyphrase

Use the following command to delete an existing SNMP user.
delete snmp usm user username

Use the following command to view existing SNMP users.
show snmp usm user username
show snmp users

Arguments

<table>
<thead>
<tr>
<th>Argument</th>
<th>Range: 1 to 31 alphanumeric characters with no spaces, backslash, or colon characters.</th>
</tr>
</thead>
<tbody>
<tr>
<td>username</td>
<td></td>
</tr>
<tr>
<td>seclvl</td>
<td>Security Level. Select from the following:</td>
</tr>
<tr>
<td>&lt;authPriv</td>
<td>authNoPriv—User has authentication and privacy pass phrases and can connect with or without privacy encryption.</td>
</tr>
<tr>
<td>authNoPriv</td>
<td>authPriv—User has only an authentication pass phrase and can connect only without privacy encryption.</td>
</tr>
<tr>
<td>authPriv</td>
<td>authPrivReq—User must use authentication and privacy encryption pass phrases to connect.</td>
</tr>
<tr>
<td>authpassphrase</td>
<td>Range: 8-128 characters.</td>
</tr>
<tr>
<td>privpassphrase</td>
<td>Range: 8-128 characters.</td>
</tr>
</tbody>
</table>
Show SNMP Implementation and Trap Commands

    show snmp
daemon
community
trapreceiver
traps
snmp trapPduAgent
snmp location
snmp contact
SNMP Error Messages

This section lists and explains certain common error status values that can appear in SNMP messages. Within the protocol-data unit (PDU), the third field can include an error-status integer that refers to a specific problem. The integer zero (0) means that no errors were detected. When the error-field is anything other than 0, the next field, includes an error-index value that identifies the variable, or object, in the variable-bindings list that caused the error.
See the table below for the error status codes and their corresponding meanings.

<table>
<thead>
<tr>
<th>Error Status Code</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>noError</td>
</tr>
<tr>
<td>1</td>
<td>tooBig</td>
</tr>
<tr>
<td>2</td>
<td>NoSuchName</td>
</tr>
<tr>
<td>3</td>
<td>BadValue</td>
</tr>
<tr>
<td>4</td>
<td>ReadOnly</td>
</tr>
<tr>
<td>5</td>
<td>genError</td>
</tr>
<tr>
<td>6</td>
<td>noAccess</td>
</tr>
<tr>
<td>7</td>
<td>wrongType</td>
</tr>
<tr>
<td>8</td>
<td>wrongLength</td>
</tr>
<tr>
<td>9</td>
<td>wrongEncoding</td>
</tr>
<tr>
<td>10</td>
<td>wrongValue</td>
</tr>
<tr>
<td>11</td>
<td>noCreation</td>
</tr>
<tr>
<td>12</td>
<td>inconsistentValue</td>
</tr>
<tr>
<td>13</td>
<td>resourceUnavailable</td>
</tr>
<tr>
<td>14</td>
<td>commitFailed</td>
</tr>
<tr>
<td>15</td>
<td>undoFailed</td>
</tr>
<tr>
<td>16</td>
<td>authorizationError</td>
</tr>
<tr>
<td>17</td>
<td>notWritable</td>
</tr>
<tr>
<td>18</td>
<td>inconsistentName</td>
</tr>
</tbody>
</table>

Note - You do not necessarily see the codes. The SNMP manager or utility interprets the codes and displays and logs the appropriate message.

The subsequent, or fourth field, contains the error-index when the error-status field is nonzero, that is, when the error-status field returns a value other than zero, which indicates that an error occurred. The error-index value identifies the variable, or object, in the variable-bindings list that caused the error. The first variable in the list has index 1, the second has index 2, and so on.
The next, or fifth field, is the variable-bindings field. It consists of a sequence of pairs; the first is the identifier. The second element is one of the following five: value, unSpecified, noSuchObject, noSuchInstance, and EndofMibView. The table below describes each element.

<table>
<thead>
<tr>
<th>Variable-Binding</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>value</td>
<td>the value associated with each object instance; specified in a PDU request</td>
</tr>
<tr>
<td>unSpecified</td>
<td>a NULL value is used in retrieval requests</td>
</tr>
<tr>
<td>noSuchObject</td>
<td>indicates that the agent does not implement the object referred to by this object identifier</td>
</tr>
<tr>
<td>noSuchInstance</td>
<td>indicates that this object does not exist for this operation</td>
</tr>
<tr>
<td>endOfMIBView</td>
<td>indicates an attempt to reference an object identifier that is beyond the end of the MIB at the agent</td>
</tr>
</tbody>
</table>

**GetRequest**

The following are possible value field sets in the response PDU or error-status messages when performing a *GetRequest*.

<table>
<thead>
<tr>
<th>Value Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>noSuchObject</td>
<td>If a variable does not have an <em>OBJECT IDENTIFIER</em> prefix that exactly matches the prefix of any variable accessible by this request, then its value field is set to <em>noSuchObject</em>.</td>
</tr>
<tr>
<td>noSuchInstance</td>
<td>If the variable's name does not exactly match the name of a variable, then its value field is set to <em>noSuchInstance</em>.</td>
</tr>
<tr>
<td>genErr</td>
<td>If the processing of a variable fails for any other reason, the responding entity returns <em>genErr</em> and a value in the error-index field that is the index of the problem object in the variable-bindings field.</td>
</tr>
<tr>
<td>tooBig</td>
<td>If the size of the message that encapsulates the generated response PDU exceeds a local limitation or the maximum message size of the request’s source party, then the response PDU is discarded and a new response PDU is constructed. The new response PDU has an error-status of <em>tooBig</em>, an error-index of zero, and an empty variable-bindings field.</td>
</tr>
</tbody>
</table>
**GetNextRequest**

The only values that can be returned in as the second element in the
variable-bindings field to a GetNextRequest when an error-status code occurs are
unSpecified or endOfMibView.

**GetBulkRequest**

The GetBulkRequest minimizes the number of protocol exchanges by letting an
SNMPv2 manager request that the response be as large as possible given the
constraints on the message size.

The GetBulkRequest PDU has two fields that do not appear in the other PDUs:
non-repeaters and max-repetitions. The non-repeaters field specifies the number of
variables in the variable-bindings list for which a single-lexicographic successor is
to be returned. The max-repetitions field specifies the number of lexicographic
successors to be returned for the remaining variables in the variable-bindings list.

If at any point in the process, a lexicographic successor does not exist, the
endofMibView value is returned with the name of the last lexicographic successor,
or, if there were no successors, the name of the variable in the request.

If the processing of a variable name fails for any reason other than endofMibView,
no values are returned. Instead, the responding entity returns a response PDU with
an error-status of genErr and a value in the error-index field that the is the index of
the problem object in the variable-bindings field.
Chapter 7
IPv6 Commands

Use the commands in this chapter to configure most IPv6 settings for your system.

In This Chapter

- Configuration Summary  page 194
- Interface Commands  page 195
- Neighbor Discovery Protocol  page 197
- IPv6 to IPv4  page 199
- IPv6 Over IPv4  page 200
- IPv6 Routing Configuration  page 201
Configuration Summary

Use the following command to show a summary of IPv6 configuration on your system:

`show ipv6 config`
Interface Commands

Use the following commands to associate an IPv6 address with a logical interface, anycast address, or IPv6 address family:

```
add interface if_name
    ipv6prefix ip6_address/mask
    anycast ip6_address
    family inet6
```

Use the following commands to disassociate an IPv6 address from a logical interface, anycast address, or IPv6 address family:

```
delete interface if_name
    ipv6prefix ip6_address/mask
    anycast ip6_address
    family inet6
```

**Arguments**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface if_name</td>
<td>Specifies the name of an existing logical interface.</td>
</tr>
<tr>
<td>Note</td>
<td>You cannot disable an IPv6 interface configured for a virtual router when the router is in the master state. If you try to disable the interface, when the router is in the master state, the console displays an error message. To disable the IPv6 interface, you must first delete the interface as a VRRP virtual address. You can, however, disable an IPv6 interface enabled on a virtual router when the router is in a backup state.</td>
</tr>
<tr>
<td>ipv6prefix</td>
<td>Specifies the IPv6 address and mask length. The mask length range is &lt;8–126&gt;.</td>
</tr>
<tr>
<td>ip6_address/mask</td>
<td>- Format: IPv6 Prefix/&lt;8–126&gt;</td>
</tr>
<tr>
<td></td>
<td>- Example: 1000:50:32::3/64</td>
</tr>
<tr>
<td>anycast ip6_address</td>
<td>Specifies an anycast address. When you assign an IPv6 anycast address to multiple interfaces (typically on different systems), packets sent to an anycast address are routed to the nearest interface that matches the address of the packet.</td>
</tr>
<tr>
<td>family inet6</td>
<td>Add an IPv6 address family to the specified logical interface.</td>
</tr>
</tbody>
</table>
Use the following commands to view information about IPv6 interfaces configured on your system.

show ipv6
  interfaces
  interface if_name
show interface if_name ipv6prefix

Arguments

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interfaces</td>
<td>Displays summary information about all configured IPv6 interfaces.</td>
</tr>
<tr>
<td>interface if_name</td>
<td>Displays information about a specified logical interface.</td>
</tr>
<tr>
<td>interface if_name ipv6prefix</td>
<td>Displays configured IPv6 prefixes for the specified logical interface.</td>
</tr>
</tbody>
</table>
Neighbor Discovery Protocol

The Neighbor Discovery Protocol (NDP) allows you to map an IPv6 address to a physical machine address recognized in the local network.

Use the following command to add a new static Neighbor Discovery entry:
```
add neighbor-entry address ip6_address macaddress mac_address
```

Use the following command to remove a static Neighbor Discovery entry:
```
delete neighbor-entry address ip6_address
```

**Arguments**

<table>
<thead>
<tr>
<th>Address</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>address ip6_address</td>
<td>Specifies the IPv6 address of the static NDP entry to add or delete.</td>
</tr>
<tr>
<td></td>
<td>• Format: IPv6 address</td>
</tr>
<tr>
<td></td>
<td>• Example: 1000:50:32::2</td>
</tr>
</tbody>
</table>

| macaddress mac_address | Specifies the MAC address for the associated IPv6 interface address.          |
|                        | • Format: hexadecimal digits                                                  |
|                        | • Example: 00:a0:8e:86:73:60                                                   |

Use the following commands to configure global NDP properties:
```
set neighbor
duplicate-detection <1-100>
multicast-limit <1-100>
queue-limit <1-3>
unicast-limit <1-100>
```

**Arguments**

<table>
<thead>
<tr>
<th>Address</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>duplicate-detection</td>
<td>Specifies the number of times to retry Duplicate Address Detection NDP requests.</td>
</tr>
<tr>
<td></td>
<td>• Default: 3</td>
</tr>
</tbody>
</table>

| multicast-limit       | Specifies the number of times to retry Multicast NDP requests.                |
|                       | • Default: 3                                                                 |
**Neighbor Discovery Protocol**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>queue-limit &lt;1-3&gt;</td>
<td>Specifies the maximum number of output packets to be queued while resolving link-layer destination address.</td>
</tr>
<tr>
<td>unicast-limit &lt;1-100&gt;</td>
<td>Specifies the number of times to retry Unicast NDP requests.</td>
</tr>
</tbody>
</table>

Use the following commands to view NDP configuration details:

- `show neighbor`
- `dynamic-table`
- `interface-table`
- `parameters`
- `static-table`
- `table`

**Arguments**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dynamic-table</td>
<td>Displays the dynamically learned neighbor IPv6 addresses and their respective MAC addresses.</td>
</tr>
<tr>
<td>interface-table</td>
<td>Displays the IPv6 addresses and MAC addresses of currently configured interfaces listed in the neighbor table.</td>
</tr>
<tr>
<td>parameters</td>
<td>Displays neighbor table parameters, including each configurable field and its associated value.</td>
</tr>
<tr>
<td>static-table</td>
<td>Displays neighbor table static entries.</td>
</tr>
<tr>
<td>table</td>
<td>Displays the entire neighbor table including static entries, interface entries, and dynamic entries.</td>
</tr>
</tbody>
</table>
IPv6 to IPv4

Use the commands in this section to configure an IPv6 interface attached to an IPv4 network that does not have IPv6 native support. This feature allows you to connect IPv6 domains through IPv4 clouds without explicit tunnels.

Use the following commands to create and configure an IPv6 to IPv4 interface, or to delete existing IPv6 to IPv4 settings. The time to live (TTL) argument is optional.

set ipv6toipv4

    active on address ip_address enable [ttl <1–255>] [instance instance_name]
    disable [instance instance_name]

Use the following command to activate or deactivate an existing IPv6 to IPv4 interface:

set ipv6toipv4 active <on | off> [instance instance_name]

Arguments

active on address ip_address ✦ Activates the IPv6 to IPv4 feature. You must specify the local IPv4 address to activate this feature if the interface association does not already exist or if you disable it.

ttl <1–255> ✦ Specifies the time to live (TTL) of packets sent on the tunnel. This argument is optional.

Default: 255

instance instance_name ✦ Specifies the name of the routing instance to which this command applies. This argument is valid only if you already configured multiple routing instances.

disable ✦ Deletes the settings.

<on | off> ✦ Activates or deactivates existing IPv6 to IPv4 settings. If you use active off, you do not lose the current settings.

Use the following command to view the IPv6 to IPv4 configuration on your system:

show ipv6toipv4
**IPv6 Over IPv4**

Use the following commands to create and enable or disable an IPv6 interface attached to an IPv4 network that does not have IPv6 native support. This feature allows you to transmit IPv6 traffic over IPv4 domains without explicit tunnels.

Use the following commands to create and configure IPv6 to IPv4 features, or to delete IPv6 to IPv4 settings. The time to live (TTL) argument is optional.

```
set ipv6overipv4
  active on address ip_address enable [ttl <1-255>] [instance instance_name]
  disable [instance instance_name]
```

Use the following command to activate or deactivate the IPv6 to IPv4 settings for an interface.

```
set ipv6overIPv4 active <on | off> [instance instance_name]
```

**Arguments**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>active on address ip_address enable [ttl &lt;1-255&gt;] [instance instance_name]</td>
<td>Activates the IPv6 over IPv4 feature. You must specify the local IPv4 address to activate this feature if the interface association does not already exist or if you disable it.</td>
</tr>
<tr>
<td>ttl &lt;1-255&gt;</td>
<td>Specifies the time to live (TTL) of packets sent on the tunnel. This argument is optional.</td>
</tr>
<tr>
<td>instance instance_name</td>
<td>Specifies the name of the routing instance to which this command applies. This argument is valid only if you already configured multiple routing instances. For IPv6 over IPv4, only the default instance is accepted.</td>
</tr>
<tr>
<td>disable</td>
<td>Deletes the settings.</td>
</tr>
<tr>
<td>&lt;on</td>
<td>off&gt;</td>
</tr>
</tbody>
</table>

Use the following command to view the IPv6 to IPv4 configuration on your system:

```
show ipv6overipv4
```
IPv6 Routing Configuration

Use the commands in this section to configure IPv6 routing on your system.

RIPng

Use this group of commands to set and view parameters for RIP next generation (RIPng).

Note - IPSO does not have CLI commands for route filtering and redistribution. You must configure inbound routing policies and redistribution of routes through Voyager. You can configure route maps and route aggregation using CLI commands. Route map configuration done through the CLI takes precedence over route filtering and redistribution configured in Voyager. For example if RIP uses route maps for inbound filtering, anything configured on the Voyager page for inbound route filters for RIP is ignored. You can still use Voyager to configure route redistribution into RIP.

Interfaces

Use the following commands to configure RIPng properties for specific interfaces:

set ipv6 ripng interface if_name
  <on | off >
  metric <0-16>
  metric default

Arguments

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td>metric &lt;0-16&gt;</td>
<td>Specifies the RIP metric added to routes that use the specified interface.</td>
</tr>
<tr>
<td>metric default</td>
<td>Specifies a value of 0.</td>
</tr>
</tbody>
</table>

Show Commands

Use the following commands to monitor and troubleshoot RIPng:

show ipv6 ripng
Route Aggregation

Use the following group of commands to aggregate numerous specific routes into one route. Route aggregation potentially reduces the number of routes that given protocol advertises.

Only the receiver, and not the originator, of an aggregate route uses it for forwarding packets. The originator of the aggregate route uses individual component routes to determine reachability. A router that receives a packet that does not match one of the component routes of the aggregate responds with an Internet Control Message Protocol (ICMP) network unreachable message. This message prevents packets or unknown component routes from following a default route to another network where they would be continually forwarded back to the border router until their time to live (TTL) expires.

Create an aggregate route by first specifying the network address and mask length. Next, provide a set of contributing routes. To define a contributing route, specify a source (static route, interface route, or routing protocol) and a route filter (an IPv6 prefix). An aggregate route can have many contributing routes, but at least one of the routes must be present to generate an aggregate. The off argument deactivates a specified IPv6 aggregate route.

```
set [instance instance_name] ipv6 aggregate ip6_prefix
  off
  contributing-protocol
  <all | direct | static | aggregate | ripng> off
  contributing-protocol
  <all | direct | static | aggregate | ripng>
  contributing-route <all | ip6_prefix> <on | off>
```
Static Routes

Arguments

```
<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip6_prefix</td>
<td>Specifies the IPv6 address and mask length of the new aggregate route and</td>
</tr>
<tr>
<td></td>
<td>the contributing protocol or interface route:</td>
</tr>
<tr>
<td></td>
<td>• Example: 1000:50:32::/64</td>
</tr>
<tr>
<td>off</td>
<td>Deactivates the specified aggregate route.</td>
</tr>
<tr>
<td>contributing-protocol</td>
<td>Specifies the contributing route source type or protocol to turn off:</td>
</tr>
<tr>
<td>&lt;all</td>
<td>direct</td>
</tr>
<tr>
<td>contributing-route</td>
<td>Specifies the contributing route to turn on or off for the specific</td>
</tr>
<tr>
<td>&lt;all</td>
<td>ip6_prefix&gt;</td>
</tr>
<tr>
<td></td>
<td>contributing protocol. You must use this argument after specifying a</td>
</tr>
<tr>
<td></td>
<td>contributing protocol.</td>
</tr>
<tr>
<td></td>
<td>• all — Contribute all the routes for a specific source type or protocol.</td>
</tr>
<tr>
<td></td>
<td>• ip6_prefix — Contribute a specific route.</td>
</tr>
</tbody>
</table>
```

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.

Use the following group of commands to configure specific static routes:
```
set slot <1-15> [instance instance_name] ipv6 static-route
  ip6_prefix nexthop gateway ip6_address priority <1-8> <on | off>
default nexthop gateway ip6_address priority < 1-8> <on | off>
  ip6_prefix nexthop gateway ip6_address interface if_name priority <1-8> <on | off>
```
default nexthop gateway ip6_address interface if_name <on | off>

ip6_prefix nexthop reject
default nexthop reject

ip6_prefix nexthop blackhole
default nexthop blackhole

ip6_prefix off
default off

Arguments

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>static-route ip6_prefix</td>
<td>Specifies the IPv6 prefix and mask length of the static route. Use the off argument to disable the specified route. Use the other arguments to configure properties of the specified route and enable or disable them.</td>
</tr>
<tr>
<td>static-route default</td>
<td>Specifies the default static route. Use the off argument to disable the default route. Use the other arguments to configure default route properties and enable or disable them.</td>
</tr>
<tr>
<td>nexthop gateway ip6_address &lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td>nexthop gateway ip6_address interface if_name &lt;on</td>
<td>off&gt;</td>
</tr>
</tbody>
</table>

Address example: 1000:50.32::/64
Address example: 1000:50:32::1
Interface example: eth-s1p1c0
**ICMP Router Discovery**

Use this group of commands to set and view parameters for the ICMP router discovery protocol.

**Interfaces**

Use the following commands to configure router discovery properties for specific interfaces:

```bash
set ipv6 rdisc6 interface if_name
  <on | off>
  min-adv-interval <3-1800>
  min-adv-interval default
  max-adv-interval <4-1800>
  max-adv-interval default
  hop-limit <0-255>
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>priority &lt;1-8&gt;</td>
<td>Specifies the order in which next hops are selected. The lower the value the more preferred the link. The next preferred value is selected as the next hop only when an interface fails. A non-reachable link is not selected as the next hop.</td>
</tr>
<tr>
<td>Note - The priority option also supports equal-cost multipath routing. For each priority value, you can configure as many as eight gateway addresses. The nexthop gate address for each packet to the destination is selected based on the nexthop algorithm that is configured.</td>
<td></td>
</tr>
<tr>
<td>ip6_prefix nexthop</td>
<td>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.</td>
</tr>
<tr>
<td>reject</td>
<td></td>
</tr>
<tr>
<td>ip6_prefix nexthop</td>
<td>Specifies for packets to be dropped rather than forwarded but does not specify for unreachable messages to be sent to the packet originator.</td>
</tr>
<tr>
<td>backhole</td>
<td></td>
</tr>
<tr>
<td>ip6_prefix off</td>
<td>Deletes the specified static route and deletes any next hops associated with the route.</td>
</tr>
<tr>
<td>default off</td>
<td>Deletes the default route and deletes any next hops associated with the route.</td>
</tr>
</tbody>
</table>
hop-limit default
managed-config <on | off>
other-config <on | off>
reach-time <0–3600000>
reach-time default
retransmit-timer integer
retransmit-timer default
router-lifetime integer
router-lifetime default
send-mtu <on | off>

Use the following commands only if the mask length is not greater than 64:
set ipv6 rdisc6 interface if_name
   address ip6_address autonomous <on | off>
   address ip6_address on-link <on | off>
   address ip6_address prefix-pref-lifetime integer
   address ip6_address prefix-pref-lifetime default
   address ip6_address prefix-valid-lifetime integer
   address ip6_address prefix-valid-lifetime default

Arguments

<on | off> Specifies whether to run ICMPv6 router discovery on a specified interface.
min-adv-interval <3–1800> Specifies the minimum time (in seconds) allowed between sending unsolicited broadcast or multicast ICMPv6 router advertisements on the interface.

Note - Beginning with IPSO 3.8.1 and as part of the new support of VRRP for IPv6 interfaces, only the router in a VRRP master state sends router discovery advertisements, and the advertisements are sent with the virtual IP address as the source address and the virtual MAC address as the MAC address. Routers in a VRRP backup state do not send router discovery advertisements. For more information about how to configure VRRP for IPv6 interfaces, see “VRRP for IPv6” on page 209.
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>min-adv-interval</td>
<td>Specifies a value of 450 seconds.</td>
</tr>
<tr>
<td>max-adv-interval</td>
<td>Specifies the maximum time (in seconds) allowed between sending unsolicited broadcast or multicast ICMPv6 router advertisements on the interface.</td>
</tr>
<tr>
<td>max-adv-interval default</td>
<td>Specifies a value of 600 seconds.</td>
</tr>
<tr>
<td>hop-limit &lt;0-255&gt;</td>
<td>Specifies the value placed in the Cur Hop Limit field in the router advertisement packet. Systems use this value in the Hop Count field of the IP header for outgoing IP packets. This value should be set to the current diameter of the Internet. The value zero (0) means unspecified (by this router).</td>
</tr>
<tr>
<td>hop-limit default</td>
<td>Specifies a value of 64.</td>
</tr>
<tr>
<td>managed-config &lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td>other-config &lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td>reachable-time &lt;0-3600000&gt;</td>
<td>Specifies the time a node assumes a neighbor is reachable after having received a reachability confirmation. The reachable time is placed in the Reachable Time field in the router advertisement packet. This value is used by the Neighbor Unreachability Detection. The value zero (0) means unspecified (by this router).</td>
</tr>
<tr>
<td>reachable-time default</td>
<td>Specifies a value of zero (0).</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>retransmit-timer integer</td>
<td>Specifies the time between retransmitted Neighbor Solicitation messages if the system does not receive a response. The retransmission timer is placed in the Retrans Timer field in the router advertisement packet. Address resolution and Neighbor Unreachability Detection uses this value. The value zero (0) means unspecified (by this router).</td>
</tr>
<tr>
<td>retransmit-timer default</td>
<td>Specifies a value of zero (0).</td>
</tr>
<tr>
<td>router-lifetime integer</td>
<td>Specifies the value (in seconds) placed in the Router Lifetime field of the router advertisements packet. A value of zero (0) indicates that the router is not to be used as a default router.</td>
</tr>
<tr>
<td>router-lifetime default</td>
<td>Specifies a value of 1800 seconds.</td>
</tr>
<tr>
<td>send-mtu &lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td>off</td>
<td></td>
</tr>
<tr>
<td>autonomous &lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td>on</td>
<td></td>
</tr>
<tr>
<td>on-link &lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td>prefix-valid-lifetime integer</td>
<td>Specifies the length of time in seconds (relative to the time the packet is sent) that the prefix is valid for the purpose of on-link determination. This value is placed in the Valid Lifetime field in the Prefix Information option. The designated value of all 1s (0xffffffff) represents infinity.</td>
</tr>
<tr>
<td>prefix-valid-lifetime default</td>
<td>Specifies a value of 2592000 seconds (30 days).</td>
</tr>
</tbody>
</table>
Show Commands

Use the following commands to monitor and troubleshoot your ICMP router discovery implementation:

```
show ipv6 rdisc6
  interfaces
  interface if_name
  stats
  summary
```

VRRP for IPv6

Check Point supports VRRP for IPv6 interfaces with two implementations:

- VRRP version 3
- Monitored circuit

The CLI commands for these implementations are explained in the following sections.

All Implementations

The following command applies to all VRRP implementations for IPv6, that is, both VRRPv3 and Monitored Circuit:

```
set ipv6 vrrp6
  monitor-firewall <on | off>
```
Arguments

monitor-firewall  Specifies to monitor the state of the firewall and respond appropriately. If a VRRP master detects that the firewall is not ready to handle traffic or is not functioning properly, the master fails over to a backup system. If all the firewalls on all the systems in the VRRP group are not ready to forward traffic, no traffic is forwarded.

Note - If firewall is not installed, this option does not affect the function of VRRP for IPv6.

VRRPv3

Use this group of commands to configure and set parameters for VRRP version 3 for IPv6 interfaces.

set ipv6 vrrp6 interface if_name
  off
  virtual-router vrid <1-255> address ip_address on
  virtual-router backup-vrid <1-255> address ip_address on
  vrid <1-255> off
  vrid <1-255> address ip_address <on | off>
  vrid <1-255> accept-mode <on | off>
  vrid <1-255> hello-interval <1-4095>
  vrid <1-255> hello interval default
  vrid <1-255> priority <1-254>
  vrid <1-255> preempt-mode <on | off>
  vrid <1-255> vmac-mode default-vmac
  vrid <1-255> vmac-mode extended-vmac
  vrid <1-255> vmac-mode interface-vmac
  vrid <1-255> vmac-mode static-vmac mac_address
## VRRP for IPv6

### Arguments

<table>
<thead>
<tr>
<th>off</th>
<th>Specifies to disable VRRPv3 on the specified IPv6 interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>virtual router vrid &lt;1-255&gt; address ip_address on</td>
<td>Specifies the virtual router ID for the virtual router used to back up the IP addresses of the local interface. The vrid must be unique for all virtual routers running on the network of the interface. Specify an IPv6 address for the virtual router. The address configured must be a link-local address.</td>
</tr>
<tr>
<td>virtual-router backup-vrid &lt;1-255&gt; address ip_address on</td>
<td>Specifies the virtual router ID for the virtual router used to back up the IPv6 addresses of another system. The router you are backing up must also have this virtual router configured for its addresses. Specify an IPv6 address to assign to the virtual router used to back up the IP addresses of another system. The address configured must be a link-local address. Global addresses should belong to the interface's subnet and link-local addresses must belong to the fe80::/64 subnet.</td>
</tr>
<tr>
<td>vrid &lt;1-255&gt; off</td>
<td>Specifies to remove the specified virtual router.</td>
</tr>
<tr>
<td>vrid &lt;1-255&gt; address ip_address &lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td>vrid &lt;1-255&gt; accept-mode &lt;on</td>
<td>off&gt;</td>
</tr>
</tbody>
</table>

off.
vrid <1-255>
hello-interval <1-4095>

Specifies in centiseconds, that is, in one-hundredths of a second, the interval between VRRP advertisement transmissions.

100

vrid <1-255>
hello-interval default

Specifies to set the interval between VRRP advertisements to 100 centiseconds, that is, one second.

vrid <1-255> priority <1-254>

Specifies the priority of this physical router during contention for the IPv6 addresses of a failed router. The router with the highest priority becomes the new master when a failure occurs on the existing master.

100

vrid <1-255>
preempt-mode <on | off>

Specifies for this virtual router to become the new master router if has a higher priority than the current master router. Enter off to disable this feature.

on

vrid <1-255> vmac-mode <default-vmac | extended-vmac | interface-vmac | static-vmac mac_address>

Specifies how the virtual MAC address for the backup address is created. You must choose the same option on each physical router that participates on the virtual router.

- default-vmac: Uses the VRRP protocol specification to set the virtual MAC address. If this option does not create a unique VMAC on the network, choose one of the other options.

- extended-vmac: Causes the system to use several variable to calculate the VMAC address so that the virtual routers with the same ID do not use the same address.

- interface-vmac: Specifies that the MAC address of the associated physical interface be used as the VMAC address.

- static-vmac **mac_address**: Uses the specified MAC address

default-vmac


**Monitored Circuit for IPv6 Interfaces**

Use the following group of commands to configure and set parameters for monitored circuit for IPv6 interfaces

```
set ipv6 vrrp6 interface if_name
  off

monitored-circuit vrid <1-255> address ip_address on
vrid <1-255> off
vrid <1-255> address ip_address <on | off>
vrid <1-255> accept-mode <on | off>
vrid <1-255> hello-interval <1-4095>
vrid <1-255> hello interval default
vrid <1-255> monitored-interface if_name priority-delta
  <1-254> <on | off>
vrid <1-255> monitored-interface if_name off
vrid <1-255> preempt-mode <on | off>
vrid <1-255> auto-deactivation <on | off>
vrid <1-255> vmac-mode default-vmac
vrid <1-255> vmac-mode extended-vmac
vrid <1-255> vmac-mode interface-vmac
vrid <1-255> vmac-mode static-vmac mac_address
```

**Arguments**

- `off` Specifies to disable monitored circuit on the specified IPv6 interface

- `monitored-circuit vrid <1-255> address ip_address <on | off>` Specifies the ID for a virtual router with monitored circuit dependencies and an IP address for the virtual router. The address configured must be a link-local address. Global addresses should belong to the interface's subnet, and link-local addresses must belong to the fe80::/64 subnet.

- `vrid <1-255> off` Specifies to remove the specified virtual router with monitored circuit dependencies.
vrid <1-255> address
ip_address <on | off>
Specifies to add or delete an IPv6 address for this virtual router.

vrid <1-255>
accept-mode <on | off>
Specifies for the virtual router in a master state to accept packets addressed to virtual IP addresses.

off

vrid <1-255>
hello-interval
<1-4095>
Specifies in centiseconds, that is, in one-hundredths of a second, the interval between VRRP advertisement transmissions.

100

vrid <1-255>
hello-interval default
Specifies to set the interval between VRRP advertisements to 100 centiseconds, that is, one second.

vrid <1-255>
monitored-interface
<br>if_name priority delta
<1-254> <on | off>
Specifies an interface with a dependency on the virtual router and the priority delta associated with the interface you selected. When an interface goes down, the priority delta value for the that interface is subtracted from the base priority value of the virtual router, resulting in the effective priority value. This effective priority value of the virtual router is used to determine the election of the VRRP master router.
You can also use this command to change the priority delta of an existing monitored interface.

vrid <1-255>
monitored-interface
<br>if_name off
Specifies to remove the monitored interface associated with the specified virtual router.

vrid <1-255>
preempt-mode <on | off>
Specifies for this virtual router to become the new master router if has a higher priority than the current master router. Enter off to disable this feature.

on

vrid <1-255>
autodeactivation
default <on | off>
Specifies to set the minimum value for the effective priority of the virtual router to zero (0). The default is off, which sets the lowest value for the effective priority of the virtual router to one (1). A VRRP virtual router with an effective priority of 0 does not become the master even if there are not other VRRP routers with a higher priority for this virtual router.

off
Show Routing Summary Commands

Use the commands in this section to view summary information about routes on your system.

Use the following command for information about active, inactive, and all RIPng routes on your system:

```
show ipv6 route
```
ripng
inactive ripng
all ripng

Use the following command to show information about active, inactive, and all aggregate routes on your system:
show [instance instance_name] ipv6 route
    aggregate
    inactive aggregate
    all aggregate

Use the following command to show additional information about routes on your system:
show [slot <1-15>] [instance instance_name] ipv6 route
    all
    all direct
    all static
direct
inactive
inactive direct
inactive static
static
summary
destination ipv6_address
exact ipv6_prefix
less-specific ipv6_prefix
more-specific ipv6_prefix

Host Name Configuration

Use the following commands to add or delete logical IPv6 hosts on your system:
add ipv6host
   localhost
Network Access and Services

name name ipv6 ip6_address
delete ipv6host
localhost
name name

Use the following command to change the IPv6 address associated with the specified host name:
set ipv6host name name ipv6 ip6_address

Arguments

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>localhost</td>
<td>Adds or deletes an IPv6 local host. The associated address is ::1.</td>
</tr>
<tr>
<td>ipv6host name name</td>
<td>Specifies a logical host name. Use alphanumeric characters, dashes (-), and periods (;) must be followed by a letter or a digit. The host name cannot end in a dash or a period.</td>
</tr>
<tr>
<td>ipv6 ip6_address</td>
<td>Specifies the IPv6 address to associate with the host name:</td>
</tr>
</tbody>
</table>

Example: 1000:50:32::2

Use the following command to view the logical hosts and the associated IPv6 addresses configured on your system:
show ipv6host names

Use the following command to view the IPv6 address associated with the specified static host:
show ipv6host name name ipv6

Network Access and Services

Use the following set commands to enable or disable network access to this system for FTP, TFTP, and TELNET sessions. Use the show commands to view the current status of network access to the system by using FTP, TFTP, and TELNET.
set
ipv6ftpaccess <enable | disable>
ipv6tftpaccess <enable | disable>
ipv6telnetaccess <enable | disable>
show
ipv6ftpaccess
ipv6tftpaccess
ipv6telnetaccess
Chapter 8

Network Security and Access Commands

This chapter describes the commands that you use to manage the security and access features of your system. It also explains how to enable or disable a VPN accelerator card and display VPN acceleration information.

In This Chapter

- Network Access and Services  page 220
- Licenses  page 224
- AAA  page 244
- SSH  page 258
- Voyager Web Access (SSL)  page 269
- Password and Account Management  page 273
- Users and Roles Management  page 278
- Group Management  page 285
- VPN Acceleration  page 286
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.

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

Use the following commands to configure a USB modem.

```plaintext
set modem
    country code country
    dialback <on | off>
    dialback-number number
    disable
    enable
    rings <1-4>
```

Use the following commands to view network access configurations.

```plaintext
show
    net-access
    net-access ftp
    net-access tftp
    net-access telnet
    net-access admin-net-login
    net-access com2-login
    net-access com3-login
    net-access com4-login
```
Use the following commands to configure types of services.

```
set services
  echo <yes | no>
  discard <yes | no>
  chargen <yes | no>
  daytime <yes | no>
  time <yes | no>
```

Use the following commands to view service configurations.

```
show
  services
  services echo
  services discard
  services chargen
  services daytime
  services time
```

### Arguments

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ftp &lt;yes</td>
<td>no&gt;</td>
</tr>
<tr>
<td>port &lt;1-65535&gt;</td>
<td>Specifies a port on which the ftpd server listens.</td>
</tr>
<tr>
<td>tftp &lt;yes</td>
<td>no&gt;</td>
</tr>
<tr>
<td>telnet &lt;yes</td>
<td>no&gt;</td>
</tr>
<tr>
<td>Configuration</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------</td>
</tr>
<tr>
<td>admin-net-login</td>
<td>Specifies “admin” login for telnet access to the platform. This will not affect admin connections through Voyager or FTP.</td>
</tr>
<tr>
<td>com2-login</td>
<td>Specifies login on the serial port ttyd1 com2.</td>
</tr>
<tr>
<td>com3-login</td>
<td>Specifies login on the serial port ttyd2 com3.</td>
</tr>
<tr>
<td>country code country</td>
<td>Sets modem parameters to comply with standards of the specified country.</td>
</tr>
<tr>
<td>dialback</td>
<td>When enabled, an incoming call on the modem is dropped after you log in, and the modem automatically calls the dialback number and connects a login process to the line.</td>
</tr>
<tr>
<td>dialback-number</td>
<td>Specifies the number that the modem should dial when dialback is enabled. You can enter commas to cause the dialing to pause briefly. To increase the length of the pause, enter multiple adjacent commas, as in 650,,555,,1212.</td>
</tr>
<tr>
<td>disable</td>
<td>Prevent login through a modem attached to the USB port.</td>
</tr>
<tr>
<td>enable</td>
<td>Allow login through a modem attached to the USB port.</td>
</tr>
<tr>
<td>rings</td>
<td>Specifies the number of times the incoming call should ring before the modem answers the call.</td>
</tr>
<tr>
<td>echo</td>
<td>Specifies echo service, which sends back any data received by the platform to the originating source.</td>
</tr>
<tr>
<td>discard</td>
<td>Specifies discard service, which discards any data received by the platform.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>chargen &lt;yes</td>
<td>no&gt;</td>
</tr>
<tr>
<td></td>
<td>no</td>
</tr>
<tr>
<td>daytime &lt;yes</td>
<td>no&gt;</td>
</tr>
<tr>
<td></td>
<td>no</td>
</tr>
<tr>
<td>time &lt;yes</td>
<td>no&gt;</td>
</tr>
<tr>
<td></td>
<td>no</td>
</tr>
</tbody>
</table>
Licenses

To purchase a license or increase your limit on your current license, contact your Check Point representative.

Configuring Software Licenses

Use the following commands to add a software license to your platform.

```
set licensing
    bgp-key license_key
    dvmrp-rip-key license_key
    dvmrp-ospf-key license_key
    igrp-key license_key
    dvmrp-key license_key
```

Use the following commands to delete a software license from your platform.

```
delete licensing
    bgp-key
    dvmrp-rip-key
    dvmrp-ospf-key
    igrp-key
    dvmrp-key
```

Use the following commands to show your software licenses.

```
show
    licensing
    licensing bgp-key
    licensing dvmrp-rip-key
    licensing dvmrp-ospf-key
    licensing igrp-key
    licensing dvmrp-key
```
### Arguments

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bgp-key license_key</td>
<td>Enables BGP feature.</td>
</tr>
<tr>
<td>dvmrp-rip-key license_key</td>
<td>Enables DVMRP with RIP feature.</td>
</tr>
<tr>
<td>dvmrp-ospf-key license_key</td>
<td>Enables DVMRP with OSPF feature.</td>
</tr>
<tr>
<td>igrp-key license_key</td>
<td>Enables IGRP feature.</td>
</tr>
<tr>
<td>dvrmp-key license_key</td>
<td>Enables DVMRP feature.</td>
</tr>
</tbody>
</table>
IPsec Commands (IPSO Implementation)

This section describes the CLI commands you use to configure the IPSO implementation of IP Security (IPsec) on your system and to view current settings. IPsec is the industry standard that ensures the construction of secure virtual private networks (VPNs).

Use the commands in this section to configure and view different IPsec entities including filters, proposals, rules, policies, keys, X509 certificates, tunnels, and transports. You can also configure IPsec options such as debugging level and hardware acceleration.

Note - Because the IP2250 and IP2255 platforms require the use of Check Point’s SecureXL, these platforms do not support IPSO’s implementation of IPsec.

General IPsec Commands

Use the following command to turn off IPsec. This command clears the complete IPsec tree in the system on which the command is issued. Use it only when you want to turn off IPsec on the system.

```
set ipsec clear
```

Use the following command to show a summary of all IPsec configuration, including configured rules, proposals, filters, policies, and other IPsec information:

```
show ipsec all
```

Proposal Commands

IPsec proposals specify the encryption and authentication algorithms, ordered by priority, available to the gateway at the remote endpoint of the IPsec tunnel. This list is shared among all IPsec tunnel interfaces. The two types of proposals are:

- Encapsulating security payload (ESP)
- Authentication header (AH).

Note - AH proposals do not use an encryption algorithm.

Each proposal indicates one transform along with its mode. You cannot configure transform parameters, such as cipher-key length. The IPSO CLI implementation does not support user configuration of IKE proposals, which are derived from the IPsec proposals.
Use the following `add` command to create a proposal. If you specify only the proposal name, the proposal is ESP with SHA1 authentication and DES encryption. Use the `set` command to modify one or more properties of an existing proposal. You cannot modify the proposal type.

**Note** - You cannot use the word `all` for the value of a command variable represented by `name`. In other words, do not use `all` to identify a proposal, policy, or rule.

```plaintext
add ipsec proposal name
add ipsec proposal name type
type <esp | ah>
  esp
  ah auth <sha1 | md5>
  crypto <des | 3des | blowfish | null>
set ipsec proposal name
auth <sha1 | md5>
crypto <des | 3des | blowfish | null>
```

### Arguments

<table>
<thead>
<tr>
<th>proposal name</th>
<th>Specifies a unique identifier for the proposal:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Format: single word, no spaces allowed</td>
</tr>
<tr>
<td></td>
<td>• Example: 3des-md5</td>
</tr>
<tr>
<td>type &lt;esp</td>
<td>ah&gt;</td>
</tr>
<tr>
<td></td>
<td>esp</td>
</tr>
<tr>
<td>auth &lt;sha1</td>
<td>md5&gt;</td>
</tr>
<tr>
<td></td>
<td>md5</td>
</tr>
<tr>
<td>crypto &lt;des</td>
<td>3des</td>
</tr>
<tr>
<td></td>
<td>des</td>
</tr>
</tbody>
</table>

Use the following command to list the attributes of one or all proposals:

```plaintext
show ipsec proposal
  all
  name
```

### Arguments

| proposal all | Shows information about all proposals. |
Filter Commands

Use the following command to delete the specified proposal. If the proposal is linked to a policy, the proposal cannot be deleted unless the policy is deleted first (see “Policy Commands” on page 235).

delete ipsec proposal
   all
   name

**Arguments**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>proposal all</td>
<td>Deletes all proposals. You cannot delete proposals that are linked to a policy.</td>
</tr>
<tr>
<td>proposal name</td>
<td>Specifies the name of the proposal to delete.</td>
</tr>
</tbody>
</table>

**Filter Commands**

Filters specify the list of addresses or subnet addresses that the IPsec engine matches against the address field of an IP packet. If the address matches, IPsec is applied. This list is shared among all IPsec tunnel interfaces. Every connection can have two or more filters since each filter indicates either source or destination options.

Use the following add command to create a filter on an IPv4 or IPv6 network. If you do not specify a protocol or port, the default value for these fields is *any* and no port. Use the set command to modify one or more properties of an existing filter.

add ipsec filter name
   address ip_address mask <0–32>
   proto <tcp | udp | icmp | any>
   port <0–65535>
   address6 ip6_address mask <0–128>
   proto <tcp | udp | icmp | any>
   port <0–65535>

set ipsec filter name
   address ip_address mask <0–128>
   address6 ip6_address mask6 <0–128>
proto <tcp | udp | icmp | any>
port <0—65535>

Arguments

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>filter name</td>
<td>Specifies a name for the filter:</td>
</tr>
<tr>
<td></td>
<td>• Format: single word, no spaces allowed</td>
</tr>
<tr>
<td></td>
<td>• Example: 3des-md5</td>
</tr>
<tr>
<td>address ip_address</td>
<td>Specifies the IP address of the desired subnetwork with host bits as zeroes (0):</td>
</tr>
<tr>
<td></td>
<td>• Example: 10.2.0.0</td>
</tr>
<tr>
<td>mask &lt;0—32&gt;</td>
<td>Specifies the mask length for the network.</td>
</tr>
<tr>
<td>address6 ip6_address</td>
<td>Specifies the IPv6 address of the desired subnetwork:</td>
</tr>
<tr>
<td></td>
<td>• Example: 1000:50:32::</td>
</tr>
<tr>
<td>mask6 &lt;0—128&gt;</td>
<td>Specifies the mask length for the network.</td>
</tr>
<tr>
<td>proto &lt;tcp</td>
<td>udp</td>
</tr>
<tr>
<td></td>
<td>any</td>
</tr>
<tr>
<td>port &lt;0—65535&gt;</td>
<td>Specifies the port number of the packet to filter, if appropriate, ignored otherwise.</td>
</tr>
</tbody>
</table>

Use the following command to show information about the specified filter:

```bash
show ipsec filter
   all
   name
```

Arguments

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>filter all</td>
<td>Shows information about all filters.</td>
</tr>
<tr>
<td>filter name</td>
<td>Shows information about a specified filter.</td>
</tr>
</tbody>
</table>

Use the following command to delete the specified filter. If the filter is linked to any connection, the filter cannot be deleted unless the connection is deleted first.

```bash
delete ipsec filter
   all
```
Certificate Commands

Peer systems use certificates to authenticate each other. To do this, a system presents a trusted certificate to its peer to prove that it is what it claims. The IPSO IPsec implementation allows installation of x509 certificates, which can be used in IKE negotiation. The certificates can be either certification authority (CA) certificates or device certificates.

The CA certificates are trusted certificates. If the certificate for a device is found to be signed by the same CA as another device, the other device is trusted too. Device certificates are used as the identity of a host and are presented to peers during IKE negotiation.

Use the following add command to install an x509 CA or device certificate on a system. Use the set command to install a new certificate under the same x509 certificate name. None of the attributes for the new certificate is derived from the old certificate. You must specify all parameters when you install the new certificate. The realm, username, and password parameters are optional and valid only when you specify URL as the certificate source.

```
add ipsec x509cert name type <dev | ca> source
   pem file name
   url url url
   realm name [user username password password]
```

```
set ipsec x509cert name source
   pem file name
   url url url
   realm name [user username password password]
```

Arguments

|x509 name| Specifies the name of the certificate.|
|filter all| Delete all filters.|
|filter name| Specifies a name of the filter to delete.|
Use the following command to show information about the specified certificate or all certificates:

type <dev | ca> Specifies the type of certificate to create. You can use all uppercase or all lowercase:
  • dev: device certificate
  • ca: CA certificate

source <pem | url> Specifies how to obtain certificate. You can use all uppercase or all lowercase:
  • pem: obtain as input by using a simple file with PEM encoding.
  • url: obtain directly from a URL to be installed in the local host.

file name Specifies the file, including the path, containing the CA certificate or the signed DEV certificate.
  Note - This parameter is valid only if the source is PEM.

url url Specifies the location where certificate can be found. The certificate can be downloaded from an HTTP, FTP, LDAP or file server:
  • Format: Standard URL format.
  • Example: http://test.acme.com/dev1.cert
  • Example: ftp://test.acme.com/dev1.cert
  • Example: file:///tmp/dev1.cert
  • Example: ldap://test.acme.com/cn=dev1.acme.com?pem_x509?sub

This argument does not have a default value.

realm name If the URL you specified is under access control, you must specify the name of the realm containing the certificate. This field is optional.

user username Specifies the username for access to the realm. This field is optional.

password password Specifies the password associated with the username. This field is optional.
Certificate Commands

```
show ipsec x509cert
  all
  options <attribs | content | decoded>
name
  options <attribs | content | decoded>
```

**Arguments**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>x509cert all</td>
<td>Shows information about all certificates.</td>
</tr>
<tr>
<td>x509 name</td>
<td>Shows information about the specified certificate.</td>
</tr>
<tr>
<td>options &lt;attribs</td>
<td>Specifies the information to show:</td>
</tr>
<tr>
<td>content</td>
<td>decoded&gt;</td>
</tr>
<tr>
<td>attribs</td>
<td></td>
</tr>
<tr>
<td>content</td>
<td></td>
</tr>
<tr>
<td>decoded</td>
<td></td>
</tr>
</tbody>
</table>

Use the following command to delete the specified certificate. Using the keyword all instead of a certificate name deletes all certificates.

delete ipsec x509cert
  all
  name

**Arguments**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>x509cert all</td>
<td>Deletes all certificates.</td>
</tr>
<tr>
<td>x509 name</td>
<td>Specifies the name of the certificate to delete.</td>
</tr>
</tbody>
</table>

IPSO can generate a set of RSA/DSA public and private keys. The public key can be included in a certificate request, along with other attributes, enabling the certificate to be signed by a CA.
Use the following `add` command to generate a certificate request to be sent to a CA. Use the following `set` command to generate a new certificate request under the same name. None of the attributes for the new certificate are derived from the old certificate. You must specify all parameters when you set the certificate request.

```
add ipsec x509certreq name key-len <512 | 768 | 1024> sig-algo <dsa | rsa> pass-phrase phrase country country state state locality org name org-unit name dns-name name
   ip-address ip_address email email_address
   ip-address6 ip6_address email email_address
set ipsec x509certreq name key-len <512 | 768 | 1024> sig-algo <dsa | rsa> pass-phrase phrase country country state state locality org name org-unit name dns-name name
   ip-address ip_address email email_address
   ip-address6 ip6_address email email_address
```

**Arguments**

- `x509certreq name` Specifies the name of the certificate request.
- `key-len <512 | 768 | 1024>` Specifies how large (and therefore how secure) your newly generated private key is. It is specified in bits. 1024
- `sig-algo <dsa | rsa>` Specifies the algorithm to use to generate the keys. rsa
- `pass-phrase phrase` Specifies the passphrase to use to protect private key.
- `country country` Specifies the two-letter code indicating your country, for example, US.
- `state state` Specifies the name of your state or province, for example, California.
- `locality locality` Specifies the locality (town or city) name, for example, San Francisco.
- `org name` Specifies the name of your company or organization, for example, Check Point.
- `org-unit name` Specifies the name of your subunit within your company or organization, for example, Check Point Engineering Department.
Certificate Commands

Use the following command to show information about the specified certificate request or all certificate requests:

```
show ipsec x509certreq
   all
   options <attrs | content | decoded>
   name
   options <attrs | content | decoded>
```

**Arguments**

- `x509certreq all`: Shows information about all x509 certificate requests.
- `x509certreq name`: Shows information about the specified certificate request.
- `options <attrs | content | decoded>`: Specifies the information to show:
  - `attrs`: shows location and other attributes of certificate.
  - `content`: shows the original content of the certificate.
  - `decoded`: shows the decoded human-readable form of the certificate.

---

**Options**

- `dns-name name`: Specifies the common DNS name (fully qualified domain name), for example: `www.dns.example.com`.
- `ip-address ip_address`: Specifies a valid IPv4 address:
  - Example: `192.168.50.5`
- `ip-address6 ip6_address`: Specifies a valid IPv6 address:
  - Example: `1000:50:32::2`
- `email`: Specifies the email address to contact the person responsible for this system or for its certificate, for example, `webmaster@engineering.example.com`. The CA sends notification to this address.
Use the following command to delete all x509 certificate requests or a specific certificate request:

```
delete ipsec x509certreq
    all
    name
```

**Arguments**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>x509certreq all</td>
<td>Deletes all x509 certificate requests.</td>
</tr>
<tr>
<td>x509certreq name</td>
<td>Specifies the name of the certificate request to delete.</td>
</tr>
</tbody>
</table>

**Policy Commands**

Policy defines the use of filters together with a list of IPsec proposals, ordered by priority. These policies can be applied to one or several IPsec tunnel interfaces, which creates a secure tunnel.

Use the following `add` command to create a policy, which can be used to create a connection. Use the `set` command to modify one or more properties of an existing policy. You can set the properties together or individually. Lifetime values must be set to the same value between peers when negotiation is initiated. If they are not set the same, IPSO IPsec may deny the negotiation.

```
add ipsec policy name proposal name priority integer
    psk secret_key
    life-sec <0—700000>
    life-mb <0—65000>
    ike-group <1 | 2 | 5>
    pfs-group <1 | 2 | 5 | none>
    x509cert name
    life-sec <0—700000>
    life-mb <0—65000>
    ike-group <1 | 2 | 5>
    pfs-group <1 | 2 | 5 | none>
set ipsec policy name
    proposal name priority integer
    psk secret_key
```
x509cert name
life-sec <0—700000>
life-mb <0—65000>
ike-group <1 | 2 | 5>
pfs-group <1 | 2 | 5 | none>

**Arguments**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>policy name</td>
<td>Specifies the name of the policy to add.</td>
</tr>
<tr>
<td>proposal name</td>
<td>Specifies the proposal with which to associate this policy. The proposal must already exist.</td>
</tr>
<tr>
<td>priority integer</td>
<td>Specifies the priority of the policy. A higher value indicates lower priority.</td>
</tr>
<tr>
<td>psk secret_key</td>
<td>Specifies the preshared-secret key. It must be between 8 and 256 characters.</td>
</tr>
<tr>
<td>x509cert name</td>
<td>Specifies the name of the predefined device certificate.</td>
</tr>
<tr>
<td>life-sec &lt;0—700000&gt;</td>
<td>Specifies the number of seconds from security association (SA) creation to start the rekeying. This parameter is optional.</td>
</tr>
<tr>
<td>life-mb &lt;0—65000&gt;</td>
<td>Specifies the amount of megabytes of data transferred before rekeying is started. This parameter is optional.</td>
</tr>
<tr>
<td>ike-group &lt;1</td>
<td>2</td>
</tr>
<tr>
<td>pfs-group &lt;1</td>
<td>2</td>
</tr>
</tbody>
</table>

Use the following command to view information about the specified policy or all policies:

```
show ipsec policy
```
Rule Commands

all
name

Arguments

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>policy all</td>
<td>Shows information about all policies.</td>
</tr>
<tr>
<td>policy name</td>
<td>Shows information about a specified policy.</td>
</tr>
</tbody>
</table>

Use the following command to delete the specified policy or all policies. If you specify a proposal, this removes the proposal from the named policy. If a policy is linked to any connection, it cannot be deleted unless the connection is deleted first.

```
delete ipsec policy
    all
    name
    proposal name
```

Arguments

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>policy all</td>
<td>Delete all policies</td>
</tr>
<tr>
<td>policy name</td>
<td>Specifies the name of the policy to delete. The policy must already exist.</td>
</tr>
<tr>
<td></td>
<td>If you do not specify a proposal, the policies matching the name are deleted.</td>
</tr>
<tr>
<td>proposal name</td>
<td>Specifies the proposal to delete from the policy. The proposal must already exist.</td>
</tr>
</tbody>
</table>

Rule Commands

IPsec rules specify the set of actions to be performed on packets matching the selectors. A rule can be specified in tunnel mode or in transport mode.

For a tunnel mode rule, if you specify a separate logical interface, it is automatically created. Additionally, the remote endpoint is also added to the classifier so that the reverse classifier lookup can be done in the input path. For both tunnel and transport mode rules, the destination filters are added to the IPsec classifier so that packets are directed to the engine in the output path.
Use the following `add` command to add an IPsec tunnel mode rule for an IPv4 network or an IPv6 network. You can specify any combination (or all) of the third-level parameters in the same `add` command. Use the `set` command to modify one or more properties of an existing rule. Once you add a rule, you cannot change the rule mode or indicate whether a separate logical interface is needed for a tunnel mode rule.

```
add ipsec rule name mode tunnel
  local-address ip_address remote-address ip_address
  policy name
  src-filter name
  dst-filter name
  inc-end-points <on | off>
  logical-interface <on | off>
  hello-prot <on | off> [hello-inv <0—21666> dead-inv <0—65000>]
local-address6 ip6_address remote-address6 ip6_address
  policy name
  src-filter name
  dst-filter name
  inc-end-points <on | off>
  logical-interface <on | off>
  hello-prot <on | off> [hello-inv <0—21666> dead-inv <0—65000>]
set ipsec rule name
  local-address ip_address
  remote-address ip_address
  local-address6 ip6_address
  remote-address6 ip6_address
  policy name
  src-filter name
  dst-filter name
  inc-end-points <on | off>
```
hello-prot <on | off>
hello-inv <0—21666>
dead-inv <0—65000>

Use the following add command to add an IPsec transport mode rule. Use the set command to change one or more values for the existing transport mode rule.

add ipsec rule name mode transport
    policy name
    src-filter name
    dst-filter name

set ipsec rule name
    policy name
    src-filter name
    dst-filter name

Arguments

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rule name</td>
<td>Specifies the name of the rule to add.</td>
</tr>
<tr>
<td>mode &lt;tunnel</td>
<td>transport&gt;</td>
</tr>
<tr>
<td>local-address</td>
<td>Specifies the local IP address used as the tunnel endpoint. It must be an address of another interface configured for this system:</td>
</tr>
<tr>
<td></td>
<td>• Example: 10.2.0.1</td>
</tr>
<tr>
<td>remote-address</td>
<td>Specifies the IP address of the multicast router at the remote end of the tunnel. It cannot be the local address of any interface of this system:</td>
</tr>
<tr>
<td></td>
<td>• Example: 10.2.0.2</td>
</tr>
<tr>
<td>local-address6</td>
<td>Specifies the local IPv6 address used as the tunnel endpoint. It must be an address of another interface configured for this system:</td>
</tr>
<tr>
<td></td>
<td>• Example: 1000:50:32::1</td>
</tr>
</tbody>
</table>
Use the following command to display information about a specified rule. Also, you can show all tunnel mode rules, all transport mode rules, or all rules.

```bash
show ipsec rule
  all [mode <tunnel | transport>]
  name
```
Some arguments are described below:

- `rule all` shows information about all rules.
- `mode <tunnel | transport>` specifies whether to show all tunnel mode rules or all transport mode rules. This parameter is optional.
- `rule name` shows information about a specific rule.

Miscellaneous IPsec Commands

Use the following command to detach a policy from a rule, delete a source or destination filter from the specified rule, or delete the specified rule entirely. Also, you can delete all rules or all rules of a specified mode.

```
delete ipsec rule
    all [mode <tunnel | transport>]
    name
    policy name
    src-filter name
    dst-filter name
```

Arguments

- `mode <tunnel | transport>` specifies the rule mode. This allows you to delete all tunnel mode rules or all transport mode rules.
- `rule name` specifies the name of the rule.
- `policy name` specifies the name of the policy to be detached from the rule.
- `src-filter name` specifies an existing source filter for the rule.
- `dst-filter name` specifies an existing destination filter for the rule.
- `rule all` deletes all rules. If you do not use the optional mode parameter, you delete all tunnel and transport mode rules.
### Miscellaneous IPsec Commands

```
set ipsec
    log-level <error | debug | info>
    hardware-accl <on | off>
    allow-interfaceless-tunnels <on | off>
```

**Arguments**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>log-level &lt;error</td>
<td>debug</td>
</tr>
<tr>
<td>hardware-accl &lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td>allow-interfaceless-tunnels &lt;on</td>
<td>off&gt;</td>
</tr>
</tbody>
</table>

Use the following commands to add or delete a specified LDAP server to the IPsec lookup list. The certificate revocation lists (CRLs) for the IPsec CA certificates are obtained from the specified LDAP server.

```
add ipsec ldap url
delete ldap url
```

**Arguments**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ldap url</td>
<td>Specifies the URL of the LDAP server.</td>
</tr>
</tbody>
</table>

Use the following commands to view miscellaneous information about IPsec properties:

```
show ipsec
    log-level
    ldap
    hardware-accl
```
allow-interfaceless-tunnels
AAA

Use the following group of commands to configure AAA.

Viewing AAA Configuration

Use the following command to view the AAA configuration.

show aaa all

Configuring Service Modules

Use the following command to create a new AAA service and associate it with a service profile.

add aaa service name profile name

Use the following command to delete a service entry.

delete aaa service name

Use the following command to change the configuration of an existing AAA service and associate it with a new service profile.

set aaa service name profile name

Use the following commands to view the service module configuration and a service profile entry of a particular service.

show aaa

    services

    service name
Arguments

<table>
<thead>
<tr>
<th>service name</th>
<th>The name of an application or service that is to use AAA.</th>
</tr>
</thead>
<tbody>
<tr>
<td>profile name</td>
<td>A service profile entry created by the command <code>add aaa profile</code> and may have associated authentication, account, and session profiles. The following profiles are included in the IPSO operating system:</td>
</tr>
<tr>
<td></td>
<td>• base_prof_httpd</td>
</tr>
<tr>
<td></td>
<td>• base_prof_login</td>
</tr>
<tr>
<td></td>
<td>• base_prof_other</td>
</tr>
<tr>
<td></td>
<td>• base_prof_snmpd</td>
</tr>
<tr>
<td></td>
<td>• base_prof_sshd</td>
</tr>
</tbody>
</table>

Configuring Service Profiles

Use the following commands to create new service profiles and associate authentication, account, and session profiles to new or existing services profiles or add to existing service profiles.

`add aaa profile name`  
  authprofile name acctprofile name sessprofile name  
  authprofile name  
  acctprofile name  
  sessprofile name

Use the following command to delete profiles or authentication, account and session profiles grouped under a service profile.

`delete aaa`  
  profile name  
  profile name authprofile name  
  profile name acctprofile name  
  profile name sessprofile name  
  profile name auth-priority name  
  profile name acct-priority name  
  profile name sess-priority name
Use the following commands to set the order in which multiple authentication, account or session profiles will run for a given service profile.

```plaintext
set aaa profile name
  authprofile name auth-priority integer
  acctprofile name acct-priority integer
  sessprofile name sess-priority integer
```

Use the following commands to view particular service profile entries.

```plaintext
show aaa
  profiles
  profile name
  profile name authcount
  profile name acctcount
  profile name sesscount
  profile name authprofiles
  profile name auth-priority integer
  profile name acctprofiles
  profile name acct-priority integer
  profile name sessprofiles
  profile name sess-priority integer
```

**Arguments**

- `profile name`: A service profile entry created by the command `add aaa profile name` and may have associated authentication, account, and session profiles. The following profiles are included in the IPSO operating system:
  - `base_prof_httpd`
  - `base_prof_login`
  - `base_prof_other`
  - `base_prof_snmpd`
  - `base_prof_sshd`
Configuring Authentication Profiles

Use the following command to create an authentication profile entry.

```
add aaa authprofile name [authtype name authcontrol name]
```
Use the following command to delete an authentication profile entry.
\texttt{delete aaa authprofile name}

Use the following command to change authentication profile configurations.
\texttt{set aaa authprofile name}
  \begin{itemize}
  \item \texttt{authtype name}
  \item \texttt{authcontrol name}
  \end{itemize}

Use the following command to view authentication profile configurations.
\texttt{show aaa}
  \begin{itemize}
  \item \texttt{authprofiles}
  \item \texttt{authprofile name}
  \item \texttt{authprofile name authtype}
  \item \texttt{authprofile name authcontrol}
  \end{itemize}

\textbf{Arguments}

\begin{tabular}{ll}
\textbf{authprofile name} & The name of a new authentication profile (add) or existing authentication profile (delete, set, show). The IPSO operating system includes the following authentication profiles:
\end{tabular}

\begin{itemize}
\item base_httpd_authprofile
\item base_login_authprofile
\item base_other_authprofile
\item base_snmpd_authprofile
\item base_sshd_authprofile
\end{itemize}
authtype name

The name of the authentication algorithm. The IPSO operating system includes the following authentication algorithms:

- HTTPD
- PERMIT
- RADIUS
- ROOTOK
- SECURETTY
- SKEY
- SNMPD
- TACPLUS
- UNIX

authcontrol name

The name of a control value. The control value determines how the results of multiple authentication algorithms are applied and when additional algorithms are invoked. A control value other than required is only effective when multiple authentication profiles are defined for a given service profile. The IPSO operating system includes the following control values:

- required—The result is retained and the next algorithm is invoked.
- requisite—A result of error is reported immediately and no further algorithms are invoked. Otherwise, the result is retained and the next algorithm is invoked.
- sufficient—A result of error is ignored; If a previous algorithm has reported error, or the result of this algorithm is error, the next algorithm is invoked.
- optional —A result of error is ignored and a result of success is retained. The next algorithm is always invoked.
- nokia-server-auth-sufficient—Same as “sufficient,” except a result of error for this module is reported immediately and no further modules are invoked.
Configuring Account Profiles

Use the following command to create an account profile entry.
add aaa acctprofile name accttype name acctcontrol name

Use the following command to delete an account profile entry.
delete aaa acctprofile name

Use the following command to change account profile configurations.
set aaa acctprofile name
   authtype name
   authcontrol name

Use the following command to view account profile configurations.
show aaa
   acctprofiles
   acctprofile name
   acctprofile name accttype
   acctprofile name acctcontrol

Arguments

acctprofile name

The name of a new accounting profile (add) or existing accounting profile (delete, set, show). The IPSO operating system includes the following account profiles:

- base_httpd_acctprofile
- base_login_acctprofile
- base_other_acctprofile
- base_snmpd_acctprofile
- base_sshd_acctprofile
### Configuring Session Profiles

Use the following command to create a session profile entry.
```
add aaa sessprofile name sessstype name sesscontrol name
```

Use the following command to delete an session profile entry.
```
del aaa sessprofile name
```
delete aaa sessprofile name

Use the following command to change session profile configurations.
set aaa sessprofile name
    sessstype name
    sesscontrol name

Use the following command to view session profile configurations.
show aaa
    sessprofiles
    sessprofile name
    sessprofile name sessstype
    sessprofile name sesscontrol

Arguments

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sessprofile name</td>
<td>The name of a new session profile (add) or existing session profile (delete, set, show). The IPSO operating system includes the following session profiles:</td>
</tr>
<tr>
<td></td>
<td>- base_httpd_sessprofile</td>
</tr>
<tr>
<td></td>
<td>- base_login_sessprofile</td>
</tr>
<tr>
<td></td>
<td>- base_other_sessprofile</td>
</tr>
<tr>
<td></td>
<td>- base_snmpd_sessprofile</td>
</tr>
<tr>
<td></td>
<td>- base_sshd_sessprofile</td>
</tr>
<tr>
<td>sessstype name</td>
<td>The name of the session management algorithm. The IPSO operating system includes the following session management algorithms:</td>
</tr>
<tr>
<td></td>
<td>- PERMIT—(pam.permit.so.1.0) The algorithm returns PAM_SUCCESS when invoked.</td>
</tr>
<tr>
<td></td>
<td>- UNIX—(pam.unix.sess.so.1.0) The algorithm logs a message to indicate that a session has started or stopped.</td>
</tr>
</tbody>
</table>
Configuring RADIUS

Use the following command to configure RADIUS for use in a single authentication profile.

add aaa radius-servers authprofile name priority integer host IPv4 address port integer <secret name | prompt-secret> timeout integer maxtries integer

Use the following command to delete a RADIUS configuration.

delete aaa radius-servers authprofile name priority integer

Use the following commands to change the configuration of a RADIUS entry.

set aaa radius-servers authprofile name priority integer
    host IPv4 address
    port integer
    secret name
    prompt-secret
    timeout integer
    maxtries integer

The name of a control value. The control value determines how the results of multiple session algorithms are applied and when additional algorithms are invoked. A control value other than required is only effective when multiple session profiles are defined for a given service profile. The IPSO operating system includes the following control values:

• required—The result is retained and the next algorithm is invoked.

• requisite—A result of error is reported immediately and no further algorithms are invoked. Otherwise, the result is retained and the next algorithm is invoked.

• sufficient—A result of error is ignored; If a previous algorithm has reported error, or the result of this algorithm is error, the next algorithm is invoked.

• optional — A result of error is ignored and a result of success is retained. The next algorithm is always invoked.
new-priority integer

Use the following command to view a list of all servers associated with an authentication profile.
show aaa radius-servers authprofile name list

Use the following commands to view a RADIUS configuration.
show aaa radius-servers authprofile name priority integer
  host
  port
  timeout
  maxtries
  new-priority

Arguments

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>authprofile name</td>
<td>An authentication profile entry. The following authentication profiles are included in the IPSO operating system:</td>
</tr>
<tr>
<td>priority integer</td>
<td>A number indicating the priority of the server. When you configure multiple servers, the priority determines which should be tried first. A smaller number indicates a higher priority. No default. You must enter a value.</td>
</tr>
<tr>
<td>host IPv4 address</td>
<td>The IP address of the RADIUS server in dot-delimited format.</td>
</tr>
</tbody>
</table>
### Configuring TACPLUS

**port 1-65535**  
The UDP port to contact on the server host. You determine the correct value by the configuration of your RADIUS server. Common values are 1812 (specified by the standard) and 1645 (nonstandard but used traditionally).

*port* also takes the keyword *unset*, which indicates that no value is set in the database so the default is used.

**1812**

**secret name**  
The “shared secret” used to authenticate the RADIUS server and the local client to each other. The same value should be configured on your RADIUS server.

**prompt secret**  
Prompts you to enter the “shared secret” during the run of the command.

**timeout integer**  
The number of seconds to wait, after contacting the server, for a response. The default value 3 seconds.

**maxtries integer**  
The number of attempts to make to contact the server. 3 (includes the first attempt, so a value of 3 means two retries)

**new-priority integer**  
Changes the priority number of the server.

**list**  
Displays a list of all servers associated with an authentication profile.

---

**Configuring TACPLUS**

Use the following command to configure TACPLUS for use in a single authentication profile.

```bash
add aaa tacplus-servers authprofile name priority integer host IPv4 address port integer <secret name | prompt-secret> timeout integer maxtries integer
```

Use the following command to delete a TACPLUS configuration.

```bash
delete aaa tacplus-servers authprofile name priority integer
```

Use the following commands to change the configuration of a TACPLUS entry.

```bash
set aaa tacplus-servers authprofile name priority integer host IPv4 address
```
port integer
secret name
prompt-secret
timeout integer
new-priority integer

Use the following command to view a list of all servers associated with an authentication profile.
show aaa radius-servers authprofile name list

Use the following commands to view a TACPLUS configuration.
show aaa tacplus-servers authprofile name priority integer
host
port
timeout

**Arguments**

<table>
<thead>
<tr>
<th>authprofile name</th>
<th>An authentication profile entry. The following authentication profiles are included in the IPSO operating system:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• base_httpd_authprofile</td>
</tr>
<tr>
<td></td>
<td>• base_login_authprofile</td>
</tr>
<tr>
<td></td>
<td>• base_other_authprofile</td>
</tr>
<tr>
<td></td>
<td>• base_snmpd_authprofile</td>
</tr>
<tr>
<td></td>
<td>• base_sshd_authprofile</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>priority integer</th>
<th>A number indicating the priority of the server. When you configure multiple servers, the priority determines which should be tried first. A smaller number indicates a higher priority. No default. You must enter a value.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>host IPv4 address</th>
<th>The IP address of the TACPLUS server in dot-delimited format.</th>
</tr>
</thead>
</table>
port <1-65535> The UDP port to contact on the server host. You determine the correct value by the configuration of your TACPLUS server. Common values are 1812 (specified by the standard) and 1645 (nonstandard but used traditionally).

*port* also takes the keyword *unset*, which indicates that no value is set in the database so the default is used.

1812

secret name The “shared secret” used to authenticate the TACPLUS server and the local client to each other. The same value should be configured on your TACPLUS server.

prompt secret Prompts you to enter the “shared secret” during the run of the command.

timeout integer The number of seconds to wait, after contacting the server, for a response. The default value 3 seconds.

new-priority integer Changes the priority number of the server.

list Displays a list of all servers associated with an authentication profile.
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. |
|-------------------------|-------------------------------------------------------------|
| 1                       |                                                            |

**Configuring Server Options**

The commands in this section allow you to configure SSH server options.

**Configuring Server Access Control**

Use the following commands to configure who is allowed to log in to your platform.

```
set ssh server
    allow-groups name
    allow-users name
    deny-groups name
    deny-users name
    permit-root-login <yes | no | without-password>
```

Use the following commands to show login configurations.

```
show ssh server
```
Configuring Server Options

allow-groups
allow-users
deny-groups
deny-users
permit-root-login

Arguments

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>allow-groups name</td>
<td>Specifies that only a user whose primary or supplementary group name matches this pattern may log in. You may use wildcard characters ‘*’, '?' and specify multiple user names or patterns separated by spaces. Numerical group identifications are not recognized. Login is allowed for all groups by default.</td>
</tr>
<tr>
<td>allow-users name</td>
<td>Specifies that only a user whose login name matches this pattern may log in. You may use wildcard characters ‘*’, '?' and specify multiple user names or patterns separated by spaces. Numerical user identifications are not recognized. If the pattern takes the form USER@HOST then USER and HOST are checked separately. Login is allowed for all users by default.</td>
</tr>
<tr>
<td>deny-groups name</td>
<td>Specifies groups forbidden to log in. Each user has only one primary group, identified by the group id in the user’s configuration.</td>
</tr>
<tr>
<td>deny-users name</td>
<td>Specifies users forbidden to log in.</td>
</tr>
<tr>
<td>permit-root-login</td>
<td>Specifies whether admin can log in using SSH. The without-password setting allows admin to log in, but not by using the password mode of authentication.</td>
</tr>
</tbody>
</table>

Configuring Server Authentication of Users

Use the following commands to configure the type of authentication the server will use to authenticate users.

set ssh server
   pubkey-authentication <0 | 1>
   password-authentication <0 | 1>
   rhosts-authentication <0 | 1>
Configuring Server Options

rhosts-rsa-authentication <0 | 1>
rsa-authentication <0 | 1>

Use the following commands to show user authentication configurations.
show ssh server
  pubkey-authentication
  password-authentication
  rhosts-authentication
  rhosts-rsa-authentication
  rsa-authentication

Arguments

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>pubkey-authentication</td>
<td>Specifies whether pure DSA authentication is allowed (for version 2 of the protocol only).</td>
</tr>
<tr>
<td>password-authentication</td>
<td>Allows authentication using the standard log in password. If this is set to 0, other forms of authentication may be used. This may require additional configuration.</td>
</tr>
<tr>
<td>rhosts-authentication</td>
<td>Specifies whether authentication using rhosts or hosts.equiv is sufficient.</td>
</tr>
<tr>
<td>rhosts-rsa-authentication</td>
<td>Specifies whether rhosts or hosts.equiv authentication is accepted when combined with successful RSA host authentication.</td>
</tr>
<tr>
<td>rsa-authentication</td>
<td>Specifies whether pure RSA authentication is allowed (for version 1 of the protocol only).</td>
</tr>
</tbody>
</table>

Configuring User Login Environment

Use the following commands to configure the user environment.
Configuring Server Options

```
set ssh server
    print-motd <0 | 1>
    use-login <0 | 1>

Use the following commands to show user environment configurations.
show ssh server
    print-motd
    use-login

Arguments
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>print-motd</td>
<td>Specifies whether text from /etc/motd is displayed when the user logs in interactively.</td>
</tr>
<tr>
<td>use-login</td>
<td>Specifies whether the login utility is used for interactive logins.</td>
</tr>
</tbody>
</table>

Configuring Server Protocol Details

Use the following commands to configure SSH protocols.
```
set ssh server
    ciphers name
    keepalives <0 | 1>
    listen-addr ip_address
    listen-addr2 ip_address
    port <1-65535>
    protocol <1 | 2 | 1,2>
    server-key-bits <512 | 640 | 768 | 864 | 1024>

Use the following commands to show SSH protocol configurations.
show ssh server
    ciphers
    keepalives
    listen-addr
```
Configuring Server Options

listen-addr2
port
protocol
server-key-bits

Arguments

ciphers name

The following list of ciphers are used as the default setting:

- 3des-cbc
- blowfish-cbc
- arcfour
- cast128-cbc
- aes128-cbc
- aes192-cbc
- aes256-cbc

When you use the set command to specify a cipher, or series of ciphers separated by commas, all other ciphers not specified are turned off.

keepalives <0 | 1>

Specifies whether the system should send keepalive messages to the other side.

1

listen-addr ip_address

Specifies the IP address on which to listen for incoming connections. Use dot-delimited format.

listen-addr2 ip_address

Specifies the IP address on which to listen for incoming connections. Use dot-delimited format.

port <1-65535>

Specifies the TCP port number on which the SSH server listens. The default port is 22.

protocol <1 | 2 | 1,2>

Specifies which of the two versions of the SSH protocols to support. Both versions 1 and 2 are on by default. When you use the set command to specify a protocol version, the other protocol version is turned off.

1,2

server-key-bits <512 | 640 | 768 | 864 | 1024>

Defines the number of bits in the server key.

768
**Configuring Service Details**

Use the following commands to configure service details.

```
set ssh server
  gateway-ports <0 | 1>
  ignore-rhosts <0 | 1>
  ignore-user-known-hosts <0 | 1>
  key-regeneration-time integer
  login-grace-time integer
  max-starups integer
```

Use the following commands to show service detail configurations.

```
show ssh server
  gateway-ports
  ignore-rhosts
  ignore-user-known-hosts
  key-regeneration-time
  login-grace-time
  max-starups
```

**Arguments**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>gateway-ports &lt;0</td>
<td>1&gt;</td>
</tr>
<tr>
<td>ignore-rhosts &lt;0</td>
<td>1&gt;</td>
</tr>
</tbody>
</table>
Configuring Server Options

**ignore-user-known-hosts <0 | 1>**
Specifies whether the *known_hosts* file is used during *rhosts+RSA* authentication. The value for no is zero (0).

0

**key-regeneration-time integer**
Specifies the amount of time in seconds when the server key is automatically regenerated. Default is 3600 seconds. A value of 0 means the key is never regenerated.

**login-grace-time integer**
Specifies the amount of time in seconds for the user to log in. Default is 600 seconds. A value of 0 means unlimited time.

**max-startups integer**
Specifies the maximum number of unauthenticated connections which will be allowed at one time. Default is 10.

**Configuring Server Implementation**

Use the following commands to set the level of verbosity of sshd logged messages and to specify whether to check file modes and ownership of files and directories at log in.

```bash
set ssh server
  log-level name
  strict-modes <0 | 1>
```

Use the following commands to show service detail configurations.

```bash
show ssh server
  log-level
  strict-modes
```
### Arguments

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>log-level name</td>
<td>Specifies the verbosity level used when logging messages from <code>sshd</code>. The following are the values you can designate from least to most verbose:</td>
</tr>
<tr>
<td></td>
<td>- QUIET</td>
</tr>
<tr>
<td></td>
<td>- FATAL</td>
</tr>
<tr>
<td></td>
<td>- ERROR</td>
</tr>
<tr>
<td></td>
<td>- INFO</td>
</tr>
<tr>
<td></td>
<td>- VERBOSE</td>
</tr>
<tr>
<td></td>
<td>- DEBUG</td>
</tr>
<tr>
<td>Default is INFO.</td>
<td></td>
</tr>
</tbody>
</table>

| strict-modes <0 | 1> | Specifies whether to check file modes and ownership of certain files and directories before allowing the user to log in. The value for yes is 1. |

1

---

**Configuring and Managing SSH Key Pairs**

The commands in the following section allow you to configure SSH key pairs and to obtain the current public keys.

### Creating and Viewing Host Keys

Use the following commands to generate new host keys.

```bash
set ssh hostkey
    v1 size integer
    v2 <dsa | rsa> size integer
```

Use the following commands to view the current public host keys.

```bash
show ssh hostkey
    v1
    v2 <dsa | rsa> [ssh2-format]
```
Generating New User Identity Keys

Use the following commands to generate new user identity keys that will be used to authenticate users with other SSH servers.

set ssh identity

v1 user name size integer <passphrase string | prompt-passphrase>

v2 <dsa | rsa> user name size integer <passphrase string | prompt-passphrase>

Use the following commands to obtain the public identity keys.

show ssh identity

v1 user name

v2 <dsa | rsa> [ssh2-format]
Managing Authorized Keys

Use the following commands to add authorized public keys for users, enabling the users to log in to their accounts using their keys.

```
add ssh authkeys
```

```
v1 user name bits integer exponent integer modulus string [comment name]
```

```
v2 <dsa | rsa> user name <openssh-format string | ssh2-format file name> [comment name]
```

Use the following commands to delete authorized keys.

```
delete ssh authkeys
```

```
v1 user name id number
```

```
v2 <dsa | rsa> user name id number
```

Use the following commands to view authorized keys configured for user accounts.

```
show ssh authkeys
```

```
v1 user name < list | id number>
```

---

v2 <dsa | rsa> Creates a new DSA or RSA v2 public/private key pair that will be used to authenticate the given user to other SSH servers when connecting using SSH protocol version 2.

user name Identifies the user for which you want to create a new key pair.

size integer Specifies the size of the key in bits. 1024 bits is recommended. Other common key sizes are 512, 640, 768, and 864. The key must be at least 512 bits.

passphrase string Provides an optional passphrase that is used to encrypt the private key. The user must enter this passphrase when using the key. If you use this argument, the passphrase text is echoed on the screen as you enter it.

prompt-passphrase Tells the system to prompt you for the optional passphrase after you enter the command. The passphrase is not displayed on the screen as you enter it.
# Configuring and Managing SSH Key Pairs

```bash
v2 <rsa | dsa> user name < list | id number>
```

## Arguments

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>v1</strong></td>
<td>Specifies that the authorized key being added is an RSA v1 public key.</td>
</tr>
<tr>
<td>v2 &lt;dsa</td>
<td>rsa&gt;</td>
</tr>
<tr>
<td>user name</td>
<td>Identifies the user account for which you are authorizing the key.</td>
</tr>
<tr>
<td>bits integer exponent</td>
<td>Provides the RSA v1 key as follows:</td>
</tr>
<tr>
<td>integer modulus string</td>
<td>• bits integer—key size, for example 1024.</td>
</tr>
<tr>
<td></td>
<td>• exponent integer—usually the second number making up an RSA v1 key, for example 35.</td>
</tr>
<tr>
<td></td>
<td>• modulus string—a very long number that is usually the third value of an RSA key.</td>
</tr>
<tr>
<td>&lt;openssh-format string</td>
<td>ssh2-format file name&gt;</td>
</tr>
<tr>
<td></td>
<td>• openssh-format string—the text of key in OpenSSH format, which is a long string of characters, numbers, and punctuation. Omit the “ssh-dss” or “ssh-rsa” label that might come before the key.</td>
</tr>
<tr>
<td></td>
<td>• ssh2-format file name—the file on the local system that contains the SSHv2 formatted key.</td>
</tr>
<tr>
<td>comment string</td>
<td>Specifies an optional comment which can be used to help identify the key.</td>
</tr>
<tr>
<td>id number</td>
<td>The identification number associated with a particular key. The ID value is assigned by the system and is used to specify the key for viewing or deletion.</td>
</tr>
<tr>
<td>list</td>
<td>Shows ID values and any optional comments associated with authorized keys.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>daemon-enable</td>
<td>Enables and disables web configuration for the platform.</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>port</td>
<td>Specifies the port number on which the Voyager web configuration tool can be accessed when <em>not</em> using SSL-secured connections.</td>
</tr>
<tr>
<td>&lt;1-65535&gt;</td>
<td>If you change the port number, you will have to change the URL used when accessing Voyager from <a href="http://hostname/">http://hostname/</a> to <a href="http://hostname:PORTNUMBER/">http://hostname:PORTNUMBER/</a> 80</td>
</tr>
</tbody>
</table>
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

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/ 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.
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.

    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 email address that could be used for contacting the person responsible for platform and its certificate, for example, “webmaster@ship.wwwidgets.dom”
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 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.

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 when generating the certificate and private key or certificate request. Using this syntax will not echo your passphrase as you type.
Password and Account Management

Use these commands to set policies for managing user passwords and accounts. The features included in password and account management are a global and comprehensive way to manage password policy. For more information about these features, see the “Managing Security and Access” chapter of the Check Point Network Voyager Reference Guide for IPSO 6.2 http://supportcontent.checkpoint.com/documentation_download?ID=10293.

To manage individual user accounts, see “Managing System Users” on page 278 and “Managing Roles” on page 280 for more information.

To view password and account management configuration, use these commands.

show password-controls
  min-password-length
  complexity
  palindrome-check
  history-checking
  history-length
  password-expiration
  expiration-warning-days
  expiration-lockout-days
  force-change-when
  deny-on-fail enable
  deny-on-fail failures-allowed
  deny-on-fail allow-after
  deny-on-nonuse enable
  deny-on-nonuse allowed-days
  all

To change password and account management configuration, use these commands.

set password-controls
  min-password-length <6-128>
  complexity <2-4>
  palindrome-check <on | off>
history-checking <on | off>
history-length <1-1000>
password-expiration <never | 1-1827>
expiration-warning-days <1-366>
expiration-lockout-days <never | 1-1827>
force-change-when <no | password | first-password>
deny-on-fail enable <on | off>
deny-on-fail failures-allowed <2-1000>
deny-on-fail allow-after <60-604800>
deny-on-nonuse enable <on | off>
deny-on-nonuse allowed-days <30-1827>

Arguments

min-password length <6-128> Specifies the minimum number of characters of a password that is to be allowed for users or SNMP users. Does not apply to passwords that have already been set.

6
### complexity <1-4>

Specifies how complex users must make their passwords. Password characters are divided into four types: upper case alphabetic (A-Z), lower case alphabetic (a-z), digits (0-9), and other (everything else such as !, #,.&.). The following is a description of the values:

- 1 disables complexity checking.
- 2 requires that passwords are comprised of a minimum of two character types, for example, abcABC.
- 3 requires that passwords are comprised of a minimum of three character types, for example, ab1ABC.
- 4 requires that passwords are comprised of a minimum of four character types, for example, ab1AB#.

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Disables complexity checking.</td>
</tr>
<tr>
<td>2</td>
<td>Requires a minimum of two character types.</td>
</tr>
<tr>
<td>3</td>
<td>Requires a minimum of three character types.</td>
</tr>
<tr>
<td>4</td>
<td>Requires a minimum of four character types.</td>
</tr>
</tbody>
</table>

### palindrome-check <on | off>

Checks for passwords that are read the same left to right or right to left, such as racecar or the phrase straw warts.

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>on</td>
<td>Checks for palindromic passwords.</td>
</tr>
<tr>
<td>off</td>
<td>Does not check for palindromic passwords.</td>
</tr>
</tbody>
</table>

### history-checking <on | off>

Enables a check for passwords being reused.

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>on</td>
<td>Enables password history checking.</td>
</tr>
<tr>
<td>off</td>
<td>Disables password history checking.</td>
</tr>
</tbody>
</table>

### history-length <1-1000>

Specifies the number of past passwords that will be kept and checked against for reuse for each user.

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>Specifies that the history length is 10.</td>
</tr>
</tbody>
</table>
Password and Account Management

password-expiration <never | 1-1827>

Specifies the number of days since the last password change before a user is required to set a new password. Once the specified number of days have passed without a password change, the password expires and the user is required to change password again the next time the user logs in. The value “never” disables the feature. Password expiration applies to regular users, not to SNMP users.

never

expiration-warning-days <1-366>

Specifies the number of days before a password expires that a user starts receiving warnings that the password is due to expire.

7 days

expiration-lockout-days <never | 1-1827>

Specifies the number of days after password expiration that a user is locked out if the user has not set a new password.

never

force-change-when <no | password | first-password>

Specifies whether to force users to change their passwords.

• no disables forcing a user to change an assigned password at login.

• password forces a user to change a password after an administrator sets it with the set user command or with the Network Voyager User Management page. The forced password change does not apply to passwords set by the user through a self-password change.

• first-password forces a new user to change password from the initial password assigned by the administrator when the user account is created.

no
### Password and Account Management

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>**deny-on-fail enable &lt;on</td>
<td>off&gt;**</td>
</tr>
<tr>
<td><strong>deny-on-fail failures-allowed &lt;2-1000&gt;</strong></td>
<td>Sets the number of failed logins a user can have before being locked out.</td>
</tr>
<tr>
<td><strong>deny-on-fail allow-after &lt;60-604800&gt;</strong></td>
<td>Sets the number of seconds a user has to wait before being able to log in after being locked out because of failed logins.</td>
</tr>
<tr>
<td>**deny-on-nonuse enable &lt;on</td>
<td>off&gt;**</td>
</tr>
<tr>
<td><strong>deny-on-nonuse allowed-days &lt;30-1827&gt;</strong></td>
<td>Sets the number of days after a user has last logged in before they are locked out.</td>
</tr>
</tbody>
</table>
Users and Roles Management

Use the commands in “Managing System Users” to add and delete new system users. The system has default admin and monitor users. You can use the commands in “Changing the Admin and Monitor Password” to change the password for admin and monitor.

To create an IPSO cluster, you must create a cluster configuration on each system that participates in the cluster. When you do this, the system creates a cadmin user on each of these systems, and you must create the same password for the cadmin user on each system. (You use the cadmin user to manage a cluster.) You can use the commands described in this section to manage the password for the cadmin user.

This command set also includes commands for configuring an S/Key, a one-time password system that authenticates remote telnet and FTP users.

Managing System Users

Use these commands to add new users and to set and change user passwords, user ID, group ID, home directory, and default shell.

For information on setting SNMP users, see “Managing SNMP Users”.

Use the following commands to view configuration and conditions.

show users
show user username
    force-password-change
    lock-out

Using the following command to delete an existing user.

delete user username

Use the following commands to add or modify user accounts.

set user username
    passwd
    newpass passwd
    info string
    uid <0-65535>
    gid <0-65535>
Managing System Users

homedir \textit{unix\_path\_name}
shell \textit{string}
homepage \textit{tcl\_script\_name}
force-password-change <on | off>
lock-out off

\textbf{add user} \textit{username}
uid <0-65535> homedir Unix path name

\textbf{Note} - You can use the \textit{add user} command to add new users, but you must use the \textit{set user name passwd} command to set the password and allow the user to log on to the system.

\section*{Arguments}

\begin{tabular}{|l|p{0.8\textwidth}|}
\hline
\textit{user} \textit{username} & Specifies the new user name or an existing user name. The valid characters are alphanumeric characters, dash (-), and underscore (_). Range: 1-32 characters \\
\hline
\textit{passwd} & Starts a password change dialog. You will be asked to enter a new password for the user and then asked to verify it by re-entering it. The password you enter will not be visible on terminal. \\
\hline
\textit{newpass} \textit{passwd} & Specifies a new password for the user. If you use this keyword to change the password, you will not be asked to verify the new password and the password you enter is visible on the terminal. \\
\hline
\textit{info} \textit{string} & Specifies a string describing the specified users. This string is used as the sender’s name in any email sent by this user. Use alphanumeric characters and the space key only. \\
\hline
\textit{uid} <0-65535> & Specifies the specified user’s user ID, which is used to identify the user’s permissions. \\
\hline
\textit{gid} <0-65535> & Specifies the ID for the primary group to which a user belongs. Use the group management commands to specify membership in other groups. \\
\hline
\end{tabular}
Managing Roles

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>homedir Unix_path_name</td>
<td>Specifies the user's home directory, where the user is placed on login. Enter the full Unix path name. If the directory doesn't already exist, it is created. The home directory for all users must be in /var/emhome/.</td>
</tr>
<tr>
<td>shell string</td>
<td>Specifies the user's shell, which is invoked when the user logs in. The default shell is /bin/csh. To change the shell, enter the new shell path name. Consult the /etc/shells file for valid login shells.</td>
</tr>
<tr>
<td>homepage tcl_script_name</td>
<td>This argument is not supported. Its use will not cause an error but it has no effect.</td>
</tr>
<tr>
<td>force-password-change</td>
<td>On forces the user to change password the next time they log in. Off overrides any condition forcing the user to change password.</td>
</tr>
<tr>
<td>lock-out off</td>
<td>Clears any lockout conditions that are present on the user account and allows the user to log in.</td>
</tr>
</tbody>
</table>

For information on removing access mechanism permissions from a user, see the delete rba user commands below.

**Managing Roles**

To view existing role configurations, use these commands.

```
show rba
  all
  role rolename
  roles
  user username
  users
```

To add a role use the following command.

```
add rba role rolename domain-type <System | Cluster | MRI>
  [readonly-features featurelist readwrite-features featurelist]
```

To grant or change the access-mechanisms assigned to a user, use the following command.

```
add rba user username access-mechanisms <Voyager | CLI>
```
To assign a role to a user on a system which does not have clustering or MRI enabled, use the following command.

```
add rba user username roles rolename
```

To assign a role to a user on a system which has clustering or MRI enabled, use the following command.

```
add rba user username role rolename domains <System | Cluster | MRI>
```

**Arguments**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>role rolename</td>
<td>Specifies the name of the role.</td>
</tr>
<tr>
<td>domain-type</td>
<td>Specify the role type. System roles apply only to this machine, cluster roles apply to each node in the cluster, and MRI roles apply to specified MRIs.</td>
</tr>
<tr>
<td>[readonly-features featurelist]</td>
<td>List each feature which you want to include in the role as having either read-only or read/write access. Separate each with a comma and do not use spaces. For a list of available features, use the tab completion in the CLI.</td>
</tr>
<tr>
<td>readwrite-features featurelist</td>
<td></td>
</tr>
<tr>
<td>access-mechanisms &lt;Voyager</td>
<td>CLI&gt;</td>
</tr>
<tr>
<td>domains &lt;System</td>
<td>Cluster</td>
</tr>
</tbody>
</table>

To remove features from a role, use this command.

```
delete rba role rolename [readonly-features featurelist readwrite-features featurelist]
```

To remove privileges for access mechanisms from a user, use this command.

```
delete rba user username access-mechanisms <Voyager | CLI>
```

To remove a role assignment from a user, use this command.

```
delete rba user username roles rolename
```

To remove access to an MRI from a user, use this command.

```
delete rba user username role rolename domains MRI MRIid
```

**Arguments**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rba user username</td>
<td>Specifies the user.</td>
</tr>
</tbody>
</table>
Changing the Admin and Monitor Password

Use the following commands to change the password for admin and monitor. Admin and Monitor are default users. Typically, you set the initial passwords for admin and monitor at system startup.

`set user <admin | monitor> newpass passwd`
`set user <admin | monitor> passwd`

**Arguments**

<admin | monitor> Specifies whether to change the admin or the monitor password.

newpass passwd Specifies the new password. If you use this keyword, you will not be asked to confirm the new password and the password you enter is visible on the terminal.

passwd Specifies that you want to change the password. If you use this keyword, you will be prompted for the new password and then asked to verify the password by re-entering it. The password you enter is not visible on the terminal.

**Note** - Only users with admin user permissions can change the user and admin passwords.
Configuring S/Key for Admin and Monitor

Use the following commands to configure S/Key for admin and monitor. S/Key is a one-time password system that authenticates telnet and FTP users.

set skey
  user <admin | monitor> mode <disabled | allowed | required>
  user <admin | monitor> key
  user <admin | monitor> currpass passwd secret string
  pass-phrase seed value sequence value
  pass-phrase seed value sequence value secret string
  pass-phrase seed value sequence value count value
  pass-phrase seed value sequence value count value secret string

Arguments

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>user &lt;admin</td>
<td>monitor&gt; mode &lt;disabled</td>
</tr>
<tr>
<td>user &lt;admin</td>
<td>monitor&gt; key currpass passwd secret string</td>
</tr>
<tr>
<td>pass-phrase seed value sequence value</td>
<td>Generates one S/Key pass-phrase using the seed and sequence values provided. The command prompts you to enter a secret.</td>
</tr>
<tr>
<td>pass-phrase seed value sequence value count value</td>
<td>Generates count S/Key pass-phrases using the seed and sequence values provided. The command prompts you to enter a secret.</td>
</tr>
<tr>
<td>pass-phrase seed value sequence value secret string</td>
<td>Generates one S/Key pass-phrase using the seed, sequence, and secret values provided.</td>
</tr>
<tr>
<td>pass-phrase seed value sequence value count value secret string</td>
<td>Generates count S/Key pass-phrases using the seed, sequence, and secret values provided.</td>
</tr>
</tbody>
</table>
Show Commands

Use the following commands to view current users, their settings and permissions.

- `show users`
- `show user name`
- `show skey all`
- `user <admin | monitor>`
- `user <admin | monitor> sequence`
- `user <admin | monitor> seed`
- `user <admin | monitor> mode`

Arguments

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show users</code></td>
<td>Displays all users, their user IDs, primary group IDs, user shells, home directories, and home pages.</td>
</tr>
<tr>
<td><code>show user name</code></td>
<td>Displays information about the specified user, including the user ID, primary group ID, user shell, home directory and home page.</td>
</tr>
<tr>
<td><code>show skey all</code></td>
<td>Displays whether S/Key is enabled or disabled for both admin and monitor and the configured sequence and seed values if S/Key is enabled.</td>
</tr>
<tr>
<td>`user &lt;admin</td>
<td>monitor&gt;`</td>
</tr>
<tr>
<td>`user &lt;admin</td>
<td>monitor&gt; sequence`</td>
</tr>
<tr>
<td>`user &lt;admin</td>
<td>monitor&gt; seed`</td>
</tr>
<tr>
<td>`user &lt;admin</td>
<td>monitor&gt; mode`</td>
</tr>
</tbody>
</table>
Group Management

The commands in this section allow you to manage groups.

Managing Groups

Use the following commands to create and delete groups and to add and remove members.

set group string gid <100-65530>
add group string gid <100-65530>
delete group string
add group string member username
delete group string member username

Arguments

group string gid <100-65530> Specifies to create a new group and the group's ID. Enter a string of alphanumerical characters of 1 to 8 characters long. The name must be unique on your system, and the numeric ID you specify must be unique on your system. Note that ID ranges 0-99 and 65531-65535 are reserved for system use. If you specify a value within these ranges, an error message is displayed.

group string member username Specifies to add an existing user to an existing group, including users admin and monitor.

Show Commands

Use the following commands to view existing groups and group members.

show groups
show group string

Arguments

groups Displays names of all existing groups, including wheel—the admin and root group—and the corresponding group ID and members.

group string Displays information about the specified group name, including the group ID and members.
VPN Acceleration

If you have a VPN accelerator card installed in your system, you can use CLI commands to enable or disable it and view information.

Configuring VPN Acceleration

Use the following commands to disable or enable a VPN accelerator card.

set cryptaccel <disable | enable>

Displaying VPN Accelerator Information

Use the following commands to display VPN accelerator status or statistics.

show cryptaccel <status | statistics>

VPN accelerator status information includes the following:

• Device ID
• Status (up or down)

VPN accelerator statistics information includes the following:

• Contexts (created and current)
• Packets (received, dropped, and processed)
• Bytes (received, dropped, and processed)
• Errors (received digest, random number, buffer alignment, device, memory, context, and packet header)
Chapter
Routing Commands

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

In This Chapter

Route Map Commands  page 289
BGP  page 305
OSPF  page 324
RIP  page 343
IGRP  page 347
IGMP  page 352
PIM  page 356
Static Multicast Routes  page 366
Route Aggregation  page 368
BOOTP  page 371
DVMRP  page 373
DVMRP  page 373
Static Routes  page 377
ICMP Router Discovery  page 380
IP Broadcast Helper  page 382
Network Time Protocol  page 385
Routing Option Commands  page 390
Trace Routing Commands  page 393
Show Route Summary Commands  page 403
Show Routing Daemon (IPSRD) Commands  page 405
Show MFC Commands  page 408
Route Map Commands

Route maps are used to control which routes are accepted and announced by dynamic routing protocols. Use route maps to configure inbound route filters, outbound route filters and to redistribute routes from one protocol to another.

You can define route maps only using the CLI, this feature is not available in Network Voyager.

Route maps support both IPv4 and IPv6 protocols, including RIP, BGP, RIPng, OSPFv2, and OSPFv3. BGP4++ policy can only be specified using route maps. For the other protocols, you can use either route maps or the Route Redistribution and Inbound Route Filters features that you configure using Network Voyager. Route map for import policy corresponds to Inbound Route Filters; route map for export policy corresponds to Route Redistribution.

Note - Route maps offer more configuration options than the based configuration for route redistribution and inbound route filters. They are not functionally equivalent.

Protocols can use route maps for redistribution and Network Voyager settings for inbound route filtering and vice versa. However, if one or more route maps are assigned to a protocol (for import or export) any corresponding Network Voyager configuration (for route redistribution or inbound route filters) is ignored.

Each route maps includes a list of match criteria and set statements. You can apply route maps to inbound, outbound, or redistribution routes. Routes are compared to the match criteria, and all the actions specified in the set criteria are applied to those routes which meet all the match conditions. You can specify the match conditions in any order. If you do not specify any match conditions in a route map, that route map then matches all routes.

You define route maps, then assign them to protocols for export or import policy for that protocol. Route maps take precedence over voyager based configuration.

To create a route map, use CLI commands to specify a set of criteria that must be matched for the command to take effect. If the criteria are matched, then the system executes the actions you specify. A route map is identified by name and also has an identifying number, an allow or restrict clause, and a collection of match and set statements.
There can be more than one instance of a route map (same name, different ID). The lowest numbered instance of a route map is checked first. Route map processing stops when either all the match criteria of some instance of the route map are satisfied, or all the instances of the particular route map are exhausted. If the match criteria are satisfied, the actions in the set section are performed.

Routing protocols can use more than one route map when you specify distinct preference values for each. The appropriate route map with lowest preference value is checked first.

**Set Routemap Commands**

Use the following commands to set a route map.

```
set routemap rm_name id <1-65535>
  <off|on>
  allow
  inactive
  restrict
```

**Arguments**

- `routemap rm_name` Specify the name of the routemap.
- `id <1-65535>` Specify the ID of the routemap. You can enter the keyword default or the default value 10.
- `<off|on>` Use on to create a routemap, use off to delete a routemap.
- `allow` Specifies to allow routes that match the routemap.
- `inactive` Use this argument to temporarily disable a routemap. To activate the routemap, use the allow or restrict arguments.
- `restrict` Specifies that routes that match the routemap are not allowed.

To specify actions for a routemap, use the following commands.

```
set routemap rm_name id id_number action
```

**Note** - Some statements affect only a particular protocol. For information on which statements affect a given protocol, see the "Supported Route Map Statements by Protocol" section, below.

Also, the same parameter cannot appear both as a match and action statement in a routemap. These include Community, Metric, and Nexthop.
aspath-prepend-count <1-25>
community <append | replace | delete> [on|off]
community <1-65535> as <1-65535> [on|off]
community no-export [on|off]
community no-advertise [on|off]
community no-export-subconfed [on|off]
community none [on|off]
localpref <1-65535>
metric <add|subtract> <1-16>
metric igp [add | subtract] <1-4294967295>
metric value <1-4294967295>
nexthop <ip ipv4_address | ipv6 ipv6_address>
precedence <1-65535>
preference <1-65535>
route-type <type-1 | type-2>
remove action_name
ospfautomaticitag tag
ospfmanualtag tag
riptag tag

drugenmap rm name Specify the name of the routemap.
id id number Specify the ID of the routemap. You can enter the keyword default or the default value 10.
aspath-prepend-count Specifies to affix AS numbers at the beginning of the AS path. It indicates the number of times the local AS number should be prepended to the AS PATH before sending out an update. BGP only.
Set Routemap Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>community &lt;append</td>
<td>replace</td>
</tr>
<tr>
<td>community &lt;1-65535&gt; as &lt;1-65535&gt; [on</td>
<td>off]</td>
</tr>
<tr>
<td>community no-export [on</td>
<td>off]</td>
</tr>
<tr>
<td>community no-advertise [on</td>
<td>off]</td>
</tr>
<tr>
<td>community no-export-subconfed [on</td>
<td>off]</td>
</tr>
<tr>
<td>community none [on</td>
<td>off]</td>
</tr>
<tr>
<td>localpref &lt;1-65535&gt;</td>
<td>Set the local preference for BGP route. BGP only.</td>
</tr>
<tr>
<td>metric [&lt;add</td>
<td>subtract&gt;] &lt;1-16&gt;</td>
</tr>
<tr>
<td>metric igp [&lt;add</td>
<td>subtract&gt; &lt;1-4294967295&gt;]</td>
</tr>
<tr>
<td>metric value &lt;1-4294967295&gt;</td>
<td>Set the metric value. For RIP the metric is metric, for OSPF the metric is cost, and for BGP the metric is MED.</td>
</tr>
</tbody>
</table>
To specify the criteria that must be matched for the routemap to take effect, use the following commands.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>set routemap rm_name id &lt;1-65535&gt; match</code></td>
<td>Set IPv4 or IPv6 Nexthop Address. BGP only.</td>
</tr>
<tr>
<td>`as &lt;1-65535&gt; [on</td>
<td>off]`</td>
</tr>
<tr>
<td>`aspath-regex [&quot;regular_expression&quot;</td>
<td>empty] origin &lt;any</td>
</tr>
<tr>
<td>`community &lt;1-65535&gt; as &lt;1-65535&gt; [on</td>
<td>off]`</td>
</tr>
<tr>
<td>`community exact [on</td>
<td>off]`</td>
</tr>
<tr>
<td>`community no-export [on</td>
<td>off]`</td>
</tr>
<tr>
<td>`community no-advertise [on</td>
<td>off]`</td>
</tr>
<tr>
<td>`community no-import [on</td>
<td>off]`</td>
</tr>
<tr>
<td>`community no-import-subconfed [on</td>
<td>off]`</td>
</tr>
</tbody>
</table>

Note - Some statements affect only a particular protocol. For information on which statements affect a given protocol, see the “Supported Route Map Statements by Protocol” section, below.

Also, the same parameter cannot appear both as a match and action statement in a routemap. These include Community, Metric, and N(x)exthop.
community none [on|off]
ifaddress <IPv4_addr | IPv6_addr> [on | off]
interface interface_name [on | off]
metric value <1-4294967295>
neighbor <IPv4_addr | IPv6_addr> [on | off]
network <IPv4_network | IPv6_network> / masklength
<all | exact | off | refines>
network <IPv4_network | IPv6_network> / masklength between
masklength and masklength
nexthop IPv4_addr | IPv6_addr [on | off]
protocol
<ospf2 | ospf2ase | ospf3 | ospf3ase | bgp | rip | ripng | static | direct | aggregate>
route-type <type-1 | type-2 | inter-area | intra-area>
[on | off]
remove match_condition_name

Arguments

as <1-65535>
[on | off]

aspath-regexp
["<regular-expression>" | empty] origin <any | igp | incomplete>

community <1-65535>
as <1-65535> [on|off]

community exact
[on|off]

aspath-regex
Match the specified autonomous system number with the AS number of a BGP peer. For BGP only.
Match the specified aspath regular expression. For BGP only.

Note: Enter the regular expression in quotation marks. Use the empty keyword to match a null ASPath.

Specify the BGP community value.

Specify that the communities present in the route must exactly match all the communities in the routemap. In absence of the exact clause, the route can have other community values associated with it in addition to the ones contained in the routemap. You can have multiple community statements in a route map to form a community string.
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>`community no-export [on</td>
<td>off]`</td>
</tr>
<tr>
<td>`community no-advertise [on</td>
<td>off]`</td>
</tr>
<tr>
<td>`community no-export-subconfed [on</td>
<td>off]`</td>
</tr>
<tr>
<td>`community none [on</td>
<td>off]`</td>
</tr>
<tr>
<td>`ifaddress &lt;IPv4_addr</td>
<td>IPv6_addr&gt; [on</td>
</tr>
<tr>
<td>`interface interface_name [on</td>
<td>off]`</td>
</tr>
<tr>
<td><code>metric value &lt;1-4294967295&gt;</code></td>
<td>Match the specified metric value.</td>
</tr>
<tr>
<td>`neighbor &lt;IPv4_addr</td>
<td>IPv6_addr&gt; [on</td>
</tr>
</tbody>
</table>
Set Routemap Commands

network <IPv4_network | IPv6_network> / masklength

Use with the following keywords:
- **all**: Match all networkds belonging to this prefix and masklength. This is a combination of exact and refines.
- **between** masklength and masklength: Specify a range of masklengths to be accepted for the specified prefix.
- **exact**: Match prefix exactly.
- **off**: Delete the network match statement.
- **refines**: Match networks with more specific mask lengths only. Matches only subnets.

There can be multiple network match statements in a route map.

nexthop <IPv4_addr | IPv6_addr>
[on | off]

Match the specified nexthop address.

protocol <ospf2 | ospf2ase | ospf3 | ospf3ase | bgp | rip | ripng | static | direct | aggregate>

Match the specified protocol. Use this for route redistribution.

route-type <type-1 | type-2 | inter-area | intra-area> [on|off]

As a match statement in routemap for export policy, it can be used by any protocol to redistribute OSPF routes. If route-type of inter-area or intra-area is specified, the protocol match condition should be set to ospf2 or ospf3 and if route-type of type-1 or type-2 is specified, then protocol match condition should be set to ospf2ase or ospf3ase.

While exporting OSPF ASE routes to other protocol, if metric match condition is set but route-type match condition is not set, it will try to match the metric value for both type-1 and type-2 routes.

There can be multiple route-type match statements.
Show Routemap Commands

show routemap rm_name <all | id VALUE>
show routemaps

Routemap Protocol Commands

To assign routemaps to protocols, use the following commands. The preference value specifies which order the protocol will use each routemap.

set <ospf | rip | ipv6 ospfv3 | ipv6 ripng> export-routemap rm_name preference VALUE on
set <ospf | rip | ipv6 ospfv3 | ipv6 ripng> import-routemap rm_name preference VALUE on

To turn a routemap off, use the following commands.

set <ospf | rip | ipv6 ospfv3 | ipv6 ripng> export-routemap rm_name off
set <ospf | rip | ipv6 ospfv3 | ipv6 ripng> import-routemap rm_name off

To view routemaps assigned to protocols, use the following command.

show <ospf | rip | ipv6 ospfv3 | ipv6 ripng> routemap

To set BGP routemaps for export and import policies, use the following commands.

Note - BGP supports both IPv4 and IPv6 routes; use the family option to specify for which address family the routemap will be used. Default is inet. To use for IPv6 routes the family should be set to inet6 or inet-and-inet6.

set bgp external remote-as <1-65535> export-routemap rm_name  
off

    preference <1-65535> [family 
<inet | inet6 | inet-and-inet6>] on

set bgp external remote-as <1-65535> import-routemap rm_name  
off

    preference <1-65535> [family 
<inet | inet6 | inet-and-inet6>] on

remove match_condition_name

Remove the specified match condition from the routemap. For match conditions which can have multiple match statements (such as network, neighbor), this argument removes all of them.
set bgp internal export-routemap \textit{rm\_name}
\begin{verbatim}
    off
    preference <1-65535> [family <inet | inet6 | inet-and-inet6>] on
\end{verbatim}
set bgp internal import-routemap \textit{rm\_name}
\begin{verbatim}
    off
    preference <1-65535> [family <inet | inet6 | inet-and-inet6>] on
\end{verbatim}

\textbf{Note} - You cannot use routemaps in BGP confederations. To configure route filters and redistribution for BGP confederations, use the Inbound Route Filters and Route Redistribution pages in Network Voyager.

\section*{Supported Route Map Statements by Protocol}

Some statements affect only a particular protocol, for example, matching the Autonomous System Number is applicable only to BGP. If such a condition is in a routemap used by OSPF, the match condition is ignored. Any non-applicable match conditions or actions are ignored and processing is done as if they do not exist. A log message is generated in /var/log/messages for any such statements.

\textbf{Note} - The same parameter cannot appear both as a match and action statement in a routemap. These include Community, Metric, and Nexthop.

\subsection*{RIP/RIPng}

- Import Match conditions: Neighbor, Network, Interface, Ifaddress, Metric, Neighbor, Nexthop.
- Import Actions: Precedence, Metric Add/Subtract
- Export Match conditions when exporting from RIP/RIPng - Interface, Ifaddress, Metric, Network, Nexthop
- Export Match Conditions when redistributing using Protocol match: According to the protocol from which route is being redistributed.
- Export Actions when exporting from RIP/RIPng - Metric Add/Subtract
- Export Actions when redistributing - Metric Set
**Supported Route Map Statements by Protocol**

### OSPFv2/OSPFv3
- Import Match conditions: Network (Route Prefix)
- Import Actions: Precedence
- Export Match conditions when other protocols redistribute OSPF routes: Network, Interface, Ifaddress, Metric, Route-type, Nexthop
- Export Match conditions when OSPF redistributes routes from other protocols: Conditions supported by that protocol
- Export Actions when redistributing to AS External: Metric, Route-type

### BGP
- Import Match conditions: Network (Route Prefix), AS number, ASPATH Regular Expression/Origin, Community String, Neighbor (BGP Peer), Interface, Ifaddress, Metric (MED), Nexthop
- Import Actions: Precedence, LocalPref, Preference (Weight), Nexthop IP/IPv6
- Export Match conditions when exporting from BGP - Metric (MED), Network, Nexthop, Interface, Ifaddress, AS Number, ASPATH, Community String
- Export Match conditions when redistributing other route into BGP using Protocol Match statement - Conditions supported by that protocol.
- Export Actions - Community String (Append, Replace, Delete), Metric (MED) (Set, IGP, Add to IGP, Subtract from IGP), Nexthop IP/IPv6, Aspath Prepend Count

### Redistributing Static, Interface, or Aggregate Routes
When redistributing static routes into BGP, OSPFv2/v3 or RIP/RIPng the following match conditions are supported:
- Network Prefix,
- Nexthop
- Interface
- Ifaddress
- Protocol (proto = static)

When redistributing interface/direct routes into BGP, OSPFv2/v3 or RIP/RIPng the following match conditions are supported:
- Network Prefix
• Interface
• Ifaddress
• Protocol (proto = direct)

When redistributing **aggregate** routes into BGP, OSPFv2/v3 or RIP/RIPng the following match conditions are supported:

• Network Prefix
• Protocol (proto = aggregate)

## Route Map Examples

### Example 1

Redistribute interface route for eth3c0 into ospf, and set the ospf route-type to AS type-2 with cost 20.

```plaintext
set routemap direct-to-ospf id 10 on
set routemap direct-to-ospf id 10 match interface eth3c0
set routemap direct-to-ospf id 10 match protocol direct
set routemap direct-to-ospf id 10 action route-type type-2
set routemap direct-to-ospf id 10 action metric value 20

set ospf export-routemap direct-to-ospf preference 1 on
```

### Example 2

Do not accept routes from RIP neighbor 10.1.2.3, accept routes from neighbor 10.1.2.4 as is, and for all other routes increment the metric by 2.

```plaintext
set routemap rip-in id 10 on
set routemap rip-in id 10 restrict
set routemap rip-in id 10 match neighbor 10.1.2.3

set routemap rip-in id 15 on
set routemap rip-in id 15 match neighbor 10.1.2.4
```
Route Map Examples

Example 3
Redistribute all static routes into BGP AS group 400. Set the MED value to 100, prepend our AS number to the aspath 4 times. If the route belongs to the prefix 10.0.0.0/8, do not redistribute. Send all BGP routes whose aspath matches the regular expression (100 200+) and set the MED value to 200.

```
set routemap static-to-bgp id 10 on
set routemap static-to-bgp id 10 restrict
set routemap static-to-bgp id 10 match protocol static
set routemap static-to-bgp id 10 match network 10.0.0.0/8 all

set routemap static-to-bgp id 15 on
set routemap static-to-bgp id 15 match protocol static
set routemap static-to-bgp id 15 action metric 100
set routemap static-to-bgp id 15 action aspath-prepend-count 4

set routemap bgp-out id 10 on
set routemap bgp-out id 10 match aspath-regex "(100 200+)" origin any
set routemap bgp-out id 10 action metric 200
```

Note - We do not need match protocol statement for routes belonging to the same protocol.

```
set bgp external remote-as 400 export-routemap bgp-out preference 1 family inet on
```
set bgp external remote-as 400 export-routemap
static-to-bgp preference 2 family inet on

Example 4

Redistribute all OSPFv3 (internal and external) routes into BGP group 400, setting the outgoing community string to [no-export, 200 as 100]. For BGP IPv6 routes, send them with an empty community string. For all routes set the nexthop value to 3003::abcd:1012 (the address on the interface connecting to the peers).

Note - To exchange IPv6 routes in BGP the multiprotocol capability must be turned ON in BGP Configuration for the peer.

set routemap ospf3-to-bgp id 10 on
set routemap ospf3-to-bgp id 10 match protocol ospf3
(OSPF3 INTERNAL ROUTES)
set routemap ospf3-to-bgp id 10 action community replace on
set routemap ospf3-to-bgp id 10 action community no-export on
set routemap ospf3-to-bgp id 10 action community 200 as 100 on
set routemap ospf3-to-bgp id 10 action nexthop ipv6 3003::abcd:1012

set routemap ospf3-to-bgp id 20 on
set routemap ospf3-to-bgp id 20 match protocol ospf3ase
(FOR AS EXTERNAL ROUTES)
set routemap ospf3-to-bgp id 20 action community replace on
set routemap ospf3-to-bgp id 20 action community no-export on
set routemap ospf3-to-bgp id 20 action community 200 as 100 on
set routemap ospf3-to-bgp id 10 action nexthop ipv6 3003::abcd:1012
set routemap bgp-out id 10 on
set routemap bgp-out id 10 action community replace on
set routemap bgp-out id 10 action community none on
set routemap ospf3-to-bgp id 10 action nexthop ipv6 3003::abcd:1012

set bgp external remote-as export-routemap bgp-out preference 1 family inet6 on
set bgp external remote-as export-routemap ospf3-to-bgp preference 2 family inet6 on
Multiple Routing Instances

Use the following command to set up multiple routing instances for a single system. Each multiple routing instance has its own routing table and forwarding table. For information on how to configure specific instances using either OSPF or Static Routes, see the sections for using “OSPF” (see page 324) and “Static Routes” (see page 377) commands.

To enable multiple routing instances, enter the following command at the command line:

dbset xpand:instance t

To disable multiple routing instances, enter the following command at the command line.

dbset xpand:instance

**Warning** - Before you disable multiple routing instances, you must first delete all the configuration for each instance. You can continue to maintain any configuration under default, that is any routing configuration that is not part of a multiple routing instance.

Use the following commands to delete and add specific instances.

```plaintext
add instance instance_name
delete instance instance_name
```

**Arguments**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>add instance</td>
<td>Specifies a name for a specific multiple routing instance. The name must use alphanumeric characters and be no more than 16 characters long. Do not use names that refer to protocols, such as rip, static, VRRP, bgp.</td>
</tr>
<tr>
<td>delete instance</td>
<td>Specifies to delete the specific multiple routing instance.</td>
</tr>
</tbody>
</table>
When you do initial configuration, set the router ID. You can also use the following commands to change the router ID.

```
set [instance instance_name] router-id
  default
  ip_address
```

**Arguments**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>Selects the highest interface address when OSPF is enabled.</td>
</tr>
<tr>
<td>ip_address</td>
<td>Specifies a specific IP address to assign as the router ID. Do not use 0.0.0.0 as the router ID address. Check Point recommends setting the router ID rather than relying on the default setting. Setting the router ID prevents the ID from changing if the default interface used for the router ID goes down.</td>
</tr>
</tbody>
</table>

Use the following group of commands to set and view parameters for BGP.

```
set as
  as_number
  off
```

**Arguments**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>as as_number</td>
<td>Specifies the local autonomous system number of the router. This number is mutually exclusive from the confederation and routing domain identifier. The router can be configured with either the autonomous system number or confederation number, not both.</td>
</tr>
</tbody>
</table>

**Caution:** When you change the autonomous system number, all current peer sessions are reset and all BGP routes are deleted. Include the multiple instance routing name if you have configured multiple routing instances.

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>as off</td>
<td>Disables the configured local autonomous system number.</td>
</tr>
</tbody>
</table>
External BGP

Use the following commands to configure external sessions of the protocol, that is, between routers in different autonomous systems.

set bgp external remote-as as_number
  <on | off>
  aspath-prepend-count <1-25 | default>
  description text
  local-address ip_address <on | off>
  virtual-address <on | off>
  outdelay <0-65535>
  outdelay off

Arguments

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>as_number &lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td>aspath-prepend-count &lt;1-25</td>
<td>default&gt;</td>
</tr>
<tr>
<td>description text</td>
<td>You can enter a brief text description of the group.</td>
</tr>
<tr>
<td>local-address ip_address &lt;on</td>
<td>off&gt;</td>
</tr>
</tbody>
</table>
Use the following commands to configure BGP peers. IPSO supports both IPv4 and IPv6 addresses for BGP peers.

A BGP IPv6 address can be either link local or global scoped. If a link local address is used for peering, the outgoing interface must also be configured.

```
set bgp external remote-as as_number peer ip_address
<on | off>
med-out <0-4294967294 | default>
accept-med <on | off>
multihop <on | off>
no-aggregator-id <on | off>
holdtime <6-65535 | default>
keepalive <2-21845 | default>
ignore-first-ashop <on | off>
send-keepalives <on | off>
```
BGP Peers

send-route-refresh [request | route-update] [ipv4 | ipv6 | All] [unicast]
route-refresh <on | off>
accept-routes <all | none>
passive-tcp <on | off>
removeprivateas <on | off>
authtype none
authtype md5 secret secret
throttle-count <0–65535 | off>
ttl <1–255 | default>
suppress-default-originate <on | off>
log-state-transitions <on | off>
log-warnings <on | off>
trace bgp_traceoption <on | off>
capability <default | ipv4-unicast | ipv6-unicast>
graceful-restart-helper <on | off>
graceful-restart-helper-stalepath-time seconds

Arguments

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td>med-out &lt;0–4294967294</td>
<td>Specifies the multi-exit discriminator (MED) metric used as the primary metric on all routes sent to the specified peer address. This metric overrides the default metric on any metric specified by the redistribute policy. External peers uses MED values to decide which of the available entry points into an autonomous system is preferred. A lower MED value is preferred over a higher MED value. 4294967294</td>
</tr>
<tr>
<td>accept-med &lt;on</td>
<td>off&gt;</td>
</tr>
</tbody>
</table>
BGP Peers

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>multihop &lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td>no-aggregator-id</td>
<td>Specifies the router’s aggregate attribute as zero (rather than the router ID value). This option prevents different routers in an AS from creating aggregate routes with different AS paths.</td>
</tr>
<tr>
<td>holdtime &lt;6-65535</td>
<td>default&gt;</td>
</tr>
<tr>
<td></td>
<td>180 seconds</td>
</tr>
<tr>
<td>keepalive &lt;2-21945</td>
<td>default&gt;</td>
</tr>
<tr>
<td></td>
<td>60 seconds</td>
</tr>
<tr>
<td>ignore-first-ashop</td>
<td>Specifies to ignore the first autonomous system number in the autonomous system path for routes learned from the corresponding peer. Set this option only if you are peering with a route server in transparent mode, that is, when the route server is configured to redistribute routes from multiple other autonomous systems without prepending its own autonomous system number.</td>
</tr>
<tr>
<td>send-keepalives</td>
<td>Specifies for this router always to send keepalive messages even when an update message is sufficient. This option allows interoperability with routers that do not strictly adhere to protocol specifications regarding updates.</td>
</tr>
<tr>
<td>send-route-refresh</td>
<td>Specifies that the router dynamically request BGP route updates from peers or respond to requests for BGP route updates.</td>
</tr>
<tr>
<td><strong>route-refresh</strong> &lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td><strong>accept-routes</strong> &lt;all</td>
<td>none&gt;</td>
</tr>
<tr>
<td><strong>passive-tcp</strong> &lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td><strong>removeprivateas</strong> &lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td><strong>authtype</strong> none</td>
<td>Specifies not to use an authentication scheme between peers. Using an authentication scheme guarantees that routing information is accepted only from trusted peers.</td>
</tr>
<tr>
<td><strong>authtype</strong> md5 secret secret</td>
<td>Specifies to use md5 authentication between peers. In general, peers must agree on the authentication configuration to and from peer adjacencies. Using an authentication scheme guarantees that routing information is accepted only from trusted peers.</td>
</tr>
<tr>
<td><strong>throttle-count</strong> &lt;0-65535</td>
<td>off&gt;</td>
</tr>
</tbody>
</table>
### BGP Peers

**ttl <1-255 | default>**

Specifies the value of the TTL (time to live) parameter, the number of hops over which the external BGP multihop session is established. Configure this value only if the multihop option is enabled.

**suppress-default-origin <on | off>**

Specifies NOT to generate a default route when the peer receives a valid update from its peer.

**log-state-transition <on | off>**

Specifies for the router to log a message whenever a peer enters or leave the established state.

**log-warnings <on | off>**

Specifies for the router to log a message whenever a warning scenario is encountered in the codepath.

**trace bgp traceoption <on | off>**

Specifies tracing options for your BGP implementation. Log messages are saved in the var/log/isprd directory. Enter the following words to set each trace option:

- packets—Trace all BGP packets to this peer.
- open—Trace all BGP open messages to this peer.
- update—Trace all BGP update messages to this peer.
- keepalive—Trace all keepalive messages to this peer.
- all—Trace all message types.
- general—Trace message related to Route and Normal.
- route—Trace routing table changes for routes installed by this peer.
- normal—Trace normal protocol occurrences. Abnormal protocol occurrences are always traced.
- state—Trace state machine transitions in the protocol.
- policy—Trace application of the protocol and user-specified policy to routes being imported and exported.

**capability <default | ipv4-unicast | ipv6-unicast>**

Specifies capabilities setting. Default is IPv4 unicast.
### graceful-restart-helper <on | off>
Specifies whether the Check Point system should maintain the forwarding state advertised by peer routers even when they restart to minimize the negative effects caused by peer routers restarting.

### graceful-restart-helper-stalepath-time seconds
Specifies the maximum amount of time that routes previously received from a restarting router are kept so that they can be revalidated. The timer is started after the peer sends an indication that it has recovered.

---

**BGP Confederations**

Use the following commands to configure BGP confederations. You can configure a BGP confederation in conjunction with external BGP.

```
set bgp
    confederation identifier as_number
    confederation identifier off
    confederation aspath-loops-permitted <1-10>
    confederation aspath-loops-permitted default
    routing-domain identifier as_number
    routing-domain identifier off
    routing-domain aspath-loops-permitted <1-10>
    routing-domain aspath-loops-permitted default
    synchronization <on | off>
```

**Arguments**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>confederation identifier as_number</td>
<td>Specifies the identifier for the entire confederation. This identifier is used as the autonomous system number in external BGP sessions. Outside the confederation, the confederation id is the autonomous system number of a single, large autonomous system. Thus the confederation id must be a globally unique, typically assigned autonomous system number.</td>
</tr>
<tr>
<td>confederation identifier off</td>
<td>Disables the confederation identifier.</td>
</tr>
</tbody>
</table>
Use the following commands to configure BGP route reflection. You can configure route reflection as an alternative to BGP confederations. Route reflection supports both internal and external BGP routing groups.

```
set bgp
  cluster-id ip_address
cluster-id off
```
default-med <0-65535>
default-med off
default-route-gateway ip_address
default-route-gateway off

Arguments

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cluster-id ip_address</td>
<td>Specifies the cluster ID used for route reflection. The cluster ID default is that of the router id. Override the default if the cluster has more than one route reflector</td>
</tr>
<tr>
<td>cluster-id off</td>
<td>Disables the cluster ID.</td>
</tr>
<tr>
<td>default-med &lt;0-65535&gt;</td>
<td>Specifies the multi-exit discriminator (MED) metric used to advertise routes through BGP.</td>
</tr>
<tr>
<td>default-med off</td>
<td>Disables the specified MED metric.</td>
</tr>
<tr>
<td>default-route-gateway ip_address</td>
<td>Specifies the default route. This route has a higher rank than any configured default static route for this router. If you do not want a BGP peer considered for generating the default route, use the peer &lt;ip_address&gt; suppress-default-originate on command.</td>
</tr>
<tr>
<td>default-route-gateway off</td>
<td>Disables the configured default BGP route.</td>
</tr>
</tbody>
</table>

**BGP Route Dampening**

Use the following commands to configure BGP route dampening. BGP route dampening maintains a history of flapping routes and prevents advertising these routes. A route is considered to be flapping when it is repeatedly transitioning from available to unavailable or vice versa.

set bgp dampening
  <on | off>
suppress-above <2-32>
suppress-above default
reuse-below <1-32>
reuse-below default
max-flat <3-64>
max-flat default
reachable-decay <1-900>
reachable-decay default
unreachable-decay <1-2700>
unreachable-decay default
keep-history <2-5400>
keep-history default

### Arguments

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td>suppress-above &lt;2-32&gt;</td>
<td>Specifies the value of the instability metric at which route suppression takes place. A route is not installed in the forwarding table or announced even if it reachable during the period that it is suppressed.</td>
</tr>
<tr>
<td>suppress-above default</td>
<td>Specifies an instability metric value for suppressing routes of 3.</td>
</tr>
<tr>
<td>reuse-below metric &lt;1-32&gt;</td>
<td>Specifies the value of the instability metric at which a suppressed route becomes unsuppressed if it is reachable but currently suppressed. The value assigned to the reuse-below metric must be lower than the suppress-above value.</td>
</tr>
<tr>
<td>reuse-below metric default</td>
<td>Specifies an instability metric value for announcing previously suppressed routes of 2.</td>
</tr>
<tr>
<td>max-flap &lt;3-64&gt;</td>
<td>Specifies the upper limit of the instability metric. The value must be greater than the suppress-above value plus 1. Each time a route becomes unreachable, 1 is added to the current instability metric.</td>
</tr>
<tr>
<td>max-flat default</td>
<td>Specifies the upper limit of the instability metric as 16.</td>
</tr>
<tr>
<td>reachable-decay &lt;1-900&gt;</td>
<td>Specifies the time for the instability metric to reach half of its value when the route is reachable. The smaller the value the sooner a suppressed route becomes reusable.</td>
</tr>
</tbody>
</table>
Internal BGP

Use the following commands to configure internal BGP sessions, that is, between routers within the same autonomous system.

```
set bgp internal
  <on | off>
  description text
  med <0-65535>
  med default
  outdelay <0-65535>
  outdelay off
  nexthop-self <on | off>
  local-address ip_address <on | off>
  virtual-address <on | off>
  interface [all | if_name] <on | off>
  protocol [all | bgp_internal_protocol] <on | off>
  peer ip_address peer_type <on | off>
  peer ip_address weight <0-65535>
  peer ip_address weight off
  peer ip_address no-aggregator id <on | off>
```
peer ip_address holdtime <6-65535>
peer ip_address holdtime default
peer ip_address keepalive <2-21845>
peer ip_address keepalive default
peer ip_address ignore-first-ashop <on | off>
peer ip_address send-keepalives <on | off>
peer ip_address send-route-refresh [request | route-update] [ipv4 | ipv6 | All] [unicast]
peer ip_address accept-routes all
peer ip_address accept-routes none
peer ip_address passive-tcp <on | off>
peer ip_address authtype none
peer ip_address authtype md5 secret secret
peer ip_address throttle-count <0-65535>
peer ip_address throttle-count off
peer ip_address log-state-transitions <on | off>
peer ip_address log-warnings <on | off>
peer ip_address trace bgp_traceoption <on | off>
peer ip_address capability <default | ipv4-unicast | ipv6-unicast> <on | off>
graceful-restart-helper <on | off>
graceful-restart-helper-stalepath-time seconds
route-refresh <on | off>

Arguments

| <on | off> | Specifies whether to enable or disable an internal BGP group. |
| description text | You can enter a brief text description of the group. |
| med <0-65535> | |
### Internal BGP

**med default**

**outdelay <0-65535>**

Specifies the amount of time in seconds that a route must be present in the routing database before it is redistributed to BGP. The configured value applies to all peers configured in this group. This feature dampens route fluctuation. Zero (0), which means that this feature is disabled.

0

**outdelay off**

Disables outdelay.

**nexthop-self<on | off>**

Specifies for this router to send one of its own IP addresses as the BGP next hop.

off

**local-address ip_address <on | off>**

Specifies the IP address used on the local end of the TCP connection with the peer. A peer session is maintained when any interface with the specified local address is operating.

**virtual-address<on | off>**

Specifies for this router to use the VRRP virtual IP address as the local endpoint for TCP connections. You must also configure a local address to enable this option. See the command above. You can configure this option only on a VRRP master.

**Default**: off.

**interface [all | if_name]<on | off>**

Specifies whether to enable the specified internal peer group on all interfaces or a specific interface.

**protocol [all bgp_internal_protocol]<on | off>**

Specifies whether to enable all internal routing protocols on the specified internal peer group or specific internal protocols. You can enter the following specific internal protocols: direct, rip, static, ospf, and ospfase.
### peer ip_address peer_type <on | off>
Specifies an internal peer address and peer type. Enter `reflector-client` to specify that the local router acts as a route reflector for the group of peers named. That is, the local router is the route reflection server, and the named peers are route reflection clients. Normally, the routing daemon readvertises, or reflect, routes it receives from one of its clients to all other IBGP peers, including the other peers in that client's group. Enter `no-client-reflector` to specify that a reflection client's routes are reflected only to internal BGP peers in other groups. Clients in the group are assumed to be direct IBGP peers of each other. Enter `none` if you do not want to specify route reflection.

### peer_ip_address weight <0-65535>
Specifies the weight associated with the specified peer. BGP implicitly stores any rejected routes by not mentioning them in a route filter. BGP explicitly mentions them within the routing table by using a restrict keyword with a negative weight. A negative weight prevents a route from becoming active, which prevents it from being installed in the forwarding table or exported to other protocols. This eliminates the need to break and reestablish a session upon reconfiguration if import route policy is changed.

### peer ip_address weight off
Disables the weight associated with the specified peer.

### peer ip_address aggregator id <on | off>
Specifies the router's aggregate attribute as zero (rather than the router ID value). This option prevents different routers in an AS from creating aggregate routes with different AS paths.

### peer ip_address holdtime <6-65535>
Specifies the BGP holdtime interval, in seconds, when negotiating a connection with the specified peer. If the BGP speaker does not receive a keepalive update or notification message from its peer within the period specified in the holdtime field of the BGP open message, the BGP connection is closed.

### peer ip_address holdtime default
Specifies a holdtime of 180 seconds.
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>peer ip_address keepalive &lt;2-21845&gt;</td>
<td>The keepalive option is an alternative way to specify a holdtime value in seconds when negotiating a connection with the specified peer. You can use the keepalive interval instead of the holdtime interval. You can also use both interval, but the holdtime value must be 3 times the keepalive interval value.</td>
</tr>
<tr>
<td>peer ip_address keepalive default</td>
<td>Specifies a keepalive interval of 60 seconds.</td>
</tr>
<tr>
<td>peer ip_address ignore-first-ashop &lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td>peer ip_address send-keepalives &lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td>send-route-refresh [request</td>
<td>route-update] [ipv4</td>
</tr>
<tr>
<td>peer ip_address accept-routes all</td>
<td>Specifies an inbound BGP policy route if one is not already configured. Enter all to specify accepting routes and installing them with an invalid preference. Depending on the local inbound route policy, these routes are then made active or inactive.</td>
</tr>
<tr>
<td>peer ip_address accept-routes none</td>
<td>Specifies an inbound BGP policy route if one is not already configured. Enter none to specify deleting routes learned from a peer. This option saves memory overhead when many routes are rejected because no inbound policy exists.</td>
</tr>
</tbody>
</table>
### peer ip_address passive-tcp <on | off>

Specifies for the router to wait for the specified peer to issue an open message. No tcp connections are initiated by the router.

**off**

### peer ip_address authtype none

Specifies not to use an authentication scheme between peers. Using an authentication scheme guarantees that routing information is accepted only from trusted peers.

### peer ip_address authtype md5 secret secret

Specifies to use md5 authentication between peers. In general, peers must agree on the authentication configuration to and from peer adjacencies. Using an authentication scheme guarantees that routing information is accepted only from trusted peers.

### peer ip_address throttle-count <0-65535>

Specifies the number of BGP updates to send at one time. The throttle count option limits the number of BGP updates when there are many BGP peers.

### peer ip_address throttle-count off

Disables the throttle count option.

### peer ip_address log-state-transitions <on | off>

Specifies for the router to log a message whenever a peer enters or leave the established state.

### peer ip_address log-warnings <on | off>

Specifies for the router to log a message whenever a warning scenario is encountered in the codepath.
### Internal BGP

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>peer ip_address trace bgp_traceoption &lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td>capability &lt;default</td>
<td>ipv4-unicast</td>
</tr>
<tr>
<td>graceful-restart-helper &lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td>graceful-restart-helper-stalepath-time seconds</td>
<td>Specifies the maximum amount of time that routes previously received from a restarting router are kept so that they can be revalidated. The timer is started after the peer sends an indication that it has recovered.</td>
</tr>
<tr>
<td>route-refresh &lt;on</td>
<td>off&gt;</td>
</tr>
</tbody>
</table>
BGP Communities

Use the following command to configure BGP communities. A BGP community is a group of destinations that share the same property. However, a community is not restricted to one network or autonomous system. Use communities to simplify the BGP inbound and route redistribution policies. Use the BGP communities commands in conjunction with inbound policy and route redistribution.

```
set bgp communities
  <on | off>
```

**Arguments**

| <on | off> | Specifies whether to enable or disable BGP policy options based on communities. |

**BGP Show Commands**

Use the following commands to monitor and troubleshoot your BGP implementation.

```
show bgp
show bgp
groups
memory
errors
paths
stats
peers
peers detailed
peer ip_address detailed
peers established
peer ip_address advertise
peer ip_address received
summary
```
OSPF

Use the following group of commands to set and view parameters for OSPF. OSPFv2 is used with IPv4 and OSPFv3 is used with IPv6. The commands for OSPFv3 are similar to those for OSPFv2, except that in place of `ospf` you enter `ipv6 ospf3`. This syntax is shown below for each set of commands and any differences in arguments used for OSPFv2 and OSPFv3 are noted in the argument tables.

You also have the option of configuring multiple routing instances with OSPF. For more information on enabling multiple routing instances and adding individual instances, see “Multiple Routing Instances” on page 304.

When you do initial configuration, set the router ID. You can also use the following commands to change the router ID.

```markdown
set [instance instance_name] router-id
  default
  ip_address
```

<table>
<thead>
<tr>
<th>Arguments</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>router-id default</td>
<td>Selects the highest interface address when OSPF is enabled.</td>
</tr>
<tr>
<td>router-id ip_address</td>
<td>Specifies a specific IP address to assign as the router ID. Do not use 0.0.0.0 as the router ID address. Check Point recommends setting the router ID rather than relying on the default setting. Setting the router ID prevents the ID from changing if the default interface used for the router ID goes down.</td>
</tr>
</tbody>
</table>

**OSPF Areas**

Use the following commands to configure OSPF areas, including the backbone and stub areas.
For OSPFv2 use the following commands.

```
set [instance instance_name] ospf area
  backbone <on | off>
set ospf area ospf_area
  <on| off>
stub <on | off>
stub default-cost <1-677215>
stub summary <on | off>
nssa <on | off>
nssa default-cost <1-677215>
nssa default-metric-type <1-2>
nssa import-summary-routes <on | off>
nssa translator-role <always | candidate>
nssa translator-stability-interval <1-65535>
nssa redistribution <on | off>
nssa range ip_addr [restrict] <on | off>
```

For OSPFv3 use the following commands. NSSA is not available for OSPFv3.

```
set ipv6 ospf3 area
  backbone <on | off>
set ipv6 ospf3 area ospf_area
  <on| off>
stub <on | off>
stub default-cost <1-677215>
stub summary <on | off>
```

**Arguments**

| backbone <on | off> | Specifies whether to enable or disable the backbone area. By default, the backbone area is enabled. You can disable the backbone area if the system does not have interfaces on the backbone area. |
### OSPF Areas

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td>stub &lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The backbone area cannot be a stub area.</td>
</tr>
<tr>
<td>stub default-cost &lt;1-677215&gt;</td>
<td>Specifies a default route into the stub area with the specified cost.</td>
</tr>
<tr>
<td>stub summary &lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td>nssa &lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The backbone area cannot be an NSSA area.</td>
</tr>
<tr>
<td>nssa default-cost &lt;1-677215&gt;</td>
<td>Specifies the cost associated with the default route to the NSSA.</td>
</tr>
<tr>
<td>nssa default-metric-type &lt;1-2&gt;</td>
<td>Specifies the type of metric. The default, type 1, is equivalent to the Default ASE Route Type on the OSPF Voyager page. A type 1 route is internal and its metric can be used directly by OSPF for comparison. A type 2 route is external and its metric cannot be used for comparison directly.</td>
</tr>
<tr>
<td>nssa import-summary-routes &lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td>nssa translator-role &lt;always</td>
<td>candidate&gt;</td>
</tr>
<tr>
<td>nssa translator-stability-inter val &lt;1-65535&gt;</td>
<td>Specifies how long in seconds this elected Type-7 translator will continue to perform its translator duties once it has determined that its translator status has been assumed by another NSSA border router. Default: 40 seconds.</td>
</tr>
</tbody>
</table>
Use the following commands to configure a backbone and other areas, such as stub areas, for specified interfaces.

For OSPFv2 use the following commands:

```
set [instance instance_name] ospf
  area <backbone | ospf_area> range ip_prefix <on | off>
  area <backbone | ospf_area> range ip_prefix restrict <on | off>
  stub-network ip_prefix <on | off>
  stub-network ip_prefix stub-network-cost <1-677722>
  interface if_name area <backbone | ospf_area> <on | off>
  interface if_name hello-interval <1-65535>
  interface if_name hello-interval default
  interface if_name dead-interval <1-65535>
  interface if_name dead-interval default
  interface if_name retransmit-interval <1-65535>
  interface if_name retransmit-interval default
  interface if_name cost <1-65535>
  interface if_name priority <0-255>
  interface if_name passive <on | off>
  interface if_name virtual-address <on | off>
  interface if_name authtype none
  interface if_name simple password
```

### OSPF Interfaces

Specifies if both Type-5 and Type-7 LSAs or only Type-7 LSAs will be originated by this NSSA border router.

Specify the range of addresses to reduce the number of Type-5 LSAs for the NSSA border router. To prevent a specific prefix from being advertised, use the restrict argument.
interface if_name md5 key authorization key id secret md5 secret
interface if_name md5 key authorization key id

For OSPFv3 use the same arguments as for OSPFv2 but precede them with the following:
set ipv6 ospf3

Arguments

| area <backbone | ospf_area> range | ip_prefix <on | off> |
|----------------|------------------|------------------|
| Specifies the OSPF area to which the specified interface range belongs. Select an area from the areas already configured. Any area can be configured with any number of address ranges. These ranges are used to reduce the number of routing entries that a given area transmits to other areas. If a given prefix aggregates a number of more specific prefixes within an area, you can configure an address range that becomes the only prefix advertised to other areas. Be careful when configuring an address range that covers part of a prefix that is not contained within an area. An address range is defined by an IP prefix and a mask length. If you mark a range as restrict, it is not advertised to other areas. |

| area <backbone | ospf_area> range | ip_prefix restrict <on | off> |
|----------------|------------------|-------------------|
| Any area can be configured with any number of address ranges. These ranges are used to reduce the number of routing entries that a given area transmits to other areas. If a given prefix aggregates a number of more specific prefixes within an area, you can configure an address range that becomes the only prefix advertised to other areas. Be careful when configuring an address range that covers part of a prefix that is not contained within an area. An address range is defined by an IP prefix and a mask length. If you mark a range as restrict, it is not advertised to other areas. |
stub-network ip_prefix <on | off>
Specifies a stub network to which the specified interface range belongs. Configure a stub network to advertise reachability to prefixes that are not running OSPF. The advertised prefix appears as an OSPF internal route and is filtered at area borders with the OSPF area ranges. The prefix must be directly reachable on the router where the stub network is configured, that is, one of the router’s interface addresses must fall within the prefix range to be included in the router-link-state advertisement. Use a mask length of 32 to configure the stub host. The local address of a point-to-point interface can activate the advertised prefix and mask. To advertise reachability to such an address, enter an IP address for the prefix and a non-zero cost for the prefix.

stub-network ip_prefix
stub-network-cost <1-677722>
Configure a stub network to advertise reachability to prefixes that are not running OSPF. The advertised prefix appears as an OSPF internal route and is filtered at area borders with the OSPF area ranges. The prefix must be directly reachable on the router where the stub network is configured, that is, one of the router’s interface addresses must fall within the prefix range to be included in the router-link-state advertisement. Use a mask length of 32 to configure the stub host. The local address of a point-to-point interface can activate the advertised prefix and mask. To advertise reachability to such an address, enter an IP address for the prefix and a non-zero cost for the prefix.

interface if_name area <backbone | ospf area> <on | off>
Specifies the OSPF area to which the specified interface belongs.

interface if_name hello-interval <1-65535>
Specifies the interval, in seconds, between hello packets that the router sends on the specified interface. For a given link, this value must be the same on all routers or adjacencies do not form.

interface if_name hello-interval default
Specifies the default value for the hello interval, which is 10 seconds.
<table>
<thead>
<tr>
<th>OSPF Interfaces</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>interface if_name</strong></td>
</tr>
<tr>
<td><strong>dead-interval</strong></td>
</tr>
<tr>
<td><strong>default</strong></td>
</tr>
<tr>
<td><strong>interface if_name</strong></td>
</tr>
<tr>
<td><strong>retransmit-interval</strong></td>
</tr>
<tr>
<td><strong>default</strong></td>
</tr>
<tr>
<td><strong>interface if_name</strong></td>
</tr>
<tr>
<td><strong>cost</strong></td>
</tr>
<tr>
<td><strong>interface if_name</strong></td>
</tr>
<tr>
<td><strong>priority</strong></td>
</tr>
<tr>
<td>Command</td>
</tr>
<tr>
<td>--------------------------</td>
</tr>
<tr>
<td>`interface if_name</td>
</tr>
<tr>
<td>passive &lt;on</td>
</tr>
<tr>
<td>`interface if_name</td>
</tr>
<tr>
<td>virtual-address &lt;on</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>`interface if_name</td>
</tr>
<tr>
<td>authtype none</td>
</tr>
<tr>
<td>`interface if_name</td>
</tr>
<tr>
<td>authtype simple password</td>
</tr>
<tr>
<td>`interface if_name</td>
</tr>
<tr>
<td>authtype md5 key</td>
</tr>
</tbody>
</table>

---

Chapter 9   Routing Commands   331
**OSPF Virtual Links**

Use the following commands to configure OSPF virtual links. Configure a virtual link if the router is a border router that does not have interfaces in the backbone area. The virtual link is effectively a tunnel across an adjacent non-backbone area whose endpoint must be any of the adjacent area’s border routers that has an interface in the backbone area.

For OSPFv2 use the following commands:
```
set [instance instance_name] ospf area backbone virtual-link
    ip_address transit-area ospf_area <on | off>
    ip_address transit-area ospf_area hello-interval <1-65535>
    ip_address transit-area ospf_area hello-interval default
    ip_address transit-area ospf_area dead interval <1-4294967295>
    ip_address transit-area ospf_area dead interval default
    ip_address transit-area ospf_area retransmit-interval <1-4294967295>
    ip_address transit-area ospf_area retransmit-interval default
    ip_address transit-area ospf_area authtype none
    ip_address transit-area ospf_area authtype simple password
    ip_address transit-area ospf_area authtype md5 key authorization key id secret md5 key
    ip_address transit-area ospf_area authtype md5 key authorization key id off
```

For OSPFv3 use the following with the same arguments as for OSPFv2:
```
set ipv6 ospf3 area backbone virtual-link
```
### Arguments

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip_address transit-area ospf_area &lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td>ip_address transit-area ospf_area hello-interval &lt;1-65535&gt;</td>
<td>Specifies the interval, in seconds, between hello packets that the router sends on the specified interface. For a given link, this value must be the same on all routers or adjacencies do not form.</td>
</tr>
<tr>
<td>ip_address transit-area ospf_area hello-interval default</td>
<td>Specifies an interval of 10 seconds.</td>
</tr>
<tr>
<td>ip_address transit-area ospf_area dead-interval &lt;1-4294967295&gt;</td>
<td>Specifies the number of seconds after which a router stops receiving hello packets that it declares the neighbor down. Generally, you should set this value at 4 times the value of the hello interval. Do not set the value at 0. For a given link, this value must be the same on all routers or adjacencies do not form.</td>
</tr>
<tr>
<td>ip_address transit-area ospf_area dead-interval default</td>
<td>Specifies a value of 40 seconds.</td>
</tr>
<tr>
<td>ip_address transit-area ospf_area retransmit-interval &lt;1-4294967295&gt;</td>
<td>Specifies the number of seconds between link state advertisement transmissions for adjacencies belonging to the specified interface. This value also applies to database description and link state request packets. Set this value conservatively, that is, at a significantly higher value than the expected round-trip delay between any two routers on the attached network.</td>
</tr>
<tr>
<td>ip_address transit-area ospf_area retransmit-interval default</td>
<td>Specifies a value of 5 seconds.</td>
</tr>
</tbody>
</table>
OSPF Global Settings

Use the following commands to configure settings that apply to all configured OSPF areas, including the backbone and stub areas.

For OSPFv2 use the following commands:

```bash
set [instance instance_name] ospf
rfcl583-compatibility <on | off>
spf-delay <1-60>
spf-delay default
spf-holdtime <1-60>
spf-holdtime default
default-ase-cost <1-677215>
default-ase-type <1 | 2>
graceful-restart-helper <on | off>
```

For OSPFv3 use the following commands:

```bash
ip_address transit-area
ospf_area authtype none
```

Specifies not to use an authentication scheme for the specified interface.

```bash
ip_address transit-area
ospf_area authtype simple password
```

Specifies to use simple authentication for the specified interface. Enter an ASCII string that is 8 characters long. Generally, routers on a given link must agree on the authentication configuration to form neighbor adjacencies. Use an authentication scheme to guarantee that routing information is accepted only from trusted peers.

```bash
ip_address transit-area
ospf_area authtype md5
key_authorization key id
secret MD5 secret
```

Specifies to use MD5 authorization. Enter at least one key ID and its corresponding MD5 secret. If you configure multiple key IDs, the largest key ID is used for authenticating outgoing packets. All keys can be used to authenticate incoming packets. Generally, routers on a given link must agree on the authentication configuration to form neighbor adjacencies. Use an authentication scheme to guarantee that routing information is accepted only from trusted peers.
set ipv6 ospf3
    spf-delay <1-60>
interface ifname virtual-address
    spf-delay default
spf-holdtime <1-60>
    spf-holdtime default
default-ase-cost <1-677215>
default-ase-type <1 | 2>

Arguments

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rfc1583-compatibility &lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td>on</td>
<td>Specifies the time, in seconds, to wait before recalculating the OSPF routing table after a change in the topology.</td>
</tr>
<tr>
<td>spf-delay &lt;1-60&gt;</td>
<td>Specifies an spf-delay time of 2 seconds.</td>
</tr>
<tr>
<td>spf-holdtime &lt;1-60&gt;</td>
<td>Specifies the minimum time, in seconds, between recalculations of the OSPF routing table.</td>
</tr>
<tr>
<td>spf-holdtime default</td>
<td>Specifies an spf-holdtime of 5 seconds.</td>
</tr>
<tr>
<td>default-ase-cost &lt;1-677215&gt;</td>
<td>Specifies the cost assigned to routes from other protocols that are redistributed into OSPF as autonomous systems external. If the route has a cost already specified, that cost takes precedent.</td>
</tr>
<tr>
<td>default-ase-type &lt;1</td>
<td>2&gt;</td>
</tr>
</tbody>
</table>
**OSPF Show Commands**

Use the following commands to monitor and troubleshoot your OSPF implementation.

To view a summary of your OSPF implementation, including the number of areas configured and the number of interfaces configured within each area, use `show [instance instance_name] ospf` (for OSPFv2) or `show ipv6 ospf3` (for OSPFv3).

For OSPFv2 use the following commands:

- `show [instance instance_name] neighbors`
- `show [instance instance_name] neighbors ip_address`
- `show [instance instance_name] interfaces`
- `show [instance instance_name] interfaces stats`
- `show [instance instance_name] interfaces detailed`
- `show [instance instance_name] interface ifname`
- `show [instance instance_name] interface ifname stats`
- `show [instance instance_name] interface ifname detailed`
- `show [instance instance_name] packets`
- `show [instance instance_name] errors`
- `show [instance instance_name] errors dd`
- `show [instance instance_name] errors hello`
- `show [instance instance_name] errors ip`

---

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default-ase-type &lt;1</td>
<td>2&gt;</td>
</tr>
<tr>
<td>graceful-restart-helper &lt;on</td>
<td>off&gt;</td>
</tr>
</tbody>
</table>
errors lsack
errors lsr
errors lsu
errors protocol
events
border-routers
database
database areas
database area ospf_area
database asbr-summary-1sa
database checksum
database database-summary
database detailed
database external-1sa
database network-1sa
database router-1sa
database summary-1sa
database type <1 | 2 | 3 | 4 |5 | 7> [detailed]
database nssa-external-1sa [detailed]
summary

For OSPFv3 use the following commands:
show ipv6 ospf3
   neighbors
   neighbor ip_address
   interface ifname <on | off>
   interfaces
   interfaces stats
   interfaces detailed
   interface ifname
OSPF Show Commands

interface ifname stats
interface ifname detailed
packets
errors
dd
errors
errors hello
errors ip
errors lsack
errors lsr
errors lsu
errors protocol
events
border-routers
database
database areas
database area ospf area
database checksum
database database-summary
database detailed
database external-lsa
database inter-area-prefix
database inter-area-router-lsa
database intra-area-prefix-lsa
database link-lsa
database network-lsa
database router-lsa
database type <1-5>
database events
summary
## Arguments

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>neighbors</td>
<td>Displays the IP addresses of neighboring interfaces, their priority and status, and the number of errors logged for each interface.</td>
</tr>
<tr>
<td>neighbor ip_address</td>
<td>Displays the priority, status, and number of errors logged for the specified IP address.</td>
</tr>
<tr>
<td>interface ifname &lt;on</td>
<td>Displays the use of the VRRP virtual link-local address as the source of its control packets</td>
</tr>
<tr>
<td>&lt;on</td>
<td>Displays the use of the VRRP virtual link-local address as the source of its control packets</td>
</tr>
<tr>
<td>interface ifname &lt;on</td>
<td>Displays the use of the VRRP virtual link-local address as the source of its control packets</td>
</tr>
<tr>
<td>interfaces</td>
<td>Displays the names of all configured logical interfaces, their corresponding IP addresses, to area to which each interface is assigned, each interface's status and the IP addresses of each logical interface's designated router and backup designated router.</td>
</tr>
<tr>
<td>interfaces stats</td>
<td>Displays the number of each type of error message logged for each OSPF interface as well as the number of link state advertisements sent by each interface.</td>
</tr>
<tr>
<td>interfaces detailed</td>
<td>Displays detailed information about each OSPF interface, including the authentication type configured if any, the router IDs and IP addresses of the designated router and backup designated router, the timer intervals configured for hello wait, dead, and retransmit messages, and the number of neighbors for each interface.</td>
</tr>
<tr>
<td>interface if_name</td>
<td>Displays the IP address, area ID, status, number of errors logged, and the IP address of the designated router and backup designated router for the specified interface.</td>
</tr>
<tr>
<td>interface if_name &lt;on stats</td>
<td>Displays the number of each type of error message logged by the specified interface as well as the number of link-state advertisements sent by the specified interface.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>----------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>interface if_name detailed</strong></td>
<td>Displays detailed information about the specified interface, including the authentication type configured if any, the router IDs and IP addresses of the designated router and backup designated router, the timer intervals configured for hello wait, dead, and retransmit messages, and the number of neighbors for each interface.</td>
</tr>
<tr>
<td>packets</td>
<td>Displays the number of each type of packet sent, including hello packets, link-state update packets, and link-state acknowledgment and link-state request packets.</td>
</tr>
<tr>
<td>errors</td>
<td>Displays the number of each type of error message sent, including hello protocol errors, database description errors, protocol errors, link-state acknowledgment errors, link-state request errors, link-state update errors, and IP errors.</td>
</tr>
<tr>
<td>errors dd</td>
<td>Displays the number of each type of database description error messages only.</td>
</tr>
<tr>
<td>errors hello</td>
<td>Displays the number of each type of hello error message only.</td>
</tr>
<tr>
<td>errors ip</td>
<td>Displays the number of each type of IP errors message only.</td>
</tr>
<tr>
<td>errors lsack</td>
<td>Displays the number of each type of link-state acknowledgment error message only.</td>
</tr>
<tr>
<td>errors lsu</td>
<td>Displays the number of each type of link-state update error message only.</td>
</tr>
<tr>
<td>errors lsr</td>
<td>Displays the number of each type of link-state request error messages only.</td>
</tr>
<tr>
<td>errors protocol</td>
<td>Displays the number of each type of protocol error message only.</td>
</tr>
<tr>
<td>border-routers</td>
<td>Displays the IP address of each area border router, the OSPF area of each border router, and the cost associated with each IP address.</td>
</tr>
<tr>
<td>database</td>
<td>Displays router-link state and network-link state statistics for each OSPF area. Also displays the checksum, sequence number, and link count of each OSPF interface.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td><code>database areas</code></td>
<td>Displays router-link state, network-link state, AS-border-router link state, AS-external link state, and summary-link state statistics for each OSPF area. Also displays the checksum, sequence number, and link count of each OSPF interface.</td>
</tr>
<tr>
<td><code>database area ospf_area</code></td>
<td>Displays router-link state, network-link state, AS-border-router-link state, AS-external-link state, and summary-link state statistics for the specified OSPF area. Also displays the checksum, sequence number, and link count of each IP address configured within the specified OSPF area.</td>
</tr>
<tr>
<td><code>database asbr-summary</code></td>
<td>Displays a summary of AS-border-router link state statistics for each OSPF area. For OSPFv2 only.</td>
</tr>
<tr>
<td><code>database inter-area-router-lsa</code></td>
<td>Displays a summary of AS-border-router link state statistics for each OSPF area. For OSPFv3 only.</td>
</tr>
<tr>
<td><code>database external</code></td>
<td>Displays AS-external-link state statistics for each OSPF area.</td>
</tr>
<tr>
<td><code>database database-summary</code></td>
<td>Displays a summary of router-link-state, network-link state, summary-link-state, and AS-border-router-link state statistics.</td>
</tr>
<tr>
<td><code>database network</code></td>
<td>Displays network-link-state statistics, including the advertised router, sequence number, and checksum of each OSPF interface. For OSPFv2 only.</td>
</tr>
<tr>
<td><code>database nssa-external-lsa [detailed]</code></td>
<td>Displays type 7 LSAs (NSSA). This argument applies only to OSPF v2; OSPFv3 is not NSSA aware.</td>
</tr>
<tr>
<td><code>database router-lsa</code></td>
<td>Displays router-link-state statistics, including the advertised router, sequence number, checksum, and link count, of each OSPF interface. For OSPFv2 only.</td>
</tr>
<tr>
<td><code>database summary-lsa</code></td>
<td>Displays a summary of link-state statistics for each OSPF area. For OSPFv2 only.</td>
</tr>
<tr>
<td><code>database inter-area-prefix-lsa</code></td>
<td>Displays a Type 3 summary of link-state statistics for each OSPF area. For OSPFv3 only.</td>
</tr>
</tbody>
</table>
In OSPFv3 all addressing information is removed from router Lsa and network Lsa and intra-area-prefix-Lsa carries this addressing information. It associates a list of IPv6 address prefixes with a transit network link by referencing a network Lsa or a router Lsa. A stub link's prefixes are carried by an intra-area-prefix Lsa that references a router-Lsa. For OSPFv3 only.

Describes a router's link-local address and the IPv6 address prefixes associated with a link. For OSPFv3 only.

 Displays link-state statistics associated with the specified number:

- 1—router-link-state statistics.
- 2—network-link-state statistics.
- 3—summary-link-state statistics.
- 4—AS-border-router-link-state statistics.
- 5—AS-external-link-state statistics.
- 7—NSSA. This option applies only to OSPF v2; OSPFv3 is not NSSA aware.

Displays the number of interface up/down events; virtual interface up/down events; designated router election events; router ID changes; area border router changes; AS border router changes, and link state advertisement messages.
RIP

Use this group of commands to set and view parameters for RIP.

**Note** - IPSO does not have CLI commands for route filtering and redistribution. You must configure inbound routing policies and redistribution of routes through Voyager. You can configure route maps and route aggregation using CLI commands. Route map configuration done through the CLI takes precedence over route filtering and redistribution configured in Voyager. For example if RIP uses route maps for inbound filtering, anything configured on the Voyager page for inbound route filters for RIP is ignored. You can still use Voyager to configure route redistribution into RIP.

Use these commands to configure RIP properties for specific interfaces.

**RIP Interfaces**

```
set rip interface if_name
    off
    version <1 | 2> on
    metric <0-16>
    metric default
    accept-updates <on | off>
    send-updates <on | off>
    transport multicast
    transport broadcast
    authtype none
    authtype simple password
    authtype md5 secret secret [cisco-compatibility] <on | off>
    virtual address <on | off>
```

**General RIP Properties**

Use these commands to configure RIP properties that apply to all interfaces configured for RIP.

```
set rip
```
auto-summary <on | off>
update-interval <1-65535>
update-interval default
expire-interval <1-65535>
expire-interval default

Arguments

<1 | 2> Specifies the version of RIP to run.

metric <0–16> Specifies the rip metric added to routes set that use the specified interface.

metric default Specifies a value of 0.

accept-updates <on | off> Specifies whether to accept RIP packets using the specified interface.
	off

send-updates <on | off> Specifies whether RIP packets should be sent using the specified interface.

transport multicast Specifies for RIP version 2 packets to be multicast on the specified interface.

transport broadcast Specifies for RIP version 1 packets that are compatible with rip version 2 to be broadcast on the specified interface.

authtype none Specifies not to implement an authentication scheme for the specified interface to accept routing information from neighboring routers. This option applies to rip version 2 only.

authtype simple password Specifies to implement a simple authentication scheme for the specified interface to accept routing information from neighboring routers. The password must contain alphanumeric characters only and can be between one and 16 characters long. This option applies to RIP version 2 only.

authtype md5 secret secret Specifies to implement an authentication scheme that uses an MD5 algorithm for the specified interface to accept routing information from neighboring routers. This option applies to RIP version 2 only.
### RIP Show Commands

Use these commands to monitor and troubleshoot RIP.

**show rip**

- **interfaces**
  Interface <if_name>

---

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>`interface if_name</td>
<td>Enables RIP on the virtual IP address associated with this interface. This</td>
</tr>
<tr>
<td>virtual &lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td></td>
<td>configure VRRP to accept connections to VRRP IPs. See “ICMP Router</td>
</tr>
<tr>
<td></td>
<td>Discovery” for more information.</td>
</tr>
<tr>
<td></td>
<td><strong>Default</strong>: off</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: You must use Monitored Circuit mode when configuring virtual IP</td>
</tr>
<tr>
<td></td>
<td>support for any dynamic routing protocol, including RIP. Do not use VRRPv2</td>
</tr>
<tr>
<td></td>
<td>when configuring virtual IP support for RIP or any dynamic routing protocol.</td>
</tr>
<tr>
<td>`cisco-compatibility</td>
<td>Specifies whether to interoperate with Cisco routers also using the MD5</td>
</tr>
<tr>
<td>&lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td></td>
<td><strong>Default</strong>: off</td>
</tr>
<tr>
<td>`auto-summary</td>
<td>Specifies whether to aggregate and distribute non-classful routes when</td>
</tr>
<tr>
<td>&lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td></td>
<td><strong>Default</strong>: on</td>
</tr>
<tr>
<td>`update-interval</td>
<td>Specifies the amount of time, in seconds, between RIP updates.</td>
</tr>
<tr>
<td>&lt;1-65535&gt;</td>
<td><strong>Default</strong>: Specifies a value of 30 seconds.</td>
</tr>
<tr>
<td>`expire-interval</td>
<td>Specifies the amount of time, in seconds, that must pass without receiving</td>
</tr>
<tr>
<td>&lt;1-65535&gt;</td>
<td>an update for a given route before the route is considered to have timed out.</td>
</tr>
<tr>
<td></td>
<td>This value should be 6 times the update interval in order to allow for the</td>
</tr>
<tr>
<td></td>
<td>possibility that packets containing an update could be dropped by the network.</td>
</tr>
<tr>
<td></td>
<td><strong>Default</strong>: Specifies a value of 180 seconds.</td>
</tr>
</tbody>
</table>
RIP Show Commands

packets
errors
neighbors
summary
IGRP

Use these commands to set and view parameters for the Interior Gateway Routing Protocol.

**Note** - IPSO does not have CLI commands for route filtering and redistribution. You must configure inbound routing policies and redistribution of routes through Voyager. You can configure route maps and route aggregation using CLI commands. Route map configuration done through the CLI takes precedence over route filtering and redistribution configured in Voyager. For example if RIP uses route maps for inbound filtering, anything configured on the Voyager page for inbound route filters for RIP is ignored. You can still use Voyager to configure route redistribution into RIP.

**General IGRP Properties**

```plaintext
set igrp
    as <0-65535>
    as off
    default-delay <0-16777215>
    default-delay off
    default-bandwidth <1-677215>
    default-bandwidth off
    default-reliability <0-255>
    default-reliability off
    default-load <1-255>
    default-load off
    default-mtu <1-65535>
    default-mtu off
    k1 <0-16777215>
    k1 default
    k2 <0-16777215>
    k2 default
    holddown <on | off>
    max-hop-count <1-255>
    max-hop-count default
```
IGRP Interfaces

Use these commands to configure IGRP properties for specific interfaces.

```
set igrp interface if_name
    <on | off>
    delay <1-16777215>
    bandwidth <1-6777215>
    accept-updates <on | off>
```

**Arguments**

- `as <0-65535>`: Specifies the autonomous system number of IGRP packets. You do not have to use an officially registered as number, but if your organization has one, you should use that number. Update messages also include the as number.
- `as off`: Specifies to disable the autonomous system number. Because you must enable an autonomous system number to run IGRP, disabling the as and not configuring a new as means that you cannot run IGRP.
- `default-delay <0-16777215>`: Specifies IGRP delay metrics in units of 10 microseconds. Set this option if you are exporting routes into IGRP.
default-bandwidth <1-16777215> Specifies the IGRP bandwidth metric in units of inverted bits/second scaled by a factor of 10,000,000,000. Set this option if you are exporting routes into IGRP.

default-reliability <0-255> Specifies the IGRP reliability metric as a fraction of 255, that is, 255=100%. Set this option if you are exporting routes into IGRP.

default-load <1-255> Specifies the IGRP load metric as a fraction of 255, that is, 255=100%. Set this option if you are exporting routes into IGRP.

default-mtu <0-65535> Specifies the IGRP maximum transmission unit. Set this option if you are exporting routes into IGRP.

k1 <0-1677215> Specifies the IGRP bandwidth multiplier constant used in the composite metric computation.

k1 default Specifies a value of 1.

k2 <0-1677215> Specifies the IGRP delay multiplier constant used in the composite metric computation.

k2 default Specifies a value of 1.

holddown <on | off> Specifies whether IGRP performs "holddown loop" prevention measures. This setting should be consistent throughout an autonomous system. Enabling holddowns has the effect of disabling the stronger form of route poisoning.

on

max-hop-count <1-255> Specifies the maximum allowable "hop count" an incoming route must have in order to be accepted. For a route to be marked as "reachable" in an update, its "hop count" must not exceed this value.

max-hop-count default Specifies a value of 100.

update-interval <1-65535> Specifies the amount of time, in seconds, between regularly scheduled updates.

update-interval default Specifies a value of 90.

invalid-interval <1-65535> Specifies the amount of time, in seconds, that must pass without receiving an update for a given route before the route is considered to have timed out.
invalid-interval
default

Specifies a value of 3 times the update interval value.

hold-interval
<1-65535>

Specifies the amount of time, in seconds, that a route remains in a "hold down" state. The interval should be several times the value of the update interval. The hold interval must be at least as long as the flush interval minus the value of the invalid interval. When a route has become unreachable (or the metric has increased enough to cause poisoning), the route goes into a "hold down" state (when the Holddown field is enabled). During this state, no new route is accepted for the same destination for this amount of time.

hold-interval default

Specifies a value that is 3 times the configured update interval value plus 10.

flush-interval
<1-65535>

Specifies the amount of time, in seconds, before a routing table entry is removed. The interval should be longer than the sum of the invalid interval and the hold interval values. After the Invalid interval expires, a route is timed out and marked "unreachable". The routing table entry for the destination remains, in order to enforce the holddown.

flush-interval default

Specifies a value 7 times the configured update interval value.

validate-fields
<on | off>

Specifies that IGRP should not check that reserved fields are zero in incoming IGRP request packets. Normally, IGRP rejects request packets when the reserved fields are not zero. The reserved fields in a request packet are the "edition" number and the three "route counts". When you enable this option, any possible trailing data after the IGRP header is ignored. Normally, IGRP rejects request packets that are not exactly the size of the IGRP header.

interface if_name
<on | off>

Specifies whether to enable or disable IGRP on the specified interface.

interface if_name delay
<1-1677215>

Specifies the IGRP delay metric in units of 10 microseconds.

interface if_name bandwidth
<1-1677215>

Specifies the IGRP bandwidth metric in units of inverted bits/second scaled by a factor of 10,000,000.
IGRP Show Commands

Use these commands to monitor and troubleshoot IGRP.

```
show igrp
  errors
  interfaces
  interface if_address
  neighbors
  packets
  policy
  route-stats
```
IGMP

Use this group of commands to configure parameters for the internet group management protocol.

IGMP Commands

Use these commands to configure IGMP for specific interfaces.

```
set igmp interface if_name
   last-member-query-interval <1-25>
   last-member=query-interval default
   local-group address <on | off>
   loss-robustness <1-255>
   loss-robustness default
   query-interval <1-3600>
   query-interval default
   query-response-interval <1-25>
   query-response-interval default
   router-alert <on | off>
   static-group address <on | off>
   version <1 | 2 | 3>
```

Use the following commands when IP clustering is enabled. You must be logged in as a cluster administrator. These commands are not functional unless IP clustering is enabled.

```
set igmp network ip_address/mask length
   last-member-query-interval <1-25>
   last-member=query-interval default
   local-group address <on | off>
   loss-robustness <1-255>
   loss-robustness default
   query-interval <1-3600>
   query-interval default
```
IGMP Commands

query-response-interval <1-25>
query-response-interval default
router-alert <on | off>
static-group address <on | off>
version <1 | 2 | 3>

Arguments.

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>network ip_address/mask length</td>
<td>Specifies the cluster network on which IGMP should be enabled.</td>
</tr>
<tr>
<td>last-member-query-interval &lt;1-25&gt;</td>
<td>Specifies the maximum response time, in seconds, inserted into IGMP group-specific queries.</td>
</tr>
<tr>
<td>last-member-query-interval default</td>
<td>Specifies a value of 1.</td>
</tr>
<tr>
<td>local-group address &lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td>loss-robustness &lt;1-255&gt;</td>
<td>Specifies a value that corresponds to the expected packet loss on a subnet.</td>
</tr>
<tr>
<td>loss-robustness default</td>
<td>Specifies a value of 2.</td>
</tr>
<tr>
<td>query-interval &lt;1-3600&gt;</td>
<td>Specifies the interval, in seconds, between IGMP general queries.</td>
</tr>
<tr>
<td>query-interval default</td>
<td>Specifies a value of 125.</td>
</tr>
<tr>
<td>query-response-interval &lt;1-25&gt;</td>
<td>Specifies the maximum response time, in seconds, inserted into the periodic IGMP general queries.</td>
</tr>
<tr>
<td>query-response-interval default</td>
<td>Specifies a value of 10.</td>
</tr>
<tr>
<td>router-alert &lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td>off</td>
<td></td>
</tr>
</tbody>
</table>

Chapter 9  Routing Commands  353
IGMP Show Commands

Use these commands to monitor and troubleshoot IGMP.

show igmp
  stats
  stats receive
  stats transmit
  stats error
  interfaces
  interfaces if_address
  groups [interface logical_interface] [local | static]
  group if_address
  if-stats
  if-stat if_address
  summary

Use the following commands to monitor and troubleshoot IGMP when IP clustering is enabled.

show igmp

static-group address <on | off>
  Specifies a multicast group address. IPSO acts as a receiver for this group and build the reverse path forwarding tree without waiting for requests from downstream hosts. IGMP informs the parent multicast protocol about the simulated local receiver but does not send a membership report out of this interface.

version <1 | 2 | 3>
  Specifies which version of IGMP to run. IGMP version 2 is compatible with IGMP version 1, and version 3 is compatible with versions 2 and 1. Check Point recommends that you use version 1 only on networks that include multicast routers that are not upgraded to IGMP versions 2 or 3.
networks
network ip_address/mask length
show igmp net-stats
show igmp net-stat ip_address/masklength
stats [receive | transmit | summary]
summary
PIM

Use this group of commands to configure parameters for PIM.

set pim mode
  <dense | sparse | ssm>

PIM Interfaces

After you set PIM to run either dense or sparse mode, use the following commands to configure PIM for specific interfaces.

set pim interface if_name
  <on | off>
  virtual-address <on | off>
  local-address ip_address
  dr-priority <0-4294967295>
  dr-priority default

PIM With IP Clustering

To use the following commands, you must be logged in as cadmin. These commands are not available unless you are logged in as cadmin. Any configuration you perform when logged in as cadmin is automatically propagated to each node of the cluster. When a new node joins a cluster, the local configuration of that node is replaced by the configuration obtained from the master.

set pim network ip_address/mask length
  <on | off>
  dr-priority <0-4294967295>
  dr-priority default

Sparse Mode PIM

Use the following commands to configure parameters for sparse mode PIM only.

set pim
ha-mode <on | off>
bootstrap-candidate <on | off>
bootstrap-candidate local-address ip_address
bootstrap-candidate priority <0-255>
bootstrap-candidate priority default
candidate-rp <on | off>
candidate-rp local-address ip_address
candidate-rp priority <0-255>
candidate-rp priority default
candidate-rp multicast group mcast_ip_prefix <on | off>
static-rp off
static-rp rp-address ip_address < on | off>
static-rp rp-address ip_address multicast-group mcast_ip_prefix <on | off>
register-suppress-interval <60-3600>
register-suppress-interval default
candidate-rp advertise-interval <1-3600>
candidate rp-advertise-interval default
cisco compatibility <on | off>
spt-threshold multicast mcast_ip_prefix threshold <0-1000000> <on | off>
spt-threshold multicast mcast_ip_prefix threshold infinity <on | off>
nat-mode <on | off>
state-refresh <on | off>
state-refresh-interval <0 - 255>
state-refresh-ttl <1 - 255>
Timer and Assert Rank Parameters for Dense Mode and Sparse Mode

Use these commands to change or restore default values for timers and assert ranks.

```
set pim
  hello-interval <1-21845>
  hello-interval default
  data-interval <11-3600>
  data-interval default
  assert-interval <1-3600>
  assert-interval default
  assert-limit <10-10000>
  assert-limit default
  assert-limit <0>
  jp-interval <1-3600>
  jp-interval default
  jp-delay-interval <1-3600>
  jp-delay-interval default
  jp-suppress-interval <2-3600>
  jp-suppress-interval default
  assert-rank protocol protocol name rank <0-255>
  assert-rank protocol protocol name rank default
```

Arguments

- `<dense | sparse | ssm>`: Specifies the mode PIM should use.
- `interface if_name <on | off>`: Specifies whether to enable or disable PIM on a specified interface.
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>virtual-address &lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td>local-address ip_address</td>
<td>Specifies the local address used in all advertisements sent on the interface. This option is useful when multiple IP addresses are configured on the interface. If you enter an address other than one configured for that interface, PIM ignores your configured address and selects one of the addresses configured on the interface. Warning: If neighboring routers choose advertisement addresses that do not appear to be on a shared subnet, all messages from the neighbor will be rejected. Thus, a PIM router on a shared LAN must have at least one interface address with a subnet prefix shared by all neighboring PIM routers.</td>
</tr>
</tbody>
</table>
Timer and Assert Rank Parameters for Dense Mode and Sparse Mode

**ha-mode <on | off>**

Specifies whether to enable or disable the High Availability (HA) mode. Enable the High-Availability (HA) mode when two routers are configured to back each other up to forward multicast traffic and sparse-mode PIM is implemented. When this option is enabled, all PIM-enabled interfaces are available only if each interface is up and has a valid address assigned. If any PIM-enabled interface goes down or all its valid addresses are deleted, then all PIM-enabled interfaces become unavailable and remain in that state until all interfaces are back up.

- The HA mode feature applies only to sparse-mode PIM. The HA mode feature does not affect the functioning of dense-mode PIM.

**Note** - Beginning with IPSO 3.8, you can configure PIM to advertise the virtual VRRP IP address on a interface with PIM enabled. You do not need to enable HA mode if you configure the interface to advertise the virtual VRRP IP address.

**off**

**dr-priority <0-4294967295>**

Specifies the dr-priority advertised in the PIM hello messages sent on the corresponding interface. This value, which has a default of 1, is used for DR election on a LAN. The router with the highest priority and the highest IP address is elected the designated router. To break a tie, the DR is selected on the basis of the highest IP address. If even one router does not advertise a dr-priority value in its hello messages, the DR election is based on the IP address.

**dr-priority default**

Specifies a value of 1.

**bootstrap-candidate <on | off>**

Specifies that the platform is a candidate bootstrap router. The bootstrap router collects candidate rendezvous point information and disseminates rp-set information associated with each group prefix. To avoid a single point of failure, configure more than router in a domain as a candidate bootstrap router.

**off**
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bootstrap-candidate</td>
<td>Specifies the IP address of the bootstrap router used in bootstrap messages. By default, the router picks an address from one of the interfaces on which PIM is enabled.</td>
</tr>
<tr>
<td>local-address</td>
<td></td>
</tr>
<tr>
<td>ip_address</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Specifies the value used to elect the bootstrap router from among the candidate bootstrap routers. The candidate bootstrap router with the highest priority value is elected bootstrap router for the domain. The highest priority value is 0, so the lower the value, the higher the priority.</td>
</tr>
<tr>
<td>priority &lt;0-255&gt;</td>
<td></td>
</tr>
<tr>
<td>bootstrap-candidate</td>
<td>Specifies a value of 0.</td>
</tr>
<tr>
<td>priority default</td>
<td></td>
</tr>
<tr>
<td>candidate-rp</td>
<td>Specifies that the platform is a candidate rendezvous point router.</td>
</tr>
<tr>
<td>&lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td></td>
<td>off</td>
</tr>
<tr>
<td>candidate-rp</td>
<td>Specifies the IP address of the candidate rendezvous point router used in candidate rendezvous point messages. By default, the router picks an address from one of the interfaces on which PIM is enabled.</td>
</tr>
<tr>
<td>local-address</td>
<td></td>
</tr>
<tr>
<td>ip_address</td>
<td></td>
</tr>
<tr>
<td>candidate-rp priority</td>
<td>Specifies the priority of the candidate rendezvous point included in the corresponding multicast group address. The higher the priority, the lower the value.</td>
</tr>
<tr>
<td>&lt;0-255&gt;</td>
<td></td>
</tr>
<tr>
<td>candidate-rp priority</td>
<td>Specifies a value of 0.</td>
</tr>
<tr>
<td>default</td>
<td></td>
</tr>
<tr>
<td>candidate-rp</td>
<td>Specifies the multicast address advertised in the candidate rendezvous point advertisements. For the multicast IP prefix value, you must enter an IP address and mask length. If you do not specify a group multicast address, the candidate rendezvous point advertises itself as the rendezvous point for all multicast groups.</td>
</tr>
<tr>
<td>multicast-group</td>
<td></td>
</tr>
<tr>
<td>mcast_ip_prefix</td>
<td></td>
</tr>
<tr>
<td>&lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td>static-rp off</td>
<td>Disables the static rendezvous point option.</td>
</tr>
<tr>
<td>static-rp rp-address</td>
<td>Specifies to enable or disable a static rendezvous point. If you do not specify an associated multicast group and prefix, the static-rp is considered to be responsible for all multicast groups (224.0.0.0/4).</td>
</tr>
<tr>
<td>ip_address &lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>static-rp rp-address</strong></td>
<td>Specifies the IP address associated with the static rendezvous point and the multicast IP address for which the rendezvous point is responsible. For the multicast IP prefix value, you must enter an IP address and mask length.</td>
</tr>
<tr>
<td><strong>ip_address</strong></td>
<td></td>
</tr>
<tr>
<td><strong>multicast-group</strong></td>
<td></td>
</tr>
<tr>
<td><strong>mcast_ip_prefix</strong></td>
<td></td>
</tr>
<tr>
<td>**&lt;on</td>
<td>off&gt;**</td>
</tr>
<tr>
<td><strong>register-suppress-interval</strong></td>
<td>Specifies the mean interval between receiving a register-stop and allowing registers to be sent again. A lower value means more frequent register bursts at the rendezvous point, while a higher value means a longer join latency for new receivers.</td>
</tr>
<tr>
<td><strong>&lt;60-3600&gt;</strong></td>
<td></td>
</tr>
<tr>
<td><strong>register-suppress-interval default</strong></td>
<td>Specifies a value of 60.</td>
</tr>
<tr>
<td><strong>candidate-rp advertise-interval</strong></td>
<td>Specifies the interval between which candidate-rendezvous point routers send candidate-rendezvous point advertisements.</td>
</tr>
<tr>
<td><strong>&lt;1-3600&gt;</strong></td>
<td></td>
</tr>
<tr>
<td><strong>candidate-rp advertise-interval default</strong></td>
<td>Specifies a value of 60.</td>
</tr>
<tr>
<td><strong>cisco-compatibility</strong></td>
<td>The checksum of the PIM register messages is calculated without including the multicast payload. Earlier releases of Cisco’s IOS calculate the checksum by including the multicast payload. If you experience difficulties having PIM register messages sent by your Check Point appliance being accepted by a Cisco router that is the elected rendezvous point (RP), configure this option. A Check Point appliance that is the elected RP, accepts register messages that calculate the checksum with or without the multicast payload, that is it accepts all register messages.</td>
</tr>
<tr>
<td>**&lt;on</td>
<td>off&gt;**</td>
</tr>
<tr>
<td><strong>spt-threshold multicast mcast_ip_prefix threshold &lt;0-1000000&gt;</strong></td>
<td>Specifies the multicast group address to apply to the shortest path tree (spt) threshold and the data rate in kbits/sec to trigger the spt switch over.</td>
</tr>
<tr>
<td>**spt-threshold multicast mcast_ip_prefix threshold infinity &lt;on</td>
<td>off&gt;**</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>hello interval</td>
<td>Specifies the interval, in seconds, at which PIM hello messages are sent on the LAN.</td>
</tr>
<tr>
<td>hello interval default</td>
<td>Specifies a value of 30.</td>
</tr>
<tr>
<td>data-interval</td>
<td>Specifies the interval, in seconds, after which multicast (S,G) state for a silent source is deleted.</td>
</tr>
<tr>
<td>data-interval default</td>
<td>Specifies a value of 210.</td>
</tr>
<tr>
<td>assert-interval</td>
<td>Specifies the interval between the last time an assert is received and the assert is timed out.</td>
</tr>
<tr>
<td>assert-interval default</td>
<td>Specifies a value of 180.</td>
</tr>
<tr>
<td>assert-limit</td>
<td>Specifies the number of asserts to send per second.</td>
</tr>
<tr>
<td>assert-limit default</td>
<td>Specifies a value of 10.</td>
</tr>
<tr>
<td>assert-limit &lt;0</td>
<td>Disables the limit placed on the number of asserts that can be sent per second.</td>
</tr>
<tr>
<td>jp-interval &lt;1-3600&gt;</td>
<td>Specifies the interval, in seconds, between which join/prune messages are sent.</td>
</tr>
<tr>
<td>jp-interval default</td>
<td>Specifies a value of 60.</td>
</tr>
<tr>
<td>jp-delay-interval &lt;1-3600&gt;</td>
<td>Specifies maximum interval, in seconds, between the time when the RPF neighbor changes and a triggered Join/Prune message is sent.</td>
</tr>
<tr>
<td>jp-delay-interval default</td>
<td>Specifies a value of 5.</td>
</tr>
<tr>
<td>jp-suppress-interval &lt;2-3600&gt;</td>
<td>Specifies the mean interval between receiving a Join/Prune with a higher “holdtime” and allowing duplicate Join/Prunes to be sent again. Check Point recommends that you set the join/prune suppress interval 1.25 times that of the join/prune interval.</td>
</tr>
<tr>
<td>jp-suppress-interval default</td>
<td>Specifies a value of 75.</td>
</tr>
</tbody>
</table>
Show PIM Commands

Use these commands to monitor and troubleshoot PIM. These commands apply to both dense-mode and sparse-mode implementations.

show pim

assert-rank protocol protocol name rank <0-255>

Specifies the value assigned to a particular protocol in assert messages. This value is used to compare protocols to determine which router will forward multicast packets on a multi-access LAN. The value is included in assert messages when more than one router on a LAN is capable of forwarding multicast packets and one router detects the other routers’ duplicate packets. Use the following protocol names to set this option: ospf; kernel; igrp; rip; static; bgp; direct and ospfase. The values assigned to each protocol must match for each router on a multi-access LAN.

assert-rank protocol protocol name rank default

Specifies default assert-rank values for supported protocols that match other implementations. The direct default value is 0. The ospf default value is 10; the kernel default value is 40; the static route default value is 60; the IGRP default value is 80; the rip default value is 100; the bgp default value is 170.

nat-mode <on | off>

Translates the addresses in a PIM protocol message to the relevant address(es) for the interface on which the message is being sent.

state-refresh <on | off>

Directs dense mode to use state refresh messages to delay timing out prune state of multicast traffic that has no active receivers. This helps suppress the flood-and-prune cycle inherent to dense mode.

state-refresh-interval <0 – 255>

Specifies the interval at which state refresh messages are sent for multicast traffic originated by directly-connected sources.

state-refresh-ttl <1 – 255>

Specifies the time-to-live (TTL) placed in the state refresh messages originated for multicast traffic from directly-connected sources. This value can be used to limit the forwarding of state refresh messages in the network.
interfaces
interfaces if_address
neighbors
neighbor ip_address
memory
timers
stats
summary

The following show commands apply only to sparse-mode PIM implementations. show pim
  bootstrap
candidate-rp
joins
rps
sparse-mode-stats
group-rp-mapping <mcast_address>

The following show commands apply only to PIM when IP clustering is enabled. show pim
  networks
  network ip_address
**Static Multicast Routes**

Use the commands explained in this section to configure static multicast routes for PIM. PIM expects packets to arrive on the reverse-path forwarding (RPF) interface, that is, the interface used to reach the source of the multicast data. PIM also checks the RPF to learn which interface it should use to send join/prune messages. By default, PIM identifies the RPF interface by checking the unicast routing table, but you can use static multicast routes to provide an alternative route table to use for the RPF check. If both a static multicast route and a unicast route are available for a specific destination, PIM uses the static multicast route.

Static multicast routes allow PIM to be independent of unicast routing and let you deploy topologies in which multicast and unicast traffic flow over different paths. For instance, if you want to balance your traffic load by separating the path used by HTTP traffic from the path used by streaming stock quotes, you could configure a static multicast route to the source network that specifies a next hop gateway address that is different from the next hop address (for the same source) in the unicast routing table.

**Note** - PIM is the only protocol that uses static multicast routes.

```plaintext
set static-mroute <sender_IP_address/mask | default>
  nexthop gateway
  address gateway_address <on | off | priority <1-8>>
  logical logical_interface priority <on | off | priority <1-8>>
  off
show static-mroute
```

**Arguments**

- `sender_IP_address/mask` Specifies the address and network mask of the multicast sender.
- `default` Specifies a default gateway to use for RPF lookups.
- `gateway_address` Specifies the address of the gateway router.
- `logical_interface` Specifies the name of the logical interface that connects to the gateway router.
### Static Multicast Routes

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>priority &lt;1-8&gt;</strong></td>
<td>Specifies the order in which the next hops are selected when there are multiple next hops for the same destination. The next hop with the lowest priority value is used. If the interface for this next hop fails, IPSO uses the next hop with the next lowest value.</td>
</tr>
<tr>
<td><strong>on</strong></td>
<td>Enables the specified multicast static route.</td>
</tr>
<tr>
<td><strong>off</strong></td>
<td>Disables the specified multicast static route.</td>
</tr>
</tbody>
</table>
Route Aggregation

Use the following group of commands to take numerous specific routes and aggregate them into one encompassing route. Route aggregation potentially reduces the number of routes advertised by a given protocol.

Only the receiver uses aggregate routes to forward packets. A router that receives a packet that does not match one of the component routes that resulted in the generation of an aggregate route responds with an Internet Control Message Protocol (ICMP) network unreachable message. This message prevents packets or unknown component routes from following a default route to another network where they would be continually forwarded back to the border router until their TTL expires.

Create an aggregate route by first specifying the network address and mask length. Second, provide a set of contributing routes. To define a contributing route, specify a source (routing protocol, static route, or interface route) and a route filter (an IP prefix). An aggregate route can have many contributing routes, but at least one of the routes must be present to generate an aggregate.

```
set [instance instance_name] aggregate ip_prefix
  contributing protocol protocol contributing-route
  <all | ip_prefix> <on | off>
  contributing protocol protocol contributing-route <ip_prefix>
     exact on
  contributing protocol protocol contributing-route ip_prefix
     refines on
    off
  contributing protocol <protocol> off
  rank default
  rank <0-255>
  weight default
  aspath-truncate <on | off>
```
### Arguments

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>contributing protocol</strong></td>
<td>Specifies the IP address and mask length of the new aggregate route and the contributing protocol or interface route. To specify a protocol, enter <code>direct</code>, <code>static</code>, <code>ospf2</code>, <code>ospf2ase</code>, <code>bgp</code>, <code>rip</code>, <code>igrp</code>, <code>rip</code>, or <code>aggregate</code>. To specify a contributing route, enter <code>all</code> to contribute all the routes for a specific protocol or enter the IP address and mask length to contribute a specific route.</td>
</tr>
<tr>
<td><strong>contributing-route ip_prefix exact on</strong></td>
<td>Specifies the IP address and the mask length of the new aggregate route and the contributing protocol and its corresponding IP address and mask length. The designation <code>exact on</code> means that the contributing route is limited to the specified IP address and mask length only.</td>
</tr>
<tr>
<td><strong>contributing-route ip_prefix refines on</strong></td>
<td>Specifies the IP address and mask length of the new aggregate route and the contributing protocol and its corresponding IP address and mask length. The designation <code>refines on</code> means that the contributing route is based on addresses with a greater value than the specified mask length of the specified IP address. You cannot enable both <code>exact on</code> and <code>refines on</code> at the same time. If you enable <code>refines on</code> when <code>exact on</code> is enabled, <code>exact on</code> is automatically disabled.</td>
</tr>
<tr>
<td><strong>rank default</strong></td>
<td>Specifies the rank to assign to the aggregate route when routes from different protocols to the same destination are present. For each route, the route from the protocol with the lowest rank is used. Each routing protocol has a different default rank value. Aggregate routes have a default rank of 130.</td>
</tr>
<tr>
<td><strong>rank &lt;0-255&gt;</strong></td>
<td>Specifies the rank to assign to the aggregate route when routes from different protocols to the same destination are present. For each route, the route from the protocol with the lowest rank is used. Each routing protocol has a different default rank value.</td>
</tr>
</tbody>
</table>
weight default

Specifies a value that breaks a tie if select routes going to the same destination have the same rank value. The route with the highest weight is the active route. The active route is installed in the kernel forwarding table and redistributed to the other routing protocols.

The default weight value is 0.

weight <0-65535>

Specifies a value that breaks a tie if select routes going to the same destination have the same rank value. The route with the highest weight is the active route. The active route is installed in the kernel forwarding table and redistributed to the other routing protocols.

aspath-truncate <on | off>

Specifies that the autonomous system (AS) path be truncated to the longest common AS path. The default, or off, option, specifies building an AS path that consists of sets and sequences of all contributing AS paths.

off
BOOTP

Use this group of commands to set and view parameters for the bootstrap protocol.

**BOOTP Interfaces**

Use this group of commands to configure BOOTP properties for specific interfaces.

```
set bootp interface if_name
  primary ip_address wait-time <0-65535> on
  relay-to ip_address <on | off>
  off
```

**Arguments**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>primary ip_address</td>
<td>Specifies the ip_address to stamp as the gateway address on all BOOTP requests. The wait-time value specifies the minimum amount of time, in seconds, to wait before forwarding a bootp request. Each client-generated bootp request includes the elapsed time since the client began the booting process. The bootp relay does not forward the request until the indicated elapsed time at least equals the specified wait time. This delay provides an opportunity for a local configuration server to reply before attempting to relay to a remote server.</td>
</tr>
<tr>
<td>wait-time &lt;0-65535&gt; on</td>
<td></td>
</tr>
<tr>
<td>relay-to ip_address</td>
<td>Specifies the server to which BOOTP requests are forwarded. You can specify more than one server.</td>
</tr>
<tr>
<td>&lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td>off</td>
<td>Disables BOOTP on the specified interface.</td>
</tr>
</tbody>
</table>

**BOOTP Show Commands**

Use this group of commands to monitor and troubleshoot BOOTP implementation.

```
show bootp
```
interfaces
interface if_name
stats
stats receive
stats request
stats reply
DVMRP

Use the following group of commands to set and view parameters for DVMRP.

**DVMRP Interfaces**

Use the following commands to configure DVMRP properties for specific interfaces.

```
set dvmrp interface if_name
<on | off>
threshold <1-255>
threshold default
metric <1-32>
metric default
```

*Arguments*

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td>threshold &lt;1-255&gt;</td>
<td>Specifies the minimum time to live (TTL) required for a multicast packet to be forwarded. Note that the TTL of forwarded packets is only compared to the threshold; it is not decremented by the threshold. Every multicast router decrements the TTL by 1. The packet is forwarded only if the TTL of the packet is greater than the threshold set for the outbound port. When connecting to the Internet Multicast Backbone (MBONE) the following values are recommended. For a link within a set the threshold value at 1; for a site boundary set the value at 32; for a regional boundary, set the value at 64; and for a continental boundary, set the value at 128.</td>
</tr>
<tr>
<td>threshold default</td>
<td>Specifies a value of 1.</td>
</tr>
<tr>
<td>metric &lt;1-32&gt;</td>
<td>Specifies the cost associated with sending a packet on the interface. It may be used to influence the choice of routes. A less expensive interface (smaller metric) is preferred to a more expensive interface (larger metric). You should use the smallest possible metric.</td>
</tr>
<tr>
<td>metric default</td>
<td>Specifies a value of 1.</td>
</tr>
</tbody>
</table>
DVMRP Timers

Use the following commands to configure values for DVMRP timers. Check Point recommends that if you have a core multicast network, configure the timer values so that they are uniform throughout a network. Otherwise, you can rely on the default timer values.

```plaintext
set dvmrp

neighbor-probe-interval <5-30>
neighbor-probe-interval default
neighbor-timeout-interval <35-8000>
neighbor-timeout-interval default
route-report-interval <10-2000>
route-expiration-time <20-4000>
route-expiration-time default
route-holddown-period <0-8000>
route-holddown-period default
cache-lifetime <60-86400>
cache-lifetime default
```

**Arguments**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>neighbor-probe-interval &lt;5-30&gt;</td>
<td>Specifies the interval, in seconds, at which probe messages are sent on each DVMRP interface.</td>
</tr>
<tr>
<td>Default: 10</td>
<td></td>
</tr>
<tr>
<td>neighbor-probe-interval default</td>
<td>Specifies a value of 10 seconds</td>
</tr>
<tr>
<td>neighbor-timeout-interval &lt;35-8000&gt;</td>
<td>Specifies the interval, in seconds, after which a silent neighbor is timed out.</td>
</tr>
<tr>
<td>For DVMRPv3 neighbors, the default is 35, and for non-DVMRPv3 neighbors, the default is 140.</td>
<td></td>
</tr>
<tr>
<td>neighbor-timeout-interval default</td>
<td></td>
</tr>
<tr>
<td>route-report-interval &lt;10-2000&gt;</td>
<td>Specifies the interval, in seconds, at which routing updates are sent on each DVMRP interface.</td>
</tr>
<tr>
<td>Default: 60</td>
<td></td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>show dvmrp</td>
<td>Use the following commands to monitor and troubleshoot your DVMRP implementation.</td>
</tr>
<tr>
<td>interfaces</td>
<td>show dvmrp</td>
</tr>
<tr>
<td>interfaces if_name</td>
<td></td>
</tr>
<tr>
<td>neighbors</td>
<td></td>
</tr>
<tr>
<td>neighbor ip_address</td>
<td></td>
</tr>
<tr>
<td>stats</td>
<td></td>
</tr>
<tr>
<td>mfc</td>
<td></td>
</tr>
<tr>
<td>reports</td>
<td></td>
</tr>
<tr>
<td>route</td>
<td></td>
</tr>
<tr>
<td>neighbor-routes</td>
<td></td>
</tr>
<tr>
<td>route-report-interval default</td>
<td>Specifies a value of 60 seconds.</td>
</tr>
</tbody>
</table>
| route-expiration-time <20-4000>     | Specifies the interval, in seconds, after which a route that has not been refreshed is placed in the route hold-down queue. 
Default: 140. |
| route-expiration-time default       | Specifies a value of 140 seconds.                                           |
| route-holddown-period <0-8000>      | Specifies the interval, in seconds, for which routes in the hold-down queue are advertised with a metric of infinity before they are deleted. 
Default: 120. |
| route-holddown-period default       | Specifies a value of 120 seconds.                                           |
| cache-lifetime <60-86400>           | Specifies the interval, in seconds, that a cached forwarding entry is maintained in the kernel forwarding table before it is timed out because of inactivity. 
Default: 300. |
| cache-lifetime default              | Specifies a value of 300 seconds.                                           |
summary
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 slot <1-15> [instance instance_name] 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

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>next hop gateway address &lt;1-8&gt; on</td>
<td>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 &quot;non-reachability&quot; 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.</td>
</tr>
<tr>
<td>next hop logical if name priority &lt;1-8&gt; on</td>
<td>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 &quot;non-reachability&quot; 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.</td>
</tr>
<tr>
<td>next hop gateway address off</td>
<td>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.</td>
</tr>
<tr>
<td>next hop gateway logical if name off</td>
<td>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.</td>
</tr>
</tbody>
</table>
Configuring Static Routes

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>
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>set static-route default</code></td>
<td>Enables the default static route to be used.</td>
</tr>
<tr>
<td><code>next hop gateway address gateway_address priority &lt;1-8&gt; on</code></td>
<td>Specifies the next hop for the default route.</td>
</tr>
<tr>
<td><code>nexthop gateway logical gateway_address priority &lt;1-8&gt; on</code></td>
<td>Specifies the logical next hop for the default route.</td>
</tr>
<tr>
<td><code>nexthop gateway address gateway_address off</code></td>
<td>Disables the next hop for the default route.</td>
</tr>
<tr>
<td><code>nexthop gateway logical gateway_address off</code></td>
<td>Disables the logical next hop for the default route.</td>
</tr>
<tr>
<td><code>nexthop reject</code></td>
<td>Specifies that packets are dropped rather than forwarded.</td>
</tr>
<tr>
<td><code>nexthop blackhole</code></td>
<td>Specifies that packets are dropped rather than forwarded. Unlike the reject option, it does not result in unreachable messages being sent to the packet originators.</td>
</tr>
<tr>
<td><code>ip_prefix off</code></td>
<td>Disables prefix routing.</td>
</tr>
<tr>
<td><code>ip_prefix rank default</code></td>
<td>Sets the default rank for prefix routing.</td>
</tr>
<tr>
<td><code>ip_prefix rank &lt;0-255&gt;</code></td>
<td>Sets the rank for prefix routing.</td>
</tr>
</tbody>
</table>
ICMP Router Discovery

Use this group of commands to set and view parameters for the ICMP router discovery protocol.

ICMP Router Discovery Interfaces

Use the following commands to configure router discovery properties for specific interfaces.

set rdisc interface if_name
   <on | off>
   min-adv-interval <3-1800>
   min-adv-interval default
   max-adv-interval <4-1800>
   max-adv-interval default
   adv-lifetime integer
   adv-lifetime default
   advertise ip_address <on | off>
   advertise ip_address preference ineligible
   advertise ip_address preference integer

Arguments

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td>min-adv-interval &lt;3-1800&gt;</td>
<td>Specifies the minimum time (in seconds) allowed between sending unsolicited broadcast or multicast ICMP router advertisements on the interface.</td>
</tr>
<tr>
<td>min-adv-interval default</td>
<td>Specifies a value of 450 seconds.</td>
</tr>
<tr>
<td>max-adv-interval &lt;4-1800&gt;</td>
<td>Specifies the maximum time (in seconds) allowed between sending unsolicited broadcast or multicast ICMP router advertisements on the interface.</td>
</tr>
<tr>
<td>max-adv-interval default</td>
<td>Specifies a value of 600 seconds.</td>
</tr>
</tbody>
</table>
ICMP Router Discovery Show Commands

Use the following commands to monitor and troubleshoot your ICMP router discovery implementation.

```
show rdisc
  interfaces
  interface if_name
  stats
  summary
```

**adv-lifetime integer**
- Specifies the time (in seconds) placed in the lifetime field of router advertisement packets sent from the interface. Enter an integer value between the configured value for the maximum advertisement interval and 9000.

**adv-lifetime default**
- Specifies a value of 1800 or 3 times the configured maximum advertisement interval.

**advertise ip_address <on | off>**
- Specifies whether to advertise the specified IP address that is associated with the interface should be advertised in router advertisement packets.

**advertise ip_address preference ineligible**
- Specifies not to use the specified IP address as a default router.

**advertise ip_address preference integer**
- Specifies the preferability of the specified IP address as a default router address relative to other router addresses on the same subnet.
IP Broadcast Helper

Use the following group of commands to set and view parameters for IP Broadcast Helper.

IP Broadcast Helper Forwarding

Use the following commands to control whether to forward packets that are not locally originated by a source directly on the receiving interface.

```plaintext
set iphelper
forward-nonlocal <on | off>
```

IP Broadcast Helper Interfaces

Use the following commands configure IP Broadcast Helper properties for specific interfaces.

```plaintext
set iphelper interface if_name
off
udp-port <1-65535> off
udp-port <1-65535> relay-to ip_address <on | off>
```

Arguments

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>forward-nonlocal &lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td>interface &lt;if_name&gt; off</td>
<td>Specifies to disable the interface configured for iphelper</td>
</tr>
<tr>
<td>udp-port &lt;1-65535&gt; off</td>
<td>Specifies to disable the UDP services configured for this interface.</td>
</tr>
</tbody>
</table>
show iphelper
  services
  stats

udp-port <1-65535>
relay-to ip_address <on | off>

Specifies the UDP services defined for forwarding on the interface. Client UDP packets with the specified UDP port number are forwarded to the configured server(s). The IP address for the UDP port specifies a new server to send client packets received on the associated interface and UDP service.
Network Address Translation

Network Address Translation (NAT) is an IETF standard that enables a local area network (LAN) to use one set of IP addresses for internal traffic and a second set of addresses for external traffic.

- **Interface**—Specifies whether NAT is enabled on the specified interface. User can select only one internal and only one external interface.
  - **Options:** On/Off.
  - **Default:** Off.
- **External translated address**—External translated address to be configured by the user. The address configured will be the translation for all the internal addresses.
  - **Range:** Dotted-quad ([0-255].[0-255].[0-255].[0-255]).
  - **Default:** None.

Use these commands to set and view NAT interface parameters:

```
set nat interface
set nat external-translated-address
show nat interfaces
show nat translations
```

**Arguments**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>set nat interface IFACE off</code></td>
<td>Enables NAT on the specified interface.</td>
</tr>
<tr>
<td><code>set nat interface IFACE internal</code></td>
<td>Specifies the NAT interface as internal.</td>
</tr>
<tr>
<td><code>set nat interface IFACE external</code></td>
<td>Specifies the NAT interface as external.</td>
</tr>
<tr>
<td>`set nat external-translated-address IFACE on</td>
<td>off`</td>
</tr>
<tr>
<td><code>show nat interfaces</code></td>
<td>Displays NAT interfaces.</td>
</tr>
<tr>
<td><code>show nat translations</code></td>
<td>Displays NAT translations.</td>
</tr>
</tbody>
</table>
Network Time Protocol

Use the following commands to set and view parameters for network time protocol (NTP). NTP lets you synchronize time among different machines.

**Configuring an NTP Server**

```
set ntp
  server ip_address version <1-3>
  prefer server ip_address
  peer ip_address version <1-3>
  prefer peer ip_address
  master source ip_address stratum <0-15>
```

**Adding an NTP Server**

Use the following commands to add a new NTP server.

```
add ntp
  server ip_address version <1-3>
  prefer server ip_address
  peer ip_address version <1-3>
  prefer peer ip_address
```

**Deleting an NTP Server**

Use the following commands to delete an NTP server.

```
delete ntp
  server ip_address
  peer ip_address
```
## NTP Show Commands

Use the following commands to monitor and troubleshoot your NTP implementation.

```
show ntp
  active
  ntp master
  ntp peer ip_address
  ntp peers
  ntp server ip_address
  ntp servers
```

### Arguments

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>server ip_address version</td>
<td>Specifies the IP address of the time server from which your system synchronizes its clock. The specified time server does not synchronize to the local clock of your system. The version number specifies which version of NTP to run. Check Point recommends that you run version 3.</td>
</tr>
<tr>
<td>prefer server ip_address</td>
<td>Specifies to prefer the specified time server if more than one configured time server is functioning.</td>
</tr>
<tr>
<td>peer ip_address version</td>
<td>Specifies the IP address of the time server from which this system synchronizes its clock. The specified peer time can synchronize to the local clock of your system. The version number specifies which version of NTP to run. Check Point recommends that you run version 3.</td>
</tr>
<tr>
<td>prefer peer ip_address</td>
<td>Specifies to prefer the specified peer time server if more than one configured time server is functioning.</td>
</tr>
<tr>
<td>master source ip_address</td>
<td>Specifies to use this system as the source of time. Enter the system’s IP address. Straatum specifies the number of hops away from a correct source of time this system’s clock should appear to be.</td>
</tr>
<tr>
<td>stratum</td>
<td>Note - Check Point recommends that you maintain this default value.</td>
</tr>
</tbody>
</table>

Note: Check Point recommends that you maintain this default value.
Dial on Demand Routing

Use the following commands to create, delete, or view the configuration of a dial on demand routing (DDR) list and add or delete ISDN interfaces to it. If you do not assign an ISDN interface to a DDR list, any traffic passed to the interface will cause it to attempt to set up a connection.

Dial on Demand Routing Commands

Use the commands in this section to configure DDR lists, and rules for the DDR lists.

```plaintext
add ddrlist name
show ddrlist
delete ddrlist name
add ddrlist name interface log_if_name
delete ddrlist name interface log_if_name
```

**Arguments**

<table>
<thead>
<tr>
<th>name</th>
<th>Specifies a unique name for the DDR list. Names can contain letters, numbers, and underscores but must begin with a letter and must be no longer than 15 characters.</th>
</tr>
</thead>
</table>

Use the following commands to create rules that you assign to DDR lists. These rules tell the system which packets should trigger it to set up or maintain an ISDN connection. When you create a DDR list, a default rule is automatically created for it.

```plaintext
add ddrlist name rule rule_num
  action <skip | ignore | accept>
  src-address ip_address
  src-masklen <0–32>
  dest-address ip_address
  dest-masklen <0–32>
  src-port <0–65535>
  dst-port <0–65535>
  protocol name
```
Use the following commands to configure DDR rules. Before you can configure DDR rules, you must assign a logical ISDN interface to the DDR list by entering add ddrlist name interface log_if_name.

```
set ddrlist name rule rule_num
  action <skip | ignore | accept>
  src-address ip_address
  src-masklen <0–32>
  dest-address ip_address
  dest-masklen <0–32>
  src-port <0–65535>
  dst-port <0–65535>
  protocol name
```

delete ddrlist name rule rule_num

The default values shown in the following table apply automatically created default rule.

### Arguments

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>add ddrlist name rule</td>
<td>rule_num is the number of an existing rule. The new rule being created will</td>
</tr>
<tr>
<td>rule_num</td>
<td>be positioned and numbered before the existing rule (and the number of the</td>
</tr>
<tr>
<td></td>
<td>existing rule will be incremented by one). The default rule's number is 1</td>
</tr>
<tr>
<td></td>
<td>until you create additional rules.</td>
</tr>
<tr>
<td>set ddrlist name rule</td>
<td>When you use the set version of these commands, rule_num is the number of</td>
</tr>
<tr>
<td>rule_num</td>
<td>the rule you want to modify.</td>
</tr>
<tr>
<td>delete ddrlist name</td>
<td>Deletes the rule with the number of rule_num.</td>
</tr>
<tr>
<td>rule rule_num</td>
<td></td>
</tr>
<tr>
<td>action &lt;skip</td>
<td>ignore</td>
</tr>
<tr>
<td></td>
<td>encounters packets that match the rules' criteria. If action is set to</td>
</tr>
<tr>
<td></td>
<td>ignore, matching packets will be passed over an existing connection but</td>
</tr>
<tr>
<td></td>
<td>will not trigger the initiation of a connection. If action is set to</td>
</tr>
<tr>
<td></td>
<td>skip, the system will not use compare packets against the rule—the rule</td>
</tr>
<tr>
<td></td>
<td>is turned off.</td>
</tr>
<tr>
<td>skip</td>
<td></td>
</tr>
<tr>
<td>src-address ip_address</td>
<td>Specifies a source IP address to match against this rule.</td>
</tr>
</tbody>
</table>
Dial on Demand Routing Commands

### src-masklen <0–32>
Specifies a mask length for the source IP address.
0

### dest-address
ip_address
Specifies a destination IP address to match against the rule.

### dest-masklen <0–32>
Specifies a mask length for the destination IP address.
0

### src-port <0–65535>
Specifies a specific port or range of ports for the source of a connection. This argument is only valid if the protocol for the rule is TCP, UDP, or any.

### dst-port <0–65535>
Specifies a specific port or range of ports for the destination of a connection. This argument is only valid if the protocol for the rule is TCP, UDP, or any.

### protocol name
Specifies the IP protocol that the rule applies to. Only one protocol can be specified per rule (unless you use the default value of any, in which case the rule applies to all protocols). This argument is not case-sensitive.
Routing Option Commands

Use the commands in this section to configure a variety of miscellaneous options that affect routing.

Equal-cost Path Splitting (Load Sharing)

Use the following command to specify a value for the maximum number of equal-cost paths that will be used when there is more than one equal-cost path to a destination. Only OSPF routes and Static routes are able to use more than one "next hop".

```
set [instance instance_name] max-path-splits <1-8>
```

**Arguments**

<table>
<thead>
<tr>
<th>max-path-splits &lt;1-8&gt;</th>
<th>Indicates the maximum number of equal-cost paths that will be used when there is more than one equal-cost path to a destination.</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td></td>
</tr>
</tbody>
</table>

Use the following command to determine which “next hop” algorithm is used for forwarding when there is more than one “next hop” to a particular destination.

```
set [instance instance_name] nexthop-selection
  src-dest-hash
  dest-hash
  src-hash
  rr
```
Protocol Rank

Arguments

- src-dest-hash: Source/destination hash: The IP forwarding code performs a hash function on the source and destination IP address of each packet that is forwarded to a multipath destination. This result is used to determine which next hop to use.
- dest-hash: Destination hash: Operates the same as source/destination hash but only the destination IP address is used. Packets that are being sent to the same destination address will all use the same "next hop".
- src-hash: Source hash: Operates the same as source/destination hash but only the source IP address is used. Packets that are being sent from the same source address will all use the same "next hop".
- rr: Round robin: Each time a set of "next hop"s is used for forwarding, a different "next hop" is used in a round-robin manner. This results in equal load sharing, but it is not recommended because it may result in out-of-order packet delivery for the same session.

Protocol Rank

Rank is used by the routing system when there are routes from different protocols to the same destination. For each route, the route from the protocol with lowest rank number will be used.

```
set protocol-rank protocol
  bgp rank <0–255>
  bgp rank default
  igrp rank <0–255>
  igrp rank default
  rip rank <0–255>
  rip rank default
set [instance instance_name] protocol-rank protocol
  ospf rank <0–255>
  ospf rank default
  ospfase rank <0–255>
  ospfase rank default
```
## Arguments

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>protocol rank &lt;0–255&gt;</code></td>
<td>Specifies the protocol rank value.</td>
</tr>
<tr>
<td><code>bgp rank default</code></td>
<td>The default rank value for BGP is 170.</td>
</tr>
<tr>
<td><code>igrp rank default</code></td>
<td>The default rank value for IGRP is 80.</td>
</tr>
<tr>
<td><code>rip rank default</code></td>
<td>The default rank value for RIP is 100.</td>
</tr>
<tr>
<td><code>ospf rank default</code></td>
<td>The default rank value for OSPF is 10.</td>
</tr>
<tr>
<td><code>ospfase rank default</code></td>
<td>The default rank value for OSPF ASE routes is 150.</td>
</tr>
</tbody>
</table>
Trace Routing Commands

The routing system can optionally log information about errors and events. Logging is configured for each protocol or globally. Logging is not generally turned on during normal operations, as it can decrease performance. Log messages for the default instance are saved in `/var/log/ipsrd.log`. If you have configured multiple instances, log messages are saved in `/var/log/<instance_name>.log`.

Configuring the Trace Log File

Use the following commands to configure the log file options for trace routing.

```
set [instance instance_name] tracefile
  size <1—4095>
  size default
  maxnum <1—4294967295>
  maxnum default
```

Arguments

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>size &lt;1—4095&gt;</td>
<td>Limits the maximum size of the trace file to the specified size, in megabytes.</td>
</tr>
<tr>
<td>size default</td>
<td>The default maximum trace file size is 1 MB.</td>
</tr>
<tr>
<td>maxnum &lt;1—4294967295&gt;</td>
<td>When the trace file reaches the specified size, it is renamed to file.0, then file.1, file.2, up to the maximum number of files.</td>
</tr>
<tr>
<td>maxnum default</td>
<td>The default maximum number of trace files is 10.</td>
</tr>
</tbody>
</table>

Trace Option Variables

You can specify a variety of different trace options with the `trace` command. While there are trace options specific to each protocol, many protocols share a set of options. These common trace options are specified in the `traceoption` variable.

The following table lists the `traceoption` parameters.

Arguments

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Trace all of the options in <code>traceoptions</code>.</td>
</tr>
<tr>
<td>general</td>
<td>Trace both <code>normal</code> and <code>route</code>.</td>
</tr>
</tbody>
</table>
Trace Option Variables

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>normal</td>
<td>Trace normal protocol occurrences. Abnormal protocol occurrences are always traced.</td>
</tr>
<tr>
<td>policy</td>
<td>Trace the application of protocol- and user-specified policy to routes being imported and exported.</td>
</tr>
<tr>
<td>route</td>
<td>Trace routing table changes for routes installed by this protocol or peer.</td>
</tr>
<tr>
<td>state</td>
<td>Trace state machine transitions in the protocols.</td>
</tr>
<tr>
<td>task</td>
<td>Trace system interface and processing associated with this protocol or peer.</td>
</tr>
<tr>
<td>timer</td>
<td>Trace timer usage by this protocol or peer.</td>
</tr>
</tbody>
</table>

Use the following command to turn BGP trace options on or off.

```
set trace bgp
    keepalive <on | off>
    open <on | off>
    update <on | off>
    packets <on | off>
    traceoptions <on | off>
```

**Arguments**

- **keepalive**: Trace BGP keepalive messages
- **open**: Trace BGP open packets. These packets are sent between peers when they are establishing a connection.
- **update**: Trace update packets. These packets provide routing updates to BGP systems.
- **packets**: Trace all BGP protocol packets.
- **traceoptions**: `<all | general | normal | policy | route | state | task | timer>`

Use the following command to turn DVMRP trace options on or off.

```
set trace dvmrp
    graft <on | off>
    mfc <on | off>
    mapper <on | off>
```
Trace Option Variables

neighbor <on | off>
probe <on | off>
prune <on | off>
report <on | off>
packets <on | off>
traceoptions <on | off>

Arguments

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>graft</td>
<td>Trace DVMRP graft and graftack packets.</td>
</tr>
<tr>
<td>mfc</td>
<td>Trace DVMRP multicast forwarding cache packets</td>
</tr>
<tr>
<td>mapper</td>
<td>Trace DVMRP neighbor and neighbor2 packets.</td>
</tr>
<tr>
<td>neighbor</td>
<td>Trace DVMRP neighbor packets.</td>
</tr>
<tr>
<td>probe</td>
<td>Trace DVMRP probe packets.</td>
</tr>
<tr>
<td>prune</td>
<td>Trace DVMRP prune packets.</td>
</tr>
<tr>
<td>report</td>
<td>Trace DVMRP route report packets.</td>
</tr>
<tr>
<td>packet</td>
<td>Trace all DVMRP packets.</td>
</tr>
<tr>
<td>traceoptions</td>
<td>&lt;all</td>
</tr>
</tbody>
</table>

Use the following command to turn ICMP trace options on or off.

set trace icmp
  error <on | off>
  info <on | off>
  routerdiscovery <on | off>
packets <on | off>
traceoptions <on | off>
## Arguments

<table>
<thead>
<tr>
<th>error</th>
<th>Trace only ICMP error packets, which include:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• time exceeded</td>
</tr>
<tr>
<td></td>
<td>• parameter problem</td>
</tr>
<tr>
<td></td>
<td>• unreachable</td>
</tr>
<tr>
<td></td>
<td>• source quench</td>
</tr>
<tr>
<td>info</td>
<td>Trace only ICMP informational packets, which include:</td>
</tr>
<tr>
<td></td>
<td>• mask request/response</td>
</tr>
<tr>
<td></td>
<td>• info request/response</td>
</tr>
<tr>
<td></td>
<td>• echo request/response</td>
</tr>
<tr>
<td></td>
<td>• time stamp request/response</td>
</tr>
<tr>
<td>routerdiscovery</td>
<td>Trace only ICMP router discovery packets.</td>
</tr>
<tr>
<td>packets</td>
<td>Trace all ICMP packets.</td>
</tr>
<tr>
<td>traceoptions</td>
<td>&lt;all</td>
</tr>
</tbody>
</table>

Use the following command to turn IGRP trace options on or off.

```
set trace igrp
   packets <on | off>
   traceoptions <on | off>
```

## Arguments

| packets   | Trace all IGRP packets.                      |
| traceoptions | <all | general | normal | policy | route | state | task | timer> |

Use the following command to turn IGMP trace options on or off.

```
set trace igmp
   group <on | off>
   leave <on | off>
   mtrace <on | off>
   query <on | off>
   report <on | off>
```
Trace Option Variables

request <on | off>
packets <on | off>
traceoptions <on | off>

Arguments

group  Trace multicast group add, delete, refresh and accelerated leave.
leave  Trace IGMP “leave group” messages.
mtrace Trace details of IGMP multicast traceroute request processing.
query  Trace IGMP membership query packets (both general and
        group-specific).
report Trace IGMP membership report packets (both IGMPv1 and
        IGMPv2).
request Trace IGMP multicast traceroute request packets.
packets Trace all IGMP packets.
traceoptions <all | general | normal | policy | route | state | task | timer>

Use the following command to turn IP broadcast helper trace options on or off.
set trace iphelper
    packets <on | off>
    traceoptions <on | off>

Arguments

packets Trace all IP broadcast helper packets.
traceoptions <all | general | normal | policy | route | state | task | timer>

Use the following command to turn MFC trace options on or off.
set trace mfc
    alerts <on | off>
    cache <on | off>
    interface <on | off>
mcastdist <on | off>
packets <on | off>
Trace Option Variables

resolve <on | off>
wrongif <on | off>
traceoptions <on | off>

Arguments

alerts Trace multicast protocol alert callback functions.
cache Trace log details of cache maintenance. These include:
  • addition or deletion of orphan entries (in other words, entries with no route to source).
  • addition or deletion of normal entries.
  • cache state aging and refresh.
interface Trace log changes requested by external ipsrd modules (IGMP and multicast routing protocols) affecting the forwarding dependencies on an interface. These include:
  • addition or deletion of a forwarding interface due to routing changes.
  • changing of the parent (reverse path forwarding) interface due to routing changes.
mcastdist Trace kernel multicast distribution entries. Both generic and PIM register encapsulation and decapsulation types.
packets Trace all MFC related packets.
resolve Trace kernel external resolve requests (both normal and PIM register types).
wrongif Trace kernel multicast incoming interface violation notifications (both physical interface and PIM register types).
traceoptions <all | general | normal | policy | route | state | task | timer>

Use the following command to turn PIM trace options on or off.
set trace pim
  assert <on | off>
  bootstrap <on | off>
  crp <on | off>
  graft <on | off>
### Trace Option Variables

- `hello <on | off>`
- `join <on | off>`
- `mfc <on | off>`
- `mrt <on | off>`
- `packets <on | off>`
- `rp <on | off>`
- `register <on | off>`
- `trap <on | off>`
- `traceoptions <on | off>`

#### Arguments

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>assert</td>
<td>Trace PIM assert messages.</td>
</tr>
<tr>
<td>bootstrap</td>
<td>Trace bootstrap messages (sparse-mode only).</td>
</tr>
<tr>
<td>crp</td>
<td>Trace candidate-RP-advertisements (sparse-mode only).</td>
</tr>
<tr>
<td>graft</td>
<td>Trace graft and graft acknowledgment packets.</td>
</tr>
<tr>
<td>hello</td>
<td>Trace PIM router hello packets.</td>
</tr>
<tr>
<td>join</td>
<td>Trace PIM join/prune messages.</td>
</tr>
<tr>
<td>mfc</td>
<td>Trace interaction with multicast forwarding cache.</td>
</tr>
<tr>
<td>mrt</td>
<td>Trace PIM multicast routing table events.</td>
</tr>
<tr>
<td>packets</td>
<td>Trace all PIM packets.</td>
</tr>
<tr>
<td>rp</td>
<td>Trace RP-specific events. This includes both RP set-specific and bootstrap-specific events (sparse-mode only).</td>
</tr>
<tr>
<td>register</td>
<td>Trace register and register-stop packets (sparse-mode only).</td>
</tr>
<tr>
<td>trap</td>
<td>Trace PIM trap messages.</td>
</tr>
<tr>
<td>traceoptions</td>
<td>&lt;all</td>
</tr>
</tbody>
</table>

Use the following command to turn BGP trace options on or off.

```plaintext
set trace rip
    packets <on | off>
    traceoptions <on | off>
```
Arguments

packets Trace all RIP packets.
traceoptions <all | general | normal | policy | route | state | task | timer>

Use the following command to turn VRRP trace options on or off.
set trace vrrp
   advertise <on | off>
   traceoptions <on | off>

Arguments

advertise Trace all VRRP packets.
traceoptions <all | general | normal | policy | route | state | task | timer>

Use the following command to turn ICMP router discovery trace options on or off.
set trace router-discovery option <on | off>
   traceoptions

Arguments

traceoptions <all | general | normal | policy | route | state | task | timer>

Use the following command to turn global trace options on or off.
set trace global
   adv <on | off>
   parse <on | off>
   traceoptions <on | off>

Arguments

adv Trace the allocation of and freeing of policy blocks.
parse Trace the lexical analyzer and parser.
traceoptions <all | general | normal | policy | route | state | task | timer>
Use the following command to turn kernel trace options on or off.

```bash
set trace kernel
   iflist <on | off>
   interface <on | off>
   packets <on | off>
   remnants <on | off>
   request <on | off>
   routes <on | off>
   traceoptions <on | off>
```

**Arguments**

- **iflist**: Trace iflist, the interface list scan.
- **interface**: Trace interface status messages that are received from the kernel.
- **packets**: Trace packets that are read from the kernel.
- **remnants**: Trace remnants, which specify routes read from the kernel when the routing daemon starts.
- **request**: Trace requests, which specify to add, delete, or change routes in the kernel forwarding table.
- **routes**: Trace routes that are exchanged with the kernel, including add, delete, or change messages and add, delete, or change messages received from other processes.
- **traceoptions**: `<all | general | normal | policy | route | state | task | timer>`

Use the following command to turn OSPF trace options on or off.

```bash
set [instance instance_name] trace ospf
   ack <on | off>
   dd <on | off>
   dr <on | off>
   hello <on | off>
   lsa <on | off>
   packets <on | off>
   request <on | off>
```
Trace Option Variables

.. code-block::

    spf <on | off>
    trap <on | off>
    update <on | off>
    traceoptions <on | off>

Arguments

- **ack**: Trace link-state acknowledgment packets.
- **dd**: Trace all database description packets.
- **dr**: Trace designated router packets.
- **hello**: Trace hello packets.
- **lsa**: Trace link-state announcement packets.
- **packets**: Trace OSPF packets.
- **request**: Trace link-state request packets.
- **spf**: Trace shortest-path-first (SPF) calculations.
- **trap**: Traces OSPF trap packets.
- **update**: Trace link-state updates packets.
- **traceoptions**: `<all | general | normal | policy | route | state | task | timer>`
Show Route Summary Commands

Use the commands in this section to view summary information about routes on your system.

Route Summary Commands

Use the following command to show information about active, inactive or all (both active and inactive) routes on your system for BGP, IGRP and RIP protocols.

```
show route
  igrp
  rip
  bgp
  <aspath | communities | detailed | metrics | suppressed>
  inactive <bgp | igrp | rip>
  all <bgp | igrp | rip>
```

Use the following command to show information about active, inactive, or all routes on your system for the OSPF protocol.

```
show [instance instance_name] route
  ospf
  inactive ospf
  all ospf
```

Use the following command to show information about active, inactive and all aggregate routes on your system.

```
show [instance instance_name] route
  aggregate
  inactive aggregate
  all aggregate
```

Use the following command to show additional information about routes on your system.

```
show [slot <1-15>] [instance instance_name] route
```
all
direct
static
inactive
direct
inactive static
static
summary
destination ip_address
exact ip_prefix
less-specific ip_prefix
more-specific ip_prefix
Show Routing Daemon (IPSRD) Commands

Use the following commands to view general information recorded by the IPSO routing daemon (IPSRD).

```
show ipsrd
  memory
  resources
  krt
  version
```

Arguments

`memory` Displays the memory usage of the routing daemon. It shows the information for each routing protocol running on the system.

- Total memory usage
- MFC - memory used for the multicast forwarding cache (MFC)
- Core - memory used by IPSRD for its internal purpose
- Protocol - memory used by the given protocol
resources Displays the following system information:

- Total uptime
- Total user time
- Total system time
- Page faults
- Page reclaim
- File system writes
- File system reads
- Message writes
- Message reads
- Signals received
- Total swaps
- Voluntary context switches
- Involuntary context switches

krt Displays statistical information about the messages sent and received on the raw sockets between the kernel and IPSRD.

- KRT interface message count
- KRT interface message length
- KRT route message count (rx)
- KRT route message length (rx)
- KRT route message count (tx)
- KRT route message length (tx)
- KRT route adds
- KRT route changes
- KRT route deletes
version Displays the following system information:
  • IPSRD version
  • System start time
  • Current time
  • System uptime
Show MFC Commands

Use the following commands to view information about multicast forwarding cache (MFC) on your system.

```
show mfc
  cache
  summary
  interface
  orphans
  stats
```

Arguments

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cache</td>
<td>Displays MFC state information.</td>
</tr>
<tr>
<td>summary</td>
<td>Displays the following MFC state information:</td>
</tr>
<tr>
<td></td>
<td>• Number of interfaces enabled</td>
</tr>
<tr>
<td></td>
<td>• Number of cache entries</td>
</tr>
<tr>
<td></td>
<td>• Kernel forwarding entry limit</td>
</tr>
<tr>
<td></td>
<td>• Number of kernel forwarding entries</td>
</tr>
<tr>
<td></td>
<td>• Cache entry average lifetime</td>
</tr>
<tr>
<td></td>
<td>• Prune average lifetime</td>
</tr>
<tr>
<td></td>
<td>• Cache age cycle</td>
</tr>
<tr>
<td></td>
<td>• Data rate update interval</td>
</tr>
<tr>
<td></td>
<td>• Multicast protocol (instance)</td>
</tr>
<tr>
<td>interface</td>
<td>Displays MFC interface state information.</td>
</tr>
<tr>
<td>orphans</td>
<td>Displays MFC orphan state information.</td>
</tr>
<tr>
<td>stats</td>
<td>Displays various information about the following MFC properties:</td>
</tr>
<tr>
<td></td>
<td>• Resolve task summary</td>
</tr>
<tr>
<td></td>
<td>• Resolve requests</td>
</tr>
<tr>
<td></td>
<td>• RPF failure notifications</td>
</tr>
<tr>
<td></td>
<td>• MFC maintenance</td>
</tr>
</tbody>
</table>
Chapter 10

Traffic Management Commands

This chapter describes the commands you use to configure traffic management functionality on your system and to view current settings.

In This Chapter

Access Control List Commands  page 412
Aggregation Class Commands  page 420
Queue Class Commands  page 422
Policy Based Routing Commands  page 427
DSCP to VLAN Priority Commands  page 432
Netflow Commands  page 433
Access Control List Commands

Access control lists (ACLs) sort incoming network traffic into discrete packet streams based on fields in the packet header. An access list contains a set of rules called the ruleset. When a packet matches a rule, the system executes the action specified in the rule. Using the access list CLI commands, you can configure an access list to control the traffic from one or more interfaces. Also, each access list can be associated with incoming or outgoing traffic from each interface.

**ACL Node Commands**

Use the following command to show all created ACLs in the system.

```
show acl
```

Use the following command to create a new, uniquely-named ACL. You have the option to create an association between the ACL rule and the specified logical interface. The interface binding is related to the traffic flow direction. You can specify a logical interface for outgoing traffic, incoming traffic, or both. If you do not specify a version or interface bindings, the ACL will automatically be for IPv4 traffic and have no interface bindings.

```
add acl
  name
  name version <ip | ip6>
  name outinterface if_name
  name ininterface if_name
```

Use the following command to create an association between an existing ACL rule and the specified logical interface. The interface binding is related to the flow direction. You can specify a logical interface for outgoing traffic, incoming traffic, or both.

```
set acl name
  outinterface if_name
  ininterface if_name
  disable <on | off>
```
Use the following command to remove the ACL from live configuration or to delete the association between an ACL rule and an interface. Specifying only the ACL name deletes the whole ACL and all interface associations, if they exist. To delete the interface association, specify a logical interface for outgoing traffic, incoming traffic, or both.

```
delete acl
   name
   name outinterface if_name
   name ininterface if_name
```

**Arguments**

- `acl name`: Specifies the name of the ACL. Use alphanumeric characters.
- `version <ip4 | ip6>`: Specifies the protocol version, either `ip` (IPv4) or `ip6` (IPv6). This parameter is optional.
- `outinterface if_name`: Specifies the output interface of the access list. Protocol support is checked against the interface. IPv4 is accepted on all interfaces unless the interface has the “IPv6 only” flag on.
- `ininterface if_name`: Specifies the input interface of the access list. Protocol support is checked against the interface. IPv4 is accepted on all interfaces unless the interface has the “IPv6 only” flag on.

Use the following command to activate or deactivate the ACL bypass mode. Turning the bypass on allows you to bypass all traffic control blocks (for example, the classifier, meter, and policer).

```
set acl name bypass <on | off>
```

**Arguments**

- `acl name`: Specifies the name of the ACL. Use alphanumeric characters.
- `bypass <on | off>`: Set the traffic control block bypass: on or off.
ACL Ruleset Commands

Use the following command to show information about all existing ACL rulesets.
show aclrules

**Note** - Every ACL has a default rule that is originally in position 1. When you use the `show` command, the default rule will be marked as such. You cannot delete the default rule. This rule can only accept “accept” and “drop” as its action values.

Use the following command to show information about a specific ACL ruleset.
show aclrule name

**Arguments**

<table>
<thead>
<tr>
<th>aclrule name</th>
<th>Specifies the name of the ACL for which to display ruleset information. Use alphanumeric characters.</th>
</tr>
</thead>
</table>

Use the following command to add an ACL ruleset for an existing ACL.
add aclrule name position integer | newrule

**Arguments**

<table>
<thead>
<tr>
<th>aclrule name</th>
<th>Specifies the name of the ACL where the new ruleset will be added. The ACL must already exist. Use alphanumeric characters.</th>
</tr>
</thead>
<tbody>
<tr>
<td>position integer</td>
<td>Specifies the ruleset position number within the ACL. Position number specifies ruleset priority within the ACL. The highest ruleset priority is position_num = 1.</td>
</tr>
<tr>
<td>newrule</td>
<td>Adds a new rule after the last rule.</td>
</tr>
</tbody>
</table>
Use the following command to set ACL ruleset for the specified ACL. The default ruleset, which is marked as “default” when you use the `show` command, can only accept or drop as the action value.

```
set aclrule name position integer
  netflow-meter <on | off>
  action
  <accept | drop | reject | prioritize | skip | pbr_table | bypass-fw | shape> srcaddr ip_address/netmask destaddr
  ip_address/netmask srcport <0–65535> destport <0–65535>
  protocol <any | tcp | udp | 0–255> tcp-estab <yes | no> tos
  <0x0–0xff> dsfield <none | 0x00–0xff> qspec <none | 0–7>
  aggrclass name
  new-position integer
```

**Arguments:**

- **aclrule name**: Specifies the name of the ACL. Use alphanumeric characters. The command checks the existence of the ACL.
- **position integer**: Specifies the ruleset position number within the ACL. The command checks the existence of the rule.
- **new-position integer**: Specifies the new position in the aclrule set for the aclrule.
- **aggrclass name**: Specifies the name of the aggregation class associated with this AclRule. Use alphanumeric characters.
- **netflow-meter <on | off>**: Specifies whether this rule should be used to define network flows, which are exported to a Netflow collector.
action <accept | drop | reject | prioritize | skip | shape | pbr-table | bypass-fw >

Specifies the action to take when the interface associate with the rule encounters a packet matching the rule. The default ruleset, which is marked as “default” when you use the `show` command, can only accept accept or drop as the action value.

The aggregation class must be configured when rule has priority action.

Actions are as follows:

- **accept** - Best effort queuing for packet.
- **drop** - No service for packet: the packet is dropped
- **reject** - No service for packet, similar to drop, but ICMP error packet is sent to the source.
- **prioritize** - See “Queue Class Commands” on page 422.
- **skip** - Skip the specified rule. It does not apply.
- **pbr** - Direct traffic to policy based routing table. See “Policy Based Routing Commands” on page 427.
- **ICMP traffic will not be sent to the firewall. Applies only to ICMP.**
- **shape** - Rate shaping. See “Aggregation Class Commands” on page 420.
### srcaddr

**ip_address/netmask**

Specifies the source IP address and netmask to be used for matching this rule.

#### IPv4

- **Range**: dotted-quad  
  0-255.0-255.0-255.0-255/0-32
- **Example**: 192.168.50.1/24
- **Default**: 0.0.0.0/0

#### IPv6

- **Range**: IPv6 prefix format/0-126
- **Example**: 2222::1:2:3:4/0
- **Default**: ::/0

*Note*: This should be an IPV6 prefix format, not an IPv6 address. Therefore, the prefix/mask 222::223/65 is not valid, while 222::223/0 and 222::/65 are valid.

### destaddr

**ip_address/netmask**

Specifies the destination IP address and netmask to be used for matching this rule.

#### IPv4

- **Range**: dotted-quad  
  0-255.0-255.0-255.0-255/0-32
- **Example**: 192.168.50.1/24
- **Default**: 0.0.0.0/0

#### IPv6

- **Range**: IPv6 prefix format/0-126
- **Example**: 2222::1:2:3:4/0
- **Default**: ::/0

*Note*: This should be an IPV6 prefix format, not an IPv6 address. Therefore, the prefix/mask 222::223/65 is not valid, while 222::223/0 and 222::/65 are valid.

### srcport <0–65535>

Specifies the source port number or port range. The default is the entire range, 0–65535.
Use the following `set` command to associate an ACL rule with the specified aggregation class. Use the `delete` command to disassociate an ACL rule with the specified aggregation class. For information on aggregation class commands, see “Aggregation Class Commands” on page 420.

```
set aclrule name position integer aggrclass name
delete aclrule name position integer aggrclass name
```

Use the following command to delete an ACL ruleset from the specified ACL.

```
delete aclrule name position integer
```
## Arguments

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>aclrule name</td>
<td>Specifies the name of the ACL. Use alphanumeric characters.</td>
</tr>
<tr>
<td>position integer</td>
<td>Specifies the ruleset position number within the ACL.</td>
</tr>
<tr>
<td>new-position integer</td>
<td>Specifies the new position in the aclrule set for the aclrule.</td>
</tr>
<tr>
<td>aggrclass name</td>
<td>Specifies the name of the aggregation class associated with this AclRule.</td>
</tr>
<tr>
<td></td>
<td>Use alphanumeric characters.</td>
</tr>
</tbody>
</table>
Aggregation Class Commands

An aggregation class provides the mechanism to meter traffic flows and shape or police them to a configurable rate. Use the commands in this section to create new or delete existing aggregation classes and to modify the mean rate or burstsize.

Set, Change, and View Aggregation Classes

Use the following command to show all existing aggregation classes.

```
show aggrclasses
```

Use the following command to show a specific aggregation class.

```
show aggrclass name
```

**Arguments**

<table>
<thead>
<tr>
<th>aggrclass name</th>
<th>Specifies the name of the aggregation class to display. Use alphanumeric characters.</th>
</tr>
</thead>
</table>

Use the following command to add an aggregation class together with its meanrate and burstsize.

```
add aggrclass name meanrate <10-10000000> burstsize <1500-150000>
```

Use the following command to set a new meanrate, burstsize or both meanrate and burstsize values for an existing aggregation class.

```
set aggrclass name
  meanrate <10-10000000>
  burstsize <1500-150000>
```

**Arguments**

<table>
<thead>
<tr>
<th>aggrclass name</th>
<th>Specifies the name of the aggregation class. Use alphanumeric characters.</th>
</tr>
</thead>
</table>

| meanrate <10-10000000> | Specifies the packet stream mean rate in kilobytes. Range 10-10000000 Kbps |

| burstsize <1500-150000> | Specifies the burst value of the packet stream in bytes. Range 1500 - 150000 bytes |
Use the following command to delete an existing aggregation class.

delete aggrclass name

**Arguments**

| aggrclass name | Specifies the name of the aggregation class to delete. Use alphanumeric characters. |
Queue Class Commands

Queue classes are used as templates for queue structures which can be associated with physical interfaces. You may configure items such as the depth of the queues, assign logical names to some of the queues, and set up a queue specifier.

Set, Change, and View Queue Classes

Use the following command to show all existing queue classes.
show qclasses

Use the following command to show a specific queue class.
show qclass name

Arguments

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>qclass name</td>
<td>Specifies the name of the queue class to display. Use alphanumeric characters.</td>
</tr>
</tbody>
</table>

Use the following command to add a queue class.
add qclass name

Arguments

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>qclass name</td>
<td>Specifies the name of the queue class to add. Use alphanumeric characters.</td>
</tr>
</tbody>
</table>

Use the following command to specify the scheduling algorithm for a queue class. The specified queue class must exist before you use this command.
set qclass name type <strict | wrr | cas>

Use the following commands to set values for one or multiple queue class properties. The specified queue class must exist before you use these commands. You can set the queue specifier and queue length in the same command, but you must use a separate command to set the logical name for the queue priority.
set qclass name priority <0–7>
  name name
  qspec <0–5>
  qlength <0–256>
  weight <0–8>
Set, Change, and View Queue Classes

dropper <tail | wred>
maxth value
minth value
const <1–16>
dr1 value
dr2 value
dr3 value

Arguments

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>qclass name</td>
<td>Specifies the name of the queue class. Use alphanumeric characters.</td>
</tr>
<tr>
<td>type &lt;strict</td>
<td>wrr</td>
</tr>
<tr>
<td></td>
<td>strict: strict priority</td>
</tr>
<tr>
<td></td>
<td>wrr: weighted round robin</td>
</tr>
<tr>
<td></td>
<td>cas: cascade</td>
</tr>
<tr>
<td>priority &lt;0–7&gt;</td>
<td>Specifies the strict priority of queue. A lower priority value has greater preference for service. Three priorities are reserved for Internetwork Control, Expedited Forwarding and Best Effort traffic, which are priorities 0, 1, and 7, respectively</td>
</tr>
<tr>
<td>name name</td>
<td>Specifies the logical name for a priority level. It is used to help identify the use of a queue.</td>
</tr>
</tbody>
</table>

- Format: Alphanumeric characters and underscore with no spaces
- Default: The default values for priority queues 2 to 6 are: Priority 2 - Q_priority_2 Priority 3 - Q_priority_3 Priority 4 - Q_priority_4 Priority 5 - Q_priority_5 Priority 6 - Q_priority_6
Set, Change, and View Queue Classes

<table>
<thead>
<tr>
<th>qscl</th>
<th>Description</th>
</tr>
</thead>
</table>
| qspec <0–5> | Queue specifier is used within the class as a logical identifier. Use the Queue Specifier with the classifier to direct traffic to a specific queue. The following specifiers are predefined:  
  - 7 - Internetwork Control  
  - 6 - Expedited Forwarding  
  - 0 - Best Effort  
  Identifiers 7, 6 and 0 are reserved for internetwork control, expedited forwarding and best effort respectively (RFC 791).  
  - Range 0-5  
  For queues 3 to 7 the default is 0 |
| qlength <0–256> | Specifies the maximum number of packets that may be queued before packets are dropped (range 10 - 256). A value of zero (0) is used to disable a queue. Neither the Internetwork Control nor the Best Effort queue can be disabled. The range is zero (0) through 256.  
  Varies based on use of queue for queues 3 to 7. For NetControl the default is 16, for Expedited Forwarding the default is 32, and for Best Effort the default is 64. |
| weight <0–8> | Specifies the weight for a queue, which configures the proportions in which the link capacity is to be divided among the queues. If you use WRR, you can assign weight values of 0-8. For cascade scheduling, queue 7 and queue 6 must be assigned strict priority (weight 0) and the weights for the remaining queues must be in descending order. You can configure adjacent queues to have identical weights, but the weight assigned to a given queue cannot be greater than that assigned to a queue with a greater queue specifier.  
  This option is not available if the scheduling algorithm is strict priority. |
| dropper <tail | wred> | Specifies the drop method: |
|------------|---------------------------------|
| • tail: Drop any packets that arrive for a queue after the queue is full. |
| • wred: Drop packets as configured by WRED options. |
| This option is not available if the scheduling algorithm is strict priority. |

<table>
<thead>
<tr>
<th>maxth value</th>
<th>Maximum threshold: If the average queue length is greater than or equal to this value, all arriving packets are dropped. Applies only to WRED.</th>
</tr>
</thead>
<tbody>
<tr>
<td>64</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>minth value</th>
<th>Minimum threshold: If the average queue length is less than or equal to this value, no packets are dropped. Applies only to WRED.</th>
</tr>
</thead>
<tbody>
<tr>
<td>32</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>const &lt;1–16&gt;</th>
<th>Specifies how adaptive WRED is to traffic bursts. Choosing a higher value creates a slower moving average, which has the benefit of reducing the variation in queue length (and therefore reducing packet drops caused by traffic bursts) but causes the system to react slower to congestion. Choosing a lower value allows the system to react faster to congestion but might result in packet drops caused by overreactions to temporary bursts in traffic. Applies only to WRED.</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>dr1 value</th>
<th>Drop rate for low precedence traffic. If the value is 1024, IPSO drops one packet after servicing approximately 1024 packets. Applies only to WRED.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1024</td>
<td></td>
</tr>
</tbody>
</table>
Set, Change, and View Queue Classes

Use the following command to associate a queue class with a given physical interface.

```
set qclass name interface if_name qmode
<disabled | maxthroughput | minlatency>
```

**Arguments**

- `qclass name` Specifies the name of the queue class. Use alphanumeric characters.
- `interface if_name` Specifies the name of the physical interface.
- `qmode <disabled | maxthroughput | minlatency>` Specifies the QoS queue mode for the interface. The options are: disabled, maximum throughput or minimal latency

Use the following command to delete a queue class.

```
delete qclass name
```

**Arguments**

- `qclass name` Specifies the name of the aggregation class to delete. Use alphanumeric characters.

Use the following command to view queue class statistics for interfaces associated with the queue class.

```
show qclass-statistics
```
Policy Based Routing Commands

This section describes command line interface commands you can use to configure policy based routing (PBR).

Use the following commands to create a PBR table.

```
add pbr table pbr_name
    network ip_address
    netmask mask_length
```

Use the following commands to configure PBR

```
set pbr table pbr_name
    default comment comment
    default nexthop gateway address ip_address
    default nexthop gateway logical unnumbered_if
    default nexthop-select multipath_type
    default nexthop-type type
    default route <on | off>
    network ip_address netmask mask_length comment comment
    network ip_address netmask mask_length nexthop gateway address ip_address
    network ip_address netmask mask_length nexthop gateway logical unnumbered_if
    network ip_address netmask mask_length nexthop-select multipath_type
    network ip_address netmask mask_length nexthop-type type
```

Use the following commands to delete a PBR configuration.

```
delete pbr table pbr_name
    default nexthop gateway address ip_address
    default nexthop gateway logical unnumbered_if
    network ip_address netmask mask_length nexthop gateway address ip_address
    network ip_address netmask mask_length nexthop gateway logical unnumbered_if
```
Use the following commands to show information on your PBR configuration.

```
show pbr table pbr_name
  default nexthop-select
  default nexthop-type
  default route
  network value netmask mask_length nexthop-select
  network value netmask mask_length nexthop-type
```

**Arguments**

- **pbr table pbr_name**
  Specifies the name of the table. Use alphanumeric characters.

- **network ip_address**
  Defines the IP address of a new static route. The static route should not have any host bits set, that is, there should be no bits in the address set beyond the specified mask length.
  Range: Dotted-quad (0-255. 0-255. 0-255. 0-255.)

  None

- **netmask mask_length**
  Defines the mask length for the new static route.
  Range: 0-32

  None

- **default comment comment**
  Specify a unique description about the PBR static route.

- **default nexthop gateway address ip_address**
  Gateway Address: Specifies the IP address of the gateway to which packets for this PBR static route are sent. The address must be the address of a router that is directly connected to the system you are configuring.
  Range: Dotted-quad (0-255. 0-255. 0-255. 0-255.)

  None

- **default nexthop gateway logical unnumber_if**
  Gateway Logical: Specifies an unnumbered interface as the next hop gateway.
ATM QoS

Asynchronous transfer mode (ATM) quality of service (QoS) descriptor configuration describes the traffic parameters for ATM virtual channels (VCs). The QoS configuration for an ATM VC is done by associating the VC with an ATM QoS descriptor.

<table>
<thead>
<tr>
<th><strong>default nexthop-select</strong></th>
<th>multipath_type</th>
<th>This option is only available if the next hop type is Multipath. The following are the options:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>• None: Traffic is dropped. Use this option to prevent this route from being used.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• scrdsthash: The system chooses the outgoing interface based on a hash of the source and destination addresses.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• srchash: The system chooses the outgoing interface based on a hash of the source address.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• dsthash: The system chooses the outgoing interface based on a hash of the destination address.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• roundrobin: The system chooses the outgoing interface based on a round robin method.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>default nexthop-type</strong></th>
<th>type</th>
<th>Specifies the next hop type for the static route. The following are the types:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Normal</td>
<td>• Normal</td>
</tr>
<tr>
<td></td>
<td>Reject</td>
<td>• Reject</td>
</tr>
<tr>
<td></td>
<td>Blackhole</td>
<td>• Blackhole</td>
</tr>
<tr>
<td></td>
<td>Multipath</td>
<td>• Multipath</td>
</tr>
</tbody>
</table>

| **default route**           | <on | off> | On enables the configured policy based static route. Off disables the static route.          |
ATM QoS descriptors belong to one of two categories: unspecified bit rate (UBR) or constant bit rate (CBR). The UBR does not have any QoS guarantees and is the default category used for an ATM VC in the absence of any explicit QoS descriptor association. The CBR does have some QoS guarantee. The CBR limits the maximum cell output rate to adhere to the requirements on CBR traffic that the network imposes. Use the commands in this section to:

- Add, delete, or show ATM QoS descriptors
- Add, delete, or show association of ATM QoS descriptors with ATM VCs
- Show available or reserved bandwidth on an ATM interface

### Configuring ATM QoS Descriptors

Use the following command to add an ATM QoS descriptor with a specified peak cell rate:

```plaintext
add atmqos qosd name pcr <64–146000>
```

Use the following command to delete the specified ATM QoS descriptor:

```plaintext
delete atmqos qosd name
```

Use the following command to show all ATM QoS descriptors:

```plaintext
show atmqos qosd
```

**Arguments**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>qosd name</td>
<td>Specifies the name of the ATM QoS descriptor. The category for any descriptor you create is CBR.</td>
</tr>
<tr>
<td>pcr &lt;64–146000&gt;</td>
<td>Specifies the maximum cell rate, in kilobits per second, used in the output direction on a CBR channel. Peak cell rate is rounded down to a multiple of 64 kbps. One cell per second corresponds to 424 bits per second.</td>
</tr>
</tbody>
</table>

Use the following command to associate an ATM QoS descriptor with an ATM VC on the specified physical interface:
set atmqos interface if_name vc integer qosd name

Use the following command to delete the association of an ATM QoS descriptor with a VC on the specified physical ATM interface:

delete atmqos interface if_name vc <vpc/vci | vci>

Arguments

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface if_name</td>
<td>Specifies the name of the ATM physical interface on which the VC is riding. Example: atm-s3p1</td>
</tr>
<tr>
<td>vc &lt;vpc/vci</td>
<td>vci&gt;</td>
</tr>
<tr>
<td>qosd name</td>
<td>Specifies the name of the ATM QoS descriptor to associate with the VC.</td>
</tr>
</tbody>
</table>

Use the following commands to show all ATM QoS descriptor and VC associations on the specified physical ATM interface:

show atmqos interface if_name settings

Use the following command to show available or reserved bandwidth on the specified physical ATM interface:

show atmqos interface if_name bandwidth  
<available | reserved>
DSCP to VLAN Priority Commands

Differentiated Services Code Point (DSCP) to virtual LAN (VLAN) priority mapping allows you to utilize fixed class of service (CoS) values on your network. You can map the DSCP of the IP and IPv6 packets to VLAN priority tags in the egress (outgoing) direction. In the ingress (incoming) direction, no mapping occurs from VLAN priority tags to DSCPs.

You can enable and disable mapping by using CLI commands, but you cannot configure the DSCP to VLAN priority values. The DSCP values correspond to the following CoS values:

- DSCP 0–7 = CoS 0
- DSCP 8–15 = CoS 1
- DSCP 16–23 = CoS 2
- DSCP 24–31 = CoS 3
- DSCP 32–39 = CoS 4
- DSCP 40–47 = CoS 5
- DSCP 48–55 = CoS 6
- DSCP 56–63 = CoS 7

When you enable mapping, it is done similarly for each Ethernet frame that has a VLAN tag, regardless of the VLAN ID.

Configuring DSCP to VLAN Mapping

Use the following command to enable or disable mapping of DSCP to VLAN priority service to this system.

```
set custom dscp-to-vlanprio <on | off>
```

Use the following command to show the status of mapping between VLAN priority and DSCP service on this system.

```
show custom dscp-to-vlanprio
```
You can use the Netflow support in IPSO to collect information about network traffic patterns and volume. To provide this information, IPSO tracks network “flows.” A flow is a unidirectional stream of packets that share a given set of characteristics. Use the following commands to configure Netflow services.

```
set netflow
  active-timeout seconds
  collector ip ip_address port port_number
  enable-acl <on | off>
  enable-flows <on | off>
  export-format <Netflow_V5 | Netflow_V9 | None>
  inactive-timeout seconds
  srcaddr ip_address
show netflow
  all
  active-timeout
  collector
  enable-acl
  enable-flows
  export-format
  inactive-timeout
  srcaddr
```

**Arguments**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>active-timeout seconds</td>
<td>Specifies the number of seconds after which IPSO should export a record for a flow when the flow is still active.</td>
</tr>
<tr>
<td>collector ip ip_address port port_number</td>
<td>Specifies the IP address and port number of the Netflow collector.</td>
</tr>
<tr>
<td>enable-acl &lt;on</td>
<td>off&gt;</td>
</tr>
</tbody>
</table>
enable-flows
<on | off>
Enables or disables flow metering mode. If you use this mode, a flow is any sequence of packets that share
• Source and destination IP addresses
• Source and destination port numbers
• IP protocol
IPSO exports each flow in an individual flow record.

export-format
<Netflow_V5 | Netflow_V9 | None>
Specifies the format of the export flow records. This format must be supported by the collector.

inactive-timeout
seconds
Specifies the number of seconds to wait while a flow is inactive (no traffic) but has not been terminated. If the specified number of seconds elapses, IPSO exports a record for the flow.

srcaddr ip_address
Specifies the source (local) IP address to be used in export records. If this is not configured, the address is chosen based on the route to the collector’s address.
Chapter 11

Monitoring Commands

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

If you use Tab command completion for certain monitoring commands, you see relative listed as a possible option. Do not use this option. It is used internally when an IPSO cluster is present to allow Cluster Voyager to display aggregated data for the cluster.

Current and Historical Network Reports  page 436
Useful System Information  page 442
Displaying Hardware Monitors  page 449
Current and Historical Network Reports

Use the commands in the following sections to configure various system reports.

Saving Reports to Files

You can save system reports to files and specify a delimiter to separate fields in the reports. For example, to create a memory utilization report and download it to a file, you could use the following command:

```
show monitor summary hourly memoryutilization delimiter <, | ; | Tab> filename name
```

Report files are saved in the directory /var/log/monitor.

Configuring How Much Data is Stored

Use the following commands to configure and see how much historical data is collected on the system:

```
set monitor config maxhour <24-167>
show monitor config maxhour
```

Arguments

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>maxhour &lt;24-167&gt;</td>
<td>Specifies how many hours worth of collected data is stored on the system. Data that is older than the specified number of hours is deleted. This option controls how much data is available when you use the <code>starttime/endtime</code> form of the <code>show monitor</code> commands. It does not affect how much data is available when you use the <code>summary</code> form of the <code>show monitor</code> commands. Check Point recommends that you set this option to 24 hours on diskless systems to avoid exhausting the available storage space.</td>
</tr>
</tbody>
</table>

Configuring CPU Utilization Reports

Use the following commands to turn data collection on or off and to set the data collection time interval.

```
set monitor config
```
Configuring Memory Utilization Reports

Use the following commands to turn data collection on or off and to set the data collection time interval.
set monitor config
   maxhour
      memoryutilization state <on | off>
      memoryutilization interval <60-2100000>

Use the following commands to view whether data collection is on or off and the data collection time interval.
show monitor config
   maxhour
      memoryutilization state
      memoryutilization interval

Use the following command to specify a start time and an end time for the memory utilization report.
show monitor
   start time <date time year> endtime <date time year>
   memoryutilization

Configuring Memory Utilization Reports

Use the following commands to view whether data collection is on or off and the data collection time interval.
show monitor config
   cpuutilization state
   cpuutilization interval <60-2100000>

Use the following command to specify a start time and an end time for the CPU utilization report.
show monitor
   starttime <date time year> endtime <date time year>
   cpuutilization
   summary <hourly | daily | weekly | monthly> cpuutilization
Configuring Interface Linkstate Reports

summary <hourly | daily | weekly | monthly>
memoryutilization

Arguments

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>state &lt;on</td>
<td>off&gt;</td>
</tr>
<tr>
<td>interval &lt;60-2100000&gt;</td>
<td>Specifies the data collection time in seconds.</td>
</tr>
<tr>
<td>starttime &lt;date time year&gt;</td>
<td>Specifies the start time for a data collection report. You must enter the date, time and year between quotes. The following is an example of how you enter the date: “Oct 27 02:21:55 2001”</td>
</tr>
</tbody>
</table>

Configuring Interface Linkstate Reports

Use the following commands to turn date collection on or off and to set the data collection time interval.

set monitor config
    linkstate state <on | off>
    linkstate interval <60-2100000 seconds>

Use the following commands to view whether data collection is on or off and the data collection time interval.

show monitor config
    linkstate state
    linkstate interval

Use the following command to specify a linkstate report start time and end time for a given interface.

show monitor
    starttime <date time year> endtime <date time year>
    linkstate interface-type <logical | physical>
    interface <name>

Use the following command to view the state of a given interface over a specified period of time.
### Configuring Rate Shaping Bandwidth Reports

Use the following commands to turn data collection on or off and to set the data collection time interval.

```
set monitor config
  rateshape type <bytesdelayed | packetdelayed> state <on | off>
  rateshape interval <60-2100000 seconds>
```

Use the following commands to view whether data collection is on or off and the data collection time interval.

```
show monitor config
  rateshape type <bytesdelayed | packetdelayed> state
  rateshape interval
```

Use the following command to specify a rate shaping bandwidth report start time and end time for a given rate shape data and aggregation class.

```
show monitor starttime <date time year> endtime <date time year>
  rateshape type <bytesdelayed | packetdelayed>
  aggregate <name>
```

Use the following command to view rate shaping data over a specified period of time.

```
show monitor summary <hourly | daily | weekly | monthly>
  rateshape type <bytesdelayed | packetdelayed>
  aggregate <name>
```

### Configuring Interface Throughput Reports

Use the following commands to turn date collection on or off and to set the data collection time interval.

```
set monitor config
  throughput type <bytes | packets | multicast | broadcast> state <on | off>
  throughput interval <60-2100000 seconds>
```
Use the following commands to view whether data collection is on or off and the data collection time interval.

```
show monitor config
    throughput type <bytes | packets | multicast | broadcast>
    state

    throughput interval
```

Use the following command to specify a interface throughput report start time and end time for a given interface.

```
show monitor starttime <date time year> endtime <date time year>
    throughput type <bytes | packets | multicast | broadcast>
    interface-type <logical | physical> interface <name> network <ip_address>
```

Use the following command to view the state of a given interface over a specified period.

```
show monitor summary <hourly | daily | weekly | monthly>
    throughput type <bytes | packets | multicast | broadcast>
    interface-type <logical | physical> interface <name>
```

**Arguments**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>aggregate &lt;name&gt;</td>
<td>Specifies information for a given aggregation class. The name is case-sensitive.</td>
</tr>
<tr>
<td>endtime &lt;date time year&gt;</td>
<td>Specifies the start time for a data collection report. You must enter the date, time and year between quotes. The following is an example of how you enter the date: “Oct 27 02:21:55 2001”</td>
</tr>
<tr>
<td>interface &lt;name&gt;</td>
<td>Specifies the name of a given interface of which you want to collect data.</td>
</tr>
<tr>
<td>interface-type &lt;logical</td>
<td>physical&gt;</td>
</tr>
<tr>
<td>interval &lt;60-2100000&gt;</td>
<td>Specifies the data collection time in seconds.</td>
</tr>
<tr>
<td>rateshape type &lt;bytesdelayed</td>
<td>packetdelayed&gt;</td>
</tr>
<tr>
<td>state &lt;on</td>
<td>off&gt;</td>
</tr>
</tbody>
</table>

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>state</td>
<td>on</td>
</tr>
</tbody>
</table>
### Configuring Interface Throughput Reports

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>starttime &lt;date time year&gt;</code></td>
<td>Specifies the start time for a data collection report. You must enter the date, time and year between quotes. The following is an example of how you enter the date: “Oct 27 02:21:55 2001”</td>
</tr>
<tr>
<td><code>throughput type</code></td>
<td>Specifies the type of data that you want to collect.</td>
</tr>
<tr>
<td>`&lt;bytes</td>
<td>packets</td>
</tr>
</tbody>
</table>

**Table:**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>starttime &lt;date time year&gt;</code></td>
<td>Specifies the start time for a data collection report. You must enter the date, time and year between quotes. The following is an example of how you enter the date: “Oct 27 02:21:55 2001”</td>
</tr>
<tr>
<td><code>throughput type</code></td>
<td>Specifies the type of data that you want to collect.</td>
</tr>
<tr>
<td>`&lt;bytes</td>
<td>packets</td>
</tr>
</tbody>
</table>
Useful System Information

Use the following commands to view various information about your system.

Displaying Useful System Statistics

Use the following commands to display useful system statistics.
show useful-stats

The useful system statistics summarize configuration information such as the following:
• The number of configured active routes
• The number of forwarded packets
• The number of configured VRRP masters
• The percentage of real memory in use
• The percentage of system disk space used on the system

Displaying Interface Settings

Use the following command to display interface settings.
show interfacemonitor

Arguments

| interfacemonitor | Displays the interface settings. |

Displaying System Logs

Use the following commands to display system logs.
show

logging
logininfo all
logininfo user
log auditlog
log httpd-access-log
log httpd-error-log
### Displaying System Logs

**log messagelog**

*type name date name keyword name case-sensitive include-zipped name*

#### Arguments

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>logging</td>
<td>Displays the system log configuration.</td>
</tr>
<tr>
<td>logininfo all</td>
<td>Displays the login/logout activity for all users.</td>
</tr>
<tr>
<td>logininfo name</td>
<td>Displays the login/logout activity for the named user.</td>
</tr>
<tr>
<td>log auditlog</td>
<td>Displays a log that shows configuration changes made by users.</td>
</tr>
<tr>
<td>log httpd-access-log</td>
<td>Displays the httpd_access_log generated by the web-server, which shows access to the platform made through the web server. The information includes the client IP address, time of access, and page accessed.</td>
</tr>
<tr>
<td>log httpd-error-log</td>
<td>Displays the log file generated by the web server showing errors that the web server detects.</td>
</tr>
<tr>
<td>log messagelog</td>
<td>Displays the complete system-wide log messages or a search can be performed based on type of log messages, log dates a particular keyword etc. Searches can case-sensitive or case-insensitive. Archived log files can be included in the search.</td>
</tr>
</tbody>
</table>
Displaying Interface Traffic and Error Statistics

Use the following commands to display interface traffic statistics.

show iftrafficstats

<table>
<thead>
<tr>
<th>type name</th>
<th>date name</th>
<th>keyword name</th>
<th>case-sensitive</th>
<th>include-zipped name</th>
</tr>
</thead>
</table>

Specifies the type of log messages to be displayed. The type is the severity of the log message, from least severe to most severe, and can be specified by one of the following keywords:

- emerg
- alert
- crit
- error
- warning
- notice
- info
- debug

To include all kinds of log message either specify the keyword "all" or skip this part of the command.

If date is specified only messages matching that date are displayed. The date is specified in one of the following forms: Oct or "Oct 12" that is, short form of month or a combination of month and date. Date cannot be specified without specifying a month.

Enter a keyword to search for in the system-wide log file. By default the search is case-insensitive. To do a case-sensitive search, specify the word "case-sensitive" in the command.

Enter a list of comma-separated zipped files to be included in the search, or just specify the keyword "all" to include all available zipped files. If a list is specified it should be of the form: messages.1.gz,messages.0.gz,messages.2.gz No spaces are allowed in the list.
The interface traffic statistics contains information about the state of the device represented by the physical and logical interface.

Physical interface information includes the following:
- Physical, which is the name of the physical interface
- Up, which shows the running state of the physical interface
- InBytes, which is the input bytes counter for the physical interface
- OutBytes, which is the output bytes counter for the physical interface
- InErrs, which is the input error counter for the physical interface
- OutErrs, which is the output error counter for the physical interface

Logical interface information includes the following:
- Logical, which is the name of the logical interface
- Active, which is the logical interface administrative status
- Up, which is the running state of the logical interface
- Type, which is the type of device or virtual circuit accessed through the logical interface (for example, Ethernet, ATM, FDDI).
- InBytes, which is the input bytes counter for the logical interface.
- OutBytes, which is the output bytes counter for the logical interface.

Use the following commands to display interface input error counters:
```
show interface phys_if_name statistics
```

The output of this command displays counters for the following errors:
- RxError: Counts the number of packets received in which I_RX_ER was asserted by the PHY.
- RxNoBuffer: Counts the number of times that frames were received when there were no available buffers in host memory to store those frames (receive descriptor head and tail pointers were equal). The packets are still received if there is space in the FIFO.
- CarrierExtnError: Counts the number of packets received in which the carrier extension error was signaled across the internal PHY interface. The PHY propagates carrier extension errors to the MAC when an error is detected during the carrier extended time of a packet reception.
- LengthError: Counts receive length error events. A length error occurs if an incoming packet passes the filter criteria but is undersized or oversized.
Displaying the Interface Monitor

Use the following commands to display the interface monitor.

```
show interfacemonitor
```

The interface monitor provides information such as the following:

- Interface name
- Status (up or down)
- Logical name
- State (multiple conditions where present)
- Maximum transmission Unit (MTU)
- Up to down transitions

Displaying Resource Statistics

Use the following commands to display resource statistics.

```
show resource-statistics
```

Resource statistics include the following:

- Total uptime
- Total user time
- Total system time
- Major page faults
- Minor page faults
- File system writes
- File system reads
- Message writes
- Message reads
Displaying the Forwarding Table

Use the following commands to display the forwarding table.

```
show forwarding-table
```

Note - The `show forwarding-table` command displays only the default instance forwarding table.

Forwarding table information includes the following:

- **Destination**, which is the destination host or network
- **Gateway**, which is the IP address or the interface name of the outgoing interface that is the next-hop device through which packets should be routed
- **Flags**, which is information about the route stored as binary choices. The mapping between codes and flags is as follows:

<table>
<thead>
<tr>
<th>Code</th>
<th>Flag</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>RTF_PROTO1: Protocol specific routing flag 1</td>
</tr>
<tr>
<td>2</td>
<td>RTF_PROTO2: Protocol specific routing flag 2</td>
</tr>
<tr>
<td>3</td>
<td>RTF_PROTO3: Protocol specific routing flag 3</td>
</tr>
<tr>
<td>B</td>
<td>RTF_BLACKHOLE: Just discard packets during updates</td>
</tr>
<tr>
<td>C</td>
<td>RTF_CLONING: Generate new routes on use</td>
</tr>
<tr>
<td>C</td>
<td>RTF_PRCLONING: Protocol-specified generate new routes on use</td>
</tr>
<tr>
<td>D</td>
<td>RTF_DYNAMIC: Created dynamically by redirect</td>
</tr>
<tr>
<td>G</td>
<td>RTF_GATEWAY: Destination requires forwarding by intermediary</td>
</tr>
<tr>
<td>H</td>
<td>RTF_HOST: Host entry net otherwise</td>
</tr>
<tr>
<td>L</td>
<td>RTF_LLINFO: Valid protocol to link address translation</td>
</tr>
<tr>
<td>M</td>
<td>RTF_MODIFIED: Modified dynamically by redirect</td>
</tr>
<tr>
<td>R</td>
<td>RTF_REJECT: Host or net unreachable</td>
</tr>
</tbody>
</table>

- Signals received
- Total swaps
- Voluntary context switches
- Involuntary context switches
Displaying the Forwarding Table

- **S**  RTF_Static: Manually added
- **U**  RTF_Up: Route usable
- **W**  RTF_WASCLONED: Route was generated as a result of cloning
- **X**  RTF_XRESOLVE: External daemon translates proto to link address

- Netif, which is the name of the local interface
Displaying Hardware Monitors

The commands described in this section display the status for various system components. Components for which the status can be displayed include temperature sensors, watchdog timers, voltage sensors, power supplies, and fan sensors. The command returns status only for installed components.

Use the following commands to display all system status information.
show sysenv all

Displaying a Temperature Sensor Information

Use the following commands to display temperature sensor information.
show sysenv temperature
   all
   sensor sensor-number
   <all | location | status | current | limit | hysteresis>

Temperature sensor information includes the following:

- Location
- Status
- Current value
- Temp limit
- Temp hysteresis

Arguments

| all |
| Displays information about all of the temperature sensors. |
Displaying a Watchdog Timer Information

Use the following commands to display watchdog timer information.

```
show sysenv watchdog-timer
<all | status | mode | tickles | last-reboot>
```

Watchdog timers track a specific amount of time. If that time runs out before an expected event occurs, some action, such as a reboot or an error-message generation, is triggered.

Watchdog timer information includes the following:

- Present
- Status
- Mode
- Tickles
- Last reboot

**Arguments**

```
all  Displays all watchdog timer information.
status  Displays the watchdog timer status.
```
Displaying Voltage Sensor Information

Use the following commands to display voltage sensor information.

```
show sysenv voltage
  all
  sensor sensor-number
  <all | location | status | nominal | measured | error | lo\n  -limit | hi-limit>
```

Voltage sensor information includes the following:

- Location
- Status
- Nominal
- Measured
- Error
- Low Limit
- High Limit

Arguments

| all         | Displays all voltage sensor information. |
Displaying Power Supply Information

Use the following commands to display power supply information.

```
show sysenv power-supply
    all
        id pwr-supply-id
            <all | present | volts | amps | status | revision>
```

Power supply information includes the following:

- Present (yes or no)
- Volts
- Amps
- Status (for example, OK)
- Revision
Displaying Fan Sensor Information

Use the following commands to display fan sensor information.

show sysenv fan
  all
  id pwr-supply-id <all | present | volts | amps | status | revision>

Arguments

- all: Displays all voltage sensor information.
- id pwr-supply-id <all | present | volts | amps | status | revision>: all displays all information about the power supply specified by pwr-supply-id. present indicates whether or not the power supply specified by pwr-supply-id is present. volts displays voltage information for the power supply specified by pwr-supply-id. amps displays amperage information for the power supply specified by pwr-supply-id. status displays status information (for example, OK) for the power supply specified by pwr-supply-id. revision displays the revision for the power supply specified by pwr-supply-id.

Fan sensor information includes the following:
- Location (for example, lm79_FAN1)
- Status (for example, Normal)
- Current Value
- Normal Value
Displaying a Network Interface Card Slot Status

Use the following command to display the network interface card (NIC) slot status for each slot in the system.

```
show sysenv slot-status
```

Network interface card slot status information includes the following:

- State (for example, empty or online)
- Driver
- ID (for example, DEC_21152)
Index

A

AAA 244
  Account Profiles, Configuring 250
  Authentication Profiles, Configuring 247
  Configuration, Viewing 244
  Radius 253
  Service Modules, Configuring 244
  Service Profiles, Configuring 245
  Session Profiles, Configuring 251
  TACAS+ 255
Access Control Lists 412
Access Control, SSH Server 258
Access, IPv6 217
Access, Network 219
Account Profiles, AAA 250
ACL
  Bypass Mode 413
  Node 412
  Rule and Aggregation Class, Associating 418
  Ruleset 414
  Viewing 412
  add instance instance_name 304
Aggregation Class 420
  Configuring 420
  Viewing 420
Aggregation, Routes 368
Alert, System Failure 103
All 209
Area Backbone, OSPF 332
Areas, OSPF 324
ARP 38
  Proxy, Adding 39
ATM
  Configuring Interfaces 41
  ATM QoS
    Descriptors 429
    Viewing 431
Authentication Profiles, AAA 247
  Authorized Keys, SSH 267
B
Backup
  Monitoring and Troubleshooting 96
Backup Files 88
  Transferring to a Remote Server 92
Backups
  Manual 88
  Scheduling 89
Bandwidth, Rate Shaping 439
Banner message 76
BGP 305
  Communities 323
  Confederations 312
  External 306
  Internal 316
  Route Dampening 314
  Route Reflection 313
  Trace 394
  Viewing Configurations 323
BOOTP 371
  Interfaces 371
  Monitoring and Troubleshooting 371
C
Certificates
  IPsec 230
  SSL 272
Certificates, SSL 270
CLI
  Editing 25
  Environment, Configuring 16
  Features 20
  Formats, Output 18
  Inactivity timeout 27
  Invoking 14
  Mode, Transaction 18
  Modes 14
  Movement 25
  Operations 20
  Clock, Setting 127
Cluster
  Commands 160
  Configuring an Existing Cluster 161
  Creating 160
  Installing Images 174
  IP-Pool 160
  Join-Time Shared Features 173
  Join-Time Shared Features, Configuring 173
  Reboot 174
  Shared Features 173
  Viewing 169
  VPN-Tunnel 160
Command
  Completion 21
  Default Values 23
  Executing Previous 24
  Expanding 21
  Help 24
  Loading from a File 29
  Recall 24
  Reusing 25
  Command File 29
  Commit 18
  Communities, BGP 323
  Confederations, BGP 312
Configuration
  Copy Running to Startup 113
  Load 113
  Save 31
Configuration Files
  Managing Sets 113
  Saving 113
  Viewing 113
  Configuration Locks, Setting 27
  Copy Configurations 113
  core files
X509 Certificate
Request 233
IPSO Images
Booting Options 109
Deleting 109
Downloading 111
Managing 109
Viewing 109
IPSO Shell, Options 15
Ipsrd 405
IPv6
Commands 193
Configuration Summary 194
Host Name
   Configuration 216
ICMP Interfaces 205
ICMP Router Discovery 205
ICMP Router Discovery,
   Monitoring 209
Interface, Configuring 195
Monitored Circuit 213
Neighbor Discovery
   Protocol 197
Network Access And
   Services 217
RIPng 201
RIPng, Monitoring and
   Troubleshooting 201
Route Aggregation 202
Routing Configuration 201
Routing Summary 215
Static Routes 203
Tunnels 66
VRRP for IPv6 209
VRRP, All
   Implementations 209
VRRPv3 210
IPv6 Over IPv4, Configuring 200
IPv6 To Ipv4, Configuring 199

K
Kernel, Trace 401
Keys, User Identity 266

L
LDAP, IPsec 242
Licenses 224
Link Aggregation 52
Linkstate Reports 438
Load Sharing 390
Loading Commands 29
Local Server, Restore Files 94
Logging, System 116
Logical Interface, Deleting 35
Login, SSH 260
Logs, System 442
Loopback
   Interfaces 64
   Logical Interfaces 64
   Physical Interfaces 65

M
Mail Relay, Configuring 115
Memory Utilization, Reports 437
Memory, Viewing 28
Messages
   banner 76
   FTP welcome 76
   MOTD 76
MFC
   Commands, Viewing
   Information 408
   Trace 397
Modem Interfaces 70
Monitored 213
Monitoring 435
MOTD 76

N
Network Access 220
Network Access, IPv6 217
Network Interface Card,
   Status 454
Network Security And
   Access 219
Network Services 217, 220
Network Time Protocol 385
Network Time Protocol,
   Configuring 137
NIC Slot, Status 454
Notification, Failure 103
NTP
   Adding a Server 385
   Configuring 137
   Deleting a Server 385
   Monitoring and
   Troubleshooting 386

O
Operations, CLI 20
OSPF 324
   area commands 324
   Areas 324
   Global Settings 334
   interfaces commands 327
   Monitoring and
   Troubleshooting 336
   Trace 401
   Virtual Links 332
Output Formats 18
Output Screen, Exiting 26

P
Package 141
   Adding 142
   Deleting 143
   Upgrade 142
Passwords
   Changing Admin and Monitor
   Passwords 282
   Configuring Policies 273
   Password Controls
   Commands 273
PIM 356
   Interfaces 356
   IP Clustering 356
Monitoring and Troubleshooting 364
Sparse Mode 356
Timer And Assert Rank Parameters 358
Trace 398
Policy, IPsec 235
Power Supply 452
Private Keys, SSL 272
Processes, Viewing 28
Proposal, IPsec 226
Protocol Rank 391
Proxy ARP 38

Q
Queue Class 422
Configuring 422
Statistics 426

R
Radius, Configuring 253
Rank, Protocol 391
Rate Shaping Bandwidth Reports 439
Reboot, IPSO 109
Recall, Command 24
Related Commands, Displaying 22
Remote Server, Restore Files 95
Remote Server, Transferring Files 92
Reports
Configuring Amount of Data 436
CPU Utilization 436
Interface Linkstate 438
Interface Throughput 439
Memory Utilization 437
Rate Shaping Bandwidth 439
Resource Statistics 446
Restore Files 88
Restore Files, Locally Stored 94
Reusing Commands 25
RIP 343
Interfaces 343
Monitoring and Troubleshooting 345
Trace 399
RIPng
IPv6 201
IPv6 Interfaces 201
Rollback 18
Route Aggregation 368
IPv6 202
Route Summary, Show 403
Router Discovery Protocol 380
Routes, Static 377
Routing 287
Routing Daemon 405
Routing Summary, IPv6 215
Routing, Miscellaneous Commands 390
Rule, IPsec 237
S
S/Key, Configuring 283
Saving Configuration Changes 31
Scheduling Jobs 100
Security, Network 219
Server Authentication Of Users 259
Services, IPv6 217
Session Profiles, AAA 251
Shell Options 15
SNMP
Check Point Implementation 178
Commands 177
Configuring 179
Enabling and Disabling 181
Traps, Enabling And Disabling 184
Viewing Implementation And Traps 188
SNMPv3
Usm Users 187
Sparse Mode PIM 356
SSH 258
Authorized Keys 267
Configuring Server Options 258
Host Keys 265
Key Pairs 265
Login Environment 260
Service Details, Configuring 263
Service, Enabling and Disabling 258
User Identity Keys 266
SSH Server
Access Control 258
Authentication 259
Implementation 264
Protocol Details 261
SSL
Private Key and Certificate 270
Voyager Web Access 269
Static ARP 38
Static Host Address Assignment 106
Static Routes 377
Static Routes, IPv6 203
Statistics
Interface 444
Interface Traffic 444
Resource 446
System 442
Statistics, System 35
Status 35
Swapping, Viewing Memory 28
System Configuration 73
Summary 75
System Environment, Viewing 449
System Failure Notification 103
System Health 442
System Logging, Configuring 116
System Logs, Viewing 442
System Monitoring 435
System Statistics 35, 442
System Status 35
System Tuning 144
T
Tab Key 21
TACAS+, AAA 255
TCP/IP Stack, Tuning 144
TELNET
Access 220
IPv6 Access 217
Temperature Sensor 449
Test Boot, IPSO 109
TFTP
  Access 220
  IPv6 Access 217
Throughput Reports 439
Time, Configuring 127
Trace Routing 393
Trace, Global Options 400
Traffic Management 411
Traffic Statistics 444
Transaction Mode 18
  transaction mode
    CLI commands 18
  Transparent Mode 49
  Tune, TCP/IP Stack 144
Tunnels 35
  IPv6 66

W
Watchdog Timer 450

X
X509 Certificate Request 233
X509 Certificate, IPsec 230

U
Upgrading Packages 142
User Identity Keys 266
User Management 273
Users
  System 278

V
Virtual Links, OSPF 332
Voltage Sensor 451
Voyager SSL Certificate 270
Voyager Web Access, SSL 269
VPN Accelerator
  Configuring 286
  Displaying Information 286
  Set 286
VRRP 380
  Monitored Circuit, Full 153
  Monitored Circuit,
    Legacy 380
  Monitored Circuit,
    Simplified 151